# Développements pour l'agrégation

David Michel

2016-2017

## Table des matières

# Première partie
# Algèbre et Géométrie

## 1 Algorithme de Berlekamp

V. Beck, J. Malick, G. Peyré, *Objectif Agrégation*, 2e édition, H&K. Théorème 5.36 page 245

Recasage : 121, 122, 123, 141

**Algorithme :** On considère un polynôme $P \in \mathbb{F}_q[X]$ sans facteur carré.

– On note $S_P$ l'endomorphisme d'élévation à la puissance $q$ dans l'anneau $\mathbb{F}_q[X]/(P)$. Calculer $r = \deg(P) - \mathrm{rg}(S_p - \mathrm{Id})$.

– Si $r > 1$
  ⋆ Calculer $V \in \mathbb{F}_q[X]$ tel que $V \bmod P$ n'est pas contant et $V \bmod P \in \mathrm{Ker}(S_P - \mathrm{Id})$.
  ⋆ Calculer $\mathrm{pgcd}(P, V - \alpha)$ pour $\alpha \in \mathbb{F}_q$.
  ⋆ Appliquer l'algorithme aux $\mathrm{pgcd}(P, V - \alpha)$ non triviaux.

– Si $r = 1$, alors $P$ est irréductible.

▷ Montrons qu'on obtient ainsi la décomposition en facteurs irréductibles de $P \in \mathbb{F}_q[X]$ sans facteur carré. Notons $P = P_1 \cdots P_r$ avec $P_1, \dots, P_r$ irréductibles deux à deux premiers entre eux.

– *Étape 1 : Calcul de $r$.* D'après le théorème chinois, on dispose d'un isomorphisme

$$\varphi : \mathbb{F}_q[X]/(P) \longrightarrow K_1 \times \cdots \times K_r$$

où $\forall i \in [\![1, r]\!]$, $K_i = \mathbb{F}_q[X]/(P_i)$ est un corps. Posons $\widetilde{S_P} = \varphi \circ S_P \circ \varphi^{-1}$. Alors

$$\widetilde{S_P}(x) = \varphi((\varphi^{-1}(x))^q) = \big(\varphi(\varphi^{-1}(x))\big)^q = x^q$$

et

$$\begin{aligned}(x_1, \dots, x_r) \in \mathrm{Ker}(\widetilde{S_P} - \mathrm{Id}) &\iff \forall i \in [\![1, r]\!],\ x_i^q = x_i \text{ dans } K_i \\ &\iff \forall i \in [\![1, r]\!],\ x_i \in \mathbb{F}_q \hookrightarrow K_i.\end{aligned}$$

En effet, les éléments de $\mathbb{F}_q \hookrightarrow K_i$ sont $q$ racines du polynôme $X^q - X$ sur $K_i$. Comme $K_i$ est un corps et $\deg(X^q - X) = q$, ce sont donc ses seules racines.

Ainsi, $\mathrm{Ker}(\widetilde{S_P} - \mathrm{Id}) = \mathbb{F}_q^r$. Comme $\varphi$ est un isomorphisme, $\mathrm{Ker}(\widetilde{S_P} - \mathrm{Id}) = \varphi(\mathrm{Ker}(S_P - \mathrm{Id}))$ et

$$\dim \mathrm{Ker}(S_P - \mathrm{Id}) = \dim \mathrm{Ker}(\widetilde{S_P} - \mathrm{Id}) = r.$$

– *Étape 2 : Factorisation de $P$.* On suppose que $r > 1$. La droite vectorielle $\mathbb{F}_q \cdot 1$ de $\mathbb{F}_q[X]/(P)$ étant de dimension 1 et $\mathrm{Ker}(S_P - \mathrm{Id})$ étant de dimension $r > 1$, on peut trouver $V \in \mathbb{F}_q[X]$ tel que $(V \bmod P) \in \mathrm{Ker}(S_P - \mathrm{Id})$ et $(V \bmod P)$ n'est pas contant. Or

$$(V \bmod P) \in \mathrm{Ker}(S_P - \mathrm{Id}) \qquad \iff \qquad \forall i \in [\![1, r]\!],\ (V \bmod P_i) \in \mathbb{F}_q.$$

Notons alors $\alpha_i = (V \bmod P_i) \in \mathbb{F}_q$, $\forall i \in [\![1, r]\!]$.

Montrons que $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$. Comme $\mathrm{pgcd}(P, V - \alpha)$ divise $P$, on peut écrire $\mathrm{pgcd}(P, V - \alpha) = P_{i_1} \cdot P_{i_k}$ avec $i_1, \dots, i_k \in [\![1, r]\!]$. Or les polynômes $P_{i_1}, \dots, P_{i_k}$ sont deux à deux premiers entre eux donc ils divisent tous $V - \alpha$. Or

$$P_i | V - \alpha \qquad \iff V - \alpha = 0 \bmod P_i \qquad \iff \alpha = \alpha_i$$

donc $\mathrm{pgcd}(P, V-\alpha) = \prod_{\alpha_i=\alpha} P_i$. Alors,

$$P = \prod_{i=1}^{r} P_i = \prod_{\alpha\in\mathbb{F}_q} \left( \prod_{\alpha_i=\alpha} P_i \right) = \prod_{\alpha\in\mathbb{F}_q} \mathrm{pgcd}(P, V-\alpha).$$

– *Étape 3 : L'algorithme se termine.* À partir de cette décomposition de $P$, on applique l'algorithme aux $\mathrm{pgcd}(P, V-\alpha)$ distincts de 1. Montrons que le nombre de leurs facteurs irréductibles est strictement inférieur à $r$. Comme $V \bmod P$ n'est pas constant, il existe $i, j$ tels que $\alpha_i \neq \alpha_j$. Alors $\mathrm{pgcd}(P, V-\alpha_i) = \prod_{\alpha_k=\alpha_i} P_k$ et $\mathrm{pgcd}(P, V-\alpha_j) = \prod_{\alpha_k=\alpha_j}$ sont distincts et ont donc strictement moins que $r$ facteurs irréductibles. □

# 2 Décomposition de Dunford

X. Gourdon, *Les maths en tête : Algèbre*, 2e édition, Ellipses. Théorème 1 page 175, proposition 1 page 194, théorème 3 page 195

Recasage : 153, 154, 157

**Lemme 2.1**

*Soient $f \in \mathscr{L}(E)$ et $P \in K[X]$. Notons $P = P_1 \cdots P_s$ avec $P_1, \dots, P_s$ premiers entre eux deux à deux, pour tout $i$, $E_i = \operatorname{Ker}(P_i(f))$. Alors, $\operatorname{Ker} P(f) = E_1 \oplus \cdots \oplus E_s$ et, pour tout $i$, le projecteur de la somme directe sur $E_i$ parallèlement à $\bigoplus_{j \neq i} E_j$ est un polynôme en $f$.*

▷ Montrons le résultat par récurrence sur $s \geq 2$.

– $s = 2$. Comme $P_1$ et $P_2$ sont premiers entre eux, d'après le théorème de Bézout, il existe $U_1, U_2 \in K[X]$ tels que

$$U_1 P_1 + U_2 P_2 = 1.$$

En particulier,

$$\forall x \in E, \qquad U_1(f) \circ P_1(f)(x) + U_2(f) \circ P_2(f)(x) = x. \tag{$*$}$$

⋆ Soit $x \in E_1 \cap E_2$. D'après $(*)$, on a donc $x = 0$. Ainsi, $E_1$ et $E_2$ sont en somme directe. Notons $p_1 : E_1 \oplus E_2 \to E_1$ et $p_2 : E_1 \oplus E_2 \to E_2$ les projecteurs associés.

⋆ Soit $x \in \operatorname{Ker} P(f)$. On a

$$P_2(f)(U_1(f) \circ P_1(f)(x)) = U_1(f) \circ P(f)(x) = 0$$

et, de même, $P_1(f)(U_2(f) \circ P_2(f))(x) = 0$ donc $\operatorname{Ker} P(f) \subset E_1 \oplus E_2$.

⋆ Soit $x = p_1(x) + p_2(x) \in E_1 \oplus E_2$. Alors

$$P(f)(x) = P_2(f) \circ P_1(f)(p_1(x)) + P_1(f) \circ P_2(f)(p_2(x)) = 0.$$

Ainsi, $E_1 \oplus E_2 \subset \operatorname{Ker} P(f)$.

On a donc montré que

$$\operatorname{Ker} P(f) = E_1 \oplus E_2$$

ainsi que, grâce à $(*)$ et $\star_2$, $p_1 = U_2(f) \circ P_2(f)$ et $p_2 = U_1(f) \circ P_1(f)$.

– $s \to s+1$. Si $P = P_1 \cdots P_s P_{s+1}$ avec $P_1, \dots, P_{s+1}$ premiers entre eux deux à deux. En posant $Q_1 = P_1 \cdots P_s$ et $Q_2 = P_{s+1}$, on $P = Q_1 Q_2$ avec $Q_1$ et $Q_2$ premiers entre eux. D'après le cas précédent, et par hypothèse de récurrence,

$$\operatorname{Ker} P(f) = (E_1 \oplus \cdots \oplus E_s) \oplus E_{s+1}$$

et, pour tout $i \in [\![1, s+1]\!]$, si $\displaystyle\sum_{k=1}^{s+1} U_k \prod_{j \neq k} P_j = 1$.

$$\begin{array}{rccc} & E_1 \oplus \cdots \oplus E_{s+1} & \to & E_i \\ p_i : & & & \\ & x & \mapsto & \left( U_i(f) \displaystyle\prod_{j \neq i} P_j(f) \right)(x) \end{array}$$

□

**Théorème 2.2**

*Soit $f \in \mathscr{L}(E)$ tel que $\chi_f$ est scindé. Il existe un unique couple $(d,n) \in \mathscr{L}(E)^2$ tel que :*
*(i) $d$ est diagonalisable et $n$ est nilpotent,*
*(ii) $f = d + n$ et $d \circ n = n \circ d$.*
*De plus, $d$ et $n$ sont des polynômes en $f$.*

▷ *– Étape 1 : Existence.* Notons $\chi_f = (-1)^n \prod_{i=1}^{s} (X-\lambda_i)^{m_i}$ et, pour tout $i$, $N_i = \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)^{m_i}$. Avec les notations du lemme, on dispose d'une famille de projecteurs $p_i = P_i(f)$ sur $N_i$ parallèlement à $\bigoplus_{j \neq i} N_j$. Posons alors $d = \sum_{i=1}^{s} \lambda_i p_i$ et $n = f - d = \sum_{i=1}^{s} (f - \lambda_i \mathrm{Id}_E) p_i$. Par construction, $d$ est diagonalisable et

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

Or, pour $p = \max m_i$, on a

$$(f - \lambda_i \mathrm{Id}_E)^p p_i = [(X-\lambda_i)^p P_i](f) = 0$$

car $\chi_f | (X-\lambda_i)^p P_i$. Donc $n^p = 0$. Comme les $p_i$ sont des polynômes en $f$, $d$ et $n$ également. En particulier, ils commutent.

*– Étape 2 : Unicité.* Soit $(d', n') \in \mathscr{L}(E)^2$ vérifiant $(i)$ et $(ii)$. $d'$ et $n'$ commutent donc ils commutent avec $d' + n' = f$. Or $d$ et $n$ sont des polynômes en $f$. Donc $d, n, d', n'$ commutent. Alors, $d$ et $d'$ sont diagonalisables dans une même base, donc $d - d'$ est diagonalisable. Or $d - d' = n' - n$ est nilpotent. Donc $d - d' = n' - n = 0$ *ie.* $d = d'$ et $n = n'$. □

# 3 Ellipsoïde de John-Loewner

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 3*, 2e édition, Cassini. Exercice 3.37 page 229

Recasage : 152, 160, 170, 171, 203, 219, 253.

**Théorème 3.1**

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

▷ *– Étape 1 : Calcul du volume d'un ellipsoïde.* Un ellipsoïde a pour équation $q(x) \leq 1$ où $q \in Q^{++}$ [1]. Pour $q \in Q^{++}$ on note donc $\mathcal{E}_q = \{x \in \mathbb{R}^n,\ q(x) \leq 1\}$. En considérant une base $\mathcal{B}$ orthonormée telle que

$$\forall x \in \mathbb{R}^n, \qquad q(x) = \sum_{i=1}^{n} a_i x_i^2,$$

par changement de base orthonormée, on obtient

$$\mathrm{Vol}(\mathcal{E}_q) = \int_{q(x)\leq 1} \mathrm{d}\lambda_n(x) = \int_{a_1x_1^2+\cdots+a_nx_n^2\leq 1} \mathrm{d}x_1\cdots\mathrm{d}x_n.$$

Soit $\phi : \begin{array}{ccc} \mathbb{R}^n & \to & \mathbb{R}^n \\ (x_1,\ldots,x_n) & \mapsto & \left(\dfrac{x_1}{\sqrt{a_1}},\ldots,\dfrac{x_n}{\sqrt{a_n}}\right) \end{array}$ un $\mathcal{C}^1$-difféomorphisme. Par la formule du changement de variables, on a :

$$\mathrm{Vol}(\mathcal{E}_q) = \int_{\phi(\{\|x\|_2\leq\}1)} \mathrm{d}x_1\cdots\mathrm{d}x_n = \frac{1}{\sqrt{a_1\cdots a_n}} \int_{\|x\|_2\leq 1} \mathrm{d}x_1\cdots\mathrm{d}x_n.$$

En notant $D(q) = \det(q) = \sqrt{a_1\cdots a_n}$ (indépendant de la base orthonormée) et $V_0 = \mathrm{Vol}(\{\|x\|_2 \leq 1\})$, on a donc

$$\mathrm{Vol}(\mathcal{E}_q) = \frac{V_0}{D(q)}.$$

On va donc montrer qu'il existe une unique forme quadratique $q \in Q^{++}$ maximisant $D(q)$ avec $\forall x \in K,\ q(x) \leq 1$.

*– Étape 2 : Existence.* On munit $Q$ de la norme

$$N : q \in Q \mapsto \sup_{\|x\|=1} |q(x)|$$

et on définit l'ensemble

$$\mathcal{A} = \{q \in Q^+,\ \forall x \in K, q(x) \leq 1\}.$$

⋆ $\mathcal{A}$ est non vide. En effet, comme $K$ est compact, il existe $M > 0$ tel que $\forall x \in K,\ \|x\| \leq M$. Alors, en définissant $q$ par $q(x) = \dfrac{\|x\|^2}{M^2}$, on a bien $q \in \mathcal{A}$.

⋆ $\mathcal{A}$ est fermé. En effet, si $(q_n) \in \mathcal{A}^{\mathbb{N}}$ converge vers $q \in Q$, alors, comme

$$\forall n \in \mathbb{N}, \forall x \in \mathbb{R}^n, \qquad |q(x) - q_n(x)| \leq N(q - q_n)\,\|x\|^2$$

on a $\forall x \in \mathbb{R}^n,\ q_n(x) \xrightarrow[n\to+\infty]{} q(x)$. On en déduit que $q \in \mathcal{A}$.

⋆ $\mathcal{A}$ est borné. En effet, $K$ est d'intérieur non vide donc il existe $a \in K$ et $r > 0$ tels que $B(a, r) \subset K$. Soit $q \in \mathcal{A}$. Si $\|x\| \leq r$, on a $a + x \in K$ donc $q(a + x) \leq 1$ et donc, par l'inégalité de Minkowski ($q \in Q^+$), on a :

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

1. On note $Q, Q^+, Q^{++}$ l'ensemble des formes quadratiques sur $\mathbb{R}^n$, respectivement des formes quadratiques positives, respectivement des formes quadratiques définies positives.

donc $q(x) \leq 4$. Alors, si $\|x\| \leq 1$, on a :

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

donc $N(q) \leq \dfrac{4}{r^2}$.

Ainsi, $\mathcal{A}$ est un compact non vide. Comme $D$ est continue, elle y atteint un maximum en $q_0 \in \mathcal{A}$. Comme $D\left(x \mapsto \dfrac{\|x\|^2}{M^2}\right) > 0$, on a $D(q_0) > 0$ donc $q_0 \in Q^{++}$.

*Étape 3 : Unicité.* $\mathcal{A}$ est convexe donc si $q \in \mathcal{A}$ alors $\dfrac{q+q_0}{2} \in \mathcal{A}$. Supposons que $D(q) = D(q_0)$. Alors $q \in Q^{++}$ et par stricte log-concavité de det sur $Q^{++}$, on a

$$D\left(\frac{q+q_0}{2}\right) \geq \sqrt{D(q)}\sqrt{D(q_0)} = D(q_0)$$

donc il y a égalité dans cette inégalité, donc $q = q_0$. □

**Lemme 3.2**

*Soient $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ et $\alpha, \beta \in [0,1]$ tels que $\alpha + \beta = 1$. Alors*

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

*avec égalité si et seulement si $A = B$ ou $\alpha\beta = 0$.*

▷ – *Étape 1 : Pseudo-réduction simultanée.* $A$ est définie positive donc elle définit un produit scalaire, noté $\langle \cdot, \cdot \rangle$. Alors, $B$ définit une forme quadratique qui peut s'écrire $x \mapsto \langle x, f(x)\rangle$ où $f = f^*$. Il existe alors une base orthonormée $\mathcal{B}$ pour $\langle \cdot, \cdot \rangle$ telle que $D = \mathrm{Mat}_{\mathcal{B}}(f)$ est diagonale réelle. En notant $Q$ la matrice de passage de la base canonique à $\mathcal{B}$, on a

$$^tQAQ = I_n \qquad \text{et} \qquad ^tQBQ = D.$$

En notant $P = Q^{-1}$, on a $A = {}^tPP$ et $B = {}^tPBP$.

– *Étape 2 : Conclusion* On a

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

$$\det(\alpha A + \beta B) = (\det P)^2 \det(\alpha I_n + \beta D)$$

donc il suffit de montrer que $\det(\alpha I_n + \beta D) \geq (\det D)^\beta$ c'est-à-dire que

$$\prod_{i=1}^n (\alpha + \beta\lambda_i) \geq \left(\prod_{i=1}^n \lambda_i\right)^\beta$$

où $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. En prenant le log[1], cela équivaut à

$$\sum_{i=1}^n \ln(\alpha + \beta\lambda_i) \geq \beta \sum_{i=1}^n \ln \lambda_i.$$

Or $\ln(\alpha + \beta\lambda_i) \geq \alpha \ln 1 + \beta \ln \lambda_i = \beta \ln \lambda_i$ par concavité de ln, d'où le résultat en sommant.

Si $\alpha \in ]0,1[$ et $A \neq B$, alors un des $\lambda_i$ est différent de 1 donc une des inégalité ci-dessus est stricte, donc l'inégalité est stricte. □

1. Les $\lambda_i$ sont strictement positifs car $f$ défini positif.

# 4 Équation de Pell-Fermat

P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométries, Tome second*, Calvage & Mounet. Proposition 1.5 page 388.

Recasage : 126.

**Théorème 4.1**

*Soit $d \geq 2$ sans facteur carré et soit $\mathscr{H}$ l'hyperbole ayant pour équation $X^2 - dY^2 = 1$ dans le repère $OXY$ du plan $\mathbb{R}^2$. Soit $M_0 = (1,0)$. On admet qu'il existe $M_1 = (X_1, Y_1) \in \mathscr{H}$ avec $X_1, Y_1 \in \mathbb{N}^*$ et $Y_1$ aussi petit que possible. Alors, l'ensemble des points entiers de la branche de $\mathscr{H}$ qui contient $M_0$ est le groupe engendré par $M_1$. L'ensemble des points entiers de $\mathscr{H}$ forme un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.*

▷ *– Étape 1 : coordonnées de la loi de groupe.* Soit $\varphi : M \in \mathscr{H} \mapsto M_1 * M$. Calculons les coordonnées de $\varphi(M)$. Pour cela, on change de repère en posant :

$$\begin{cases} x = X + \sqrt{d}Y \\ y = X - \sqrt{d}Y \end{cases}$$

de sorte que $(x,y) \in \mathscr{H} \Leftrightarrow xy = 1$. Dans le repère $Oxy$, $M_0$ a pour coordonnées $(1,1)$ et notons $(x_1, y_1)$ les coordonnées de $M_1$. Si $M \in \mathscr{H}$ a pour coordonnées $(x,y)$ dans $Oxy$, alors $\varphi(M)$ a pour coordonnées $(x_1 x, y_1 y)$. En effet, la droite $\Delta_{M_1 M}$ a pour équation dans $Oxy$ :

$$\bar{y} - 1 = \frac{y - y_1}{x - x_1}(\bar{x} - 1).$$

Ainsi, les coordonnées $(\bar{x}, \bar{y})$ de $\varphi(M)$ dans $Oxy$ doivent satisfaire cette équation ainsi que $\bar{x}\bar{y} = 1$. On en déduit le résultat. Un calcul montre que dans le repère $OXY$, le point $\varphi(M)$ a pour équation $(XX_1 + dYY_1, X_1 Y + XY_1)$.

*– Étape 2 : sous-groupe et définition d'un ordre.* Notons $\mathscr{H}_0$ la branche de l'hyperbole contenant $M_0$. On a $(x,y) \in \mathscr{H}_0 \Leftrightarrow xy = 1$ et $x > 0$. Alors, le calcul de coordonnées effectué pour $\varphi$ montre que $\mathscr{H}_0$ est un sous-groupe de $(\mathscr{H}, *)$, de même que $\mathscr{H}_0 \cap \mathbb{Z}^2$. De plus, la projection $(x,y) \in \mathscr{H}_0 \mapsto x \in \mathbb{R}_+^*$ est bijective donc on peut transporter l'ordre de $\mathbb{R}_+^*$ à $\mathscr{H}_0$. Remarquons que l'ordre peut se lire dans le repère $Oxy$ sur la coordonnée $x$ et dans le repère $OXY$ sur la coordonnée $Y$ en vertu de la relation $x = \sqrt{1 + dY^2} + \sqrt{d}Y$ (cette fonction de $Y$ étant strictement croissante). Comme $x_1 > 1$, $\varphi$ est strictement croissante.

*– Étape 3 : $\mathscr{H}_0 \cap \mathbb{Z}^2$ est engendré par $M_1$.* Pour $n \in \mathbb{Z}$, notons $M_n = M_1^n = \varphi^n(M_1) = (X_n, Y_n)$ dans $OXY$. Par définition de $M_0$, on a $M_{-1} = (X_1, -Y_1)$ et, par récurrence, $Y_{-n} = -Y_n$, $\forall n \in \mathbb{N}$.

Comme $\varphi$ est strictement croissante et $\forall n \in \mathbb{Z}$, $M_{n+1} = \varphi(M_n)$, la suite $(M_n)_{n\in\mathbb{Z}}$ est strictement croissante. De plus, comme $\forall n \in \mathbb{N}$, $X_n \geq 1$ et $Y_1 \geq 1$, on a $Y_{n+1} > Y_n$ $\forall n \in \mathbb{Z}$. Comme $(Y_n)_{n\in\mathbb{N}} \subset \mathbb{N}$, on en déduit que $Y_n \xrightarrow[n\to\pm\infty]{} \pm\infty$.

Soit alors $M = (X,Y)$ un point entier de $\mathscr{H}_0$. D'après ce qui précède, il existe $n \in \mathbb{Z}$ tel que $Y_n \leq Y < Y_{n+1}$. Soit $M' = M_{-n} * M$. Comme $\varphi$ est strictement croissante, $\varphi^{-n}$ l'est également donc $M_0 \leq M' < M_1$. Comme on a supposé que $M_1$ était solution minimale de l'équation de Pell-Fermat, $M' = M_0$ et $M = M_n$. Ainsi, $\mathscr{H}_0 \cap \mathbb{Z}^2 = \langle M_1 \rangle$.

*– Étape 4 : Ensemble des points entiers de $\mathscr{H}$.* La réflexion $(X,Y) \mapsto (-X,Y)$ échange les branches et préserve $\mathbb{Z}^2$ donc $\mathscr{H} \cap \mathbb{Z}^2 = \{(\pm X_n, Y_n),\ n \in \mathbb{Z}\}$. On vérifie alors que l'application :

$$\begin{array}{ccc} \{\pm 1\} \times \mathbb{Z} & \to & \mathscr{H} \cap \mathbb{Z}^2 \\ (\varepsilon, n) & \mapsto & (\pm X_n, Y_n) \end{array}$$

est un isomorphisme (loi produit pour le premier groupe). □

**Corollaire 4.2**

*Soit $d \geq 2$ sans facteur carré. Il existe une solution fondamentale $(X_1, Y_1)$, coordonnée de $x_1 = X_1 + \sqrt{d}Y_1$ dans $\mathbb{Z}[\sqrt{d}]$, de l'équation de Pell-Fermat $X^2 - dY^2 = 1$ telle que l'ensemble des solutions soit les coordonnées dans $\mathbb{Z}[\sqrt{d}]$ de $\{\pm x_1^n,\ n \in \mathbb{Z}\}$.*

**Corollaire 4.3**

*Soit $d \geq 2$ sans facteur carré tel que $-1$ ne soit pas un carré modulo $d$. Alors $\mathbb{Z}[\sqrt{d}]^\times \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

▷ Dans ce cas, un élément est inversible si et seulement si sa norme $X^2 - dY^2$ est égale à 1 : équation de Pell-Fermat. □

# 5 Étude de $O(p,q)$

P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométries, Tome premier*, Calvage & Mounet. Proposition A.2 page 211.

Recasage : 156, 158, 170, 171.

**Théorème 5.1**

*Soient $p,q \neq 0$. On a un homéomorphisme*

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

▷ *– Étape 1 : Application de la décomposition polaire.* Soit $M \in O(p,q)$. Soit $(O,S) \in O(n) \times \mathcal{S}_n^{++}(\mathbb{R})$ $(n = p+q)$ la décomposition polaire de $M$. Montrons que $O, S \in O(p,q)$.
Posons $T = {}^tMM = S^2$. Comme $M \in O(p,q)$, on a $MI_{p,q}{}^tM = I_{p,q}$ donc ${}^tM^{-1}I_{p,q}M^{-1} = I_{p,q}$ d'où ${}^tM^{-1} \in O(p,q)$. On en déduit que ${}^tM \in O(p,q)$. Ainsi, $S^2 = T \in O(p,q)$. Comme $T \in \mathcal{S}_n^{++}(\mathbb{R})$ et $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ réalise un homémorphisme, il existe $U \in \mathcal{S}_n(\mathbb{R})$ tel que $T = \exp(U)$. Alors,

$$\begin{aligned}
T \in O(p,q) &\iff TI_{p,q}{}^tT = I_{p,q} \\
&\iff {}^tT = I_{p,q}^{-1}T^{-1}I_{p,q} \\
&\iff {}^t\exp(U) = I_{p,q}^{-1}\exp(-U)I_{p,q} \\
&\iff \exp\left({}^tU\right) = \exp\left(-I_{p,q}^{-1}UI_{p,q}\right) \\
&\underset{\exp \text{ bijective}}{\iff} U = {}^tU = -I_{p,q}^{-1}UI_{p,q} \\
&\iff UI_{p,q} + I_{p,q}U = 0 \\
&\iff \frac{U}{2}I_{p,q} + I_{p,q}\frac{U}{2} = 0 \\
&\iff {}^t\exp\left(\frac{U}{2}\right) = I_{p,q}^{-1}\exp\left(\frac{U}{2}\right)I_{p,q}
\end{aligned}$$

d'où $\exp\left(\frac{U}{2}\right) \in O(p,q)$. Or $\exp\left(\frac{U}{2}\right) \in \mathcal{S}_n^+(\mathbb{R})$ et $\exp\left(\frac{U}{2}\right)^2 = T$ donc, par unicité de la racine carrée dans $\mathcal{S}_n^+(\mathbb{R})$, on a $S = \exp\left(\frac{U}{2}\right) \in O(p,q)$. On en déduit que $O \in O(p,q)$.

Ainsi, la décomposition polaire induit l'homéomorphisme

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

*– Étape 2 : Étude de $O(n) \cap O(p,q)$.* Soit $O \in O(n) \cap O(p,q)$. Écrivons $O = \begin{pmatrix} A & C \\ B & D \end{pmatrix} \in \mathcal{M}_{p+q,p+q}(\mathbb{R})$. Alors

$$O \in O(n) \cap O(p,q) \iff \begin{cases} {}^tAA - {}^tBB = I_p \\ {}^tAC - {}^tBD = 0 \\ {}^tCA - {}^tDB = 0 \\ {}^tCC - {}^tDD = -I_q \end{cases} \quad \text{et} \quad \begin{cases} {}^tAA + {}^tBB = I_p \\ {}^tAC + {}^tBD = 0 \\ {}^tCA + {}^tDB = 0 \\ {}^tCC + {}^tDD = I_q \end{cases}$$

$$\iff \begin{cases} B = C = 0 \\ A \in O(p) \\ D \in O(q) \end{cases}$$

Ainsi, $O(n) \cap O(p,q) = \left\{ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix},\ A \in O(p), D \in O(q) \right\} \simeq O(p) \times O(q)$.

– *Étape 3 : Étude de* $\mathcal{S}_n(\mathbb{R}) \cap O(p,q)$. Posons

$$L = \{M \in \mathcal{M}_n(\mathbb{R}),\ MI_{p,q} + I_{p,q}M = 0\}.$$

On a vu précédemment que exp réalise un homéomorphisme $L \cap \mathcal{S}_n(\mathbb{R}) \simeq O(p,q) \cap \mathcal{S}_n^{++}(\mathbb{R})$. Soit $S \in L \cap \mathcal{S}_n(\mathbb{R})$, $S = \begin{pmatrix} A & B \\ {}^tB & D \end{pmatrix}$. Alors

$$SI_{p,q} + I_{p,q}S = 0 \qquad \Longleftrightarrow \qquad A = D = 0$$

donc $L \cap \mathcal{S}_n(\mathbb{R}) = \left\{ \begin{pmatrix} 0 & B \\ {}^tB & 0 \end{pmatrix},\ B \in \mathcal{M}_{p,q}(\mathbb{R}) \right\} \simeq \mathbb{R}^{pq}$.

– *Conclusion.* On a montré que

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

□

# 6 Étude de l'anneau $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$

D. Perrin, *Cours d'Algèbre*, Ellipses. Paragraphe II.5 page 53

Recasage : 122

**Théorème 6.1**

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

▷ – *Étape 1 : Détermination des inversibles de A.* Notons $\alpha = \dfrac{1+i\sqrt{19}}{2}$. Comme $\alpha+\overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 5$, on a $\alpha^2-\alpha+5 = 0$ donc

$$A = \{a + b\alpha,\ (a,b) \in \mathbb{Z}^2\}$$

est un sous-anneau de $\mathbb{C}$. Il est donc intègre. De plus, $A$ est stable par conjugaison car $\overline{\alpha} = 1-\alpha$. Définissons sur $A$ la norme $N$ par

$$\forall a,b \in \mathbb{Z}, \qquad N(a+b\alpha) = (a+b\alpha)\overline{a+b\alpha} = a^2+ab+5b^2 = \left(a+\frac{b}{2}\right)^2 + \frac{19}{4}b^2 \geq 0.$$

On en déduit que $\forall z \in A$, $N(z) \in \mathbb{N}$ et $N(z) = 0$ si et seulement si $z = 0$. Alors, si $z \in A^\times$, on a $1 = N(zz^{-1}) = N(z)N(z^{-1})$, ce qui impose $N(z) = 1$. En notant $z = a+b\alpha$ avec $a,b \in \mathbb{Z}$,

$$\left(a+\frac{b}{2}\right)^2 + \underbrace{\frac{19}{4}}_{>1} b^2 = 1$$

donc $b = 0$ et $a = \pm 1$. Ainsi, $A^\times = \{\pm 1\}$.

– *Étape 2 : A n'est pas euclidien.* Si $A$ est euclidien, alors il existe $x \in A\backslash A^\times$ tel que la restriction de la projection canonique $A \to A/(x)$ à $A^\times \cup \{0\}$ est surjective. Mais alors, $A/(x)$ est un corps à deux ou trois éléments. On a donc un morphisme d'anneaux $\pi : A \to K$ surjectif, avec $K = \mathbb{F}_2$ ou $K = \mathbb{F}_3$. En particulier, $\beta = \pi(\alpha)$ vérifie $\beta^2-\beta+5 = 0$ dans $K$. Or on vérifie à la main que cette équation n'a pas de solution. Donc $A$ n'est pas euclidien.

– *Étape 3 : Pseudo-division euclidienne.* Montrons que pour $a,b \in A\backslash\{0\}$, il existe $q,r \in A$ tel que $N(r) < N(b)$ et

$$a = bq + r \qquad \text{ou} \qquad 2a = bq + r.$$

Notons $x = \dfrac{a}{b} = \dfrac{a\overline{b}}{b\overline{b}} = u + v\alpha$ avec $u,v \in \mathbb{Q}$, et $n = \lfloor v \rfloor$.

⋆ 1er cas : $v \notin \left]n+\dfrac{1}{3}, n+\dfrac{2}{3}\right[$. Soient $s$ et $t$ les entiers les plus proches, respectivement, de $u$ et $v$. On a alors

$$|s-u| \leq \frac{1}{2} \qquad \text{et} \qquad |t-v| \leq \frac{1}{3}$$

donc, en posant $q = s+t\alpha \in A$ on a

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

donc avec $r = a-bq = b(x-q)$ on a bien $N(r) < N(b)$.

⋆ 2e cas : $v \in \left[n+\dfrac{1}{3}, n+\dfrac{2}{3}\right]$ alors $2v \in \left[2n+\dfrac{2}{3}, 2n+1+\dfrac{1}{3}\right]$ donc l'entier le plus proche de $2v$ est $t = 2n+1$ et $|t-2v| \leq \dfrac{1}{3}$ et on conclut comme au cas précédent.

– *Étape 4 : (2) est un idéal maximal de A.* On a $A \simeq \mathbb{Z}[X]/(X^2-X+5)$ donc le théorème d'isomorphisme montre que

$$A/(2) \simeq \mathbb{Z}[X]/(2, X^2-X+5) \simeq \mathbb{F}_2[X]/(X^2-X+5).$$

Or $X^2 - X + 5$ est de degré 2 et n'a pas de racine dans $\mathbb{F}_2$ donc $A/(2)$ est un corps, donc (2) est un idéal maximal.

– *Étape 5 : $A$ est principal.* Soit $I \neq \{0\}$ un idéal de $A$. Soit $a \in I\backslash\{0\}$ tel que $N(a)$ est minimal. Si $I \neq (a)$, soit $x \in I\backslash(a)$. On effectue la pseudo-division euclidienne de $x$ par $a$ :

⋆ si $x = aq + r$ avec $N(r) < N(a)$ alors, comme $r \in I$, on a $x \in (a)$ : absurde.

Donc $2x = aq + r$ avec $N(r) < N(a)$ et, de même, $r = 0$ donc $2x = aq$. Comme (2) est maximal, donc premier, $a \in (2)$ ou $q \in (2)$. Si $q \in (2)$ on aurait $q = 2q'$ et donc $x \in (a)$ absurde. Donc $q \notin (2)$ et $a = 2a'$, donc $x = a'q \in (a')$. Il suffit alors de montrer que $a' \in I$, ce qui contredira la minimalité de $N(a)$. Comme $q \notin (2)$ et (2) est maximal, on a $(2, q) = A$ donc il existe $u, v \in A$ tels que $2u + qv = 1$. Donc $a' = 2ua' + qva' = ua + vx \in (I)$.

Ainsi, $I = (a)$ et $A$ est principal. □

# 7 Formule de Poisson pour les groupes abéliens finis

G. Peyré, *L'algèbre discrète de la transformée de Fourier*, Ellipses. Théorème 3.2 page 44.

Recasage : 110.

**Théorème 7.1**

*Soient $G$ un groupe abélien fini et $H \subset G$ un sous-groupe. Pour $f : G \to \mathbb{C}$ on a :*

$$\forall g \in G, \qquad \sum_{h\in H} f(gh) = \frac{|H|}{|G|} \sum_{\chi \in H^\sharp} \widehat{f}(\overline{\chi})\chi(g)$$

*où $\widehat{f} : \widehat{G} \to \mathbb{C}$ est la transformée de Fourier de $f$ et $H^\sharp = \{\chi \in \widehat{G},\ \chi(H) = \{1\}\}$.*

▷ Soit $S$ un système de représentants de $G/H$ dans $G$. On note $gH$ l'image de $g \in S$ dans $G/H$. Posons

$$\widetilde{f} : \begin{array}{ccc} G & \to & \mathbb{C} \\ g & \mapsto & \displaystyle\sum_{h\in H} f(gh). \end{array}$$

Pour $g \in S$ et $g' \in gH$, disons $g' = gh'$ avec $h' \in H$, on a :

$$\widetilde{f}(g') = \sum_{h\in H} f(gh'h) = \sum_{h\in H} f(gh) = \widetilde{f}(g)$$

car $h \in H \mapsto h'h \in H$ est bijective. On peut donc quotienter et définir

$$F : \begin{array}{ccc} G/H & \to & \mathbb{C} \\ gH & \to & \displaystyle\sum_{h\in H} f(gh). \end{array}$$

Décomposons $F$ en série de Fourier :

$$\forall g \in S, \qquad F(gH) = \sum_{\chi \in \widehat{G/H}} \langle F, \chi\rangle \chi(gH)$$

où

$$\langle F, \chi\rangle = \frac{1}{|G/H|} \sum_{g\in S} F(gH)\overline{\chi(gH)} = \frac{|H|}{|G|} \sum_{g\in S}\sum_{h\in H} f(gh) \underbrace{\overline{\chi(gH)}}_{\overline{\chi(ghH)}}$$

Or $(g, h) \in S \times H \mapsto gh \in G$ est bijective et

$$\varphi : \begin{array}{ccc} \widehat{G/H} & \to & H^\sharp \\ \chi & \mapsto & \widetilde{\chi} : \begin{array}{ccc} G & \to & \mathbb{C} \\ g & \mapsto & \chi(gH) \end{array} \end{array}$$

est un isomorphisme de groupes donc

$$\langle F, \chi\rangle = \frac{|H|}{|G|} \sum_{g\in G} f(g)\overline{\varphi(\chi)(g)} = \frac{|H|}{|G|} \widehat{f}(\overline{\varphi(\chi)})$$

et :

$$\forall g \in S, \qquad F(gH) = \frac{|H|}{|G|} \sum_{\chi \in \widehat{G/H}} \widehat{f}(\overline{\varphi(\chi)})\varphi(\chi)(g) = \frac{|H|}{|G|} \sum_{\chi \in H^\sharp} \widehat{f}(\overline{\chi})\chi(g).$$

On en déduit bien

$$\forall g \in G, \qquad \sum_{h\in H} f(gh) = \frac{|H|}{|G|} \sum_{\chi \in H^\sharp} \widehat{f}(\overline{\chi})\chi(g).$$

□

**Remarque :** Cela semble être utile dans le cas $G = \mathbb{F}_2^k$ et trouver des applications en codes correcteurs...

On a utilisé le lemme suivant.

**Lemme 7.2**

$$\begin{array}{rccc} & \widehat{G/H} & \to & H^\sharp \\ \varphi : & \chi & \mapsto & \widetilde{\chi} : \begin{array}{ccc} G & \to & \mathbb{C} \\ g & \mapsto & \chi(gH) \end{array} \end{array}$$

*est un isomorphisme de groupes.*

▷ $-$ $\varphi$ est bien défini : si $h \in H$ et $\chi \in \widehat{G/H}$ alors $\widetilde{\chi}(h) = \chi(H) = 1$ donc $\varphi\left(\widehat{G/H}\right) \subset H^\sharp$.

$-$ $\varphi$ est un morphisme de groupes : si $\chi, \chi' \in \widehat{G/H}$ alors

$$\forall g \in G, \qquad \varphi(\chi\chi')(g) = \chi\chi'(gH) = \chi(gH)\chi'(gH) = \varphi(\chi)(g)\varphi(\chi')(g).$$

$-$ $\varphi$ est injective : si $\varphi(\chi) = 1_{G\to\mathbb{C}}$ alors $\chi = \mathbf{1}_{G/H\to\mathbb{C}}$.

$-$ $\varphi$ est surjective : si $\widetilde{\chi} \in H^\sharp$ alors $H \subset \operatorname{Ker}\widetilde{\chi}$ donc on peut quotienter et définir $\chi(gH) = \widetilde{\chi}(g)$ et on a bien $\chi \in \widehat{G/H}$. Ainsi, $\varphi$ est un isomorphisme de groupes. □

# 8 Groupe simple d'ordre 60

I. Nourdin, *Agrégation de mathématiques épreuve orale*, 2e édition, Dunod. Proposition 2.19.28 page 236.

Recasage : 101, 103, 105, 190.

**Théorème 8.1**

*Soit $G$ un groupe fini simple d'ordre 60. Alors $G \simeq \mathfrak{A}_5$.*

▷ L'idée est de trouver un ensemble de cardinal 5 sur lequel on fera agir fidèlement $G$. On va montrer qu'on peut considérer l'ensemble des 2-Sylow de $G$.

– *Étape 1 : Premières applications du théorème de Sylow.* On a $60 = 2^2 \times 3 \times 5$. Notons $n_p$ le nombre de $p$-Sylow de $G$, pour $p \in \{2, 3, 5\}$. D'après le théorème de Sylow, on a :

$$\begin{cases} n_2 \equiv 1\,[2] \\ n_2 | 15 \end{cases} \qquad \begin{cases} n_3 \equiv 1\,[3] \\ n_3 | 20 \end{cases} \qquad \begin{cases} n_5 \equiv 1\,[5] \\ n_5 | 12 \end{cases}$$

On en déduit que $n_5 \in \{1, 6\}$. Si $n_5 = 1$ alors l'unique 5-Sylow de $G$ est distingué, ce qui contredit la simplicité de $G$. Donc $n_5 = 6$.

De même, on a $n_3 \in \{4, 10\}$. Supposons par l'absurde que $n_3 = 4$. Alors, d'après le théorème de Sylow, $G$ agit transitivement par conjugaison sur l'ensemble des 3-Sylow qui est de cardinal 4 donc il existe un morphisme non trivial $\rho : G \to \mathfrak{S}_4$. Comme $G \neq \operatorname{Ker}\rho \lhd G$ et $G$ est simple, on en déduit que $\rho$ est injectif, donc $|G| \leq |\mathfrak{S}_4| = 24$ : absurde. Donc $n_3 = 10$.

De même, $n_2 \in \{5, 15\}$.

– *Étape 2 : Montrons que $n_2 = 5$.* Supposons par l'absurde que $n_2 = 15$. Soient $S_1 \neq S_2$ des 2-Sylow (d'ordre 4). Montrons que $S_1 \cap S_2 = \{1\}$. On procède à nouveau par l'absurde en supposant $|S_1 \cap S_2| > 1$. Alors $|S_1 \cap S_2| = 2$ et $S_1 \cap S_2 = \{1, u\}$. Notons $H = \langle S_1, S_2\rangle$. D'après le théorème de Lagrange, $|H|\,|60$ et $4\,|\,|H|$. Comme $|H| > 4$, on a donc $|H| \in \{12, 20, 60\}$.

⋆ Supposons $|H| = 60$, ie $H = G$. Comme $S_1$ et $S_2$ sont d'ordre 4, ils sont abéliens donc $S_1 \cup S_2 \subset C_G(u) = \{g \in G,\ gu = ug\}$, le centralisateur de $u$. Donc $G = \langle S_1 \cup S_2\rangle \subset C_G(u) \subset G$ donc $u \in Z(G)$. Or $Z(G)$ est un sous-groupe normal de $G$ donc $Z(G) = \{1\}$ ou $G$. Comme un groupe abélien d'ordre 60 n'est pas simple, on en déduit que $Z(G) = \{1\}$ : contradiction.

⋆ Supposons $|H| = 20$. Alors, d'après le théorème de Sylow, $H$ a un unique 5-Sylow $H_5$ qui est donc distingué dans $H$. On en déduit que $H$ est un sous-groupe du normalisateur $N_G(H_5)$. Or, si l'on considère l'action de $G$ par conjugaison sur ses 5-Sylow, on a :

$$n_5 = |\Omega_{H_5}| = [G : N_G(H_5)]$$

d'où

$$|N_G(H_5)| = \frac{|G|}{n_5} = 10 < 20 = |H| \qquad \text{contradiction.}$$

⋆ Donc $|H| = 12$. Notons $n_2'$ (resp. $n_3'$) le nombre de 2-Sylow (resp 3-Sylow) de $H$. D'après le théorème de Sylow, on a :

$$\begin{cases} n_2' \equiv 1\,[2] \\ n_2' | 3 \end{cases} \qquad \begin{cases} n_3' \equiv 1\,[3] \\ n_3' | 4 \end{cases}$$

Or $S_1, S_2 \subset H$ donc $n_2' = 3$. Soit $S_3$ le troisième 2-Sylow de $H$. Comme $u \in Z(H)$ et $S_1$ et $S_3$ sont conjugués dans $H$, on a $u \in S_3$. On peut donc conclure qu'il y a $|S_1 \cup S_2 \cup S_3 \backslash \{1\} = 7$ éléments d'ordre 2 ou 4 dans $H$. Comptons le nombre d'éléments d'ordre 3.

Si $n_3' = 1$, notons $H_3$ l'unique 3-Sylow de $H$, qui est donc normal dans $H$. Alors, comme précédemment, $H \leq N_G(H_3)$ et

$$|N_G(H_3)| = \frac{|G|}{n_3} = 6 < 12 = |H| \qquad \text{contradiction.}$$

Donc $n_3' = 4$. Or, comme les groupes d'ordre 3 sont engendrés par tout élément distinct du neutre, les intersections des 3-Sylow sont réduites à $\{1\}$. On en déduit qu'il y a 8 éléments d'ordre 3 dans $H$. On a donc trouvé $1 + 7 + 8 = 16 > 12$ éléments dans $H$ : contradiction.

Ainsi, $S_1 \cap S_2 = \{1\}$ donc il y a $3 \times 15 = 45$ éléments d'ordre 2 ou 4. Comme $G$ a 10 3-Sylow, il a 20 éléments d'ordre 3 : absurde. Donc $n_2 = 5$.

– *Étape 3 : conclusion.* Ainsi, $n_2 = 5$. Faisons agir transitivement $G$ sur l'ensemble des 2-Sylow par conjugaison : $\rho : G \to \mathfrak{S}_5$. Cette action est non triviale et $G$ est simple, donc $\rho$ est fidèle. $G$ est donc isomorphe à un sous-groupe d'indice $\dfrac{|\mathfrak{S}_5|}{|G|} = 2$. C'est donc $\mathfrak{A}_5$. □

**Remarque :** $\mathfrak{A}_n$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$. En effet, soit $H$ un sous-groupe d'indice 2 de $\mathfrak{S}_n$. Alors $H$ est distingué. Soit $\pi : \mathfrak{S}_n \to \mathfrak{S}_n/H$ la projection canonique. L'application $\pi$ est un morphisme non trivial de $\mathfrak{S}_n$ sur $\{\pm 1\}$ donc $\pi = \varepsilon$ et $H = \operatorname{Ker}\pi = \operatorname{Ker}\varepsilon = \mathfrak{A}_n$. En effet, $\pi$ est déterminé par les images des transpositions (qui engendrent $\mathfrak{S}_n$). Or les transpositions sont toutes conjuguées. Comme $\pi$ n'est pas trivial, $\pi$(transposition)$=-1$ donc $\pi = \varepsilon$.

# 9 Invariants de similitude

X. Gourdon, *Les maths en tête : Algèbre*, 2e édition, Ellipses. Théorème 1 page 290.

Recasage : 150, 151, 153, 154, 159.

**Théorème 9.1**

*Soient $E$ un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathscr{L}(E)$. Il existe une unique famille $(P_1, \dots, P_r)$ de polynômes unitaires telle que $P_r | \dots | P_1$ et une famille de sous-espaces vectoriels $E_1, \dots, E_r$ de $E$ stables par $u$ telles que $E = E_1 \oplus \cdots \oplus E_r$ et pour tout $1 \leq i \leq r$, $u_{E_i}$ est cyclique de polynôme minimal $P_i$.*

▷ On admet le résultat suivant.

**Lemme 9.2**

*Soit $u \in \mathscr{L}(E)$. Il existe $x \in E$ tel que $\pi_{u,x} = \pi_u$, où $\pi_{u,x}$ est le générateur unitaire de l'idéal $\{P \in \mathbb{K}[X], P(u)(x) = 0\}$.*

Existence : Soient $E$ un $\mathbb{K}$-espace vectoriel de dimension $n$ et $u \in \mathscr{L}(E)$. Soit $x \in E$ tel que $\pi_{u,x} = \pi_u$. Alors, le sous-espace vectoriel

$$F = \mathrm{Vect}\{u^i(x),\, i \in \mathbb{N}\} = \mathrm{Vect}(x, u(x), \dots, u^{d-1}(x)),$$

où $d = \deg \pi_u$, est stable par $u$ et $u_F$ est cyclique de polynôme minimal $\pi_u$.

Montrons que $F$ admet un sous-espace vectoriel stable. On procède par dualité en considérant $\varphi \in E^*$ telle que $\varphi(u^i(x)) = \delta_{i,d-1}$ et en posant

$$\Phi = \mathrm{Vect}\{{}^t u^i(\varphi),\, i \in \mathbb{N}\}.$$

Montrons que $G = \Phi^0 = \{y \in E,\, \forall \psi \in \Phi,\, \psi(y) = 0\}$ est un supplémentaire stable de $F$.

⋆ $G$ est stable par $u$ car si $y \in G$, pour tout $\psi \in \Phi$,

$$\psi(u(y)) = \underbrace{{}^t u(\psi)}_{\in \Phi}\, y = 0$$

donc $u(y) \in G$.

⋆ $F \cap G = \{0\}$ car si $y \in F \cap G$, on peut écrire $y = \alpha_0 x + \cdots + \alpha_{d-1} u^{d-1}(x)$ de sorte que $0 = \varphi(y) = \alpha_{d-1}$ puis, $0 = {}^t u(\varphi) y = \alpha_{d-2} = 0$ et, par récurrence, $\alpha_i = 0$ pour tout $0 \leq i \leq d-1$.

⋆ Il suffit donc de montrer que $\dim F + \dim G = n$. Comme $\dim G = \dim E - \dim \Phi$, il suffit de montrer que $\dim \Phi = \dim F$.

De l'égalité $F \cap G = \{0\}$, on déduit $\dim F + \dim G = \dim(F + G) \leq n$ d'où $\dim \Phi \geq \dim F$. De plus, si $i \in \mathbb{N}$, ${}^t u^i(\varphi) = \varphi(u^i)$, donc la famille $(\varphi, {}^t u(\varphi), \dots, {}^t u^{d-1}(\varphi))$ engendre $\Phi$ et $\dim \Phi \leq d = \dim F$ (par définition de $\pi_{u,x}$). Ainsi, $\dim \Phi = \dim F$.

On conclut par récurrence sur la dimension de $E$.

Unicité : Supposons par l'absurde que $Q_1, \dots, Q_s$ soit une autre famille de polynômes telle que $Q_s | \dots Q_1$ et telle qu'il existe $F_1, \dots, F_s$ des sous-espaces stables par $u$ tels que $E = F_1 \oplus \cdots \oplus F_s$ et $u_{F_i}$ est cyclique de polynôme minimal $Q_i$. On a $P_1 = Q_1 = \pi_u$ donc on peut considérer $i = \min\{i \in \mathbb{N},\, P_i \neq Q_i\}$. On a

$$P_i(u)(E) = \bigoplus_{j=1}^{r} P_i(u)(E_j) = \bigoplus_{j<i} P_i(u)(E_j)$$

et

$$P_i(u)(E) = \bigoplus_{j=1}^{s} P_i(u)(F_j).$$

Pour $j < i$, $u_{E_j}$ et $u_{F_j}$ sont cycliques de polynôme minimal $P_j = Q_j$ donc semblables à la matrice compagnon $C_{P_j}$. On en déduit que $\dim P_i(u)(E_j) = \dim P_i(u)(F_j)$. Alors, en comparant les dimensions dans les égalités précédentes, on obtient $\forall i \leq j \leq s$, $P_i(u)(F_j) = 0$. Ainsi, pour $j = i$, $Q_i | P_i$. Par symétrie, on en déduit que $P_i = Q_i$ : absurde.

□

# 10 Lemme de Dedekind et application

S. Francinou, H. Gianella, *Exercices pour l'agrégation, Algèbre 1*, Masson. Exercice B.4 page 243.

Recasage : 125, 151, 162.

**Lemme 10.1 (*Dedekind*)**

*Soient $K, L$ deux corps. Soient $f_1, \dots, f_n : K \to L$ des morphismes de corps distincts. Alors $f_1, \dots, f_n$ sont linéairement indépendants sur $L$.*

▷ Supposons par l'absurde que la famille $(f_1, \dots, f_n)$ est liée. Parmi l'ensemble non vide des combinaisons linéaires nulles non triviales, on en choisit une de taille minimale, que l'on écrit, quitte à réordonner les $f_i$ :

$$a_1 f_1 + \cdots + a_k f_k = 0 \tag{1}$$

avec $a_1, \dots, a_k \in L^\times$. Comme $f_1 \neq f_k$, il existe $z \in K$ tel que $f_1(z) \neq f_k(z)$. Alors,

$$\forall x \in K, \qquad a_1 f_1(xz) + \cdots + a_k f_k(xz) = 0$$

d'où

$$a_1 f_1(z) f_1 + \cdots + a_k f_k(z) f_k = 0. \tag{2}$$

L'opération $(2) - f_1(z) \times (1)$ donne :

$$a_2(f_2(z) - f_1(z)) f_2 + \cdots + a_k(f_k(z) - f_1(z)) f_k = 0$$

qui est une relation de liaison non triviale puisque $f_k(z) \neq f_1(z)$, ce qui contredit la minimalité de $k$. □

**Théorème 10.2**

*Soient $K$ un corps et $G$ un groupe fini d'automorphismes de $K$. Notons $K^G = \{x \in K, \forall g \in G, g(x) = x\}$. Alors $K^G$ est un sous-corps de $K$ et $[K : K^G] = |G|$.*

▷ Notons $n = |G|$ et $g_1 = e, g_2, \dots, g_n$ les éléments de $G$.

– *Étape 1 : Supposons par l'absurde que* $[K : K^G] < n$. Soit alors $x_1, \dots, x_p$ $(p < n)$ une base de $K$ en tant que $K^G$-espace vectoriel. Considérons l'application linéaire $f : K^n \to K^p$ ayant pour matrice dans les bases canoniques : $(g_j(x_i))_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}}$. Comme $p < n$, d'après le théorème du rang, $\operatorname{Ker} f \neq (0)$ donc il existe $z_1, \dots, z_n \in K \backslash \{(0, \dots, 0)\}$ tels que

$$\forall 1 \leq i \leq p, \qquad z_1 g_1(x_i) + \cdots + z_n g_n(x_i) = 0.$$

Soit $a \in K$. Il existe $\lambda_1, \dots, \lambda_p \in K^G$ tels que $a = \sum_{i=1}^{p} \lambda_i x_i$. Alors,

$$\begin{aligned} \sum_{j=1}^{n} z_j g_j(a) &= \sum_{j=1}^{n} z_j \sum_{i=1}^{p} g_j(\lambda_i) g_j(x_i) \\ &\underset{\lambda_i \in K^G}{=} \sum_{i=1}^{p} \lambda_i \underbrace{\left( \sum_{j=1}^{n} z_j g_j(x_i) \right)}_{=0} = 0. \end{aligned}$$

Ainsi, $z_1 g_1 + \cdots + z_n g_n \equiv 0_K$ ce qui contredit le lemme de Dedekind.

– *Étape 2 : Supposons par l'absurde qu'il existe* $x_1, \dots, x_{n+1}$ $n+1$ *éléments de $K$ linéairement indépendants sur $K^G$.* Pour $1 \leq i \leq n+1$, posons

$$X_i = \begin{pmatrix} g_1(x_i) \\ \vdots \\ g_n(x_i) \end{pmatrix}.$$

On dispose donc d'une famille $(X_1, \dots, X_{n+1})$ de $(n+1)$ vecteurs de $K^n$, qui est donc liée : en considérant une combinaison linéaire non triviale nulle de taille minimale, et quitte à réordonner les $X_i$, on peut écrire

$$z_1 X_1 + \cdots + z_k X_k = 0 \tag{3}$$

avec $z_1, \dots, z_k \in K^\times$. Considérons l'action de $G$ sur $K^n$ définie par

$$\forall g \in G, \forall (u_1, \dots, u_n) \in K^n, \qquad g \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} g(u_1) \\ \vdots \\ g(u_n) \end{pmatrix}.$$

Comme la translation $\begin{array}{ccc} G & \to & G \\ h & \mapsto & gh \end{array}$ est une bijection, un élément $g \in G$ agit sur $X_i$ par permutation des lignes. En faisant agir $g \in G$ sur (3), on obtient

$$g(z_1) g \cdot X_1 + \cdots + g(z_n) g \cdot X_k = 0$$

soit, après réorganisation des lignes,

$$g(z_1) X_1 + \cdots + g(z_k) X_k = 0. \tag{4}$$

En effectuant l'opération (3) $\times\, g(z_1) -$ (4) $\times\, z_1$ on obtient :

$$(z_2 g(z_1) - z_1 g(z_2)) X_2 + \cdots + (z_k g(z_1) - z_1 g(z_k)) X_k = 0.$$

Par minimalité de $k$, chacun des coefficients doit être nul, pour tout $g$, donc

$$\forall g \in G, \forall 1 \leq i \leq k, \qquad g(z_i z_1^{-1}) = z_i z_1^{-1}$$

*ie.* $\lambda_i = z_i z_1^{-1} \in K^G$ $\forall i$. Alors, l'équation (3) s'écrit

$$z_1 \lambda_1 X_1 + \cdots + z_1 \lambda_k X_k = 0$$

soit, comme $z_1 \neq 0$,

$$\lambda_1 X_1 + \cdots + \lambda_k X_k = 0$$

d'où

$$\forall 1 \leq j \leq n, \qquad g_j \left( \sum_{i=1}^{k} \lambda_i x_i \right) = 0$$

et donc

$$\sum_{i=1}^{k} \lambda_i x_i = 0$$

ce qui contredit la liberté de $(x_1, \dots, x_{n+1})$.

– *Conclusion.* L'extension $K/K^G$ est donc finie et $[K : K^G] = n = |G|$. □

# 11 Morphismes de $(\mathcal{S}^1, \times)$ dans $(\mathrm{GL}_n(\mathbb{R}), \times)$

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 2*, 2e édition, Cassini. Exercice 4.29 page 251.

Recasage : 102, 155, 156.

**Proposition 11.1**

*Pour tout morphisme de groupes continu $\varphi : (\mathcal{S}^1, \times) \to (\mathrm{GL}_n(\mathbb{R}), \times)$, il existe $Q \in \mathrm{GL}_n(\mathbb{R}), r \in \mathbb{N}, k_1, \dots, k_r \in \mathbb{Z}^*$ tels que*

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

*où, $\forall \theta \in \mathbb{R}$, $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.*

▷ Analyse : Soit $\varphi : \mathcal{S}^1 \to \mathrm{GL}_n(\mathbb{R})$ un morphisme de groupes continu.

– *Étape 1 : Montrons que $\varphi(\mathcal{S}^1) \subset \mathrm{SL}_n(\mathbb{R})$.* Notons $\psi : \det \circ \varphi$. Comme $\psi$ est continu et $\mathcal{S}^1$ est connexe, $\psi(\mathcal{S}^1)$ est un intervalle de $\mathbb{R}^*$. Comme $\psi(1) = 1$, on a donc $\psi(\mathcal{S}^1) \subset \mathbb{R}_+^*$. De plus, comme $\mathcal{S}^1$ est compact, $\psi(\mathcal{S}^1)$ est un segment. En particulier, $\psi(\mathcal{S}^1)$ est borné. Comme $\psi(\mathcal{S}^1)$ est un sous-groupe de $(\mathbb{R}^*, \times)$, on en déduit que $\psi(\mathcal{S}^1) = \{1\}$. Ainsi, $\forall z \in \mathcal{S}^1$, $\varphi(z) \in \mathrm{SL}_n(\mathbb{R})$.

– *Étape 2 : Montrons que les valeurs propres des images sont de module 1.* Comme $\varphi(\mathcal{S}^1)$ est compact, pour une norme $\|.\|$ quelconque sur $\mathcal{M}_n(\mathbb{R})$, il existe une constante $M > 0$ telle que $\forall z \in \mathcal{S}^1$, $\|\varphi(z)\| \leq M$. On en déduit que

$$\forall z \in \mathcal{S}^1, \forall \lambda \in \mathrm{Sp}(\varphi(z)), \qquad |\lambda| \leq M.$$

Soient $z \in \mathcal{S}^1$ et $\lambda \in \mathrm{Sp}(\varphi(z))$. Pour tout $p \in \mathbb{Z}$, $\lambda^p \in \mathrm{Sp}(\varphi(z)^p) = \mathrm{Sp}(\underbrace{\varphi(z^p)}_{\in \varphi(\mathcal{S}^1)})$ donc $|\lambda^p| \leq M$. Ainsi, la suite $(|\lambda|^p)_{p \in \mathbb{Z}}$ est bornée. Donc $|\lambda| = 1$.

– *Étape 3 : Relèvement.* Notons $\psi : t \mapsto \varphi(e^{it})$. $\psi$ est un morphisme de groupes continu de $(\mathbb{R}, +)$ dans $(\mathrm{GL}_n(\mathbb{R}), \times)$. En fait, $\psi$ est dérivable. En effet, posons $F : x \in \mathbb{R} \mapsto \displaystyle\int_0^x \psi(t)\mathrm{d}t$. $F$ est $\mathcal{C}^1$ sur $\mathbb{R}$ et, en particulier, $F'(0) = I_n$. Ainsi, $\dfrac{1}{t}F(t) \xrightarrow[t\to 0]{I}{}_n$. Comme $\mathrm{GL}_n(\mathbb{R})$ est ouvert, on en déduit que $\dfrac{1}{t}F(t)$, donc $F(t)$ est inversible pour $t$ petit. Soit donc $a > 0$ tel que $F(a) \in \mathrm{GL}_n(\mathbb{R})$. Alors, en intégrant $\psi(x + t) = \psi(x)\psi(t)$, on obtient

$$\int_0^a \psi(x+t)\mathrm{d}t = \psi(x) \int_0^a \psi(t)\mathrm{d}t \qquad ie \qquad \psi(x) = F(a)^{-1} \int_x^{x+a} \psi(t)\mathrm{d}t.$$

Donc $\psi$ est dérivable. Alors, de $\psi(x + t) = \psi(x)\psi(t)$ on déduit $\psi'(x + t) = \psi'(t)\psi(x)$ d'où, pour $t = 0$, $\psi'(x) = \psi'(0)\psi(x)$. En notant $A = \psi'(0)$, on obtient

$$\forall t \in \mathbb{R}, \qquad \psi(t) = e^{tA}.$$

– *Étape 4 : $A$ est diagonalisable.* Comme $\psi$ est $2\pi$-périodique, $e^{tA} = e^{tA+2\pi A} = e^{tA}e^{2\pi A}$ donc $e^{2\pi A} = I_n$. On a donc $\mathrm{Sp}(e^{2\pi A}) = \{e^{2\pi\lambda}, \lambda \in \mathrm{Sp}(A)\}$ donc

$$\forall \lambda \in \mathrm{Sp}(A), \qquad e^{2\pi\lambda} = 1 \qquad ie\ \lambda \in i\mathbb{Z}.$$

De plus, si $A = D + N$ est la décomposition de Dunford de $A$ dans $\mathcal{M}_n(\mathbb{C})$, comme $D$ et $N$ commutent, on a $I_n = e^{2\pi A} = e^{2\pi D}e^{2\pi N}$. Or $D$ est diagonalisable et a les mêmes valeurs propres que $A$, donc $e^{2\pi D}$ est diagonalisable et ses valeurs propres sont $\{e^{2\pi\lambda}, \lambda \in \mathrm{Sp}(A)\} = \{1\}$. Donc $e^{2\pi D} = I_n$. Ainsi, $e^{2\pi N} = I_n$. Si, par l'absurde, $N \neq 0$, on a, pour $X \in \mathrm{Ker}\, N^2 \setminus \mathrm{Ker}\, N (\neq \emptyset)$,

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

ce qui contredit $e^{2\pi N} = I_n$. Ainsi, $N = 0$ et $A$ est diagonalisable dans $\mathbb{C}$.

*Étape 5 : Conclusion.* $A$ est diagonalisable dans $\mathbb{C}$ et ses valeurs propres non nulles sont conjuguées et dans $i\mathbb{Z}$, donc il existe $k_1, \dots, k_r \in \mathbb{Z}^*$ et $P \in \mathrm{GL}_n(\mathbb{C})$ tels que $A = P\mathrm{diag}(ik_1, -ik_1, \dots, ik_r, -ik_r, 1, \dots, 1)P^{-1}$. Alors,

$$\forall t \in \mathbb{R}, \qquad e^{tA} = P \begin{pmatrix} e^{ik_1} & & & & & & & & \\ & e^{-ik_1} & & & & & & & \\ & & \ddots & & & & & & \\ & & & e^{ik_r} & & & & & \\ & & & & e^{-ik_r} & & & & \\ & & & & & 1 & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1 & \end{pmatrix} P^{-1}.$$

Or, pour $\theta \in \mathbb{R}$,

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} = \begin{pmatrix} -i & 1 \\ 1 & -i \end{pmatrix} R_\theta \begin{pmatrix} -i & 1 \\ 1 & -i \end{pmatrix}^{-1}.$$

Donc il existe $Q \in \mathrm{GL}_n(\mathbb{C})$ tel que

$$e^{tA} = Q \begin{pmatrix} R_{tk_1} & & & & & & \\ & \ddots & & & & & \\ & & R_{tk_r} & & & & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \end{pmatrix} Q^{-1}.$$

Comme les matrices semblables sont réelles, on peut prendre $Q \in \mathrm{GL}_n(\mathbb{R})$.

– Synthèse : soit $\varphi : e^{it} \mapsto \psi(t)$ comme ci-dessus. $\varphi$ est bien défini car $R_{tk}$ ne dépend que de $t$ mod $2\pi$ pour $k \in \mathbb{Z}$. C'est un morphisme de groupes car $R_{(t+t')k} = R_{tk}R_{t'k}$ pour $k \in \mathbb{Z}$. Il est continu car, pour $k \in \mathbb{Z}$, $|e^{itk} - e^{ikt'}| \leq |k||e^{it} - e^{it'}|$ d'où

$$|\cos(kt) - \cos(kt')| \leq |k||e^{it} - e^{it'}| \qquad |\sin(kt) - \sin(kt')| \leq |k||e^{it} - e^{it'}|.$$

□

# 12 Polynômes irréductibles sur $\mathbb{F}_q$

S. Franciou, H. Gianella, *Exercices de mathématiques pour l'agrégation : Algèbre 1*, Masson. Exercice 5.10 page 189.

Recasage : 121, 123, 125, 141, 144, 190.

**Théorème 12.1**

*Pour $n \in \mathbb{N}^*$, on note $A(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré $n$ dans $\mathbb{F}_q[X]$ et $I(n,q)$ son cardinal. On a :*

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

▷ *– Étape 1 : Montrons que* $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P$.

⋆ Soient un diviseur $d$ de $n$ et $P \in A(d,q)$. Soit $x$ une racine de $P$ et $K = \mathbb{F}_q(x)$ un corps de rupture de $P$. Comme $P$ est irréductible, $[K : \mathbb{F}_q] = \deg(P) = d$ donc, par unicité des corps finis, $K = \mathbb{F}_{q^d}$. On en déduit en particulier que $x^{q^d} = x$. Mais alors, comme $d|n$,

$$x^{q^n} = x^{(q^d)^{\frac{n}{d}}} = \left(x^{q^d}\right)^{(q^d)^{\frac{n}{d}-1}} = x^{(q^d)^{\frac{n}{d}-1}} = \cdots = x$$

par récurrence, donc $x$ est racine de $X^{q^n} - X$. Comme $P$ est irréductible sur $\mathbb{F}_q$, il est à racine simple sur toute extension de $\mathbb{F}_q$ (les corps finis sont parfaits). On a donc montré que $P | X^{q^n} - X$.

⋆ Soit $P$ un facteur irréductible de $X^{q^n} - X$ et notons $d$ son degré. Comme $X^{q^n} - X$ est scindé dans $\mathbb{F}_{q^n}$, on peut considérer une racine $x \in \mathbb{F}_{q^n}$ de $P$. Alors, $K = \mathbb{F}_q(x)$ est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ donc

$$[\mathbb{F}_{q^n} : K] \underbrace{[K : \mathbb{F}_q]}_{d} = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$$

donc $d|n$. De plus, comme les racines de $X^{q^n} - X$ sont simples, ses facteurs irréductibles ont une multiplicité égale à 1. Comme $X^{q^n} - X$ est unitaire, on a donc montré que

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

*– Étape 2 : Inversion de Möbius.* En considérant les degrés dans l'égalité précédente, on obtient :

$$q^n = \sum_{d|n} dI(p,q)$$

donc, par la formule d'inversion de Möbius :

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

d'où le résultat. □

**Remarque :** Notons $I(n,q) = \dfrac{q^n + r_n}{n}$ avec $r_n = \sum_{\substack{d|n \\ d<n}} \mu\left(\frac{n}{d}\right) q^d$. Alors,

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

On en déduit :

⋆ $|r_n| < \dfrac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{q-1} \leq \dfrac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{\frac{q}{2}} = 2q^{\lfloor \frac{n}{2} \rfloor} \leq q^n$ donc pour tout $n \geq 1$, $I(n,q) > 0$ : il existe donc des polynômes irréductibles sur $\mathbb{F}_q$ de tout degré.

⋆ $|r_n| \leq \dfrac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{q-1} = o(q^n)$ donc $I(n,q) \underset{n \to +\infty}{\sim} \dfrac{q^n}{n}$.

**Lemme 12.2 (*Inversion de Möbius*)**

*Soit* $g : n \in \mathbb{N}^* \mapsto \sum_{d|n} f(d)$. *On a :*

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

▷ – *Étape 1 : Montrons que* $\sum_{d|n} \mu(d) = \delta_{1,n}$. Si $n = 1$, le résultat est évident. Supposons $n > 1$ et notons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $\alpha_i \geq 1$ et $p_i$ premiers distincts. Si $d|n$, on a $\mu(d) \neq 0$ si et seulement si $d$ est sans facteurs carrés *ie.* $d = p_{i_1} \cdots p_{i_1} \cdots p_{i_k}$ avec $i_1, \ldots, i_k$ distincts. Alors,

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{r} \underbrace{\mu(p_i)}_{-1} + \sum_{i \neq j} \underbrace{\mu(p_i p_j)}_{1} + \cdots + \underbrace{\mu(p_1 \cdots p_r)}_{(-1)^r} \\ &= \sum_{i=0}^{r} \binom{n}{i} (-1)^i = (1-1)^r = 0\end{aligned}$$

– *Conclusion.* On en déduit que

$$\begin{aligned}\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d|n} \sum_{d' | \frac{n}{d}} \mu(d) f(d') = \sum_{dd'|n} \mu(d) f(d') \\ &= \sum_{d|n} f(d) \left( \sum_{d' | \frac{n}{d}} \mu(d') \right) \\ &= f(n).\end{aligned}$$

□

# 13 Réduction de Jordan d'un endomorphisme nilpotent

Présenté le jour J (leçon 157, résultat 16/20)

X. Gourdon, *Les maths en tête : Algèbre*, 2e édition, Ellipses. Théorème 4 page 197.
J. Grifone, *Algèbre linéaire*, 5e édition, Cépaduès. Proposition 6.36 page 198 pour la taille des blocs.

Recasage : 157.

**Théorème 13.1**

*Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent. Il existe une base $\mathcal{B}$ de $E$ et des entiers $k_1, \dots, k_r \in \mathbb{N}^*$ tels que :*

$$Mat_B(u) = \begin{pmatrix} J_{k_1} & & 0 \\ & \ddots & \\ 0 & & J_{k_r} \end{pmatrix}$$

*où*

$$J_{k_i} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} \in \mathcal{M}_{k_i}(\mathbb{R})$$

▷ Notons $r \in \mathbb{N}^*$ l'indice de nilpotence de $u$,*ie.* $u^{r-1} \neq 0$ et $u^r = 0$. Pour $1 \leq i \leq r$, notons $F_i = \mathrm{Ker}(u^i)$.

– *Étape 1 : Noyaux itérés* Montrons que $\forall 1 \leq i \leq r$, $u(F_i) \subset F_{i-1}$ et

$$\{0\} = F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_r = E.$$

Pour tout $1 \leq i \leq r$ et $x \in F_i$, on a $0 = u^i(x) = u^{i-1}(u(x))$ donc $u(x) \in F_{i-1}$. De plus, $u^{i+1}(x) = u(u^i(x)) = 0$ donc $x \in F_{i+1}$. Enfin, si $F_{i+1} = F_i$, alors, si $x \in F_{i+2}$, on a $u^{i+2}(x) = 0$ donc $u(x) \in F_{i+1} = F_i$ donc $x \in F_{i+1}$. Ainsi, $F_{i+2} \subset F_{i+1}$, donc $F_{i+2} = F_i$. On en déduit que $E = F_r = F_i$ donc $u^i = 0$ *ie.* $i = r$, par définition de $r$.

– *Étape 2 : Construction d'une décomposition de $E$.* Soit $G_r$ un supplémentaire de $F_{r-1}$ dans $F_r$ :

$$F_r = G_r \oplus F_{r-1}.$$

D'après ce qui précède, on a $u(G_r) \subset u(F_r) \subset F_{r-1}$ et même $u_{|G_r}$ est injective. En effet,

$$(\mathrm{Ker}\, u) \cap G_r = F_1 \cap G_r \subset F_{r-1} \cap G_r = \{0\}.$$

Par ailleurs, $u(G_r) \cap F_{r-2} = \{0\}$. En effet, si $y \in u(G_r) \cap F_{r-2}$, $y = u(x)$ pour $x \in G_r$ et $0 = u^{r-2}(y) = u^{r-1}(x)$ donc $x \in G_r \cap F_{r-1} = \{0\}$ donc $y = 0$.

Ainsi, $u(G_r) \oplus F_{r+2} \subset F_{r-1}$ donc il existe un sous-espace vectoriel $H_{r-1}$ de $F_{r-1}$ tel que $\underbrace{u(G_r) \oplus H_{r-1}}_{G_{r-1}} \oplus F_{r-2} = F_{r-1}$.

On a donc construit $G_r, G_{r-1}, H_{r-1}$ tels que

$$F_r = G_r \oplus F_{r-1}, \qquad G_{r-1} = u(G_r) \oplus H_{r-1}, \qquad u_{|G_r} : G_r \to G_{r-1} \text{ injective.}$$

Par récurrence descendante, on construit de même des sous-espaces vectoriel de $E$, $G_1, \dots, G_r$, $H_1, \dots, H_{r-1}$ tels que :
$(i)$ $\forall 1 \leq i \leq r$, $F_i = G_i \oplus F_{i-1}$
$(ii)$ $\forall 1 \leq i \leq r-1$, $G_i = u(G_{i+1}) \oplus H_i$
$(iii)$ $\forall 1 \leq i \leq r-1$, $u_{|G_{i+1}} : G_{i+1} \to G_i$ est injective.

En particulier, $G_1 = F_1 = \mathrm{Ker}\, u$ et $E = F_r = \bigoplus_{i=1}^{r} G_i$.

– *Conclusion.* À partir d'une base $\varepsilon_1, \dots, \varepsilon_k$ de $G_i$ on obtient une famille libre de $G_{i-1}$ en considérant $(u(\varepsilon_1, \dots, u(\varepsilon_k)))$, que l'on peut compléter en une base de $G_{i-1}$. On construit ainsi le tableau suivant.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $e_{r,1}$ | $\dots$ | $e_{r,s_r}$ | | | | | | | | |
| $u(e_{r,1})$ | $\dots$ | $u(e_{r,s_r})$ | $e_{r-1,1}$ | $\dots$ | $e_{r-1,s_{r-1}}$ | | | | | |
| $u^2(e_{r,1})$ | $\dots$ | $u^2(e_{r,s_r})$ | $u(e_{r-1,1})$ | $\dots$ | $u(e_{r-1,s_{r-1}})$ | $e_{r-2,1}$ | $\dots$ | | | |
| $\dots$ | $\dots$ | $\dots$ | $\dots$ | $\dots$ | $\dots$ | $\dots$ | $\dots$ | | | |
| $u^{r-1}(e_{r,1})$ | $\dots$ | $u^{r-1}(e_{r,s_r})$ | $u^{r-2}(e_{r-1,1})$ | $\dots$ | $u^{r-2}(e_{r-1,s_{r-1}})$ | $u^{r-3}(e_{r-2,1})$ | $\dots$ | $e_{1,1}$ | $\dots$ | $e_{1,s_1}$ |

En lisant le tableau de bas en haut, de gauche à droite, on obtient une base $(e_1, \dots, e_n)$ de $E$ telle que $u(e_i) = e_{i-1}$ si $e_i$ n'est pas sur la dernière ligne et $u(e_i) = 0$ sinon. On obtient bien des blocs de Jordan. □

**Remarque :** Si $n_p$ est le nombre de blocs de taille $1 \leq p < r$, on a

$$n_p = 2\dim F_p - \dim F_{p-1} - \dim F_{p+1}.$$

En effet, si $p < r$, on a $n_p = \dim H_p$ et

$$F_p = G_p \oplus F_{p-1} \qquad G_p = u(G_{p+1}) \oplus H_p \qquad F_{p+1} = G_{p+1} \oplus F_p$$

donc, comme $u_{|G_{p+1}}$ est injective,

$$\dim F_p = \dim G_p + \dim F_{p-1}$$
$$\dim G_p = \dim G_{p+1} + \dim H_p$$
$$\dim F_{p+1} = \dim G_{p+1} + \dim F_p$$

d'où le résultat.

Si $p = r$, on a $n_r = \dim G_r = n - \dim F_{r-1}$.

# 14 Réduction des endomorphismes normaux

E. Ramis, C. Deschamps, J. Odoux, *Cours de mathématiques, tome 2.*

X. Gourdon, *Les maths en tête : Algèbre*, 2e édition, Ellipses. Théorème 4 page 260.

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 3*, 2e édition, Cassini. Exercice 1.36 page 65.

Recasage : 153, 154, 155, 160.

**Lemme 14.1**

*Soit $E$ un espace euclidien de dimension $n > 0$. Soit $u \in \mathscr{L}(E)$ un endomorphisme normal. Si $F$ est est stable par $u$, alors $F$ est stable par $u^*$. De plus $(u_F)^* = u_F^*$ et $u_F$ est normal.*

▷ Soit $\mathcal{B} = \mathcal{B}_F \cup \mathcal{B}_{F^\perp}$ une base orthonormée adaptée à la décomposition $E = F \oplus F^\perp$. On peut donc écrire :

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \qquad \mathrm{Mat}_{\mathcal{B}}(u^*) = \begin{pmatrix} {}^tA & 0 \\ {}^tB & {}^tC \end{pmatrix}$$

L'égalité $uu^* = u^*u$ impose alors $A\,{}^tA + B\,{}^tB = {}^tAA$. Or $\mathrm{Tr}(A\,{}^tA) = \mathrm{Tr}({}^tAA)$ donc $0 = \mathrm{Tr}(B\,{}^tB) = \sum_{i,j} b_{ij}^2$, donc $B = 0$.

Ainsi $\mathrm{Mat}_{\mathcal{B}}(u^*) = \begin{pmatrix} {}^tA & 0 \\ 0 & {}^tC \end{pmatrix}$ donc $F$ est stable par $u^*$.

Comme $B = 0$, on a $A\,{}^tA = {}^tAA$ d'où $u_F u_F^* = u_F^* u_F$. □

**Théorème 14.2**

*Soit $E$ un espace euclidien de dimension $n > 0$. Soit $u \in \mathscr{L}(E)$ un endomorphisme normal. Il existe une base orthonormée $\mathcal{B}$ de $E$ dans laquelle la matrice de $u$ est de la forme :*

$$\begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & 0 & \\ & & \lambda_r & & & & \\ & & & \tau_1 & & & \\ & & & & & \ddots & \\ & 0 & & & & & \\ & & & & & & \tau_s \end{pmatrix}$$

*où $\lambda_j \in \mathbb{R}$ et $\tau_i = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$.*

▷ On procède par récurrence forte sur $n = \dim E$.

– $n = 1$ : ok.

– Supposons que le résultat est vrai en dimension $\leq n-1$, $n \geq 2$. Soit $E$ un espace euclidien de dimension $n$ et $u$ un endomorphisme normal de $E$.

⋆ *1er cas : $u$ a une valeur propre réelle $\lambda$.* Posons $F = E_\lambda^\perp$. Alors $F$ est stable par $u^*$ et, d'après le lemme, par $u^{**} = u$. De plus, $u_F$ est normal. Comme $\dim F \leq n-1$, par hypothèse de récurrence, il existe une base orthonormale $\mathcal{B}_F$ de $F$ dans laquelle la matrice de $u_F$ a la forme voulue. Si $\mathcal{B}_{E_\lambda}$ est une base orthonormée de $E_\lambda$, dans la base $\mathcal{B}_{E\lambda} \cup \mathcal{B}_F$, la matrice de $u$ est de la forme voulue.

⋆ 2ecas : $u$ n'a pas de valeur propre réelle.

→ *$u$ admet un plan stable.* En effet, la décomposition de $\chi_u$ en facteurs irréductibles est de la forme :

$$\chi_u = \prod_{i=1}^{r} (X^2 + b_i X + c_i)$$

avec $\forall i$, $b_i^2 < 4c_i$. D'après le théorème de Cayley-Hamilton, $0 = \det(\chi_u(u)) = \prod_{i=1}^{r} \det(u^2 + b_i u + c_i \mathrm{Id}_E)$ donc l'un des endomorphismes $u^2 + b_i u + c_i \mathrm{Id}_E$ n'est pas injectif. Il existe donc $b, c \in \mathbb{R}$, $x \in E \backslash \{0\}$ tels que

$$u^2(x) + bu(x) + cx = 0. \tag{5}$$

Comme $u$ n'a pas de valeur propre réelle, $u(x)$ et $x$ ne sont pas colinéaires, donc $F = \mathrm{Vect}(x, u(x))$ est de dimension 2. De plus, d'après (5), il est stable par $u$. Alors, d'après le lemme, $F$ est stable par $u^*$ et $u_F$ est normal.

$\to$ *Réduction de* $u_F$. Notons $\mathcal{B}_F$ une base orthonormée de $F$. Alors, il existe $a, b, c, d \in \mathbb{R}$ tels que

$$M = \mathrm{Mat}_{\mathcal{B}_F}(u_F) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Comme $u$ n'a pas de valeur propre réelle, $u_F$ non plus, donc $b \neq 0$. De plus, $M$ est normale donc ${}^tMM = M\,{}^tM$ d'où

$$\begin{cases} a^2 + b^2 = a^2 + c^2 \\ ac + bd = ab + cd \end{cases}$$

La première équation impose $b = \pm c$. Si $b = c$, $M$ serait symétrique et aurait donc une valeur propre réelle. Donc $b = -c$. La deuxième équation impose donc, comme $b \neq 0$, $a = d$. Ainsi, $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

$\to$ *Conclusion.* $F^\perp$ est stable par $u^*$ et $u^{**} = u$ et $u_{F^\perp}$ est normal donc, comme $\dim(F^\perp) = n - 2 < n - 1$, par hypothèse de récurrence, il existe une base orthonormée $\mathcal{B}_{F^\perp}$ dans laquelle la matrice de $u_{F^\perp}$ est de la forme voulue. Alors, dans la base $\mathcal{B}F^\perp \cup \mathcal{B}_F$, la matrice de $u$ est de la forme souhaitée. □

**Remarque :** On en déduit, par exemple, les théorèmes de réduction des endomorphismes symétriques, orthogonaux et antisymétriques.

**Corollaire 14.3**

$\exp : \mathcal{A}_n(\mathbb{R}) \to \mathrm{SO}_n(\mathbb{R})$ *est surjective.*

▷ – *Étape 1 :* $\exp : \mathcal{A}_n(\mathbb{R}) \to \mathrm{SO}_n(\mathbb{R})$ *est bien définie.* Si $A \in \mathcal{A}_n(\mathbb{R})$, alors

$${}^t\exp(A)\exp(A) = \exp({}^tA)\exp(A) = \exp(-A)\exp(A) = I_n$$

donc $\exp(A) \in O_n(\mathbb{R})$. De plus,

$$\det(\exp(A)) = \exp(\mathrm{Tr}(A)) = e^0 = 1$$

donc $\exp(A) \in \mathrm{SO}_n(\mathbb{R})$.

– *Étape 2 : surjectivité.* Soit $U \in \mathrm{SO}_n(\mathbb{R})$. Il existe $P \in O_n(\mathbb{R})$ telle que

$${}^tPUP = \begin{pmatrix} I_r & & & 0 \\ & R_{\theta_1} & & \\ & & \ddots & \\ 0 & & & R_{\theta_s} \end{pmatrix} = M$$

en écrivant $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = R_\pi$ pour le nombre pair de $-1$. Notons $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Alors $\exp(\theta J) = R_\theta$ donc, si

$$A = \begin{pmatrix} 0_r & & & 0 \\ & \theta_1 J & & \\ & & \ddots & \\ 0 & & & \theta_s J \end{pmatrix} \in \mathcal{A}_n(\mathbb{R})$$

on $M = \exp(A)$. Alors $U = PM{}^tP = \exp(PA{}^tP)$ avec $PA{}^tP \in \mathcal{A}_n(\mathbb{R})$. □

# 15 Simplicité de $\mathrm{SO}_3(\mathbb{R})$

P. Caldero, J. Germoni, *Histoires hédonistes de groupes et géométries, Tome premier*, Calvage & Mounet. Proposition A.3 page 239.

Recasage : 108, 161, 183.

**Proposition 15.1**

*Pour tout $n \geq 2$, $\mathrm{SO}_n(\mathbb{R})$ est compact et connexe par arcs.*

▷ – Définissons $\varphi : M \in \mathcal{M}_n(\mathbb{R}) \to {}^tMM$. $\varphi$ est continue donc $\mathrm{SO}_n(\mathbb{R}) = \varphi^{-1}(\{I_n\}) \cap \det{}^{-1}(\{1\})$ est fermé. De plus, munissons $\mathcal{M}_n(\mathbb{R})$ de la norme associée au produit scalaire $\langle A, B\rangle = \mathrm{Tr}({}^tAB)$. Pour tout $M \in \mathrm{SO}_n(\mathbb{R})$, on a $\|M\| = \sqrt{\mathrm{Tr}(I_n)} = \sqrt{n}$. Ainsi, $\mathrm{SO}_n(\mathbb{R})$ est fermé borné dans $\mathcal{M}_n(\mathbb{R})$ qui est de dimension finie, donc $\mathrm{SO}_n(\mathbb{R})$ est compact.

– Soit $M \in \mathrm{SO}_n(\mathbb{R})$. Il existe $r, s \in \mathbb{N}$, $\theta_1, \dots, \theta_s \in \mathbb{R}$, $P \in \mathrm{O}_n(\mathbb{R})$ tels que

$$M = P \begin{pmatrix} I_r & & & \\ & R_{\theta_1} & & \\ & & \ddots & \\ & & & R_{\theta_s} \end{pmatrix} {}^tP$$

(l'espace propre associé à $-1$ est de dimension paire car $\det = 1$). Posons

$$\gamma : \begin{array}{ccc} [0,1] & \to & \mathrm{SO}_n(\mathbb{R}) \\ t & \mapsto & P \begin{pmatrix} I_r & & & \\ & R_{t\theta_1} & & \\ & & \ddots & \\ & & & R_{t\theta_s} \end{pmatrix} {}^tP. \end{array}$$

$\gamma$ est un chemin continu tracé dans $\mathrm{SO}_n(\mathbb{R})$ tel que $\gamma(0) = I_n$ et $\gamma(1) = M$. Ainsi, $\mathrm{SO}_n(\mathbb{R})$ est connexe par arcs. □

**Théorème 15.2**

*$\mathrm{SO}_3(\mathbb{R})$ est simple.*

▷ Soit $H$ un sous-groupe distingué non trivial de $\mathrm{SO}_3(\mathbb{R})$.

– *Étape 1 : Il suffit de montrer que $H$ contient un retournement.* Supposons que $r_D \in H$ soit un retournement d'axe la droite $D$. Soit $D'$ une autre droite de $\mathbb{R}^3$. Alors il existe une rotation $s \in \mathrm{SO}_3(\mathbb{R})$ telle que $s(D) = D'$. Considérons $r = sr_Ds^{-1}$. Cet endomorphisme a le spectre de $r_D$ donc c'est un retournement, l'espace propre associé à la valeur propre 1 est $D'$, donc $r$ est un retournement d'axe $D'$. De plus, comme $H$ est distingué, $r \in H$. Ainsi, $H$ contient tous les retournements. Comme $\mathrm{SO}_3(\mathbb{R})$ est engendré par les retournements[1], $H = \mathrm{SO}_3(\mathbb{R})$.

– *Étape 2 : Exhibons un retournement dans $H$.* Soit $h \in H \backslash \{I_3\}$. On considère l'application continue

$$\varphi : \begin{array}{ccc} \mathrm{SO}_3(\mathbb{R}) & \to & \mathbb{R} \\ g & \mapsto & \mathrm{Tr}([g,h]) \end{array}.$$

Comme la trace d'un élément de $\mathrm{SO}_3(\mathbb{R})$ est de la forme $1 + 2\cos\theta$, $\theta \in \mathbb{R}$, $\varphi(\mathrm{SO}_3(\mathbb{R})) \subset ]-\infty, 3]$. De plus, comme $\mathrm{SO}(3)$ est connexe, compact et contient $I_3$, son image par $\varphi$ est de la forme $[a, 3]$, $a \leq 3$.

Supposons par l'absurde que $a = 3$. Alors, $\forall g \in \mathrm{SO}_3(\mathbb{R})$, $[g, h] = I_3$ donc $h \in Z(\mathrm{SO}_3(\mathbb{R})) = I_3$ : absurde.

Donc $a < 3$ et on peut trouver $n \in \mathbb{N}^*$ tel que $a < 1 + 2\cos\dfrac{\pi}{n} < 3$ car 3 est la limite de cette suite strictement croissante. Soit alors $g_n \in \mathrm{SO}_3(\mathbb{R})$ tel que $\varphi(g_n) = 1 + 2\cos\dfrac{\pi}{n}$. Alors $h_n = g_nhg_n^{-1}h^{-1} \in H$ (distingué) est une rotation d'angle $\pm\dfrac{\pi}{n}$. Alors, $h_n^n \in H$ est un retournement. □

1. $\mathrm{O}_3(\mathbb{R})$ est engendré par les réflexions. Ces réflexions sont en nombre pair pour des raisons de déterminant. Si $u \in \mathrm{SO}_3(\mathbb{R})$, on peut écrire $u = r_1 \circ \cdots \circ r_{2k}$ et donc $u = (-r_1) \circ \cdots \circ (-r_{2k})$ et $-r_i$ est un retournement (regarder le spectre).

# 16 Sommes de Newton et algorithme de Faddeev

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*, 3e édition, Cassini. Exercice 5.31 page 209 pour le premier théorème.

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 2*, 2e édition, Cassini. Exercice 2.7 page 79 pour le second théorème.

Recasage : 142, 144.

**Théorème 16.1**

*Soit $K$ un corps. Pour $x_1, \dots, x_n \in K$ et $k \in \mathbb{N}$ on note $S_k = \sum_{j=1}^{n} x_j^k$ la $k$-ième somme de Newton. Si $\sigma_1, \dots, \sigma_n$ sont les fonctions symétriques élémentaires en $x_1, \dots, x_n$ et $\sigma_0 = 1$, on a :*

$$\forall k \in [\![0, n]\!], \qquad S_k - \sigma_1 S_{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1}S_1 + (-1)^k k\sigma_k = 0.$$

▷ Notons $P = \prod_{i=1}^{n}(X - x_i)$ de sorte que $P = \sum_{k=0}^{n}(-1)^k \sigma_k X^{n-k}$. Pour tout $i \in [\![1, n]\!]$, on a :

$$\begin{aligned}
\frac{XP}{X - x_i} &= \frac{P}{1 - \frac{x_i}{X}} = \left(\sum_{k=0}^{n}(-1)^k\sigma_k X^{n-k}\right)\left(\sum_{k=0}^{\infty}\frac{x_i^k}{X^k}\right) \\
&= \sum_{k=0}^{n}\left(\sum_{j=0}^{k}(-1)^j\sigma_j X^{n-j}\frac{x_i^{k-j}}{X^{k-j}}\right) \\
&= \sum_{k=0}^{n}\left(\sum_{j=0}^{k}(-1)^j\sigma_j x_i^{k-j}\right)X^{n-k}
\end{aligned}$$

donc

$$XP' = \sum_{i=1}^{n}\frac{XP}{X - x_i} = \sum_{k=0}^{n}\left(\sum_{j=0}^{k}(-1)^j\sigma_j S_{k-j}\right)X^{n-k}.$$

Or

$$XP' = \sum_{k=0}^{n-1}(-1)^k\sigma_k(n-k)X^{n-k}$$

donc par unicité de l'écriture de $XP'$ dans la base canonique,

$$\forall k \in [\![0, n-1]\!], \qquad \sum_{j=0}^{k}(-1)^j\sigma_j S_{k-j} = (-1)^k\sigma_k(n-k)$$

*ie.*

$$\forall k \in [\![0, n-1]\!], \qquad \sum_{j=0}^{k-1}(-1)^j\sigma_j S_{k-j} + (-1)^k\sigma_k S_0 = (-1)^k\sigma_k(n-k)$$

d'où

$$\forall k \in [\![0, n-1]\!], \qquad \sum_{j=0}^{k-1}(-1)^k\sigma_k S_{k-j} + (-1)^k k\sigma_k$$

De plus, des deux écritures de $XP'$ on déduit également

$$\sum_{j=0}^{n}(-1)^j\sigma_j S_{n-j} = 0,$$

ce qu'il fallait démontrer puisque $S_0 = n$. □

**Proposition 16.2**

*Soit $A \in \mathcal{M}_n(\mathbb{C})$. On définit $A_0 = A$ et*

$$\forall k \in \mathbb{N}, \qquad A_{k+1} = A\left(A_k - \frac{\mathrm{Tr}(A_k)}{k+1} I_n\right).$$

*Alors*

$$\chi_A = (-1)^n \left(X^n - \sum_{k=1}^{n} \frac{\mathrm{Tr}(A_{k-1})}{k} X^{n-k}\right).$$

▷ Notons $\lambda_1, \dots, \lambda_n$ les valeurs propres de $A$, $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires et $S_0 = n, S_1, \dots, S_n$ les sommes de Newton associées.

– *Étape 1 : Montrons par récurrence sur $k \in [\![0, n-1]\!]$ que $A_k = A^{k+1} - \sum_{i=0}^{k-1} \frac{\mathrm{Tr}(A_i)}{i+1} A^{k-i}$ et $\mathrm{Tr}(A_k) = (-1)^k (k+1)\sigma_{k+1}$.*

⋆ $k = 0$ : ok.

⋆ Soit $k \in [\![0, n-2]\!]$ tel que le résultat est vrai. Par hypothèse de récurrence, on a :

$$A_{k+1} = A^{k+2} - \sum_{i=0}^{k-1} \frac{\mathrm{Tr}(A_i)}{i+1} A^{k+1-i} - \frac{\mathrm{Tr}(A_k)}{k+1} A = A^{k+2} - \sum_{i=0}^{k} \frac{\mathrm{Tr}(A_i)}{i+1} A^{k+1-i}$$

et

$$\begin{aligned}
\mathrm{Tr}(A_{k+1}) &= \mathrm{Tr}(A^{k+2}) - \sum_{i=0}^{k} \frac{\mathrm{Tr}(A_i)\,\mathrm{Tr}(A^{k+1-i})}{i+1} \\
&\underset{\text{HR}}{=} S_{k+2} - \sum_{i=0}^{k} (-1)^i \sigma_{i+1} S_{k+1-i} \\
&= S_{k+2} - \sigma_1 S_{k+2} + \cdots + (-1)^{k+1} \sigma_{k+1} S_1 \\
&\underset{\text{Newton}}{=} (-1)^{k+1} (k+2) \sigma_{k+2}
\end{aligned}$$

– *Conclusion.* On en déduit que

$$\chi_A = (-1)^n X^n + \sum_{k=1}^{n} (-1)^{n-k} \sigma_k X^{n-k} = (-1)^n \left(X^n - \sum_{k=1}^{n} \frac{\mathrm{Tr}(A_{k-1})}{k} X^{n-k}\right).$$

□

# 17 Sous-groupes compacts de $\mathrm{GL}_n(\mathbb{R})$

M. Alessandri, *Thèmes de géométrie*, Dunod. Page 141.

Recasage : 101, 106, 150, 181, 203.

**Lemme 17.1**

*Soient $V$ un espace vectoriel de dimension finie, $K$ un compact convexe non vide de $V$ et $G$ un sous-groupe compact de $\mathrm{GL}(V)$ tel que*

$$\forall u \in G, \qquad u(K) \subset K.$$

*Alors il existe $x \in K$ tel que $\forall u \in G$, $u(x) = x$.*

▷ *– Étape 1 : Construction d'une norme $G$-invariante.* Soit $N$ une norme euclidienne sur $V$. On pose

$$\forall x \in V, \qquad N'(x) = \max_{u \in G} N(u(x)).$$

Pour chaque $x \in V$, $\mathrm{ev}_x : u \in \mathscr{L}(V) \mapsto u(x) \in V$ est (linéaire) continue donc, comme $N$ est continue, l'image de $G$ par $N \circ \mathrm{ev}_x$ est compacte, donc $N'$ est bien définie. C'est une norme sur $V$ car $N$ en est une. De plus, pour $u_0 \in G$ et $x \in V$, $N'(u_0(x)) = N'(x)$ car la translation $u \mapsto u \circ u_0$ est une bijection de $G$ (groupe), donc $N'$ est $G$-invariante. Enfin, si $x$ et $y$ vérifient $N'(x+y) = N'(x) + N'(y)$, alors il existe $u \in G$ tel que

$$N'(x+y) = N(u(x) + u(y)) \leq N(u(x)) + N(u(y)) \leq N'(x) + N'(y)$$

donc $N(u(x) + u(y)) = N(u(x)) + N(u(y))$ et donc, comme $N$ est euclidienne, $u(x)$ et $u(y)$ sont positivement liés, donc, comme $u$ est inversible, $x$ et $y$ sont positivement liés.

*– Étape 2 : Construction d'un point fixe.* Pour $u \in G$ posons $F_u = \{x \in K,\, u(x) = x\}$ et montrons que

$$\bigcap_{u \in G} F_u \neq \emptyset.$$

Comme les $F_u$ sont fermés dans le compact $K$, par la propriété de Borel-Lebesgue, il suffit de montrer :

$$\forall p \in \mathbb{N}^*, \forall (u_1, \ldots, u_p) \in G^p, \qquad \bigcap_{i=1}^{p} F_{u_i} \neq \emptyset.$$

Avec ces notations, posons $u = \dfrac{1}{p} \displaystyle\sum_{i=1}^{p} u_i$ et montrons que $u$ admet un point fixe. Fixons $x_0 \in K$ et définissons :

$$\forall k \in \mathbb{N}^*, \qquad x_k = \frac{1}{k+1} \sum_{\ell=0}^{k} \underbrace{u^\ell(x_0)}_{\in K} \in K \text{ par convexité.}$$

Comme $K$ est compact, il existe une extraction $\varphi$ et $a \in K$ telle que $x_{\varphi(k)} \to a$. Or

$$\forall k \in \mathbb{N}^*, \qquad u(x_k) = x_k + \frac{1}{k+1}\left(u^{k+1}(x_0) - x_0\right)$$

donc, comme $u(K) \subset K$ compact, le second membre tend vers 0 et donc $u(x_{\varphi(k)}) \to a$. Par continuité de $u$ et unicité de la limite, on en déduit que $u(a) = a$. Alors,

$$N'(a) \underset{G\text{-invariance}}{=} \frac{1}{p} \sum_{i=1}^{p} N'(u_i(a)) \geq N'(u(a)) \underset{G\text{-invariance}}{=} N'(a)$$

donc les $u_i(a)$ sont positivement liés. Comme ils sont de même normes $N'(a)$, ils sont égaux. Comme leur moyenne vaut $a$, on a $\forall i$, $u_i(a) = a$ *ie.* $a \in \displaystyle\bigcap_{i=1}^{p} F_{u_i}$. □

**Théorème 17.2**

*Soit $G$ un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$. Il existe une forme quadratique définie positive $q$ sur $\mathbb{R}^n$ telle que $G \subset O(q)$.*

▷ *– Étape 1 : Représentation de $G$.* On définit une loi de groupe sur $G$ par

$$\forall (A,B)\in G,\qquad A*B=BA.$$

Considérons l'application $\rho : G\to \mathrm{GL}(\mathcal{S}_n(\mathbb{R}))$ définie par :

$$\forall A\in G, \forall S\in\mathcal{S}_n(\mathbb{R}),\qquad \rho(A)(S)={}^tASA.$$

Comme $\rho(A*B)=\rho(A)\circ\rho(B)$ et $\rho(I_n)=\mathrm{Id}$, $\rho$ est bien définie.

Comme $\rho$ est continue et $G$ est compact, l'image $\widetilde{G}=\rho(G)$ est compacte.

*– Étape 2 : Construction d'un compact convexe non vide $\widetilde{G}$-stable.* Comme $G$ est compact, $\{{}^tMM,\ M\in G\}$ est un compact non vide inclus dans $\mathcal{S}_n^{++}(\mathbb{R})$ qui est convexe puisque

$$\mathcal{S}_n^{++}(\mathbb{R})=\bigcap_{X\in\mathbb{R}^n}\underbrace{\{A\in\mathcal{S}_n(\mathbb{R}),\ {}^tXAX>0\}}_{\text{convexe}}.$$

Alors, l'enveloppe convexe $K=\mathrm{Conv}(\{{}^tMM,\ M\in G\})$ est compacte et incluse dans $\mathcal{S}_n^{++}(\mathbb{R})$. De plus, elle est $\widetilde{G}$-stable. En effet, pour $A,M\in G$ on a

$$\rho(A)({}^tMM)={}^t(MA)(MA)$$

et on conclut par linéarité de $\rho(A)$ et la définition de $K$.

*– Étape 3 : Conclusion.* D'après le lemme, il existe $S\in K$ tel que $\forall u\in\widetilde{G}$, $u(S)=S$. Alors, $S\in\mathcal{S}_n^{++}(\mathbb{R})$ et, pour tout $A\in G$, ${}^tASA=S$, *ie.* $G\subset O(q_S)$. □

# 18 Sous-groupes distingués et caractères

F. Ulmer, *Théorie des groupes*, Ellipses. Lemme 17.20 et Proposition 17.22 page 158.

Recasage : 101, 103, 104, 107.

**Lemme 18.1**

*Soit $G$ un groupe fini et $\rho : G \to \mathrm{GL}(V)$ une représentation de caractère $\chi$. Alors $\forall g \in G$, $|\chi(g)| \leq \chi(1)$ et*

$$g \in \operatorname{Ker}\chi = \{g \in G,\ \chi(g) = \chi(1)\} \iff g \in \operatorname{Ker}\rho.$$

▷ Soit $g \in G$. D'après le théorème de Lagrange, il est d'ordre fini, donc $\rho(g)$ aussi. Ainsi, $\rho(g)$ est diagonalisable et les valeurs propres de $\rho(g)$ sont de module 1. Notons-les $\lambda_1, \dots, \lambda_{\dim V}$. Alors,

$$|\chi(g)| = \left| \sum_{i=1}^{\dim V} \lambda_i \right| \leq \dim V = \chi(1)$$

avec égalité si et seulement si ($|\lambda_i| = 1$) $\lambda_1 = \cdots = \lambda_{\dim V}$ et dans ce cas, $\lambda_i = 1$, $\forall i$, donc $\rho(g) = \mathrm{Id}$ *ie.* $g \in \operatorname{Ker}\rho$. Ainsi, $\operatorname{Ker}\chi \subset \operatorname{Ker}\rho$ et l'inclusion réciproque est immédiate. □

**Théorème 18.2**

*Soit $G$ un groupe fini et $\chi_1, \dots, \chi_m$ ses caractères irréductibles. Tout sous-groupe distingué $H \lhd G$ est de la forme*

$$H = \bigcap_{j \in J} \operatorname{Ker}\chi_j$$

*avec $J \subset \{1, \dots, m\}$.*

▷ Soit $H \lhd G$.

– *Étape 1 : $H$ est le noyau d'un caractère.* On considère l'action de $G$ sur $G/H$ par translation à gauche et $\varphi : G \to \mathfrak{S}_{|G/H|}$ le morphisme associé. Considérons la représentation par permutation

$$\rho_\varphi : \begin{array}{ccc} G & \to & \mathrm{GL}(V) \\ g & \mapsto & \big((e_i) \mapsto e_{\varphi(g)(i)}\big) \end{array}$$

où $V$ est un $\mathbb{C}$-espace vectoriel de dimension $\dfrac{|G|}{|H|}$ et $(e_i)$ est une base de $V$. Soit $\chi$ le caractère de cette représentation. D'après le lemme,

$$\operatorname{Ker}\chi = \operatorname{Ker}\rho_\varphi = \operatorname{Ker}\varphi = H.$$

Ainsi, les groupes distingués sont des noyaux de caractères de $G$.

– *Étape 2 : Conclusion.* Soit $V = \bigoplus_{i=1}^{s} a_i V_i$ une décomposition en sous-représentations irréductibles telle que $\chi_i$ est le caractère de $V_i$, $\forall i$. Alors :

$$g \in \operatorname{Ker}\chi \Leftrightarrow g \in \operatorname{Ker}\rho \Leftrightarrow \forall i,\ g \in \operatorname{Ker}\rho_i \Leftrightarrow \forall i,\ g \in \operatorname{Ker}\chi_i$$

donc $H = \operatorname{Ker}\chi = \bigcap_{i=1}^{s} \operatorname{Ker}\chi_i$. □

La table de $\mathfrak{S}_4$ est :

| | $(\mathrm{Id})_1$ | $(12)_6$ | $(123)_8$ | $(1234)_6$ | $(12)(34)_3$ |
|---|---|---|---|---|---|
| $\chi_{\mathrm{triv}}$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_\varepsilon$ | 1 | −1 | 1 | −1 | 1 |
| $\chi$ | 2 | 0 | −1 | 0 | 2 |
| $\chi_3$ | 3 | 1 | 0 | −1 | −1 |
| $\chi_W$ | 3 | −1 | 0 | 1 | −1 |

Les sous-groupes distingués de $\mathfrak{S}_4$ sont donc

$$\{\mathrm{Id}\}, \langle (12)(34) \rangle, \mathfrak{A}_4, \mathfrak{S}_4.$$

# 19 Table de $\mathfrak{S}_4$

Recasage : 161, 183.

– *Étape 1 : classes de conjugaison.* Il y a cinq classes de conjugaison, déterminées par le type de la permutation :
— $\{\mathrm{Id}\}$ : un élément
— les transpositions : $\binom{4}{2} = 6$ éléments
— les 3-cycles : $\binom{4}{3} \times 2 = 8$ éléments
— les 4-cycles : $4! \times \frac{1}{4} = 6$ éléments
— les doubles transpositions : $\binom{4}{2} \times \frac{1}{2} = 3$ éléments.
Il y a donc cinq caractères irréductibles.

– *Étape 2 : premiers caractères irréductibles.* On connait deux caractères de degré 1 : $\chi_{\mathrm{triv}}$ et $\chi_\varepsilon$.

| | $(\mathrm{Id})_1$ | $(12)_6$ | $(123)_8$ | $(1234)_6$ | $(12)(34)_3$ |
|---|---|---|---|---|---|
| $\chi_{\mathrm{triv}}$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_\varepsilon$ | 1 | $-1$ | 1 | $-1$ | 1 |
| | | | | | |
| | | | | | |
| | | | | | |

– *Étape 3 : isométries du tétraèdre régulier.* Notons $T$ un tétraèdre régulier centré en l'origine. Notons $e_1, e_2, e_3, e_4$ les sommets. On définit un morphisme de groupes

$$\begin{array}{rccl} & \mathfrak{S}_4 & \to & \mathrm{Is}(T) \\ \varphi : & & & \\ & \sigma & \mapsto & u : \begin{array}{ccc} T & \to & T \\ e_i & \mapsto & e_{\sigma(i)} \end{array} \end{array}$$

$\varphi$ est bien définie car $T$ est régulier et $(e_1, e_2, e_3, e_4)$ est un repère affine. De plus, $\sigma \in \operatorname{Ker}\varphi \Leftrightarrow \forall i,\ \sigma(i) = i \Leftrightarrow \sigma = \mathrm{Id}$ donc $\varphi$ est injective. Enfin, $\varphi$ est surjective puisqu'une isométrie envoie un sommet sur un sommet. Donc $\varphi$ est un isomorphisme.

On a donc $\varphi : \mathfrak{S}_4 \to \mathrm{Is}(T) \subset O(\mathbb{R}^3) \hookrightarrow \mathrm{GL}(\mathbb{C}^3)$ donc $\varphi$ induit une représentation de degré 3. Le caractère $\chi_3$ associé est $\forall \sigma \in \mathfrak{S}_4,\ \chi_3(\sigma) = \mathrm{Tr}(\varphi(\sigma))$. On effectue les calculs dans la base $(e_1, e_2, e_3)$ sachant que $e_4 = -e_1 - e_2 - e_3$. On a :

$$\mathrm{Mat}\,\varphi((12)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{donc} \qquad \chi_3((12)) = 1$$

$$\mathrm{Mat}\,\varphi((123)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad \text{donc} \qquad \chi_3((123)) = 0$$

$$\mathrm{Mat}\,\varphi((1234)) = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix} \qquad \text{donc} \qquad \chi_3((1234)) = -1$$

$$\mathrm{Mat}\,\varphi((12)(34)) = \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix} \qquad \text{donc} \qquad \chi_3((12)(34)) = -1.$$

De plus, $\chi_3$ est irréductible car

$$\langle \chi_3, \chi_3 \rangle = \frac{1}{|\mathfrak{S}_4|} \sum_{\sigma \in \mathfrak{S}_4} |\chi_3(\sigma)|^2 = \frac{1}{24} \left(3^2 + 6 \times 1^2 + 6 \times (-1)^2 + 3 \times (-1)^2\right) = 1.$$

On complète donc la table.

| | $(\mathrm{Id})_1$ | $(12)_6$ | $(123)_8$ | $(1234)_6$ | $(12)(34)_3$ |
|---|---|---|---|---|---|
| $\chi_{\mathrm{triv}}$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_\varepsilon$ | 1 | $-1$ | 1 | $-1$ | 1 |
| | | | | | |
| $\chi_3$ | 3 | 1 | 0 | $-1$ | $-1$ |
| | | | | | |

– *Étape 4 : construction d'une nouvelle représentation.* Considérons la représentation $W = \mathrm{Hom}_{\mathbb{C}}(V_3, V_\varepsilon)$. On a $\chi_W = \overline{\chi_3}\chi_\varepsilon = (3, -1, 0, 1, -1)$ donc $\chi_W$ est un nouveau caractère. De plus, il est irréductible car $\langle \chi_W, \chi_W \rangle = 1$. On complète donc la table :

| | $(\mathrm{Id})_1$ | $(12)_6$ | $(123)_8$ | $(1234)_6$ | $(12)(34)_3$ |
|---|---|---|---|---|---|
| $\chi_{\mathrm{triv}}$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_\varepsilon$ | 1 | $-1$ | 1 | $-1$ | 1 |
| | | | | | |
| $\chi_3$ | 3 | 1 | 0 | $-1$ | $-1$ |
| $\chi_W$ | 3 | $-1$ | 0 | 1 | $-1$ |

– *Étape 5 : relations d'orthogonalité.* Soit $\chi$ le dernier caractère irréductible. On a :

$$24 = |\mathfrak{S}_4| = \chi_{\mathrm{triv}}(\mathrm{Id})^2 + \chi_\varepsilon(\mathrm{Id})^2 + \chi_3(\mathrm{Id})^2 + \chi_W(\mathrm{Id})^2 + \chi(\mathrm{Id})^2 = 20 + \chi(\mathrm{Id})^2$$

donc $\chi$ est de degré 2. De plus, grâce à

$$\forall \sigma \in \mathfrak{S}_4 \backslash \{\mathrm{Id}\}, \qquad 0 = \sum_{\chi' \in \mathrm{Irr}(\mathfrak{S}_4)} \chi'(\mathrm{Id})\chi'(\sigma),$$

on obtient $\chi = (2, 0, -1, 0, 2)$ d'où la table

| | $(\mathrm{Id})_1$ | $(12)_6$ | $(123)_8$ | $(1234)_6$ | $(12)(34)_3$ |
|---|---|---|---|---|---|
| $\chi_{\mathrm{triv}}$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_\varepsilon$ | 1 | $-1$ | 1 | $-1$ | 1 |
| $\chi$ | 2 | 0 | $-1$ | 0 | 2 |
| $\chi_3$ | 3 | 1 | 0 | $-1$ | $-1$ |
| $\chi_W$ | 3 | $-1$ | 0 | 1 | $-1$ |

**Remarque :** Les sous-groupes distingués de $\mathfrak{S}_4$ sont les $\bigcap_{\chi \in \mathrm{Irr}(\mathfrak{S}_4)} \mathrm{Ker}\,\chi$ où $\mathrm{Ker}(\chi) = \{\sigma \in \mathfrak{S}^4,\ \chi(\sigma) = \chi(\mathrm{Id})\}$. On obtient que les sous-groupes distingués sont

$$\{\mathrm{Id}\}, \langle (12)(34) \rangle, \mathfrak{A}_4, \mathfrak{S}_4.$$

# 20 Théorème de Frobenius-Zolotarev

V. Beck, J. Malick, G. Peyré, *Objectif agrégation*, 2e édition, H&K. Exercice 5.4 page 251.

Recasage : 103, 105, 106, 108, 120, 123, 152.

**Théorème 20.1**

*Soient $p$ un nombre premier impair et $V$ un $\mathbb{F}_p$-espace vectoriel de dimension finie $n \in \mathbb{N}$. Pour tout $u \in \mathrm{GL}(V)$,*

$$\varepsilon(u) = \left(\frac{\det u}{p}\right)$$

*où, $\varepsilon(u)$ désigne la signature de $u$ vu comme permutation de $V$ et, pour $a \in \mathbb{F}_p$, le symbole de Legendre est défini par*

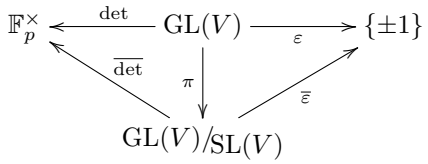
$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a = 0 \text{ mod } p \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon.} \end{cases}$$

▷ La restriction de la signature, $\varepsilon : \mathrm{GL}(V) \subset \mathfrak{S}(V) \to \{\pm 1\}$, toujours notée $\varepsilon$, est un morphisme de groupes.

– *Étape 1 : Montrons qu'il se factorise par le déterminant.* Comme $p > 2$, le groupe dérivé $D\,\mathrm{GL}(V)$ est $\mathrm{SL}(V)$. De plus, pour $u, v \in \mathrm{GL}(V)$,

$$\varepsilon(uvu^{-1}v^{-1}) = \varepsilon(u)\varepsilon(v)\varepsilon(u)^{-1}\varepsilon(v)^{-1} = 1$$

donc $\mathrm{SL}(V) = \langle uvu^{-1}v^{-1}, u, v \in \mathrm{GL}(V)\rangle \subset \operatorname{Ker}\varepsilon$. D'après la propriété universelle du quotient, $\varepsilon$ se factorise par un unique morphisme $\overline{\varepsilon}$ de sorte que $\varepsilon = \overline{\varepsilon} \circ \pi$ où $\pi : \mathrm{GL}(V) \to \mathrm{GL}(V)/\mathrm{SL}(V)$ est la projection canonique. De plus, $\det : \mathrm{GL}(V) \twoheadrightarrow \mathbb{F}_p^\times$ a pour noyau $\mathrm{SL}(V)$. Il existe donc un unique isomorphisme $\overline{\det}$ tel que le diagramme suivant est commutatif :




Posons $\delta = \overline{\varepsilon} \circ \overline{\det}^{-1}$ de sorte que $\delta$ est un morphisme de groupes $\mathbb{F}_p^\times \to \{\pm 1\}$ et $\varepsilon = \delta \circ \det$. (Par surjectivité de det, un tel $\delta$ est unique)

– *Étape 2 : Montrons que $\delta$ n'est pas le morphisme trivial.* Comme $V$ et $\mathbb{F}_{p^n}$ sont isomorphes comme espaces vectoriels, il suffit de trouver une bijection $\mathbb{F}_p$-linéaire de $\mathbb{F}_{p^n}$ sur lui-même de signature $-1$.

$\mathbb{F}_{p^n}^\times$ est cyclique de cardinal $p^n - 1$. Soit $g$ un générateur. L'application $\tau_g : x \in \mathbb{F}_{p^n} \mapsto gx \in \mathbb{F}_{p^n}$ est bien une bijection $\mathbb{F}_p$-linéaire de $\mathbb{F}_{p^n}$ sur lui-même et agit sur $\mathbb{F}_{p^n}^\times$ comme le $(p^n-1)$-cycle $(g, g^2, \ldots, g^{p^n-1})$, donc sa signature est $-1$ car $p^n - 1$ est pair.

– *Étape 3 : Montrons que $\delta$ est le symbole de Legendre.*

Analyse : Comme $\delta \not\equiv 1$, $\operatorname{Ker}\delta$ est un sous-groupe de $\mathbb{F}_p^\times$ d'indice 2. Or il existe un unique sous-groupe $H$ d'indice 2 dans $\mathbb{F}_p^\times$. Alors, si $x \notin H$, on a une partition $\mathbb{F}_p^\times = H \sqcup xH$ et $\delta(y) = 1$ si $y \in H$ et $\delta(y) = 0$ si $y \in xH$. $\delta$ est donc déterminé de façon unique. Il y a donc au plus un morphisme non trivial $\mathbb{F}_p^\times \to \{\pm 1\}$.

Synthèse : le symbole de Legendre est bien un morphisme de groupes car pour $a \in \mathbb{F}_p^\times$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. Il est non trivial car il y a exactement $\dfrac{p-1}{2}$ carrés dans $\mathbb{F}_p^\times$. □

**Application au morphisme de Frobenius :** Soit $n \geq 2$. On rappelle que le morphisme de Frobenius est défini par :

$$\varphi : \begin{array}{ccc} \mathbb{F}_{p^n} & \to & \mathbb{F}_{p^n} \\ x & \mapsto & x^p. \end{array}$$

$\varphi$ est d'ordre $n$. En effet, pour tout $x \in \mathbb{F}_{p^n}$,

$$\varphi^n(x) = x^{p^n} = x$$

donc $\varphi^n = \mathrm{Id}_{\mathbb{F}_{p^n}}$. Si $m \leq n$ et $\varphi^m = \mathrm{Id}_{\mathbb{F}_{p^n}}$ alors $X^{p^m} - X$ est non nul et a $|\mathbb{F}_{p^n}| = p^n$ racines sur le corps $\mathbb{F}_{p^n}$, donc $m = n$.

**On admet**[1] qu'il existe une base adaptée à $\varphi$ : il existe $x \in \mathbb{F}_{p^n}$ tel que $\mathcal{B} = (x, \varphi(x), \dots, \varphi^{n-1}(x))$ forme une base du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_{p^n}$. On a :

$$\mathrm{Mat}_{\mathcal{B}}(\varphi) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

qui est la matrice de permutation associée au $n$-cycle $\sigma \in \mathfrak{S}_n$. Alors $\det(\varphi) = \varepsilon(\sigma) = (-1)^{n-1}$. D'après le théorème de Frobenius-Zolotarev,

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

**Lemme 20.2**

*Si $k$ est un corps de cardinal $\geq 3$ et $n \geq 2$, alors le groupe dérivé $D\,\mathrm{GL}_n(k)$ de $\mathrm{GL}_n(k)$ est $\mathrm{SL}_n(k)$.*

▷ Voir Oraux X-ENS algèbre 2.

Soit $A, B \in \mathrm{GL}_n(k)$. On a $\det(ABA^{-1}B^{-1}) = \det(A)\det(B)\det(A)^{-1}\det(B)^{-1} = 1$ donc $D\,\mathrm{GL}_n(k) \subset \mathrm{SL}_n(k)$.

$\mathrm{SL}_n(k)$ étant engendré par les matrices de transvections, il suffit de montrer que toute matrice de transvection est un commutateur. Pour $1 \leq i \neq j \leq n$ et $\lambda \in k$, on pose $T_{ij}(\lambda) = I_n + \lambda E_{ij}$. Soit $a \notin \{0, 1\}$ et $D_i(a)$ la matrice de dilation où $a$ est à la position $ii$. Pour $b \in k$,

$$D_i(a)T_{ij}(b)D_i(a)^{-1} = D_i(a)(I_n + bE_{ij})D_i(a)^{-1} = I_n + abE_{ij} = T_{ij}(ab)$$

donc

$$D_i(a)T_{ij}(b)D_i(a)^{-1}T_{ij}(b)^{-1} = T_{ij}((a-1)b).$$

Lorsque $b$ décrit $k$, le scalaire $(a-1)b$ décrit $k$. Donc toute matrice de transvection est un commutateur. Donc $\mathrm{SL}_n(k) \subset D\,\mathrm{GL}_n(k)$. □

1. Ma proposition : on a $\pi_\varphi | X^n - 1$ et, si $\deg(\pi_\varphi) < n$, on a $\pi_\varphi = X^m + a_{m-1}X^{m-1} + \cdots + a_0$ avec $a_i \in \mathbb{F}_p$. Alors, $\varphi^m + a_{m-1}\varphi^{m-1} + \cdots + a_0\mathrm{Id}_{\mathbb{F}_{p^n}} = 0$ donc la famille $(\mathrm{Id}_{\mathbb{F}_{p^n}}, \varphi, \dots, \varphi^m)$ est liée dans $\mathbb{F}^p$ donc dans $\mathbb{F}^{p^n}$ ce qui contredit le lemme de Dedekind (voir le développement qui lui est consacré). Donc $\pi_\varphi = X^n - 1$. Alors, il existe $x \in \mathbb{F}_{p^n}$ tel que $\pi_{\varphi,x} = \pi_\varphi$ c'est-à-dire tel que $(x, \varphi(x), \dots, \varphi^{n-1}(x))$ est une base.

# 21 Théorème de Kronecker et application aux sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*, 3e édition, Cassini. Exercice 5.33 page 213 pour le premier théorème.

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 2*, 3e édition, Cassini. Exercice 3.20 page 205 pour le second théorème.

Recasage : 142, 144.

**Théorème 21.1**

*Soit $P \in \mathbb{Z}[X]$ unitaire dont les racines complexes sont de module inférieur ou égal à 1. On suppose que $P(0) \neq 0$. Alors les racines de $P$ sont des racines de l'unité.*

▷ Notons $\Omega_n$ l'ensemble des polynômes unitaires de $\mathbb{Z}[X]$, de degré $n$, dont les racines sont de module inférieur ou égal à 1.

– *Étape 1 : Montrons que $\Omega_n$ est fini.* Soit $P \in \Omega_n$. Notons $z_1, \dots, z_n$ ses racines et $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires associées. Pour tout $k \in [\![1, n]\!]$, on a $\sigma_k \in \mathbb{Z}$ et, comme $|z_1|, \dots, |z_n| \leq 1$,

$$|\sigma_k| = \left| \sum_{\substack{I \in \mathfrak{P}([\![1,n]\!]) \\ \#I = k}} \prod_{i \in I} z_i \right| \leq \#\{I \in \mathfrak{P}([\![1, n]\!]),\ \#I = k\} = \binom{n}{k}.$$

L'ensemble des $(\sigma_k)_{1 \leq k \leq n}$ est donc fini. Comme tout $P \in \Omega_n$ s'écrit $P = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n$, on en déduit que $\Omega_n$ est fini (et $|\Omega_n| \leq 2^n - 1$).

– *Étape 2 : Principe des tiroirs.* Soit $P \in \Omega_n$ que l'on écrit

$$P = \prod_{i=1}^{n} (X - z_i).$$

Montrons que pour tout $k \in \mathbb{N}^*$, $P_k = \prod_{i=1}^{n} (X - z_i^k) \in \Omega_n$.

⋆ $P_k$ est bien unitaire de degré $n$ et ses racines $z_i^k$ sont de module inférieur ou égal à 1.

⋆ Il reste donc à vérifier que $P_k \in \mathbb{Z}[X]$. Or pour $i \in [\![1, n]\!]$, le coefficient de $X^{n-i}$ dans l'écriture de $P_k$ dans la base canonique est $(-1)^i \sigma_i(z_1^k, \dots, z_n^k)$ où $\sigma_i(z_1^k, \dots, z_n^k)$ sont les fonctions symétriques élémentaires associées à $z_1^k, \dots, z_n^k$. Ces fonctions sont des polynômes symétriques en $z_1, \dots, z_n$ à coefficients dans $\mathbb{Z}$. D'après le théorème de structure, $\sigma_i(z_1^k, \dots, z_n^k) \in \mathbb{Z}[\sigma_1, \dots, \sigma_n]$ pour tout $1 \leq i \leq n$. Ainsi, $P_k \in \mathbb{Z}[X]$.

Ainsi, comme $\Omega_n$ est fini, il existe $k > \ell$ tel que $P_k = P_\ell$ donc $\forall 1 \leq i \leq n$, $z_i^k = z_i^\ell$, d'où, comme 0 n'est pas une racine de $P$, $z_i^{k-\ell} = 1$, $\forall 1 \leq i \leq n$. □

**Corollaire 21.2**

*Soient $m \geq 3$ et $n \in \mathbb{N}$. Si $G$ est un groupe fini de $\mathrm{GL}_n(\mathbb{Z})$ alors $G$ est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$.*

▷ Il suffit de montrer que la projection canonique $G \to \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$ est injective.

Soit $A \in G$ tel que $\overline{A} = \overline{I_n} \in \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$. Il existe $B \in \mathcal{M}_n(\mathbb{Z})$ telle que $A = I_n + B$. Soit $\beta$ une valeur propre de $B$. Alors $\alpha = 1 + m\beta$ est valeur propre de $A$. Or, d'après le théorème de Lagrange, $A^{|G|} = I_n$ donc $\alpha^{|G|} = 1$ et en particulier $|\alpha| = 1$. Alors,

$$|\beta| = \frac{|\alpha - 1|}{m} \leq \frac{2}{m} < 1.$$

Ainsi, $(-1)^n \chi_B \in \mathbb{Z}[X]$ est unitaire et ses racines sont de module $< 1$. On déduit du théorème de Kronecker que $\chi_B = (-X)^n$.

Or, comme $X^{|G|} - 1$ est scindé à racines simples et annule $A$, $A$ est diagonalisable, donc $B$ est diagonalisable. Ainsi, $B = 0$ et $A = I_n$. □

**Corollaire 21.3**

*Si $G$ est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$, alors*

$$|G| \leq (3^n - 3^{n-1})(3^n - 3^{n-2}) \cdots (3^n - 3)(3^n - 1).$$

# 22 Théorème de Sophie Germain

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*, 3e édition, Cassini. Exercice 4.39 page 167.

Recasage : 120, 121, 126.

**Théorème 22.1**

*Soit $p$ un nombre premier de Sophie Germain ie. $q = 2p+1$ est aussi premier. Il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $xyz \equiv 0$ mod $q$ et $x^p + y^p + z^p = 0$.*

▷ Soit, par l'absurde, $(x,y,z) \in \mathbb{Z}^3$ tel que $xyz \equiv 0 \bmod q$ et $x^p + y^p + z^p = 0$. Quitte à considérer $x' = \dfrac{x}{x \wedge y \wedge z}, y' = \dfrac{y}{x \wedge y \wedge z}, z' = \dfrac{z}{x \wedge y \wedge z}$ on peut considérer $x \wedge y \wedge z = 1$.

– *Étape 1 : $q$ divise l'un des trois entiers.* Supposons par l'absurde que $q$ ne divise pas $x, y$ et $z$. Alors, par le petit théorème de Fermat, $x^{q-1} \equiv 1 \bmod q$ donc $(x^p)^2 \equiv 1 \bmod q$ d'où, comme $\mathbb{Z}/q\mathbb{Z}$ est un corps, $x^p \equiv \pm 1 \bmod q$. De même, $y, z \equiv \pm 1 \bmod q$. Alors, $0 = x^p + y^p + z^p \bmod q \in \{\pm 1, \pm 3\}$ : absurde. On peut donc supposer que $q$ divise $x$. On a également montré que toute puissance $p$-ième est congrue à 0, 1, ou $-1$ modulo $q$.

– *Étape 2 : $x, y, z$ sont premiers entre eux deux à deux.* Si, par l'absurde, $x \wedge y \neq 1$, soit $p'$ un diviseur premier commun à $x$ et $y$. Alors, $p'|x^p + y^p = -z^p$ donc $p'|z^p$ donc $p'|z$, ce qui contredit $x \wedge y \wedge z = 1$. Ainsi, $x \wedge y = 1$ et de même pour les autres couples. On en déduit que $q \nmid y, z$.

– *Étape 3 : Factorisation de $x^p, y^p, z^p$ en produit de puissance $p$-ièmes.* On a :

$$-x^p = y^p + z^p = (y+z)\left(\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k\right).$$

Supposons par l'absurde que $y+z$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ ne sont pas premiers entre eux et soit $p'$ un diviseur premier commun. Alors $p'^2 | -x^p$ donc $p'|x$. De plus, $y \equiv -z \bmod p'$ donc

$$0 \equiv \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p y^{p-1} \bmod p'$$

donc $p'|py^{p-1}$. Comme $p'$ est premier :
⋆ soit $p'|p$ *ie.* $p' = p$ et alors $p|x$ et $p|xyz$ : absurde.
⋆ soit $p'|y^{p-1}$ donc $p'|y$ et $x \wedge y \geq p'$ : absurde.

Ainsi, $y+z$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux et leur produit est une puissance $p$-ième. Alors il existe $(a, \alpha) \in \mathbb{Z}^2$ tel que

$$y + z = a^p \qquad \text{et} \qquad \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p.$$

De même, il existe $b, c \in \mathbb{Z}$ tels que $x + y = c^p$ et $x + z = b^p$.

– *Conclusion.* Comme $y \equiv c^p \bmod q$ et $q \nmid y$, on a $y \equiv \pm 1 \bmod q$. De même, $z \equiv \pm 1 \bmod q$. Supposons par l'absurde que $q \nmid a$. Alors $a^p \equiv \pm 1 \bmod q$ et donc

$$0 \equiv 2x = b^p + c^p - a^p \bmod q \in \{\pm 1, \pm 3\} \qquad \text{absurde.}$$

Donc $q|a$. Ainsi, $y + z = a^p \equiv 0 \bmod q$, donc

$$\alpha^p = \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p y^{p-1} \equiv p \bmod q$$

ce qui contredit $\alpha^p \bmod q \in \{0, \pm 1\}$. □

**Lemme 22.2**

*Soient $a, b$ deux entiers naturels non nuls premiers entre eux et $k \geq 2$. S'il existe $c \in \mathbb{N}$ tel que $ab = c^k$ alors $a$ et $b$ sont aussi puissance $k$-ièmes d'entiers.*

▷ Écrivons la décomposition de $a, b$ et $c$ en produits de facteurs premiers :

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p} \qquad b = \prod_{p \in \mathcal{P}} p^{\beta_p} \qquad c = \prod_{p \in \mathcal{P}} p^{\gamma_p}$$

où $(\alpha_p), (\beta_p), (\gamma_p) \in \mathbb{N}^{(\mathcal{P})}$. Comme $ab = c^k$, l'unicité de la décomposition de $ab$ donne

$$\forall p \in \mathcal{P}, \qquad \alpha_p + \beta_p = k\gamma_p.$$

Or comme $a \wedge b = 1$, $\forall p \in \mathcal{P}$, $\alpha_p \beta_p = 0$, donc $\forall p \in \mathcal{P}$, $k | \alpha_p, \beta_p$. □

# 23 Théorème de structure des groupes abéliens finis

P. Colmez, *Éléments d'analyse et d'algèbre*, 2011, Éditions de l'École polytechnique.. Proposition I.2.28, Lemme I.2.32 et Théorème I.2.33 page 250.

Recasage : 102, 104, 107, 110.

**Lemme 23.1**

*Soit $G$ un groupe abélien fini. L'application*

$$i : \begin{array}{ccc} G & \to & \widehat{\widehat{G}} \\ g & \mapsto & (\chi \mapsto \chi(g)) \end{array}$$

*est un isomorphisme de groupes.*

▷ *– Étape 1 : $i$ est un morphisme de groupes.*

*– Étape 2 :* $|G| = |\widehat{\widehat{G}}|$. Comme $G$ est abélien, les classes de conjugaison sont réduites à un élément et sont au nombre de $|G|$. De plus, comme $G$ est abélien, $\widehat{G}$ est l'ensemble des caractères irréductibles de $G$. D'après la formule de Burnside, on a alors $|\widehat{G}| = |G|$. Comme $\widehat{G}$ est abélien, le même raisonnement montre que $|\widehat{\widehat{G}}| = |\widehat{G}| = |G|$. Il suffit donc de montrer le point suivant.

*– Étape 3 : $i$ est injectif.* Soit $g \in G$ tel que $i(g) = i(e)$. Alors, $\forall \chi \in \widehat{G}$, $\chi(g) = \chi(e) = 1$. Notons $\mathbf{1}_{\{g\}} : h \in G \mapsto \delta_{gh}$ et décomposons-là dans la base des caractères :

$$\mathbf{1}_{\{g\}} = \sum_{\chi \in \widehat{G}} \langle \mathbf{1}_{\{g\}}, \chi \rangle \chi = \sum_{\chi \in \widehat{G}} \left( \frac{1}{|G|} \sum_{h \in G} \mathbf{1}_{\{g\}} \overline{\chi(h)} \right) \chi = \sum_{\chi \in \widehat{G}} \frac{\overline{\chi(g)}}{|G|} \chi = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi.$$

En évaluant cette égalité en $e$, on obtient :

$$\mathbf{1}_{\{g\}}(e) = \frac{|\widehat{G}|}{|G|} = 1$$

donc $g = e$, et $i$ est injectif. □

**Lemme 23.2**

*Soit $G$ un groupe abélien fini. Alors $G$ et $\widehat{G}$ ont même exposant.*

▷ Notons $N_G, N_{\widehat{G}}$ les exposants respectifs de $G$ et $\widehat{G}$. Pour $\chi \in \widehat{G}$, on a :

$$\forall g \in G, \qquad \chi^{N_G}(g) = \chi(g)^{N_G} = \chi(g^{N_G}) = \chi(e) = 1$$

donc $N_2 \leq N_1$. Le même raisonnement montre que $N_{\widehat{\widehat{G}}} \leq N_{\widehat{G}}$. Or $\widehat{\widehat{G}} \simeq G$ donc $N_G = N_{\widehat{\widehat{G}}} \leq N_{\widehat{G}} \leq N_G$ donc $N_G = N_{\widehat{G}}$. □

**Théorème 23.3**

*Soit $G$ un groupe abélien fini. Il existe $r \in \mathbb{N}$, $N_1, \dots, N_r \in \mathbb{N}$ avec $N_1$ l'exposant de $G$, tels que $\forall 1 \leq i \leq r-1$, $N_{i+1} | N_i$ et $G \simeq \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$.*

▷ On procède par récurrence forte sur $n = |G|$.

– $n = 1$ : ok.

– Soit $n \in \mathbb{N}^*$ tel que le théorème est vrai pour tout groupe abélien de cardinal $\leq n$. Soit un groupe abélien $G$ de cardinal $n+1$. Notons $N_1$ l'exposant de $G$. Comme $\widehat{G}$ est abélien, son exposant (égal à $N_1$ d'après le lemme) est le maximum des ordres de ses éléments. Soit donc $\chi_1 \in \widehat{G}$ d'ordre $N_1$.

⋆ *Étape 1 : $\chi_1(G) = \mathbb{U}_{N_1}$, le groupe des racines $N_1$-ièmes de l'unité.* En effet,$\chi_1(G)$ en est un sous-groupe car $\chi_1^{N_1} \equiv 1$. De plus, si, par l'absurde $|\chi(G)| < N_1$ alors pour tout $g \in G$, l'ordre de $\chi(g)$ dans $\mathbb{U}_{N_1}$ est $< N_1$. Alors, l'exposant

$N_2$ de $\chi(G)$ vérifie $N_2 < N_1$, *ie.* $\chi^{N_2} \equiv 1$, ce qui contredit le fait que $\chi_1$ est d'ordre $N_1$.

$\star$ *Étape 2 : $G \simeq \mathbb{Z}/N_1\mathbb{Z} \times G_1$ avec $|G_1| \leq n$.* Soit $x_1$ tel que $\chi(x_1) = e^{2i\pi/N_1}$. Alors $x_1$ est d'ordre $N_1$ donc $H_1 = \langle x_1 \rangle$ est isomorphe à $\mathbb{Z}/N_1\mathbb{Z}$. Si $N_1 = |G|$, alors on a démontré le résultat. On suppose désormais $N_1 \neq |G|$. Posons $G_1 = \operatorname{Ker} \chi_1$. On a bien $|G_1| \leq n$. $\chi_1$ induit un morphisme surjectif de $H_1$ sur $\mathbb{U}_{N_1}$. Par égalité des cardinaux finis, il est bijectif. Notons $\alpha$ sa réciproque et montrons que $G = H_1 G_1$. Si $x \in G$, alors $a = \alpha(\chi_1(x)) \in H_1$ et $b = a^{-1}x$ vérifie $\chi_1(b) = \chi_1(a)^{-1}\chi_1(x) = 1$ donc $b \in G_1$ et on a bien $x \in H_1 G_1$. Comme de plus $H_1 \cap G_1 = \{1\}$ par injectivité de $\chi_1$ sur $H_1$, on en déduit que $G \simeq H_1 \times G_1$.

$\star$ On conclut par hypothèse de récurrence car $|G_1| \leq n$. □

## Deuxième partie
# Analyse et probabilité

## 24 Densité des polynômes orthogonaux

V. Beck, J. Malick, G. Peyré, *Objectif Agrégation*, 2e édition, H&K. Exercice 3.7 page 140

Recasage : 201, 202, 207, 209, 213, 245, 250.

**Théorème 24.1**

*Soit $I$ un intervalle de $\mathbb{R}$ et $\rho$ une fonction poids telle qu'il existe $a > 0$ tel que*

$$\int_I e^{a|x|}\rho(x)dx < +\infty.$$

*La famille des polynômes orthogonaux $(P_n)_{n\in\mathbb{N}}$ associés à $\rho$ forme une base hilbertienne de $L^2(I,\rho)$.*

▷ Comme $(P_n)_{n\in\mathbb{N}}$ est orthonormée, il suffit de vérifier que la famille est totale. Notons $g_n : x \mapsto x^n$. Comme $\mathrm{Vect}(P_n) = \mathrm{Vect}(g_n)$, d'après le critère de densité, il suffit de considérer $f \in \mathrm{Vect}(g_n)^\perp$ et montrer que $f = 0$.

– *Étape 1 : Transformation de Fourier et prolongement.* Posons $\varphi = f\rho\mathbf{1}_I$. On a $\forall t \in \mathbb{R}$, $|t| \leq \dfrac{1+t^2}{2}$ donc

$$\int_{\mathbb{R}} |\varphi| = \int_I |f|\rho \leq \int_I (1+|f|)\rho < +\infty$$

donc $\varphi \in L^1(\mathbb{R})$. Notons

$$\widehat{\varphi} : \xi \in \mathbb{R} \mapsto \int_{\mathbb{R}} \varphi(x)e^{-i\xi x}\mathrm{d}x$$

sa transformée de Fourier et montrons que $\widehat{\varphi}$ se prolonge en une fonction holomorphe sur $B_a = \left\{z \in \mathbb{C},\, |\operatorname{Im} z| < \dfrac{a}{2}\right\}$. Posons

$$g : \begin{array}{ccc} B_a \times I & \to & \mathbb{R} \\ (z,x) & \mapsto & e^{-izx}f(x)\rho(x). \end{array}$$

On a :
- ⋆ $\forall z \in B_a$, $x \in I \mapsto g(z,x)$ est mesurable,
- ⋆ $\forall x \in I$, $z \in B_a \mapsto g(z,x)$ est holomorphe,
- ⋆ $\forall (z,x) \in B_a \times I$, $|g(z,x)| \leq e^{\frac{a|x|}{2}}|f(x)|\rho(x)$ indépendante de $z$ et intégrable sur $I$ car,

$$\int_I |g(z,x)|\mathrm{d}x \leq \int_I e^{\frac{a|x|}{2}}|f(x)|\rho(x)\mathrm{d}x \leq \left(\int_I e^{a|x|}\rho(x)\mathrm{d}x\right)^{1/2}\left(\int_I |f(x)|^2\rho(x)\mathrm{d}x\right)^{1/2} < +\infty$$

par l'inégalité de Cauchy-Schwarz dans $L^2(I,\rho)$. D'après le théorème d'holomorphie de Lebesgue, la fonction

$$F : \begin{array}{ccc} B_a & \to & \mathbb{C} \\ z & \mapsto & \displaystyle\int_I g(z,x)\mathrm{d}x \end{array}$$

est holomorphe sur $B_a$ et

$$\forall n \in \mathbb{N}, \forall z \in B_a, \qquad F^{(n)}(z) = (-i)^n \int_I x^n e^{-izx}f(x)\rho(x)\mathrm{d}x.$$

– *Conclusion.* On a donc

$$\forall n \in \mathbb{N}, \qquad F^{(n)}(0) = (-1)^n\langle f, g_n\rangle_\rho = 0.$$

Par unicité du développement en série entière d'une fonction holomorphe, il existe un voisinage $V \subset B_a$ de 0 sur lequel $F \equiv 0$. Alors, d'après le principe des zéros isolés, $F \equiv 0$ sur $B_a$. En particulier, $\widehat{\varphi} = F_{\restriction \mathbb{R}} = 0$ d'où, par injectivité de la transformée de Fourier sur $L^1$, $\varphi = 0$ presque partout. Alors, comme $\rho > 0$, on a $f = 0$ presque partout. □

**Contre exemple lorsque la condition de décroissance n'est pas vérifiée** Considérons $I = \mathbb{R}_+^*$ et $\rho(x) = x^{-\ln x}$. Soit $f(x) = \sin(2\pi \ln x)$. On a $f \in L^2(I, \rho)$ et, pour tout $n \in \mathbb{N}$,

$$\begin{aligned}\int_{\mathbb{R}_+^*} x^n \sin(2\pi \ln x) x^{-\ln x} \mathrm{d}x &\underset{y=\ln x}{=} \int_{\mathbb{R}} e^{(n+1)y} \sin(2\pi y) e^{-y^2} \mathrm{d}y \\ &= e^{\left(\frac{n+1}{2}\right)^2} \int_{\mathbb{R}} e^{-\left(y^2 - \frac{n+1}{2}\right)} \sin(2\pi y) \mathrm{d}y \\ &\underset{t=y-\frac{n+1}{2}}{=} e^{\left(\frac{n+1}{2}\right)^2} \int_{\mathbb{R}} e^{-t^2} \sin(2\pi t) \mathrm{d}t = 0\end{aligned}$$

donc $f \in \mathrm{Vect}(g_n)^\perp$.

# 25 Équation de Bessel

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Analyse 4*, Cassini. Exercice 2.15 page 101

Recasage : 152, 160, 170, 171, 203, 219, 253.

**Proposition 25.1**

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

$$xy'' + y' + xy = 0 \tag{E}$$

*vérifiant* $J_0(0) = 1$. *De plus, si* $f$ *est solution de* $(E)$ *sur* $]0, a[$ *alors* $(f, J_0)$ *est libre si et seulement si* $f$ *n'est pas bornée au voisinage de 0.*

▷ On commence par chercher une solution de $(E)$ développable en série entière au voisinage de 0.

– *Étape 1 : Analyse.* Soit $f$ une solution de $(E)$ développable en série entière au voisinage de 0. Il existe $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ et $R > 0$ tels que

$$\forall x \in ]-R, R[, \qquad f(x) = \sum_{n=0}^{+\infty} a_n x^n.$$

Or, pour $x \in ]-R, R[$, on a

$$xf(x) = \sum_{n=1}^{+\infty} a_{n-1} x^n,$$

$$f'(x) = \sum_{n=1}^{+\infty} n a_n x^{n-1} = \sum_{n=0}^{+\infty} (n+1) a_{n+1} x^n,$$

$$xf''(x) = \sum_{n=2}^{+\infty} n(n-1) a_n x^{n-1} = \sum_{n=1}^{+\infty} (n+1) n a_{n+1} x^n,$$

donc, comme $f$ satisfait $(E)$,

$$\forall x \in ]-R, R[, \qquad a_1 + \sum_{n=1}^{+\infty} \left[(n+1)^2 a_{n+1} + a_{n-1}\right] x^n = 0.$$

Par unicité du développement en série entière de $x \mapsto 0$, on en déduit :

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

On en déduit par récurrence que $\forall n \in \mathbb{N}$, $a_{2n+1} = 0$ et

$$a_{2n} = \frac{-a_{2(n-1)}}{(2n)^2} = \frac{a_{2(n-2)}}{(2n)^2 (2(n-1))^2} = \cdots = \frac{(-1)^n a_0}{(2n)^2 (2(n-1))^2 \cdots 2^2} = \frac{(-1)^n a_0}{4^n (n!)^2}.$$

Ainsi,

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

– *Étape 2 : Synthèse.* Cette série entière a un rayon de convergence $R = \infty$ d'après le critère de d'Alembert puisque

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

Alors, les calculs précédents assurent que $f$ est solution de $(E)$.

Posons $J_0 : x \in \mathbb{R} \mapsto \sum_{n=0}^{+\infty} \frac{(-1)^n}{4^n (n!)^2} x^{2n}$. On a montré que $J_0$ est l'unique solution de $(E)$ développable en série entière au voisinage de 0 valant 1 en 0.

Soit $f$ une solution de $(E)$ sur un intervalle $]0, a[$.

– *Étape 3 : condition nécessaire.* Supposons que $(f, J_0)$ est une famille liée. Alors $f$ est bornée au voisinage de 0.

– *Étape 4 : condition suffisante.* Supposons que $(f, J_0)$ est libre. Sur $]0, a[$, $(E)$ s'écrit

$$y'' + \frac{1}{x} y' + y = 0$$

donc, d'après le théorème de Cauchy-Lipschitz linéaire, l'espace des solutions est de dimension 2. Ainsi, $(f, J_0)$ en est une base, donc le wronskien $w = f' J_0 - f J_0'$ ne s'annule pas. Or

$$\forall x \in ]0, a[, \qquad w'(x) = \frac{-w(x)}{x}$$

donc il existe $C \neq 0$ telle que $\forall x \in ]0, a[$, $w(x) = \frac{C}{x}$.

Supposons par l'absurde que $f$ est bornée au voisinage de 0. Alors, comme $J_0(x) \xrightarrow[x \to 0^+]{} 1$ et $J_0'(x) \xrightarrow[x \to 0^+]{} 0$, l'égalité

$$\forall x \in ]0, a[, \qquad f'(x) J_0(x) - f(x) J_0'(x) = \frac{C}{x}$$

implique que $f'(x) \underset{x \to 0^+}{\sim} \frac{C}{x}$. Alors, d'après le théorème de sommation des équivalents, pour $x_0 \in ]0, a[$,

$$f(x) - f(x_0) = \int_{x_0}^{x} f'(t) \mathrm{d}t \underset{x \to 0^+}{\int_{x_0}^{x}} \frac{C}{t} \mathrm{d}t = C(\ln x - \ln x_0)$$

donc $f(x) \underset{x \to 0^+}{\sim} C \ln x$ : absurde.

– *Conclusion :* $J_0$ est bien l'unique solution de $(E)$ vérifiant $J_0(0) = 1$. □

# 26 Équation de la chaleur dans une barre

H. Queffélec, C. Zuily, *Analyse pour l'agrégation*, 4e édition, Dunod. Théorème VI.7, page 109.

Recasage : 209, 222, 241, 256.

On considère le problème suivant : trouver une fonction $u$ telle que

$$u \in \mathcal{C}^0(\overline{Q}) \cap \mathcal{C}_1^2(Q) \tag{6}$$
$$\partial_t u - \partial_{xx}^2 u = 0 \qquad \text{sur } Q \tag{7}$$
$$u(0,t) = u(L,t) = 0 \qquad t \geq 0 \tag{8}$$
$$u(x,0) = h(x) \quad x \in [0,L]. \tag{9}$$

où $h \in \mathcal{C}^1([0,L])$ telle que $h(0) = h(L) = 0$, et $\mathcal{C}_1^2(Q)$ est l'ensemble des fonctions de $(x,t)$ dérivables en $t$ et deux fois dérivables en $x$.

Montrons que $(1)-(4)$ admet une solution de classe $\mathcal{C}^\infty$ sur $Q$.

On cherche $u$ de la forme $u(x,t) = f(x)g(t)$. Alors (2) impose

$$\forall (x,t) \in Q, \qquad g'(t)f(x) = f''(x)g(t).$$

En supposant que $u$ ne s'annule pas sur $Q$, on en déduit qu'il existe une constante $\lambda \in \mathbb{R}$ telle que

$$\forall (x,t) \in Q, \qquad \frac{f''(x)}{f(x)} = \lambda = \frac{g'(t)}{g(t)}.$$

$\star$ 1er cas : $\lambda > 0$. Alors il existe $A, B \in \mathbb{R}$ tels que $\forall x \in [0,L]$, $f(x) = Ae^{\sqrt{\lambda}x} + Be^{-\sqrt{\lambda}x}$. Mais (3) impose

$$\begin{cases} A + B &= 0 \\ Ae^{\sqrt{\lambda}L} + Be^{-\sqrt{\lambda}L} &= 0. \end{cases}$$

Comme $\begin{vmatrix} 1 & 1 \\ e^{\sqrt{\lambda}L} & e^{-\sqrt{\lambda}L} \end{vmatrix} = -2\operatorname{sh}(\sqrt{\lambda}L) \neq 0$, on en déduit que $A = B = 0 = u(x,t)$ ce qui contredit l'hypothèse.

$\star$ 2e cas : $\lambda = 0$. Alors il existe $A, B \in \mathbb{R}$ tels que $\forall x \in [0,L]$, $f(x) = Ax + B$. Mais (3) impose $B = 0$ et $A = 0$ : contradiction.

Ainsi, $\lambda = -\xi^2$ avec $\xi \in \mathbb{R}$. Il existe donc $(A,B) \in \mathbb{R}^2 \backslash \{(0,0)\}$ tel que :

$$\forall (x,t) \in Q, \qquad f(x) = A\cos\xi x + B\sin\xi x \qquad g(t) = e^{-\xi^2 t}.$$

La condition (3) impose $A = 0$ et $B\sin\xi L = 0$ d'où, $\xi \in \dfrac{\pi}{L}\mathbb{Z}$.

On a donc une famille de solutions possibles pour (1)-(3) :

$$\forall (b_n)_{n\in\mathbb{Z}} \in \mathbb{R}^{\mathbb{Z}}, \forall n \in \mathbb{Z}, \qquad u_n : (x,t) \in \overline{Q} \mapsto b_n \sin\left(\frac{n\pi x}{L}\right) \exp\left(-\frac{n^2\pi^2}{L^2}t\right).$$

On cherche désormais à remplir la condition (4), en s'appuyant sur la linéarité de l'équation.

Soit $\widetilde{h}$ la fonction $2L$-périodique, impaire, telle que $\widetilde{h}_{|[0,L]} = h$. Comme $h(0) = h(L) = 0$, $\widetilde{h}$ est continue sur $\mathbb{R}$ et $\mathbb{C}^1$ par morceaux. Sa série de Fourier converge donc uniformément sur $\mathbb{R}$ vers $\widetilde{h}$. Comme $\widetilde{h}$ est impaire, on a donc :

$$\forall x \in \mathbb{R}, \qquad \widetilde{h}(x) = \sum_{n=1}^{+\infty} b_n \sin\left(\frac{n\pi x}{L}\right)$$

où, pour tout $n \in \mathbb{Z}$, $b_n = \dfrac{2}{L}\displaystyle\int_0^L h(x)\sin\left(\frac{n\pi x}{L}\right)\mathrm{d}x$ et la série converge normalement sur $\mathbb{R}$. On définit :

$$u : (x,t) \in \overline{Q} \mapsto \sum_{n=1}^{+\infty} b_n \sin\left(\frac{n\pi x}{L}\right) \exp\left(-\frac{n^2\pi^2}{L^2}t\right) =: \sum_{n=1}^{+\infty} u_n(x,t). \tag{5}$$

Comme les $(u_n)_{n\in\mathbb{N}^*}$ sont continues et la série converge uniformément, $u$ est continue sur $\overline{Q}$. Montrons qu'elle est $\mathcal{C}^\infty$ sur $Q$ et qu'on peut dériver terme à terme. Les $(u_n)$ sont de classe $\mathcal{C}^\infty$ sur $Q$ et, pour tout $n\in\mathbb{N}^*$, $\alpha\in\mathbb{N}^2$ et $\varepsilon>0$, on a :

$$\forall (x,t)\in[0,L]\times[\varepsilon,+\infty[,\qquad |\partial^\alpha u_n(x,t)|\leq C_k|b_n|n^{2k}\exp\left(-\frac{n^2\pi^2}{L^2}\varepsilon\right)$$

qui est le terme général d'une série convergente, uniformément en $(t,x)$. D'après le théorème de dérivation, $u$ est donc $\mathcal{C}^\infty$ sur $Q$ et on peut dériver terme à terme.

Ainsi,

— $u$ vérifie (1).

— On vérifie que $\partial_t u-\partial^2_{xx}u=\sum_{n=1}^{+\infty}(\partial_t u_n-\partial^2_{xx}u_n)=0$ donc $u$ vérifie (2).

— si $t\geq 0$, $u(0,t)=u(0,L)=0$ donc $u$ vérifie (3).

— si $x\in[0,L]$, $u(x,0)=\sum_{n=1}^{+\infty}b_n\sin\left(\frac{n\pi x}{L}\right)=\widetilde{h}(x)=h(x)$ donc $u$ vérifie (4).

On a donc exhibé une solution $u$ à l'équation de la chaleur, de classe $\mathcal{C}^\infty$ à l'intérieur de la barre juste après l'instant initial.

Y-a-t-il unicité ? Démontrons le lemme suivant.

**Lemme 26.1 (*Principe du maximum*)**

*Soit $u\in\mathcal{C}^0(\overline{Q})\cap\mathcal{C}^2_1(Q)$ telle que $Pu(x,t)\geq 0$ sur $Q$, où $P=\partial^2_{xx}-\partial_t$. Soient $T>0$ et $K=[0,L]\times[0,T]$. Alors*

$$\sup_K u=\sup_{K\cap\partial Q}u.$$

▷ Soient $\varepsilon>0$ et $u_\varepsilon:(x,t)\in\overline{Q}\mapsto u(x,t)+\varepsilon x^2$. Alors $Pu_\varepsilon=Pu+2\varepsilon\geq 2\varepsilon$ sur $Q$. Par ailleurs, soit $m_\varepsilon=(x_\varepsilon,t_\varepsilon)\in K$ tel que $u_\varepsilon(m_\varepsilon)=\max_K u$.

Supposons par l'absurde que $(x_\varepsilon,t_\varepsilon)\notin K\cap\partial Q$.

⋆ Comme $0<x_\varepsilon<L$, $\partial_x u_\varepsilon(m_\varepsilon)=0$ et $\partial^2_{xx}u_\varepsilon(m_\varepsilon)\leq 0$.

⋆ Comme $0<t_\varepsilon\leq T$, $\partial_t u_\varepsilon(m_\varepsilon)=\lim_{h\to0^+}\dfrac{u_\varepsilon(x_\varepsilon,t_\varepsilon-h)-u_\varepsilon(m_\varepsilon)}{-h}\geq 00.$

Ainsi, $Pu_\varepsilon(m_\varepsilon)\leq 0$ ce qui contredit $Pu_\varepsilon\geq 2\varepsilon$. Donc $m_\varepsilon\in K\cap\partial Q$ et

$$\sup_K u\leq\sup_K u_\varepsilon=\sup_{K\cap\partial Q}u_\varepsilon\leq\sup_{K\cap\partial Q}u+\varepsilon L^2.$$

À la limite $\varepsilon\to 0$, on obtient le résultat car $\sup_K u\geq\sup_{K\cap\partial Q}u$. □

Soit désormais deux solutions $u,v$ de (1)-(4). Posons $w=v-u$. Alors $w$ vérifie (1), (2) et

$$\forall(x,t)\in\partial Q,\qquad w(x,t)=0.$$

Soit $T>0$. Comme de plus $Pw=0$ sur $Q$, d'après le principe du maximum,

$$\forall x\in[0,L],\qquad w(x,T)\leq 0.$$

De même, $P(-w)=0$ sur $Q$ donc $-w(\cdot,T)\leq 0$. Ainsi, $w(\cdot,T)=0$. Ceci étant vrai pour tout $T>0$, $w=0$ sur $Q$.

On a donc montré le théorème suivant.

**Théorème 26.2**

*Le problème (1)-(4) admet une unique solution $u$, et $u\in\mathcal{C}^0(\overline{Q})\cap\mathcal{C}^\infty(Q)$ est donnée par (5).*

# 27 Formule des compléments

E. Amar, E. Matheron, *Analyse complexe*, Cassini. Paragraphe 8.4.4 page 249.

Recasage : 236, 245

**Théorème 27.1**

$\forall 0 < Re(z) < 1, \qquad \Gamma(z)\Gamma(1-z) = \dfrac{\pi}{\sin \pi z}.$

▷ – D'après le théorème des zéros isolés, il suffit de montrer le résultat pour $z = \alpha \in ]0,1[$. Soit $\alpha \in ]0,1[$. D'après le théorème de Fubini-Tonelli :

$$\Gamma(\alpha)\Gamma(1-\alpha) = \int_{(\mathbb{R}_+^*)^2} t^{\alpha-1}s^{-\alpha}e^{-s-t}\mathrm{d}t\mathrm{d}s = \int_{(\mathbb{R}_+^*)^2} \left(\frac{t}{s}\right)^{\alpha} e^{-(s+t)}\mathrm{d}s\mathrm{d}t.$$

Considérons $\varphi : (s,t) \in (\mathbb{R}_+^*)^2 \mapsto (u,v) = \left(s+t, \dfrac{s}{t}\right)$. $\varphi$ est un $\mathcal{C}^1$-difféomorphisme de $(\mathbb{R}_+^*)^2$ sur lui-même et, si $(\mathbb{R}_+^*)^2 \ni (s,t) = \varphi^{-1}(u,v)$,

$$|\det(D\varphi(s,t))| = -\begin{vmatrix} 1 & 1 \\ \dfrac{1}{t} & \dfrac{-s}{t^2} \end{vmatrix} = \frac{s}{t^2} + \frac{1}{t} = \frac{v+1}{t}$$

donc

$$\Gamma(\alpha)\Gamma(1-\alpha) = \int_{(\mathbb{R}_+^*)^2} \frac{e^{-u}}{v^{\alpha}(1+v)}\mathrm{d}u\mathrm{d}v = \int_{\mathbb{R}_+^*} \frac{\mathrm{d}v}{v^{\alpha}(1+v)} := I_{\alpha}.$$

– Soit $\Omega = \mathbb{C}\backslash\mathbb{R}_+$ et on considère la détermination de l'argument associée à valeurs dans $]0, 2\pi[$. On pose alors

$$f : z \mapsto \frac{1}{z^{\alpha}(1+z)} = \frac{1}{r^{\alpha}e^{i\alpha\theta}(1+re^{i\theta})} \text{ si } z = re^{i\theta},\ \theta \in ]0,2\pi[.$$

$f$ est holomorphe dans $\Omega\backslash\{-1\}$ et a un pôle simple en -1 avec

$$\mathrm{Res}(f,-1) = \frac{1}{(-1)^{\alpha}} = e^{-i\pi\alpha}.$$

– Pour $R > 1$, on définit le chemin $\gamma_R = \mathscr{C}_R \cup I_R^+ \cup \Gamma_R \cup I_R^-$ où

⋆ $\mathscr{C}_R = \left\{ \dfrac{1}{R}e^{i\theta},\ \theta \in \left[\dfrac{\pi}{2}, \dfrac{3\pi}{2}\right] \right\}$

⋆ $I_R^{\pm} = \left\{ t \pm \dfrac{i}{R},\ t \in \left[0, \sqrt{R^2 - \dfrac{1}{R^2}}\right] \right\}$

⋆ $\Gamma_R = \{Re^{i\theta},\ \theta \in [\theta_R, 2\pi - \theta_R]\}$ où $\theta_R = \mathrm{Arctan}\left(\dfrac{\frac{1}{R}}{\sqrt{R^2 - \frac{1}{R^2}}}\right)$.

D'après le théorème des résidus

$$\int_{\gamma_R} f(z)\mathrm{d}z = 2i\pi e^{-i\pi\alpha}.$$

Faisons tendre $R \to +\infty$.

⋆ Sur $\mathscr{C}_R$ :

$$\left|\int_{\mathscr{C}_R} f(z)\mathrm{d}z\right| \leq \frac{1}{\frac{1}{R^{\alpha}}(1-\frac{1}{R})} \times \frac{\pi}{R} = \frac{\pi}{R^{1-\alpha}(1-\frac{1}{R})} \xrightarrow[R\to+\infty]{} 0.$$

⋆ Sur $I_R^+$. On a, pour $t > 0$,

$$\left(t + \frac{i}{R}\right)^{\alpha} = \left(t^2 + \frac{1}{R^2}\right)^{\alpha/2} \exp\left(i\alpha \mathrm{Arctan}\left(\frac{\frac{1}{R}}{t}\right)\right) \xrightarrow[R\to+\infty]{} t^{\alpha}$$

donc :

– $\mathbf{1}_{]0,\sqrt{R^2-\frac{1}{R^2}}[}(t) f\left(t + \dfrac{i}{R}\right) \xrightarrow[R\to+\infty]{} \mathbf{1}_{\mathbb{R}_+^*}(t) f(t)$ mesurable,

$$- \left| \mathbf{1}_{]0,\sqrt{R^2-\frac{1}{R^2}}[}(t) f\left(t+\frac{i}{R}\right) \right| \leq \mathbf{1}_{\mathbb{R}_+^*}(t) f(t) \in L^1(\mathbb{R})$$

donc d'après le théorème de convergence dominée, $\lim_{R\to+\infty} \int_{I_R^+} f(z)\mathrm{d}z = \int_{\mathbb{R}_+^*} f(t)\mathrm{d}t$.

⋆ Sur $I_R^-$. De même, pour $t > 0$,

$$\left(t \pm \frac{i}{R}\right)^\alpha = \left(t^2 + \frac{1}{R^2}\right)^{\alpha/2} \exp\left(i\alpha\left(2\pi - \mathrm{Arctan}\left(\frac{\frac{1}{R}}{t}\right)\right)\right) \xrightarrow[R\to+\infty]{} t^\alpha e^{2i\pi\alpha}$$

et, comme précédemment, par le théorème de convergence dominée, $\lim_{R\to+\infty} \int_{I_R^-} f(z)\mathrm{d}z = e^{-2i\pi\alpha} \int_{\mathbb{R}_+^*} f(t)\mathrm{d}t$.

⋆ Sur $\Gamma_{\varepsilon,R}$. On a :

$$\left| \int_{\Gamma_R} f(z)\mathrm{d}z \right| \leq L(\Gamma_R) \max_{z\in\Gamma_R} \frac{1}{|z|^\alpha |1+z|} \leq \frac{2\pi R}{R^\alpha (R-1)} = \frac{2\pi R^{1-\alpha}}{R-1} \xrightarrow[R\to+\infty]{} 0.$$

Ainsi, à la limite $R \to +\infty$, on obtient :

$$(1 + e^{-2i\pi\alpha}) I_\alpha = 2i\pi e^{-i\pi\alpha}$$

soit

$$I_\alpha = \frac{\pi}{\sin \pi\alpha}.$$

□

# 28 Formule sommatoire de Poisson

X. Gourdon, *Les maths en tête : Analyse*, 2e édition, Ellipses. Problème 4 page 272.

Recasage : 236, 241, 246.

**Théorème 28.1 (*Formule sommatoire de Poisson*)**

*Soit $f : \mathbb{R} \to \mathbb{C}$ de classe $\mathcal{C}^1$ telle que $f(x) = \underset{|x|\to+\infty}{\mathcal{O}}\left(\frac{1}{x^\alpha}\right)$ et $f'(x) = \underset{|x|\to+\infty}{\mathcal{O}}\left(\frac{1}{|x|^\beta}\right)$ pour $\alpha, \beta > 1$. Alors la série de fonctions de terme général $(f(\cdot + n))_{n\in\mathbb{Z}}$ converge normalement sur tout compact de $\mathbb{R}$ et*

$$\forall x \in \mathbb{R}, \qquad \sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n) e^{2i\pi nx}$$

*où, pour tout $\xi \in \mathbb{R}$, $\widehat{f}(\xi) = \displaystyle\int_{-\infty}^{+\infty} f(t)e^{-2i\pi\xi t}dt$.*

▷ – Montrons que la série de terme général $(f(\cdot + n))_{n\in\mathbb{Z}}$ converge normalement sur tout compact de $\mathbb{R}$. Soit $M > 0$ tel que pour tout $|x| \geq 1$, $|f(x)| \leq \dfrac{M}{|x|^\alpha}$. Alors, pour $R > 0$, par l'inégalité triangulaire,

$$\forall x \in [-R, R], \forall |n| > R + 1, \qquad |f(x+n)| \leq \frac{M}{|x+n|^\alpha} \leq \frac{M}{||n| - R|^\alpha},$$

qui est le terme général, indépendant de $x$, d'une série convergente, d'où le résultat.

On en déduit en particulier que la série converge simplement sur $\mathbb{R}$. Notons $F$ sa somme.

– De même, la série de terme général $(f'(\cdot + n))_{n\in\mathbb{Z}}$ converge normalement sur tout compact de $\mathbb{R}$. Alors, d'après le théorème de dérivation des séries de fonctions, $F$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}$.

– Par ailleurs, $F$ est 1-périodique. En effet, pour $x \in \mathbb{R}$,

$$\forall N \in \mathbb{N}, \qquad \sum_{n=-N}^{N} f(x+1+n) = \sum_{n=-N+1}^{N+1} f(x+n)$$

d'où, à la limite $N \to +\infty$, $F(x+1) = F(x)$.

Calculons les coefficients de Fourier de $F$ : pour $n \in \mathbb{N}$,

$$\begin{aligned} c_n(f) &= \int_0^1 F(t)e^{2i\pi nt}\mathrm{d}t \underset{\text{cvu}}{=} \sum_{k\in\mathbb{Z}} \int_0^1 f(t+k)e^{2i\pi nt}\mathrm{d}t \\ &= \sum_{k\in\mathbb{Z}} \int_k^{k+1} f(t)e^{2i\pi nt}\mathrm{d}t = \int_{-\infty}^{+\infty} f(t)e^{2i\pi nt}\mathrm{d}t = \widehat{f}(n) \end{aligned}$$

– Comme $F$ est de classe $\mathcal{C}^1$, sa série de Fourier converge uniformément sur $\mathbb{R}$ vers $F$ donc

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

□

**Proposition 28.2**

*Soit $\theta : t \in \mathbb{R}_+^* \mapsto \displaystyle\sum_{n\in\mathbb{Z}} e^{-\pi n^2 t}$. $\theta$ est bien définie sur $\mathbb{R}_+^*$ et*

$$\forall t \in \mathbb{R}_+^*, \qquad \theta(t) = \frac{1}{\sqrt{t}}\theta\left(\frac{1}{t}\right).$$

▷ Soit $\alpha > 0$. On applique la formule sommatoire de Poisson à $f : x \in \mathbb{R} \mapsto e^{-\alpha x^2}$. On a :

$$\forall n \in \mathbb{Z}, \qquad \widehat{f}(n) = \int_{-\infty}^{+\infty} e^{-\alpha t^2} e^{-2i\pi nt} \mathrm{d}t = \frac{1}{\sqrt{\alpha}} \int_{-\infty}^{+\infty} e^{-u^2} e^{-2i\pi \frac{n}{\sqrt{\alpha}} u} \mathrm{d}u = \frac{1}{\sqrt{\alpha}} I\left(\frac{n}{\sqrt{\alpha}}\right)$$

où l'on a défini $I : x \in \mathbb{R} \mapsto \displaystyle\int_{-\infty}^{+\infty} e^{-u^2} e^{-2i\pi xu} \mathrm{d}u$. Cherchons une équation différentielle satisfaite par $I$.

– $I$ est de classe $\mathcal{C}^1$. En effet,
  ⋆ $\forall x \in \mathbb{R}$, $u \in \mathbb{R} \mapsto e^{-u^2} e^{-2i\pi xu} \in L^1_u(\mathbb{R})$ car $e^{-u^2} \in L^1_u(\mathbb{R})$,
  ⋆ $\forall u \in \mathbb{R}$, $x \in \mathbb{R} \mapsto e^{-u^2} e^{-2i\pi xu} \in \mathcal{C}^1(\mathbb{R})$,
  ⋆ $\forall (u, x) \in \mathbb{R}^2$, $\left|e^{-u^2} e^{-2i\pi xu}\right| \leq e^{-u^2} \in L^1_u(\mathbb{R})$ indépendant de $x$,
  donc d'après le théorème de dérivation des intégrales à paramètres, $I$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R}, \qquad I'(x) = -2i\pi \int_{-\infty}^{+\infty} u e^{-u^2} e^{-2i\pi xu} \mathrm{d}u$$

– Or, par intégration par parties, pour tout $x \neq 0$,

$$I(x) = \left[e^{-u^2} \frac{e^{-2i\pi ux}}{-2i\pi x}\right]_{-\infty}^{+\infty} - \frac{1}{2i\pi x} \int_{-\infty}^{+\infty} 2u e^{-u^2} e^{-2i\pi ux} \mathrm{d}u = \frac{1}{2i\pi x} \frac{1}{i\pi} I'(x)$$

donc, comme $I'(0) = 0$,

$$\forall x \in \mathbb{R}, \qquad I'(x) = -2\pi^2 x I(x).$$

On en déduit, comme $I(0) = \sqrt{\pi}$, que :

$$\forall x \in \mathbb{R}, \qquad I(x) = I(0) e^{-\pi^2 x^2} = \sqrt{\pi} e^{-\pi^2 x^2}.$$

– Ainsi, $\forall n \in \mathbb{Z}$, $\widehat{f}(n) = \sqrt{\dfrac{\pi}{\alpha}} e^{-\frac{\pi^2 n^2}{\alpha}}$. D'après la formule de Poisson :

$$\forall x \in \mathbb{R}, \qquad \sum_{n \in \mathbb{Z}} e^{-\alpha(x+n)^2} = \sqrt{\frac{\pi}{\alpha}} \sum_{n \in \mathbb{Z}} e^{-\frac{\pi^2 n^2}{\alpha}} e^{2i\pi nx}$$

donc, en $x = 0$ et avec $\alpha = \pi t$,

$$\forall t > 0, \qquad \sum_{n \in \mathbb{Z}} e^{-\pi n^2 t} = \frac{1}{\sqrt{t}} \sum_{n \in \mathbb{Z}} e^{-\frac{\pi n^2}{t}}$$

*ie.*

$$\forall t > 0, \qquad \theta(t) = \frac{1}{\sqrt{t}} \theta\left(\frac{1}{t}\right).$$

□

# 29 Image de l'exponentielle

M. Zavidovique, *Un Max de Math*, Calvage & Mounet. Problème 9 page 48.

Recasage : 156, 204.

**Théorème 29.1**

*Soit $A \in \mathcal{M}_n(\mathbb{C})$. Alors* $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$.

▷ – *Étape 1 :* $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$ L'inclusion $\subset$ est évidente. Si $M \in \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$ alors, $M^{-1}$ comme est un polynôme en $M$, c'est bien un polynôme en $A$.

– *Étape 2 :* $\exp(\mathbb{C}[A]) \subset \mathbb{C}[A]^\times$. En effet, si $M = \exp(N)$ avec $N \in \mathbb{C}[A]$ alors $I_n = \exp(N)\exp(-N) = M\exp(-N)$ donc $M \in \mathrm{GL}_n(\mathbb{C})$. De plus, $\mathbb{C}[A]$ est fermé comme sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ donc $M = \exp(N) \in \mathbb{C}[A]$. Le point précédent permet de conclure.

– *Étape 3 :* $\mathbb{C}[A]^\times$ *est un ouvert connexe de* $\mathbb{C}[A]$. On a $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap \overset{-1}{\det}(\mathbb{C}^*)$ donc $\mathbb{C}[A]^\times$ est un ouvert de $\mathbb{C}[A]$. Montrons qu'il est connexe par arcs. Pour $M, N \in \mathbb{C}[A]^\times$ on a :

$$\forall z \in \mathbb{C}, \qquad M(z) = zM + (1-z)N \in \mathbb{C}[A].$$

On va donc chercher un chemin de la forme

$$\forall t \in [0,1], \qquad M(z(t)) = z(t)M + (1-z(t))N$$

avec $t \mapsto z(t)$ continue telle que $z(0) = 0$ et $z(1) = 1$. De plus, l'application $z \mapsto \det(M(z))$ est polynomiale en $z$ donc elle a un nombre fini de zéros. En considérant

$$\forall a \in \mathbb{R}, \forall t \in [0,1], \qquad z_a(t) = t + iat(1-t),$$

comme $(t,a) \mapsto z_a(t)$ est injective, on peut trouver $a \in \mathbb{R}$ tel que $\forall t \in [0,1]$, $\det(M(z_a(t))) \neq 0$ et $z_a(0) = z_a(1) = 1$.

– *Étape 4 :* $\exp(\mathbb{C}[A])$ *est ouvert.* On a $\exp(0) = I_n$ et $\mathrm{d}\exp(0) = \mathrm{Id}_{\mathcal{M}_n(\mathbb{C})}$ donc, d'après le théorème d'inversion locale, il existe des voisinages ouverts $\mathcal{U}$ de 0 dans $\mathbb{C}[A]$ et $\mathcal{V}$ de $I_n$ dans $\exp(\mathbb{C}[A])$ tels que l'exponentielle réalise un $\mathcal{C}^1$-difféomorphisme de $U$ dans $V$. Alors, pour $B \in \mathbb{C}[A]$, on a

$$\exp(B + \mathcal{U}) = \exp(B)\exp(\mathcal{U}) = \exp(B)V$$

(car $B$ commute avec les éléments de $\mathcal{U}$) donc $\exp(B)V$ est un voisinage ouvert de $\exp(B)$ inclus dans $\exp(\mathbb{C}[A])$.

– *Étape 5 :* $\exp(\mathbb{C}[A])$ *est fermé dans* $\mathbb{C}[A]^\times$. On a :

$$\mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A]) = \bigcup_{M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])} \underbrace{M\exp(\mathbb{C}[A])}_{\text{ouvert}}.$$

En effet,

$$\mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A]) = \bigcup_{M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])} M\{\exp(0)\} \subset \bigcup_{M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])} M\exp(\mathbb{C}[A])$$

et si $M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])$ et $N = M\exp(B)$ avec $B \in \mathbb{C}[A]$, alors $N \in \mathbb{C}[A]^\times$ et $M = N\exp(-B) \notin \exp(\mathbb{C}[A])$ donc $N \notin \exp(\mathbb{C}[A])$.

– *Conclusion :* Par connexité de $\mathbb{C}[A]^\times$, on a $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$. □

**Corollaire 29.2**

$\exp(\mathcal{M}_n(\mathbb{C})) = \mathrm{GL}_n(\mathbb{C})$.

▷ Soit $A \in \mathrm{GL}_n(\mathbb{C})$. On a $A \in \mathbb{C}[A]^\times = \exp(\mathbb{C}[A]) \subset \exp(\mathcal{M}_n(\mathbb{C}))$. □

**Corollaire 29.3**

$\exp(\mathcal{M}_n(\mathbb{R})) = \{A^2,\ A \in \mathrm{GL}_n(\mathbb{C})\}$.

▷ Soit $M \in \mathcal{M}_n(\mathbb{R})$. Alors $\exp(M) = \exp(M/2)^2$.

Soit $M = A^2 \in \mathrm{GL}_n(\mathbb{C})$. Alors il existe $P \in \mathbb{C}[X]$ tel que $\exp(P(A)) = A$. Comme $A$ est à coefficients réels, $\exp(\overline{P}(A)) = \exp(\overline{P(A)}) = \overline{A} = A$ donc $\exp((P+\overline{P})(A)) = M \in \exp(\mathbb{R}[A]) \subset \exp(\mathcal{M}_n(\mathbb{R}))$. □

# 30 Inégalité de Heisenberg

B. Candelpergher, *Calcul intégral*, Cassini. Paragraphe 7.11.1 page 383

Recasage : 250.

**Théorème 30.1**

*Notons, pour $f \in \mathcal{S}(\mathbb{R})$,*

$$x_0^{(f)} = \int_{\mathbb{R}} x|f(x)|^2 dx \qquad \xi_0^{(f)} = \int_{\mathbb{R}} \xi|\mathcal{F}f(\xi)|^2 d\xi$$

$$V(f) = \int_{\mathbb{R}} (x-x_0)^2|f(x)|^2 dx \qquad V(\mathcal{F}f) = \int_{\mathbb{R}} (\xi-\xi_0)^2|\mathcal{F}f(\xi)|^2 d\xi.$$

*Soit $f \in \mathcal{S}(\mathbb{R})$ telle que $\|f\|_2 = 1$. Alors*

$$V(f)V(\mathcal{F}f) \geq \frac{1}{16\pi^2}.$$

▷ *−Étape 1 : Réduction au cas $x_0 = 0, \xi_0 = 0$.* Posons

$$g : x \in \mathbb{R} \mapsto e^{-2i\pi x\xi_0} f(x+x_0).$$

Alors

$$\forall \xi \in \mathbb{R}, \qquad \mathcal{F}g(\xi) = e^{2i\pi x_0(\xi+\xi_0)}\mathcal{F}f(\xi+\xi_0).$$

On a :

$$|g|^2 = |f(\cdot+x_0)|^2 \qquad |\mathcal{F}g|^2 = |\mathcal{F}f(\cdot+\xi_0)|^2$$

d'où l'on déduit que $\|g\|_2 = 1$ et $x_0^{(g)} = 0$, $\xi_0^{(g)} = 0$ et $V(f) = V(g)$, $V(\mathcal{F}f) = V(\mathcal{F}g)$ et

$$V(g) = \|x \mapsto xg(x)\|_2^2 \qquad V(\mathcal{F}g) = \|\xi \mapsto \xi\mathcal{F}g(\xi)\|_2^2.$$

*−Étape 2 : Réduction au même espace.* On a :

$$\forall \xi \in \mathbb{R}, \qquad \mathcal{F}g'(\xi) = 2i\pi\xi\mathcal{F}g(\xi)$$

*ie.*

$$\forall \xi \in \mathbb{R}, \qquad \xi\mathcal{F}g(\xi) = \frac{1}{2\pi}\mathcal{F}\left(\frac{1}{i}g'\right)(\xi)$$

donc

$$\|\xi \mapsto \xi\mathcal{F}g(\xi)\|_2 = \frac{1}{2\pi}\left\|\mathcal{F}\left(\frac{1}{i}g'\right)\right\|_2 = \frac{1}{2\pi}\left\|\frac{1}{i}g'\right\|_2$$

car $\mathcal{F}$ est une isométrie sur $L^2$. Il suffit donc de montrer que

$$\forall g \in \mathcal{S}(\mathbb{R}), \qquad \frac{1}{2\pi}\|x \mapsto xg(x)\|_2 \left\|\frac{1}{i}g'\right\|_2 \geq \frac{1}{4\pi}\|g\|_2^2.$$

*−Étape 3 : opérateurs autoadjoints et relation de commutation.* Posons

$$P : g \in \mathcal{S}(\mathbb{R}) \mapsto \frac{1}{i}g' \in \mathcal{S}(\mathbb{R})$$

$$Q : g \in \mathcal{S}(\mathbb{R}) \mapsto (x \mapsto xg(x)) \in \mathcal{S}(\mathbb{R}).$$

En munissant $\mathcal{S}(\mathbb{R})$ du produit scalaire hermitien $\langle .,. \rangle$ de $L^2$, $P$ et $Q$ sont autoadjoint, et on a

$$i(P \circ Q - Q \circ P) = \mathrm{Id}.$$

Alors, pour $g \in \mathcal{S}(\mathbb{R})$,

$$\begin{array}{rcl} \|g\|_2^2 & = & \langle g, g\rangle \\ & = & \langle i(P\circ Q - Q\circ P)g, g\rangle \\ & = & -i\left(\langle Qg, Pg\rangle - \langle Pg, Qg\rangle\right) \\ & = & 2\,\mathrm{Im}\langle Qg, Pg\rangle \\ & \leq & 2\,|\langle Qg, Pg\rangle| \\ & \leq & 2\,\|Qg\|_2\,\|Pg\|_2 \end{array}$$

d'où l'on déduit :

$$\forall g \in \mathcal{S}(\mathbb{R}), \qquad \frac{1}{2\pi}\|x \mapsto xg(x)\|_2 \left\|\frac{1}{i}g'\right\|_2 \geq \frac{1}{4\pi}\|g\|_2^2.$$

□

**Exemple :** On définit, pour $a > 0$,

$$f : x \in \mathbb{R} \mapsto ce^{-ax^2}$$

où $c = \left(\frac{\pi}{2a}\right)^{-1/4}$. Alors

$$V(f) = \frac{1}{4a} \qquad \text{et} \qquad V(\mathcal{F}f) = \frac{a}{4\pi^2}$$

donc

$$V(f)V(\mathcal{F}f) = \frac{1}{16\pi^2}.$$

Les gaussiennes réalisent au mieux l'inégalité d'Heisenberg.

# 31 Inversion de la fonction caractéristique

B. Candelpergher, *Théorie des probabilités*, Calvage & Mounet. Page 222.

Recasage : 235, 239, 261.

**Théorème 31.1**

*La fonction caractéristique caractérise la loi d'une variable aléatoire réelle.*

▷ Soit $X$ une variable aléatoire réelle. On va montrer que la fonction de répartition $F_X : t \in \mathbb{R} \mapsto \mathbb{P}(X \leq t)$ s'exprime en fonction de $\varphi_X(t) = \mathbb{E}[e^{itX}]$.

– On commence par exprimer $\mathbb{P}(X \in ]a,b[) = \displaystyle\int_{\mathbb{R}} \mathbf{1}_{]a,b[} \mathrm{d}\mathbb{P}_X$ pour $a < b$. L'idée est de remplacer $\mathbf{1}_{]a,b[}$ par une expression faisant intervenir $e^{i\cdot t}$.

**Lemme 31.2**

*Soient $T > 0$ et*

$$K_T : x \in \mathbb{R} \mapsto \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} e^{ixt} dt.$$

*On a :*

*(i) $K_T$ est uniformément bornée en $T$,*

*(ii) $\forall x \in \mathbb{R}$, $K_T(x) \xrightarrow[T\to+\infty]{} \mathbf{1}_{]a,b[}(x) + \dfrac{1}{2}(\mathbf{1}_{\{a\}}(x) + \mathbf{1}_{\{b\}}(x))$,*

*(iii) $\displaystyle\int_{\mathbb{R}} K_T d\mathbb{P}_X = \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} \varphi_X(t) dt.$*

▷ On a :

$$\int_{-T}^{T} \frac{e^{i(x-a)t}}{it} \mathrm{d}t = \int_0^T \frac{e^{i(x-a)t} - e^{-i(x-a)t}}{it} \mathrm{d}t = 2\int_0^{T(x-a)} \frac{\sin u}{u} \mathrm{d}u$$

donc

$$\forall x \in \mathbb{R}, \qquad K_T = \frac{1}{\pi}\left(\mathrm{Si}(T(x-a)) - \mathrm{Si}(T(x-b))\right)$$

où $\mathrm{Si} : y \in \mathbb{R} \mapsto \displaystyle\int_0^y \frac{\sin u}{u} \mathrm{d}u$. Or Si est impaire et continue sur $\mathbb{R}$ et vérifie $\lim\limits_{y\to\pm\infty} \mathrm{Si}(y) = \pm\dfrac{\pi}{2} < \infty$ donc Si est bornée sur $\mathbb{R}$. On en déduit que $K_T$ est uniformément bornée.

*(ii)* De plus, si $x \in ]a,b[$, $\mathrm{Si}(T(x-a)) \xrightarrow[T\to+\infty]{} \dfrac{\pi}{2}$ et $\mathrm{Si}(T(x-b)) \xrightarrow[T\to+\infty]{} -\dfrac{\pi}{2}$ donc $K_T(x) \xrightarrow[T\to+\infty]{} 1$. On établit de même que

$$\forall x \in \mathbb{R}, \qquad K_T(x) = \mathbf{1}_{]a,b[}(x) + \frac{1}{2}(\mathbf{1}_{\{a\}}(x) + \mathbf{1}_{\{b\}}(x)).$$

*(iii)* D'après le théorème de Fubini,

$$\int_{\mathbb{R}} K_T \mathrm{d}\mathbb{P}_X = \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} \left( \int_{\mathbb{R}} e^{ixt} \mathrm{d}\mathbb{P}_X(x) \right) \mathrm{d}t = \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} \varphi_X(t) \mathrm{d}t.$$

Le théorème de Fubini s'applique car

$$\int_{\mathbb{R}} \left( \int_{-T}^{T} \frac{|e^{-iat} - e^{ibt}|}{t} \mathrm{d}t \right) \mathrm{d}\mathbb{P}_X = \int_{-T}^{T} \frac{\sqrt{(\cos at - \cos bt)^2 + (\sin at - \sin bt)^2}}{|t|} \mathrm{d}t < +\infty$$

d'après la règle de Riemann puisque

$$\sqrt{|t|} \times \frac{\sqrt{(\cos at - \cos bt)^2 + (\sin at - \sin bt)^2}}{|t|} \underset{t\to 0}{\sim} \frac{(b-a)|t|}{\sqrt{|t|}} \xrightarrow[t\to 0]{} 0.$$

□

On déduit du lemme que

$$\mathbb{P}(X \in ]a,b[) = \int_{\mathbb{R}} \mathbf{1}_{]a,b[} \mathrm{d}\mathbb{P}_X = \int_{\mathbb{R}} \left( \lim_{T\to+\infty} K_T \right) \mathrm{d}\mathbb{P}_X - \int_{\mathbb{R}} \frac{1}{2}(\mathbf{1}_{\{a\}} + \mathbf{1}_{\{b\}}) \mathrm{d}\mathbb{P}_X$$

d'où, par le théorème de convergence dominée ($K_T$ étant uniformément bornée et $\mathbb{P}_X$ est de masse finie) :

$$\begin{aligned}\mathbb{P}(X \in ]a,b[) &= \lim_{T\to+\infty} \int_{\mathbb{R}} K_T \mathrm{d}\mathbb{P}_X - \frac{\mathbb{P}(X=a)+\mathbb{P}(X=b)}{2} \\ &= \lim_{T\to+\infty} \frac{1}{2\pi}\int_{-T}^{T} \frac{e^{-iat}-e^{-ibt}}{it}\varphi_X(t)\mathrm{d}t - \frac{\mathbb{P}(X=a)+\mathbb{P}(X=b)}{2}.\end{aligned}$$

Comme $F_X(b) - F_X(a) = \mathbb{P}(X \in ]a,b[) + \mathbb{P}(X=b)$, on en déduit :

$$F_X(b) - F_X(a) = \lim_{T\to+\infty} \frac{1}{2\pi}\int_{-T}^{T} \frac{e^{-iat}-e^{-ibt}}{it}\varphi_X(t)\mathrm{d}t - \frac{\mathbb{P}(X=a)-\mathbb{P}(X=b)}{2}$$

et, en particulier, si $a$ et $b$ ne sont pas des points de discontinuité de $F_X$ :

$$F_X(b) - F_X(a) = \lim_{T\to+\infty} \frac{1}{2\pi}\int_{-T}^{T} \frac{e^{-iat}-e^{-ibt}}{it}\varphi_X(t)\mathrm{d}t.$$

$F_X$ étant une fonction croissante, ses points de discontinuité forment un ensemble $D$ dénombrable. De plus, on a :

$$\lim_{\substack{a\to-\infty \\ a\notin D}} (F_X(b) - F_X(a)) = F_X(b)$$

donc, pour tout $b \notin D$,

$$F_X(b) = \lim_{\substack{a\to-\infty \\ a\notin D}} \lim_{T\to+\infty} \frac{1}{2\pi}\int_{-T}^{T} \frac{e^{-iat}-e^{-ibt}}{it}\varphi_X(t)\mathrm{d}t.$$

Enfin, comme la fonction $F_X$ est continue à droite, la relation ci-dessus détermine $F_X$ sur $\mathbb{R}$. □

# 32 Méthode de Laplace

Présenté le jour J (leçon 218, résultat : 16/20, pas eu le temps de parler de l'application)

F. Rouvière, *Petit guide de calcul différentiel*, 4e édition, Cassini. Exercice 113 page 349.

Recasage : 218, 224, 235, 239.

**Théorème 32.1 (*Méthode de Laplace*)**

*Soient $a < b \leq \infty$, $\varphi \in \mathcal{C}^2([a,b[,\mathbb{R})$ telle que $\varphi' > 0$ sur $]a,b[$, et $f : [a,b[\to \mathbb{C}$ continue en $a$ telle que $f(a) \neq 0$. On suppose qu'il existe $t_0 \in \mathbb{R}$ tel que $e^{-t_0\varphi} f \in L^1(]a,b[)$. Alors, $F : t \mapsto \displaystyle\int_a^b e^{-t\varphi(x)} f(x)dx$ est définie pour $t \geq t_0$ et*

*(i) si $\varphi'(a) > 0$, alors $F(t) \underset{t\to+\infty}{\sim} \dfrac{1}{\varphi'(a)} \dfrac{e^{-t\varphi(a)} f(a)}{t}$ ;*

*(ii) si $\varphi'(a) = 0$ et $\varphi''(a) > 0$, alors $F(t) \underset{t\to+\infty}{\sim} \sqrt{\dfrac{\pi}{2\varphi''(a)}} \dfrac{e^{-t\varphi(a)} f(a)}{\sqrt{t}}$.*

**Heuristique** Dans les deux cas considérés, $\varphi$ croît strictement sur $[a,b[$ donc, pour $t$ grand, $e^{-t\varphi}$ décroit rapidement et la masse de l'intégrale est concentrée sur un petit intervalle $[a, a+\alpha]$ sur lequel on peut considérer

$$f(x) \simeq f(a) \qquad \varphi(x) \simeq \varphi(a) + \varphi'(a)(x-a)$$

respectivement

$$f(x) \simeq f(a) \qquad \varphi(x) \simeq \varphi(a) + \frac{\varphi''(a)}{2}(x-a)^2$$

d'où

$$F(t) \simeq e^{-t\varphi(a)} \int_a^\infty e^{-t\varphi'(a)(x-a)} f(a)\mathrm{d}x = \frac{1}{\varphi'(a)} \frac{e^{-t\varphi(a)} f(a)}{t}$$

respectivement

$$F(t) \simeq e^{-t\varphi(a)} \int_a^\infty e^{-t\varphi''(a)(x-a)^2/2} f(a)\mathrm{d}x = \sqrt{\frac{\pi}{2\varphi''(a)}} \frac{e^{-t\varphi(a)} f(a)}{\sqrt{t}}.$$

**Démonstration** – On peut considérer $t_0 = 0$ en remplaçant $t - t_0$ par $t$ et $e^{t_0\varphi} f$ par $f$.

– L'hypothèse, avec $t_0 = 0$, impose que $f \in \mathrm{L}^1(a,b)$ et, comme $\varphi$ est croissante,

$$\forall t \geq 0, \qquad \int_a^b |e^{-t\varphi(x)} f(x)|\mathrm{d}x \leq e^{-t\varphi(a)} \|f\|_{L^1(a,b)} < +\infty$$

donc $F(t)$ est bien définie pour $t \geq 0$.

– Comme $f$ est continue en $a$, prenons $\alpha > 0$, $M \geq 0$ tels que

$$\forall x \in [a, a+\alpha], \qquad |f(x)| \leq M.$$

– Considérons un premier exemple : $a = 0$ et $\varphi(x) = x$. Pour $t > 0$,

$$t\int_0^\alpha e^{-tx} f(x)\mathrm{d}x \underset{u=tx}{=} \int_0^{\alpha t} e^{-u} f\left(\frac{u}{t}\right)\mathrm{d}u \xrightarrow[t\to+\infty]{} f(0)$$

d'après le théorème de convergence dominée, l'hypothèse de domination étant vérifiée grâce à la majoration de $f$ sur $[0,\alpha]$. De plus,

$$\left|\int_\alpha^b e^{-tx} f(x)\mathrm{d}x\right| \leq e^{-t\alpha} \|f\|_{L^1(a,b)} = \underset{t\to+\infty}{o}\left(\frac{1}{t}\right).$$

Ceci montre que

$$F(t) \underset{t\to+\infty}{\sim} \frac{f(0)}{t}.$$

– On peut désormais traiter le point $(i)$ du théorème. On se ramène au cas précédent par changement de variable. Posons $\Phi(x) = \varphi(x) - \varphi(a)$ de sorte que $\Phi \in \mathcal{C}^1$, pour tout $x \in [a,b[$, $\Phi'(x) = \varphi'(x) > 0$ et $\Phi(a) = 0$. Alors $\Phi$ réalise

un $\mathcal{C}^1$-difféomorphisme $[a,b[\to[0,c[$ pour $c\in\mathbb{R}\cup\{+\infty\}$. Notons $\psi$ sa réciproque. D'après le théorème de changement de variable, pour $t\geq 0$,

$$F(t)=e^{-t\varphi(a)}\int_a^b e^{-t\Phi(x)}f(x)\mathrm{d}x=e^{-t\varphi(a)}\int_0^c e^{-ty}f(\psi(y))\psi'(y)\mathrm{d}y.$$

Or $\psi'\times f\circ\psi$ est continue et non nulle en 0 donc, d'après l'exemple précédent,

$$F(t)\underset{t\to+\infty}{\sim}\frac{e^{-t\varphi(a)}f(\psi(0))\psi'(0)}{t}=\frac{e^{-t\varphi(a)}f(a)}{\varphi'(a)t}.$$

– Considérons un deuxième exemple : $a=0$ et $\varphi(x)=x^2$. Pour $t>0$,

$$\sqrt{t}\int_0^\alpha e^{-tx^2}f(x)\mathrm{d}x\underset{u=\sqrt{t}x}{=}\int_0^{\alpha\sqrt{t}}e^{-u^2}f\left(\frac{u}{\sqrt{t}}\right)\mathrm{d}u\xrightarrow[t\to+\infty]{}\frac{\sqrt{\pi}}{2}f(0)$$

d'après le théorème de convergence dominée, comme précédemment. De plus,

$$\left|\int_\alpha^b e^{-tx^2}f(x)\mathrm{d}x\right|\leq e^{-t\alpha^2}\left\|f\right\|_{L^1(a,b)}=\underset{t\to+\infty}{o}\left(\frac{1}{\sqrt{t}}\right).$$

Ceci montre que

$$F(t)\underset{t\to+\infty}{\sim}\frac{\sqrt{\pi}}{2}\frac{f(0)}{\sqrt{t}}.$$

– On peut désormais traiter le point $(ii)$ du théorème. On se ramène au cas précédent par changement de variable. Posons $\Phi(x)=\sqrt{\varphi(x)-\varphi(a)}$ de sorte que $\Phi(a)=0$ et $\Phi'(x)=\dfrac{\varphi'(x)}{2\sqrt{\varphi(x)-\varphi(a)}}$ pour $x>a$ (car $\varphi$ est strictement croissante). De plus,

$$\Phi'(x)\underset{x\to a^+}{\sim}\frac{(x-a)\varphi''(a)}{2\sqrt{\frac{\varphi''(a)}{2}(x-a)^2}}\underset{x\to a^+}{\sim}\sqrt{\frac{\varphi''(a)}{2}}>0.$$

Ainsi, $\Phi$ se prolonge en un $\mathcal{C}^1$ difféomorphisme $[a,b[\to[0,c[$ et, en notant $\psi=\Phi^{-1}$, d'après le théorème de changement de variable, pour $t>0$,

$$F(t)=e^{-t\varphi(a)}\int_a^b e^{-t\Phi(x)^2}f(x)\mathrm{d}x=e^{-t\varphi(a)}\int_0^c e^{-ty^2}f(\psi(y))\psi'(y)\mathrm{d}y.$$

Comme $\psi'\times f\circ\psi$ est continue en 0, d'après l'exemple précédent,

$$F(t)\underset{t\to+\infty}{\sim}\frac{\sqrt{\pi}}{2}\frac{e^{-t\varphi(a)}f(\psi(0))\psi'(0)}{\sqrt{t}}=\sqrt{\frac{\pi}{2\varphi''(a)}}\frac{e^{-t\varphi(a)}f(a)}{\sqrt{t}}.$$

**Remarque :** Si $f(a)=0$ ou $\varphi'(a)=\varphi''(a)=0$, on peut pousser les développements limités à un ordre supérieur et obtenir des résultats analogues.

**Application : formule de Stirling** On a

$$\forall t>0,\qquad\Gamma(t+1)=\int_0^{+\infty}e^{-x}x^t\mathrm{d}x.$$

Comme $e^{-x}x^t$ est maximal en $x=t$, on fait le changement de variables $x=t(u+1)$ pour se ramener à un maximum en $u=0$ :

$$\Gamma(t+1)=t^{t+1}\int_{-1}^{\infty}e^{-t\varphi(u)}\mathrm{d}u$$

avec $\varphi(u)=u+1-\ln(u+1)$ et on écrit

$$\Gamma(t+1)=t^{t+1}\left(\int_{-1}^0 e^{-t\varphi(u)}\mathrm{d}u+\int_0^\infty e^{-t\varphi(u)}\mathrm{d}u\right)=t^{t+1}\left(\int_0^1 e^{-t\varphi(-u)}\mathrm{d}u+\int_0^\infty e^{-t\varphi(u)}\mathrm{d}u\right).$$

On a $\varphi(0)=1,\varphi'(0)=0,\varphi''(0)=1$ et $\varphi'>0$ sur $[0,+\infty[$ et $(\varphi(-\cdot))'>0$ sur $[0,1]$ donc la méthode s'applique et

$$\Gamma(t+1)\underset{t\to+\infty}{\sim}t^{t+1}\left(\sqrt{\frac{\pi}{2}}\frac{e^{-t}}{\sqrt{t}}+\sqrt{\frac{\pi}{2}}\frac{e^{-t}}{\sqrt{t}}\right)=\sqrt{2\pi}t^te^{-t}$$

# 33 Méthode de Newton

Cours d'analyse numérique de Benjamin Boutin (Université Rennes 1) pour le théorème 1.

I. Nourdin, *Agrégation de mathématiques, épreuve orale*, 2e édition, Dunod. Proposition 1.24.5 page 101 pour le théorème 2.

Recasage : 205, 208, 215, 218, 226, 233.

**Théorème 33.1**

*Soit $\Omega$ un ouvert de $\mathbb{R}^n$. On suppose $f \in \mathcal{C}^1(\Omega, \mathbb{R}^n)$ et $x^* \in \Omega$ tel que :*
- *$f(x^*) = 0$*
- *$df(x^*) \in \mathrm{GL}(\mathbb{R}^n)$ et on note $C > 0$ tel que $\left\| df(x^*)^{-1} \right\| \leq C$*
- *$\exists R, L > 0, \forall x, y \in B(x^*, R)$, $\|df(x) - df(y)\| \leq L \|x - y\|$.*

*Alors il existe $r > 0$ tel que $B(x^*, r) \subset \Omega$ et pour tout $x_0 \in B(x^*, r)$, la suite définie par*

$$\forall k \in \mathbb{N}, \qquad x_{k+1} = x_k - [df(x_k)^{-1}] f(x_k)$$

*est bien définie et converge vers $x^*$ avec*

$$\forall k \geq 0, \qquad \|x_{k+1} - x^*\| \leq CL \|x_k - x^*\|^2 .$$

▷ On montre que la suite est bien définie. On aura alors montré au passage l'inégalité souhaitée.

– *Étape 1 :* $\exists r > 0, \forall x \in B(x^*, r)$, $df(x) \in \mathrm{GL}(\mathbb{R}^n)$. Soit $x \in B(x^*, R)$. On a :

$$\mathrm{d}f(x) = \mathrm{d}f(x^*) - (\mathrm{d}f(x^*) - \mathrm{d}f(x)) = \mathrm{d}f(x^*)(\mathrm{Id} - \underbrace{[\mathrm{d}f(x^*)^{-1}](\mathrm{d}f(x^*) - \mathrm{d}f(x))]}_{A(x)})$$

avec

$$\|A(x)\| \leq \left\| \mathrm{d}f(x^*)^{-1} \right\| \|\mathrm{d}f(x^*) - \mathrm{d}f(x)\| \leq CL \|x^* - x\| .$$

Alors, avec $r = \min\left(R, \dfrac{1}{2CL}\right)$, pour tout $x \in B(x^*, r)$, $\|A(x)\| \leq \dfrac{1}{2} < 1$ donc $\mathrm{Id} + A(x) \in \mathrm{GL}(\mathbb{R}^n)$. De plus,

$$\left\| \mathrm{d}f(x)^{-1} \right\| \leq \left\| \mathrm{d}f(x^*)^{-1} \right\| \left\| (\mathrm{Id} - A(x))^{-1} \right\| \leq \frac{\left\| \mathrm{d}f(x^*)^{-1} \right\|}{1 - \|A(x)\|} \leq 2C.$$

– *Étape 2 : on construit la suite $(x_k)$ par récurrence.* Soit $x_0 \in B(x^*, r)$ et supposons $x_k \in B(x^*, r)$ défini pour $k \in \mathbb{N}$. Alors $\mathrm{d}f(x_k) \in \mathrm{GL}(\mathbb{R}^n)$ donc on peut poser

$$x_{k+1} = x_k - [\mathrm{d}f(x_k)^{-1}] f(x_k).$$

Alors,

$$\begin{aligned}
\|x_{k+1} - x^*\| &\leq \left\| x_k - x^* - [\mathrm{d}f(x_k)^{-1}](f(x_k) - f(x^*)) \right\| \\
&\leq \left\| [\mathrm{d}f(x_k)^{-1}](f(x^*) - f(x_k) - \mathrm{d}f(x_k)(x^* - x_k) \right\| \\
&\leq \left\| \mathrm{d}f(x_k)^{-1} \right\| \left\| \int_0^1 \mathrm{d}f(x_k + t(x^* - x_k))(x^* - x_k)\mathrm{d}t - \int_0^1 \mathrm{d}f(x_k)(x^* - x_k)\mathrm{d}t \right\| \\
&\leq 2C \int_0^1 \|\mathrm{d}f(x_k + t(x^* - x_k)) - \mathrm{d}f(x_k)\| \|x^* - x_k\| \, \mathrm{d}t \\
&\leq 2CL \|x_k - x^*\|^2 \int_0^1 t \mathrm{d}t \\
&\leq CL \|x_k - x^*\|^2 \leq \frac{r}{2}.
\end{aligned}$$

On a donc montré que $(x_k)$ est bien définie et prend ses valeurs dans $B(x^*, r)$ et

$$\forall k \in \mathbb{N}, \qquad \|x_{k+1} - x^*\| \leq CL \|x_k - x^*\|^2 .$$

Posons $u_k = CL\|x_k - x^*\|$. Alors $0 \leq u_{k+1} \leq u_k^2$ et $u_0 = CL\|x_0 - x^*\| \leq CLr \leq \dfrac{1}{2}$ donc, par récurrence,

$$\forall k \in \mathbb{N}, \qquad 0 \leq u_k \leq (u_0)^{2^k} \leq \left(\frac{1}{2}\right)^{2^k} \xrightarrow[k\to+\infty]{} 0.$$

□

**Remarque :** Doit-on craindre les erreurs numériques inhérentes à l'utilisation d'un ordinateur ? En effet, partant de $x_0$, on voudrait définir $x_1$ par $x_1 = f(u_0$. Mais ce n'est pas possible et on obtient en fait une valeur approchée à $\varepsilon$ près de $x_1$, notée $v_1$. On applique ensuite $f$ à $v_1$ et non à $x_1$. Est-ce que ces erreurs s'accumulent ? Pour des méthodes de résolution basée sur le théorème de Picard, la réponse est non en vertu du théorème suivant.

**Théorème 33.2**

*Soient $(E, \|.\|)$ un espace de Banach, $a \in E$, $r > 0$, $\varepsilon > 0$, $0 \leq k < 1$. Soit $\phi : B(a,r) \to B(a,r)$ une application $k$-contractante et soient $(u_n), (v_n) \in B(a,r)^{\mathbb{N}}$ telles que*

- *$u_0 = v_0 \in B(a,r)$*
- *$\forall n \in \mathbb{N}$, $u_{n+1} = \phi(v_n)$*
- *$\forall n \in \mathbb{N}$, $\|u_n - v_n\| \leq \varepsilon$.*

*Alors $\phi$ admet un unique point fixe $x^* \in B(a,r)$ et*

$$\forall n \in \mathbb{N}, \qquad \|v_n - x^*\| \leq \frac{k^n}{1-k}\|u_1 - u_0\| + \frac{\varepsilon}{1-k}.$$

▷ $f$ admet un unique point fixe d'après le théorème de Picard. Montrons par récurrence sur $n \in \mathbb{N}^*$ que

$$\|v_n - x^*\| \leq \frac{k^n}{1-k}\|u_1 - u_0\| + \varepsilon \sum_{i=0}^{n-1} k^i.$$

- $n = 1$ : On a

$$\|u_1 - x^*\| = \|\phi(u_0) - \phi(x^*)\| \leq k\|u_0 - x^*\| \leq k\|u_0 - u_1\| + k\|u_1 - x^*\|$$

d'où $\|u_1 - x^*\| \leq \dfrac{k}{1-k}\|u_1 - u_0\|$ donc

$$\|v_1 - x^*\| \leq \|u_1 - x^*\| + \|u_1 - v_1\| \leq \frac{k}{1-k}\|u_1 - u_0\| + \varepsilon.$$

- Supposons le résultat pour $n \in \mathbb{N}^*$. Alors

$$\begin{aligned} \|v_{n+1} - x^*\| &\leq \|u_{n+1} - x^*\| + \|v_{n+1} - u_{n+1}\| \\ &\leq \|\phi(v_n) - \phi(x^*)\| + \varepsilon \leq k\|v_n - x^*\| + \varepsilon \\ &\leq \frac{k^{n+1}}{1-k}\|u_1 - u_0\| + \varepsilon \sum_{i=0}^{n} k^i. \end{aligned}$$

□

# 34 Méthode du gradient à pas optimal

J.-B. Hirriat-Urruty, *Optimisation et analyse convexe*, EDP Sciences. Exercice I.9 page 17 pour le lemme 1.
Cours de Thibaut Deheuvels (ENS Rennes), pour le théorème 2.

Recasage : 158, 162, 181, 215, 219, 229, 233, 253.

**Lemme 34.1 (*Kantorovitch*)**

*Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$. Pour tout $x \in \mathbb{R}^n$,*

$$\|x\|^4 \leq \langle Ax, x\rangle\langle A^{-1}x, x\rangle \leq \frac{1}{4}\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^2 \|x\|^4$$

*où $\lambda_1 \geq \cdots \geq \lambda_n > 0$ sont les valeurs propres de $A$.*

▷ Par homogénéité, il suffit de montrer le résultat pour $\|x\| = 1$. De plus, on peut supposer $\lambda_1 > \lambda_n$ car sinon le résultat est immédiat.

– Comme $A \in \mathcal{S}_n^{++}(\mathbb{R})$, il existe $P \in \mathcal{O}_n(\mathbb{R})$ telle que ${}^tPAP = \operatorname{diag}(\lambda_1, \ldots, \lambda_n) = \Delta$ et ${}^tPA^{-1}P = \operatorname{diag}\left(\frac{1}{\lambda_1}, \ldots, \frac{1}{\lambda_n}\right) = \Delta^{-1}$. Alors,

$$\forall x \in \mathbb{R}^n, \qquad \langle Ax, x\rangle\langle A^{-1}x, x\rangle = \langle \Delta(Px), Px\rangle\langle \Delta^{-1}(Px), Px\rangle.$$

En effectuant le changement de variables $x \mapsto Px$, il suffit de montrer que

$$\forall y \in \mathbb{R}^n,\ \|y\| = 1, \qquad 1 \leq \langle \Delta y, y\rangle\langle \Delta^{-1}y, y\rangle \leq \frac{1}{4}\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^2.$$

– Soit $y \in \mathbb{R}^n$. Pour $k \in [\![1, n]\!]$, on note $M_k$ le point de coordonnées $\left(\lambda_k, \frac{1}{\lambda_k}\right)$. Soit $M$ le barycentre des points $M_k$ affectés des coefficients $y_k^2$. Alors $M$ a pour coordonnées

$$\left(\sum_{k=1}^n \lambda_k y_k^2, \sum_{k=1}^n \frac{y_k^2}{\lambda_k}\right) = \left(\langle \Delta y, y\rangle, \langle \Delta^{-1}y, y\rangle\right).$$

Tous les $M_k$ sont dans l'intersection de l'épigraphe de $u \mapsto u^{-1}$ et du demi-plan inférieur délimité par la droite $(M_1M_n)$, qui est convexe, donc $M$ est aussi dans ce domaine. On peut donc borner l'ordonnée de $M$ :

$$\frac{1}{\langle \Delta y, \Delta y\rangle} \leq \langle \Delta^{-1}y, y\rangle \leq \frac{-1}{\lambda_1\lambda_n}\langle \Delta y, y\rangle + \frac{1}{\lambda_1} + \frac{1}{\lambda_n}$$

d'où

$$1 \leq \langle \Delta y, y\rangle\langle \Delta^{-1}y, y\rangle \leq \frac{\langle \Delta y, y\rangle(\lambda_n + \lambda_1 - \langle \Delta y, y\rangle)}{\lambda_1\lambda_n}.$$

Or la fonction $u \mapsto \dfrac{u(\lambda_1 + \lambda_n - u)}{\lambda_1\lambda_n}$ atteint son maximum en $u = \dfrac{\lambda_1 + \lambda_n}{2}$ et on obtient

$$1 \leq \langle \Delta y, y\rangle\langle \Delta^{-1}y, y\rangle \leq \frac{(\lambda_1 + \lambda_n)^2}{4\lambda_1\lambda_n} = \frac{1}{4}\left(\frac{\lambda_1}{\lambda_n} + \frac{\lambda_n}{\lambda_1} + 2\right) = \frac{1}{4}\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^2.$$

□

**Méthode du gradient à pas optimal** On veut minimiser $f : x \in \mathbb{R}^n \mapsto \langle Ax, x\rangle - \langle b, x\rangle$ où $A \in \mathcal{S}_n^{++}$, et $b \in \mathbb{R}^n$. Pour cela, on se donne $x_0 \in \mathbb{R}^n$ et on construit par récurrence la suite $(x_k)_{k\geq 0}$. Supposons $x_k$ défini. Alors si $d_k = -\nabla f(x_k) = 0$ alors $x_k$ est un minimum et on s'arrête. Sinon, on définit $\rho_k$ l'unique réel positif minimisant $t \mapsto f(x_k + \rho d_k)$ et on pose $x_{k+1} = x_k + \rho_k d_k$.

**Théorème 34.2**

*$f$ a un unique minimum, atteint en $x^*$.. Notons $\kappa_A = \|A\|_2 \left\|A^{-1}\right\|_2 = \dfrac{\lambda_1}{\lambda_n}$ le conditionnement de $A$. Alors, pour tout*

$k \in \mathbb{N}$,

$$\|x_k - x^*\| \leq \sqrt{\kappa_A}\left(\frac{\kappa_1 - 1}{\kappa_A + 1}\right)^k \|x_0 - x^*\|.$$

▷ – *Étape 1 : détermination du pas optimal.* On a, pour $k \in \mathbb{N}$,

$$f(x_{k+1}) = \inf_{\rho \in \mathbb{R}} f(x_k + \rho d_k)$$

donc $\langle \nabla f(x_{k+1}), d_k\rangle = 0$ d'où $\langle d_{k+1}, d_k\rangle = 0$ et $\langle A(x_k + \rho d_k) - b, d_k = 0$ *ie.* $\langle -d_k + \rho A d_k, d_k\rangle = 0$ d'où

$$\rho_k = \frac{\|d_k\|^2}{\langle Ad_k, d_k\rangle}.$$

– *Étape 2 : estimation de l'erreur.* On pose $e_k = x_k - x^*$. On a alors

$$\lambda_n \|e_k\|^2 \leq \langle Ae_k, e_k\rangle \leq \lambda_1 \|e_k\|^2.$$

De plus, $Ae_k = Ax_k - b - (Ax^* - b) = -d_k$, pour tout $k \in \mathbb{N}$. Alors,

$$\begin{aligned}
\langle Ae_{k+1}, e_{k+1}\rangle &= \langle Ae_{k+1}, e_k + \rho_k d_k\rangle \\
&= \langle Ae_{k+1}, e_k\rangle \\
&= \langle Ae_k, e_k\rangle + \rho_k \langle Ad_k, e_k\rangle \\
&= \langle Ae_k, e_k\rangle \left(1 + \frac{\|d_k\|^2}{\langle Ad_k, d_k\rangle}\frac{\langle Ad_k, e_k\rangle}{\langle Ae_k, e_k\rangle}\right) \\
&= \langle Ae_k, e_k\rangle \left(1 - \frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle\langle A^{-1}d_k, d_k\rangle}\right) \\
&\underset{\text{Kantorovitch}}{\leq} \langle Ae_k, e_k\rangle \left(1 - \frac{4\lambda_1\lambda_n}{(\lambda_1 + \lambda_n)^2}\right) \\
&\leq \langle Ae_k, e_k\rangle \left(\frac{\lambda_1 - \lambda_n}{\lambda_1 + \lambda_n}\right)^2 \\
&\leq \langle Ae_k, e_k\rangle \left(\frac{\kappa_A - 1}{\kappa_A + 1}\right)^2.
\end{aligned}$$

Ainsi,

$$\forall k \in \mathbb{N}, \qquad \langle Ae_k, e_k\rangle \leq \left(\frac{\kappa_A - 1}{\kappa_A + 1}\right)^{2k} \langle Ae_0, e_0\rangle$$

d'où

$$\forall k \in \mathbb{N}, \qquad \|x_k - x^*\|^2 \leq \frac{\lambda_1}{\lambda_n}\left(\frac{\kappa_A - 1}{\kappa_A + 1}\right)^{2k} \|x_0 - x^*\|^2$$

d'où le résultat. □

# 35 Modèle de Galton-Watson

Recasage : 223, 226, 260, 264.

Soit $X$ une variable aléatoire discrète intégrable. On note $p_k = \mathbb{P}(X = k)$ et $m = \mathbb{E}[X] = \sum_{k=0}^{\infty} kp_k$.

Soient $(X_{i,n})_{i,n}$ des variables aléatoires iid de loi $\mathbb{P}_X$. On pose $Z_0 = 1$ et

$$\forall n \in \mathbb{N}, \qquad Z_{n+1} = \sum_{i=1}^{Z_n} X_{i,n}.$$

$Z_n$ représente le nombre d'individus à la $n$-ième génération. $X_{i,n}$ est le nombre de descendant de l'individu $i$ de la génération $n$.
On s'intéresse à la probabilité d'extinction $\mathbb{P}(\exists n \in \mathbb{N},\, Z_n = 0)$.

**Lemme 35.1**

*Pour tout $n \in \mathbb{N}$, $i \in \mathbb{N}$, $Z_n \perp\!\!\!\perp X_{i,n}$.*

▷ Par récurrence, car $Z_n$ dépend de $Z_{n-1}$ et $X_{i,n-1}$. □

– On note $\pi_n = \mathbb{P}(Z_n = 0)$ et

$$\pi_\infty = \mathbb{P}(\exists n \in \mathbb{N},\, Z_n = 0) = \mathbb{P}\left(\bigcup_{n\in\mathbb{N}} \uparrow \{Z_n = 0\}\right) = \lim_{n\to+\infty} \pi_n.$$

– Si $p_0 = 0$, alors $\forall n$, $Z_n \geq 1$ ps et donc $\pi_\infty = 0$.
– Si $p_0 = 1$, alors $\forall n$, $Z_n = 0$ ps et $\pi_\infty = 1$.
– On suppose désormais que $p_0 \in ]0, 1[$. On définit la série génératrice des moments de $X$ par

$$G(s) = \mathbb{E}[s^X] = \sum_{k=0}^{\infty} p_k s^k.$$

**Proposition 35.2**

*(i) $G$ est $\mathcal{C}^1$ sur $[0, 1]$.*
*(ii) $G$ est strictement croissante sur $]0, 1[$.*
*(iii) $G$ est convexe sur $]0, 1[$.*
*(iv) $G$ est strictement convexe sur $]0, 1[$ si et seulement si $p_0 + p_1 < 1$.*

▷ *(i)* Pour tout $k \geq 0$, $s \mapsto p_k s^k$ est $\mathcal{C}^1$ sur $[0, 1]$, la série $\sum_{k\geq 0} p_k$ converge, la série $\sum_{k\geq 0} p_k s^k$ converge normalement donc uniformément sur $[0, 1]$. On en déduit que $G$ est $\mathcal{C}^1$ sur $[0, 1]$.

$G$ est la somme d'une série entière sur $[0, 1[$ donc $G'(s) = \sum_{k=1}^{+\infty} kp_k s^{k-1}$ et $G''(s) = \sum_{k=2}^{+\infty} k(k-1)s^{k-2}$. Soit $k_0 > 0$ tel que $p_{k_0} > 0$.
*(ii)* $G'(s) \geq k_0 p_{k_0} s^{k_0-1} > 0$ donc $G$ est strictement croissante sur $]0, 1[$.
*(iii)* $G''(s) \geq k_0(k_0 - 1)p_{k_0} s^{k_0-2} \geq 0$ donc $G$ est convexe.
*(iv)* Si $p_0 + p_1 = 1$ alors $G$ est affine et donc pas strictement convexe.
Si $p_0 + p_1 < 1$, il existe $k_0 > 1$ tel que $p_{k_0} > 0$ et comme en *(iii)*, $G''(s) > 0$ et $G'$ est strictement convexe. □

Pour tout $n \geq 0$, on définit la fonction génératrice des moments de $Z_n$ :

$$G_n(s) = \mathbb{E}[s^{Z_n}] = \sum_{k=0}^{+\infty} \mathbb{P}(Z_n = k)s^k.$$

**Proposition 35.3**

*On a :*

$$\forall n \in \mathbb{N}, \qquad G_n = \underbrace{G \circ \cdots \circ G}_{n \text{ fois}}$$

*et* $\mathbb{E}[Z_n] = m^n$.

▷ Montrons-le par récurrence. C'est vrai pur $n = 1$ et

$$G_{n+1}(s) = \mathbb{E}[s^{X_{1,n}+\cdots+X_{Z_n,n}}] = \mathbb{E}\left[\sum_{k=0}^{+\infty} \mathbf{1}_{\{Z_n=k\}} \prod_{i=1}^{k} s^{X_{i,n}}\right] \underset{\substack{\text{Fubini}\\ \text{Tonelli}\\ +\perp\!\!\!\perp}}{=} \sum_{k=0}^{+\infty} \mathbb{P}(Z_n = k) \prod_{i=1}^{k} \underbrace{\mathbb{E}[s^{X_{i,n}}]}_{\mathbb{E}[s^X]}$$

$$= \sum_{k=0}^{+\infty} \mathbb{P}(Z_n = k) G(s)^k = G_n(G(s)).$$

Alors,

$$G'_{n+1}(s) = G'(s) G'_n(G(s))$$

donc, en $s = 1$ et par récurrence,

$$\mathbb{E}[Z_{n+1}] = \mathbb{E}[X] G'_n(1) = m^{n+1}$$

□

**Proposition 35.4**

*$\pi_\infty$ est le plus petit point fixe de $G$ sur $[0, 1]$.*

▷ On a $G_{n+1}(s) = G(G_n(s))$ donc, en $s = 0$, $\pi_{n+1} = G(\pi_n)$. Comme $G$ est continue, on en déduit $\pi_\infty = G(\pi_\infty)$. Soit de plus $u \in [0, 1]$ un point fixe de $G$. Montrons par récurrence que $\pi_n \leq u$. On a $\pi_1 = G(\pi_0) = G(\mathbb{P}(Z_0 = 0)) = G(0) \leq G(u) = u$ car $G$ est croissante. De plus, si $\pi_n \leq u$, alors, par croissance de $G$, $\pi_{n+1} = G(\pi_n) \leq G(u) = u$. □

**Théorème 35.5**

*Si $m \leq 1$ alors $\pi_\infty = 1$. Si $m > 1$ alors $\pi_\infty$ est l'unique point fixe de $G$ sur $]0, 1[$.*

**Remarque :** $G(1) = 1$ et $G$ a au plus deux points fixes. En effet, si $p_0 + p_1 = 1$, alors $G$ est affine et $G(0) = p_0 > 0$ donc $G$ n'a qu'un seul point fixe.

Si $p_0 + p_1 < 1$ alors $G$ est strictement convexe. Supposons par l'absurde que $G$ a trois points fixes distincts. Alors d'après le théorème de Rolle, $G' - 1$ s'annule en $a$ et $b$, avec $0 < a < b < 1$. Comme $G' - 1$ est croissante, on en déduit que $G' - 1$ est nulle sur $[a, b]$ ce qui contredit la stricte croissance de $G' - 1$, qui vient de la stricte convexité de $G$.

▷ Notons $h = G - \mathrm{Id}$. (Raisonner sur les tableaux de variations)

Cas $m > 1$. $h'(0) = p_1 - 1 < 0 < m - 1 = h'(1)$ donc, comme $h$ est continue, il existe $\alpha \in ]0, 1[$ tel que $h'(\alpha) = 0$. Comme $h'$ est croissante, on en déduit que $h$ est décroissante sur $[0, \alpha]$ et croissante sur $[\alpha, 1]$. Comme $h(1) = 0$ et $\alpha < 1$, on en déduit que $h$ s'annule sur $]0, 1[$ : il existe $y_0 \in ]0, 1[$ tel que $G(y_0) = y_0$. 1 et $y_0$ sont donc deux points fixes de $G$. $y_0$ est donc l'unique point fixe dans $]0, 1[$.

Cas $m < 1$. $h'$ est croissante sur $]0, 1[$et $h'(1) = m - 1 \leq 0$ donc $h$ est décroissante sur $[0, 1]$ et vaut 0 en 1. Comme $h$ ne s'annule qu'au plus deux fois, 1 est le seul point d'annulation de $h$ *ie.* l'unique point fixe de $G$. □

# 36 Probabilité que deux entiers soient premiers entre eux

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*, 3e édition, Cassini. Exercice 4.33 page 156.

Recasage : 190, 230.

**Proposition 36.1**

*Pour $n \in \mathbb{N}^*$, on note $r_n$ la probabilité que deux entiers choisis au hasard dans $[\![1,n]\!]^2$ soient premiers entre eux. On a :*

$$r_n \xrightarrow[n\to+\infty]{} \frac{6}{\pi^2}.$$

*– Étape 1 : Montrons que pour tout $n \in \mathbb{N}^*$, $r_n = \dfrac{1}{n^2}\displaystyle\sum_{d=1}^{n} \mu(d)\left\lfloor \frac{n}{d}\right\rfloor^2$, où*

$$\forall d \in \mathbb{N}^* \mu(d) = \begin{cases} 1 & \text{si } d = 1 \\ 0 & \text{si } d \text{ a un facteur carré} \\ (-1)^k & \text{si } d = p_1 \dots p_k \text{ avec les } p_i \text{ premiers distincts.} \end{cases}$$

Soit $n \in \mathbb{N}^*$. On note $A_n = \{(a,b) \in [\![1,n]\!]^2,\ a \wedge b = 1\}$ de sorte que $r_n = \dfrac{\operatorname{Card} A_n}{n^2}$. Soit $\{p_1, \dots, p_k\}$ l'ensemble des nombres premiers distincts dans $[\![1,n]\!]$. Pour $i \in \{1,\dots,k\}$, notons $U_i = \{(a,b) \in [\![1,n]\!]^2,\ p_i|a \text{ et } p_i|b\}$. On a :

$$A_n = \left(\bigcup_{i=1}^{k} U_i\right)^c$$

donc

$$\operatorname{Card} A_n = n^2 - \operatorname{Card}\left(\bigcup_{i=1}^{k} U_i\right).$$

On utilise la formule du crible :

**Lemme 36.2**

*Soient $U_1, \dots, U_k$ des ensembles finis. On a :*

$$\operatorname{Card}\left(\bigcup_{i=1}^{k} U_i\right) = \sum_{\emptyset \neq I \subset [\![1,k]\!]} (-1)^{1+\operatorname{Card} I} \operatorname{Card}\left(\bigcap_{i\in I} U_i\right).$$

Pour $I = \{i_1, \dots, i_\ell\} \subset [\![1,k]\!]$, on a :

$$\operatorname{Card}\left(\bigcap_{i\in I} U_i\right) = \operatorname{Card}\left\{(a,b) \in [\![1,n]\!]^2,\ p_{i_1}\cdots p_{i_\ell}|a \text{ et } p_{i_1}\cdots p_{i_\ell}|b\right\} = \left\lfloor \frac{n}{p_{i_1}\cdots p_{i_\ell}}\right\rfloor^2.$$

Ainsi,

$$\begin{aligned} \operatorname{Card} A_n &= n^2 - \sum_{\{i_1,\dots,i_\ell\}\subset[\![1,k]\!]} (-1)^{\ell+1}\left\lfloor \frac{n}{p_{i_1}\cdots p_{i_\ell}}\right\rfloor^2 \\ &= n^2 + \sum_{\{i_1,\dots,i_\ell\}\subset[\![1,k]\!]} \mu(p_{i_1}\cdots p_{i_\ell})\left\lfloor \frac{n}{p_{i_1}\cdots p_{i_\ell}}\right\rfloor^2 \\ &= \sum_{d=1}^{n} \mu(d)\left\lfloor \frac{n}{d}\right\rfloor^2. \end{aligned}$$

On a donc montré que

$$\forall n \in \mathbb{N}^*, \qquad r_n = \frac{1}{n^2}\sum_{d=1}^{n} \mu(d)\left\lfloor \frac{n}{d}\right\rfloor^2.$$

– *Étape 2 : Exploitons l'équivalent* $\frac{1}{n^2}\left\lfloor\frac{n}{d}\right\rfloor^2 \underset{n\to+\infty}{\sim} \frac{1}{d^2}$. Considérons

$$\left|r_n - \sum_{d=1}^{n}\frac{\mu(d)}{d^2}\right| = \left|\sum_{d=1}^{n}\mu(d)\left(\frac{1}{n^2}\left\lfloor\frac{n}{d}\right\rfloor^2 - \frac{1}{d^2}\right)\right|.$$

Pour tout $1 \leq d \leq n$, on a $\left\lfloor\frac{n}{d}\right\rfloor > \frac{n}{d} - 1$ d'où l'on déduit

$$\frac{1}{n^2} - \frac{2}{nd} < \frac{1}{n^2}\left\lfloor\frac{n}{d}\right\rfloor^2 - \frac{1}{d^2} \leq 0.$$

Alors,

$$\left|r_n - \sum_{d=1}^{n}\frac{\mu(d)}{d^2}\right| \leq \sum_{d=1}^{n}\left(\frac{2}{nd} + \frac{1}{n^2}\right) = \frac{2}{n}\sum_{d=1}^{n}\frac{1}{d} + \frac{1}{n} = \underset{n\to+\infty}{\mathcal{O}}\left(\frac{\ln n}{n}\right)$$

grâce à l'équivalent des sommes partielles de la série harmonique. Comme la série $\sum_{d\geq 1}\frac{\mu(d)}{d^2}$ converge absolument,

$$r_n \xrightarrow[n\to+\infty]{} \sum_{d=1}^{+\infty}\frac{\mu(d)}{d^2}.$$

– *Étape 3 : Il ne reste plus qu'à montrer que* $\left(\sum_{d=1}^{+\infty}\frac{\mu(d)}{d^2}\right)\left(\sum_{n=1}^{+\infty}\frac{1}{n^2}\right) = 1$. Les deux séries convergeant absolument, la famille $\left(\frac{\mu(d)}{(nd)^2}\right)_{(n,d)\in\mathbb{N}^2}$ est sommable. Alors,

$$\left(\sum_{d=1}^{+\infty}\frac{\mu(d)}{d^2}\right)\left(\sum_{n=1}^{+\infty}\frac{1}{n^2}\right) = \sum_{(n,d)\in\mathbb{N}^2}\frac{\mu(d)}{(nd)^2} = \sum_{p=1}^{+\infty}\sum_{d|p}\frac{\mu(d)}{p^2} = \sum_{p=1}^{+\infty}\frac{1}{p^2}\sum_{d|p}\mu(d).$$

Montrons que, pour $n \in \mathbb{N}^*$, $\sum_{d|n}\mu(d) = \delta_{1n}$. Pour $n = 1$, c'est vrai. Soit $n \geq 2$. On écrit $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ avec $\alpha_\ell \geq 1$ pour tout $1 \leq \ell \leq k$ et $p_1, \ldots, p_r$ des nombres premiers distincts. Pour $d|n$, $\mu(d) \neq 0$ si et seulement si $d = p_{i_1}\cdots p_{i_\ell}$ et dans ce cas $\mu(d) = (-1)^\ell$. Pour un $\ell \in \{1, \ldots, k\}$ fixé, il y a $\binom{k}{\ell}$ tels choix de $d$. Ainsi,

$$\sum_{d|n}\mu(d) = \sum_{\ell=1}^{k}\binom{k}{\ell}(-1)^\ell = 0.$$

Ainsi,

$$\left(\sum_{d=1}^{+\infty}\frac{\mu(d)}{d^2}\right)\left(\sum_{n=1}^{+\infty}\frac{1}{n^2}\right) = 1$$

d'où

$$\lim_{n\to+\infty} r_n = \frac{6}{\pi^2}.$$

# 37 Théorèmes angulaire d'Abel et taubérien faible

X. Gourdon, *Les maths en tête : Analyse*, 2e édition, Ellipses. Exercices 10 et 11 page 252.

Recasage : 207, 223, 224, 230, 235, 241, 243

**Théorème 37.1 (*Abel*)**

*Soit $\sum_{n\geq 0} a_n z^n$ une série entière de rayon de converge $\geq 1$ telle que $\sum_{n\geq 0} a_n$ converge. On note $f$ la somme de cette série entière sur $B(0,1)$. Pour $\theta_0 \in [0, \frac{\pi}{2}[$. On pose*

$$\Delta_{\theta_0} = \{z \in B(0,1),\ \exists \rho > 0, \exists \theta \in [-\theta_0, \theta_0],\ z = 1 - \rho e^{i\theta}\}.$$

*Alors, la limite suivante existe et*

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

▷ Notons $S = \sum_{n=0}^{+\infty} a_n$ et, pour $N \in \mathbb{N}$, $S_n = \sum_{n=0}^{N} a_n$ et $R_N = S - S_N$.

Soient $z \in B(0,1)$ et $N \in \mathbb{N}$. Par une transformation d'Abel, on obtient :

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

Comme $\sum_{n=0}^{N} a_n z^n \xrightarrow[N\to+\infty]{} f(z)$, $S_N \xrightarrow[N\to+\infty]{} S$, et $R_N(z^N - 1) \xrightarrow[N\to+\infty]{} 0$, on en déduit que la série de terme général $(R_n z^n)$ converge et :

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

Soient $\varepsilon > 0$ et $N \geq 0$ tel que $\forall n > N$, $|R_n| \leq \varepsilon$. Alors,

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

Supposons $z \in \Delta_{\theta_0}$ avec $z = 1 - \rho e^{i\theta}$, $\theta \in [-\theta_0, \theta_0]$. Alors, $|z|^2 = 1 - 2\rho\cos\theta + \rho^2$ et, si $\rho \leq \cos\theta_0$,

$$\frac{|z-1|}{1-|z|} = \frac{|z-1|}{1-|z|^2}(1+|z|) \leq \frac{2\rho}{2\rho\cos\theta - \rho^2} \leq \frac{2}{2\cos\theta - \rho} \leq \frac{2}{\cos\theta_0}.$$

Soit $\alpha > 0$ tel que $\alpha\sum_{n=0}^{N} |R_n| \leq \varepsilon$. Alors, tout pour $z \in \Delta_{\theta_0}$ tel que $|z-1| \leq \min(\alpha, \cos\theta_0)$, on a $|f(z) - S| \leq \varepsilon\left(1 + \frac{2}{\cos\theta_0}\right)$. Ainsi, $\lim_{\substack{z\to 1 \\ z\in\Delta_{\theta_0}}} f(z) = S$. □

**Remarques :** – On en déduit

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{2n+1} = \lim_{x\to 1^-} \sum_{n=0}^{+\infty} \frac{(-1)^n}{2n+1} x^n = \lim_{x\to 1^-} \operatorname{Arctan} x = \frac{\pi}{4}$$

car la série de terme général $\dfrac{(-1)^n}{2n+1}$ converge par le critère des séries alternées.

– L'existence de la limite n'implique pas la convergence au bord :

$$\lim_{x\to 1^-} (-1)^n x^n = \lim_{x\to 1^-} \frac{1}{1+z} = \frac{1}{2}$$

mais la série de terme général $(-1)^n$ ne converge pas.

On a une réciproque partielle si $a_n = \underset{n\to+\infty}{o}\left(\dfrac{1}{n}\right)$.

**Théorème 37.2 (*Taubérien faible*)**

*Soit $\sum_{n\geq 0} a_n z^n$ une série entière de rayon de convergence égal à 1. Notons $f$ sa somme sur $B(0,1)$. On suppose qu'il existe $S \in \mathbb{C}$ tel que $\lim_{x\to 1^-} f(x) = S$. Si $a_n = \underset{n\to+\infty}{o}\left(\dfrac{1}{n}\right)$, alors la série de terme général $(a_n)$ converge et $\sum_{n=0}^{+\infty} a_n = S$.*

▷ Pour $N \in \mathbb{N}$, notons $S_N = \sum_{n=0}^{N} a_n$. Pour tout $N \in \mathbb{N}^*$ et $x \in ]0,1[$,

$$S_N - f(x) = \sum_{n=1}^{N} a_n(1-x^n) - \sum_{n=N+1}^{+\infty} a_n x^n.$$

Or, pour tout $n \in \mathbb{N}^*$ et $x \in ]0,1[$, $(1-x^n) \leq (1-x)(1+x+\cdots+x^{n-1}) \leq n(1-x)$ donc, en notant $M$ un majorant de $(n|a_n|)_{n\in\mathbb{N}}$ (bornée car convergente), on a :

$$\forall x \in ]0,1[, \forall N > 0, \qquad |S_N - f(x)| \leq MN(1-x) + \frac{\sup_{n>N} n|a_n|}{N(1-x)}.$$

Soit $\varepsilon \in ]0,1[$ et $N_0 \in \mathbb{N}$ tel que $\sup_{n>N_0} n|a_n| \leq \varepsilon^2$. Alors, pour $N \geq N_0$,

$$\left|S_N - f\left(1-\frac{\varepsilon}{N}\right)\right| \leq (M+1)\varepsilon.$$

De plus, il existe $N_1 \geq N_0$ tel que $\forall N \geq N_1$, $\left|f\left(1-\dfrac{\varepsilon}{N}\right) - S\right| \leq \varepsilon$. Donc, pour $N \geq N_1$,

$$|S_N - S| \leq \left|S_N - f\left(1-\frac{\varepsilon}{N}\right)\right| + \left|f\left(1-\frac{\varepsilon}{N}\right) - S\right| \leq (M+2)\varepsilon$$

donc $S_N \xrightarrow[N\to+\infty]{} S$. □

# 38 Théorème central limite

H. Queffélec, C. Zuily, *Analyse pour l'agrégation*, 4e édition, Dunod. Théorème II.22 page 540.

Recasage : 261, 262, 263.

**Théorème 38.1**

*Soit $(X_n)$ une suite de variables aléatoires indépendantes identiquement distribuées dans $L^2$ avec $S_n = \sum_{i=1}^{n} X_i$, $m = \mathbb{E}[X_1]$ et $\sigma^2 = \mathrm{Var}(X_1) > 0$. Alors*

$$\frac{S_n - nm}{\sqrt{n\sigma^2}} \xrightarrow[n\to+\infty]{\mathscr{L}} \mathcal{N}(0,1).$$

▷ Quitte à considérer $\dfrac{X_i - m}{\sigma}$ on peut supposer $m = 0$ et $\sigma = 1$. Grâce au théorème de Paul Lévy, il suffit de montrer que, si $X \sim \mathcal{N}(0,1)$,

$$\forall t \in \mathbb{R}, \qquad \varphi_{\frac{S_n}{\sqrt{n}}}(t) \xrightarrow[n\to+\infty]{} \varphi_X(t).$$

Or

**Lemme 38.2**

*Si $X \sim \mathcal{N}(0,1)$, $\forall t \in \mathbb{R}$, $\varphi_X(t) = e^{-t^2/2}$.*

▷ Pour tout $t \in \mathbb{R}$, on a $\varphi_X(t) = \mathbb{E}[e^{iXt}] = \dfrac{1}{\sqrt{2\pi}} \displaystyle\int_{-\infty}^{+\infty} e^{-\frac{x^2}{2}} e^{-ixt} \mathrm{d}x$ d'après le théorème de transfert. Or

- $\forall t \in \mathbb{R}$, $x \in \mathbb{R} \mapsto e^{-\frac{x^2}{2}} e^{ixt} \in L^1(\mathbb{R})$
- $\forall x \in \mathbb{R}$, $t \in \mathbb{R} \mapsto e^{-\frac{x^2}{2}} e^{ixt}$ est de classe $\mathcal{C}^1$
- $\forall (t,x) \in \mathbb{R}^2$, $\left| e^{-\frac{x^2}{2}} ixe^{ixt} \right| = |x| e^{-\frac{x^2}{2}}$ intégrable et indépendant de $t$

donc d'après le théorème de dérivation, $\varphi_X$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}$ et

$$\forall t \in \mathbb{R}, \qquad \varphi'_X(t) = \frac{it}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} xe^{-\frac{x^2}{2}} e^{ixt} \mathrm{d}t.$$

Par intégration par parties, on a donc, pour $t \in \mathbb{R}$,

$$\varphi'_X(t) = \frac{it}{\sqrt{2\pi}} \left[ -e^{-\frac{x^2}{2}} e^{ixt} \right]_{-\infty}^{+\infty} + \frac{(it)^2}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-\frac{x^2}{2}} e^{ixt} \mathrm{d}x = -t^2 \varphi_X(t).$$

On en déduit que

$$\forall t \in \mathbb{R}, \qquad \varphi_X(t) = \varphi_X(0) e^{-\frac{t^2}{2}} = e^{-\frac{t^2}{2}}.$$

□

Notons $\varphi = \varphi_{X_1}$. Comme $X_1 \in L^2$, le théorème de dérivation des intégrales à paramètres permet de monter que $\varphi$ est de classe $\mathcal{C}^2$ et

$$\varphi'(0) = \mathbb{E}[iX] = 0 \qquad \varphi''(0) = \mathbb{E}[-X^2] = -1.$$

De plus, comme les $X_i$ sont indépendantes,

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

Or $\varphi$ est de classe $\mathcal{C}^2$ donc d'après la théorème de Taylor-Young,

$$\varphi\left( \frac{t}{\sqrt{n}} \right) = \varphi(0) + \frac{t}{\sqrt{n}} \varphi'(0) + \frac{t^2}{2n} \varphi''(0) + \frac{\varepsilon_n}{n} = 1 - \frac{t^2}{2n} + \frac{\varepsilon_n}{n}$$

avec $\varepsilon_n \xrightarrow[n\to+\infty]{} 0$. Ainsi,

$$\forall t \in \mathbb{R}, \qquad \varphi_{\frac{S_n}{\sqrt{n}}}(t) = \left( 1 - \frac{t^2}{2n} + \frac{\varepsilon_n}{n} \right)^n.$$

Il suffit donc de montrer le lemme suivant :

**Lemme 38.3**

*Soit $(z_n) \in \mathbb{C}^{\mathbb{N}}$ convergeant vers $z \in \mathbb{C}$. Alors*

$$\left(1+\frac{z_n}{n}\right)^n \xrightarrow[n\to+\infty]{} e^z.$$

▷ Pour tout $n \in \mathbb{N}$, on a :

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

avec

$$a_{n,k} = \begin{cases} \dfrac{1}{k!}\left(1 - \dfrac{n(n-1)\cdots(n-k+1)}{n^k}\right) & \text{si } k \leq n \\ \dfrac{1}{k!} & \text{si } k \geq n. \end{cases}$$

Comme $a_{n,k} \geq 0$, on a :

$$\begin{aligned}
\left|e^{z_n} - \left(1+\frac{z_n}{n}\right)^n\right| &\leq \sum_{k=0}^{+\infty} a_{n,k}|z_n|^k \\
&\leq e^{|z_n|} - \left(1 - \frac{|z_n|}{n}\right)^n \\
&\leq e^{|z_n|} - e^{n\ln\left(1-\frac{z_n}{n}\right)} \\
&\underset{\ln(1+x)\geq x-\frac{x^2}{2}}{\leq} e^{|z_n|} - e^{|z_n| - \frac{|z_n|^2}{2n}} \\
&\leq e^{|z_n|}\left(1 - e^{-\frac{|z_n|^2}{2n}}\right) \\
&\underset{e^x\geq x+1}{\leq} e^{|z_n|}\frac{|z_n|^2}{2n}.
\end{aligned}$$

Ainsi,

$$\left|e^z - \left(1+\frac{z_n}{n}\right)^n\right| \leq |e^z - e^{z_n}| + e^{|z_n|}\frac{|z_n|^2}{2n} \xrightarrow[n\to+\infty]{} 0.$$

□

□

# 39 Théorèmes de Dini et Glivenko-Cantelli

X. Gourdon, *Les maths en tête : Analyse*, 2e édition, Ellipses. Exercice 5 page 228
Y. Nourdin, *Agrégation de mathématiques épreuve orale*, 2e édition, Dunod. Théorème 1.25.9 page 109

Recasage : 228, 229, 241, 262, 263

**Théorème 39.1 (*Deuxième théorème de Dini*)**

*Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions réelles croissantes*[1] *définies sur un segment $[a,b]$ de $\mathbb{R}$. Si $(f_n)_{n\in\mathbb{N}}$ converge simplement vers une fonction $f$ continue sur $[a,b]$, alors la convergence est uniforme.*

▷ − $f$ est continue sur le compact $[a,b]$ donc, d'après le théorème de Heine, $f$ y est uniformément continue. Soit $\varepsilon>0$. Il existe donc $\eta>0$ tel que

$$\forall x,y\in[a,b],\qquad |x-y|<\eta \quad\Rightarrow\quad |f(x)-f(y)|<\varepsilon.$$

− Donnons-nous une subdivision $a=x_0<x_1<\cdots<x_p=b$ de pas $<\eta$. Comme $f_n(x_i)\xrightarrow[n\to+\infty]{} f(x_i)$ pour tout $i\in\{1,\dots,p\}$, il existe $N\geq 0$ tel que

$$\forall n\geq N,\qquad |f(x_i)-f_n(x_i)|\leq\varepsilon.$$

− Soient $x\in[a,b]$ et $i$ tel que $x\in[x_i,x_{i+1}]$. On a, comme les $f_n$ sont croissantes,

$$\begin{aligned}|f(x)-f_n(x)| &\leq |f(x)-f(x_i)|+|f(x_i)-f_n(x_i)|+|f_n(x_i)-f_n(x)|\\ &\leq \varepsilon+\varepsilon+f_n(x)-f_n(x_i)\\ &\leq 2\varepsilon+f_n(x_{i+1})-f_n(x_i)\\ &\leq 2\varepsilon+|f_n(x_{i+1})-f(x_{i+1})|+|f(x_{i+1})-f(x_i)|+|f(x_i)-f_n(x_i)|\\ &\leq 5\varepsilon.\end{aligned}$$

□

**Théorème 39.2**

*Soient $(X_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires iid. Soit $F$ la fonction de répartition commune des $X_n$. Pour $t\in\mathbb{R}$ et $n\in\mathbb{N}^*$, on pose*

$$F_n(t)=\frac{1}{n}\sum_{k=1}^{n}\mathbf{1}_{\{X_k\leq t\}}.$$

*Alors, presque sûrement, $\sup_{t\in\mathbb{R}}|F_n(t)-F(t)|\xrightarrow[n\to+\infty]{}0$.*

▷ D'après la loi forte des grands nombres, $F_n(t)\xrightarrow[n\to+\infty]{}F(t)$ presque sûrement. On veut une convergence uniforme en $t$. Comme les $F_n$ sont croissantes, on pense au théorème de Dini. Problème : il n'y a pas de continuité et on ne travaille pas sur un compact. On s'y ramène grâce à l'inverse généralisé.

**Lemme 39.3**

*On définit $F^{\leftarrow}:u\in[0,1]\mapsto\inf\{x\in\mathbb{R},\,F(x)\geq u\}$. On a :*

$$\forall x\in\mathbb{R},\forall u\in[0,1],\quad F^{\leftarrow}(u)\leq x\quad\Longleftrightarrow\qquad u\leq F(x).$$

▷ − Si $F^{\leftarrow}(u)\leq x$ alors il existe $y\leq x$ tel que $F(y)\geq u$. Comme $F$ est croissante, $F(x)\geq F(y)\geq u$.
− Si $u\leq F(x)$ alors $x\in\{y\in\mathbb{R},\,F(y)\geq u\}$ donc $x\geq\inf\{y\in\mathbb{R},\,F(y)\geq u\}=F^{\leftarrow}(u)$. □

**Corollaire 39.4**

*Si $Y$ est une variable aléatoire réelle de fonction de répartition $G$ et $U\sim\mathcal{U}([0,1])$ alors $G^{\leftarrow}(U)$ a la même loi que $Y$.*

▷ On a $\mathbb{P}(G^{\leftarrow}(U)\leq x)=\mathbb{P}(U\leq G(x))=G(x)$. □

− On se ramène alors au cas de variables aléatoires suivant la loi uniforme sur [0,1]. Soit $(U_n)_{n\in\mathbb{N}}$ une suite de variables indépendantes suivant la loi uniforme sur $[0,1]$. On a l'égalité de loi suivante :

$$\begin{aligned}\sup_{t\in\mathbb{R}}|F_n(t)-F(t)|\sim\sup_{t\in\mathbb{R}}\left|\frac{1}{n}\sum_{k=1}^{n}\mathbf{1}_{\{F^{\leftarrow}(U_k)\leq t\}}-F(t)\right| &= \sup_{t\in\mathbb{R}}\left|\frac{1}{n}\sum_{k=1}^{n}\mathbf{1}_{U_k\leq F(t)}-F(t)\right|\\ &\leq \sup_{s\in[0,1]}\left|\frac{1}{n}\sum_{k=1}^{n}\mathbf{1}_{\{U_k\leq s\}}-s\right|.\end{aligned}$$

1. Contrairement à ce qui est écrit dans le Gourdon, il n'est pas nécessaire que les $f_n$ soient continues.

Il suffit donc de traiter le cas de variables uniformes sur $[0,1]$.

– D'après la loi forte des grands nombres, pour tout $s \in [0,1]$, il existe $N_s \subset \Omega$ tel que $\mathbb{P}(N_s) = 0$ et

$$\forall \omega \in N_s^c, \qquad \frac{1}{n}\sum_{k=1}^{n} \mathbf{1}_{\{U_k(\omega)\leq s\}} \xrightarrow[n\to+\infty]{} s.$$

Comme une réunion dénombrable de négligeables est négligeable, il existe $N \subset \Omega$ tel que $\mathbb{P}(N) = 0$ et

$$\forall s \in [0,1]\cap\mathbb{Q}, \forall \omega \in N^c, \qquad \frac{1}{n}\sum_{k=1}^{n} \mathbf{1}_{\{U_k(\omega)\leq s\}} \xrightarrow[n\to+\infty]{} s.$$

C'est encore vrai pour tout $s \in [0,1]$. En effet, soient $s \in [0,1]$, $\varepsilon > 0$ et $\omega \in N$. Il existe $p, q \in \mathbb{Q}$ tels que $s - \varepsilon \leq p \leq s \leq q \leq s + \varepsilon$. Comme $s \mapsto \frac{1}{n}\sum_{k=1}^{n} \mathbf{1}_{\{U_k(\omega)\leq s\}}$ est croissante,

$$\frac{1}{n}\sum_{k=1}^{n} \mathbf{1}_{\{U_k(\omega)\leq p\}} \leq \frac{1}{n}\sum_{k=1}^{n} \mathbf{1}_{\{U_k(\omega)\leq s\}} \leq \frac{1}{n}\sum_{k=1}^{n} \mathbf{1}_{\{U_k(\omega)\leq q\}}$$

d'où

$$s - \varepsilon \leq \liminf_{n\to+\infty} \frac{1}{n}\sum_{k=1}^{n} \mathbf{1}_{\{U_k(\omega)\leq s\}} \leq \limsup_{n\to+\infty} \frac{1}{n}\sum_{k=1}^{n} \mathbf{1}_{\{U_k(\omega)\leq s\}} \leq s + \varepsilon,$$

d'où le résultat.

– On a donc montré, pour $\omega \in N^c$,

⋆ $s \mapsto \frac{1}{n}\sum_{k=1}^{n} \mathbf{1}_{\{U_k(\omega)\leq s\}}$ est croissante pour tout $n \in \mathbb{N}^*$,

⋆ $\frac{1}{n}\sum_{k=1}^{n} \mathbf{1}_{\{U_k(\omega)\leq s\}} \xrightarrow[n\to+\infty]{} s$ et $s \mapsto s$ continue.

D'après le théorème de Dini, on a donc convergence uniforme presque partout.

□

# 40 Théorème de Grothendieck

M. Zavidovique, *Un Max de Math*, Calvage & Mounet. Problème 30 page 180.

Recasage : 205, 208, 234.

**Théorème 40.1**

*Soit $(\Omega, \mathcal{A}, \mu)$ un espace de probabilités et $p \in [1, +\infty[$. Soit $S$ un sous-espace vectoriel fermé de $L^p_\mu(\Omega)$ tel que $S \subset L^\infty_\mu(\Omega)$. Alors $S$ est de dimension finie.*

▷ *– Étape 1 : Les normes $\|.\|_p$ et $\|.\|_\infty$ sont équivalentes sur $S$.* On a

$$\forall f \in S, \qquad \|f\|_p = \left(\int_\Omega |f|^p \mathrm{d}\mu\right)^{\frac{1}{p}} \leq \|f\|_\infty$$

donc l'inclusion canonique $i : (S, \|.\|_\infty) \hookrightarrow (S, \|.\|_p)$ est continue. De plus, $(S, \|.\|_p)$ est fermé dans $L^p_\mu(\Omega)$ donc $S = i^{-1}(S)$ est fermé dans $L^\infty_\mu(\Omega)$. Alors, comme $L^p_\mu(\Omega)$ et $L^\infty_\mu(\Omega)$ sont des espaces de Banach, il en va de même pour $(S, \|.\|_p)$ et $(S, \|.\|_\infty)$. Comme $i$ est linéaire continue et surjective, d'après le théorème de l'application ouverte, il existe $\alpha > 0$ telle que

$$\forall f \in S, \qquad \|f\|_\infty \leq \alpha \|f\|_p .$$

*– Étape 2 : $(S, \|.\|_2) \hookrightarrow (S, \|.\|_\infty)$ est continue.*

⋆ si $p < 2$ alors $1 < \dfrac{2}{p}$ et par l'inégalité de Hölder :

$$\forall f \in S, \qquad \int_\Omega |f|^p \times 1 \mathrm{d}\mu \leq \left(\int_\Omega |f|^{p \times \frac{2}{p}} \mathrm{d}\mu\right)^{\frac{p}{2}}$$

donc $\forall f \in S$, $\|f\|_p \leq \|f\|_2$, d'où $\|f\|_\infty \leq \alpha \|f\|_2$.

⋆ si $p \geq 2$ alors, pour $f \in S$, $|f(x)|^p \leq \|f\|_\infty^{p-2} |f(x)|^2$ $\mu$-p.p donc $\|f\|_p^p \leq \|f\|_\infty^{p-2} \|f\|_2^2$. On en déduit que

$$\|f\|_\infty^p \leq \alpha^p \|f\|_p^p \leq \|f\|_\infty^{p-2} \|f\|_2$$

d'où $\|f\|_\infty \leq \alpha^{\frac{p}{2}} \|f\|_2$.

Dans tous les cas, $\forall f \in S$, $\|f\|_\infty \leq M \|f\|_2$.

*– Étape 3 : Majorons le cardinal d'une famille orthonormée de $S$.* Soit $n \in \mathbb{N}$ et $(f_1, \ldots, f_n) \in S$ une famille orthonormée dans $L^2_\mu(\Omega)$. Montrons qu'il existe $\Omega'$ de mesure pleine tel que

$$\forall x \in \Omega', \forall (c_1, \ldots, c_n) \in \mathbb{R}^n, \qquad \left|\sum_{i=1}^n c_i f_i(x)\right| \leq M \sqrt{\sum_{i=1}^n c_i^2}.$$

Pour $c = (c_1, \ldots, c_n) \in \mathbb{Q}^n$,

$$\left\|\sum_{i=1}^n c_i f_i\right\|_\infty \leq M \left\|\sum_{i=1}^n c_i f_i\right\|_2 \underset{\text{Pythagore}}{=} M \sqrt{\sum_{i=1}^n c_i^2}$$

donc il existe $N_c$ tel que $\mu(N_c) = 0$ et

$$\forall x \in \Omega \backslash N_c, \qquad \left|\sum_{i=1}^n c_i f_i(x)\right| \leq M \sqrt{\sum_{i=1}^n c_i^2}.$$

Posons $N = \bigcup_{c \in \mathbb{Q}^n} N_c$. Alors $\mu(N) \leq \sum_{c \in \mathbb{Q}^n} \mu(N_c) = 0$ et

$$\forall x \in \Omega' = \Omega \backslash N, \forall (c_1, \ldots, c_n) \in \mathbb{Q}^n, \qquad \left|\sum_{i=1}^n c_i f_i(x)\right| \leq M \sqrt{\sum_{i=1}^n c_i^2}.$$

Comme $(c_1,\dots,c_n)\in\mathbb{R}^n \mapsto \left|\sum_{i=1}^n c_i f_i(x)\right|$ est continue pour chaque $x\in\Omega'$, on a

$$\forall x\in\Omega', \forall (c_1,\dots,c_n)\in\mathbb{R}^n, \qquad \left|\sum_{i=1}^n c_i f_i(x)\right| \leq M\sqrt{\sum_{i=1}^n c_i^2}.$$

Alors, pour $x\in\Omega'$, avec $c_i = f_i(x)$ on a

$$\left(\sum_{i=1}^n f_i(x)^2\right)^2 \leq M^2 \sum_{i=1}^n f_i(x)^2$$

d'où $\sum_{i=1}^n f_i(x)^2 \leq M^2$. Alors, en intégrant,

$$n = \int_{\Omega'} \sum_{i=1}^n f_i(x)^2 \mathrm{d}\mu(x) \leq M^2.$$

– *Conclusion :* Comme de toute famille libre de $S$, par Gram-Schmidt, on peut construire une famille orthonormée de même cardinal, toute famille libre de $S$ a un cardinal $\leq M^2$. Ainsi, $\dim S \leq M^2$. □

# 41 Théorème de Hadamard-Lévy

H. Queffélec, C. Zuily, *Analyse pour l'agrégation*, 4e édition, Dunod. Théorème V.3 page 399.

Recasage : 204, 214, 215, 220.

**Théorème 41.1**

*Soit $f \in \mathcal{C}^2(\mathbb{R}^n, \mathbb{R}^n)$. Les assertions suivantes sont équivalentes :*
*(i) $f$ réalise un difféomorphisme de $\mathbb{R}^n$ sur $\mathbb{R}^n$.*
*(ii) $f$ est propre et $\forall x \in \mathbb{R}^n$, $\det(df(x)) \neq 0$.*

**Rappel :** Une application $f : \mathbb{R}^n \to \mathbb{R}^n$ est dite propre si l'image réciproque de tout compact par $f$ est un compact.

▷ $(i) \Rightarrow (ii)$ : Ok.

$(ii) \Rightarrow (i)$ : Quitte à considérer $\widetilde{f} = f - f(0)$, on peut supposer $f(0) = 0$.

⋆ Il suffit de montrer qu'il existe une application $g : \mathbb{R}^n \to \mathbb{R}^n$ telle que :
— $f \circ g = \mathrm{Id}_{\mathbb{R}^n}$,
— $g$ est surjective.

En effet, sous ces conditions, si $x, x' \in \mathbb{R}^n$ vérifient $f(x) = f(x')$, alors il existe $y, y' \in \mathbb{R}^n$ tels que $g(y) = x$ et $g(y') = y'$ d'où $y = f(g(y)) = f(x) = f(x') = f(g(y')) = y'$ et donc $x = x'$, ce qui prouve l'injectivité de $f$. De plus, la condition $f \circ g = \mathrm{Id}_{\mathbb{R}^n}$ entraîne immédiatement que $f$ est surjective. Ainsi, $f$ est bijective. Comme $\det(f(x)) \neq 0$ pour tout $x \in \mathbb{R}^n$, d'après le théorème d'inversion locale, $f$ réalise un $\mathcal{C}^2$-difféomorphisme local. En particulier, $f^{-1}$ est $\mathcal{C}^2$ sur $\mathbb{R}^n$.

⋆ On va construire une fonction régulière $x : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ telle que

$$\forall (t, y) \in \mathbb{R} \times \mathbb{R}^n, \qquad f(x(t, y)) = ty$$

et on posera $g : y \in \mathbb{R}^n \mapsto x(1, y)$. Pour $y \in \mathbb{R}^n$, considérons le problème suivant :

$$\left\{ \begin{array}{l} \dot{x}(t) = [\mathrm{d}f(x(t))]^{-1} y \quad \forall t \in \mathbb{R} \\ x(0) = 0. \end{array} \right. \tag{$\mathscr{S}$}$$

Comme $f$ est de classe $\mathcal{C}^2$, l'application $F : x \mapsto [\mathrm{d}f(x)]^{-1} y$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}^n$ donc, d'après le théorème de Cauchy-Lipschitz, $(\mathscr{S})$ admet une solution maximale $x(t, y)$ définie sur un intervalle $I = ]-T^*, T^*[$, $T^* > 0$. Sur $I$, on a

$$\frac{\mathrm{d}}{\mathrm{d}t}(f(x(t, y))) = \mathrm{d}f(x(t, y))\dot{x}(t, y) = y$$

donc, comme $f(x(0, y)) = f(0) = 0$, $\forall t \in I$, $f(x(t, y)) = ty$.

⋆ Supposons par l'absurde que $T^* < +\infty$. Pour tout $t \in I$, on a $\|f(x(t, y))\| \leq T^* \|y\|$ donc $x(t, y) \in f^{-1}(\overline{B(0, T^* \|y\|)})$ qui est un compact (par hypothèse), ce qui contredit le théorème de sortie de tout compact. Ainsi, $T^* = +\infty$. En particulier, $x(t, y)$ existe sur $[0, 1]$ et pour $t \in [0, 1]$, $x(t, y) \in f^{-1}(\overline{B(0, \|y\|)})$.

⋆ On peut donc définir une application $g : y \in \mathbb{R}^n \mapsto x(1, y)$. D'après les calculs précédents, pour tout $y \in \mathbb{R}^n$, $f(g(y)) = f(x(1, y)) = y$ donc $f \circ g = \mathrm{Id}_{\mathbb{R}^n}$.

⋆ Pour démontrer la surjectivité de $g$, on fera usage de sa continuité. Démontrons-là. Soit $y_0 \in \mathbb{R}^n$. Pour $\|y - y_0\| \leq 1$, on a $\|y\| \leq \|y_0\| + 1$. On définit le compact $K_0 = f^{-1}(\overline{B(0, 1 + \|y_0\|)})$ et on considère une boule fermée $B_0$ centrée en 0 et contenant $K_0$. Pour tout $t \in \mathbb{R}$, d'après ce qui précède, $x(t, y_0), x(t, y) \in K_0$ donc $\lambda x(t, y_0) + (1 - \lambda)x(t, y) \in B_0$ pour tout $\lambda \in [0, 1]$. De plus, pour $t \in \mathbb{R}$,

$$\dot{x}(t, y_0) - \dot{x}(t, y) = [\mathrm{d}f(x(t, y_0))]^{-1} y_0 - [\mathrm{d}f(x(t, y))]^{-1} y.$$

Alors,

$$x(t,y_0)-x(t,y) = \int_0^t \left([\mathrm{d}f(x(s,y_0))]^{-1}y_0-[\mathrm{d}f(x(s,y))]^{-1}y\right)\mathrm{d}s$$

$$= \underbrace{\int_0^t [\mathrm{d}f(x(s,y_0))]^{-1}(y_0-y)\mathrm{d}s}_{A} + \underbrace{\int_0^t \left\{[\mathrm{d}f(x(s,y_0))]^{-1}-[\mathrm{d}f(x(s,y))]^{-1}\right\}y\mathrm{d}s}_{B}.$$

On a, pour $t\in[0,1]$ :

$$\|A\| \leq \sup_{z\in B_0}\left\|[\mathrm{d}f(z)]^{-1}\right\|\|y-y_0\| \leq M\|y-y_0\|$$

et

$$\|B\| = \left|\int_0^t\left(\int_0^1 \mathrm{d}F\left(\lambda x(s,y_0)+(1-\lambda)x(s,y)\right).(x(s,y_0)-x(s,y))\mathrm{d}\lambda\right)\mathrm{d}s\right|$$

$$\leq \int_0^t \sup_{z\in B_0}\|\mathrm{d}F(z)\|\,\|x(s,y_0)-x(s,y)\|\,\mathrm{d}s$$

$$\leq C\int_0^t \|x(s,y_0)-x(s,y)\|\,\mathrm{d}s.$$

On a donc, pour tout $t\in\mathbb{R}$,

$$\|x(t,y_0)-x(t,y)\| \leq M\|y-y_0\| + C\int_0^t \|x(s,y_0)-x(s,y)\|\,\mathrm{d}s.$$

D'après le lemme de Gronwall, on en déduit que

$$\|g(y)-g(y_0)\| \leq M\|y-y_0\|\,e^C$$

donc $g$ est continue.

$\star$ Pour montrer que $g$ est surjective, comme $\mathbb{R}^n$ est connexe, il suffit de montrer que $g(\mathbb{R}^n)$ est ouvert et fermé.

$-$ $g(\mathbb{R}^n)$ est fermé. Soit $(y_k=g(x_k))$ une suite de $g(\mathbb{R}^n)$ qui converge vers $y\in\mathbb{R}^n$. Alors $f(y_k)=x_k$ donc, comme $f$ est continue, $x_k\to f(y)$. Alors, comme $g$ est continue, $g(x_k)\to g(f(y))$. Or $g(x_k)\to y$ donc $y=g(f(y))\in g(\mathbb{R}^n)$.

$-$ $g(\mathbb{R}^n)$ est ouvert. Soit $y_0=g(x_0)\in g(\mathbb{R}^n)$. Alors $f(y_0)=x_0$ donc, d'après le théorème d'inversion locale, comme $\mathrm{d}f(y_0)$ est inversible, il existe des voisinages ouverts $U_{y_0}\in\mathcal{V}(y_0)$ et $V_{x_0}\in\mathcal{V}(x_0)$ tels que $f$ réalise un $\mathcal{C}^1$-difféomorphisme de $U_{y_0}$ sur $V_{x_0}$. Comme $g$ est continue et $g(x_0)=y_0$, il existe un voisinage ouvert $W_{x_0}\subset V_{x_0}$ contenant $x_0$ tel que $g(W_{x_0})\subset U_{y_0}$. Soit $x\in W_{x_0}$. On a $f^{-1}(x)\in U_{y_0}$ et $g(x)\in U_{y_0}$ et $f(f^{-1}(x))=x=f(g(x))$ d'où, par injectivité de $f$ sur $U_{x_0}$, $f^{-1}(x)=g(x)$ donc $f^{-1}(W_{x_0})\subset g(\mathbb{R}^n)$. Comme $f$ est continue, $f^{-1}(W_{x_0})$ est un ouvert contenant $y_0$ inclus dans $g(\mathbb{R}^n)$.

□

# 42 Théorème de Lax-Milgram

I. Nourdin, *Agrégation de mathématique épreuve orale*, 2e édition, Dunod. Théorème 1.13.1 page 50 pour le théorème
H. Brézis, *Analyse fonctionnelle*, Dunod. Exemple 2 page 138 pour l'application.

Recasage : 201, 205, 213, 222, 234.

**Théorème 42.1**

*Soient $(H, \langle .,. \rangle, \|.\|)$ un espace de Hilbert, $a$ une forme bilinéaire continue coercive sur $H \times H$ :*

$$\exists \alpha, C > 0, \qquad |a(u,v)| \leq C \|u\| \|v\| \qquad a(u,u) \geq \alpha \|u\|^2 \qquad \forall u, v \in H,$$

*et $\ell$ une forme linéaire continue sur $H$. Il existe un unique $u \in H$ tel que*

$$\forall v \in H, \qquad a(u,v) = \ell(v).$$

*Si de plus $a$ est symétrique, alors $u$ est l'unique minimum de $J : v \in H \mapsto \dfrac{1}{2} a(v,v) - \ell(v)$.*

▷ – $\ell$ est une forme linéaire continue sur $H$ donc d'après le théorème de représentation de Riesz, il existe un unique $f \in H$ tel que $\forall v \in H$, $\ell(v) = \langle f, v \rangle$.

– De même, par continuité de $a$, pour $u \in H$, l'application $v \mapsto a(u,v)$ est une forme linéaire continue sur $H$. Il existe donc un unique $a_u \in H$ tel que $\forall v \in H$, $a(u,v) = \langle a_u, v \rangle$. Posons $A : u \in H \mapsto a_u \in H$. Il faut donc montrer :

$$\exists ! u \in H, \qquad Au = f.$$

Il suffit donc de montrer que $A : H \to H$ est bijective.

– Pour $u, v \in H$ et $\lambda \in \mathbb{R}$ on a

$$\forall w \in H, \qquad \langle A(u + \lambda v), w \rangle = a(u + \lambda v, w) = a(u,w) + \lambda a(v,w) = \langle Au + \lambda Av, w \rangle$$

donc $A(u + \lambda v) = Au + \lambda Av$ et $A$ est linéaire. De plus,

$$\forall u \in H, \qquad \|Au\|^2 = \langle Au, Au \rangle = a(u, Au) \leq C \|u\| \|Au\|$$

donc $A$ est continue.

– De la coercivité de $a$, on déduit que $\forall u \in H$, $\langle Au, u \rangle = a(u,u) \geq \alpha \|u\|^2$ d'où $\operatorname{Ker} A = \{0\}$. On en déduit également que $\operatorname{Im} A$ est fermée. En effet, si $(v_n = Au_n) \in (\operatorname{Im} A)^{\mathbb{N}}$ converge vers $v \in H$, on a :

$$\alpha \|u_p - u_q\|^2 \leq a(u_p - u_q) = \langle A(u_p - u_q), u_p - u_q \rangle \leq \|v_p - v_q\| \|u_p - u_q\|$$

d'où $\alpha \|u_p - u_q\| \leq \|v_p - v_q\| \xrightarrow[p,q \to +\infty]{} 0$ et la suite $(u_n)$ est de Cauchy dans $H$. Elle converge donc vers $u \in H$. Alors, par continuité de $A$, on a $Au = \lim Au_n = v \in \operatorname{Im} A$.

– Pour montrer la surjectivité, il suffit donc de vérifier que $(\operatorname{Im} A)^\perp = \{0\}$. Soit $v \in (\operatorname{Im} A)^\perp$. Alors

$$0 = \langle Av, v \rangle = a(v,v) \geq \alpha \|v\|^2$$

donc $v = 0$.

– On a donc montré que $A$ est bijective. En particulier, il existe un unique $u \in H$ tel que $\forall v \in H$, $a(u,v) = \ell(v)$.

– On suppose désormais que $a$ est symétrique. Alors, pour $v \in H$,

$$J(u+v) = J(u) + a(u,v) - \ell(v) + \frac{1}{2} a(v,v) = J(u) + \frac{1}{2} a(v,v) \geq J(u) + \frac{\alpha}{2} \|v\|^2$$

donc $\forall v \in H, v \neq u$, $J(v) > J(u)$ donc $u$ est l'unique minimum de $J$ sur $H$. □

**Application au problème de Sturm-Liouville** On considère le problème

$$\begin{cases} -(pu')' + qu = f \quad \text{sur } ]0,1[ \\ u(0) = u(1) = 0 \end{cases}$$

où $p \in \mathcal{C}^1([0,1]), q \in \mathcal{C}([0,1])$ et $f \in L^2(0,1)$ sont donnés avec $p(x) \geq \alpha > 0 \ \forall x \in [0,1]$ et $q \geq 0$.

La formulation variationnelle associée à ce problème est :

$$\forall v \in H_0^1(0,1), \qquad \int_0^1 pu'v' + \int_0^1 quv = \int_0^1 fv.$$

On se place donc dans le cadre $H = H_0^1(0,1)$ muni de $\|.\|_{H^1(0,1)}$.

$$\forall u, v \in H_0^1(0,1), \qquad a(u,v) = \int_0^1 pu'v' + \int_0^1 quv,$$

$$\forall v \in H_0^1(0,1), \qquad \ell(v) = \int_0^1 fv.$$

Pour $u, v \in H_0^1(0,1)$, on a, d'après l'inégalité de Cauchy-Schwarz dans $L^2(0,1)$,

$$|\ell(v)| \leq \int_0^1 |fv| \leq \|f\|_{L^2(0,1)} \|v\|_{L^2(0,1)}$$

et

$$|a(u,v)| \leq \|p\|_\infty \|u'\|_{L^2(0,1)} \|v'\|_{L^2(0,1)} + \|q\|_\infty \|u\|_{L^2(0,1)} \|v\|_{L^2(0,1)} \leq C \|u\|_{H_0^1(0,1)} \|v\|_{H^1(0,1)}$$

donc $a$ et $\ell$ sont continues sur $H_0^1(0,1)$. De plus, pour $u \in H_0^1(0,1)$,

$$a(u,u) = \int_0^1 pu'^2 + \int_0^1 qu^2 \geq \alpha \|u'\|_{L^2(0,1)} \geq C \|u\|_{H^1(0,1)}$$

avec $C > 0$ d'après l'inégalité de Poincaré, donc $a$ est coercive. D'après le théorème de Lax-Milgram, il existe un unique $u \in H_0^1(0,1)$ tel que $a(u,v) = \ell(v)$, $\forall v \in H_0^1(0,1)$.

**Remarque :** On en déduit, par définition, que $pu' \in H^1(0,1)$ donc $u' = \dfrac{1}{p} pu' \in H^1(0,1)$ et donc $u \in H^2(0,1)$. Comme $pu' \in H^1(0,1)$, par intégration par parties,

$$\int_0^1 pu'v' = [pu'v]_0^1 - \int_0^1 (pu')'v = -\int_0^1 (pu')'v$$

donc

$$\forall v \in H_0^1(0,1), \qquad \int_0^1 (-(pu')' + qu - f)v = 0.$$

En particulier,

$$\forall \varphi \in \mathcal{D}(]0,1[), \qquad \int_0^1 \underbrace{(-(pu')' + qu - f)}_{\in L^2(0,1)} v = 0$$

donc, par densité de $\mathcal{D}(]0,1[)$ dans $L^2$,

$$-(pu')' + qu = f \qquad \text{p.p.}$$

Si de plus $f \in \mathcal{C}([0,1])$, alors comme $q, u \in \mathcal{C}([0,1])$, on a $pu' \in \mathcal{C}^1([0,1])$ donc $u' = \dfrac{1}{p} pu' \in \mathcal{C}^1([0,1])$ donc $u \in \mathcal{C}^2([0,1])$ et l'égalité presque partout est vrai partout.

On a donc montré qu'il existe une unique solution faible du problème, donc une unique solution forte. De plus, cette solution faible est en fait solution forte.

# 43 Théorème de stabilité en première approximation

F. Rouvière, *Petit guide de calcul différentiel*, 4e édition, Cassini. Exercice 46 page 138.

Recasage : 220, 221.

**Théorème 43.1**

*On considère le système différentiel*

$$(\mathcal{S}) \quad \begin{cases} y' = f(y) \\ y(0) = y_0 \end{cases}$$

*où $y_0 \in \mathbb{R}^n$ et $f : \mathbb{R}^n \to \mathbb{R}$ est de classe $\mathcal{C}^1$ et vérifie $f(0) = 0$. Si $Df(0)$ a toutes ses valeurs propres de partie réelle strictement négative, alors 0 est un équilibre asymptotiquement stable de $(\mathcal{S})$.*

▷ Notons $A = Df(0)$.

– *Étape 1. Montrons que 0 est un équilibre asymptotiquement stable du système linéarisé :*

$$(\mathcal{L}) \qquad \begin{cases} z' = Az \\ z(0) = y_0 \end{cases}$$

La solution de cette équation différentielle est donnée par $\forall t \in \mathbb{R}$, $z(t) = e^{tA}y_0$.

D'après le lemme des noyaux, en notant $\lambda_1, \dots, \lambda_k$ les valeurs propres distinctes de $A$ et $m_1, \dots, m_k$ leurs multiplicités respectives, on a :

$$\mathbb{C}^n = \bigoplus_{i=1}^{k} \underbrace{\mathrm{Ker}(A - \lambda_i I_n)^{m_i}}_{E_i}.$$

Écrivons la donnée initiale $y_0$ dans cette décomposition : $y_0 = y_1 + \cdots + y_k$. Soit $i \in [\![1, k]\!]$. On a :

$$e^{tA}y_i = e^{t\lambda_i}e^{t(A-\lambda_i I_n)}y_i = e^{t\lambda_i} \sum_{i=0}^{m_i-1} \frac{t^p}{p!}(A - \lambda_i I_n)^p y_i.$$

Alors, pour $\|.\|$ une norme quelconque sur $\mathbb{C}^n$ :

$$\left\|e^{tA}y_i\right\| \leq e^{t\mathrm{Re}\lambda_i} C_i (1 + |t|^{m_i-1}) \left\|y_i\right\| \leq C_i e^{t\mathrm{Re}\lambda_i}(1 + |t|^{n-1}) \left\|y_i\right\|.$$

On en déduit que

$$\left\|e^{tA}y_0\right\| \leq \sum_{i=1}^{k} \left\|e^{tA}y_i\right\| \leq C(1 + |t|^{n-1}) \left(\max_{i=1}^{k} \|y_i\|\right) \exp\left(t \sum_{i=1}^{k} \mathrm{Re}\lambda_i\right).$$

Notons $a > 0$ un réel tel que $\forall i \in [\![1, k]\!]$, $\mathrm{Re}\lambda_i \leq -a < 0$. Alors, pour une constante $C > 0$, par équivalence des normes et puisque $(1 + |t|)^n e^{at} e^{t\mathrm{Re}\lambda_i}$ bornée, on a

$$\|z(t)\| = \left\|e^{tA}y_0\right\| \leq Ce^{-at} \|y_0\|$$

et 0 est un point d'équilibre asymptotiquement stable.

– *Étape 2. Cherchons une fonction de Lyapunov pour le système linéarisé.* Pour $x_1, x_2 \in \mathbb{R}^n$, d'après l'inégalité de Cauchy-Schwarz et ce qui précède,

$$|\langle e^{tA}x_1, e^{tA}x_2\rangle| \leq \left\|e^{tA}x_1\right\| \left\|e^{tA}x_2\right\| \leq C^2 e^{-2ta} \|x_1\| \|x_2\|.$$

Ainsi, l'application

$$b : \begin{array}{ccc} \mathbb{R}^n \times \mathbb{R}^n & \to & \mathbb{R} \\ (x_1, x_2) & \mapsto & \displaystyle\int_0^{+\infty} \langle e^{tA}x_1, e^{tA}x_2\rangle \mathrm{d}t \end{array}$$

est bien définie, et est une forme bilinéaire symétrique sur $\mathbb{R}^n$. Notons $q$ la forme quadratique associée. Pour $x \in \mathbb{R}^n$,

$$q(x) = \int_0^{+\infty} \left\|e^{tA}x\right\|^2 \mathrm{d}t \geq 0$$

et $q(x) = 0$ si et seulement si, par continuité de la fonction $t \mapsto \left\|e^{tA}x\right\|^2$, $\forall t \geq 0$, $\left\|e^{tA}x\right\| = 0$ *ie.* $x = 0$. $q$ est donc définie positive.

Pour $x_1, x_2 \in \mathbb{R}^n$ et $t \in \mathbb{R}$, $q(x_1 + tx_2) = q(x_1) + 2tb(x_1, x_2) + t^2 q(x_2)$ donc, comme $q$ est différentiable sur $\mathbb{R}^n$, pour $x_1, x_2 \in \mathbb{R}^n$, $\mathrm{d}q(x_1).x_2 = 2b(x_1, x_2)$. On a alors

$$\forall x \in \mathbb{R}^n, \quad \langle \nabla q(x), Ax \rangle = 2b(x, Ax) = \int_0^\infty \underbrace{2\langle e^{tA}x, e^{tA}Ax \rangle}_{\frac{\mathrm{d}}{\mathrm{d}t}\|e^{tA}x\|^2} \mathrm{d}t = \left[ \left\| e^{tA}x \right\|^2 \right]_0^\infty = - \|x\|^2$$

par hypothèse sur $A$. En particulier, $q$ est une fonction de Lyapunov stricte pour $A$.

– *Étape 3. Application au problème non-linéaire.* Comme $f$ est de classe $\mathcal{C}^1$, le problème $(\mathcal{S})$ admet une unique solution maximale $y$ définie sur $I = ]T^-, T^+[$, $T^- < 0 < T^+$. On pose $r(y) = f(y) - Ay$. Sur $I$, on a :

$$q(y)' = \mathrm{d}q(y).y' = 2b(y, y') = 2b(y, Ay) + 2b(y, r(y)) = - \|y\|^2 + 2b(y, r(y)).$$

Or, $b$ étant symétrique définie positive, par l'inégalité de Cauchy-Schwarz,

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

Soit $\varepsilon > 0$. Comme $r(y) = f(y) - f(0) - \mathrm{d}f(0)y$ et $f$ est $\mathcal{C}^1$, par équivalence des normes sur $\mathbb{R}^n$, il existe $\alpha > 0$ tel que si $q(y) \leq \alpha$, $\sqrt{q(r(y))} \leq \varepsilon\sqrt{q(y)}$. Alors, pour $q(y) \leq \alpha$, $b(y, r(y)) \leq 2\varepsilon q(y)$. Or, par équivalence des normes, $Cq(y) \leq \|y\|^2$, donc

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

Ainsi, pour $0 < \varepsilon < C/2$, on a :

$$\forall t \in I, \qquad q(y(t)) \leq \alpha \quad \Rightarrow \quad q(y)'(t) \leq -\beta q(y(t)) \tag{$*$}$$

avec $\beta > 0$.

– *Conclusion.* Supposons par l'absurde qu'il existe $t \in I$ tel que $q(y(t)) > \alpha$. Soit alors $t_0 = \min\{t \in I \cap \mathbb{R}_+,\ q(y(t)) = \alpha\}$. On a $q(y(t_0)) = \alpha$ donc d'après $(*)$, $q(y)'(t_0) \leq -\beta q(y(t_0)) < 0$. On en déduit qu'il existe $\delta > 0$ tel que

$$\forall t \in ]t_0, -\delta, t_0[, \qquad q(y(t)) > q(y(t_0)) = \alpha$$

ce qui contredit la définition de $t_0$. Ainsi,

$$\forall t \in I, \qquad q(y(t)) \leq \alpha.$$

D'après le théorème de sortie de tout compact, on en déduit que $T^+ = +\infty$. Alors, d'après $(*)$, pour $t \geq 0$,

$$q(y(t)) \leq q(y_0) - \beta \int_0^t q(y(s))\mathrm{d}s$$

d'où, d'après le lemme de Gronwall,

$$\forall t \geq 0, \qquad q(y(t)) \leq q(y_0)e^{-\beta t}$$

et, en particulier, $y(t) \xrightarrow[t \to +\infty]{} 0$. □

# 44 Théorème de Weierstrass par Bernstein

H. Queffélec, C. Zuily, *Analyse pour l'agrégation*, 4e édition, Dunod. Théorème II.3 page 518 pour le théorème et Exemple IV.1 page 247 pour le lemme.

Recasage : 201, 202, 209, 228, 241, 260, 264.

**Théorème 44.1**

*Soient $f : [0,1] \to \mathbb{C}$ une fonction continue et $\omega$ son module de continuité uniforme :*

$$\forall h \geq 0, \qquad \omega(h) = \sup\{|f(x) - f(y)|,\ |x-y| \leq h\}.$$

*Pour $n \geq 1$, on pose $B_n = \sum_{k=0}^{n} \binom{n}{k} X^k (1-X)^{n-k} f\left(\frac{k}{n}\right)$. Alors*

$$\forall n \geq 1, \qquad \|f - B_n\|_\infty \leq \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right)$$

*et cette estimation est optimale.*

On aura besoin des résultats suivants sur le module de continuité uniforme d'une fonction continue.

**Lemme 44.2**

*$\omega$ est une fonction croissante, sous-additive, telle que*

$$\forall h, \lambda \geq 0, \qquad \omega(\lambda h) \leq (\lambda + 1)\omega(h).$$

▷ – Si $h \leq h'$ alors $\{|f(x) - f(y)|,\ |x-y| \leq h\} \subset \{|f(x) - f(y),\ |x-y| \leq h'\}$ donc $\omega(h) \leq \omega(h')$.
– Si $h, h' \in \mathbb{R}_+$ et $|x-y| \leq h + h'$, soit $z$ tel que $|x-z| \leq h$ et $|z-y| \leq h'$. Alors

$$|f(x) - f(y)| \leq |f(x) - f(z)| + |f(z) - f(y)| \leq \omega(h) + \omega(h')$$

donc $\omega(h + h') \leq \omega(h) + \omega(h')$.
– On en déduit par récurrence que $\forall n \in \mathbb{N}$, $\omega(nh) \leq n\omega(h)$.
– Soit $h, \lambda \geq 0$. Comme $\lfloor \lambda \rfloor \leq \lambda \leq \lfloor \lambda \rfloor + 1$, d'après les points précédents :

$$\omega(\lambda h) \leq \omega((\lfloor \lambda \rfloor + 1)h) \leq (\lfloor \lambda \rfloor + 1)\omega(h) \leq (\lambda + 1)\omega(h).$$

□

On peut désormais démontrer le théorème.

▷ Soit $x \in [0,1]$. Considérons $(X_n)_{n \geq 1}$ une suite de variables aléatoires indépendantes de loi de Bernoulli $b(x)$ et $S_n = \sum_{k=1}^{n} X_k$. On a $\mathbb{E}[S_n] = nx$ et $\mathrm{Var}(S_n) = nx(1-x)$ et

$$\mathbb{E}\left[f\left(\frac{S_n}{n}\right)\right] = \sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^k f\left(\frac{k}{n}\right) = B_n(x).$$

Alors,

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

D'après le lemme, on a donc

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

Or $x = \mathbb{E}\left[\frac{S_n}{n}\right]$ donc $\left\|x - \frac{S_n}{n}\right\|_2 = \mathrm{Var}\left(\frac{S_n}{n}\right) = \sqrt{\frac{x(1-x)}{n}}$ d'où

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

Ainsi, $\|f - B_n\|_\infty \leq \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right)$. □

Exhibons une fonction $f$ telle que $\|f - B_n\|_\infty \geq C\omega\left(\frac{1}{\sqrt{n}}\right)$ avec $C > 0$. Considérons $f : x \in [0,1] \mapsto \left|x - \frac{1}{2}\right|$. D'après la deuxième inégalité triangulaire, $\omega(h) \leq h$. De plus,

$$\|f - B_n\|_\infty \geq \left|B_n\left(\frac{1}{2}\right)\right| = \mathbb{E}\left[\left|\frac{S_n}{n} - \frac{1}{2}\right|\right] = \frac{1}{2n}\mathbb{E}[2S_n - n] = \frac{1}{2n}\mathbb{E}[\varepsilon_1 + \cdots + \varepsilon_n]$$

où pour tout $k$ on a posé $\varepsilon_k = 2X_k - 1$ de sorte que les $(\varepsilon_n)_{n\geq 1}$ sont indépendantes et suivent la loi de Rademacher.

On conclut grâce au lemme suivant.

**Lemme 44.3 (*Khintchine*)**

$\|\varepsilon_1 + \cdots + \varepsilon_n\|_1 \geq \sqrt{\frac{n}{e}}$.

▷ Notons $s = \varepsilon_1 + \cdots + \varepsilon_n$. Soit $g \in L^\infty$. On a $\mathbb{E}[|sg|] \leq \|s\|_1 \|g\|_\infty$ donc si $g \neq 0$, $\|s\|_1 \geq \frac{\mathbb{E}[|sg|]}{\|g\|_\infty} \geq \frac{|\mathbb{E}[sg]|}{\|g\|_\infty}$.

Posons $g = \prod_{j=1}^{n}\left(1 + i\frac{\varepsilon_j}{\sqrt{n}}\right)$. Alors

$$|g(\omega)| = \prod_{j=1}^{n}\sqrt{1 + \frac{\varepsilon_j^2}{n}} = \prod_{j=1}^{n}\sqrt{1 + \frac{1}{n}} \leq \prod_{j=1}^{n}\sqrt{e^{1/n}} = \sqrt{e}$$

car $1 + x \leq e^x, \forall x$. Ainsi, $\|g\|_\infty \leq \sqrt{e}$. De plus,

$$\mathbb{E}[sg] = \sum_{k=1}^{n}\mathbb{E}\left[\varepsilon_k \prod_{j=1}^{n}\left(1 + i\frac{\varepsilon_j}{\sqrt{n}}\right)\right] \underset{\perp\!\!\!\perp}{=} \sum_{k=1}^{n}\mathbb{E}\left[\varepsilon_k\left(1 + i\frac{\varepsilon_k}{\sqrt{n}}\right)\right] = \sum_{k=1}^{n}\frac{i}{\sqrt{n}} = i\sqrt{n}.$$

Ainsi,

$$\|\varepsilon_1 + \cdots + \varepsilon_n\|_1 \geq \sqrt{\frac{n}{e}}.$$

□

# 45 Théorème des extrema liés

Emmanuel Hebey, *Introduction à l'analyse non linéaire sur les variétés*, Diderot Éditeur Arts Sciences. Paragraphe 5.7.3 page 224 pour le théorème.

F. Rouvière, *Petit guide de calcul différentiel*, 4e édition, Cassini. Exercice 129 page 408 pour l'application.

Recasage : 159, 214, 219.

**Théorème 45.1**

*Soient $(E, \|.\|)$ un espace de Banach, $\Omega$ un ouvert de $E$, $f : \Omega \to \mathbb{R}$ une fonction différentiable sur $\Omega$, et $\Phi : \Omega \to \mathbb{R}^n$ de classe $\mathcal{C}^1$ sur $\Omega$ de composantes $\Phi_1, \dots, \Phi_n$. Soit $a \in \mathbb{R}^n$ tel que $\Phi^{-1}(a) \neq \emptyset$. Si $x_0 \in \mathbb{R}^n$ est tel que $f(x_0) = \min_{x \in \Phi^{-1}(a)} f(x)$ et $D\Phi(x_0) \in \mathscr{L}(E, \mathbb{R}^n)$ est surjective, alors il existe $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ tels que*

$$Df(x_0) = \lambda_1 D\Phi_1(x_0) + \cdots + \lambda_n D\Phi_n(x_0).$$

▷ Comme $\dim(E/\operatorname{Ker} D\Phi(x_0)) = \operatorname{rg} D\Phi(x_0) = n$, il existe un sous-espace vectoriel $F$ de dimension $n$ tel que$E = \operatorname{Ker} D\Phi(x_0) \oplus F$. Notons $\chi$ la restriction de $D\Phi(x_0)$ à $F$, de sorte que $\chi$ réalise un isomorphisme de $F$ sur $\mathbb{R}^n$.

– Montrons que $(D\Phi_1(x_0), \dots, D\Phi_n(x_0))$ forme une base de $F^*$. Comme $\dim F^* = \dim F = n$, il suffit de vérifier que la famille est libre. Soient $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ tel que $\lambda_1 D\Phi_1(x_0) + \cdots + \lambda_n D\Phi_n(x_0) = 0$. Comme $\operatorname{Im} D\Phi(x_0) = \mathbb{R}^n$, en notant $(e_1, \dots, e_n)$ la base canonique, il existe $x_1, \dots, x_n \in E$ tels que $D\Phi(x_0)x_i = e_i$, $\forall i$, c'est-à-dire $D\Phi_k(x_0) = \delta_{ki}$ pour tout $k, i$. On obtient donc $\lambda_i = 0$ pour tout $i$.

– Comme $Df(x_0)_{|F} \in F^*$, il existe $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ tels que

$$\forall x \in F, \qquad Df(x_0)x = \lambda_1 D\Phi_1(x_0)x + \cdots + \lambda_n D\Phi_n(x_0)x. \tag{$*$}$$

Il faut maintenant montrer que $\operatorname{Ker} D\Phi(x_0) \subset \operatorname{Ker} Df(x_0)$.

– Pour $x$ dans un voisinage de 0, on pose $\Psi(x) = \Phi(x_0 + x) - a$ de sorte que $\Phi(0) = 0$ et $D\Psi(0) = D\Phi(x_0)$. Notons $\Pi_1$ la projection $E \to \operatorname{Ker} D\Phi(x_0$ et posons $h = \chi^{-1} \circ \psi + \pi_1$ sur un voisinage de 0. $h$ est de classe $\mathcal{C}^1$ et

$$Dh(0) = D(\chi^{-1})(\psi(0)) \circ D\Psi(0) + \Pi_1 = \chi^{-1} \circ D\Phi(x_0) + \Pi_1 = \mathrm{Id}_E.$$

D'après le théorème d'inversion locale, il existe des voisinages $U_1$ et $U_2$ de 0 tels que $h$ réalise un $\mathcal{C}^1$-difféomorphisme de $U_1$ sur $U_2$.

Soit $\Pi_2$ la projection $E \to F$. On a $\Pi_2 \circ h = \chi^{-1} \circ \psi$ donc $\chi \circ \Pi_2 \circ h = \Psi$. De plus, comme $D\Psi(0) = D\Phi(x_0) = \chi \circ \Pi_2$, on a $D\Psi(0) \circ h = \Psi$.

– Soit $v \in \operatorname{Ker} D\Phi(x_0)$. Soient $\varepsilon > 0$ et $\gamma_1 : t \in ]-\varepsilon, \varepsilon[ \mapsto tv$. Pour $\varepsilon > 0$ suffisamment petit, $\gamma_1(]-\varepsilon, \varepsilon[) \subset U_2 \cap D\Phi(x_0)$. Posons alors $\gamma_2 = h^{-1} \circ \gamma_1$. On a $\Psi \circ \gamma_2 = D\Psi(0) \circ \gamma_1 = 0$. En posant $\gamma_3 = x_0 + \gamma_2$, on en déduit que $\gamma_3$ est tracé dans $\Phi^{-1}(a)$. On a $\gamma_3(0) = x_0$ et $\gamma_3'(0) = \gamma_2'(0) = Dh^{-1}(0)v = Dh(0)v = v$. Comme $f \circ \gamma_3$ atteint en 0 son minimum sur $]-\varepsilon, \varepsilon[$, $(f \circ \gamma_3)'(0) = 0$ *ie.* $Df(x_0)v = 0$, d'où le résultat.

– $(*)$, $E = \operatorname{Ker} D\phi(x_0) \oplus F$ et $\operatorname{Ker} D\Phi(x_0) \subset Df(x_0)$ permettent de conclure. □

**Proposition 45.2**

*Soit $Q$ une forme quadratique définie positive de matrice dans la base canonique $A$. On note $\mathscr{E} = \{x \in \mathbb{R}^n,\ Q(x) = 1\}$ l'ellipsoïde associé. La fonction $\|.\|^2$ atteint :*

- *son maximum global sur l'ellipsoïde $\dfrac{1}{\lambda_1}$ en les vecteurs $a \in \mathscr{E} \cap E_{\lambda_1}$,*
- *son minimum global sur l'ellipsoïde $\dfrac{1}{\lambda_n}$ en les vecteurs $b \in \mathscr{E} \cap E_{\lambda_n}$,*

*où $0 < \lambda_1 \leq \cdots \leq \lambda_n$ sont les valeurs propres de $A$.*

▷ On a $\forall x, h \in \mathbb{R}^n$, $DQ(x)h = 2\langle h, Ax\rangle$ donc la forme linéaire $DQ(x)$ n'est pas nulle pour $x \in \mathscr{E}$. Comme $f : x \mapsto \|x\|^2$ est de classe $\mathcal{C}^1$, d'après le théorème des extrema liés, si $a \in \mathscr{E}$ réalise un extremum de $f$ sur $\mathscr{E}$ alors il existe $\lambda \in \mathbb{R}$ tel que

$$\forall h \in \mathbb{R}^n, \qquad \langle h, 2a\rangle = \lambda\langle h, 2Aa\rangle$$

*ie.* $a = \lambda Aa$ et, $f(a) = {}^t aa = \lambda Q(a) = \lambda$. Ainsi, $a$ doit être vecteur propre de norme $\dfrac{1}{\sqrt{\lambda}}$ associé à la valeur propre $\dfrac{1}{\lambda}$ de $A$.

Changeons de base orthonormée : on introduit les coordonnées telles que

$$Q(x) = \sum_{k=1}^{n} \lambda_i x_i^2 \qquad \text{et} \qquad f(x) = \sum_{k=0}^{n} x_i^2$$

où $0 < \lambda_1 \leq \cdots \leq \lambda_n$ sont les valeurs propres de $A$. On a :

$$\forall x \in \mathbb{R}^n, \qquad \lambda_1 f(x) \leq Q(x) \leq \lambda_n f(x)$$

donc

$$\forall x \in \mathscr{E}, \qquad \frac{1}{\lambda_n} \leq f(x) \leq \frac{1}{\lambda_1}.$$

Ainsi, le maximum global $\dfrac{1}{\lambda_1}$ est atteint en les $a \in \mathscr{E} \cap E_{\lambda_1}$ et le minimum global en tout $b \in \mathscr{E} \cap E_{\lambda_n}$.

Si $\lambda_j \in ]\lambda_1, \lambda_n[$, et $a \in \mathscr{E} \cap E_{\lambda_j}$, alors $f(a) = \dfrac{1}{\lambda_j}$ n'est pas un extremum global. □

# 46 Théorème des lacunes de Hadamard

H. Queffélec, C. Zuily, *Analyse pour l'agrégation*, 4e édition, Dunod. Théorème IV.2 page 51 et Théorème IV.6 page 55.

Recasage : 203, 207, 241, 243

**Théorème 46.1**

*Soit* $\sum_{n\geq 0} a_n z^n$ *une série entière de rayon de convergence* $R=1$. *Il existe un point singulier* $a \in \mathscr{C}(0,1)$.

▷ À l'oral, on ne fait que le dessin et on explique que c'est la compacité de $\overline{D(0,1)}$ qui fait marcher la chose.

On note $D = D(0,1)$.

Supposons par l'absurde que pour tout $a \in \mathscr{C}(0,1)$, il existe $r_a > 0$ tel que $f$ admet un prolongement analytique sur le disque $D_a = D(a, r_a)$.

Tout le problème est de prouver ce qu'on voit sur le dessin : on en déduit un prolongement sur un $D(0, 1+\delta)$, ce qui contredit $R = 1$.

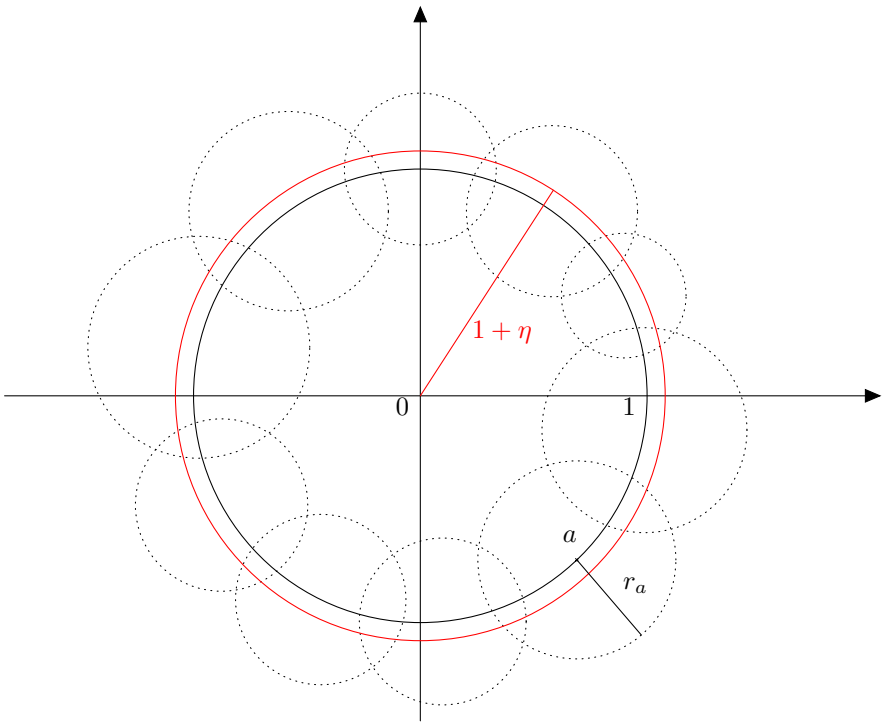



Figure 1 – Situation pour un nombre fini de boules. On pourrait s'y ramener directement grâce à la compacité de $\overline{D}$ mais on utilisera plutôt la compacité plus tard.

– *Étape 1 : Pour* $a \neq b$, *montrons que* $D_a \cap D_b \neq \emptyset \Rightarrow D \cap D_a \cap D_b \neq \emptyset$. Si $D_a \cap D_b \neq \varnothing$ alors $|a-b| < r_a + r_b$. Posons $\lambda = \dfrac{r_b}{r_a + r_b}$ et $w = \lambda a + (1-\lambda)b$. Comme $a$ et $b$ ne sont pas colinéaires, l'inégalité triangulaire est stricte et $|w| < 1$. De plus, $|w - a| = (1-\lambda)|b-a| < r_a$ et de même, $|w-b| < r_b$ donc on a $w \in D \cap D_a \cap D_b$.

– *Étape 2 : Pour* $a \neq b$, *montrons que* $D_a \cap D_b \neq \emptyset \Rightarrow f_a = f_b$ *sur* $D_a \cap D_b$. On a $D_a \cap D_b$ convexe donc connexe. De plus, $f_a = f_b = f$ sur $D_a \cap D_b \cap D \neq \emptyset$. D'après le théorème du prolongement analytique, $f_a = f_b$ sur $D_a \cap D_b$.

– On définit donc sans ambigüité une fonction holomorphe sur $\Omega = \bigcup_{a \in \mathscr{C}(0,1)} (D \cup D_a)$ par $F(z) = f_a(z)$ si $z \in D_a \cup D$.

– *Conclusion :* On peut supposer que $\forall a \in \mathscr{C}(0,1)$, $r_a < 1$ de sorte que $\Omega \subset D(0,2)$. Posons $L = \mathbb{C}\backslash\Omega$. C'est un fermé non vide de $\mathbb{C}$. De plus, $\overline{D} \subset \Omega$ donc $\overline{D}(0,1) \cap L = \emptyset$. Comme $\overline{D}$ est compact, la distance $\delta = d(\overline{D}, L)$ est strictement positive. Donc, pour $0 < \eta < \delta$, on a $D(0, 1+\eta) \subset \Omega$. $F$ est holomorphe sur $D(0,1+\eta)$ donc il existe une série entière

$\sum_{n\geq 0} b_n z^n$ telle que

$$\forall |z| < 1+\eta, \qquad F(z) = \sum_{n=0}^{+\infty} b_n z^n.$$

Comme $F_{|D} = f$, on a, par unicité du développement en série entière, $\forall n \in \mathbb{N}$, $a_n = b_n$ ce qui contredit $R = 1$.

□

**Théorème 46.2 (*Hadamard*)**

*Soit $(\lambda_n)_{n\in\mathbb{N}} \in (\mathbb{N}_*)^{\mathbb{N}}$ telle que $\dfrac{\lambda_{n+1}}{\lambda_n} \geq \alpha > 1$ pour tout $n \in \mathbb{N}$. Soit $\sum_{n\geq 0} a_n z^{\lambda_n}$ une série entière de rayon de convergence 1. Alors tout point de $\mathscr{C}(0,1)$ est singulier. On dit que $\mathscr{C}(0,1)$ est une coupure de $\sum_{n\geq 0} a_n z^{\lambda_n}$.*

▷ Soit un entier $p \geq 1$ tel que $p\lambda_{n+1} > (p+1)\lambda_n$ pour tout $n \in \mathbb{N}$. Supposons par l'absurde que la somme $f$ de la série admette un prolongement analytique $g$ dans $D \cup D(1,\varepsilon)$. On pose $\Omega = D \cup D(1,\varepsilon)$ et $\varphi : z \in \mathbb{C} \mapsto \dfrac{z^p + z^{p+1}}{2}$.

– – Montrons qu'il existe $R > 1$ tel que $\varphi(\overline{D}(0,R)) \subset \Omega$. On a $\varphi(1) = 1 \in \Omega$ et si $z \neq 1$, alors $|z+1| < 2$ donc

$$|\varphi(z)| = \frac{|z|^p}{2}|1+z| < 1.$$

Ainsi, $\varphi(\overline{D}) \subset \Omega$. Or $\varphi$ est continue et $\Omega$ ouvert donc $\varphi^{-1}(\Omega)^c$ est un fermé, qui est non vide. Comme $\overline{D}$ est compact, la distance $\delta = d(\overline{D}, \varphi^{-1}(\Omega)^c)$ est strictement positive. Si $0 < \eta < \delta$, alors $R = 1+\eta$ vérifie $\varphi(\overline{D}(0,R)) \subset \Omega$.

– Alors, $g \circ \varphi$ est holomorphe sur $D(0,R)$. Il existe donc une série entière $\sum_{n\geq 0} b_n z^n$ telle que

$$\forall |z| < R, \qquad g\left(\frac{z^p + z^{p+1}}{2}\right) = \sum_{n=0}^{+\infty} b_n z^n.$$

De plus,

$$\forall |z| < 1, \qquad g\left(\frac{z^p + z^{p+1}}{2}\right) = f\left(\frac{z^p + z^{p+1}}{2}\right) = \sum_{n=0}^{+\infty} a_n \left(\frac{z^p + z^{p+1}}{2}\right)^{\lambda_n} = \sum_{n=0}^{+\infty} a_n P_n(z)$$

où $P_n$ est un polynôme donc les degrés des monômes varient entre $p\lambda_n$ et $(p+1)\lambda_n$. En particulier, il n'y pas de mélange entre les $\left(\dfrac{z^p + z^{p+1}}{2}\right)^{\lambda_n}$ pour différentes valeurs de $n$. Ainsi, pour $N \in \mathbb{N}$,

$$\forall z \in \mathbb{C}, \qquad \sum_{n=0}^{N} a_n \left(\frac{z_p + z^{p+1}}{2}\right)^{\lambda_n} = \sum_{n=0}^{(p+1)N} b_n z^n$$

par unicité du développement en série entière. Fixons $z \in ]1, R[$ et soit $w = \dfrac{z^p + z^{p+1}}{2} > 1$. Par définition de $\sum_{n\geq 0} b_n z^n$, on a :

$$\sum_{n=0}^{N} a_n w^{\lambda_n} \xrightarrow[N\to+\infty]{} g(w)$$

ce qui contredit que 1 est le rayon de convergence de $\sum_{n\geq 0} a_n z^n$. Ainsi, 1 est un point singulier.

– Soit $z_0 \in \mathscr{C}(0,1)$. La série entière $\sum_{n\geq 0} a_n z_0^{\lambda_n} z^{\lambda_n}$ a pour rayon de convergence 1. Donc 1 est singulier pour cette série, donc $z_0$ est singulier pour $\sum_{n\geq 0} a_n z^{\lambda_n}$. □

**Exemple :** $\lambda_n = 2^n$, $a_n = 1$. La série entière $\sum_{n\geq 0} z^{2^n}$ admet le cercle unité comme coupure.

# Troisième partie
# Développements inutilisés

## 47 Automorphismes de $k(X)$

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*, 3e édition, Cassini. Exercice 5.54 page 244

Non utilisé

**Théorème 47.1**

*Soient $k$ un corps et $\mathrm{Aut}_k(k(X))$ le groupe des automorphismes de la $k$-algèbre $k(X)$. Montrons que*

$$\mathrm{Aut}_k(k(X)) = \left\{ F \in k(X) \mapsto F\left(\frac{aX+b}{cX+d}\right),\ (a,b,c,d) \in k^4,\ ad-bc \neq 0 \right\}.$$

▷ • ⋆ Soit $\Phi : k(X) \to k(X)$ un endomorphisme d'algèbres. Notons $F = \Phi(X)$. Pour $P \in k[X]$, avec $P = \sum_{i=0}^{d} p_i X^i$, on a :

$$\Phi(P) = \sum_{i=0}^{d} p_i \Phi(X^i) = \sum_{i=0}^{d} p_i F^i = P \circ F.$$

Soit $G = \dfrac{P}{Q}$ avec $P, Q \in k[X]$. Alors $\Phi(P) = \Phi(QG) = \Phi(Q)\Phi(G)$ donc

$$\Phi(G) = \frac{\Phi(P)}{\Phi(Q)} = \frac{P \circ F}{Q \circ F} = G \circ F.$$

⋆ Réciproquement, pour tout $F \in k(X)$, l'application

$$\Phi_F : \begin{array}{ccc} k(X) & \to & k(X) \\ G & \mapsto & G \circ F \end{array}$$

est bien un morphisme de $k$-algèbres.

• Déterminons une condition nécessaire et suffisante pour que $\Phi_F$ soit un automorphisme.

⋆ Supposons que $\Phi_F$ est un automorphisme. Alors il est surjectif et en particulier il existe $G \in k(X)$ tel que $\Phi(G) = G \circ F = X$. Soient $A, B, P, Q \in k[X]$ tels que $A \wedge B = 1 = P \wedge Q$ et $F = \dfrac{A}{B}$ et $G = \dfrac{P}{Q}$. De tels polynômes existent car $F, G \neq 0$. Notons

$$P = \sum_{i=1}^{d_p} p_i X^i \qquad \text{et} \qquad Q = \sum_{i=1}^{d_q} q_i X^i$$

avec $d_p = \deg(P)$ et $d_q = \deg(Q)$. Alors, l'hypothèse $P \circ F = X \times (Q \circ F)$ se réécrit

$$\sum_{i=0}^{d_p} p_i F^i = X \sum_{i=0}^{d_q} q_i F^i$$

soit, en multipliant par $B^m$, avec $m = \max(d_p, d_q)$,

$$\sum_{i=0}^{d_p} p_i A^i B^{m-i} = X \sum_{i=0}^{d_q} q_i A^i B^{m-i}. \tag{10}$$

⋆ Montrons que $\deg(A) \leq 1$. En effet, d'après l'égalité précédente, $A | (p_0 - q_0 X) B^m$ donc, comme $A \wedge B = 1$, d'après le théorème de Gauss, $A | p_0 - q_0 X$. De plus, $(p_0, q_0) \neq 0$ car sinon $X | P$ et $X | Q$, donc $\deg(A) \leq 1$.

⋆ Montrons que $\deg(B) \leq 1$.

– Si $m = d_p = d_q$, alors, d'après $(*)$, $B|(p_m - q_m X)A^m$ donc, $B|(p_m - q_m X)$. Comme $p_m, q_m \neq 0$, on en déduit le résultat.

– Si $m = d_p > d_q$, alors, d'après $(*)$, $B|p_m Apm$, d'où $B|p_m \neq 0$.

– Si $m = d_q > d_p$, alors, d'après $(*)$, $B|q_m XB^m$, d'où $B|q_m X$.

Dans tous les cas, $\deg(B) \leq 1$.

⋆ Ainsi, il existe $(a, b, c, d) \in k^4$ tel que

$$F = \frac{aX + b}{cX + D}.$$

Comme $\Phi_F$ est surjective, $F$ n'est pas constante donc $ad - bc \neq 0$.

⋆ Réciproquement, pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$, notons

$$\Phi_M : \begin{array}{ccc} k(X) & \to & k(X) \\ G & \mapsto & G\left(\dfrac{aX+b}{cX+d}\right) \end{array}$$

et montrons que $\Phi_M$ est un automorphisme. Pour $M, N \in \mathrm{GL}_2(k)$, on a :

$$\Phi_M \circ \Phi_N = \Phi_{NM}$$

donc $\Phi_M$ est un automorphisme (d'inverse $\Phi_{M^{-1}}$).

• On a montré que

$$\Psi : \begin{array}{ccc} \mathrm{GL}_2(k) & \to & \mathrm{Aut}_k(k(X)) \\ M & \mapsto & \Phi_{M^{-1}} \end{array}$$

est un morphisme de groupes surjectif. Comme $\operatorname{Ker}\Psi = k^\times I_2$, d'après le théorème d'isomorphisme,

$$\mathrm{Aut}_k(k(X)) \simeq \mathrm{GL}_2(k)/_{k^\times I_2} = \mathrm{PGL}_2(k)$$

donc les automorphismes de $k(X)$ sont les homographies. □

# 48 Partitions d'un entier en parts fixées

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Analyse 2*, 2e édition, Cassini. Exercice 3.15 page 197.

Inutilisé.

Soient $a_1, \dots, a_k \in \mathbb{N}^*$ des entiers premiers entre eux. Pour $n \geq 1$, on pose

$$u_n = \#\{(x_1, \dots, x_k) \in \mathbb{N}^k,\ a_1x_1 + \cdots + a_kx_k = n\}.$$

Montrons que l'on a l'équivalent suivant :

$$u_n \underset{n\to+\infty}{\sim} \frac{1}{a_1 \cdots a_k} \frac{n^{k-1}}{(k-1)!}.$$

– Considérons la série génératrice :

$$f(X) = \sum_{n=0}^{\infty} u_n X^n = \sum_{n=0}^{\infty} \left( \sum_{\substack{(x_1,\dots,x_k)\in\mathbb{N} \\ a_1x_1+\cdots+a_kx_k=n}} 1 \right) X^n.$$

On peut la réécrire comme un produit de Cauchy :

$$f(X) = \prod_{i=1}^{k} \left( \sum_{n=0}^{\infty} X^{a_i n} \right) = \prod_{i=1}^{k} \frac{1}{1 - X^{a_i}}.$$

– $f$ est donc une fraction rationnelle, dont on va effectuer la décomposition en éléments simples.

⋆ Les pôles de $f$ sont les racines $a_i$-ièmes de l'unité, pour $1 \leq i \leq k$. Ils sont d'ordre $\leq k$ car $(1 - X^{a_i})$ est à racines simples. En effet, $(1 - X^{a_i})' = a_i X^{a_i - 1}$ n'admet pour racine que 0 puisque $a_i \in \mathbb{N}^*$.

⋆ 1 est un pôle d'ordre $k$. Montrons que c'est le seul. Soit $\omega$ un pôle d'ordre $k$, c'est-à-dire $\omega^{a_i} = 1$ pour tout $1 \leq i \leq k$. Comme $a_1, \dots, a_k$ sont premiers entre eux, d'après le théorème de Bézout, il existe $v_1, \dots, v_k \in \mathbb{Z}$ tels que

$$a_1v_1 + \cdots + a_kv_k = 1.$$

Alors,

$$\omega = \omega^{a_1v_1+\cdots+a_kv_k} = \prod_{i=1}^{k} (\omega^{a_i})^{v_i} = 1.$$

⋆ Notons $\mathcal{P} = \{\omega_1, \omega_2, \dots, \omega_p\}$ les pôles de $f$, avec $\omega_1 = 1$. D'après le théorème de décomposition en éléments simples, il existe $\alpha \in \mathbb{C}$ et $c_{ij} \in \mathbb{C}$ pour tout $1 \leq i \leq k$ et $1 \leq j \leq k-1$ tels que

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

– Effectuons le développement en série formelle des termes $\dfrac{1}{(\omega_i - X)^j}$, pour $1 \leq i \leq k$ et $1 \leq j \leq k$. On l'obtient par dérivation du développement :

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

En effet,

$$\begin{aligned}
\frac{1}{(\omega - X)^j} &= \frac{1}{(j-1)!} \frac{\mathrm{d}^{j-1}}{\mathrm{d}X^{j-1}} \left( \frac{1}{\omega - X} \right) \\
&= \frac{1}{(j-1)!} \sum_{n=0}^{\infty} n(n-1)\cdots(n-j+2) \frac{X^{n-j+1}}{\omega^{n+1}} \\
&= \sum_{n=0}^{\infty} \frac{(n+j-1)\cdots(n+1)}{(j-1)!} \frac{X^n}{\omega^{n+j}} = \sum_{n=0}^{\infty} \binom{n+j-1}{n} \frac{X^n}{\omega^{n+j}}.
\end{aligned}$$

– On obtient donc un nouveau développement en séries formelles pour $f$ :

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

Par unicité du développement en série formelle de $f$, on en déduit :

$$\forall n \in \mathbb{N}, \qquad u_n = \alpha \binom{n+k-1}{n} + \sum_{\substack{1\leq i\leq k\\ 1\leq j\leq k-1}} \binom{n-j+1}{n} \frac{c_{ij}}{\omega_i^{n+j}}.$$

– Comparons les différents termes en présence. Pour $r \in \mathbb{N}^*$, on a

$$\binom{n-r+1}{n} = \frac{(n-r+1)\cdots(n+1)}{(r-1)!} \underset{n\to+\infty}{\sim} \frac{n^{r-1}}{(r-1)!}$$

donc, comme $|\omega| = 1$,

$$\forall 1 \leq i \leq k, \forall 1 \leq j \leq k-1, \qquad \binom{n-j+1}{n} \frac{c_{ij}}{\omega^{n+j}} = \underset{n\to+\infty}{o}\left(n^{k-1}\right).$$

Ainsi,

$$u_n = \alpha \frac{n^{k-1}}{(k-1)!} + \underset{n\to+\infty}{o}(n^{k-1}).$$

– Conclusion : calcul de $\alpha$. On a

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

donc évaluant en 1 la fonction rationnelle associée, on obtient

$$\alpha = \frac{1}{a_1 \cdots a_k}$$

d'où le résultat.

# 49 Théorème de Burnside

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 2*, 2e édition, Cassini. Exercice 3.8 page 185.

Inutilisé.

**Théorème 49.1**

*Soit $G$ un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$. On suppose que $G$ est d'exposant fini : il existe $N \in \mathbb{N}$, $\forall A \in G$, $A^N = I_n$. Alors $G$ est fini et $|G| \leq N^{n^3}$.*

▷ On va construire une injection $f$ telle que $f(G)$ est finie.

– *Étape 1 : Construction d'une injection $f : G \to \mathbb{C}^m$.* Soit $(M_1, \dots, M_m) \in G^m$ une base de $\mathrm{Vect}(G)$. On définit :

$$f : \begin{array}{ccc} G & \to & \mathbb{C}^m \\ A & \mapsto & (\mathrm{Tr}(AM_i))_{1\leq i\leq m} \end{array}$$

Supposons que $f(A) = f(B)$ pour $A, B \in G$. Alors, par linéarité de la trace,

$$\forall M \in \mathrm{Vect}(G), \qquad \mathrm{Tr}(AM) = \mathrm{Tr}(BM).$$

En particulier, avec $D = AB^{-1}$, on a :

$$\forall k \in \mathbb{N}^*, \qquad \mathrm{Tr}(D^k) = \mathrm{Tr}(A \underbrace{B^{-1}D^{k-1}}_{\in G \subset \mathrm{Vect}(G)}) = \mathrm{Tr}(BB^{-1}D^{k-1}) = \mathrm{Tr}(D^{k-1})$$

donc $\forall k \in \mathbb{N}$, $\mathrm{Tr}(D^k) = \mathrm{Tr}(I_n) = n$. Montrons que $D - I_n$ est nilpotente. Alors, pour $k \in \mathbb{N}^*$,

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

Il en découle que $D - I_n$ est nilpotente.

Or, $X^N - 1$ est scindé à racines simples et annule les matrices de $G$. On en déduit que les matrices de $G$ sont diagonalisables. En particulier, $D$ est diagonalisable et $D - I_n = 0$ *ie.* $A = B$.

– *Étape 2 : $f(G)$ est fini.* Par définition de $f$, on a $f(G) \subset T^m$ où

$$T = \{\mathrm{Tr}\, A,\ A \in G\} = \left\{ \sum_{\lambda \in \mathrm{Sp}(A)} \lambda,\ A \in G \right\}.$$

Or, pour tout $A \in G$, $\mathrm{Sp}(A) \subset \{\lambda_1, \dots, \lambda_N\}$ où

$$X^N - 1 = \prod_{i=1}^{N} (X - \lambda_i).$$

Donc $T \subset \{\lambda_{i_1} + \cdots + \lambda_{i_n},\ (i_1, \dots, i_n) \in [\![1, N]\!]^n\}$. Comme, de plus, $m \leq n^2$, on en déduit que

$$|G| = |f(G)| \leq |T|^m \leq (N^n)^{n^2} = N^{n^3}.$$

□

On a utilisé le résultat suivant.

**Lemme 49.2**

*Soit $A \in \mathcal{M}_n(\mathbb{C})$. Si $\forall k \in \mathbb{N}^*$, $\mathrm{Tr}(A^k) = 0$, alors $A$ est nilpotente.*

▷ Supposons par l'absurde que $A^n \neq 0$. Soit alors $\lambda_1, \dots, \lambda_r$ les valeurs propres distinctes non nulles de $A$. Notons $n_1, \dots, n_r$ les multiplicités respectives. Comme $A$ est trigonalisable, on a

$$\forall k \in \mathbb{N}^*, \qquad 0 = \mathrm{Tr}(A^k) = n_1\lambda_1^k + \cdots + n_r\lambda_r^k.$$

En particulier,

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

Comme $\lambda_i \neq 0$ et $\lambda_i \neq \lambda_j$, on a $\det(M) \neq 0$ donc $n_1 = \cdots = n_r = 0$ : absurde. □

# 50 Théorème de Lie-Kolchin

A. Chambert-Loir, *Algèbre corporelle*, version pdf sur la page personnelle de l'auteur, page 98.

Inutilisé.

**Théorème 50.1 (*Lie-Kolchin*)**

*Tout sous-groupe connexe résoluble $G$ de $\mathrm{GL}_n(\mathbb{C})$ est conjugué à un sous-groupe de $\mathcal{T}_n(\mathbb{C})$, le groupe des matrices triangulaires supérieures.*

Dans la suite, on identifiera $\mathcal{M}_n(\mathbb{C})$ et $\mathscr{L}(\mathbb{C}^n)$.

▷ Montrons par récurrence sur $s = n + m \geq 2$ ($n \geq 1, m \geq 1$) que tout sous-groupe connexe résoluble $G$ de $\mathrm{GL}_n(\mathbb{C})$ tel que $D^m(G) = \{I_n\}$ et $D^{m-1}(G) \neq \{I_n\}$ est conjugué à un sous-groupe de $\mathcal{T}_n(\mathbb{C})$.

– $s = 2$ : Si $n = m = 1$, alors le résultat est vrai.

– Soit $s = n + m > 2$ et supposons le résultat vrai pour tout $s' < n$.

⋆ 1er cas : soit $\{0\} \subsetneq V \subsetneq \mathbb{C}^n$ tel que $V$ est stable par $G$. Notons $r = \dim V$. Alors, si $V'$ est un supplémentaire de $V$ dans $\mathbb{C}^n$, dans une base adaptée à $\mathbb{C}^n = V \oplus V'$, les éléments $g \in G$ ont une matrice de la forme $\begin{pmatrix} A_g & * \\ 0 & B_g \end{pmatrix}$ où $A_g \in \mathrm{GL}_r(\mathbb{C}), B_g \in \mathrm{GL}_{n-r}(\mathbb{C})$. L'application $g \in G \mapsto A_g \in \mathrm{GL}_r(\mathbb{C})$ est un morphisme de groupes continu donc son image est un sous-groupe $G'$ de $\mathrm{GL}_r(\mathbb{C})$ qui est connexe et résoluble[1]. De même, l'image $G''$ de l'application $g \in G \mapsto B_g \in \mathrm{GL}_{n-r}(\mathbb{C})$ est un sous-groupe connexe résoluble de $\mathrm{GL}_{n-r}(\mathbb{C})$. De plus, $s(G'), s(G'') < s$ ([2]) donc, par hypothèse de récurrence, il existe $P \in \mathrm{GL}_r(\mathbb{C})$,$Q \in \mathrm{GL}_{n-r}(\mathbb{C})$ telles que $P^{-1}G'P \subset \mathcal{T}_r(\mathbb{C})$ et $Q^{-1}G''Q \subset \mathcal{T}_{n-r}(\mathcal{C})$. Alors,

$$\begin{pmatrix} P & \\ & Q \end{pmatrix}^{-1} G \begin{pmatrix} P & \\ & Q \end{pmatrix} \subset \mathcal{T}_n(\mathbb{C}).$$

⋆ 2e cas : on suppose qu'un tel espace n'existe pas (la représentation de $G$ sur $V = \mathbb{C}^n$ est *irréductible*).

• Si $m = 1$, alors $G$ est commutatif et tous les éléments de $G$ ont un vecteur propre $0 \neq v \in \mathbb{C}^n$ en commun. Alors, comme $V$ est irréductible, $V = \mathbb{C}v$ et $n = 1$ et le cas est déjà traité.

• Supposons par l'absurde que $m > 1$. Posons $H = D(G) \neq \{I_n\}$. Alors $H$ est un sous-groupe connexe résoluble de $\mathrm{GL}_n(\mathbb{C})$ et $m(H) = m(G) - 1$ donc, par hypothèse de récurrence, il existe $0 \neq v_0 \in \mathbb{C}^n$ tel que $\forall h \in H$, $hv_0 = \lambda(h)v_0$ où $\lambda(h) \in \mathbb{C}^*$. Notons que $\lambda \in H^*$ l'ensemble des caractères continus de $H$.

Posons $W = \bigoplus_{\chi \in H^*} V_\chi$ où

$$V_\chi = \{v \in V,\, \forall h \in H,\, h(v) = \chi(h)v\}.$$

Pour tout $g \in G$, on a $gV_\chi \subset V_{g\chi}$ où $g\chi(h) = \chi(g^{-1}hg)$, $\forall h \in H$.. En effet, si $v \in V_\chi$, alors

$$hg(v) = g\underbrace{g^{-1}hg}_{\in H \text{ car } H \lhd G}(v) = g\left(\chi(g^{-1}hg)v\right) = \chi(g^{-1}hg)g(v).$$

Ainsi, comme $g\chi \in H^*$, le sev $W$ est stable par $G$. Comme $0 \neq v_0 \in W$ et $V$ est irréductible, $W = V$. Ceci signifie que $H \subset \mathcal{D}_n(\mathbb{C})$ l'ensemble des matrices diagonales.

Soit $h \in H \backslash \{I_n\}$. Pour tout $g \in G$, $g^{-1}hg \in H$ est diagonale et a les mêmes valeurs propres que $h$. Il y a un nombre fini de telles matrices. L'application $g \in G \mapsto g^{-1}hg \in H$ est donc continue d'un ensemble connexe à valeurs dans un ensemble fini. Elle est donc constante. Comme $I_n$ a pour image $h$, $\forall g \in G$, $g^{-1}hg = h$. Ainsi, $H \subset Z(G)$.

Soit $\lambda \in \mathbb{C}^*$ une valeur propre de $h$ et $E$ l'espace propre associé. Alors $E$ est stable par $G$ donc, comme $V$ est irréductible, $E = V$ donc $h = \lambda I_n$. Comme $H \subset \mathrm{SL}_n(\mathbb{C})$ (commutateurs), $\lambda^n = 1$. Ainsi, $H \subset \{\lambda I_n,\, \lambda \in \mathbb{C}^*,\, \lambda^n = 1\}$. Comme $H$ est connexe et $I_n \in H$, $\lambda = 1$ et $H = \{I_n\}$ : contradiction. □

1. Si $G$ est un groupe et s'il existe un morphisme surjectif d'un groupe résoluble dans $G$, alors $G$ est résoluble.
2. La dimension a baissé et $m(G'), m(G'') \leq m(G)$.

# 51 Théorème de Müntz

X. Gourdon, *Les maths en tête : Analyse*, 2e édition, Ellipses. Problème 23 p. 291.

Inutilisé.

**Lemme 51.1**

*Soit $E$ un espace préhilbertien réel et $x_1, \dots, x_n \in E$. On appelle matrice de Gram de $(x_1, \dots, x_n)$ la matrice $(\langle x_i, x_j \rangle)_{1 \leq i,j \leq n}$ et déterminant de Gram son déterminant, noté $G(x_1, \dots, x_n)$. C'est une matrice symétrique positive, qui est définie si et seulement si $(x_1, \dots, x_n)$ est libre. Dans ce dernier cas, si $V = \mathrm{Vect}(x_1, \dots, x_n)$, on a*

$$\forall x \in E, \qquad d(x, V)^2 = \frac{G(x_1, \dots, x_n, x)}{G(x_1, \dots, x_n)}.$$

**Lemme 51.2**

*Soient $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{R}$ tels que $a_i + b_j \neq 0$ pour tout $i, j$. Alors*

$$\det\left(\left(\frac{1}{a_i + b_j}\right)_{1 \leq i,j \leq n}\right) = \frac{\displaystyle\prod_{1 \leq i < j \leq n} (a_j - b_i)(b_j - b_i)}{\displaystyle\prod_{1 \leq i,j \leq n} (a_i + b_j)}.$$

**Théorème 51.3 (*Müntz*)**

*Soit $(\alpha_n)_{n \in \mathbb{N}} \in (\mathbb{R}_+^*)^{\mathbb{N}}$ une suite strictement croissante telle que $\alpha_0 = 0$ et $\lim\limits_{n \to +\infty} \alpha_n > 1$. $\mathrm{Vect}(x \mapsto x^{\alpha_n}, n \in \mathbb{N})$ est dense dans $(\mathcal{C}([0,1]), \|.\|_\infty)$ si et seulement si $\displaystyle\sum_{n \geq 1} \frac{1}{\alpha_n}$ diverge.*

▷ Notations : On notera $x^{\alpha_n}$ la fonction $x \in [0,1] \mapsto x^{\alpha_n}$. On munit $\mathcal{C}([0,1])$ du produit scalaire $\langle f, g \rangle = \displaystyle\int_0^1 fg$. Pour $N \in \mathbb{N}$, on note $E_N = \mathrm{Vect}(x^{\alpha_i}, 0 \leq i \leq N)$. Pour $t \in \mathbb{R}_+^*$, on note $\Delta_N(t) = d_{\|.\|_2}(x^t, E_N)$.

– *Étape 1 : Calculons* $\Delta_N(t)$. D'après le lemme 1, comme $(x^{\alpha_i})_{0 \leq i \leq N}$ est libre, on a :

$$\Delta_N(t)^2 = \frac{G(x^{\alpha_0}, \dots, x^{\alpha_N}, x^t)}{G(x^{\alpha_0}, \dots, x^{\alpha_N})}.$$

Or, pour $a, b \in \mathbb{R}_+$, $\langle x^a, x^b \rangle = \dfrac{1}{a + b + 1}$, donc, d'après le lemme 2,

$$G(x^{\alpha_0}, \dots, x^{\alpha_N}, x^t) = \frac{\displaystyle\prod_{0 \leq i \leq i < j \leq N} (\alpha_j - \alpha_i)^2 \prod_{i=1}^{N} (t - \alpha_i)^2}{(2t+1) \displaystyle\prod_{0 \leq i,j \leq N} (\alpha_i + \alpha_j + 1) \prod_{i=1}^{N} (\alpha_i + t + 1)^2}$$

et

$$G(x^{\alpha_0}, \dots, x^{\alpha_N}) = \frac{\displaystyle\prod_{0 \leq i < j \leq N} (\alpha_j - \alpha_i)^2}{\displaystyle\prod_{0 \leq i,j \leq N} (\alpha_i + \alpha_j + 1)}$$

d'où

$$\Delta_N(t) = \frac{1}{\sqrt{2t+1}} \prod_{i=0}^{N} \left| \frac{\alpha_i - t}{\alpha_i + t + 1} \right|.$$

Notons $E = \mathrm{Vect}(x^{\alpha_i}, i \in \mathbb{N})$.

– *Étape 2 : Supposons que* $\overline{E}^{\|.\|_2} = \mathcal{C}([0,1])$. *Montrons que* $\sum_{n\geq 1} \frac{1}{\alpha_n}$ *diverge.* Soit $t \in \mathbb{R}_+^*$ tel que $t \neq \alpha_n$ $\forall n \in \mathbb{N}$. Alors $x^t \in \overline{E}^{\|.\|_2}$ donc la suite $(\Delta_N(t))_{N\in\mathbb{N}})$ tend vers 0. Ainsi,

$$\prod_{i=0}^{N} \left| \frac{\alpha_i - t}{\alpha_i + t + 1} \right| \xrightarrow[N\to+\infty]{} 0 \qquad (*)$$

⋆ 1er cas : $(\alpha_n)_{n\in\mathbb{N}}$ est bornée. Alors le résultat est vrai.

⋆ 2e cas : $\alpha_n \xrightarrow[n\to+\infty]{} +\infty$. Soit $N_0 \in \mathbb{N}$ tel que $\forall n \geq N_0$, $\alpha_n > t$. D'après $(*)$, $\sum_{n=N_0}^{+\infty} \ln\left(\frac{\alpha_n - t}{\alpha_n + t + 1}\right) = -\infty$. Or,

$$\ln\left(\frac{\alpha_n - t}{\alpha_n + t + 1}\right) = \ln\left(1 - \frac{2t+1}{\alpha_n + t + 1}\right) \underset{n\to+\infty}{\sim} -\frac{2t+1}{\alpha_n}.$$

D'après le théorème de comparaison, la série $\sum_{n\geq N_0} \frac{1}{\alpha_n}$ diverge.

– *Étape 3 : Supposons que* $\sum_{n\geq 1} \frac{1}{\alpha_n}$ *diverge. Montrons que* $\overline{E}^{\|.\|_2} = \mathcal{C}([0,1])$. D'après le théorème de Weierstrass, comme $\|.\|_2 \leq \|.\|_\infty$, il suffit de montrer que $\forall m \in \mathbb{N}$, $x^m \in \overline{E}^{\|.\|_2}$. Soit $m \in \mathbb{N}$. Il suffit de montrer que

$$\lim_{N\to+\infty} \prod_{i=0}^{N} \left| \frac{\alpha_i - m}{\alpha_i + m + 1} \right| = 0.$$

⋆ 1er cas : $m = \alpha_{n_0}$, alors le résultat est vrai.

⋆ 2e cas : si $(\alpha_n)_{n\in\mathbb{N}}$ est bornée, alors $\left| \frac{\alpha_n - m}{\alpha_n + m + 1} \right| \not\xrightarrow[n\to+\infty]{} 1$ donc la série $\sum_{n\geq 0} \ln \left| \frac{\alpha_n - m}{\alpha_n + m + 1} \right|$ diverge (grossièrement) d'où le résultat.

⋆ 3e cas : si $\alpha_n \xrightarrow[n\to+\infty]{} +\infty$, alors comme précédemment, $\ln\left(\frac{\alpha_n - m}{\alpha_n + m + 1}\right) \underset{n\to+\infty}{\sim} -\frac{2m+1}{\alpha_n}$ donc d'après le théorème de comparaison, $\sum_{n\geq N_0} \ln\left(\frac{\alpha_n - m}{\alpha_n + m + 1}\right) = -\infty$ d'où le résultat.

– *Étape 4 : Montrons que* $\overline{E}^{\|.\|_\infty} = \mathcal{C}([0,1])$ *si et seulement si* $\sum_{n\geq 1} \frac{1}{\alpha_n}$ *diverge.* Si $\overline{E}^{\|.\|_\infty} = \mathcal{C}([0,1])$ alors, comme $\|.\|_2 \leq \|.\|_\infty$, $E^{\|.\|_2} = \mathcal{C}([0,1])$ et d'après ce qui précède, $\sum_{n\geq 1} \frac{1}{\alpha_n}$ diverge.

Réciproquement, supposons que $\sum_{n\geq 1} \frac{1}{\alpha_n}$ diverge. Comme $\lim \alpha_n > 1$, il existe $N \in \mathbb{N}$ tel que $\alpha_N > 1$ et on peut supposer $\alpha_1 > 1$ (en n'enlevant qu'un nombre fini de termes à la série). D'après le théorème de Weierstrass, il suffit de montrer que tout polynôme $P$ est dans $\overline{E}^{\|.\|_\infty}$. Soient $p$ un polynôme et $\varepsilon > 0$. La série $\sum_{n\geq 1} \frac{1}{\alpha_n - 1}$ diverge donc, d'après ce qui précède, il existe $g \in \mathrm{Vect}(x^{\alpha_n - 1}, n \in \mathbb{N}^*)$ tel que $\|p' - g\|_2 \leq \varepsilon$. Notons $h$ la primitive de $g$ telle que $h(0) = P(0)$ et $q = h - p$. Alors, $h \in E$ et

$$\forall x \in [0,1], \qquad q(x) = \int_0^x q'(t)\mathrm{d}t$$

donc, d'après l'inégalité de Cauchy-Schwarz,

$$|q(x)| \leq \left( \int_0^x q'(t)^2 \mathrm{d}t \right)^{1/2} \sqrt{x} \leq \|q'\|_2 = \|p' - g\|_2 \leq \varepsilon.$$

Ainsi, $\|p - h\|_\infty \leq \varepsilon$ donc $p \in \overline{E}^{\|.\|_\infty}$. □

# 52 Transformation d'Euler

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Analyse 1*, 2e édition, Cassini. Exercice 3.33 page 182.

Inutilisé.

**Proposition 52.1**

*Soit $f : \mathbb{R}_+ \to \mathbb{R}_+$ de classe $\mathcal{C}^\infty$ telle que $\forall p \in \mathbb{N}, \forall x \geq 0$, $(-1)^p f^{(p)}(x) \geq 0$. On suppose de plus que $f(n) \xrightarrow[n\to+\infty]{} 0$. Alors, la série $\sum_{n\geq 0}(-1)^n f(n)$ converge et, pour tout $p \in \mathbb{N}$,*

$$\sum_{n=0}^{+\infty}(-1)^n f(n) = \sum_{n=0}^{p-1}\frac{\Delta^p f(0)}{2^{n+1}} + R_p$$

*avec $|R_p| \leq \dfrac{|\Delta^p f(0)|}{2^p} \xrightarrow[p\to+\infty]{} 0$, où $\Delta f : x \in \mathbb{R}_+ \mapsto f(x) - f(x+1)$.*

▷ La série $\sum_{n\geq 0}(-1)^n f(n)$ converge d'après le critère des séries alternées.

– Montrons, pour tout suite $(u_n)_{n\in\mathbb{N}}$ de réels positifs décroissante vers 0, que pour tout $p \in \mathbb{N}$, la série $\sum_{n\geq 0}(-1)^n \Delta^p u_n$ converge et

$$\sum_{n=0}^{+\infty}(-1)^n u_n = \sum_{n=0}^{p-1}\frac{\Delta^n u_0}{2^{n+1}} + \frac{1}{2^p}\sum_{n=0}^{+\infty}(-1)^n \Delta^p u_n$$

où $(\Delta u_n)_{n\in\mathbb{N}} = (u_n - u_{n+1})_{n\in\mathbb{N}}$. On procède par récurrence sur $p \in \mathbb{N}$.

⋆ $p = 0$ : ok.

⋆ $p \to p+1$ : Soit $N \in \mathbb{N}$.

$$\sum_{n=0}^{N}(-1)^n \Delta^{p+1} u_n = \sum_{n=0}^{N}(-1)^n \Delta^p u_n - \sum_{n=0}^{N}(-1)^n \Delta^p u_{n+1} = \sum_{n=0}^{N}(-1)^n \Delta^p u_n + \sum_{n=1}^{N+1}(-1)^n \Delta^p u_n$$

donc, par hypothèse de récurrence, la série $\sum_{n\geq 0}(-1)^n \Delta^p u_n$ converge et

$$\sum_{n=0}^{+\infty}(-1)^n \Delta^{p+1} u_n = 2\sum_{n=0}^{+\infty}(-1)^n \Delta^p u_n - \Delta^p u_0 = 2^{p+1}\left(\sum_{n=0}^{+\infty}(-1)^n u_n - \sum_{n=0}^{p-1}\frac{\Delta^n u_0}{2^{n+1}}\right) - \Delta^p u_0$$

donc

$$\sum_{n=0}^{+\infty}(-1)^n u_0 = \sum_{n=0}^{p}\frac{\Delta^n u_0}{2^{n+1}} + \frac{1}{2^{p+1}}\sum_{n=0}^{+\infty}(-1)^n \Delta^{p+1} u_n.$$

– Posons, pour $n \in \mathbb{N}$, $u_n = f(n)$. Par hypothèse, $f$ et $-f'$ sont positives sur $\mathbb{R}_+$ donc $(u_n)$ est positive et décroissante. De plus, par hypothèse, $u_n \xrightarrow[n\to+\infty]{} 0$. D'après ce qui précède, pour tout $p \in \mathbb{N}$,

$$\sum_{n=0}^{+\infty}(-1)^n f(n) = \sum_{n=0}^{p-1}\frac{\Delta^p f(0)}{2^{n+1}} + \underbrace{\frac{1}{2^p}\sum_{n=0}^{+\infty}(-1)^n \Delta^p f(n)}_{R_p}.$$

– Pour démontrer la majoration sur $R_p$, montrons que la série $\sum_{n\geq 0}(-1)^n \Delta^p f(n)$ vérifie le critère des séries alternées, car alors la somme est inférieure à son premier terme.

– Montrons par récurrence sur $p \in \mathbb{N}$ que $\forall f \in \mathcal{C}^\infty(\mathbb{R}_+, \mathbb{R}_+)$ telle que $(-1)^n f^{(n)} \geq 0$ pour tout $n \in \mathbb{N}$, on a $\Delta^p f \geq 0$ sur $\mathbb{R}_+$.

⋆ $p = 0$ : ok.

$\star$ $p \to p+1$ : Soit $f \in \mathcal{C}^\infty(\mathbb{R}_+, \mathbb{R}_+)$ telle que $(-1)^n f^{(n)} \geq 0$ pour tout $n \in \mathbb{N}$. Alors, $-f'$ vérifie également cette hypothèse et, par hypothèse de récurrence appliquée à $-f'$, on a $\Delta^p(-f') \geq 0$ sur $\mathbb{R}_+$. Mais $\Delta^p(-f') = -(\Delta^p f)'$ donc $\Delta^p f$ est décroissante sur $\mathbb{R}_+$, donc $\Delta^{p+1}$ est positive.

– On a également montré que, pour tout $p \in \mathbb{N}$, $(\Delta^p f(n))_{n\in\mathbb{N}}$ est décroissante. De plus, on a déjà montré que, pour tout $p \in \mathbb{N}$, $\sum_{n\geq 0}(-1)^n \Delta^p f(n)$ converge donc, en particulier, $\Delta^p f(n) \xrightarrow[n\to+\infty]{} 0$. Ainsi, d'après le critère des séries alternées,

$$\forall p \in \mathbb{N}, \qquad |R_p| \leq \frac{|\Delta^p f(0)|}{2^p}.$$

– Enfin, pour tout $p \in \mathbb{N}$, $\Delta^{p+1} f(0) = \Delta^p f(0) - \underbrace{\Delta^p f(1)}_{\geq 0} \leq \Delta^p f(0)$ donc la suite $(\Delta^p f(0))_{p\in\mathbb{N}}$ est décroissante. Ainsi,

$$|R_p| \leq \frac{f(0)}{2^p} \xrightarrow[p\to+\infty]{} 0.$$

□

**Application :** On considère $f : x \in \mathbb{R}_+ \mapsto \dfrac{1}{x+1}$. Pour tout $p \in \mathbb{N}$,

$$\forall x \in \mathbb{R}_+, \qquad f^{(p)}(x) = \frac{(-1)^p p!}{(x+1)^{p+1}}.$$

Pour $p = 30$, on a $\dfrac{\Delta^p f(0)}{2^{30}} = \dfrac{1}{31 \times 2^{30}} < 4 \times 10^{-11}$ donc $\displaystyle\sum_{n=0}^{29} \frac{\Delta^n f(0)}{2^{n+1}}$ est une valeur approchée à moins de $4 \times 10^{-11}$ près de $\ln 2$.

On a $\Delta^n f(0) = \displaystyle\sum_{k=0}^{n} \binom{n}{k} (-1)^k f(k)$ donc l'évaluation précédente requiert $\displaystyle\sum_{n=0}^{29}(n+1) = \frac{30 \times 31}{2} = 465$ additions.

Or, d'après la majoration obtenue par le critère des séries alternées,

$$\left| \ln 2 - \sum_{n=0}^{465} (-1)^n f(n) \right| \leq \frac{1}{466} > 0,002.$$

De fait, $\ln 2 - \displaystyle\sum_{n=0}^{465} (-1)^n f(n) \geq 10^{-3}$.

# 53 Un calcul lié à l'avance du périhélie de Mercure

F. Rouvière, *Petit guide de calcul différentiel*, 4e édition, Cassini. Exercice 79 page 236.

Inutilisé

On considère la fonction $f$ définie sur $\mathbb{R}^2$ par

$$\forall (\varepsilon, x) \in \mathbb{R}^2, \qquad f(\varepsilon, x) = (x-a)(b-x) + \varepsilon x^3$$

où $a < b$ sont des réels fixés et $\varepsilon > 0$ un paramètre.

Pour $\varepsilon = 0$, l'équation $f(0,x)$ a pour solutions $a$ et $b$ sur $\mathbb{R}$. Qu'en est-il pour l'équation $f(\varepsilon, x) = 0$, d'inconnue $x \in \mathbb{R}$.

Montrons que pour $\varepsilon > 0$ assez petit, $f(\varepsilon, x) = 0$ a trois racines distinctes $x_1(\varepsilon) < x_2(\varepsilon) < x_3(\varepsilon)$. Démontrons alors le développement asymptotique

$$I(\varepsilon) = \int_{x_1(\varepsilon)}^{x_2(\varepsilon)} \frac{\mathrm{d}x}{\sqrt{f(\varepsilon, x)}} = \pi + \frac{3\pi}{4}(a+b)\varepsilon + \underset{\varepsilon \to 0}{\mathcal{O}}(\varepsilon^2).$$

**Motivation :** Cette intégrale apparaît en physique dans l'étude des planètes. Plus précisément, le terme d'ordre $\varepsilon$, qui provient d'une correction relativiste, a permis d'expliquer l'avance du périhélie de Mercure de 43 secondes d'arc par siècle.

**Preuve.** On sait que $f(0,a) = 0$ et $\partial_x f(0,a) = b - a > 0$ donc, comme $f$ est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}^2$, d'après le théorème des fonctions implicites, il existe un voisinage ouvert $V_1$ de 0, un voisinage ouvert $W_1$ de $a$ et une fonction $x_1 \in \mathcal{C}^\infty(V_1, W_1)$ tels que

$$(\varepsilon, x) \in V_1 \times W_1 \text{ et } f(\varepsilon, x) = 0 \qquad \Longleftrightarrow \qquad \varepsilon \in V_1 \text{ et } x = x_1(\varepsilon).$$

On sait que $x_1(0) = a$ et en dérivant la relation

$$\forall \varepsilon \in V_1, \qquad 0 = f(\varepsilon, x_1(\varepsilon))$$

il vient

$$(-2x_1(\varepsilon) + a + b + 3\varepsilon x_1(\varepsilon)^2) x_1'(\varepsilon) + x_1(\varepsilon)^3 = 0$$

d'où l'on déduit

$$x_1'(0) = \frac{-a^3}{b-a}.$$

Alors, d'après le théorème de Taylor-Young,

$$x_1(\varepsilon) = a - \frac{a^3}{b-a}\varepsilon + \underset{\varepsilon \to 0}{\mathcal{O}}(\varepsilon^2).$$

En permutant $a$ et $b$, on obtient un voisinage ouvert $V_2$ de 0, un voisinage ouvert $W_2$ de $b$ et une fonction $x_2 \in \mathcal{C}^\infty(V_2, W_2)$ tels que

$$(\varepsilon, x) \in V_2 \times W_2 \text{ et } f(\varepsilon, x) = 0 \qquad \Longleftrightarrow \qquad \varepsilon \in V_2 \text{ et } x = x_2(\varepsilon)$$

et

$$x_2(\varepsilon) = b + \frac{b^3}{b-a}\varepsilon + \underset{\varepsilon \to 0}{\mathcal{O}}(\varepsilon^2).$$

De plus,

$$\forall (\varepsilon, x) \in \mathbb{R}^2, \qquad f(\varepsilon, x) = \varepsilon x^3 - x^2 + (a+b)x - ab$$

donc, d'après les relations coefficients-racines, la troisième racine $x_3(\varepsilon) \in \mathbb{C}$ de $f$ vérifie

$$x_1(\varepsilon) + x_2(\varepsilon) + x_3(\varepsilon) = \frac{1}{\varepsilon}$$

d'où

$$\mathbb{R} \ni x_3(\varepsilon) = \frac{1}{\varepsilon} - (a+b) - (a^2 + ab + b^2)\varepsilon + \underset{\varepsilon \to 0}{\mathcal{O}}(\varepsilon^2).$$

Pour $\varepsilon > 0$ assez petit, on a donc trois solutions distinctes.

En notant $x_i = x_i(\varepsilon)$ pour $i = 1, 2, 3$, on remarque que

$$\forall (\varepsilon, x) \in \mathbb{R}^2, \qquad f(\varepsilon, x) = (x - x_1)(x_2 - x)(1 - \varepsilon(x + x_1 + x_2))$$

de sorte que

$$I(\varepsilon) = \int_{x_1}^{x_2} \frac{(1 - \varepsilon(x + x_1 + x_2))^{-1/2}}{\sqrt{(x - x_1)(x_2 - x)}} \mathrm{d}x.$$

En posant $u = \dfrac{x_1 + x_2}{2}$ et $v = \dfrac{x_2 - x_1}{2}$ et en effectuant le changement de variables $x = u + v \sin t$, on obtient

$$I(\varepsilon) = \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} (1 - \varepsilon(3u + v \sin t))^{-1/2} \, \mathrm{d}t.$$

Or, d'après les développements limités précédents,

$$3u + v \sin t = \frac{3}{2}(a + b) + \frac{b - a}{2} \sin t + r(\varepsilon, t)$$

avec $|r(\varepsilon, t)| \leq C\varepsilon$ uniformément en $t$ car $|\sin t| \leq 1$. De plus, d'après le théorème de Taylor-Lagrange,

$$\forall |x| \leq \frac{1}{2}, \qquad (1 - x)^{-1/2} = 1 + \frac{1}{2} z + \alpha \frac{z^2}{2}$$

avec $|\alpha| \leq 3\sqrt{2}$ (en majorant la dérivée seconde). Il en découle que, pour $\varepsilon > 0$ assez petit,

$$(1 + \varepsilon(3u + v \sin t))^{-1/2} = 1 + \frac{\varepsilon}{2}(3u + v \sin t) + s(\varepsilon, t)$$

avec $|s(\varepsilon, t)| \leq C\varepsilon^2$ uniformément en $t$ car $|\sin t| \leq 1$.

Ainsi, grâce à l'uniformité en $t$ des majorations de $r(\varepsilon, t)$ et $s(\varepsilon, t)$,

$$I(\varepsilon) = \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \left(1 + \frac{3}{4}(a + b)\varepsilon + \frac{b - a}{4} \varepsilon \sin t\right) \mathrm{d}t + \underset{\varepsilon \to 0}{\mathcal{O}}(\varepsilon^2)$$

et finalement,

$$I(\varepsilon) = \pi + \frac{3\pi}{4}(a + b)\varepsilon + \underset{\varepsilon \to 0}{\mathcal{O}}(\varepsilon^2).$$