ENS Rennes - Université de Rennes I

Développements pour l'Agrégation

Brieuc Frénais

Année 2019/2020

Table des matières

Chapitre I

Algèbre

1 Caractères et sous-groupes distingués

Leçons 103, 107(, 101)

Ref : [Ulm12] 17.3, [Lav18]

Ce développement consiste à démontrer le théorème suivant, qui donne une méthode permettant de connaître les sous-groupes distingués d'un groupe fini, en étudiant ses caractères irréductibles. Tel quel, il n'est pas très long, et il peut être intéressant d'ajouter un exemple pratique. J'en propose deux à l'issue de la démonstration.

Définition 1.1 On appelle *noyau* d'un caractère χ associé à une représentation linéaire d'un groupe fini G l'ensemble

$$\ker(\chi) := \{g \in G,\ \chi(g) = \chi(1)\}.$$

Théorème 1.2 Soit G un groupe fini de cardinal n et de caractères irréductibles $\chi_1, .., \chi_m$. Alors les sous-groupes distingués de G sont exactement les sous-groupes H_I de la forme

$$H_I := \bigcap_{i \in I} \ker(\chi_i),$$

où I désigne une partie quelconque de $[\![1, m]\!]$.

Démonstration.

Étape 1. Un lien entre le caractère et la représentation.

Lemme 1.3 Soit (V, ρ) une représentation linéaire de G de caractère χ. Alors $\ker(\chi) = \ker(\rho)$.

Soit $g \in G$. D'après le théorème de Lagrange, $g^n = 1$. On en déduit que $\rho(g)^n$ est l'identité sur V. En particulier, le polynôme $X^n - 1$ annule $\rho(g)$. Mais comme ce polynôme est simplement scindé sur $\mathbb{C}$, $\rho(g)$ est diagonalisable, et ses valeurs propres sont des racines n-ièmes de l'unité. On note $(\lambda_i)_{1 \leq i \leq p}$ ces valeurs propres, qui sont en particulier de module 1. On a alors

$$\chi(g) = \mathrm{Tr}(\rho(g)) = \sum_{i=1}^{p} \lambda_i.$$

Ainsi, on a par inégalité triangulaire

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

De plus, l'unique cas d'égalité est celui où toutes les valeurs propres sont 1, c'est-à-dire si $\rho(g)$ est l'identité. Il y a donc bien équivalence entre l'appartenance de g à $\ker(\rho)$ et le fait que $\rho(g)$ valent $\rho(1)$.

Étape 2. Un sous-groupe distingué est le noyau d'un caractère.

Soit H un sous-groupe distingué de G. On considère l'action à gauche φ de G sur G/H. On considère également un espace vectoriel V dont une base est indexée par G/H. [1] Ainsi, V peut être vu comme une représentation linéaire de G, via l'action ρ_φ par permutation des vecteurs de base. Alors le noyau de ρ_φ est bien sûr le même que celui de φ, et c'est donc H. D'après le lemme on a donc $H = \ker(\chi)$, où χ est le caractère associé à cette représentation linéaire.

Étape 3. Décomposition des noyaux de caractères.

On se donne maintenant une représentation quelconque (V, ρ) de G, et on note χ le caractère associé. On décompose V en somme de représentations irréductibles

$$V = \bigoplus_{i=1}^{m} V_i^{\oplus n_i} = \bigoplus_{i \in I} V_i^{\oplus n_i},$$

où $I = \{i \in [\![1, m]\!],\ n_i \neq 0\} \subset [\![1, m]\!]$. On a alors, pour $g \in G$ fixé, la chaîne d'équivalences suivantes (on applique entre autres deux fois le lemme de l'étape 1) :

$$\begin{array}{rc} & g \in \ker(\chi) \\ \iff & g \in \ker(\rho) \\ \iff & \forall i \in I \quad g \in \ker(\rho_{|V_i}) \\ \iff & \forall i \in I \quad g \in \ker(\chi_i) \\ \iff & g \in \bigcap_{i \in I} \ker(\chi_i). \end{array}$$

On a bien montré $\ker(\chi) = \bigcap_{i \in I} \ker(\chi_i)$.

Réciproquement, le lemme montre que si $H = \bigcap_{i \in I} \ker(\chi_i)$, H est intersection de noyaux de morphismes de groupes (les $\rho_{|V_i}$), donc H est distingué dans G. □

Application 1.4 On donne les tables de caractères de deux groupes, le groupe symétrique $\mathfrak{S}_4$ (voir développement 16) et le groupe des quaternions $\mathbb{H}_8$ [2].

$\mathfrak{S}_4$	id 1	(1 2) 6	(1 2 3) 8	(1 2)(3 4) 3	(1 2 3 4) 6
$\mathbb{1}$	1	1	1	1	1
ε	1	−1	1	1	−1
χ_2	2	0	−1	2	0
χ_Δ	3	1	0	−1	−1
$\varepsilon\chi_\Delta$	3	−1	0	−1	1

$\mathbb{H}_8$	1 1	−1 1	i 2	j 2	k 2
$\mathbb{1}$	1	1	1	1	1
χ_i	1	1	1	−1	−1
χ_j	1	1	−1	1	−1
χ_k	1	1	−1	−1	1
χ_2	2	−2	0	0	0

On obtient donc les résultats suivants :

- pour $\mathfrak{S}_4$,
  - $\ker(\mathbb{1}) = \mathfrak{S}_4$,
  - $\ker(\varepsilon) = \mathfrak{A}_4$,
  - $\ker(\chi_2) = \langle (1\ 2)(3\ 4) \rangle = V_4$,
  - $\ker(\chi_\Delta) = \ker(\varepsilon\chi_\Delta) = \{\mathrm{id}\}$.

1. On peut par exemple choisir de considérer la représentation régulière de G/H.

2. Cette table est décrite dans plusieurs livres mais généralement sans démonstration. Celle-ci n'est pas compliquée. Pour les caractère de degré 1, on peut simplement observer que $\chi(-1)$ est d'ordre 2 dans $\mathbb{C}^*$ et $\chi(z)$ d'ordre 4 pour $z \in \{\mathrm{i}, \mathrm{j}, \mathrm{k}\}$, puis dire qu'on teste les plus simples et qu'on obtient bien trois caractères irréductibles distincts. Ensuite, le caractère de degré 2 se déduit par les relations d'orthogonalité.

Comme ces groupes sont inclus les uns dans les autres, on a obtenu ici tous les sous-groupes distingués de $\mathfrak{S}_4$.

– pour $\mathbb{H}_8$,
  — $\ker(\mathbb{1}) = \mathbb{H}_8$,
  — $\ker(\chi_z) = \langle z \rangle$, pour $z \in \{\mathrm{i}, \mathrm{j}, \mathrm{k}\}$,
  — $\ker(\chi_2) = \{1\}$.

  Finalement, les sous-groupes distingués de $\mathbb{H}_8$ sont $\{1\}, \langle -1 \rangle = \langle \mathrm{i} \rangle \cap \langle \mathrm{j} \rangle, \langle \mathrm{i} \rangle, \langle \mathrm{j} \rangle, \langle \mathrm{k} \rangle$ et $\mathbb{H}_8$.

2 Commutant et polynômes d'endomorphisme

Leçons 151, 162

Ref : [FGN09b]2.45

Pour $A \in \mathcal{M}_n(\mathbb{K})$, on note $\mathcal{C}(A) := \{B \in \mathcal{M}_n(\mathbb{K}),\ AB = BA\}$ le *commutant* de A, et $\mathbb{K}[A] := \{P(A),\ P \in \mathbb{K}[X]\}$ l'espace des polynômes en A. On note aussi $T_n(\mathbb{K})$ l'espace des matrices triangulaires supérieures de taille n sur $\mathbb{K}$.

Théorème 2.1 Pour toute matrice A dans $\mathcal{M}_n(\mathbb{K})$, $\mathcal{C}(A) = \mathbb{K}[A]$ si et seulement si les polynômes minimaux et caractéristiques de A sont les mêmes.

Démonstration. On se donne une matrice $A = (a_{ij})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K})$.

Étape 1. Dimension du commutant.

On va montrer que la dimension de $\mathcal{C}(A)$ est de manière générale supérieure à n. Pour cela, on étudie le système d'équations

$$AX - XA = 0 \tag{S}$$

d'inconnue $X = (x_{ij})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K})$. On note S le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ des solutions de ce système, de sorte que l'on a bien sûr $S = \mathcal{C}(A)$.

- On suppose tout d'abord que A est trigonalisable, et, quitte à changer de base, qu'elle est triangulaire supérieure. On cherche les solutions triangulaires supérieures de (S). Les solutions correspondent aux X de $T_n(\mathbb{K})$ (qui est de dimension $\frac{n(n+1)}{2}$) satisfaisant les $\frac{n(n+1)}{2}$ équations de nullité des coefficients de la partie triangulaire supérieure. Mais les équations dûes aux coefficients diagonaux sont toujours vérifiées si $A, X \in T_n(\mathbb{K})$. Il y a donc $\frac{n(n-1)}{2}$ équations pour $\frac{n(n+1)}{2}$ inconnues, donc l'espace $S \cap T_n(\mathbb{K})$ est au moins de dimension n, et S également.
- Le résultat est toujours vrai dans le cas où A n'est pas trigonalisable : en effet, la dimension de l'espace des solutions d'un système linéaire ne dépend pas de l'extension de corps dans laquelle on cherche les solutions. Ainsi, dans la clôture algébrique $\mathbb{L}$ de $\mathbb{K}$, A est trigonalisable et le raisonnement précédent permet de conclure.

Ainsi, la dimension de $\mathcal{C}(A)$ est au moins n.

Étape 2. Sens direct par égalité de degrés.

Supposons que $\mathbb{K}[A] = \mathcal{C}(A)$. Alors $\mathbb{K}[A]$ est de dimension n. Or la dimension de $\mathbb{K}[A]$ est le degré du polynôme minimal, donc le polynôme minimal est de degré au moins n. Mais comme le polynôme caractéristique de A est de degré au plus n, et qu'il est divisible par le polynôme minimal (par théorème de Cayley-Hamilton), alors ceux-ci sont égaux (car unitaires). Donc $\mu_A = \chi_A$.

Étape 3. Sens réciproque par égalité de dimensions.

On suppose que $\mu_A = \chi_A$. On pose μ_x le polynôme minimal en x de A, c'est-à-dire le polynôme unitaire qui engendre l'idéal $\{P \in \mathbb{K}[X],\ P(A)x = 0\}$. On sait qu'il existe $x \in \mathbb{K}^n$, tel que $\mu_A = \mu_x$ [2]. Alors μ_x est de degré n (car égal à χ_A), ce qui prouve que la famille $(x, Ax, .., A^{n-1}x)$ est libre, et forme donc une base de $\mathbb{K}^n$. On en déduit que A est cyclique. On considère l'application

$$f : \left| \begin{array}{ccc} \mathcal{C}(A) & \longrightarrow & \mathbb{K}^n \\ B & \longmapsto & Bx \end{array} \right. .$$

Elle est linéaire. De plus, si $Bx = 0$, alors $BA^kx = A^kBx = 0$ pour tout k, ce qui signifie que B est nulle, car nulle en tout point d'une base de $\mathbb{K}^n$. Donc f est injective. Ainsi, la dimension du commutant est inférieure à n. Or $\mathbb{K}[A]$ est un sous-espace vectoriel de $\mathcal{C}(A)$, de dimension $\deg(\mu_A) = \deg(\chi_A) = n$. Donc, par un argument de dimensions, $\mathbb{K}[A] = \mathcal{C}(A)$. □

2. Si on a le temps, il peut être bon de démontrer ce résultat. On trouvera par exemple une preuve dans [Gou09].

3 Coniques passant par six points

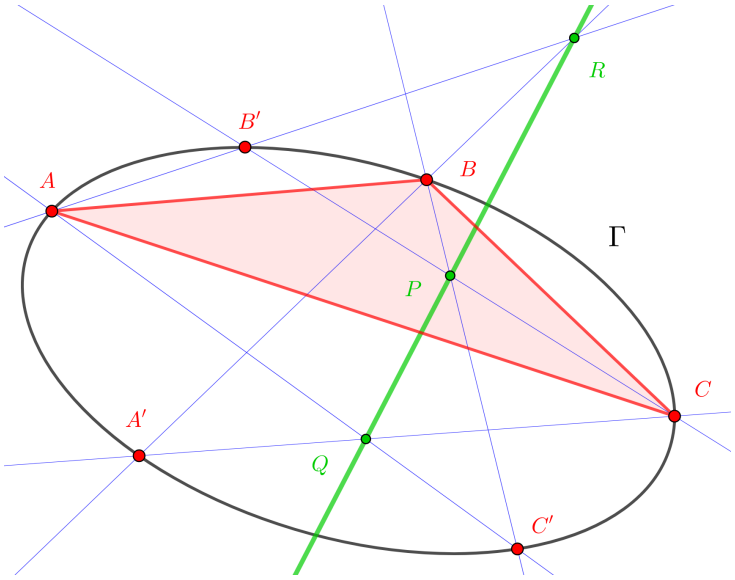
Leçons 152, 171, 181(, 162, 191)

Ref : [Eid09] II.2.1 et II.3

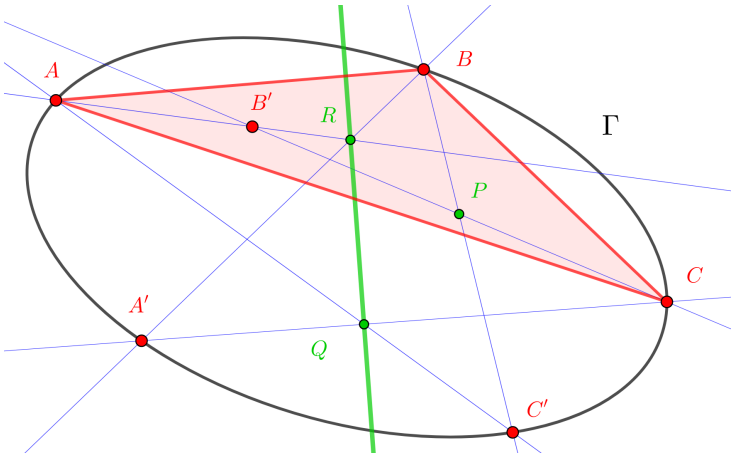
On démontre ici le théorème de Pascal et une application à l'existence d'une conique passant par six points dans certains cas. On a plusieurs options pour ce développement. On peut l'axer coniques et barycentres, en démontrant le théorème de Pascal et son application, ou bien démontrer seulement l'application, sans utiliser le théorème, et en étudiant un déterminant 6×6 qui se calcule par blocs (plutôt pour la leçon 152 donc), comme c'est fait dans la foulée dans [Eid09].

Théorème 3.1 (Pascal) On se donne six points A, B, C, A', B' et C', les trois premiers étant non alignés. On note P, Q et R les intersections respectives des droites (BC') et $(B'C)$, (AC') et $(A'C)$, et (AB') et $(A'B)$. Alors P, Q et R sont alignés si et seulement si par les six points A, B, C, A', B' et C' passe une conique.

Remarque 3.2 La situation est résumée sur la figure 3.1 : on a tracé dans les deux cas l'unique conique Γ passant par les points A, B, C, A' et C'. Dans le premier cas, on voit qu'elle passe aussi par B', et que les trois points verts sont alignés ; dans le second cas, le point P n'est pas sur la droite RQ et le point B' n'est pas sur la conique.



(a) Cas favorable



(b) Cas défavorable

Figure 3.1 – Illustration du théorème de Pascal pour les coniques

Démonstration.

Étape 1. Équation barycentrique d'une conique passant par A, B et C.

On se place dans le repère barycentrique (A, B, C), relié au repère cartésien $(A, \overrightarrow{AB}, \overrightarrow{AC})$ par les relations suivantes :

- un point de coordonnées cartésiennes (u, v) est de coordonnées barycentriques (X, Y, Z), avec $X = 1 - u - v, Y = u$ et $Z = v$,
- un point de coordonnées barycentriques (X, Y, Z) est de coordonnées cartésiennes (u, v), avec $u = \dfrac{Y}{X+Y+Z}$ et $v = \dfrac{Z}{X+Y+Z}$.

On se donne une conique d'équation

$$\alpha_1 u^2 + \alpha_2 uv + \alpha_3 v^2 + \beta_1 u + \beta_2 v + \gamma = 0,$$

avec donc α_1, α_2 et α_3 non tous nuls. En passant aux coordonnées barycentriques, on obtient

$$\gamma X^2 + (\alpha_1 + \beta_1 + \gamma)Y^2 + (\alpha_3 + \beta_2 + \gamma)Z^2 + (\beta_1 + 2\gamma)XY + (\beta_2 + 2\gamma)XZ + (\alpha_1 + \beta_1 + \beta_2 + 2\gamma)YZ = 0.$$

Or on veut que A, B et C soient sur la conique, on en déduit que les coefficients en X^2, Y^2 et Z^2 sont nuls (en écrivant respectivement que $A : (1, 0, 0)$, $B : (0, 1, 0)$ et $C : (0, 0, 1)$ vérifient l'équation). Ainsi, l'équation devient

$$pXY + qXZ + rYZ = 0,$$

avec p, q, r non tous nuls. Réciproquement, on voit en remontant de cette équation aux coordonnées cartésiennes qu'on obtient bien l'équation d'une conique contenant les points A, B et C.

Étape 2. Condition équivalente d'existence de la conique.

Si une conique de la forme recherchée dans l'énoncé existe, en notant $(x, y, z), (x', y', z')$ et (x'', y'', z'') les coordonnées barycentriques de A', B' et C', il existe des coefficients p, q, r non tous nuls tels que

$$\begin{cases} pxy + qxz + ryz = 0 \\ px'y' + qx'z' + ry'z' = 0 \\ px''y'' + qx''z'' + ry''z'' = 0 \end{cases}$$

ce qui est équivalent au fait que le déterminant $\begin{vmatrix} xy & xz & yz \\ x'y' & x'z' & y'z' \\ x''y'' & x''z'' & y''z'' \end{vmatrix}$ soit nul.

Étape 3. Condition équivalente d'alignement des points et conclusion.

On ramène aussi la condition d'alignement des points P, Q et R à la nullité d'un déterminant. La droite (BC') est d'équation

$$\begin{vmatrix} 0 & 1 & 0 \\ x'' & y'' & z'' \\ X & Y & Z \end{vmatrix} = z''X - x''Z = 0,$$

et la droite $(B'C)$ d'équation

$$\begin{vmatrix} 0 & 0 & 1 \\ x' & y' & z' \\ X & Y & Z \end{vmatrix} = x'Y - y'X = 0.$$

On en déduit les coordonnées barycentriques de P, qui sont égales à $(x'x'', y'x'', x'z'')$ (on doit traiter à part les cas où $x' = 0$ et $z'' = 0$ mais on obtient la même formule, simplifiée). De la même manière on obtient les coordonnées respectives (xy, yy'', yz) et (xz, yz, zz') de Q et R, et le fait que les trois points soient alignés est alors équivalent à la nullité du déterminant

$$\begin{vmatrix} x'x'' & y'x'' & x'z'' \\ xy'' & yy'' & yz'' \\ xz' & zy' & zz' \end{vmatrix}.$$

Or en développant les deux déterminants, on voit qu'ils sont opposés. Donc leur nullité est équivalente, ce qui prouve le théorème de Pascal. □

Application 3.3 On fixe un triangle (ABC), supposé non plat, et deux points M et N distincts et ailleurs que sur les côtés du triangle. On note M_A le point d'intersection des droites (AM) et (BC), et M_B, M_C, N_A, N_B et N_C les points analogues (voir figure 3.2). Alors ces six points sont sur une même conique.

Démonstration. On définit A' comme étant l'intersection de (M_BN_C) et (N_BM_C), et B' et C' de façon analogue. D'après le théorème de Pascal, montrer le résultat est équivalent à montrer que A', B' et C' sont alignés. On va montrer qu'ils sont sur la droite (MN). On se place dans le repère barycentrique (A, B, C), et on note (x, y, z) et (x', y', z') les coordonnées respectives de M et N. Ainsi, on veut montrer que les points A', B' et C' sont sur la droite d'équation

$$\begin{vmatrix} x & y & z \\ x' & y' & z' \\ X & Y & Z \end{vmatrix} = 0.$$

On étudie le cas de A', les autres se traitant de même. Le point M_B est sur les droites (BM) et (AC). Il vérifie donc les équations

$$\begin{cases} \begin{vmatrix} 0 & 1 & 0 \\ x & y & z \\ X & Y & Z \end{vmatrix} = zX - Zx = 0 \\ \\ \begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ X & Y & Z \end{vmatrix} = -Y = 0 \end{cases}$$

Ainsi, si $x = 0$, $X = 0$ et donc $Z \neq 0$, donc les coordonnées de M_B sont $(0, 0, z)$, et si $x = 0$, $Z = X\dfrac{z}{x}$ et donc en prenant $X = x$, les coordonnées de M_B sont $(x, 0, z)$, formule qui est donc valable que x soit nul ou pas. De la même manière, on obtient les jeux de coordonnées suivants :

- M_C : $(x, y, 0)$,
- N_B : $(x', 0, z')$,
- N_C : $(x', y', 0)$.

On veut montrer que A' est sur la droite (MN), c'est-à-dire que les trois droites (M_BN_C), (M_CN_B) et (MN) sont concourantes. Pour cela il faut montrer que le système linéaire formé de leurs trois équations n'est pas de Cramer, à savoir que le déterminant des vecteurs formés par les coefficients des équations est nul. Les trois équations concernées sont

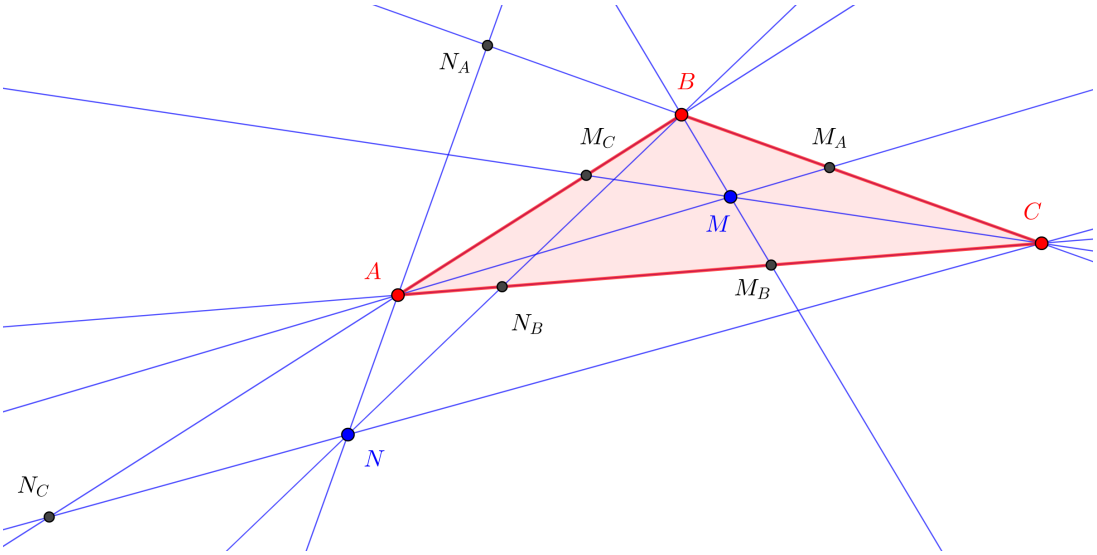
$$\begin{vmatrix} x & 0 & z \\ x' & y' & 0 \\ X & Y & Z \end{vmatrix} = 0, \quad \begin{vmatrix} x & y & 0 \\ x' & 0 & y' \\ X & Y & Z \end{vmatrix} = 0, \quad \begin{vmatrix} x & y & z \\ x' & y' & z' \\ X & Y & Z \end{vmatrix} = 0.$$

Il faut donc montrer que l'on a

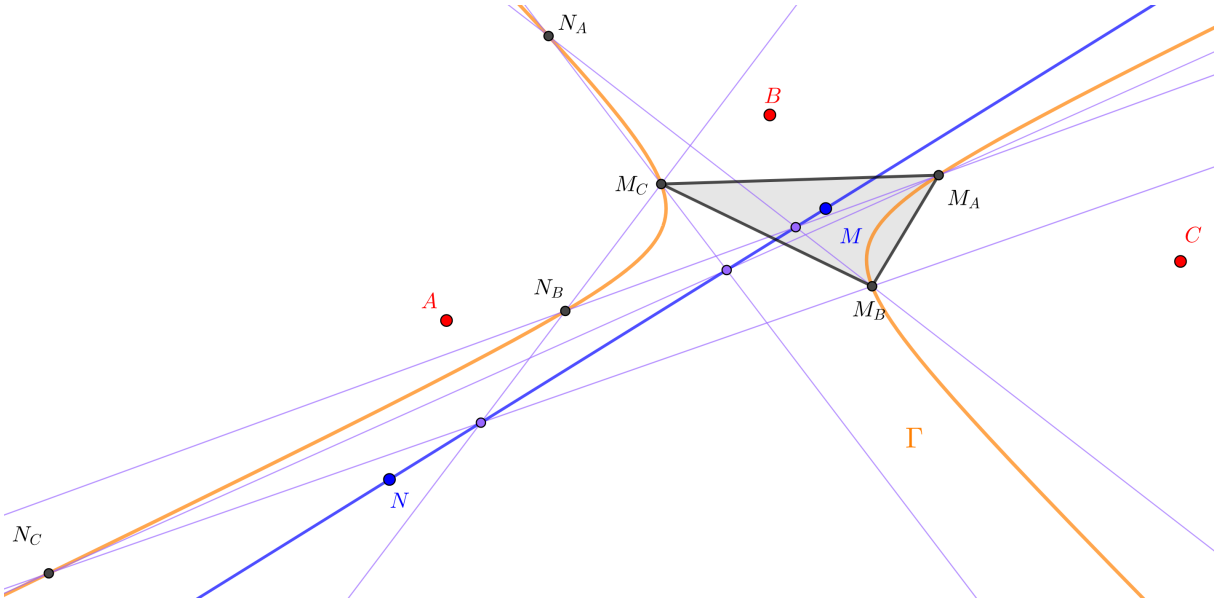
$$\begin{vmatrix} -y'z & x'z & xy' \\ yz' & -xz' & -x'y \\ yz' - y'z & x'z - xz' & xy' - x'y \end{vmatrix} = 0.$$

Or ceci est évident puisque la somme des deux premières lignes est la dernière.

Finalement, A' est sur la droite (MN), et le même raisonnement montre que c'est aussi le cas de B' et C'. Le théorème de Pascal justifie alors l'existence d'une conique Γ sur laquelle on trouve les six points M_A, M_B, M_C, N_A, N_B et N_C. □



(a) Triangle initial



(b) Théorème de Pascal pour les points M_A, M_B, M_C, N_A, N_B et N_C

Figure 3.2 – Illustration de l'application 3.3

4 Décomposition de Dunford et application

Leçons 153, 154, 155, 156, 157

Ref : [Gou09] IV.4 Th2, [BMP05] Exo 4.18

On se donne un $\mathbb{K}$-espace vectoriel E de dimension finie sur un corps $\mathbb{K}$ quelconque.

Théorème 4.1 (Décomposition de Dunford) Soit $u \in L(E)$ un endomorphisme dont le polynôme caractéristique χ est scindé sur $\mathbb{K}$. Il existe alors un unique couple d'endomorphismes (d, n), le premier étant diagonalisable et le second nilpotent, qui commutent, et dont la somme est u.

Démonstration. On écrit la décomposition du polynôme caractéristique de u en produit de facteurs de degré 1, comptés avec multiplicité :

$$\chi = \prod_{i=1}^{r} (X - \lambda_i)^{\alpha_i}.$$

On note de plus, pour $i \in [\![1, r]\!]$, $N_i := \ker\left((u - \lambda_i \operatorname{Id}_E)^{\alpha_i}\right)$ les sous-espaces caractéristiques.

Étape 1. Existence d'une décomposition de Dunford.

D'après le lemme des noyaux couplé au théorème de Cayley-Hamilton, on a

$$E = \bigoplus_{i=1}^{r} N_i.$$

Ainsi, il suffit de définir d et n sur chaque N_i. L'intuition suggère de prendre $d(x) = \lambda_i x$ sur N_i. On définit donc

$$\begin{cases} d_{|N_i} = d_i := \lambda_i \operatorname{Id}_{N_i} \\ n_{|N_i} = n_i := u_{|N_i} - \lambda_i \operatorname{Id}_{N_i} \end{cases}$$

Bien sûr, N_i est stable par d_i, et aussi par n_i puisque N_i est stable par u[3]. Ainsi, d_i et n_i sont des endomorphismes de N_i.

En concaténant des bases de chaque N_i, on obtient une base de E formée de vecteurs propres pour d, donc d est diagonalisable. De plus, on a $n_i^{\alpha_i} = 0$ pour tout $i \in [\![1, r]\!]$ par définition de N_i. Ainsi, si $\alpha = \max \alpha_i$, n^α s'annule sur chaque N_i, et donc sur E. Donc n est nilpotent. Reste à montrer que d et n commutent. Comme les d_i sont des homothéties, d_i et n_i commutent pour tout i, et donc d et n commutent sur tous les N_i, donc sur E.

Étape 2. Unicité de la décomposition.

On se donne une seconde décomposition $u = d' + n'$. Comme d' et n' commutent, u commute avec d' et n'. On en déduit notamment que pour $x \in N_i$, on a

$$(u - \lambda_i \operatorname{Id})^{\alpha_i}(d'(x)) = d'\left((u - \lambda_i \operatorname{Id})^{\alpha_i}(x)\right) = d'(0) = 0,$$

et donc N_i est stable par d'. Ainsi, d_i étant une homothétie sur N_i, d_i commute avec $d'_{|N_i}$ (qui est bien un endomorphisme de N_i), et donc d et d' commutent. Comme ce sont de plus deux endomorphismes diagonalisables, ils sont codiagonalisables, et donc $d - d'$ est diagonalisable.

De plus, comme $n = u - d$ et $n' = u - d'$, et comme d et d' commutent, n et n' commutent, et donc on a pour $k \in \mathbb{N}$

$$(n - n')^k = \sum_{j=0}^{k} \binom{k}{j} n^j (-n')^{k-j},$$

et donc en prenant $k \geq 2\dim(E)$, la somme s'annule, ce qui montre que $n - n'$ est nilpotent. Ainsi, $n - n' = d' - d$ est nilpotent et diagonalisable, donc nul. On en déduit l'unicité de la décomposition. □

On prend cette fois $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ (pour définir l'exponentielle d'endomorphisme).

Application 4.2 Si $u \in L(E)$, u est diagonalisable si et seulement si $\exp(u)$ l'est.

3. En tant que noyau d'un polynôme en u.

Démonstration. On note $u = d + n$ la décomposition de Dunford de u, et p l'indice de nilpotence de n. Tout d'abord, comme d est diagonalisable, $\exp(d)$ l'est (on prend une base de vecteurs propres pour d, et $\exp(d)$ agit par homothétie sur chaque droite propre, le rapport étant l'exponentielle de la valeur propre de d correspondante). Il faut donc montrer la réciproque.

Étape 1. Décomposition de Dunford de $\exp(u)$.

Montrons que la décomposition de Dunford de $\exp(u)$ est

$$\exp(u) = \exp(d) + \exp(d)n',$$

avec $n' = \exp(n) - \mathrm{Id} = \sum_{k=1}^{p-1} \frac{n^k}{k!}$. On a déjà vu que $\exp(d)$ est diagonalisable. De plus, comme d et n commutent, $\exp(d)$ et $\exp(n)$ commutent aussi, donc $\exp(d)$ et n' commutent, et $\exp(d)$ et $\exp(d)n'$ aussi. Il reste à montrer que $\exp(d)n'$ est nilpotente. Or n' est le produit de n et d'un polynôme en n, donc comme n est nilpotent, n' l'est aussi. De plus, comme $\exp(d)$ et n' commutent, $(\exp(d)n')^k = \exp(d)^k n'^k$ et donc $\exp(d)n'$ est bien nilpotent.

Étape 2. Condition suffisante de diagonalisabilité.

On suppose donc maintenant que $\exp(u)$ est diagonalisable, c'est-à-dire que $\exp(u)$ est égale à la partie diagonalisable de sa décomposition de Dunford [4]. Cela signifie que $\exp(d)n'$ est nulle, et donc que n' est nulle (car $\exp(d) \in GL(E)$), c'est-à-dire que $\exp(n) = \mathrm{Id}$. Ainsi, le polynôme $X + \cdots + \frac{X^{n-1}}{(n-1)!}$ annule n. Comme le polynôme minimal de n est X^p, on a $X^p \Big| X + \cdots + \frac{X^{n-1}}{(n-1)!}$ et donc nécessairement $p = 1$. Finalement, $n = 0$ et $u = d$ est diagonalisable. □

Pour la leçon 156, il faut clairement insister sur l'application. Pour la 154, plutôt sur la démonstration du théorème de décomposition. Pour la 153, on peut présenter cette autre version de la démonstration, qui justifie aussi que d et n sont des polynômes en u. On utilise en particulier le résultat suivant.

Proposition 4.3 Si $E = \bigoplus_{i=1}^{r} N_i$ est la décomposition de E adaptée à la décomposition en facteur irréductibles d'un polynôme annulateur P de u, les projecteurs sur les N_i parallèlement aux N_j sont des polynômes en u.

Pour démontrer cette proposition, on note $P = \prod_{i=1}^{r} P_i^{\alpha_i}$, $Q_i = \prod_{j \neq i} P_j^{\alpha_j}$, $\sum_{i=1}^{r} U_i Q_i = 1$ une relation de Bézout, et on montre que $p_i = U_i Q_i(u)$.

Finalement, on montre le théorème de Dunford.

Démonstration.

Étape 1. Existence de la décomposition de Dunford.

Comme χ annule u (théorème de Cayley-Hamilton), la proposition s'applique : on note p_i le projecteur sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$, qui est donc un polynôme en u. On pose alors

$$d := \sum_{i=1}^{r} \lambda_i p_i.$$

Au vu de sa définition, d est bien sûr diagonalisable (prendre une base propre de chaque N_i). Montrons que $n = u - d$ est nilpotent. On a

$$n = u - d = \sum_{i=1}^{r} (u - \lambda_i \,\mathrm{Id}) p_i.$$

Par propriété des projecteurs, et comme p_i commute avec $u - \lambda_j \,\mathrm{Id}$, on en déduit que pour $k \geq 0$, on a

$$n^k = \sum_{i=1}^{r} (u - \lambda_i \,\mathrm{Id})^k \circ p_i = \sum_{i=1}^{k} p_i \circ (u - \lambda_i \,\mathrm{Id})^k.$$

Donc n est nilpotent d'indice $\max \alpha_i$. Comme d et n sont des polynômes en u, ils commutent.

4. En effet, comme u est diagonalisable, $u = u + 0$ est une (et donc la seule) décomposition de Dunford de u.

Étape 2. Unicité de la décomposition.

On utilise la même preuve que dans la première démonstration, à ceci près qu'il suffit de rappeler que d et n sont des polynômes en u pour montrer que si d' et n' commutent, ils commutent avec d et n (puisqu'ils commutent avec u). □

5 Décomposition de Frobenius

Leçons 150, 153, 154(, 122, 151, 159)

Ref : [Gou09] B.2 Th1

Le théorème suivant donne une manière de réduire les endomorphisme dans n'importe quel cadre, sans avoir besoin de se placer sur un corps où les polynômes ont des racines. On peut notamment en déduire le théorème de réduction de Jordan si l'on ajoute l'hypothèse de clôture algébrique sur le corps.

On se donne donc un corps $\mathbb{K}$ et un espace vectoriel E de dimension n.

Théorème 5.1 (Réduction de Frobenius) Soit $u \in L(E)$. Il existe un unique entier $r \geq 1$, et des sous-espaces $F_1, \cdots, F_r$ de E stables par u, tels que

(i) $E = F_1 \oplus \cdots \oplus F_r$,

(ii) pour $i \in [\![1, r]\!]$, la restriction $u_i := u_{|F_i}$ est un endomorphisme cyclique sur F_i,

(iii) en notant μ_i le polynôme minimal de u_i, $\mu_{i+1} | \mu_i$, et les polynômes $\mu_1, \cdots, \mu_r$ ne dépendent que de u, et pas des sous-espaces F_i.

On dit que les μ_i sont les *invariants de similitude* de u.

Démonstration.

Étape 1. Supplémentaire du plus grand espace sur lequel u est cyclique.

On note $k > 0$ le degré du polynôme minimal μ de u, et on se donne $x \in E$ tel que $\mu_{u,x} = \mu$. Alors le sous-espace $F := E_{u,x} = \{P(u)(x),\ P \in \mathbb{K}[X]\}$ est de dimension k, et est bien sûr stable par u. De plus, la famille $(e_1, \cdots, e_k) = (x, u(x), \cdots, u^{k-1}(x))$ forme une base de F. On complète cette famille en une base $(e_1, \cdots, e_n)$ de E, et on note $(e_1^*, \cdots, e_n^*)$ sa base duale. On définit la partie $\Gamma := \left\{ {}^t u^i(e_k^*),\ i \in \mathbb{N} \right\}$, et on fixe le sous-espace $G = \Gamma^0$ de E. C'est l'ensemble des vecteurs tels que la k-ième coordonnée de $u^i(x)$ (dans la base $(e_j)_{1 \leq j \leq n}$) est nulle pour tout i. En particulier, c'est un sous-espace stable par u.

Montrons que G est un supplémentaire de F dans E. Soit $y = \sum_{i=1}^{p} a_i e_i$ un vecteur de $F \cap G$, en ayant choisi p de manière à ce que ce soit le plus grand parmis les indices des coefficients non nuls de y dans la base $(e_j)_{1 \leq j \leq n}$. Comme $y \in F$, $p \leq k$. On a de plus

$$0 = {}^t u^{k-p}(e_k^*)(y) = e_k^*(a_1 e_{k-p+1} + \cdots + a_p e_k) = a_p,$$

où la première égalité est due au fait que $y \in G$. Ceci est bien sûr absurde si $y \neq 0$. Donc F et G sont en somme directe. De plus, on a

$$\dim(G) = \dim(E) - \dim(\mathrm{Vect}(\Gamma)).$$

On doit donc montrer que $\mathrm{Vect}\,\Gamma$ est de dimension k. On considère pour cela l'application

$$\varphi : \left| \begin{array}{ccc} \mathbb{K}[u] & \longrightarrow & \mathrm{Vect}(\Gamma) \\ v & \longmapsto & {}^t v(e_k^*) \end{array} \right.$$

Par défition de $\mathrm{Vect}(\Gamma)$, φ est surjective. Soit $v = \sum_{i=1}^{p} a_i u^i \in \mathbb{K}[u]$, avec $p \leq k$ et maximal parmi les indices dont le coefficient a_i est non nul, tel que $\varphi(g) = 0$. Alors

$$0 = \varphi(v)(u^{k-p}(x)) = e_k^*(a_1 e_{k-p+1} + \cdots + a_p e_k) = a_p,$$

ce qui est une nouvelle fois absurde si $v \neq 0$. Donc φ est injective. Donc $\mathrm{Vect}(\Gamma)$ est de même dimension que $\mathbb{K}[u]$, c'est-à-dire k. Finalement, F et G sont tous les deux stables par u et sont supplémentaires l'un de l'autre.

Étape 2. Existence des invariants de similitude par récurrence finie.

On note μ_1 le polynôme minimal de $u_{|F}$, et P_1 le polynôme minimal de $u_{|G}$. Tout d'abord, $\mu_1 = \mu_{u,x}$ par construction, et donc en fait c'est le polynôme minimal de u. De plus, comme G est u-stable, $u_{|G} \in L(G)$ et les polynômes en $u_{|G}$ sont bien définis ; on observe alors que $\mu_1(u_{|G}) = 0$, et donc $P_1 | \mu_1$. On itère alors l'algorithme, en appliquant le raisonnement précédent à $u_{|G}$ sur G. Comme G est de dimension strictement inférieure à celle de E, l'algorithme se termine en au plus n étapes. À ce moment-là, le polynôme minimal est égal au polynôme caractéristique, et $u_{|F_r}$ est cyclique. Ainsi, E est somme directe de tous les F_i. Par construction, u est cyclique sur chaque F_i. De plus, le polynôme P_i construit à l'étape i est le polynôme minimal de $u_{|F_{i+1}}$ par construction, donc on a en fait $P_i = \mu_{i+1}$, ce qui donne (iii).

Étape 3. Unicité des invariants de similitude.

On suppose l'existence de deux familles de sous-espaces $(F_1, \cdots, F_r)$ et $(G_1, \cdots, G_s)$ vérifiant les points de l'énoncé. On note cette fois μ'_j les polynômes correspondants à la famille (G_j). Les axiomes impliquent que le premier polynôme des deux familles est le polynôme minimal de u : en effet, si P est un polynôme annulateur de u, en particulier P annule u_1, donc μ_1 et μ'_1 divisent P ; de plus, si $i \in [\![1, r]\!]$ (resp $j \in [\![1, s]\!]$), μ_i divise μ_1 (resp. μ'_j divise μ'_1) donc μ_1 (resp. μ'_1) annule $u_{|F_i}$ (resp. $u_{|G_j}$). Donc $\mu_1 = \mu = \mu'_1$.

Supposons maintenant que les familles $(\mu_i)_{1\leq i\leq r}$ et $(\mu'_j)_{1\leq j\leq s}$ sont distinctes. Alors, comme par (i) et (ii), on a

$$\sum_{i=1}^{r} \deg(\mu_i) = n = \sum_{j=1}^{s} \deg(\mu'_j),$$

il existe des indices $i > 1$ tels que $\mu_i \neq \mu'_i$, et on choisit le plus petit d'entre eux. Comme μ_j divise μ_i pour $j \geq i$, on a par (ii)

$$\mu_i(u)(E) = \mu_i(u)(F_1) \oplus \cdots \oplus \mu_i(u)(F_{i-1}).$$

On a aussi

$$\mu_i(u)(E) = \mu_i(u)(G_1) \oplus \cdots \oplus \mu_i(u)(G_s).$$

On se donne, pour $j \leq i$, des bases B_j et B'_j adaptées à la cyclicité de $u_{|F_j}$ et $u_{|G_j}$, et on en déduit que ces deux endomorphismes sont semblables. Donc $\mu_i(u_{|F_j})$ et $\mu_i(u_{|G_j})$ sont semblables, et on en déduit que $\mu_i(u)(F_j)$ et $\mu_i(u)(G_j)$ sont de même dimension. En passant à la dimension dans les deux expressions de $\mu_i(u)(E)$, on en déduit que $\mu_i(u)(G_j)$ est réduit à $\{0\}$ pour $j \in [\![i, s]\!]$, et donc en particulier, en prenant $j = i$, on obtient que $\mu'_i|\mu_i$. Par symétrie de rôle, on obtient aussi que $\mu_i|\mu'_i$. Mais comme ces deux polynômes sont unitaires, on en déduit qu'ils sont égaux, ce qui est absurde. Finalement les deux familles sont bien les mêmes. □

Le forme de Frobenius de u est alors la matrice de u dans une base adaptée à la cyclicité de u sur chacun des F_i, formée de matrices compagnons pour les P_i.

Si le temps le permet, il peut être intéressant d'ajouter la démonstration de lemme suivant.

Lemme 5.2 Il existe $x \in E$ tel que $\mu = \mu_{u,x}$.

Démonstration.

Étape 1. Propriétés des espaces $E_{u,x}$ et des polynômes $\mu_{u,x}$.

On montre deux résultats sur les espaces $E_{u,x} := \{P(u)(x),\ P \in \mathbb{K}[X]\}$. On se donne pour cela $x, y \in E$.

– Supposons que $E_{u,x} \cap E_{u,y} = \{0\}$. Comme $\mu_{u,x+y}(u)(x + y) = 0$, on a

$$\mu_{u,x+y}(u)(x) = -\mu_{u,x+y}(u)(y).$$

Ces deux éléments sont respectivement dans $E_{u,x}$ et $E_{u,y}$, donc nuls. Donc $\mu_{u,x}$ et $\mu_{u,y}$ divisent $\mu_{u,x+y}$. Comme on a aussi

$$\operatorname{ppcm}(\mu_{u,x}, \mu_{u,y})(u)(x + y) = \operatorname{ppcm}(\mu_{u,x}, \mu_{u,y})(u)(x) + \operatorname{ppcm}(\mu_{u,x}, \mu_{u,y})(u)(y) = 0,$$

on en déduit que $\mu_{u,x+y} = \operatorname{ppcm}(\mu_{u,x}, \mu_{u,y})$.

– Supposons que $\mu_{u,x}$ et $\mu_{u,y}$ sont premiers entre eux. On se donne $z \in E_{u,x} \cap E_{u,y}$. Alors $z = P(u)(x) = Q(u)(y)$, avec $P, Q \in \mathbb{K}[X]$. On a alors

$$0 = P(u) \circ \mu_{u,x}(u)(x) = \mu_{u,x}(u) \circ P(u)(x) = \mu_{u,x}(u)(z) = (\mu_{u,x}Q)(u)(y).$$

Donc $\mu_{u,y}|\mu_{u,x}Q$, et donc d'après le lemme de Gauß, $\mu_{u,y}|Q$. On en déduit que z est nul, donc $E_{u,x}$ et $E_{u,y}$ sont en somme directe. De plus, on en déduit aussi que $\mu_{u,x+y} = \mu_{u,x}\mu_{u,y}$, et donc

$$\dim(E_{u,x+y}) = \deg(\mu_{u,x+y}) = \deg(\mu_{u,x}) + \deg(\mu_{u,y}) = \dim(E_{u,x}) + \dim(E_{u,y}).$$

De plus, si $U\mu_{u,x} + V\mu_{u,y} = 1$, on a pour tout $z = P(u)(x + y) \in E_{u,x+y}$

$$z = (PU\mu_{u,x})(u)(x + y) + (PV\mu_{u,y})(u)(x + y) = (PU\mu_{u,x})(u)(y) + (PV\mu_{u,y})(u)(x) \in E_{u,x} + E_{u,y}.$$

On a finalement montré que $E_{u,x+y} \subset E_{u,x} \oplus E_{u,y}$, et donc par égalité de dimension $E_{u,x+y} = E_{u,x} \oplus E_{u,y}$.

Étape 2. Cas des facteurs du polynôme minimal.

Soit P un facteur irréductible de μ et α sa multiplicité : $\mu = P^\alpha Q$, avec Q premier avec P et donc P^α. Grâce au lemme des noyaux, on a donc

$$E = \ker(P^\alpha(u)) \oplus \ker(Q(u)).$$

Soit $x \in \ker(P^\alpha(u))$. Alors $\mu_{u,x} | P^\alpha$, donc (comme P est irréductible) il existe $\beta_x \leq \alpha$ tel que $\mu_{u,x} = P^{\beta_x}$. On cherche $x \in \ker(P^\alpha(u))$ tel que $\beta_x = \alpha$. Supposons qu'un tel x n'existe pas, et donc que pour tout $x \in \ker(P^\alpha(u))$, $P^{\alpha-1}(u)(x) = 0$, c'est-à-dire que $\ker(P^{\alpha-1}(u)) = \ker(P^\alpha(u))$. Alors en appliquant le lemme des noyaux dans l'autre sens, on obtient que $P^{\alpha-1}Q$ annule u, ce qui contredit la minimalité de μ. Donc il existe $x \in \ker(P^\alpha(u))$ tel que $\mu_{u,x} = P^\alpha$.

On note maintenant $\mu = \prod_{i=1}^{k} P_i^{\alpha_i}$ la décomposition de μ en produit d'irréductibles, et x_i un vecteur de $\ker(P_i^{\alpha_i}(u))$ tel que $\mu_{u,x_i} = P_i^{\alpha_i}$. Alors en appliquant $k-1$ fois la première étape, on en déduit que $E_{u,x_1+\cdots+x_k} = E_{u,x_1} \oplus \cdots \oplus E_{u,x_k} =$ et donc

$$\mu_{u,x_1+\cdots+x_k} = \prod_{i=1}^{k} P_i^{\alpha_i} = \mu.$$

□

6 Décomposition polaire et applications

Leçons 106, 155, 158, 160(, 150)

Ref : [CG13] VI.1+[FGN09c] 2.28

Ce développement consiste à démontrer le théorème analogue à celui de décomposition polaire dans $\mathbb{C}$: on sait bien sûr que tout élément de $\mathbb{C}^*$ s'écrit de manière unique sous la forme $z = \rho e^{i\theta}$, pour $\rho \in \mathbb{R}_+^*$ et $\theta \in [0, 2\pi)$. On va donc démontrer le théorème suivant, en se plaçant cette fois dans $\mathcal{M}_n(\mathbb{C})$. On note ici $H_n = H_n(\mathbb{C})$ l'espace des matrices hermitiennes de $\mathcal{M}_n(\mathbb{C})$, $H_n^{++} = H_n^{++}(\mathbb{C})$ son sous-espace des matrices définies positives, et $U_n = U_n(\mathbb{C})$ l'espace des matrices unitaires de $\mathcal{M}_n(\mathbb{C})$.

On peut adapter ce développement pour qu'il rentre plus dans le cadre des leçons dans lesquelles on veut le présenter. Par exemple, il est plus judicieux de présenter le théorème et la démonstration (qui est la même) sous leur forme réelle dans le cadre de la leçon 160. De plus, les deux corollaires présentés en fin de développements sont deux applications dont les démonstrations prennent des durées différentes, ce qui permet de moduler en fonction du temps restant à l'issu de la démonstration du théorème de décomposition polaire. Enfin, si l'on n'a pas d'autre idée de développement pour la leçon 150, on peut toujours l'y faire figurer, en donnant l'énoncé sous la forme "action de groupes" : le théorème montre que les éléments de $H_n^{++}(\mathbb{C})$ (resp. $S_n^{++}(\mathbb{R})$) caractérisent les orbites de l'action à droite (resp. à gauche) de $U_n(\mathbb{C})$ (resp. $O_n(\mathbb{R})$) sur $GL_n(\mathbb{C})$ (resp. $GL_n(\mathbb{R})$).

Théorème 6.1 L'application

$$\Phi : \left| \begin{array}{ccc} H_n^{++} \times U_n & \longrightarrow & GL_n(\mathbb{C}) \\ (H, Q) & \longmapsto & HQ \end{array} \right.$$

est un homéomorphisme. En particulier, tout élément M de $GL_n(\mathbb{C})$ s'écrit donc de manière unique sous la forme

$$M = R \exp(i\Theta),$$

avec $R \in H_n^{++}$ et $\Theta \in H_n$.

Démonstration. Étape 1. Surjectivité de Φ.

On se donne $M \in GL_n(\mathbb{C})$. On remarque tout d'abord que MM^* est hermitienne définie positive. En effet, on a

- $(MM^*)^* = M^{**}M^* = MM^*$
- si X est un vecteur non nul de $\mathbb{C}^n$, alors $\langle MM^*X, X\rangle = \langle M^*X, M^*X\rangle = \|M^*X\|^2 > 0$, car M^* est inversible.

Ainsi, d'après le théorème spectral, il existe une matrice unitaire $U \in U_n$ qui diagonalise MM^*, c'est à dire qu'il existe des réels $d_1, .., d_n$ tous strictement positifs tels que

$$MM^* = U^*DU,$$

avec $D = \mathrm{diag}(d_i)_{1\leq i\leq n}$. On note alors $\sqrt{D} := \mathrm{diag}(\sqrt{d_i})_{1\leq i\leq n}$, et on pose

$$H := U^*\sqrt{D}U.$$

On voit alors que puisque U est unitaire, $H^2 = MM^*$. On pose alors $Q := H^{-1}M$, de sorte que l'on a $HQ = M$. Comme on a $H^* = H$, H est hermitienne. De plus, ses valeurs propres sont des réels strictement positifs (les $\sqrt{d_i}$), donc elle est définie positive. On a également $Q^*Q = M^*H^{-2}M = I_n$, donc Q est unitaire. On en déduit que $M = \Phi(H, Q)$.

Étape 2. Injectivité de Φ.

On se donne une seconde décomposition $M = H'Q'$ de M dans $H_n^{++}\times U_n$. On a alors

$$M^* = (H'Q')^* = Q'^*H'^* = Q'^{-1}H'.$$

On en déduit que $MM^* = H'^2$. Or on a déjà vu que $MM^* = H^2$. On se donne un polynôme $P \in \mathbb{R}[X]$ qui interpole les d_i sur les $\sqrt{d_i}$. On a alors $H = U^*P(D)U = P(U^*DU) = P(MM^*) = P(H'^2)$. Donc H est un polynôme en H', et donc H et H' commutent. Mais comme elles sont toutes les deux diagonalisables (d'après le théorème spectral), elles sont codiagonalisables. Il existe donc deux familles $(h_i)_{1\leq i\leq n}$ et $(h'_i)_{1\leq i\leq n}$ de réels strictement positifs et une matrice $R \in GL_n(\mathbb{C})$ telles que

$$\left\{ \begin{array}{l} H = R^{-1}\mathrm{diag}(h_i)R \\ H' = R^{-1}\mathrm{diag}(h'_i)R \end{array} \right.$$

Mais comme $H^2 = H'^2$, on doit donc avoir $h_i^2 = h_i'^2$ pour tout i, et donc $h_i = h_i'$ puisque ces coefficients sont des réels positifs. Finalement, on obtient $H = H'$. On en déduit également $Q = Q'$. Donc Φ est injective.

Étape 3. Continuité de Φ^{-1}.

Puisque le produit matriciel est continu, Φ l'est. Il reste à montrer que Φ^{-1} l'est aussi. Puisque l'on se trouve dans des espaces métriques, on va montrer qu'elle est séquentiellement continue. On se donne donc une suite $(M_k)_{k\in\mathbb{N}}$, qui converge dans $GL_n(\mathbb{C})$ vers M. On note également pour tout k

$$M_k = H_k Q_k$$

la décomposition polaire de M_k, et de même $M = HQ$. On sait que l'espace U_n est compact, car fermé et borné (et $\mathcal{M}_n(\mathbb{C})$ est de dimension finie). Donc la suite $(Q_k)_{k\in\mathbb{N}}$ admet une valeur d'adhérence, que l'on note A. Il existe donc une extractrice φ telle que la suite $(Q_{\varphi(k)})_{k\in\mathbb{N}}$ converge vers A. Par continuité du produit matriciel, la suite $(H_{\varphi(k)})_{k\ni\mathbb{N}}$ converge alors vers $S := MA^*$. Comme l'espace H_n^+ des matrices semi-définies positives est fermé, et S est limite d'une suite d'éléments de $H_n^{++} \subset H_n^+$, elle est semi-définie positive, et elle est aussi inversible puisque M et A^* le sont, donc elle est finalement définie positive. Donc SA est une décomposition polaire de M. Ainsi, par unicité, on a $S = H$ et $A = Q$. Ainsi, la valeur d'adhérence est unique, ce qui prouve que la suite $(Q_k)_{k\in\mathbb{N}}$ converge vers Q, et donc $(H_k)_{k\in\mathbb{N}}$ vers H. □

Exemple. On prend $M = \begin{pmatrix} 1+\mathrm{i}\sqrt{2} & 0 \\ 0 & \mathrm{i} \end{pmatrix}$. On a alors

$$M = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mathrm{e}^{\mathrm{i}\frac{\pi}{3}} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\frac{\pi}{2}} \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \exp\left(\mathrm{i} \begin{pmatrix} \frac{\pi}{3} & 0 \\ 0 & \frac{\pi}{2} \end{pmatrix} \right),$$

ce qui donne une décomposition polaire de M sous la forme $M = H \exp \mathrm{i}\Theta$.

La version réelle du théorème est aussi valable.

Théorème 6.2 L'application

$$\Phi : \left| \begin{array}{ccc} S_n^{++}(\mathbb{R}) \times O_n(\mathbb{R}) & \longrightarrow & GL_n(\mathbb{R}) \\ (S, O) & \longmapsto & OS \end{array} \right.$$

est un homéomorphisme.

Corollaire 6.3 Si $A \in GL_n(\mathbb{R})$, alors $|||A|||_2 = \sqrt{\rho\,({}^tAA)}$.

Démonstration. Soit $A = OS \in GL_n(\mathbb{R})$. Alors comme $O \in O_n(\mathbb{R})$, on a $\|Ax\| = \|Sx\|$ pour tout vecteur $x \in \mathbb{R}^n$. On a donc $|||A|||_2 = |||S|||_2$. Comme S est symétrique réelle, elle est diagonalisable dans une base orthonormée $(e_1, .., e_n)$ de $\mathbb{R}^n$, composée de vecteurs propres pour les valeurs correspondantes, qui sont positives strictement, $\lambda_1 \geq .. \geq \lambda_n > 0$. Soit alors $x = \sum_{i=1}^{n} x_i e_i$ de norme 1, on a

$$\|Sx\|^2 \leq \left\| \sum_{i=1}^{n} \lambda_i x_i e_i \right\|^2 \leq |\lambda_1|^2 \|x\|^2 = |\lambda_1|.$$

De plus, le cas d'égalité est atteint pour $x = e_1$. Donc $|||S|||_2 = \rho(s)$. On en déduit :

$$|||A|||_2 = |||S|||_2 = \rho(S) = \sqrt{\lambda_1^2} = \sqrt{\rho(S^2)} = \sqrt{\rho({}^tAA)}$$

car ${}^tAA = {}^t S {}^tOOS = S^2$. □

Corollaire 6.4 Les points extrêmaux de la boule unité de $\mathcal{M}_n(\mathbb{C})$ sont exactement les éléments de $U_n(\mathbb{C})$.

Démonstration.

– Montrons que $Q \in U_n(\mathbb{C})$ est extrêmal. Supposons que $Q = A + B$, avec A, B deux éléments de norme inférieure à 1. On a pour $x \in E$ unitaire

$$\|x\| = \|Qx\| = \frac{1}{2}\|Ax + Bx\| \leq \frac{1}{2}\left(\|Ax\| + \|Bx\|\right) \leq \frac{1}{2}\left(|||A||| + |||B|||\right) \leq 1.$$

Comme x est de norme 1, toutes les inégalités sont des égalités. On en déduit que A et B sont de norme 1, que Ax et Bx sont de norme 1, et qu'ils sont positivement liés. Ainsi, on a nécessairement $Ax = Bx$, et donc $A = B$ car ceci est vrai pour tout vecteur unitaire. Donc Q est extrêmal.

– Réciproquement, si A est de norme inférieure à 1 et non unitaire, on écrit $A = HQ$ la décomposition polaire de A (ici, H est seulement semi-définie positive). Comme H est hermitienne, elle est orthodiagonalisable : il existe $P \in U_n(\mathbb{C})$ et D diagonale à coefficients réels telles que $H = P^*DP$. Comme $|||H||| = |||A|||$, les coefficients diagonaux λ_i sont tous compris entre -1 et 1. De plus, comme A n'est pas unitaire, au moins l'un des λ_i (supposons que c'est λ_1) est strictement compris entre -1 et 1. On pose alors $\lambda_1 = \dfrac{\alpha+\beta}{2}$ avec $\alpha \neq \beta \in [-1, 1]$, et on note $D' = \mathrm{diag}(\alpha, \lambda_2, ..\lambda_n)$ et $D'' = \mathrm{diag}(\beta, \lambda_2, ..\lambda_n)$. Alors $A = \dfrac{1}{2}\left(P^*D'PQ + P^*D''PQ\right)$. On a de plus, pour x unitaire

$$\|P^*D'PQx\|^2 = \|D'PQx\|^2 \leq |||D'|||^2 \|PQx\|^2 \leq 1,$$

donc $P^*D'PQ$ est dans la boule unité, ainsi que $P^*D''PQ$. Donc A est combinaison convexe de deux éléments de la boule, et n'est donc pas extrêmal.

□

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

Leçons 123, 125, 141, 142, 144, 190

Ref : [Goz09] Lemme VII.26, Th VII.27, Déf VII.33

Le but de ce développement est de donner une idée du nombre de polynômes irréductibles unitaires sur les corps finis. On introduit pour cela la fonction de Möbius, dont on va donner quelques propriétés, avant de s'intéresser à la structure des polynômes sur les corps finis.

Il faut moduler ce développement en fonction de la leçon. Pour les leçons 141, 142 et 144, on peut admettre le théorème d'inversion et parler presque uniquement de polynômes, de racines et de pgcd. Pour la 190 au contraire, il faut absolument passer du temps sur Möbius. Pour les leçons sur les corps, on peut passer du temps sur les deux dernières étapes de la démonstration, et et choisir ce que l'on préfère entre le lemme d'arithmétique et les propriétés de Möbius qui sont décrites ci-dessous.

On se place dans la $\mathbb{C}$-algèbre [5] $\mathcal{S} = \mathbb{C}^{\mathbb{N}^*}$, où le produit interne est défini par

$$u * v(n) := \sum_{d|n} u\left(\frac{n}{d}\right) v(d) = \sum_{d|n} u(d) v\left(\frac{n}{d}\right).$$

C'est une algèbre commutative unitaire, dont le neutre est $\chi = \delta_1$.

Définition 7.1 On définit la fonction de Möbius μ par les axiomes suivants

(i) $\mu(1) = 1$,

(ii) si les p_i sont deux à deux distincts, $\mu(p_1 \cdots p_k) = (-1)^k$,

(iii) si n a un facteur carré, $\mu(n) = 0$.

Alors μ est l'inverse dans $\mathcal{S}$ de la fonction $\mathbb{1}$ constante égale à 1.

Démonstration. Comme le produit est commutatif, il suffit de montrer $\mu * \mathbb{1} = \chi$. Tout d'abord, l'axiome (i) justifie le calcul suivant :

$$\mu * \mathbb{1}(1) = \mu(1)\mathbb{1}(1) = 1 = \chi(1).$$

On doit maintenant montrer que si $n > 1$, $\mu * \mathbb{1}(n) = 0$. Soit $p \in \mathfrak{P}$ et $k \in \mathbb{N}^*$. On a grâce aux trois axiomes

$$\mu * \mathbb{1}(p^k) = \sum_{d|p^k} \mu(d) = \sum_{i=0}^{k} \mu(p^i) = \mu(1) + \mu(p) = 0.$$

Maintenant, si $n = \prod_{j=1}^{r} p_j^{k_j}$, on a

$$\mu * \mathbb{1}(n) = \sum_{i_1 \leq k_1, .., i_r \leq k_r} \mu(p_1^{i_1} \cdots p_r^{i_r}).$$

La somme ci-dessus possède en fait 2^r termes non nuls : ce sont les termes tels que $i_j \in \{0, 1\}$ pour tout j, et qui sont donc en bijection avec $\mathcal{P}([\![1, r]\!])$. Finalement,

$$\mu * \mathbb{1}(n) = \sum_{A \in \mathcal{P}([\![1,r]\!])} (-1)^{|A|} = \sum_{l=0}^{r} \binom{r}{l} (-1)^l = 0.$$

□

On en déduit immédiatement le théorème suivant.

Théorème 7.2 (Inversion de Möbius) Soient u et v dans $\mathcal{S}$, tels que

$$u(n) = \sum_{d|n} g(d).$$

Alors on a pour tout $n \in \mathbb{N}^*$

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

5. Si on n'a pas envie de recevoir trop de questions poussées sur la notion d'algèbre, on peut juste dire que c'est un espace vectoriel avec un produit sympatique.

On en vient aux polynômes irréductibles sur le corps $\mathbb{F}_p$. On note $\mathcal{I}_n(p)$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_p$, et $I_n(p) = |\mathcal{I}_n(p)|$.

Application 7.3 Pour $n \in \mathbb{N}^*$, on a

$$I_n(p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

En particulier, $I_n(p) \sim \dfrac{p^n}{n}$.

Démonstration.

Étape 1. Un lemme dans les anneaux euclidiens.

On commence par montrer le lemme suivant.

Lemme 7.4 Soit A un anneau euclidien. On se donne $a \in A^\times$. Alors pour tout couple (m, n) d'entiers naturels non nuls, m divise n dans $\mathbb{Z}$ si et seulement si $a^m - 1$ divise $a^n - 1$ dans A.

On note $n = qm + r$ la division euclidienne de n par m. Alors on a

$$a^n - 1 = (a^{qm} - 1)a^r + a^r - 1 = (a^m - 1) \sum_{i=0}^{q-1} a^{im+r} + a^r - 1.$$

Ainsi, les diviseurs communs à $a^n - 1$ et $a^m - 1$ sont les diviseurs communs à $a^m - 1$ et $a^r - 1$. On applique alors l'algorithme d'Euclide pour calculer le pgcd de m et n. On construit alors une suite de restes $r_1, .., r_N, 0$, où r_N est donc le pgcd recherché. En itérant le raisonnement fait plus haut, on voit que $a^n - 1$ et $a^m - 1$ ont les mêmes diviseurs communs que $a^{r_N} - 1$ et $a^{r_{N+1}} - 1 = 0$. Donc le pgcd de $a^n - 1$ et $a^m - 1$ est $a^{\mathrm{pgcd}(m,n)} - 1$. Finalement, on a

$$\begin{array}{cc} & m|n \\ \iff & \mathrm{pgcd}(m,n) = m \\ \iff & a^{\mathrm{pgcd}(m,n)} - 1 = a^m - 1 \\ \iff & \mathrm{pgcd}\left(a^n - 1, a^m - 1\right) = a^m - 1 \\ \iff & a^m - 1 | a^n - 1 \end{array}$$

La seconde équivalence est vraie (son sens réciproque) car l'anneau est intègre et a non inversible.

Étape 2. Facteurs irréductibles de $X^{p^n} - X$.

On note $q = p^n$. On veut montrer le résultat suivant :

$$X^q - X = \prod_{d|n} \prod_{Q \in \mathcal{I}_d(p)} Q.$$

On applique pour cela le lemme à $A = \mathbb{Z}$, pour déduire que d divise n si et seulement si $p^d - 1$ divise $p^n - 1$, puis en réappliquant le lemme dans $A = \mathbb{F}_p[X]$, en obtient que d divise n si et seulement si $X^{p^d-1} - 1$ divise $X^{q-1} - 1$ dans $\mathbb{F}_p[X]$.

Or, si $Q \in \mathcal{I}_d(p)$ est différent de X, comme $\mathbb{F}_{p^d} = \mathbb{F}_p[X]/(Q)$, en fixant l'image α du polynôme X dans $\mathbb{F}_{p^d}$, $\alpha^{p^d-1} = 1$ (par théorème de Lagrange) donc Q divise $X^{p^d-1} - 1$, et donc $X^{q-1} - X$. Finalement, tout polynôme qui se trouve dans l'un des $\mathcal{I}_d(p)$ divise $X^q - X$. Comme tous ces polynômes sont irréductibles, ils sont premiers entre eux, donc leur produit divise aussi $X^q - X$.

On note donc

$$X^q - X = P \prod_{d|n} \prod_{Q \in \mathcal{I}_d(p)} Q.$$

On veut montrer que $P = 1$. On suppose par l'absurde que $P \neq 1$, c'est-à-dire (comme tous les polynômes considérés sont unitaires) que P est au moins de degré 1. Soit F un facteur irréductible de P, et d le degré de ce facteur. Alors $F \in \mathcal{I}_d(p)$, donc F divise $X^q - X$, et aussi $X^{p^d} - X$ (par le même raisonnement que précédemment). Donc il divise leur pgcd, que l'on note Δ. D'après le lemme, on a en notant $\delta = \mathrm{pgcd}(n, d)$

$$\Delta = X \,\mathrm{pgcd}(X^{q-1} - 1, X^{p^d-1} - 1) = X(X^{\mathrm{pgcd}(p^n-1, p^d-1)} - 1) = X^{p^\delta} - X.$$

Donc Δ est un polynôme de degré p^δ à coefficients dans $\mathbb{F}_p$, donc dans le corps de rupture $\mathbb{F}_p[X]/(F) = \mathbb{F}_{p^d}$, et il est nul dans ce corps (car divisible par F), donc il y a p^d racines. Ainsi, $p^d \leq p^\delta$, et donc $d = \delta$. Ainsi, d divise n. Finalement, $F \in \mathcal{I}_d(p)$ donc F^2 divise $X^{p^n} - X$. Ceci est absurde, puisque $X^{p^n} - X$ est sans facteur carré. Donc $P = 1$. Finalement, on a montré

$$X^q - X = \prod_{d|n} \prod_{Q \in \mathcal{I}_d(p)} Q.$$

Étape 3. Conclusion par inversion.

On passe au degré dans l'égalité précédente. On en déduit

$$p^n = \sum_{d|n} d I_d(p).$$

Il suffit alors d'utiliser le théorème d'inversion de Möbius pour conclure : on obtient

$$n I_n(p) = \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

L'équivalent se déduit immédiatement. □

8 Groupes d'isométries du tétraèdre et du cube

Leçons 101, 105, 161, 191

Ref : [CG13], XII Prop 3.12 & Prop 3.15

Ce développemment consiste à étudier les groupes d'isométries laissant stables le tétraèdre et le cube.

Si C est un ensemble de points de $\mathbb{R}^n$, on appelle groupe d'isométries de C, et on note $\mathrm{Iso}(C)$, l'ensemble des isométries affines de $\mathbb{R}^n$ laissant stable l'ensemble C. On note aussi $\mathrm{Iso}^+(C)$ l'ensemble des isométries affines positives de $\mathrm{Iso}(C)$. On appelle Δ_4 le tétraèdre régulier et C_8 le cube, qui sont deux ensembles de $\mathbb{R}^3$.

Théorème 8.1 Le groupe des isométries du tétraèdre est $\mathrm{Iso}(\Delta_4) \simeq \mathfrak{S}_4$, et le groupes des isométries positives du tétraèdre est $\mathrm{Iso}^+(\Delta_4) \simeq \mathfrak{A}_4$.

Démonstration. On note A, B, C et D les sommets du tétraèdre, comme sur la figure 8.1a. On définit le morphisme

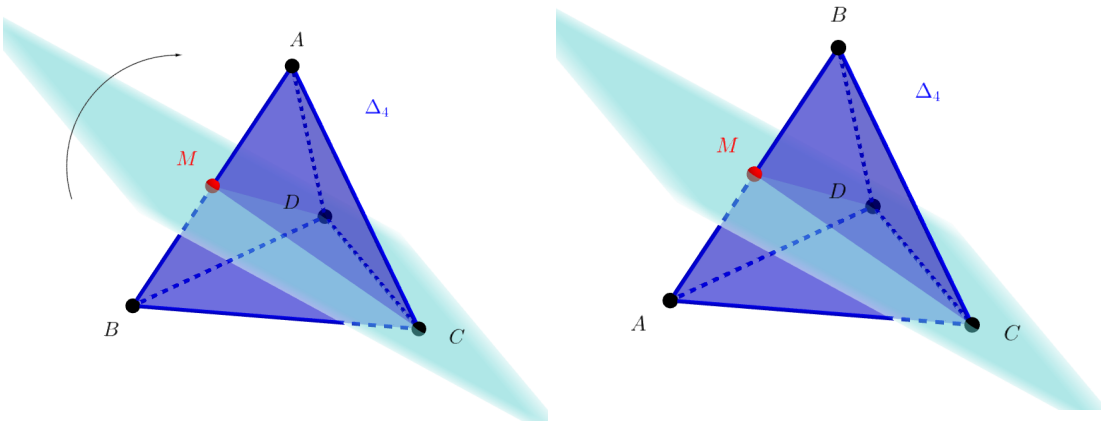
$$\varphi : \left| \begin{array}{ccc} \mathrm{Iso}(\Delta_4) & \longrightarrow & \mathfrak{S}(A,B,C,D) \simeq \mathfrak{S}_4 \\ f & \longmapsto & f_{|\{A,B,C,D\}} \end{array} \right.$$

Ce morphisme est bien défini puisque $\{A, B, C, D\}$ est par définition stable par les éléments de $\mathrm{Iso}(\Delta_4)$. On va montrer que φ est bijectif.

- On se donne f tel que $\varphi(f)$ est l'identité. Puisque les vecteurs AB, AC, et AD forment une base de $\mathbb{R}^3$, l'image de f sur cette base caractérise f, et donc f est l'identité sur $\mathbb{R}^3$. Donc φ est injectif.
- On veut maintenant montrer que φ est surjectif. On cherche tout d'abord un antécédent à la permutation $(A\ B)$. On doit trouver une isométrie qui échange A et B sans toucher à C et D. On note alors M le milieu de $[AB]$, et on considère la réflexion de plan (CDM), qui est bien une isométrie, et qui effectue exactement les déplacements recherchés. Donc $(A\ B)$ est dans l'image de φ, et par symétrie de la figure, toutes les transpositions aussi. Or les transpositions engendrent $\mathfrak{S}_4$, donc tous les éléments de $\mathfrak{S}_4$ sont dans l'image. Donc φ est surjectif.

On en déduit donc que le groupe des isométries du tétraèdre est $\mathfrak{S}_4$.

De plus, comme $SO_3(\mathbb{R})$ est d'indice 2 dans $O_3(\mathbb{R})$, et comme par symétrie centrale de Δ_4, tout élément de $\mathrm{Iso}^+(\Delta_4)$ correspond bijectivement à un élément de $\mathrm{Iso}^-(\Delta_4)$, $\mathrm{Iso}^+(\Delta_4)$ est aussi d'indice 2 dans $\mathrm{Iso}(\Delta_4)$. Or le seul sous-groupe d'indice 2 dans $\mathfrak{S}_4$ est $\mathfrak{A}_4$, donc $\mathrm{Iso}^+(\Delta_4) = \mathfrak{A}_4$.



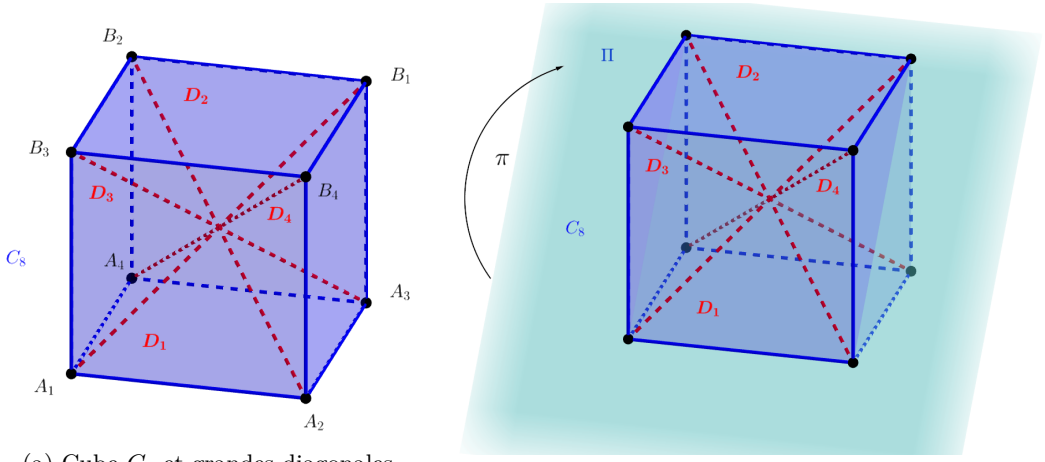
(a) Tétraèdre régulier Δ_4 et plan (CDM)

(b) Tétraèdre après transformation par la réflexion de plan (CDM)

Figure 8.1 – Tétraèdre régulier Δ_4 et isométries

□

Théorème 8.2 Le groupe des isométries du cube est $\mathrm{Iso}(C_8) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ et le groupe des isométries positives du cube est $\mathrm{Iso}^+(C_8) \simeq \mathfrak{S}_4$.



(a) Cube C_8 et grandes diagonales

(b) Cube et transformation par la rotation du plan Π

Figure 8.2 – Cube C_8 et isométries

Démonstration. On numérote les sommets du cube selon la figure 8.2a. On remarque tout d'abord que toute isométrie laissant stable le cube doit laisser stable les quatre grandes diagonales $D_i = [A_iB_i]$. En effet, comme une isométrie conserve les distances, et comme les couples (A_i, B_i) sont les couples de points les plus éloignés de C_8, l'ensemble de ces couples est stable par toute isométrie du cube. On définit alors le morphisme de groupe

$$\varphi : \left| \begin{array}{ccc} \mathrm{Iso}^+(C_8) & \longrightarrow & \mathfrak{S}(\mathcal{D}) \simeq \mathfrak{S}_4 \\ f & \longmapsto & f_{|\mathcal{D}} \end{array} \right.$$

où $\mathcal{D}$ désigne l'ensemble des couples (A_i, B_i). On va montrer que φ est un isomorphisme.

- On se donne f tel que $\varphi(f)$ est l'identité, et on suppose par l'absurde que f n'est pas l'identité. Comme f n'est pas l'identité, l'un des sommets A_i de la face du bas n'est pas stable par f (sinon, pour conserver les diagonales, f doit laisser stables tous les points du cube, et donc f est l'identité). Mais alors, $f(A_i) = B_i$ puisque l'ensemble $\{A_i, B_i\}$ est stable par f. Mais comme f conserve les distances, cela implique que pour tout $j \in [\![1, 4]\!]$, $f(A_j) = B_j$. On en déduit que f est l'opposée de l'identité, ce qui est absurde puisque cette isométrie est négative. Donc f est l'identité, et φ est injectif.
- On note maintenant Π le plan engendré par les diagonales D_1 et D_2, et on considère la rotation ρ d'angle π autour de autour de l'axe orthogonal à Π passant par le centre O du cube (qui est bien une isométrie positive). Alors, comme on le voit sur la figure 8.2b, D_1 et D_2 sont stables, mais D_3 et D_4 sont échangées. On en déduit que $\varphi(\rho) = (D_3\ D_4)$. Un raisonnement similaire sur les autres couples de diagonales successives montre que toutes les transpositions $(D_i\ D_{i+1})$ sont dans $\varphi(\mathrm{Iso}^+(C_8))$. Or ces transpositions engendrent $\mathfrak{S}(\mathcal{D})$, donc φ est surjectif.

On en déduit bien que $\mathrm{Iso}^+(C_8) \simeq \mathfrak{S}_4$.

Par le même argument que précédemment, $\mathrm{Iso}^+(C_8)$ est d'indice 2 dans $\mathrm{Iso}(C_8)$. En particulier, il est distingué. De même, le sous-groupe $\{\pm \mathrm{Id}\}$ est distingué puisque l'identité et son opposée commutent avec toutes les isométries de $\mathbb{R}^3$. De plus, l'intersection de ces deux groupes est triviale, et toute isométrie du cube est soit positive, soit opposée d'une isométrie positive. On en déduit que le groupe des isométrie du cube est le produit direct de ces deux groupes :

$$\mathrm{Iso}(C_8) = \mathrm{Iso}^+(C_8) \times \{\pm \mathrm{Id}\} \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}.$$

□

9 Isométries directes sur $\mathbb{F}_q^2$

Leçons 120, 123, 190, (104, 106, 125)

Ref : [CG13] VIII Prop 3.5

Ce développement consiste à déterminer le groupe des isométries directes sur $\mathbb{F}_q^2$.

Théorème 9.1 Soit $p \in \mathfrak{P}$ un nombre premier impair, $n \in \mathbb{N}^*$ et $q = p^n$. Alors le groupe spécial orthogonal $SO_2(\mathbb{F}_q)$ est isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$ si -1 est un carré dans $\mathbb{F}_q^*$, et à $\mathbb{Z}/(q+1)\mathbb{Z}$ sinon.

On note dans la suite $\mathbb{F}_q^{*(2)} := \left\{x^2, \quad x \in \mathbb{F}_q^*\right\}$ les carrés de $\mathbb{F}_q^*$.

Démonstration. Étape 1. Description du groupe spécial orthogonal analogue au cas réel.

On commence par décrire $SO_2(\mathbb{F}_q)$. On rappelle que les éléments A de ce groupe sont caractérisés dans $\mathcal{M}_2(\mathbb{F}_q)$ par la relation ${}^tAA = I_2$ et par le fait que leur déterminant est 1. Ainsi, on a

$$SO_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad (a,b,c,d) \in \mathbb{F}_q^4, \ ad - bc = a^2 + b^2 = c^2 + d^2 = 1, ac + bd = 0 \right\}.$$

Soit $(a,b) \in \mathbb{F}_q^2$ tel que $a^2 + b^2 = 1$. On étudie le système

$$\begin{cases} ac + bd = 0 \\ ad - bc = 1 \end{cases} \tag{S}$$

d'inconnue $(c,d) \in \mathbb{F}_q^2$. Alors (S) est équivalent à

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Mais comme la matrice $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ est inversible (car de déterminant non nul par hypothèse sur (a,b)), ce système a une unique solution, et elle est donnée par $\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} -b \\ a \end{pmatrix}$. On a alors également $c^2 + d^2 = 1$. Réciproquement, si une matrice est de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ avec $a^2 + b^2 = 1$, alors on vérifie que c'est un élément de $SO_2(\mathbb{R})$. L'application

$$\Phi : \left| \begin{array}{ccc} \mathbb{S}^1(\mathbb{F}_q) & \longrightarrow & SO_2(\mathbb{F}_q) \\ \begin{pmatrix} a \\ b \end{pmatrix} & \longmapsto & \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \end{array} \right. ,$$

où $\mathbb{S}^1(\mathbb{F}_q)$ désigne la sphère unité de $\mathbb{F}_q$, est donc une bijection.

Étape 2. Cas où -1 est un carré dans $\mathbb{F}_q^*$.

On se donne $\omega \in \mathbb{F}_q^*$ tel que $\omega^2 = -1$, et $(a,b) \in \mathbb{F}_q^2$. On a alors

$$(a,b) \in \mathbb{S}^1(\mathbb{F}_q) \iff a^2 + b^2 = 1 \iff (a + b\omega)(a - b\omega) = 1.$$

On effectue alors le changement de variable

$$\begin{cases} x = a + b\omega \\ y = a - b\omega \end{cases},$$

qui est licite puisque le changement de variable inverse est donné par

$$\begin{cases} a = \dfrac{x+y}{2} \\ b = \dfrac{x-y}{2\omega} \end{cases},$$

où ω et 2 sont bien inversibles dans $\mathbb{F}_q$ (on est en caractéristique différente de 2). On a donc

$$(a,b) \in \mathbb{S}^1(\mathbb{F}_q) \iff xy = 1.$$

Comme les ensembles considérés sont tous finis et en bijection, on a

$$|SO_2(\mathbb{F}_q)| = \left|\mathbb{S}^1(\mathbb{F}_q)\right| = \left|\left\{(x,y) \in \mathbb{F}_q^2, \quad xy = 1\right\}\right| = q-1,$$

où la dernière égalité vient du fait que l'on peut choisir x quelconque dans $\mathbb{F}_q^*$ et que y est alors fixé ($y = x^{-1}$).

On pose alors

$$\varphi : \left| \begin{array}{ccc} SO_2(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_q^* \\ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} & \longmapsto & a + b\omega \end{array} \right. .$$

On peut vérifier que φ est un morphisme de groupes. De plus, si $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ est dans le noyau de φ, alors $a + b\omega = 1$, et donc $a - b\omega = \dfrac{a^2+b^2}{a+b\omega} = 1$, ce qui montre que $a = 1$ et $b = 0$, et donc que A est l'identité. Ainsi, φ est injectif. Il est donc bijectif puisque les cardinaux des deux groupes sont les mêmes. Ainsi, c'est un isomorphisme. Comme $\mathbb{F}_q^*$ est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$ [6], on en déduit le théorème dans le cas où -1 est un carré dans $\mathbb{F}_q^*$.

Étape 3. Cas où -1 n'est pas un carré dans $\mathbb{F}_q^*$.

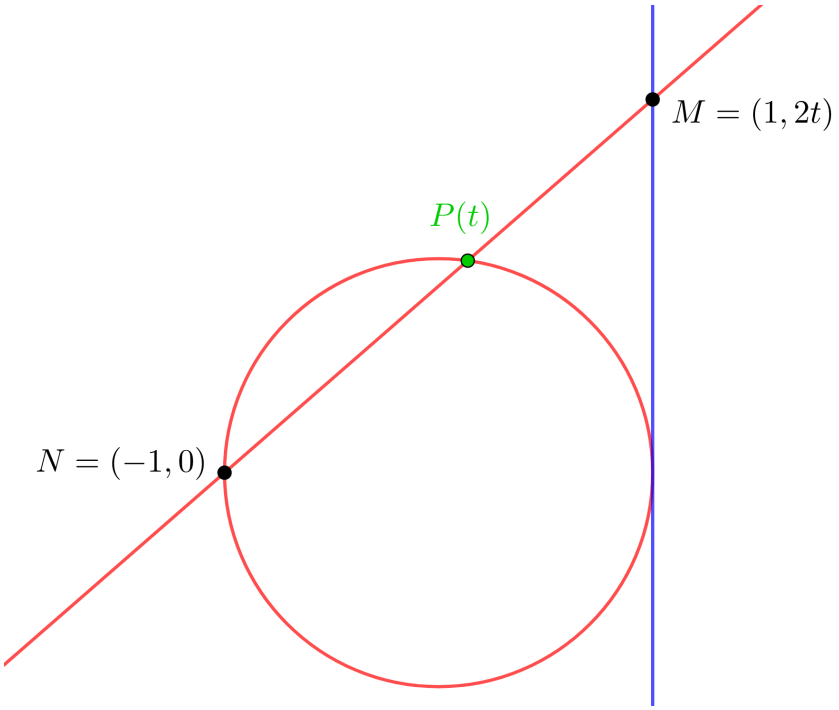


Figure 9.1 – Projection stéréographique de $\mathbb{S}^1(\mathbb{R})$

On utilise ici la projection stéréographique du cercle sur la droite $x = 1$ (voir figure 9.1 pour la situation analogue dans le cas du corps des réels). Notons $N = (-1, 0) \in \mathbb{F}_q^2$, et $M = (1, 2t) \in \mathbb{F}_q$ pour un certain $t \in \mathbb{F}_q$. Alors la droite (NM) coupe le cercle unité en N et en un second point $P(t)$. En effet, la droite a pour équation $y = t(x+1)$ dans le plan $\mathbb{F}_q^2$ [7], et le cercle a pour équation $x^2 + y^2 = 1$. Ainsi, l'équation de leur intersection est

$$\left\{ \begin{array}{l} y = t(x+1) \\ x^2(1+t^2) + 2t^2x + (t^2-1) = 0 \end{array} \right. .$$

Comme -1 n'est pas un carré dans $\mathbb{F}_q^*$, la seconde équation, celle qui détermine x, est de degré 2 en x. Le calcul du discriminant montre qu'elle admet deux solutions, $x = -1$ et $x = \dfrac{1-t^2}{1+t^2}$. Le premier cas

6. Le groupe multiplicatif d'un corps fini est toujours cyclique.

7. On écrit que son équation est $y = \alpha x + \beta$, et on trouve α et β en inversant le système obtenu en observant que N et M vérifient cette équation. Notons qu'on a pour cela une nouvelle fois besoin de choisir $p \neq 2$.

correspond bien sûr au point N, et donc on a bien un second point d'intersection $P(t)$ donné par

$$P(t) = \begin{pmatrix} \dfrac{1-t^2}{1+t^2} \\ \dfrac{2t}{1+t^2} \end{pmatrix}.$$

Réciproquement, si $M' = (x, y) \in \mathbb{S}^1(\mathbb{F}_q)$ est différent de N, alors $x \neq -1$. Ainsi, la droite (NM') possède un unique point d'intersection avec la droite $\{x = 1\}$. Donc tout point de la droite correspond à un unique point du cercle, et réciproquement. Il y a donc une bijection entre $\mathbb{F}_q$ et $\mathbb{S}^1(\mathbb{F}_q)\backslash\{N\}$, ce qui montre que $\mathbb{S}^1(\mathbb{F}_q)$ est de cardinal $q+1$, et $SO_2(\mathbb{F}_q)$ aussi d'après de l'étape 1. Il reste alors à montrer que $SO_2(\mathbb{F}_q)$ est cyclique.

Pour cela, on injecte $SO_2(\mathbb{F}_q)$ dans $\mathbb{F}_{q^2}^*$. Le corps $\mathbb{F}_{q^2}$ est une extension de $\mathbb{F}_q$ de degré 2 dans laquelle -1 est un carré. En effet, X^2+1 est irréductible dans $\mathbb{F}_q[X]$ (car de degré 2 sans racine) donc $\mathbb{F}_q[X]/(X^2+1)$ est une extension de degré 2 de $\mathbb{F}_q$ qui est un corps de rupture de -1. Mais comme c'est un corps de cardinal q^2, par unicité des corps finis, ce corps de rupture est isomorphe à $\mathbb{F}_{q^2}$. On effectue alors un raisonnement analogue à celui de l'étape 2 : $SO_2(\mathbb{F}_q)$ s'injecte dans $\mathbb{F}_{q^2}^*$ en utilisant une racine carrée ω de -1 dans $\mathbb{F}_{q^2}^*$ et en produisant le même raisonnement que pour l'injectivité de φ. Ainsi, d'après le théorème d'isomorphisme, $SO_2(\mathbb{F}_q)$ est isomorphe (en tant que groupe) à son image par cette injection, qui est un sous-groupe du groupe cyclique $\mathbb{F}_{q^2}^*$. Donc $SO_2(\mathbb{F}_q)$ est cyclique[8], et est donc isomorphe à $\mathbb{Z}/(p+1)\mathbb{Z}$. □

La question naturelle qui suit cette démonstration est celle du cas $p = 2$. Je n'ai pas trouvé de livre traitant de cette question, mais elle n'est pas compliquée. On cherche à caractériser les éléments de $SO_2(\mathbb{F}_q)$, avec $q = 2^n$. Les équations décrites dans la première étape montrent que ce sont exactement les matrices de la forme $\begin{pmatrix} 1+b & b \\ b & 1+b \end{pmatrix}$, pour $b \in \mathbb{F}_q$. De plus, il se trouve que l'application qui associe l'élément b à cette matrice est un morphisme de groupes entre $SO_2(\mathbb{F}_q)$ et $\mathbb{F}_q$, surjectif par ce qui précède. Bien sûr, il est aussi injectif (étude du noyau). Finalement, on obtient

$$SO_2(\mathbb{F}_q) \simeq \mathbb{F}_q.$$

Ce résultat est très rapide à montrer donc peut permettre de combler si jamais il reste une ou deux minutes à la fin du développement. Dans tous les cas, je pense qu'il est bon de l'avoir en tête, cela me paraît être la question la plus évidente que le jury pourrait poser.

8. Tout sous-groupe d'un groupe cyclique est cyclique.

10 Irréductibilité des polynômes cyclotomiques sur $\mathbb{Z}$

Leçons 102, 141(, 120, 121, 144)

Ref : [Per96] III.4

On démontre ici l'irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$, et on en déduit celle sur $\mathbb{Z}$. Les arguments en gris peuvent suivant la leçon être à énoncer rapidement, ou bien demandent un peu plus d'attention et de détails.

On introduit le n-ième polynôme cyclotomique sur le corps $\mathbb{K}$, que l'on note $\Phi_{n,\mathbb{K}}$. Si $\mathbb{K} = \mathbb{Q}$, on notera simplement Φ_n. On note μ_n (resp. μ_n^*) l'ensemble des racines (resp. primitives) n-ième de l'unité.

Proposition 10.1 Φ_n est à coefficients dans $\mathbb{Z}$.

Démonstration. On procède par récurrence forte sur n. Comme $\Phi_1(X) = X - 1$, le résultat est vrai pour $n = 1$. Supposons maintenant qu'il l'est pour tout $d < n$, avec $n \geq 2$. On note $P = \prod_{d|n, d\neq n} \Phi_d$, qui est un polynôme à coefficients dans $\mathbb{Z}$ par hypothèse de récurrence. De plus, puisque tous les $\Phi_{k,\mathbb{K}}$ sont unitaires, quelquesoit l'entier k et le corps $\mathbb{K}$, P est unitaire. On peut donc effectuer la division euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$: $X^n - 1 = PQ + R$ avec $Q, R \in \mathbb{Z}[X]$ et $\deg(R) < \deg(P)$. Or on sait que $X^n - 1 = \Phi_n P$ [9], donc $R = P(\Phi_n - Q)$, et pour des raisons de degré, les deux membres de l'égalité sont nuls. Donc $\Phi_n = Q \in \mathbb{Z}[X]$. □

Théorème 10.2 Φ_n est irréductible sur $\mathbb{Z}$.

Démonstration.

Étape 1. Polynômes minimaux des racines primitives de l'unité sur $\mathbb{Q}$.

On se donne un corps de décomposition de Φ_n sur $\mathbb{Q}$, que l'on note $\mathbb{K}$, et une racine n-ième primitive de l'unité $\zeta \in \mathbb{K}$. On note μ le polynôme minimal de ζ sur $\mathbb{Q}$. Montrons que $\mu \in \mathbb{Z}[X]$ et μ divise Φ_n dans $\mathbb{Z}[X]$.

Comme $\mathbb{Z}[X]$ est factoriel, on écrit $\Phi_n = P_1..P_r$ la décomposition de Φ_n en produit d'irréductibles dans $\mathbb{Z}$. Puisque Φ_n est unitaire, on peut supposer (quitte à le multiplier par -1) que P_i est unitaire, pour tout $i \in [\![1, r]\!]$. Mais comme ζ est racine de l'un des P_i, et que celui-ci est irréductible unitaire sur $\mathbb{Z}$, et donc sur $\mathbb{Q}$, on a $\mu = P_i$. Donc $\mu \in \mathbb{Z}[X]$ est μ divise Φ_n dans $\mathbb{Z}$.

Étape 2. Les puissances d'une même racine primitive ont le même polynôme minimal.

Soit maintenant $p \in \mathfrak{P}$ un nombre premier ne divisant pas n. Alors ζ^p est aussi une racine primitive n-ième de l'unité dans $\mathbb{K}$. On note ν son polynôme minimal. Montrons que $\mu = \nu$. Supposons par l'absurde que c'est faux. Alors μ et ν sont deux polynômes irréductibles distincts qui divisent Φ_n dans $\mathbb{Z}$, donc leur produit le divise aussi. De plus, comme $\nu(\zeta^p) = 0$, ζ est racine de $\nu(X^p) \in \mathbb{Z}[X]$. On en déduit que μ divise $\nu(X^p)$ dans $\mathbb{Q}[X]$. Montrons que c'est aussi vrai dans $\mathbb{Z}[X]$: on se donne $P \in \mathbb{Q}[X]$ tel que $\nu(X^p) = \mu(X)P(X)$. On se donne $q \in \mathbb{Q}$ tel que $P = qQ$ et $Q \in \mathbb{Z}[X]$ soit primitif, et on applique le lemme de Gauß :

$$1 = c(\nu(X^p)) = qc(\mu)c(Q) = q,$$

car ν et μ sont unitaires, et Q primitif. Donc $q = 1$, ce qui signifie que P est bien dans $\mathbb{Z}[X]$.

On projette alors cette égalité dans $\mathbb{F}_p$. On a $\overline{\nu}(X^p) = \overline{\nu}(X)^p$.

En effet, on note $\nu(X) = \sum_{i=0}^{k} a_i X^i$, et on a $\overline{\nu}(X^p) = \sum_{i=0}^{k} \overline{a_i} X^{pi} = \left(\sum_{i=0}^{k} \overline{a_i} X^i\right)^p = \overline{\nu}(X)^p$.

Ainsi, $\overline{\nu}^p = \overline{\mu}\overline{P}$. On se donne un facteur irréductible φ de $\overline{\mu}$ sur $\mathbb{F}_p$. D'après le lemme d'Euclide, comme φ divise $\overline{\nu}^p$, alors il divise $\overline{\nu}$. Or comme $\mu\nu$ divise Φ_n sur $\mathbb{Z}$, $\overline{\mu\nu}$ divise $\overline{\Phi_n}$ sur $\mathbb{F}_p$, mais $\overline{\Phi_n}$ est en fait $\Phi_{n,\mathbb{F}_p}$ [10], donc $\overline{\mu\nu}$ divise $\Phi_{n,\mathbb{F}_p}$ sur $\mathbb{F}_p$. Donc φ^2 est un facteur carré de $\Phi_{n,\mathbb{F}_p}$, ce qui est absurde.

En effet, la dérivée de $X^n - 1$ est nX^{n-1}, qui n'admet que 0 comme racine dans $\mathbb{F}_p$, car n et p sont premiers entre eux. Donc, comme 0 n'est pas racine de $X^n - 1$, celui-ci n'a que des racines simples. On en déduit que sur $\mathbb{F}_p$, les polynômes cyclotomiques n'ont pas de facteurs carrés.

9. Cela vient de l'égalité $\mu_n(\mathbb{K}) = \bigcup_{d|n} \mu_d^*(\mathbb{K})$.

10. Cela se montre par récurrence forte en utilisant un procédé similaire à celui de la proposition précédente.

Donc $\mu = \nu$.

Étape 3. Autres racines et conclusion.

Si ζ' est une racine primitive n-ième de l'unité, on peut écrire $\zeta' = \zeta^m$, avec m premier avec n, et donc décomposable en un produit $p_1..p_r$ de nombre premiers ne divisant pas n. Par récurrence sur r [11], on montre alors en appliquant directement la seconde étape que ζ' et ζ ont le même polynôme minimal sur $\mathbb{Q}$, et que celui-ci est μ. Donc, comme μ admet les $\varphi(n)$ racines primitives de l'unité comme zéros, il est de degré au moins $\varphi(n)$. Or Φ_n est de degré $\varphi(n)$, divisible par μ, et les deux sont unitaires. Donc $\mu = \Phi_n$, et donc Φ_n est irréductible sur $\mathbb{Q}$. Comme il est unitaire et à coefficients dans $\mathbb{Z}$, il est primitif, et donc irréductible sur $\mathbb{Z}$. □

11. On applique l'étape 2 à $\widetilde{\zeta} := \zeta^{p_1 \cdots p_{r-1}}$ et $\widetilde{\zeta}^{p_r} = \zeta'$ pour montrer que leur polynôme minimal sur $\mathbb{Q}$ est le même.

11 Loi de réciprocité quadratique

Leçons 121, 123, 126, 170

Ref : [CG13] V.C

Le but de ce développement est de montrer un résultat important de la théorie des corps finis, qui permet de relier le fait que deux nombres premiers impairs soient respectivement des carrés l'un modulo l'autre. Il utilise notamment le théorème de classification des formes quadratiques sur les corps finis.

On rappelle la définition suivante.

Définition 11.1 Soit p un entier premier impair et a un élément de $\mathbb{F}_p$. On définit le *symbole de Legendre* de a par

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 \text{ si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 \text{ si } a = 0 \end{cases}.$$

Théorème 11.2 (Loi de réciprocité quadratique) Soient p et q deux entiers premiers impairs distincts. Alors on a

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Démonstration. L'idée de la preuve consiste à calculer les cardinaux de deux sphères unités de $\mathbb{F}_q^p$ pour deux formes quadratiques équivalentes, et de montrer que ce sont les mêmes. On aura par ailleurs besoin du lemme suivant [12].

Lemme 11.3 Soit a un élément de $\mathbb{F}_p^*$ (où p désigne toujours un nombre premier impair). Alors on a

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

Démonstration. Le membre de gauche correspond au nombre de racine du polynôme $aX^2 - 1$, de degré 2, dans le corps $\mathbb{F}_p$. On distingue deux cas :

- si a n'est pas un carré modulo p, a^{-1} non plus et alors le polynôme n'a pas de racine dans $\mathbb{F}_p$: l'égalité est donc correcte
- si a est un carré, a^{-1} aussi, et on note alors ε une racine de a^{-1} ; ε et $-\varepsilon$ sont alors deux racines distinctes (car $\varepsilon \neq 0$) de $aX^2 - 1$, et comme ce polynôme est de degré, il ne peut en avoir d'autre, ce qui prouve que l'égalité tient aussi.

□

Étape 1. Dénombrement de la sphère unité de $\mathbb{F}_q^p$ modulo p.

On veut connaître le cardinal de la sphère unité de $\mathbb{F}_q^p$

$$S := \left\{(x_1, .., x_p) \in \mathbb{F}_q^p, \quad \sum_{i=1}^{p} x_i^2 = 1\right\}.$$

On fait agir le groupe $\mathbb{Z}/p\mathbb{Z}$ par permutation cyclique des coordonnées sur $\mathbb{F}_q^p$:

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

où l'on voit bien sûr les indices modulo p. On étudie en particulier l'action de $\mathbb{Z}/p\mathbb{Z}$ sur S [13]. On classifie les orbites de S sous cette action : d'après la relation orbite-stabilisateur, on a pour tout $x \in S$

$$|O_x||\mathrm{Stab}_x| = |\mathbb{Z}/p\mathbb{Z}| = p,$$

et comme p est premier on en déduit que les orbites sont de deux types :

- le point $(x, .., x) \in S$ pour $x \in \mathbb{F}_q^p$ est sa propre orbite, et son stabilisateur est $\mathbb{Z}/p\mathbb{Z}$; de plus on a nécessairement $px^2 = 1$ puisque $(x, .., x) \in S$

12. En fonction du temps, on peut choisir de le démontrer ou de l'admettre.
13. Si $x \in S$, alors pour tout $k \in \mathbb{Z}/p\mathbb{Z}$, $k \cdot x$ est toujours un élément de S.

– les autres orbites sont de cardinal p et ont un stabilisateur trivial ; on note k le nombre de ces orbites.

Comme S est union disjointe de ses orbites, on a alors

$$|S| = \left|\left\{x \in \mathbb{F}_q, \quad px^2 = 1\right\}\right| \times 1 + k \times p.$$

Ainsi, d'après le lemme, comme p est inversible dans $\mathbb{F}_q$ puisqu'il est premier et différent de q, on en déduit

$$|S| \equiv \left(\frac{p}{q}\right) + 1 \quad [p].$$

Étape 2. Une seconde sphère unité de $\mathbb{F}_q^p$ équipotente à S.

On définit la forme quadratique φ par

$$\forall x = (x_1, .., x_p) \in \mathbb{F}_q^p, \quad \varphi(x) = 2\left(x_1x_2 + .. + x_{p-2}x_{p-1}\right) + ax_p^2$$

où $a = (-1)^{\frac{p-1}{2}}$. On note aussi $d = \dfrac{p-1}{2}$, et on définit $S' := \left\{x \in \mathbb{F}_q^p,\ \varphi(x) = 1\right\}$ la sphère unité pour φ. La matrice de φ dans la base canonique est

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

et son déterminant est $\det(A) = (-1)^d a = 1$. D'après le théorème de classification des formes quadratiques, les formes φ et $\displaystyle\sum_{i=1}^{p} x_i^2$ sont donc équivalentes, et le changement de variable linéaire qui permet de passer de l'un à l'autre fournit une bijection entre S et S'. On a donc $|S| = |S'|$.

Étape 3. Dénombrement de S' modulo p.

On distingue deux types de points dans S' :

– ceux pour lesquels $x_1 = x_3 = ..x_{p-2} = 0$; il suffit de choisir $x_p \in \left\{x \in \mathbb{F}_q, \quad ax^2 = 1\right\}$ $\left(1 + \left(\dfrac{a}{q}\right)\right.$ possibilités d'après le lemme) et on a alors q^d possibilités pour les coordonnées restantes

– si au moins l'une des coordonnées $x_1, x_3, .., x_{p-2}$ est non nulle ($q^d - 1$ possibilités) et que x_p est aussi fixé (q possibilités), il reste à choisir un point $(x_2, .., x_{p-1})$ dans un hyperplan affine de $\mathbb{F}_q^d$, soit q^{d-1} possibilités

On a donc

$$|S'| = q^d\left(1 + \left(\frac{a}{q}\right) + q^d - 1\right) = q^d\left(q^d + ((-1)^d)^{\frac{q-1}{2}}\right).$$

Or on a aussi $q^d = \left(\dfrac{q}{p}\right)$, donc en utilisant les résultats des deux premières étapes, on a :

$$\left(\frac{q}{p}\right)\left(\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) \equiv \left(\frac{p}{q}\right) + 1 \quad [p].$$

Or $\left(\dfrac{q}{p}\right)^2 = 1$, donc on peut simplifier les 1 de chaque côté. Il reste l'égalité suivante dans $\mathbb{Z}/p\mathbb{Z}$:

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

Or les deux membres de cette équation dans $\mathbb{Z}/p\mathbb{Z}$ sont dans $\{\pm 1\}$. Comme p est supérieur à 2, cette équation reste vraie dans $\mathbb{Z}$, et on en déduit la loi de réciprocité quadratique. □

12 Parties génératrices de $SL(E)$ et $GL(E)$

Leçons 106, 108

Ref : [Per96] IV.2

On se donne un $\mathbb{K}$-espace vectoriel E de dimension finie $n \in \mathbb{N}^*$ (où $\mathbb{K}$ est un corps commutatif).

Théorème 12.1 Le groupe spécial linéaire $SL(E)$ est engendré par les transvections.

Démonstration. La démonstration repose sur deux lemmes qui construisent des transvections utiles pour décomposer un endomorphisme quelconque de $SL(E)$.

Lemme 12.2 On se donne deux hyperplans distincts H_1 et H_2 de E, et un point x qui n'est dans aucun des deux (voir figure 12.1). Alors il existe une transvection $u \in SL(E)$ telle que

$$\begin{cases} u(H_1) = H_2 \\ u(x) = x \end{cases}.$$

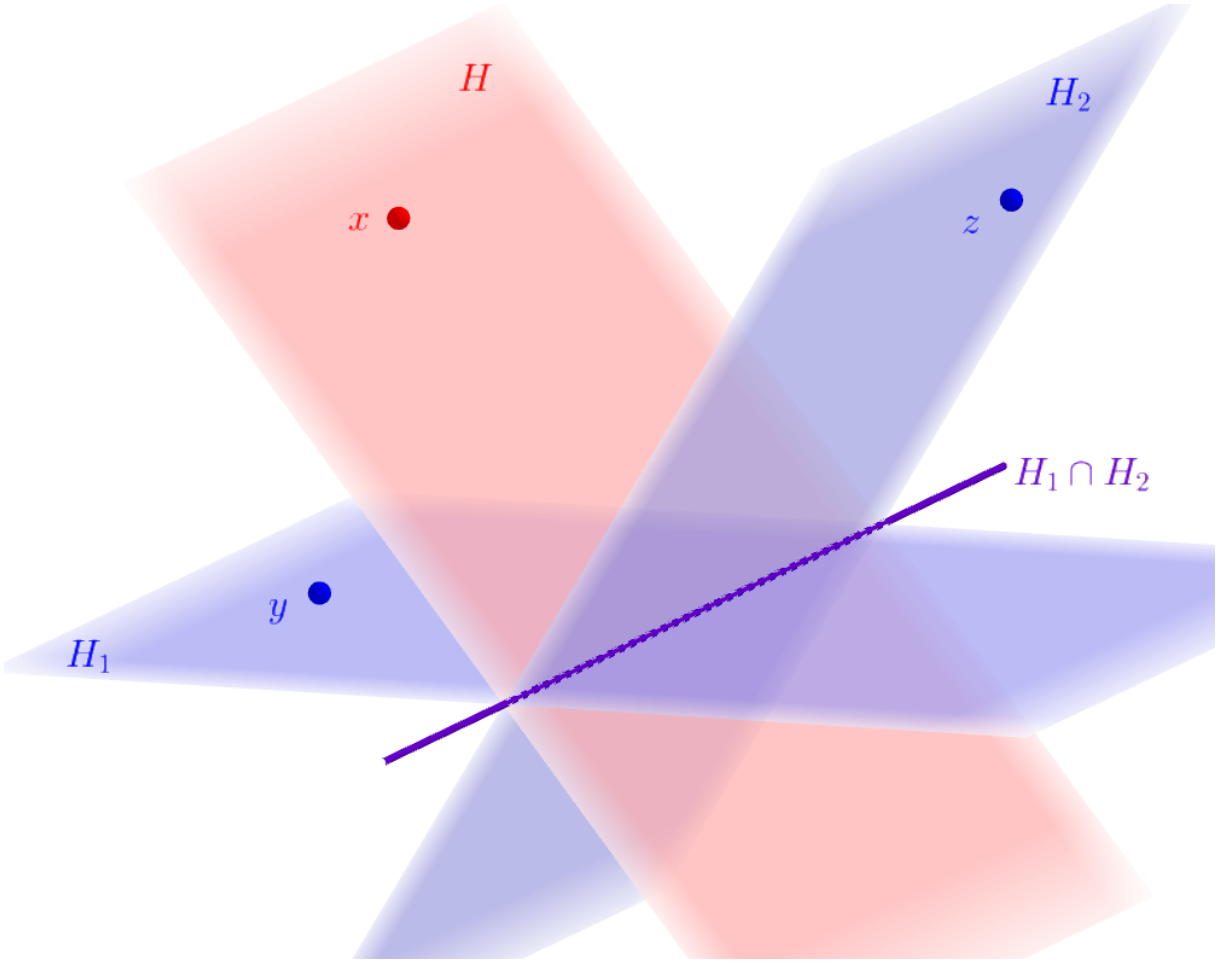


Figure 12.1 – Hyperplans concernés par le premier lemme

Démonstration. On note H l'hyperplan contenant x et $H_1 \cap H_2$ (voir figure 12.1), qui est celui qui est fixé par la transvection recherchée. On remarque que puisque x est dans H et pas dans H_1, on dispose de l'égalité

$$E = H + H_1.$$

On se donne $z \in H_2 \backslash H$. Alors il existe $a \in H$ et $y \in H_1$ tels que $z = a + y$. De plus, comme z n'est pas dans H, y n'est pas dans H. Si l'on se donne une équation f de H (i.e. une forme linéaire non nulle f telle que $H = \ker(f)$), y n'annule donc pas f, et on peut ainsi supposer $f(y) = 1$. On pose alors

$$\forall t \in E, \quad u(t) = t + f(t)a.$$

Puisque a est un élément non nul de H (sinon, z serait dans $H_1 \cap H_2$ et donc dans H), u est une transvection qui laisse stable l'hyperplan H. En particulier, $u(x) = x$. De plus, on a

$$u(y) = y + f(y)a = z.$$

Ainsi, comme y n'est pas dans H_2 (car sinon il serait dans $H_1 \cap H_2$ et donc dans H), $\mathbb{K}y$ est un supplémentaire de $H_1 \cap H_2$ dans H_1, et donc tout élément t de H_1 s'écrit $t = h + \lambda y$, avec $\lambda \in \mathbb{K}$ et $h \in H_1 \cap H_2 \subset H$. Ainsi, on a

$$u(t) = u(h) + \lambda u(y) = h + z \in H_2.$$

□

Lemme 12.3 Soient x et y deux points de E non nuls. Si E est de dimension supérieure à 2, il existe un produit u de une ou deux transvections de E tel que $u(x) = y$.

Démonstration. On traite deux cas distincts.

- Si x et y ne sont pas colinéaires, alors x et $x - y$ non plus, et il existe donc un hyperplan H de E qui contient $x - y$ et pas x. On se donne alors une équation f de H telle que $f(x) = 1$, et la transvection u définie par
$$\forall t \in E, \quad u(t) = t + f(t)(y - x)$$
convient.
- Si x et y sont colinéaires, comme E est au moins de dimension 2, on peut se donner un point $z \in E$ non colinéaire à x et y. Le premier cas permet alors de construire deux transvections u_1 et u_2 telles que
$$\begin{cases} u_1(x) = z \\ u_2(z) = y \end{cases}$$
Alors l'endomorphisme $u_2 \circ u_1$ convient.

□

On démontre maintenant le théorème par récurrence sur la dimension n de E. Dans le cas où $n = 1$, il n'y a rien à démontrer. On suppose maintenant que le théorème est vrai au rang $n-1$, avec $n \geq 2$. On se donne alors $u \in SL(E)$, $x \in E$, et H un hyperplan de E ne contenant pas x.

Quitte à composer u à gauche par le produit d'une ou deux transvections obtenu en appliquant le second lemme aux points $u(x)$ et x, on peut supposer que $u(x) = x$. De plus, comme x n'est pas dans H, ni dans l'hyperplan $u(H)$ (car $u(x) = x$), d'après le premier lemme, quitte à composer une nouvelle fois à gauche par un transvection, on peut supposer $u(H) = H$. Alors on peut écrire, par hypothèse de récurrence, $u_{|H} \in SL(H)$ comme un produit de transvections sur H :

$$u_{|H} = \prod_{i=1}^{r} v_i.$$

Maintenant, comme les v_i sont des transvections, elles s'étendent de manière unique à E comme transvections (notées u_i), de la manière suivante :

$$\begin{cases} \forall h \in H, \quad u_i(h) = v_i(h) \\ u_i(x) = x \end{cases}$$

Ainsi, on a $u = \prod_{i=1}^{r} u_i$. □

Corollaire 12.4 $GL(E)$ est engendré par les transvections et les dilatations.

Démonstration. Si $u \in GL(E)$ est de déterminant $\lambda \neq 0$, et si on pose $v = \frac{1}{\lambda}\,\mathrm{Id}$ la dilatation de rapport $\frac{1}{\lambda}$, alors $u \circ v \in SL(E)$, et le théorème permet de conclure. □

13 Polygones réguliers constructibles

Leçons 102, 125, 151, 191(, 104, 141, 144)

Ref : [Mer04]

Définition 13.1 Les nombres de Fermat sont les nombres premiers F_β s'écrivant $F_\beta = 1 + 2^{2^\beta}$, pour $\beta \in \mathbb{N}$.

Théorème 13.2 Soit $p \in \mathfrak{P}$ impair, et $\alpha \in \mathbb{N}^*$. Alors le polygône $\mathcal{P}_n$ régulier à n côtés, avec $n = p^\alpha$, est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat.

Démonstration. On rappelle que $\mathcal{P}_n$ est constructible si et seulement si $\cos\left(\frac{2\pi}{n}\right)$ l'est.

$\Longrightarrow$ On suppose $\mathcal{P}_n$ constructible et on pose $\omega = \mathrm{e}^{\frac{2i\pi}{n}}$. Le théorème de Wantzel montre que $\mathbb{Q}(\omega)$ est le m-ième terme d'une suite d'extensions quadratiques de $\mathbb{Q}$. De plus, comme le polynôme minimal de ω est Φ_n, on a

$$2^m = [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\Phi_n) = p^{\alpha-1}(p-1).$$

Comme p est impair, on a donc $\alpha = 1$ et $p = 1 + 2^m$. Montrons que m est une puissance de 2. On écrit $m = \lambda 2^\beta$, avec $\beta \in \mathbb{N}$ et $\lambda \in \mathbb{N}^*$ impair. Ainsi, -1 est racine de $X^\lambda + 1$, donc $X + 1$ divise $X^\lambda + 1$ sur $\mathbb{Z}$. On en déduit que F_β divise $p = 1 + \left(2^{2^\beta}\right)^\lambda$. Mais comme p est premier, on a alors égalité : p est un nombre premier de Fermat.

$\Longleftarrow$ Soit $p = F_\beta$ un nombre premier de Fermat. On note $q = 2^\beta$, de sorte que $p = 1 + 2^q$. On pose aussi $\omega = \mathrm{e}^{\frac{2i\pi}{p}}$.

Étape 1. Description des automorphismes de $\mathbb{Q}(\omega)$.
On a alors

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\Phi_p) = 2^q.$$

On note G le groupe des automorphismes de corps sur $\mathbb{Q}(\omega)$ laissant $\mathbb{Q}$ invariant [14]. Ainsi, si $g \in G$, il est entièrement déterminé par l'image de ω. Comme $\omega^p = 1$, $g(\omega)^p = 1$, donc $g(\omega)$ est une racine p-ième de l'unité, ce qui permet de décrire G [15] :

$$G = \left\{ g : \omega \longmapsto \omega^i,\ i \in [\![1, p-1]\!] \right\}.$$

On voit alors que l'application

$$\varphi : \left| \begin{array}{ccc} G & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \\ g_i & \longmapsto & i \end{array} \right.$$

est un isomorphisme de groupes [16], ce qui prouve que G est un groupe cyclique.

Étape 2. Une tour d'extensions de corps.
On notera dans la suite g un générateur de G. On définit pour $i \in [\![0, n]\!]$ le sous-corps

$$K_i := \ker\left(g^{2^i} - \mathrm{id}\right).$$

Comme $g^{2^{i+1}} = (g^{2^i})^2$, on a $K_i \subset K_{i+1}$. Montrons que $K_0 = \mathbb{Q}$. On remarque que les $(g^i(\omega))_{0 \le i \le p-2}$ forment une base de $\mathbb{Q}(\omega)$ sur $\mathbb{Q}$. Soit $z \in K_0$. On écrit $z = \sum_{i=0}^{p-2} z_i g^i(\omega)$. On a alors

$$z = g(z) = \sum_{i=0}^{p-2} z_i g^{i+1}(\omega).$$

Il vient que les z_i sont tous égaux, et on a donc

$$z = z_0 \sum_{i=0}^{p-1} g^i(\omega) = z_0 \sum_{i=1}^{p-1} \omega^i = -z_0 \in \mathbb{Q}.$$

Donc $K_0 \subset \mathbb{Q}$. Réciproquement, comme g est $\mathbb{Q}$-invariant, l'inclusion inverse est vraie aussi, et $K_0 = \mathbb{Q}$. De même, comme g est un générateur du groupe G, qui est d'ordre 2^q, on a $K_q = \mathbb{Q}(\omega)$.

14. Si on veut passer vite sur certains arguments, une des possibilités (si l'on maîtrise un peu la théorie de Galois) est de dire que ce groupe est le groupe de Galois de $\mathbb{Q}(\omega)/\mathbb{Q}$, et certaines choses démontrées plus bas en découlent directement.
15. On vérifie que l'on obtient ainsi $p - 1$ automorphismes distincts.
16. On a $\varphi(g_i \circ g_j) = \varphi(g_{ij}) = ij = \varphi(g_i)\varphi(g_j)$.

Étape 3. Extensions quadratiques et conclusion.
Montrons que K_i est une extension quadratique de K_{i-1}, pour $i \geq 1$. On considère cette fois $z = \sum_{k=0}^{2^{q-i}-1} g^{k2^i}(\omega)$. On a

$$g^{2^i}(z) = \sum_{k=0}^{2^{q-i}-1} g^{(k+1)2^i}(\omega) = \sum_{k=1}^{2^{q-i}-1} g^{k2^i}(\omega) + \underbrace{g^{2^q}(\omega)}_{=\omega=g^0(\omega)} = z.$$

Donc $z \in K_i$. De plus,

$$g^{2^{i-1}}(z) = \sum_{k=0}^{2^{q-i}-1} g^{k2^i+2^{i-1}}(\omega).$$

Comme on a décalé chaque coordonnée non nulle de z de 2^{i-1}, alors que celles-ci sont espacées de 2^i, les coordonnées non nulles de z et $g(z)$ ne sont pas les mêmes. Donc $z \notin K_{i-1}$. Donc la suite

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq .. \subsetneq K_q = \mathbb{Q}(\omega)$$

est une suite d'extensions strictes. En passant au degré, on a alors

$$2^q = [\mathbb{Q}(\omega) : \mathbb{Q}] = \prod_{i=0}^{q-1} \underbrace{[K_{i+1} : K_i]}_{\geq 2} \geq 2^q,$$

ce qui implique que les extensions K_{i+1}/K_i sont quadratiques. Donc $\cos\left(\frac{2\pi}{p}\right) = \frac{\omega + \omega^{-1}}{2}$ est dans une extension qui est le terme d'une suite d'extensions quadratiques de $\mathbb{Q}$, donc est constructibles d'après le théorème de Wantzel, ce qui montre que $\mathcal{P}_p$ est constructible.

□

Théorème 13.3 (Gauß-Wantzel) Les seuls polygones réguliers constructibles sont les polygones à n côtés, avec $n = 2^m p_1..p_r$, où $m \in \mathbb{N}$ et les p_i sont des nombres premiers de Fermat distincts.

Démonstration. On démontre un lemme qui nous permettra d'effectuer une récurrence.

Lemme 13.4
- Pour $n \geq 3$, $\mathcal{P}_n$ est constructible si et seulement si $\mathcal{P}_{2n}$ l'est.
- Si pour $n, m \geq 3$ premiers entre eux, $\mathcal{P}_n$ et $\mathcal{P}_m$ sont constructibles si et seulement si $\mathcal{P}_{mn}$ l'est.

Démonstration.
- Si $\mathcal{P}_{2n}$ est construit, prendre un point sur deux permet de construire $\mathcal{P}_n$. Réciproquement, si $\mathcal{P}_n$ est construit, on trace les médiatrices de ses côtés, et leur intersection avec le cercle circonscrit forment les points manquants de $\mathcal{P}_{2n}$.
- Si $\mathcal{P}_{nm}$ est construit, prendre un point sur m (resp. un point sur n) permet de construire $\mathcal{P}_n$ (resp. $\mathcal{P}_m$). Pour la réciproque, on se donne une relation de Bézout $1 = un + vm$. On a alors

$$\frac{2\pi}{mn} = u\frac{2\pi}{m} + v\frac{2\pi}{n}.$$

Ainsi, si l'on reporte u fois l'angle $\frac{2\pi}{m}$ (que l'on a puisque $\mathcal{P}_m$ est construit) puis v l'angle $\frac{2\pi}{n}$, on obtient $\frac{2\pi}{mn}$.

□

□

14 Quaternions et groupe spécial orthogonal

Leçons 106, 160, 161(, 101, 108, 154, 191)

Ref : [Per96] VII.2

On note dans la suite $\mathbb{H}$ le *corps (non commutatif) des quaternions*, i.e. le $\mathbb{R}$-espace vectoriel de dimension 4 dont une base est $(1, i, j, k)$, avec les relations

$$i^2 = j^2 = k^2 = ijk = -1.$$

Pour $q = a+ib+jc+kd \in \mathbb{H}$, on appelle $\overline{q} = a-ib-jc-kd$ le *conjugué* de q. L'application $q \longmapsto \sqrt{q\overline{q}}$ est une norme multiplicative (appelée *norme quaternionique*), et correspond en fait à la norme euclidienne sur $\mathbb{H}$ dans la base donnée précédemment.

On définit également le *groupe des quaternions* G comme l'ensemble des quaternions de norme 1, muni du produit. L'inverse d'un élément q est alors son conjugué.

Théorème 14.1 Il existe un isomorphisme de groupes entre $G/\{\pm 1\}$ et $SO_3(\mathbb{R})$.

Démonstration. Étape 1. Action de G sur $\mathbb{H}$.

On considère l'action de G sur $\mathbb{H}$ par conjugaison : pour $q \in G$, on définit l'application

$$S_q : \left| \begin{array}{ccc} \mathbb{H} & \longrightarrow & \mathbb{H} \\ q' & \longmapsto & qq'\overline{q} \end{array} \right.$$

Tout d'abord, cette application est linéaire (car $\mathbb{R}$ est central dans $\mathbb{H}$) et bijective, puisque $S_{\overline{q}}$ fournit un inverse à S_q (cela découle du fait que l'action par conjugaison est bien une action de groupes). On en déduit que le morphisme de l'action $S : G \longrightarrow \mathfrak{S}(\mathbb{H})$ est à valeurs dans le groupe des automorphismes de $\mathbb{R}$-espace vectoriel de $\mathbb{R}^4$, qui est isomorphe à $GL_4(\mathbb{R})$. On a donc un morphisme de groupe

$$S : G \longrightarrow GL_4(\mathbb{R}).$$

De plus, son noyau est par définition la trace dans G du centre de $\mathbb{H}$, c'est à dire $\mathbb{R} \cap G = \{\pm 1\}$.

Étape 2. Restriction de l'action à l'espace des quaternions purs.

Pour un élément $q \in G$ donné, S_q préserve la norme quaternionique, et donc la norme euclidienne sur $\mathbb{R}^4$: c'est dire que S_q est un élément de $O_4(\mathbb{R})$. De plus, G agit trivialement sur $\mathbb{R}$ (puisque $\mathbb{R} = Z(\mathbb{H})$), et donc laisse également stable son orthogonal, qui est l'ensemble $P := \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ des quaternions purs. Ainsi, $s_q := S_{q|P}$ est un élément de $O_3(\mathbb{R})$, et on construit ainsi un nouveau morphisme

$$s : G \longrightarrow O_3(\mathbb{R})$$

de noyau $\{\pm 1\}$. De plus, cette application est continue (pour la topologie naturelle sur $O_3(\mathbb{R})$, vu comme un sous-espace vectoriel de $\mathcal{M}_3(\mathbb{R}) \simeq \mathbb{R}^9$). En effet, le calcul de la matrice de s_q dans la base (i, j, k) de P montre que ses coefficients sont des polynômes homogènes de degré 2 en les coefficients de q : si $q = a + ib + jc + kd$, on a par exemple

$$s_q(i) = (ia - b - kc + jd)(a - ib - jc - kd) = (a^2 + b^2 - c^2 - d^2)i + 2(ad + bc)j + 2(bd - ac)k,$$

et les trois coefficients sont bien polynomiaux. Donc, en composant avec le déterminant, qui est aussi continu, on obtient une application $\det \circ s : G \longrightarrow \{\pm 1\}$ continue. Or G est connexe (car isomorphe à la sphère $\mathbb{S}^3 = \{(a, b, c, d) \in \mathbb{R}^4,\ a^2 + b^2 + c^2 + d^2 = 1\}$) donc cette application est constante. Comme G contient l'élément 1, son image contient l'identité, et donc elle est inclue dans $SO_3(\mathbb{R})$ [17].

Étape 3. Surjectivité de l'action obtenue.

On va maintenant montrer que l'image de s est $SO_3(\mathbb{R})$. Tout d'abord, si q est un élément de $G \cap P$, $s_q(q) = q\overline{q} = q$, donc s_q fixe la droite vectorielle $\mathbb{R}q$. De plus, comme $q^2 = -q\overline{q} = -1$ (puisque q est un quaternion pur, donc $\overline{q} = -q$), $s_q^2 = s_{-1} = \mathrm{Id}$. Donc s_q est une involution. Mais alors nécessairement, puisqu'elle est de déterminant 1, c'est un renversement (car $s_q \neq \mathrm{Id}$ comme $q \notin \{\pm 1\}$). Comme on connaît la droite fixée par s_q, on en conclut que s_q est justement le renversement d'axe $\mathbb{R}q$. Finalement, comme

17. Si on manque de temps, on peut directement invoquer le fait que la composante connexe de l'identité dans $O_3(\mathbb{R})$ est $SO_3(\mathbb{R})$.

toutes les droites vectorielles de P contiennent un élément de $G \cap P$, $s(G)$ contient tous les renversements. Mais comme ceux-ci engendrent $SO_3(\mathbb{R})$, on a bien $s(G) = SO_3(\mathbb{R})$. D'après le théorème d'isomorphisme, on en déduit que s induit un isomorphisme

$$\overline{s} : G/\{\pm 1\} \longrightarrow SO_3(\mathbb{R}).$$

□

Remarque.

- L'isomorphisme obtenu est explicite, mais son inverse est difficile à exprimer puisqu'il faut résoudre les équations polynomiales de degré 2 associées aux coefficients d'une matrice de $SO_3(\mathbb{R})$.
- Malgré tout, on peut à l'oral évoquer le fait que les calculs de rotations faits par les ordinateurs (dans les jeux vidéos par exemple) se font souvent à partir de cet isomorphisme, en calculant dans G.

15 Simplicité de $\mathfrak{A}_n$

Leçons 101, 103, 104, 105, 108

Ref : [Per96] Prop I.4.10, Th I.8.1

Théorème 15.1 Le groupe alterné $\mathfrak{A}_n$ est simple pour $n \geq 5$

Démonstration. Étape 1. Conjugaison des 3-cycles dans $\mathfrak{A}_n$.

La première étape de cette démonstration repose sur le lemme suivant, qui décrit l'action de $\mathfrak{A}_n$ sur $[\![1, n]\!]$.

Lemme 15.2 Pour $n \geq 3$, l'action de $\mathfrak{A}_n$ sur $[\![1, n]\!]$ est $n-2$-transitive.

Démonstration. On se donne deux familles d'éléments deux à deux distincts de $[\![1, n]\!]$, notées $(a_1, .., a_{n-2})$ et $(b_1, .., b_{n-2})$. On doit montrer qu'il existe un élément σ de $\mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$ pour tout $1 \leq i \leq n-2$. On commence par noter a_{n-1} et a_n (resp. b_{n-1} et b_n) les deux éléments de $[\![1, n]\!]$ qui ne sont pas dans la famille $(a_i)_{1\leq i\leq n-2}$ (resp. $(b_i)_{1\leq i\leq n-2}$), puis on se donne une permutation $\sigma \in \mathfrak{S}_n$ telle que $\sigma(a_i) = b_i$ pour tout $1 \leq i \leq n$ (σ existe car l'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]$ est n-transitive). Si σ est paire, alors $\sigma \in \mathfrak{A}_n$ convient. Sinon, la permutation $\sigma(a_{n-1}\ a_n) \in \mathfrak{A}_n$ convient. □

On déduit de ce lemme que pour $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$: en effet, si l'on se donne deux cycles $(a_1\ a_2\ a_3)$ et $(b_1\ b_2\ b_3)$, puisque $n - 2 \geq 3$, l'action de $\mathfrak{A}_n$ sur $[\![1, n]\!]$ est 3-transitive, et donc il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$ pour tout $1 \leq i \leq 3$. Ainsi, on a

$$(b_1\ b_2\ b_3) = \sigma(a_1\ a_2\ a_3)\sigma^{-1}.$$

Étape 2. Simplicité de $\mathfrak{A}_5$.

Le même raisonnement permet de montrer que les bitranspositions $(a_1\ a_4)(a_2\ a_5)(a_3)$ et $(b_1\ b_4)(b_2\ b_5)(b_3)$ sont conjuguées dans $\mathfrak{A}_5$.

On se donne maintenant un sous-groupe distingué $H \lhd \mathfrak{A}_5$ différent de $\{\mathrm{id}\}$. Commençons par lister les 60 éléments de $\mathfrak{A}_5$:

- l'identité
- les éléments d'ordre 2 sont les bitranspositions, il y en a 15
- les éléments d'ordre 3 sont les 3-cycles, il y en a 20
- les éléments d'ordre 5 sont les 5-cycles, il y en a 24

Si H contient les éléments d'ordre 2 (resp. 3), il les contient tous d'après ce qui précède (resp. d'après l'étape 1). De plus, si H contient un 5-cycle, il contient le sous-groupe qu'il engendre, qui est un 5-Sylow de $\mathfrak{A}_5$. Comme les 5-Sylows sont conjugués, il les contient tous, et donc il contient tous les 5-cycles. Comme H n'est pas réduit au neutre, il contient au moins un de ces trois types d'éléments. Comme $1 + 15, 1 + 20$ et $1 + 24$ ne divisent pas 60, H ne peut pas contenir un seul de ces trois types d'éléments. Ainsi, son cardinal est au moins $1 + 15 + 20 = 36$, mais comme il divise 60, il est égal à 60. Donc $H = \mathfrak{A}_5$. On en déduit bien que $\mathfrak{A}_5$ est simple.

Étape 3. Simplicité de $\mathfrak{A}_n$.

On se donne cette fois un sous-groupe distingué $H \lhd \mathfrak{A}_n$ différent de $\{\mathrm{id}\}$, et on prend $\sigma \in H$ non trivial. On va se ramener au cas de l'étape 2 en fabriquant à partir de σ un élément de H agissant sur $[\![1, 5]\!]$ (i.e. ayant $n - 5$ points fixes).

Comme σ n'est pas l'identité, il existe un élément $a \in [\![1, n]\!]$ tel que $\sigma(a) = b \neq a$. On se donne $c \in [\![1, n]\!]\backslash\{a, b, \sigma(b)\}$ (possible car $n > 3$). On note alors τ le 3-cycle $(a\ c\ b)$ (c'en est un puisque a, b et c sont distincts), et $\rho = [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c))$. Comme $b = \sigma(a)$, l'ensemble $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ possède au plus 5 éléments, et on suppose quitte à en rajouter qu'il y en a exactement 5. Alors les $n-5$ éléments qui ne sont pas dans F sont des points fixes de ρ. De plus,

$$\rho(b) = \tau\sigma\tau^{-1}(a) = \tau\sigma(b) \neq b$$

car $\tau^{-1}(b) = c \neq \sigma(b)$. Donc ρ n'est pas l'identité. Comme F possède 5 éléments, l'ensemble $\mathfrak{A}(F)$ de ses permutations paires est isomorphe à $\mathfrak{A}_5$, et il s'injecte bien sûr dans $\mathfrak{A}_n$ par extension en l'identité sur

$[\![1,n]\!]\backslash F$ d'un élément de $\mathfrak{A}(F)$ (l'identité est de signature 1). On pose alors $H_F = H \cap \mathfrak{A}(F)$ [18]. Bien sûr, H_F est distingué dans $\mathfrak{A}(F)$, et ρ est un élément non trivial de H_F. On en déduit, comme $\mathfrak{A}(F)$ est simple (car isomorphe à $\mathfrak{A}_5$), que $H_F = \mathfrak{A}_F$. Ainsi, H_F contient les 3-cycles de $\mathfrak{A}(F)$, et donc H contient leur prolongements, qui sont des 3-cycles de $\mathfrak{A}_n$. Mais comme les 3-cycles sont conjugués, H les contient tous. Or les 3-cycles engendrent $\mathfrak{A}_n$, donc $H = \mathfrak{A}_n$. □

Remarque. Le cas des groupes alternés pour $n \leq 4$ est simple à résoudre :

- $\mathfrak{A}_2$ est le groupe trivial
- $\mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est cyclique d'ordre premier, donc simple
- Le groupe dérivé de $\mathfrak{A}_4$ est le groupe de Klein V_4, qui est non trivial, donc $\mathfrak{A}_4$ n'est pas simple

18. Ici, on identifie les éléments de $\mathfrak{A}(F)$ avec leur prolongement comme éléments de $\mathfrak{A}_n$.

16 Table de caractère de $\mathfrak{S}_4$ et tétraèdre

Leçons 105, 107, 161(, 101, 103, 104, 160)

Ref : [CG13]

On propose ici de déterminer la table de caractère du groupe symétrique $\mathfrak{S}_4$ en étudiant son action sur le tétraèdre régulier, puis d'en déduire l'ensemble de ses sous-groupes distingués. On utilisera pour cela le résultat suivant (qui fait également l'objet d'un développement, voir développement 1). Je n'ai pas de référence exacte pour ce développement. La deuxième étape est dans [CG13] (et est d'ailleurs l'objet du développement 8), la première et la quatrième utilisent les techniques basiques d'études des tables de caractère, et la troisième étape se fait bien quand on visualise correctement le tétraèdre.

Théorème 16.1 Soit G un groupe fini de cardinal n et de caractères irréductibles $\chi_1, .., \chi_m$. Alors les sous-groupes distingués de G sont exactement les sous-groupes H_I de la forme

$$H_I := \bigcap_{i \in I} \ker(\chi_i),$$

où I désigne une partie quelconque de $[\![1, m]\!]$.

On énonce le résultat principal de ce développement.

Théorème 16.2 (Table de $\mathfrak{S}_4$) On note Δ le tétraèdre régulier, et $\mathrm{Iso}(\Delta)$ son groupe d'isométries. Alors $\mathrm{Iso}(\Delta)$ est isomorphe à $\mathfrak{S}_4$. On peut alors en déduire la table de caractère de $\mathfrak{S}_4$, qui est la suivante :

$\mathfrak{S}_4$	id 1	(1 2) 6	(1 2 3) 8	(1 2)(3 4) 3	(1 2 3 4) 6
$\mathbb{1}$	1	1	1	1	1
ε	1	-1	1	1	-1
χ_2	2	0	-1	2	0
χ_Δ	3	1	0	-1	-1
$\varepsilon\chi_\Delta$	3	-1	0	-1	1

Démonstration. Étape 1. Les deux premières lignes.

On commence par rappeler que les classes de conjugaisons de $\mathfrak{S}_4$ sont les sous-groupes des permutations de même profil. On les dénombre ainsi :

- l'identité
- $\binom{4}{2} = 6$ transpositions
- $2\times\binom{4}{3} = 8$ 3-cycles
- $\frac{1}{2}\times\binom{4}{2} = 3$ bitranspositions
- 3! 4-cycles

On en déduit que la table possède 5 lignes et 5 colonnes. De plus, les deux premiers caractères sont donnés par le morphisme trivial et le morphisme signature, ce qui donne les deux premières lignes de la table :

$\mathfrak{S}_4$	id 1	(1 2) 6	(1 2 3) 8	(1 2)(3 4) 3	(1 2 3 4) 6
$\mathbb{1}$	1	1	1	1	1
ε	1	-1	1	1	-1

Étape 2. Groupe d'isométries du tétraèdre.

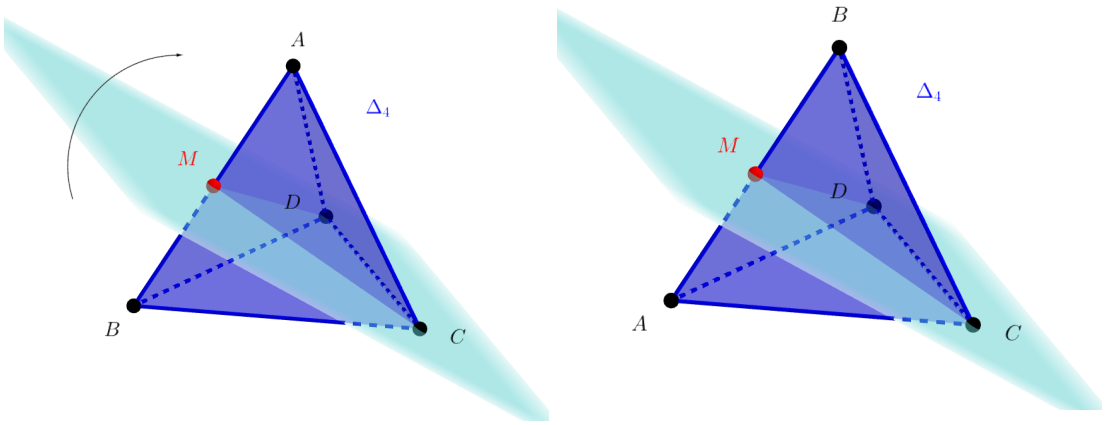
On cherche à connaître le groupe des isométries du tétraèdre, dont on note A, B, C et D les sommets (voir figure 16.1). On définit le morphisme de groupes

$$\varphi : \left| \begin{array}{ccc} \mathrm{Iso}(\Delta) & \longrightarrow & \mathfrak{S}_4 \\ f & \longmapsto & f_{|\Delta} \end{array} \right.$$

Ce morphisme est bien défini puisque Δ est par définition stable par les éléments de $\mathrm{Iso}(\Delta)$. On va montrer que φ est bijectif.

- On se donne f tel que $\varphi(f)$ est l'identité. Puisque les vecteurs AB, AC, et AD forment une base de $\mathbb{R}^3$, l'image de f sur cette base caractérise f, et donc f est l'identité sur $\mathbb{R}^3$. Donc φ est injectif.
- On veut maintenant montrer que φ est surjectif. On cherche tout d'abord un antécédent à la permutation $(A\ B)$. On doit trouver une isométrie qui échange A et B sans toucher à C et D. On note alors M le milieu de $[AB]$, et on considère la réflexion de plan (CDM), qui est bien une isométrie, et qui effectue exactement les déplacements recherchés. Donc $(A\ B)$ est dans l'image de φ, et par symétrie de la figure, toutes les transpositions aussi. Or les transpositions engendrent $\mathfrak{S}_4$, donc tous les éléments de $\mathfrak{S}_4$ sont dans l'image. Donc φ est surjectif.

On en déduit donc que le groupe des isométries du tétraèdre est $\mathfrak{S}_4$.



(a) Tétraèdre régulier Δ et plan (CDM)

(b) Tétraèdre après transformation par la réflexion de plan (CDM)

Figure 16.1 – Tétraèdre régulier Δ et isométries

□

Étape 3. Interprétation géométrique des éléments de $\mathfrak{S}_4$ et caractère associé.

On déduit de l'isomorphisme précédent une représentation linéaire du groupe $\mathfrak{S}_4$ de dimension 3 :

$$\rho : \mathfrak{S}_4 \simeq \mathrm{Iso}(\Delta) \hookrightarrow O_3(\mathbb{R}) \hookrightarrow GL_3(\mathbb{C}).$$

On va calculer son caractère χ_Δ et observer qu'il est irréductible. Pour cela, on doit interpréter géométriquement l'action de chaque profil de permutation sur le tétraèdre.

- Bien sûr, on a $\chi_\Delta(\mathrm{id}) = \dim(\mathbb{C}^3) = 3$.
- On a vu que les transpositions correspondaient à une réflexion, et ont donc la forme $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ dans la bonne base. On a donc $\chi_\Delta((1\ 2)) = 1$.
- Les 3-cycles correspondent à des rotations d'angle $\dfrac{2\pi}{3}$ de l'hyperplan parallèle à la base formée par les trois points déplacés. Donc on a

$$\chi_\Delta((1\ 2\ 3)) = 1 + 2\cos\left(\frac{2\pi}{3}\right) = 0.$$

– Les bitranspositions consistent à échanger deux couples de points. Par exemple, pour la bitransposition (1 2)(3 4), on fixe le milieu M de (AB) et le milieu N de (CD). Alors la rotation d'angle π et d'axe (MN) échange correctement A et B ainsi que C et D. Ainsi, on a

$$\chi_\Delta((1\ 2)(3\ 4)) = 1 + 2\cos(\pi) = -1.$$

– On cherche à étudier l'action du 4-cycle (1 2 3 4). On note O le centre de gravité du tétraèdre, et on se place dans la base $(\overrightarrow{OA}, \overrightarrow{OB}, \overrightarrow{OC})$ de $\mathbb{R}^3$ pour chercher la matrice de la partie linéaire de la permutation (ou plutôt de l'isométrie affine f associée) et en déduire la trace. On a

$$O + \overrightarrow{OB} = B = f(A) = f(O + \overrightarrow{OA}) = f(O) + \vec{f}(\overrightarrow{OA}) = O + \vec{f}(\overrightarrow{OA}),$$

où $f(O) = O$ se déduit du fait que f préserve les barycentres (et donc les centres de gravité) en tant qu'application affine. On obtient alors $\vec{f}(\overrightarrow{OA}) = \overrightarrow{OB}$. De même, $\vec{f}(\overrightarrow{OB}) = \overrightarrow{OC}$ et $\vec{f}(\overrightarrow{OC}) = \overrightarrow{OD} = -(\overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC})$ (puisque O est le centre de gravité). Donc la matrice de f dans cette base s'écrit $\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$, et on a ainsi

$$\chi_\Delta((1\ 2\ 3\ 4)) = -1.$$

On vérifie que le caractère obtenu est de norme 1 :

$$1\times 9 + 6\times 1 + 9\times 0 + 3\mathbb{1} + 6\times 1 = 24 = |\mathfrak{S}_4|.$$

On peut donc l'ajouter à la table :

$\mathfrak{S}_4$	id 1	(1 2) 6	(1 2 3) 8	(1 2)(3 4) 3	(1 2 3 4) 6
$\mathbb{1}$	1	1	1	1	1
ε	1	-1	1	1	-1
χ_Δ	3	1	0	-1	-1

Étape 4. Détermination des deux dernières lignes.

Le produit des caractères signature et du tétraèdre fournissent un nouveau caractère irréductible, que l'on ajoute à la dernière ligne. De plus, on sait que la somme des carrés des dimensions des représentations irréductibles est 24, donc on sait que la dernière est de dimension 2. On peut ensuite compléter les cases manquantes en rappelant que les colonnes sont orthogonales (et la première colonne est complète). On obtient finalement la table complète :

$\mathfrak{S}_4$	id 1	(1 2) 6	(1 2 3) 8	(1 2)(3 4) 3	(1 2 3 4) 6
$\mathbb{1}$	1	1	1	1	1
ε	1	-1	1	1	-1
χ_2	2	0	-1	2	0
χ_Δ	3	1	0	-1	-1
$\varepsilon\chi_\Delta$	3	-1	0	-1	1

Corollaire 16.3 Les sous-groupes propres distingués de $\mathfrak{S}_4$ sont $\mathfrak{A}_4$ et V_4.

Démonstration. On étudie la table obtenue sous le prisme du théorème 16.1. On a

– $\ker(\mathbb{1}) = \mathfrak{S}_4$
– $\ker(\varepsilon) = \mathfrak{A}_4$
– $\ker(\chi_2) = V_4$
– $\ker(\chi_\Delta) = \ker(\varepsilon\chi_\Delta) = \{\mathrm{id}\}$

Comme ces groupes sont inclus les uns dans les autres, cette liste fournit tous les sous-groupes distingués de $\mathfrak{S}_4$. □

17 Théorème de Burnside

Leçons 104, 106, 157

Ref : [FGN09b] 3.6, 2.33, 1.10

Ce développement consiste à démontrer le résultat suivant concernant les sous-groupes multiplicatifs de matrices.

Théorème 17.1 (Burnside) Soit $n \geq 1$ un entier et G un sous-groupe de $GL_n(\mathbb{C})$. Si G est d'exposant fini $N \geq 1$, i.e.

$$\forall A \in G \quad A^N = I_n,$$

alors G est fini.

Démonstration.

Étape 1. Un lemme sur les matrices nilpotentes.

On commence par démontrer le lemme suivant.

Lemme 17.2 Soit $A \in \mathcal{M}_n(\mathbb{C})$. Si pour tout entier $k \geq 1$, la trace de A^k est nulle, alors A est nilpotente.

Soit donc A une matrice telle que

$$\forall k \geq 1, \quad \mathrm{Tr}(A^k) = 0.$$

On suppose par l'absurde que A n'est pas nilpotente. Son polynôme caractéristique χ_A est scindé sur $\mathbb{C}$, et comme A n'est pas nilpotente, ce polynôme possède des racines non nulles. On note alors $\lambda_1, .., \lambda_r$ les racines non nulles de χ_A, et $n_1, .., n_r$ leur multiplicités (strictement positives) respectives (et n_0, éventuellement nulle, celle de 0). Ainsi, il existe une matrice $P \in GL_n(\mathbb{C})$ et une matrice T triangulaire supérieure avec une diagonale $(\underbrace{0, .., 0}_{n_0}, \underbrace{\lambda_1, .., \lambda_1}_{n_1}, .., \underbrace{\lambda_r, ..\lambda_r}_{n_r})$ telles que $A = PTP^{-1}$. Ainsi, on a

$$\forall k \geq 1, \quad 0 = \mathrm{Tr}(A^k) = \mathrm{Tr}(T^k) = \sum_{i=1}^{r} n_i \lambda_i^k.$$

On en déduit que le vecteur $\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix}$ est solution (non nulle) du système $VX = 0$ où $X \in \mathbb{C}^r$ est l'inconnue et

$$V = \begin{pmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_r \\ \lambda_1^2 & \lambda_2^2 & \dots & \lambda_r^2 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^r & \lambda_2^r & \dots & \lambda_r^r \end{pmatrix} \in \mathcal{M}_r(\mathbb{C})$$

est la donnée. Or puisque les λ_i sont tous non nuls, cette matrice V est inversible[2], ce qui est absurde. Donc A est bien nilpotente.

Étape 2. Introduction d'une injection de G dans un espace vectoriel complexe.

On se donne une base $(M_i)_{1 \leq i \leq m}$ du sous-espace vectoriel $F := \mathrm{vect}(G)$ de $\mathcal{M}_n(\mathbb{C})$, et on définit l'application

$$f : \left| \begin{array}{ccc} G & \longrightarrow & \mathbb{C}^m \\ A & \longmapsto & (\mathrm{Tr}(AM_i))_{1 \leq i \leq m} \end{array} \right.$$

On va montrer que f est injective. On se donne donc deux éléments de G, A et B, et on suppose $f(A) = f(B)$. On va commencer par montrer que $AB^{-1} - I_n$ est nilpotente, en appliquant le lemme. On pose $D := AB^{-1} \in G$. Alors, pour tout $k \geq 1$, puisque G est un groupe, $B^{-1}D^{k-1}$ est un élément de G.

2. En effet, en factorisant le déterminant de V par $\prod_{i=1}^{r} \lambda_i \neq 0$, on obtient un déterminant de Vandermonde. Finalement, puisque les λ_i sont distincts, V est de déterminant $\prod_{i=1}^{r} \lambda_i \prod_{1 \leq i < j \leq r} \lambda_j - \lambda_i$ (formule obtenue par récurrence sur r) non nul, et donc inversible.

De plus, on a $\mathrm{Tr}(D^k) = \mathrm{Tr}(AB^{-1}D^{k-1})$. Mais comme $f(A) = f(B)$, et comme la trace est additive, on a pour tout $M \in G$

$$\mathrm{Tr}(AM) = \mathrm{Tr}(BM).$$

On en déduit donc

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

Donc par récurrence, D^k est de trace n pour tout entier $k \geq 0$. On a alors

$$\begin{aligned}
\mathrm{Tr}((D-I_n)^k) &= \mathrm{Tr}\left(\sum_{i=0}^{k}\binom{k}{i}D^i I_n^{k-i}\right) \quad \text{car } I_n \text{ et } D \text{ commutent} \\
&= \sum_{i=0}^{k}\binom{k}{i}(-1)^{k-i}\,\mathrm{Tr}(D^i) \\
&= n\sum_{i=0}^{k}\binom{k}{i}(-1)^{k-i} \\
\mathrm{Tr}((D-I_n)^k) &= n(1-1) = 0
\end{aligned}$$

Donc d'après le lemme, $D - I_n = AB^{-1} - I_n$ est nilpotente.

On rappelle maintenant que comme N est l'exposant de G, le polynôme $X^N - 1$ annule tous les éléments de G. Or, comme ce polynôme est scindé à racines simples, tout élément de G est donc diagonalisable. Donc AB^{-1} est diagonalisable, et donc $AB^{-1} - I_n$ aussi [19]. Or cette matrice est nilpotente ; elle est donc nulle. On en déduit que $AB^{-1} = I_n$, c'est-à-dire $A = B$. Donc f est injective.

Étape 3. Plongement de G dans un ensemble fini.

On va conclure en montrant que l'image de f est finie. On note $X := \{\mathrm{Tr}(A),\ A \in G\}$. Comme $X^N - 1$ annule les éléments de G, leur valeurs propres sont des racines N-ièmes de l'unité. Ainsi, X est fini, de cardinal inférieur à Nn. Or comme pour tout $A \in G$, et pour tout $i \in [\![1, m]\!]$, AM_i est dans G, on en déduit que l'image $f(G)$ est inclue dans X^m, qui est de cardinal inférieur à Nnm. Or f est injective d'après l'étape précédente, donc G est également de cardinal inférieur à Nnm, donc fini. □

19. Car si M et N sont deux matrices diagonalisables qui commutent, leur somme l'est aussi.

Chapitre II

Analyse

1 Banach-Steinhauß et séries de Fourier

Leçons 205, 208, 246(, 241)

Ref : [BB18]

La convergence des séries de Fourier pose souvent problème, et les théorèmes nécessitent des hypothèses plus forte que la simple continuité de la fonction étudiée. Ce développement permet justement d'affirmer que l'hypothèse de classe C^1 par morceaux du théorème de Dirichlet est nécessaire, et qu'il existe des fonctions continues dont la série de Fourier ne converge pas. Plus précisément, s'il est possible de donner un contre-exemple explicite, on va ici utiliser un résultat d'analyse fonctionnelle pour montrer qu'il en existe en fait beaucoup.

On peut donner deux versions de ce développement, selon les leçons dans lesquelles on souhaite le placer. Un premier axe consiste à démontrer le théorème de Banach-Steinhauß puis le premier théorème sur les séries de Fourier, pour les leçons 205 et 208. La seconde option demande d'admettre Banach-Steinhauß pour prendre le temps de démontrer le résultat plus précis sur les séries de Fourier, qui est le deuxième point du développement rédigé dans [BB18], ce qui colle très bien avec la leçon 246, et qui peut rentrer éventuellement dans la 241.

Théorème 1.1 (Banach-Steinhauß) Soit $(E, \|\cdot\|_E)$ un espace de Banach, $(F, \|\cdot\|_F)$ un espace vectoriel normé, et $(T_i)_{i\in I}$ une famille d'applications linéaires continues de E vers F. Alors l'une (et une seule) des affirmations suivantes est vérifiée :

(i) la famille $(T_i)_{i\in I}$ est bornée dans $\mathcal{L}(E, F)$

(ii) il existe un G_δ dense D de E tel que

$$\forall x \in A \quad \sup_{i\in I} \|T_i(x)\|_F = +\infty.$$

Démonstration. On rappelle qu'un G_δ est une intersection dénombrable d'ouverts de E. Il est clair que les deux assertions proposées sont contradictoires. Dans la suite, on cherche donc à montrer que l'une des deux est vérifiée, et l'autre ne l'est donc pas. On pose pour $n \geq 1$

$$D_n := \left\{ x \in E,\ \sup_{i\in I} \|T_i(x)\|_F > n \right\}.$$

On voit que D_n est l'union d'ensembles de la forme $\{x \in E,\ \|T_i(x)\|_F > n\}$, qui sont des ouverts de E en tant qu'image réciproque d'ouverts de $\mathbb{R}$ par des applications continues. Donc D_n est un ouvert de E. On traite alors deux cas.

– **1er cas :** Tous les D_n sont denses dans E.
On applique alors le théorème de Baire (c'est licite car E est complet). L'ensemble

$$D := \bigcap_{n\geq 1} D_n$$

est dense, et c'est par définition un G_δ. De plus, par définition, D vérifie le point (ii) du théorème.

– **2è cas :** Il existe un entier n_0 tel que D_{n_0} n'est pas dense dans E.
Alors il existe $x_0 \in E$ et $r_0 > 0$ tel que $D_n \cap B(x_0, r_0) = \emptyset$. On en déduit

$$\forall x \in B(x_0, r_0)\ \forall i \in I \quad \|T_i(x)\|_F \leq n_0.$$

Ainsi, pour x dans la boule unité de E, on a

$$r_0 \|T_i(x)\|_F = \|T_i(r_0 x)\|_F \leq \|T_i(r_0 x + x_0)\|_F + \|T_i(x_0)\|_F \leq 2n_0.$$

Donc tous les T_i sont de norme inférieure à $\dfrac{2n_0}{r_0}$, et on est dans le cas (i).

□

Application 1.2 Il existe un G_δ dense D de $\left(C^0(\mathbb{T}), \|\cdot\|_\infty\right)$ (espace des fonctions continues 2π-périodiques sur $\mathbb{R}$ à valeurs complexes, muni de la norme uniforme) tel que pour toute fonction $f \in D$, la somme partielle de la série de Fourier [1]

$$S_N(f) = D_N * f = \sum_{n=-N}^{N} c_n(f) e_n$$

diverge en 0.

Démonstration. On note E l'espace donné dans l'énoncé, qui est de Banach. On note aussi $F = (\mathbb{C}, |\cdot|)$, et on pose pour $N \geq 0$

$$T_N : \left| \begin{array}{ccc} E & \longrightarrow & F \\ f & \longmapsto & S_N(f)(0) \end{array} \right.$$

Les applications T_N sont bien sûr linéaires. On va montrer qu'elles sont continues : soit $N \geq 0$ et $f \in E$. On a

$$|T_N(f)| \leq \frac{1}{2\pi} \int_{-\pi}^{\pi} |D_N(-t) f(t)|\ dt = \frac{1}{2\pi} \int_{-\pi}^{\pi} |D_N(t)||f(t)|\ dt \leq \|f\|_\infty \|D_N\|_{L^1},$$

en utilisant la parité des noyaux de Dirichlet. Donc T_N est continue et de norme inférieure à $\|D_N\|_{L^1}$. On va montrer que l'on a trouvé la bonne norme. Pour exhiber un élément qui tel que l'inégalité du dessus soit une égalité, il faudrait que f soit du signe de D_N, et de valeur absolue constante ; mais c'est impossible pour une fonction continue, puisque D_N change de signe. On va cependant créer une approximation du signe de D_N : on note, pour $\varepsilon > 0$

$$f_\varepsilon : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{C} \\ t & \longmapsto & \dfrac{D_N(t)}{|D_N(t)| + \varepsilon} \end{array} \right.$$

On voit que f_ε converge simplement vers le signe de D_N, et est majoré par 1. Ainsi, la quantité $\dfrac{(D_N(t))^2}{|D_N(t)| + \varepsilon}$ converge simplement à t fixé vers $|D_N(t)|$ quand ε tend vers 0, et est borné par $|D_N(t)|$, qui est intégrable et indépendante de ε. Donc, par convergence dominée, on a

$$T_N(f_\varepsilon) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{(D_N(t))^2}{|D_N(t)| + \varepsilon} dt \underset{\varepsilon \to 0}{\longrightarrow} \|D_N\|_{L^1},$$

et donc T_N est de norme $\|D_N\|_{L^1}$. On s'intéresse maintenant à la norme obtenue. On a, pour $N \geq 0$

$$\begin{aligned}
\|D_N\|_{L^1} &= \frac{1}{2\pi} \int_{-pi}^{\pi} \left| \frac{\sin\left(\left(N + \frac{1}{2}\right) t\right)}{\sin\left(\frac{t}{2}\right)} \right| dt \\
&= \frac{1}{\pi} \int_{0}^{\pi} \left| \frac{\sin\left(\left(N + \frac{1}{2}\right) t\right)}{\sin\left(\frac{t}{2}\right)} \right| dt \qquad \text{par parité} \\
&\geq \frac{2}{\pi} \int_{0}^{\pi} \left| \frac{\sin\left(\left(N + \frac{1}{2}\right) t\right)}{t} \right| dt \qquad \text{car } \sin\left(\frac{t}{2}\right) \leq \frac{t}{2} \\
\|D_N\|_{L^1} &\geq \frac{2}{\pi} \int_{0}^{\left(N+\frac{1}{2}\right)\pi} \left| \frac{\sin(u)}{u} \right| du \qquad \text{par changement de variable } u = \left(N + \frac{1}{2}\right) t
\end{aligned}$$

1. On définit auparavant les polynômes trigonométriques $e_n(t) = \mathrm{e}^{int}$ et les noyaux de Dirichlet D_N.

Or l'intégrale obtenue diverge, donc la norme de D_N, et donc celle de T_N, tend vers l'infini quand N tend vers l'infini. En appliquant le théorème de Banach-Steinhauß aux applications $(T_N)_{N\geq 0}$, on voit que l'on ne peut donc pas être dans le cas (i), et qu'il existe donc un G_δ dense D de $C^0(\mathbb{T})$ tel que pour tout élément f de D, la suite $(S_N(f)(0))_{N\geq 0}$ n'est pas bornée, et donc la somme partielle de la série de Fourier de f diverge. □

On peut même obtenir un résultat plus fort.

Application 1.3 Il existe un G_δ dense $\widetilde{D}$ de $\left(C^0(\mathbb{T}), \|\cdot\|_\infty\right)$ tel que pour toute fonction $f \in \widetilde{D}$, il existe un G_δ dense Δ_f de $\mathbb{R}$ tel que la série de Fourier de f diverge en tout point de Δ_f.

2 Escalier de Cantor

Leçons 228, 261(, 229)

Ref : [BP15] 14.3

Toute fonction continue croissante dérivable de dérivée nulle sur $[0,1]$ est constante. Le but de ce développement est de fournir un contre-exemple dans le cas où l'hypothèse de dérivée nulle est affaiblie, au sens où l'on suppose seulement que la dérivée est nulle presque partout.

Théorème 2.1 (Construction de l'escalier de Cantor) Il existe une fonction f continue croissante sur $[0,1]$ telle que

$$\begin{cases} f(0) = 0 \\ f(1) = 1 \\ f' = 0 \ \ \lambda\text{-presque partout sur } [0,1] \end{cases}$$

On peut également énoncer le même théorème dans une version probabiliste : on sait que si une loi est absolument continue par rapport à la mesure de Lebesgue, elle est à densité et sa fonction de répartition est continue. En revanche, la réciproque est fausse, et ce résultat en est un contre-exemple.

Théorème 2.2 Il existe une loi de probabilité continue qui n'est pas absolument continue.

Démonstration. L'idée consiste à construire une suite de fonctions continues qui converge absolument sur $[0,1]$, et qui possède les propriétés de f, sauf celle de dérivée nulle, puis de passer à la limite pour déduire l'existence de f. On se base sur la définition de l'ensemble de Cantor pour construire cette suite de fonctions.

Étape 1. Définition d'une suite de fonctions continues croissantes.

On définit la suite $(A_n)_{n\in\mathbb{N}}$ de parties de $[0,1]$ par

$$\begin{cases} A_0 = [0,1] \\ A_{n+1} = \dfrac{1}{3}A_n \cup \dfrac{1}{3}(2 + A_n), \quad \forall n \in \mathbb{N} \end{cases}$$

On vérifie immédiatement par récurrence que l'ensemble A_n est alors la réunion de 2^n intervalles disjoints de longueur 3^{-n} inclus dans $[0,1]$, et ainsi que $\lambda(A_n) = \left(\dfrac{2}{3}\right)^n$. On peut démontrer que l'*ensemble de Cantor*, défini par

$$A = \bigcap_{n\geq 0} A_n,$$

est un borélien de mesure nulle mais équipotent à $[0,1]$. On pose alors pour $x \in [0,1]$

$$f_n(x) := \left(\frac{3}{2}\right)^n \int_0^x \mathbb{1}_{A_n}(t)\ dt.$$

Il est clair que $f_n(0) = 0$, et, au vu de la remarque précédente, que $f_n(1) = 1$. De plus, en tant qu'intégrale d'une fonction positive, f_n est une fonction continue croissante sur $[0,1]$ (comme on peut le voir pour les premiers éléments sur la figure 2.1). Au vu de ces propriétés, f_n est la fonction de répartition d'une variable aléatoire à valeurs dans $[0,1]$ presque sûrement. La loi sous-jacente est, au vu de la formule, la loi uniforme sur A_n, qui est à densité par rapport à la mesure de Lebesgue.

Étape 2. Majoration de la différence entre deux éléments successifs.

On fixe $n \geq 0$ et on se donne l'un des 2^n intervalles compacts I qui compose A_n.

- Comme I est un intervalle de longueur 3^{-n} inclus dans A_n, on a

$$\left(\frac{3}{2}\right)^n \int_I \mathbb{1}_{A_n}(t)\ dt = 2^{-n}.$$

- Comme $I \cap A_{n+1}$ est un la réunion de deux intervalles compacts et disjoints trois fois plus petits que I, on a $\lambda(I \cap A_{n+1}) = \dfrac{2}{3}\lambda(A_n) = \dfrac{2}{3^{n+1}}$, et donc

$$\left(\frac{3}{2}\right)^{n+1} \int_I \mathbb{1}_{A_{n+1}}(t)\ dt = 2^{-n}.$$

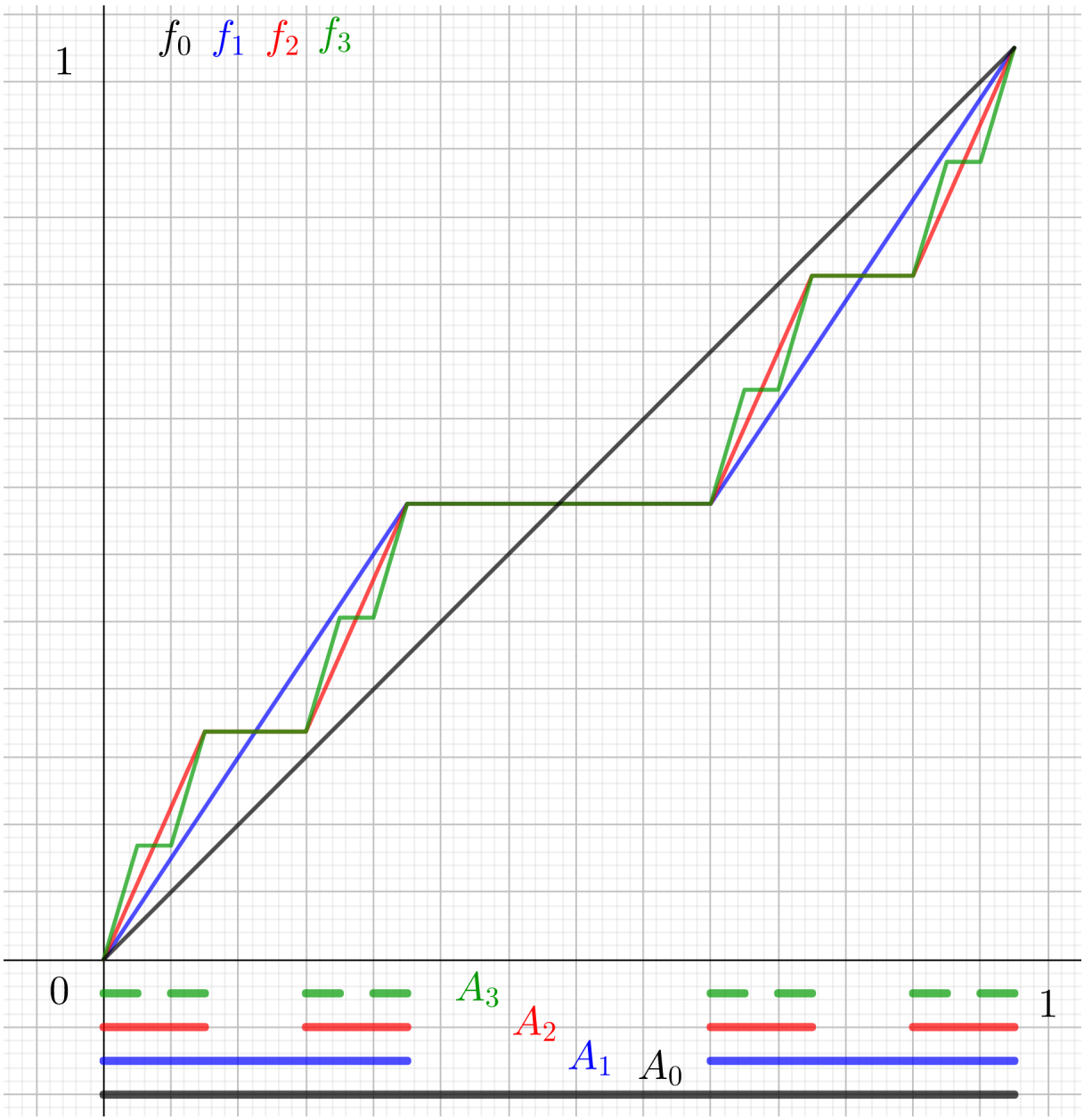


Figure 2.1 – Les premiers éléments de la suite approchant l'escalier de Cantor

Du point de vue probabiliste, les deux valeurs calculées sont $\mathbb{P}(X_n \in I)$ et $\mathbb{P}(X_{n+1} \in I)$. On obtient le premier résultat en observant que la loi de X_n est uniforme sur A_n, qui est composé de 2^n intervalles disjoints de même taille que I, et le second en observant que la loi de X_{n+1} est uniforme sur A_{n+1}, et que chaque composante de A_n correspond à deux composantes de A_{n+1}, et donc que l'événement $X_{n+1} \in I$ correspond à la réunion de deux événements $X_{n+1} \in I_1$ et $X_{n+1} \in I_2$, où I_1 et I_2 sont deux des 2^{n+1} composantes de A_{n+1}, et que sa probabilité est donc $2{\times}2^{-(n+1)}$.

On remarque que comme $\mathbb{1}_{A_n}$ s'annule sur les $2^n - 1$ intervalles ouverts J qui composent A_n^c, f_n est constante sur ces intervalles ; de même f_{n+1} l'est puisque $A_n^c \subset A_{n+1}^c$. Ainsi, en utilisant le fait que les deux intégrales calculées plus haut sont égales, on obtient pour $x \in A_n^c$

$$\begin{aligned} f_n(x) &= \sum_{I \subset A_n \cap [0,x]} \left(\frac{3}{2}\right)^n \int_I \mathbb{1}_{A_n}(t)\, dt \\ &= \sum_{I \subset A_n \cap [0,x]} \left(\frac{3}{2}\right)^{n+1} \int_I \mathbb{1}_{A_{n+1}}(t)\, dt \\ f_n(x) &= f_{n+1}(x) \end{aligned}$$

en faisant porter les sommes sur les intervalles I composant A_n.

Ce calcul s'écrit aussi

$$f_n(x) = \mathbb{P}(X_n \leq x) = \mathbb{P}\left(\bigcup_{I \subset A_n \cap [0,x]} X_n \in I\right) = \mathbb{P}\left(\bigcup_{I \subset A_n \cap [0,x]} X_{n+1} \in I\right) = \mathbb{P}(X_{n+1} \leq x) = f_{n+1}(x).$$

Il reste à majorer la différence sur A_n. On se donne donc une nouvelle fois une composante I de A_n. En particulier, en posant $x_0 = \min(I)$, x_0 est également la borne supérieure d'un des intervalles ouverts J composant A_n^c, et comme f_n et f_{n+1} sont continues sur $J \cup I$ et égales sur J, on a $f_n(x_0) = f_{n+1}(x_0)$. On en déduit que pour $x \in I$, on a

$$\begin{array}{rcl} |f_{n+1}(x) - f_n(x)| & \leq & |f_{n+1}(x) - f_{n+1}(x_0)| + |f_n(x_0) - f_n(x)| \\ & = & \left(\frac{3}{2}\right)^{n+1} \int_{x_0}^{x} \mathbb{1}_{A_{n+1}}(t)\ dt + \left(\frac{3}{2}\right)^{n} \int_{x_0}^{x} \mathbb{1}_{A_n}(t)\ dt \\ & \leq & \left(\frac{3}{2}\right)^{n+1} \int_{I} \mathbb{1}_{A_{n+1}}(t)\ dt + \left(\frac{3}{2}\right)^{n} \int_{I} \mathbb{1}_{A_n}(t)\ dt \\ |f_{n+1}(x) - f_n(x)| & \leq & 2^{-n+1} \end{array}$$

On en déduit ainsi

$$\|f_{n+1} - f_n\|_\infty \leq 2^{-n+1},$$

résultat valable pour tout $n \geq 0$.

Étape 3. Conclusion par construction d'une limite.

La majoration uniforme de la différence entre deux termes successifs de la suite étant le terme général d'une série convergente, on en déduit que la suite $(f_n)_{n\geq 0}$ est de Cauchy dans l'espace complet des fonctions continues sur le compact $[0,1]$ (muni de la norme uniforme). Donc elle converge dans cet espace : c'est dire que la suite de fonction f_n converge uniformément vers une certaine fonction f, qui est donc nécessairement continue croissante sur $[0,1]$, et qui vérifie

$$\begin{cases} f(0) = 0 \\ f(1) = 1 \end{cases}$$

Comme par construction, pour $m \geq n$, A_n^c est inclus dans A_m^c, et on peut donc généraliser le raisonnement de l'étape 2 pour en déduire que f_n et f_m coïncident sur A_n^c. On en déduit donc que f et f_n coïncident sur A_n^c. Or f_n y est constante, donc dérivable et de dérivée nulle. Ainsi, f est dérivable et de dérivée nulle sur l'ouvert A^c complémentaire de l'ensemble de Cantor, qui est la réunion des A_n^c. Elle vérifie donc bien

$$f' = 0 \ \ \lambda\text{-presque partout},$$

puisque A est de mesure nulle. □

On peut construire une variable aléatoire X possédant f pour fonction de répartition (on peut appeler *loi de Cantor* cette loi de probabilité). Moralement, la construction nous incite à dire que X peut être vu comme un nombre choisi uniformément sur l'ensemble de Cantor A. Cela revient en fait à choisir aléatoirement le développement triadique d'un nombre compris entre $[0,1]$, en choisissant les chiffres de ce nombre en base 3 comme étant égal soit à 0, soit à 2, avec même probabilité : si Y_n sont des variables aléatoires indépendantes identiquement réparties de loi donnée par

$$\mathbb{P}(Y_1 = 0) = \mathbb{P}(Y_1 = 2) = \frac{1}{2},$$

alors la variable aléatoire

$$X := \sum_{n\geq 1} \frac{Y_n}{3^n}$$

suit la loi de Cantor.

3 Espace de Bergman

Leçons 201, 213, 234, 245(, 205, 208, 235, 243)

Ref : [BB18]

On étudie dans ce développement l'espace de Bergman du disque unité :

$$A^2(\mathbb{D}) := \mathcal{H}(\mathbb{D}) \cap L^2(\mathbb{D}).$$

C'est bien sûr un sous-espace vectoriel de $L^2(\mathbb{D})$, qui est donc muni du produit scalaire usuel

$$\langle f, g\rangle := \int_{\mathbb{D}} f(z)\overline{g(z)}\, dxdy,$$

dont on note $\|\cdot\|_2$ la norme associée.

Théorème 3.1 L'espace de Bergman $A^2(\mathbb{D})$ est un espace de Hilbert, dont une base hilbertienne est donnée par les fonctions

$$e_n : \left| \begin{array}{ccc} \mathbb{D} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \sqrt{\dfrac{n+1}{\pi}} z^n \end{array} \right. ,$$

pour $n \in \mathbb{N}$.

Démonstration.

Étape 1. Comparaison des normes $\|\cdot\|_\infty$ et $\|\cdot\|_2$.

On commence par démontrer un lemme qui donne un élément de comparaison entre les normes qui s'adaptent à la convergence des fonctions holomorphes et la norme sur L^2.

Lemme 3.2 Soit K un compact de $\mathbb{D}$. On a alors

$$\forall f \in A^2(\mathbb{D}) \qquad \|f\|_{\infty,K} \leq \frac{1}{\sqrt{\pi} d(K, \mathbb{S}^1)} \|f\|_2 .$$

On fixe $f \in A^2(\mathbb{D})$. Soit a un élément de K. Comme $\mathbb{D}$ est ouvert, il existe un certain réel $r > 0$ tel que la boule ouverte $B(a, r)$ soit incluse dans $\mathbb{D}$. On a alors, d'après la formule de la moyenne, pour tout $\rho \in (0, r)$:

$$f(a) = \frac{1}{2\pi} \int_0^{2\pi} f(a + \rho\, \mathrm{e}^{\mathrm{i}\theta})\, d\theta.$$

On multiplie alors par ρ, puis on intègre sur $(0, r)$, et on obtient finalement

$$f(a) = \frac{1}{\pi r^2} \int_0^r \int_0^{2\pi} f(a + \rho\, \mathrm{e}^{\mathrm{i}\theta})\rho\, d\rho d\theta = \frac{1}{\pi r^2} \int_{B(a,r)} f(z)\, dxdy.$$

Mais on peut alors appliquer l'inégalité de Cauchy-Scwharz, pour obtenir

$$\begin{aligned} |f(a)| &\leq \frac{1}{\pi r^2} \left(\int_{B(a,r)} |f(z)|^2 dxdy \right)^{\frac{1}{2}} \left(\int_{B(a,r)} dxdy \right)^{\frac{1}{2}} \\ |f(a)| &\leq \frac{1}{r\sqrt{\pi}} \|f\|_2 \end{aligned}$$

On fait maintenant tendre r vers $d(a, \mathbb{S}^1)$ pour obtenir

$$|f(a)| \leq \frac{\|f\|_2}{\sqrt{\pi} d(a, \mathbb{S}^1)}.$$

On conclut finalement en observant que $d(K, \mathbb{S}^1) \leq d(a, \mathbb{S}^1)$.

Étape 2. Complétude de l'espace de Bergman.

On se donne une suite de Cauchy $(f_n)_{n\geq 0}$ dans $A^2(\mathbb{D})$. Pour tout compact K de $\mathbb{D}$, et on a d'après le lemme

$$\forall m,n\in\mathbb{N} \qquad \|f_n-f_m\|_{\infty,K}\leq \frac{1}{\sqrt{\pi}d(K,\mathbb{S}^1)}\|f_m-f_n\|_2\,.$$

Cela signifie que la suite (f_n) est de Cauchy dans $C^0(K,\mathbb{C})$. Or on sait que la norme uniforme munit cet espace d'une structure de Banach, donc il existe une unique fonction f limite uniforme de la suite (f_n) sur chaque compact de $\mathbb{D}$. D'après le théorème de Weierstraß, on sait de plus que f est holomorphe sur $\mathbb{D}$.

Comme $L^2(\mathbb{D})$ est également complet, la suite (f_n) admet aussi une limite g dans $L^2(\mathbb{D})$. D'après le théorème de Riesz-Fisher, on sait aussi qu'il existe une suite extraite de (f_n) qui converge presque partout sur $\mathbb{D}$ vers g. Donc, puisque la suite (f_n) converge simplement (car uniformément) vers f, f et g coïncident presque partout sur $\mathbb{D}$. Ainsi, la suite (f_n) converge pour la norme L^2 (et donc celle que l'on a mise sur l'espace de Bergman) vers f, qui est donc un élément de $A^2(\mathbb{D})$.

Étape 3. Base hilbertienne de l'espace de Bergman.

On vérifie tout d'abord le caractère orthonormé : on se donne m et n deux entiers naturels, et on a

$$\begin{aligned}
\langle e_n,e_m\rangle &= \frac{\sqrt{(n+1)(m+1)}}{\pi}\int_{\mathbb{D}} z^n\overline{z}^m\,dxdy\\
&= \frac{\sqrt{(n+1)(m+1)}}{\pi}\left(\int_0^1 r^{n+m+1}dr\right)\left(\int_0^{2\pi}\mathrm{e}^{\mathrm{i}(n-m)\theta}\,d\theta\right)\\
&= \frac{2\sqrt{(n+1)(m+1)}}{n+m+2}\delta_{n,m}\\
\langle e_n,e_m\rangle &= \delta_{n,m}
\end{aligned}$$

On se donne maintenant une fonction $f\in A^2(\mathbb{D})$ orthogonale à $\mathrm{Vect}(e_n)_{n\in\mathbb{N}}$, c'est-à-dire que pour tout $n\in\mathbb{N}$, on a

$$c_n(f):=\langle f,e_n\rangle=0.$$

Comme f est holomorphe, elle est analytique sur $\mathbb{D}$, et donc en 0 : il existe une famille $(a_n)_{n\geq 0}$ de complexes telle que

$$\forall z\in\mathbb{D} \qquad f(z)=\sum_{n=0}^{+\infty}a_nz^n.$$

On a alors une nouvelle expression du coefficient de f contre e_n :

$$\begin{aligned}
c_n(f) &= \sqrt{\frac{n+1}{\pi}}\int_{\mathbb{D}} f(z)\overline{z}^n\,dxdy\\
&= \sqrt{\frac{n+1}{\pi}}\lim_{r\to 1}\left(\int_{|z|<r} f(z)\overline{z}^n\,dxdy\right) && \text{par convergence dominée, car } |f(z)\overline{z}^n|\leq|f|\in L^1\\
c_n(f) &= \sqrt{\frac{n+1}{\pi}}\lim_{r\to 1}\left(\sum_{k=0}^{+\infty}a_k\int_{|z|<r} z^k\overline{z}^n\,dxdy\right) && \text{par convergence normale de la série entière}
\end{aligned}$$

On calcule alors l'intégrale obtenue en passant aux coordonnées polaires (comme plus haut), pour $k\in\mathbb{N}$:

$$\int_{|z|<r} z^k\overline{z}^n\,dxdy=\frac{2\pi r^{n+k+2}}{n+k+2}\delta_{k,n}=\frac{\pi}{n+1}r^{2(n+1)}\delta_{k,n}.$$

Finalement, on obtient

$$c_n(f)=\sqrt{\frac{\pi}{n+1}}\lim_{r\to 1}\left(a_nr^{2(n+1)}\right)=\sqrt{\frac{\pi}{n+1}}a_n.$$

On en déduit que a_n est nul, et donc que f est nulle sur $\mathbb{D}$. Donc, par critère de densité, la famille $(e_n)_{n\geq 0}$ est une base hilbertienne de $A^2(\mathbb{D})$. □

On peut, si le temps le permet, aller plus loin et démontrer l'énoncé suivant, qui donne l'existence d'un noyau de reproduction pour les fonctions de $A^2(\mathbb{D})$:

Proposition 3.3 On pose pour $(\zeta,z)\in\mathbb{D}^2$

$$K(\zeta,z)=\frac{1}{\pi}\frac{1}{(1-\zeta\,\overline{z})^2}.$$

Alors $K(\zeta,\cdot) \in A^2(\mathbb{D})$ pour tout $\zeta \in \mathbb{D}$, et si T_K est l'opérateur à noyau associé à K sur $A^2(\mathbb{D})$, on a $T_K = \mathrm{Id}_{A^2(\mathbb{D})}$.

Démonstration. On voit tout d'abord que la fonction $K(\zeta,\cdot)$ est, à ζ fixé dans $\mathbb{D}$, holomorphe sur $\mathbb{D}$. De plus, la formule qui la définit donne une fonction continue sur $\overline{\mathbb{D}}$, qui compact, et elle est donc de carré intégrable sur $\mathbb{D}$. Donc $K(\zeta,\cdot) \in A^2(\mathbb{D})$.

On se donne une fonction $f \in A^2(\mathbb{D})$. On veut montrer que $T_K f = f$, c'est-à-dire que pour tout $\zeta \in \mathbb{D}$, on a

$$f(\zeta) = T_K f(\zeta) = \int_{\mathbb{D}} \frac{f(z)}{\pi(1-\zeta\,\overline{z})^2} dxdy = \left\langle f, \overline{K(\zeta,\cdot)} \right\rangle.$$

On cherche à calculer le produit scalaire obtenu par la formule de Parseval. On s'intéresse donc à la quantité

$$\left\langle e_n, \overline{K(\zeta,\cdot)} \right\rangle = \overline{\langle \overline{e_n}, K(\zeta,\cdot)\rangle} = \langle K(\zeta,\cdot), \overline{e_n}\rangle,$$

pour $n \in \mathbb{N}$. On a

$$\begin{aligned}
\langle K(\zeta,\cdot), \overline{e_n}\rangle &= \frac{\sqrt{n+1}}{\pi^{\frac{3}{2}}} \int_{\mathbb{D}} \frac{z^n}{(1-\zeta\,\overline{z})^2} dxdy \\
&= \frac{\sqrt{n+1}}{\pi^{\frac{3}{2}}} \int_{\mathbb{D}} \left(\sum_{k=0}^{+\infty} \zeta^k \overline{z}^k \right)' z^n \; dxdy \\
&= \frac{\sqrt{n+1}}{\pi^{\frac{3}{2}}} \int_{\mathbb{D}} \left(\sum_{k=0}^{+\infty} (k+1)\zeta^k \overline{z}^k \right) z^n \; dxdy \\
&= \frac{\sqrt{n+1}}{\pi^{\frac{3}{2}}} \sum_{k=0}^{+\infty} (k+1)\zeta^k \int_{\mathbb{D}} \overline{z}^k z^n dxdy \\
&= \frac{\sqrt{n+1}}{\pi^{\frac{3}{2}}} \sum_{k=0}^{+\infty} (k+1)\zeta^k \frac{2\pi}{2k+2} \delta_{n,k} \\
\langle K(\zeta,\cdot), \overline{e_n}\rangle &= \sqrt{\frac{n+1}{\pi}} \zeta^n.
\end{aligned}$$

La formule de Parseval donne alors, en notant une nouvelle fois a_n les coefficients du développement analytique de f en 0 :

$$\begin{aligned}
T_K f(\zeta) &= \left\langle f, \overline{K(\zeta,\cdot)} \right\rangle \\
&= \sum_{n=0}^{+\infty} \underbrace{\langle f, e_n\rangle}_{c_n(f)} \left\langle e_n, \overline{K(\zeta,\cdot)} \right\rangle \\
&= \sum_{n=0}^{+\infty} a_n \zeta^n \\
T_K f(\zeta) &= f(\zeta).
\end{aligned}$$

□

4 Formule des compléments

Leçons 236, 245(, 235, 239)

Ref : [BB18] ou [AM04] Sec. 8.4.4

Ce développement consiste à démontrer la formule relative à la fonction spéciale Γ d'Euler, définie sur $U := \{z \in \mathbb{C},\ \mathrm{Re}(z) > 0\}$ par

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

On utilisera la branche coprincipale du logarithme, définie sur l'ouvert $\mathbb{C}\backslash\mathbb{R}_+$ par

$$\mathrm{Log}(r\,\mathrm{e}^{\mathrm{i}\theta}) := \ln(r) + \mathrm{i}\theta \qquad \forall r \in \mathbb{R}_+^*, \forall \theta \in (0, 2\pi),$$

qui est bien sûr holomorphe. De même, la puissance d'un nombre complexe est classiquement définie par

$$z^x := \exp(x\,\mathrm{Log}(z)) \qquad \forall z \in \mathbb{C}\backslash\mathbb{R}_+, \forall x \in \mathbb{C}.$$

Théorème 4.1 (Euler, Formule des compléments) On note $\Omega := \{z \in \mathbb{C},\ \mathrm{Re}(z) \in (0,1)\}$. On a alors pour tout z dans Ω

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}.$$

Démonstration. On commence par démontrer le lemme suivant.

Lemme 4.2 Pour tout réel x dans $(0,1)$, on a

$$I(x) := \int_0^{+\infty} \frac{dt}{t^x(1+t)} = \frac{\pi}{\sin(\pi x)}.$$

Étape 1. Application du théorème des résidus.

On remarque tout d'abord que, d'après le critère de Riemann, la quantité $I(x)$ est bien définie pour $x \in (0,1)$. On définit la fonction

$$f : \left| \begin{array}{ccc} \mathbb{C}\backslash(\mathbb{R}_+ \cup \{-1\}) & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \dfrac{1}{z^x(1+z)} \end{array} \right.$$

Comme Log est holomorphe sur $\mathbb{C}\backslash\mathbb{R}_+$ et exp sur $\mathbb{C}$, et comme le dénominateur ne s'annule pas, f est holomorphe. Ainsi, on va pouvoir appliquer la formule de résidus : f admet -1 comme unique pôle sur $\mathbb{C}\backslash\mathbb{R}_+$. On définit alors pour $\varepsilon \in (0,1)$ et $R \in (1,+\infty)$ le contour fermé de classe C^1 par morceaux $\Gamma_{\varepsilon,R}$ comme la concaténation des chemins c_ε, $I^+_{\varepsilon,R}$, et $C_{\varepsilon,R}$ et $I^-_{\varepsilon,R}$ dessinés sur la figure 4.1. On notera également $\theta_{\varepsilon,R}$ l'angle qui paramètre l'arc de cercle $C_{\varepsilon,R}$, et on a d'après le théorème de Pythagore

$$\theta_{\varepsilon,R} = \arctan\left(\frac{\varepsilon}{\sqrt{R^2-\varepsilon^2}}\right).$$

Comme -1 est pôle d'ordre 1 de f, on a

$$\mathrm{Res}_{-1}(f) = \lim_{z\to-1}(z+1)f(z) = \mathrm{e}^{-\mathrm{i}\pi x}.$$

Le théorème des résidus permet donc d'affirmer que

$$\int_{\Gamma_{\varepsilon,R}} f(z)\ dz = 2\mathrm{i}\pi\,\mathrm{e}^{-\mathrm{i}\pi x}. \tag{4.1}$$

Étape 2. Calcul des différentes contributions.

On calcule maintenant les contributions asymptotiques des quatre chemins sur lesquels on intègre f, en faisant tendre ε vers 0 et R vers l'infini.

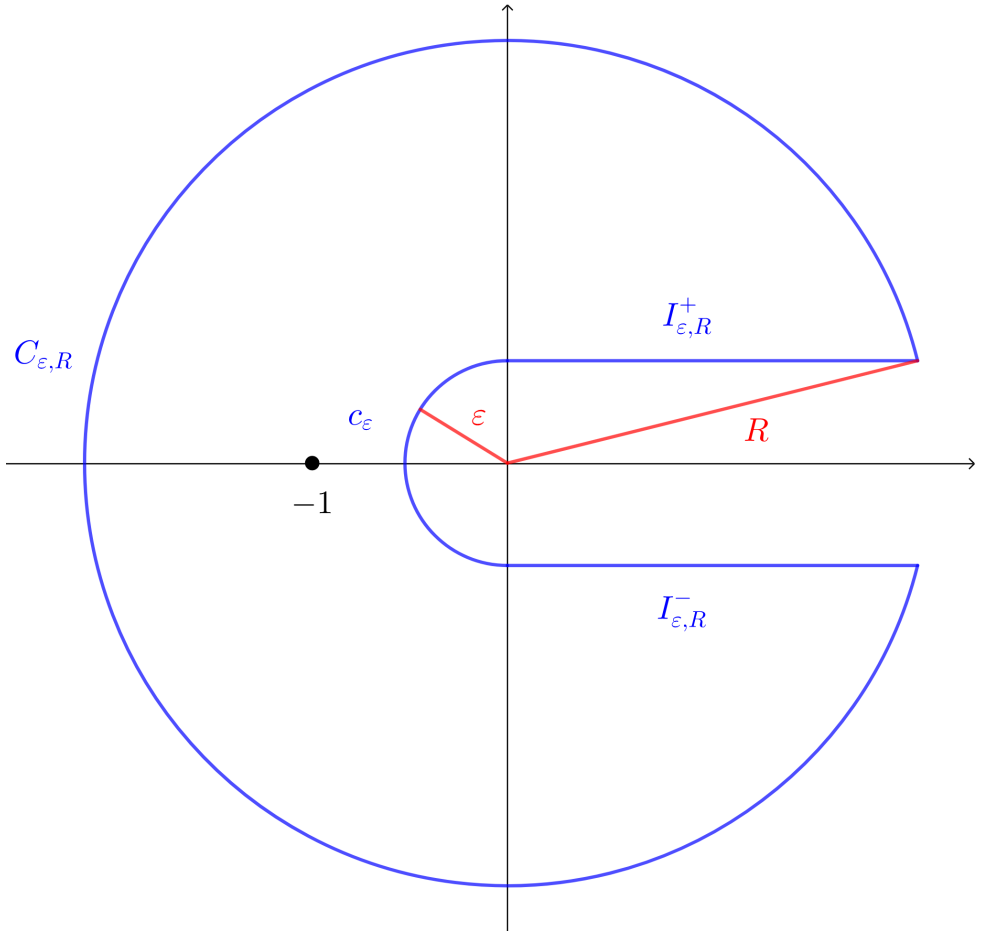


Figure 4.1 – Définition du lacet C^1_{pm} $\Gamma_{\varepsilon,R}$

– On paramètre le chemin $C_{\varepsilon,R}$ par

$$\gamma_1 : \left| \begin{array}{ccc} [\theta_{\varepsilon,R}, 2\pi - \theta_{\varepsilon,R}] & \longrightarrow & \mathbb{C} \\ t & \longmapsto & R\,\mathrm{e}^{\mathrm{i}t} \end{array} \right.$$

On a alors

$$\begin{aligned} \int_{C_{\varepsilon,R}} f(z)\,dz &= \int_{\theta_{\varepsilon,R}}^{2\pi-\theta_{\varepsilon,R}} f(R\,\mathrm{e}^{\mathrm{i}t})\mathrm{i}R\,\mathrm{e}^{\mathrm{i}t}\,dt \\ &= \int_{\theta_{\varepsilon,R}}^{2\pi-\theta_{\varepsilon,R}} \frac{\mathrm{i}R\,\mathrm{e}^{\mathrm{i}t}}{R^x\,\mathrm{e}^{\mathrm{i}tx}(1+R\,\mathrm{e}^{\mathrm{i}t})}dt \\ \int_{C_{\varepsilon,R}} f(z)\,dz &= \mathrm{i}\int_{\theta_{\varepsilon,R}}^{2\pi-\theta_{\varepsilon,R}} \frac{R^{1-x}\,\mathrm{e}^{\mathrm{i}(1-x)t}}{1+R\,\mathrm{e}^{\mathrm{i}t}}dt \end{aligned}$$

Or, au vu de son expression, $\theta_{\varepsilon,R}$ tend vers 0 quand ε tend vers 0, et la fonction intégrée est continue sur le compact $[0, 2\pi]$ donc

$$\int_{C_{\varepsilon,R}} f(z)\,dz \underset{\varepsilon\to 0}{\longrightarrow} \mathrm{i}\int_0^{2\pi} \frac{R^{1-x}\,\mathrm{e}^{\mathrm{i}(1-x)t}}{1+R\,\mathrm{e}^{\mathrm{i}t}}dt.$$

De plus, on a

$$\left|\frac{R^{1-x}\,\mathrm{e}^{\mathrm{i}(1-x)t}}{1+R\,\mathrm{e}^{\mathrm{i}t}}\right| \leq \frac{R^{1-x}}{R-1}$$

donc

$$\left|\mathrm{i}\int_0^{2\pi} \frac{R^{1-x}\,\mathrm{e}^{\mathrm{i}(1-x)t}}{1+R\,\mathrm{e}^{\mathrm{i}t}}dt\right| \leq \int_0^{2\pi} \frac{R^{1-x}}{R-1}dt = 2\pi\frac{R^{1-x}}{R-1} \underset{R\to+\infty}{\longrightarrow} 0.$$

On en déduit que la contribution de $C_{\varepsilon,R}$ est asymptotiquement nulle.

– Le même raisonnement permet de voir que la contribution de c_ε est aussi asymptotiquement nulle :

$$\left|\int_{c_\varepsilon} f(z)\,dz\right| \leq \int_{\frac{\pi}{2}}^{\frac{3\pi}{2}} \frac{\varepsilon^{1-x}}{1-\varepsilon}dt \underset{\varepsilon\to 0}{\longrightarrow} 0.$$

– On paramètre le chemin $I^-_{\varepsilon,R}$ par

$$\gamma_2 : \left| \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{C} \\ t & \longmapsto & -\mathrm{i}\varepsilon + \sqrt{R^2-\varepsilon^2}(1-t) \end{array} \right.$$

On a alors pour $t \in [0,1]$

$$\frac{\gamma_2'(t)}{\gamma_2^x(t)(1+\gamma_2(t))} \underset{\varepsilon\to 0}{\longrightarrow} \frac{-R\,\mathrm{e}^{-2\mathrm{i}\pi x}}{(R-Rt)^x(1+R-Rt)}$$

car l'argument de $-\mathrm{i}\varepsilon + \sqrt{R^2-\varepsilon^2}(1-t)$ tend vers 2π, et de plus

$$\left|\frac{\gamma_2'(t)}{\gamma_2^x(t)(1+\gamma_2(t))}\right| \leq \frac{R}{(R-Rt)^x(1+R-Rt)}.$$

Donc en faisant tendre ε vers 0, puis en effectuant le changement de variable linéaire $u = R - Rt$ on obtient

$$\int_{I^-_{\varepsilon,R}} f(z)\,dz \underset{\varepsilon\to 0}{\longrightarrow} \int_0^R \frac{-\,\mathrm{e}^{-2\mathrm{i}\pi x}}{u^x(1+u)}du.$$

– De manière analogue, on a

$$\int_{I^+_{\varepsilon,R}} f(z)\,dz \underset{\varepsilon\to 0}{\longrightarrow} \int_0^R \frac{1}{u^x(1+u)}du$$

et, une nouvelle fois par convergence dominée, on a

$$\int_{I^+_{\varepsilon,R}} f(z)\,dz + \int_{I^-_{\varepsilon,R}} f(z)\,dz \underset{\substack{\varepsilon\to 0 \\ R\to+\infty}}{\longrightarrow} (1-\mathrm{e}^{-2\mathrm{i}\pi x})I(x).$$

L'équation (4.1) se réécrit alors

$$2\mathrm{i}\pi\,\mathrm{e}^{-\mathrm{i}\pi x} = (1-\mathrm{e}^{-2\mathrm{i}\pi x})I(x)$$

et donc

$$I(x) = \frac{\pi}{\sin(\pi x)}.$$

Étape 3. Formule des compléments sur $(0,1)$.

On va maintenant démontrer la formule des compléments sur $(0,1)$. On se donne donc $x \in (0,1)$. On a

$$\begin{array}{rcll}
\Gamma(x)\Gamma(1-x) & = & \left(\displaystyle\int_0^{+\infty} t^{x-1}\,\mathrm{e}^{-t}\,dt\right)\left(\int_0^{+\infty} s^{-x}\,\mathrm{e}^{-s}\,ds\right) & \\
& = & \displaystyle\int_{\mathbb{R}_+^{*2}} \left(\frac{t}{s}\right)^x \frac{1}{t}\,\mathrm{e}^{-(t+s)}\,dsdt & \text{par théorème de Fubini-Tonelli} \\
& = & \displaystyle\int_{\mathbb{R}_+^{*2}} v^x\,\mathrm{e}^{-u}\,\frac{1+v}{uv}\frac{u}{(1+v)^2}dudv & \text{par changement de variable}\,[2] \\
& = & \underbrace{\left(\displaystyle\int_0^{+\infty}\mathrm{e}^{-u}\,du\right)}_{1}\underbrace{\left(\int_0^{+\infty} v^x\frac{dv}{v(1+v)}\right)}_{I(1-x)} & \text{par théorème de Fubini-Tonelli} \\
& = & I(1-x) & \\
& = & \dfrac{\pi}{\sin(\pi(1-x))} & \text{d'après l'étape 2} \\
\Gamma(x)\Gamma(1-x) & = & \dfrac{\pi}{\sin(\pi x)} &
\end{array}$$

Ainsi, la formule est bien vraie sur l'intervalle $(0,1)$.

2. On pose $\varphi : \left| \begin{array}{ccc} \mathbb{R}_+^{*2} & \longrightarrow & \mathbb{R}_+^{*2} \\ (s,t) & \longmapsto & \left(t+s, \frac{t}{s}\right) \end{array} \right.$. On peut donner l'expression de sa bijection réciproque : $\varphi^{-1} : \left| \begin{array}{ccc} \mathbb{R}_+^{*2} & \longrightarrow & \mathbb{R}_+^{*2} \\ (u,v) & \longmapsto & \left(\frac{u}{1+v}, \frac{uv}{1+v}\right) \end{array} \right.$. De plus, son jacobien est $J_{\varphi^{-1}}(u,v) = \dfrac{u}{(1+v)^2} > 0$, et c'est un C^1-difféomorphisme.

Étape 4. Prolongement analytique à Ω.

L'ensemble Ω est un ouvert connexe (par arcs) de $\mathbb{C}$, et la fonction $(z \longmapsto \Gamma(z)\Gamma(1-z))$ y est définie comme une fonction holomorphe. De plus, la fonction $\left(z \longmapsto \dfrac{\pi}{\sin(\pi z)}\right)$ a ces mêmes caractéristiques. Donc, comme elles coïncident sur un intervalle ouvert non vide inclus dans Ω d'après l'étape 3, elles sont égales par principe de prolongement analytique. □

5 Inégalité de Høffding

Leçons 261, 262, 266(, 253)

Ref : [BB18] ou [Ouv19]

Théorème 5.1 (Inégalité de Høffding) Soit $(X_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires réelles indépendantes centrées telle que pour tout $n \in \mathbb{N}$, il existe une constante $c_n > 0$ telle que

$$|X_n| < c_n \text{ p.s..}$$

Alors on a pour tout $\varepsilon > 0$

$$\mathbb{P}\left(|S_n| > \varepsilon\right) \leq 2\,\mathrm{e}^{-\frac{\varepsilon^2}{2a}},$$

où S_n désigne la somme $\displaystyle\sum_{i=1}^{n} X_i$, et $a = \displaystyle\sum_{i=1}^{n} c_i^2$.

Démonstration. On commence par démontrer le lemme suivant.

Lemme 5.2 Soit X une variable aléatoire réelle centrée telle que $|X| < 1$ presque sûrement. Alors on a

$$\forall t \in \mathbb{R} \qquad \mathbb{E}\left(e^{tX}\right) \leq \mathrm{e}^{\frac{t^2}{2}}.$$

Démonstration. On se donne un réel $x \in [-1, 1]$. Alors si $\lambda := \dfrac{1}{2}(1 + x)$ est dans $[0, 1]$, et donc $1 - \lambda = \dfrac{1}{2}(1 - x)$ aussi. De plus, on a $x = 2\lambda - 1 = \lambda\times 1 + (1 - \lambda)\times(-1)$. Donc, par convexité de l'exponentielle, on a

$$\forall t \in \mathbb{R} \qquad \mathrm{e}^{tx} = \mathrm{e}^{t(\lambda\times 1+(1-\lambda)\times(-1))} \leq \lambda\,\mathrm{e}^{t} + (1 - \lambda)\,\mathrm{e}^{-t}.$$

De plus, comme X est bornée par 1, e^{tX} est intégrable pour tout $t \in \mathbb{R}$, et on a d'après ce qui précède

$$\mathrm{e}^{tX} \leq \frac{1}{2}(1 + X)\,\mathrm{e}^{t} + \frac{1}{2}(1 - X)\,\mathrm{e}^{-t}.$$

Ainsi, en passant à l'espérance et en rappelant que X est centrée, on obtient

$$\mathbb{E}\left(\mathrm{e}^{tX}\right) = \mathrm{ch}(t).$$

On compare alors les développements en série entière de l'exponentielle et du cosinus hyperbolique : comme on a pour tout n l'inégalité

$$\frac{1}{(2n)!} \leq \frac{1}{2^n n!},$$

on en déduit

$$\forall t \in \mathbb{R} \qquad \mathrm{ch}(t) \leq \mathrm{e}^{\frac{t^2}{2}},$$

ce qui permet de déduire le résultat souhaité. □

On se donne maintenant $t \in \mathbb{R}$ et $n \in \mathbb{N}$. D'après le lemme, on a

$$\mathbb{E}\left(\mathrm{e}^{t\frac{X_n}{c_n}}\right) \leq \mathrm{e}^{\frac{t^2}{2}}.$$

En prenant $s = \dfrac{t}{c_n} \in \mathbb{R}$, on en déduit

$$\mathbb{E}\left(\mathrm{e}^{sX_n}\right) \leq \mathrm{e}^{\frac{s^2c_n^2}{2}},$$

et ceci est donc vrai pour tout $s \in \mathbb{R}$ et $n \in \mathbb{N}$. On en déduit par indépendance des X_i :

$$\forall t \in \mathbb{R} \qquad \mathbb{E}\left(\mathrm{e}^{tS_n}\right) = \prod_{i=1}^{n} \mathbb{E}\left(\mathrm{e}^{tX_i}\right) \leq \mathrm{e}^{\frac{at^2}{2}},$$

où a désigne la somme $\displaystyle\sum_{i=1}^{n} c_i^2$.

On se donne maintenant $\varepsilon > 0$. On a alors pour $t > 0$

$$\begin{aligned}
\mathbb{P}(S_n > \varepsilon) &= \mathbb{P}\left(\mathrm{e}^{tS_n} > \mathrm{e}^{t\varepsilon}\right) && \text{par croissance de l'exponentielle et positivité de } t \\
&\leq \frac{\mathbb{E}\left(\mathrm{e}^{tS_n}\right)}{\mathrm{e}^{t\varepsilon}} && \text{par inégalité de Markov} \\
&\leq \mathrm{e}^{\frac{at^2}{2} - \varepsilon t}
\end{aligned}$$

Or le minimum de la fonction

$$f : \left| \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ t & \longmapsto & \dfrac{at^2}{2} - \varepsilon t \end{array} \right.$$

est atteint en $\dfrac{\varepsilon}{a}$ et vaut $-\dfrac{\varepsilon^2}{2a}$. Donc

$$\mathbb{P}(S_n > \varepsilon) \leq \mathrm{e}^{-\frac{\varepsilon^2}{2a}}.$$

Puisque les variables $-X_n$ vérifient les mêmes propriétés que les variables X_n, le résultat est aussi vrai en prenant $-S_n$ à la place de S_n. On en déduit l'inégalité de Høffding. □

Corollaire 5.3 On se donne des observations $X_1, .., X_n$ indépendantes identiquement réparties d'une loi inconnue de moyenne m, pour un modèle paramétrique $(\mathcal{H}^n, (\mathbb{Q}_\theta)_{\theta\in\Theta})$. On désigne alors par $\overline{X}_n$ la moyenne empirique associée aux observations $X_1, .., X_n$. On suppose qu'il existe une constante $c > 0$ telle que

$$\forall \theta \in \Theta \ \forall i \in [\![1, n]\!] \qquad |X_i - m| \leq c \ \ \mathbb{Q}_\theta - \text{p.s..}$$

Alors, pour $\alpha \in (0, 1)$ fixé, l'intervalle

$$ICE_{1-\alpha} := \left[\overline{X}_n - c\sqrt{\frac{2}{n}\ln\left(\frac{2}{\alpha}\right)}, \overline{X}_n + c\sqrt{\frac{2}{n}\ln\left(\frac{2}{\alpha}\right)}\right]$$

est un intervalle de confiance par excès de niveau $1 - \alpha$ pour la moyenne $m = m(\theta)$.

Démonstration. Il suffit d'appliquer l'inégalité de Høffding aux X_i : on a ici $a = nc^2$, d'où

$$\forall q > 0 \quad \mathbb{P}\left(|\overline{X}_n| > q\right) = \mathbb{P}\left(|S_n| > nq\right) \leq 2\,\mathrm{e}^{-\frac{nq^2}{2c^2}}.$$

Prendre la bonne valeur de q pour avoir $1 - \alpha = 2\,\mathrm{e}^{-\frac{nq^2}{2c^2}}$ fournit alors l'intervalle de confiance $ICE_{1-\alpha}$. □

6 Intégrale de Fresnel

Leçons 235, 236, 239

Ref : [Gou08] Rem 3.3.6 & Exo 5.4.4

Proposition 6.1 L'intégrale de Fresnel est finie et vaut

$$\varphi = \int_0^{+\infty} \mathrm{e}^{\mathrm{i}x^2}\, dx = \frac{\sqrt{\pi}}{2}\,\mathrm{e}^{\mathrm{i}\frac{\pi}{4}}.$$

Démonstration.

Étape 1. Convergence de Cesàro.

On commence par démontrer le lemme suivant [3], analogue à la convergence au sens de Cesàro des suites numériques.

Lemme 6.2 Soit $f : \mathbb{R}_+ \longrightarrow \mathbb{C}$ une fonction continue, qui admet une limite finie l en $+\infty$. Alors les intégrales $\dfrac{1}{T}\displaystyle\int_0^T f(t)\,dt$ convergent également, pour T tendant vers $+\infty$, vers l.

Par définition de la convergence de f, il existe pour tout $\varepsilon > 0$ un réel $M(\varepsilon) > 0$ tel que pour tout $t > M(\varepsilon)$, $|f(t) - l| < \varepsilon$. On se donne alors un réel $\varepsilon > 0$. Ainsi, on a pour $T > M(\varepsilon/2)$

$$\left|\int_0^T f(t)\,dt - Tl\right| \leq \underbrace{\left|\int_0^{M(\varepsilon/2)} f(t) - l\,dt\right|}_{:=K(\varepsilon)} + (T - M(\varepsilon))\int_{M(\varepsilon/2)}^T |f(t) - l|\,dt \leq K(\varepsilon) + T\frac{\varepsilon}{2}.$$

Ainsi,

$$\left|\frac{1}{T}\int_0^T f(t)\,dt - l\right| \leq \frac{K(\varepsilon)}{T} + \frac{\varepsilon}{2}$$

Finalement, pour $T > M'(\varepsilon) = \max\left(M\left(\dfrac{\varepsilon}{2}\right), \dfrac{2K(\varepsilon)}{\varepsilon}\right)$, on a

$$\left|\frac{1}{T}\int_0^T f(t)\,dt - l\right| \leq \varepsilon.$$

Étape 2. Convergence de l'intégrale impropre.

La fonction $x \longmapsto \mathrm{e}^{\mathrm{i}x^2}$ est continue sur $\mathbb{R}_+$. Seule la question de l'intégrabilité en $+\infty$ se pose. On fixe $T > 1$. On a

$$\begin{aligned}
\int_1^T \mathrm{e}^{\mathrm{i}x^2}\,dx &= \int_1^{T^2} \frac{\mathrm{e}^{\mathrm{i}u}}{2\sqrt{u}}\,du && \text{par changement de variable } u = x^2\\
\int_1^T \mathrm{e}^{\mathrm{i}x^2}\,dx &= \left[\frac{\mathrm{e}^{\mathrm{i}u}}{2\mathrm{i}\sqrt{u}}\right]_1^{T^2} + \int_1^{T^2} \frac{\mathrm{e}^{\mathrm{i}u}}{4\mathrm{i}u^{\frac{3}{2}}}\,du && \text{par intégration par parties}
\end{aligned}$$

Le membre de gauche converge puisque $\mathrm{e}^{\mathrm{i}u}$ est borné, et $\dfrac{1}{\sqrt{u}}$ tend vers 0 en l'infini, et l'intégrale de droite converge absolument, donc converge. Finalement, l'intégrale de Fresnel est convergente, et vaut

$$\varphi = \lim_{T\to+\infty} \int_0^T \mathrm{e}^{\mathrm{i}x^2}\,dx.$$

3. Je n'ai pas de référence exacte pour cette preuve, mais elle n'est pas très compliquée, et si on a vraiment besoin d'une bouée de secours, le raisonnement est adapté de l'exo 4.1.2 de [Gou08].

Étape 3. Une intégrale convergente.

On pose pour $t \geq 0$

$$\begin{cases} F(t) = \displaystyle\int_{[0,t]^2} \mathrm{e}^{\mathrm{i}(x^2+y^2)}\, dxdy \\ f(t) = \displaystyle\int_0^t \mathrm{e}^{\mathrm{i}x^2}\, dx \end{cases}$$

et aussi $g(x,y) = \mathrm{e}^{\mathrm{i}(x^2+y^2)}$. On observe que g est symétrique, de même que le domaine $[0,t]^2$ sur lequel on l'intègre, ce qui permet d'affirmer que l'on a

$$F(t) = 2\int_{\Delta_t} g(t)\ dt,$$

avec $\Delta_t := \left\{(x,y) \in \mathbb{R}^2,\ 0 \leq y \leq x \leq t\right\}$. De plus, la forme de g nous incite à passer en coordonnées polaires. Le compact Δ_t est représenté par le compact

$$K_t = \left\{(r,\theta) \in \mathbb{R}_+ \times \left[0, \frac{\pi}{4}\right],\ 0 \leq r\cos(t) \leq t\right\}.$$

On a ainsi

$$\begin{aligned} F(t) &= 2\int_{K_t} \mathrm{e}^{\mathrm{i}r^2}\, r\ drd\theta && \text{par changement de variable} \\ &= 2\int_0^{\frac{\pi}{4}} \left(\int_0^{\frac{t}{\cos(\theta)}} \mathrm{e}^{\mathrm{i}r^2}\, r\ dr\right) d\theta && \text{par théorème de Fubini} \\ &= 2\int_0^{\frac{\pi}{4}} \left[\frac{1}{2\mathrm{i}}\mathrm{e}^{\mathrm{i}r^2}\right]_0^{\frac{t}{\cos(\theta)}} d\theta \\ F(t) &= \frac{\mathrm{i}\pi}{4} - \mathrm{i}\int_0^{\frac{\pi}{4}} \mathrm{e}^{\mathrm{i}\frac{t^2}{\cos(\theta)^2}}\, d\theta \end{aligned}$$

On pose alors

$$I(T) := \frac{1}{T}\int_0^T F(t)\ dt.$$

On a alors

$$I(T) = \frac{\mathrm{i}\pi}{4} - \frac{\mathrm{i}}{T}\int_0^T \left(\int_0^{\frac{\pi}{4}} \mathrm{e}^{\mathrm{i}\frac{t^2}{(\cos(\theta))^2}}\, d\theta\right) dt.$$

On applique alors le théorème de Fubini, la fonction $(t,\theta) \longmapsto \mathrm{e}^{\mathrm{i}\frac{t^2}{(\cos(\theta))^2}}$, étant continue sur le compact $[0,T]\times\left[0,\frac{\pi}{4}\right]$:

$$\begin{aligned} I(T) &= \frac{\mathrm{i}\pi}{4} - \frac{\mathrm{i}}{T}\int_0^{\frac{\pi}{4}} \left(\int_0^T \mathrm{e}^{\mathrm{i}\frac{t^2}{(\cos(\theta))^2}}\, dt\right) d\theta \\ &= \frac{\mathrm{i}\pi}{4} - \frac{\mathrm{i}}{T}\int_0^{\frac{\pi}{4}} \int_0^{\frac{T}{\cos(\theta)}} \mathrm{e}^{\mathrm{i}u^2}\cos(\theta)\ du && \text{par changement de variable} \\ I(T) &= \frac{\mathrm{i}\pi}{4} - \frac{\mathrm{i}}{T}\int_0^{\frac{\pi}{4}} \cos(\theta) f\left(\frac{T}{\cos(\theta)}\right) d\theta \end{aligned}$$

Or d'après la première étape, f est bornée puisque l'intégrale de Fresnel est semi-convergente. On en déduit que $I(T)$ converge vers $\dfrac{\mathrm{i}\pi}{4}$ quand T tend vers l'infini.

Étape 4. Lien entre f et F et conclusion.

On fait finalement le lien entre les fonctions f et F, à l'aide du théorème de Fubini : on a

$$F(t) = \left(\int_{[0,t]} \mathrm{e}^{\mathrm{i}x^2}\, dx\right)\left(\int_{[0,t]} \mathrm{e}^{\mathrm{i}y^2}\, dy\right) = f(t)^2.$$

On en déduit une autre formule pour l'intégrale I calculée à l'étape précédente :

$$I(T) = \frac{1}{T}\int_0^T f(t)^2 dt.$$

Ainsi, comme f tend vers φ, f^2 tend vers φ^2 et donc sa moyenne de Cesàro aussi (d'après le lemme). Finalement, on obtient donc que $\varphi^2 = \dfrac{\mathrm{i}\pi}{4}$, et en passant à la racine carrée

$$\varphi = \pm\frac{\sqrt{\pi}}{2}\,\mathrm{e}^{\mathrm{i}\frac{\pi}{4}}\,.$$

Reste donc à déterminer le signe. Par exemple, la partie imaginaire de φ vaut

$$\int_0^{+\infty} \sin(u^2)\;du = \frac{1}{2}\int_0^{+\infty} \frac{\sin(u)}{\sqrt{u}}\;du = \sum_{n=0}^{+\infty} u_n$$

avec

$$u_n = \int_{2n\pi}^{2(n+1)\pi} \frac{\sin(u)}{2\sqrt{u}}\;du = \int_{2n\pi}^{(2n+1)\pi} \frac{\sin(u)}{2}\left(\frac{1}{\sqrt{u}} - \frac{1}{\sqrt{u+\pi}}\right)du \geq 0.$$

On peut donc conclure :

$$\varphi = \frac{\sqrt{\pi}}{2}\,\mathrm{e}^{\mathrm{i}\frac{\pi}{4}}\,.$$

□

7 Lax-Milgram et problème aux limites de Neumann

Leçons 205, 213, 222(, 201, 208)

Ref :[Bré05] V.3 & VIII.4 [4]

La première étape de la démonstration du théorème de Lax-Milgram est très simple. On peut la faire si le reste ne prend pas assez de temps, si on veut accentuer le côté "complétude" du développement, mais il ne faut pas non plus y passer 5 minutes. Si au contraire on veut insister sur d'autres points, on peut même l'admettre ou le démontrer en une phrase à l'oral. De plus, il faut savoir (et éventuellement savoir pourquoi [5] aussi) que l'hypothèse de symétrie n'est pas nécessaire et simplifie juste la preuve du théorème, ce qui permet (en temps limité) de montrer l'application au problème aux limites.

Théorème 7.1 (Lax-Milgram) Soit $\mathcal{H}$ un Hilbert réel, et a une forme bilinéaire symétrique continue coercive sur $\mathcal{H}$, et f une forme linéaire continue sur $\mathcal{H}$. Alors il existe un unique $u \in \mathcal{H}$ tel que

$$\forall v \in \mathcal{H} \quad a(u,v) = f(v).$$

Démonstration.

Étape 1. Normes équivalentes et complétude.

On commence par démontrer un lemme faisant le lien entre deux structures de Banach sur un même espace.

Lemme 7.2 Si $(E, \|\cdot\|_E)$ est un espace de Banach, et $\|\cdot\|$ une autre norme sur E, équivalente à $\|\cdot\|_E$, alors $(E, \|\cdot\|)$ est un Banach.

Comme les normes sont équivalentes, on se donne α et β deux réels positifs tels que pour tout $x \in E$, on a

$$\alpha \|x\| \leq \|x\|_E \leq \beta \|x\| .$$

On se donne maintenant une suite de Cauchy $(x_n)_n$ dans $(E, \|\cdot\|)$. Il existe donc pour tout $\varepsilon > 0$ un entier $n(\varepsilon)$ tel que

$$\forall\ p,q > n(\varepsilon) \quad \|x_p - x_q\| \leq \varepsilon.$$

On en déduit que

$$\forall\ p,q > n(\varepsilon/\beta) \quad \|x_p - x_q\|_E \leq \beta \|x_p - x_q\| \leq \varepsilon.$$

Donc la suite $(x_n)_n$ est de Cauchy dans $(E, \|\cdot\|_E)$. Comme E est de Banach, elle converge donc vers un certain $x \in E$. Il existe donc un entier $N(\varepsilon)$ tel que

$$\forall p > N(\varepsilon) \quad \|x_p - x\|_E \leq \varepsilon.$$

Ainsi, en prenant $N'(\varepsilon) = N(\alpha\varepsilon)$, on a

$$\forall p > N'(\varepsilon)\ \|x_p - x\| \leq \frac{1}{\alpha} \|x_p - x\|_E \leq \varepsilon.$$

Donc $(x_n)_n$ converge dans $(E, \|\cdot\|)$, qui est donc de Banach.

Étape 2. Structure de Hilbert sur $(\mathcal{H}, a)$.

On montre maintenant que a définit une nouvelle structure d'espace de Hilbert sur $\mathcal{H}$. Comme a est une forme bilinéaire symétrique, il suffit de montrer qu'elle est définie positive pour montrer que c'est un produit scalaire. Soit $u \in \mathcal{H}\backslash\{0\}$. On a

$$a(u,u) \geq \alpha \|u\|^2 > 0,$$

par hypothèse de coercivité. Donc a munit $\mathcal{H}$ d'une structure d'espace préhilbertien. De plus, on a, par coercivité (à gauche) et continuité (à droite) de a, pour $u \in \mathcal{H}$:

$$\alpha \|u\|^2 \leq a(u,u) \leq |||a||| \, \|u\|^2 ,$$

où $|||a|||$ désigne la norme de a en tant qu'application bilinéaire continue. On en déduit que la norme sur $\mathcal{H}$ induite par a est équivalente à celle induite par le produit scalaire. Donc, comme $\mathcal{H}$ est un Hilbert pour le produit scalaire, c'est aussi un Hilbert pour a.

4. La dernière partie s'inspire de ce qui est fait dans le Brézis mais ce n'est pas une copie conforme.
5. On le démontre généralement à l'aide du théorème de point fixe de Banach-Picard, voir [Bré05].

Étape 3. Théorème de Riesz sous un nouvel angle.

Le théorème de Lax-Milgram se déduit alors du théorème de Riesz. En effet, puisque f est une forme linéaire continue sur $\mathcal{H}$, elle est aussi continue (par équivalence des deux normes) sur $(\mathcal{H}, a)$. On en déduit qu'il existe un unique vecteur $u \in \mathcal{H}$ vérifiant pour tout $v \in \mathcal{H}$ la relation

$$a(u,v) = f(v).$$

□

Dans la suite, on note $\mathcal{H} = \mathcal{H}^1(0,1)$, qui est un espace de Hilbert pour le produit scalaire

$$\langle u, v\rangle = \int_0^1 u'(t)v'(t) + u(t)v(t)\ dt.$$

Application 7.3 Le problème aux limites associé à des conditions au bord de Neumann (E) suivant, consistant à trouver u de classe C^2 sur $[0,1]$ telle que

$$\begin{cases} -u'' = f \quad \text{sur } (0,1) \\ u'(0) = \alpha,\ u'(1) = \beta \end{cases}$$

α et β étant deux réels donnés et f une fonction continue sur $[0,1]$, admet une unique solution.

Démonstration.

Étape 1. Formulation variationnelle du problème.

On suppose disposer d'une solution u au problème (E). On se donne alors $v \in C^1(0,1)$. Comme u est aussi dans $\mathcal{H}$, en multipliant l'équation de u par v et en intégrant par parties sur $[0,1]$, on a alors

$$\int_0^1 u'(t)v'(t)dt = \int_0^1 f(t)v(t)\ dt + \beta v(1) - \alpha v(0).$$

On pose alors $L : \left|\begin{array}{ccc} \mathcal{H} & \longrightarrow & \mathbb{R} \\ v & \longmapsto & \langle f, v\rangle_{L^2} + \beta v(1) - \alpha v(0) \end{array}\right.$ et $a : \left|\begin{array}{ccc} \mathcal{H}\times\mathcal{H} & \longrightarrow & \mathbb{R} \\ (u,v) & \longmapsto & \langle u', v'\rangle_{L^2} \end{array}\right.$, de sorte que u vérifie le problème variationnel (EV)

$$a(u,v) = L(v).$$

Étape 2. Résolution faible par Lax-Milgram.

Tout d'abord, L est une forme linéaire sur $\mathcal{H}$. De plus, on a

$$|L(v)| \leq |\langle f, v\rangle_{L^2}| + (|\alpha| + |\beta|)\|v\|_\infty .$$

On applique Cauchy-Schwarz dans L^2, on en déduit $|\langle f, v\rangle_{L^2}| \leq \|f\|_{L^2}\|v\|_{L^2} \leq \|f\|_{L^2}\|v\|$. De plus, la théorie des Sobolev montre que la norme infinie est moins fine que la norme sur $\mathcal{H}$. Donc $\|v\|_\infty \leq C\|v\|$, et finalement L est continue.

De même, a est une forme bilinéaire, et comme la norme L^2 est inférieure à la norme de $\mathcal{H}$, en appliquant Cauchy-Schwarz, on obtient que a est continue. De plus, on a, en notant C la constante donnée par l'inégalité de Poincaré sur $(0,1)$,

$$(1+C)a(v,v) = \|v'\|_{L^2}^2 + C\|v'\|_{L^2}^2 \geq \|v\|^2 .$$

Donc a est coercive. Finalement, comme $\mathcal{H}$ est un Hilbert, on peut appliquer le théorème de Lax-Milgram à L et a sur $\mathcal{H}$: il existe une unique $u \in \mathcal{H}$ solution de (EV).

Étape 3. Résolution du problème initial.

On voudrait maintenant remonter au problème initial. Comme u vérifie (EV), en prenant $v \in \mathcal{D}(0,1) \subset \mathcal{H}$, on en déduit que l'on a $-\langle u'', v\rangle_{\mathcal{D}',\mathcal{D}} = \langle u', v'\rangle_{\mathcal{D}',\mathcal{D}} = \langle f, v\rangle_{\mathcal{D}',\mathcal{D}}$, et donc $-u'' = f$ dans $\mathcal{D}'(0,1)$. Comme $\mathcal{D}'$ est dense dans L^2, cette égalité se fait aussi dans L^2. Mais comme f est continue, on en déduit que u'' l'est aussi, et donc l'égalité est en fait une égalité de fonctions continues. Donc u est de classe C^2. En prenant alternativement $v \in C^\infty(0,1)$ vérifiant $v(0) = 1, v(1) = 0$ et $v(0) = 0, v(1) = 1$, on déduit en intégrant par parties que u vérifie aussi $u'(0) = \alpha$ et $u'(1) = \beta$. On a donc bien résolu le problème de Laplace avec conditions de Neumann. □

8 Méthode des caractéristiques

Leçons 220, 221, 222(, 215)

Ref :

Pour ce développement, je me suis inspiré d'un cours de Master 1, et je n'ai pas trouvé de référence qui me plaise vraiment. La méthode des caractéristiques est bien sûr présentée dans les livres classiques sur les EDPs (voir [Eva10] par exemple) mais toujours avec un formalisme beaucoup plus lourd que nécessaire au niveau de l'Agrégation.

On applique donc la **méthode des caractéristiques** à la résolution des équations hyperboliques linéaires, de la forme suivante

$$\begin{cases} \partial_t u + \langle a, \nabla_x u \rangle + a_0 u = f \quad \text{sur } \mathbb{R}\times\mathbb{R}^d & \text{(8.1a)} \\ u(x,0) = u_0(x) \quad \forall x \in \mathbb{R}^d & \text{(8.1b)} \end{cases}$$

Les hypothèses sont les suivantes :

- t est une variable de temps de dimension 1,
- x est une variable d'espace de dimension d,
- $f : \mathbb{R}^d\times\mathbb{R} \longrightarrow \mathbb{R}$ et $a_0 : \mathbb{R}^d\times\mathbb{R} \longrightarrow \mathbb{R}$ sont des données, de classe C^1 sur $\mathbb{R}^d\times\mathbb{R}$,
- $a : \left| \begin{array}{ccc} \mathbb{R}^d\times\mathbb{R} & \longrightarrow & \mathbb{R}^d \\ (x,t) & \longmapsto & \begin{pmatrix} a_1(x,t) \\ \vdots \\ a_d(x,t) \end{pmatrix} \end{array} \right.$ est une autre donnée, de classe C^1 et globalement lipschitzienne par rapport à la variable d'espace,
- $u_0 : \mathbb{R}^d \longrightarrow \mathbb{R}$ est la donnée initiale, de classe C^1.

Théorème 8.1 Le problème (8.1) admet une unique solution u de classe C^1 sur $\mathbb{R}^d\times[0,T]$ [6], pour tout $T > 0$, et on en connaît l'expression.

Démonstration. On raisonne par analyse-synthèse. On suppose qu'il existe une solution u au problème, et on étudie celle-ci le long de courbes paramétrées par la variable temporelle.

Étape 1. Choix des courbes caractéristiques.

On se donne donc $X : \mathbb{R} \longrightarrow \mathbb{R}^d$ la paramétrisation d'une de ces courbes. On pose alors pour $s \in [0,T]$

$$v(s) = u(X(s), s).$$

On utilise la règle de dérivation en chaîne [7] pour dériver v :

$$v'(s) = \langle \nabla_x u(X(s),s), X'(s) \rangle + \partial_t u(X(s),s). \tag{8.2}$$

Le principe est maintenant de choisir la courbe X de manière à simplifier cette équation. Au vu de (8.1a), on souhaiterait que $X'(s)$ soit égal à $a(X(s),s)$. On considère donc le problème de Cauchy suivant, associé aux données $(x,t) \in \mathbb{R}^d\times[0,T]$:

$$\begin{cases} X'(s) = a(X(s),s) & \text{(8.3a)} \\ X(t) = x & \text{(8.3b)} \end{cases}$$

Comme a est lipschitzienne, celui-ci admet, d'après le théorème de Cauchy-Lipschitz, une unique solution définie sur $[0,T]$, que l'on note $X(\,\cdot\,; x, t)$. Si l'on choisit ces courbes [8], on remarque (8.2) devient l'EDO suivante

$$v'(s) = -a_0(X(s),s)v(s) + f(X(s),s). \tag{8.4}$$

6. On n'est pas obligé d'en parler, cette condition est juste là pour pouvoir intégrer sans se poser de questions.
7. Il faut bien comprendre tous les objets présents : la dérivée de u en x est son vecteur gradient (spatial), à d composantes, la dérivée X' de X est simplement un vecteur composé des dérivées de chaques composantes de X.
8. Pour l'instant, la valeur de x et t n'importe pas.

Étape 2. Expression de v.

On intègre alors cette équation : l'équation homogène a pour solution

$$v_h(s) = \lambda \exp\left(-\int_0^s a_0(X(\sigma),\sigma)d\sigma\right).$$

On applique alors la méthode de variation de la constante. On se donne une fonction $\lambda : [0,T] \longrightarrow \mathbb{R}$ telle que

$$v(s) = \lambda(s) \exp\left(-\int_0^s a_0(X(\sigma),\sigma)d\sigma\right).$$

Alors on a

$$\lambda'(s) = f(X(s),s) \exp\left(\int_0^s a_0(X(\sigma),\sigma)d\sigma\right),$$

donc en intégrant, avec la condition $\lambda(0) = v(0)$, on obtient

$$\lambda(s) = v(0) + \int_0^s f(\sigma) \exp\left(\int_0^\sigma a_0(X(\tau),\tau)d\tau\right) d\sigma.$$

Finalement, on a

$$v(s) = v(0) \exp\left(-\int_0^s a_0(X(\sigma),\sigma)d\sigma\right) + \int_0^s f(X(\sigma),\sigma) \exp\left(-\int_\sigma^s a_0(X(\tau),\tau)d\tau\right) ds.$$

Étape 3. Détermination de la solution.

La condition initiale est donnée par

$$v(0) = u(X(0;x,t),0) = u_0(X(0;x,t)).$$

On remarque également que, comme $X(t;x,t) = x$, on a

$$v(t) = u(X(t;x,t),t) = u(x,t).$$

Finalement, on a donc

$$u(x,t) = u_0\left(X(0;x,t)\right) \exp\left(-\int_0^t a_0\left(X(\sigma;x,t),\sigma\right) d\sigma\right) + \int_0^t f\left(X(\sigma;x,t),\sigma\right) \exp\left(-\int_\sigma^t a_0\left(X(\tau;x,t),\tau\right) d\tau\right) d\sigma.$$

On fait maintenant la synthèse. L'unicité du théorème de Cauchy-Lipschitz montre qu'il y a une loi de groupe sur les caractéristiques : pour tout $x \in \mathbb{R}^d$ et $s,\sigma,t \in [0,T]$, on a

$$X(\sigma;X(s;x,t),s) = X(\sigma;x,t).$$

Cette relation, permet d'obtenir, à partir de l'expression de u, que v vérifie l'équation (8.2), et donc que u vérifie l'équation (8.1a) sur tous les points de la forme $(X(s;x,t),s)$ de $\mathbb{R}^d \times [0,T]$. Or, toujours grâce à loi de groupe, à s et t fixés, $x \longmapsto X(s;x,t)$ induit un difféomorphisme de $\mathbb{R}^d$ sur $\mathbb{R}^d$. Donc en fait u vérifie l'équation sur tout $\mathbb{R}^d \times [0,T]$. Elle vérifie aussi les conditions initiales, et elle est de classe C^1. On a donc exhibé l'unique solution de (8.1). □

Exemple. On étudie une équation en dimension 1 :

$$\begin{cases} \partial_t u + \alpha x \partial_x u + \beta u = 0 \\ u(x,t) = u_0(x) \end{cases}$$

Alors on pose $v(s) = u(X(s),s)$. On a donc, en dérivant s

$$v'(s) = \partial_x u(X(s),s)X'(s) + \partial_t u(X(s),s).$$

On résout donc l'équation ordinaire

$$X'(s) = \alpha X(s).$$

La solution de cette équation, avec condition initiale $X(t;x,t) = 0$, est

$$X(s;x,t) = x\,\mathrm{e}^{\alpha(s-t)}.$$

On peut tracer les courbes pour voir ce qui se passe. On trace s en fonction de $X(s;x,t)$. On a $s = \ln\left(\frac{y}{x}\right) + t$. On a alors

$$v'(s) = -\beta v(s).$$

Ainsi, $v(s) = v(0)\,\mathrm{e}^{-\beta s} = u_0(x\,\mathrm{e}^{-\alpha t})\,\mathrm{e}^{-\beta s}$. Finalement,

$$u(x,t) = u_0(x\,\mathrm{e}^{-\alpha t})\,\mathrm{e}^{-\beta t}\,.$$

Par exemple, si α et β sont positifs, on observe que la courbe s'applatit et s'affaisse.

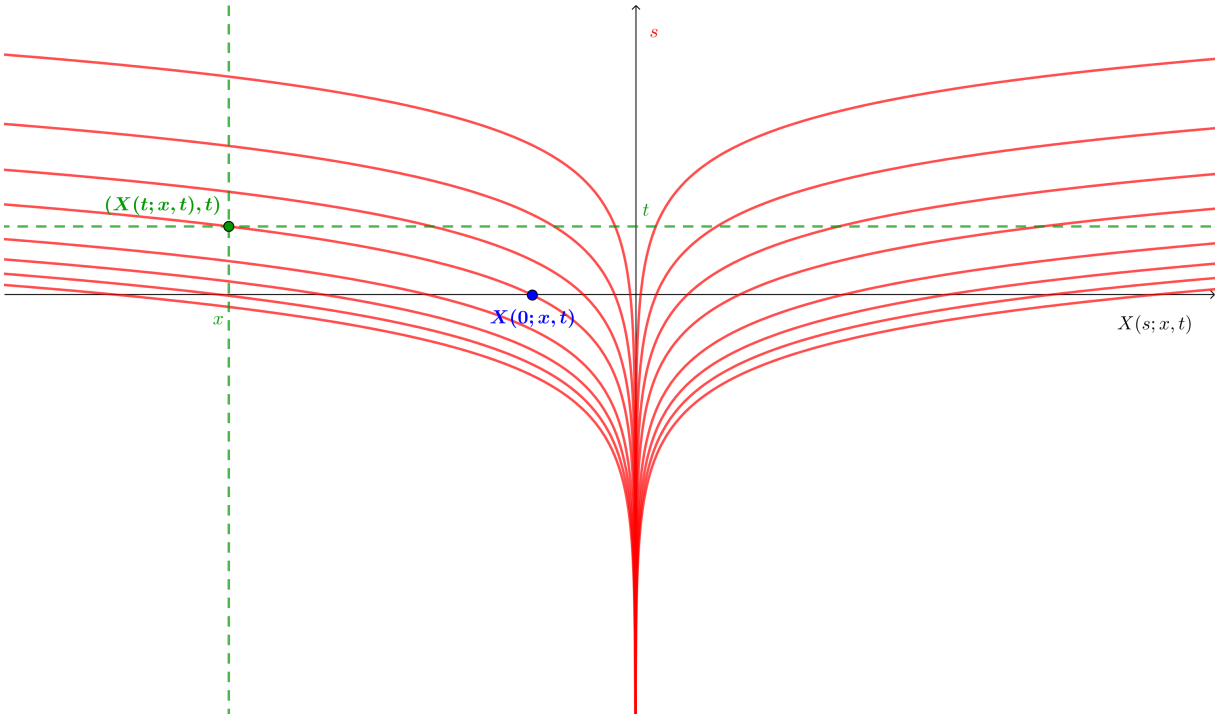


Figure 8.1 – Tracé des caractéristique du problème hyperbolique pour $a(x,t) = x$

On peut choisir son équation de transport préférée à la place de celle-là. On peut essayer de passer en dimension 2 aussi, avec des exemples simples c'est pas trop compliqué. En revanche, la dimension 1 est facile à tracer, contrairement à la dimension 2. On n'a pas forcément le temps de tout faire. Il faut passer vite sur les arguments EDO dans la leçon 222, c'est mieux de faire l'exemple. Pour les 220 et 221, mieux vaut privilégier les arguments EDO et ne pas faire l'exemple.

9 Théorème de Steinhauß

Leçons 207, 241(, 230, 262)

Ref : [ZQ13] Chap XIII Th III.1

On sait qu'une série entière admet au moins un point singulier sur le bord de son disque de convergence. Sinon, tous les points seraient réguliers, et on pourrait alors, par compacité du cercle unité (on se ramène au cas d'une série dont le rayon de convergence est 1), prolonger la fonction en une fonction holomorphe sur le disque ouvert de rayon $1+\varepsilon$. Mais alors, la nouvelle fonction est analytique, et donc holomorphe sur le grand disque, et les deux développements en série entière coïncident, donc les deux séries sont les mêmes (principe des zéros isolés). Donc le rayon de la série entière est d'au moins $1+\varepsilon$, ce qui est absurde.

On voudrait maintenant savoir s'il est possible d'avoir "beaucoup" de points singuliers. On dit que le cercle $\mathbb{S}^1$ est une *coupure* pour la série entière si tous ses points sont singuliers. La série $\sum_{n\geq 0} z^{2^n}$ par exemple admet toutes les racines 2^k-ièmes de l'unité comme points singuliers, et donc par densité, le cercle en est une coupure. Le théorème suivant montre que ce cas est tout sauf un cas isolé.

Théorème 9.1 (Steinhauß) Soit $\sum_{n\geq 0} a_n z^n$ une série entière de rayon de convergence 1, et $W=(W_n)_{n\geq 0}$ une suite de variables aléatoires complexes indépendantes indentiquement réparties selon la loi uniforme sur le cercle $\mathbb{S}^1$. Alors, presque sûrement, le cercle est une coupure pour la série $\sum_{n\geq 0} a_n W_n z^n$.

Démonstration. On note $A = \left\{ \mathbb{S}^1 \text{ est une coupure pour } \sum_{n\geq 0} a_n W_n z^n \right\}$. Le but est de montrer que A est un événement de probabilité 1. On note $\mathbb{D}$ le disque unité ouvert, et

$$\mathbb{S}^1_{\mathbb{Q}} := \left\{ \mathrm{e}^{2\mathrm{i}\pi\theta},\ \theta\in\mathbb{Q} \right\},$$

qui est dénombrable et dense dans $\mathbb{S}^1$.

Étape 1. Exhibition d'un recouvrement dénombrable de $\overline{A}$.

On se donne une réalisation $w=(w_n)_{n\geq 0}$ de la suite W. On suppose que $z_0\in\mathbb{S}^1$ est un point régulier de la série $f_w := \sum_{n\geq 0} a_n w_n z^n$. Il existe donc un voisinage ouvert de z_0 dans $\mathbb{C}$ qui ne contient que des points réguliers pour f_w ; quitte à le réduire on peut supposer que son intersection avec $\mathbb{S}^1$ est de la forme

$$I := \left\{ \mathrm{e}^{2\mathrm{i}\pi\theta},\ \theta\in(a,b) \right\},$$

avec $a<b$ rationnels. On note $\mathcal{C}$ l'ensemble des arcs de cercles ouverts de $\mathbb{S}^1$ à extrémités dans $\mathbb{S}^1_{\mathbb{Q}}$, et on définit

$$A_I := \{\text{Tous les points de } I \text{ sont réguliers pour } f_w\}.$$

Alors, d'après ce qui précède, $\overline{A}$ est l'ensemble des réalisations w de W telles qu'il existe un arc $I\in\mathcal{C}$, tel que A_I est vrai. Ainsi, on doit montrer que $\bigcup_{I\in\mathcal{C}} A_I$ est un événement de probabilité nulle, et donc, comme $\mathcal{C}$ est dénombrable, il suffit de montrer que les A_I sont des événements de probabilité nulle.

Étape 2. Les A_I sont des événements.

On se donne $I\in\mathcal{C}$, $z_0\in I$, et une réalisation w de W qui est dans A_I. Par définition de I, z_0 est régulier pour f_w et il existe donc $\varepsilon>0$ tel que f_w se prolonge de manière holomorphe à $\mathbb{D}\cup B(z_0,\varepsilon)$. Ainsi, il existe un réel $\eta>\frac{1}{2}$ tel que f_w se prolonge de manière holomorphe à $B\left(\frac{z_0}{2},\eta\right)$ (voir figure 9.1), et réciproquement. Ainsi, on a pour tout $z\in B\left(\frac{z_0}{2},\eta\right)$

$$f_w(z) = \sum_{n\geq 0} \frac{f_w^{(n)}\left(\frac{z_0}{2}\right)}{n!}\left(z-\frac{z_0}{2}\right)^n.$$

Donc z_0 est régulier si et seulement si le rayon de convergence de cette série est strictement supérieur à $\frac{1}{2}$, c'est-à-dire, d'après le théorème de Cauchy-Hadamard, si et seulement si

$$\overline{\lim_{n\to+\infty}} \left| \frac{f_w^{(n)}\left(\frac{z_0}{2}\right)}{n!} \right|^{\frac{1}{n}} < 2.$$

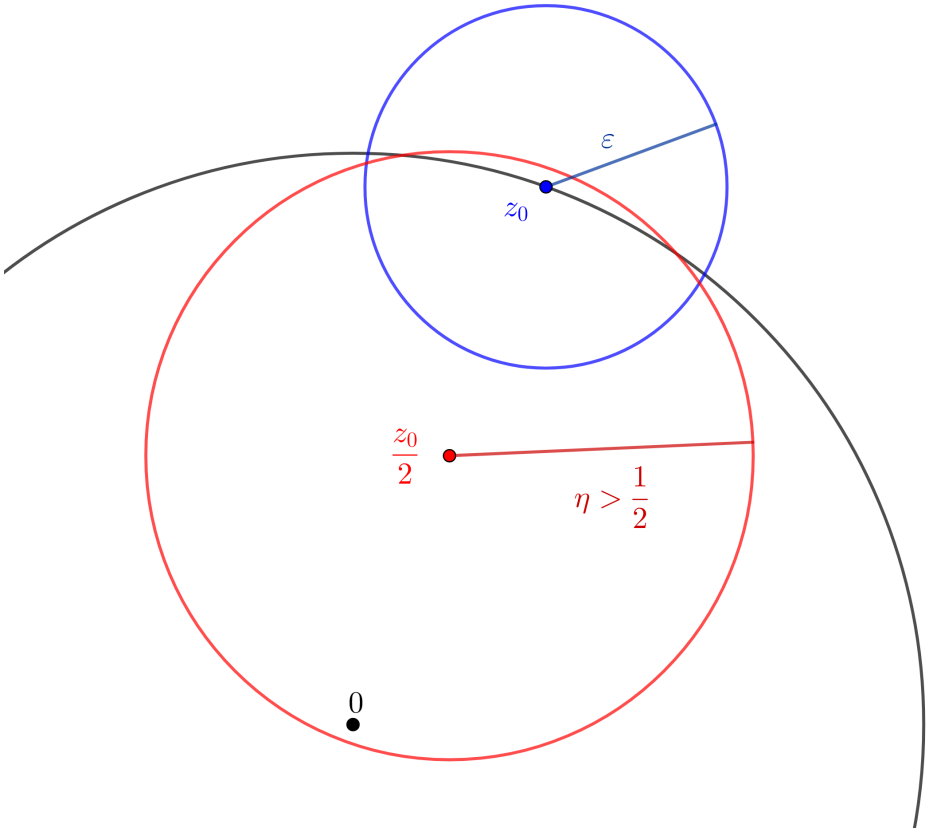


Figure 9.1 – Prolongement de f_w à un disque sortant de $\mathbb{D}$.

On a donc

$$\begin{aligned} A_I &= \left\{ w \in (\mathbb{S}^1)^{\mathbb{N}},\ \forall z_0 \in I\ \ \overline{\lim_{n\to+\infty}} \left| \frac{f_w^{(n)}\left(\frac{z_0}{2}\right)}{n!} \right|^{\frac{1}{n}} < 2 \right\} \\ &= \left\{ w \in (\mathbb{S}^1)^{\mathbb{N}},\ \forall z_0 \in I \cap \mathbb{S}^1_{\mathbb{Q}}\ \ \overline{\lim_{n\to+\infty}} \left| \frac{f_w^{(n)}\left(\frac{z_0}{2}\right)}{n!} \right|^{\frac{1}{n}} < 2 \right\} \quad \text{par densité de } \mathbb{S}^1_{\mathbb{Q}} \\ A_I &= \bigcap_{z_0 \in I \cap \mathbb{S}^1_{\mathbb{Q}}} \underbrace{\left\{ w \in (\mathbb{S}^1)^{\mathbb{N}},\ \overline{\lim_{n\to+\infty}} \left| \frac{f_w^{(n)}\left(\frac{z_0}{2}\right)}{n!} \right|^{\frac{1}{n}} < 2 \right\}}_{\substack{\text{événement comme image réciproque} \\ \text{d'une limite supérieure de v.a.}}} \end{aligned}$$

Donc A_I est un événement comme intersection dénombrable d'événements.

Étape 3. Application de la loi de Kolmogorov.

Puisque l'expression $f_W^{(n)}\left(\frac{z_0}{2}\right)$ ne dépend pas des variables $W_0, .., W_{n-1}$, l'événement A_I, tel qu'il est décomposé à l'étape précédente, appartient à la tribu asymptotique associée aux $(W_n)_{n\in\mathbb{N}}$. Or ces variables aléatoires sont indépendantes, donc d'après la loi du 0-1 de Kolmogorov, A_I est de probabilité 0 ou 1. Il suffit donc d'exclure le cas $\mathbb{P}(A_I) = 1$.

On se donne J un second arc de même longueur que I : il existe alors un réel θ tel que

$$J = \mathrm{e}^{\mathrm{i}\theta}\, I.$$

On pose alors pour $n \in \mathbb{N}$

$$W_n^\theta := W_n\, \mathrm{e}^{-\mathrm{i}\theta}\,.$$

Puisque le cercle est invariant par rotation et que les W_n suivent une loi uniforme, W_n et W_n^θ sont de même loi. De plus, par construction, I est régulier pour f_w si et seulement si J l'est pour f_{w^θ}. On en déduit que $\mathbb{P}(A_J) = \mathbb{P}(A_I)$. Supposons par l'absurde qu'un intervalle I soit tel que A_I est de probabilité

1. Alors il existe un recouvrement de $\mathbb{S}^1$ par des intervalles $I_1, .., I_N$ de même longueur que I. Mais alors

$$\mathbb{P}\left(\bigcap_{j=1}^{N} A_{I_j}\right) = 1,$$

et cette intersection est en fait l'événement {Tous les points du cercle sont réguliers}. C'est absurde, puisque l'on sait que cet événement est vide d'après la remarque préliminaire. Donc $\mathbb{P}(A_I) = 0$. □

10 Théorème d'Hadamard-Lévy

Leçons 203, 204, 214, 215, 220

Ref : [BB18]

On montre dans ce développement un résultat proche du théorème d'inversion globale : on relaxe l'hypothèse d'injectivité faite dans celui-ci, et on demande en contrepartie que la fonction considérée soit propre. La preuve du théorème est compliquée dans le cas de f de classe C^1, et on fait l'hypothèse simplificatrice de classe C^2, qui permet d'avoir les hypothèses nécessaires au théorème de Cauchy-Lipschitz.

Théorème 10.1 On se donne une fonction $f \in C^2(\mathbb{R}^n, \mathbb{R}^n)$. Il y a équivalence entre

(i) f est un C^1-difféomorphisme de $\mathbb{R}^n$ sur $\mathbb{R}^n$,

(ii) pour tout $x \in \mathbb{R}^n$, df_x est inversible, et f est propre [9].

Démonstration.

Étape 1. Sens direct.

On commence par le sens le plus simple. Puisque f est un C^1-difféomorphisme, on a $f^{-1} \circ f = \mathrm{Id}_{\mathbb{R}^n}$, et donc par dérivation on chaîne, on a pour $x \in \mathbb{R}^n$

$$df^{-1}_{f(x)} \circ df_x = \mathrm{Id}_{\mathbb{R}^n}.$$

Donc df_x est inversible à gauche, et comme on est en dimension finie, on en déduit que df_x est inversible, et que son inverse est $df^{-1}_{f(x)}$.

On fixe maintenant $r > 0$. L'image réciproque de la boule fermée $\overline{B(0,r)}$ est l'image directe par f^{-1} de cette même boule. Comme f^{-1} est continue, cette image est compacte, donc fermée bornée, disons incluse dans $\overline{B(0,R)}$, pour $R > 0$. Ainsi, si $\|x\| > R$, $\|f(x)\| > r$. Donc f est propre.

Étape 2. Un candidat pour l'inverse.

On suppose que f est nulle en 0 (quitte à la changer par $f - f(0)$). On fixe un intervalle ouvert I contenant 0 et 1, et $s : I \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$ une application de classe C^1 par rapport à la première variable. On souhaite [10] avoir pour tout $(t,x) \in I \times \mathbb{R}^n$

$$f \circ s(t,x) = tx.$$

On dérive cette relation par rapport à la première variable : on a

$$df_{s(t,x)} \circ \partial_t s(t,x) = x.$$

Donc, comme la différentielle de f est inversible en tout point, on a la relation souhaitée si et seulement si pour tout $(t,x) \in \mathbb{R}^n$

$$\begin{cases} \partial_t s(t,x) = (df_{s(t,x)})^{-1}(x) \\ f \circ s(0,x) = 0 \end{cases}$$

C'est dire que s convient si et seulement si $s(\,\cdot\,, x)$ est solution sur I, pour $x \in \mathbb{R}^n$, du problème de Cauchy

$$\begin{cases} \dfrac{dy}{dt} = (df_y)^{-1}(x) \\ y(0) = 0 \end{cases}$$

Étape 3. Existence de l'inverse à droite.

On pose ainsi

$$F : \left| \begin{array}{ccc} \mathbb{R}^n \times \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ (x,y) & \longmapsto & (df_y)^{-1}(x) \end{array} \right.$$

Cette application est de classe C^1, comme composée des fonctions de classe C^1 suivantes :

- les projections sur la première et deuxième coordonnée (applications linéaires),
- $y \longmapsto df_y$, qui est de classe C^1 puisque f est C^2,

9. À savoir que $\|f(x)\|$ tend vers l'infini si $\|x\|$ tend vers l'infini.
10. En fait, l'important n'est pas que cela fonctionne sur tout I, mais sur un intervalle contenant 0 et 1.

– l'inversion dans $GL_n(\mathbb{R})$
– $(A, x) \longmapsto A(x)$ quand A est linéaire (application bilinéaire)

En particulier, $F(x, \cdot)$ est de classe C^1 pour tout x, donc le problème de Cauchy admet une unique solution maximale (Cauchy-Lipschitz) $s(\cdot, x)$ sur I. On note $(t^-(x), t^+(x))$ l'intervalle sur lequel $s(\cdot, x)$ est défini. On sait que celui-ci contient 0, on veut montrer qu'il contient aussi 1. Supposons donc par l'absurde que $t^+(x_0)$ est inférieur à 1, pour un certain $x_0 \in \mathbb{R}^n$. D'après le principe de sortie de tout compact, $s(t, x_0)$ tend donc vers l'infini (en norme) quand t tend vers $t^+(x_0)$. Comme f est propre, c'est donc aussi le cas de $f \circ s(t, x_0)$. Mais cette quantité vaut tx_0, c'est absurde puisque

$$\|tx_0\| \underset{t \to t^+(x_0)}{\longrightarrow} t^+(x_0)\, \|x_0\| < +\infty.$$

Donc $t^+(x_0) > 1$. Ainsi, l'application $s(1, \cdot)$ est définie sur $\mathbb{R}^n$, et d'après le raisonnement effectué, est un inverse à droite de f.

Étape 4. Conclusion par connexité et inversion locale.

D'après le théorème de Cauchy-Lipschitz à paramètres ([BG10] Th 5.15), l'application s est de classe C^1 sur $[0, 1]\times\mathbb{R}^n$, donc $s_1 := s(1, \cdot)$ est de classe C^1 sur $\mathbb{R}^n$. De plus, comme $f \circ s = \mathrm{Id}_{\mathbb{R}^n}$, f est nécessairement surjective, et s_1 injective. Il reste donc à montrer que f est injective. Pour cela, on montre que s_1 est surjective. On raisonne par connexité, en montrant que $s_1(\mathbb{R}^n)$ est ouvert et fermé dans $\mathbb{R}^n$.

– On se donne une suite $(x_n)_n$ d'éléments de $\mathbb{R}^n$ telle que $s_1(x_n)$ converge vers un certain $y \in \mathbb{R}^n$. Alors la suite x_n converge vers $f(y)$, par continuité de f et parce que s_1 est un inverse à droite de f. Comme s_1 est continue, on en déduit que $s_1(x_n)$ converge vers $s_1 \circ f(y)$. Donc, par unicité de la limite, $y = s_1(f(y)) \in s_1(\mathbb{R}^n)$. Donc $s_1(\mathbb{R}^n)$ est fermé.
– Soit $y = s_1(x) \in s_1(\mathbb{R}^n)$. On veut exhiber un voisinage ouvert de y inclus dans $s_1(\mathbb{R}^n)$. En différenciant au point x la relation $f \circ s_1 = \mathrm{Id}_{\mathbb{R}^n}$, on obtient

$$df_{s_1(x)} \circ ds_{1x} = \mathrm{Id}_{\mathbb{R}^n}.$$

Par le raisonnement effectué à l'étape 1, ds_{1x} est inversible. D'après le théorème d'inversion locale, il existe donc un voisinage U autour de x dans $\mathbb{R}^n$ et un voisinage V de $y = s_1(x)$ dans $\mathbb{R}^n$ tel que s_1 réalise un difféomorphisme entre U et V. En particulier, V est un ouvert inclus dans $s_1(\mathbb{R}^n)$ contenant y. Donc $s_1(\mathbb{R}^n)$ est ouvert.

Finalement $s_1(\mathbb{R}^n)$ est ouvert et fermé, non vide, donc égal à $\mathbb{R}^n$, ce qui montre que s_1 est surjective. Ainsi, s_1 est bijective, et en composant par s_1^{-1} à droite dans l'égalité

$$f \circ s_1 = \mathrm{Id}_{\mathbb{R}_n},$$

on obtient $f = s_1^{-1}$. Donc f est bijective, d'inverse s_1, qui est bien de classe C^1. □

Remarque. Le raisonnement présenté ici est le même que dans [BB18], aux détails près de la preuve d'ouverture de $s_1(\mathbb{R}^n)$ et de la bijectivité de f, que je trouve un poil plus simples de cette manière.

11 Sommation d'Abel pour les séries de Fourier

Leçons 209, 235, 241, 246

Ref : [BB18]

On note $C^0_{\text{pm}}(0,2\pi)$ l'ensemble des fonctions continues par morceaux sur $[0,2\pi]$ étendues à $\mathbb{R}$ par 2π-périodicité, et $C^0(0,2\pi)$ l'ensemble des fonctions continues sur $[0,2\pi]$ étendues à $\mathbb{R}$ par 2π-périodicité. On appelle également *régularisée* d'un élément $f \in C^0_{\text{pm}}(0,2\pi)$ la fonction $\widetilde{f}$ définie par

$$\widetilde{f}(x) = \frac{1}{2}\left(f(x)_+ + f(x)_-\right), \quad \forall x \in \mathbb{R},$$

$f(x)_+$ et $f(x)_-$ désignant les limites respectivement à droite et à gauche de f en x. Ce développement consiste à démontrer le résultat suivant.

Proposition 11.1 Soit $f \in C^0_{\text{pm}}(0,2\pi)$, et $r \in (0,1)$. La série

$$c_0(f) + \sum_{n\geq 1} r^n \left(c_n(f)e_n + c_{-n}(f)e_{-n}\right)$$

converge normalement sur $\mathbb{R}$, et on note f_r sa somme. On a de plus les résultats qui suivent :

- f_r converge simplement vers $\widetilde{f}$ sur $\mathbb{R}$, quand r tend vers 1_-
- si de plus f est continue sur $[0,2\pi]$, alors f_r converge uniformément vers f sur $\mathbb{R}$, quand r tend vers 1_-.

Démonstration. Étape 1. Convergence normale de la série.

On fixe $r \in (0,1)$. On rappelle le lemme de Riemann-Lebesgue : les coefficients de Fourier de f tendent vers 0. En particulier, la suite $(c_n(f))_{n\in\mathbb{Z}}$ est bornée, disons par $M > 0$. On a alors

$$|r^n \left(c_n(f)e_n(x) + c_{-n}(f)e_{-n}(x)\right)| \leq 2Mr^n, \quad \forall x \in \mathbb{R}, \forall n \in \mathbb{N}.$$

En particulier, comme la série $2M\sum_{n\geq 1} r^n$ converge dans $\mathbb{R}$ puisque $|r| < 1$, la série

$$c_0(f) + \sum_{n\geq 1} r^n \left(c_n(f)e_n + c_{-n}(f)e_{-n}\right)$$

converge normalement, et on peut donc définir la somme f_r de sa série (car elle est à valeurs dans $\mathbb{C}$, qui est complet).

Étape 2. Introduction des noyaux de Poisson.

On cherche ici à exprimer f_r comme un produit de convolution. Soit donc $x \in \mathbb{R}$. On a

$$f_r(x) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\ dt + \frac{1}{2\pi}\sum_{n=1}^{+\infty} r^n \left(\int_{-\pi}^{\pi} f(t)\,\mathrm{e}^{-\mathrm{i}nt}\,\mathrm{e}^{\mathrm{i}nx}\,dt + \int_{-\pi}^{\pi} f(t)\,\mathrm{e}^{\mathrm{i}nt}\,\mathrm{e}^{-\mathrm{i}nx}\,dt\right).$$

On rappelle que l'on raisonne à x fixé, et on pose

$$\varphi_n(t) := r^n f(t)\left(\mathrm{e}^{\mathrm{i}n(x-t)} + \mathrm{e}^{\mathrm{i}n(t-x)}\right), \quad \forall t \in \mathbb{R},$$

de sorte que

$$f_r(x) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\ dt + \frac{1}{2\pi}\sum_{n=1}^{+\infty}\int_{-\pi}^{\pi} \varphi_n(t)\ dt.$$

On a, pour $n \in \mathbb{N}$ et $t \in \mathbb{R}$, $|\varphi_n(t)| \leq 2\|f\|_\infty r^n$, et donc, toujours car $|r| < 1$, la série $\sum_{n\geq 1}\varphi_n$ converge normalement sur le segment $[-\pi,\pi]$. D'après le théorème d'interversion série-intégrale, puisque les fonctions φ_n sont également continues, et donc intégrables sur $[-\pi,\pi]$, alors on a

$$\sum_{n=1}^{+\infty}\int_{-\pi}^{\pi}\varphi_n(t)\ dt = \int_{-\pi}^{\pi}\left(\sum_{n=1}^{+\infty}\varphi_n(t)\right)\ dt,$$

et donc

$$f_r(x) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\left(1+\sum_{n=1}^{+\infty} r^n\left(\mathrm{e}^{\mathrm{i}n(x-t)}+\mathrm{e}^{-\mathrm{i}n(x-t)}\right)dt\right).$$

On reconnaît alors le produit de convolution recherché : si on définit

$$P_r(x) = 1+\sum_{n=1}^{+\infty} r^n\left(\mathrm{e}^{\mathrm{i}nx}+\mathrm{e}^{-\mathrm{i}nx}\right),$$

alors on a

$$f_r(x) = f * P_r(x).$$

On appelle les P_r *noyaux de Poisson*, et on a en calculant la somme infinie

$$P_r(x) = \frac{1-r^2}{1-2r\cos(x)+r^2}.$$

En particulier, P_r hérite de la parité du cosinus en x.

Étape 3. Approximation de l'unité.

On va montrer que $(P_r)_{r\in(0,1)}$ vérifie trois axiomes qui font qu'elle est une approximation de l'unité améliorée.

(i) P_r **est positif, pour tout** $r\in(0,1)$**.**
Le numérateur de P_r est bien positif. On étudie le dénominateur. On cherche donc le signe du trinôme $1-2X\cos(x)+X^2$ sur $\mathbb{R}$. Son discriminant est $\Delta = 4(\cos^2(x)-1)\geq 0$, donc le trinôme est bien positif ou nul sur $(0,1)$ (et même strictement positif en étudiant le cas d'égalité).

(ii) P_r **est d'intégrale** 2π**, pour tout** $r\in(0,1)$**.**
On prend simplement à cette endroit de la preuve $f\equiv 1$. On a alors

$$\begin{cases} c_0(f) = 1 \\ c_n(f) = 0, \quad \forall n\in\mathbb{Z}^\times \end{cases}$$

Ainsi, on a

$$1 = f_r(0) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)P_r(-t)\,dt = \frac{1}{2\pi}\int_{-\pi}^{\pi} P_r(t)\,dt.$$

(iii) P_r **se concentre en** 0**.**
Ici, on va montrer précisément

$$\forall\delta\in(0,\pi)\quad \sup_{x\in(-\pi,-\delta)\cup(\delta,\pi)}|P_r(x)| \underset{r\to 1_-}{\longrightarrow} 0. \tag{11.1}$$

On se donne donc $\delta\in(0,\pi)$. Comme r est positif et le cosinus décroissant sur $[0,\pi]$, on a pour $x\in(\delta,\pi)$

$$1-2r\cos(x)+r^2 \geq 1-2r\cos(\delta)+r^2 \geq 0.$$

Par parité de P_r, on en déduit

$$\sup_{x\in(-\pi,-\delta)\cup(\delta,\pi)}|P_r(x)| \leq \frac{1-r^2}{1-2r\cos(\delta)+r^2},$$

et en faisant tendre r vers 1, on déduit (11.1).

En plus de ces trois résultats, on déduit par parité de P_r, en utilisant (ii), le résultat suivant :

$$\frac{1}{2\pi}\int_0^{\pi} P_r(t)\,dt = \frac{1}{2\pi}\int_{-\pi}^{0} P_r(t)\,dt = \frac{1}{2}. \tag{11.2}$$

Étape 3. Convergence simple vers la régularisée.

Soit $x\in\mathbb{R}$. On étudie la convergence de $(f_r(x))_{r\in(0,1)}$. En utilisant (11.2), on remarque que pour $r\in(0,1)$, on a

$$\begin{aligned} f_r(x)-\widetilde{f}(x) &= P_r * f(x) - \frac{1}{2}\left(f(x)_+ + f(x)_-\right) && \text{par commutativité de } * \\ f_r(x)-\widetilde{f}(x) &= \frac{1}{2\pi}\left(\int_{-\pi}^{0} P_r(t)\left(f(x-t)-f(x)_+\right)dt + \int_0^{\pi} P_r(t)\left(f(x-t)-f(x)_-\right)dt\right) \end{aligned}$$

On fixe alors $\varepsilon > 0$. Par définition des limites $f(x)_+$ et $f(x)_-$, il existe $\delta = \delta(\varepsilon) \in (0, \pi)$ tel que

$$\begin{cases} \forall t \in (-\delta, 0) & |f(x-t) - f(x)_+| \leq \varepsilon \\ \forall t \in (0, \delta) & |f(x-t) - f(x)_-| \leq \varepsilon \end{cases}$$

On a alors, comme P_r est positif (2.(i)), et en utilisant l'expression précédente,

$$\begin{aligned} \left|f_r(x) - \widetilde{f}(x)\right| \leq \frac{1}{2\pi} \Bigg(& \int_{-\pi}^{-\delta} P_r(t) \, |f(x-t) - f(x)_+| \, dt + \int_{-\delta}^{0} P_r(t) \, |f(x-t) - f(x)_+| \, dt \\ & + \int_{0}^{\delta} P_r(t) \, |f(x-t) - f(x)_-| \, dt + \int_{\delta}^{\pi} P_r(t) \, |f(x-t) - f(x)_-| \, dt \Bigg). \end{aligned}$$

Une nouvelle fois, la positivité de P_r permet d'affirmer, en appliquant aussi le point 2.(ii) ainsi que (11.2),

$$\frac{1}{2\pi} \int_{-\delta}^{0} P_r(t) \, |f(x-t) - f(x)_+| \, dt \leq \frac{\varepsilon}{2\pi} \int_{-\delta}^{0} P_r(t) \, dt \leq \frac{\varepsilon}{2\pi} \int_{-\pi}^{0} P_r(t) \, dt \leq \frac{\varepsilon}{2}$$

et de même

$$\frac{1}{2\pi} \int_{0}^{\delta} P_r(t) \, |f(x-t) - f(x)_-| \, dt \leq \frac{\varepsilon}{2}.$$

De plus, on a

$$\frac{1}{2\pi} \int_{-\pi}^{-\delta} P_r(t) \, |f(x-t) - f(x)_+| \, dt \leq 2(\pi - \delta) \, \|f\|_\infty \sup_{x \in (-\pi, -\delta)} P_r(x) \leq 2\pi \, \|f\|_\infty \sup_{x \in (-\pi, -\delta) \cup (\delta, \pi)} P_r(x)$$

et de même

$$\frac{1}{2\pi} \int_{\delta}^{\pi} P_r(t) \, |f(x-t) - f(x)_-| \, dt \leq 2\pi \, \|f\|_\infty \sup_{x \in (-\pi, -\delta) \cup (\delta, \pi)} P_r(x).$$

Ainsi, en se donnant grâce à la convergence (11.1) un réel $r_0 = r_0(\delta) = r_0(\varepsilon) \in (0, 1)$, tel que pour tout $r \in (r_0, 1)$ on a

$$\sup_{x \in (-\pi, -\delta) \cup (\delta, \pi)} P_r(x) \leq \varepsilon,$$

on obtient pour $r \in (r_0, 1)$

$$\left|f_r(x) - \widetilde{f}(x)\right| \leq \varepsilon \left(1 + 4\pi \, \|f\|_\infty\right).$$

On en déduit bien que $f_r(x)$ tend vers $\widetilde{f}(x)$ quand r tend vers 1_-.

Étape 4. Convergence uniforme vers f.

Le problème vient ici du fait que l'on a raisonné dans toute l'étape 3 à x fixé, ce qui implique que δ et r_0 dépendent également de x. On doit donc s'affranchir de cette dépendance en utilisant un argument de continuité uniforme. Ici, la périodicité de f nous sauve : pour démontrer le point (ii) de la proposition, on suppose que f est continue sur $[0, 2\pi]$; d'après le théorème de Heine, elle est y est donc uniformément continue, et sa périodicité permet d'affirmer qu'elle est uniformément continue sur $\mathbb{R}$. Cette fois, on dispose donc de $\delta_0 = \delta_0(\varepsilon) > 0$ tel que

$$\forall x, y \in \mathbb{R} \quad (|x - y| \leq \delta_0 \Longrightarrow |f(x) - f(y)| \leq \varepsilon$$

On peut une nouvelle fois choisir de prendre $\delta_0 \in (0, \pi)$ (quitte à le diminuer), et donc on a cette fois par la convergence (11.1) l'existence de $r_0 \in (0, 1)$ qui ne dépend cette fois plus que du réel ε tel que pour $r \in (r_0, 1)$

$$\sup_{x \in (-\pi, -\delta_0) \cup (\delta_0, \pi)} P_r(x) \leq \varepsilon.$$

Un calcul presque identique à celui de l'étape 3 donne alors

$$\left|f_r(x) - \widetilde{f}(x)\right| \leq \varepsilon \left(1 + 4\pi \, \|f\|_\infty\right),$$

mais cette fois-ci pour tout réel x, ce qui permet de conclure sur le point (ii) de la proposition.

□

Chapitre III

Algèbre & Analyse

1 Constante de connectivité du réseau hexagonal

Leçons 190, 223, 230, 243(, 241)

Ref :

Ce développement s'inspire du travail que j'ai effectué pendant mon stage de Master 1, je n'ai donc pas de référence disponible le jour de l'Agrégation pour les étapes 1, 2 et 5. En revanche, le théorème de Cauchy-Hadamard est démontré dans [EA11], et le lemme de Fekete dans [FGN09a].

On se donne un entier $d \geq 1$, et on se place sur le réseau $\mathbb{Z}^d$ de $\mathbb{R}^d$.

Définition 1.1 On appelle *sommet* tout élément du réseau $\mathbb{Z}^d$, et *arête* tout segment reliant deux sommets.

Définition 1.2 On appelle *chemin* ω de taille $n \geq 0$, ou *n-chemin*, les positions successives notées $(\omega_0, .., \omega_n)$ d'une marche aléatoire sur un réseau, partant de l'origine de $\mathbb{R}^d$. Si de plus la marche passe au plus une fois par chaque sommet, on dit que la marche et le chemin sont *auto-évitants*. On appelle aussi *taille* de ω le nombre $\ell(\omega) = n$ d'étapes effectuées.

On note c_n le nombre de chemins auto-évitants de taille n sur le réseau hexagonal. On énonce le théorème qui donne la vitesse de croissance exponentielle de cette suite, dont on ne donne pas la preuve complète, qui prendrait bien trop de temps.

Théorème 1.3 La constante de connectivité du réseau hexagonal est $\mu = x_c^{-1} = \sqrt{2+\sqrt{2}}$, où x_c est le rayon de convergence de la série génératrice $\sum_{n\geq 0} c_n z^n$.

Démonstration.

Étape 1. Comportement asymptotique des chemins auto-évitants.

On montre va d'abord montrer que le nombre de chemins auto-évitants de taille n croit exponentiellement vite, et on a même pour tout $n \geq 0$

$$\sqrt{2}^n \leq c_n \leq 3 \cdot 2^{n-1}.$$

- On construit un premier chemin auto-évitant, comme sur la figure 1.1, en suivant toujours l'arête qui va de gauche à droite sans changer l'ordonnée (en rouge), quand celle-ci est disponible, c'est-à-dire une étape sur deux ; et quand elle ne l'est pas, on prend au hasard l'une des deux possibilités restantes (en bleu) : ainsi, on a un choix à faire entre deux possibilités toutes les deux étapes. Donc, en tout, il y a $2^{\left[\frac{n}{2}\right]}$ possibilités. On en déduit que l'on a bien
$$c_n \geq \sqrt{2}^n.$$
- Pour le premier pas, on a toujours trois possibilités, qui sont les trois sommets adjacents à l'origine ; ensuite, on a au plus deux possibilités, puisque pour qu'un chemin soit auto-évitant, il ne doit pas

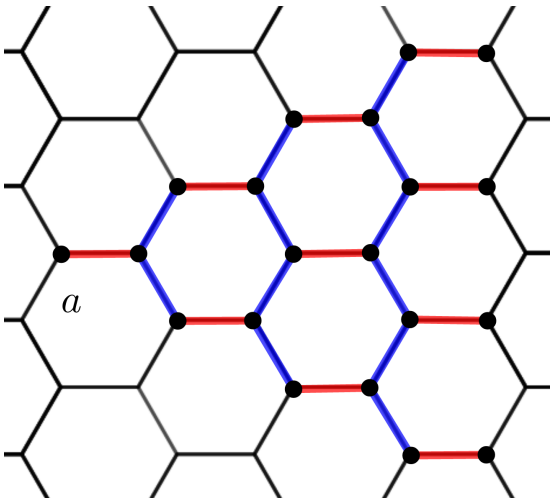


Figure 1.1 – Une borne inférieure du nombre de n-chemins auto-évitants

revenir sur ses pas, donc au plus deux des trois sommets adjacents (ceux dont on ne vient pas) sont disponibles. Cela montre que l'on a

$$c_n \leq 3 \cdot 2^{n-1}.$$

Donc si elle existe, la constante de connectivité est comprise entre $\sqrt{2}$ et 2.

Étape 2. Sous-mutliplicativité du nombre de chemins auto-évitants.

On va montrer que la suite $(c_n)_{n\geq 0}$ est sous-multiplicative :

$$\forall n, m \in \mathbb{N} \quad c_{n+m} \leq c_n c_m. \tag{1.1}$$

Soient n et m deux entiers. On se donne un chemin ω de Ω_{n+m}, et on le coupe au n-ième sommet : on définit alors deux chemins $\omega_I \in \Gamma_n$ et $\omega_{II} \in \Gamma_m$ de la manière suivante :

$$\begin{cases} \forall i \in [\![0, n]\!] & \omega_{I,i} = \omega_i \\ \forall i \in [\![0, m]\!] & \omega_{II,i} = \omega_{n+i} - \omega_n \end{cases}$$

de sorte que $\omega = \omega_I \circ \omega_{II}$. Si la concaténation de deux chemins auto-évitants n'est pas forcément un chemin auto-évitant, la réciproque est vraie : en coupant comme on vient de le faire un chemin auto-évitant, on obtient deux chemins auto-évitants. On le voit sur la figure 1.2b, où l'on a coupé le chemin qui va de a à c au point b, créant ainsi deux chemins auto-évitants, celui en rouge, et celui en orange. Cela se démontre formellement : si pour deux entiers i et j, on a $\omega_{I,i} = \omega_{I,j}$, alors $\omega_i = \omega_j$, ce qui contredit le fait que ω est auto-évitant, donc ω_I l'est nécessairement ; et le même raisonnement par l'absurde montre que ω_{II} est lui aussi auto-évitant. On en déduit l'inégalité ensembliste suivante :

$$\Omega_{n+m} \subset \Omega_n \times \Omega_m.$$

En passant au cardinal de ces ensembles finis, on déduit l'inégalité (1.1).

Étape 3. Lemme de Fekete.

Lemme 1.4 (Fekete) Soit $(a_n)_{n\geq 1}$ une suite de réels sous-additive au sens classique, i.e. vérifiant

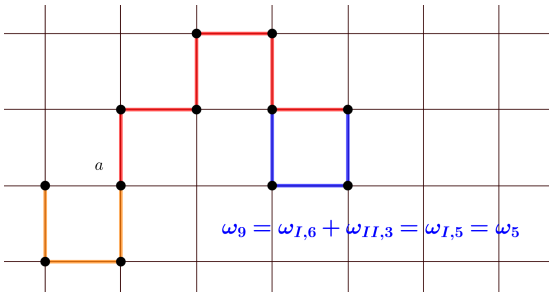
$$\forall n, m \in \mathbb{N} \quad a_{n+m} \leq a_n + a_m.$$

Alors la limite de la suite $\left(\frac{a_n}{n}\right)_{n\geq 1}$ existe dans $[-\infty, +\infty)$, et elle est égale à la borne inférieure de la suite :

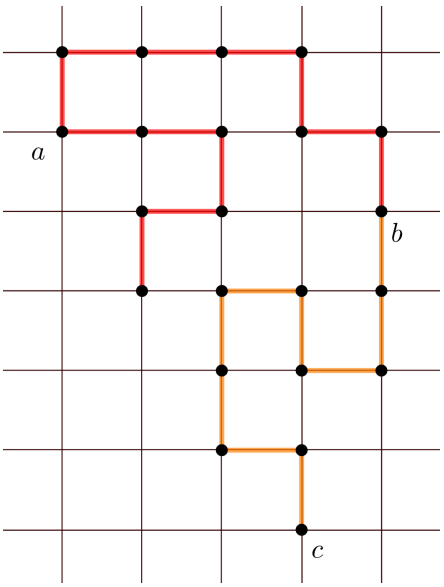
$$\lim_{n\to\infty} \frac{a_n}{n} = \inf_{n\to\infty} \frac{a_n}{n}. \tag{1.2}$$

On effectue une preuve de ce lemme en deux temps. On commence par fixer $k \in \mathbb{N}$, et on va montrer

$$\overline{\lim_{n\to\infty}} \frac{a_n}{n} \leq \frac{a_k}{k}, \tag{1.3}$$



(a) Concaténation de deux chemins auto-évitants



(b) Troncature d'un chemin auto-évitant

Figure 1.2 – Concaténation, troncature de chemins auto-évitants et nature des chemins créés

où $\overline{\lim}$ désigne la limite supérieure. On note $A_k = \max_{1\leq r\leq k} a_r$, et on se donne les deux entiers $q \in \mathbb{N}$ et $r \in [\![1,k]\!]$ (uniquement déterminés par division euclidienne) tels que $n = qk + r$. On a alors par sous-additivité

$$a_n \leq qa_k + a_r \leq \frac{n}{k} a_k + A_k.$$

On divise alors par n des deux côtés de l'inégalité, et on passe à la limite supérieure. Le terme $\frac{A_k}{n}$ étant borné au numérateur (puisque k est fixé), il disparaît à la limite en n, ce qui montre effectivement l'inégalité (1.3).

On passe ensuite à la limite inférieure en k dans (1.3), ce qui permet de montrer que les deux limites, supérieures et inférieures, sont égales. Ainsi, la limite existe, et en passant à la borne inférieure en k dans (1.3), on montre qu'elle vaut bien $\inf_{n\to\infty} \frac{a_n}{n}$. De plus, cela montre que la limite ne peut valoir $+\infty$.

Étape 4. Règle de Cauchy et théorème de Cauchy-Hadamard.

On se donne une suite de réels positifs $(u_n)_{n\geq 0}$ et on considère

$$L = \overline{\lim}(u_n)^{\frac{1}{n}},$$

qui est réel ou égal à $+\infty$.

- Supposons $L < 1$. On se donne $a \in (L, 1)$. Il existe donc un nombre fini d'entiers n tels que $u_n^{\frac{1}{n}} > a$. Donc pour $n \geq N$, où N est plus grand que tous ces entiers, on a $u_n \leq a^n$. Or la série $\sum a_n$ converge, donc $\sum u_n$ aussi.
- À l'inverse, si $L > 1$, il existe une infinité d'entiers n tels que $u_n > 1$ (car $u_n^{\frac{1}{n}} > 1$). La suite $(u_n)_{n\geq 0}$ ne tend donc pas vers 0, donc la série $\sum u_n$ diverge grossièrement.

On applique cela aux séries entières : le rayon de convergence de la série $\sum_{n\geq 0} a_n z^n$ est $R = \left(\overline{\lim}\, a_n^{\frac{1}{n}}\right)^{-1}$.

Étape 5. Constante de connectivité et lien avec la fonction génératrice.

On va finalement démontrer l'existence de la constante de connectivité de la suite $(c_n)_{n\geq 0}$, définie par

$$\mu := \lim_{n\to\infty} c_n^{\frac{1}{n}}. \tag{1.4}$$

On considère la suite $(\ln(c_n))_{n\geq 1}$, qui est, d'après l'étape 2, sous-additive. D'après le lemme de Fekete, la suite $\left(\frac{\ln(c_n)}{n}\right)_{n\geq 1}$ converge donc vers sa borne inférieure, que l'on note $\widetilde{\mu}$. De plus, on a pour tout

$n \geq 1$ toujours au moins un élément dans Ω_n, ce qui montre que $c_n \geq 1$ et donc que la suite $\left(\frac{\ln(c_n)}{n}\right)_{n\geq 1}$ est à valeurs positives. Ainsi, sa limite est positive. Le fait qu'elle soit finie est une autre conséquence du lemme. On pose alors $\mu = \mathrm{e}^{\tilde{\mu}} \geq 1$, et par composition des limites, on a bien

$$c_n^{\frac{1}{n}} \underset{n\to\infty}{\longrightarrow} \mu \tag{1.5}$$

De plus, on déduit de l'étape 4 que l'étude de la série génératrice $\sum_{n\geq 0} c_n z^n$ fournit la valeur de cette constante, à partir de celle de x_c. □

La fin de la démonstration consiste à utiliser différentes caractéristiques des chemins auto-évitants et du réseau hexagonal pour déterminer la valeur de ce rayon de convergence. L'intérêt est ici d'utiliser des techniques d'analyse pour faire de la combinatoire et compter des objets, comme justement les chemins auto-évitants.

Remarque.

- Au vu de la preuve du lemme de Fekete, rien de permet d'affirmer que la limite ne peut pas être $-\infty$. D'ailleurs, c'est possible ! Cela se voit en prenant $a_n = -n^2$, qui donne bien une suite sous-additive, mais la suite $\left(\frac{a_n}{n}\right)_{n\geq 1}$ est la suite $(-n)_{n\geq 1}$, qui diverge vers $-\infty$.

2 Différentielle du déterminant

Leçons 152, 215

Ref : [Rou03] Exo 26 & Exo 94

Théorème 2.1 Le déterminant est de classe C^1 sur $\mathcal{M}_n(\mathbb{R})$, et sa différentielle est donnée par

$$\forall M, H \in \mathcal{M}_n(\mathbb{R}) \quad d_M \det(H) = \mathrm{Tr}\left({}^t\mathrm{Com}(M)H\right).$$

Démonstration.

On munit $\mathcal{M}_n(\mathbb{R})$ d'une norme quelconque, puisque les normes sont équivalentes. Le déterminant étant polynomial sur $\mathcal{M}_n(\mathbb{R})$, il y est donc de classe C^1 (et même C^∞).

Étape 1. Différentielle en l'identité.

On note I la matrice identité de taille n. On se donne $H \in \mathcal{M}_n(\mathbb{R})$, et on note $(\lambda_1, .., \lambda_n)$ ses valeurs propres (complexes). On a alors pour $t \in \mathbb{R}$

$$\begin{array}{rcl} \det(I+tH) & = & \prod_{i=1}^{n} 1+t\lambda_i \\ & = & 1 + t\,\mathrm{Tr}(H) + O(t^2) \\ \det(I+tH) & = & 1 + t\,\mathrm{Tr}(H) + o(t) \end{array}$$

Par définition de la différentielle, on a donc $d_I \det = \mathrm{Tr}$.

Étape 2. Différentielle en une matrice inversible.

Soit $M \in GL_n(\mathbb{R})$, et $H \in \mathcal{M}_n(\mathbb{R})$. On se ramène au cas de l'identité :

$$\begin{array}{rcll} \det(M+H) & = & \det(M(I+M^{-1}H)) & \text{car } M \in GL_n(\mathbb{R}) \\ & = & \det(M)\det(I+M^{-1}H) & \\ & = & \det(M)(1+\mathrm{Tr}(M^{-1}H)+o(\|H\|)) & \text{d'après l'étape 1} \\ \det(M+H) & = & \det(M)+\mathrm{Tr}\left({}^t\mathrm{Com}(M)H\right)+o(\|H\|) & \text{car } \det(M)M^{-1} = {}^t\mathrm{Com}(M) \end{array}$$

Donc on a une nouvelle fois la formule souhaitée.

Étape 3. Conclusion par densité.

Les matrices inversibles forment un ouvert dense de $\mathcal{M}_n(\mathbb{R})$. Or le déterminant est de classe C^1, donc sa différentielle est continue : comme l'étape 2 donne sa formule sur un ouvert dense, on peut la prolonger par continuité à $\mathcal{M}_n(\mathbb{R})$. Comme les applications qui associent respectivement à une matrice sa transposée et sa comatrice sont elles aussi continues (car polynomiales), la formule obtenue est stable par continuité : on a bien

$$\forall M, H \in \mathcal{M}_n(\mathbb{R}) \quad d_M \det(H) = \mathrm{Tr}\left({}^t\mathrm{Com}(M)H\right).$$

□

Application 2.2 $SL_n(\mathbb{R})$ est une sous-variété de $\mathcal{M}_n(\mathbb{R})$ de dimension n^2-1, et son plan tangent en M est donné par

$$T_M SL_n(\mathbb{R}) = \left\{H \in \mathcal{M}_n(\mathbb{R}),\ \mathrm{Tr}(M^{-1}H) = 0\right\}.$$

Démonstration. Tout d'abord, $\mathcal{M}_n(\mathbb{R})$ est isomorphe à $\mathbb{R}^{n^2}$, donc on peut bien parler de "sous-variété de $\mathcal{M}_n(\mathbb{R})$" comme quand on parle de "sous-variété de $\mathbb{R}^n$" [1]. On définit l'application

$$F : \left| \begin{array}{ccc} GL_n(\mathbb{R}) & \longrightarrow & \mathbb{R} \\ M & \longmapsto & \det(M)-1 \end{array} \right. ,$$

qui est définie d'un ouvert de $\mathcal{M}_n(\mathbb{R})$ dans $\mathbb{R}$. Le théorème précédent montre que F est polynomiale et que sa différentielle en $M \in GL_n(\mathbb{R})$ est donnée par

$$\forall H \in GL_n(\mathbb{R}) \quad d_M F(H) = \det(M)\,\mathrm{Tr}(M^{-1}H).$$

1. Ca permet de ne pas définir les variétés différentielles en elles-même...

En particulier, comme M est inversible, c'est une forme n-linéaire non nulle, donc surjective, ce qui prouve que F est une submersion, et donc $F^{-1}(\{0\}) = SL_n(\mathbb{R})$ est une sous-variété de $\mathcal{M}_n(\mathbb{R})$ de dimension $n^2 - 1$. De plus, on sait que son plan tangent en $M \in SL_n(\mathbb{R})$ est le noyau de la différentielle de F en M :

$$T_M SL_n(\mathbb{R}) = \ker(d_M F) = \left\{ H \in \mathcal{M}_n(\mathbb{R}),\ \mathrm{Tr}(M^{-1}H) = 0 \right\}.$$

□

3 Ellispsoïde de John Löwner

Leçons 152, 158, 171, 219, 229, 253(, 150, 160, 191, 203, 215)

Ref : [FGN09c] 3.37

On munit $\mathbb{R}^n$ de sa structure euclidienne usuelle. On note respectivement $\mathcal{Q}$, $\mathcal{Q}^+$ et $\mathcal{Q}^{++}$ les ensembles des formes quadratiques, quadratiques semi-définies positives, et quadratiques définies postives sur $\mathbb{R}^n$. On note B_q, pour $q \in \mathcal{Q}^{++}$, la boule unité fermée de q :

$$B_q := \{x \in \mathbb{R}^n,\ q(x) \leq 1\}.$$

Théorème 3.1 Soit K un compact d'intérieur non vide de $\mathbb{R}^n$. Il existe une unique ellipsoïde de volume minimal, centrée en 0, contenant K.

Démonstration.

Comme les ellipsoïdes sont exactement les boules unité des formes quadratiques définies positives, ce problème revient à trouver un élément q de $\mathcal{Q}^{++}$ tel que B_q soit de volume minimal parmi les boules unités des éléments de $\mathcal{Q}^{++}$ contenant K.

Étape 1. Volume de la boule unité et reformulation.

Soit $q \in \mathcal{Q}^{++}$. On calcule pour commencer le volume de B_q, que l'on note V_q. On se donne une base orthonormée $(e_1, .., e_n)$ de $\mathbb{R}^n$ dans laquelle $q(x) = \sum_{i=1}^{n} a_i x_i^2$, pour tout $x = \sum_{i=1}^{n} x_i e_i$, avec $a_1, .., a_n$ strictement positifs. On note $D(q) = a_1..a_n$ le déterminant de q dans n'importe quelle base orthonormée de $\mathbb{R}^n$. On a alors

$$\begin{aligned} V_q &= \int_{B_q} dx_1..dx_n \\ &= \int_{a_1x_1^2+..+a_nx_n^2 \leq 1} dx_1..dx_n \\ &= \int_{t_1^2+..+t_n^2} \frac{dt_1..dt_n}{\sqrt{D(q)}} \qquad \text{par changement de variable } x_i = \frac{t_i}{\sqrt{a_i}} \\ V_q &= \frac{V_0}{\sqrt{D(q)}} \end{aligned}$$

où V_0 désigne le volume de la boule unité pour la norme euclidienne. Ainsi, montrer le théorème revient à montrer qu'il existe une forme quadratique $q \in \mathcal{Q}^{++}$ qui maximise le déterminant parmi celles dont la boule unité contient K.

Étape 2. Restriction à un convexe compact non vide.

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

$$\forall q \in \mathcal{Q} \quad N(q) := \sup_{\|x\| \leq 1} |q(x)|.$$

On pose alors $\mathcal{A} = \{q \in \mathcal{Q}^+,\ \forall x \in K\ q(x) \leq 1\}$. On va chercher à maximiser le déterminant sur ce domaine.

- $\mathcal{A}$ est convexe car si q et q' sont dans $\mathcal{A}$, et $\lambda \in [0,1]$, $\lambda q + (1-\lambda)q'$ est semi-définie positive, et on a pour $x \in K$
$$\lambda q(x) + (1-\lambda)q'(x) \leq \lambda + 1 - \lambda = 1.$$
- Soit $(q_n)_{n\geq 0}$ une suite d'éléments de $\mathcal{A}$ convergeant vers $q \in \mathcal{Q}$. Alors pour $x \in \mathbb{R}^n$, on a
$$|q_n(x) - q(x)| \leq N(q_n - q)\|x\|^2.$$
On en déduit que $q_n(x)$ converge vers $q(x)$. Mais comme q_n est définie, cette suite est positive, donc $q(x)$ est positive, ce qui signifie que q est semi-définie positive. De plus, si x est dans K, la suite $(q_n(x))_{n\geq 0}$ est aussi majorée par 1, donc la limite aussi. Cela signifie que $q \in \mathcal{A}$. Ainsi, $\mathcal{A}$ est fermé dans $\mathcal{Q}$.

– Comme K est d'intérieur non vide [2], on peut se donner $a \in K$ et $r > 0$ tels que la boule $B(a,r)$ soit incluse dans K. Soit $q \in \mathcal{A}$. Si $\|x\| \leq r$, alors $q(a+x) \leq 1$ car $a + x \in B(a,r)$. De plus, $q(a) = q(-a) \leq 1$. On a alors

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

par inégalité de Minkowski. Ainsi, $q(x) \leq 4$. On en déduit que si $\|x\| \leq 1$, on a

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

Donc $N(q) \leq \dfrac{4}{r^2}$ et $\mathcal{A}$ est bornée.

– Comme K est compact, il est inclus dans la boule fermée $B(0,M)$, pour un certain $M > 0$, et donc si $q(x) = \dfrac{\|x\|^2}{M^2}$, q est dans $\mathcal{A}$. Donc $\mathcal{A}$ est non vide.

On a donc montré que $\mathcal{A}$ est un convexe compact non vide de $\mathcal{Q}$ [3].

Étape 3. Stricte convexité logarithmique du déterminant.

Lemme 3.2 Soit $A, B \in S_n^{++}(\mathbb{R})$ et $\lambda \in (0,1)$. Alors on a

$$\det(\lambda A + (1-\lambda)B) \geq \det(A)^\lambda \det(B)^{1-\lambda},$$

avec égalité si et seulement si $A = B$.

Démonstration. Comme $A \in S_n^{++}(\mathbb{R})$ et $B \in S_n^{++}(\mathbb{R}) \subset S_n(\mathbb{R})$, on peut appliquer le théorème de pseudo-réduction simultanée : il existe $P \in GL_n(\mathbb{R})$ telle que $A = {}^tPP$ et une famille de réels $(d_i)_{1\leq i\leq n}$ tels que $B = {}^tPDP$, où $D = \mathrm{diag}(d_i)$. Comme $B \in S_n^{++}(\mathbb{R})$ les d_i sont tous positifs strictement [4]. On a alors pour $\lambda \in [0,1]$

$$\begin{cases} \det(A)^\lambda \det(B)^{1-\lambda} = \det(P)^{2\lambda} \det(P)^{2(1-\lambda)} \det(D)^{1-\lambda} = \det(P)^2 \det(D)^{1-\lambda} \\ \det(\lambda A + (1-\lambda)B) = \det(P)^2 \det(\lambda I + (1-\lambda)D) \end{cases}$$

On a alors

$$\begin{aligned} & \det(\lambda A + (1-\lambda)B) \geq \det(A)^\lambda \det(B)^{1-\lambda} \\ \iff & \det(\lambda I + (1-\lambda)D) \geq \det(D)^{1-\lambda} \\ \iff & \prod_{i=1}^n \lambda + (1-\lambda)d_i \geq \left(\prod_{i=1}^n d_i\right)^{1-\lambda} \\ \iff & \sum_{i=1}^n \ln(\lambda + (1-\lambda)d_i) \geq (1-\lambda) \sum_{i=1}^n \ln(d_i) \end{aligned}$$

Or la dernière ligne est vraie par concavité du logarithme. De plus, l'inégalité est stricte si et seulement si l'un des d_i est différent de 1 (par stricte concavité du logarithme), ce qui est équivalent à dire que $A \neq B$. □

Étape 4. Maximisation du déterminant sur $\mathcal{A}$.

Comme l'application déterminant est continue, l'application

$$D : \left| \begin{array}{ccc} \mathcal{Q} & \longrightarrow & \mathbb{R} \\ q & \longmapsto & D(q) \end{array} \right.$$

est continue sur le compact non vide $\mathcal{A}$. Elle admet donc un maximum, en un point $q_0 \in \mathcal{A}$. De plus, $\mathcal{A}$ contient comme on l'a vu la forme $\dfrac{\|\cdot\|^2}{M^2}$, qui est définie positive. Donc $D(q_0)$ est strictement positif, et $q_0 \in \mathcal{Q}^{++}$. Il existe donc un ellipsoïde de volume minimal contenant K. Montrons qu'il est unique.

2. C'est le seul endroit où l'on a besoin de cette hypothèse.

3. $\mathcal{Q}$ est un espace vectoriel de dimension finie, donc ses compacts sont les fermés bornés.

4. Tout d'abord, ne pas confondre les d_i avec les valeurs propres de B, P n'est pas orthogonale. Le résultat se montre en fixant par l'absurde un d_i négatif. On se donne $X = P^{-1}e_i$. On a alors

$${}^tXBX = {}^te_iDe_i = d_i \leq 0,$$

ce qui est absurde puisque B est définie positive.

On se donne $q \in \mathcal{A}$ un autre maximum de D, on suppose par l'absurde que $q \neq q_0$. On note S_q et S_{q_0} les matrices respectives de q et q_0 dans la base canonique de $\mathbb{R}^n$ (qui sont donc symétriques définies positives). Par stricte concavité logarithmique du déterminant, on a

$$D\left(\frac{q+q_0}{2}\right) = \det\left(\frac{S_q + S_{q_0}}{2}\right) > \sqrt{\det(S_q)\det(S_{q_0})} = \sqrt{D(q_0)^2} = D(q_0),$$

ce qui contredit la maximalité de $D(q_0)$. Donc l'ellipsoïde obtenue est bien unique. □

On peut privilégier l'étape 1 ou l'étape 3 suivant la leçon : la marche à suivre est globalement de démontrer l'étape 1 dans les leçons d'algèbre et l'étape 3 dans les leçons d'analyse. Si celui-ci ne figure pas dans le plan, il peut être bon de préciser que l'on admet le théorème de pseudo-réduction simultanée pour la démonstration de l'étape 3.

4 Gradient à pas optimal

Leçons 162, 219, 226, 229, 233, 253(, 181, 215)

Ref : [HU09] Exos I.9 & II.8

Ce développement démontre la convergence d'une méthode d'approximation du minimum d'une fonctionnelle, qui peut également servir à approcher la solution d'un système linéaire. On doit mentionner dans le plan les résultats préliminaires, et bien sûr présenter l'algorithme de gradient à pas optimal.

On fixe une matrice $A \in \mathcal{M}_n(\mathbb{R})$ symétrique définie positive, $b \in \mathbb{R}^n$ et $c \in \mathbb{R}$. On pose alors, pour $x \in \mathbb{R}^n$

$$f(x) = \frac{1}{2}\langle Ax, x\rangle - \langle b, x\rangle + c.$$

On cherche alors à minimiser la fonctionnelle f sur $\mathbb{R}^n$. Comme f est strictement convexe et 1-coercive, il existe une unique solution $\overline{x} \in \mathbb{R}^n$ à ce problème, caractérisé par le fait d'être l'unique solution du système linéaire

$$Ax = b,$$

ce qui se démontre en étudiant les zéros du gradient de f.

Voici l'algorithme dont nous allons étudier la convergence.

Algorithme 4.1 (Gradient à pas optimal) On fixe $x^{(0)} \in \mathbb{R}^n$. Pour construire récursivement la suite $(x^{(k)})_{k\in\mathbb{N}}$, on suppose les premiers éléments construits, et on pose

$$\begin{cases} d_k = -\nabla f(x^{(k)}) = b - Ax^{(k)} \\ x^{(k+1)} = x^{(k)} + t_k d_k \end{cases}$$

où t_k est l'unique réel (positif) minimisant la fonction $t \longmapsto f(x^{(k)} + td_k)$. On s'arrête quand on a atteint un seuil de tolérance $\varepsilon > 0$ fixé au préalable, c'est-à-dire quand $\left\|\nabla f(x^{(k)})\right\| < \varepsilon$.

Lemme 4.2 (Inégalité de Kantorovitch) Soit $A \in S_n^{++}(\mathbb{R})$, $\lambda_1 \geq .. \geq \lambda_n$ ses valeurs propres. On a alors pour $x \in \mathbb{R}^n$

$$\|x\|^4 \leq \langle Ax, x\rangle \left\langle A^{-1}x, x\right\rangle \leq \frac{1}{4}\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^2 \|x\|^4 .$$

Démonstration. Il suffit bien sûr de montrer ce résultat pour les vecteurs de norme 1. Soit donc $x \in \mathbb{S}^{n-1}$. On se donne $P \in O_n(\mathbb{R})$ tel que $D = PA{}^tP$ soit diagonale, avec les λ_i sur la diagonale. Via le changement de variable $y = Px$, il faut alors montrer [5]

$$1 \leq \langle Dy, y\rangle \left\langle D^{-1}y, y\right\rangle \leq \frac{1}{4}\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^2 .$$

On suppose que A n'est pas une homothétie (sinon il n'y a rien à démontrer), et on a donc $\lambda_1 > \lambda_n$. On pose $\alpha_i = y_i^2$, de sorte que

$$\begin{cases} \langle Dy, y\rangle = \displaystyle\sum_{i=1}^n \alpha_i\lambda_i =: \overline{\lambda} \\ \left\langle D^{-1}y, y\right\rangle = \displaystyle\sum_{i=1}^n \frac{\alpha_i}{\lambda_i} \end{cases}$$

ce qui signifie que ces deux quantités sont des combinaisons convexes respectives des λ_i et des $\dfrac{1}{\lambda_i}$ (puisque $\displaystyle\sum_{i=1}^n \alpha_i = \|y\|^2 = 1$). On considère alors le graphe de la fonction inverse sur $\mathbb{R}_+^*$, et on note $M_i = \left(\lambda_i, \dfrac{1}{\lambda_i}\right)$ les différents points du graphe correspondant aux valeurs propres de A. Le barycentre M de ces points, associés aux coefficients α_i, est alors dans le domaine $\mathcal{D}$ délimité par le graphe et la droite (M_1M_n) (voir figure 4.1). On considère alors les points M^* et M_*, qui ont la même abscisse $\overline{\lambda}$ que M et qui sont respectivement sur la droite (M_1M_n) et sur le graphe de la fonction inverse.

5. Comme P est orthogonale, y est toujours de norme 1.

– M est d'ordonnée $\left\langle D^{-1}y, y\right\rangle$;
– M_* est d'ordonnée $\dfrac{1}{\overline{\lambda}}$;
– M^* est d'ordonnée $\dfrac{1}{\lambda_1} + \dfrac{1}{\lambda_n} + \dfrac{\overline{\lambda}}{\lambda_1\lambda_n}$.

La convexité de la fonction inverse montre que l'ordonnée de M est plus petite que celle de M^* et plus grande que celle de M_*, soit

$$\begin{cases} \left\langle D^{-1}y, y\right\rangle \geq \dfrac{1}{\overline{\lambda}} & \text{i. e.} \qquad \langle Dy, y\rangle \left\langle D^{-1}y, y\right\rangle \geq 1 \\ \left\langle D^{-1}y, y\right\rangle \leq \dfrac{\lambda_1 + \lambda_n - \overline{\lambda}}{\lambda_1\lambda_n} & \text{i. e.} \qquad \langle Dy, y\rangle \left\langle D^{-1}y, y\right\rangle \leq \dfrac{\overline{\lambda}(\lambda_1 + \lambda_n - \overline{\lambda})}{\lambda_1\lambda_n} \end{cases}$$

On fait une étude de fonction pour déterminer le maximum de $u \longmapsto \dfrac{u(\lambda_1 + \lambda_n - u)}{\lambda_1\lambda_n}$. Celui-ci vaut

$$\frac{1}{\lambda_1\lambda_n}\left(\frac{\lambda_1 + \lambda_n}{2}\right)^2 = \frac{1}{4}\left(\frac{\lambda_1}{\lambda_n} + \frac{\lambda_n}{\lambda_1} + 2\right) = \frac{1}{4}\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^2,$$

ce qui permet de conclure.

□

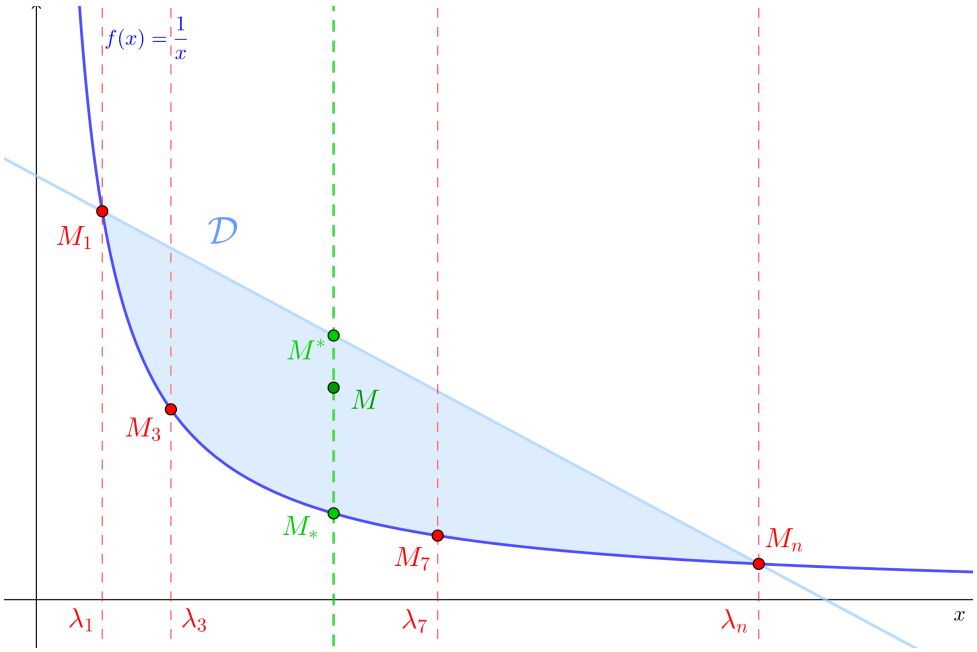


Figure 4.1 – Convexité dans le lemme de Kantorovitch

Théorème 4.3 La méthode du gradient à pas optimal converge de manière géométrique, la vitesse étant reliée au conditionnement de la matrice A, donnée par $\dfrac{c(A) - 1}{c(A) + 1}$.

Démonstration.

Étape 1. Expression de t_k et de $f(x^{(k+1)})$.

On étudie la fonction f_k définie sur $\mathbb{R}$ par

$$f_k(t) := f(x^{(k)} + td_k) = f(x_k) + t\left\langle Ax^{(k)} - b, d_k\right\rangle + \frac{t^2}{2}\left\langle Ad_k, d_k\right\rangle.$$

On suppose $d_k = b - Ax^{(k)}$ non nul (sinon l'algorithme s'arrête). Comme A est définie positive et d_k non nul, f_k est un polynôme de degré 2 avec coefficient dominant srtictement positif, et est donc minoré sur

$\mathbb{R}$ par sa valeur en $t_k = \dfrac{\|d_k\|^2}{\langle Ad_k, d_k\rangle} > 0$. On en déduit la valeur de $f(x^{(k+1)})$:

$$f(x^{(k+1)}) = f(x^{(k)}) - \frac{1}{2}\frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle}. \tag{4.1}$$

On cherche à évaluer l'écart de $f(x^{(k)})$ au minimum $\overline{f}$ de f, dont on sait qu'il vaut

$$\overline{f} = f(\overline{x}) = -\frac{1}{2}\left\langle A^{-1}b, b\right\rangle + c.$$

On a d'après (4.1)

$$f(x^{(k+1)}) - \overline{f} = \left(f(x^{(k)}) - \overline{f}\right)\left(1 - \frac{\|d_k\|^4}{2(f(x^{(k)}) - \overline{f})\langle Ad_k, d_k\rangle}\right).$$

On observe alors que

$$\begin{aligned}\left\langle A^{-1}d_k, d_k\right\rangle &= \left\langle A^{-1}(b - Ax^{(k)}), b - Ax^{(k)}\right\rangle \\ &= 2\left(\frac{1}{2}\left\langle Ax^{(k)}, x^{(k)}\right\rangle - \left\langle b, x^{(k)}\right\rangle + \frac{1}{2}\left\langle A^{-1}b, b\right\rangle\right)\end{aligned}$$

$$\left\langle A^{-1}d_k, d_k\right\rangle = 2\left(f(x^{(k)} - \overline{f})\right)$$

On a donc finalement

$$f(x^{(k+1)}) - \overline{f} = \left(f(x^{(k)}) - \overline{f}\right)\left(1 - \frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle\left\langle A^{-1}d_k, d_k\right\rangle}\right).$$

Étape 2. Conditionnement et vitesse de convergence.

On introduit finalement le *conditionnement* de la matrice A :

$$c(A) := \rho(A)\rho(A^{-1}) = \frac{\lambda_1}{\lambda_n}.$$

Cette valeur est celle qui dirige la convergence de la méthode du gradient. On se donne $k \in \mathbb{N}$, et on suppose que l'algorithme n'est pas encore terminé à l'étape k. On déduit de l'inégalité de Kantorovitch, toujours avec $d_k \neq 0$:

$$\frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle\left\langle A^{-1}d_k, d_k\right\rangle} \geq 4\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^{-2} = 4\frac{\lambda_1/\lambda_n}{(\lambda_1/\lambda_n + 1)^2} = 4\frac{c(A)}{(c(A)+1)^2}.$$

On déduit alors de la relation obtenue à la première étape que l'on a

$$f(x^{(k+1)}) - \overline{f} \leq \left(f(x^{(k)}) - \overline{f}\right)\left(1 - 4\frac{c(A)}{(c(A)+1)^2}\right) = \left(f(x^{(k)}) - \overline{f}\right)\left(\frac{c(A)-1}{c(A)+1}\right)^2.$$

On obtient finalement par récurrence

$$f(x^{(k)}) - \overline{f} \leq \left(f(x^{(0)}) - \overline{f}\right)\left(\frac{c(A)-1}{c(A)+1}\right)^{2k}. \tag{4.2}$$

On peut également exprimer la vitesse de convergence de la suite $(x^{(k)})$: on a

$$\begin{aligned}f(x^{(k)}) - \overline{f} &= \frac{1}{2}\left\langle Ax^{(k)}, x^{(k)}\right\rangle + \left\langle b, x^{(k)}\right\rangle + c - \overline{f} \\ &= \frac{1}{2}\left\langle A(x^{(k)} - \overline{x}), x^{(k)} - \overline{x}\right\rangle \\ f(x^{(k)}) - \overline{f} &\geq \frac{1}{2}\lambda_n\left\|x^{(k)} - \overline{x}\right\|^2\end{aligned}$$

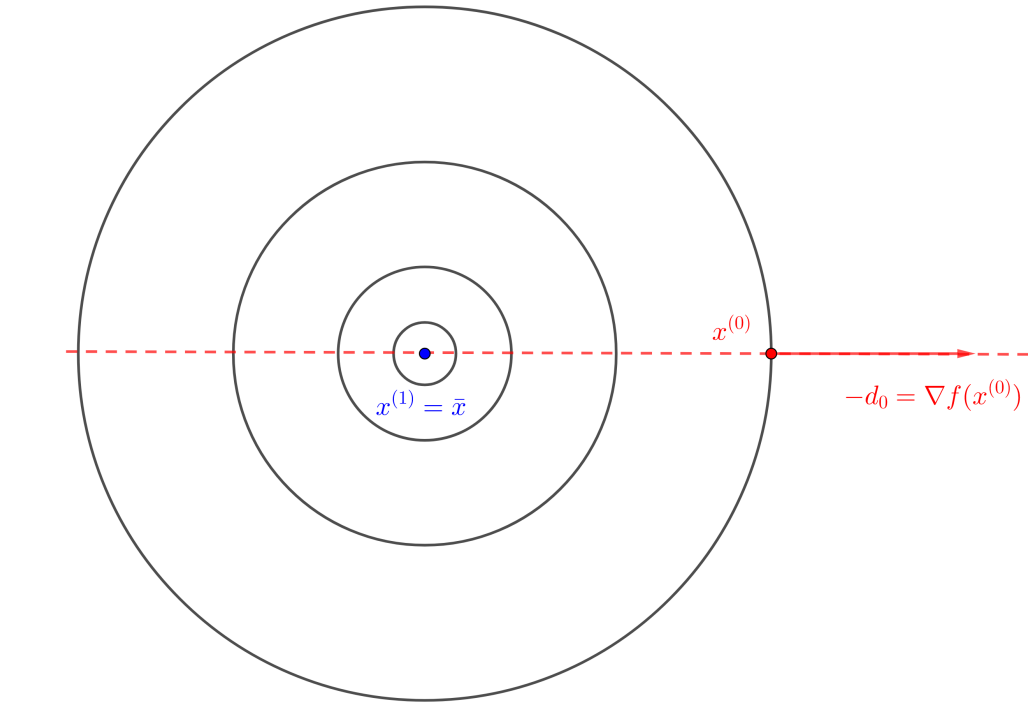
On déduit donc de (4.2)

$$\left\|x^{(k)} - \overline{x}\right\| \leq \left(\frac{2(f(x^{(0)}) - \overline{f})}{\lambda_n}\right)^{\frac{1}{2}}\left(\frac{c(A)-1}{c(A)+1}\right)^k \tag{4.3}$$

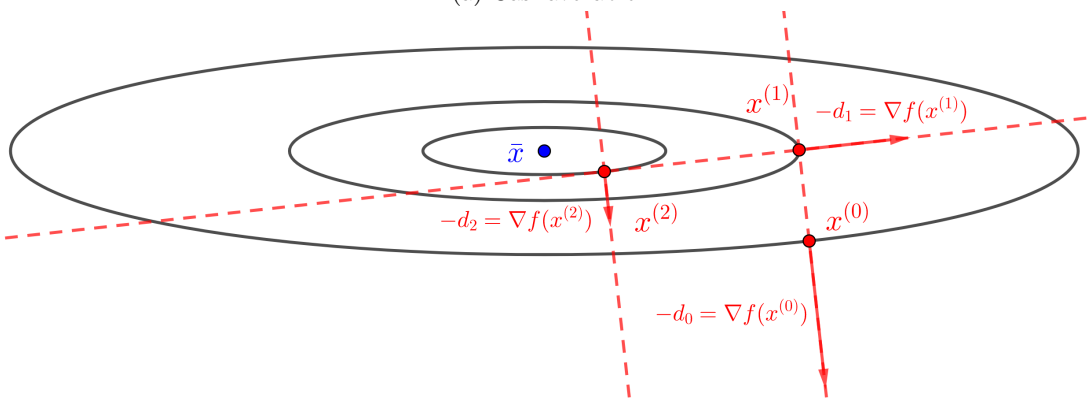
□

Remarque 4.4 On observe les phénomènes suivants, qui sont montrés sur la figure 4.2.

- On peut montrer que les directions successives dans lesquelles on se déplace sont orthogonales : $\langle d_k, d_{k+1} \rangle = 0$.
- On observe ainsi que plus le conditionnement est proche de 1, plus la convergence est rapide. Le cas optimal est donné par les homothéties, dont le conditionnement est 1, et pour lesquelles, en vertu de (4.3), le minimum est obtenu dès la première étape. On est dans le cas où les valeurs propres sont identiques. Dans le cas $n = 2$, les courbes de niveau de f sont des cercles (figure 4.2a).
- Le cadre le moins favorable est celui où les valeurs propres extrêmales sont éloignées. Les courbes de niveau sont alors des ellipses presque plates, et la convergence est beaucoup plus lente (figure 4.2b).



(a) Cas favorable



(b) Cas défavorable

Figure 4.2 – Premières itérations de l'algorithme du gradient à pas optimal

5 Lemme de Morse

Leçons 158, 171, 214, 215

Ref : [Rou03] Exo 114

On commence par donner une forme analytique de la réduction des formes quadratiques.

Lemme 5.1 (Réduction des formes quadratiques) Soit $A \in S_n(\mathbb{R})$ inversible. Alors il existe un voisinage V de A dans $GL_n(\mathbb{R})$ et une application $\rho : V \longrightarrow GL_n(\mathbb{R})$ de classe C^1 telle que pour tout $M \in V$, on a

$$M = {}^t\rho(M)A\rho(M).$$

Remarque 5.2 En d'autres terme, M se ramène par changement de base C^1 à A. En particulier, toute matrice assez proche de A a la même signature que A.

Démonstration. L'application $\gamma : M \longmapsto {}^tMAM$ est polynomiale, donc de classe C^1 sur $\mathcal{M}_n(\mathbb{R})$. Calculons sa différentielle en l'identité. On a pour $H \in \mathcal{M}_n(\mathbb{R})$

$$\gamma(I_n + H) - \gamma(I_n) = {}^tHA + AH + \underbrace{{}^tHAH}_{O(\|H\|^2)},$$

et donc comme A est symétrique

$$d\gamma_{I_n}(H) = {}^t(AH) + AH.$$

Le noyau de cette forme linéaire est formé des matrices $M \in \mathcal{M}_n(\mathbb{R})$ telles que AM est antisymétrique. Elle est de plus surjective, car si $H = \frac{1}{2}A^{-1}M$, on a $d\gamma_{I_n}(H) = M$.

On considère maintenant le sous-espace F des matrices telles que AM soit symétrique. Comme $\mathcal{M}_n(\mathbb{R})$ est somme directe de $A_n(\mathbb{R})$ et $S_n(\mathbb{R})$, F est un supplémentaire de $\ker(d\gamma_{I_n})$. De plus, $I_n \in F$. On note $\psi = \gamma_{|F}$, de sorte que la différentielle $d\psi_{I_n}$ est bijective. D'après le théorème d'inversion locale, il existe un voisinage U de l'identité dans F tel que ψ soit un C^1-difféomorphisme de U sur $V = \psi(U)$. Quitte à restreindre U et V, on suppose que U est inclus dans l'ouvert $GL_n(\mathbb{R})$ de $\mathcal{M}_n(\mathbb{R})$. Ainsi, V est un voisinage ouvert de $\psi(I_n) = A = \gamma(I_n)$, et pour toute matrice M de V, on a

$$M = {}^t\rho(M)A\rho(M),$$

où $\rho = \psi^{-1}$ est de classe C^1. □

On se donne maintenant un ouvert U de $\mathbb{R}^n$ contenant l'origine, et une application $f : U \longrightarrow \mathbb{R}$ de classe C^3. On suppose que 0 est un point critique quadratique non dégénéré de f, c'est-à-dire que df_0 est la forme linéaire nulle et d^2f_0 est une forme quadratique non dégénérée sur $\mathbb{R}^n$, dont on note $(p, n-p)$ la signature.

Théorème 5.3 (Lemme de Morse) Il existe un C^1-difféomorphisme entre deux voisinages de l'origine dans $\mathbb{R}^n$ tels que $\varphi(0) = 0$ si et seulement si

$$f(x) - f(0) = \varphi_1(x)^2 + \cdots + \varphi_p(x)^2 - \varphi_{p+1}(x)^2 - \cdots - \varphi_n(x)^2.$$

Démonstration. On écrit la formule de Taylor avec reste intégral à l'ordre 2 en 0 pour f :

$$f(x) - f(0) = \int_0^1 (1-t)\, d^2f_{tx}(x,x)\ dt. \tag{5.1}$$

On note alors $\mathcal{H}f(tx)$ la matrice hessienne de f en tx, et on définit la matrice symétrique

$$Q(x) := \int_0^1 (1-t)\mathcal{H}f(tx)\ dt,$$

de sorte que (5.1) se réécrit

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

Comme f est de classe C^3, Q est de classe C^1 sur U. Comme $Q(0) = \frac{1}{2}\mathcal{H}f(0)$ est symétrique et inversible (puisque d^2f_0 est non dégénérée), on peut appliquer le lemme de réduction des formes quadratiques : il existe un voisinage V de $Q(0)$ et un changement de variable $\rho : V \longrightarrow \rho(V)$ tels que, pour $M \in V$, on a

$$M = {}^t\rho(M)Q(0)\rho(M).$$

Or Q est de classe C^1, donc au voisinage de 0, $Q(x) \in V$. On peut donc définir l'application $P = \rho \circ Q$ de classe C^1 au voisinage de 0 dans $\mathbb{R}^n$, à valeurs dans $GL_n(\mathbb{R})$, de manière à avoir

$$Q(x) = {}^tP(x)Q(0)P(x).$$

Ainsi, en posant $y = P(x)x$, on a sur ce voisinage de 0

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

Or $Q(0)$ est de signature $(p, n-p)$, donc il existe un changement de variable linéaire A tel que

$${}^tAQ(0)A = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & \ddots & \\ & & & & & -1 \end{pmatrix}.$$

On pose alors $\varphi(x) = A^{-1}y = A^{-1}P(x)x$, qui est bien une fonction de classe C^1 telle que $\varphi(0) = 0$. On a alors

$$\begin{aligned} f(x) - f(0) &= {}^tyQ(0)y \\ &= {}^t\varphi(x) \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & \ddots & \\ & & & & & -1 \end{pmatrix} \varphi(x) \end{aligned}$$

$$f(x) - f(0) = \varphi_1(x)^2 + \cdots + \varphi_p(x)^2 - \varphi_{p+1}(x)^2 - \cdots - \varphi_n(x)^2.$$

De plus, on a

$$\varphi(h) = A^{-1}P(h)h = A^{-1}P(0)h + o(\|h\|),$$

donc la différentielle de φ en 0 est $A^{-1}P(0)$ qui est inversible. D'après le théorème d'inversion locale, φ est donc un C^1-difféomorphisme entre deux voisinages de 0 dans $\mathbb{R}^n$. □

Comme toujours, il est important d'avoir en tête des applications de ce développement. Dans [Rou03], quelques exercices donnent des interprétations du lemme de Morse en terme de position relative d'une surface et de ses plans tangents (l'exercice 111 par exemple). Je présente ici un autre résultat, démontré avec la preuve du lemme de Morse dans [BB18]. On considère toujours la même fonction f, dont la hessienne en 0 est supposée définie positive (donc de signature $(n, 0)$). On considère le système différentiel

$$\begin{cases} \dot{X} = Y \\ \dot{Y} = -\nabla f(X) \end{cases}$$

où X est à valeurs dans U et Y dans $\mathbb{R}^n$. On peut alors montrer en utilisant le changement de variable donné par le lemme de Morse pour montrer que 0 est un équilibre stable non asymptotiquement stable de ce système.

6 Méthode QR pour les valeurs propres

Leçons 157, 162, 233

Ref : [Cia90] 6.3

Ce développement consiste à démontrer une méthode de calcul des valeurs propres d'une matrice. Elle englobe des cas plus généraux que la méthode de Jacobi par exemple, qui ne fonctionne que pour des matrices symétriques, et elle est (dans ces cas-là) au moins aussi efficace que celle-ci.

Théorème 6.1 Soit $A \in GL_n(\mathbb{C})$ une matrice dont les valeurs propres sont échelonnées en degré ; on les note $\lambda_1, .., \lambda_n$ et on peut donc supposer

$$|\lambda_1| > .. > |\lambda_n| > 0.$$

On se donne aussi la matrice $P \in GL_n(\mathbb{C})$ telle que $A = PDP^{-1}$, avec D diagonale avec coefficients λ_i (rangés dans l'ordre). On suppose que P^{-1} admet une décomposition LU. Alors la suite de matrices $(A_k)_{k\geq 1}$ définie par

$$\begin{cases} A_1 = A \\ A_{k+1} = R_k Q_k \text{ en notant } A_k = Q_k R_k \text{ la décomposition QR de } A_k, \ \forall k \geq 1 \end{cases}$$

converge vers une matrice triangulaire supérieure dont les coefficients diagonaux sont les valeurs propres $\lambda_1, .., \lambda_n$ de A.

Remarque. On rappelle que l'on dit que $M \in GL_n(\mathbb{C})$ admet une décomposition LU s'il existe L triangulaire inférieure avec des 1 sur la diagonale et U triangulaire supérieure telles que $M = LU$. C'est vrai si les mineurs principaux de M sont non nuls.

Démonstration.

Étape 1. Deux identités matricielles[6]

On note, pour tout entier $k \geq 1$,

$$\begin{cases} Q^{(k)} := Q_1..Q_k \\ R^{(k)} := R_k..R_1 \end{cases}$$

On a alors une première identité qui donne la décomposition QR de A^k

$$A^k = Q^{(k)} R^{(k)}. \tag{6.1}$$

En effet, on a

$$A^k = (Q_1R_1)^k = Q_1(R_1Q_1)^{k-1}R_1 = Q_1A_2^{k-1}R_1 = Q_1Q_2(R_2Q_2)^{k-2}R_2R_1 = .. = Q_1..Q_kR_k..R_1,$$

d'où le résultat. On montre également par récurrence le résultat suivant :

$$A_{k+1} = Q^{(k)*} A Q^{(k)}. \tag{6.2}$$

Pour $k = 1$, on a bien $A_2 = R_1Q_1 = Q_1^*Q_1R_1Q_1 = Q_1^*AQ_1$, et si k est un entier plus grand que 1, on a bien

$$\begin{array}{rcll} A_{k+2} & = & R_{k+1}Q_{k+1} & \text{par définition de la suite } (A_k)_{k\geq 1} \\ & = & Q_{k+1}^*Q_{k+1}R_{k+1}Q_{k+1} & \text{car } Q_{k+1} \text{ est unitaire} \\ & = & Q_{k+1}^*A_{k+1}Q_{k+1} & \\ & = & Q_{k+1}^*Q^{(k)*}AQ^{(k)}Q_{k+1} & \text{par hypothèse de récurrence} \\ A_{k+2} & = & Q^{(k+1)*}AQ^{(k+1)} & \end{array}$$

Étape 2. Une autre expression de la décomposition QR de A^k.

On cherche ici à donner une autre expression des matrices $Q^{(k)}$ puisque l'on voit via (6.2) qu'elles vont diriger le comportement asymptotique de la suite $(A_k)_{k\geq 1}$. Pour cela, on utilise l'unicité de la décomposition QR : trouver une "autre" décomposition de A^k que celle donnée par (6.1) nous donnera par unicité une autre formule pour $Q^{(k)}$. On note alors $P = QR$ la décomposition QR de P (existe car

6. Si l'on a peur de manquer de temps, on peut simplement évoquer que la première se montre par un calcul direct et la seconde par récurrence.

P est inversible) et $P^{-1} = LU$ la décomposition LU de son inverse, dont l'existence fait l'objet d'une hypothèse du théorème. Comme A est inversible, D l'est aussi et son inverse est la matrice D^{-1} diagonale à coefficients λ_i^{-1}. On a alors

$$A^k = PD^kP^{-1} = QRD^kLU = QR(D^kLD^{-k})D^kU.$$

Mais on a pour tout $(i,j) \in [\![1,n]\!]^2$

$$(D^kLD^{-k})_{ij} = \begin{cases} 0 & \text{si } i < j \\ 1 & \text{si } i = j \\ \left(\dfrac{\lambda_i}{\lambda_j}\right)^k L_{ij} & \text{si } i > j \end{cases}$$

Mais comme $|\lambda_i| < |\lambda_j|$ si $i > j$, cette matrice tend vers l'identité. Ainsi, par continuité du produit matriciel, $RD^kLD^{-k}R^{-1}$ converge aussi vers l'indentité. Comme cette matrice est inversible, elle admet une décomposition QR, que l'on note O_kT_k, et comme la décomposition QR est un homéomorphisme [7], O_k et T_k convergent vers l'identité. De plus, on rappelle que l'on a maintenant

$$A^k = QO_kT_kRD^kU.$$

Le facteur QO_k est unitaire puisque Q et O_k le sont. Le second facteur T_kRD^kU est bien triangulaire supérieur, mais ses coefficients diagonaux peuvent être non réels strictement positifs [8]. Cependant, si l'on note Θ_k la matrice diagonale dont les coefficients diagonaux sont les $\mathrm{e}^{-\mathrm{i}\theta_j}$, où les θ_j sont les arguments des coefficients diagonaux de T_kRD^kU, on en déduit que $(QO_k\Theta_k^*)(\Theta_kT_kRD^kU)$ est la décomposition polaire de A^k. Donc, par unicité, on a

$$Q^{(k)} = QO_k\Theta_k.$$

Étape 3. Convergence de la suite $(A_k)_{k\geq 1}$.

On a maintenant, en utilisant le résultat de l'étape précédente avec (6.2) :

$$A_{k+1} = \Theta_k^*O_k^*Q^*AQO_k\Theta_k.$$

Or on rappelle que $A = QRDR^{-1}Q^{-1}$, donc on en déduit

$$A_{k+1} = \Theta_k^*O_k^*RDR^{-1}O_k\Theta_k.$$

Or RDR^{-1} est triangulaire supérieur avec coefficients diagonaux égaux à λ_i [9]. Ainsi, par continuité de la mutliplication matricielle et comme les O_k sont unitaires et convergent vers l'identité, la suite définie par $D^{(k)} := O_k^*RDR^{-1}O_k$ tend vers cette même matrice. Or $A_{k+1} = \Theta_k^*D^{(k)}\Theta_k$, et comme Θ_k est diagonale à coefficients diagonaux de module 1, A_{k+1} a bien les mêmes coefficients diagonaux que $D^{(k)}$. En passant à la limite, on voit que A_k tend bien vers une matrice triangulaire supérieure de la forme voulue. □

7. La démonstration similaire à celle du fait que la décomposition polaire est homéomorphisme, présentée dans le développement I.6.

8. On rappelle que la décomposition QR donne l'unicité en ajoutant la condition de diagonale strictement positive seulement pour R. Si ses coefficients diagonaux peuvent être quelconques, il existe une infinité de décompositions possibles.

9. Les λ_i sont toujours triés par module décroissant. Cela se voit en faisant le calcul explicite des coefficients diagonaux de RDR^{-1}.

7 Théorème de d'Alembert-Gauß

Leçons 144, 204(, 214)

Ref : [GT96]

Ce développement consiste à démontrer le théorème fondamental de l'algèbre.

Théorème 7.1 (D'Alembert-Gauß) Le corps $\mathbb{C}$ est algébriquement clos : tout polynôme non constant de $\mathbb{C}[X]$ admet une racine.

Démonstration. Pour obtenir ce résultat, on va montrer que tout polynôme non constant de $\mathbb{C}[X]$ est surjectif, et donc que 0 admet en particulier un antécédent. Cette démonstration utilise des résultats de connexité. On se donne $P \in \mathbb{C}[X]$ non constant, et on appelle S l'ensemble des racines de P'. Alors S est fini (puisque tout polynôme possède un nombre fini de racines) et donc $P(S)$ aussi. On définit également

$$\begin{cases} \Omega = P(\mathbb{C})\backslash P(S) \\ \mathbb{L} = \mathbb{C}\backslash P(S) \end{cases}$$

On va montrer que Ω et $\mathbb{L}$ sont les mêmes ensembles. On en déduira alors que $P(\mathbb{C}) = \mathbb{C}$, et donc que P est surjectif.

Étape 1. Connexité de $\mathbb{L}$.

On va montrer que $\mathbb{L}$ est connexe en montrant qu'il est connexe par arcs. On se donne a et b dans $\mathbb{L}$. On définit pour un point z de $\mathbb{C}$ l'ensemble $\mathcal{D}_z$ des droites du plan complexe (assimilé à $\mathbb{R}^2$) passant par z. En particulier, comme $\mathcal{D}_z$ est en bijection avec $[0, \pi)$, c'est un ensemble infini, et comme $P(S)$ est un ensemble fini, il existe pour tout $z \in \mathbb{L}$ une droite de $\mathcal{D}_z$ ne passant par aucun point de S. On se donne donc $\Delta_a \in \mathcal{D}_a$ et $\Delta_b \in \mathcal{D}_b$ deux droites passant respectivement par a et b et ne passant pas par $P(S)$ (voir figure 7.1). On se donne un réel $R > 0$ tel que la boule centrée en l'origine et de rayon R, notée $B(0, R)$, contienne $P(S) \cup \{a, b\}$ (R existe car cet ensemble est fini). Comme Δ_a et Δ_b sont des droites passant par l'intérieur de $B(0, R)$, elles coupent toutes les deux le disque $\partial B(0, R)$ en deux points. On en choisit un pour chacune, que l'on note respectivement a' et b'. Alors le chemin $[a, a'] \cup \mathcal{C} \cup [b', b]$, où $[z_1, z_2]$ désigne le segment reliant z_1 à z_2 dans $\mathbb{C}$, et $\mathcal{C}$ l'un des deux arcs de cercles reliant a' à b' sur $\partial B(0, R)$ forme, comme on le voit sur la figure 7.1, un chemin continu de a à b ne passant par aucun point de $P(S)$, c'est à dire inclus dans $\mathbb{L}$. Donc $\mathbb{L}$ est connexe.

Étape 2. Ω est ouvert dans $\mathbb{L}$.

On se donne $x \in \Omega$. Alors en partculier, x est dans l'image de P, et on peut donc se donner $z \in \mathbb{C}$ tel que $P(z) = x$. Comme x n'est pas dans $P(S)$, $P'(z)$ est non nul. On en déduit que c'est un élément inversible de $\mathbb{C}$. On applique à P le théorème d'inversion locale en z : $\mathbb{C}$ est un Banach, et P une application polynomiale donc de classe C^1 de $\mathbb{C}$ vers $\mathbb{C}$, et $P'(z)$ est inversible dans $\mathbb{C}$. On en déduit qu'il existe un ouvert U_z autour de z dans $\mathbb{C}$ et un voisinage U_x autour de $x = P(z)$ dans $\mathbb{C}$ tel que P soit un C^1-difféomorphisme de U_z vers U_x. En particulier, U_x est inclus dans $P(\mathbb{C})$. On en déduit que $U_x \cap \mathbb{L}$ est inclus dans $P(\mathbb{C}) \cap \mathbb{L} = \Omega$. Donc Ω est ouvert dans $\mathbb{L}$.

Étape 3. Ω est fermé dans $\mathbb{L}$.

On se donne une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de Ω qui converge vers un élément $x \in \mathbb{L}$. On va montrer que $x \in \Omega$. Comme pour $n \in \mathbb{N}$, x_n est dans Ω, on peut se donner un élément $z_n \in \mathbb{C}$ tel que $P(z_n) = x_n$. Or les fonctions polynomiales sont propres :

$$\lim_{|z|\to+\infty} |P(z)| = +\infty.$$

On en déduit, comme la suite $(P(z_n))_{n\in\mathbb{N}} = (x_n)_{n\in\mathbb{N}}$ est bornée car convergente dans $\mathbb{L}$, que la suite $(z_n)_{n\in\mathbb{N}}$ l'est aussi. Donc, par théorème de Bolzano-Weierstraß, il existe une extractrice φ et un complexe z tels que

$$z_{\varphi(n)} \underset{n\to+\infty}{\longrightarrow} z.$$

Par continuité de la fonction polynomiale P, on en déduit que

$$P(z_{\varphi(n)}) \underset{n\to+\infty}{\longrightarrow} P(z).$$

Or cette suite est aussi la suite $(x_{\varphi(n)})_{n\in\mathbb{N}}$, qui converge vers x, donc par unicité de la limite, on a $x = P(z)$. On en déduit que x est dans Ω. Donc Ω est fermé dans $\mathbb{L}$.

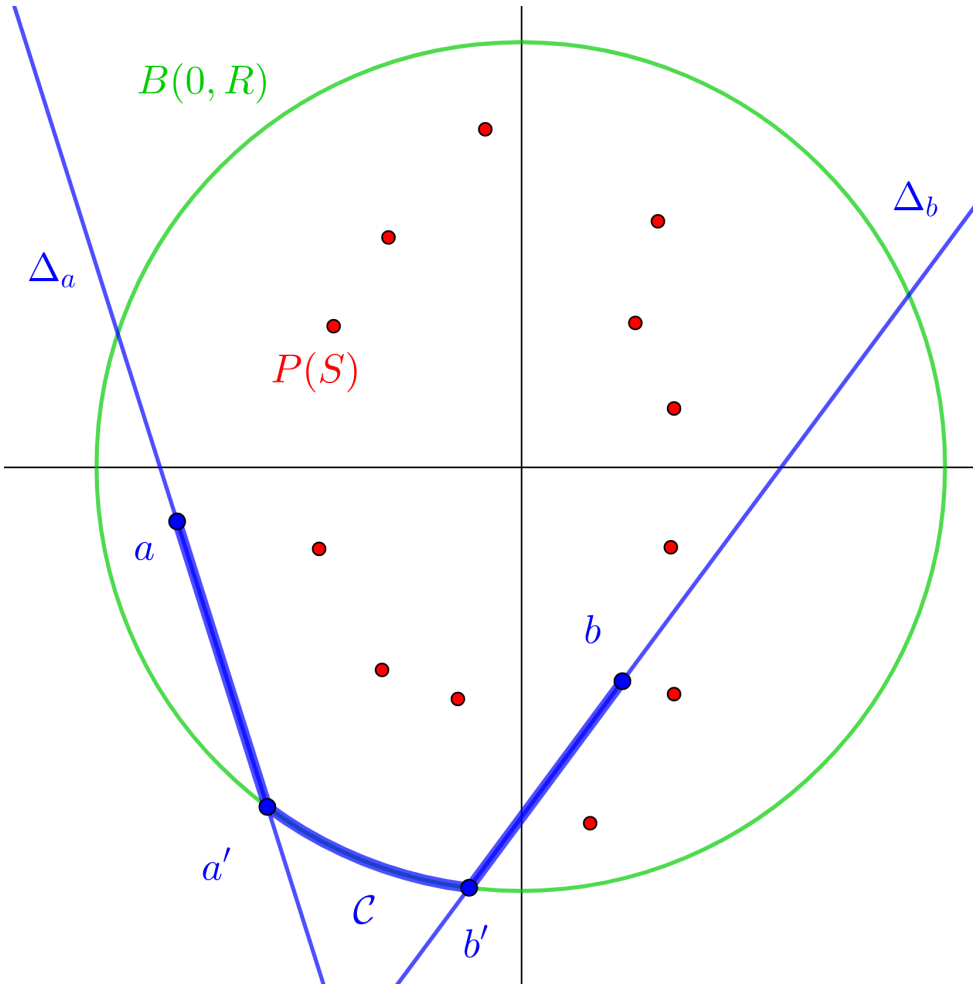


Figure 7.1 – Construction d'un chemin entre deux points de $\mathbb{L}$

Étape 4. Conclusion.

$\mathbb{L}$ étant connexe, et Ω ouvert et fermé dans $\mathbb{L}$, on a $\Omega = \emptyset$ ou $\Omega = \mathbb{L}$. Or comme P est non constant, $P(\mathbb{C})$ est infini, et donc comme $P(S)$ est fini, Ω n'est pas vide. Donc $\Omega = \mathbb{L}$, ce qui permet de conclure.

□

8 Théorème de Kalman

Leçons 221(, 151)

Ref : [Tré05] II.1 Th 2.2

Ce développement s'intéresse à la contrôlabilité d'une équation différentielle linéaire. On considère l'équation

$$x'(t) = Ax(t) + Bu(t) \tag{8.1}$$

où

- $x \in C^0([0,T], \mathbb{R}^n)$ est l'inconnue
- $A \in \mathcal{M}_n(\mathbb{R})$ et $B \in \mathcal{M}_{n,m}(\mathbb{R})$ sont des données fixées
- $u \in C^0([0,T], \mathbb{R}^m)$ est une donnée variable appelée *contrôle* du système.

Le théorème de Cauchy-Lipschitz affirme que le problème

$$\begin{cases} x'(t) = Ax(t) + Bu(t) \\ x(0) = x_0 \end{cases} \tag{8.2}$$

associé à toute donnée initiale $x_0 \in \mathbb{R}^n$, admet une unique solution x.

Définition 8.1 On dit que l'équation (8.1) est *contrôlable en temps* T si pour tout couple (x_0, x_f) d'éléments de $\mathbb{R}^n$, il existe un contrôle $u \in C^0([0,T], \mathbb{R}^m)$ tel que la solution du problème (8.2) associé vérifie $x(T) = x_f$.

Théorème 8.2 (Kalman) Le système (8.1) est contrôlable en temps T si et seulement si la *matrice de Kalman* K qui lui est associée, définie par

$$K = \left(\begin{array}{c|c|c|c} B & AB & \cdots & A^{n-1}B \end{array} \right) \in \mathcal{M}_{n,mn}(\mathbb{R}),$$

est de rang n.

Remarque. On remarque que la CNS ne dépend pas du temps T, donc le système est soit contrôlable en tout temps, soit jamais contrôlable.

Démonstration. La démonstration est basée sur le lemme suivant, qui établit une caractérisation du fait que la matrice de Kalman est de rang maximal.

Lemme 8.3 K est de rang n si et seulement si l'application

$$\Phi : \left| \begin{array}{ccc} C^0([0,T], \mathbb{R}^m) & \longrightarrow & \mathbb{R}^n \\ u & \longmapsto & \displaystyle\int_0^T \mathrm{e}^{(T-t)A} Bu(t)\, dt \end{array} \right.$$

est surjective.

Étape 1. Sens réciproque du lemme par contraposée.

On suppose que K est de rang strictement inférieur à n, c'est-à-dire que K n'est pas surjective, et donc que l'orthogonal de son image contient un élément $v \in \mathbb{R}^n$ non nul. On a donc

$$\forall y \in \mathbb{R}^{mn}, \quad \langle v, Ky \rangle = {}^t vKy = 0.$$

Ainsi, l'application ${}^t vK$, qui est une forme linéaire sur $\mathbb{R}^{mn}$, est nulle. En développant le produit matriciel, on a donc

$$K = \left(\begin{array}{c|c|c|c} {}^t vB & {}^t vAB & \cdots & {}^t vA^{n-1}B \end{array} \right) = 0.$$

On en déduit que pour tout $k \in [\![0, n-1]\!]$, ${}^t vA^k B$ est la matrice nulle. Or le théorème de Cayley-Hamilton fournit une écriture de A^n comme combinaison linéaire des A^k, pour $k \in [\![0, n-1]\!]$. Donc on a également ${}^t vA^n B = 0$, et par récurrence c'est donc vrai pour tout $k \in \mathbb{N}$. Ainsi, on a pour tout réel $t \geq 0$ et pour tout $N \in \mathbb{N}$

$$\sum_{k=0}^{N} {}^t v \frac{t^k A^k}{k!} B = 0.$$

Ainsi, en factorisant par ${}^tv$, et en passant à la limite quand N tend vers l'infini, par continuité du produit matriciel, on obtient

$$ {}^tv\,\mathrm{e}^{tA}\,B = 0. $$

Ainsi, en se donnant un contrôle $u \in C^0([0,T],\mathbb{R}^m)$ et un réel $t \in [0,T]$, on a ${}^tv\,\mathrm{e}^{(T-t)A}\,Bu(t) = 0$, ce qui s'intègre en

$$ \langle v, \Phi(u)\rangle = {}^t v\Phi(u) = 0. $$

On en déduit que v est un élément non nul de l'orthogonal de l'image de Φ, et donc que Φ n'est pas surjective.

Étape 2. Sens direct du lemme par contraposée.

On suppose cette fois que Φ n'est pas surjective, et donc on se donne un élément $w \in \mathbb{R}^n$ non nul dans l'orthogonal de son image :

$$ \forall u \in C^0([0,T],\mathbb{R}^m), \quad {}^tw\Phi(u) = \int_0^T {}^tw\,\mathrm{e}^{(T-t)A}\,Bu(t)\;dt = 0. $$

On choisit

$$ u : \left| \begin{array}{ccc} [0,T] & \longrightarrow & \mathbb{R}^m \\ t & \longmapsto & {}^t\big({}^tw\,\mathrm{e}^{(T-t)A}\,B\big) \end{array} \right. , $$

qui est un élément de $C^0([0,T],\mathbb{R}^m)$, et on obtient alors

$$ 0 = \int_0^T {}^tw\,\mathrm{e}^{(T-t)A}\,Bu(t)\;dt = \int_0^T \|u(t)\|^2\,dt. $$

Ainsi, on en déduit

$$ \forall t \in [0,T], \quad {}^tw\,\mathrm{e}^{(T-t)A}\,B = 0. $$

En particulier, en spécialisant en $t = T$, on obtient ${}^twB = 0$. De plus, les deux membres de cette expression sont en fait de classe C^∞. En la dérivant k fois, pour $k \in [\![0, n-1]\!]$, on obtient ${}^twA^kB = 0$. On en déduit donc que la matrice wK est nulle. Ainsi, on a

$$ \forall y \in \mathbb{R}^{mn}, \quad \langle w, Ky\rangle = {}^t wKy = 0, $$

et donc w est un vecteur non nul de l'orthogonal de l'image de K. Donc K n'est pas surjective, et donc elle est de rang strictement inférieur à n.

Étape 3. Équivalence entre contrôlabilité et surjectivité de Φ.

Il reste à montrer que le système (8.1) est contrôlable si et seulement si l'application Φ est surjective. C'est une application directe de la formule de Duhamel : ici la résolvante s'écrit $R(t,s) = \mathrm{e}^{(t-s)A}$, et donc si x vérifie (8.2), on a

$$ x(T) = \mathrm{e}^{TA}\,x_0 + \int_0^T \mathrm{e}^{(T-t)A}\,Bu(t)\;dt = \mathrm{e}^{TA}\,x_0 + \Phi(u). $$

Donc le système est contrôlable en temps T si et seulement si $x_f - \mathrm{e}^{TA}\,x_0$ admet un antécédent par Φ pour tout $(x_0, x_f) \in (\mathbb{R}^n)^2$, ce qui est équivalent à la surjectivité de Φ. □

Remarque.

- Plusieurs contrôles peuvent bien sûr permettre de passer de x_0 à x_f en temps T, puisque le noyau de Φ est de dimension infinie.
- On peut demander que les contrôles soient mieux que continus : il suffit de pouvoir prendre le u définit à l'étape 2 comme contrôle, donc comme celui-ci est de classe C^∞, la preuve fonctionne toujours en demandant que les contrôles soient de classe C^∞.

Exemple. On considère les deux systèmes d'équations suivants

$$ \left\{ \begin{array}{l} x' = x + u \\ y' = x \end{array} \right. \qquad\qquad \left\{ \begin{array}{l} x' = x + u \\ y' = y \end{array} \right. $$

On voit que le système de gauche (resp. droite) est sous la forme (8.1) avec $A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ (resp. $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$) et $B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Ainsi, dans le premier cas, la matrice de Kalman est $K = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de rang 2, donc

le système est contrôlable, alors que dans le second cas, elle est égale à $K = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ de rang 1, et donc le système n'est pas contrôlable. Ce résultat rejoint l'intuition, puisque l'on se dit que dans le premier cas, puisque y "dépend de x", on peut contrôler x et y en faisant varier u, alors que dans le second, y est indépendant de x et donc le contrôle de u n'intervient pas sur y.

Références

[AM04] Éric Amar et Étienne Matheron. *Analyse complexe*. Cassini, 2004.

[BB18] Julien Bernis et Laurent Bernis. *Analyse pour l'agrégation de mathématiques*. 2018.

[BG10] Sylvie Benzoni-Gavage. *Calcul différentiel et équations différentielles*. Dunod, 2010.

[BMP05] Vincent Beck, Jérôme Malick et Gabriel Peyré. *Objectif Agrégation*. 2005.

[BP15] Marc Briane et Gilles Pagès. *Théorie de l'intégration*. Vuibert, 2015.

[Bré05] Haïm Brézis. *Analyse fonctionnelle*. Dunod, 2005.

[CG13] Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométrie, Tome premier*. Calvage & Mounet, 2013.

[Cia90] Philippe G. Ciarlet. *Introduction à l'analyse numérique matricielle et à l'optimisation*. 1990.

[EA11] Mohammed El Amrani. *Suites et séries numériques, suites et séries de fonctions*. Ellipses, 2011.

[Eid09] Jean-Denis Eiden. *Géométrie analytique classique*. Calvage & Mounet, 2009.

[Eva10] Lawrence Evans. *Partial Differential Equations*. American Mathematical Society, 2è édition, 2010.

[FGN09a] Serge Francinou, Hervé Gianella et Serge Nicolas. *Oraux X-ENS, Analyse I*. 2009.

[FGN09b] Serge Francinou, Hervé Gianella et Serge Nicolas. *Oraux X-ENS, Algèbre II*. 2009.

[FGN09c] Serge Francinou, Hervé Gianella et Serge Nicolas. *Oraux X-ENS, Algèbre III*. 2009.

[Gou08] Xavier Gourdon. *Analyse*. 2008.

[Gou09] Xavier Gourdon. *Algèbre*. Ellipses, 2è édition, 2009.

[Goz09] Ivan Gozard. *Théorie de Galois*. Ellipses, 2009.

[GT96] Stéphane Gonnord et Nicolas Tosel. *Topologie et Analyse fonctionnelle*. 1996.

[HU09] Jean-Baptiste Hiriart-Urruty. *Optimisation et analyse convexe*. EDP Sciences, 2009.

[Lav18] Florian Lavigne. *70 développements possibles pour l'agrégation de mathématiques*. 2018.

[Mer04] Dany-Jack Mercier. *Cours de géométrie*. 2004.

[Ouv19] Jean-Yves Ouvrard. *Probabilités, Tome 2*. 2019.

[Per96] Daniel Perrin. *Cours d'algèbre*. 1996.

[Rou03] François Rouvière. *Petit guide de calcul différentiel*. Cassini, 2è édition, 2003.

[Tré05] Emmanuel Trélat. *Contrôle optimal : théorie et applications*. Vuibert, 2005.

[Ulm12] Felix Ulmer. *Théorie des groupes*. Ellipses, 2012.

[ZQ13] Claude Zuily et Hervé Queffélec. *Analyse pour l'agrégation*. Dunod, 4è édition, 2013.