Résultats développés de Mathématiques

Simon Masson

2015-2016

Introduction

Ces développements sont (pour la plupart) classiques. Tous ont une référence bibliograhique sauf le premier sur les pavages. Il y a très probablement des erreurs. Merci de me les signaler à l'adresse suivante : `simon.masson@yahoo.fr`.

Table des matières

Références

[1] Michel Alessandri. Thèmes de géométrie, groupes en situation géométrique.
[2] Haïm Brezis. Analyse fonctionnelle.
[3] Xavier Gourdon. Les maths en tête, algèbre.
[4] Xavier Gourdon. Les maths en tête, analyse.
[5] Claude Zuily Hervé Queffélec. Analyse pour l'agrégation.
[6] Jean-Yves Mérindol. Nombres et algèbre.
[7] Daniel Perrin. Cours d'algèbre.
[8] Jérôme Germoni Philippe Caldéro. Histoires hédonistes de groupes et de géométries.
[9] Gérard Rauch. Les groupes finis et leurs représentations.
[10] François Rouvière. Petit guide de calcul différentiel à l'usage de la licence et de l'agrégation.
[11] Hervé Gianella Serge Francinou. Exercices de mathématiques pour l'agrégation, algèbre 1.
[12] Serge Nicolas Serge Francinou, Hervé Gianella. Oraux x-ens, algèbre 1.
[13] Serge Nicolas Serge Francinou, Hervé Gianella. Oraux x-ens, algèbre 2.
[14] Serge Nicolas Serge Francinou, Hervé Gianella. Oraux x-ens, algèbre 3.
[15] Serge Nicolas Serge Francinou, Hervé Gianella. Oraux x-ens, analyse 2.
[16] Aviva Szpirglas. Mathématiques l3 algèbre.
[17] Felix Ulmer. Théorie des groupes.
[18] Gavriel Peyré Vincent Beck, Jérôme Malick. Objectif agrégation, 2ème édition.
[19] Maxime Zavidovique. Un max de math.

1 Pavages du plan affine euclidien

Soit $\mathcal{E}$ un plan affine euclidien, $G < \mathrm{Is}^+(\mathcal{E})$ un sous-groupe des déplacements de $\mathcal{E}$, qui de plus est paveur.

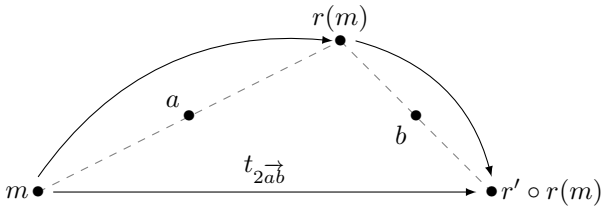
1.1 Le groupe des translation est un réseau

On va montrer que si $H = \{\vec{u} \in E, t_{\vec{u}} \in G\}$, alors il existe $(\vec{u}_0, \vec{v}_0)$ base de E telle que $H = \mathbb{Z}\vec{u}_0 + \mathbb{Z}\vec{v}_0$.

Soit φ la restriciton à G du morphisme de groupe défini en proposition **??** par

$$\varphi : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathcal{O}^+(2,\mathbb{R}) \\ g & \longmapsto & \vec{g} \end{array} \right.$$

Il est bien à valeurs dans $\mathcal{O}^+(2,\mathbb{R})$ car $G < \mathrm{Is}^+(\mathcal{E})$. On a $\ker\varphi = T = \{\text{translations de } G\}$.

1. Montrons que $T \neq \{0\}$
   Supposons **par l'absurde** que φ est injective. Alors, $G \simeq \varphi(G) \subset \mathcal{O}^+(2,\mathbb{R})$ qui est abélien. Donc G est abélien. De plus, G ne contient que des rotations (il n'y a pas de translation).
   Deux rotations qui commutent ont même centre. En effet, si (r_1, Ω_1) et (r_2, Ω_2) deux rotations qui commutent, alors $r_1 r_2(\Omega_1) = r_2 r_1(\Omega_1) = r_2(\Omega_1)$. Donc $r_2(\Omega_1) = \Omega_1$. Donc $\Omega_1 = \Omega_2$.
   Donc les éléments de G sont des rotations de même centre.
   $\bigcup_{g\in G} g(P)$ est donc incluse dans un disque. **Absurde** car $\bigcup_{g\in G} g(P)$ doit paver tout le plan.
2. Montrons que T contient au moins deux translations linéairement indépendantes
   Supposons **par l'absurde** que $H \subset \mathbb{R}\vec{u}$, c'est-à-dire que les directions de T sont toutes parallèles. Comme $T = \ker\varphi$, $T \lhd G$ et si $g \in G$, $g \circ t_{\vec{u}} \circ g^{-1} = t_{\vec{g}(\vec{u})}$. Donc $\forall g \in G, \vec{g}(\vec{u}) = \pm\vec{u}$. Ainsi, si $g \in G\backslash T$, g est une symétrie autour d'un point. Or, si r et r' sont deux symétries autour de a et b (distincts), alors
   $$r' \circ r = t_{2\overrightarrow{ab}}$$
   En effet,
   $$\begin{aligned} r' \circ r(m) = r'(m + 2\overrightarrow{ma}) = m + 2\overrightarrow{ma} + 2\overrightarrow{r(m)b} &= m + 2\overrightarrow{ma} - \overrightarrow{ma} + \overrightarrow{ab} - \overrightarrow{br(m)} \\ &= m + \overrightarrow{ma} + \overrightarrow{ab} + \overrightarrow{r(m)b} \\ &= m + \overrightarrow{ar(m)} + \overrightarrow{ab} + \overrightarrow{r(m)b} \\ &= m + 2\overrightarrow{ab} \end{aligned}$$
   

   Tous les centres des éléments de $G\backslash T$ doivent être alignés sur une droite D parallèle à $\vec{u}$, donc $\bigcup_{g\in G} g(P)$ est contenu dans une bande d'axe D. **Absurde** car $\bigcup_{g\in G} g(P)$ doit paver tout le plan.
3. Montrons que H est un réseau
   On a déjà montré que T contient deux translations linéairement indépendantes.

On souhaite maintenant trouver $\vec{u}_0, \vec{v}_0$ tels que $t_{\vec{u}_0}, t_{\vec{v}_0} \in G$, et pour tout $t_{\vec{w}} \in G, \vec{w} \in \mathbb{Z}\vec{u}_0 + \mathbb{Z}\vec{v}_0$.
On définit

$$A := \inf\left\{\|\vec{w}\|, t_{\vec{w}} \in G, \vec{w} \neq \vec{0}\right\}$$

Soit $\vec{w}_n$ tel que $\|\vec{w}_n\| \longrightarrow A$. La suite $\vec{w}_n$ est dans un compact donc quitte à considérer une sous-suite extraite, on peut supposer que $\vec{w}_n \longrightarrow \vec{v}$. On pose ensuite

$$g_n := t_{\vec{w}_{n+1} - \vec{w}_n}$$

Pour $x \in \overset{\circ}{P}$, on a

$$g_n(x) = t_{\vec{w}_{n+1}-\vec{w}_n}(x) = x + \vec{w}_{n+1} - \vec{w}_n \longrightarrow x + \vec{0} = x$$

c'est-à-dire qu'il existe N tel que pour $n \geq N$, $g_n(\overset{\circ}{P}) \cap \overset{\circ}{P} \neq \varnothing$. Donc pour $n \geq N$, $g_n = \mathrm{id}$ (par définition d'un pavage).
Donc $\vec{w}_{n+1} = \vec{w}_n =: \vec{u}_0$.
$t_{\vec{u}_0} \in G$, et $\|\vec{u}_0\| = A$, avec $\vec{u}_0$ non-nul. Donc $A > 0$.
De même,

$$B := \inf\left\{\|\vec{w}\|, \vec{w} \in E - \mathbb{R}\vec{u}_0, t_{\vec{w}} \in G\right\}$$

est atteint en $\vec{v}_0$: $\|\vec{v}_0\| = B > 0$.

$$\langle t_{\vec{u}_0}, t_{\vec{v}_0}\rangle = t_{\mathbb{Z}\vec{u}_0 + \mathbb{Z}\vec{v}_0} \subset T$$

On veut montrer l'inclusion réciproque, c'est-à-dire que si $t_{\vec{w}} \in G$, alors $\vec{w} \in \mathbb{Z}\vec{u}_0 + \mathbb{Z}\vec{v}_0$.
On a déjà $\vec{w} = a\vec{u}_0 + b\vec{v}_0$ avec a, b réels.
Il existe $n, m \in \mathbb{Z}$ tels que $\vec{w}' := t_{n\vec{u}_0 + m\vec{v}_0}(\vec{w}) = \alpha\vec{u}_0 + \beta\vec{v}_0$, avec $0 \leq \alpha < 1$ et $0 \leq \beta < 1$.
On montre que $\vec{w}' \in \mathbb{Z}\vec{u}_0 + \mathbb{Z}\vec{v}_0$.

- Si $\alpha = 0$, alors $\vec{w}' = \beta\vec{v}_0$ avec $0 \leq \beta < 1$, et $\|\vec{w}'\| = \beta\|\vec{v}_0\| < \|\vec{v}_0\|$. Donc $\vec{w}' \in \langle\vec{u}_0\rangle$ par minimalité de $\|\vec{v}_0\|$. Donc $\vec{w}' = \vec{0}$.
- Si $\beta = 0$, on raisonne de même : $\|\vec{w}'\| < \|\vec{u}_0\|$ d'où $\vec{w}' = \vec{0}$.
- Si $0 < \alpha < 1$ et $0 < \beta < 1$,

$$\begin{aligned}\|\vec{w}'\|^2 = \|\alpha\vec{u}_0 + \beta\vec{v}_0\|^2 &\leq \alpha^2\|\vec{u}_0\|^2 + \beta^2\|\vec{v}_0\|^2 + 2\alpha\beta|\langle\vec{u}_0, \vec{v}_0\rangle| \\ &< \alpha^2\|\vec{u}_0\|^2 + \beta^2\|\vec{v}_0\|^2 + 2\alpha\beta\|\vec{u}_0\| \cdot \|\vec{v}_0\| \quad \text{(C.S. + non-colinéarité)} \\ &\leq (\alpha^2 + \beta^2 + 2\alpha\beta)\|\vec{v}_0\|^2 \qquad\qquad \text{car } \|\vec{u}_0\| \leq \|\vec{v}_0\|\end{aligned}$$

  Donc $\|\vec{w}'\| < (\alpha + \beta)\|\vec{v}_0\|$.
  On en déduit, pour les mêmes raisons que dans les cas précédents, que

$$\alpha + \beta > 1$$

  On considère ensuite $\vec{w}'' := (1-\alpha)\vec{u}_0 + (1-\beta)\vec{v}_0$. On raisonne de même : $1 - \alpha + 1 - \beta > 1$.
  On a donc

$$\alpha + \beta < 1$$

  Contradiction, ce cas est impossible.

Donc $\vec{w}' \in \mathbb{Z}\vec{u}_0 + \mathbb{Z}\vec{v}_0$. Donc $w = w' - n\vec{u}_0 - m\vec{v}_0 \in \mathbb{Z}\vec{u}_0 + \mathbb{Z}\vec{v}_0$.

1.2 Étude de la partie linéaire

On peut désormais montrer que si G est un groupe paveur de $\mathrm{Is}^+(\mathcal{E})$, alors il n'y a que cinq valeurs possibles pour l'angle de rotation de la partie linéaire.

On considère l'application de la proposition **??** :

$$\varphi : G \longrightarrow \mathcal{O}^+(2,\mathbb{R})$$

Le noyau de φ est $\ker\varphi = \{t_{n\vec{u}_0+m\vec{v}_0}, n, m \in \mathbb{Z}\}$.
Pour $g \in G$, $gt_{n\vec{u}_0+m\vec{v}_0}g^{-1} \in G$, c'est-à-dire $t_{\vec{g}(n\vec{u}_0+m\vec{v}_0)} \in G$.

$$\vec{g}(n\vec{u}_0 + m\vec{v}_0) = n'\vec{u}_0 + m'\vec{v}_0 \qquad n', m' \in \mathbb{Z}$$

Si $m = 0$, $n = 1$, $\vec{g}(\vec{u}_0) = n_1\vec{u}_0 + m_1\vec{v}_0$ avec $n_1, m_1 \in \mathbb{Z}$.
Si $m = 1$, $n = 0$, $\vec{g}(\vec{v}_0) = n_2\vec{u}_0 + m_2\vec{v}_0$ avec $n_2, m_2 \in \mathbb{Z}$.
Donc dans la base $(\vec{u}_0, \vec{v}_0)$, la matrice de $\vec{g}$ est

$$\mathrm{Mat}_{(\vec{u}_0,\vec{v}_0)}(\vec{g}) = \begin{pmatrix} n_1 & n_2 \\ m_1 & m_2 \end{pmatrix}$$

Comme toute rotation, M s'écrit dans une base orthonormée :

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

On en déduit par invariance de la trace par changement de base, que $2\cos\theta = n_1 + m_2 \in \mathbb{Z}$. Donc

$$-2 \leq \underbrace{2\cos\theta}_{\in\mathbb{Z}} \leq 2$$

Donc $2\cos\theta \in \{-2, -1, 0, 1, 2\}$. D'où $\cos\theta \in \{0, \pm\frac{1}{2}, \pm 1\}$ et $\vec{g} \in \{-\mathrm{id}, r_{\frac{2\pi}{3}}, r_{\frac{\pi}{2}}, r_{\frac{\pi}{3}}, \mathrm{id}\}$.

2 Simplicité de $\mathrm{SO}_3(\mathbb{R})$ [8] page 239

2.1 $\mathrm{SO}_n(\mathbb{R})$ est connexe (par arcs), compact

$\mathrm{SO}_n(\mathbb{R})$ est un sous-groupe de $\mathcal{M}(n,\mathbb{R})$ qui est de dimension finie (n^2). Les compacts sont donc les fermés bornés.

Fermé $\mathrm{SO}_n(\mathbb{R})$ est fermé comme intersection de deux fermés :

$$\mathrm{SO}_n(\mathbb{R}) = \det^{-1}(\{1\}) \cap f^{-1}(\{0\})$$

où $f : M \mapsto MM^t - \mathrm{id}$ et det sont continues car polynômiales en les coefficients de M.

Borné En dimension finie, toutes les normes sont équivalentes. On utilise la norme $\|M\| = \sqrt{\mathrm{Tr}(MM^t)}$.
Pour $M \in \mathrm{SO}_n(\mathbb{R})$, on a $\|M\| = \sqrt{\mathrm{Tr}(\mathrm{id})} = \sqrt{n}$ d'où $\mathrm{SO}_n(\mathbb{R}) \subset B(0, \sqrt{n})$.

Connexe par arcs On montre que tout élément de $\mathrm{SO}_n(\mathbb{R})$ peut être relié par un chemin continu à id :
Soit $M \in \mathrm{SO}_n(\mathbb{R})$. D'après le théorème de réduction en base orthonormée, il existe une base orthonormée telle que

$$M = \begin{pmatrix} I_p & & & & 0 \\ & -I_{2q} & & & \\ & & R_{\theta_1} & & \\ & & & \ddots & \\ 0 & & & & R_{\theta_r} \end{pmatrix} \qquad R_{\theta_i} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix}$$

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

$$M(t) = \begin{pmatrix} I_p & & & & & & 0 \\ & R_{t\pi} & & & & & \\ & & \ddots & & & & \\ & & & R_{t\pi} & & & \\ & & & & R_{\theta_1(t)} & & \\ & & & & & \ddots & \\ 0 & & & & & & R_{\theta_r(t)} \end{pmatrix}$$

$\gamma : t \mapsto M(t)$ est un chemin continu tel que $\gamma(0) = \mathrm{id}$, $\gamma(1) = M$.

2.2 Les renversements sont conjugués dans $\mathrm{SO}_3(\mathbb{R})$

Soient r_1 et r_2 deux retournements de $\mathbb{R}^3$ de droite d_1 et d_2 (on rappelle qu'un retournement de $\mathbb{R}^3$ est une rotation d'angle π autour d'une droite). On choisit e_i unitaire sur d_i (pour $i = 1, 2$). En prenant une base (u_i, v_i) de $e_i^\perp$ constituée de vecteurs unitaires, la matrice de passage de (e_1, u_1, v_1) à (e_2, u_2, v_2) est une matrice orthogonale (matrice de passage entre deux bases orthogonales). Quitte à remplacer e_1 par $-e_1$, on obtient une matrice de déterminant 1, donc dans $\mathrm{SO}_3(\mathbb{R})$.

2.3 Existence d'un renversement dans $\mathrm{SO}_3(\mathbb{R})$

Soit H un sous-groupe non-trivial de $\mathrm{SO}_3(\mathbb{R})$, et $h \in H$, $h \neq \mathrm{id}$. On définit

$$\begin{array}{rccc} \varphi : & \mathrm{SO}_3(\mathbb{R}) & \longmapsto & \mathbb{R} \\ & g & \longmapsto & \mathrm{Tr}(ghg^{-1}h^{-1}) \end{array}$$

φ est continue comme composée de fonctions continues. Comme $\mathrm{SO}_3(\mathbb{R})$ est connexe compact, $\varphi(\mathrm{SO}_3(\mathbb{R}))$ est un intervalle fermé borné de $\mathbb{R}$. Notons-le $[a, b]$.
Comme $\varphi(\mathrm{id}) = 3$, on a $a \leq 3 \leq b$.
Par réduction en base orthonormée, il existe θ tel que

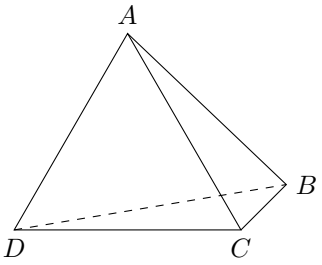
$$\mathrm{Tr}(ghg^{-1}h^{-1}) = 1 + 2\cos\theta \in [-1, 3]$$

donc $b = 3$.
Supposons que $a = 3$. Alors, pour tout $g \in \mathrm{SO}_3(\mathbb{R})$, $\mathrm{Tr}(ghg^{-1}h^{-1}) = 3$. Par unicité de la réduction en base orthonormée, $ghg^{-1}h^{-1} = \mathrm{id}$. Donc $gh = hg$ et $h \in Z(\mathrm{SO}_3(\mathbb{R})) = \{\mathrm{id}\}$. Absurde car on a supposé $h \neq \mathrm{id}$.
On peut alors choisir $n \in \mathbb{N}$ tel que $a < 1 + 2\cos(\pi/n) < 3$, et on note g_n l'élément tel que $\varphi(g_n) = 1 + 2\cos(\pi/n)$. Alors, $h_n = g_n h g_n^{-1} h^{-1} \in H$ (car $g_n h g_n^{-1} \in H$ et $h^{-1} \in H$) est une rotation d'angle $\pm\pi/n$. D'où $h_n^n \in H$ est une rotation d'angle π, c'est-à-dire un retournement.

3 Isométries du tétraèdre et du cube [8] page 363

On utilise la magie des actions de groupes.

3.1 Isométries du tétraèdre



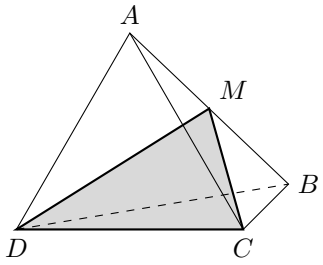
On fait agir $\mathrm{Is}(T)$ sur l'ensemble des sommets de T. C'est bien une action car les sommets de T sont les points extrêmaux de T. On obtient un morphisme

$$\rho : \mathrm{Is}(T) \longrightarrow \mathfrak{S}_{\{A,B,C,D\}} \simeq \mathfrak{S}_4$$

Reste à montrer que ρ est injectif et surjectif :

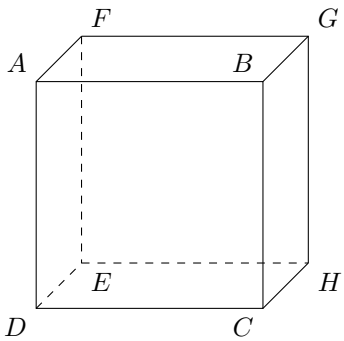
Injectivité Soit $g \in \mathrm{Is}(T)$ tel que $g \cdot A = A$, $g \cdot B = B$, $g \cdot C = C$, $g \cdot D = D$. Comme $(A, \overrightarrow{AB}, \overrightarrow{AC}, \overrightarrow{AD})$ est un repère affine de $\mathbb{R}^3$, le tétraèdre est fixé, et $g = \mathrm{id}_T$. Donc $\ker \rho = \{\mathrm{id}\}$ et ρ est injectif.

Surjectivité On utilise le fait que les transpositions engendrent $\mathfrak{S}_4$. On montre donc seulement que les transpositions sont atteintes. Quitte à renommer les sommets, il suffit de montrer que $(A\ B)$ est atteinte. Notons M le milieu de $[A, B]$. La symétrie par rapport au plan (CDM) stabilise le tétraèdre. De plus, elle échange A et B car M est le milieu de $[A, B]$, et $(CDM) \perp (AB)$ car C, D, et M sont équidistants de A et B. Enfin, elle fixe C et D qui sont dans le plan de symétrie.



3.2 Isométries du cube

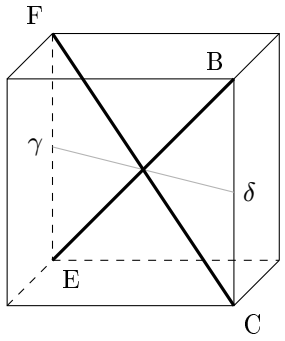
On fait agir $\mathrm{Is}(C)$ sur les grandes diagonales du cube.



Les grandes diagonales étant les plus grands segments du cube, et les isométries conservant les distances, on obtient ainsi une action de groupe

$$g : \mathrm{Is}(C) \longrightarrow \mathfrak{S}_{\{D_1,D_2,D_3,D_4\}} \simeq \mathfrak{S}_4$$

Surjectivité On raisonne de la même manière que dans le tétraèdre en montrant que les transpositions sont atteintes. Pour échanger deux diagonales, et fixer les autres, il suffit de prendre la rotation d'angle π (c'est-à-dire le retournement) autour de la droite reliant les milieux des côtés opposés (contenant les quatres sommets intervenant) :



(FC) et (BE) sont échangées par cette rotation : en effet, B et C sont échangés car $(\gamma\delta) \perp (BC)$, et de même, E et F sont échangés. (FC) est donc envoyée sur (BE) et réciproquement.
Les deux autres grandes diagonales sont envoyées sur elles-mêmes par cette rotation puisqu'elles sont dans un plan orthogonal à $(\gamma\delta)$ (les quatres sommets de ces diagonales sont équidistants de la droite $(\gamma\delta)$).

Noyau Soit $s \in \mathrm{Is}(C)$ telle que $s(D_i) = D_i$ pour $1 \leq i \leq 4$. Supposons que $s \neq \mathrm{id}$. Comme s conserve toutes les diagonales, il existe une diagonale qu'on peut supposer (AH) (quitte à renommer les sommets) telle que $s(A) = H$ et $s(H) = A$. Mais alors $s(B) \in \{B, E\}$ car s conserve (BE), et comme s est une isométrie, $d(A,B) = d(s(A), s(B)) = d(H, s(B))$. Donc $s(B) \in \{C, E, G\}$. Finalement, $s(B) \in \{B, E\} \cap \{C, E, G\}$ donc $s(B) = E$. En raisonnant de même pour les autres sommets, on en déduit que $s = s_O$ (la symétrie par rapport à O, centre de gravité du cube). D'où $\ker g = \langle s_O \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. Par le premier théorème d'isomorphisme,

$$\mathrm{Is}(C)/\left(\mathbb{Z}/2\mathbb{Z}\right) \simeq \mathfrak{S}_4$$

Si on regarde les classes dans le quotient $\mathrm{Is}(C)/\langle s_O \rangle$, elles sont de la forme $\{f, s_O \circ f\}$. En particulier, chaque classe contient un déplacement et un anti-déplacement. On en déduit que $\mathrm{Is}^+(C) \simeq \mathfrak{S}_4$ et donc $\mathrm{Is}(C)/\langle s_O \rangle \simeq \mathrm{Is}^+(C)$. On a alors $|\mathrm{Is}(C)| = |\langle s_O \rangle| \times |\mathrm{Is}^+(C)|$.
$\langle s_O \rangle \cap \mathrm{Is}^+(C) = \{\mathrm{id}\}$ car $\det s_O = -1$.
$\mathrm{Is}^+(C) \lhd \mathrm{Is}(C)$ car c'est un sous-groupe d'indice 2.
On a alors un produit semi-direct : $\mathrm{Is}(C) \simeq \langle s_O \rangle \rtimes \mathrm{Is}^+(C)$.
Pour montrer que le produit est en fait direct, on considère le morphisme suivant :

$$\varphi : \left\{ \begin{array}{rcl} \mathrm{Is}(C) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathrm{Is}^+(C) \\ f & \longmapsto & (\det(f), \overline{f}) \end{array} \right.$$

C'est bien un morphisme par multiplicativité du déterminant. C'est même un isomorphisme car une isométrie est entièrement définie par son déterminant et l'isométrie positive correspondante. On obtient finalement

$$\mathrm{Is}(C) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{Is}^+(C)$$

4 Densité des polynômes orthogonaux [18] page 140

Théorème. *Soit I un intervalle de $\mathbb{R}$. Soit ω une fonction poids sur $L^2(I)$. On suppose qu'il existe $a > 0$ tel que*

$$\int_I \mathrm{e}^{a|x|}\,\omega(x)\,dx < +\infty$$

Alors, on peut trouver une famille de polynômes orthogonaux associés à ω formant une base hilbertienne de $L^2(I,\omega)$.

Remarque (idée de la preuve). On montre seulement la densité. L'orthonormalisation s'obtient avec Gram-Schmidt. On montre que si $\langle f, x^n\rangle = 0$, alors $f = 0$. Pour ça :

1. On étend f en une fonction L^1 qu'on note φ. On regarde sa transformée de Fourier $\hat{\varphi}$.
2. On étend $\hat{\varphi}$ sur B_a en une fonction F.
3. On montre que $F = 0$.
4. On en déduit $\hat{\varphi} = 0$ puis $\varphi = 0$ puis $f = 0$.

Démonstration. Soit $f \in L^2(I,\omega)$ vérifiant

$$\langle f, x^n\rangle_{L^2(I,\omega)} = 0 \qquad \forall n \in \mathbb{N}$$

On va montrer que $f = 0$, ce qui donnera la densité.

1. On veut calculer la transformée de Fourier de f. On pose

$$\varphi(x) = \begin{cases} f(x)\omega(x) & x \in I \\ 0 & x \notin I \end{cases}$$

On montre que $\varphi \in L^1(\mathbb{R})$ (pour pouvoir appliquer la transformée de Fourier) :

$$\int_{\mathbb{R}} |\varphi(x)|\mathrm{d}x = \int_I |f(x)|\omega(x)\mathrm{d}x \overset{\text{C-S}}{\leq} \underbrace{\left(\int_I |f(x)|^2\omega(x)\mathrm{d}x\right)^{1/2}}_{<+\infty \text{ car } f\in L^2(I,\omega)} \cdot \underbrace{\left(\int_I 1^2\omega(x)\mathrm{d}x\right)^{1/2}}_{<+\infty \text{ car } \omega \text{ est un poids}} < +\infty$$

La transformée de Fourier de φ est donc bien définie : pour $\xi \in \mathbb{R}$,

$$\hat{\varphi}(\xi) = \int_I \mathrm{e}^{-ix\xi}\, f(x)\omega(x)\mathrm{d}x$$

2. On étend $\hat{\varphi}$ à B_a où $B_a = \{z \in \mathbb{C}, |\Im z| < a/2\}$.

$$F(z) = \int_I \mathrm{e}^{-ixz}\, f(x)\omega(x)\mathrm{d}x$$

On applique le théorème d'holomorphie sous l'intégrale :

(*i*) $x \mapsto \mathrm{e}^{-ixz}\, f(x)\omega(x)$ est une fonction mesurable pour tout $z \in B_a$.

(*ii*) $z \mapsto \mathrm{e}^{-ixz}\, f(x)\omega(x)$ est une fonction holomorphe pour tout $x \in I$.

(*iii*) Si $z \in B_a$, $z = u + iv$ avec $|v| < a/2$. D'où

$$|\,\mathrm{e}^{-ixz}\,| = |\,\mathrm{e}^{-ix(u+iv)}\,| = |\,\mathrm{e}^{-ixu}\,\mathrm{e}^{xv}\,| = |\,\mathrm{e}^{xv}\,| \leq \mathrm{e}^{|x|.|v|} \leq \mathrm{e}^{|x|a/2}$$

Donc

$$|\,\mathrm{e}^{-ixz}\, f(x)\omega(x)| = |\,\mathrm{e}^{-ixz}\,|.|f(x)|.\omega(x) \leq \mathrm{e}^{|x|a/2}\,|f(x)|\omega(x) =: g(x)$$

$g(x) \in L^1(\mathbb{R})$ car

$$\int_{\mathbb{R}} g(x)\mathrm{d}x = \int_I \mathrm{e}^{|x|a/2}\,|f(x)|\omega(x)\mathrm{d}x \overset{\text{C-S}}{\leq} \underbrace{\left(\int_I \mathrm{e}^{a|x|}\,\omega(x)\mathrm{d}x\right)^{1/2}}_{<+\infty \text{ par hypothèse}} \cdot \underbrace{\left(\int_I |f(x)|^2\omega(x)\mathrm{d}x\right)^{1/2}}_{<+\infty \text{ car } f\in L^2(I,\omega)} < +\infty$$

Le théorème d'holomorphie sous l'intégrale donne :

$$F^{(n)}(z) = \int_I (-ix)^n \, \mathrm{e}^{-ixz} \, f(x)\omega(x)\mathrm{d}x \qquad \forall n \in \mathbb{N}$$

d'où $F^{(n)}(0) = \int_I (-ix)^n \, \mathrm{e}^0 \, f(x)\omega(x)\mathrm{d}x = (-i)^n \int_I x^n f(x)\omega(x)\mathrm{d}x = (-i)^n \langle f, x^n \rangle_{L^2(I,\omega)} = 0$.

3. F est holomorphe, et donc sur un voisinage de 0, on a

$$F(z) = \sum_{n \geq 0} \frac{F^{(n)}(0)}{n!} z^n$$

Par unicité du développement en série entière, on en déduit que F est nulle sur un voisinage de 0. Par le théorème des zéros isolés, on en déduit que $\boxed{F \text{ est nulle}}$ sur l'ouvert connexe B_a.

4. $\boxed{\hat{\varphi} \text{ est nulle}}$ car $\mathbb{R} \subset B_a$, et $F_{|\mathbb{R}} = \hat{\varphi}$.
Comme l'application $\hat{}$ est injective, on en déduit que $\boxed{\varphi \text{ est nulle}}$ pour presque tout $x \in I$.
Comme ω est une fonction strictement positive, on a donc $\boxed{f \text{ est nulle}}$ pour presque tout $x \in I$.

On a donc montré que la famille $(x^n)_{n\in\mathbb{N}}$ est dense dans $L^2(I,\omega)$. Pour construire une famille orthonormée, on applique Gram-Schmidt à cette famille. □

5 Ellipsoïde de John Lowner [14] page 229

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

Démonstration. Un ellipsoïde de $\mathbb{R}^n$ est la donnée d'une inégalité du type $q(x) \leq 1$ où q est une forme quadratique définie positive. Dans la suite, on note $\mathcal{E}_q = \{x \in \mathbb{R}^n, q(x) \leq 1\}$.
On commence par calculer le volume $V(\mathcal{E}_q)$: on peut trouver une base orthonormée $(e_1, \ldots, e_n)$ telle que $q(x) = \sum_{i=1}^n a_i x_i^2$. On obtient alors :

$$V(\mathcal{E}_q) = \int \int \ldots \int_{a_1 x_1^2 + \ldots + a_n x_n^2 \leq 1} \mathrm{d}x_1 \ldots \mathrm{d}x_n$$

On effectue alors le changement de variable $y_i := \sqrt{a_i} x_i$. Le jacobien vaut $\frac{1}{\sqrt{a_1 \ldots a_n}}$. Si on note S la matrice de q dans une base orthonormée, on peut diagonaliser S en base orthonormée : $S = P\mathrm{Diag}(a_1, \ldots, a_n)P^t$, et $\det(S) = a_1 \ldots a_n$. Ce déterminant ne dépend donc pas de la base choisie. On le note désormais $D(q)$. Le changement de variables donne alors :

$$V(\mathcal{E}_q) = \int \int \ldots \int_{y_1^2 + \ldots + y_n^2 \leq 1} \frac{\mathrm{d}y_1 \ldots \mathrm{d}y_n}{\sqrt{D(q)}} = \frac{V_0}{\sqrt{D(q)}}$$

où V_0 désigne le volume de la boule unité de $\mathbb{R}^n$.
Le problème peut donc se reformuler ainsi : on cherche l'unique forme quadratique $q \in Q_{++}$ maximisant $D(q)$, et telle que pour tout $x \in K$, $q(x) \leq 1$.
On munit l'espace Q de la norme N définie par $N(q) = \sup_{\|x\| \leq 1} |q(x)|$, et on considère l'ensemble

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

On cherche à maximiser D sur ce domaine.
Montrons que $\mathcal{A}$ est un compact convexe non-vide de Q.

$\mathcal{A}$ **est convexe** Soit $q, q' \in \mathcal{A}$ et $\lambda \in [0,1]$. Pour $x \in \mathbb{R}^n$,

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

et $\lambda q + (1-\lambda)q'$ est une forme quadratique positive. De plus, si $x \in K$,

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

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

$\mathcal{A}$ **est fermé** Soit $(q_n)_{n\in\mathbb{N}}$ une suite de $\mathcal{A}$ convergeant dans Q vers q. Pour $x \in \mathbb{R}^n$, on a

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

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

$$\forall x \in \mathbb{R}^n, q(x) = \lim_{n\to+\infty} q_n(x) \geq 0$$

$$\forall x \in K, q(x) = \lim_{n\to+\infty} q_n(x) \leq 1$$

donc $q \in \mathcal{A}$.

$\mathcal{A}$ **est borné** Comme K est d'intérieur non-vide, il existe $a \in K$ et $r > 0$ tel que $B(a,r) \subset K$. Soit $q \in \mathcal{A}$. Si $\|x\| \leq r$, alors $x + a \in K$ donc $q(x+a) \leq 1$. D'autre part, $q(-a) = q(a) \leq 1$. Donc par l'inégalité de Minkowski,

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

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

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

ce qui montre que $N(q) \leq \frac{4}{r^2}$.

$\mathcal{A}$ **est non-vide** Comme K est compact, il est borné. Soit $M > 0$ tel que pour tout $x \in K$, $\|x\| \leq M$. Alors, si $\tilde{q}$ est définie par $\tilde{q}(x) = \frac{\|x\|^2}{M^2}$, on a pour $x \in K$, $q(x) \leq 1$.

L'application $q \mapsto D(q)$ est continue sur le compact $\mathcal{A}$, donc atteint son maximum sur $\mathcal{A}$, disons en q_0. Comme $\mathcal{A}$ contient $\tilde{q}$ qui est définie positive, q_0 est aussi définie positive, et donc $q_0 \in Q_{++}$. On a prouvé qu'il existe $\mathcal{E}_{q_0}$ de volume minimal contenant K.

Reste à montrer l'unicité : supposons $q_1 \in \mathcal{A}$ tel que $D(q_0) = D(q_1)$. On note S_0, S_1 leur matrices respectives dans la base canonique de $\mathbb{R}^n$. Comme $\mathcal{A}$ est convexe, $\frac{q_0+q_1}{2}$ est aussi dans $\mathcal{A}$, et par un résultat de convexité logarithmique du déterminant sur $\mathcal{S}_{++}$, on a

$$D\left(\frac{1}{2}(q_0+q_1)\right) = \det\left(\frac{1}{2}(S_0+S_1)\right) > (\det S_0)^{1/2}(\det S_1)^{1/2} \geq \det S_0 \geq D(q_0)$$

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

6 Loi de réciprocité quadratique [8] page 185

p et q sont deux nombres premiers impairs distincts.

Lemme. *Le nombre de solutions de l'équation* $px^2 = 1$ *dans* $\mathbb{F}_q$ *est* $1 + \left(\frac{p}{q}\right)$.

Démonstration. Comme p et q sont premiers entre eux, p est inversible, et on a

$$px^2 = 1 \iff x^2 = p^{-1}$$

On sait que p^{-1} est un carré, si et seulement si, p est un carré. En effet, $p^{-1} = r^2 \iff p = \left(r^{-1}\right)^2$.
Si p^{-1} est un carré, l'équation possède au moins une solution, et elle en possède alors deux : r et $-r$ qui sont distincts car $\mathrm{Car}(\mathbb{F}_q) \neq 2$.
Si p^{-1} n'est pas un carré, l'équation ne possède pas de solution.
Au final, si $\left(\frac{p}{q}\right) = 1$, le nombre de solution est 2 ; si $\left(\frac{p}{q}\right) = -1$, le nombre de solution est 0. □

Théorème (loi de réciprocité quadratique)**.**

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

Démonstration. On va calculer le cardinal de l'ensemble

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

de deux manières différentes :

Par une action de groupe On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par l'action

$$\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} \times X & \longrightarrow & X \\ (k, (x_1, \ldots, x_p)) & \longmapsto & (x_{1+k}, \ldots, x_{p+k}) \end{array}$$

Les orbites sont de deux types :

1. Celles de la forme $(x, \ldots, x)$ avec $x \in \mathbb{F}_q$. Ces éléments ont pour stabilisateur $\mathbb{Z}/p\mathbb{Z}$.
2. Les autres, de stabilisateur trivial.

Le nombre d'éléments des orbites du type 1 sont le nombre de solutions de l'équation $px^2 = 1$, c'est-à-dire (par le lemme) $1 + \left(\frac{p}{q}\right)$.

Le cardinal des orbites de type 2 est divisible par p car $\#\mathrm{Orb} = \frac{|\mathbb{Z}/p\mathbb{Z}|}{\#\mathrm{Stab}} = \frac{p}{1} = p$.
On a donc

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

Par les formes quadratiques Les matrices suivantes sont congruentes car elles ont même rang et même discriminant :

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

On en déduit que

$$|X| = \#\left\{(y_1, \ldots, y_d, z_1, \ldots, z_d, t) \in \mathbb{F}_q^p, 2\sum_{i=1}^{d} y_i z_i + at^2 = 1\right\} \qquad d = \frac{p-1}{2} \qquad a = (-1)^d$$

— Si $y_1 = \ldots = y_d = 0$, alors on a $at^2 = 1$ et q possibilités pour chaque z_i, donc au total, $\left(1 + \left(\frac{a}{q}\right)\right) q^d$ possibilités.

— S'il existe un y_i non-nul, on fixe $(y_1, \dots, y_d, t)$ avec $(q^d-1)q$ possibilités. On peut ensuite écrire z_1 en fonction de $z_2, \dots, z_d$, donc il y a q^{d-1} possibilités pour fixer les z_i. Au total, on a $(q^d-1)q^d$ possibilités.

On a donc

$$|X| = q^d \left(q^d + \left(\frac{p}{q}\right) \right) \tag{2}$$

En égalisant (1) et (2), on obtient

$$1 + \left(\frac{p}{q}\right) = q^{\frac{p-1}{2}} \left(q^{\frac{p-1}{2}} + \left(\frac{a}{q}\right) \right) = \underbrace{q^{p-1}}_{=1} + \underbrace{q^{\frac{p-1}{2}}}_{=\left(\frac{q}{p}\right)} (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

c'est-à-dire

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

□

7 Théorèmes d'Abel angulaire et taubérien faible [4] page 252

Théorème (Abel angulaire)**.** *Soit $\sum_n a_n z^n$ une série entière de rayon de convergence ≥ 1 telle que $\sum_n a_n$ converge. On note f la somme de cette série entière sur le disque unité. On fixe $\theta_0 \in [0, \pi/2[$ et on pose*

$$\Delta_{\theta_0} = \{z \in \mathbb{C}, |z| < 1 \text{ et } \exists \rho > 0, \exists \theta_0 \in [-\theta_0, \theta_0], z = 1 - \rho\, \mathrm{e}^{i\theta}\}$$

Alors on a

$$\lim_{z \to 1, z \in \Delta_{\theta_0}} f(z) = \sum_{n \geq 0} a_n$$

Démonstration. On note $S = \sum_{n\geq 0} a_n$, $S_n = \sum_{k=0}^n a_k$ et $R_n = S - S_n$ pour $n \in \mathbb{N}$. On va majorer $|f(z) - S|$. Soit $z \in \mathbb{C}^*$, $|z| < 1$. Pour $N \in \mathbb{N}^*$, on a

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

d'où quand $N \to +\infty$,

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

Comme $R_n \to 0$, pour $\varepsilon > 0$, il existe $N \in \mathbb{N}$ tel que pour $n > N$, $|R_n| < \varepsilon$. Donc pour $|z| < 1$,

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

Prenons maintenant $z \in \Delta_{\theta_0}$. Il existe $\rho > 0$ et $|\varphi| \leq \theta_0$ tel que $z = 1 - \rho\, \mathrm{e}^{i\varphi}$. On a donc

$$|z| = 1 - 2\rho\cos\varphi + \varphi^2$$

et lorsque $\rho \leq \cos\theta_0$, on a

$$\frac{|z-1}{1-|z|} = \frac{|z-1|}{1-|z|^2}(1+|z|) = \frac{\rho}{2\rho\cos\varphi - \rho^2}(1+|z|) \leq \frac{2}{2\cos\varphi - \rho} \leq \frac{2}{2\cos\theta_0 - \cos\theta_0} = \frac{2}{\cos\theta_0}$$

Si on prend α tel que $\alpha\left(\sum_{n=0}^{N}|R_n|\right)<\varepsilon$, alors si $z\in\Delta_{\theta_0}$ et $|z-1|\leq\inf(\alpha,\cos\theta_0)$, alors on a

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

□

Remarques.

1. On peut calculer $\pi/4$ grâce à l'égalité :

$$\sum_{n=0}^{+\infty}\frac{(-1)^n}{2n+1}=\lim_{x\to1,x<1}\sum_{n\geq0}\frac{(-1)^n}{2n+1}x^n=\lim_{x\to1,x<1}\arctan x=\arctan 1=\pi/4$$

2. Si la série converge absolument, le théorème est évident.
3. La réciproque est fausse : il suffit de considérer la série $\sum_{n\geq0}(-1)^nz^n$. On a cependant une réciproque partielle : le théorème taubérien faible.

Théorème (taubérien faible)**.** *Soit $\sum_n a_nz^n$ une série entière de rayon de convergence 1, et f la somme de cette série entière sur le disque unité. On suppose que*

$$\exists S\in\mathbb{C}\qquad\lim_{z\to1,z<1}f(z)=S$$

Si $a_n=o(1/n)$, alors $\sum_n a_n$ converge et $\sum_n a_n=S$.

Démonstration. Avec les mêmes notations que précédemment, on a pour $n\in\mathbb{N}^*$, $x\in]0,1[$,

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

et comme $(1-x^k)=(1-x)(1+x+\ldots+x^{k-1})\leq k(x-1)$ pour $0<x<1$. On en déduit

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

où M est un majorant de $(k|a_k|)_k$ (elle est majorée car tend vers 0). Fixons $\varepsilon>0$ tel que $\varepsilon<1$. On a alors

$$\forall n\in\mathbb{N}^*,|S_n-f(1-\varepsilon/n)|\leq M\varepsilon+\frac{\sup_{k>n}k|a_k|}{\varepsilon}$$

Si N_0 est choisi tel que $\sup_{k>N_0}k|a_k|<\varepsilon^2$ (on peut car $ka_k\to0$), on a

$$\forall n\geq N_0,|S_n-f(1-\varepsilon/n)|\leq M\varepsilon+\varepsilon=(M+1)\varepsilon$$

Par hypothèse, $f(x)$ tend vers S quand $x\to1^-$ donc il existe $N_1\geq N_0$ tel que $|f(1-\varepsilon/n)-S|<\varepsilon$ pour $n\geq N_1$. Ainsi,

$$\forall n\geq N_1,|S_n-S|\leq|S_n-f(1-\varepsilon/n)|+|f(1-\varepsilon/n)-S|\leq(M+2)\varepsilon$$

donc S_n converge vers S. □

Remarque. Le résultat reste vrai si on suppose $a_n=O(1/n)$. C'est le théorème taubérien fort (plus difficile à démontrer).

8 Chevalley-Warning et Erdos-Ginzburg-Ziv [19] page 32

Soit p un nombre premier, $n, m \in \mathbb{N}^*$, et $q = p^n$.
Pour $f : K \to K$, on note $S(f) = \sum_{x \in K} f(x)$.

Théorème (Chevalley-Warning)**.** *Soit $(f_a)_{a \in A}$ une famille de polynômes de $\mathbb{F}_q[X_1, \ldots, X_m]$ vérifiant $\sum_{a \in A} \deg f_a < m$. Alors, on a*

$$\#Z(f_a, a \in A) \equiv 0 \mod p$$

où $Z(f_a, a \in A)$ est l'ensemble des zéros de tous les f_a.

Lemme. *Soit $u \in \mathbb{N}$. Alors,* $S(X^u) = \begin{cases} -1 & u > 0 \text{ et } q-1 \mid u \\ 0 & \text{sinon.} \end{cases}$

Démonstration. Si $u = 0$, $S(X^0) = \sum_{x \in \mathbb{F}_q} 1 = q = 0$.
Si $u > 0$ et $q - 1 \mid u$, alors $u = \alpha(q-1)$ et

$$\sum_{x \in \mathbb{F}_q} x^u = 0^u + \sum_{x \in \mathbb{F}_q^\times} (x^{q-1})^\alpha = \sum_{x \in \mathbb{F}_q^\times} 1 = q - 1 = -1$$

Si $q - 1 \not| u$, comme $\mathbb{F}_q^\times$ est cyclique, $\exists y$ tel que $y^u \neq 1$ ($\mathbb{F}_q^\times = \langle y \rangle$). L'application $x \mapsto yx$ est une bijection. D'où

$$\sum_{x \in \mathbb{F}_q} x^u = \sum_{x \in \mathbb{F}_q} (yx)^u = y^u \sum_{x \in \mathbb{F}_q} x^u$$

d'où $S(X^u) = 0$. □

Démonstration. (du théorème) On pose

$$P = \prod_{a \in A} (1 - f_a^{q-1})$$

On montre que P est la fonction indicatrice de $Z(f_a, a \in A)$. En effet, si $x \in Z(f_a, a \in A)$, alors $P(x) = \prod(1-0) = 1$. Si $x \notin Z(f_a, a \in A)$, il existe a_0 tel que $f_{a_0}(x) \neq 0$. Par Lagrange, $(f_{a_0}(x))^{q-1} = 1$, et donc $1 - f_{a_0}^{q-1}(x) = 0$. D'où $P(x) = 0$.

On en déduit

$$S(P) = \sum_{x \in \mathbb{F}_q} P(x) = \sum_{\substack{x \in \mathbb{F}_q \\ x \in Z(f_a, a \in A)}} 1 + \sum_{\substack{x \in \mathbb{F}_q \\ x \notin Z(f_a, a \in A)}} 0 \equiv \#Z(f_a, a \in A) \mod p$$

Comme $\sum_{a \in A} \deg f_a < m$, $\deg P < m(q-1)$. On peut écrire P comme combinaison linéaire de monômes X^u avec $\sum u_i < m(q-1)$. Par le principe des tiroirs, $\exists i_0$ tel que $u_{i_0} < q - 1$. Par le lemme précédent ($q - 1$ ne divise pas u_{i_0}), $S(X_{i_0}^{u_{i_0}}) = 0$ et donc

$$S(X^u) = S(X_{i_0}^{u_{i_0}}) S(X_1^{u_1} \ldots \hat{X}_{i_0}^{u_{i_0}} \ldots X_m^{u_m}) = 0$$

□

Théorème (Erdös-Ginzburg-Ziv)**.** *Soient $a_1, \ldots, a_{2n-1}$ des entiers. Alors on peut trouver $a_{i_1}, \ldots, a_{i_n}$ tels que $\sum_{j=1}^n a_{i_j} \equiv 0 \mod n$.*

Démonstration.

1. On montre que le résultat est vrai pour les nombres premiers.
   On se place dans $\mathbb{F}_p$, et soient $a_1, \dots, a_{2p-1}$ des entiers. On considère

$$P_1(X_1, \dots, X_{2p-1}) = \sum_{i=1}^{2p-1} X_i^{p-1} \qquad P_2(X_1, \dots, X_{2p-1}) = \sum_{i=1}^{2p-1} \bar{a}_i X_i^{p-1}$$

   $P_1, P_2 \in \mathbb{F}_p[X]$ et $\deg P_1 + \deg P_2 = 2p - 2 < 2p - 1$ donc on peut appliquer le théorème de Chevalley-Warning. On a déjà une racine (0), donc il existe une deuxième racine $(x_1, \dots, x_{2p-1})$. On pose $W = \{i, x_i \neq 0\}$. Comme $P_1(x_1, \dots, x_{2p-1}) = 0$, on en déduit que

$$0 \equiv \sum_{i=1}^{2p-1} x_i^{p-1} \equiv \sum_{i \in W} x_i^{q-1} \equiv \sum_{i \in W} 1 \equiv |W| \mod p$$

   Donc $1 \leq |W| \leq 2p - 1$ et $|W|$ est divisible par p, donc $|W| = p$. On note $W = \{i_1, \dots, i_p\}$.

$$P_2(x_1, \dots, x_{2p-1}) \equiv \sum_{j=1}^{p} a_{i_j} \equiv 0 \mod p$$

2. On montre que c'est stable par multiplication.
   Soient n et m vérifiant la propriété. Soient $a_1, \dots, a_{2mn-1}$ des entiers.
   Comme n vérifie la propriété, on peut trouver un ensemble $I_1 \subset [\![1, 2mn - 1]\!]$ de cardinal n tel que

$$\sum_{i \in I_1} a_i \equiv 0 \mod n$$

   On peut aussi trouver I_2 dans $[\![1, 2mn - 1]\!] \backslash I_1$ de cardinal n tel que

$$\sum_{i \in I_2} a_i \equiv 0 \mod n$$

   On peut itérer le raisonnement $2m - 2$ fois et on construit $I_1, \dots, I_{2m-1}$. Il reste alors $2nm - 1 - n(2m - 2) = 2n - 1$ entiers et on ne peut plus construire de I_j.
   On pose alors, pour $j \in [\![1, 2m - 1]\!]$, c_j tel que

$$\sum_{i \in I_j} a_i = c_j n$$

   On a donc $c_1, \dots, c_{2m-1}$ entiers. Comme m vérifie la propriété, $\exists j_1, \dots, j_m$ tels que

$$\sum_{k=1}^{m} c_{j_k} \equiv 0 \mod m$$

   D'où

$$\begin{aligned} \sum_{k=1}^{m} \sum_{i \in I_{j_k}} a_i = \sum_{k=1}^{m} n c_{j_k} &= n \sum_{k=1}^{m} c_{j_k} \\ &\equiv 0 \mod mn \end{aligned}$$

□

9 Intégrale de Fresnel [4] page 342

$$\boxed{\int_0^{+\infty} \mathrm{e}^{ix^2} \, \mathrm{d}x = \frac{\sqrt{\pi}}{2} \mathrm{e}^{i\pi/4}}$$

9.1 Le théorème de Césaro-continu

Théorème (Césaro-continu). *Si $f : \mathbb{R}_+ \longrightarrow \mathbb{R}$ vérifie $f(t) \xrightarrow{t\to+\infty} l \in \mathbb{R}$, alors*

$$\frac{1}{T}\int_0^T f(t)dt \xrightarrow{T\to+\infty} l$$

Démonstration. Quitte à poser $g = f - l$, on peut supposer que $l = 0$.
Comme $f \xrightarrow{t\to+\infty} 0$, on a

$$\forall \varepsilon > 0, \exists t_0 \in \mathbb{R}_+, \forall t > t_0, |f(t)| < \varepsilon/2$$

On calcule ensuite

$$\left|\int_0^T f(t)\mathrm{d}t\right| = \left|\int_0^{t_0} f(t)\mathrm{d}t + \int_{t_0}^T f(t)\mathrm{d}t\right| \leq \left|\int_0^{t_0} f(t)\mathrm{d}t\right| + (T - t_0)\varepsilon/2$$

On pose $T_0 = \max\left(t_0, \frac{2}{\varepsilon}\left|\int_0^{t_0} f(t)\mathrm{d}t\right|\right)$. On a alors :

$$\left|\int_0^T f(t)\mathrm{d}t\right| \leq \frac{\varepsilon}{2}T_0 + \frac{\varepsilon}{2}(T - T_0) = T\varepsilon$$

□

9.2 Convergence de l'intégrale

On pose, pour $0 < a < T$, $f_a(T) = \int_a^T \mathrm{e}^{ix^2}\,\mathrm{d}x$.

$$f_a(T) \overset{u=x^2}{=} \int_{a^2}^{T^2} \frac{\mathrm{e}^{iu}\,\mathrm{d}u}{2\sqrt{u}} \overset{\text{IPP}}{=} \underbrace{\left[\frac{\mathrm{e}^{iu}}{2i\sqrt{u}}\right]_{a^2}^{T^2}}_{=\frac{\mathrm{e}^{iT^2}}{2iT} - \frac{\mathrm{e}^{ia^2}}{2ia}} - \underbrace{\int_{a^2}^{T^2} \frac{\mathrm{e}^{iu}\,\mathrm{d}u}{4iu\sqrt{u}}}_{\text{absolument convergente en } +\infty}$$

donc l'intégrale converge vers $I < +\infty$.

9.3 Etude de f^2

On pose $f(t) = \int_0^t \mathrm{e}^{ix^2}\,\mathrm{d}x$. On a montré que $f(t) \xrightarrow{t\to+\infty} I$ (et donc $f^2(t) \xrightarrow{t\to+\infty} I^2$).
On a

$$f^2(t) = \iint_{[0,t]^2} \mathrm{e}^{i(x^2+y^2)}\,\mathrm{d}x\mathrm{d}y = 2\iint_{\Delta_t} \mathrm{e}^{i(x^2+y^2)}\,\mathrm{d}x\mathrm{d}y$$

où $\Delta_t = \{(x, y) \in [0, t]^2, y \leq x\}$.
Comme $\partial\Delta_t$ est de mesure nulle,

$$f^2(t) = 2\int_{0<y<x<t} \mathrm{e}^{i(x^2+y^2)}\,\mathrm{d}x\mathrm{d}y$$

On fait le changement de variable

$$\begin{cases} x = r\cos\theta \\ y = r\sin\theta \end{cases} \qquad \begin{matrix} 0 < \theta < \pi/4 \\ 0 < r < t/\cos\theta \end{matrix} \qquad \mathrm{d}x\mathrm{d}y = r\mathrm{d}r\mathrm{d}\theta$$

On obtient

$$f^2(t) = 2\int_0^{\pi/4}\int_0^{t/\cos\theta} \mathrm{e}^{ir^2}\,r\mathrm{d}r\mathrm{d}\theta = \frac{1}{i}\int_0^{\pi/4}\left[\mathrm{e}^{ir^2}\right]_0^{t/\cos\theta}\mathrm{d}\theta = -i\int_0^{\pi/4}\mathrm{e}^{it^2/\cos^2\theta}\,\mathrm{d}\theta + \frac{i\pi}{4}$$

Par le théorème de Césaro-continu,

$$\frac{1}{T}\int_0^T f^2(t)\mathrm{d}t \xrightarrow{T\to+\infty} I^2$$

De plus,

$$\frac{1}{T}\int_0^T f^2(t)\mathrm{d}t = \underbrace{\frac{-i}{T}\int_0^{\pi/4}\int_0^T \mathrm{e}^{it^2/\cos^2\theta}\,\mathrm{d}t\mathrm{d}\theta}_{:=A_T} + \frac{i\pi}{4}$$

$$A_T = \frac{-i}{T}\int_0^{\pi/4}\int_0^{T/\cos\theta} \mathrm{e}^{-iu^2}\cos\theta\mathrm{d}u\mathrm{d}\theta \overset{u=t/\cos\theta}{=} \frac{-i}{T}\int_0^{\pi/4} f(T/\cos\theta)\cos\theta\mathrm{d}\theta = \frac{-i}{T}\int_0^{\pi/4} f(T/\cos\theta)\cos\theta\mathrm{d}\theta$$

f converge donc est bornée par M, et

$$\left|\frac{-i}{T}\int_0^{\pi/4} f(T/\cos\theta)\cos\theta\mathrm{d}\theta\right| \leq \frac{M}{T}\int_0^{\pi/4}\cos\theta\mathrm{d}\theta \xrightarrow{T\to+\infty} 0$$

Par unicité de la limite, $I^2 = \frac{i\pi}{4}$ et donc $I \in \left\{\mathrm{e}^{i\pi/4}\,\frac{\sqrt{\pi}}{2}, \mathrm{e}^{-i\pi/4}\,\frac{\sqrt{\pi}}{2}\right\}$.
Reste à étudier le signe de $\Im I$:

$$\begin{aligned}
\Im I = \int_0^{+\infty}\sin(x^2)\mathrm{d}x \overset{u=x^2}{=} \int_0^{+\infty}\frac{\sin u}{\sqrt{u}}\mathrm{d}u = \frac{1}{2}\sum_{n\geq 0}\int_{2n\pi}^{2n\pi+2\pi}\frac{\sin u}{\sqrt{u}}\mathrm{d}u &= \frac{1}{2}\sum_{n\geq 0}\left(\int_{2n\pi}^{2n\pi+\pi}\frac{\sin u}{\sqrt{u}}\mathrm{d}u + \int_{2n\pi+\pi}^{2n\pi+2\pi}\frac{\sin u}{\sqrt{u}}\mathrm{d}u\right)\\
&= \frac{1}{2}\sum_{n\geq 0}\left(\int_{2n\pi}^{2n\pi+\pi}\frac{\sin u}{\sqrt{u}}\mathrm{d}u + \int_{2n\pi}^{2n\pi+\pi}\frac{-\sin u}{\sqrt{u-\pi}}\mathrm{d}u\right)\\
&= \frac{1}{2}\sum_{n\geq 0}\int_{2n\pi}^{2n\pi+\pi}\underbrace{\sin u}_{\geq 0}\underbrace{\left(\frac{1}{\sqrt{u}} - \frac{1}{\sqrt{u-\pi}}\right)}_{\geq 0}\mathrm{d}u\\
&\geq 0
\end{aligned}$$

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

10 Nombres de Bell [12] page 12

On note pour $n \in \mathbb{N}^*$, B_n le nombre de partitions de $[\![1, n]\!]$, avec pour convention $B_0 = 1$.

Théorème. *On a la formule*

$$B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_k$$

En notant $f(z) = \sum_{n=0}^{+\infty}\frac{B_n}{n!}z^n$, le rayon de convergence de f est > 0. On peut en déduire que

$$B_k = \frac{1}{\mathrm{e}}\sum_{n=0}^{+\infty}\frac{n^k}{n!}$$

Démonstration. Pour $k \in [\![0, n]\!]$, on considère l'ensemble E_k des partitions de $[\![1, n+1]\!]$ tel que $n+1$ appartient à un ensemble de $k+1$ éléments. On a

$$\operatorname{Card} E_k = \binom{k}{n}B_{n-k}$$

En effet, l'ensemble qui contient $n+1$ est constitué de $n+1$, et de k éléments parmi les n restants, et on complète avec une partition des $(n+1)-(k+1) = n-k$ éléments restant.
$E_0, \dots, E_n$ forment une partition de l'ensemble des partitions de $[\![1, n+1]\!]$. On en déduit donc que

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} = \sum_{k=0}^{n} \binom{n}{k} B_k$$

grâce au changement de variable $k \leftarrow n-k$.
Pour minorer le rayon de convergence R de f, on majore B_n : on montre par récurrence que $B_n \leq n!$.
La propriété est vrai pour $n = 0$. Supposons la propriété vérifiée jusqu'au rang n. Alors,

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k \leq \sum_{k=0}^{n} \binom{n}{k} k! = n! \sum_{k=0}^{n} \frac{1}{(n-k)!} \leq (n+1)!$$

On a donc $\frac{B_n}{n!} \leq 1$ et $R \geq 1$.
On peut alors calculer $f(z)$ pour $z \in]-R, R[$:

$$f(z) = 1 + \sum_{n=0}^{+\infty} \frac{B_{n+1}}{(n+1)!} z^{n+1}$$

En dérivant f, on obtient

$$f'(z) = \sum_{n=0}^{+\infty} \frac{B_{n+1}}{n!} z^n$$

On en déduit de ce qui précède, que

$$f'(z) = \sum_{n=0}^{+\infty} \frac{1}{n!} \left(\sum_{k=0}^{n} \binom{n}{k} B_k \right) z^n = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} \frac{B_k}{k!} \frac{1}{(n-k)!} \right) z^n$$

On reconnaît alors le produit de Cauchy des séries $\sum \frac{B_n}{n!} z^n$ et $\sum \frac{z^n}{n!}$, c'est-à-dire de $f(z)$ et e^z (sur $]-R, R[$). Pour $z \in]-R, R[$, on a donc

$$f'(z) = f(z)\, \mathrm{e}^z$$

donc

$$f(z) = C\, \mathrm{e}^{\mathrm{e}^z} \qquad C > 0$$

Comme $f(0) = B_0 = 1$, on en déduit que $C = \frac{1}{e}$. Finalement, $f(z) = \frac{1}{\mathrm{e}}\, \mathrm{e}^{\mathrm{e}^z} = \mathrm{e}^{\mathrm{e}^z - 1}$.
Pour $z \in \mathbb{C}$, on peut écrire

$$\mathrm{e}^{\mathrm{e}^z} = \sum_{n=0}^{+\infty} \frac{\mathrm{e}^{nz}}{n!} = \sum_{n=0}^{+\infty} \frac{1}{n!} \sum_{k=0}^{+\infty} \frac{(nz)^k}{k!}$$

Par Fubini (la série double de terme général $u_{n,k} = \frac{(nz)^k}{n!k!}$ est absolument sommable), on peut échanger les deux sommes :

$$f(z) = \frac{1}{\mathrm{e}} \sum_{n \geq 0} \left(\sum_{k \geq 0} u_{n,k} \right) = \frac{1}{\mathrm{e}} \sum_{k \geq 0} \left(\sum_{n \geq 0} u_{n,k} \right) = \sum_{k \geq 0} \left(\frac{1}{\mathrm{e}} \sum_{n \geq 0} \frac{n^k}{n!} \right) \frac{z^k}{k!}$$

Par l'unicité du développement en série entière, on obtient que pour $k \in \mathbb{N}$,

$$B_k = \frac{1}{\mathrm{e}} \sum_{n \geq 0} \frac{n^k}{n!}$$

□

11 Théorème de Frobénius-Zolotarev [18] page 251

Théorème (Frobénius-Zolotarev)**.** *Soit $p \neq 2$ un nombre premier, et V un $\mathbb{F}_p$-espace vectoriel de dimension finie. Alors, pour tout $u \in \mathrm{GL}(V)$,*

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

où ε désigne la signature de u vu comme permutation.

Démonstration.

1. Tout morphisme $\varphi : \mathrm{GL}(V) \longrightarrow M$ où M est un groupe abélien, se factorise par le déterminant. Comme $p \neq 2$, $D(\mathrm{GL}_n(k)) = \mathrm{SL}_n(k)$. Le morphisme φ se factorise donc en $\tilde{\varphi} : \mathrm{GL}_n(k)/\mathrm{SL}_n(k) \longrightarrow M$, avec $\varphi = \tilde{\varphi} \circ \pi$ où π est la projection canonique sur $\mathrm{SL}_n(k)$. Comme det est un morphisme de $\mathrm{GL}(V)$ dans $k^\times$, il se factorise en $\overline{\det} : \mathrm{GL}(V)/\mathrm{SL}(V) \longrightarrow k^\times$, et cette factorisation est même un isomorphisme. On peut alors écrire :

   $$\varphi = \left(\tilde{\varphi} \circ (\overline{\det})^{-1}\right) \circ \det$$

   $\delta = \tilde{\varphi} \circ (\overline{\det})^{-1}$ convient. L'unicité provient de la surjectivité du déterminant. Supposons δ' tel que $\varphi = \delta' \circ \det$. Soit $x \in \mathbb{F}_p^\times$, il existe a tel que $x = \det(a)$. On a alors

   $$\delta'(x) = \delta' \circ \det(a) = \varphi(a) = \delta \circ \det(a) = \delta(x)$$

   donc $\delta = \delta'$.
2. Le symbole de Legendre est l'unique morphisme non-trivial de $\mathbb{F}_p^\times$ dans $\{\pm 1\}$.
   Le symbole de Legendre est bien non-trivial car certains éléments ne sont pas des carrés.
   Réciproquement, soit $\alpha : \mathbb{F}_p^\times \longrightarrow \{\pm 1\}$. $H = \ker \alpha$ est un sous-groupe d'indice 2. H est unique et on peut donc écrire $\mathbb{F}_p^\times = H \cup xH$ avec $x \notin H$. $\alpha(y) = 1$ si $y \in H$ et $\alpha(y) = -1$ si $y \in xH$. α est alors entièrement déterminé et c'est le symbole de Legendre.
3. Le morphisme $\varepsilon : \mathrm{GL}(V) \longrightarrow \{\pm 1\}$ se factorise (par 1.) en $\delta \circ \det$. Il reste à montrer que ε est non-trivial (ce sera alors le symbole de Legendre).
   $\mathbb{F}_p$ est inclu dans $\mathbb{F}_{p^d}$ (où $d = \dim(V)$). V et $\mathbb{F}_{p^d}$ sont des $\mathbb{F}_p$-espaces vectoriels isomorphes. Prenons g un générateur de $(\mathbb{F}_{p^d})^\times$ (qui est cyclique). La permutation $x \mapsto gx$ fixe 0 et agit comme le cycle $(g, g^2, \ldots, g^{p^d-1})$. La signature est donc $(-1)^{p^d} = -1$ et cette permutation est bien un élément de $\mathrm{GL}(\mathbb{F}_{p^d})$.

□

12 Sous-groupes distingués et caractères [17] page 158

Définition (noyau d'un caractère)**.** Soit G un groupe, et χ un caractère associé à une représentation de G. On définit le noyau de χ comme étant $\ker \chi := \{g \in G, \chi(g) = \chi(e)\}$.

Lemme. *Soit G un groupe fini, $\rho : G \longrightarrow \mathrm{GL}(V)$ une représentation et χ le caractère associé. Pour $g \in G$, on a $|\chi(g)| \leq \chi(e)$ et $\chi(g) = \chi(e) \iff g \in \ker(\rho)$ (c'est-à-dire $\ker \chi = \ker \rho$).*

Démonstration. La matrice $\rho(g)$ est diagonalisable car le groupe est fini (disons d'ordre N) donc $g^N = e$ et $\mathrm{id} = \rho(e) = \rho(g)^N$ donc $X^N - 1$ est un polynôme annulateur de $\rho(g)$ et ses racines sont simples. Les valeurs propres de $\rho(g)$ sont des racines de l'unité donc de module 1. Comme $\chi(g) = \sum_{j=1}^{\dim(V)} \lambda_j$, on a

$$|\chi(g)| = \left|\sum_{j=1}^{\dim(V)} \lambda_j\right| \leq \sum_{j=1}^{\dim(V)} |\lambda_j| = \dim(V) = \chi(e)$$

$\chi(g) = \chi(e)$ si, et seulement si, tous les λ_i sont égaux à 1 si, et seulement si, $\rho(g) = \mathrm{id}$ si, et seulement si, $g \in \ker \rho$. □

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

$$\bigcap_{j\in J} \ker \chi_j \qquad J \subset [\![1, m]\!]$$

Démonstration.

1. Soit $H \lhd G$. Montrons que c'est le noyau d'un caractère.
   On considère l'action de G par translation à gauche sur G/H, qui donne lieu à un morphisme $\varphi : G \longrightarrow \mathfrak{S}_{|G/H|}$. Soit χ le caractère associé. Comme $\ker\varphi = H$, on obtient par le lemme que $\ker\chi = H$. Il en résulte que tout sous-groupe distingué est le noyau d'un caractère.
2. On exprime ensuite les noyaux de caractères en fonction des noyaux des caractères irréductibles. On décompose $V = \oplus_i V_i$ et χ_i les caractères irréductibles associés. On a alors

   $$g \in \ker\chi \iff g \in \ker\rho \iff \forall i, g \in \ker\rho_{|V_i} \iff \forall i, g \in \ker\chi_i$$

   donc $\ker\chi = \bigcap_i \ker\chi_i$.

□

13 Nombres de polynômes irréductibles sur $\mathbb{F}_q$ [11] page 93–189

Lemme (fonction de Möbius)**.** *On rappelle que la fonction de Möbius μ est la fonction multiplicative définie sur $\mathbb{N}^*$ par $\mu(1) = 1$, $\mu(n) = 0$ si n a un facteur carré, et $\mu(q_1 \dots q_r) = (-1)^r$ si les q_j sont premiers distincts.*

1. *μ est multiplicative, i.e si $n \wedge m = 1$, alors $\mu(nm) = \mu(n)\mu(m)$.*
2. *Pour $n > 1$, $\sum_{d|n} \mu(d) = 0$.*
3. *Si $g(n) = \sum_{d|n} f(d)$, alors,*

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

Démonstration.

1. Si n ou m a un facteur carré, alors nm aussi, et on a bien l'égalité puisque $\mu(nm) = 0 = \mu(n)\mu(m)$. Sinon, on écrit $n = \prod_{i=1}^r p_i$ et $m = \prod_{j=1}^s q_j$. Comme n et m sont premiers entre eux, $p_i \neq q_j$ pour tous i, j. On a finalement $\mu(nm) = (-1)^{r+s}$ et $\mu(n)\mu(s) = (-1)^r(-1)^s = (-1)^{r+s}$.
2. On décompose $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Alors,

   $$\sum_{d|n} \mu(d) = \sum_{k=0}^{r} \sum_{i_1<\dots<i_k} \mu(p_{i_1} \dots p_{i_k}) = \sum_{k=0}^{r} \sum_{i_1<\dots<i_k} (-1)^k = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = (1-1)^r = 0$$

   car $r > 0$.
3. On calcule :

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

   L'autre égalité s'obtient par un changement de variables dans la somme.

□

Proposition. *Soit $\mathbb{F}_q$ un corps fini de cardinal q. Pour $n \in \mathbb{N}^*$, il existe un polynôme irréductible sur $\mathbb{F}_q$ de degré n. Le nombre de tels polynômes est équivalent à $\frac{q^n}{n}$ quand $n \to +\infty$.*

Démonstration. On note $A(n,q)$ l'ensemble des polynômes irréductibles unitaire de degré n sur $\mathbb{F}_q$, et $I(n,q) = \#A(n,q)$. On commence par montrer que

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

Soit d un diviseur de n et $P \in A(d,q)$. Montrons que $P \mid X^{q^n} - X$. On pose $K = \mathbb{F}_q[X]/(P)$ un corps de rupture de P, et on note x la classe de X dans K. Comme $[K : P] = \deg(P) = d$, K est isomorphe à $\mathbb{F}_{q^d}$ et donc $x^{q^d} = x$. On en déduit que

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

donc $P \mid X^{q^n} - X$.
Inversement, montrons que si P est un diviseur irréductible de $X^{q^n} - X$, alors le degré d de P divise n. Le polynôme $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$. Notons x une racine de P dans $\mathbb{F}_{q^n}$, et $K = \mathbb{F}_q(x)$. K est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$, et on a $[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K][K : \mathbb{F}_q]$ d'où $d \mid n$.
On a finalement :

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

En passant au degré, on obtient

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

Par la formule d'inversion de Möbius, on obtient :

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

En notant $r_n = \sum_{d|n, d \neq n} \mu(\frac{n}{d}) q^d$, on a donc

$$nI(n,q) = q^n + r_n$$

On peut ensuite majorer grossièrement $|r_n|$:

$$|r_n| \leq \sum_{d=0}^{\lfloor \frac{n}{2} \rfloor} q^d = q \frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1}$$

Comme $|r_n| < q^n$, $I(n,q) > 0$ et il y a des polynômes irréductibles de tout degré. De plus, $|r_n| = O(q^{\lfloor \frac{n}{2} \rfloor}) = o(q^n)$. D'où

$$I(n,q) \sim \frac{q^n}{n} \qquad n \to +\infty$$

□

14 Irréductibilité des polynômes cyclotomiques [7] page 82

Théorème. *Le polynôme cyclotomique $\varphi_n(X)$ ($\in \mathbb{Z}[X]$) est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.*

Démonstration. Soit K un corps de décomposition de φ_n sur $\mathbb{Q}$, et $\zeta \in K$ une racine n-ème primitive de 1. Soit p un nombre premier, ne divisant pas n.

1. ζ^p est une autre racine primitive de 1. En effet, les générateurs de $\mu_n(K)$ sont les ζ^m avec m premier avec n.
2. Soit $f \in \mathbb{Q}[X]$ (resp. g) le polynôme minimal de ζ (resp. ζ^p) sur $\mathbb{Q}$. Alors, on a $f, g \in \mathbb{Z}[X]$. En effet, comme $\mathbb{Z}[X]$ est factoriel, on a

$$\varphi_n(X) = \prod_{i=1}^{r} f_i(X)^{\alpha_i} \qquad f_i \in \mathbb{Z}[X] \text{ irréductible}$$

   Comme φ_n est unitaire, il en est de même pour les f_i (quitte à multiplier f_i par -1). Mais alors ζ est racine de l'un des f_i, et f_i est unitaire et irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$, donc $f_i = f$. De même pour g. On note au passage que f et g divisent φ_n, dans $\mathbb{Z}[X]$.
3. On montre que $f = g$.
   Par l'absurde, supposons $f \neq g$. Comme ils sont irréductibles et distincts, le produit fg divise φ_n dans $\mathbb{Z}[X]$. Comme $g(\zeta^p) = 0$, ζ est racine de $g(X^p)$, donc $f(X)$ divise $g(X^p)$, a priori dans $\mathbb{Q}[X]$, mais aussi dans $\mathbb{Z}[X]$:

$$g(X^p) = f(X)h(X) \qquad h \in \mathbb{Z}[X]$$

   (si $h \in \mathbb{Q}[X]$, on écrit $h = \frac{a}{b}h'$ et on utilise le lemme de Gauss)
   On projète alors sur $\mathbb{F}_p$:

$$g(X) = a_r X^r + \ldots + a_0 \qquad a_i \in \mathbb{Z}$$
$$g(X^p) = a_r X^{pr} + \ldots + a_1 X^p + a_0$$

   mais modulo p, on a $\bar{a}_i = \bar{a}_i^p$ donc

$$\bar{g}(X^p) = (\bar{a}_r X^r + \ldots + \bar{a}_0)^p = \bar{g}(X)^p$$

   Soit alors $\varphi(X)$ un facteur irréductible de $\bar{f}(X)$ sur $\mathbb{F}_p$. On a $\bar{g}(X)^p = \bar{f}(X)\bar{h}(X)$ donc par le lemme d'Euclide, φ divise $\bar{g}$.
   Comme fg divise φ_n dans $\mathbb{Z}[X]$, $\bar{f}\bar{g}$ divise $\bar{\varphi}_n$ dans $\mathbb{F}_p[X]$. Donc φ^2 divise $\bar{\varphi}_n$. Mais alors dans un corps de décomposition de φ_n sur $\mathbb{F}_p$, $\bar{\varphi}_n$ aura une racine double. Absurde car φ_n n'a que des racines simples (car p ne divise pas n).
4. $f = \varphi_n$.
   Si ζ' est une racine primitive m-ème, on a $\zeta' = \zeta^m$ avec $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ et p_i ne divise pas n. Par ce qui précède, ζ' et ζ ont même polynôme minimal sur $\mathbb{Q}$, donc $f(\zeta') = 0$, de sorte que f admet toutes les racines primitives de l'unité comme zéro. Donc $\deg(f) \geq \varphi(n)$, mais f divise φ_n donc finalement, $f = \varphi_n$.
   Il en résulte que φ_n est irréductible sur $\mathbb{Q}$ donc sur $\mathbb{Z}$ puisque le contenu de φ_n est 1 (car il est unitaire).

□

15 Table de $\mathfrak{S}_4$ [9] page 46

15.1 Classes de conjugaison

On commence par dénombrer les classes de conjugaison dans $\mathfrak{S}_4$:
— L'identité e est seule dans sa classe
— Les transpositions forment une classe dont un représentant est (12).
  Son nombre d'éléments est $\frac{4\times3}{2} = 6$.
— Les 3-cycles forment une classe dont un représentant est (123).
  Son nombre d'éléments est $\frac{4\times3\times2}{3} = 8$.

— Les 4-cycles forment une classe dont un représentant est (1234).
Son nombre d'éléments est $\frac{4\times3\times2\times1}{4} = 6$.
— Les double-transpositions à support disjoint forment une classe dont un représentant est (12)(34).
Son nombre d'éléments est $\frac{\frac{4\times3}{2}}{2} = 3$.

Il y a donc 5 caractères irréductibles qu'on va désormais déterminer.

15.2 Deux représentations de degré 1 faciles à trouver

La représentation triviale est une première représentation irréductible

$$\rho_t : g \in \mathfrak{S}_4 \mapsto 1 \in \mathrm{GL}_1(\mathbb{C})$$

et donne le caractère $\chi_t : g \mapsto \mathrm{Tr}(1) = 1$.
On obtient la première ligne :

	e	(12)	(123)	(1234)	(12)(34)
χ_t	1	1	1	1	1

Une deuxième représentation de degré 1 est la représentation associée à la signature :

$$\rho_s : g \in \mathfrak{S}_4 \mapsto \mathrm{sgn}(g) \in \mathrm{GL}_1(\mathbb{C})$$

On obtient la seconde ligne :

	e	(12)	(123)	(1234)	(12)(34)
χ_s	1	-1	1	-1	1

15.3 Une représentation de degré 3 par action de $\mathfrak{S}_4$ sur un tétraèdre régulier

L'action de $\mathfrak{S}_4$ sur les sommets d'un tétraèdre régulier donne un isomorphisme

$$\mathfrak{S}_4 \simeq \mathrm{Is}(T)$$

On obtient une représentation

$$\rho_T : \mathfrak{S}_4 \longmapsto \mathrm{GL}_3(\mathbb{C})$$

En prenant O le barycentre du tétraèdre $ABCD$, et $(\overrightarrow{OA}, \overrightarrow{OB}, \overrightarrow{OC})$ comme base de $\mathbb{R}^3$, on obtient que

$$e \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (12) \longmapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (123) \longmapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$(1234) \longmapsto \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix} \qquad (12)(34) \longmapsto \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix}$$

Le point D a pour coordonnées dans la base choisie $(-1,-1,-1)$ par définition du barycentre du tétraèdre O.
On vérifie que cette le caractère associé est irréductible :

$$\langle \chi_T, \chi_T \rangle = \frac{1}{24}(3^2 + 6.1^2 + 8.0^2 + 6.(-1)^2 + 3.(-1)^2) = 1$$

On obtient alors la troisème ligne :

	e	(12)	(123)	(1234)	(12)(34)
χ_T	3	1	0	-1	-1

15.4 Une représentation de degré 3 par action de $\mathfrak{S}_4$ sur un cube

L'action de $\mathfrak{S}_4$ sur les grandes diagonales d'un cube donne un isomorphisme

$$\mathfrak{S}_4 \simeq \mathrm{Is}^+(C)$$

On obtient une représentation

$$\rho_C : \mathfrak{S}_4 \longmapsto \mathrm{GL}_3(\mathbb{C})$$

Les matrices associées aux éléments de $\mathfrak{S}_4$ sont des rotations, et on prend ensuite leur trace $(1+2\cos\theta)$ pour en déduire le caractère.

$$e \longmapsto r_0 \qquad (12) \longmapsto r_\pi \qquad (123) \longmapsto r_{2\pi/3} \qquad (1234) \longmapsto r_{\pi/2} \qquad (12)(34) \longmapsto r_\pi$$

Pour la transposition (12)*, l'axe de la rotation est la droite qui passe par les milieux des côtés du cube qui contiennent les points des deux diagonales concernées.*
Pour le 3*-cycle* (123)*, l'axe de la rotation est la droite n°* 4*.*
Pour le 4*-cycle* (1234) *et pour la double transposition* (12)(34)*, l'axe de rotation est l'axe vertical passant par le milieu du cube.*
On vérifie que cette le caractère associé est irréductible :

$$\langle \chi_C, \chi_C \rangle = \frac{1}{24}(1.3^2 + 6.(-1)^2 + 8.0^2 + 6.(1)^2 + 3.(-1)^2) = 1$$

On obtient alors la quatrième ligne :

	e	(12)	(123)	(1234)	(12)(34)
χ_C	3	-1	0	1	-1

15.5 La dernière représentation

On peut déjà déterminer le degré n (du dernier caractère χ_d) par la formule :

$$\sum_\rho \deg(\rho)^2 = 24$$

On obtient $1^2 + 1^2 + 3^2 + 3^2 + n^2 = 24$ donc $n = 2$.
On obtient la dernière ligne en utilisant l'orthogonalité des colonnes. Finalement,

$\mathfrak{S}_4$	e	(12)	(123)	(1234)	(12)(34)
χ_t	1	1	1	1	1
χ_s	1	-1	1	-1	1
χ_T	3	1	0	-1	-1
χ_C	3	-1	0	1	-1
χ_d	2	0	-1	0	2

16 Partition d'un entier en parts fixées [15] page 197

Théorème. *Soient $a_1, \ldots, a_k$ des entiers naturels non-nuls premiers entre eux. Pour $n \geq 1$, on note u_n le nombre de k-uplets $(x_1, \ldots, x_k) \in \mathbb{N}^k$ tels que $a_1x_1 + \ldots + a_kx_k = n$. Alors,*

$$u_n \sim \frac{1}{a_1 \ldots a_k} \frac{n^{k-1}}{(k-1)!} \qquad n \to +\infty$$

Démonstration. Les séries $\sum_{x_i \in \mathbb{N}} z^{x_i a_i}$ (pour $1 \leq i \leq k$) ont toute pour rayon de convergence 1. Considérons le produit de Cauchy de ces k séries entières : le coefficient de z^n dans ce produit de Cauchy est $\sum_{(x_1,\ldots,x_k)\in\mathbb{N}^k, \sum x_i a_i = n} 1 = u_n$.
On considère alors pour $|z| < 1$,

$$f(z) = \sum_{n=0}^{+\infty} u_n z^n = \prod_{i=1}^{k} \left(\sum_{n \geq 0} z^{a_i x_i} \right) = \prod_{i=1}^{k} \frac{1}{1 - z^{a_i}}$$

f est la série génératrice de la suite $(u_n)_n$. Ses pôles sont les racines a_1-ièmes, ..., a_k-ièmes de l'unité. Le pôle 1 est de multiplicité k, et tous les autres sont de multiplicité $< k$. En effet, par le théorème de Bézout, il existe $v_1, \ldots, v_k$ tels que $a_1 v_1 + \ldots + a_k v_k = 1$. Si ω vérifie $\omega^{a_i} = 1$ pour $1 \leq i \leq k$, alors on a

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

Si on note $P = \{\omega_1, \omega_2, \ldots, \omega_p\}$ les pôles de f (avec $\omega_1 = 1$), alors en décomposant f en éléments simples, on obtient pour $|z| < 1$,

$$f(z) = \frac{\alpha}{(z-1)^k} + \sum_{2 \leq i \leq p, 1 \leq j \leq k-1} \frac{c_{ij}}{(\omega_i - z)^j}$$

Pour $\omega \in P$ et $j \in \mathbb{N}$, la fonction $z \mapsto \frac{1}{(\omega - z)^j}$ est développable en série entière de rayon de convergence 1. Ses coefficients s'obtiennent en dérivant $j-1$ fois le développement en série entière de la fonction $z \mapsto \frac{1}{\omega - z}$. On a pour $|z| < 1$,

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

puis pour $j \leq k-1$,

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

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

On déduit de ce qui précède le coefficient u_n de z^n dans les différents développements en série entière :

$$u_n = \alpha \binom{n+k-1}{n} + \sum_{2 \leq i \leq p, 1 \leq j \leq p-1} c_{ij} \binom{n+j-1}{n} \omega^{-n-j}$$

Le premier terme correspond correspond au développement de $\frac{1}{(1-z)^k}$, et est équivalent quand $n \to +\infty$, à $\alpha \frac{n^{k-1}}{(k-1)!}$. Les autres termes sont négligeables devant n^{k-1}. Donc

$$u_n \sim \alpha \frac{n^{k-1}}{(k-1)!} \qquad n \to +\infty$$

On calcule α en multipliant $f(z)$ par $(1-z)^k$ et en faisant $z = 1$. On obtient :

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

et donc $\alpha = \frac{1}{a_1 \ldots a_k}$. Finalement,

$$u_n \sim \frac{1}{a_1 \ldots a_k} \frac{n^{k-1}}{(k-1)!} \qquad n \to +\infty$$

□

17 Décomposition de Dunford [3] page 194

Théorème (décomposition de Dunford)**.** *Soit E un k-espace vectoriel de dimension $n \in \mathbb{N}^*$, et f un endomorphisme de E tel que χ_f soit scindé. Alors, il existe un unique couple (d,n) d'endomorphismes de E tel que $u = d+n$ avec $dn = nd$, d diagonalisable, n nilpotent. De plus, d et n sont des polynômes en u.*

Lemme. *Soit f un endomorphisme de E, et F un polynôme annulateur de f, $F = \beta M_1^{\alpha_1} \dots M_s^{\alpha_s}$. On note $N_i = \ker M_i^{\alpha_i}(f)$. Alors, $E = \oplus_{i=1}^s N_i$ et les projecteurs sur N_i parallèlement à $\oplus_{j\neq i} N_j$ sont des polynômes en u.*

Démonstration. Par le lemme des noyaux, on a $E = \oplus_{i=1}^s N_i$. On note $Q_i = \prod_{j\neq i} M_j^{\alpha_j}$. Les Q_i sont premiers entre eux, donc par Bézout, il existe $U_1, \dots, U_s$ tels que

$$\sum_{i=1}^{s} U_i Q_i = 1$$

On obtient l'égalité sur les polynômes d'endomorphismes :

$$\sum_{i=1}^{s} U_i(f) \circ Q_i(f) = \mathrm{id}_E$$

On note alors $P_i = U_i Q_i$ et $p_i = P_i(f) = U_i(f) \circ Q_i(f)$.
On va montrer que les p_i sont les projecteurs recherchés. On a déjà l'égalité $\mathrm{id}_E = \sum_{i=1}^s p_i$. Pour $i \neq j$,

$$p_i(f) \circ p_j(f) = U_i U_j(f) \circ Q_i Q_j(f) = 0$$

car $Q_i Q_j$ est divisible par F, qui annule f.
On en déduit en appliquant p_i sur l'égalité précédente que $p_i = p_i^2$ et p_i est un projecteur.
On montre désormais que $\Im(p_i) = N$. Si $y \in \Im(p_i)$, $y = p_i(x)$. On a alors

$$M_i^{\alpha_i}(f)(y) = M_i^{\alpha_i}(f)(p_i(x)) = M_i^{\alpha_i} U_i(f) Q_i(f)(x) = 0$$

car $F = M_i^{\alpha_i} Q_i$ annule f. Réciproquement, si $x \in N$, $x = \sum p_j(x) = p_i(x) \in \Im(p_i)$.
Donc p_i projète bien sur N_i. Montrons qu'il projète parallèlement à $\oplus_{j\neq i} p_j$: soit $x \in N_j$ pour un $j \neq i$.

$$p_i(x) = U_i(f) Q_i(f)(x) = 0$$

Par définition, les p_i sont des polynômes en f, ce qui termine la preuve. □

Démonstration. On applique le lemme à $F = \chi_f$. Les N_i sont les sous-espaces caractéristiques.
On pose $d = \sum_i \lambda_i p_i$ où les λ_i sont les valeurs propres de f. d est bien diagonale. On pose de plus $n = f - d$. On a

$$n = \sum_{i=1}^{s} (f - \lambda_i \mathrm{id}) p_i$$

Comme $p_i \circ p_j = 0$ et $p_i^2 = p_i$, on a donc

$$n^q = \sum (f - \lambda_i \mathrm{id})^q p_i$$

En prenant $q = \max \alpha_i$, n est bien nilpotent.
Pour l'unicité, supposons $f = d+n = d'+n'$. d' commute avec n', donc commute aussi avec $f = d'+n'$. Comme d est un polynôme en f, d commute avec d'. Donc d et d' sont codiagonalisables et $d - d'$ est diagonalisable. De même, n et n' commutent et $n' - n$ est nilpotent. Finalement, $d - d' = n' - n$ est diagonalisable et nilpotent donc nul. □

18 Demi-plan de Poincaré [6] page 569

Définition. On note $\mathbb{H}$ le demi-plan de Poincaré, c'est-à-dire $\mathbb{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$. On définit l'ensemble des droites hyperboliques comme étant les droites verticales à l'axe réel, et les cercles dont le centre est sur l'axe réel.

Lemme. *Soit $z, w \in \mathbb{H}$. Il existe une unique droite hyperbolique passant par z et w.*

Démonstration. On considère le cercle $\mathscr{C}$ passant par z, w, et $\bar{z}$. Comme il est clair que $[z, w, \bar{z}, \bar{w}] \in \mathbb{R}$ (il suffit de conjuguer pour le vérifier), ce cercle passe aussi par $\bar{w}$. Son symétrique $\overline{\mathscr{C}}$ par rapport à l'axe réel passe donc aussi par ces quatre points, et on obtient que $\mathscr{C} = \overline{\mathscr{C}}$. Donc $\mathscr{C}$ est soit une droite verticale, soit un cercle de centre réel. L'intersection de $\mathbb{H}$ et de $\mathscr{C}$ est la droite hyperbolique recherchée. L'unicité provient du fait que deux droites hyperboliques distinctes ont au plus un point commun. □

Théorème.

1. $\mathrm{PSL}_2(\mathbb{R})$ *agit transitivement sur* $\mathbb{H}$.
2. $\mathrm{PSL}_2(\mathbb{R})$ *agit transitivement sur les droites hyperboliques.*

Démonstration. Deux matrices M et N donnent la même homographie si, et seulement si, $\exists \lambda \in \mathbb{R}$ tel que $M = \lambda N$. Ainsi, $\mathrm{PSL}_2(\mathbb{R}) = \{h \in \mathrm{PGL}_2(\mathbb{R}), \det(h) > 0\}$.

1. Soit $z \in \mathbb{H}$ et $h : z \mapsto \frac{az+b}{cz+d} \in \mathrm{PSL}_2(\mathbb{R})$. En posant $z = x + iy$, on a

$$h(z) = \frac{ax + b + iay}{cx + d + icy} = \frac{(ax + b + iay)(cx + d - icy)}{(cx + d + icy)(cx + d - icy)}$$

$$= \frac{acx^2 + adx - icaxy + bcx + bd - icby + iacxy + iady + acy^2}{(cx + d)^2 + (cy)^2}$$

   et $\Im(h(z))$ est du signe de $-bcy + ady = (ad - bc)\Im(z) > 0$.
   Pour la transitivité, on remarque que les translations et les homothéties de rapport positif sont dans $\mathrm{PSL}_2(\mathbb{R})$.

2. Comme les homographies conservent les droites et cercles, on a une action de $\mathrm{PGL}_2(\mathbb{R})$ sur les droites ou cercles de $\mathbb{P}^1(\mathbb{C})$. Par 1., on a donc une action de $\mathrm{PSL}_2(\mathbb{R})$ sur les droites hyperboliques.
   Soit $z \in \mathbb{H}$, et D une droite hyperbolique passant par z. Par 1., il existe $g \in \mathrm{PSL}_2(\mathbb{R})$ tel que $g(z) = i$. Donc $g(D)$ est une droite hyperbolique passant par i.
   Soit D_i une droite hyperbolique passant par i, différente de $i\mathbb{R}_+^*$. C'est un demi-cercle coupant l'axe réel en deux points. Choisissons-en un : t. On peut trouver $\theta \in]-\pi/2, \pi/2[$ tel que $\tan(\theta) = t$.
   On note alors h_θ l'homographie de matrice

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

   h_θ fixe i car $h_\theta(i) = \frac{\cos\theta i - \sin\theta}{\sin\theta i + \cos\theta} = (\cos\theta i - \sin\theta)(\cos\theta - i\sin\theta) = i\cos^2\theta + i\sin^2\theta = i$.
   $h_\theta(t) = 0$ car $h_\theta(t) = \frac{\cos\theta t - \sin\theta}{\sin\theta t + \cos\theta} = \frac{\sin\theta - \sin\theta}{\sin\theta t + \cos\theta} = 0$.
   Donc $h_\theta(\overline{D_i}) = i\mathbb{R}_+$.
   On peut donc envoyer toute droite hyperbolique sur $i\mathbb{R}_+^*$ et l'action est transitive.

□

19 Automorphismes de $K(X)$ [12] page 224

Théorème. *Soit K un corps. Les automorphismes de la K-algèbre $K(X)$ sont les homographies.*

Démonstration. Soit φ un tel automorphisme.
On commence par déterminer l'image d'un polynôme de $K[X]$: soit $P = \sum_k a_k X^k$,

$$\varphi(P) = \sum_k a_k \varphi(X)^k = P \circ F \qquad F = \varphi(X)$$

Soit maintenant $G = \frac{P}{Q} \in K(X)$.

$$\varphi(P) = \varphi\left(\frac{P}{Q} \times Q\right) = \varphi\left(\frac{P}{Q}\right)\varphi(Q)$$

donc

$$\varphi(G) = \frac{\varphi(P)}{\varphi(Q)} = \frac{P \circ F}{Q \circ F} = G \circ F$$

On note maintenant $\varphi_F : G \mapsto G \circ F$ le morphisme de la K-algèbre $K(X)$. On cherche les conditions sous lesquelles φ_F est un automorphisme.

Condition nécessaire Si φ_F est un automorphisme, alors il existe $G = \frac{P}{Q}$ (avec $P \wedge Q = 1$) tel que $\varphi_F(G) = X$. On note $F = \frac{A}{B}$ (avec $A \wedge B = 1$), et

$$P = \sum_{k=0}^{p} a_k X^k \qquad Q = \sum_{k=0}^{q} b_k X^k$$

$$G \circ F = X \iff P \circ F = X(Q \circ F) \iff \sum_{k=0}^{p} a_k F^k = X \sum_{k=0}^{q} b_k F^k \iff \sum_{k=0}^{p} a_k \frac{A^k}{B^k} = X \sum_{k=0}^{q} b_k \frac{A^k}{B^k}$$

En notant $m = \max(p, q)$, on obtient

$$\sum_{k=0}^{p} a_k A^k B^{m-k} = X \sum_{k=0}^{q} b_k A^k B^{m-k}$$

En isolant le terme pour $k = 0$, on obtient que $A \mid (a_0 - b_0 X)B^m$. Par le lemme de Gauss, $A \mid a_0 - b_0 X$. Donc $\deg(A) \leq 1$ (et le couple (a_0, b_0) n'est pas nul car sinon P et Q ne seraient pas premiers entre eux).
En isolant le terme pour k maximal, on obtient de même que
— Si $m = q = p$, $B \mid a_p - b_p X$, et le couple (a_p, b_p) est non-nul car P est de degré p.
— Si $m = q > p$, $B \mid b_q X$, et $b_q \neq 0$
— Si $m = p > q$, $B \mid a_p$ et $a_p \neq 0$
Dans tous les cas, $\deg(B) \leq 1$.
On en déduit que $F = \frac{aX+b}{cX+d}$ avec $a, b, c, d \in K$. Comme F n'est pas constant (sinon φ_F n'est pas surjectif), $F' \neq 0$ donc $\underline{ad - bc \neq 0}$.

Condition suffisante Soit $a, b, c, d \in K$ tels que $ad - bc \neq 0$. On note $\varphi_{a,b,c,d} : X \mapsto \frac{aX+b}{cX+d}$. C'est bien un automorphisme car on peut faire agir $\mathrm{GL}_2(K)$ sur K^2 pour obtenir les homographies : $\varphi_{a,b,c,d}$ provient de l'action de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Comme la matrice est inversible, on obtient l'inverse de $\varphi_{a,b,c,d}$ en faisant agir l'inverse de cette matrice.

□

20 Borne de Bézout [16] page 592

Remarque. C'est beaucoup moins détaillé dans [16] qu'ici!

Théorème. *Soit k un corps commutatif de cardinal infini, et $A, B \in k[X,Y]$ de degrés totaux respectifs m et n. Si A et B sont premiers entre eux, alors $\#(Z(A) \cap Z(B)) \leq mn$.*

Démonstration. Si A et B n'ont pas de racine commune, le résultat est évident et dans toute la suite, on suppose que $Z(A) \cap Z(B)$ est non vide.
On note $R_Y = \mathrm{Res}_Y(A,B)$ et $R_X = \mathrm{Res}_X(A,B)$. Pour $(x,y) \in Z(A) \cap Z(B)$, on a $R_Y(x) = R_X(y) = 0$. Comme A et B sont premiers entre eux, R_Y est un polynôme non-nul de $k[X]$ et a donc au plus $\deg(R_Y)$ racines. En raisonnant de même pour R_X, on obtient que

$$\#(Z(A) \cap Z(B)) \leq \deg(R_X)\deg(R_Y)$$

On note désormais

$$A(X,Y) = \sum_{k=0}^{p} a_k(X)Y^k \qquad B(X,Y) = \sum_{k=0}^{q} b_k(X)Y^k$$

où $\deg a_k \leq m-k$ et $\deg b_k \leq n-k$.
On a alors,

$$R_Y = \begin{vmatrix} a_p & \cdots & \cdots & \cdots & a_0 & & 0 \\ & \ddots & & & & \ddots & \\ 0 & & a_p & \cdots & \cdots & \cdots & a_0 \\ b_q & \cdots & \cdots & b_0 & & & 0 \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ 0 & & & b_q & \cdots & \cdots & b_0 \end{vmatrix}$$

En notant $\mathcal{M}$ la matrice, on a

$$\forall i \in [\![1,q]\!] \qquad \mathcal{M}_{ij} = \begin{cases} a_{p-(j-i)} & \text{si } 0 \leq j-i \leq p \\ 0 & \text{sinon} \end{cases}$$

d'où $\deg \mathcal{M}_{ij} \leq m-p+j-i$.

$$\forall i \in [\![q+1, q+p]\!] \qquad \mathcal{M}_{ij} = \begin{cases} b_{i-j} & \text{si } i-q \leq j \leq p-q+i \\ 0 & \text{sinon} \end{cases}$$

d'où $\deg \mathcal{M}_{ij} \leq n-i+j$.
On obtient alors par la formule générale du déterminant :

$$R_Y = \sum_{\sigma \in \mathfrak{S}_{p+q}} \varepsilon(\sigma) \prod_{i=1}^{p+q} \mathcal{M}_{i,\sigma(i)}$$

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

$$\begin{aligned} \deg\left(\varepsilon(\sigma)\prod_{i=1}^{p+q}\mathcal{M}_{i,\sigma(i)}\right) = \sum_{i=1}^{p+q}\deg \mathcal{M}_{i,\sigma(i)} &= \sum_{i=1}^{q} m-p+\sigma(i)-i + \sum_{i=q+1}^{q+p} n-i+\sigma(i) \\ &= qm-qp+pn = mn + \underbrace{(m-p)(q-n)}_{\leq 0} \leq mn \end{aligned}$$

donc $\deg R_Y \leq mn$, et de même, $\deg R_X \leq mn$. Donc $\#(V(A) \cap V(B)) \leq (mn)^2$.
On note ensuite (x_i, y_i) les élements de $Z(A) \cap Z(B)$ (avec $i \in [\![1,r]\!]$), et on pose

$$\mathcal{E} = \left\{ \frac{x_i - x_j}{y_j - y_i}, y_i \neq y_j, i,j \in [\![1,r]\!] \right\}$$

Comme $\#k^\times$ est infini, on peut trouver $u \in k^\times \backslash \mathcal{E}$, et donc on a

$$\forall i,j \in [\![1,r]\!] \qquad x_i - x_j \neq u(y_j - y_i) \iff x_i + uy_i \neq x_j + uy_j$$

On effectue alors le changement de variables :

$$X' = X + uY \qquad Y' = Y$$

On note $\tilde{A}(X',Y') = A(X,Y)$ et $\tilde{B}(X',Y') = B(X,Y)$.
Soit alors φ défini par

$$\begin{array}{rccc} \varphi : & Z(A) \cap Z(B) & \longrightarrow & Z(\mathrm{Res}_{Y'}(\tilde{A},\tilde{B})) \\ & (x,y) & \longmapsto & x+uy \end{array}$$

φ est bien définie car si $(x,y) \in Z(A) \cap Z(B)$, $A(x,y) = B(x,y) = 0$ donc $\tilde{A}(x+uy,y) = \tilde{B}(x+uy,y) = 0$ et donc $\mathrm{Res}_{Y'}(\tilde{A},\tilde{B})(x+uy) = 0$.
φ est injective car on a choisi $u \notin \mathcal{E}$. On en déduit que $\#\left(Z(A) \cap Z(B)\right) \leq \#Z(\mathrm{Res}_{Y'}(\tilde{A},\tilde{B})) \leq \deg \mathrm{Res}_{Y'}(\tilde{A},\tilde{B}) \leq mn$. □

21 Formule sommatoire de Poisson et inversion de Fourrier [4] page 273

Théorème. *Soit $f \in \mathcal{S}(\mathbb{R})$. Alors, pour $T > 0$,*

$$\sum_{k\in\mathbb{Z}} f(kT) = \frac{1}{T} \sum_{k\in\mathbb{Z}} \hat{f}\left(\frac{2k\pi}{T}\right)$$

Démonstration. Soit $f \in \mathcal{S}(\mathbb{R})$, et $T > 0$. La série de fonctions $\sum_{k\in\mathbb{Z}} f(x+kT)$ converge uniformément sur tout segment de $\mathbb{R}$. En effet, comme $f \in \mathcal{S}(\mathbb{R})$, $\exists M > 0$ tel que $\forall x \in \mathbb{R}$, $|x^2 f(x)| \leq M$

$$\forall |x| \geq 1, |f(x)| \leq \frac{M}{x^2}$$

Soit $C > 0$. Pour $x \in [-C,C]$ et $k \in \mathbb{Z}$ tel que $|kT| \geq C+1$,

$$|f(x+kT)| \leq \frac{M}{(x+kT)^2} \leq \frac{M}{(|kT|-C)^2}$$

car $|x+kT| \geq ||kT| - |x|| \geq |kT| - |x| \geq |kT| - C \geq 1$.
En particulier, $\sum_{k\in\mathbb{Z}} f(x+kT)$ converge simplement sur $\mathbb{R}$.
Notons F sa somme.
Par le même raisonnement sur f', on obtient que $\sum_{k\in\mathbb{Z}} f'(x+kT)$ converge uniformément sur tout segment de $\mathbb{R}$. Donc $F \in \mathcal{C}^1(\mathbb{R})$.
Par ailleurs, F est T-périodique car

$$F(x+T) = \sum_{k\in\mathbb{Z}} f(x+T+kT) = \sum_{k\in\mathbb{Z}} f(x+(k+1)T) = \sum_{k\in\mathbb{Z}} f(x+kT) = F(x)$$

On peut donc calculer les coefficients de Fourier de F :

$$\begin{aligned}
c_n(F) &= \frac{1}{T}\int_0^T F(t)\,\mathrm{e}^{-i\frac{2\pi}{T}nt}\,\mathrm{d}t \\
&= \frac{1}{T}\int_0^T \sum_{k\in\mathbb{Z}} f(t+kT)\,\mathrm{e}^{-i\frac{2\pi}{T}nt}\,\mathrm{d}t \\
&= \frac{1}{T}\sum_{k\in\mathbb{Z}}\int_0^T f(t+kT)\,\mathrm{e}^{-i\frac{2\pi}{T}nt}\,\mathrm{d}t \\
&= \frac{1}{T}\sum_{k\in\mathbb{Z}}\int_{kT}^{(k+1)T} f(t)\,\mathrm{e}^{-i\frac{2\pi}{T}nt}\,\mathrm{d}t \qquad t \leftarrow t+kT \\
&= \frac{1}{T}\int_{\mathbb{R}} f(t)\,\mathrm{e}^{-i\frac{2\pi}{T}nt}\,\mathrm{d}t \\
&= \frac{1}{T}\hat{f}\left(\frac{2\pi n}{T}\right)
\end{aligned}$$

Or, $F \in \mathcal{C}^1(\mathbb{R})$ d'où

$$F(x) = \sum_{k\in\mathbb{Z}} f(x+kT) = \frac{1}{T}\sum_{k\in\mathbb{Z}} \hat{f}\left(\frac{2\pi k}{T}\right)\mathrm{e}^{i\frac{2\pi}{T}kx}$$

En évaluant en 0, on obtient

$$\sum_{k\in\mathbb{Z}} f(kT) = \frac{1}{T}\sum_{k\in\mathbb{Z}} \hat{f}\left(\frac{2k\pi}{T}\right)$$

□

Corollaire. *Soit $f \in \mathcal{S}(\mathbb{R})$,*

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

Démonstration. Il suffit de montrer la formule en $x = 0$ (quitte à étudier la fonction $g : x \mapsto f(x+x_0)$). Montrons donc que

$$f(0) = \frac{1}{2\pi}\int_{\mathbb{R}} \hat{f}(\xi)\mathrm{d}\xi$$

On utilise la formule démontrée précédemment :

$$\sum_{k\in\mathbb{Z}} f(kT) = f(0) + \sum_{k\in\mathbb{Z}^*} f(kT)$$

On a $|f(kT)| \leq \frac{\beta}{k^2T^2}$ d'où

$$\sum_{k\in\mathbb{Z}^*} |f(kT)| \leq \frac{\beta}{T^2}\sum_{k\in\mathbb{Z}^*}\frac{1}{k^2} \xrightarrow{T\to+\infty} 0$$

donc

$$\sum_{k\in\mathbb{Z}} f(kT) \xrightarrow{T\to+\infty} f(0)$$

Posons alors $\varepsilon = \frac{2\pi}{T}$.

$$\frac{1}{T}\sum_{k\in\mathbb{Z}} \hat{f}\left(\frac{2k\pi}{T}\right) = \frac{\varepsilon}{2\pi}\sum_{k\in\mathbb{Z}} \hat{f}(k\varepsilon) = \frac{1}{2\pi}\left(\varepsilon\sum_{k\in\mathbb{Z}} \hat{f}(k\varepsilon)\right)$$

On reconnait une somme de Riemann quand $T \to +\infty$, c'est-à-dire quand $\varepsilon \to 0$. D'où

$$f(0) = \frac{1}{2\pi} \int_{\mathbb{R}} \hat{f}(\varepsilon) \mathrm{d}\varepsilon$$

□

Remarque. Le corollaire n'est pas tiré de [4].

22 Théorème central limite [5] page 540

Lemme. *Soit $(z_n)_{n\in\mathbb{N}}$ une suite de nombre complexes de limite $z \in \mathbb{C}$. Alors, on a*

$$\left(1 + \frac{z_n}{n}\right)^n \xrightarrow{n\to+\infty} \mathrm{e}^z$$

Démonstration.

$$\mathrm{e}^z - \left(1 + \frac{z}{n}\right)^n = \sum_{k\geq 0} \frac{z^k}{k!} - \sum_{k=0}^{n} \binom{n}{k} \frac{z^k}{n^k} = \sum_{k\geq 0} a_k^{(n)} z^k \qquad a_k^{(n)} = \begin{cases} \frac{1}{k!}\left(1 - \frac{n(n-1)\ldots(n-k+1)}{n^k}\right) & \text{si } k \leq n \\ \frac{1}{k!} & \text{sinon} \end{cases}$$

Les $a_k^{(n)}$ sont positifs. Pour $|z| = r$,

$$\begin{aligned} \left|\mathrm{e}^z - \left(1 + \frac{z}{n}\right)^n\right| &\leq \sum_{k\geq 0} a_k^{(n)} r^k \\ &= \mathrm{e}^r - \left(1 + \frac{z}{n}\right)^n \qquad \text{valeur réelle !} \\ &= \mathrm{e}^r - \mathrm{e}^{n\ln(1+r/n)} \\ &\leq \mathrm{e}^r - \mathrm{e}^{r-r^2/2n} \leq \mathrm{e}^r(1 - \mathrm{e}^{-r^2/2n}) \leq \frac{r^2}{2n}\mathrm{e}^r \end{aligned}$$

donc

$$\left|\mathrm{e}^z - \left(1 + \frac{z_n}{n}\right)^n\right| \leq |\,\mathrm{e}^z - \mathrm{e}^{z_n}\,| + \left|\left(1 + \frac{z_n}{n}\right)^n - \mathrm{e}^{z_n}\right| \leq |\,\mathrm{e}^z - \mathrm{e}^{z_n}\,| + \frac{|z_n|^2}{2n}\,\mathrm{e}^{|z_n|}$$

Comme $(z_n)_n$ converge, elle est bornée, et par continuité de l'exponentielle, le terme de droite tend vers 0. □

Théorème (central limite)**.** *Soit $(X_n)_{n\geq 1}$ une suite de variables aléatoires indépendantes identiquement distribuées. On note $S_n = \sum_{k=1}^n X_k$. Si $\mathrm{Var}(X_1) < +\infty$, alors*

$$\frac{S_n - n\mathbb{E}[X_1]}{\mathrm{Var}(X_1)\sqrt{n}} \xrightarrow{\mathcal{L}} \mathcal{N}(0, \mathrm{Var}(X_1))$$

Démonstration. Sans perte de généralité, on peut supposer que les variables aléatoires sont centrées réduites (quitte à considèrer $\frac{X_n - \mathbb{E}[X_n]}{\sqrt{\mathrm{Var}(X_n)}}$).

Notons $Z_n = \frac{S_n}{\sqrt{n}}$. Montrons que $Z_n \xrightarrow{\mathcal{L}} \mathcal{N}(0,1)$:

Pour montrer la convergence en loi des variables aléatoires, on utilise le théorème de Paul Lévy, c'est-à-dire on montre la convergence simple sur $\mathbb{R}$ des fonctions caractéristiques.

$$\varphi_{Z_n}(t) = \mathbb{E}[\exp(itZ_n)] = \mathbb{E}[\exp(itS_n/\sqrt{n})] = \varphi_{S_n}(t/\sqrt{n}) = \left(\varphi_{X_1}(t/\sqrt{n})\right)^n$$

On peut alors faire le développement de Taylor-Young à l'ordre 2 pour φ_{X_1}. En effet, X_1 est de carré intégrable et donc sa fonction caractéristique est deux fois dérivable en 0. On a $\varphi'_{X_1}(0) = \mathbb{E}[X_1] = 0$

et $\varphi''_{X_1}(0) = -\mathbb{E}[X_1^2] = -1$.
On a donc le développement limité en 0 :

$$\varphi_{X_1}(u) = 1 - \frac{u^2}{2} + o(u^2) \qquad u \to 0$$

En remplaçant u par $t/\sqrt{n}$, on obtient pour $t \in \mathbb{R}$,

$$\varphi_{X_1}(t/\sqrt{n}) = 1 - \frac{t^2}{2n} + o(n) \qquad n \to +\infty$$

et finalement,

$$\varphi_{Z_n}(t) = \left(1 - \frac{t^2}{2n} + o(n)\right)^n \qquad n \to +\infty$$

Attention, ici on ne peut pas utiliser le logarithme réel car des complexes se cachent dans le $o(n)$! D'où l'utilisation du lemme pour conclure. □

23 Théorème de Burnside [13] page 185

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

Démonstration. On note $\lambda_1, \ldots, \lambda_r$ les valeurs propres de A (de multiplicité respective $n_1, \ldots, n_r$). Comme pour tout $k \in \mathbb{N}^*$, $\mathrm{Tr}(A^k) = 0$, on a

$$n_1\lambda_1^k + \ldots + n_r\lambda_r^k = 0$$

En écrivant cette équation pour k variant entre 1 et r, on obtient

$$\begin{pmatrix} \lambda_1 & \cdots & \lambda_r \\ \lambda_1^2 & \cdots & \lambda_r^2 \\ \vdots & & \vdots \\ \lambda_1^r & \cdots & \lambda_r^r \end{pmatrix} \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

et on reconnait une matrice de Vandermonde, qui est donc inversible puisque les λ_i sont tous distincts. D'où $n_1 = \ldots = n_r = 0$ □

Théorème (Burnside)**.** *Tout sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ d'exposant fini (c'est-à-dire tel qu'il existe un entier N tel que $A^N = I$ pour tout $A \in G$) est fini.*

Démonstration. Soit $(M_i)_{1 \le i \le m}$ une base de $\mathrm{Vect}(G)$ et

$$\begin{array}{rccc} f: & G & \longrightarrow & \mathbb{C}^m \\ & A & \longmapsto & (\mathrm{Tr}(AM_i))_{1 \le i \le m} \end{array}$$

1. Toutes les matrices de G sont diagonalisables.
   En effet, les matrices de G sont annulées par le polynôme $X^N - 1$ qui est scindé à racines simples sur $\mathbb{C}$.
2. Si $f(A) = f(B)$ pour $A, B \in G$, alors $AB^{-1} - I$ est nilpotente.
   Par linéarité de la trace, on a $\mathrm{Tr}(AM) = \mathrm{Tr}(BM)$ pour tout $M \in G$. On pose $D = AB^{-1}$. Soit $k \in \mathbb{N}^*$,
   $$\mathrm{Tr}(D^k) = \mathrm{Tr}(A\underbrace{B^{-1}D^{k-1}}_{\in G}) = \mathrm{Tr}(BB^{-1}D^{k-1}) = \mathrm{Tr}(D^{k-1})$$

Donc pour tout $k \in \mathbb{N}$, $\mathrm{Tr}(D^k) = \mathrm{Tr}(I_n) = n$. On en déduit que :

$$\mathrm{Tr}((D-I_n)^k) = \mathrm{Tr}\left(\sum_{j=0}^{k}\binom{k}{j}(-1)^j D^{k-j}\right) = \sum_{j=0}^{k}\binom{k}{j}(-1)^j \mathrm{Tr}(D^{k-j}) = n\sum_{j=0}^{k}\binom{k}{j}(-1)^j = (1-1)^k = 0$$

Par le lemme précédent, $D - I_n = AB^{-1} - I_n$ est nilpotente.

3. On en déduit que $AB^{-1} - I_n$ est nulle :
Par 1., A est diagonalisable, et par 2., A est nilpotente. Donc c'est la matrice nulle. On a donc $A = B$ et f est injective.
4. Par injectivité de f, le cardinal de G est inférieur à celui de l'image de f. Or, l'image de f est inclue dans X^m où X est l'ensemble des traces des éléments de G. Comme les valeurs propres des éléments de G sont des racines N-èmes de l'unité, il n'y a qu'un nombre fini possible de valeurs propres et donc le cardinal de X est fini et par injectivité de f, le cardinal de G est fini.

□

24 Lemme de Morse [10] page 209–354

Lemme (réduction des formes quadratiques, version différentiables)**.** *Soit $A_0 \in \mathcal{S}_n(k) \cap \mathrm{GL}_n(k)$. Soit $\varphi : \mathcal{M}_n(k) \longrightarrow \mathcal{S}_n(k)$ l'application $M \mapsto {}^tMA_0M$. Alors, il existe un voisinage V de A_0 dans $\mathcal{S}_n(k)$ tel que pour tout A dans V, il existe $M \in \mathrm{GL}_n(k)$ tel que $A = {}^tMA_0M$. L'application $A \mapsto M$ est $\mathcal{C}^1(V, \mathrm{GL}_n(k))$.*

Démonstration. L'idée est d'appliquer le théorème d'inversion locale.
L'application φ est $\mathcal{C}^1$ car polynômiale. Pour $H \in \mathcal{M}_n(k)$, on a :

$$\varphi(I+H) - \varphi(I) = {}^tHA_0 + A_0H + {}^tHA_0H = {}^t(A_0H) + A_0H + O(\|H\|^2)$$

Donc

$$\mathrm{d}\varphi(I)H = {}^t(A_0H) + A_0H$$

Le noyau de $\mathrm{d}\varphi(I)$ est donc formé des matrices H telles que A_0H soit antisymétrique.
Cette application est par ailleurs surjective : pour $A \in \mathcal{S}_n(k)$, on a $\mathrm{d}\varphi(I)(\frac{1}{2}A_0^{-1}A) = A$.
Come $\mathcal{M}_n(k) = \mathcal{S}_n(k) \oplus \mathcal{A}_n(k)$, on pose $F = \{M, A_0M \in \mathcal{S}_n(k)\}$ et on a donc la somme directe

$$\mathcal{M}_n(k) = \ker \mathrm{d}\varphi(I) \oplus F$$

On restreint alors φ à F (pour appliquer le théorème d'inversion locale) : $\psi = \varphi_{|F}$. $\ker \mathrm{d}\psi(I) = \ker \mathrm{d}\varphi(I) \cap F = 0$ par la somme directe. On peut alors appliquer le théorème d'inversion locale : il existe un voisinage ouvert U de I dans F (que l'on peut supposer contenu dans l'ouvert des matrices inversibles) tel que ψ soit un difféomorphisme de classe $\mathcal{C}^1$ de U sur $V = \psi(U)$. Ainsi, V est un voisinage ouvert de $A_0 = \psi(I) = \varphi(I)$ dans S, et pour $A \in V$, il existe une unique matrice inversible $M \in U$ telle que

$$A = {}^tMA_0M$$

et $M = \psi^{-1}(A)$ est une fonction continûment différentiable de A. □

Lemme (de Morse)**.** *Soit $f \in \mathcal{C}^3(U, \mathbb{R})$ où U est un ouvert de $\mathbb{R}^n$ contenant 0. On suppose que $Df(0) = 0$ et que $D^2f(0)$ est non-dégénérée, de signature $(p, n-p)$. Alors, il existe un difféomorphisme $\varphi : x \mapsto u$ entre deux voisinages de $\mathbb{R}^n$ contenant 0, de classe $\mathcal{C}^1$, tel que $\varphi(0) = 0$, et*

$$f(x) - f(0) = u_1^2 + \ldots + u_p^2 - u_{p-1}^2 - \ldots - u_n^2$$

Démonstration. Par une formule de Taylor avec reste intégral, on a

$$f(x) = f(0) + \int_0^1 (1-t)^t x D^2 f(tx) x \mathrm{d}t$$

c'est-à-dire

$$f(x) - f(0) = {}^t x Q(x) x$$

avec $Q(x) = \int_0^1 (1-t) D^2 f(tx) \mathrm{d}t$, fonction de classe $\mathcal{C}^1$ de x. Par le lemme précédent, il existe $M(x)$ inversible $\mathcal{C}^1$ de x au voisinage de 0 dans $\mathbb{R}^n$ telle que

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

donc

$$f(x) - f(0) = {}^t y Q(0) y \qquad y = M(x)x$$

Or, $Q(0) = \frac{D^2 f(0)}{2}$ est de signature $(p, n-p)$. En appliquant le théorème de Sylvester, on obtient que

$$Q(0) = {}^t P \begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix} P$$

Finalement,

$$f(x) - f(0) = {}^t x {}^t M(x) {}^t P \begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix} PM(x)x = {}^t(PM(x)x) \begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix} (PM(x)x)$$

En posant $\varphi(x) = PM(x)x$, on a

$$f(x) - f(0) = {}^t \varphi(x) \begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix} \varphi(x)$$

et donc avec $u = \varphi(x)$, on a bien $\varphi(0) = 0$, et $f(x) - f(0) = u_1^2 + \ldots + u_p^2 - u_{p+1}^2 - \ldots - u_n^2$.
Il reste à montrer que φ définit un $\mathcal{C}^1$-difféomorphisme entre deux voisinages de 0 dans $\mathbb{R}^n$. φ est $\mathcal{C}^1$ car M l'est (c'est là qu'on utilise que f doit être $\mathcal{C}^3$ au début). On calcule la différentielle de φ en 0 :

$$\varphi(h) - \varphi(0) = PM(h)h = P(M(0) + \mathrm{d}M(0).h + o(\|h\|))h = PM(0) + o(\|h\|)$$

Comme $PM(0) \in \mathrm{GL}_n(\mathbb{R})$, $\mathrm{d}\varphi(0)$ est inversible D'après le théorème d'inversion locale, φ est un un $\mathcal{C}^1$-difféomorphisme entre deux voisinages de l'origine dans $\mathbb{R}^n$. □

25 Extrémas liés [4] page 317–327

Théorème (des extrémas liés)**.** *Soient $f, g_1, \ldots, g_r : U \subset \mathbb{R}^n \longrightarrow \mathbb{R}$ des fonctions de classe $\mathcal{C}^1$, où U est un ouvert de $\mathbb{R}^n$. On pose $\Gamma = \{x \in U, g_1(x) = \ldots = g_r(x) = 0\}$. Si $f_{|\Gamma}$ admet un extrémum relatif en $a \in \Gamma$, et si les formes linéaires $dg_{1,a}, \ldots, dg_{r,a}$ sont linéairement indépendantes, alors il existe des réels $\lambda_1, \ldots, \lambda_r$ tels que*

$$df_a = \sum_{i=1}^{r} \lambda_i dg_{i,a}$$

Les λ_i sont appelés multiplicateurs de Lagrange.

Démonstration. On note $s = n - r$. On identifie $\mathbb{R}^n$ à $\mathbb{R}^s \times \mathbb{R}^r$. On écrit les éléments de $\mathbb{R}^n$ de la forme $(x, y) \in \mathbb{R}^s \times \mathbb{R}^r$. On écrit en particulier $a = (\alpha, \beta)$.
On commence par remarquer que $r \leq n$ car les $\mathrm{d}g_{i,a}$ forment une famille libre, et le dual de $\mathbb{R}^n$ est de dimension n. Si $r = n$ le résultat est évident car les $\mathrm{d}g_{i,a}$ forment alors une base. On suppose désormais

$r \leq n-1$, c'est-à-dire $s \geq 1$.
Comme la famille $(\mathrm{d}g_{i,a})_i$ est libre, la matrice

$$\begin{pmatrix} \frac{\partial g_1}{\partial x_1}(a) & \dots & \frac{\partial g_1}{\partial x_s}(a) & \frac{\partial g_1}{\partial y_1}(a) & \dots & \frac{\partial g_1}{\partial y_r}(a) \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial g_r}{\partial x_1}(a) & \dots & \frac{\partial g_r}{\partial x_s}(a) & \frac{\partial g_r}{\partial y_1}(a) & \dots & \frac{\partial g_r}{\partial y_r}(a) \end{pmatrix}$$

est de rang r. On peut donc en extraire une sous-matrice de taille $r \times r$ inversible, et quitte à changer le nom des variables, on peut supposer que c'est celle tout à droite, donc on peut supposer que

$$\det\left(\frac{\partial g_i}{\partial y_j}(a)\right)_{1 \leq i,j \leq r} \neq 0$$

Par le théorème des fonctions implicites appliqué à $g = (g_1, \dots, g_r)$, on peut trouver U' voisinage de $\alpha \in \mathbb{R}^s$, Ω voisinage de a dans $\mathbb{R}^n$, et $\varphi = (\varphi_1, \dots, \varphi_r) : U' \to \mathbb{R}^r$ de classe $\mathcal{C}^1$ tels que

$$g(x,y) = 0 \text{ avec } x \in U' \text{ et } (x,y) \in \Omega \qquad \Longleftrightarrow \qquad y = \varphi(x)$$

On pose alors $h(x) = f(x, \varphi(x))$. h admet un extremum local en $x = \alpha$ car $(\alpha, \varphi(\alpha)) = a$, et $(x, \varphi(x)) \in \Gamma$, ce qui entraîne :

$$\forall i, 1 \leq i \leq s, \qquad 0 = \frac{\partial h}{\partial x_i}(\alpha) = \frac{\partial f}{\partial x_i}(a) + \sum_{j=1}^{r} \frac{\partial \varphi_j}{\partial x_i}(\alpha) \frac{\partial f}{\partial y_j}(a)$$

Par ailleurs, en dérivant par rapport à x_i la fonction g, et avec l'équation $g(x, \varphi(x)) = 0$, on obtient :

$$\forall 1 \leq k \leq r, \forall 1 \leq i \leq s, \qquad 0 = \frac{\partial g_k}{\partial x_i}(\alpha) = \frac{\partial g_k}{\partial x_i}(a) + \sum_{j=1}^{r} \frac{\partial \varphi_j}{\partial x_i}(\alpha) \frac{\partial g_k}{\partial y_j}(a)$$

Autrement dit, les s premiers vecteurs colonnes de la matrice

$$\begin{pmatrix} \frac{\partial f}{\partial x_1}(a) & \dots & \frac{\partial f}{\partial x_s}(a) & \frac{\partial f}{\partial y_1}(a) & \dots & \frac{\partial f}{\partial y_r}(a) \\ \frac{\partial g_1}{\partial x_1}(a) & \dots & \frac{\partial g_1}{\partial x_s}(a) & \frac{\partial g_1}{\partial y_1}(a) & \dots & \frac{\partial g_1}{\partial y_r}(a) \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial g_r}{\partial x_1}(a) & \dots & \frac{\partial g_r}{\partial x_s}(a) & \frac{\partial g_r}{\partial y_1}(a) & \dots & \frac{\partial g_r}{\partial y_r}(a) \end{pmatrix}$$

s'expriment linéairement en fonction des r derniers vecteurs colonnes. Donc la matrice est de rang $\leq r$. Comme la matrice a $r+1$ lignes, on en déduit que la famille constituée des $r+1$ lignes est liée, et donc $\exists \mu_0, \dots, \mu_r telsque \mu_0 \mathrm{d}f_a + \sum_{i=1}^{r} \mu_i \mathrm{d}g_{i,a} = 0$. Comme $(\mathrm{d}g_{i,a})_i$ est libre, $\mu_0 \neq 0$, et en posant $\lambda_i = -\mu_i/\mu_0$, on obtient

$$\mathrm{d}f_a = \sum_{i=1}^{r} \lambda_i \mathrm{d}g_{i,a}$$

□

26 Sous-groupes compacts de $\mathrm{GL}_n(\mathbb{R})$ [1] page 141–161

Lemme. *Soit K un compact convexe non-vide de $\mathbb{R}^n$. Soit G un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$ vérifiant pour tout $u \in G$, $u(K) \subset K$. Alors il existe $a \in K$ tel que pour tout $u \in G$, $u(a) = a$.*

Démonstration. On se fixe une norme euclidienne $\|\cdot\|$ sur $\mathbb{R}^n$, et on considère $N(x) = \sup_{u\in G} \|u(x)\|$.
N est clairement une norme sur $\mathbb{R}^n$. Par compacité de G, le sup est en fait un max.
Prenons $x, y \in K$ tels que $N(x+y) = N(x) + N(y)$, et $u \in G$ tel que $N(x+y) = \|u(x+y)\|$. On a alors

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

L'égalité dans l'inégalité triangulaire donne que $u(x)$ et $u(y)$ sont positivement liés, et donc x et y aussi.
Par compacité de K, il existe $a \in K$ tel que $N(a) = \min_{x\in K} N(x) = \alpha$.
a est unique. En effet, supposons b tel que $N(b) = \alpha$. Alors,

$$N\left(\frac{a+b}{2}\right) \leq \frac{N(a)+N(b)}{2} \leq \alpha$$

Donc par minimalité de α, il y a égalité ci-dessus, et a et b sont donc positivement liés. Si $a = 0$, il est bien unique car $b = 0$. Si $a \neq 0$, $\exists \lambda > 0$ tel que $a = \lambda b$. On a alors

$$\alpha = N(a) = N(\lambda b) = \lambda N(b) = \lambda\alpha$$

et $\lambda = 1$ d'où l'unicité.
Enfin, si $g \in G$, $N(g(a)) = \max_{u\in G} \|u(g(a))\| = \max_{v\in G} \|v(a)\| = N(a) = \alpha$. Par unicité de a, $g(a) = a$. □

Théorème. *Soit G un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$. Alors, il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que $PGP^{-1} \subset \mathcal{O}_n(\mathbb{R})$.*

Démonstration. On considère l'application

$$\begin{array}{rccc} \rho: & G & \longrightarrow & \mathrm{GL}(\mathcal{S}_n(\mathbb{R})) \\ & A & \longmapsto & S \mapsto ASA^t \end{array}$$

Elle est continue car polynômiale et $\rho(AB) = \rho(A) \circ \rho(B)$.
On pose $C = \{MM^t, M \in G\} \subset \mathcal{S}_n^{++}$. C est compact (c'est l'image de G par une application continue) et non-vide. Son enveloppe convexe (qu'on note K) est un compact convexe non-vide de $\mathcal{S}_n^{++}$.
C est stable par $\rho(G)$: Soit $MM^t \in C$, $A \in G$, $\rho(A)(MM^t) = AMM^tA^t = (AM)(AM)^t \in C$.
Par linéarité de $\rho(\cdot)$, K est aussi stable par $\rho(G)$.
K est donc un compact convexe non-vide de $\mathcal{S}_n^{++}$, et $\rho(G)$ est compact. Par le lemme, il existe $S \in K \subset \mathcal{S}_n^{++}$ fixé par tous les éléments de $\rho(G)$.

$$\forall A \in G, \rho(A)(S) = S \iff ASA^t = S$$

Autrement dit, G est inclu dans le groupe orthogonal de la forme quadratique associée à S.
En utilisant la décomposition de Choleski $S = RR^t$, on obtient pour $A \in G$,

$$ARR^tA^t = RR^t$$

donc

$$R^{-1}ARR^tA^t(R^t)^{-1} = I_n$$
$$(R^{-1}AR)(R^{-1}AR)^t = I_n$$

donc $R^{-1}AR \in \mathcal{O}_n(\mathbb{R})$ et $G \subset R\mathcal{O}_n(\mathbb{R})R^{-1}$. □

Remarque. La fin de la preuve du lemme n'est pas faite comme dans [1].

27 Méthode de Newton [10] page 152

Soit $f : [c,d] \longrightarrow \mathbb{R}$ une fonction de classe $\mathcal{C}^2$. On suppose $c < d$, $f(c) < 0 < f(d)$, et $f'(x) > 0$ pour tout $x \in [c,d]$. Par le théorème des valeurs intermédiaires, f a un unique zéro $a \in [c,d]$. On va montrer que si on prend x_0 assez proche de a, alors la suite suivante définie par :

$$x_{n+1} = F(x_n) \qquad n \geq 0$$

avec $F(x) = x - \frac{f(x)}{f'(x)}$, converge vers a et la convergence est quadratique.
Si de plus f est convexe, alors $I = [a,d]$ est stable par F et pour tout $x_0 \in I$, la suite $(x_n)_n$ est strictement décroissante (ou constante) et on a l'équivalent

$$x_{n+1} - a \sim \frac{1}{2}\frac{f''(a)}{f'(a)}(x_n - a)^2 \qquad n \to +\infty$$

1. On montre que si $x \in [c,d]$, il existe z entre a et x tel que $F(x) - a = \frac{1}{2}\frac{f''(z)}{f'(x)}(x-a)^2$.

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

   On applique la formule de Taylor à l'ordre 2 au numérateur :

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

   On en déduit qu'il existe $C > 0$ tel que $|F(x) - a| \leq C|x-a|^2$ (en prenant $C = \max|f''|/\min|f'|$).
2. On montre qu'un intervalle de la forme $I = [a-\alpha, a+\alpha]$ avec $\alpha > 0$ est stable par F.
   Soit $\alpha > 0$ tel que $I \subset [c,d]$ et $C\alpha < 1$. Si $x \in I$, on a $|x-a| \leq \alpha < 1/C$. On a donc pour $x \in I$,

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

   car $C\alpha < 1$. Donc $F(x) \in I$ et $F(I) \subset I$.
   En choisissant $x_0 \in I$, on a $x_n \in I$ pour tout n et

   $$|x_{n+1} - a| = |F(x_n) - a| \leq C|x_n - a|^2 \leq (C|x_0 - a|)^{2^n} \leq (C\alpha)^{2^n}$$

   et la convergence est d'ordre 2 puisque $C\alpha < 1$.
3. Supposons désormais que f est convexe, et montrons que $I = [a,d]$ est stable par F. Soit $x \in [a,d]$. On a $f'(x) > 0$ et $f(x) \geq 0$ donc

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

   avec inégalité stricte si $x > a$. D'après 1., on a

   $$F(x) - a = \frac{1}{2}\frac{f''(z)}{f'(x)}(x-a)^2 \geq 0$$

   donc $F(x) \geq a$ ($<$ si $x > a$) et $F(x) \in [a,d]$.
   Si on fixe donc $x_0 \in I, x_0 \neq a$, on a pour tout n, $a < x_n \leq d$. De plus, la suite $(x_n)_n$ est strictement décroissante. Si $x_0 = a$, la suite est constante. La suite admet donc une limite ℓ qui vérifie $F(\ell) = \ell$, ou encore $f(\ell) = 0$, et donc $\ell = a$.
   On a montré précédemment que la convergence est quadratique, c'est-à-dire que

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

   Cette inégalité est essentiellement optimale : si $x_0 \in]a,d]$, on a $x_n > a$ et pour tout n,

   $$\frac{x_{n+1} - a}{(x_n - a)^2} = \frac{1}{2}\frac{f''(z_n)}{f'(x_n)} \qquad z_n \in]a, x_n]$$

   La fraction tend donc vers $f''(a)/2f'(a)$ quand $n \to +\infty$.

28 Théorème de Riesz-Fischer [2] page 57

Théorème (Riesz-Fischer)**.** *L^p est un espace de Banach pour $1 \leq p \leq \infty$.*

Démonstration.

1. L^∞ est un espace complet.
   Soit $(f_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans L^∞. Etant donné $k \geq 1$, il existe N_k tel que
   $$\|f_m - f_n\|_\infty \leq \frac{1}{k} \qquad m, n \geq N_k$$
   donc il existe E_k négligeable tel que
   $$|f_m(x) - f_n(x)| \leq \frac{1}{k} \qquad \forall x \in \Omega\backslash E_k \qquad \forall m, n \geq N_k$$
   En posant $E = \bigcup_k E_k$, et pour $x \in \Omega\backslash E$, $f_n(x)$ est une suite de Cauchy dans $\mathbb{R}$ qui est complet donc converge vers $f(x)$.
   En prenant $m \to +\infty$, on obtient
   $$|f(x) - f_n(x)| \leq \frac{1}{k} \qquad \forall x \in \Omega\backslash E \qquad \forall n \geq N_k$$
   et finalement $f \in L^\infty$ et $\|f - f_n\|_\infty \leq \frac{1}{k}$ pour tout $n \geq N_k$. Donc $\|f - f_n\|_\infty \xrightarrow{n\to+\infty} 0$.
2. L^p est un espace complet pour $1 \leq p < \infty$.
   Soit $(f_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans L^p. On va trouver une sous-suite extraite qui converge dans L^p.
   Il existe N_1 tel que $\forall m, n \geq N_1$, $\|f_n - f_m\|_p \leq \frac{1}{2}$.
   Il existe N_2 tel que $\forall m, n \geq N_2$, $\|f_n - f_m\|_p \leq \frac{1}{2^2}$.
   etc.
   On construit de la sorte une suite $(n_k)_k$ telle que
   $$\|f_{n_{k+1}} - f_{n_k}\|_p \leq \frac{1}{2^k} \qquad \forall k \geq 1$$
   En écrivant f_k au lieu de f_{n_k}, on a donc
   $$\|f_{k+1} - f_k\|_p \leq \frac{1}{2^k} \forall k \geq 1$$
   On pose ensuite $g_n(x) = \sum_{k=1}^n |f_{k+1}(x) - f_k(x)|$. On a donc $\|g_n(x)\|_p \leq 1$. La suite de fonction $(g_n^p)_n$ est une suite croissante de fonctions mesurables positives, par le théorème de convergence dominée,
   $$\int \underbrace{\lim_{n\to+\infty} g_n^p}_{g^p} = \lim_{n\to+\infty} \int g_n^p$$
   et $\|g\|_p < +\infty$. Donc presque partout sur Ω, $g_n(x) \xrightarrow{n\to+\infty} g(x)$ et $g \in L^p$.
   Pour $m \geq n \geq 2$,
   $$|f_m(x) - f_n(x)| \leq |f_m(x) - f_{m-1}(x)| + \ldots + |f_{n+1}(x) - f_n(x)| = g_{m-1}(x) - g_{n-1}(x) \leq g(x) - g_{n-1}(x)$$
   donc presque partout sur Ω, $(f_n(x))_n$ est une suite de Cauchy et converge donc vers $f(x)$ (par complétude de $\mathbb{R}$). Presque partout sur Ω, on a
   $$|f(x) - f_n(x)| \leq g(x) - g_{n-1}(x) \leq g(x) \qquad n \geq 2$$
   Comme L^p est un espace vectoriel, $f \in \mathbb{L}^p$.
   Enfin, $\|f_n - f\|_p \xrightarrow{n\to+\infty} 0$: $|f_n(x) - f(x)|^p$ tend vers 0 presque partout, et $|f_n(x) - f(x)|^p \leq g^p(x)$ qui est intégrable. Par convergence dominée, $\|f_n - f\|_p \xrightarrow{n\to+\infty} 0$.

□

29 Réduction des endomorphismes normaux [3] page 255

Lemme (1)**.** *Soit E un espace euclidien, et $u \in \mathcal{L}(E)$,*

1. *Si F est un sous-espace vectoriel de E stable par u, alors $F^\perp$ est stable par u^*.*
2. *Si u est normal et E_λ est un sous-espace propre de u, alors $E_\lambda^\perp$ est aussi stable par u.*

Démonstration.

1. Si $x \in F$, et $y \in F^\perp$, $\langle u^*(y), x\rangle = \langle y, \underbrace{u(x)}_{\in F}\rangle = 0$. Donc $u^*(y) \in F^\perp$ et $F^\perp$ est stable par u^*.
2. Comme u et u^* commutent (u est normal), E_λ est table par u^*. D'après 1., $E_\lambda^\perp$ est stable par $(u^*)^* = u$.

□

Lemme (2)**.** *Soit E un espace euclidien de dimension 2, et $u \in \mathcal{L}(E)$ normal n'admettant pas de valeur propre réelle. Alors, dans toute base orthonormée B de E, on a*

$$Mat_B(u) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \qquad b \neq 0$$

Démonstration. On écrit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On a $b \neq 0$ car u est sans valeur propre réelle. Comme u est normal, $MM^t = M^tM$, ce qui donne au niveau des matrices :

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

donc $b = \pm c$ par la première égalité. Mais si $b = c$, alors M est symétrique donc diagonalisable sur $\mathbb{R}$. Absurde car u est sans valeur propre réelle. Donc $b = -c$. La deuxième égalité donne alors $a = d$ et on a le résultat.

□

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

$$Mat_B(u) = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & 0 & \\ & & \lambda_r & & & & \\ & & & \tau_1 & & & \\ & 0 & & & \ddots & & \\ & & & & & & \tau_s \end{pmatrix}$$

avec les λ_i réels, et $\tau_i = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$.

Démonstration. On démontre le résultat par récurrence forte sur $n = \dim(E)$. Pour $n = 1$, le résultat est évident. Supposons le résultat vrai pour tout espace euclidien de dimension $\leq n-1$, et on considère E euclidien de dimension n.

Si u a une valeur propre réelle λ, alors on peut considérer E_λ et $F = E_\lambda^\perp$. F est stable par u et par u^* (lemme 1), et on peut alors considérer $u_{|F}$ et son adjoint. Ils commutent et on peut appliquer l'hypothèse de récurrence sur F qui est de dimension $\leq n-1$.

Si u n'a pas de valeur propre réelle, on va se ramener au cas $n = 2$ avec un bon espace.

On considère $Q(X) = X^2 - 2\alpha X + \beta$ un facteur irréductible de χ_u (donc $\alpha^2 - \beta < 0$). On pose $N = \ker(Q(u))$.

$N \neq 0$: On scinde Q sur $\mathbb{C}$: $Q(X) = (X - \lambda)(X - \bar{\lambda})$. On a donc $\det(u - \lambda \mathrm{id}) = 0$ et on en déduit que $\det(Q(u)) = \det(u - \lambda \mathrm{id}) \det(u - \bar{\lambda}\mathrm{id}) = 0$ donc $Q(u)$ n'est pas inversible et donc non-injective. Donc $\ker(Q(u)) \neq 0$.

On définit ensuite $v = u_{|N}$. v est bien défini car N est stable par u : si $x \in N$, $u^2(x) = 2\alpha u(x) - \beta x$ et en appliquant u à cette égalité, $u(x) \in N$. L'endomorphisme vv^* est alors symétrique réel donc il possède une valeur propre réelle μ. Prenons x un vecteur propre non-nul associé à μ.

On pose $F = \mathrm{Vect}(x, u(x))$. F est stable par u car $u(x) \in F$ et $u^2(x) = 2\alpha u(x) - \beta x \in F$.

$F = \mathrm{Vect}(u(x), u^2(x))$ car $0 \leq \alpha^2 < \beta$ donc $\beta \neq 0$.

F est aussi stable par u^* :

$$u^*(u(x)) = v^* v(x) = \mu x$$

$$u^*(u^2(x)) = u(u^* \circ u(x)) = u(\mu x) = \mu u(x)$$

On peut alors considérer $u_{|F}$ et $u_{|F^\perp}$: Par le lemme 2., on peut trouver une base B_1 de F telle que la matrice de $u_{|F}$ soit de la forme τ_i. On applique ensuite l'hypothèse de récurrence sur $F^\perp$ (de dimension $n - 2$) et on trouve B_2 base de $F^\perp$, telle que la matrice de $u_{|F^\perp}$ soit de la forme voulue. En prenant $B = B_1 \cup B_2$, on a le résultat.

□

30 Théorème de Cauchy-Lipschitz [10] page 179

Théorème. *Soit I un intervalle de $\mathbb{R}$ est $f : I \times \mathbb{R}^m \longrightarrow \mathbb{R}^m$ une application continue, globalement lipschitzienne en la seconde variable :*

$$\forall K \text{ compact} \subset I \qquad \exists k > 0 \qquad \forall t \in K, \forall y, z \in \mathbb{R}^m$$

$$\|f(t, y) - f(t, z)\| \leq k\|y - z\|$$

où $\|\cdot\|$ est une norme sur $\mathbb{R}^m$.
Alors, si $t_0 \in I$, et $x \in \mathbb{R}^m$ sont donnés, le système

$$(P) \qquad \begin{cases} y'(t) = f(t, y(t)) \\ y(t_0) = x \end{cases}$$

admet une unique solution définie sur I tout entier.

Démonstration.

Si I est compact On va se ramener à un problème de point fixe : on remarque qu'une solution du problème (P) vérifie $y(t) = x + \int_{t_0}^t f(s, y(s))\mathrm{d}s$. La recherche d'une solution de (P) équivaut à la recherche d'un point fixe de l'application

$$\begin{array}{rccc} F : & \mathcal{C}(I, \mathbb{R}^m) & \longrightarrow & \mathcal{C}(I, \mathbb{R}^m) \\ & y & \longmapsto & F(y) : t \mapsto x + \int_{t_0}^t f(s, y(s))\mathrm{d}s \end{array}$$

On va donc montrer que F possède un unique point fixe.

On note k la constante de Lipschitz de f sur l'intervalle I, et ℓ la longueur de I. On utilise la norme

$$\|y\|_k := \max_{t \in I} \mathrm{e}^{-k|t - t_0|} \|y(t)\|$$

$\|\cdot\|_k$ et $\|\cdot\|_\infty$ sont équivalentes puisque $\mathrm{e}^{-k\ell}\,\|y\|_\infty \leq \|y\|_k \leq \|y\|_\infty$. On en déduit que $(\mathcal{C}(I,\mathbb{R}^m), \|\cdot\|_k)$ est un espace complet.
Pour $y, z \in \mathcal{C}(I,\mathbb{R}^m)$, $t \in I$, $t \geq t_0$, on a

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

d'où

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

En raisonnant de même pour $t \leq t_0$, on a

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

d'où pour $t \in I$,

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

En prenant le max, on obtient :

$$\|F(y) - F(z)\|_k \leq (1 - \mathrm{e}^{-k\ell})\|y - z\|_k$$

donc F est contractante et on peut appliquer le théorème de point fixe.

Si I n'est pas compact on écrit $I = \bigcup_j I_j$ où les I_j sont des compacts contenant t_0, et la suite $(I_j)_j$ est croissante pour l'inclusion. En appliquant ce qui précède sur chaque I_j, on obtient une unique solution y_j sur chaque I_j.
Si y est une solution du problème (P), y coïncide avec y_j sur chaque I_j (par unicité). Inversement, les y_j se raccordent :la fonction

$$y(t) = y_j(t) \qquad \forall j \text{ tel que } t \in I_j$$

est bien définie et donne une solution sur I.
La problème sur un intervalle quelconque admet donc une unique solution, définie sur I tout entier.

□

31 $\mathbb{Z}[i]$ et le théorème des deux carrés [7] page 56

On définit $\mathbb{Z}[i] := \mathbb{Z} + i\mathbb{Z}$. On définit sur $\mathbb{Z}[i]$ la norme $N : z \mapsto z\bar{z} = |z|^2$.

Proposition. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Démonstration. On vérifie aisément que $\pm 1, \pm i$ sont inversibles dans $\mathbb{Z}[i]$. Réciproquement, soit $z \in \mathbb{Z}[i]^\times$. Alors il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$. En passant à la norme, on obtient

$$1 = N(1) = N(z)N(z')$$

et donc $N(z) = 1$ et z est de module 1 à coefficients entiers, donc $z \in \{\pm 1, \pm i\}$. □

Proposition. *$\mathbb{Z}[i]$ est euclidien pour la norme N.*

Démonstration. Soit z et t deux éléments de $\mathbb{Z}[i]$. On veut écrire $z = qt + r$ avec $N(r) < N(t)$. On considère $z/t = x + iy \in \mathbb{C}$. On choisit $q = a + ib \in \mathbb{Z}[i]$ tel que q soit l'entier de Gauss le plus proche de z/t. Par pythagore, on obtient que

$$|z/t - q| \leq \frac{\sqrt{2}}{2} < 1$$

et en posant $r = z - tq$, on a

$$|r| = |t||z/t - q| < |t|$$

puis en élevant au carré ces nombres positifs,

$$N(r) = |r|^2 < |t|^2 = N(t)$$

□

Remarque. $\mathbb{Z}[i]$ est euclidien donc principal donc factoriel.

Théorème. *Soit p un nombre premier. p est somme de deux carrés (on note $p \in \Sigma$) $\iff$ $p = 2$ ou $p \equiv 1 \mod 4$.*

Démonstration. Le sens direct est facile : raisonnons par contraposée. Si $p \equiv 3 \mod 4$, alors ce n'est pas une somme de deux carrés. En effet, supposons $p = a^2 + b^2$. Modulo 4, les carrés sont 0 et 1, et leur somme ne peut être égale à 3.
Pour l'équivalence, on va devoir utiliser le lemme suivant :

Lemme. *$p \in \Sigma \iff p$ n'est pas irréductible de $\mathbb{Z}[i]$.*

Démonstration. Si $p \in \Sigma$, $p = a^2 + b^2 = (a + ib)(a - ib)$ et $a, b \neq 0$ donc p n'est pas irréductible dans $\mathbb{Z}[i]$. Réciproquement, si $p = zz'$, en passant à la norme, on a $p^2 = N(z)N(z')$ et comme z, z' sont non-inversibles, on a $N(z) = p$ et $p \in \Sigma$. □

Par factorialité de $\mathbb{Z}[i]$, on a donc $p \in \Sigma \iff (p)$ n'est pas premier dans $\mathbb{Z}[i] \iff \mathbb{Z}[i]/(p)$ n'est pas intègre. Par théorème d'isomorphisme, on a

$$\mathbb{Z}[i]/(p) \simeq \left(\mathbb{Z}[X]/(X^2+1)\right)/(p) \simeq \left(\mathbb{Z}[X]/(p)\right)/(X^2+1) \simeq \mathbb{F}_p[X]/(X^2+1)$$

donc $p \in \Sigma \iff -1$ est un carré dans $\mathbb{F}_p \iff p = 2$ ou $p \equiv 1 \mod 4$ (en utilisant le symbole de Legendre par exemple). □