Université de Rennes
École Normale Supérieure
2025

Développements pour l'Agrégation

Agrégation 2025

Kylian Prigent

école
normale
supérieure
rennes

Table des matières

I Développements d'algèbre

Formes de Hankel [4]

I.A Formes de Hankel (144) (148) (159) (170) (171)

Théorème 1:

Soit $P \in \mathbb{R}[X]$ de degré n. Notons $x_1, \dots, x_t$ ses racines distinctes et $m_1, \dots, m_t$ leur multiplicité. Soit $s_k = \sum_{i=1}^{t} m_i x_i^k$ les sommes de Newton associées. Alors

$$\sigma = \sum_{1 \leqslant i,j \leqslant n-1} s_{i+j} X_i X_j$$

définit une forme quadratique sur $\mathbb{C}^n$. Elle définit également une forme quadratique sur $\mathbb{R}^n$. On notant (p, q) sa signature, alors le nombre de racines réelles distinctes de P est $p - q$.

Démonstration. Comme σ est un polynôme homogène de degré 2 sur $\mathbb{C}$, on a que σ définit une forme quadratique sur $\mathbb{C}$.

C'est de plus une forme quadratique sur $\mathbb{R}$ car $s_k \in \mathbb{R}$.
En effet, pour toute racine x de P on a l'un des deux cas exclusifs suivants :

1. $x \in \mathbb{R}$;
2. sinon comme P est à coefficients réels, x et $\overline{x}$ sont toutes les deux racines de P. Alors $x^k + \overline{x}^k = 2\Re(x^k) \in \mathbb{R}$.

On pose φ_k la forme linéaire $\varphi_k = \sum_{i=1}^{n} x^{i-1} e_i^*$. Donc dans la base duale de la base canonique de $\mathbb{C}^n$, on a :

$$\begin{pmatrix} 1 & \dots & 1 \\ x_1 & \dots & x_t \\ \vdots & & \vdots \\ x_1^{t-1} & \dots & x_t^{t-1} \\ \vdots & & \vdots \\ x_1^{n-1} & \dots & x_t^{n-1} \end{pmatrix}$$

Or on reconnaît dans cette matrice une matrice de Vandermonde de taille t. Elle est inversible car les racines sont deux à deux distinctes.
Donc cette matrice est de rang t (dans $\mathbb{C}$).

On définit la forme quadratique $\rho = \sum_{i=k}^{t} m_k \varphi_k^2$. Cette forme quadratique coïncide avec σ car le terme en $X_i X_j$ de ρ est :

$$\begin{cases} \sum_{k=1}^{t} 2 m_k x_k^{i+j} = 2 s_{i+j} & \text{si } i \neq j \\ \sum_{k=1}^{t} m_k x_k^{i+j} = s_{i+j} & \text{si } i = j \end{cases}$$

Ce qui correspond aux coefficients dans σ. Or par définition de la signature, le rang de σ est $p + q$. Mais le rang est invariant par extension de corps donc $p + q = t$.

Il reste donc à régler la question de savoir comment les φ_k interagissent avec la signe en fonction de x_k.
On a toujours les deux cas exclusifs précédents :

1. $x_k \in \mathbb{R}$, alors φ_k^2 est une forme quadratique réelle de signature $(1,0)$ car φ_k est une forme linéaire non nulle ;
2. sinon, on a que $\overline{\varphi_k}$ correspond à la forme associée à $\overline{x_k}$, et alors $\varphi_k^2 + \overline{\varphi_k}^2 = 2\Re(\varphi_k)^2 - 2\Im(\varphi_k)^2$ est une forme quadratique réelle et comme $x_k \neq \overline{x_k}$, la matrice

$$\begin{pmatrix} 1 & 1 \\ x_k & \overline{x_k} \\ \vdots & \vdots \\ x_k^{n-1} & \overline{x_k}^{n-1} \end{pmatrix}$$

est de rang 2 pour les mêmes raisons que précédemment. Donc les formes linéaires φ_k et $\overline{\varphi_k}$ sont linéairement indépendantes ; donc la forme quadratique réelle $\varphi_k^2 + \overline{\varphi_k}^2 = 2\Re(\varphi_k)^2 - 2\Im(\varphi_k)^2$ est de signature $(1,1)$.

Au total, les racines réelles jouent toutes pour $(1,0)$ dans la signature est les couples de racines complexes conjuguées jouent chacun pour $(1,1)$ dans la signature.

Finalement en notant r le nombre de racines réelles, on a :

$$(p,q) = (r,0) + \left(\frac{t-r}{2}\frac{t-r}{2}\right).$$

On en déduit ainsi $r = p - q$. ■

I.B Loi de la réciprocité quadratique (101) (120) (121) (123) (170) (190)

Théorème 2: Loi de la réciprocité quadratique

Pour tous p et q nombre premiers impairs distaincts, on a :

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

Démonstration. On calcule de deux manières différentes le cardinal de : $X = \{x = (x_1, \dots, x_p) \in \mathbb{F}_q \quad / \quad x_1^2 + \cdots + x_p^2 = 1\}$.

1. On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par translation. On a une action naturelle de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{F}_q$ par translation, on restreint alors simplement cette action. La relation stabilisateur orbite fournit que le cardinal d'une orbite divise le cardinal du groupe qui agit, i.e. p. Les orbites ont donc 1 élément ou p.

   On s'intéresse aux orbites à 1 élément. Il y a $1 + \left(\frac{p}{q}\right)$ orbite(s) à 1 élément. En effet les orbites à 1 élément vérifient $x_1 = x_2 = \cdots = x_p$ et $px_1^2 = 1$. Or cette dernière équation a 0 solution si p n'est pas un carré modulo q et en a 2 sinon.

   Alors l'équation aux classes nous donne que $\#X = 1 + \left(\frac{p}{q}\right) \mod p$

2. On considère maintenant les deux matrices suivantes :

$$A = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & a \end{pmatrix} \in \mathcal{M}_p(\mathbb{F}_q) \qquad \text{et} \qquad I_p = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \in \mathcal{M}_p(\mathbb{F}_q)$$

   où $a = (-1)^{p-1}$.

   Elles sont toutes deux symétriques donc représentent deux forment quadratiques sur $\mathbb{F}_q$. Or elles ont même rang et même déterminant (donc a fortiori même discriminant). Par le théorème de classification des forment quadratiques sur les corps finis, les deux matrices sont congruentes.

   Soit alors $P \in \mathrm{GL}_p(\mathbb{F}_q)$ tel que $I_p = {}^tPAP$.
   On peut alors écrire :

$$\begin{aligned} X &= \{x \in \mathbb{F}_q \quad / \quad {}^txx = 1\} \\ &= \{x \in \mathbb{F}_q \quad / \quad {}^txI_px = 1\} \\ &= \{P^{-1}x \in \mathbb{F}_q \quad / \quad {}^tx\,{}^tPI_pPx = 1\} \\ &= \{P^{-1}x \in \mathbb{F}_q \quad / \quad {}^txAx = 1\} \\ &= P^{-1}\{x \in \mathbb{F}_q \quad / \quad {}^txAx = 1\} \end{aligned}$$

   Donc X est en bijection avec

   $\{x \in \mathbb{F}_q \quad / \quad {}^txAx = 1\} = \{x = (y_1, z_1, y_2, z_2, \dots, y_q, z_d, t) \in \mathbb{F}_q \quad / \quad 2(y_1z_1 + \cdots + y_dz_d) + at^2 = 1\}$

   où $d = \frac{p-1}{2}$

   On compte le nombre d'élément de ce dernier ensemble.

— Si tous les y_i sont nuls, alors on choisit les z_i comme on veut dans $\mathbb{F}_q$ (il y a q^q choix) et l'équation $at^2 = 1$ a $1 + \left(\frac{a}{q}\right) = 1 + a^{\frac{q-1}{2}} = 1 + (-1)^{\frac{q-1}{2}\frac{p-1}{2}}$ solutions.

— l'un au moins des y_i est non nul (il y a $q^d - 1$ choix) et on fixe t (il y a q choix). Alors on obtient l'équation d'un hyperplan de $\mathbb{F}_q^d$. Il y a donc q^{d-1} choix pour les z_i.

Au total, on obtient :

$$\begin{aligned}\#X &= q^d \times \left(1 + (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\right) + \left(q^d - 1\right) \times q \times q^{d-1} \\ &= q^d \times \left(q^d + (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\right) \\ &= q^{p-1} + (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \times q^d\end{aligned}$$

3. Au total :

$$\#X = q^{p-1} + (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \times q^d = 1 + \left(\frac{p}{q}\right) \mod p$$

Or $q^{p-1} = 1 \mod p$. Et part la formule d'Euler, on a : $q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$.

On obtient donc ainsi le résultat annoncé mais modulo p. Or comme $p \neq 2$ et que les deux membres de l'égalité valent ± 1 dans $\mathbb{Z}$, on peut remonter cette égalité dans $\mathbb{Z}$, ce qui conclut.

■

I.C Dévissage de $O(p,q)$ (106) (155) (157) (158) (170) (171)

Théorème 3: Dévissage de $O(p,q)$

Soit $p,q \neq 0$. Il existe un homéomorphisme :

$$\mathrm{O}(p,q) \cong \mathrm{O}(p) \times \mathrm{O}(q) \times \mathbb{R}^{pq}$$

Démonstration. Soit $M \in \mathrm{O}(p,q)$,.

1. Commençons par montrer que $\mathrm{O}(p) \times \mathrm{O}(q)$ est stable par transposition, on a :

$$M \in \mathrm{O}(p,q) \Leftrightarrow M\mathrm{I}_{p,q}{}^tM = \mathrm{I}_{p,q} \Leftrightarrow {}^tM^{-1}\mathrm{I}_{p,q}M^{-1} = \mathrm{I}_{p,q} \Leftrightarrow {}^tM^{-1} \in \mathrm{O}(p,q) \Rightarrow {}^tM \in \mathrm{O}(p,q)$$

2. Par décomposition polaire, il existe deux matrices $O \in \mathrm{O}_n(\mathbb{R})$ et $S \in \mathscr{S}_n^{++}(\mathbb{R})$ telles que $M = OS$. On commence par montrer que S est dans $\mathrm{O}(p,q)$ puis le même résultat découlera pour O. Soit $T = {}^tMM$. Alors $S^2 = T \in \mathscr{S}_n^{++}(\mathbb{R})$ (attention de ne pas dire que $\mathscr{S}_n^{++}(\mathbb{R})$ est un groupe ! On peut justifier l'assertion précédente par le fait que les valeurs propres de S^2 sont les valeurs propres de S au carré).

   Du premier point, on en déduit : $T = {}^tMM \in \mathrm{O}(p,q)$.
   De plus, comme $\exp : \mathscr{S}_n(\mathbb{R}) \to \mathscr{S}_n^{++}(\mathbb{R})$ réalise un homéomorphisme il existe un unique $U \in \mathscr{S}_n(\mathbb{R})$ tel que $T = \exp U$.

$$\begin{aligned}
T \in \mathrm{O}(p,q) &\Leftrightarrow T\mathrm{I}_{p,q}{}^tT = \mathrm{I}_{p,q} \\
&\Leftrightarrow \exp U = T = {}^tT = \mathrm{I}_{p,q}T^{-1}\mathrm{I}_{p,q} = \mathrm{I}_{p,q}^{-1}(\exp U)^{-1}\mathrm{I}_{p,q} = \mathrm{I}_{p,q}\exp(-U)\mathrm{I}_{p,q} \\
&\Leftrightarrow \exp U = \exp\left(-\mathrm{I}_{p,q}U\mathrm{I}_{p,q}\right) \\
&\Leftrightarrow U = {}^tU = -\mathrm{I}_{p,q}^{-1}U\mathrm{I}_{p,q} \qquad (\exp : \mathscr{S}_n \to \mathscr{S}_n^{++} \text{ bijective}) \\
&\Leftrightarrow U\mathrm{I}_{p,q} + \mathrm{I}_{p,q}U = 0 \qquad (\text{condition linéaire, elle nous servira dans la dernière partie}) \\
&\Leftrightarrow \frac{U}{2}\mathrm{I}_{p,q} + \mathrm{I}_{p,q}\frac{U}{2} = 0 \\
&\Leftrightarrow \frac{U}{2} = -\mathrm{I}_{p,q}\frac{U}{2}\mathrm{I}_{p,q} \\
&\Leftrightarrow \exp\left(\frac{U}{2}\right) = \exp\left(-\mathrm{I}_{p,q}^{-1}\frac{U}{2}\mathrm{I}_{p,q}\right) = \mathrm{I}_{p,q}\left(\exp\left(\frac{U}{2}\right)\right)^{-1}\mathrm{I}_{p,q}.
\end{aligned}$$

   Or, on a : $\exp(U/2) \in \mathscr{S}_n(\mathbb{R})^{++}$ et $\exp^2(U/2) = \exp U = T$puis par unicité de la racine carrée : $\exp(U/2) = S$ et par suite $S \in \mathrm{O}(p,q)$ et aussi $O \in \mathrm{O}(p,q)$. Enfin la décomposition polaire $M = OS \mapsto (O,S)$ induit l'homéomorphisme :

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

3. Soit $O \in \mathrm{O}(p,q) \cap \mathrm{O}(n)$. On découpe O en blocs de tailles p et q.

   D'une part :

$$O = \begin{pmatrix} A & C \\ B & D \end{pmatrix} \in \mathrm{O}(p,q) \Leftrightarrow \begin{cases} {}^tAA - {}^tBB = \mathrm{I}_p \\ {}^tAC - {}^tBD = 0 \\ {}^tCA - {}^tDB = 0 \\ {}^tCC - {}^tDD = -\mathrm{I}_q \end{cases}$$

D'autre part :

$$O = \begin{pmatrix} A & C \\ B & D \end{pmatrix} \in \mathrm{O}(p,q) \Leftrightarrow \begin{cases} {}^tAA + {}^tBB = \mathrm{I}_p \\ {}^tAC + {}^tBD = 0 \\ {}^tCA + {}^tDB = 0 \\ {}^tCC + {}^tDD = \mathrm{I}_q \end{cases}$$

En sommant bien les relations obtenues, on a ${}^tAA = \mathrm{I}_p$ et ${}^tDD = \mathrm{I}_q$ et B et C sont nulles. On a donc :

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

4. On définit $L = \{U \in \mathscr{M}_n(\mathbb{R}), \quad U\mathrm{I}_{p,q} + \mathrm{I}_{p,q}{}^tU = 0\}$. Avec la relation établie au point 2. on obtient l'homéomorphisme :

$$\mathscr{S}_n(\mathbb{R}) \cap L \cong \mathrm{O}(p,q) \cap \mathscr{S}_n^{++}(\mathbb{R})$$

Soit $U = \begin{pmatrix} A & B \\ {}^tB & C \end{pmatrix} \in \mathscr{S}_n(\mathbb{R}) \cap L$. Alors $UI_{p,q} + I_{p,q}{}^tU = \begin{pmatrix} 2A & 0 \\ 0 & 2C \end{pmatrix}$. Donc $A = 0$ et $C = 0$ et B est quelconque de taille $p \times q$.

Finalement : $\mathrm{O}(p,q) \cap \mathscr{S}_n^{++}(\mathbb{R}) \cong \mathbb{R}^{pq}$, d'où au final l'homéomorphisme :

$$\mathrm{O}(p,q) \cong \mathrm{O}(p) \times \mathrm{O}(q) \times \mathbb{R}^{pq}$$

■

I.D Isométries et coloriages du cube et coloriages (101) (104) (105) (161) (190) (191)

Proposition 4

Le groupe des isométries positives du cube est

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

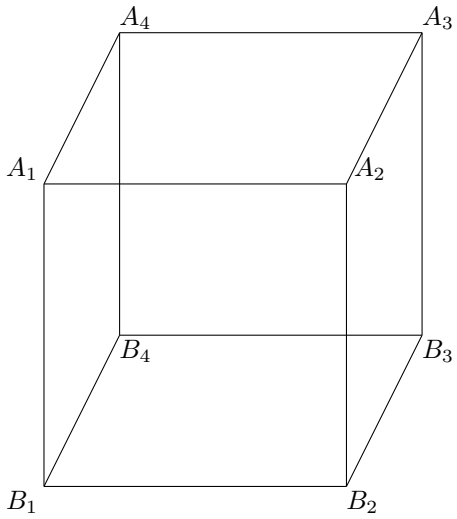
Démonstration. L'idée ici est d'exhiber une action de groupe sous la forme d'un morphisme de groupe, de montrer que cette action est fidèle et d'utiliser un système de générateurs particulier pour obtenir en plus la surjectivité.

1. Une isométrie préserve les longueurs donc transforme une grande diagonale (plus grande longueur dans le cube) en une grande diagonale. On note $\mathcal{D}$ l'ensemble des quatre grandes diagonales.

   On obtient ainsi l'action de $\mathrm{Iso}^+(C)$ sur l'ensemble $\mathscr{D} = \{D_1, D_2, D_3, D_4\}$ des grandes diagonales du cube (voir le dessin) définie par :

   $$\begin{aligned} \varphi : \mathrm{Iso}^+(C) &\longrightarrow \mathfrak{S}_4 \\ g &\longmapsto g_{1\ a} \end{aligned}$$

   C'est un morphisme de groupes car les distances sont conservées. On note $D_1 = [A_1, B_1]$ le segment non orienté.

2. L'action φ que nous venons de définir est fidèle.
   Soit en effet $g \in \ker(\varphi)$ (i.e. $g_{|\mathcal{D}} = \mathrm{id}$), montrons que g est le neutre. Comme g fixe les grandes diagonales alors pour $i = 1, 2, 3, 4$, g permute A_i et B_{i+2} ou les laisse tous deux fixes.

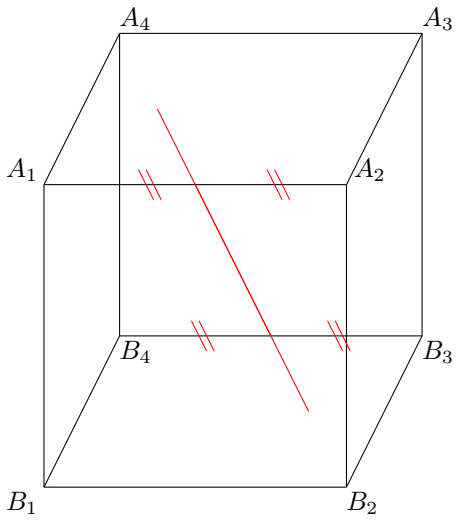
   Supposons que g laisse fixe A_1. On sait que g envoie A_2 sur A_2 ou sur B_2. Mais comme g est une isométrie on a aussi que g envoie A_2 sur A_2, A_4 ou B_1 puisque g préserve la longueur A_1A_2. Finalement g envoie A_2 sur A_2. On a de même que g fixe A_4 et B_1. Or (A_1, A_2, A_4, B_1) est un repère affine de l'espace donc g est le neutre.

   Supposons maintenant que g envoie A_1 sur B_1, alors en notant s la symétrie centrale du cube, on a que $g \circ s$ envoie A_1 sur A_1 et, d'après ce qui précède $g \circ s = \mathrm{id}$ mais g et id sont deux isométries positives et s est de déterminant -1. C'est donc absurde et ce cas est exclus.

   On déduit de ce deuxième point que $\mathrm{Iso}^+(C) \subset \mathfrak{S}_4$ (à isomorphisme près).

3. Pour obtenir l'égalité, il suffit de montrer qu'un système de générateurs de $\mathfrak{S}_4$ est réalisé par φ.

   Soit h la rotation d'angle π autour de l'axe rouge passant par les milieux des arêtes $[A_1, A_2]$ et $[B_3, B_4]$.



   Alors h : $A_1B_3 \longleftrightarrow A_2B_4$ i.e. $D_1 \longleftrightarrow D_2$ mais laisse fixe les autres grandes diagonales. Donc $\varphi(h) = (1\ 2)$.
   De même φ réalise $(2\ 3)$ et $(3\ 4)$. Or ces trois transpositions engendrent $\mathfrak{S}_4$. Donc φ est surjectif et ceci conclu la preuve de la proposition.

■

Application 5: Coloriages du cube

Soit $n \in \mathbb{N}^*$ un nombre de couleurs. Alors le nombres de manières différentes de colorier le cube est :

$$\frac{1}{24}\left(n^6 + 3n^4 + 12n^3 + 8n^2\right)$$

Démonstration. Ici il va s'agir d'utiliser une bonne action de groupe puis la formule de Burnside et enfin de compter pour trouver le résultat.

Soient Γ l'ensemble des n couleurs et Φ l'ensemble des faces du cube. Un coloriage du cube est une fonction $\Phi \to \Gamma$. On a donc l'action :

$$\begin{array}{ccccc} \mathrm{Iso}^+(C) & \times & \mathcal{F}(\Phi,\Gamma) & \to & \mathcal{F}(\Phi,\Gamma) \\ g & , & f & \mapsto & f \circ g^{-1} \end{array}$$

(on met g^{-1} parce qu'on regarde la couleur par rapport à la face de départ)
On dit que deux coloriages sont identiques s'ils sont dans la même orbite pour cette action. Trouver le nombre coloriages (différents) c'est donc trouver le nombre d'orbites. On note Ω l'ensemble des orbites.
La formule de Burnside donne :

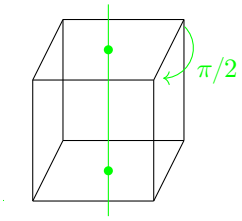
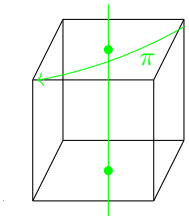
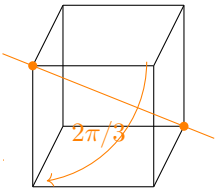
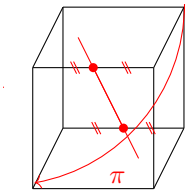
$$\#\Omega = \frac{1}{|\mathrm{Iso}^+(C)|} \sum_{g \in \mathrm{Iso}^+(C)} \#\mathrm{fix}(g).$$

Mais, soit $f \in \mathcal{F}(\Phi,\Gamma)$ et soit $g \in \mathrm{Iso}^+(C)$, on a :

$$f \in \mathrm{fix}(g) \iff f = f \circ g^{-1} \iff f \text{ est constante sur chaque orbite de l'action } \langle g \rangle \curvearrowright \Phi$$

Et chacune de ces orbites peut être coloriée de n couleurs.
A g fixé, il y a donc $n^{\rho(g)}$ possibilités, où $rho(g)$ désigne le nombre d'orbite de $\langle g \rangle \curvearrowright \Phi$. Donc $\#\mathrm{fix}(g) = n^{\rho(g)}$.

Il ne reste donc plus qu'à dresser un tableau et à compter !

$\mathrm{Iso}^+(C)$	**Nombre**	**Dessin**	**Nombre d'orbites**
id	1		6
centres et angle $\pm\pi/2$	3+3		3
centres et angle π	3		4
sommets et angle $\pm 2\pi/3$	4+4		2
arêtes et angle π	6		3
	$\sum = 24$		

La justification du nombre d'orbite est laissée au lecteur (elle n'est pas compliquée mais très géométrique et se voit bien avec les mains).
Au total, en regroupant toutes les données que l'on a exhibées, on retrouve la formule avancée. ■

I.E Automorphismes diagonalisables (101) (104) (106) (123) (151) (152) (190)

Théorème 6: Dénombrement de $DL(E)$

Soient $n \in \mathbb{N}$ et $q = p^r$ où p est premier et $r \in \mathbb{N}^*$. Soit $DL_n(\mathbb{F}_q)$ l'ensemble des matrices inversibles diagonalisables de taille n sur $\mathbb{F}_q$. Ou soit E un $\mathbb{F}_q$-espace vectoriel de dimension n. La cardinal de $DL(E)$ est :

$$|DL_n(E)| = \sum_{\substack{(n_k)_{1\leqslant k\leqslant q-1}\in\mathbb{N}^{q-1} \\ n_1+\cdots+n_{q-1}=n}} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q-1} |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}$$

Démonstration. Soit E un $\mathbb{F}_q$-e.v. de dimension n. On va commencer par décrire les éléments de $DL(E)$, puis en faisant agir $\mathrm{GL}(E)$ sur un ensemble en bijection avec $DL(E)$, on déterminera le cardinal cherché.

1. Montrons que $DL(E) = \{u \in \mathrm{GL}(E) \quad / \quad u^{q-1} = u\}$.
   On pense raisonnablement à cela car on sait que le groupe multiplicatif d'un corps fini est cyclique.

   • Soit $u \in DL(E)$. Comme u est diagonalisable, son polynôme minimal est scindé simple sur $\mathbb{F}_q$:

   $$\mu_u = \prod_{\lambda\in\mathrm{Sp}(u)} (X-\lambda).$$

   Comme $\mathrm{Sp}(u) \subset \mathbb{F}_q^\times$, puisqu'il est scindé simple : $\mu_u \mid \prod_{\lambda\in\mathbb{F}_q^\times} (X-\lambda) = X^{q-1} - X$. Donc $u^{q-1} = u$.

   • Réciproquement, si $u^{q-1} = u$, alors u admet un polynôme annulateur scindé simple $(X^{q-1} - 1)$, donc est diagonalisable.

Par le lemme des noyaux, on a donc :

$$E = \bigoplus_{\lambda\in\mathbb{F}_q^\times} \ker(u - \lambda\mathrm{id}).$$

2. Dans tout ce qui suit, E_k désignera un sous-espace vectoriel de E.
   On note :

   $$\mathcal{F} = \left\{ (E_k)_{1\leqslant k\leqslant q-1} : E = \bigoplus_{k=1}^{q-1} E_k \right\}.$$

   Montrons que E est $\mathcal{F}$ ont même cardinal. Pour cela on définit l'application suivante :

   $$\varphi : \begin{array}{ccc} DL_n(E) & \longrightarrow & \mathcal{F} \\ u & \longmapsto & (\ker(u - \lambda_k\mathrm{id}))_{1\leqslant k\leqslant q-1} \end{array}.$$

   • Cette application est bien définie par le lemme des noyaux.
   • Elle est injective car si $\varphi(u) = \varphi(v)$ alors $\forall \lambda \in \mathbb{F}_q^\times \quad \forall x \in \ker(u - \lambda\mathrm{id}) = \ker(v - \lambda\mathrm{id}$, on a $u(x) = \lambda x = v(x)$. Mais comme $E = \bigoplus E_k$, on a donc $u = v$.
   • Elle est surjective car si $(E_k) \in \mathcal{F}$ alors on considère u tel que $u_{|E_k} = \lambda_k \mathrm{id}_{E_k}$. Alors $u \in DL(E)$ et $\varphi(u) = (E_k)$

Il en résulte que :

$$|DL(E)| = |\mathcal{F}|.$$

Et c'est ce dernier cardinal que l'on va chercher à expliciter grâce à une action bien choisie.

3. Pour $n_1, \dots, n_{q-1}$ entiers tels que $\sum_{k=1}^{q-1} n_k = n$, on note :

$$\mathcal{F}_{(n_1,\dots,n_{q-1})} = \left\{ (E_k)_{1\leqslant k\leqslant q-1} \in \mathcal{F} : \forall k \in [\![1, q-1]\!], \dim(E_k) = n_k \right\}$$

Et on a alors que ces ensembles partitionnent $\mathcal{F}$.

Soit $n_1, \dots, n_{q-1}$ entiers tels que $\sum_{k=1}^{q-1} n_k = n$. On considère l'action suivante :

$$\psi : \begin{array}{ccccc} \mathrm{GL}(E) & \times & \mathcal{F}_{(n_1,\dots,n_{q-1})} & \to & \mathcal{F}_{(n_1,\dots,n_{q-1})} \\ u & , & (E_k)_k & \mapsto & (u(E_k))_k \end{array}.$$

• ψ est bien définie car si $u \in \mathrm{GL}(E)$ et $(E_k) \in \mathcal{F}_{(n_1,\dots,n_{q-1})}$ alors $E = u(E)$ et $\dim(u(E_k)) = \dim(E_k)$.
• Elle définit bien une action car :
  * $\mathrm{id} \cdot (E_k) = (E_k)$;
  * $(u \circ v) \cdot (E_k) = (u \circ v(E_k)) = u \circ (v(E_k)) = u \cdot (v \cdot E_k))$.

• Elle est transitive car si $(E_k) \in \mathcal{F}_{(n_1,\dots,n_{q-1})}$ et $(F_k) \in \mathcal{F}_{(n_1,\dots,n_{q-1})}$, alors en considérant des bases $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_{q-1})$, où $\mathcal{B}_k$ est une base de E_k, et $\mathcal{C} = (\mathcal{C}_1, \dots, \mathcal{C}_{q-1})$, où $\mathcal{C}_k$ est une base de F_k ; et $u : \mathcal{B} \mapsto \mathcal{C}$ (qui est alors entièrement déterminé et bien défini car les bases ont même cardinal) on a clairement $(F_k) = u((E_k))$.

4. Il ne nous reste plus qu'à étudier cette action pour conclure.

Montrons que le stabilisateur de $(E_k)_{1\leqslant k\leqslant q}$ a pour cardinal $\prod_{k=1}^{q-1} |GL_{n_k}(\mathbb{F}_q)|$. En effet :

• on a que $u \in \mathrm{Stab}\left((E_k)_{1\leqslant k\leqslant q-1}\right)$ si et seulement si par définition $u(E_k) \subseteq E_k$ pour tout $1 \leqslant k \leqslant q-1$. Mais pour des raisons de dimensions on a même $u \in \mathrm{Stab}\left((E_k)_{1\leqslant k\leqslant q-1}\right)$ si et seulement si $u(E_k) = E_k$ pour tout $1 \leqslant k \leqslant q-1$, soit si et seulement si $u_{|E_k} \in \mathrm{GL}(E_k)$ pour tout $1 \leqslant k \leqslant q-1$. Donc $\mathrm{Stab}\left((E_k)_{1\leqslant k\leqslant q}\right)$ est en bijection avec les matrices diagonales par blocs dont les blocs ont pour tailles $n_1, \dots, n_{q-1}$ sont des matrices inversibles. On a donc

$$\left|\mathrm{Stab}\left((E_k)_{1\leqslant k\leqslant q-1}\right)\right| = \prod_{k=1}^{q-1} |\mathcal{GL}_{n_k}(\mathbb{F}_q)|$$

L'action étant transitive, l'équation aux classes (ou la relation orbite/stabilisateur) donne :

$$\#\left(\mathcal{F}_{(n_1,\dots,n_{q-1})}\right) \times \left|\mathrm{Stab}\left((E_k)_{1\leqslant k\leqslant q-1}\right)\right| = |\mathrm{GL}(E)|$$

c'est-à-dire

$$\#\left(\mathcal{F}_{(n_1,\dots,n_{q-1})}\right) = \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}.$$

Et on conclut en utilisant la partition de $\mathcal{F}$.

■

I.F Forme normale de Smith (122) (142) (162)

Soit (A, δ) un anneau euclidien. Soient $m, n \in \mathbb{N}^*$.

Théorème 7: Forme normale de Smith

Pour tout $M \in \mathcal{M}_{m,n}(A)$, il existe $P \in \mathrm{GL}_m(A)$ et $Q \in \mathrm{GL}_n(A)$ telles que :

$$M = P \begin{pmatrix} d_1 & & & & (0) \\ & \ddots & & & \\ & & d_s & & \\ & & & 0 & \\ (0) & & & & \ddots \\ & & & & & 0 \end{pmatrix} Q$$

avec $d_1, \cdots, d_s \in A$ tels que $d_1 | \cdots | d_s$, et les d_i sont uniques au sens où si

$$M \sim \begin{pmatrix} d'_1 & & & & (0) \\ & \ddots & & & \\ & & d'_t & & \\ & & & 0 & \\ (0) & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

alors $t = s$ et $d_i \sim_A d'_i$.

Démonstration. Il s'agit d'une preuve algorithmique.

Voici l'algorithme :

1. Si $M = \mathbf{O}$ alors renvoyer M ;
   Sinon passer à l'étape 2
2. Il existe i_0, j_0 tel que $M_{i_0,j_0} \neq 0$.
   Faire $C_1 \longleftrightarrow C_{i_0}$ et $L_1 \longleftrightarrow L_{j_0}$. et passer à l'étape 3 ;

$$M \sim \begin{pmatrix} \overset{\neq 0}{m_{1,1}} & & \\ & * & \\ & & \end{pmatrix}$$

3. On effectue la division euclidienne de $m_{i,1}$ par $m_{1,1}$:

$$m_{i,1} = q_i \times m_{1,1} + r_i \qquad \text{avec} \quad \delta(r_i) < \delta(m_{1,1})$$

   Faire $L_i \longleftarrow L_i - q_i L_1$.
   Si il existe $i > 1$ tel que $m_{i,1} \neq 0$ alors Faire $L_1 \longleftrightarrow L_i$ et retourner à 3 ;
   Sinon passer à 4 ;

$$M \sim \begin{pmatrix} m_{1,1} & & \\ 0 & & \\ 0 & & \\ \vdots & * & \\ 0 & & \\ 0 & & \end{pmatrix}$$

4. On procède de la même manière qu'à l'étape précédente mais sur la première ligne :

$$m_{1,j} = q_j \times m_{1,1} + r_j \qquad \text{avec} \quad \delta(r_j) < \delta(m_{1,1})$$

Faire $C_j \longleftarrow C_j - q_j C_1$.
Si il existe $j > 1$ tel que $m_{1,j} \neq 0$ alors Faire $C_1 \longleftrightarrow C_j$ et retourner à 3 ;
Sinon passer à 5 ;

$$M \sim \begin{pmatrix} m_{1,1} & 0 \\ 0 & \begin{pmatrix} & \\ & M' \\ & \end{pmatrix} \end{pmatrix}$$

5. Si il existe (i_1, j_1) tel que $m_{1,1} \nmid m_{i_1,j_1}$ alors Faire $C_1 \longleftarrow C_1 + C_{j_1}$ et retourner à 3 ;
Sinon retourner à 1 avec la matrice M'.

Justifions la terminaison de cet algorithme. Il y a seulement les étapes 3,4 et 5 où l'on peut effectuer un retour en arrière, sinon on passe toujours à l'étape suivante.

* En 3, lors d'un retour en 3 $\delta(m_{1,1})$ décroît strictement, or c'est un entier naturel, donc on ne peut faire qu'un nombre fini de retour en 3 et on passe à l'étape 4.
* En 4 soit en avance en 5 soit on retourne en 3. Si on retourne en 3 alors on le fait en faisant décroître $\delta(m_{1,1})$. Donc on fait qu'un nombre fini de retour en 3 pour la même raison et on passe à l'étape 5.
* En 5, si on retourne à 3 (après être retourné en 3) alors d'après la condition de retour il existe i tel que $\delta(m_{i,1}) < \delta(m_{1,1})$ donc on fait un autre retour en 3 et donc $\delta(m_{1,1})$ décroît encore strictement. On ne fait toujours qu'un nombre fini de retour en 3. On fini donc par obtenir une matrice

$$\begin{pmatrix} m_{1,1} & 0 \\ 0 & \begin{pmatrix} & \\ & M' \\ & \end{pmatrix} \end{pmatrix}$$

avec $m_{1,1} | M'$.
On applique alors l'algorithme à M' (si elle existe) qui est de taille $(m-1, n-1)$. On fait donc décroître strictement la taille de la matrice (le produit des deux dimensions) qui est un entier naturel donc il y a un nombre fini de matrice sur lesquelles on travaille.

Finalement on sort de l'algorithme.

Il nous reste à démontrer l'unicité.
On note $\Delta_j(M)$ le pgcd des mineurs de taille j de M.

Supposons

$$M \sim D = \begin{pmatrix} d_1 & & & & & (0) \\ & \ddots & & & & \\ & & d_s & & & \\ & & & 0 & & \\ & & & & \ddots & \\ (0) & & & & & 0 \end{pmatrix} \qquad \text{et} \qquad M \sim D' = \begin{pmatrix} d'_1 & & & & & (0) \\ & \ddots & & & & \\ & & d'_t & & & \\ & & & 0 & & \\ & & & & \ddots & \\ (0) & & & & & 0 \end{pmatrix}.$$

On démontre le résultat intermédiaire suivant :

Lemme 8:

Si $U \sim U'$ alors $\Delta_j(U) \sim_A \Delta_j(U')$ pour tout j.

Démonstration. Si $U = PU'$ alors les lignes de U sont des combinaisons linéaires de celles de U'. Donc par multilinéarité du déterminant un mineur de taille j de U est combinaison linéaire de mineurs de tailles j de U'. Donc :

$$\Delta_j(U) \in \langle \Delta_j(U') \rangle \qquad \text{i.e.} \qquad \Delta_j(U') | \Delta_j(U).$$

Comme on a $U' = P^{-1}U$, on a aussi de la même manière $\Delta_j(U) | \Delta_j(U')$.

Au total si $U = PU'$ alors $\Delta_j(U) \sim_A \Delta_j(U')$.

Si $U = U'Q$, alors on obtient $\Delta_j(U) \sim_A \Delta_j(U')$ directement du premier point simplement en transposant ($\det(U) = \det({}^tU)$).

Le cas général se déduit alors facilement. ■

Finalement $M \sim D \sim D'$ entraîne $\Delta_j(D) \sim_A \Delta_j(D')$ pour tout j donc t et s sont égaux et $d_s \sim_A d'_s$ (regarder Δ_1) puis par induction comme $d_1 \dots d_j \sim_A d'_1 \dots d'_j$, on a $\forall i \quad d_i \sim_A d'_i$ et ceci conclut l'unicité. ■

I.G $SO(3)$ et les quaternions (102) (103) (108) (151) (158) (161) (191)

Théorème 9:

Soit G le groupe des quaternions de norme 1. On a l'isomorphisme suivant :

$$G/\{-1,1\} \xrightarrow{\sim} SO_3(\mathbb{R})$$

On note N la norme qui est une forme quadratique réelle associée à la forme polaire $q_1, q_2 \mapsto \frac{1}{2}(q_1\overline{q_2} + q_2\overline{q_1})$. C'est évidemment une forme quadratique non dégénérée.

$$G = \{q \in \mathbb{H} \quad / \quad N(q) = q\overline{q} = 1\} \simeq \mathbb{S}^3$$

Démonstration. Comme $\mathbb{H}$ n'est pas commutatif, l'idée est de faire agir G sur le corps des quaternions $\mathbb{H}$ par automorphisme intérieur (action par conjugaison). L'idée de la preuve est de se rapprocher pas à pas de $SO(3)$, en commençant par aller dans $O(4)$ puis en décomposant $\mathbb{H}$ pour aller dans $O(3)$, utiliser la connexité de $\mathbb{S}^4$pour être dans $SO(3)$ et enfin utiliser les générateurs de $SO(3)$ pour conclure que c'est $SO(3)$.

1. Soit S_q la conjugaison par q dans $\mathbb{H}$.
   Soit $q \in G$. On a :
   $$\begin{array}{ccc} \mathbb{H} & \to & \mathbb{H} \\ q' & \mapsto & qq'\overline{q} = qq'q^{-1} \end{array}$$
   C'est une application $\mathbb{R}$-linéaire. Comme de plus $S_{\overline{q}} = (S_q)^{-1}$, elle est bijective. Notons tout de suite une autre relation importante $S_{q_1q_2} = S_{q_1} \circ S_{q_2}$:
   $$S_{q_1q_2}(q) = q_1\ q_2\ q\ \overline{q_1}\ \overline{q_2} = S_{q_1}(S_{q_2}(q)).$$
   Nous avons en outre, puisque $q \in G$:
   $$N(S_q(q')) = N(q\ q'\ \overline{q}) = \underbrace{N(q)}_{=1}N(q')\underbrace{N(\overline{q})}_{=1} = N(q').$$
   Donc $S_q \in O(N) \simeq O(4)$ pour tout $q \in G$.
2. On note $\mathbb{P}$ l'ensemble des quaternions purs, alors $\mathbb{H} = \mathbb{R} \overset{N}{\perp\!\!\!\oplus} \mathbb{P}$ mais par $\mathbb{R}$-linéarité il vient alors que $(S_q)_{|\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$. Donc $S_q(\mathbb{P}) = \mathbb{P}$ et on désigne alors par s_q le $\mathbb{R}$-endomorphisme induit sur $\mathbb{P}$. On a donc $s_q \in O(N_{|\mathbb{P}}) \simeq O(3)$.
3. Soit $s : \begin{array}{ccc} G & \to & O(3) \\ q & \mapsto & s_q \end{array}$. C'est un morphisme de groupe par la propriété importante remarquée dans la première partie. On va utiliser le théorème d'isomorphisme pour conclure.

   $$\ker(s) = \{q \in G \quad / \quad s_q = \mathrm{id}\} = \{q \in G \quad / \quad q \in Z(G)\} = G \cap \mathbb{R} = \{+1, -1\}.$$
   Munissons maintenant $O(3)$ de sa topologie usuelle (sous-espace de $\mathbb{R}^9$). En écrivant s_q dans la base (i,j,k), si on note $q = a + ib + jk + kd$ avec $a,b,c,d \in \mathbb{R}^4$, on constate que $s_q(i), s_q(j), s_q(k)$ sont des polynômes de degré 2 en a,b,c,d. Donc s est une application polynomiale en les composantes de q, et donc s est continue.

   Il résulte de cela que $\det \circ s : G \to \{-1,+1\}$ est une application continue. Or $G \simeq \mathbb{S}^3$ est connexe et la connexité est préservée par image continue et $s(1) = \mathrm{id}$. Donc $\det \circ s(G) = \{1\}$ et donc $S(G) \subset SO(3) \simeq SO(P)$.

4. Pour conclure il reste à montrer que $s(G)$ contient un système de générateurs de $SO(3)$ (les retournements).

   Soit $p \in \mathbb{P} \cap G$ (un axe normalisé). Alors $s_p(p) = p \overbrace{p\,\overline{p}}^{=N(p)=1} = p$. Donc s_p est une rotation d'axe p (on sait que $s_p \in SO(3)$). Mais $p \in \mathbb{P} \implies \overline{p} = -p$ puis $p \in G \implies p^2 = -p\overline{p} = -1$ donc $(s_p)^2 = s_{p^2} = s_{-1} = \mathrm{id}$.

   On a donc obtenu que s_p est une rotation d'axe p et est une involution, donc est d'ordre 1 ou 2. C'est donc l'identité ou un retournement (d'axe p).
   Or si $\mathbb{P}\backslash\{0\} \ni q \perp p$ i.e. $q\overline{p} + p\overline{q} = 0$ i.e. $-qp - pq = 0$; alors $s_p(q) = pqp^{-1} = pq\overline{p} = -q$. Donc s_p n'est pas triviale et c'est donc un retournement d'axe p.
   Or ceci vaut pour tout $p \in \mathbb{P}\backslash\{0\}$. Donc $s(G)$ contient tous les retournements dans $SO(3)$, mais puisque $SO(3)$ est engendré par les retournements, on a donc $s(G) \simeq SO(3)$.
   D'où finalement le résultat avancé en utilisant le théorème d'isomorphisme.

   ■

I.H Réduction de Frobenius (148) (150) (151) (159)

Lemme 10: Noyaux itérés

Soit u un endomorphisme. La suite $\left(\ker(P^k(u))\right)_k$ est strictement croissante puis stationnaire.

Démonstration. Soit k le premier entier tel que $\ker(P^k(u)) = \ker(P^{k+1}(u))$ (un tel cas existe car on est en dimension finie).
Montrons par récurrence que la suite stationne à partir de ce rang.

Initialisation : pour $n = 1$ c'est l'hypothèse

Hérédité : Soit $n \geqslant 1$, supposons la propriété vraie au rang n, c'est-à-dire : $\ker(P^k(u)) = \ker(P^{k+n}(u))$. Soit $x \in \ker(P^{k+n+1}(u))$. Alors $P^{k+n+1}(u)(x) = P^{k+n}(P(u)(x))$. Donc $P(u)(x) \in \ker(P^{k+n}(u)) = \ker(P^k(u))$ c'est-à-dire $u \in \ker(P^{k+1}(u)) = \ker(P^k(u))$. On a donc :

$$\ker(P^k(u)) \subset \ker(P^{k+n+1}(u)) \subset \ker(P^k(u))$$

et ceci conclut la preuve du lemme. ■

Proposition 11

Soit u un endomorphisme. Alors il existe $x \in E$ tel que $\mu_{u,x} = \mu_u$.

Démonstration. On écrit $\mu_u = \prod_{k=1}^r P_k^{\alpha_k}$ comme produit d'irréductibles distincts et on prend $x_k \in \ker(P_k^{\alpha_k}) \backslash \ker(P_k^{\alpha_k - 1})$. On notera que x_k est bien défini par minimalié de μ_u. Alors en prenant $x = x_1 + \cdots + x_r$, on obtient : $\mu_{u,x} = \prod_{k=1}^r P_k^{\alpha_k} = \mu_u$. ■

Lemme 12:

Soit $u \in \mathcal{L}(E)$. Soit $x \in E$ tel que $\mu_{u,x} = \mu_u$, alors $E_{u,x} := \{P(u)(x) \ / \ P \in \mathbb{K}[X]\}$ (le plus petit sous-espace stable par u contenant x) admet un supplémentaire stable

Démonstration. Notons p la dimension de $E_{u,x}$.
On pose :

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

Alors $(e_1, \ldots, e_p)$ forme une base de $E_{u,x}$ car $\deg(\mu_{u,x}) = \deg(\mu_u) = p$ et la famille ainsi créée est stable par u.

On complète $(e_1, \ldots, e_p)$ en une base $(e_1, \ldots, e_n)$ de E et on considère la base duale $(e_1^*, \ldots, e_n^*)$. On définit $F = \bigcap_{j=0}^{+\infty} \ker(e_p^* \circ u^j)$. On a immédiatement que F est stable par u.

Montrons $F \oplus E_{u,x} = E$:

— $F \cap E_{u,x} = \{0\}$:

Si $y \in F \cap E_{u,x}$, alors il s'écrit :

$$y = \sum_{j=0}^{p-1} a_j e_{j+1} = \sum_{j=0}^{p-1} a_j u^j(x) \in E_{u,x}$$

De plus $y \in F$ donc pour tout j :

$$e_p^* \circ u^j(y) = 0 \iff \sum_{k=0}^{p-1} a_j e_p^*\left(u^{k+j}(x)\right) = 0$$

Pour $j = 0$ on obtient donc $a_{p-1} = 0$, puis pour $j = 1$ on a $a_{p-2} = 0$, etc et finalement $y = 0$.

— $\dim F + \dim G = n$:
On a $\dim(E_{u,x}) = \deg(\mu_{u,x}) = \deg(\mu_u) = p$. Donc $F = \cap_{j=0}^{p-1} \ker(e_p^* \circ u^j)$. La famille $(e_p^* \circ u^0, \dots, e_p^* \circ u^{p-1}$ est libre car si :

$$\sum_{j=0}^{p-1} a_j e_p^* \circ u^j = 0_{E*}$$

alors en évaluant sur la famille $\big(x, u(x), \dots, u^{p-1}(x)\big)$, on obtient $a_j = 0$ pour tout j, puis la famille est libre.
On a donc que F est intersection de p hyperplans associés à des formes linéaires indépendantes.
On a donc que F est de codimension p.

Par argument de dimension on a donc finalement :

$$E_{u,x} \oplus F = E.$$

Et $E_{u,x}$ admet donc un supplémentaire stable. ■

Théorème 13: Réduction de Frobenius

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n.
Soit $u \in \mathcal{L}(E)$.
Alors il existe une unique suite finie $(P_1, \dots, P_r)$ de polynômes unitaires et une unique décomposition $E = \bigoplus_{i=1}^{r} E_i$ telle que $\forall i \in [\![1, \dots, r-1]\!] \quad P_{i+1} | P_i$ et $\forall i \in [\![1, \dots, r-1]\!] \quad u_{|E_i}$ est un endomorphisme cyclique de polynôme minimal de P_i.

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

— ***Existence*** : On procède par récurrence sur la dimension de E.

Initialisation : si $\dim(E) = 1$ alors il n'y a rien à faire.

Hérédité : soit $n \in \mathbb{N}^*$. Soit E un espace vectoriel de dimension $n+1$. Supposons la proposition vraie jusqu'au rang n.
Soit $x \in E$ tel que $\mu_u = \mu_{u,x}$.
On pose $E_1 = E_{u,x}$. Alors u est cyclique sur E_1. Soit F un supplémentaire de E_1 stable par u.
On a $\mu_1 = \mu_{u,x} = P_1$.

Par hypothèse de récurrence, il existe alors $P2, \dots, P_r$ telle que $F = \bigoplus_{i=2}^{r} E_i$ et $P_{i+1} | P_i$ pour tout $i \in [\![2, r-1]\!]$ et $P_2 | \mu_u$ car comme $\mu_u(u_{|F}) = 0$ alors $\mu_{u_{|F}} | \mu_u$.

On a alors que la décomposition : $E = \bigoplus_{i=1}^{r} E_i$ vérifie les conditions.

— ***Unicité*** : soient $(P_1, \dots, P_r)$ et $(Q_1, \dots, Q_s)$ deux familles de polynômes associées à deux décompositions $E = \bigoplus_{i=1}^{r} E_i$ et $E = \bigoplus_{i=1}^{s} F_i$.
Par construction on a $P_1 = Q_1 = \mu_u$ et

$$\sum_{i=1}^{r} \deg(P_i) = \sum_{i=1}^{r} \dim(E_i) = \dim(E) = \sum_{i=1}^{s} \deg(F_i) = \sum_{i=1}^{s} \deg(Q_i)$$

La première et la dernière égalités proviennent de la cyclicité de u sur chacun des sous-espaces.

Supposons que ces deux réductions soient distinctes. On remarquera que lon ne peut pas avoir l'égalité de tous les polynômes mais $r \neq s$.
On note j l'indice minimal tel que $P_i \neq Q_i$.

Pour tout $i \geqslant j$, on a $P_i | P_j$ et $Q_i | Q_j$ et on a donc $P_j(u_{|E_i}) = 0$.
Puis $P_j(u)(E) = \bigoplus_{i=1}^{r} P_j(u)(E_i) = \bigoplus_{i=1}^{j-1} P_j(u)(E_i)$. Or

$$P_j(u)(E) = \bigoplus_{i=1}^{r} P_j(u)(F_i) = \bigoplus_{i=1}^{r} P_j(u)(E_i).$$

Donc en regardant les dimensions, on obtient :

$$\forall j \leqslant i \leqslant s \qquad \dim(P_j(u)(F_i)) = 0.$$

En effet, on a :

$$\forall i < j \qquad \dim\left(P_j(u)(E_i)\right) = \operatorname{rg}(P_j(u_{E_i})) = \operatorname{rg}(P_j(u_{F_i})) = \dim\left(P_j(u)(F_i)\right)$$

car les deux endomorphismes sont cycliques et de même polynôme minimal par minimalité de j.
Cela entraîne :

$$\forall j \leqslant i \leqslant s \qquad P_j(u_{|F_i}) = 0$$

D'où :

$$P_j(u_{|F_j}) = 0$$

On obtient alors que P_j annule $u_{|F_j}$ et donc $\mu_{u_{|F_j}} = Q_j | P_j$.

Par symétrie des rôles de P et Q, on a $P_j | Q_j$. Ils sont donc associés et comme ils sont unitaires, ils sont égaux. C'est absurde.

■

Détails supplémentaires

Remarque 14

Si $p = \deg(\mu_u)$, alors $\mathbb{K}[u] := \{P(u) \mid P \in \mathbb{K}[X]\}$ est un sev de $\mathcal{L}(E)$ de dimension p, dont une base est $(\mathrm{Id}_E, u, \ldots, u^{k-1})$.

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

Démonstration.

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

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

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

Donc

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

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

Idem avec

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

■

I.I Théorème de Jordan-Chevalley (150) (152) (156)

Théorème 15: Jordan-Chevalley

Soit $k = \mathbb{C}$ et $A = \mathcal{M}_n(k)$. (ou k un corps parfait et A une k-algèbre de dimension finie.
Alors pour tout $a \in A$ il existe un unique couple (s, n) d'éléments de A tels que :
- s est semi-simple
- n est nilpotent
- $sn = ns$
- $a = s + n$

De plus, s et n sont des polynômes en a et μ_s est la partie sans facteur carré de μ_a.

Démonstration.
Unicité :
Si (s, n) et (s', n') sont deux décompositions qui vérifient les conditions, alors :

$$s - s' = n' - n$$

Puis s et s' sont des polynômes en a, ils commutent et s' commute avec u car :

$$s' \circ u = s' \circ (s' + n') = (s')^2 + s' \circ n' = (s')^2 + n' \circ s' = u \circ s'$$

Ainsi, en se plaçant dans un corps de décomposition de μ_u par exemple, on a que s et s' sont tous deux diagonalisables. Ainsi, comme ils commutent ils sont diagonalisables dans une même base et donc $s - s'$ est diagonalisable dans cette même base.
De même, n et n' commutent et donc $n' - n$ est nilpotente. Finalement on a : $s - s' = n' - n$ est diagonalisable et nilpotente. Il s'agit donc de l'endomorphisme nul, ce qui conclut à l'unicité de la décomposition.

Existence :
On montre l'existence par une idée de Chevalley : on va fabriquer s comme racine de $P(x) = 0$ par la méthode de Newton !

Avec $P = \text{rad}(\mu_a)$: si $\mu_a = \prod_{i=1}^{r} P_i^{\alpha_i}$ alors $P = \prod_{i=1}^{r} P_i$. En caractéristique nulle on peut écrire $P = P_1 \dots P_r = \frac{\mu_a}{\mu_a \wedge \mu_a'}$.

Tous les calculs se font dans $k[a]$.
Commençons par justifier que l'on utilise la méthode de Newton : si $u = s + n$ avec s racine de P et n nilpotent (infinitésimal) alors on est assez proche de la racine s pour converger vers cette racine.

Par construction il existe r (par exemple $r = \max(\alpha_i)$) tel que $\mu_a | P^r$. Donc, $P(a)^r = 0$. On note $\varepsilon = P(a)$. Il s'agit donc d'un élément nilpotent car $P^{\deg(\mu_a)}$ est divisible par μ_a et donc $P^{\deg(\mu_a)}(a) = 0$.
Et si x est un élément de l'idéal engendré par ε^n alors on note $x = \mathcal{O}(\varepsilon^n)$. Les facteurs P_i sont à racines simples sur $\bar{k}$ car k est parfait (définitions équivalentes d'un corps parfait).
En particulier, P et P' sont premiers entre eux. On écrit alors une relation de Bézout entre ces deux éléments :

$$UP + VP' = 1$$

et si l'on trouve que s est racine de P, alors on aura :

$$U(s)P(s) + V(s)P'(s) = V(s)P'(s) = 1.$$

Donc $P'(s) \in k[u]^\times$.
On sait déjà que $P'(a) \in k[u]^\times$ car $P | \mu_a | P^{\deg(\mu_a)}$ et on a Bézout entre μ_a et P'.

On introduit maintenant l'algorithme de Newton :

$$\begin{cases} a_0 & = & a \\ a_{n+1} & = & a_n - \frac{P(a_n)}{P'(a_n)} = a_n - P'(a_n) \circ P(a_n) \end{cases}$$

où l'on notera bien que le quotient à un sens car $k[u]$ est une k-algèbre commutative.

On montre par récurrence les trois points suivants :

(i) a_n est bien défini

(ii) $P(a_n) = \mathcal{O}\left(\varepsilon^{2^n}\right)$

(iii) $a_n - a = \mathcal{O}(\varepsilon)$

Initialisation : Pour le cas $n = 0$, on a $P(a_0) = P(a) = \varepsilon = \mathcal{O}(\varepsilon)$ et $a_0 - a = 0 = \mathcal{O}(\varepsilon)$.

Hérédité :

1. $P'(a_{n+1}) = P'(a_n - \frac{P(a_n)}{P'(a_n)})$
   Mais $P(X,Y) = P(X) + YP'(X) + Y^2Q(X,Y)$ par Taylor-Lagrange. Donc :
   $$P'(a_{n+1}) = P'(a_n) - \frac{P(a_n)}{P'(a_n)}(\dots)$$
   est par hypothèse de récurrence la somme d'un inversible ($P'(a_n)$) et d'un nilpotent qui commutent. Donc $P'(a_{n+1})$ est inversible.
2. La formule de Taylor-Lagrange donne : $P(a_{n+1}) = P(a_n - \frac{P(a_n)}{P'(a_n)}) = P'(a_n) - \frac{P(a_n)}{P'(a_n)} \times P'(a_n) + \left(-\frac{P(a_n)}{P'(a_n)}\right)^2 Q(a_n, -\frac{P(a_n)}{P'(a_n)})$.
   Les deux premiers termes du membres de droite sont opposés. Donc on obtient $P(a_{n+1}) = \left(-\frac{P(a_n)}{P'(a_n)}\right)^2 Q(a_n, -\frac{P(a_n)}{P'(a_n)})$
   Mais par hypothèse de récurrence, $\frac{P(a_n)}{P'(a_n)} = \mathcal{O}\left(\varepsilon^{2^n}\right)$. Donc $P(a_{n+1}) = \mathcal{O}\left(\varepsilon^{2^{n+1}}\right)$.
3. $$a_{n+1} - a = a_n - a - \frac{P(a_n)}{P'(a_n)} = \mathcal{O}(\varepsilon) + \mathcal{O}\left(\varepsilon^{2^n}\right) = \mathcal{O}(\varepsilon).$$

Si $n \geqslant \lceil \log_2(\deg(\mu_a)) \rceil$ alors on a $\varepsilon^{2^n} = 0$.
Donc l'algorithme stationne à $s = a_\infty = a_n$ qui est dès lors racine de P par le deuxième point de la récurrence. De plus $n := a - s = a - a_\infty = \mathcal{O}(\varepsilon)$ est nilpotent par le troisième point de la récurrence.

Enfin s est annulé par le polynôme P qui est sans facteurs carrés. Donc s est semi-simple.
On a ainsi montrer l'existence d'une décomposition de Jordan-Chevalley. L'unicité est la partie facile mais hors sujet ici. ■

Remarque 16

Cet algorithme est effectif (en caractéristique nulle c'est facile, sinon il y a encore un peu de travail) et il stationne donc converge très vite. De plus il est totalement inutile de connaître les valeurs propres de a pour en effectuer la décomposition, ce qui est une très bonne chose car la détermination algorithmique des valeurs propres est à éviter à tout prix du fait de son coût proéminent.

Remarque 17

Les relations de divisibilité suivantes
$$\mu_s | \mu_a | \mu_s^d \qquad \text{où} \quad d = \dim_k(A)$$
disent que μ_s et μ_a ont même liste de facteurs irréductibles. On montre ces relations.

Démonstration.
On a d'une part :
$$0 = \mu_a(a) = \mu_a(s+n) = \mu_a(s) + n(\dots)$$
Donc :
$$\mu_a(s) = -n(\dots)$$

or s est diagonalisable sur une clôture algébrique de k et n est nilpotent. Donc $\mu_a(s) = 0$ et donc $\mu_s | \mu_a$
On a d'autre part :

$$0 = \mu_s(s) = \mu_s(a - n) = \mu_s(a) - n(\dots)$$

Donc :

$$\mu_s(a) = n(\dots)$$

or n est nilpotent, donc en élevant à la puissance d on obtient :

$$\mu_s(a)^d = 0.$$

■

I.J Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$ (102) (120) (121) (125) (127) (141)

Lemme 18:

1) Pour tout $n \in \mathbb{N}^*$, on a $X^n - 1 = \prod_{d|n} \phi_d$;
2) Le polynôme ϕ_n est unitaire et à coefficients dans $\mathbb{Z}$ pour tout n ;
3) Si $P = QR$ avec $P \in \mathbb{Z}[X]$ et $Q, R \in \mathbb{Q}[X]$ unitaires, alors $Q, R \in \mathbb{Z}[X]$.

Démonstration.

1) $X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mu_n^\times} (X - \zeta) = \prod_{d|n} \phi_d$
2) On procède par récurrence :
si $n = 1$ alors $\phi_1 = X - 1$;
si on suppose le résultat vrai jusqu'au rang $n - 1$ alors, par le premier point :
$$X^n - 1 = \phi_n \prod_{d|n \ , \ d<n} \phi_d$$
Il s'agit de la division euclidienne de $X^n - 1$ par $\prod_{d|n \ , \ d<n} \phi_d$ qui est bien dans $\mathbb{Z}[X]$ unitaire par HR. Donc le quotient est dans $Z[X]$. Et c'est aussi la division euclidienne dans $Q[X]$, mais celle-ci est unique. D'où le deuxième point (le caractère unitaire se voit sur les coefficients dominants).
3) On note q le générateur positif de l'idéal $\{n \in \mathbb{Z} \quad / \quad nQ \in \mathbb{Z}[X]\}$. Alors $qQ \in \mathbb{Z}[X]$ et est primitif par définition de q et car Q est unitaire. En effet si $p|qQ$, alors en particulier en regardant le coefficient dominant $p|q$. Donc $\frac{q}{p}Q \in \mathbb{Z}[X]$ et par minimalité de q, on a donc $p = 1$.
On obtient de même $r \in \mathbb{Z}$ tel que $rR \in \mathbb{Z}[X]$ primitif.
Alors $qrP = qQrR$ et en passant au contenu il vient que $qr \ \mathrm{c}(P) = 1$ donc q et r sont dans $\mathbb{Z}$ inversibles. Ils valent donc tous deux ± 1.

■

Théorème 19:

Pour tout $n \in \mathbb{N}^*$, ϕ_n est irréductible sur $\mathbb{Q}$.

Démonstration. Soit $\zeta \in \mu_n^\times$. On va montrer que $\phi_n = \mu_\zeta$

1. Soit $\zeta' \in \mu_n^\times$. Alors il existe $m \in [\![1, \dots, n-1]\!]$ premier avec n tel que $\zeta' = \zeta^m$, il s'écrit
$$m = p_1^{\alpha_1} \dots p_k^{\alpha_k}.$$
Quitte à raisonner par récurrence sur le nombre de diviseurs premiers de m, OPS $m = p$ est premier.
2. Montrons que $\mu_\zeta = \mu_{\zeta^p}$. On note $f = \mu_\zeta$ et $g = \mu_{\zeta^p}$. Alors on a immédiatement que $f|g(X^p)$. Donc il existe $h \in \mathbb{Q}[X]$ tel que $fh = g(X^p)$.
On a de plus que f et g sont à coefficients entiers. En effet, l'anneau $\mathbb{Z}[X]$ est factoriel, donc $\phi_n = f_1\beta_1 \dots f_r\beta_r$ en produit d'irréductibles.
Alors l'un des f_{i_0} annule ζ et est unitaire et irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$. Par minimalité du polynôme minimal, on a donc $f = f_{i_0}$. Il en est de même pour g.

Par le lemme on obtient donc que $h \in \mathbb{Z}[X]$. On a donc $fh = g(x^p)$ dans $\mathbb{Z}[X]$. On peut donc réduire cette équation modulo p.
Supposons que $f \neq g$. Alors f et g sont deux irréductibles distincts divisant ϕ_n, et donc $fg \mid \phi_n$.

Soit φ un diviseur irréductible de $\overline{f}$. Alors $\varphi \mid \overline{fh} = \overline{g(X^p)} = \overline{g(X)}^p$. Donc par le lemme d'Euclide, $\varphi \mid \overline{g}$. On a alors :

$$\varphi^2 \mid \overline{f}\overline{g} \mid \overline{\phi_n} \mid \overline{X^n - 1}$$

Or le polynôme dérivé de $\overline{X^n - 1}$ est $\overline{nX^{n-1}}$ qui est non nul car p et n sont premiers entre eux. Mais alors 0 est la seule racine de $\overline{nX^{n-1}}$ sans être racine de $\overline{X^n - 1}$. Il n'a donc pas de racine multiple, c'est absurde et donc $f = g$.

3. On a donc $\mu_\zeta = f = g = \mu_{\zeta^m}$ pour tout $1 \leqslant m \leqslant n-1$ premier avec n. Donc μ_ζ admet $\varphi(n) = \deg(\phi_n)$ racines. De plus $\phi_n(\zeta) = 0$ donc ϕ_n est annulateur pour ζ et $\mu_\zeta \mid \phi_n$. Les deux polynômes sont donc associés. Comme de plus ils sont tous deux unitaires, ils sont égaux. Donc ϕ_n est un polynôme minimal et donc il est irréductible.

■

I.K Théorème de Minkowski (127) (149) (181) (191)

J'ai appris ce développement dans mon cours de théorie des nombres de M1 assuré par Florent Ivorra. La proposition et l'application provienne de son cours et je n'ai pas d'autres référence pour ces deux résultat. Le reste se trouve dans le livre de Pierre Samuel [14].

Pour la 149 je fais la proposition mais pas l'application, pour les autres (127,181,191) je fais l'application mais pas la proposition.

On suppose que E est un $\mathbf{R}$-espace vectoriel euclidien.

Pour $e = (e_1, \dots, e_n)$ une $\mathbb{Z}$-base d'un réseau H, on désigne par P_e le parallélogramme $P_e = \{\sum_{j=1}^{n} a_{i,j} e_j \quad / \quad \forall i \ 0 \leqslant a_i < 1\}$

Lemme 20:

Le volume $\mu(P_e)$ de P_e (avec μ la mesure de Lebesgue sur $\mathbb{R}^n$ est indépendante de la base e choisie pour H.
On l'appelle covolume de H et on note $\mathrm{Covol}(H)$.

Démonstration. Si $f = (f_1, \dots, f_n)$ est une autre $\mathbb{Z}$-base de H alors comme $f_i \in H$ pour tout i, on a :

$$f_= \sum_{j=1}^{n} \alpha_{i,j} e_j \qquad \text{avec} \quad \alpha_{i,j} \in \mathbb{Z}.$$

Soit u l'endomorphisme $\mathbb{R}$-linéaire de $\mathbb{R}^n$ tel que $u(e) = f$. La matrice de u dans la base e est inversible et à coefficients dans $\mathbb{Z}$, c'est $(\alpha_{i,j})_{1 \leqslant i,j \leqslant n}$. Son déterminant est donc inversible dans $\mathbb{Z}$ donc égal à ± 1.

Soit b une base orthonormée de $\mathbb{R}^n$. Alors :

$$\mu(P_f) = |\det_b(f)| = |\det_b(u(e))| = |\det(u)||\det_b(e)| = |\pm 1|\mu(P_e) = \mu(P_e).$$

Il y a aussi indépendance vis-à-vis de la base orthonormée choisie (multplication par une matrice orthonale donc de déterminant ± 1). ■

La proposition suivante permet d'exprimer le covolume d'un réseau sans faire usage d'une base orthonormée de l'espace euclidien.

Proposition 21

Soit H un réseau d'un $\mathbb{R}$-espace euclidien E. Alors, pour toute $\mathbf{Z}$-base $(e_1, \dots, e_n)$ de H

$$\mathrm{Covol}(H) = \begin{vmatrix} \langle e_1 \mid e_1 \rangle & \cdots & \langle e_1 \mid e_n \rangle \\ \vdots & & \vdots \\ \langle e_n \mid e_1 \rangle & \cdots & \langle e_n \mid e_n \rangle \end{vmatrix}.$$

Démonstration. Soient $\mathscr{B} = (b_1, \dots, b_n)$ une base orthonormale. On écrit $e_i = \sum_{j=1}^{n} \langle e_i \mid b_j \rangle b_j$. Soit

$$A = \begin{pmatrix} \langle e_1 \mid b_1 \rangle & \cdots & \langle e_n \mid b_1 \rangle \\ \vdots & & \vdots \\ \langle e_1 \mid b_n \rangle & \cdots & \langle e_n \mid b_n \rangle \end{pmatrix} \mathscr{M}_n(\mathbb{R})$$

Par définition $\mathrm{Covol}(H) = |\det(A)|$. Ainsi a-t-on

$$\mathrm{covol}(H)^2 = \det(A)^2 = \det\left({}^tA\right)\det(A) = \det\left({}^tAA\right).$$

Or ${}^tAA[i,j] = \sum_{k=1}^{n} \langle e_i \mid b_k\rangle\langle e_j \mid b_k\rangle = \left\langle e_i \ , \ \sum_{k=1}^{n} \langle e_j \mid b_k\rangle b_k \right\rangle = \langle e_i \mid e_j\rangle$

On obtient donc

$$\operatorname{covol}(L)^2 = \begin{pmatrix} \langle e_1 \mid e_1\rangle & \cdots & \langle e_1 \mid e_n\rangle \\ \vdots & & \vdots \\ \langle e_n \mid e_1\rangle & \cdots & \langle e_n \mid e_n\rangle \end{pmatrix}$$

On trouve ainsi la formule annoncée reliant le covolume du réseau au déterminant de Gram de l'une de ses $\mathbb{Z}$-bases. ■

Lemme 22:

Soit H un réseau de $\mathbb{R}^n$. Soit S une partie mesurable de E telle que $\mu(A) > \operatorname{covol}(L)$. Alors il existe alors des éléments $x, y \in S$ distincts tels que $x - y \in H$.

Démonstration. Soit $e = (e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de H et soit P_e le domaine fondamental associé. Alors $S = \coprod_{h\in H} [(h + P_e) \cap S)]$. On a donc :

$$\mu(S) = \sum_{h\in H} \mu(S \cap (h + P_e))$$

Mais la mesure de Lebesgue est invariante par translation, donc on a

$$\mu(S \cap (h + P_e)) = \mu\left((-h + S) \cap P_e\right).$$

Ceci impose dès lors que les ensembles $(-h + S) \cap P_e$ ne sont pas disjoints deux à deux car sinon

$$\mu(S) = \sum_{h\in H} \mu\left((-h + S) \cap P_e\right) \leqslant \mu(P_e)$$

ce qui est exclus. On peut donc trouver h et $\tilde{h}$ dans H distincts tels que

$$((-h + S) \cap P_e) \cap ((-\tilde{h} + S) \cap P_e) \neq \varnothing.$$

De là on tire qu'il existe $x, y \in S$ tels que $-h + x = -\tilde{h} + y$. c'est-à-dire $x - y = h - \tilde{h} \in H$ (structure de groupe de H) et comme $h \neq \tilde{h}$, on a aussi $x \neq y$. ■

Théorème 23: Minkowski

Soit H un réseau de $\mathbb{R}^n$ et soit S une partie mesurable de $\mathbb{R}^n$ telle que

1. S est convexe ;
2. S est symétrique par rapport à l'origine ;
3. la mesure de $\mu(S) > 2^n \operatorname{covol}(H)$

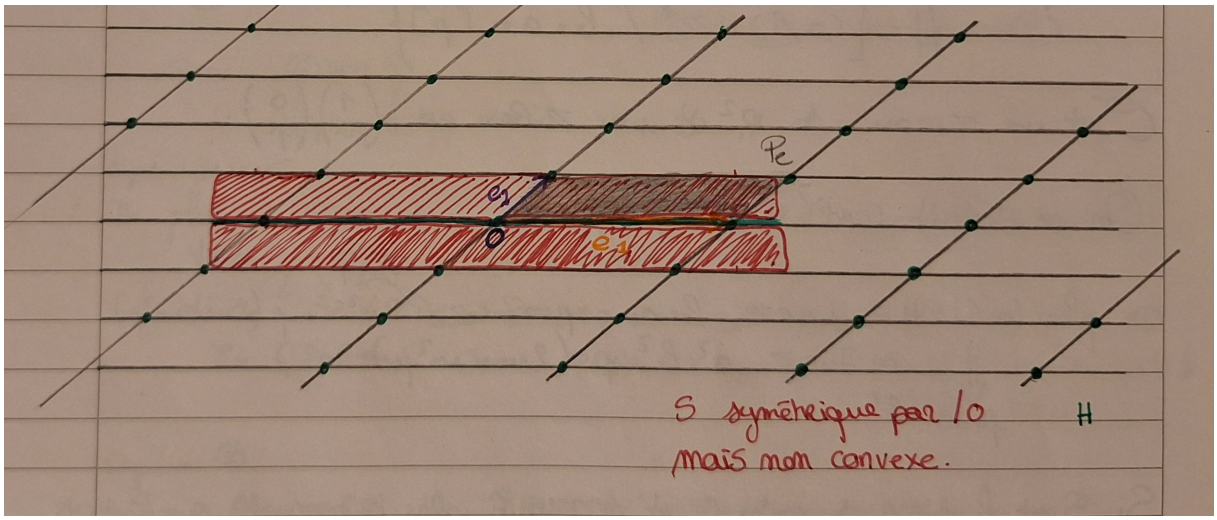
Alors S contient un élément de H non nul.

Le dessin suivant aide à comprendre pourquoi l'hypothèse de convexité est nécessaire. La surface rouge est constitué de deux bandes ouvert situées dans les demis plans $y > 0$ et $y < 0$.

Démonstration. L'ensemble $2H = \{2x \quad / \quad x \in H\}$ est un réseau et si $(e_1, \ldots, e_n)$ est une $\mathbf{Z}$-base du réseau H alors $(2e_1, \ldots, 2e_n)$ est une $\mathbf{Z}$-base de $2H$. Par multilinéarité du déterminant il vient alors :

$$\operatorname{covol}(2H) = 2^n \operatorname{covol}(H).$$

Ainsi la condition (3) se réécrit en $\mu(S) > \operatorname{covol}(2H)$. Le lemme précédent assure l'existence de $x, y \in S$ distincts tels que $x - y \in 2H$. Puis $\frac{x-y}{2} \in H$. Mais comme S est symétrique $-y \in S$ et comme S est convexe $\frac{x-y}{2} =\in S$. ■



Application 24: le théorème des deux carrés

Soit p un nombre premier impair. Alors p est la somme de deux carrés d'entiers si et seulement si $p \equiv 1 \mod 4$.

Démonstration. On va utiliser de manière cruciale la première loi complémentaire de la loi de réciprocité quadratique.

* Supposons $p = a^2 + b^2$. Alors $p \nmid a$ ou $p \nmid b$ car sinon si $p \mid a$ et $p \mid b$, alors $p^2 \mid a^2$ et $p^2 \mid b^2$ donc divise $p \mid a^2 + b^2 = p$ et donc $p \mid p$, ce qui est absurde.
  Par symétrie des rôles de a et b on peut supposer $p \nmid b$. On a alors $-1 = (a/b)^2$ dans $\mathbf{F}_p$. C'est-à-dire que -1 est un carré modulo p et donc $p \equiv 1 \mod 4$ par la première loi complémentaire de la loi de réciprocité quadratique.
* Réciproquement on suppose $p \equiv 1 \mod 4$. La première loi complémentaire de la loi de réciprocité quadratique assure que -1 est un carré modulo p. On dispose donc de $u \in \mathbb{Z}$ tel que $u^2 \equiv -1 \mod p$. On pose :

$$H = \{(a, b) \in \mathbf{Z}^2 \quad / \quad b \equiv ua \mod p\}.$$

  C'est un réseau de $\mathbb{R}^2$ dont une $\mathbb{Z}$-base est $\begin{pmatrix} 1 \\ u \end{pmatrix}, \begin{pmatrix} 0 \\ p \end{pmatrix}$.

  On en déduit $\mathrm{Covol}(H) = p$.

  De plus si $(a, b) \in H$, alors il existe $n \in \mathbf{Z}$ tel que $b = ua + np$. On a donc

$$b^2 = u^2a^2 + 2uanp + n^2p^2 \equiv -a^2 \mod p,$$

  ce qui donne que p divise $a^2 + b^2$.
  Soit S le disque $D(0, R)$ de centre 0 et de rayon R. Alors S est mesurable, convexe, symétrique par rapport à l'origine et

$$\mu(SA) = \pi R^2.$$

  On prend $R > \sqrt{\frac{4p}{\pi}}$, et l'on obtient $\mu(S) = \pi R^2 > 4\,\mathrm{Covol}(L) = 4p$.

  Alors le théorème de Minkowski fournit $(a, b) \in H \cap S$ non nuls. Comme $\frac{3}{2} > \frac{4}{\pi}$, en prenant $R = \sqrt{\frac{3p}{2}}$ on a :

$$0 < a^2 + b^2 < \frac{3p}{2},$$

  or $p \mid a^2 + b^2$. D'où finalement $p \mid a^2 + b^2 = p$.

■

I.L Norme dans une extension algébrique (125) (127) (144) (148) (149)

Soit K un corps. Soit L/K une extension finie de K. Soit $\alpha \in L$, on note $\pi_{K,\alpha} = X^m + \sum_{i=0}^{m-1} a_i X^i$ le polynôme minimal de α sur K et $m_\alpha : \begin{array}{ccc} L & \to & L \\ x & \mapsto & \alpha x \end{array}$ la multiplication par α dans L.
On appelle norme de α et on note $N_{L/K}(\alpha)$ le déterminant de m_α vu comme K-endomorphisme de L.

Théorème 25:

1. Soit K un corps. Soit L/K une extension finie de K. Soit $\alpha \in L$. Alors dans la K-base $\left(1, \alpha, \dots, \alpha^{m-1}\right)$ de $K(\alpha)$ (où $m = \deg(\pi_{K,\alpha})$) la matrice de m_α est la matrice compagnon associée au polynôme $\pi_{K,\alpha}$.
   Donc
   $$\pi_{K,\alpha} = \chi_{m_\alpha}$$
   et :
   $$N_{K(\alpha)/K}(\alpha) = (-1)^m a_0$$
   Si de plus L contient un corps de décomposition de $\pi_{K,\alpha}$, alors :
   $$N_{K(\alpha)/K}(\alpha) = \prod_{i=1}^{m} x_i$$
   où $x_1, \dots, x_n \in L$ sont les racines de $\pi_{K,\alpha}$.
2. Il existe une K-base de L telle que la matrice de l'endomorphisme m_α dans cette base soit diagonale par blocs de la forme :
   $$\underbrace{\begin{pmatrix} C_\alpha & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & C_\alpha & \cdots & \mathbf{O} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{O} & \cdots & \mathbf{O} & C_\alpha \end{pmatrix}}_{[L:K(\alpha)] \text{ blocs}}$$
   où C_α est la matrice compagnon évoquée dans le premier point.
   De plus :
   $$\forall \alpha \in L, \quad N_{L/K}(\alpha) = \left(N_{K(\alpha)/K}(\alpha)\right)^{[L:K(\alpha)]}$$

Démonstration. 1. La famille $\left(1, \alpha, \dots, \alpha^{m-1}\right)$ est une K-base de $K(\alpha)$. En effet :
— Elle est libre par minimalité du polynôme minimal :
si $\sum_{i=0}^{m-1} \lambda_i \alpha^i = 0$ avec les $\lambda_i \in K$, alors $\sum_{i=0}^{m-1} \lambda_i X^i$ est un polynôme annulateur pour α, mais alors par définition du polynôme minimal ce polynôme est nulle ;
— Elle est génératrice car $K(\alpha) \simeq K[X]/\pi_{K,\alpha}$ est un K-e.v. de dimension $\deg(\pi_{K,\alpha})$.
La matrice de l'endomorphisme m_α dans cette base est alors :

$$C_\alpha := \begin{pmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{m-1} \end{pmatrix}$$

Alors :

$$\chi_{m_\alpha} = \begin{vmatrix} X & 0 & 0 & \cdots & a_0 \\ -1 & X & 0 & \cdots & a_1 \\ 0 & -1 & X & \cdots & a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & X + a_{m-1} \end{vmatrix}$$

et en faisant la combinaison $L_1 \longleftarrow L_1 + XL_2 + \dots X^{m-1}L_m$ puis en développant suivant la première ligne, on obtient :

$$\begin{aligned} \chi_{m_\alpha} &= \begin{vmatrix} 0 & 0 & 0 & \cdots & \pi_{K,\alpha} \\ -1 & X & 0 & \cdots & a_1 \\ 0 & -1 & X & \cdots & a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & X + a_{m-1} \end{vmatrix} \\ &= (-1)^{m+1}\pi_{K,\alpha} \begin{vmatrix} -1 & X & 0 & \cdots & 0 \\ 0 & -1 & X & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & X \\ 0 & 0 & \cdots & 0 & -1 \end{vmatrix} \\ &= (-1)^{m+1}\pi_{K,\alpha}(-1)^{m-1} \\ &= \pi_{K,\alpha} \end{aligned}$$

On a donc obtenu que $\pi_{K,\alpha} = \chi_{m_\alpha}$ et les relations coefficients/racines fournissent en outre $N_{K(\alpha)/K}(\alpha) = \det(m_\alpha) = (-1)^m a_0$.

Si de plus L contient un corps de décomposition de $\pi_{K,\alpha}$ alors :

$$N_{K(\alpha)/K}(\alpha) = \prod_{i=1}^{m} x_i$$

2. Soit $d := [L : K(\alpha)]$, si $(e_1, \dots, e_d)$ est une $K(\alpha)$-base de L, alors d'après le théorème de la base télescopique $\left(e_1, \alpha e_1, \dots, \alpha^{m-1}e_1, e_2, \dots, \alpha^{m-1}e_2, \dots, e_d, \dots, \alpha^{m-1}e_d\right)$ est une K-base de L. Il s'en suit que la matrice dans cette base de m_α est

$$\begin{pmatrix} C_\alpha & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & C_\alpha & \cdots & \mathbf{O} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{O} & \cdots & \mathbf{O} & C_\alpha \end{pmatrix}$$

Alors $\chi_{m_\alpha} = (\chi_{C_\alpha})^d = (\pi_{K,\alpha})^d$. De cela résulte $N_{L/K}(\alpha) = N_{K(\alpha)/K}(\alpha)^d$.

■

Application 26: Norme dans un corps fini

Soit p un nombre premier. Soit $n \in \mathbb{N}^*$. Soit $q = p^n$. Alors en notant φ le morphisme de Frobenius :

$$\forall \alpha \in \mathbb{F}_q, \quad N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \prod_{i=0}^{n-1} \varphi^i(\alpha) = \alpha^{\frac{q-1}{p-1}}$$

Démonstration. Soit $\alpha_0 \in \mathbb{F}_q^\times$ un générateur du groupe multiplicatif $\mathbb{F}_q^\times = \langle \alpha_0 \rangle$. Alors $\mathbb{F}_q = \mathbb{F}_p(\alpha_0)$ (théorème de l'élément primitif dans les corps finis, voir [8] si besoin).
Donc $\pi_{\mathbb{F}_p,\alpha_0}$ est de degré n.
Comme $\varphi_{\mathbb{F}_p} = \mathrm{id}$ et que φ est un automorphisme de corps de $\mathbb{F}_q$:

$$\forall i \in [\![0, n-1]\!], \quad 0 = \varphi^i\left(\pi_{\mathbb{F}_p,\alpha_0}(\alpha_0)\right) = \pi_{\mathbb{F}_p,\alpha_0}\left(\varphi^i(\alpha_0)\right)$$

Donc $\varphi^i(\alpha_0)$ est racine de $\pi_{\mathbb{F}_p,\alpha_0}$ pour $0 \leqslant i \leqslant n-1$.

De plus elles sont toutes distinctes car si $0 \leqslant i < j \leqslant n-1$ alors $\alpha_0^{p^i} = \alpha_0^{p^j} \iff \alpha_0^{p^j-p^i} = 1 \iff p^j - p^i \in (p^n-1)\mathbb{Z} = (q-1)\mathbb{Z}$ car $\langle \alpha_0 \rangle = \mathbb{F}_q^\times$.
Mais $p^j - p^i \in [\![1, p^{n-1}-1]\!]$.

Au total, on a obtenu que $\pi_{\mathbb{F}_p,\alpha_0}$ est scindé simple sur $\mathbb{F}_q$ (avec n racines distinctes).

D'après le théorème on a alors :

$$N_{\mathbb{F}_p(\alpha_0)/\mathbb{F}_p}(\alpha_0) = N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha_0) = \prod_{i=0}^{n-1} \varphi^i(\alpha_0) = \prod_{i=0}^{n-1} \alpha_0^{p^i} = \alpha_0^{\sum_{i=0}^{n-1} p^i} = \alpha_0^{\frac{p^n-1}{p-1}} = \alpha_0^{\frac{q-1}{p-1}}$$

On en déduit donc :

$$\forall k \in \mathbb{N}, \quad N_{\mathbb{F}_q/\mathbb{F}_p}\left(\alpha_0^k\right) = N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha_0)^k = \left(\alpha_0^{\frac{q-1}{q}}\right)^k = \left(\alpha_0^k\right)^{\frac{q-1}{p-1}}$$

mais donc comme α_0 engendre $\mathbb{F}_q^\times$, il sort finalement :

$$\forall \alpha \in \mathbb{F}_q^\times, \quad N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \alpha^{\frac{q-1}{p-1}} = \prod_{i=0}^{n-1} \varphi^i(\alpha)$$

Le résultat demeure pour $\alpha = 0$.

■

Corollaire 27: Les carrés dans $\mathbb{F}_q$

$\alpha \in (\mathbb{F}_q)^2 \iff N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \in (\mathbb{F}_p)^2$.

Démonstration. Le cas $\alpha = 0$ est immédiat. Supposons donc $\alpha \in \mathbb{F}_q^\times$.

— Si $\alpha \in \left(\mathbb{F}_q^\times\right)^2$, alors il existe $\beta \in \mathbb{F}_q^\times$ tel que $\alpha = \beta^2$. La multiplicativité de la norme donne alors :

$$N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = N_{\mathbb{F}_q/\mathbb{F}_p}\left(\beta^2\right) = \left(N_{\mathbb{F}_q/\mathbb{F}_p}(\beta)\right)^2 \quad \Longrightarrow \quad N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \in \left(\mathbb{F}_p^\times\right)^2$$

— Si $N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \in \left(\mathbb{F}_p^\times\right)^2$, alors :

$$\alpha^{\frac{q-1}{2}} = \left(\alpha^{\frac{q-1}{p-1}}\right)^{\frac{p-1}{2}} = N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)^{\frac{p-1}{2}} = 1$$

par le lemme d'Euler car $N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ est un carré. En conclusion α est un carré dans $\mathbb{F}_q$.

■

Remarque 28

Si vous souhaitez une autre application, il y a une très jolie application du théorème pour déterminer les inversibles d'un entier de corps de nombre sur le site de Matthias Hostein. Vous pouvez aussi regarder le super livre (quoique pas tout-à-fait récent) de Pierre Samuel [14]. Si vous choisissez cette autre application alors il faudra que vous sachiez justifier que l'ensemble des entiers d'un corps de nombre est un anneau (c'est supposé su dans le développement de Matthias), ce qui nécessite de parler de $\mathbb{Z}$-module de type fini et de savoir que le théorème de Cayley-Hamilton se généralise dans le cas des modules. Tout ceci est fait dans le livre de théorie algébrique des nombres de Pierre Samuel (il fait aussi le joli théorème de Minkowski (ça ne se refuse pas quand on l'a déjà vu en M1 en cours de théorie des nombres) très utile pour la leçon connexité dans $\mathbb{R}^n$ si on justifie bien que l'hypothèse de convexité est cruciale mais ça c'est une autre histoire).

I.M Théorème de Gauss-Lucas (102) (144) (181)

Théorème 29: Gauss-Lucas

Soit $P \in \mathbb{C}[X]$ un polynôme non constant. Les racines de P' sont dans l'enveloppe convexe des racines de P.

Démonstration.
Comme $\mathbb{C}$ est algébriquement clos, on peut écrire $P = \lambda \prod_{k=1}^{r}(X-\lambda_k)^{n_k}$ où $r \geqslant 1$, $\lambda \in \mathbb{C}^*$, $\lambda_1, ...\lambda_r \in \mathbb{C}$ sont les racines deux à deux distinctes de P et $n_1, ..., n_r$ leur ordre respectif. Alors :

$$P' = \lambda \sum_{k=1}^{n} = n_k(X-\lambda_k)^{n_k-1} \prod_{\substack{l=1,\dots,r \\ l\neq k}} (X-\lambda_l)^{n_l}.$$

On obtient alors :

$$\frac{P'}{P} = \sum_{k=1}^{r} \frac{n_k}{X-\lambda_k}$$

Si $z \in \mathrm{Rac}(P')$, alors :

— Soit z est l'une des racines λ_k, et elle est alors évidemment dans l'enveloppe convexe des racines de P ;

— Sinon, on peut écrire :

$$0 = \frac{P'(z)}{P(z)} = \sum_{k=1}^{r} \frac{n_k}{z-\lambda_k} = \sum_{k=1}^{r} n_k \frac{\overline{z-\lambda_k}}{|z-\lambda_k|^2}$$

En conjuguant on a encore :

$$\sum_{k=1}^{r} n_k \frac{z-\lambda_k}{|z-\lambda_k|^2} = 0$$

On extrait donc z en extrayant la somme qui le comporte :

$$z = \frac{\sum_{k=1}^{r} \frac{n_k}{|z-\lambda_k|^2}\lambda_k}{\sum_{k=1}^{r} \frac{n_k}{|z-\lambda_k|^2}} = \sum_{k=1}^{r} \frac{\frac{n_k}{|z-\lambda_k|^2}}{\sum_{l=1}^{r} \frac{n_l}{|z-\lambda_l|^2}} \lambda_k$$

Cette dernière formule exprime que le fait que z s'écrit comme barycentre à coefficients dans $]0,1[$ des racines $(\lambda_1, \dots, \lambda_r)$ de P :

$$z = \mathrm{Bar}\left(\lambda_k, \frac{n_k}{|z-\lambda_k|^2} \times \sum_{l=1}^{r} \frac{n_l}{|z-\lambda_l|^2}\right).$$

On obtient donc que $z \in \mathrm{Conv}(\lambda_1, \dots, \lambda_r)$.
Soit enfin :

$$\mathrm{Rac}(P') \subset \mathrm{Conv}(\lambda_1, \dots, \lambda_r).$$

■

Corollaire 30:

Le plus grand entier $n \geqslant 2$ tel que les racines non nulles de $(X+1)^n - X^n - 1$ soient de module 1 est 7.

Démonstration.
Si $n = 2$:

$$P(X) = (X+1)^2 - X^2 - 1 = 2X$$

a une seule racine qui est 0. On peut donc supposer $n > 2$.

<u>*Si $n \geqslant 3$:*</u>

$$P(X) = (X+1)^n - X^n - 1$$

Donc

$$P'(X) = n(X+1)^{n-1} - nX^{n-1}$$

Si z est une racine de P', alors $z \neq 0$, et donc

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

C'est-à-dire qu'il existe $k \in [\![0, n-2]\!]$ tel que $\frac{z+1}{z} = e^{\frac{2ik\pi}{n-1}}$.
Mais, si $k = 0$ alors $z + 1 = z$ et c'est absurde. Donc $k \in [\![1, n-2]\!]$ et les racines de P' sont dans $\{z_k \quad / \quad k \in [\![1, n-2]\!]\}$ où z_k est défini par $\frac{z_k+1}{z_k} = e^{\frac{2ik\pi}{n-1}}$, i.e.

$$z_k = \frac{e^{\frac{-ik\pi}{n-1}}}{2i\sin\frac{k\pi}{n-1}}$$

Mais d'après le théorème de Gauss-Lucas si les racines de P sont de module 1 ou nul, alors nécessairement celles de P' sont dans le disque unité.

Or $|z_1| = \frac{1}{2\sin\left(\frac{\pi}{n-1}\right)}$ et donc si $n \geqslant 8$ alors :

$$2\sin\left(\frac{\pi}{n-1}\right) < 2\sin\left(\frac{\pi}{6}\right) = 1$$

puis $|z_1| > 1$ donc $n \leqslant 7$

<u>*Si $n = 7$:*</u>

Posons $P_0(X) = (X+1)^7 - X^7 - 1$. On a que -1 et 0 sont racines de P_0. Ainsi, P_0 s'écrit (après DE)

$$P_0(X) = X(X+1)(7X^4 + 14X^3 + 21X^2 + 14X + 7)$$

Le polynôme $Q(X) = (X^4+2X^3+3X^2+2X+1)$, est son propre polynôme réciproque : $Q(X) = X^4 Q\left(\frac{1}{X}\right)$. On peut donc l'écrire :

$$\begin{aligned}
Q(X) &= X^4 + 2X^3 + 3X^2 + 2X + 1 \\
&= X^2\left(X^2 + \frac{1}{X^2}\right) + 2X^2\left(X + \frac{1}{X}\right) + 3X^2 \\
&= X^2\left(\left(X^2 + \frac{1}{X^2}\right) + 2\left(X + \frac{1}{X}\right) + 3\right) \\
\text{en posant } Y = X + \frac{1}{X} \qquad &= X^2(Y^2 - 2 + 2Y + 3) \\
&= 7X^2(Y-1)^2 \\
&= 7X^2(X + \frac{1}{X} - 1)^2 \\
&= (X^2 + X + 1)^2
\end{aligned}$$

Au total $P_0 = 7X(X+1)(X^2+X+1)^2$ et ses racines sont exactement : $0, 1, e^{\frac{2i\pi}{3}}, e^{-\frac{2i\pi}{3}}$ qui est contenu dans le disque unité.
L'entier recherché est donc 7. ■

I.N Surjectivité de l'exponentielle matricielle (150) (155) (156)

Théorème 31:

L'exponentielle réalise une surjection de $\mathcal{M}_n(\mathbb{C})$ sur $\mathrm{GL}_n(\mathbb{C})$.

Démonstration.

1. Commençons par montrer que pour toute matrice U unipotente, il existe N une matrice nilpotente, qui s'exprime comme un polynôme en U, telle que $\exp(N) = U$.
   Soit U unipotente, la matrice $U - I_n$ est nilpotente (cela se voit facilement en trigonalisant U) et on pose :
   $$N = \sum_{k=1}^{n-1} \frac{(-1)^{k+1}}{k} (U - I_n)^k$$
   qui est une matrice nilpotente comme somme de matrices nilpotentes qui commutent (on s'inspire du DSE de la fonction logarithme au voisinage de 1 pour écrire N). A ce stade, on a que N est un polynôme en U, vérifions donc maintenant que $U = \exp(N)$
   On pose ensuite
   $$A(t) = \exp\left(-\sum_{k=1}^{n-1} \frac{(-t)^k}{k} (U - I_n)^k\right) = \exp\left(-\sum_{k=0}^{+\infty} \frac{(-t)^{k+1}}{k+1} (U - I_n)^{k+1}\right).$$
   De sorte que l'on ait $A(1) = N$. On s'est permis de modifier A pour faciliter les calculs au moment de dériver tout en conservant l'identité précédente.
   Alors :
   $$A'(t) = \left(\sum_{k=0}^{+\infty} (-t)^k (U - I_n)^k\right) \cdot (U - I_n) \cdot A(t) = (I_n + t(U - I_n))^{-1} \cdot (U - I_n) \cdot A(t)$$
   Donc $A(t)$ est solution du système différentiel
   $$\begin{cases} Y'(t) = Y(t) \cdot (U - I_n) \cdot (I_n + t(U - I_n))^{-1} \\ Y(0) = I_n \end{cases}$$
   D'après le théorème de Cauchy-Lipschitz, il y a une unique solution définie sur $\mathbb{R}^+$. Or, l'application $t \mapsto I_n + t(U - I_n)$ est également solution. On en déduit donc que les deux solutions sont égales, en particulier $\exp(N) = A(1) = U$ avec N un polynôme en U.
2. Montrons maintenant la surjectivité de l'exponentielle.
   Tout d'abord, pour tout $M \in \mathcal{M}_n(\mathbb{C})$, on a les égalité $\exp(M) \cdot \exp(-M) = \exp(M + (-M)) = \exp(0_n) = I_n$ car M et $-M$ commutent. On en déduit $\exp(M) \in \mathrm{GL}_n(\mathbb{C})$ et donc
   $$\exp(\mathcal{M}_n(\mathbb{C})) \subset \mathrm{GL}_n(\mathbb{C})$$
   Réciproquement, soit $M \in \mathrm{GL}_n(\mathbb{C})$, la décomposition de Dunford, nous donne N nilpotente et D diagonalisable, les matrices N et D étant des polynômes en M, et telles que $M = D + N$. En posant $U = M \cdot D^{-1} = N \cdot D^{-1} + I_n$, qui est unipotente, on obtient que $M = U \cdot D$. De plus, la matrice U est un polynôme en M, car D^{-1} est un polynôme en D. En effet, $\mathbb{C}[D]$ est fermé comme espace vectoriel de dimension fini et
   $$D^{-1} = \lim_{n \to +\infty} \sum_{k=0}^{n} (-1)^k (D - I_n)^k.$$
   D'après ce qui précède, il existe $Q \in \mathbb{C}[X]$ tel que $Q(U)$ soit nilpotente et $\exp(Q(U)) = U$.

D'autre part comme D est diagonalisable, il existe $P \in \mathrm{GL}_n(\mathbb{C})$ et des λ_i distincts et tous non nuls tels que $D = P \cdot \mathrm{Diag}(\lambda_1, \ldots, \lambda_1, \ldots, \lambda_r, \ldots, \lambda_r) \cdot P^{-1}$.

Pour chaque $i \in \{1, \ldots, r\}$, soit α_i tel que $\lambda_i = \exp(\alpha_i)$, et soit $R \in \mathbb{C}[X]$ le polynôme interpolateur de Lagrange tel que $\forall i \in \{1, \ldots, r\}, R(\lambda_i) = \alpha_i$.
On a alors

$$\begin{array}{rcl} \exp(R(D)) & = & \exp\left(R\left(P \cdot \mathrm{Diag}(\lambda_1, \ldots, \lambda_1, \ldots, \lambda_r, \ldots, \lambda_r) \cdot P^{-1}\right)\right) \\ & = & P \cdot \exp(R(\mathrm{Diag}(\lambda_1, \ldots, \lambda_1, \ldots, \lambda_r, \ldots, \lambda_r))) \cdot P^{-1} \\ & = & P \cdot \exp(\mathrm{Diag}(\alpha_1, \ldots, \alpha_1, \ldots, \alpha_r, \ldots, \alpha_r)) \cdot P^{-1} \\ & = & P \cdot \mathrm{Diag}(\exp(\alpha_1), \ldots, \exp(\alpha_1), \ldots, \exp(\alpha_r), \ldots, \exp(\alpha_r)) \cdot P^{-1} \\ & = & P \cdot \mathrm{Diag}(\lambda_1, \ldots, \lambda_1, \ldots, \lambda_r, \ldots, \lambda_r) \cdot P^{-1} = D \end{array}$$

Finalement, si l'on pose $A = Q(U) + R(D)$, comme U et D sont des polynômes en M, les endomorphismes $Q(U)$ et $R(D)$ commutent et A est un polynôme en M vérifiant

$$\exp(A) = \exp(Q(U)) \cdot \exp(R(D)) = U \cdot D = M$$

■

Remarque 32

On sait que $\exp(\mathcal{M}_n(\mathbb{R})) \neq \mathrm{GL}_n(\mathbb{R})$. En effet, pour tout $A \in \mathcal{M}_n(\mathbb{R})$ on a $\det(\exp(A)) = \exp(\mathrm{Tr}(A)) > 0$, donc toute matrice de déterminant strictement négatif n'a pas d'antécédent par l'exponentielle.
On montre que $\exp(\mathcal{M}_n(\mathbb{R})) = \left\{M^2, M \in \mathrm{GL}_n(\mathbb{R})\right\}$.
En effet, pour tout $M \in \mathcal{M}_n(\mathbb{R})$, on a $\exp(M) = \exp\left(\frac{1}{2}M\right)^2 \in \left\{M^2, M \in \mathrm{GL}_n(\mathbb{R})\right\}$.
Réciproquement, soit $M \in \left\{M^2, M \in \mathrm{GL}_n(\mathbb{R})\right\}$ et $B \in \mathrm{GL}_n(\mathbb{R})$ tel que $M = B^2$.
D'après ce qui précède, il existe $Q \in \mathbb{C}[X]$ tel que $\exp(Q(B)) = B$ et on a les égalités $\exp\left(\bar{Q}(B)\right) = \exp\left(\bar{Q}\left(\bar{B}\right)\right) = \exp\left(\overline{Q(B)}\right) = \overline{\exp(Q(B))} = \bar{B} = B$.
D'où $\exp\left(\left(Q + \bar{Q}\right)(B)\right) = B^2 = M$ avec $\left(Q + \bar{Q}\right) \in \mathbb{R}[X]$, et donc $\left(Q + \bar{Q}\right)(B) \in \mathcal{M}_n(\mathbb{R})$.
L'exponentielle n'est injective ni sur $\mathcal{M}_n(\mathbb{C})$ ni sur $\mathcal{M}_n(\mathbb{R})$. En effet, il existe $P \in \mathrm{GL}_n(\mathbb{C})$ telle que

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = P^{-1} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} P$$

et

$$\exp\left(2\pi \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) = P^{-1} \cdot \exp\left(2\pi \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\right) \cdot P = P^{-1} \cdot I_n \cdot P = I_n = \exp(0_n)$$

II Développements d'analyse

Formules des compléments

II.A Formules des compléments (218) (235) (236) (245)

Théorème 33: Formule des compléments

$$\forall z \in \mathbb{C}\backslash\mathbb{Z}, \quad \Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}$$

Démonstration. Quitte à utiliser le théorème du prolongement analytique, on va démontrer le théorème sur $]0,1[$ qui admet les points d'accumulation.

Soit $s \in]0,1[$,

$$\begin{aligned}
\Gamma(s)\Gamma(1-s) &= \int_0^{+\infty} x^{s-1}e^{-x}\mathrm{d}x \int_0^{+\infty} u^{-s}e^{-u}\mathrm{d}u \\
&= \int_0^{+\infty} \left(\int_0^{+\infty} u^{-s}e^{-u}\mathrm{d}u\right) x^{s-1}e^{-x}\mathrm{d}x \\
&\overset{xv=u}{=} \int_0^{+\infty} \left(\int_0^{+\infty} x^{-s}v^{-s}e^{-xv}x\mathrm{d}v\right) x^{s-1}e^{-x}\mathrm{d}x \\
&\overset{\text{Fubini-Tonnelli}}{=} \int_0^{+\infty} \left(\int_0^{+\infty} e^{-x(v+1)}\mathrm{d}x\right) v^{-s}\mathrm{d}v \\
&= \int_0^{+\infty} \frac{v^{-s}}{v+1}\mathrm{d}v \\
&\overset{\text{symétrie des rôles de } s \text{ et } 1-s}{=} \int_0^{+\infty} \frac{v^{s-1}}{v+1}\mathrm{d}v \\
&\overset{v=e^t}{=} \int_0^{+\infty} \frac{e^{ts}e^{-t}}{e^t+1}e^t\mathrm{d}t.
\end{aligned}$$

On pose $f : z \mapsto \frac{e^{zs}}{e^z+1}$. Alors f est holomorphe sauf en $i\pi + 2i\pi\mathbb{Z}$ où elle admet des pôles d'ordre 1.

Aussi, a-t-on :

$$\mathrm{Res}_{i\pi}(f) = \lim_{z\to i\pi}(z-i\pi)\frac{e^{sz}}{e^z-1} = \lim_{z\to i\pi}\frac{(z-i\pi)}{e^z-e^{i\pi}}e^{sz} = \frac{e^{i\pi s}}{e^{i\pi}} = -e^{i\pi s}$$

car on reconnaît l'inverse du taux d'accroissement de la fonction entière exponentielle et que l'on connaît sa dérivée complexe : elle-même.

Soit $R > 0$, on utilise le théorème des résidus avec le contour suivant :
On appelle γ_R le rectangle de sommets $-R,\ R,\ R+2i\pi,\ -R+2i\pi$ parcours dans le sens trigonométrique (anti-horaire)

On a :

$$\frac{1}{2i\pi}\int_{\gamma_R} f(z)\mathrm{d}z = \mathrm{Res}_{i\pi}(f)\cdot \mathrm{ind}_{\gamma_R}(i\pi) = -e^{i\pi s}$$

$$\int_{\gamma_R} f(z)\mathrm{d}z = \underbrace{\int_{-R}^{-R} \frac{e^{ts}}{e^t+1}}_{I_1} + \underbrace{i\int_0^{2\pi} \frac{e^{(R+it)s}}{e^{R+it}+1}\mathrm{d}s}_{I_2} + \underbrace{\int_R^{-R} \frac{e^{(t+2i\pi)s}}{e^{t+2i\pi}+1}\mathrm{d}s}_{I_3} + \underbrace{i\int_{2\pi}^0 \frac{e^{(-R+it)s}}{e^{-R+it}+1}\mathrm{d}s}_{I_4}.$$

On calcule séparément les 4 intégrales que l'on vient d'isoler :

— ⋆ $I_1 \underset{R\to+\infty}{\longrightarrow} \Gamma(s)\Gamma(1-s)$;

— ⋆ $I_3 = -e^{2i\pi s}\displaystyle\int_{-R}^{R} \frac{e^{ts}}{e^{t\pi}+1}\mathrm{d}s \to -e^{2i\pi s}\Gamma(s)\Gamma(1-s)$;

— ⋆ Par inégalité triangulaire ($|\,|a|-|b|\,| \leqslant |a+b|$), on peut obtenir une majoration de l'intégrande de I_2 :

$$\left|\frac{e^{(R+it)s}}{e^{R+it}+1}\right| = \frac{e^{Rs}}{|e^{R+it}+1|} \leqslant \frac{e^{Rs}}{e^R-1} \underset{R\to+\infty}{\sim} e^{R(s-1)}.$$

On déduit de cette majoration la majoration suivante :

$$|I_2| \leqslant 2\pi\frac{e^{Rs}}{e^R-1} \to 0 \qquad \text{car } s<1;$$

— ⋆ On procède de même sur I_4 :

$$\left|\frac{e^{(-R+it)s}}{e^{-R+it}+1}\right| = \frac{e^{-Rs}}{|e^{-R+it}+1|} \leqslant \frac{e^{-Rs}}{1-e^{-R}} \underset{R\to+\infty}{\sim} e^{-Rs}.$$

On déduit de cette majoration la majoration suivante :

$$|I_4| \leqslant 2\pi\frac{e^{-Rs}}{1-e^{-R}} \to 0 \qquad \text{car } s>0.$$

Ainsi au total

$$\int_{\gamma_R} f(z)\mathrm{d}z \underset{R\to\infty}{\longrightarrow} \left(1-e^{2i\pi s}\right)\Gamma(s)\Gamma(1-s)$$

$$\Rightarrow \Gamma(s)\Gamma(1-s) = \frac{-2i\pi e^{i\pi s}}{1-e^{2i\pi s}} = \frac{-2i\pi}{e^{-i\pi s}-e^{i\pi s}}\frac{e^{i\pi s}}{e^{i\pi s}} = \frac{\pi}{\sin(\pi s)}.$$

■

II.B Équation de la chaleur (221) (235) (241) (246)

Théorème 34: Équation de la chaleur

Soit $f \in \mathcal{C}^1([0,\pi],\mathbb{R})$ telle que $f(0) = f(\pi) = 0$. Notons K_f l'ensemble des éléments

$$u : \left\{ \begin{array}{ccc} [0,\pi]\times\mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ (x,t) & \longmapsto & u(x,t) \end{array} \right.$$

de $\mathcal{C}([0,\pi]\times\mathbb{R}_+)$ qui vérifient :

(1) $\partial_x u$ et $\partial_t u$ existent et sont continues sur $[0,\pi]\times\mathbb{R}_+^*$,
(2) $\partial^2_{x^2} u$ existe et est continue sur $[0,\pi]\times\mathbb{R}_+^*$,
(3) pour tout réel $t \geqslant 0, u(0,t) = u(\pi,t) = 0$,
(4) pour tout $(x,t) \in [0,\pi]\times\mathbb{R}_+^*, \partial_t u(x,t) = \partial^2_{x^2} u(x,t)$;
(5) Pour tout $x \in [0,\pi], u(x,0) = f(x)$.

Alors K_f est un singleton.

Dans ce développement il est important de commencer par modéliser le problème que l'on essaie de résoudre. Ici on se donne une barre de longueur π et on met un thermostat à chaque extrémité de la barre (par exemple des poches de glaces). On s'intéresse à l'évolution de la température en fonction du temps et de la position sur la barre lorsqu'on se donne la température en tout point à l'instant initial. On va voir ici qu'il existe une solution, qu'elle s'exprime comme une série de Fourier et que cette solution est unique.

Démonstration.

Existence

Méthode de séparation des variables

Soit $u : (x,t) \mapsto X(x)T(t)$ une application non identiquement nulle où $X \in \mathcal{C}^2([0,\pi],\mathbb{R})$ et $T \in \mathcal{C}^1(\mathbb{R}_+,\mathbb{R})$. Alors u est continue et vérifie (1) et (2).
Supposons que u vérifie aussi (3) et (4).

Alors comme $u \neq 0$, on peut trouver $(x_0,t_0) \in]0,\pi[\times\mathbb{R}_+$, tel que $u(x_0,t_0) \neq 0$ et par continuité de u, on peut même imposer $t_0 > 0$. (En particulier $X(x_0) \neq 0$ et $T(t_0) \neq 0$).
Mais alors :

$$X(x_0)T'(t_0) = X''(x_0)T(t_0)$$

On pose alors $k = -\dfrac{T'(t_0)}{T(t_0)} = -\dfrac{X''(x_0)}{X(x_0)}$.
Comme l'équation

$$X(x)T'(t) = X''(x)T(t)$$

est vérifiée pour tout x et tout t, on a en particulier $X'' = -kX$ et $T' = -kT$. On commence par résoudre ces équations simplifiées.

Supposons $k < 0$

Alors il existe (A,B), non tous deux nuls, tels que :

$$X(x) = Ae^{\sqrt{-k}x} + Be^{-\sqrt{-k}x}$$

D'après les conditions aux bords imposent alors $\begin{pmatrix} A \\ B \end{pmatrix} \in \ker\left(\begin{pmatrix} 1 & 1 \\ \exp(\sqrt{-k\pi}) & \exp(-\sqrt{-k\pi}) \end{pmatrix}\right)$ or cette matrice est inversible. C'est donc absurde car $u \neq 0$, donc $k \geqslant 0$.

Supposons $k = 0$

Alors $X(x) = Ax + B$ et les conditions aux bords imposent alors $A = B = 0$.

Donc $k > 0$

et il existe donc $(A, B) \in \mathbb{R}^2$, non nul, tel que

$$X(x) = A\cos(\sqrt{k}x) + B\sin(\sqrt{k}x)$$

Les conditions aux bords donnent alors : $A = 0$ et $\sin(\sqrt{k}\pi) = 0$. Donc il existe $n \in \mathbb{N}^*$ tel que $\sqrt{k} = n$ et donc $X(x) = B\sin(nx)$, et $T(t) = Ce^{-n^2 t}$ puis, il existe un réel $K \in \mathbb{R}^*$, et $n \in \mathbb{N}^*$ tel que :

$$u(x,t) = K\sin(nx)\exp\left(-n^2 t\right)$$

pour tout couple $(x,t) \in [0,\pi] \times \mathbb{R}_+^*$ et même, par continuité de u, pour tout $(x,t) \in [0,\pi] \times \mathbb{R}_+$.

Réciproquement, on vérifie qu'une telle fonction vérifie bien les points (1), (2), (3) et (4). Désormais, pour tout $n \in \mathbb{N}^*$ nous noterons :

$$u_n(x,t) = \sin(nx)\exp\left(-n^2 t\right)$$

Superposition des solutions

On prolonge la fonction f par 2π-périodicité et imparité sur $\mathbb{R}$. On note $\tilde{f}$ ce prolongement. On a donc $\tilde{f} \in \mathcal{C}^0 \cap \mathcal{C}^1_m$ et on note $b_n(\tilde{f})$ les coefficients de Fourier réels de $\tilde{f}$.

La série $\sum_{n\geqslant 1} b_n(\tilde{f})u_n$ converge normalement donc simplement sur $[0,\pi] \times \mathbb{R}_+$. En effet, comme $\tilde{f}$ est continue et $\mathcal{C}^1$ par morceaux, f est limite uniforme de sa série de Fourier et on a donc $\left(b_n(\tilde{f})\right)_{n\in\mathbb{N}*}$ est sommable, or pour tout $n \geqslant 1$:

$$\left\|b_n(\tilde{f})u_n\right\|_\infty \leqslant \left|b_n(\tilde{f})\right|$$

On note S la somme de la série.

La convergence normale (donc uniforme) de la série et la continuité des u_n nous assurent donc la continuité de S sur $[0,\pi] \times \mathbb{R}_+$.

On a immédiatement pour tout $t \in \mathbb{R}_+$, on a : $S(0,t) = S(\pi,t) = 0$. Donc la fonction S vérifie (3).

Montrons que S vérifie aussi (1) et (2).

Par analogie des méthodes, on traite l'existence et la continuité, par exemple de $\partial_t S$:

Soit $\varepsilon \in \mathbb{R}_+^*$. Pour tout $x \in [0,\pi]$, tout $t \in [\varepsilon, +\infty[$, et tout entier $n \geqslant 1$, $u_n(x,\cdot)$ est $\mathcal{C}^1$ et :

$$\left|\partial_t\left(b_n(\tilde{f})u_n\right)(x,t)\right| \leqslant \left|b_n(\tilde{f})\right| n^2 \mathrm{e}^{-n^2\varepsilon} = \underset{n\to+\infty}{O}\left(\left|b_n(\tilde{f})\right|\right)$$

donc, comme la série $\sum_{n\geqslant 1}\left|b_n(\tilde{f})\right|$ converge, la série $\sum_{n\geqslant 1} b_n(\tilde{f})\partial_t u_n(x,\cdot)$ converge normalement sur $]\varepsilon, +\infty[$, pour tout $x \in [0,\pi]$. Mais ε étant quelconque, S est donc dérivable selon t sur $[0,\pi] \times \mathbb{R}_+^*$, et $\partial_t S$ est obtenue en dérivant terme à terme dans la série.

De plus, $b_n(\tilde{f})\partial_t u_n$ est continue sur $[0,\pi] \times \mathbb{R}_+^*$ et la majoration

$$\left|\partial_t\left(b_n(\tilde{f})u_n(x,t)\right)\right| \leqslant |b_n(\tilde{f})| n^2 e^{-n^2\varepsilon}$$

est indépendante de x et de t, donc $\sum b_n(\tilde{f})\partial_t u_n$ converge normalement sur $[0,\pi] \times [\varepsilon, +\infty[$. Donc $\partial_t S$ est continue sur $[0,\pi] \times \mathbb{R}_+^*$.

On montre de même que $\partial_x S$ et $\partial^2_{x^2} S$ existent et sont continues et se calculent par dérivation terme à terme.

La linéarité de l'équation de la chaleur assure que S vérifie (4).

Enfin, pour tout $x \in [0,\pi]$, $S(x,0) = \sum_{n=1}^{+\infty} b_n(\tilde{f})\sin(nx)$ est la somme de la série de Fourier de $\tilde{f}$ c'est donc $\tilde{f}$ puisque $\tilde{f} \in \mathcal{C}^0 \cap \mathcal{C}^1_m$. C'est-à-dire que S vérifie (5).
Au final, $S \in K_f$.

Unicité

Soient u_1 et u_2 des éléments de K_f. Posons $u = u_1 - u_2$. Alors $u \in K_0$.
On définit sur $\mathbb{R}_+$ la fonction $H : t \mapsto \displaystyle\int_0^\pi u^2(x,t)\mathrm{d}x$.
Comme u est continue sur $[0,\pi]\times\mathbb{R}_+$, H l'est aussi sur $\mathbb{R}_+$. De plus l'existence et la continuité de $\partial_t u$ sur $[0,\pi]\times\mathbb{R}_+^*$ assurent que H est $\mathcal{C}^1$ sur $\mathbb{R}_+^*$ et que pour tout $t \in \mathbb{R}_+^*$:

$$H'(t) = \int_0^\pi 2\partial_t u(x,t)u(x,t)\mathrm{d}x = \int_0^\pi 2\partial^2_{x^2} u(x,t)u(x,t)\mathrm{d}x$$

Par IPP et conditions aux bords, on a :

$$\begin{aligned} H'(t) &= \left[2u(x,t)\partial_x u(x,t)\right]_0^\pi - 2\int_0^\pi \left(\partial_x u(x,t)\right)^2 \,\mathrm{d}x \\ &= -2\int_0^\pi \left(\partial_x u(x,t)\right)^2 \,\mathrm{d}x \leqslant 0 \end{aligned}$$

Donc H est à la fois décroissante et positive sur $\mathbb{R}_+$, et, $H(0) = 0$ par (5). Donc H est identiquement nulle, et comme u^2 est positive continue, $u_1 = u_2$. ■

De plus, on a une formule explicite pour la solution de l'équation de la chaleur :

$$\left\{\begin{array}{ccc} [0,\pi]\times\mathbb{R}_+ & \to & \mathbb{R} \\ (x,t) & \longmapsto & \displaystyle\sum_{n=1}^{+\infty} b_n(\tilde{f})\sin(nx)\mathrm{e}^{-n^2 t} \end{array}\right.$$

II.C Théorème d'Hadamard-Lévy (204) (214) (215) (220)

Théorème 35: Hadamard-Lévy

Soient $n \in \mathbb{N}^*$ et $f : \mathbb{R}^n \to \mathbb{R}^n \in \mathcal{C}^2\left(\mathbb{R}^n, \mathbb{R}^n\right)^a$. Les deux propositions suivantes sont équivalentes :

1. L'application f est un $\mathcal{C}^2$-difféomorphisme de $\mathbb{R}^n$ sur $\mathbb{R}^n$.
2. Pour tout $x \in \mathbb{R}^n$, $\mathrm{d}f(x)$ est inversible, et $\lim\limits_{\|x\| \to +\infty} \|f(x)\| = +\infty$.

Démonstration. On ne démontre que le sens difficile (à savoir $2 \implies 1$). Une idée pour démontrer cette implication est d'utiliser le théorème d'inversion globale. Pour cela on a besoin de l'injectivité de f. On va donc montrer que f jouit de cette propriété en utilisant un inverse à droite de cette fonction. On cherchera une condition suffisante sur cette inverse pour avoir l'injectivité de f et on démontrera ensuite que l'inverse possède cette propriété.

Construction d'un inverse à droite

On suppose que pour tout $x \in \mathbb{R}^n$, $\mathrm{d}f(x)$ soit inversible, et $\lim\limits_{\|x\| \to +\infty} \|f(x)\| = +\infty$.

Quitte à remplacer f par $f - f(0)$ OPS $f(0) = 0$.

Soit I un intervalle ouvert de $\mathbb{R}$ contenant 0 et 1. Si $s : I \times \mathbb{R}^n \to \mathbb{R}^n$ est dérivable selon la première variable et est telle que :

$$\forall (t,x) \in I \times \mathbb{R}^n, f \circ s(t,x) = tx \tag{1}$$

Alors $s(1, \cdot)$ sera inverse à droite de f.

Si $s : I \times \mathbb{R}^n \to \mathbb{R}^n$, dérivable selon la première variable, alors par théorème de Cauchy, l'application s vérifie (1) si et seulement si, pour tout $(t,x) \in I \times \mathbb{R}^n$ (où on voir x comme étant un paramètre fixé et t la variable pour appliquer le théorème de Cauchy qui donne existence et unicité d'une solution maximale),

$$\begin{cases} \frac{\partial}{\partial t}(f \circ s)(t,x) = \mathrm{d}f(s(t,x)) \circ \partial_t s(t,x) = x \\ f \circ s(0,x) = 0 \end{cases}$$

soit si et seulement si, pour tout $(t,x) \in I \times \mathbb{R}^n$,

$$\begin{cases} \partial_t s(t,x) = (\mathrm{d}f(s(t,x)))^{-1} \cdot x \\ s(0,x) \in f^{-1}(\{0\}) \end{cases}$$

On prend alors un élément dans l'image réciproque de $\{0\}$ par f, par l'hypothèse que l'on a fait au début, on peut choisir 0. On obtient ainsi :
si pour tout $x \in \mathbb{R}^n, s(\cdot, x)$ est solution sur l'intervalle I du problème de Cauchy autonome :

$$\begin{cases} y' &= F(x,y) \\ y(0) &= 0 \end{cases} \tag{2}$$

alors s vérifie (1) ; où l'on a noté

$$F : \begin{cases} \mathbb{R}^n \times \mathbb{R}^n & \longrightarrow \mathbb{R}^n \\ (x,y) & \longmapsto \mathrm{d}f(y)^{-1} \cdot x \end{cases}$$

L'application F est de classe $\mathcal{C}^1$ comme composée de fonctions de classe $\mathcal{C}^1$.
En particulier, elle est $\mathcal{C}^0$ et localement lipschitzienne en y. Donc par le théorème de Cauchy-Lipschitz, pour tout $x \in \mathbb{R}^n$, il existe une unique solution maximale $(s(\cdot,x),]T^-, T^+[)$ de (2), notée $s(\cdot,x)$, définie sur un intervalle ouvert $]T^-(x), T^+(x)[$ contenant 0 (à l'oral, on notera T^+ et T^- sans dépendance en x pour alléger l'écriture, mais on l'évoquera à l'oral).

On a :

$$x \in \mathbb{R} \qquad T^+(x) > 1.$$

car si $T^+(x) \leqslant 1$, alors d'après le critère d'explosion en temps fini (ou théorème de sortie de tout compact), on a : $\lim\limits_{t \to T^+(x)} \|s(t,x)\| = +\infty$ et donc comme f est coercitive, on obtient $\lim\limits_{t \to T^+(x_0)} \|f \circ s(t,x)\| = +\infty$. Or $\|f \circ s(t,x)\| = \|tx\| \underset{t \to T^+(x)}{\longrightarrow} T^+(x)\|x\| < \infty$. C'est donc absurde.

On peut donc définir l'application $s_1 = s(1,\cdot)$ et ainsi s_1 est un inverse à droite de f : $f \circ s_1 = \mathrm{id}_{\mathbb{R}^n}$.

Injectivité de f.

Soient y_1 et y_2 des éléments de $\mathbb{R}^n$ tels que $f(y_1) = f(y_2)$. **Supposons que s_1 soit surjective**, alors on dispose de x_1, x_2 tels que $y_1 = s_1(x_1)$ et $y_2 = s_1(x_2)$:

$$y_1 = s_1(x_1) \text{ et } y_2 = s_1(x_2)$$

Comme s_1 est un inverse à droite de f, on a :

$$x_1 = f \circ s_1(x_1) = f(y_1) = f(y_2) = f \circ s_1(x_2) = x_2$$

Donc $y_1 = s_1(x_1) = s_1(x_2) = y_2$. Donc f est injective.

Il faut donc montrer que s_1 est surjective.

Surjectivité de s_1.

On démontre cette assertion par un argument de connexité : on va montrer que $s_1(\mathbb{R}^n)$ est à la fois ouvert et fermé dans $\mathbb{R}^n$ qui est connexe, c'est-à-dire que $s_1(\mathbb{R}^n) = \mathbb{R}^n$.

$s_1(\mathbb{R}^n)$ **est fermé** Soit $(x_k)_{k\in\mathbb{N}}$ telle que $(s_1(x_k))_{k\in\mathbb{N}}$ converge vers $y \in \mathbb{R}^n$. Alors comme f est continue, on obtient $\lim\limits_{k\to+\infty} \underbrace{f \circ s_1(x_k)}_{=x_k} = f(y)$. **Si on suppose de plus s_1 continue** alors on a $s_1(x_k) = s_1(f(y))$. Donc $s_1(\mathbb{R}^n)$ est fermé.

$s_1(\mathbb{R}^n)$ **est ouvert (voisinage de chacun de ses points)** Soient $y \in s_1(\mathbb{R}^n)$. Il s'écrit $y = s_1(x)$ pour un certain $x \in \mathbb{R}^n$. Comme $\mathrm{d}f(y)$ est inversible, par le théorème d'inversion locale on dispose d'un voisinage ouvert $\mathcal{U}$ de $x = f(s_1(y))$, et d'un voisinage ouvert $\mathcal{V}$ de y tels que f induise un $\mathcal{C}^1$-difféomorphisme ϕ de $\mathcal{V}$ sur $\mathcal{U}$. **Si on suppose s_1 continue** alors on dispose d'un voisinage ouvert $\mathcal{U}'$ de x inclus dans $\mathcal{U}$ tel que $s_1(\mathcal{U}') \subset \mathcal{V}$. Alors

$$s_1(\mathcal{U}') = \phi^{-1}(\phi(s_1(\mathcal{U}'))) = \phi^{-1}(f(s_1(\mathcal{U}'))) = \phi^{-1}(\mathcal{U}').$$

Donc est ouvert comme image réciproque de $\mathcal{U}'$ par ϕ qui est continue. Finalement $y \in s_1(\mathcal{U}') \subset s_1(\mathbb{R}^n)$ qui contient y. Donc $s_1(\mathbb{R}^n)$ est un voisinage de y. Finalement $s_1(\mathbb{R}^n)$ est ouvert, car voisinage de chacun de ses points.

Donc, par connexité de $\mathbb{R}^n$, $s_1(\mathbb{R}^n)$ étant ouvert, fermé et non vide, on a :

$$s_1(\mathbb{R}^n) = \mathbb{R}^n$$

Il reste donc maintenant à démontrer la continuité de s_1.

Continuité de s_1

Soient $x_0 \in \mathbb{R}^n$ on dispose de r tel que $x_0 \in \overline{\mathrm{B}(0, r-1)}$.
Comme f est coercitive $f^{-1}\left(\overline{\mathrm{B}(0,r)}\right) \subset \overline{\mathrm{B}(0,R)}$ pour un certain R

On a $\|f \circ s(t,x)\| = \|tx\| \leqslant r$, pour tout $t \in [0,1]$ et tout $x \in \overline{\mathrm{B}(0,r)}$. C'est-à-dire que l'on a :

$$s([0,1] \times \overline{\mathrm{B}(0,r)}) \subset f^{-1}(\overline{\mathrm{B}(0,r)}) \subset \overline{\mathrm{B}(0,R)}$$

Comme F est de classe $\mathcal{C}^1$ sur $\overline{\mathrm{B}(0,R)}^2$ qui est à la fois convexe et compact, elle y est K-lipschitzienne (IAF) avec $K := \max_{(x,y)\in\overline{\mathrm{B}(0,R)}^2} \| \mathrm{d}F(x,y)\|_{\mathcal{L}}$.

Soit $x_1 \in \mathbb{R}^n$ tel que $\|x_1 - x_0\| \leqslant 1$. Par inégalité triangulaire on a $x_1 \in \overline{\mathrm{B}(0,r)}$. On obtient ainsi :

$$\begin{aligned}
\|s(t,x_1) - s(t,x_0)\| &= \left\| \int_0^t \partial_t s(u,x_1) - \partial_t s(u,x_0)\,\mathrm{d}u \right\| \\
&\leqslant \int_0^t \|F(x_1, s(u,x_1)) - F(x_0, s(u,x_0))\|\,\mathrm{d}u \\
&\leqslant K\|x_1 - x_0\| + \int_0^t K\|s(u,x_1) - s(u,x_0)\|\,\mathrm{d}u
\end{aligned}$$

Finalement, en utilisant le lemme de Grönwall, on a :

$$\|s(t,x_1) - s(t,x_0)\| \leqslant K\|x_1 - x_0\| e^{Kt}$$

En particulier en $t = 1$, on obtient que pour tout $x \in \overline{\mathrm{B}(x_0,1)}$, on a :

$$\|s_1(x) - s_1(x_0)\| \leqslant Ke^K\|x - x_0\|$$

Comme x_0 est quelconque, s_1 est localement lipschitzienne sur $\mathbb{R}^n$, donc en particulier continue.

Conclusion

L'application f est injective, de classe $\mathcal{C}^2$, et sa différentielle est partout inversible. Donc d'après le théorème d'inversion globale f réalise un $\mathcal{C}^2$ difféomorphisme de $\mathbb{R}^n$ sur $f(\mathbb{R}^n) = \mathbb{R}^n$.

Ceci conclut de prouver l'implication $2 \Longrightarrow 1$.

■

II.D Théorème de Lévy et TCL (209) (218) (228) (235) (250) (261) (262) (266)

On énonce un lemme très utile qu'on ne démontrera pas.

Lemme 36:

Soit x_n une suite de variables aléatoires réelles et soit X une variable aléatoire réelle. Alors il y a équivalence entre les deux assertions suivantes :

(1) $\forall f \in \mathcal{C}_b^0(\mathbb{R},\mathbb{C}) \quad \mathbb{E}[f(X_n)] \to \mathbb{E}[f(X)]$

(2) $\forall f \in \mathcal{C}_0^0(\mathbb{R},\mathbb{C}) \quad \mathbb{E}[f(X_n)] \to \mathbb{E}[f(X)]$

Théorème 37: de Paul Lévy

Soit x_n une suite de variables aléatoires réelles et soit X une variable aléatoire réelle. Alors les deux assertions suivantes sont équivalentes :

(1) $X_n \xrightarrow{\mathcal{L}oi} X$;

(2) $\varphi_{X_n} \xrightarrow{c.v.s} \varphi_X$

Démonstration.

(1) $\Longrightarrow$ (2)
L'implication (1) $\Longrightarrow$ (2) est immédiate car on applique la définition de la convergence en loi :

$$\forall f \in \mathcal{C}_b^0(\mathbb{R},\mathbb{C}) \quad \mathbb{E}[f(X_n)] \to \mathbb{E}[f(X)],$$

avec la fonction $\varphi_t : x \mapsto \mathrm{e}^{itx}$ pour tout $t \in \mathbb{R}$.

(2) $\Longrightarrow$ (1)
On va montrer que pour toute fonction $f \in \mathcal{C}_0^0(\mathbb{R},\mathbb{C})$, on a $\mathbb{E}[f(X_n)] \to \mathbb{E}[f(X)]$. Soit $f \in \mathcal{C}_0^0(\mathbb{R},\mathbb{C})$ on utilise la densité de la classe de Schwarz $\mathcal{S}(\mathbb{R})$ dans $\mathcal{C}_0^0(\mathbb{R},\mathbb{C})$. Alors pour tout $\varepsilon > 0$ il existe $f_\varepsilon \in \mathcal{S}(\mathbb{R})$ telle que $\|f - f_\varepsilon\|_\infty \leqslant \varepsilon$. Alors :

$$|\mathbb{E}[f(X_n)] - \mathbb{E}[f(X)]| \leqslant \underbrace{|\mathbb{E}[f(X_n)] - \mathbb{E}[f_\varepsilon(X_n)]|}_{\leqslant \varepsilon} + |\mathbb{E}[f_\varepsilon(X_n)] - \mathbb{E}[f_\varepsilon(X)]| + \underbrace{|\mathbb{E}[f_\varepsilon(X)] - \mathbb{E}[f(X)]|}_{\leqslant \varepsilon}.$$

Il suffit donc de montrer le résultat pour $f \in \mathcal{S}(\mathbb{R})$.

Soit alors $f \in \mathcal{S}(\mathbb{R})$. Par inversion de Fourier dans la classe de Schwarz, on a $\hat{f} \in \mathcal{S}(\mathbb{R})$ et :

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

Donc il existe $g \in \mathcal{S}(\mathbb{R})$ tel que $f = \displaystyle\int_{\mathbb{R}} g(\xi) e^{ix\xi} \mathrm{d}\xi$. On a alors, par Fubini et convergence dominée puis re-Fubini :

$$\mathbb{E}[f(X_n)] = \mathbb{E}\left[\int_{\mathbb{R}} g(\xi) e^{iX_n\xi} \mathrm{d}\xi\right] = \int_{\mathbb{R}} g(\xi) \mathbb{E}\left[e^{iX_n\xi}\right] \mathrm{d}\xi \to \int_{\mathbb{R}} g(\xi) \mathbb{E}\left[e^{iX\xi}\right] \mathrm{d}\xi = \mathbb{E}\left[\int_{\mathbb{R}} g(\xi) e^{iX\xi} \mathrm{d}\xi\right] = \mathbb{E}[f(X)].$$

Ceci établit donc le théorème sur la classe de Schwarz et on conclut par densité pour les fonctions continues nulles aux bords.

D'après le lemme on a alors la convergence en loi de X_n vers X, ce qui conclut cette preuve. ■

Théorème 38: Théorème central limite

Soit $(X_n)_{n\in\mathbb{N}^*}$ une suite de variables aléatoires réelles, indépendantes, identiquement distribuées, et éléments de $\mathbb{L}^2(\Omega,\mathcal{F},\mathbb{P})$. On suppose en outre que $\mathrm{Var}(X_1)\neq 0$. Alors on a :

$$\sqrt{n}\left(\bar{X}_n-\mathbb{E}[X_1]\right)\underset{n\to+\infty}{\mathcal{L}}\mathcal{N}(0,\mathrm{Var}(X_1))$$

Démonstration. Quitte à centrer et réduire les variables aléatoires, c'est-à-dire à remplacer X_n par $\dfrac{X_n-\mathbb{E}[X_1]}{\sqrt{\mathrm{Var}(X_1)}}$ on peut supposer que X_n centrée et réduite.

D'après le théorème de Paul Lévy, il suffit de montrer la convergence simple sur $\mathbb{R}$ de la suite de fonctions caractéristiques $\left(\varphi_{\frac{S_n}{\sqrt{n}}}\right)_{n\in\mathbb{N}^*}$ vers la fonction caractéristique de la loi normale centrée réduite :

$$t\longmapsto\exp\left(-\frac{t^2}{2}\right)$$

Soit $t\in\mathbb{R}$. Pour tout $n\in\mathbb{N}^*$, comme $X_1,\dots,X_n$ sont mutuellement indépendantes et identiquement distribuées, on a :

$$\begin{aligned}
\varphi_{S_n}\frac{S_n}{\sqrt{n}}(t)&=\mathbb{E}\left[\exp\left(it\frac{S_n}{\sqrt{n}}\right)\right]\\
&=\mathbb{E}\left[\exp\left(i\frac{t}{\sqrt{n}}\sum_{k=1}^{n}X_k\right)\right]\\
&=\mathbb{E}\left[\prod_{k=1}^{n}\exp\left(i\frac{t}{\sqrt{n}}X_k\right)\right]\\
&\overset{\perp\!\!\!\perp}{=}\prod_{k=1}^{n}\mathbb{E}\left[\exp\left(i\frac{t}{\sqrt{n}}X_k\right)\right]\\
&\overset{id}{=}\mathbb{E}\left[\exp\left(i\frac{t}{\sqrt{n}}X_1\right)\right]^n\\
&=\varphi_{X_1}\left(\frac{t}{\sqrt{n}}\right)^n
\end{aligned}$$

Or, comme $X_1\in\mathbb{L}^2$ sa fonction caractéristique est de classe C^2 sur $\mathbb{R}$, de plus on a :

$$\varphi'_{X_1}(0)=i\mathbb{E}[X_1]=0,\quad \varphi''_{X_1}(0)=-\mathbb{E}\left[X_1^2\right]=-\mathrm{Var}(X_1)=-1$$

Par Taylor-Young, on a :

$$\varphi_{X_1}\left(\frac{t}{\sqrt{n}}\right)=\ldots=1-\frac{t^2}{2n}+\frac{t^2}{n}\varepsilon\left(\frac{t}{\sqrt{n}}\right)$$

Or pour $|a|,|b|\leqslant 1$ et pour tout n, on a :

$$|a^n-b^n|=\left|(a-b)\sum_{k=0}^{n-1}a^kb^{n-k}\right|\leqslant n|a-b|.$$

Donc pour n assez grand $\left|1-\dfrac{t^2}{2n}\right|\leqslant 1$ et :

de sorte que, d'après le lemme, pour tout entier $n\geqslant N$, on ait :

$$\begin{aligned}
\left|\varphi_{\frac{S_n}{\sqrt{n}}}(t)-\left(1-\frac{t^2}{2n}\right)^n\right|&=\left|\varphi_{X_1}\left(\frac{t}{\sqrt{n}}\right)^n-\left(1-\frac{t^2}{2n}\right)^n\right|\\
&\leqslant n\left|\varphi_{X_1}\left(\frac{t}{\sqrt{n}}\right)-\left(1-\frac{t^2}{2n}\right)\right|\\
&\leqslant t^2\left|\varepsilon\left(\frac{t}{\sqrt{n}}\right)\right|\underset{n\to+\infty}{\longrightarrow}0
\end{aligned}$$

Or $\left(1-\frac{t^2}{2n}\right)^n \underset{n\to+\infty}{\longrightarrow} \exp\left(-\frac{t^2}{2}\right) = \varphi_N(t)$ où $N \sim \mathcal{N}(0,1)$.

D'où $\varphi_{\frac{S_n}{\sqrt{n}}} \xrightarrow{cvs} \varphi_N$. ■

II.E Développement asymptotique à trois termes de la suite des log itérés (218) (223) (224) (226) (230)

Théorème 39:

Soit $\begin{cases} u_0 \in \mathbb{R}_+^* \\ u_{n+1} = \ln(u_n + 1) \end{cases}$.
Le développement asymptotique à trois termes de u_n est :

$$u_n = \frac{2}{n} + \frac{2}{3}\frac{\ln(n)}{n^2} + \frac{c}{n^2} + o\left(\frac{1}{n^2}\right).$$

Démonstration. Soit $u_0 \in \mathbb{R}_+^*$ et soit u_n défini comme dans l'énoncé.

* Bien définie : $\ln(1 + \mathbb{R}_+^*) \subset \mathbb{R}_+^*$ car ln et strictement croissante et $\ln(1) = 0$.
* Convergence : Par continuité de ln si la suite $(u_n)_n$ converge alors elle converge vers un point fixe de $\ln(1 + \cdot)$ i.e. vers 0.
  Or par stricte concavité de ln, on a : $0 < \ln(1 + x) < x$ pour tout réel x strictement positif.
  On a donc que la suite $(u_n)_n$ est décroissante et minorée par 0 donc converge.
* Équivalent : soit $\alpha \neq 0$:

$$\begin{aligned} u_{n+1}^\alpha - u_n^\alpha &= (\ln(1 + u_n))^\alpha - u_n^\alpha \\ &= \left(u_n - \frac{u_n^2}{2} + o(u_n^2)\right)^\alpha - u_n^\alpha \\ &= u_n^\alpha \left(\left(1 - \frac{u_n}{2} + o(u_n)\right)^\alpha - 1\right) \\ &= u_n^\alpha \left(1 - \alpha\frac{u_n}{2} + o(u_n) - 1\right) \\ &= -\frac{\alpha}{2} u_n^{\alpha+1} + o\left(u_n^{\alpha+1}\right). \end{aligned}$$

  On prend alors $\alpha = -1$ et on obtient : $u_{n+1}^{-1} - u_n^{-1} \sim \frac{1}{2}$.
  Ainsi la série de terme général $u_{n+1}^{-1} - u_n^{-1}$ diverge grossièrement et par sommation d'équivalent dans le cas divergent (et par télescopage) :

$$\frac{1}{u_n} - \frac{1}{u_0} = \sum_{k=0}^{n-1} u_{k+1}^{-1} - u_k^{-1} \sim \frac{n}{2}.$$

  On en déduit donc :

$$u_n \sim \frac{2}{n}.$$

* Deuxième terme : Un développement limité de u_{n+1} est :

$$u_{n+1} = u_n - \frac{u_n^2}{2} + \frac{u_n^3}{3} + O(u_n^4).$$

Alors :

$$\begin{aligned}
u_{n+1}^{-1} - u_n^{-1} &= (\ln(1+u_n))^{-1} - u_n^{-1} \\
&= \left(u_n - \frac{u_n^2}{2} + \frac{u_n^3}{3} + O(u_n^4)\right)^{-1} - u_n^{-1} \\
&= u_n^{-1}\left(\left(1 - \frac{u_n}{2} + \frac{u_n^2}{3} + O(u_n^3)\right)^{-1} - 1\right) \\
&= u_n^{-1}\left(1 - \left(-\frac{u_n}{2} + \frac{u_n^2}{3}\right) + \frac{2}{2}\left(-\frac{u_n}{2} + \frac{u_n^2}{3}\right)^2 + O(u_n^3) - 1\right) \\
&= u_n^{-1}\left(\frac{u_n}{2} - \frac{u_n^2}{12} + O(u_n^3)\right) \\
&= \frac{1}{2} - \frac{u_n}{12} + O\left(u_n^2\right).
\end{aligned}$$

En utilisant l'équivalent trouvé précédemment on trouve :

$$u_{n+1}^{-1} - u_n^{-1} - \frac{1}{2} \sim \frac{-u_n}{12} \sim \frac{-2}{12n} = \frac{-1}{6n}.$$

A nouveau par sommation d'équivalent dans le cas divergent et télescopage on déduit :

$$u_n^{-1} - u_0^{-1} - \frac{n}{2} \sim \sum_{k=1}^{n} \frac{-1}{6k} \sim \frac{-\ln(n)}{6}.$$

Finalement

$$u_n = \left(\frac{n}{2} - \frac{\ln(n)}{6} + o\left(\ln(n)\right)\right)^{-1}$$

C'est-à-dire (après factorisation par $\left(\frac{n}{2}\right)^{-1}$ puis DL :

$$u_n = \frac{2}{n} + \frac{2\ln(n)}{3n^2} + o\left(\frac{\ln(n)}{n^2}\right).$$

* Troisième terme : On réinjecte l'expression que l'on vient de trouver dans le développement limité que l'on a effectué au début de la partie précédente et on trouve :

$$u_{n+1}^{-1} - u_n^{-1} - \frac{1}{2} + \frac{1}{6n} \sim -\frac{\ln(n)}{18n^2}.$$

Or la famille $\left(-\frac{\ln(n)}{18n^2}\right)_n$ est sommable par Riemann donc ses sommes partielles convergent vers une constante c_0. On a alors :

$$\sum_{k=1}^{n-1}\left(u_{k+1}^{-1} - u_k^{-1} - \frac{1}{2} + \frac{1}{6k}\right) = u_n^{-1} - u_1^{-1} - \frac{n}{2} + \frac{1}{6}\sum_{k=1}^{n-1}\frac{1}{k} \longrightarrow c_0.$$

On a alors :

$$\begin{aligned}
u_n^{-1} &= \frac{n}{2} - \frac{1}{6}\ln(n) + \underbrace{u_1^{-1} - \frac{1}{6}\gamma + c_0}_{=:c} + o(1) \\
&= \left(\frac{n}{2} - \frac{1}{6}\ln(n) + c + o(1)\right)^{-1} \\
&= \frac{2}{n}\left(1 - \frac{1}{3n}\left(\ln(n) + 6c\right) + o\left(\frac{1}{n}\right)\right)^{-1} \\
&= \frac{2}{n}\left(1 + \frac{1}{3n}\left(\ln(n) + 6c\right) + o\left(\frac{1}{n}\right)\right) \\
&= \frac{2}{n} + \frac{2}{3}\frac{\ln(n)}{n^2} + \frac{c}{n^2} + o\left(\frac{1}{n^2}\right).
\end{aligned}$$

■

II.F Caractérisation de la fonction Gamma d'Euler par log-convexité (229) (239) (253)

La fonction Gamma d'Euler est :

$$\Gamma : \left\{ \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R}_+^* \\ x & \longmapsto & \displaystyle\int_0^{+\infty} t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t \end{array} \right.$$

Théorème 40: de Bohr-Mollerup-Artin

Soit $\mathcal{F}$ l'ensemble des applications $f : \mathbb{R}_+^* \longrightarrow \mathbb{R}_+^*$ vérifiant :

i) $f(1) = 1$;

ii) pour tout $x \in \mathbb{R}_+^*$, $f(x+1) = xf(x)$;

iii) $\ln \circ f$ est convexe (on dit que f est log-convexe).

Alors $\mathcal{F} = \{\Gamma\}$.

Démonstration.

Existence : la fonction Gamma est un élément de $\mathcal{F}$

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

ii) Par IPP justifiée par la convergence du crochet qui vaut 0, on a pour tout $x > 0$:

$$\Gamma(x+1) = \int_0^{+\infty} t^x\mathrm{e}^{-t}\,\mathrm{d}t = \left[-t^x\mathrm{e}^{-t}\right]_0^{+\infty} + x\int_0^{+\infty} t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t = x\Gamma(x).$$

iii) La fonction Γ est $\mathcal{C}^2$ donc l'application $\ln\circ\Gamma$ est de classe $\mathcal{C}^2$, et $(\ln\circ\Gamma)'' = \frac{\Gamma''\Gamma - (\Gamma')^2}{\Gamma^2}$.
Soit $x \in \mathbb{R}_+^*$. On applique l'inégalité de Cauchy-Schwarz aux fonctions $t \mapsto \ln(t)t^{\frac{x-1}{2}}\mathrm{e}^{-\frac{t}{2}} \in \mathbb{L}^2(\mathbb{R}_+, \mathbb{R})$ et $t \mapsto t^{\frac{x-1}{2}}\mathrm{e}^{-\frac{t}{2}} \in \mathbb{L}^2(\mathbb{R}_+, \mathbb{R})$ et on a :

$$\begin{aligned} \Gamma'(x) &= \int_0^{+\infty} \ln(t)t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t \\ &= \int_0^{+\infty} \ln(t)t^{\frac{x-1}{2}}\mathrm{e}^{-\frac{t}{2}} \times t^{\frac{x-1}{2}}\mathrm{e}^{-\frac{t}{2}}\,\mathrm{d}t \\ &\leqslant \left(\int_0^{+\infty} \ln(t)^2 t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t\right)^{\frac{1}{2}} \left(\int_0^{+\infty} t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t\right)^{\frac{1}{2}} \\ &= \Gamma''(x)^{\frac{1}{2}}\Gamma(x)^{\frac{1}{2}} \end{aligned}$$

Il s'en suit $\Gamma''\Gamma - (\Gamma')^2 \geqslant 0$ et donc l'application $\ln\circ\Gamma \geqslant 0$, donc elle est convexe.

Unicité : Γ est le seul élément de $\mathcal{F}$
On sait maintenant que $\Gamma \in \mathcal{F}$. On va montrer que tout élément de $\mathcal{F}$ coïncide avec Γ sur $\mathbb{N}^*$, puis sur $]0,1[$ et enfin sur $\mathbb{R}_+^* \setminus \mathbb{N}$.
Soient $f \in \mathcal{F}$ et $x \in \mathbb{R}_+^*$.

1^{er} **cas : x est un entier (strictement positif).** Comme f et Γ vérifient $i)$ et $ii)$, on a :

$$f(x) = (x-1)! = \Gamma(x)$$

Ainsi f coïncide-t-elle avec Γ sur $\mathbb{N}^*$.

2^d **cas :** $x \in]0,1[$**.** Notons $g := \ln \circ f$. Soit $n \in \mathbb{N}^*$. Alors g est convexe par hypothèses, donc par le lemme des 3 pentes, on a l'inégalité suivante :

$$\underbrace{\frac{g(n)-g(n-1)}{1}}_{\text{pente 1}} \leqslant \underbrace{\frac{g(n+x)-g(n)}{x}}_{\text{pente 2}} \leqslant \underbrace{\frac{g(n+1)-g(n)}{1}}_{\text{pente3}}$$

On fera un beau dessin du courbe convexe pour illustrer le lemme.

Ainsi on obtient $\ln(n-1) \leqslant \frac{g(n+x)-g(n)}{x} \leqslant \ln(n)$, puis :

$$0 \leqslant g(n+x) - g(n) - x\ln(n-1) \leqslant x \ln\left(\frac{n}{n-1}\right)$$

Or, f vérifie ii) donc par une récurrence immédiate :

$$\begin{aligned} g(n+x) &= \ln(f(n+x)) \\ &= \ln((x+n-1)f(x+n-1)) \\ &= \dots \\ &= \ln\left(f(x)\prod_{j=1}^{n}(x+n-j)\right) = g(x) + \ln\left(\prod_{j=0}^{n-1}(x+j)\right) \end{aligned}$$

On obtient alors :

$$\begin{aligned} g(n+x) - g(n) - x\ln(n-1) &= \ln\left(f(x)\right) + \ln\left(\prod_{j=0}^{n-1}(x+j)\right) - g(n) - x\ln(n-1) \\ &= g(x) + \ln\left(\prod_{j=0}^{n-1}(x+j)\right) - \ln((n-1)!) - \ln\left((n-1)^x\right) \\ &= g(x) - \ln\left(\frac{(n-1)!(n-1)^x}{\prod_{j=0}^{n-1}(x+j)}\right). \end{aligned}$$

Enfin, par le lemme d'encadrement ($n \to \infty$)

$$g(x) = \lim_{n\to+\infty} \ln\left(\frac{n!n^x}{\prod_{j=0}^{n}(x+j)}\right);$$

puis par continuité de l'exponentielle :

$$f(x) = \lim_{n\to+\infty} \frac{n!n^x}{\prod_{j=0}^{n}(x+j)}$$

Or cette équation est vérifiée par toute fonction de $\mathcal{F}$, donc en particulier par $\Gamma \in \mathcal{F}$ et donc par unicité de la limite, f et Γ coïncident sur $]0,1[$.

3^e **cas :** $x \in]1,+\infty[\backslash\mathbb{N}$**.** Écrivons x comme la somme de sa partie entière $\lfloor x \rfloor$ et de sa partie fractionnaire $\mathrm{d}(x)$, c'est-à-dire $x = \lfloor x \rfloor + \mathrm{d}(x)$ où, remarquons le, $\mathrm{d}(x)$ est élément de $]0,1[$. Par les deux cas précédents, on a alors :

$$f(x) = (x-j) \quad f(\ \mathrm{d}(x)) = \left(\prod_{j=1}^{\lfloor x \rfloor - 1}(x-j)\right)\Gamma(\mathrm{d}(x)) = \Gamma(x).$$

Au total, l'étude des trois cas donnent que les applications f et Γ coïncident sur $\mathbb{R}_+^*$, ce qui achève de montrer l'égalité $\mathcal{F} = \{\Gamma\}$.

■

III Développements mixtes

Simplicité de $SO(3)$ [6]

III.A Simplicité de $SO(3)$ (103) (106) (108) (158) (161) (204)

Lemme 41:

Tout élément de $SO(3)$ est $O(3)$-semblable à une matrice de la forme :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

Démonstration. Soit $g \in SO(3)$. Alors comme g préserve la norme, si g admet une valeur propre réelle alors c'est ± 1. En effet $\|g(x)\| = \|x\|$ en particulier pour x un vecteur propre associé à une valeur propre réelle.

De plus comme $\deg(\chi_g) = 3$, l'endomorphisme g a nécessairement une valeur propre réelle.

Si λ est une valeur propre complexe de g, alors comme $\chi_g \in \mathbb{R}[X]$, nécessairement $\overline{\lambda}$ est aussi valeur propre de g et les valeurs propre de g sont alors : $1, \lambda, \overline{\lambda}$ avec $\lambda \in \mathbb{U}$ car alors $\det(g) = \pm\lambda\overline{\lambda} = \pm|\lambda|^2$.

Au total, on a donc :

$$\mathrm{sp}_{\mathbb{C}}(g) \in \{(1,1,1), (1,-1,-1), (1,\lambda,\overline{\lambda}) \quad / \quad \lambda \in \mathbb{U}\}.$$

Dans tous les cas on a donc 1 est valeur propre de g. Soit alors u un vecteur propre associé. Soi $F = (\mathbb{R}u)^{\perp} = \mathrm{Vect}(v, w)$. Alors F est stable par g, en effet soit $z \in F$, alors

$$\langle u, g(z)\rangle = \langle {}^t g(u), z\rangle = \langle g^{-1}(u), z\rangle = \langle u, z\rangle = 0$$

Donc g induit un endomorphisme sur F. De plus, cet endomorphisme est de déterminant 1 et conserve la norme. C'est donc un élément de $SO(2)$, c'est-à-dire une rotation du plan F. Donc sa matrice dans une certaine base de F est $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Ceci conclut la preuve du lemme. ■

Théorème 42:

Le groupe $SO(3)$ est simple.

Démonstration. Soit $H \lhd SO(3)$ un sous-groupe distingué non trivial de $SO(3)$. Montrons qu'il s'agit du groupe en entier.

$SO(3)$ est connexe par arcs. En effet, si $g \in SO(3)$, alors on dispose de $P \in O(3)$ tel que $g = PR_\theta P^{-1}$ où R_θ est définie comme dans le lemme précédent. Alors l'application :

$$\gamma : \begin{array}{ccc} [0,1] & \to & SO(3) \\ t & \mapsto & PR_{t\theta}P^{-1} \end{array}$$

est une application continue reliant I_3 et g. Ceci prouve la connexité par arcs de $SO(3)$.

Soit $h \in H$ un élément non trivial. On considère l'application

$$\varphi : \begin{array}{ccc} SO(3) & \to & \mathbb{R} \\ g & \mapsto & \mathrm{Tr}([g,h]) \end{array}$$

L'intervalle $\varphi(SO(3))$ L'application φ est continue comme composée d'application continue, donc $\varphi(SO(3))$ est connexe comme image continue d'un connexe. C'est donc un connexe de $\mathbb{R}$, donc convexe et donc c'est un intervalle.

D'une part $\varphi(I_3) = 3$.
D'autre part $\forall g \in SO(3) \;\; \varphi(g) = 1 + 2\cos\alpha$ pour αangle de g (cf lemme). Donc $\forall g \in SO(3) \;\; \varphi(g) \leqslant 3$.

Comme de plus $SO(3)$ est compacte, $\varphi(SO(3))$ est compacte comme image continue d'un compact. Donc $\varphi(SO(3)) = [a, 3]$ avec $a \leqslant 3$.

Le centre de $SO(3)$ **est trivial.** Soit $h_0 \in Z(SO(3))$. Soit D une droite de $\mathbb{R}^3$ et soit $g \in SO(3)$ une rotation d'axe D. Alors D est une droite propre de g associée à la valeur propre 1.
Comme $h_0 \circ g = g \circ h_0$, on a h_0 stabilise D. Par suite h_0 stabilise toutes les droites de l'espace. Donc $\mathrm{sp}(h_0) \in \{(1,1,1),(1,-1,-1)\}$. Supposons que $\mathrm{sp}(h_0) = (1,-1,-1)$ et soient alors u un vecteur propre pour la valeur propre 1 et v un vecteur propre pour la valeur propre -1. Alors $h_0(u+v) = u - v$. Comme u et v ne sont pas colinéaires, h_0 ne stabilise pas la droite $u + v$. C'est absurde.
Donc $\mathbb{Z}(SO(3)) = \{I_3\}$.

La borne $a < 3$**.**

$$\begin{aligned} a = 3 &\Longrightarrow \forall g \in SO(3) \quad \varphi(g) = \mathrm{Tr}(ghg^{-1}h^{-1}) = 3 \\ &\Longrightarrow \forall g \in SO(3) \quad 1 + 2\cos\theta = 3 \\ &\Longrightarrow \forall g \in SO(3) \quad \theta = 2\pi\mathbb{Z} \\ &\Longrightarrow \forall g \in SO(3) \quad ghg^{-1}h^{-1} = I_3 \\ &\Longrightarrow \forall g \in SO(3) \quad gh = hg \\ &\Longrightarrow h \in Z(SO(3)) = \{I_3\} \end{aligned}$$

C'est absurde. Donc $a < 3$.

Construction d'un retournement. On considère $\theta \;\; / \;\; 1 + 2\cos\theta = a$. On peut supposer $\theta \in [0, \pi]$. De plus l'application cos est décroissante sur $[0, \pi]$, donc :

$$\forall n \in \mathbb{N} \;\; / \;\; 0 < \frac{\pi}{n} < \theta \qquad \text{on a :} \qquad 3 > 1 + 2\cos\left(\frac{\pi}{n}\right) > a.$$

Soit $g_n \in SO(3)$ tel que $\varphi(g_n) = 1 + 2\cos\left(\frac{\pi}{n}\right)$. On définit alors $h_n = [g_n, h]$. C'est donc une rotation d'angle π/n suivant un certain axe. Il s'en suit que h_n^n est une rotation d'angle $n \times \pi/n = \pi$, c'est-à-dire un retournement.

Comme H est distingué et $h \in H$, on a $h_n = \left(g_n h g_n^{-1}\right) h^{-1} \in H$ et donc H contient un retournement.

Les retournements sont conjugués et engendrent $SO(3)$**.** Soit $h \in H$ un retournement et soit D son axe. Soit $k \in SO(3)$ un retournement et soit Δ son axe. On considère g une rotation telle que $g(D) = \Delta$. Alors $ghg^{-1} \in H \lhd SO(3)$ et c'est une rotation d'angle π et d'axe $g(D) = \Delta$ (principe de conjugaison), c'est-à-dire que ghg^{-1} est un retournement d'axe Δ. Donc $ghg^{-1} = k$.
Il s'en suit que H contient tous les retournements. Or $SO(3)$ est engendré par les retournements. Donc $H = SO(3)$. ■

III.B Lemme de Morse (157) (170) (171) (214) (215) (218)

Lemme 43:

Soit $A_0 \in S_n(\mathbb{R}) \bigcap \mathrm{GL}_n(\mathbb{R})$, alors il existe un voisinage V de A_0 dans $S_n(\mathbb{R})$ et une application $\begin{array}{ccc} V & \to & \mathrm{GL}_n(\mathbb{R}) \\ A & \mapsto & M \end{array}$ de classe $\mathcal{C}^1$ telle que pour tout $A \in V$ on ait $A = {}^tMA_0M$.

Démonstration. Soit $\psi : \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \to & S_n(\mathbb{R}) \\ M & \mapsto & {}^tMA_0M \end{array}$. Alors ψ est différentiable en I et

$$\mathrm{d}\psi_I.H = {}^tHA_0 + A_0H = {}^t(A_0H) + A_0H \in S_n(\mathbb{R}).$$

L'application $\mathrm{d}\psi_I$ est une application linéaire et $\mathrm{im}(\mathrm{d}\psi_I) \subset S_n(\mathbb{R})$.
Or son noyau est $\{H \in \mathcal{M}_n(\mathbb{R}) \mid A_0H \in A_n(\mathbb{R})\} = A_0^{-1}A_n(\mathbb{R})$, c'est un espace vectoriel de dimension $n(n-1)/2$. Donc, en vertu du théorème du rang son image est de dimension $n(n+1)/2 = \dim S_n(\mathbb{R})$, et donc $\mathrm{d}\psi(I)$ est surjective dans $S_n(\mathbb{R})$.

On pose alors $\chi = \psi_F$ la restriction de ψ à $F = \{H \in \mathcal{M}_n(\mathbb{R}) \mid A_0H \in S\}$ (c'est un supplémentaire du noyau dans $\mathcal{M}_n(\mathbb{R})$).

Alors χ est injective sur son domaine de définition (par construction) et comme

$$\mathcal{M}_n(\mathbb{R}) = \ker(\mathrm{d}\psi_I) \bigoplus F,$$

on obtient $\mathrm{d}\chi_I$ réalise une bijection de F sur $S_n(\mathbb{R})$, c'est-à-dire $\mathrm{d}\chi_I$ est inversible.

De plus, χ est de classe $\mathcal{C}^1$ (et même de classe $\mathcal{C}^\infty$) comme restriction d'une application de même régularité : en effet ψ est de classe $\mathcal{C}^\infty$ car polynomiale en les coefficients de M.

Par théorème d'inversion locale, on a un voisinage U de I dans F (quitte à restreindre U, on le choisit inclus dans $GL_n(\mathbb{R})$ qui est un ouvert dense contenant I) tel que $\chi : U \to \chi(U) =: V$ réalise un $\mathcal{C}^1$-difféomorphisme de U sur $V = \chi(U)$. De plus V est un voisinage de $\chi(I) = A_0$ dans $S_n(\mathbb{R})$

Ainsi pour tout A dans V, il existe un unique $M \in U$ (inversible) tel que $A = \chi(M) = {}^tMA_0M$ et $A \mapsto M$ est de classe $\mathcal{C}^1$. ■

Lemme 44: Lemme de Morse

Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathcal{C}^3$ sur un ouvert U de $\mathbb{R}^n$ contenant l'origine. On suppose que 0 est un point critique quadratique non dégénéré de f, c'est-à-dire $\mathrm{d}f(0) = 0$ et $\mathrm{d}^2f(0)$ non dégénérée de signature $(p, n-p)$.
Alors il existe un $\mathcal{C}^1$-difféomorphisme $x \mapsto u = \varphi(x)$ entre deux voisinages de l'origine dans $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et

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

Démonstration. On écrit la formule de Taylor avec reste intégral au premier ordre pour f, pour $x \in V_0$ voisinage de 0 :

$$f(x) = f(0) + {}^txQ(x)x,$$

où

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

Alors on a en particulier $Q(0) = \displaystyle\int_0^1 (1-t)\mathrm{d}^2f(0)\mathrm{d}t = \frac{1}{2}\mathrm{d}^2f(0)$ est une forme quadratique non dégénérée.

Par le lemme précédent, on dispose donc de $M(x) \in \mathrm{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ en x telle que pour x voisin de 0, on ait :

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

En posant $y = M(x)x$, il vient :

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

Or la signature de $Q(0)$ est la même que celle de $\mathrm{d}^2 f(0)$: $(p, n-p)$. Donc par changement de base (théorème d'inertie de Sylvester) on dispose de $A \in \mathrm{GL}_n(\mathbb{R})$ telle que

$$Q(0) = {}^tA \begin{pmatrix} I_p & \\ & I_{n-p} \end{pmatrix} A.$$

Finalement, en posant $u = Ay$, on obtient la formule annoncée :

$$f(x) - f(0) = {}^t(Ay)Q(0)(Ay) = u_1^2 + \cdots + u_p^2 - u_{p+1}^2 - \cdots - u_n^2.$$

Il reste donc pour conclure à montrer que $\nu : x \mapsto u = AM(x)x$ est un $\mathcal{C}^1$-difféomorphisme.

On a que ν est de classe $\mathcal{C}^1$ car $x \mapsto M(x)$ l'est et que le produit de matrices et de vecteurs est de classe $\mathcal{C}^\infty$.
De plus $\mathrm{d}\nu_0 : k \mapsto AM(0)k$, c'est-à-dire $\mathrm{d}\nu_0 = AM(0) \in \mathrm{GL}_n(\mathbb{R})$

Par théorème d'inversion locale, on obtient alors que ν réalise un $\mathcal{C}^1$-difféomorphisme entre deux voisinages de l'identité de $\mathbb{R}^n$. ■

Remarque 45

Ce théorème nous dit que pour une forme quadratique non dégénérée, les formes quadratiques assez proche lui sont équivalentes.

III.C Gradient à pas optimal (157) (162) (219) (226) (229) (253)

Proposition 46

Pour tout $x \in \mathbb{R}^n$, on a :

$$\nabla\phi(x) = Ax - b$$

Démonstration. On va calculer la différentielle de ϕ en $x \in \mathbb{R}^n$.

Soit $x \in \mathbb{R}^n$. Pour tout $h \in \mathbb{R}^n$, on a :

$$\begin{aligned}\phi(x+h) &= \frac{1}{2}\langle x+h, x+h\rangle_A - {}^t xb - {}^t hb \\ &= \frac{1}{2}\langle x,x\rangle_A + \frac{1}{2}\langle x,h\rangle_A + \frac{1}{2}\langle h,x\rangle_A + \frac{1}{2}\langle h,h\rangle_A - {}^t xb - {}^t hb \\ &= \frac{1}{2}\|x\| + \langle x,h\rangle_A + \frac{1}{2}\|h\|_A - {}^t xb - {}^t hb \\ &= \phi(x) + \langle x,h\rangle_A - {}^t hb + \underset{\|h\|\to 0}{o}(\|h\|)\end{aligned}$$

On en déduit la différentielle de ϕ en x appliquée à h :

$$d\phi_x(h) = \langle x,h\rangle_A - {}^t hb = \langle Ax,h\rangle - \langle h,b\rangle = \langle Ax-b,h\rangle$$

Or $d\phi_x$ est une forme linéaire continue sur $\mathbb{R}^n$ qui est un espace de Hilbert donc par théorème de représentation de Riesz, le gradient de ϕ en x est défini de manière unique et donc on peut l'identifier très simplement dans l'expression de $d\phi_x(h)$. ■

Lemme 47: Inégalité de Kantorovitch

$$\forall x \in \mathbb{R}^n\backslash\{0\} \qquad \frac{\|x\|^4}{\|x\|_A^2\|x\|_{A^{-1}}^2} \geqslant 4\frac{\lambda_n\lambda_1}{(\lambda_n+\lambda_1)^2}$$

Démonstration. Soit $x \in \mathbb{R}\backslash\{0\}$. Par le théorème spectrale, A est diagonalisable en base orthonormée. Notons $(e_1,\dots,e_n)$ une base de vecteurs propres avec e_i vecteur propre pour λ_i. On a alors que e_i est vecteur propre de A^{-1} pour la valeur propre $\frac{1}{\lambda_i}$. On désigne par x_i la i^e coordonnée de x dans la base $(e_1,\dots,e_n)$. On a donc :

$$\begin{aligned}\|x\|_A\|x\|_{A^{-1}} &= \sqrt{\sum_{i=1}^n \lambda_i x_i^2}\sqrt{\sum_{i=1}^n \frac{1}{\lambda_i}x_i^2} \\ &= \sqrt{\frac{\lambda_n}{\lambda_1}}\sqrt{\sum_{i=1}^n \frac{\lambda_i}{\lambda_n}x_i^2}\sqrt{\sum_{i=1}^n \frac{\lambda_1}{\lambda_i}x_i^2}\end{aligned}$$

Donc en utilisant l'inégalité de Young trivialisée avec $p=q=2$, on a :

$$\|x\|_A\|x\|_{A^{-1}} \leqslant \frac{1}{2}\sqrt{\frac{\lambda_n}{\lambda_1}}\left(\sum_{i=1}^n \frac{\lambda_i}{\lambda_n}x_i^2 + \sum_{i=1}^n \frac{\lambda_1}{\lambda_i}x_i^2\right)$$

C'est-à-dire :

$$\|x\|_A\|x\|_{A^{-1}} \leqslant \frac{1}{2}\sqrt{\frac{\lambda_n}{\lambda_1}}\sum_{i=1}^n\left(\frac{\lambda_i}{\lambda_n}+\frac{\lambda_1}{\lambda_i}\right)x_i^2 \tag{3}$$

Or l'application $g \left\{ \begin{array}{ccc} [\lambda_1, \lambda_n] & \to & \mathbb{R} \\ t & \mapsto & \frac{t}{\lambda_n} + \frac{\lambda_1}{t} \end{array} \right.$ est convexe comme somme de deux applications convexes.
Or on a que :

$$g(\lambda_1) = 1 + \frac{\lambda_1}{\lambda_n} = g(\lambda_n).$$

Donc par convexité de g on obtient :

$$\forall t \in [\lambda_1, \lambda_n] \qquad g(x) \leqslant 1 + \frac{\lambda_1}{\lambda_n}.$$

Et comme toutes les valeurs propres sont dans l'intervalle $[\lambda_1, \lambda_n]$ on a donc :

$$\frac{\lambda_i}{\lambda_n} + \frac{\lambda_1}{\lambda_i} \leqslant 1 + \frac{\lambda_1}{\lambda_n}. \tag{4}$$

En réinjectant l'inégalité (4) dans l'inégalité (3), on obtient finalement :

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

■

Théorème 48: Méthode du gradient à pas optimal

(i) L'application ϕ atteint son minimum en $\bar{x}$ et en $\bar{x}$ seulement.

(ii) Soit $a \in \mathbb{R}^n \backslash \{\bar{x}\}$ et soit $(x_k)_{k\in\mathbb{N}}$ la suite définie par :

$$\left\{ \begin{array}{l} x_0 = a \\ \alpha_k = \left\{ \begin{array}{ll} \dfrac{\|\nabla\phi(x_k)\|^2}{\|\nabla\phi(x_k)\|_A^2} & \text{si } x_k \neq \bar{x} \\ 0 & \text{sinon} \end{array} \right. \\ x_{k+1} = x_k - \alpha_k \nabla\phi(x_k) \end{array} \right.$$

converge vers $\bar{x}$ et

$$\forall k \in \mathbb{N} \qquad \|x_{k+1} - \bar{x}\| \leqslant \sqrt{\frac{\lambda_n}{\lambda_1}} \left(\frac{\lambda_n - \lambda_1}{\lambda_n + \lambda_1}\right)^{k+1} \|x_0 - \bar{x}\|.$$

Cette méthode est appelée méthode du gradient à pas optimal.

Remarque 49

On remarquera que le premier item justifie l'intérêt de considérer le gradient de l'application ϕ. En effet la résolution du système linéaire $Ax = b$ revient à minimiser ϕ (c'est ce premier item qui nous le dit). Or en un point $y \in \mathbb{R}^n$, si $\nabla\phi(y) \neq 0$ alors il indique le sens dans lequel ϕ croit le plus vite.

Étant donné le point x_k, il est donc naturel de chercher le terme x_{k+1} sur la droite affine dirigée par $\nabla\phi(x_k)$ et passant par x_k (on notera que si le gradient est nul alors $x_k = \bar{x_k}$ et on prend alors $x_{k+1} = x_k$). En fait l'application $f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ t & \mapsto & \phi(x_k - t\nabla\phi(x_k)) \end{array}$ atteint son minimum en $\alpha_k = \frac{\|\nabla\phi(x_k)\|^2}{\|\nabla\phi(x_k)\|_A^2}$.

Démonstration de la remarque. On démontre l'assertion

"En fait l'application $f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ t & \mapsto & \phi(x_k - t\nabla\phi(x_k)) \end{array}$ atteint son minimum en $\alpha_k = \frac{\|\nabla\phi(x_k)\|^2}{\|\nabla\phi(x_k)\|_A^2}$."

Soit $t \in \mathbb{R}$ toujours en invoquant la démonstration de la proposition III.C, on a :

$$\begin{aligned} f(t) &= \phi(x_k) - t\langle Ac_k - b, \nabla\phi(x_k)\rangle + \frac{t^2}{2}\|\nabla\phi(x_k)\|_A^2 \\ &= \phi(x_k) - t\|\nabla\phi(x_k)\|^2 + \frac{t^2}{2}\|\nabla\phi(x_k)\|_A^2 \end{aligned}$$

et le résultat provient de l'étude de ce trinôme du degré deux. Ceci explique la définition de x_{k+1}. Enfin, on notera que la dérivée de f s'annule en α_k par minimalité de f. Donc on obtient la relation d'orthogonalité :

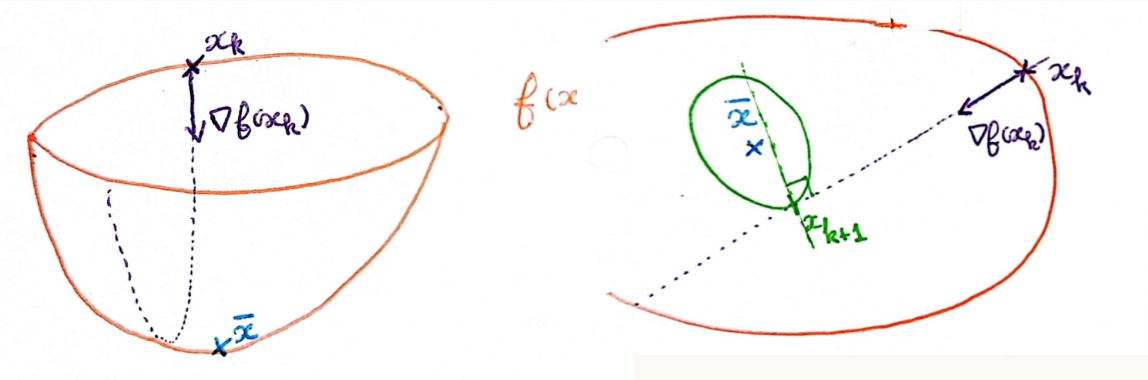
$$\langle \nabla\phi(x_{k+1}), \nabla\phi(x_k)\rangle = 0. \tag{5}$$

■

Remarque 50

On représente ce qu'il se passe géométriquement dans la méthode du gradient à pas optimal :

Et une "vue du-dessus" donne :



La droite (x_k, x_{k+1}) est tangente à la ligne de niveau de ϕ en x_{k+1}.
<u>NB</u> : les lignes de niveau de ϕ sont des sphères pour la norme $\|\cdot\|_A$.

On justifie le choix d'obtenir x_{k+1} à partir de x_k en déplaçant le point dans le sens opposé à celui donné par le gradient car la première manière d'interpréter le gradient est que géométriquement, il donne le sens de plus grande augmentation.

Démonstration du théorème. 1. Pour démontrer ce premier point on convoque directement la démonstration de la proposition III.C. Dans le cas particulier où $x = \bar{x}$, pour $h \neq 0$ on a :

$$\phi(\bar{x} + h) = \phi(\bar{x}) + \frac{1}{2}\|h\|_A^2 > \phi(\bar{x})$$

2. On laisse de côté le cas trivial où pour un entier p on a $x_p = \bar{x}$. Pour alléger les notations, on pose $g_k = \nabla\phi(x_k)$.

   Soit $p \in \mathbb{N}$. On a :

   $$\|x_{p+1} - \bar{x}\|_A = \langle A(x_{p+1} - \bar{x}), x_{p+1} - x_p\rangle + \langle A(x_{p+1} - \bar{x}), x_p - \bar{x}\rangle.$$

   Or $A(x_{p+1} - \bar{x}) = Ax_{p+1} - b = g_{p+1}$ et $x_{p+1} - x_p = -\alpha_p g_p$. Donc en utilisant la relation 5 on obtient :

   $$\langle A(x_{p+1} - \bar{x}), x_{p+1} - x_p\rangle = 0.$$

En utilisant la symétrie de A, il s'en suit :

$$\begin{aligned}\|x_{p+1}-\bar{x}\|_A &= \langle A(x_{p+1}-x_p), x_p-\bar{x}\rangle + \langle A(x_p-\bar{x}), x_p-\bar{x}\rangle \\ &= \langle x_{p+1}-x_p, A(x_p-\bar{x})\rangle + \|x_p-\bar{x}\|_A^2 \\ &= \langle -\alpha_p g_p, g_p\rangle + \|x_p-\bar{x}\|_A^2 \\ &= -\frac{\|g_p\|^4}{\|g_p\|_A^2} + \|x_p-\bar{x}\|_A^2.\end{aligned}$$

Mais par ailleurs

$$\|x_p-\bar{x}\|_A^2 = \langle A(x_p-\bar{x}), x_p-\bar{x}\rangle = \langle A(x_p-\bar{x}), A^{-1}A(x_p-\bar{x})\rangle = \|g_p\|_{A^{-1}}^2$$

et donc

$$\|x_{p+1}-\bar{x}\|_A^2 = \left(1-\frac{\|g_p\|^4}{\|g_p\|_A^2\|g_p\|_{A^{-1}}^2}\right)\|x_p-\bar{x}\|_A^2. \tag{6}$$

L'heure est venu d'utiliser notre lemme technique III.C : l'inégalité de Kantorovitch à $\frac{\|g_p\|^4}{\|g_p\|_A^2\|g_p\|_{A^{-1}}^2}$. On obtient ainsi :

$$\frac{\|g_p\|^4}{\|g_p\|_A^2\|g_p\|_{A^{-1}}^2} \geqslant 4\frac{\lambda_n\lambda_1}{(\lambda_1+\lambda_n)^2}$$

Il en résulte (en utilisant les identités remarquables

$$\left(1-\frac{\|g_p\|^4}{\|g_p\|_A^2\|g_p\|_{A^{-1}}^2}\right) \leqslant \left(1-4\frac{\lambda_n\lambda_1}{(\lambda_1+\lambda_n)^2}\right) = \frac{(\lambda_n-\lambda_1)^2}{(\lambda_n+\lambda_1)^2}$$

En réinjectant dans (6), il vient :

$$\|x_{p+1}-\bar{x}\|_A \leqslant \frac{\lambda_n-\lambda_1}{\lambda_n+\lambda_1}\|x_p-\bar{x}\|_A. \tag{7}$$

et en itérant (7), on a donc :

$$\|x_{p+1}-\bar{x}\|_A \leqslant \left(\frac{\lambda_n-\lambda_1}{\lambda_n+\lambda_1}\right)^{p+1}\|x_0-\bar{x}\|_A.$$

Enfin en utilisant que l'on a $\sqrt{\lambda_1}\|\cdot\| \leqslant \|\cdot\|_A \leqslant \sqrt{\lambda_n}\|\cdot\|$, il vient :

$$\|x_{p+1}-\bar{x}\| \leqslant \sqrt{\frac{\lambda_n}{\lambda_1}}\left(\frac{\lambda_n-\lambda_1}{\lambda_n+\lambda_1}\right)^{p+1}\|x_0-\bar{x}\|.$$

Et cette dernière inégalité assure la convergence géométrique de la suite $(x_k)_k$ vers$\bar{x}$ et conclut ainsi la preuve.

■

III.D Théorème de Perron-Frobenius et application aux chaînes de Markov (153) (206) (226) (261) (262) (264)

Lemme 51:

On a les encadrements suivants pour le rayon spectral de A :

$$\min_{1\leqslant i\leqslant n}\left(\sum_{j=1}^{n}a_{i,j}\right)\leqslant\rho(A)\leqslant\max_{1\leqslant i\leqslant n}\left(\sum_{j=1}^{n}a_{i,j}\right)$$

$$\min_{1\leqslant j\leqslant n}\left(\sum_{i=1}^{n}a_{i,j}\right)\leqslant\rho(A)\leqslant\max_{1\leqslant j\leqslant n}\left(\sum_{i=1}^{n}a_{i,j}\right)$$

De plus, S'il existe $x\in\mathbb{R}^n$ strictement positif et α,β dans $\mathbb{R}_+$ tels que $\alpha x\leqslant Ax\leqslant\beta x$[resp. $\alpha x<Ax<\beta x$], on a alors $\alpha\leqslant\rho(A)\leqslant\beta$ [resp. $\alpha<\rho(A)<\beta$].

Démonstration. Pour le premier point, on peut écrire :
On sait déjà que $\rho(A)\leqslant|||A|||_\infty=\max\limits_{1\leqslant i\leqslant n}\sum\limits_{j=1}^{n}a_{i,j}$. On note $\alpha_i=\sum_{j=1}^{n}a_{i,j}$ pour $1\leqslant i\leqslant n$ et $\alpha=\min\limits_{1\leqslant i\leqslant n}(\alpha_i)$. Pour $\alpha=0$, le résultat est évident. Pour $\alpha>0$, on a $\alpha_i>0$ pour tout i et la matrice $B=\left(\left(\frac{\alpha}{\alpha_i}a_{i,j}\right)\right)_{1\leqslant i,j\leqslant n}$ est telle que $0\leqslant B\leqslant A$, $\sum_{j=1}^{n}b_{i,j}=\alpha$ pour tout i compris entre 1 et n, ce qui nous donne $\alpha=\rho(B)\leqslant\rho(A)$.
En raisonnant avec ${}^tA$, considérant que $\rho({}^tA)=\rho(A)$ et$|||{}^tA|||_\infty=|||A|||_1$, on obtient le deuxième encadrement.

Pour le second point, l'encadrement $\alpha x\leqslant Ax\leqslant\beta x$ équivaut à $\alpha x_i\leqslant(Ax)_i\leqslant\beta x_i$ pour tout i compris entre 1 et n, ce qui entraîne :

$$\alpha\leqslant\min_{1\leqslant i\leqslant n}\frac{(Ax)_i}{x_i}\leqslant\rho(A)\leqslant\max_{1\leqslant i\leqslant n}\frac{(Ax)_i}{x_i}\leqslant\beta.$$

On procède de même pour les inégalités strictes. ■

Lemme 52:

Soient $A\in\mathcal{M}_n(\mathbb{R})$ strictement positive et $x\in\mathbb{C}^n$ un vecteur propre non nul associé à une valeur propre λ telle que $|\lambda|=\rho(A)$. Dans ce cas, $\rho(A)$ est valeur propre de A avec $|x|$ comme vecteur propre associé, ce vecteur étant strictement positif et il existe un réel θ tel que $x=e^{i\theta}|x|$.

Démonstration. On a $\rho(A)>0$ du fait que $A>0$ par le premier point du lemme précédent. De $Ax=\lambda x$ avec $|\lambda|=\rho(A)$, on déduit que $\rho(A)|x|=|Ax|\leqslant|A||x|=A|x|$,donc $y=A|x|-\rho(A)|x|$ est positif. Si ce vecteur est non nul, on a alors $Ay>0$ car A est strictement positive. En effet, pour un certain k on a alors $y_k>0$ et il en résulte alors que pour tout i, comme A est strictement positive et y est positif, on a :

$$(Ax)_i=\sum_{j=1}^{n}a_{i,j}y_j\geqslant a_{i,k}y_k>0.$$

Ceci signifie qu'en notant $x'=A|x|$, on a $\rho(A)x'<Ax'$ avec $x'>0$ (le vecteur x est non nul en temps que vecteur propre) qui entraîne que $\rho(A)<\rho(A)$ par le deuxième point du lemme précédent. C'est impossible. On a donc $y=0$, ou $A|x|=\rho(A)|x|$, ce qui signifie que $\rho(A)$ est valeur propre de A avec $|x|$ comme vecteur propre associé. En écrivant que $|x|=\frac{1}{\rho(A)}A|x|$, on déduit que $|x|>0$. De plus :

$$A|x|=\rho(A)|x|=|\lambda x|=|Ax|,$$

c'est-à-dire :

$$\forall i \in [\![1,n]\!], \qquad \sum_{j=1}^{n} |a_{i,j}x_j| = \left|\sum_{j=1}^{n} a_{i,j}x_j\right|.$$

Il s'agit d'un cas d'égalité dans l'inégalité triangulaire, donc tous les $a_{i,j}x_j$ ont le même argument. Ainsi il existe $\theta \in]-\pi,\pi]$ tel que :

$$\forall k \in [\![1,n]\!] \ \ \forall j \in [\![1,n]\!] \qquad a_{k,j}x_j = e^{i\theta_k}a_{k,j}|x_j|.$$

En simplifiant par $a_{k,j}$ des deux côtés de l'égalité (on peut le faire car $A > 0$), on a :

$$x = e^{i\theta}|x|.$$

■

Théorème 53: Perron-Frobenius

Si $A \in \mathcal{M}_n(\mathbb{R})$ est strictement positive. Alors :

(i) $\rho(A)$ est l'unique valeur propre de A de module maximum ;

(ii) l'espace propre associé à $\rho(A)$ est une droite vectorielle engendrée par un vecteur strictement positif ;

(iii) $\rho(A)$ est valeur propre simple de A.

Démonstration. (i) Si λ est une valeur propre de la matrice A telle que $|\lambda| = \rho(A)$ et si x est un vecteur propre non nul associé, on a alors $x = e^{i\theta}|x|$ avec $A|x| = \rho(A)|x|$. Le rayon spectral $\rho(A)$ est donc valeur propre de A. De plus, avec :

$$\lambda x = Ax = A\left(e^{i\theta}|x|\right) = e^{i\theta}A|x| = e^{i\theta}\rho(A)|x| = \rho(A)x$$

on déduit que $\lambda x = \rho(A)x$ avec $x \neq 0$, et $\lambda = \rho(A)$.

Donc $\rho(A)$ est l'unique valeur propre de A de module maximal.

(ii) En notant $E_{\rho(A)}$ l'espace propre associé à la valeur propre $\rho(A)$, tout vecteur non nul x dans $E_{\rho(A)}$ est tel que $|x| > 0$ par le lemme précédent, et aucune des composantes de x n'est nulle. S'il existe deux vecteurs x, y linéairement indépendants dans $E_{\rho(A)}$, le vecteur $z = x_1y - y_1x$ est alors non nul (linéaire indépendance) et dans $E_{\rho(A)}$ avec $z_1 = 0$, ce qui est exclus. On a donc que x et y sont linéairement dépends. Comme ils sont quelconques dans $E_{\rho(A)}$, on en conclut $\dim\left(E_{\rho(A)}\right) = 1$; et donc $E_{\rho(A)} = \text{Vect}(\,|x|\,)$

(iii) Pour $n = 1$, il est clair que $\rho(A)$ est valeur propre simple de A. On suppose donc que $n \geqslant 2$. Si la multiplicité (algébrique) de $\rho(A)$ comme valeur propre de A est $m \geqslant 2$, alors en se donnant un générateur $x > 0$ de l'espace propre $E_{\rho(A)}$ (de multiplicité géométrique 1), il existe $y \in \mathbb{C}^n$ linéairement indépendant de x tel que $Ay = x + \rho(A)y$ (la matrice A est semblable à une matrice de la forme

$$\begin{pmatrix} \rho(A) & 1 & \\ 0 & \rho(A) & 0 \\ & 0 & B \end{pmatrix}$$

En notant $\overline{y}$ le vecteur conjugué de y dans $\mathbb{C}^n$, on a

$$A\overline{y} = \overline{Ay} = \overline{x + \rho(A)y} = x + \rho(A)\overline{y}$$

puisque A et x sont réels.
Le vecteur $z = \frac{1}{2}(y + \overline{y}) = \Re(y)$ est alors réel et $Az = x + \rho(A)z$.
Comme $x > 0$, il existe un réel $\alpha > 0$ tel que $v = z + \alpha x > 0$. Alors :

$$Av = Az + \alpha Ax = x + \rho(A)z + \alpha\rho(A)x = x + \rho(A)v > \rho(A)v.$$

Ceci nous donne $\rho(A) > \rho(A)$ par le second point du premier lemme technique précédent. C'est impossible. Donc $\rho(A)$ est valeur propre simple de A.

■

Application 54:

Si (X_n) est une chaîne de Markov de matrice de transition ergodique (i.e. $\exists n \in \mathbb{N} \quad P^n > 0$), alors il existe une unique loi invariante :

$$\pi^* = (\pi_1^*, \dots, \pi_N^*)$$

(i.e. $\pi^* P = \pi^*$) et

$$P^n \underset{n\to+\infty}{\longrightarrow} P^\infty = \begin{pmatrix} & \pi^* & \\ & \vdots & \\ & \pi^* & \end{pmatrix}$$

et pour toute mesure de probabilité $\pi^{(0)}$ la suite des itérées $\pi^{(n)} = \pi^{(0)} P^n$ converge vers π^*.

Démonstration. Comme $P^n > 0$ et que $\rho(P) = 1$, il existe une probabilité invariante π pour P^n. Mais π est aussi une probabilité invariante pour tout $k \geqslant n$ puisque

$$P^{n+1} = PP^n = \begin{pmatrix} L_1 \\ \vdots \\ L_N \end{pmatrix} \begin{pmatrix} C_1 & \dots & C_N \end{pmatrix} = (L_i C_j)_{(i,j)\in[\![1,N]\!]^2}$$

et $C_j > 0$ pour tout $j \in [\![1, N]\!]$ et $\sum_j L_{i,j} = 1$ pour tout $i \in [\![1, N]\!]$. Par Perron-Frobenius. L'espace propre de P^n associé à la valeur propre 1 est de dimension 1. Mais $Px = x$ entraîne $P^n x = x$. Donc $E_1(P) \subseteq E_1(P^n)$. De plus, $P\mathbf{1} = \mathbf{1}$. Donc $E_1(P) = E_1(P^n)$.
On écrit alors la décomposition de Jordan de P :

$$P = Q \begin{pmatrix} 1 & & & \\ & J_{\lambda_1} & & \\ & & \ddots & \\ & & & J_{\lambda_r} \end{pmatrix} Q^{-1}$$

avec $|\lambda_i| < 1$ car $\rho(P) = 1$.
Donc on a

$$P^k \longrightarrow P^\infty = Q \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} Q^{-1}.$$

Donc P^∞ est stochastique et de rang 1. Il en résulte que l'on peut écrire :

$$P^\infty = \begin{pmatrix} & \pi^* & \\ & \vdots & \\ & \pi^* & \end{pmatrix}$$

où π^* est une mesure de probabilité.

Ceci équivaut à $P^\infty = \mathbf{1} \cdot \pi^*$. Il s'en suit :

$$\pi^* P^\infty = \pi^* \mathbf{1} \pi^* = \pi^*$$

car $\pi^* \mathbf{1} = \sum_i \pi_i^* = 1$ puisque P^∞ est stochastique.

Mais $P^\infty = PP^\infty$. Donc :

$$\pi^* = \pi^* P^\infty = \pi^* P^\infty P = \pi^* P.$$

D'où, comme la dimension de l'espace propre associé à la valeur propre 1 est 1, π^* est l'unique mesure invariante qui soit une mesure de probabilité.

Enfin, soit $\pi^{(0)}$ une mesure de probabilité quelconque, $\pi^{(n)} = \pi^{(0)} P^n \longrightarrow \pi_0 P^\infty = \pi_0 \mathbf{1} \pi^* = \sum_{j=1}^{N} \pi_j^{(0)} \pi^*$.

Or $\pi^{(0)}$ est une mesure de probabilité. Donc $\sum_{j=1}^{N} \pi_j^{(0)} = 1$ et $\pi^{(n)} \longrightarrow \pi^*$. ■

III.E Disques de Gershgorin (144) (153) (204)

Proposition 55

Si $(P_k)_k$ est une suite de polynômes unitaires de degré n qui converge vers P (dans $\mathbb{C}[X]$), alors, pour la topologie de la norme, et à réarrangement près, les racines de P_k convergent vers les racines de P.

Démonstration. On procède par récurrence pour montrer cette proposition :

— le cas $n = 1$ est immédiat, $P_k = X - \lambda_1^{(k)} \to P = X - \lambda_1$
— supposons la proposition vraie au rang n, montrons la pour le rang $n+1$.
On note $\lambda_1^{(k)} = \text{argmin}_{\lambda \in \text{Rac}(P_k)}(|\lambda_1 - \lambda^{(k)}|)$. Alors :

$$P_k = (X - \lambda_1^{(k)})Q_k(X) \qquad\qquad P = (X - \lambda_1)Q(X)$$

où (Q_k) est une suite de polynômes unitaires de degré n. Montrons que Q_k converge vers Q.
On note $a_m, a_m^{(k)}, b_m, b_m^{(k)}$ les coefficients de P, P_k, Q, Q_k. On a lors les relations suivantes :

$$\begin{aligned} a_m^{(k)} &= b_m^{(k)} - \lambda_1^{(k)} b_m^{(k)} \\ a_m &= b_m - \lambda_1 b_m \end{aligned}$$

Alors une récurrence descendante donne :

$$\begin{aligned} b_m^{(k)} &= a_{m+1}^{(k)} + \lambda_1^{(k)} a_{m+2}^{(k)} + \cdots + \left(\lambda_1^{(k)}\right)^{n-m-1} a_n^{(k)} + \left(\lambda_1^{(k)}\right)^{n-m} \\ b_m &= a_{m+1} + \lambda_1 a_{m+2} + \cdots + \lambda_1^{n-m-1} a_n + \lambda_1^{n-m} \end{aligned}$$

Or on sait que l'on a convergence de la suite $a_m^{(k)}$ vers a_m par convergence de P_k vers P, de plus $\lambda_1^{(k)}$ converge vers λ_1 car

$$|\lambda_1^{(k)} - \lambda_1| \leqslant \prod_{j=1}^{n+1} |\lambda_j^{(k)} - \lambda_1| = |P_k(\lambda_1)| \to |P(\lambda_1)| = 0$$

Donc on obtient finalement la convergence de $b_m^{(k)}$ vers b_m, c'est-à-dire la convergence de Q_k vers Q. Par hypothèse de récurrence, on conclut alors la preuve de cette proposition.

■

Théorème 56:

Soient C_j les composantes connexes de $D(A)$ et soient n_j le nombre de disque de Gershgorin dans C_j. Alors C_j contient exactement n_j valeurs propres de A.

Démonstration. On considère l'application continue :

$$\gamma \begin{array}{ccc} [0,1] & \to & \mathcal{M}_n(\mathbb{C}) \\ t & \mapsto & (a_{i,j}(t)) \end{array} \qquad \text{où} \quad a_{i,j}(t) = \begin{cases} a_{i,i} & \text{si } j = i \\ t a_{i,j} & \text{sinon} \end{cases}$$

Alors

$$\gamma(0) = \begin{pmatrix} a_{1,1} & & \\ & \ddots & \\ & & a_{n,n} \end{pmatrix} \qquad \text{et} \qquad \gamma(1) = A$$

On note $\underline{n} = (n_1, \dots, n_r)$ définis dans le théorème et on défini $\Lambda_n^r = \{\underline{k} \in \mathbb{N}^r \quad / \quad k_1 + \cdots + k_r = n\}$. On définit enfin :

$$\mathcal{E}_{\underline{k}} = \{t \in [0,1] \quad / \quad C_j \text{ contienne exactement } \underline{k}_j \text{ valeurs propres de } \gamma(t)\}.$$

On a alors

$$[0,1] = \bigsqcup_{\underline{k} \in \Lambda_n^r} \mathcal{E}_{\underline{k}}.$$

On va montrer que $\mathcal{E}_{\underline{k}}$ est fermé pour tout $\underline{k}$, et alors par connexité de $[0,1]$ (comme l'union sera une union disjointe de fermé qui partition le connexe $[0,1]$), tous les $\mathcal{E}_{\underline{k}}$ seront vides à l'exception d'un seul : $\mathcal{E}_{\underline{n}} \ni 0$.
Soit $\underline{k} \in \Lambda_n^r$, on démontre la fermeture par caractérisation séquentielle.

Soit $(t_p)_p$ une suite d'éléments de $\mathcal{E}_{\underline{k}}$ qui converge vers $t \in [0,1]$. Montrons que $t \in \mathcal{E}_{\underline{k}}$.
On note $\lambda_1^{(p)}, \dots, \lambda_n^{(p)}$ les valeurs propres de $\gamma(t_p)$ et $\lambda_1, \dots, \lambda_n$ celles de $\gamma(t)$.
Par continuité des valeurs propres (proposition précédentes) et ouverture des composantes connexes (elles sont en nombre fini), on dispose d'un entier N tel que pour tout entier $p \geqslant N$ si $\lambda_l \in C_j$ $\lambda_l^{(p)} \in C_j$. On en déduit ainsi $t \in \mathcal{E}_{\underline{k}}$, et donc $\mathcal{E}_{\underline{k}}$ est fermé.

Au total

$$[0,1] = \mathcal{E}_{\underline{n}}$$

et donc chaque composante connexe de $D(A)$ contient autant de valeurs propres de A que de disques de Gershgorin de A. ■

Références

[1] W. Appel : *Probabilités pour les non probabilistes.* HK, 2e éd édn, 2013.

[2] V. Beck, J. Malick et G. Peyré : *Objectif agrégation.* HK, 2e éd édn, 2005.

[3] L. Bernis et J. Bernis : *Analyse pour l'agrégation de mathématiques.* ellipses, 2024.

[4] P. Caldero et J. Germoni : *Nouvelles histoires hédonistes de groupes et de géométries tome 1.* ellipses, 2 édn, 2017.

[5] P. Caldero et J. Germoni : *Nouvelles histoires hédonistes de groupes et de géométries tome 2.* ellipses, 2e éd édn, 2018.

[6] P. Caldero et M. Peronnier : *Carnet de voyage en algébrie.* Calvage et Mounet, 2022.

[7] S. Francinou, H. Gionella et S. Nicollo : *Oraux X-ENS, algèbre 1.* Cassini, 2e éd édn, 2007.

[8] I. Gozart : *Théorie de Galois.* ellipses, 2e éd édn, 2009.

[9] R. Mansuy et R. Mneimné : *Algèbre linéaire : réduction des endomorphismes.* De Boeck Superieur, 3e éd édn, 2022.

[10] D. Perrin : *Cours d'Algèbre.* ellipses, 1996.

[11] J.-E. Rombaldi : *Analyse matricielle.* EDP sciences, 2e éd édn, 2019.

[12] J.-E. Rombaldi : *Algèbre et géométrie.* De Boeck Superieur, 2e éd édn, 2021.

[13] F. Rouvière : *petit guide de calcul différentiel.* CASSINI, 4 édn, 2014.

[14] P. Samuel : *Théorie algébrique des nombres.* HERMANN, 2 édn, 1971.

[15] M. Zavidovique : *Un max de maths.* Calvage et Mounet, 2013.

[16] C. Zuily et H. Queffelec : *Analyse pour l'agrégation.* Dunod, 5e éd édn, 2020.