AUTOMORPHISMES DE S_n.

Leçons : 101 104 105 108

Références : Perrin p. 31
fGN Alg 1 p. 74.

Théorème

Pour $n \neq 6$, les automorphismes de S_n sont intérieurs.

Résumé

I - LEMME : Si $\varphi \in \mathrm{Aut}\, S_n$ conserve les transpositions, c'est un automorphisme intérieur.

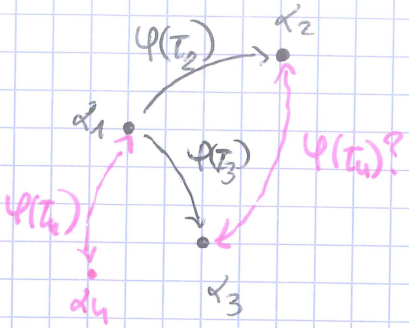
II - Les transpositions sont d'ordre 2. Donc leurs images aussi, comptons le nombre d'éléments qui commutent avec les éléments d'ordre 2.

III - Si $\sigma \in S_n$ commute avec τ, alors $\varphi(\sigma)$ commute aussi avec $\varphi(\tau)$. On a donc égalité des cardinaux des centralisateurs, ce qui permet de conclure.

I] Soit $\varphi \in \mathrm{Aut}\, S_n$ qui envoie les transpositions sur les transpositions.

• Posons $\tau_i = (1\ i)$ pour $i = 2$ à n.
→ ce n'est pas un hasard, les τ_i engendrent S_n !

• Par hypothèse, $\varphi(\tau_2) = (\alpha_1\ \alpha_2)$ est une transposition.
Comme pour $i \neq j$, τ_i et τ_j ne commutent pas, elles ont des supports non disjoints, et $\varphi(\tau_i)$ et $\varphi(\tau_j)$ aussi !
On peut donc supposer $\varphi(\tau_3) = (\alpha_1\ \alpha_3)$.
où $\alpha_2 \neq \alpha_3$ par injectivité de φ.



• Pour τ_4, on a deux possibilités :

* $\varphi(\tau_4) = (\alpha_2\ \alpha_3)$ mais alors

$$\varphi^{-1}((\alpha_1\ \alpha_2)(\alpha_1\ \alpha_3)(\alpha_2\ \alpha_3)) = \begin{cases} (1\,2)(1\,3)(1\,4) \\ \varphi^{-1}(\alpha_1\ \alpha_3) = (1\,3) \end{cases}$$

ce qui est impossible

* $\varphi(\tau_4) = (\alpha_1\ \alpha_4)$ où $\alpha_4 \notin \{\alpha_2, \alpha_3\}$.

• Par suite, et par injectivité de φ, on trouve $\alpha_1, \dots, \alpha_n$ distincts tels que

$$\varphi(\tau_i) = (\alpha_1\ \alpha_i) \qquad i = 2 \text{ à } n.$$

En posant $\alpha = (\alpha_1, \dots, \alpha_n)$ on a alors

$$\alpha\tau_i\alpha^{-1} = (\alpha_1\ \alpha_i) = \varphi(\tau_i)$$

• Donc comme les τ_i engendrent S_n, $\varphi = \sigma \mapsto \alpha\sigma\alpha^{-1}$ est un automorphisme intérieur.

II] • Si τ est une transposition, $\varphi(\tau)$ est d'ordre 2.

→ c'est donc un produit de transpositions disjointes.

• De plus, si σ commute avec τ, $\varphi(\sigma)$ commute avec $\varphi(\tau)$ on a donc l'égalité des cardinaux des centralisateurs :

$$|C(\tau)| = |C(\varphi(\tau))| \text{ pour tout élément de } S_n.$$

• Or $C(\tau)$ est la classe de conjugaison de τ, elle est donc déterminée par la suite $(k_i)_{1 \le i \le n}$ des nombres de cycles de longueur i

• Mais $\sigma\tau\sigma^{-1} = (\sigma(\tau_1), \dots, \sigma(\tau_n))$, donc pour conserver les k_i, il faut : * envoyer les cycles de longueur i sur des cycles de longueur i

* décaler entre 0 et $i-1$ fois les éléments de chaque cycle.

Au total, pour les cycles de longueur i, on a

$(k_i \cdot i) \times ((k_i-1)\cdot i) \times \cdots \times (1 \cdot i)$ possibilités.

Ce qui donne : $|C(\tau)| = \prod_{i=1}^{n} k_i ! \cdot i^{k_i}$

III | • L'égalité $|C(\tau)| = |C(\varphi(\tau))|$ donne alors, dans le cas où :

* τ est une transposition
* $\varphi(\tau)$ une composition de k 2-cycles :

Si $k \geq 2$ $\quad ((n-2)! \cdot 1^{n-2}) \times (1! \times 2^1) = ((n-2k)! \cdot 1^{n-2k}) \cdot (k! \cdot 2^k)$

• On peut le réécrire sous la forme :

$$\frac{(n-2)!}{(n-2k)!} \cdot \frac{1}{k!\,2^{k-1}} = 1$$

ou encore $\binom{n-2}{2k-2} \frac{(2k-2)!}{2^{k-1}\,k!} = \binom{n-2}{2k-2} \frac{(2k-3)(2k-5)\cdots 1}{k} = 1$

• On doit donc avoir $\frac{2k-3}{k} \leq 1$ soit $2k-3 \leq k$ ou $k \leq 3$.

$\Rightarrow$ ainsi $k=2$ ou $k=3$.

* Si $k=2$, l'égalité donne : $\frac{(n-2)(n-3)}{2} = \frac{2\times 2}{2} = 2$

soit $(n-2)(n-3) = 4$ ce qui est impossible

* Si $k=3$, on a $\binom{n-2}{4} = \frac{4 \cdot 3!}{4!} = 1$

donc $4 = n-2$ soit $n=6$

ou $n-2-4 = n-2$ ce qui est impossible.

En conclusion, si $n \neq 6$, alors $k < 2$, et l'égalité est vraie pour $k=1$, donc φ envoie les transpositions sur les transpositions.

$\Rightarrow$ Donc φ est intérieur !

ALGORITHME DE BERLEKAMP

Leçons : 123, 141, 151

Référence Objectif agrégation p. 244.

Algorithme

Soit $P \in \mathbb{F}_q[X]$, avec $q = p^s$ où p premier et $s \in \mathbb{N}^*$.

tel que $P = \prod_{i=1}^{r} P_i$ où les P_i sont irréductibles et distincts

(i.e. P n'a pas de facteur carré)

On peut factoriser P ainsi :

1 - Calcul du nombre d'irréductibles r de P :

$$r = \dim \operatorname{Ker}(S_p - Id)$$

où S_p : $\mathbb{F}_q[X]/\langle P \rangle \longrightarrow \mathbb{F}_q[X]/\langle P \rangle$, $Q(X) \bmod P \longmapsto Q(X^q) \bmod P$. est linéaire (!)

→ Si $r = 1$ on a gagné.

2 - Calcul d'un polynôme V non congru modulo P à un polynôme constant de $\mathbb{F}_q[X]$ et tel que $V \bmod P \in \operatorname{Ker}(S_p - Id)$.

On a alors $P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{PGCD}(P, V - \alpha)$

Et on recommence sur les facteurs non triviaux de ce produit.

Résumé

I - Définition et linéarité de S_p.

II - Calcul de $r = \dim(\operatorname{Ker}(S_p - Id))$.

III - Factorisation de P.

IV - Terminaison de l'algorithme

I | • Posons $\delta_1 : \mathbb{Q}(X) \longrightarrow \mathbb{Q}(X^q)$

C'est l'unique morphisme d'anneau tel que $\delta_1(a) = a$ pour $a \in \mathbb{F}_q$

$\delta_1(X) = X^q$

Mais dans $\mathbb{F}_q$, $a^q = a$, on a donc : $\delta_1(Q) = Q(X^q) = Q^q$.

Posons alors $\pi : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/\langle P \rangle$ la surjection canonique.

on a alors $\pi \circ \delta_1(P) = \pi(P^q) = \pi(P)^q = 0$.

on peut donc passer au quotient et définir :

$$\begin{array}{rccc} \delta_R : & \mathbb{F}_q[X]/\langle P \rangle & \longrightarrow & \mathbb{F}_q[X]/\langle P \rangle \\ & Q \bmod P & \longmapsto & Q(X^q) \bmod P \end{array}$$

et c'est un morphisme d'algèbre qui coïncide avec l'élévation à la puissance q car :

$$\delta_R(\pi(Q)) = \pi \circ \delta_1(Q) = \pi(Q^q) = (\pi(Q))^q.$$

II | • Considérons les $\mathbb{F}_q$-espaces vectoriels $K_i := \mathbb{F}_q[X]/\langle P_i \rangle$, ce sont des corps car les P_i sont irréductibles.

Et le théorème chinois donne l'isomorphisme d'algèbres :

$$\begin{array}{rccc} \varphi : & \mathbb{F}_q[X]/\langle P \rangle & \longrightarrow & K_1 \times \cdots \times K_r \\ & Q \bmod P & \longmapsto & (Q \bmod P_1, \ldots, Q \bmod P_r) \end{array}$$

car les P_i sont premiers deux à deux.

• On peut alors conjuguer S_p par φ : $\tilde{S}_p = \varphi \circ S_p \circ \varphi^{-1}$, et cette application est l'élévation à la puissance q dans $K_1 \times \cdots \times K_r$.

Donc $(x_1, \ldots, x_r) \in \ker(\tilde{S}_p - Id)$ ssi $(x_1^q, \ldots, x_r^q) = (x_1, \ldots, x_r)$

ie $x_i^q = x_i$ dans K_i.

• Mais on remarque que $\mathbb{F}_q \subseteq K_i$, et comme K_i est un corps, le polynôme $X^q - X$ a au plus q racines.

Or les éléments de $\mathbb{F}_q$ sont racines ! Ce sont donc les seules.

Donc $(x_1,\dots,x_r) \in \operatorname{Ker} \widetilde{S_p} - Id$ ssi $x_i \in \mathbb{F}_q$

ie $\operatorname{Ker}(\widetilde{S_p} - Id) = (\mathbb{F}_q)^r$.

- Mais on remarque que $\operatorname{Ker}(\widetilde{S_p} - Id) = \varphi(\operatorname{Ker} S_p - Id)$

donc comme φ est un isomorphisme :

$\dim \operatorname{Ker}(S_p - Id) = \dim \operatorname{Ker}(\widetilde{S_p} - Id) = \dim \mathbb{F}_q^{\,r} = r$.

III | • Supposons $r > 1$.

- Comme l'ensemble des $U \bmod P$ constants est la droite vectorielle engendrée par 1, et que $r > 1$, il existe

$V \bmod P \in \operatorname{Ker}(S_p - Id)$ non constant.

- Mais cela signifie en fait que $\alpha_i := V \bmod P_i \in \mathbb{F}_q \ (\subset K_i)$.

Dès lors, pour $\alpha \in \mathbb{F}_q$,

$\mathrm{PGCD}(P, V-\alpha)$ divise P donc est de la forme $\prod_{i \in I_\alpha} P_i$

où $I_\alpha = \left\{ i \in [\![1,r]\!] \;\middle|\; P_i \mid V-\alpha \right\}$

Or par définition de α_i,

$\alpha_i = \alpha$ ssi $V - \alpha = 0 \bmod P_i$ ssi $P_i \mid V-\alpha$.

C'est-à-dire : $\mathrm{PGCD}(P, V-\alpha) = \prod_{\{i,\, \alpha_i = \alpha\}} P_i$

- On conclut en écrivant :

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

IV | • Finalement, il ne reste plus qu'à s'assurer que l'algorithme termine.

• Comme $V \bmod P$ n'est pas constant, c'est bien une vraie factorisation car il existe alors $\alpha_i \neq \alpha_j$ pour un certain couple (i,j).

En effet, on aurait sinon $V = \alpha \bmod P_i$ pour tout i

donc $V = \alpha \bmod P$.

Remarques

• En pratique, pour calculer $\dim \mathrm{Ker}(Sp - Id)$, on doit calculer la matrice de $Sp - Id$ dans une base, par exemple $(1, x, \dots, x^{\deg P - 1})$ où $x = X \bmod P$, puis calculer son rang par Pivot de Gauss.

• Et pour calculer les PGCD, on utilise l'algorithme d'Euclide.

• On peut se débarasser des facteurs multiples en regardant $\mathrm{PGCD}(P, P')$, mais en caractéristique non nulle ce n'est pas si confortable.

→ si $P \wedge P' = 1$ c'est bon

→ si $P \wedge P' = P$ (ie $P' = 0$ dans $\mathbb{F}_q$), il existe R tel que $P = R^q$ et on applique l'algo à R.

→ sinon, $P_1 = \mathrm{PGCD}(P, P')$ ~~et $P_2 = \mathrm{PGCD}($~~

et $P_2 = P / \mathrm{PGCD}(P, P')$

sont deux facteurs non triviaux de P, et on peut itérer dessus !

apparemment on peut utiliser la décomposition de Frobenius et c'est plus "simple".

THEORÈME DE BRAUER.

Leçons : 101, 105, 108

Références : Objectif agrégation, V. Beck..

Théorème

Soit k un corps de caractéristique nulle

$n \in \mathbb{N}^*$

$\sigma, \tau \in S_n$

Alors σ et τ sont conjuguées si et seulement si P_σ et P_τ sont semblables.

Où, pour $\sigma \in S_n$, $P_\sigma = (\delta_{i,\sigma(j)})_{\substack{1\le i\le n\\ 1\le j\le n}}$.

Résumé

On va montrer que :

$\Rightarrow$ I - Si $\sigma = \gamma^{-1}\tau\gamma$ alors $P_\sigma = P_\gamma^{-1} P_\tau P_\gamma$.

$\Leftarrow$ II - On pose $c_k(\sigma)$ = le nombre de cycles de longueur k dans σ.

LEMME : Alors σ et τ sont conjuguées si et seulement si $(c_k(\sigma))_{1\le k\le n} = (c_k(\tau))_{1\le k\le n}$ (on n'a besoin que de $\Leftarrow$).

III - Si $P_\sigma = \Pi^{-1} P_\tau \Pi$, alors $\chi_{P_\sigma} = \chi_{P_\tau}$, et l'étude des racines PRIMITIVES m-ièmes de l'unité donne $\sum_{m\mid k} c_k(\sigma) = \sum_{m\mid k} c_k(\tau)$ pour tout $m \ge 1$.

IV - L'égalité de III donne $C(\sigma) = C(\tau)$.

I) $\sigma \to P_\sigma$ est un morphisme donc $P_\sigma = P_{\gamma^{-1}\tau\gamma} = P_\gamma^{-1} P_\tau P_\gamma$.

(Car si $u_\sigma \in \mathcal{L}(E)$ et $\mathrm{mat}_{\mathcal{B}_c}(u_\sigma) = P_\sigma$ alors $\mathrm{mat}_{\mathcal{B}_c}(u_\sigma \circ u_\tau) = P_{\sigma\tau}$

car $u_\sigma \circ u_\tau(e_i) = u_\sigma(e_{\tau(i)}) = e_{\sigma\circ\tau(i)} = u_{\sigma\circ\tau}$.)

II] On note $C(\sigma) = (c_k(\sigma))_{1\le k\le n}$.

$\Rightarrow$ • Si $\sigma = \gamma^{-1}\tau\gamma$, on a $\tau = \tau_1 \cdots \tau_r$ où τ_i sont des cycles à supports disjoints.

Dès lors $\sigma = \underbrace{\gamma^{-1}\tau_1\gamma}_{\sigma_1}\underbrace{\gamma^{-1}\tau_2\gamma}_{\sigma_2}\cdots\underbrace{\gamma^{-1}\tau_r\gamma}_{\sigma_r}$

• Les τ_i et σ_i sont des cycles de la même longueur et $C(\sigma) = C(\tau)$.

$\Leftarrow$ • Si $C(\sigma) = C(\tau)$, on a alors une partition $m_1, \dots, m_r$ (de n) associée à σ et τ.

et $\sigma = (i_{1,1}, \dots, i_{1,m_1}) \cdots (i_{r,1}, \dots, i_{r,m_r})$

$\tau = (j_{1,1}, \dots, j_{1,m_1}) \cdots (j_{r,1}, \dots, j_{r,m_r})$

• Posons alors γ la permutation qui envoie $i_{k,p}$ sur $j_{k,p}$.

On a $\gamma\tau\gamma^{-1}(j_{k,p}) = \gamma\tau(i_{k,p}) = \gamma(i_{k,p+1}) = j_{k,p+1}$.

• Donc $\sigma = \gamma\tau\gamma^{-1}$.

III] Supposons que $P_\sigma = M^{-1}P_\tau\Pi$ avec $\Pi \in GL_n(k)$.

(1) • Alors $\chi_{P_\sigma} = \chi_{P_\tau}$.

• Et quitte à changer de bases,

$P_\sigma = \begin{pmatrix} M_{i_1} & & 0 \\ & \ddots & \\ 0 & & \Pi_{i_t} \end{pmatrix}$ où $M_i = \begin{pmatrix} 0 & & 0 & 1 \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{pmatrix} \in \mathcal{M}_i(k)$ est la matrice de permutation d'un cycle.

(et pareil pour P_τ).

Dès lors :

$$\prod_k \underbrace{(X^k-1)}_{\chi_{\Pi_k}}^{c_k(\sigma)} = \prod_k (X^k-1)^{c_k(\tau)} \quad \text{d'après (1)}$$

• Soit alors α une racine PRIMITIVE de l'unité d'ordre m_0.

• Comme k est de caractéristique nulle, les racines de T^k-1 sont simples, et donc la multiplicité d'α dans T^k-1 est 1 si $m \mid k$ et 0 sinon.

• D'où $\sum_{m\mid k} c_k(\sigma) = \sum_{m\mid k} c_k(\tau)$ pour $m \ge 1$ (la somme porte bien sur k !)

IV] • Enfin, s'il existe un entier m tel que $c_m(\sigma) \neq c_m(\tau)$, posons $m_0 = \max\{m \mid c_m(\sigma) \neq c_m(\tau)\}$ (ens. fini !)

Comme les multiples de m_0 sont $\ge m_0$, $\sum_{m_0\mid k} c_k(\sigma) = \sum_{m_0\mid k} c_k(\tau)$ donne une contradiction et $c_{m_0}(\sigma) = c_{m_0}(\tau)$ donc σ et τ sont conjuguées.

THEORÈME DE BURNSIDE

Leçons 104, 106, 157 et éventuellement 152.

Référence FGN Algèbre 2 p. 185

Théorème

Un sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini (ie il existe $N \in \mathbb{N}^*$ tel que pour tout $A \in G$, $A^N = I$) est fini.

Résumé

I - LEMME : Soit $A \in \mathcal{M}_n(\mathbb{C})$, A est nilpotente si et seulement si pour tout $k \in \mathbb{N}^*$, $\mathrm{tr}(A^k) = 0$.

(On n'a besoin que de $\Leftarrow$, et l'autre sens se montre facilement de toute façon).

II - Étude de l'injectivité de $f : A \in G \mapsto (\mathrm{tr}(A\Pi_i))_{1 \le i \le m} \in \mathbb{C}^m$, où les $(\Pi_i)_{1 \le i \le m}$ forment une base de $\mathrm{Vect}(G)$ et conclusion.

I • Supposons que $A \in \mathcal{M}_n(\mathbb{C})$ vérifie $\mathrm{tr}\, A^k = 0$ pour $k \in \mathbb{N}^*$.

• A est trigonalisable car χ_A est scindé sur $\mathbb{C}$.
elle est même semblable à une matrice triangulaire où les coefficients diagonaux sont les valeurs propres $\lambda_0, \dots, \lambda_r$ de A, présentes avec leurs multiplicités $n_0, \dots, n_r$. On supposera que $\lambda_0 = 0$.

• Dès lors, A^k est semblable à une matrice triangulaire supérieure avec les $0, \lambda_1^k, \dots, \lambda_r^k$ sur la diagonale.

• L'hypothèse donne donc $\mathrm{tr}\, A^k = n_1 \lambda_1^k + \dots + n_r \lambda_r^k = 0$.

• ~~Comme les λ_i nuls n'apparaissent pas dans cette équation, supposons les $\lambda_i \neq 0$.~~
(on enlève juste les autres de l'équation)

• On obtient ainsi le système linéaire en $(n_1, \dots, n_r)$:

$$\underbrace{\begin{pmatrix} \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{r-1} \\ \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^{r-1} \\ \vdots & \vdots & & \vdots \\ \lambda_r & \lambda_r^2 & \cdots & \lambda_r^{r-1} \end{pmatrix}}_{A} \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

• Or A est une matrice de Vandermonde, au presque :

$$A = \lambda_1 \cdots \lambda_r \cdot \text{Vandermonde}(\lambda_1, \dots, \lambda_r)$$

• Mais on peut calculer

$$\det V(\lambda_1, \dots, \lambda_r) = \det \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & \lambda_2 - \lambda_1 & \cdots & \lambda_2^{r-1} - \lambda_2^{r-2}\lambda_1 \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_r - \lambda_1 & \cdots & \lambda_r^{r-1} - \lambda_r^{r-2}\lambda_1 \end{pmatrix} \qquad (C_i \leftarrow \lambda_1 C_{i-1})$$

$$= (\lambda_2 - \lambda_1)(\lambda_3 - \lambda_1) \cdots (\lambda_r - \lambda_1) \cdot \det V(\lambda_2, \dots, \lambda_n)$$

$$= \prod_{1 \le i < j \le n} (\lambda_j - \lambda_i)$$

• Pour $\lambda_i \neq 0$ distincts, on a donc un système de Cramer, ce qui impose $n_1 = \cdots = n_r = 0$.

→ les valeurs propres non nulles de A ont donc une "multiplicité nulle", c'est-à-dire qu'il n'y en a pas !

• Autrement dit, $\chi_A = X^n$ annule A donc A est nilpotente.

II • Soit G un sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini.

Posons $(\Pi_i)_{1 \le i \le m}$ une base du sous-espace vectoriel $\text{Vect}(G)$.

Cela permet de définir

$$f : \begin{array}{ccc} G & \longrightarrow & \mathbb{C}^m \\ A & \longmapsto & (\text{tr}(A\Pi_i))_{1 \le i \le m} \end{array}.$$

• Remarquons d'abord que les matrices de G sont annulées par le polynôme $X^N - 1$, scindé à racines simples, et sont donc diagonalisables !

• Montrons maintenant que f est injective !

• Si $f(A) = f(B)$, on a $\mathrm{tr}(A\Pi) = \mathrm{tr}(B\Pi)$ pour tout $\Pi \in G$.

Ainsi, $\mathrm{tr}\left((AB^{-1})^k\right) = \mathrm{tr}\left(\underbrace{AB^{-1}(AB^{-1})^{k-1}}_{\in G}\right)$ pour $k \geq 1$

$= \mathrm{tr}\left(BB^{-1}(AB^{-1})^{k-1}\right)$ par hypothèse

$= \mathrm{tr}\left((AB^{-1})^{k-1}\right)$

$= \mathrm{tr}(I_n) = n$ par récurrence.

Dès lors, calculons

$$\mathrm{tr}\left((AB^{-1} - I_n)^k\right) = \mathrm{tr}\left(\sum_{l=0}^{k} \binom{k}{l} (AB^{-1})^l (-1)^{k-l}\right)$$

$$= n \sum_{l=0}^{k} \binom{k}{l} (-1)^l$$

$$= n \cdot (1-1)^k = 0 \quad \text{par le binôme de Newton.}$$

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

• Mais elle est diagonalisable, donc $AB^{-1} - I_n = 0$ soit $A = B$.

Donc f est bien injective.

• Finalement, remarquons que l'image de f est finie.

En effet, $f(G)$ est inclus dans X^m, où X est l'ensemble des valeurs prises par la trace d'éléments de G.

→ Comme f est injective à valeur dans un ensemble fini, G est fini !

THEORÈME DE CARTAN-DIEUDONNÉ

Leçons 159, 170, 183

Référence Cognet, Algèbre bilinéaire p. 207
Tauvel, Géométrie p. 105

Théorème Cartan-Dieudonné vectoriel.

Soit E un $\mathbb{R}$-ev euclidien
$u \in O(E)$ une isométrie
$F_u = \ker(u - id_E)$ les points fixes de u.
On pose $p_u = n - \dim F_u$
Alors u est un produit de exactement p_u réflexions.

Théorème Cartan-Dieudonné affine.

Si $\mathcal{E}$ est un espace affine de direction E et f une isométrie affine de partie linéaire φ.
Alors
- si f a un point fixe, f est produit de exactement p_φ réflexions
- sinon f est produit de au plus $n+1$ réflexions

I] Cas vectoriel

- si $p_u = 0$: $u = id$ qui est le produit de 0 réflexions.
- si $p_u = k+1 \geq 1$:
  * on montre d'abord que u est le produit d'au plus p_u réflexions.
    - u n'est pas l'identité car $F_u \neq E$.
      donc $F_u^\perp$ n'est pas réduit à 0
      donc il existe $a \in F^\perp$ non nul.
    - on va s'intéresser à l'élément $a - u(a)$ pour exhiber une isométrie sur laquelle on pourra utiliser notre hypothèse de récurrence :
      si $p_f = k$, c'est le produit de k réflexions

- d'abord, remarquons que la réflexion orthogonale $\sigma_{u(a)-a}$ "rajoute" un point fixe à u :

$\bullet\ (u(a)+a,\ u(a)-a) = (u(a),u(a)) - (a,a) + (u(a),a) + (a,u(a)) = 0$

$\bullet$ donc $\sigma(u(a)) = \sigma(u(a)+a + u(a)-a)$

$= \underbrace{u(a)+a}_{\text{invariant}} - \underbrace{u(a)+a}_{\text{réfléchi}}$

$= 2a$

ie $\sigma(u(a)) = a$.

- ensuite, F_u est stable par u

donc $F_u^\perp$ est stable par u car u est une isométrie.

$\to u(a)-a \in F_u^\perp$.

- alors lors, $\mathbb{R}(u(a)-a) \subseteq F_u^\perp$

d'où $F_u \subseteq \mathbb{R}(u(a)-a)^\perp = F_{\sigma_{u(a)-a}}$ par définition !

On a donc montré que :

* $a \in F_{\sigma_{u(a)-a}\circ u}$
* $F_u \subseteq F_{\sigma_{u(a)-a}\circ u}$ (car alors composer par u ne change rien)

En outre :

$p_{\sigma_{u(a)-a}\circ u} = n - \dim F_{\sigma_{u(a)-a}\circ u}$

$\leq n - \dim(F_u \oplus \mathbb{R}a)$

$= p_u - 1 = k$.

Donc par hypothèse, $\sigma_{u(a)-a}\circ u$ est le produit de $p_{\sigma_{u(a)-a}\circ u}$ réflexions, donc en composant par σ à gauche on a :

u est le produit d'au plus $p_u = k+1$ réflexions.

* montrons d'abord que u est composé d'au moins p_u réflexions

- supposons $u = \sigma_{a_1} \circ \cdots \circ \sigma_{a_q}$ est le produit de q réflexions.

- dès lors, $\bigcap_{j=1}^{q} (\mathbb{R}a_j)^\perp \subseteq F_u$ (de dimension $n-k+1$)

mais $\bigcap (\mathbb{R}a_j)^\perp = (\mathrm{Vect}\{a_j\}_j)^\perp$

dont la dimension est au moins $n-q$.

- on a donc

$$\dim F_u = n-k+1 \geqslant \dim \bigcap (\mathbb{R}a_j)^\perp \geqslant n-q$$

ie $q \geqslant k+1$ ce qui prouve le théorème.

II] • Si f a un point fixe O, alors, comme on a par I :

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

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

$$f = \sigma_1 \circ \cdots \circ \sigma_p.$$

• Si f n'a pas de point fixe, on peut lui en créer un en la composant par la symétrie σ par rapport à l'hyperplan médiateur de $[O, f(O)]$ pour un certain $O \in \mathcal{E}$.

On a alors

$$\sigma \circ f(O) = O$$

Donc $\sigma \circ f$ a un point fixe, donc c'est le produit de $p_{\sigma \circ f}$ réflexions, que l'on peut majorer par n, donc f est le produit d'au plus $n+1$ réflexions.

DIMENSION DU COMMUTANT

Leçons : 151, 162

Références : Algèbre 2, Francinou Gianella Nicolas

Théorème

Soit $A \in \mathcal{M}_n(\mathbb{K})$, où $\mathbb{K}$ est un corps quelconque.

On a $\mathbb{K}[A] = \mathcal{C}(A)$ si et seulement si $\chi_A = \mu_A$.

où $\mathcal{C}(A) = \{X \in \mathcal{M}_n(\mathbb{K}) / \ AX = XA\}$

Résumé

I - Montrer que si $\mu_A = \chi_A$, alors $\mathbb{K}[A] = \mathcal{C}(A)$.

II - Montrer que $\dim \mathcal{C}(A) \geq n$.

III - Montrer que si $\mathbb{K}[A] = \mathcal{C}(A)$, alors $\mu_A = \chi_A$.

I] · On suppose que $\chi_A = \mu_A$.

· Il existe alors $x \in \mathbb{K}^n$ tel que $(x, Ax, \dots, A^{n-1}x)$ est une base de $\mathbb{K}^n$.

↳ (*) pas du tout évident, on peut le prouver à la fin s'il reste du temps ?

· On pose alors

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

· f est $\mathbb{K}$-linéaire

* injective car si $f(B) = 0$, alors $BA^k x = A^k Bx = A^k f(B) = 0$.

pour $k \in \mathbb{N}$, ce qui donne $B = 0$.

· On a donc $\dim \mathcal{C}(A) \leqslant \dim \mathbb{K}^n = n$.

· Or, d'une part $\mathbb{K}[A] \subseteq \mathcal{C}(A)$.

d'autre part $\dim \mathbb{K}[A] = \deg \mu_A = \deg \chi_A = n$.

· D'où $n = \dim \mathbb{K}[A] \leqslant \dim \mathcal{C}(A) \leqslant n$.

soit $\mathbb{K}[A] = \mathcal{C}(A)$.

II | Montrons le lemme : $\dim \mathcal{C}(A) \geqslant n$.

· $\mathcal{C}(A)$ est l'ensemble des solutions du système linéaire homogène

(S) $AX - XA = 0$. d'inconnue $X \in \mathcal{M}_n(\mathbb{K})$.

· Quitte à se placer dans une extension $\mathbb{L}$ de $\mathbb{K}$, on peut supposer que A est trigonalisable. Les dimensions des espaces solutions sur $\mathbb{L}$ et sur $\mathbb{K}$ sont encore les mêmes.

On a donc $A = PTP^{-1}$ où $T \in T_n(\mathbb{K})$.

(S) est équivalent à $PTP^{-1}X - XPTP^{-1} = 0$

soit $TP^{-1}XP - P^{-1}XPT = 0$.

On cherche donc une solution $X \in T_n(\mathbb{K})$.

La matrice $TX - XT$ est aussi triangulaire supérieure, on a donc au total $\frac{n(n+1)}{2}$ équations et autant d'inconnues.

Mais sur la diagonale, on a $a_{ii}x_{ii} - x_{ii}a_{ii} = 0$, ce qui est toujours vrai.

· Conclusion : on a $\frac{n(n+1)}{2}$ inconnues

$\frac{n(n+1)}{2} - n$ équations

→ l'espace $\mathcal{C}(A)$ des solutions est de dimension $\geqslant n$.

III · Si on a, de plus, $\mathbb{K}[A] = \mathcal{C}(A)$, alors, comme

$\deg \mu_A = \dim \mathbb{K}[A] \leqslant \deg \chi_A = n \leqslant \dim \mathcal{C}(A)$

On a $\deg \mu_A = n$.

Mais $\mu_A \mid \chi_A$ et ils sont unitaires

Donc $\chi_A = \mu_A$.

THEORÈME DE DIRICHLET FAIBLE.

Leçons : 120, 121, 141

Références : Algèbre 1, S. Francinou, H. Gianella, S. Nicolas p. 435.
(Gozard p. 84)

Théorème

Soit $n \geq 1$, il existe une infinité de nombres premiers de la forme $\lambda n+1$, avec λ entier.

Résumé

- Pour $\Phi_1 = X-1$
  $\Phi_n = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} \left(X - e^{\frac{2ik\pi}{n}}\right)$ les polynômes cyclotomiques.

I - Pour tout $n \in \mathbb{N}^*$, Φ_n est à coefficients entiers.

II - Soit p un nombre premier.
Pour $a \in \mathbb{Z}$, si $p \mid \Phi_n(a)$ mais aucun $\Phi_d(a)$ pour $d \mid n$ strictement, alors $p \equiv 1 \mod n$.

III - Posons $P = \{p \in \mathbb{N}, p \text{ premier et } p \equiv 1 \mod n\}$.
Montrons par l'absurde que P est infini.

I | • Montrons dans un premier temps que, pour $n \geq 1$,

$$X^n - 1 = \prod_{d \mid n} \Phi_d.$$

• On définit : U_n l'ensemble des racines n-ièmes de 1.
P_n l'ensemble des racines n-ièmes primitives de 1.

• On a alors :

* $X^n - 1 = \prod_{\xi \in U_n} (X - \xi)$
* $\Phi_n = \prod_{\xi \in P_n} (X - \xi)$.
* si $\xi \in U_n$, l'ordre d de ξ divise n et $\xi \in P_d$: $U_n = \bigsqcup_{d \mid n} P_d$.

- Des lors, $X^n - 1 = \prod_{d|n} \left(\prod_{\xi \in P_d} (X - \xi) \right) = \prod_{d|n} \Phi_d$.

- On peut alors montrer que $\Phi_n \in \mathbb{Z}[X]$ par récurrence :

  * si $n=1$, $\Phi_1 = X - 1 \in \mathbb{Z}[X]$.

  * si $n \in \mathbb{N}^*$ et $\Phi_k \in \mathbb{Z}[X]$ pour tout $k < n$, alors

$$X^n - 1 = \prod_{d|n} \Phi_d$$

$$\underbrace{X^n - 1}_{\in \mathbb{Z}[X]} = \Phi_n \cdot \underbrace{\prod_{\substack{d|n \\ d \neq n}} \Phi_d}_{\in \mathbb{Z}[X]}$$

donc $\Phi_n \in \mathbb{Z}[X]$, car c'est ~~le quotient de la division euclidienne~~ NON
de $X^n - 1$ par $\prod_{\substack{d|n \\ d \neq n}} \Phi_d$. car les deux autres sont unitaires
et que $X^n - 1 \in \mathbb{Z}[X]$
et $\gamma(PQ) = \gamma(P)\gamma(Q)$
PGCD des coeff.

II] - Soit p premier vérifiant $p \mid \Phi_n(a)$ mais pas $\Phi_d(a)$ $(d|n, d \neq n)$.

- On sait que $p \mid \Phi_n(a)$ et $\Phi_n \mid X^n - 1$.
Donc $p \mid a^n - 1$, et dans $\mathbb{Z}/p\mathbb{Z}^*$, l'ordre (multiplicatif !) de $\bar{a}$ divise donc n.

- Cet ordre est exactement n car :

  * si $d|n$, $d \neq n$, alors $\bar{a}^d - 1 = \prod_{d'|d} \overline{\Phi_{d'}(a)}$

  * et si $d' \mid d$, alors $d' \mid n$.

  * comme $\overline{\Phi_{d'}(a)} \neq 0$ par hypothèse, $\bar{a}^d - 1 \neq 0$.

  → l'ordre de $\bar{a}$ est donc n.

- Le théorème de Lagrange donne alors : $\text{ordre}(\bar{a}) \mid p - 1$.
ie. $p = \lambda n + 1$ pour un certain λ entier

III] • Supposons $\mathcal{P} = \{p_1, \dots, p_q\}$ fini.

• On cherche alors p premier vérifiant les hypothèses de II et n'appartenant pas à $\mathcal{P}$.

• Pour s'assurer que $p \notin \mathcal{P}$, on va changer n en $N = n p_1 p_2 \cdots p_q$.
→ dès lors, si $p \equiv 1 \bmod N$, $p \equiv 1 \bmod n$ et $p \notin \mathcal{P}$.

• Il s'agit donc de trouver $a \in \mathbb{Z}$ et p premier tels que :
$$p \mid \Phi_N(a) \quad \text{et ne divise pas} \quad B(a) = \prod_{\substack{d \mid N \\ d < N}} \Phi_d(a).$$

• B et Φ_N n'ont aucune racine en commun donc $B \wedge \Phi_N = 1$ sur $\mathbb{C}[X]$ et d'après le théorème de Bezout, il existe $U, V \in \mathbb{Q}[X]$ tels que :
$$U\Phi_N + VB = 1$$

on passe de $\mathbb{Z}[X]$ à $\mathbb{Q}[X]$ car $B, \Phi_N \in \mathbb{Q}[X]$ et que le pgcd est invariant par extension de corps (égalité de la div. euclid.) (par unicité de la division euclidienne !)

• On choisit alors ensuite $a \in \mathbb{Z}$ tel que :

i - $aU, aV \in \mathbb{Z}[X]$ (possible car ppcm(coeff(U,V)) marche).

ii - $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$ (possible car Φ_N non constant)

On a donc

(*) $\quad a = U'(a)\Phi_N(a) + V'(a)B(a) \quad$ où $U', V' = aU, aV$.

• Cherchons maintenant p : soit $p \mid \Phi_N(a)$ premier.
Alors $p \mid a^N - 1$ car $\Phi_N \mid X^N - 1$, donc $\bar{a}^N = 1$.
→ a est donc inversible dans $\mathbb{Z}/p\mathbb{Z}$, d'où $a \wedge p = 1$.

• Donc p ne divise pas $B(a)$, car si non, il diviserait a d'après (*).

• En résumé : $\left.\begin{array}{l} p \mid \Phi_N(a) \\ p \nmid \Phi_d(a) \text{ pour } d \mid n,\ d \neq n \\ p \notin \mathcal{P} \end{array}\right\}$ $p \in P$

⇒ absurde, donc $\mathcal{P}$ est infini.

DUNFORD ET L'EXPONENTIELLE DE MATRICES

Leçons 153, 156, 157.

Référence Gourdon p. 194-196.

Théorème

Soit $f \in \mathcal{L}(E)$ tel que χ_f est scindé sur $\mathbb{K}$.

Il existe un unique couple $(d,n) \in \mathcal{L}(E)$ tels que

(i) d est diagonalisable, n est nilpotente.

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

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

Enfin, cette décomposition permet de calculer l'exponentielle d'un endomorphisme !

Résumé

I – Soit $F = \beta \Pi_1^{\alpha_1} \cdots \Pi_s^{\alpha_s}$ un polynôme annulateur de f. (irréductibles !)

Posons $N_i = \ker \Pi_i^{\alpha_i}$, alors $E = \bigoplus N_i$ et la projection sur N_i par rapport à $\bigoplus N_{j \neq i}$ est un polynôme en f.

II – Preuve de Dunford et calcul pratique de la décomposition

III – Calcul de l'exponentielle de f.

I • Posons $Q_i = \prod_{j \neq i} \Pi_j^{\alpha_j}$.

Aucun facteur n'est commun à tous les Q_i, le théorème de Bezout donne alors $U_1, \dots, U_s \in \mathbb{K}[X]$ tels que

$$1 = U_1 Q_1 + \cdots + U_s Q_s$$

ie $$Id = U_1(f) \circ Q_1(f) + \cdots + U_s(f) \circ Q_s(f).$$

Posons alors $p_i = \mu_i(f) \circ Q_i(f)$.

On a

$$p_i \circ p_j = \begin{cases} Q_i Q_j(f) \circ \mu_i \mu_j(f) = 0 & \text{si } i \neq j \\ \sum_{k=1}^{s} p_i \circ p_k = p_i \circ id = p_i & \text{si } i = j. \end{cases}$$

Donc les p_i sont bien des projecteurs !

- D'une part, on a $\operatorname{Im} p_i = N_i$

  $\subseteq$ car si $y = p_i(x) \in \operatorname{Im} p_i$, on a :

  $$\Pi_i^{\alpha_i}(f)(y) = \Pi_i^{\alpha_i}(f) \circ Q_i(f) \circ \mu_i(f) = 0$$

  $\supseteq$ car si $x \in \operatorname{Ker} \Pi_i^{\alpha_i}$, on a

  $$x = p_1(x) + \dots + p_s(x) = p_i(x) \in \operatorname{Im} p_i.$$

  on a en effet $p_j(x) = \mu_j(f) \circ Q_j(f)(x) = 0$ car $\Pi_i^{\alpha_i} \mid Q_j$ pour $i \neq j$.

- D'autre part, on a $\operatorname{Ker} p_i = \bigoplus_{j \neq i} N_j$

  $\subseteq$ car si $x \in \operatorname{Ker} p_i$, $x = \sum_{j \neq i} p_j(x) \in \bigoplus_{j \neq i} N_j$.

  $\supseteq$ car si $x \in N_j$ $(j \neq i)$, $p_i(x) = \mu_i(f) \circ Q_i(f)(x) = 0$

On a donc bien prouvé notre lemme, passons à Dunford.

II • Construisons d_i pour $\chi_f = (-1)^s \prod_{i=1}^{s} (X - \lambda_i)^{\alpha_i}$ et avec les notations du lemme, on peut poser

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

→ d est diagonalisable (par le lemme des noyaux par exemple)

→ n est nilpotente car pour $q \in \mathbb{N}^*$,

$$n^q = \left(\sum_{i=1}^{s} (f - \lambda \mathrm{Id}) p_i \right)^q = \sum (f - \lambda \mathrm{Id})^q p_i$$

car $p_i p_j = 0$ si $i \neq j$, $p_i^2 = p_i$, et p_i commute avec f.

- L'unicité vient du fait que si (d,n) et (d',n') sont deux décompositions, d et d' commutent (polynômes en f) donc sont diagonalisables simultanément donc $d-d' = n'-n$ est diagonalisable ~~donc~~ et nilpotente
  → donc nulle ! d'où l'unicité.

- Un mot sur comment trouver les u_i ?
  La décomposition en éléments simples de $1/\chi_f$ s'écrit :

$$1/\chi_f = \sum_{i=1}^{s} \sum_{j=1}^{\alpha_i} \frac{x_{ij}}{(X-\lambda_i)^j}$$

En posant $u_i = \sum_{j=1}^{\alpha_i} x_{ij}(X-\lambda_i)^{\alpha_i - j}$, on a :

$$1/\chi_f = \sum_{i=1}^{s} \frac{u_i}{(X-\lambda_i)^{\alpha_i}}$$

d'où $1 = \sum_{i=1}^{s} u_i Q_i$ ce qui donne les p_i.

On est maintenant prêt·es pour calculer (enfin !) $\exp f$:

III | • On a $f = d+n$ où d et n commutent, d'où

$$\exp(d+n) = \exp(d)\exp(n).$$

On calcule alors :

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

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

Soit, en combinant les deux,

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

Point fixe de Kakutani et sous-groupes compacts de $GL(E)$

Leçons 106, 803, 208, 170

Référence Thèmes de géométrie, Alessandri.

Théorème

Soit E un $\mathbb{R}$-espace vectoriel normé

G un sous-groupe compact de $GL(E)$.

Posons K un compact convexe non vide tel que

$\forall u \in G,\ u(K) \subseteq K$.

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

Corollaire

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

Résumé

I - Un théorème de point fixe linéaire : si $u(K) \subseteq K$, et $u \in \mathcal{L}(E)$, alors u a un point fixe.

II - Définition d'une norme invariante par composition par les éléments de G et construction d'un élément point fixe de tout sous ensemble fini de G.

III - Application aux sous-groupes compacts de $GL_n(\mathbb{R})$

I • Soit $x_0 \in K$, posons $x_{n+1} = \frac{1}{n+1} \sum_{i=0}^{n} u^i(x_0)$.

• Comme K est compact, pour $i \in \mathbb{N}$, $u^i(x_0) \in K$.

Donc par convexité de K, $x_n \in K$ pour tout $n \geq 0$.

• Il existe donc une sous-suite $(x_{\varphi(n)})_{n\in\mathbb{N}}$ qui converge vers $x \in K$.

Et on a, de plus, pour une norme quelconque de E :

$$\|u(x_{\varphi(n)}) - x_{\varphi(n)}\| = \left\| \sum_{i=0}^{\varphi(n)-1} \frac{1}{\varphi(n)} (u^{i+1}(x_0) - u^i(x_0)) \right\|$$

$$= \frac{1}{\varphi(n)} \|u^{\varphi(n)}(x_0) - x_0\|$$

$$\leqslant \frac{M}{\varphi(n)} \xrightarrow{n\to\infty} 0 \quad \text{car } \varphi(n) \xrightarrow{n\to\infty} +\infty.$$

car K est un compact de $\mathbb{R}^n$ et est donc borné par un certain M.

Donc $\|u(x_{\varphi(n)}) - x_{\varphi(n)}\| \xrightarrow{n\to\infty} 0$.

Or par continuité de la norme et par continuité de u :

$$\|u(x_{\varphi(n)}) - x_{\varphi(n)}\| \longrightarrow \|u(x) - x\|$$

D'où $u(x) = x$: on a bien trouvé un point fixe.

II • On va choisir une norme agréable :

$$N(x) = \max_{u\in G} \|u(x)\|. \quad \text{bien défini par compacité de } G.$$

• C'est bien une norme car :

* si $N(x) = 0$, comme $id \in G$, $\|id(x)\| = \|x\| = 0$ donc $x = 0$.
* si $\lambda \in \mathbb{R}$, $N(\lambda x) = \max \|u(\lambda x)\|$

$$= \max |\lambda| \|u(x)\|$$

$$= |\lambda| N(x)$$

* si $x, y \in E$, $N(x+y) = \max \|u(x) + u(y)\|$

$$\leqslant \max \|u(x)\| + \|u(y)\|$$

$$\leqslant \max \|u(x)\| + \max \|u(y)\|$$

$$= N(x) + N(y)$$

avec égalité s'il existe $u \in G$ tel que $\|u(x+y)\| = \|u(x)\| + \|u(y)\|$

ie $u(x) = \lambda u(y)$ $(\lambda > 0)$ donc $x = \lambda y$ par inversibilité de u.

• Posons ensuite $\mathrm{Fix}(u) = \{x \in K \mid u(x) = x\}$ les points fixes de u sur K.
On cherche un élément dans $\bigcap_{u \in G} \mathrm{Fix}(u)$.

Comme $\mathrm{Fix}(u)$ est fermé dans K, il suffit de trouver un élément dans une union finie de la forme $\bigcap_{i=1}^{n} \mathrm{Fix}(u_i)$ avec $u_i \in G$.

• Posons comme toute à l'heure : $u = \frac{1}{n} \sum_{i=1}^{n} u_i$.

Par convexité de K, $u(K) \subseteq K$.

Et comme u est linéaire, le lemme donne un point $x \in K$ tel que

$$x = u(x) = \frac{1}{n} \sum_{i=1}^{n} u_i(x).$$

Et c'est là toute la magie de notre norme :

$$\begin{aligned} N(x) &= N(u(x)) \\ &\leq \frac{1}{n} \sum_{i=1}^{n} N(u_i(x)) \\ &= N(x) \end{aligned}$$

Par le cas d'égalité de l'inégalité triangulaire, les $u_i(x)$ sont donc positivement liés.

$\longrightarrow$ l'égalité des normes donne dès lors $x = u(x) = \frac{1}{n} \sum u_i(x) = u_i(x)$

donc $\bigcap_{i=1}^{n} \mathrm{Fix}(u_i) \neq \emptyset$.

III • Posons $\rho : G \longrightarrow GL(S_n(\mathbb{R}))$

$$A \longmapsto (S \longmapsto ASA^t)$$

où S est la forme quadratique associée à un espace quadratique euclidien $(\mathbb{R}^n, S)$.

ρ définit un morphisme de groupe car

$$\rho(A)(\rho(B)S) = A(BSB^t)A^t = (AB)S(AB)^t = \rho(AB)S.$$

et induit donc une action de G sur $S_n(\mathbb{R})$.

Posons $X = \{ A^t A = \rho(A) I_n \mid A \in G \}$ l'orbite de I_n pour cette action

et $K = \text{conv}(X)$ son enveloppe convexe.

* $X \subseteq S_n^{++}(\mathbb{R})$
* X est compact (par continuité)
* $K \subseteq S_n^{++}(\mathbb{R})$ par convexité de $S_n^{++}(\mathbb{R})$
* K est donc convexe et compact (car enveloppe convexe d'un compact)

Ainsi

Donc par le théorème de Kakutani, il existe $S \in K \subseteq S_n^{++}(\mathbb{R})$

un point fixe de tous les éléments de $\rho(G)$.

Commentons le fait que $S \in S_n^{++}(\mathbb{R})$:

* c'est la matrice d'une forme quadratique définie positive qui

induit une norme $\|\cdot\|_S : x \mapsto {}^t x S x$

dès lors si $A \in G$, $\|Ax\|_S = {}^t x {}^t A S A x = {}^t x {}^t(A {}^t A) x = {}^t x S x = \|x\|_S$

ie G est un sous groupe des isométries de $\mathbb{E}$ pour $\|\cdot\|_S$.

* on peut écrire carrément $S = R^2$ car $S \in S_n^{++}(\mathbb{R})$

et si $A \in G$, $AR^2 {}^t A = R^2$ donc $(R^{-1}AR)(R {}^t A R^{-1}) = I_n$

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

donc $R^{-1}AR \in O_n(\mathbb{R})$

donc G est un sous-groupe de $RO_n(\mathbb{R})R^{-1}$.

Nombre de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$.

Leçons 101, 123, 153, 190

Références H_2G_2 tome 1 p. 264-265 (p. 120 pour I).

FGN Alg 1 (1.10?)

En fait voir plutôt NH_2G_2, tome 2 p. 66.

Théorème

Le nombre de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$ est

$$\sum_{n_1+\dots+n_q=n} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|}$$

Résumé

I - $A \in \mathcal{M}_n(\mathbb{F}_q)$ est diagonalisable si et seulement si $A^q = A$.

II - On construit une bijection entre

$\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables

et $S = \left\{ (E_\xi, \xi \in \mathbb{F}_q) \mid E = \bigoplus_{\xi \in \mathbb{F}_q} E_\xi \right\}$ (avec éventuellement des $E_\xi = \{0\}$)

III - La formule des classes pour l'action naturelle de $GL_n(\mathbb{F}_q)$ sur S permet alors de conclure.

I • Si $A^q - A = 0$, $X^q - X$ annule A et est scindé à racines simples sur $\mathbb{F}_q$. En effet, pour tout $\xi \in \mathbb{F}_q$, $\xi^q = \xi$ est racine de $X^q - X$, on a donc q racines pour un polynôme de degré q.

Donc A est diagonalisable.

• Si A est diagonalisable, elle est semblable à $\mathrm{diag}(\xi_1, \dots, \xi_n)$.

Dès lors A^q est semblable dans la même base à $\mathrm{diag}(\xi_1^q, \dots, \xi_n^q) = \mathrm{diag}(\xi_i)$

D'où $A^q = A$.

II • Posons Φ : $\mathcal{M}(E) \longrightarrow S$

$A \longmapsto (\mathrm{Ker}(A-\zeta_1 I_n), \dots, \mathrm{Ker}(A-\zeta_q I_n))$

où l'on a écrit $\mathbb{F}_q = \{\zeta_1, \dots, \zeta_q\}$.

• D'après le lemme des noyaux, $\mathbb{F}_q^n = \bigoplus_{i=1}^{q} \mathrm{Ker}(A-\zeta_i I_n)$ (quitte à enlever les ensembles réduits à zéro).

→ donc d'une part, Φ est injective car la donnée des sous espaces propres de $A \in \mathcal{M}(E)$ la détermine.

→ d'autre part, Φ est surjective car si $E = \bigoplus E_i$, l'endomorphisme défini par $f : x \mapsto \zeta_i x$ pour $x \in E_i$ est bien défini et est diagonalisable.

III • $GL_n(\mathbb{F}_q)$ agit naturellement sur S en posant

$u \cdot (E_1, \dots, E_q) = (u(E_1), \dots, u(E_q))$. pour $u \in GL_n(\mathbb{F}_q)$, $E = \bigoplus E_i$.

La formule des classes s'écrit alors

$$|S| = \sum_{x \in S/GL(\mathbb{F}_q^n)} |Orb_x| = \sum_{x \in S/GL(\mathbb{F}_q^n)} \frac{|GL(\mathbb{F}_q^n)|}{|Stab_x|}.$$

• Regardons d'abord l'orbite de $(E_1, \dots, E_q) \in S$:

→ si $u \in GL(\mathbb{F}_q^n)$, on a bien $\dim u(E_i) = \dim E_i$.

→ si $(F_1, \dots, F_q) \in S$ $\dim E_i = \dim F_i$, on peut prendre $(e_i)_i$ et $(f_i)_i$ des bases compatibles avec les décompositions de E.

Dès lors $u : e_i \mapsto f_i$ définit un endomorphisme (linéaire) qui envoie une base sur une base et est donc bijectif.

→ Les orbites de cette action sont donc déterminées par n_i tq $n_1 + \dots + n_q = n$.

- Pour dénombrer Racine des orbites, regardons le stabilisateur d'un élément $(E_1, \dots, E_q)$ de E donné.

On remarque que $u \in GL(E)$ stabilise $(E_1, \dots, E_q)$ si et seulement si $u(E_i) = E_i$.

La matrice de u dans une base compatible est donc de la forme

$$\operatorname{diag}(A_1, \dots, A_q)$$

où A_i est la matrice de u restreint à E_i.

Comme u est inversible, A_i est inversible.

On en déduit que $|\operatorname{Stab}(E_1, \dots, E_q)| = \prod_{i=1}^{q} |GL_{m_i}(\mathbb{F}_q)|$ où $m_i = \dim E_i$.

- En résumé, on a donc :

$$|\Omega(E)| = |S| = \sum_{m_1 + \dots + m_p = n} |\operatorname{Orb}(m_1, \dots, m_q)|$$

$$= \sum_{m_1 + \dots + m_p = n} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|}$$

Suite de Polygones.

Leçons : 152, 182

Références : Algèbre, X. Gourdon p. 183.

Théorème (déterminant circulaire)

- Soit $A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & \vdots \\ a_2 & \cdots & a_n & a_1 \end{pmatrix}$ et $J = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 1 & & & 0 \end{pmatrix}$

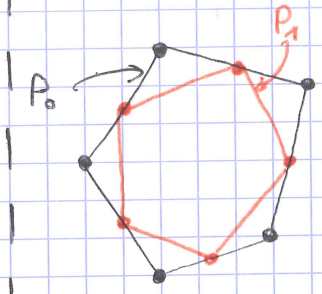
Le déterminant de A est $\prod_{j=0}^{n-1} P(\omega^j)$

où $P = a_n X^{n-1} + \dots + a_2 X + a_1$ et $\omega = e^{\frac{2i\pi}{n}}$.

Application

- Posons la suite $(P_k)_{k\in\mathbb{N}} \in \left(\mathbb{C}^{\mathbb{Z}/n\mathbb{Z}}\right)^{\mathbb{N}}$ de polygones telle que :

$P_0 \in \mathbb{C}^{\mathbb{Z}/n\mathbb{Z}}$ et $P_{k+1,i} = \frac{P_{k,i} + P_{k,i+1}}{2}$ pour $k \geq 0$, $i \in \mathbb{Z}/n\mathbb{Z}$.



- Alors P_n converge vers le point $g = \frac{1}{n} \sum_{i \in \mathbb{Z}/n\mathbb{Z}} P_{0,i}$ l'isobarycentre des P_0.

Résumé

I – Diagonaliser A en l'exprimant comme $A = P(J)$.

II – Exprimer $\det(A)$

III – Exprimer la relation entre P_k et P_{k+1} sous forme matricielle.

IV – Ecrire cette matrice comme un polynôme en J et en déduire son polynôme caractéristique et ses valeurs propres.

V – En déduire la convergence de $(P_k)_{k\in\mathbb{N}}$.

Thm **I** • Remarquons qu'itérer J décale la diagonale :

$$J^k = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 1 & \ddots & & \ddots & \ddots & & \vdots \\ 0 & & \ddots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & & \ddots & 1 \\ 0 & & & & \ddots & & 0 \\ & \ddots & & & & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \quad (1 \text{ en } k\text{-ième ligne}) = \begin{pmatrix} 0 & I_{n-k} \\ I_k & 0 \end{pmatrix}$$

• On a donc, pour $P = a_n X^{n-1} + \dots + a_2 X + a_1$:

$$P(J) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ & \ddots & \ddots & a_2 \\ & & \ddots & \vdots \\ a_2 & \cdots & & a_1 \end{pmatrix} = A.$$

• Mais on a aussi $J^n = I_n$ donc $\chi_J = X^n - 1$ est scindé à racines simples, et ses racines sont $1, \omega, \dots, \omega^{n-1}$ où $\omega = e^{\frac{2i\pi}{n}}$.

• Donc J se diagonalise en $\Omega = \mathrm{diag}(1, \omega, \dots, \omega^{n-1})$, soit $P(J)$ se diagonalise en $P(\Omega) = \mathrm{diag}(P(1), \dots, P(\omega^{n-1}))$

II • D'où $\det A = \det P(J) = \prod_{j=0}^{n-1} P(\omega^j)$.

App **III** • Revenons à nos polygones, on va écrire $P_k = \begin{pmatrix} P_{k,1} \\ \vdots \\ P_{k,n} \end{pmatrix}$.

On a alors, pour $k \geq 0$:

$$P_{k+1} = A P_k, \text{ avec } A = \begin{pmatrix} 1/2 & 1/2 & 0 & \cdots & 0 \\ 0 & 1/2 & 1/2 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1/2 & 0 & \cdots & 0 & 1/2 \end{pmatrix} = \frac{1}{2}(I_n + J).$$

IV • Intéressons nous à χ_A.

$$\chi_A = \det(XI_n - A) = \det\left(\left(X - \frac{1}{2}\right) I_n - \frac{1}{2} J\right).$$

$\to \left(X - \frac{1}{2}\right) I_n - \frac{1}{2} J$ est un polynôme en J, donc d'après **II** :

(X) $$\chi_A = \prod_{j=0}^{n-1} \left(X - \frac{1+\omega^j}{2}\right).$$

• χ_A est scindé à racines simples, on peut donc diagonaliser A :

$$A = P\, \mathrm{diag}\left(1, \frac{1+\omega}{2}, \dots, \frac{1+\omega^{n-1}}{2}\right) P^{-1} \text{ où } P \in GL_n(\mathbb{C}).$$

quelle topologie ??

V] • On a donc, par continuité du produit matriciel :

$$A^k \longrightarrow B = P\,\mathrm{diag}(1,0,\dots,0)\,P^{-1}.$$

• Pour g, on a le vecteur $\frac{1}{n}\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}$ correspondant, invariant par A.

Donc $X = \begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}$ donne $AX = X$

et $BX = X$ par continuité.

Et comme $X \in \operatorname{Im} B$ de dimension 1,

$$B = (b_1 X, \dots, b_n X) \text{ où } b_i \in \mathbb{C}.$$

• Remarquons enfin que l'isobarycentre est préservé par A car :

$$\frac{1}{n}\sum_{i\in\mathbb{Z}/n\mathbb{Z}} \frac{1}{2}(P_i + P_{i+1}) = \frac{1}{2}\left(\frac{1}{n}\sum_{i\in\mathbb{Z}/n\mathbb{Z}} P_i + \underbrace{\frac{1}{n}\sum_{i\in\mathbb{Z}/n\mathbb{Z}} P_{i+1}}_{= \frac{1}{n}\sum_{i\in\mathbb{Z}/n\mathbb{Z}} P_i}\right).$$

... donc B le préserve également !.

• En somme : $P_k \xrightarrow{k\to+\infty} BP_0 = \left(\sum b_i P_{0,i}, \dots, \sum b_i P_{0,i}\right)$

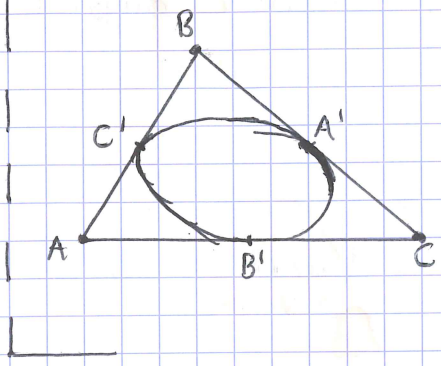
donc $b_i = 1/n$ et $P_k \xrightarrow{k\to+\infty} (g,\dots,g)$.

ELLIPSES DE STEINER

Leçons 182, 183

Référence NH2G2 tome 2 p. 180 pour l'existence
p. 202 pour l'unicité.

Théorème



- Soit ABC un triangle du plan.

I| Il existe une ellipse ~~A~~tangente aux milieux des côtés de ABC.

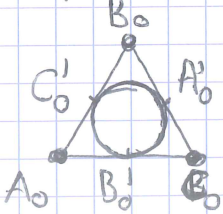
II| Cette ellipse est unique.

□| Petites remarques sur le groupe affine $GA_2(\mathbb{R})$:

- les éléments $g \in GA_2(\mathbb{R})$ préservent les barycentres :
si $\sum_{i=1}^{n} a_i \overrightarrow{GA_i} = \vec{0}$ alors $\vec{g}\left(\sum_{i=1}^{n} a_i \overrightarrow{GA_i}\right) = \sum_{i=1}^{n} a_i \overrightarrow{g(G)g(A_i)}$
$= \vec{g}(\vec{0})$
$= \vec{0}$

- $GA_2(\mathbb{R})$ agit simplement et transitivement sur les repères de $\mathbb{A}^2$:
en effet, prenons (O,I,J) et (O',I',J') deux repères de $\mathbb{A}^2$,
on a * $g(O) = g(O')$
* $\vec{g}(\overrightarrow{OI}) = \overrightarrow{OI'}$ et $\vec{g}(\overrightarrow{OJ}) = \overrightarrow{O'J'}$
on cela caractérise g complètement.

I| • Pour trouver notre ellipse, on va se ramener à un cas particulier simple : celui du triangle équilatéral.



Dans ce cas, le cercle inscrit correspond aux critères recherchés.

Mais alors on a deux repères du plan : (A_0, B_0, C_0) et (A, B, C).
Prenons alors $g \in GA_2(\mathbb{R})$ qui envoie le premier sur le deuxième.
(c'est plus simple d'envoyer l'équilatéral sur le quelconque !)

Deux remarques :

* les milieux sont envoyés sur les milieux (barycentres !).
* l'image du cercle par g est une conique compacte, c'est donc une ellipse.

• Et on garde les tangentes car g est différentiable, ce qui permet de calculer, pour un arc γ tangent à $\overrightarrow{AB}$ en 0 :

$$\begin{aligned}(g \circ \gamma)'(0) &= dg(\gamma(0))(\gamma'(0)) \\ &= \vec{g}(\overrightarrow{AB}) \\ &= \overrightarrow{g(A)g(B)}\end{aligned}$$

On a donc bien une ellipse tritangente au triangle ABC !

II/ L'idée c'est de montrer qu'une ellipse tritangente à un triangle équilatéral, bah c'est en fait le cercle inscrit.

• on va partir dans l'autre sens : on envoie notre ellipse $\mathcal{E}$ sur un cercle $\mathcal{C}$ par un élément $g \in GA_2(\mathbb{R})$ tel que $g(\mathcal{E}) = \mathcal{C}$.
Mais alors g envoie T sur $T' = g(T)$.
Supposons que T' est équilatéral, alors T et T' sont semblables, ce qui signifie que g est une similitude
$\longrightarrow$ donc $\mathcal{E} = g^{-1}(\mathcal{C})$ est en fait un cercle !

Assurons nous donc que T' est équilatéral !

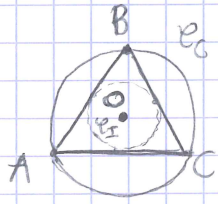
- les cercles inscrit $\mathcal{C}_I$ et circonscrits $\mathcal{C}_C$ de T' sont concentriques.
  - on a un triangle T' et un cercle tritangent à T', c'est donc le cercle inscrit de T' :

* CAR : par Pythagore, comme les rayons du cercle sont orthogonaux à la tangente au cercle, ce sont bien les plus courtes distances aux arêtes

  ⟶ des bas, c'est bien un cercle dont le centre est équidistant des milieux des côtés du triangle : le cercle inscrit

  ⇒ les rayons de $\mathcal{C}$ sont donc bien les médiatrices des côtés donc ils définissent le centre de $\mathcal{C}_C$.

- si $\mathcal{C}_I$ et $\mathcal{C}_C$ sont concentriques, le triangle est équilatéral



- soit r la rotation qui envoie A sur B.
  ⟶ elle envoie AB sur BC car :
  * A est envoyé sur B
  * AB est tangente à $\mathcal{C}_I$ donc $r(AB)$ aussi.
  * $B \in r(AB)$ donc c'est soit AB soit BC ⟶ $r(AB) = BC$
  * $B \in \mathcal{C}_C$ donc $r(AB)$ aussi ⟶ $r(B) = C$.

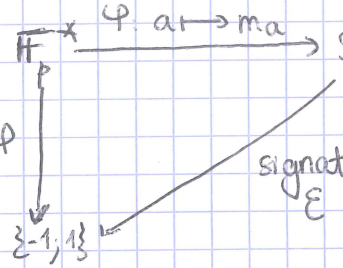
Donc $r(A) = B$, $r(B) = C$ et on peut montrer de même $r(C) = A$
⟶ ABC est équilatéral, ce qui achève la preuve !

LEMME DE ZOLOTAREV

Leçons: 105, 120, 121

Références: Caunet algèbre, P. Caldero (à paraître) avant les deux normalement :)

Résumé:



Le but du dev c'est de montrer que
- $\varepsilon(m_a) = \left(\frac{a}{p}\right)$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

pour p premier impair.

où m_a est la multiplication par a (modulo p)
et $\left(\frac{a}{p}\right)$ est le symbole de Legendre : $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \text{ est divisible par } p \\ 1 & \text{s'il existe } k \text{ tq } a \equiv k^2 \bmod p \\ -1 & \text{sinon.} \end{cases}$

On va montrer que :

I - si $\varphi : \mathbb{F}_p^* \longrightarrow \{-1;1\}$ est un morphisme non trivial alors c'est le morphisme $a \longmapsto \left(\frac{a}{p}\right)$.

II - $\phi : \mathbb{F}_p^* \longrightarrow S(\mathbb{F}_p^*)$ est un morphisme de groupes.
$a \longmapsto m_a$

III - Pour tout $a \in \mathbb{F}_p^*$, $\varepsilon(m_a) = \left(\frac{a}{p}\right)$
d'où $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

I • Soit $\chi : \mathbb{F}_p^* \longrightarrow \{-1, 1\}$ un morphisme de groupes non trivial.
et z un carré de $\mathbb{F}_p^*$, ie il existe $y \in \mathbb{F}_p^*$, tel que $z = y^2$.

· On a alors $\chi(z) = \chi(y)^2 = 1$, d'où :
$K = \{z \in \mathbb{F}_p^* \text{ carrés}\} \subseteq \ker \chi$.

• Or $|\ker\chi| \times \underbrace{|\mathrm{Im}\,\chi|}_{=|\{-1,1\}|=2} = \underbrace{|\mathbb{F}_p^*|}_{=p-1}$.

d'où $|\ker\chi| = \frac{p-1}{2}$ et $K = \ker\chi$ par égalité des cardinaux.

• Donc $\chi = \left(\frac{\cdot}{p}\right)$.

II • $a \in \mathbb{F}_p^*$ est inversible, donc $m_a^{-1} = m_{a^{-1}}$ donc m_a est bijective. ↗ $m_a \in S(\mathbb{F}_p^*)$.

• Pour $a, b \in \mathbb{F}_p^*$, z, $m_{ab}(z) = (ab)z = a(bz) = m_a \circ m_b(z)$.

• Donc ϕ est bien un morphisme de $\mathbb{F}_p^*$ dans $S(\mathbb{F}_p^*)$.

III • D'après I, si $a \mapsto \left(\frac{a}{p}\right)$ et $a \mapsto \varepsilon(m_a)$ sont deux morphismes non triviaux de $\mathbb{F}_p^*$ dans $\{-1;1\}$, alors on a gagné.

- $a \mapsto \left(\frac{a}{p}\right)$? il vaut -1 sur les non-carrés (et il y en a !)
- $a \mapsto \varepsilon(m_a)$?
  - $\mathbb{F}_p^*$ est cyclique généré par un certain $g \in \mathbb{F}_p^*$ on a alors $m_g = (1 \quad a \quad a^2 \quad \dots \quad a^{p-2})$
  - et $\varepsilon(m_g) = (-1)^{(p-1)-1} = (-1)^{p-2} = -1$.

⟶ les deux sont donc non-triviaux

+ ce sont des morphismes : $a \mapsto \left(\frac{a}{p}\right)$ par le critère d'Euler $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ mod p.
$a \mapsto \varepsilon(m_a)$ par II.

donc ce sont les mêmes

• On a donc $\left(\frac{2}{p}\right) = \varepsilon(m_2)$

et $m_2 = \begin{pmatrix} 1 & 2 & 3 & \dots & \frac{p-1}{2} & \frac{p+1}{2} & \dots & p-1 \\ 2 & 4 & 6 & & p-1 & 1 & \dots & p-2 \end{pmatrix}$ i,j tq $i<j$ et $m_2(i) > m_2(j)$

Or $\varepsilon(m_2) = (-1)^{\mathrm{Inv}(m_2)}$ où $\mathrm{Inv}(m_2)$ est le nombre d'inversions de m_2.

Et $\mathrm{Inv}(m_2) = 1 + 2 + \dots + \frac{p-1}{2} = \frac{1}{2}\underbrace{\frac{p-1}{2}\frac{p+1}{2}}_{\text{multiple de 2 car 4 divise } p-1 \text{ ou } p+1 !} = \frac{p^2-1}{8}$.

• On peut aussi remarquer que cela peut être difficile de déterminer la parité de $\frac{p^2-1}{8}$, mais si l'on regarde bien :
$\frac{p^2-1}{8}$ est pair ssi $p^2-1 \equiv 0 \bmod 16$ ie $p^2-1 \in \mathbb{Z}/16\mathbb{Z}$.

On a donc $\overline{p^2-1} = \bar{p}^2 - \bar{1} = \bar{0}$
et p étant impair $\bar{p} = \pm\bar{1}, \pm\bar{3}, \pm\bar{5}, \pm\bar{7}$
d'où $\bar{p}^2 = \pm\bar{1}, \pm\bar{9} = \pm\bar{7}, \pm\overline{25} = \pm\bar{7}, \pm\overline{49} = \pm\bar{1}$.

Conclusion : 2 est un carré modulo p si et seulement
$p \equiv \pm 1 \bmod 16$ ou $p \equiv \pm 7 \bmod 16$.

Bonus : Il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$ & p premier impair.
• Posons $\Phi : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$ c'est un morphisme de groupes.
$x \longmapsto x^2$
• Soit $a \in \ker\Phi$, on a $\Phi(a) = a^2 = 1$.
D'où $(a-1)(a+1) = 0$, soit $a = \pm 1$. (et $-1 \neq 1$ car $p > 2$).
Dès lors, $|\ker\Phi| = 2$ (par synthèse évidente)
• Ainsi, $|\mathrm{Im}\,\Phi| = \frac{|\mathbb{F}_p^*|}{|\ker\Phi|} = \frac{p-1}{2}$.

+ en fait on arrive à $p \equiv \pm 1 \bmod 8$
et il y en a une infinité grâce au petit théorème de Dirichlet.

+ le lemme de Zolotarev fournit un pont entre S_n et la théorie des nombres.

Lien avec le théorème de Zolotarev.

$\varphi : (\mathbb{F}_p)^n \longrightarrow (\mathbb{F}_p)^n$ automorphisme : $\varphi \in GL_n(\mathbb{F}_p)$.

Alors $\varepsilon(\varphi) = \left(\frac{\det \varphi}{p}\right)$.