Théorème de Frobenius-Zolotarev : 103, 104, 105, 106, 120, 121, 152

Théorème : soit p nombre premier impair et $n \in \mathbb{N}^*$ alors on a

$$\forall u \in GL_n(\mathbb{F}_q) = GL(\mathbb{F}_q^n), \quad \varepsilon(u) = \left(\frac{\det(u)}{p}\right)$$: symbole de Legendre

Remarque : . ε désigne la signature de u, vu comme permutation de $\mathbb{F}_q^n$: ensemble fini.

. Il s'agit de montrer que ε se factorise $\left(\frac{\cdot}{p}\right) \circ \det$.

On commence par un lemme de factorisation :

Lemme 1 : Soit $\mathbb{K}$ un corps et Π un groupe abélien, tq $\mathbb{K} \neq \mathbb{F}_2$ ou $n \neq 2$, $n \in \mathbb{N}^*$

Alors tout $\varphi : GL_n(\mathbb{K}) \to \Pi$ morphisme se factorise via $\det$.

i.e. $\forall \varphi \in \mathrm{Hom}_{\text{groupe}}(GL_n(\mathbb{K}), \Pi)$, $\exists! \, \delta \in \mathrm{Hom}_{\text{groupe}}(\mathbb{K}^\times, \Pi)$ tq $\varphi = \delta \circ \det$

- **preuve :** notons que comme $\mathbb{K} \neq \mathbb{F}_2$ ou $n \neq 2$, on a $D(GL_n(\mathbb{K})) = SL_n(\mathbb{K})$ $(*)$.

D'autre part, si $x, y \in GL_n(\mathbb{K})$, $\varphi([x,y]) = [\varphi(x), \varphi(y)] = 1_\Pi$ car Π est abélien et comme $D(GL_n(\mathbb{K}))$ est engendré par les commutateurs, $SL_n(\mathbb{K}) \subseteq \mathrm{Ker}(\varphi)$.

Donc $\varphi : GL_n(\mathbb{K}) \to \Pi$ se factorise de façon unique en $\bar{\varphi} : \frac{GL_n(\mathbb{K})}{SL_n(\mathbb{K})} \to \Pi$ tq $\varphi = \bar{\varphi} \circ \pi$

$$\begin{tikzcd} GL_n(\mathbb{K}) \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \Pi \\ GL_n(\mathbb{K})/SL_n(\mathbb{K}) \arrow[ur, dashed, "\bar{\varphi}"'] & \end{tikzcd}$$

De plus $\det : GL_n(\mathbb{K}) \twoheadrightarrow \mathbb{K}^\times$ est un morphisme surjectif, de noyau $SL_n(\mathbb{K})$, d'où le diagramme commutatif

$$\begin{tikzcd} GL_n(\mathbb{K}) \arrow[r, two heads, "\det"] \arrow[d, "\pi"'] & \mathbb{K}^\times \\ GL_n(\mathbb{K})/SL_n(\mathbb{K}) \arrow[ur, dashed, "\overline{\det}"'] & \end{tikzcd}$$

et $\overline{\det}$ est un isomorphisme.

On peut résumer par le diagramme suivant

$$\begin{tikzcd} \mathbb{K}^\times & GL_n(\mathbb{K}) \arrow[l, two heads, "\det"'] \arrow[r, "\varphi"] \arrow[d, "\pi"] & \Pi \\ & GL_n(\mathbb{K})/SL_n(\mathbb{K}) \arrow[ul, dashed, "\overline{\det}"] \arrow[ur, dashed, "\bar{\varphi}"'] & \end{tikzcd}$$

et donc

$$\varphi = \bar{\varphi} \circ (\overline{\det}^{-1}) \circ \overline{\det} \circ \pi$$
$$= \underbrace{\bar{\varphi} \circ \overline{\det}^{-1}}_{= \delta} \circ \det$$

La surjectivité de $\det$ assure l'unicité de la factorisation $\det = \overline{\det} \circ \pi$ et aussi celle de $\varphi = \delta \circ \det$.

Lemme 2 : Soit p premier impair, $\left(\frac{\cdot}{p}\right)$ est le seul morphisme non trivial de $\mathbb{F}_p^\times \to \{-1, 1\}$.

- **preuve :** $\left(\frac{\cdot}{p}\right)$ est bien un morphisme non trivial de $\mathbb{F}_p^\times \to \{-1,1\}$ car $\forall x \in \mathbb{F}_p^\times$, $x^2 = (-x)^2$ et donc $\begin{vmatrix} \mathbb{F}_p^\times \to \mathbb{F}_p^\times \\ x \mapsto x^2 \end{vmatrix}$ n'est pas injective $(p \geq 3)$, donc pas surjective

donc $\exists x \in \mathbb{F}_p^\times$ tq $\left(\frac{x}{p}\right) \neq 1$. $(\square)$

Réciproquement, si $\alpha \in Hom_{groupe}(\mathbb{F}_p^\times, \{-1,1\})$ est non trivial, $Ker(\alpha)$ est un sous-groupe d'indice 2 de $\mathbb{F}_p^\times$. Or $\mathbb{F}_p^\times$ est cyclique d'ordre $p-1$ pair, donc il existe un unique sous-groupe H d'indice 2 de $\mathbb{F}_p^\times$ et on a $\mathbb{F}_p^\times = H \sqcup xH$ où $x \notin H$ où $\alpha(y) = \begin{cases} 1 & \text{si } y \in H \\ -1 & \text{sinon} \end{cases}$
(Δ)

Alors: α est entièrement déterminé par H, donc il existe un unique morphisme non trivial.
$\rightarrow \alpha = \left(\frac{\cdot}{p}\right)$.

On passe à la preuve du théorème:

On montre que $\varepsilon : GL_n(\mathbb{F}_p) \rightarrow \{-1,1\}$ n'est pas trivial.

En effet, $\mathbb{F}_q := \mathbb{F}_{p^n} / \mathbb{F}_p$ est une extension de degré n de $\mathbb{F}_p$, isomorphe à $(\mathbb{F}_p)^n$ vu comme $\mathbb{F}_p$ e.v. Il suffit de trouver une bijection de $\mathbb{F}_q$ de signature -1.

Comme $\mathbb{F}_q^\times$ est cyclique d'ordre $q-1$, $\exists g \in \mathbb{F}_q$ tq $\langle g \rangle = \mathbb{F}_q$ (vus comme groupes).

Alors $x \mapsto gx$ est une bijection de $\mathbb{F}_q$ qui correspond sur $\mathbb{F}_q^n$ au $(q-1)$-cycle $(g, \dots, g^{q-1})$ de signature $(-1)^q = -1$ car $q = p^n$ est impair

$\rightarrow \varepsilon$ est non trivial.

De plus, le lemme 1 fournit un unique morphisme $\delta : \mathbb{F}_p^\times \rightarrow \{-1,1\}$ tq.
$\varepsilon = \delta \circ \det$ comme ε et $\det$ sont non triviaux, δ est un morphisme non trivial (lemme 2) et donc $\delta = \left(\frac{\cdot}{p}\right)$ d'où finalement $\varepsilon = \left(\frac{\det \cdot}{p}\right)$

Précisions:

$(*)$: $D(GL_n(\mathbb{K})) = SL_n(\mathbb{K})$ pour $(\mathbb{K}, n) \neq (\mathbb{F}_2, 2)$ $\rightarrow$ Perrin

↳ pas dur, $\subset$: évidente

$\supseteq$: montrer que toute transvection est un commutateur (elles sont toutes conjuguées)

(II): $\left(\frac{\cdot}{p}\right)$ est un morphisme : si p est un entier premier impair

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \text{ dans } \mathbb{F}_p$$

$$\rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(Δ) : Plus généralement: si $G = \langle x \rangle$ est d'ordre n, alors $\forall d | n$, $\exists ! H < G$ tq $|H| = d$ et $H = \langle x^k \rangle$ où $k = n/d$. (Josette Calais, III, 3.14)

En effet: $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ projection, $\Psi : \begin{cases} \mathbb{Z}/n\mathbb{Z} \rightarrow G \\ k \mapsto x^k \end{cases}$ est un isomorphisme donc tout sous-groupe de G est l'image par Ψ d'un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ mais l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre $d | n$ est $\mathbb{Z}/d\mathbb{Z}$, engendré par $\pi(x^{n/d})$

donc G admet un sous-groupe d'ordre d, unique, engendré par $\Psi(\pi(x^{n/d}))$.

(Objectif agreg)