Théorème de Frobenius-Zolotarev [1]

Leçons : 103, 106, 123, 152, *105*

[OA], exercice 5.4

Théorème

Soient p premier impair, $n \geqslant 1$ un entier.
Alors on a :

$$\forall u \in \mathrm{GL}_n\left(\mathbb{F}_p\right), \varepsilon(u) = \left(\frac{\det u}{p}\right)$$

On rappelle que :
- $\varepsilon(u)$ est la signature de u, vu comme permutation de $\mathbb{F}_p^n$;
- le symbole de Legendre est désigné par : $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0\ [p] \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases}$.

Démonstration :
On va montrer que $\varepsilon = \left(\frac{\cdot}{p}\right) \circ \det$ est une factorisation de la signature.

Lemme 1

Soit K un corps et M un groupe abélien. On suppose $K \neq \mathbb{F}_2$ ou $n \neq 2$.
Alors tout morphisme de groupes $\varphi : \mathrm{GL}_n(K) \to M$ se factorise par le déterminant, c'est-à-dire : il existe un unique morphisme de groupes $\delta : K^\times \to M$ tel que $\varphi = \delta \circ \det$.

Démonstration du lemme 1 :
Comme $K \neq \mathbb{F}_2$ ou $n \neq 2$, on a : $\mathcal{D}(\mathrm{GL}_n(K)) = \mathrm{SL}_n(K)$.

Pour $x, y \in \mathrm{GL}_n(K)$, $\varphi([x,y]) = [\varphi(x), \varphi(y)] = e$ car M est abélien.
Or, $\mathcal{D}(\mathrm{GL}_n(K))$ est engendré par les commutateurs ; on en déduit : $\mathcal{D}(\mathrm{GL}_n(K)) \subset \mathrm{Ker}\varphi$.
On a donc la factorisation suivante, où $\overline{\varphi}$ est l'unique morphisme tel que $\varphi = \overline{\varphi} \circ \pi$:

$$\begin{tikzcd}
\mathrm{GL}_n(K) \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"'] & M \\
\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \arrow[ur, dashed, bend right, "\overline{\varphi}"'] &
\end{tikzcd}$$

Et comme $\det : \mathrm{GL}_n(K) \to K^\times$ est un morphisme surjectif de noyau $\mathrm{SL}_n(K)$, on peut compléter ce diagramme commutatif pour le suivant, où $\overline{\det}$ est un isomorphisme (d'après le 1[er] théorème d'isomorphisme).

$$\begin{tikzcd}
K^\times \arrow[rr, dashed, bend right=80, "\delta"'] & \mathrm{GL}_n(K) \arrow[l, two heads, "\det"'] \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"] & M \\
& \mathrm{GL}_n(K)/\mathrm{SL}_n(K) \arrow[ul, bend left, "\overline{\det}"] \arrow[ur, bend right, "\overline{\varphi}"'] &
\end{tikzcd}$$

On a : $\varphi = \delta \circ \det$, où $\delta = \overline{\varphi} \circ \left(\overline{\det}\right)^{-1}$, et δ est l'unique morphisme de groupes de $K^\times$ vers M, car det est surjectif.

---

1. Donnons de ce résultat une application : le calcul du symbole de Legendre $\left(\frac{2}{p}\right)$. Posons $u : \left|\begin{array}{ccc} \mathbb{F}_p & \to & \mathbb{F}_p \\ x & \mapsto & 2x \end{array}\right.$. On a $\det u = 2$, calculons désormais la signature de la permutation u de $\mathbb{F}_p$. On construit le tableau suivant :

x	0	1	2	$\dots$	$\frac{p-1}{2}$	$\frac{p+1}{2}$	$\dots$	$p-2$	$p-1$
$u(x)$	0	2	4	$\dots$	$p-1$	1	$\dots$	$p-4$	$p-2$

Il s'agit de calculer le nombre d'inversions engendrées par cette permutation ; soit $k \geqslant \frac{p+1}{2}$, l'élément k voit sa position relative à $p-k$ éléments inversée par u. Le nombre total d'inversions est alors : $\displaystyle\sum_{k=\frac{p+1}{2}}^{p-1} p-k = \sum_{j=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2}\frac{p+1}{2}}{2} = \frac{p^2-1}{8}$. Et donc, $\varepsilon(u) = (-1)^{\frac{p^2-1}{8}}$, d'où, par Frobenius-Zolotarev : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. La même méthode permettrait de calculer $\left(\frac{-1}{p}\right)$, mais dans ce cas, il y a plus efficace.

■

Dans le cadre de ce théorème, ce lemme dit que : il existe un unique morphisme de groupes $\delta : \mathbb{F}_p^\times \to \{\pm 1\}$, tel que $\varepsilon = \delta \circ \det$.

Lemme 2

Soit p premier impair.
Le symbole de Legendre est l'unique morphisme de groupes non-trivial de $\mathbb{F}_p^\times$ dans $\{\pm 1\}$.

Démonstration du lemme 2 :

Comme p est premier impair $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ dans $\mathbb{F}_p$, d'où $\left(\frac{\cdot}{p}\right)$ est un morphisme de groupes.

C'est un morphisme non-trivial car $\Phi : \left| \begin{array}{ccc} \mathbb{F}_p^\times & \to & \mathbb{F}_p^\times \\ x & \mapsto & x^2 \end{array} \right.$ est non-injective, car $1^2 = (-1)^2$ et $1 \neq -1$ (comme $p \geqslant 3$), donc non-surjective.

Soit $\alpha : \mathbb{F}_p^\times \to \{\pm 1\}$ un morphisme de groupes non-trivial.

Nécessairement, on a : $\left(\mathbb{F}_p^\times : \operatorname{Ker} \alpha\right) = \#\operatorname{Im} \alpha = 2$ par le 1$^{\text{er}}$ théorème d'isomorphisme.

Or $\mathbb{F}_p^\times$ est cyclique [2] donc possède un unique sous-groupe d'indice 2 qu'on appelle H.

On a ainsi la partition $\mathbb{F}_p^\times = H \sqcup xH$, où $x \notin H$ et $\alpha(y) = \begin{cases} 1 & \text{si } y \in H \\ -1 & \text{sinon} \end{cases}$ donc α est entièrement déterminé.

Donc il existe un unique morphisme de groupes non-trivial de $\mathbb{F}_p^\times$ dans $\{\pm 1\}$: le symbole de Legendre. ■

Il reste alors à montrer que ε est non-trivial : $\varepsilon = \delta \circ \det$ impliquera que δ est non-trivial, puis que $\delta = \left(\frac{\cdot}{p}\right)$.

Notons $q = p^n$. Comme $\mathbb{F}_p$-espaces vectoriels, $\mathbb{F}_q$ et $\mathbb{F}_p^n$ sont isomorphes.

Il suffit donc d'exhiber une bijection $\mathbb{F}_p$-linéaire de $\mathbb{F}_q$ de signature -1.

$\mathbb{F}_q^\times$ est cyclique, notons g un de ses générateurs. La bijection $x \mapsto gx$ de $\mathbb{F}_q$ fixe 0 et donc agit sur $\mathbb{F}_q^\times$ comme la permutation $\begin{pmatrix} g & g^2 & \dots & g^{q-1} \end{pmatrix}$.

Sa signature est donc $(-1)^q = -1$, car q est impair. Et donc ε n'est pas trivial, d'où $\varepsilon = \left(\frac{\cdot}{p}\right) \circ \det$. ■

Références

[OA] V. BECK, J. MALICK et G. PEYRÉ – *Objectif Agrégation*, 2$^{\text{e}}$ éd., H&K, 2005.

2. Pour la cyclicité de $\mathbb{F}_q^\times$, on renvoie à la page **??**.