Développement. Le théorème de Frobenius-Zolotarev

Lemme 1. Soient K un corps et $n \in \mathbf{N}^*$ un entier avec $K \neq \mathbf{F}_2$ ou $n \neq 2$. Soit G un groupe abélien. Alors tout morphisme de groupes $\varphi\colon \mathrm{GL}_n(K) \longrightarrow G$ se factorise par le déterminant, c'est-à-dire il existe un unique morphisme de groupes $\delta\colon K^\times \longrightarrow G$ tel que $\varphi = \delta \circ \det$.

Preuve Comme $K \neq \mathbf{F}_2$ et $n \neq 2$, on peut écrire $\mathrm{D}(\mathrm{GL}_n(K)) = \mathrm{SL}_n(K)$. Montrons alors que $\operatorname{Ker}\varphi \supset \mathrm{D}(\mathrm{GL}_n(K))$. Soient $g, h \in \mathrm{GL}_n(K)$. Comme le groupe G est abélien et l'application φ est un morphisme de groupes, on obtient

$$\begin{aligned}\varphi([g,h]) &= \varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} \\ &= \varphi(g)\varphi(g)^{-1}\varphi(h)\varphi(h)^{-1} = 1.\end{aligned}$$

En notant $\pi\colon \mathrm{GL}_n(K) \longrightarrow \mathrm{GL}_n(K)/\mathrm{SL}_n(K)$ la projection canonique, le première théorème d'isomorphisme assure qu'il existe un unique morphisme de groupes

$$\tilde\varphi\colon \mathrm{GL}_n(K)/\mathrm{SL}_n(K) \longrightarrow G$$

tel que

$$\varphi = \tilde\varphi \circ \pi.$$

Par ailleurs, le déterminant se factorise aussi en un isomorphisme de groupes

$$\overline{\det}\colon \mathrm{GL}_n(K)/\mathrm{SL}_n(K) \longrightarrow K^\times$$

puisqu'il est lui-même surjectif. Ce dernier vérifie $\det = \overline{\det} \circ \pi$. Finalement, en considérant le morphisme de groupes

$$\delta \coloneqq \tilde\varphi \circ \overline{\det}^{-1},$$

on obtient

$$\varphi = \tilde\varphi \circ \overline{\det}^{-1} \circ \overline{\det} \circ \pi = \delta \circ \det.$$

L'unicité vient du fait que le déterminant est surjectif sur $K^\times$. ◁

$$\begin{tikzcd}
K^\times \arrow[rr, bend left, "\delta"] & \mathrm{GL}_n(K) \arrow[l, "\det"'] \arrow[r, "\varphi"] \arrow[d, "\pi"] & G \\
& \mathrm{GL}_n(K)/\mathrm{SL}_n(K) \arrow[ul, "\sim"', "\overline{\det}"] \arrow[ur, "\tilde\varphi"'] &
\end{tikzcd}$$

Lemme 2. Soient $p \geqslant 3$ un nombre premier. Alors le symbole de Legendre

$$a \in \mathbf{F}_p^\times \longmapsto \left(\frac{a}{p}\right) \in \{\pm 1\}$$

est l'unique morphisme de groupes non trivial $\mathbf{F}_p^\times \longrightarrow \{\pm 1\}$.

Preuve Notons d'abord que le symbole de Legendre n'est pas trivial puisque $p \geqslant 3$: il y a $(p-1)/2$ non carrés dans $\mathbf{F}_p^\times$. Montrons que c'est le seul. Soit $\alpha\colon \mathbf{F}_p^\times \longrightarrow \{\pm 1\}$ un morphisme de groupes non trivial. Alors il est surjectif et son noyau $\operatorname{Ker}\alpha$ est un sous-groupe d'indice 2 de $\mathbf{F}_p^\times$ puisque

$$\mathbf{F}_p^\times / \operatorname{Ker}\alpha \simeq \{\pm 1\}.$$

Par ailleurs, comme $p \geqslant 3$, le groupe $\mathbf{F}_p^\times \simeq \mathbf{Z}/(p-1)\mathbf{Z}$ est cyclique de cardinal pair, donc il admet un unique sous-groupe $H \leqslant \mathbf{F}_p^\times$ d'indice 2. D'après ce qui précède, il s'agit du sous-groupe $H = \operatorname{Ker}\alpha$. Soit $x \in \mathbf{F}_p^\times \setminus H$. On obtient alors la partition $\mathbf{F}_p^\times = H \sqcup xH$ et, pour tout $y \in \mathbf{F}_p^\times$, on peut écrire

$$\alpha(y) = \begin{cases} 1 & \text{si } y \in H, \\ -1 & \text{si } y \in xH \end{cases}$$

Ainsi l'unique sous-groupe $H \leqslant \mathbf{F}_p^\times$ d'indice 2 caractérise entièrement le morphisme α ce qui montre l'unicité de ce dernier. ◁

Un isomorphisme u d'un espace vectoriel E de dimension finie sur un corps fini est *a fortiori* un élément du groupe symétrique $\mathfrak{S}(E)$ de cet espace vectoriel. Par conséquent, on peut considérer sa signature $\varepsilon(u)$.

Théorème 3. Soient $p \geqslant 3$ un nombre premier et E un $\mathbf{F}_p$-espace vectoriel de dimension fini. Alors

$$\forall u \in \mathrm{GL}(E), \qquad \varepsilon(u) = \left(\frac{\det u}{p}\right).$$

Preuve On considère l'application signature $\varepsilon\colon \mathrm{GL}(E) \longrightarrow \{\pm 1\}$ obtenu en composant l'inclusion $\mathrm{GL}(E) \longrightarrow \mathfrak{S}(E)$ et la signature $\mathfrak{S}(E) \longrightarrow \{\pm 1\}$. Il s'agit alors d'un morphisme de groupes. Comme $p \geqslant 3$ et le groupe $\{\pm 1\}$ est abélien, le lemme nous donne un morphisme de groupes $\delta\colon \mathbf{F}_p^\times \longrightarrow \{\pm 1\}$ tel que

$$\varepsilon = \delta \circ \det.$$

On veut montrer que le morphisme δ est le symbole de Legendre. Grâce au lemme 2, il suffit de montrer qu'il n'est pas trivial. En notant $d \coloneqq \dim_{\mathbf{F}_p}(E)$ et $q \coloneqq p^d$, les $\mathbf{F}_p$-espaces vectoriels E et $\mathbf{F}_q$ sont isomorphes. Il suffit alors de trouver un élément du groupe $\mathrm{GL}(\mathbf{F}_q)$ qui est de signature -1. Le groupe $\mathbf{F}_q^\times \simeq \mathbf{Z}/(q-1)\mathbf{Z}$ est cyclique d'ordre $q-1$. Soit $g \in \mathbf{F}_q^\times$ un générateur. Considérons alors l'isomorphisme

$$(x \longmapsto gx) \in \mathrm{GL}(\mathbf{F}_q).$$

Vu comme une permutation, il s'agit du cycle $(1 \ g \ g^2 \ \cdots \ g^{q-2}) \in \mathfrak{S}(\mathbf{F}_q)$. Sa longueur vaut $q-1$, donc sa signature vaut $(-1)^q = -1$ car, comme l'entier p est impair, l'entier $q = p^d$ est impair. Ainsi le morphisme δ n'est pas trivial ce qui donne la conclusion. ◁

[1] Vincent Beck, Jérôme Malick et Gabriel Peyré. *Objectif Agrégation*. 2e édition. H&K, 2005.