Théorème de Frobenius-Zolotarev

2013 – 2014

Théorème.
Soit p un nombre premier ≥ 3 et $n \in \mathbb{N}^*$. Alors pour tout $u \in GL_n(\mathbb{F}_p)$, on a :

$$\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où $\left(\frac{a}{p}\right)$ est le symbole de Legendre :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \equiv 0 \text{ mod } p, \\ 1 \text{ si } a \text{ est un carré modulo } p \text{ (un résidu quadratique)}, \\ -1 \text{ sinon} \end{cases}$$

et où $\varepsilon(u)$ est la signature de u en tant que permutation sur l'ensemble fini $\mathbb{F}_p^n$.

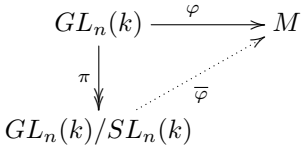
Démonstration. Il s'agit de montrer que la signature se factorise de la façon suivante : $\varepsilon = \left(\frac{\cdot}{p}\right) \circ \det$. On commence par énoncer un premier lemme.

Lemme.
Soit k un corps, M un groupe abélien et $n \in \mathbb{N}^*$. On suppose $k \neq \mathbb{F}_2$ ou $n \neq 2$. Alors tout morphisme de groupe $\varphi : GL_n(k) \to M$ se factorise par le déterminant,
i.e. il existe un unique morphisme de groupe $\delta : k^\times \to M$ tel que $\varphi = \delta \circ \det$.

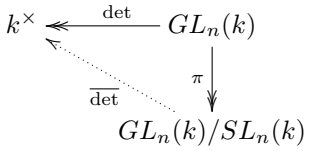
Démonstration. D'une part, puisque $k \neq \mathbb{F}_2$ ou $n \neq 2$, on a $D(GL_n(k)) = SL_n(k)$ (voir détails en fin de document).

D'autre part, pour $x, y \in GL_n(k), \varphi([x,y]) = [\varphi(x), \varphi(y)] = e$ car M est abélien.
$D(GL_n(k))$ est engendré par les commutateurs donc $D(GL_n(k)) \subseteq \ker \varphi$.

Donc $\varphi : GL_n(k) \to M$ se factorise en un unique morphisme $\overline{\varphi} : GL_n(k)/SL_n(k) \to M$:

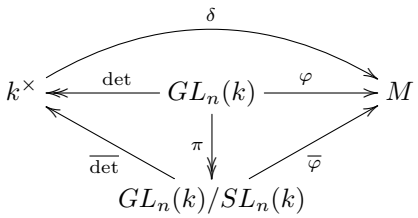


Comme det est un morphisme surjectif de $GL_n(k)$ dans $k^\times$ dont le noyau est $SL_n(k)$, on obtient le diagramme commutatif suivant :



avec $\overline{\det}$ un isomorphisme. Alors :

$$\varphi = \overline{\varphi} \circ (\overline{\det})^{-1} \circ \overline{\det} \circ \pi = \delta \circ \det \text{ avec } \delta = \overline{\varphi} \circ (\overline{\det})^{-1}$$



La surjectivité de det assure alors l'unicité du morphisme δ vérifiant $\delta \circ \det = \varphi$. □

On a, dans le cadre du théorème, $\varepsilon : GL_n(\mathbb{F}_p) \to \{-1, 1\}$ avec $\{-1, 1\}$ abélien donc, par le lemme, il existe un unique morphisme $\delta : \mathbb{F}_p^\times \to \{-1, 1\}$ tel que $\varepsilon = \delta \circ \det$. Il s'agit de montrer que δ est le symbole de Legendre. Pour cela, nous allons montrer que le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^\times$ dans $\{-1, 1\}$, puis que $\varepsilon : GL_n(\mathbb{F}_p) \to \{-1, 1\}$ n'est pas trivial.

Le symbole de Legendre est bien non trivial car $x^2 = (-x)^2$ donc :

$$\begin{aligned} \mathbb{F}_p^\times &\to \mathbb{F}_p^\times \\ x &\mapsto x^2 \end{aligned}$$

n'est pas injective ($p \geq 3$) donc n'est pas surjective.

Si $\alpha : \mathbb{F}_p^\times \to \{-1, 1\}$ est un morphisme non trivial, $\ker \alpha$ est un sous-groupe d'indice 2 de $\mathbb{F}_p^\times$. Or $\mathbb{F}_p^\times$ est un groupe cyclique de cardinal pair donc ne possède qu'un seul sous-groupe H d'indice 2.
On a ainsi la partition $\mathbb{F}_p^\times = H \sqcup xH$ où $x \notin H$ avec :

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

Ainsi, α est entièrement déterminé donc est unique, c'est le morphisme de Legendre.

Montrons maintenant que ε n'est pas trivial.

Il existe une extension $\mathbb{F}_q/\mathbb{F}_p$ de degré n (à savoir $\mathbb{F}_{p^n}$). Vus comme $\mathbb{F}_p$-espaces vectoriels, $\mathbb{F}_p^n$ et $\mathbb{F}_q$ sont isomorphes. Il suffit donc de trouver une bijection $\mathbb{F}_p$-linéaire de $\mathbb{F}_q$ de signature -1. Or $\mathbb{F}_q^\times$ est cyclique d'ordre $q-1$. Soit g un générateur de ce groupe. La bijection $\mathbb{F}_p$-linéaire $x \mapsto gx$ de $\mathbb{F}_q$ agit comme le cycle $(g, g^2, \ldots, g^{q-1})$ de longueur $q-1$. Sa signature est donc $(-1)^q = -1$ car $q = p^n$ est impair.

Finalement, ε n'est pas trivial donc $\delta \circ \det$ non plus, donc δ n'est pas trivial et il s'agit donc du symbole de Legendre. □

Détails supplémentaires

Théorème.
$D(GL_n(k)) = SL_n(k)$ pour $n \neq 2$ ou $k \neq \mathbb{F}_2$.

Démonstration. Pour $u, v \in GL_n(k)$, $[u, v] \in SL_n(k)$, donc :

$$D(GL_n(k)) \subseteq SL_n(k)$$

Pour montrer l'inclusion inverse, il suffit de montrer que toute transvection est un commutateur ($n \geq 2$). Comme toutes les transvections sont conjuguées, il suffit de le montrer pour l'une d'elles.

– Si $n \geq 3$, alors :

$$I_n + E_{1,2} = [I_n + E_{1,3}, I_n + E_{3,2}]$$

– Si la caractéristique de k est différente de 2, alors :

$$I_n + E_{1,2} = [I_n + E_{1,2}, \mathrm{Diag}(2^{-1}, 1, \ldots, 1)]$$

– Si $\mathrm{card}(k) > 3$, alors, pour $a \in k$, a différent de $-1, 0$ et 1, on a :

$$I_n + E_{1,2} = [I_n + a^2(1-a^2)E_{1,2}, \mathrm{Diag}(a, a^{-1}, 1, \ldots, 1)]$$

□

Proposition.
Le symbôle de Legendre est un morphisme.

Démonstration. Pour p premier impair,

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

D'où :

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

□

Références

[1] Vincent Beck, Jérome Malick, Gabriel Peyré, *Objectif Agrégation*, H&K, 2004, page 251.