

Théorème de Frobenius-Zolotarev

2012-2013

Référence : Vincent Beck, Jérôme Malick, Gabriel Peyré, *Objectif Agrégation*, H&K, 2004, p.251.

Théorème.

Soit p un nombre premier ≥ 3 .

Soit V un espace vectoriel sur \mathbb{F}_p de dimension finie.

Alors pour tout $u \in GL(V)$, on a :

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

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

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

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

Démonstration.

- Soit k un corps et M un groupe abélien. Montrons que si $k \neq \mathbb{F}_2$ ou $n \neq 2$, tout morphisme de groupe $\varphi : GL_n(k) \rightarrow M$ se factorise par le déterminant. i.e. il existe un unique morphisme de groupe $\delta : k^\times \rightarrow M$ tel que $\varphi = \delta \circ \det$. Si $k \neq \mathbb{F}_2$ ou $n \neq 2$, alors $D(GL_n(k)) = SL_n(k)$ (voir détails en fin de document).

Lemme.

Soit G un groupe et M un groupe abélien.

Alors tout morphisme $\varphi : G \rightarrow M$ se factorise par $G/D(G)$.

Démonstration. Pour $x, y \in G$, $\varphi([x, y]) = [\varphi(x), \varphi(y)] = e$ car M est abélien. $D(G)$ est engendré par les commutateurs donc $D(G) \subseteq \ker \varphi$, donc φ se factorise par $G/D(G)$. \square

Donc $\varphi : GL_n(k) \rightarrow M$ se factorise en un unique morphisme :

$$\bar{\varphi} : GL_n(k)/SL_n(k) \rightarrow M$$

tel que $\varphi = \bar{\varphi} \circ \pi$ où $\pi : GL_n(k) \rightarrow GL_n(k)/SL_n(k)$ est la surjection canonique.

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 :

$$\begin{array}{ccc} GL_n(k) & \xrightarrow{\det} & k^\times \\ \pi \downarrow & \nearrow \overline{\det} & \\ GL_n(k)/SL_n(k) & & \end{array}$$

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

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

$$\begin{array}{ccccc} & & \delta & & \\ & \curvearrowright & & \curvearrowleft & \\ M & \xleftarrow{\varphi} & GL_n(k) & \xrightarrow{\det} & k^\times \\ & \searrow \bar{\varphi} & \pi \downarrow & \nearrow \overline{\det} & \\ & & GL_n(k)/SL_n(k) & & \end{array}$$

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

- Soit p premier ≥ 3 , montrons que le symbole de Legendre est l'unique morphisme non trivial de \mathbb{F}_p^\times dans $\{-1, 1\}$.

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

$$\begin{array}{ccc} \mathbb{F}_p^\times & \rightarrow & \mathbb{F}_p^\times \\ x & \mapsto & x^2 \end{array}$$

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

Si $\alpha : \mathbb{F}_p^\times \rightarrow \{-1, 1\}$ 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.

- Le morphisme ε est un morphisme de groupes à valeurs dans un groupe abélien. Il existe donc un morphisme $\delta : \mathbb{F}_p^\times \rightarrow \{-1, 1\}$ tel que $\delta \circ \det = \varepsilon$. Il reste à prouver que δ est le symbole de Legendre. Pour cela, on montre qu'il existe $u \in GL(V)$ vérifiant $\varepsilon(u) = \delta \circ \det(u) = -1$. Ainsi δ n'est pas le morphisme trivial et par conséquent δ est le symbole de Legendre. Il existe une extension $\mathbb{F}_q/\mathbb{F}_p$ de degré $d = \dim V$ (à savoir \mathbb{F}_{p^d}). Vu comme \mathbb{F}_p -espaces vectoriels, V 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 permutation $x \mapsto gx$ de \mathbb{F}_q agit comme le cycle (g, g^2, \dots, g^{q-1}) de longueur $q-1$. Sa signature est donc $(-1)^q = -1$ car $q = p^d$ est impair. □

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 :

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

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

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

□

Proposition.

Le symbole 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 :

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

□