Théorème de Frobénius–Zolotarev

Pierron Théo

5 janvier 2014

Soit k un corps différent de $\mathbb{F}_2$, $n \geqslant 2$ et $(M, +)$ un groupe abélien.

Théorème *Pour tout $p \geqslant 3$ premier, et $u \in GL_n(\mathbb{F}_p)$,*

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

où $\varepsilon(u)$ est la signature de la permutation induite par u sur $\mathbb{F}_p^n$.

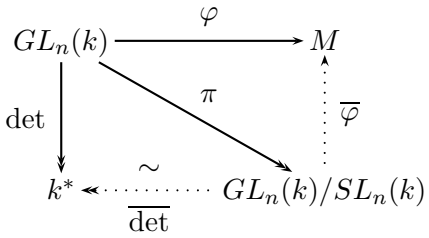
Lemme 1
Tout morphisme $\varphi : GL_n(k) \to M$ se factorise par le déterminant : il existe un unique $\delta : k^* \to M$ tel que $\varphi = \delta \circ \det$.

Démonstration. Notons d'abord que par surjectivité de det, si δ existe, il est unique.

Soit $u, v \in GL_n(k)$. Alors $\varphi([u, v]) = [\varphi(u), \varphi(v)] = 0$ car M est abélien.

Donc $\{[u, v], (u, v) \in GL_n(k)^2\} \subset \operatorname{Ker} \varphi$ donc $SL_n(k) = D(GL_n(k)) \subset \operatorname{Ker} \varphi$.

Par propriété universelle du quotient $GL_n(k)/SL_n(k)$, il existe un unique $\overline{\varphi} : GL_n(k)/SL_n(k) \to M$ tel que $\varphi = \overline{\varphi} \circ \pi$:



$\det : GL_n(k) \to k^*$ est surjectif de noyau $SL_n(k)$ donc il se factorise en $\overline{\det} \circ \pi$ avec $\overline{\det}$ bijectif.

On a alors

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

avec $\delta : k^* \to M$. ∎

Lemme 2
$L : x \mapsto \left(\frac{x}{p}\right)$ est l'unique morphisme non trivial de $\mathbb{F}_p^* \to \{\pm 1\}$.

Démonstration. L est un morphisme non trivial car il y a $\frac{p-1}{2} > 0$ non carrés dans $\mathbb{F}_p^*$.

Soit $\alpha : \mathbb{F}_p^* \to \{\pm 1\}$ non trivial (donc surjectif). Si z est un générateur de $\mathbb{F}_p^*$, on a $\alpha(z) = -1$ car α est non trivial.

Si $L(x) = 1$, x s'écrit y^2 donc $\alpha(x) = \alpha(y)^2 = 1$. Réciproquement, si $\alpha(x) = 1$, en notant $x = z^k$, on a $\alpha(x) = \alpha(z)^k = (-1)^k$ donc k est pair et $x = (z^{\frac{k}{2}})^2$ vérifie $L(x) = 1$.

Donc $\alpha = L$. ∎

On peut maintenant démontrer le théorème de Frobénius-Zolotarev.

Démonstration. $\{\pm 1\}$ est commutatif donc par le premier lemme, il existe un unique $\delta : \mathbb{F}_p^* \to \{\pm 1\}$ tel que $\delta \circ \det = \varepsilon$.

On montre que δ est non trivial. En tant que $\mathbb{F}_p$-espaces vectoriels, $\mathbb{F}_{p^n} \simeq \mathbb{F}_p^n$. Soit $q = p^n$ et g un générateur de $\mathbb{F}_q^*$.

L'application $u : x \mapsto gx$ est $\mathbb{F}_p$-linéaire et correspond au cycle $(g, g^2, \ldots, g^{q-1})$. On a

$$\varepsilon(u) = \varepsilon(g, g^2, \ldots, g^{q-1}) = (-1)^q = -1$$

En particulier $\delta(\det(u)) = -1$ donc δ est non trivial, donc $\delta = L$.

On a donc prouvé que $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$ pour tout $u \in GL_n(\mathbb{F}_p)$. ■