Théorème de Frobenius-Zolotarev

Lemme 1. Soient $K \neq \mathbb{F}_2$ un corps, M un groupe abélien et $n \neq 2$. Tout morphisme de groupes $\varphi : GL_n(K) \to M$ se factorise par le déterminant :

$$\exists!\, \delta : K^\times \to M,\ \ \varphi = \delta \circ \det .$$

Démonstration. Le groupe dérivé de $GL_n(K)$ est $SL_n(K)$. Pour tous $x, y \in GL_n(K)$, on a $\varphi([x,y]) = [\varphi(x), \varphi(y)] = 0$ puisque M est abélien. Ainsi, $D(GL_n(K)) \subset \ker \varphi$. Par théorème d'isomorphisme :

$$\exists!\, \overline{\varphi} : GL_n(K)/SL_n(K) \twoheadrightarrow M.$$

D'autre part, $\det : GL_n(K) \to K^\times$ est surjectif, de noyau $SL_n(K)$, donc :

$$\exists!\, \overline{\det} : GL_n(K)/SL_n(K) \xrightarrow{\sim} K^\times.$$

De là, $\varphi = \delta \circ \det$, en notant $\delta = \overline{\varphi} \circ (\overline{\det})^{-1}$. L'unicité découle de la surjectivité du déterminant. □

Lemme 2. Le symbole de Legendre est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^\times$ à valeurs dans $\{\pm 1\}$.

Démonstration. Pour tout $a \in \mathbb{F}_p^\times$, le théorème de Fermat assure que $a^{p-1} \equiv 1\ [p]$, donc :

$$a^{\frac{p-1}{2}} \equiv \pm 1\ [p].$$

Or $\psi : x \mapsto x^2$ a pour noyau $\{\pm 1\}$, donc il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^\times$ (par théorème d'isomorphisme). Donc si a est un carré, $a^{\frac{p-1}{2}} \equiv 1\ [p]$, et sinon $a^{\frac{p-1}{2}} \equiv -1\ [p]$. Autrement dit :

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\ [p].$$

Le symbole de Legendre est donc un morphisme de groupes non trivial de $\mathbb{F}_p^\times$ à valeurs dans $\{\pm 1\}$.
Maintenant, si α est un tel morphisme, alors $H = \ker \alpha$ est l'unique (car $2 | (p-1)$ et $\mathbb{F}_p^\times$ est cyclique) sous-groupe d'indice 2 de $\mathbb{F}_p^\times$. Donc $\mathbb{F}_p^\times = H \sqcup xH$, avec $x \notin H$, et $(\alpha_{|H}, \alpha_{|xH}) = (1, -1)$. Cela détermine entièrement tout morphisme comme ci-dessus. □

Théorème 3. Soient $n \in \mathbb{N}^*$ et p premier impair.

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

Démonstration. D'après le premier lemme, il existe (un unique) $\delta : \mathbb{F}_p^\times \to \{\pm 1\}$ tel que $\varepsilon = \delta \circ \det$. Soit $q = p^n$. Vus comme $\mathbb{F}_p$-espaces vectoriels, $\mathbb{F}_q$ et $\mathbb{F}_p^n$ sont isomorphes. De plus, si g engendre $\mathbb{F}_q^\times$ (car $\mathbb{F}_q^\times$ est cyclique), alors $x \mapsto gx$ fixe 0, est $\mathbb{F}_p$-linéaire et peut être vue comme le cycle $(g, \dots, g^{q-1})$, de signature $(-1)^q = -1$. Donc δ est non trivial. Le second lemme permet de conclure. □