Théorème de Frobenius-Zolotarev

Théorème : Soient p un nombre premier au moins égal à 3, $n \in \mathbb{N}^*$ et $u \in GL_n(\mathbb{F}_p)$. Alors u est une permutation de $\mathbb{F}_p^{\,n}$, de signature $\left(\frac{\det u}{p}\right)$.

Démonstration :

• Lemme : Soit p un nombre premier au moins égal à 3. On a $D(GL_n(\mathbb{F}_p)) = SL_n(\mathbb{F}_p)$.

→ Preuve : Tout commutateur de $GL_n(\mathbb{F}_p)$ étant dans $SL_n(\mathbb{F}_p)$, on a $D(GL_n(\mathbb{F}_p)) \subset SL_n(\mathbb{F}_p)$. Pour l'autre inclusion, on remarque que les transvections, qui sont deux à deux conjuguées dans $GL_n(\mathbb{F}_p)$, engendrent $SL_n(\mathbb{F}_p)$. Il suffit alors d'écrire la transvection $I_n + E_{1,2}$ comme un commutateur.

On a $I_n + E_{1,2} = \left[\begin{pmatrix} 2^{-1} & & (0) \\ & 1 & \\ (0) & & \ddots \;1 \end{pmatrix}, I_n + (1+2^{-1})^{-1} E_{1,2} \right]$, ce qui donne le lemme.

On passe à la preuve du théorème. On note L le symbole de Legendre.

Pour tous $x, y \in GL_n(\mathbb{F}_p)$, on a
$$\begin{aligned} \varepsilon([x,y]) &= [\varepsilon(x), \varepsilon(y)] && (\varepsilon \text{ est un morphisme de groupes}) \\ &= 1 && (\{-1,1\} \text{ est abélien}) \end{aligned}$$

donc $SL_n(\mathbb{F}_p) = D(GL_n(\mathbb{F}_p)) \subset \ker \varepsilon$. On note alors $\overline{\varepsilon} : GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p) \longrightarrow \{-1,1\}$ l'unique morphisme de groupes tel que $\varepsilon = \overline{\varepsilon} \circ \pi$, où $\pi : GL_n(\mathbb{F}_p) \twoheadrightarrow GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p)$ est la projection canonique. Le morphisme de groupes $\det : GL_n(\mathbb{F}_p) \longrightarrow \mathbb{F}_p^*$ étant surjectif, il se factorise (de manière unique) en un isomorphisme de groupes $\overline{\det} : GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p) \xrightarrow{\sim} \mathbb{F}_p^*$ (i.e $\det = \overline{\det} \circ \pi$).

On a alors $\varepsilon = \overline{\varepsilon} \circ \pi = \underbrace{\overline{\varepsilon} \circ \overline{\det}^{-1}}_{=:\delta} \circ \underbrace{\overline{\det} \circ \pi}_{=\det} = \delta \circ \det$.

On va montrer que $\delta = L$. On commence par remarquer que $L : \mathbb{F}_p^* \longrightarrow \{-1, 1\}$ est un morphisme de groupe non trivial. Soit g un générateur de $\mathbb{F}_p^*$.

Un morphisme de groupes $\alpha : \mathbb{F}_p^* \longrightarrow \{-1,1\}$ est entièrement déterminé par la valeur $\alpha(g)$: le cas $\alpha(g) = 1$ correspond au morphisme trivial

$\alpha(g) = -1$ à L

Il reste à montrer que δ n'est pas trivial. Si δ était trivial, ε le serait aussi. On va donc trouver $u \in GL_n(\mathbb{F}_p)$ tel que $\varepsilon(u) = -1$.

Comme $\mathbb{F}_p^n$ et $\mathbb{F}_q$, où $q = p^n$, sont isomorphes en tant que $\mathbb{F}_p$-espaces vectoriels, on va trouver $u \in GL(\mathbb{F}_q)$ tel que $\varepsilon(u) = -1$. Soit g un générateur de $\mathbb{F}_q^*$.

On pose alors $u : \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & gx \end{array}$, qui est dans $GL(\mathbb{F}_q)$, et est égal

au cycle $(1 \ g \ g^2 \dots g^{q-2})$. On a alors $\varepsilon(u) = (-1)^q = -1$, car q est impair.

Ceci achève la preuve, car $\delta = L$, donc pour tout $u \in GL_n(\mathbb{F}_p)$,

on a $\varepsilon(u) = L \circ \det(u) = \left(\frac{\det u}{p}\right)$.