Théorème de Frobenius-Zolotarev

Recasage : 103, 105, 106,

Référence : Beck, Malick, Peyré p 252

Théorème : soient $p \geq 3$ premier, $n \in \mathbb{N}^*$, alors $\forall u \in GL_n(\mathbb{F}_p)$, $\varepsilon(u) = \left(\frac{\det u}{p}\right)$ où $\varepsilon(u)$ désigne la signature de u vu comme permutation de l'ensemble $\mathbb{F}_p^n$, et où $\left(\frac{\cdot}{p}\right)$ désigne le symbole de Legendre défini par :

$$\forall a \in \mathbb{Z}, \left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a = 0 \bmod p \\ 1 \text{ si } a \text{ est un carré dans } \mathbb{F}_p. \\ -1 \text{ sinon} \end{cases}$$

Notons que $\varepsilon(u)$ est bien définie car $GL_n(\mathbb{F}_p) \hookrightarrow S(\mathbb{F}_p^n) \simeq S_{p^n} \simeq S(\mathbb{F}_{p^n})$ et ε est un morphisme de groupes donc n'est pas affecté par le choix des isomorphismes précédents.

Lemme : pour $p \geq 3$ premier, on a $\mathcal{D}(GL_n(\mathbb{F}_p)) = SL_n(\mathbb{F}_p)$. [Per] p 101

→ Tout commutateur de $GL_n(\mathbb{F}_p)$ étant dans $SL_n(\mathbb{F}_p)$, on a $\mathcal{D}(GL_n(\mathbb{F}_p)) \subseteq SL_n(\mathbb{F}_p)$. Réciproquement, on commence par voir que les matrices de transvection sont deux à deux conjuguées dans $GL_n(\mathbb{F}_p)$ et engendrent $SL_n(\mathbb{F}_p)$. Or si A est une matrice de transvection de $GL_n(\mathbb{F}_p)$, elle s'écrit $A = I_n + \lambda E_{i,j}$ avec $\lambda \in \mathbb{F}_p^\times$ et $i \neq j$. On a alors après calcul $A^2 = I_n + 2\lambda E_{i,j}$ et comme $\mathbb{F}_p$ est de caract. $\neq 2$, on a $2\lambda \in \mathbb{F}_p^\times$ et donc A^2 est une transvection. Elle est donc conjuguée avec A : $\exists B \in GL_n(\mathbb{F}_p)$ tq $A^2 = B^{-1}AB$ et donc $A = B^{-1}ABA^{-1} \in \mathcal{D}(GL_n(\mathbb{F}_p))$ donc a fortiori $SL_n(\mathbb{F}_p) \subseteq \mathcal{D}(GL_n(\mathbb{F}_p))$ d'où l'égalité.

Passons à la preuve du théorème. Notons L le symbole de Legendre $\left(\frac{\cdot}{p}\right)$.

Pour tous $x, y \in GL_n(\mathbb{F}_p)$, on a $\varepsilon([x,y]) = [\varepsilon(x), \varepsilon(y)]$ (car ε est un morphisme de grp)
$= 1$ (car $\{\pm 1\}$ est abélien)

donc a fortiori, $SL_n(\mathbb{F}_p) = \mathcal{D}(GL_n(\mathbb{F}_p)) \subseteq \ker \varepsilon$

$$\begin{array}{ccccc} \mathbb{F}_p^\times & \xleftarrow{\det} & GL_n(\mathbb{F}_p) & \xrightarrow{\varepsilon} & \{\pm 1\} \\ \uparrow \pi & & \downarrow \pi & \nearrow \exists! \bar{\varepsilon} \text{ tel que } \varepsilon = \bar{\varepsilon} \circ \pi & \\ \overline{\det} & & GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p) & & \end{array}$$

Or $\det$ étant surjectif, de noyau $SL_n(\mathbb{F}_p)$, il se factorise de manière unique en un isomorphisme $\overline{\det} : GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p) \longrightarrow \mathbb{F}_p^\times$ i.e $\det = \overline{\det} \circ \pi$.

On a alors $\varepsilon = \bar{\varepsilon} \circ \pi = \underbrace{\bar{\varepsilon} \circ \overline{\det}^{-1}}_{=:\delta} \circ \underbrace{\overline{\det} \circ \pi}_{\det} = \delta \circ \det$ (δ est unique car $\overline{\det}$ l'est !)

On va montrer que $\delta = L$.

Déjà, le symbole de Legendre est un morphisme de groupes entre $\mathbb{F}_p^\times$ et $\{\pm 1\}$, non trivial car il existe des éléments de $\mathbb{F}_p^\times$ qui ne sont pas des carrés. En effet, l'ensemble des carrés de $\mathbb{F}_p^\times$ est l'image du morphisme $\psi : x \mapsto x^2$, donc d'après le premier théorème d'isomorphisme, il est de cardinal $\#\mathbb{F}_p^\times / \#\ker\psi = \frac{p-1}{2}$ car $\ker\psi = \{\pm 1\}$.

NB : pour $a \in \mathbb{F}_p^\times$, on a $L(a) = \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Réciproquement, comme $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ est cyclique, si g est un générateur de $\mathbb{F}_p^\times$ et si $\alpha : \mathbb{F}_p^\times \longrightarrow \{\pm 1\}$ est un morphisme de groupes, ce dernier est entièrement déterminé par l'image $\alpha(g)$ du générateur. Ainsi, si $\alpha(g) = 1$, α est le morphisme trivial, si $\alpha(g) = -1$, α est non trivial donc nécessairement $\alpha = L$

Autre méthode : par premier théorème d'isomorphisme, $\ker\alpha$ est un sous-groupe d'indice 2 de $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Or pour tout diviseur d de $p-1$, il existe un unique sous-groupe de $\mathbb{Z}/(p-1)\mathbb{Z}$ d'indice d. On note H l'unique sous-groupe de $\mathbb{F}_p^\times$ d'indice 2 et soit $x \in \mathbb{F}_p^\times - H$, alors $\mathbb{F}_p^\times = H \sqcup xH$ et on a $\alpha(g) = 1$ si $g \in H$, $\alpha(g) = -1$ sinon. α est ainsi entièrement déterminé et il existe au plus un morphisme non trivial entre $\mathbb{F}_p^\times$ et $\{\pm 1\}$, c'est le symbole de Legendre.

Il reste à montrer que δ est non trivial. Si δ est trivial, ε l'est aussi donc il suffit de trouver $u \in GL_n(\mathbb{F}_p)$ tel que $\varepsilon(u) = -1$.

Si $q = p^n$, comme $\mathbb{F}_p^n$ et $\mathbb{F}_q$ sont isomorphes en tant que $\mathbb{F}_p$-espaces vectoriels, cela revient à trouver une bijection $\mathbb{F}_p$-linéaire de $\mathbb{F}_q$ de signature -1.

Soit g un générateur du groupe cyclique $\mathbb{F}_q^\times$. On pose $u : x \in \mathbb{F}_q \mapsto gx \in \mathbb{F}_q$ qui est dans $GL(\mathbb{F}_q)$, et qui agit comme le $(q-1)$-cycle $(1, g, g^2, \dots, g^{q-2})$.

On a alors $\varepsilon(u) = (-1)^q = -1$ car $q = p^n$ est impair.

Conclusion : $\delta = L$ donc pour tout $u \in GL_n(\mathbb{F}_p)$, $\varepsilon(u) = L \circ \det(u) = \left(\frac{\det u}{p}\right)$.

Applications : • p premier impair, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ et $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

• avec la théorie de Galois, calcul de la signature du morphisme de Frobenius sur $\mathbb{F}_q$.