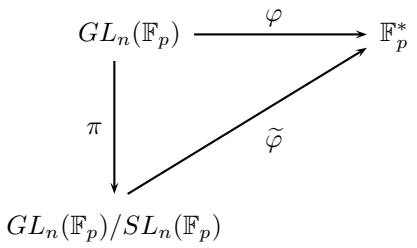
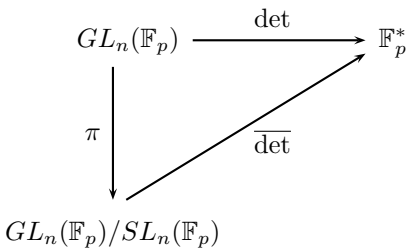
Développement : Théorème de Frobenius-Zolotarev

**Leçons** : 103, 105, 108, 120, 123, 152.

**Théorème.** *Soit $p \geq 3$, soit $u \in GL_n(\mathbb{F}_p)$. On note que $u$ définit ainsi un élément de $\mathcal{S}_{\mathbb{F}_p^n}$.*
*On a alors $\varepsilon(u) = \left(\dfrac{\det(u)}{p}\right)$ (symbole de Legendre, égal à 1 si $\det(u)$ carré dans $\mathbb{F}_p$, -1 sinon).*

*Démonstration.*
Étape 1 : Tout homomorphisme de $GL_n(\mathbb{F}_p)$ dans $\mathbb{F}_p^*$ se factorise par le déterminant.
Soit $\varphi : GL_n(\mathbb{F}_p) \to \mathbb{F}_p^*$. Comme $\mathbb{F}_p^*$ est abélien, $D(GL_n(\mathbb{F}_p)) = SL_n(\mathbb{F}_p)$ est inclus dans $\ker(\varphi)$, et il existe donc un unique morphisme $\widetilde{\varphi} : GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p) \to \mathbb{F}_p^*$ tel que $\varphi = \widetilde{\varphi} \circ \pi$. De plus, comme $\ker(\det) = SL_n(\mathbb{F}_p)$, il existe un unique morphisme $\overline{\det} : GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p) \to \mathbb{F}_p^*$ tel que $\det = \overline{\det} \circ \pi$, et c'est de plus un isomorphisme.




On pose $\delta = \widetilde{\varphi} \circ \overline{\det}^{-1}$. Alors $\varphi = \delta \circ \det$.
De plus, $\delta$ est unique : si $\varphi = \delta \circ \det = \delta' \circ \det$, soit $x \in \mathbb{F}_p^*$. Par surjectivité du déterminant, il existe $A \in GL_n(\mathbb{F}_p)$ tel que $\det(A) = x$. Alors $\delta(x) = \delta \circ \det(A) = \varphi(A) = \delta' \circ \det(A) = \delta'(x)$ et $\delta = \delta'$.

Étape 2 : Le symbole de Legendre est l'unique caractère non trivial de $\mathbb{F}_p^*$.
On a $\left(\dfrac{a}{p}\right) = a^{\frac{p-1}{2}}$, donc le symbole de Legendre est un morphisme de groupes, à valeurs dans $\{-1, 1\}$ car $\left(\dfrac{a}{p}\right)^2 = a^{p-1} = 1$ dans $\mathbb{F}_p$. Il est non trivial car il existe des éléments non carrés dans $\mathbb{F}_p^*$.
Si $\chi : \mathbb{F}_p^* \to \{-1, 1\}$ morphisme non trivial, alors par les théorèmes d'isomorphisme et de Lagrange, $\ker(\chi)$ sous-groupe d'indice 2 de $\mathbb{F}_p^*$. Or ce dernier est un groupe cyclique de cardinal pair. Or, pour $m \in \mathbb{N}$ et $d|m$, il existe un unique sous-groupe de $\mathbb{Z}/m\mathbb{Z}$ d'ordre $d$, il s'agit du sous-groupe engendré par $\frac{m}{d}$. $\mathbb{F}_p^*$ possède donc un unique sous-groupe $H$ d'indice 2. Ainsi il existe $x \in \mathbb{F}_p^*$ tel que $\mathbb{F}_p^* = H \sqcup xH$, et $H = \ker(\chi)$. Donc $\chi(H) = \{1\}, \chi(xH) = \{-1\}$ et $\chi$ est uniquement déterminé. Donc le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{-1, 1\}$.

Étape 3 : Il existe $v \in GL_n(\mathbb{F}_p)$ de signature $-1$.
$\mathbb{F}_{p^n}$ et $\mathbb{F}_p^n$ sont deux $\mathbb{F}_p$-espaces vectoriels de dimension $n$, ils sont donc isomorphes. Le groupe $\mathbb{F}_{p^n}^*$ est cyclique, soit $g$ un générateur de ce groupe. Soit $v : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, v : x \mapsto g \cdot x$. La décomposition de $v$ en cycles à supports disjoints est $v = (0)(g, g^2, \cdots, g^{p^n-1})$, ce dernier cycle étant de longueur $p^n - 1$ pair, donc $\varepsilon(v) = -1$. De plus, $v$ est clairement linéaire et inversible, $v \in GL_n(\mathbb{F}_p)$.

Étape 4 : Conclusion.
On a, d'après l'étape 1, $\varepsilon = \delta \circ \det$, avec $\delta : \mathbb{F}_p^* \to \{-1, 1\}$ morphisme de groupes. Comme $\varepsilon(v) = -1$, $\delta$ n'est pas le morphisme trivial, c'est donc le symbole de Legendre, et $\forall u, \varepsilon(u) = \left(\dfrac{\det(u)}{p}\right)$.

□

## Complément

**$SL_n(\mathbb{F}_p)$ est le groupe dérivé de $GL_n(\mathbb{F}_p)$**

$SL_n(\mathbb{F}_p)$ est engendré par les transvections (les automorphismes $u$ tels que $u - Id$ soit de rang 1 et de carré nul). Soit $u$ une transvection, montrons que $u^2$ transvection. On a $(u - Id)^2 = 0 \Leftrightarrow u^2 - Id = 2(u - Id)$. Ainsi

$u^2 - Id$ est de carré nul. Et comme 2 inversible dans $\mathbb{F}_p$ (car $p \geq 3$), $u^2 - 1$ est de rang 1, donc $u^2$ est une transvection. Or deux transvections sont conjuguées : il existe $v \in GL_n(\mathbb{F}_p)$ tel que $u^2 = vuv^{-1}$ soit $u = vuv^{-1}u^{-1}$ et $u = [u, v] \in D(GL_n(\mathbb{F}_p))$.

## Références

V. Beck, J. Malick, G. Peyré, Objectif Agrégation, H&K, p. 251.