Théorème de Frobenius - Zolotarev

Réf:
- Objectif Agrégation, V. Beck.

Leçons: 103, 105, 123, 152, 106.

Théorème

Soient p un nombre premier impair et V un $\mathbb{F}_p$-espace vectoriel de dimension finie.

Alors pour tout $u \in GL(V)$ on a

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

Preuve:

Etape 1 : Factorisation de u.

Lemme 1 :

Soient $n \in \mathbb{N}^*$ et M un groupe abélien.

Alors tout morphisme de groupes $\varphi : GL_n(\mathbb{F}_p) \longrightarrow M$ se factorise par le déterminant de façon unique.

Preuve: comme p est impair, on a :

$$\mathcal{D}(GL_n(\mathbb{F}_p)) = SL_n(\mathbb{F}_p)$$

Comme M est abélien, par propriété du groupe dérivé il existe $\overline{\varphi} : \dfrac{GL_n(\mathbb{F}_p)}{SL_n(\mathbb{F}_p)} \longrightarrow M$ un morphisme de groupes tel que le diagramme suivant

$$\begin{array}{ccc} GL_n(\mathbb{F}_p) & \xrightarrow{\varphi} & M \\ \downarrow \pi & \nearrow \overline{\varphi} & \\ \dfrac{GL_n(\mathbb{F}_p)}{SL_n(\mathbb{F}_p)} & & \end{array}$$

soit commutatif.

où $\pi : GL_n(\mathbb{F}_p) \twoheadrightarrow \frac{GL_n(\mathbb{F}_p)}{SL_n(\mathbb{F}_p)}$ est le morphisme quotient.

Par ailleurs, comme det est surjectif de noyau $SL_n(\mathbb{F}_p)$, il existe un isomorphisme de groupes $\alpha : \mathbb{F}_p^\times \xrightarrow{\sim} \frac{GL_n(\mathbb{F}_p)}{SL_n(\mathbb{F}_p)}$ tel que le diagramme

$$\begin{array}{ccc} GL_n(\mathbb{F}_p) & \xrightarrow{\det} & \mathbb{F}_p^\times \\ \downarrow \pi & \swarrow_{\alpha} & \\ \frac{GL_n(\mathbb{F}_p)}{SL_n(\mathbb{F}_p)} & & \end{array}$$

soit commutatif.

On considère alors la composée $\bar{\varphi} \circ \alpha \circ \det$ et on montre qu'elle est égale à φ.

C'est rapide : on a $\bar{\varphi} \circ \alpha \circ \det = \bar{\varphi} \circ \pi = \varphi$ par commutativité des diagrammes.

L'unicité découle du caractère surjectif du déterminant. ■

Etape 2 : le symbole de Legendre est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^\times$ dans $\{-1, 1\}$.

En effet, c'est bien un morphisme non trivial car il existe des éléments de $\mathbb{F}_p^\times$ qui ne sont pas des carrés ($\frac{(p-1)}{2}$)

Réciproquement, soit $\alpha : \mathbb{F}_p^\times \longrightarrow \{-1, 1\}$ un morphisme non trivial. Alors on a $\mathrm{Ker}(\alpha) \neq \mathbb{F}_p^\times$ donc comme $\#\mathbb{F}_p^\times = p-1 \geq 2$ il existe un isomorphisme

$$\frac{\mathbb{F}_p^\times}{\mathrm{Ker}(\alpha)} \simeq \{-1, 1\} \qquad \#\mathrm{Ker}(\alpha) = \frac{p-1}{2}.$$

c-à-d $\mathrm{Ker}(\alpha)$ est d'indice 2 dans $\mathbb{F}_p^\times$. Comme $\mathbb{F}_p^\times$ est cyclique, il admet un seul sous-groupe H d'ordre $\frac{p-1}{2}$.

Alors on a $\mathrm{Ker}(\alpha) = H$, ce qui détermine entièrement α.

Etape 3 :

Considérons $\varepsilon : GL(V) \longrightarrow \{-1,1\}$ le morphisme signature de $\mathfrak{S}_V$ restreint à $GL(V)$

Comme $\{-1,1\}$ est un groupe abélien, l'étape 1. assure l'existence d'un morphisme $\delta : \mathbb{F}_p^\times \longrightarrow \{1,-1\}$ tel que

$$\varepsilon = \delta \circ \det$$

L'étape 2 assure ensuite qu'il suffit de montrer qu'il existe $u \in GL(V)$ tel que $\varepsilon(u) = -1$ pour conclure. (δ n'est pas trivial alors, donc est le symbole de Legendre)

Notons n la dimension de V sur $\mathbb{F}_p$. Alors V et $\mathbb{F}_{p^n}$ sont isomorphes

Le groupe $\mathbb{F}_{p^n}^\times$ est cyclique. Soit g un de ces générateurs.

La permutation $x \longmapsto gx$ est alors le cycle

$$(g, g^2, \dots, g^{p^n-1})$$

de longueur p^n-1. Sa signature est donc $(-1)^{p^n} = -1$ car p est impair. De plus, la permutation $x \longmapsto gx$ est linéaire.

Cela conclut ∎