

Théorème de Frobenius - Zolotarev

Ref:
- 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: voir

Etape 1: factorisation de u .

Lemme 1:

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

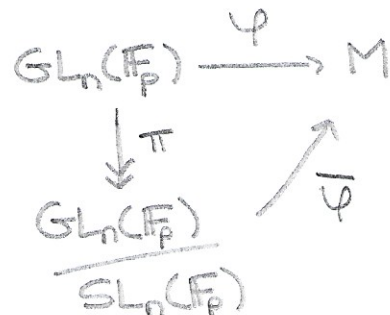
Alors tout morphisme de groupes $\psi: GL_n(\mathbb{F}_p) \rightarrow M$ se factorise par le déterminant de façon unique.

Preuve: comme p est impair, on a :

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

Comme M est abélien, par propriété du groupe dérivé il existe $\bar{\psi}: \frac{GL_n(\mathbb{F}_p)}{SL_n(\mathbb{F}_p)} \rightarrow M$ un morphisme de groupes

tel que le diagramme suivant



soit commutatif.

où $\pi : GL_n(\mathbb{F}_p) \longrightarrow \frac{GL_n(\mathbb{F}_p)}{SL_n(\mathbb{F}_p)}$ est le morphisme quotient. 2

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 $\left(\frac{p-1}{2}\right)$

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

$$\frac{\mathbb{F}_p^\times}{\text{Ker}(\alpha)} \simeq \{-1, 1\} \quad \nearrow \quad \#\text{Ker}(\alpha) = \frac{p-1}{2}$$

c-à-d $\text{Ker}(\alpha)$ 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 $\text{Ker}(\alpha) = H$, ce qui détermine entièrement α .

Etape 3 :

3

Considérons $\varepsilon : GL(V) \rightarrow \{-1, 1\}$ le morphisme signature de \mathcal{G}_V restreint à $GL(V)$.

Comme $\{-1, 1\}$ est un groupe abélien, l'étape 1 assure l'existence d'un morphisme $\delta : \mathbb{F}_p^\times \rightarrow \{-1, 1\}$ 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 δ 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 $x \mapsto gx$ est alors le cycle

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

de longueur $p^n - 1$. Sa signature est donc $(-1)^{p^n-1} = -1$

car p est impair. De plus, la permutation $x \mapsto gx$ est linéaire.

Cela conclut ■