Théorème de Frobenius-Zolotarev

Clarence Kineider

Leçons : 104, 105, 108, 120, 123, 152

Référence(s) : Beck, Malick, Peyré, *Objectif Agrégation.*

Je rappelle la définition du symbole de Legendre.

Définition : Soit q premier, $p \in \mathbf{Z}$. On définit le symbole de Legendre de p sur q par :

$$\left(\frac{p}{q}\right) = \begin{cases} 1 \text{ si } \overline{p} \text{ est un carré dans } \mathbf{F}_q^* \\ -1 \text{ si } \overline{p} \text{ est un carré dans } \mathbf{F}_q^* \\ 0 \text{ si } \overline{p} = 0 \text{ dans } \mathbf{F}_q \end{cases}$$

Théorème : Soit p premier impair, $u \in GL_n(\mathbf{F}_p)$ identifié à la permutation de $\mathbf{F}_p^n$ correspondante. Alors sa signature est $\epsilon(u) = \left(\frac{det(u)}{p}\right)$.

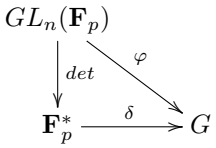
On coupe le résultat en 2 lemmes. On fixe p premier impair pour toute la suite.

Lemme : Le morphisme $\left(\frac{\cdot}{p}\right)$ est l'unique morphisme de groupe non trivial de $\mathbf{F}_p^*$ dans $\{\pm 1\}$.

Démonstration : Le groupe $\mathbf{F}_p^*$ est cyclique, donc un morphisme de $\mathbf{F}_p^*$ dans $\{\pm 1\}$ est entièrement déterminé par l'image d'un de ses générateurs. Il y a donc un unique morphisme non trivial de $\mathbf{F}_p^*$ dans $\{\pm 1\}$. Or $\left(\frac{\cdot}{p}\right)$ est non trivial, car $\begin{array}{ccc} \mathbf{F}_p^* & \to & \mathbf{F}_p^* \\ x & \mapsto & x^2 \end{array}$ est non injectif donc non surjectif. □

Lemme : Soit G un groupe abélien et $\varphi : GL_n(\mathbf{F}_p) \to G$ un morphisme. Alors il existe $\delta : \mathbf{F}_p^* \to G$ tel que $\varphi = \delta \circ det$.

Remarque 1 :
En termes savants, on cherche un δ qui rend le diagramme suivant commutatif :



Démonstration : Puisque G est abélien, $SL_n(\mathbf{F}_p) = \mathcal{D}(GL_n(\mathbf{F}_p)) \subset Ker(\varphi)$.
Donc il existe $\overline{\varphi} : GL_n(\mathbf{F}_p)/SL_n(\mathbf{F}_p) \to G$ tel que $\varphi = \overline{\varphi} \circ \pi$, où $\pi : GL_n(\mathbf{F}_p) \to GL_n(\mathbf{F}_p)/SL_n(\mathbf{F}_p)$ est la projection canonique. Or $\overline{det} : GL_n(\mathbf{F}_p)/SL_n(\mathbf{F}_p) \to \mathbf{F}_p^*$ est un isomorphisme (par le premier théorème d'isomorphisme) tel que $det = \overline{det} \circ \pi$. En posant $\delta = \overline{\varphi} \circ \overline{det}^{-1}$, on a $\varphi = \delta \circ det$. □

Démonstration du théorème : On applique le deuxième lemme à $\epsilon : GL_n(\mathbf{F}_p) \to \{\pm 1\}$ (où $GL_n(\mathbf{F}_p)$ est vu comme un sous groupe de $\mathfrak{S}(\mathbf{F}_p^n)$). Il existe donc $\delta : \mathbf{F}_p^* \to \{\pm 1\}$ tel que $\epsilon = \delta \circ det$. Il suffit de montrer que δ est non trivial (donc que ϵ est non trivial), et on aura le résultat grâce au premier lemme. Pour cela, il suffit de trouver un élément de $GL_n(\mathbf{F}_p)$ qui est un $(p^n - 1)$-cycle. On identifie $\mathbf{F}_p^n$ et $\mathbf{F}_{p^n}$. Le groupe $\mathbf{F}_{p^n}^*$ est cyclique, d'ordre $p^n - 1$. Soit g un de ses générateurs. Alors $(u : x \mapsto gx) \in GL_n(\mathbf{F}_p)$ est un $(p^n - 1)$-cycle. Or p est impair, donc $\epsilon(u) = -1$, ce qui conclut la démonstration. □

Remarque 2 :
Parmi les applications classiques de ce résultat, il y a le calcul de la signature du morphisme de Frobenius et le calcul de $\left(\frac{2}{p}\right)$.