10 Théorème de Frobenius-Zolotarev

Théorème (Frobenius-Zolotarev). *Soit p un nombre premier $\geqslant 3$ et V un espace vectoriel de dimension finie n sur $\mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de* Legendre, *qui est égal à 1 si a est un carré dans $\mathbb{F}_p$ et -1 sinon.*
Soit $u \in GL(V)$. Si $\varepsilon(u)$ désigne la signature de u en tant qu'élément de $\mathfrak{S}_{p^n}$, alors $\varepsilon(u) = \left(\frac{det\ u}{p}\right)$.

Preuve.

$\mathrm{GL}(V)$ est un sous-groupe de $\mathfrak{S}_{p^n}$ donc la signature induit un morphisme de groupes encore noté $\varepsilon : \mathrm{GL}(V) \to \{\pm 1\}$ (par restriction). Le groupe $\{\pm 1\}$ étant commutatif, ε se factorise de manière unique selon le diagramme

$$\begin{array}{ccc} \mathrm{GL}(V) & \xrightarrow{\ \varepsilon\ } & \{\pm 1\} \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \bar{\varepsilon}} & \\ \mathrm{GL}(V)/D(\mathrm{GL}(V)) & & \end{array}$$

Or on rappelle que $D(\mathrm{GL}(V)) = \mathrm{SL}(V)$ (ici $p \geqslant 3$). En effet, il est clair d'une part que $D(\mathrm{GL}(V)) \subset \mathrm{SL}(V)$. Pour l'inclusion inverse, il suffit de montrer que toute transvection est un commutateur, $\mathrm{SL}(V)$ étant engendré par les transvections (ainsi que le montre l'algorithme du pivot de Gauss). Soit donc une transvection $u \in \mathrm{GL}(V)$. Comme $\mathrm{car}(\mathbb{F}_p) \neq 2$, u^2 est également une transvection. Or toutes les transvections du groupe linéaire d'un espace de dimension finie sont conjuguées : dans une base convenable, la matrice d'une transvection est $\begin{bmatrix} 1 & & \dots & 0 \\ & \ddots & & \vdots \\ \vdots & & 1 & 1 \\ 0 & \dots & & 1 \end{bmatrix}$ (c'est d'ailleurs leur forme réduite de Jordan). Il existe donc $v \in \mathrm{GL}(V)$ tel que $u^2 = vuv^{-1}$, soit encore $u = vuv^{-1}u^{-1}$: u est un commutateur.

Par ailleurs, le morphisme surjectif $\det : \mathrm{GL}(V) \to \mathbb{F}_p^*$ a pour noyau $\mathrm{SL}(V)$ (par définition), il se factorise donc de manière unique en un isomorphisme que nous noterons $\overline{\det} : \mathrm{GL}(V)/\mathrm{SL}(V) \to \mathbb{F}_p^*$ de sorte que l'on a le diagramme :

$$\begin{array}{ccccc} & & \mathrm{GL}(V) & \xrightarrow{\ \varepsilon\ } & \{\pm 1\} \\ & \swarrow{\scriptstyle \det} & \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \bar{\varepsilon}} & \\ \mathbb{F}_p^* & \xleftarrow[\overline{\det}]{} & \mathrm{GL}(V)/\mathrm{SL}(V) & & \end{array}$$

On obtient donc un morphisme $\delta : \mathbb{F}_p^* \to \{\pm 1\}$ tel que $\delta \circ \det = \varepsilon$. Le but est de montrer qu'il s'agit en fait du morphisme (symbole) de LEGENDRE.

Nous allons voir dans un premier temps que δ n'est pas le morphisme trivial ; il nous suffit d'exhiber $u \in \mathrm{GL}(V)$ tel que $\varepsilon(u) = \delta(\det u) = -1$. Pour cela on se souvient que V est isomorphe à $\mathbb{F}_q$ (en tant que $\mathbb{F}_p$-espace vectoriel), où $q = p^n$. Nous admettrons ici que le groupe multiplicatif d'un corps fini est cyclique, soit donc ω un générateur de $\mathbb{F}_q^*$. La multiplication par ω dans $\mathbb{F}_q$ est $\mathbb{F}_p$-linéaire, c'est donc un élément u de $\mathrm{GL}(V)$. De plus u est égal en tant que permutation au cycle $(1, w, w^2, ..., w^{q-2})$ qui est de longueur paire $q-1$, d'où $\varepsilon(u) = -1$, ce qu'on voulait.

Pour conclure, on montre qu'il n'existe qu'un morphisme de groupes non trivial de $\mathbb{F}_p^*$ vers $\{\pm 1\}$. On sait que le symbole de LEGENDRE et δ sont de tels morphismes. Mais $\mathbb{F}_p^*$ étant cyclique, tout morphisme $\mathbb{F}_p^* \to \{\pm 1\}$ est défini de manière unique (et bien défini) par l'image d'un générateur. Il en y a donc exactement deux : le morphisme trivial et celui qui envoie un générateur donné sur -1. On en déduit que δ est bien le symbole de Legendre, d'où $\forall u \in \mathrm{GL}(V)\ \varepsilon(u) = \delta \circ \det(u) = \left(\frac{\det u}{p}\right)$, ce qui termine la démonstration. □

Leçons possibles
101 Groupe opérant sur un ensemble. Exemples et applications.
103 Exemples de sous-groupes distingués et de groupes quotients. Applications.
104 Groupes finis. Exemples et applications.
105 Groupe des permutations d'un ensemble fini. Applications.
106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.
108 Exemples de parties génératrices d'un groupe.
110 Nombres premiers. Applications.
112 Corps finis. Applications.

Références
[BMP05] pp. 251-252 Exercice 5.4.
[Per96] pp. 96 et suivantes sur les transvections.