Théorème de Frobenius-Zolotarev

Références : Beck, Malick, Peyré, *Objectif Agrégation*, p.251

Théorème (Frobenius-Zolotarev)**.**

Soient p un nombre premier impair et $n \in \mathbb{N}^*$. On a alors :

$$\forall u \in \mathrm{GL}_n(\mathbb{F}_p),\ \varepsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où ε désigne la signature de u vu comme permutation de l'ensemble $\mathbb{F}_p^n$.[a]

[a] Celle-ci est bien définie car $\mathrm{GL}_n(\mathbb{F}_p) \hookrightarrow \mathcal{S}(\mathbb{F}_p^n) \simeq \mathcal{S}_{p^n} \simeq \mathcal{S}(\mathbb{F}_{p^n})$ et ε est un morphisme de groupes donc n'est pas affecté par le choix des isomorphismes précédents.

On rappelle la définition du symbole de Legendre. Soit p un nombre premier et a un entier quelconque, alors on a :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si} & a \equiv 0[p] \\ 1 & \text{si} & a \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} & \end{cases} .$$

Le but de la démonstration est de factoriser la signature. Nous allons faire cela en deux étapes.

Lemme.

Soient $\mathbb{K}$ un corps et M un groupe abélien (on suppose que $\mathbb{K} \neq \mathbb{F}_2$ ou bien que $n > 2$). Pour tout morphisme $\varphi : \mathrm{GL}_n(\mathbb{K}) \to M$, il existe un unique morphisme $\delta : \mathbb{K}^* \to M$ tel que l'on ait : $\varphi = \delta \circ \det$.

Démonstration. Puisque $\mathbb{K} \neq \mathbb{F}_2$, on a : $D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$. Pour tout x, y dans $\mathrm{GL}_n(\mathbb{K})$, on a :

$$\varphi([x,y]) = [\varphi(x), \varphi(y)] = e \quad ,$$

car M est un groupe abélien. Ainsi tous les commutateurs de $\mathrm{GL}_n(\mathbb{K})$ sont dans le noyau de φ. Or les commutateurs engendrent le groupe dérivé. Ainsi le groupe dérivé de $\mathrm{GL}_n(\mathbb{K})$ est inclus dans le noyau de φ. D'après la propriété universelle du quotient, il existe un unique morphisme $\overline{\varphi}$ qui rend le diagramme suivant commutatif.

$$\begin{tikzcd}
\mathrm{GL}_n(\mathbb{K}) \arrow[r, "\varphi"] \arrow[d] & M \\
\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K}) \arrow[ur, dotted, "\overline{\varphi}"'] &
\end{tikzcd}$$

De plus le noyau du morphisme $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ est exactement $\mathrm{SL}_n(\mathbb{K})$. D'après la propriété universelle et le premier théorème d'isomorphisme, il existe un unique isomorphisme $\overline{\det}$ qui fasse commuter le diagramme suivant :

$$\begin{tikzcd}
\mathbb{K}^* & \mathrm{GL}_n(\mathbb{K}) \arrow[l, "\det"'] \arrow[r, "\varphi"] \arrow[d] & M \\
& \mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K}) \arrow[ul, dotted, "\overline{\det}"] \arrow[ur, dotted, "\overline{\varphi}"'] &
\end{tikzcd}$$

On pose $\delta = \overline{\varphi} \circ \overline{\det}^{-1}$. On obtient l'égalité voulue.

Pour l'unicité, on sait que le déterminant est surjectif, donc toute l'image de δ est fixée par φ. $\square$

Dans notre cas, pour M on a le groupe $\{\pm 1\}$ qui est abélien. On dispose donc d'un unique morphisme δ tel que l'on ait : $\varepsilon = \delta \circ \det$. Il faut à présent montrer que δ est le symbole de Legendre.

Lemme.

Soit p un nombre premier impair. Le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{\pm 1\}$.

Démonstration. Le symbole de Legendre est bien un morphisme de groupe entre $\mathbb{K}^*$ et $\{\pm 1\}$. En effet, pour $a \in \mathbb{F}_p^*$, on a $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. De plus, ce n'est pas un morphisme trivial. En effet, l'ensemble des carrés de $\mathbb{F}_p^*$ est égal à l'image du morphisme $\psi : x \in \mathbb{K}^* \mapsto x^2$. Le noyau de ce morphisme est $\{\pm 1\}$ et donc d'après le premier théorème d'isomorphisme, il n'y a que $\dfrac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$.

Réciproquement, soit $\alpha : \mathbb{F}_p^* \to \{\pm 1\}$ un morphisme non trivial. D'après le premier théorème d'isomorphisme, le noyau de α est un sous-groupe d'indice 2 de $\mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Or pour tout diviseur d de $p-1$ il existe un unique sous-groupe de $\mathbb{Z}/(p-1)\mathbb{Z}$ d'indice d [1] . On note H cet unique sous-groupe d'indice 2. Soit x un élément de $\mathbb{F}_p^* \backslash H$. On a alors la partition suivante : $\mathbb{F}_p^* = H \bigsqcup xH$. On a alors :

$$\alpha(g) = \begin{cases} 1 & \text{si } g \in H \\ -1 & \text{sinon} \end{cases}$$

Le morphisme α est donc entièrement déterminé. Il existe donc au plus un morphisme non trivial entre $\mathbb{F}_p^*$ et $\{\pm 1\}$, c'est le symbole de Legendre. □

Pour conclure il faut encore montrer que δ est non trivial. Pour cela il suffit d'exhiber un automorphisme dans $\mathrm{GL}_n(\mathbb{F}_p)$ de signature -1. En temps que $\mathbb{F}_p$-espaces vectoriel, $\mathbb{F}_p^n$ et $\mathbb{F}_{p^n}$ sont isomorphes. Il suffit donc de trouver une bijection $\mathbb{F}_p$-linéaire de $\mathbb{F}_{p^n}$ de signature -1. Soit g un générateur du groupe cyclique $\mathbb{F}_{p^n}^*$. La permutation $x \mapsto gx$ agit comme le (p^n-1)-cycle $(g, g^2, \dots, g^{p^n-1})$. Cette permutation est de signature -1 car $p^n - 1$ est pair. Ce qui achève la démonstration.

Corollaire.

Soit p un nombre premier impair, on a : $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ et $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Démonstration. On définit l'isomorphisme u suivant :

$$u : \begin{array}{ccc} \mathbb{F}_p & \to & \mathbb{F}_p \\ x & \mapsto & 2x \end{array}$$

Son déterminant est égal à 2. Il ne reste plus qu'à calculer la signature de la permutation engendrée. Pour cela il suffit de compter le nombre d'inversion. [2]

x	0	1	2	$\dots$	$\frac{p-1}{2}$	$\frac{p+1}{2}$	$\dots$	$p-2$	$p-1$
$u(x)$	0	2	4	$\dots$	$p-1$	1	$\dots$	$p-4$	$p-2$

On remarque qu'il n'y a pas d'inversion entre deux éléments inférieurs à $\dfrac{p-1}{2}$ ou supérieurs à $\dfrac{p+1}{2}$. Soit $k \geqslant \dfrac{p+1}{2}$, k voit sa position relative à $p-k$ éléments inversée par u. Le nombre d'inversions est donc

$$\sum_{k=\frac{p+1}{2}}^{p-1} p-k = \sum_{l=0}^{\frac{p-1}{2}} l = \frac{p^2-1}{8} \quad .$$

1. Car il existe un unique sous groupe d'ordre $\dfrac{n}{d}$, voir Calais, p.100
2. En effet, c'est clair au vu de la définition : $\varepsilon(u) = \prod_{i \neq j} \dfrac{u(j)-u(i)}{j-i} \in \{\pm 1\}$.

En appliquant le théorème de Frobenius-Zolotarev, on obtient donc le résultat.

Pour le deuxième résultat du théorème, on peut faire le même raisonnement avec $u : x \mapsto -x$. On peut alors soit compter le nombre d'inversions (en bidouillant un peu), soit se rendre compte que cette application s'écrit comme un produit de $\dfrac{p-1}{2}$ transpositions. $\square$

Remarques : • Dans le Objectif agrégation, ils prennent $n > 2$, mais comme p est choisi impair, on peut prendre $n \geqslant 1$, ce qui nous autorise à utiliser Frobenius-Zolotarev dans le corollaire.
• Montrons que $D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$ pour $\mathbb{K}$ un corps à au moins 3 éléments et $n \geqslant 2$. (FGNal2)
On note $D_i(a)$ la matrice de dilatation avec comme coefficient a sur la i-ème ligne de la diagonale. $T_{i,j}(b)$ est la transvection de coefficient b.
Par des calculs, on remarque que
$$[D_i(a), T_{i,j}(b)] = T_{i,j}((a-1)b).$$
Comme $(a-1)b$ parcourt $\mathbb{K}$ si a est différent de 0 et 1 (d'où la nécessité d'avoir au moins trois éléments dans le corps), toute transvection est un commutateur.
$\mathrm{SL}_n(\mathbb{K})$ est engendré par les transvections donc cela termine la preuve.
Remarquons que ce résultat est aussi vrai pour $\mathbb{K} = \mathbb{F}_2$ et $n \geqslant 3$.
• Une autre application consiste à calculer la signature du morphisme de Frobenius F sur $\mathbb{F}_q$.
On sait que F est d'ordre n. La théorie de Galois donne l'existence d'un élément x de $\mathbb{F}_q$ tel que $(x, F(x), ..., F^{n-1}(x))$ forme une base de $\mathbb{F}_q$. La matrice de F dans cette base est une simple matrice de permutation dont le déterminant est $(-1)^{n+1}$.
Le théorème de Frobenius Zolotarev donne alors, en sachant que $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,
$$\varepsilon(F) = \left(\frac{(-1)^{n+1}}{p}\right) = (-1)^{\frac{(p-1)(n+1)}{2}}.$$

Adapté du travail de Baptiste Huguet et complété par les recherches de Mario Goncalves Lamas et Anne-Elisabeth Falq.