Théorème de Frobenius-Zolotarev

V. Beck, J. Malick, G. Peyré, *Objectif agrégation*, 2e édition, H&K. Exercice 5.4 page 251.

Recasage : 103, 105, 106, 108, 120, 123, 152.

Théorème 1

Soient p un nombre premier impair et V un $\mathbb{F}_p$-espace vectoriel de dimension finie $n \in \mathbb{N}$. Pour tout $u \in \mathrm{GL}(V)$,

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

où, $\varepsilon(u)$ désigne la signature de u vu comme permutation de V et, pour $a \in \mathbb{F}_p$, le symbole de Legendre est défini par

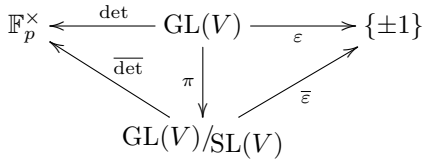
$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a = 0 \text{ mod } p \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon.} \end{cases}$$

▷ La restriction de la signature, $\varepsilon : \mathrm{GL}(V) \subset \mathfrak{S}(V) \to \{\pm 1\}$, toujours notée ε, est un morphisme de groupes.

– *Étape 1 : Montrons qu'il se factorise par le déterminant.* Comme $p > 2$, le groupe dérivé $D\,\mathrm{GL}(V)$ est $\mathrm{SL}(V)$. De plus, pour $u, v \in \mathrm{GL}(V)$,

$$\varepsilon(uvu^{-1}v^{-1}) = \varepsilon(u)\varepsilon(v)\varepsilon(u)^{-1}\varepsilon(v)^{-1} = 1$$

donc $\mathrm{SL}(V) = \langle uvu^{-1}v^{-1}, u, v \in \mathrm{GL}(V)\rangle \subset \operatorname{Ker}\varepsilon$. D'après la propriété universelle du quotient, ε se factorise par un unique morphisme $\overline{\varepsilon}$ de sorte que $\varepsilon = \overline{\varepsilon} \circ \pi$ où $\pi : \mathrm{GL}(V) \to \mathrm{GL}(V)/\mathrm{SL}(V)$ est la projection canonique. De plus, $\det : \mathrm{GL}(V) \twoheadrightarrow \mathbb{F}_p^\times$ a pour noyau $\mathrm{SL}(V)$. Il existe donc un unique isomorphisme $\overline{\det}$ tel que le diagramme suivant est commutatif :



Posons $\delta = \overline{\varepsilon} \circ \overline{\det}^{-1}$ de sorte que δ est un morphisme de groupes $\mathbb{F}_p^\times \to \{\pm 1\}$ et $\varepsilon = \delta \circ \det$. (Par surjectivité de det, un tel δ est unique)

– *Étape 2 : Montrons que δ n'est pas le morphisme trivial.* Comme V et $\mathbb{F}_{p^n}$ sont isomorphes comme espaces vectoriels, il suffit de trouver une bijection $\mathbb{F}_p$-linéaire de $\mathbb{F}_{p^n}$ sur lui-même de signature -1.

$\mathbb{F}_{p^n}^\times$ est cyclique de cardinal $p^n - 1$. Soit g un générateur. L'application $\tau_g : x \in \mathbb{F}_{p^n} \mapsto gx \in \mathbb{F}_{p^n}$ est bien une bijection $\mathbb{F}_p$-linéaire de $\mathbb{F}_{p^n}$ sur lui-même et agit sur $\mathbb{F}_{p^n}^\times$ comme le (p^n-1)-cycle $(g, g^2, \ldots, g^{p^n-1})$, donc sa signature est -1 car $p^n - 1$ est pair.

– *Étape 3 : Montrons que δ est le symbole de Legendre.*

Analyse : Comme $\delta \not\equiv 1$, $\operatorname{Ker}\delta$ est un sous-groupe de $\mathbb{F}_p^\times$ d'indice 2. Or il existe un unique sous-groupe H d'indice 2 dans $\mathbb{F}_p^\times$. Alors, si $x \notin H$, on a une partition $\mathbb{F}_p^\times = H \sqcup xH$ et $\delta(y) = 1$ si $y \in H$ et $\delta(y) = 0$ si $y \in xH$. δ est donc déterminé de façon unique. Il y a donc au plus un morphisme non trivial $\mathbb{F}_p^\times \to \{\pm 1\}$.

Synthèse : le symbole de Legendre est bien un morphisme de groupes car pour $a \in \mathbb{F}_p^\times$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. Il est non trivial car il y a exactement $\dfrac{p-1}{2}$ carrés dans $\mathbb{F}_p^\times$. □

Application au morphisme de Frobenius : Soit $n \geq 2$. On rappelle que le morphisme de Frobenius est défini par :

$$\varphi : \begin{array}{ccc} \mathbb{F}_{p^n} & \to & \mathbb{F}_{p^n} \\ x & \mapsto & x^p. \end{array}$$

φ est d'ordre n. En effet, pour tout $x \in \mathbb{F}_{p^n}$,

$$\varphi^n(x) = x^{p^n} = x$$

donc $\varphi^n = \mathrm{Id}_{\mathbb{F}_{p^n}}$. Si $m \leq n$ et $\varphi^m = \mathrm{Id}_{\mathbb{F}_{p^n}}$ alors $X^{p^m} - X$ est non nul et a $|\mathbb{F}_{p^n}| = p^n$ racines sur le corps $\mathbb{F}_{p^n}$, donc $m = n$.

On admet[1] qu'il existe une base adaptée à φ : il existe $x \in \mathbb{F}_{p^n}$ tel que $\mathcal{B} = (x, \varphi(x), \dots, \varphi^{n-1}(x))$ forme une base du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_{p^n}$. On a :

$$\mathrm{Mat}_{\mathcal{B}}(\varphi) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

qui est la matrice de permutation associée au n-cycle $\sigma \in \mathfrak{S}_n$. Alors $\det(\varphi) = \varepsilon(\sigma) = (-1)^{n-1}$. D'après le théorème de Frobenius-Zolotarev,

$$\varepsilon(\varphi) = \left(\frac{(-1)^{n-1}}{p}\right) = \left(\frac{-1}{p}\right)^{n-1} = (-1)^{\frac{(p-1)(n-1)}{2}}.$$

Lemme 2

Si k est un corps de cardinal ≥ 3 et $n \geq 2$, alors le groupe dérivé $D\,\mathrm{GL}_n(k)$ de $\mathrm{GL}_n(k)$ est $\mathrm{SL}_n(k)$.

▷ Voir Oraux X-ENS algèbre 2.

Soit $A, B \in \mathrm{GL}_n(k)$. On a $\det(ABA^{-1}B^{-1}) = \det(A)\det(B)\det(A)^{-1}\det(B)^{-1} = 1$ donc $D\,\mathrm{GL}_n(k) \subset \mathrm{SL}_n(k)$.

$\mathrm{SL}_n(k)$ étant engendré par les matrices de transvections, il suffit de montrer que toute matrice de transvection est un commutateur. Pour $1 \leq i \neq j \leq n$ et $\lambda \in k$, on pose $T_{ij}(\lambda) = I_n + \lambda E_{ij}$. Soit $a \notin \{0, 1\}$ et $D_i(a)$ la matrice de dilation où a est à la position ii. Pour $b \in k$,

$$D_i(a)T_{ij}(b)D_i(a)^{-1} = D_i(a)(I_n + bE_{ij})D_i(a)^{-1} = I_n + abE_{ij} = T_{ij}(ab)$$

donc

$$D_i(a)T_{ij}(b)D_i(a)^{-1}T_{ij}(b)^{-1} = T_{ij}((a-1)b).$$

Lorsque b décrit k, le scalaire $(a-1)b$ décrit k. Donc toute matrice de transvection est un commutateur. Donc $\mathrm{SL}_n(k) \subset D\,\mathrm{GL}_n(k)$. □

1. Ma proposition : on a $\pi_\varphi | X^n - 1$ et, si $\deg(\pi_\varphi) < n$, on a $\pi_\varphi = X^m + a_{m-1}X^{m-1} + \cdots + a_0$ avec $a_i \in \mathbb{F}_p$. Alors, $\varphi^m + a_{m-1}\varphi^{m-1} + \cdots + a_0\mathrm{Id}_{\mathbb{F}_{p^n}} = 0$ donc la famille $(\mathrm{Id}_{\mathbb{F}_{p^n}}, \varphi, \dots, \varphi^m)$ est liée dans $\mathbb{F}^p$ donc dans $\mathbb{F}^{p^n}$ ce qui contredit le lemme de Dedekind (voir le développement qui lui est consacré). Donc $\pi_\varphi = X^n - 1$. Alors, il existe $x \in \mathbb{F}_{p^n}$ tel que $\pi_{\varphi,x} = \pi_\varphi$ c'est-à-dire tel que $(x, \varphi(x), \dots, \varphi^{n-1}(x))$ est une base.