

# Théorème de Frobenius-Zolotarev

Nous démontrons le théorème de Frobenius-Zolotarev qui permet de calculer la signature d'un endomorphisme d'un espace vectoriel sur un corps fini possédant au moins 3 éléments.

Soient  $p \geq 3$  un nombre premier et  $V$  un espace vectoriel sur  $\mathbb{F}_p$  de dimension finie.

**Définition 1.** Soit  $H$  un hyperplan de  $V$  et soit  $G$  une droite supplémentaire de  $H$  dans  $V$ . La dilatation  $u$  de base  $H$ , de direction  $G$ , et de rapport  $\lambda \in \mathbb{K}^*$  est l'unique endomorphisme de  $V$  défini par

$$\forall g \in G, \forall h \in H, u(g + h) = h + \lambda g$$

[I-P]  
p. 203

*Remarque 2.* On suppose connu le fait que les transvections et les dilatations engendrent  $GL(V)$ .

[PER]  
p. 99

**Lemme 3.** Soient  $u \in GL(V)$  et  $H$  un hyperplan de  $V$  tel que  $u|_H = \text{id}_H$ . Si  $\det(u) \neq 1$ , alors  $u$  est une dilatation.

p. 96

*Démonstration.* On note  $n = \dim(V)$ . Comme  $u|_H = \text{id}_H$  et  $\dim(H) = n - 1$ , on en déduit que 1 est valeur propre de multiplicité  $n - 1$  de  $u$  et que  $H$  est le sous-espace propre associé :

$$H = E_1(u) = \text{Ker}(u - \text{id}_V)$$

On pose  $\lambda = \det(u) \notin \{0, 1\}$ .  $\lambda$  est valeur propre de  $u$  (on peut le voir par exemple en calculant le polynôme caractéristique de  $u$ ) de multiplicité 1. Donc  $u$  est diagonalisable, et dans une base  $\mathcal{B}$  adaptée à la diagonalisation, on a :

$$\text{Mat}(u, \mathcal{B}) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & \lambda \end{pmatrix}$$

d'où le résultat. □

**Lemme 4.** Les dilatations engendrent  $GL(V)$ .

[I-P]  
p. 203

*Démonstration.* Pour obtenir le résultat, il suffit de montrer que toute transvection est la composée de deux dilatations (cf. Remarque 2). Soit  $u$  une transvection d'hyperplan  $H$ . Comme  $\mathbb{F}_p$  contient au moins 3 éléments, il existe alors  $v$  une dilatation d'hyperplan  $H$  et de rapport  $\lambda \neq 1$ .

Ainsi, l'application  $w = u \circ v$  est dans  $GL(V)$  et fixe  $H$ . Comme  $\det(w) = \det(v) = \lambda \neq 1$ , le Lemme 3 permet de conclure que  $w$  est une dilatation. Ainsi,  $u = w \circ v^{-1}$  est le produit de deux dilatations  $v^{-1}$  est une dilatation (toujours d'après le Lemme 3). □

**Notation 5.** Soit  $a \in \mathbb{F}_p$ . On note  $\left(\frac{a}{p}\right)$  le symbole de Legendre de  $a$  modulo  $p$ .

**Théorème 6** (Frobenius-Zolotarev).

$$\forall u \in \text{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où  $u$  est vu comme une permutation des éléments de  $V$ .

*Démonstration.* Le groupe multiplicatif d'un corps fini est cyclique, donc il existe  $a \in \mathbb{F}_p^*$  tel que

$$\mathbb{F}_p^* = \langle a \rangle$$

En conséquence, si  $u$  est la dilatation de  $V$  de base  $H$ , de direction  $G$ , et de rapport  $\lambda \in \mathbb{F}_p^*$ , alors il existe  $k \in \mathbb{N}^*$  tel que  $\lambda = a^k$ . On en déduit que si  $v$  est la dilatation de  $V$  de base  $H$ , de direction  $G$ , et de rapport  $a$ , alors  $\forall x \in V$  écrit  $x = g + h$  avec  $g \in G$  et  $h \in H$  :

$$v^k(x) = v^k(g + h) = h + a^k g = h + \lambda g = u(g + h) = u(x)$$

d'où  $v^k = u$ . Ainsi, toute dilatation est une puissance d'une dilatation de rapport  $a$ .

Comme  $\det$ ,  $\left(\frac{\cdot}{p}\right)$  et  $\epsilon$  sont tous trois des morphismes de groupes, et comme les dilatations engendrent  $\text{GL}(V)$  (cf. Lemme 4), il suffit de montrer le résultat pour les dilatations de rapport  $a$ .

Soit  $u$  une dilatation de base  $H$ , de direction  $G$ , et de rapport  $a$ . Supposons par l'absurde que  $\left(\frac{\det(u)}{p}\right) = 1$ . Comme  $\det(u) = a$ , on a  $\left(\frac{a}{p}\right) = 1$ . Mais,  $\mathbb{F}_p^* = \langle a \rangle$ , donc  $\forall x \in \mathbb{F}_p^*$ ,  $\left(\frac{x}{p}\right) = 1$  ie. tout élément de  $\mathbb{F}_p^*$  est un carré. Or, il y a  $\frac{p-1}{2}$  carrés dans  $\mathbb{F}_p^*$  (et  $|\mathbb{F}_p^*| = p-1$ , bien-sûr) : contradiction.

Il ne reste qu'à montrer que  $\epsilon(u) = -1$ . Pour cela, on va étudier les orbites des éléments  $V$  sous l'action de  $u$ .

Soit  $h \in H$ . On a  $u(h) = h$ , donc son orbite est réduite à  $\{h\}$  qui est de cardinal 1. Elle compte donc comme un + dans le signe de  $\epsilon(u)$ .

Soit maintenant  $x \in V$  écrit  $x = g + h$  avec  $g \in G \setminus \{0\}$  et  $h \in H$  de sorte que  $u^k(x) = h + a^k g$  pour tout  $k \in \mathbb{N}$ .

- $\mathbb{F}_p^*$  est cyclique d'ordre  $p-1$ , donc  $a^{p-1} = 1$ . Ainsi,  $u^{p-1}(x) = x$ .
- Supposons par l'absurde que  $\exists 1 \leq i < j \leq p-1$  tel que  $u^i(x) = u^j(x)$ . On a,

$$\begin{aligned} h + a^j g = h + a^i g &\iff a^{j-i}(a^i - 1) \underset{\neq 0}{g} = 0 \\ &\implies a^{j-i} = 0 \text{ ou } a^i = 1 \end{aligned}$$

ce qui est absurde dans les deux cas.

L'orbite de  $x$  sous l'action de  $u$  est donc  $\{x, \dots, u^{p-2}(x)\}$  qui est de cardinal  $p-1$  (pair) et compte donc comme un - dans le signe de  $\epsilon(u)$ .

Il ne reste qu'à compter le nombre d'orbites de cardinal  $p - 1$ . Les éléments contenus dans ces orbites forment exactement l'ensemble

$$\bigcup_{h \in H} \{g + h \mid g \in G, g \neq 0\}$$

et il y en a donc

$$|H| \times (|G| - 1) = p^{n-1}(p - 1)$$

(car  $H$  est un hyperplan et  $G$  est une droite). Comme ces orbites sont de cardinal  $p - 1$ , il y a donc exactement  $p^{n-1}$  orbites. Or,  $p^{n-1}$  est impair, donc  $\epsilon(u)$  est de signe négatif. Ainsi,  $\epsilon(u) = -1$ .  $\square$

# Bibliographie

## **L'oral à l'agrégation de mathématiques**

[I-P]

Lucas ISENMANN et Timothée PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2<sup>e</sup> éd. Ellipses, 26 mars 2024.

<https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html>.

## **Cours d'algèbre**

[PER]

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.

<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.