

Frobenius-Zolotarev

Développement très cool à faire, et qui est plutôt original. On y montre le théorème de Frobenius-Zolotarev et on donne deux applications possibles.

Malheureusement, ce n'est pas un développement qui se recase très bien, mais il a le mérite de se recaser dans des leçons où il m'a été difficile de trouver des développements sympatiques. Pour ma part, les seuls recasages acceptables sont en 105 et 106.

I - Le développement



Lemme 1

Soit K un corps et $n \in \mathbb{N}^*$ tels que $K \neq \mathbb{F}_2$ ou $n \neq 2$. Soit M un groupe abélien et $\varphi : GL_n(K) \rightarrow M$ un morphisme de groupes. Alors φ se factorise par le déterminant : il existe $\delta : K^\times \rightarrow M$ un morphisme de groupes tel que $\varphi = \delta \circ \det$.

Preuve :

Nous allons utiliser le fait que $D(GL_n(K)) = SL_n(K)$ (d'où les hypothèses sur K et n). On remarque que $SL_n(K) \subset \ker(\varphi)$. En effet, puisque M est abélien :

$$\forall x, y \in GL_n(K), \varphi([x, y]) = [\varphi(x), \varphi(y)] = 1_M.$$

On peut donc factoriser φ de la manière suivante :

$$\begin{array}{ccc} GL_n(K) & \xrightarrow{\varphi} & M \\ \pi \downarrow & \nearrow \overline{\varphi} & \\ GL_n(K)/SL_n(K) & & \end{array}$$

Cependant, $\det : GL_n(K) \rightarrow K^\times$ est surjectif, de noyau $SL_n(K)$, on peut donc aussi factoriser $\det$, ce qui fournit un isomorphisme :

$$\begin{array}{ccccc} K^\times & \xleftarrow{\det} & GL_n(K) & \xrightarrow{\varphi} & M \\ & \searrow \overline{\det} & \downarrow \pi & \nearrow \overline{\varphi} & \\ & & GL_n(K)/SL_n(K) & & \end{array}$$

Finalement, $\varphi = \overline{\varphi} \circ \pi = \overline{\varphi} \circ (\overline{\det}^{-1} \circ \det) = (\overline{\varphi} \circ \overline{\det}^{-1}) \circ \det$. L'unicité découle directement du fait que l'image de δ est donnée par l'image de φ .





Lemme 2

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

Preuve :

Le symbole de Legendre $\left(\frac{\cdot}{p}\right)$ est bien un morphisme, non trivial car il y a $\frac{p-1}{2} \neq p-1$ carrés (c'est ici qu'intervient l'hypothèse $p \neq 2$).

Soit maintenant $\alpha : \mathbb{F}_p^\times \rightarrow \{-1, 1\}$ un morphisme non trivial. Par le premier théorème d'isomorphisme,

$$\left| \frac{\mathbb{F}_p^\times}{\ker(\alpha)} \right| = |\text{Im}(\alpha)| = 2.$$

Ainsi, $|\ker(\alpha)| = \frac{p-1}{2}$. Mais il est facile de vérifier que les carrés sont dans $\ker(\alpha)$, et comme ils sont au nombre de $(p-1)/2$, il vient que le noyau de α est bien l'ensemble des carrés de $\mathbb{F}_p^\times$: c'est donc le symbole de Legendre.



Théorème 3

Soit $u \in \text{GL}_n(\mathbb{F}_p)$ vu comme une permutation. Alors $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$.

Preuve :

Par le premier lemme, on dispose de $\delta : \mathbb{F}_p^\times \rightarrow \{-1, 1\}$ tel que $\varepsilon = \delta \circ \det$. Il suffit maintenant de montrer que δ est non trivial pour appliquer le second lemme, et il suffit alors de montrer que ε est non trivial.

Posons $q = p^n$: $\mathbb{F}_q$ et $\mathbb{F}_p^n$ sont $\mathbb{F}_p$ -isomorphes. Par cyclicité de $\mathbb{F}_q^\times$, prenons x un de ses générateurs. Posons $v : y \rightarrow xy$, $\mathbb{F}_p$ -linéaire. v agit comme le cycle $(x, x^2, x^3, \dots, x^{q-1})$, de longueur $q-1$. Sa signature est donc $\varepsilon(v) = (-1)^q = -1$.



II - Deux applications



Propriété 4 2nd loi complémentaire

Soit p premier impair. Alors

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Preuve :

On considère

$$\begin{aligned} u: \mathbb{F}_p &\rightarrow \mathbb{F}_p \\ x &\mapsto 2x \end{aligned}$$

Son déterminant vaut 2. Calculons sa signature, et pour cela comptons le nombre d'inversions (c'est la formule $\varepsilon(u) = \prod_{i < j} \frac{u(i)-u(j)}{i-j}$ qui permet d'utiliser cette méthode).

Remarquons qu'en voyant u comme une permutation de $\llbracket 0, p-1 \rrbracket$, on a

$$\star u(x) = 2x \text{ si } x \in \left[0, \frac{p-1}{2}\right];$$

$$\star u(x) = 2x - p \text{ si } x \in \left[\frac{p+1}{2}, p-1\right].$$

Ainsi :

$$\star \text{ si } i, j \in \left[0, \frac{p-1}{2}\right], \text{ il n'y a pas d'inversion ;}$$

$$\star \text{ si } i, j \in \left[\frac{p+1}{2}, p-1\right], \text{ il n'y a pas d'inversion ;}$$

$$\star \text{ si } i \in \left[0, \frac{p-1}{2}\right], j \in \left[\frac{p+1}{2}, p-1\right], \text{ il y a inversion si et seulement si}$$

$$2i > 2j - p \quad \text{i.e.} \quad j < i + \frac{p}{2}, \quad \text{i.e.} \quad \frac{p+1}{2} \leq j \leq \frac{p-1}{2} + i.$$

Au final, on compte

$$\sum_{i=0}^{\frac{p-1}{2}} i = \frac{p^2 - 1}{8}$$

inversions.

Le théorème de Frobenius-Zolotarev permet de conclure.



✿ Propriété 5 Signature du Frobenius

Soit $\Phi: \mathbb{F}_q \rightarrow \mathbb{F}_q$, $q = p^n$, le morphisme de Frobenius. Alors :

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

Preuve :

On suppose connu le fait que $\pi_\Phi = X^n - X$. On remarque ainsi que $\pi_\Phi = \chi_\Phi$, et donc que Φ est cyclique. En particulier, dans une base adaptée :

$$\text{Mat}(\Phi) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \ddots & & 0 \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

d'où $\det() = (-1)^{n+1}$ (en développant par rapport à la première ligne).

Par Frobenius-Zolotarev :

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



III - Remarques

1 - Développement très sympa, mais qui est un peu rapide. N'hésitez pas à rajouter une des deux applications, pour ma part j'ai rajouté le calcul de la signature du Frobenius, la 2^{nd} loi complémentaire étant un peu trop longue à démontrer.

2 - Il faut à mon avis savoir démontrer que $D(\mathrm{GL}_n(K)) = \mathrm{SL}_n(K)$ au moins dans le cas $p \neq 2$ (c'est le cas qui nous intéresse réellement).

3 - On peut présenter plusieurs alternative à la démonstration du lemme 2. J'ai choisi la preuve la plus concise possible (qui m'avait été recommandée en oral blanc).

6 - J'ai utilisé dans les démonstrations des résultats plus ou moins connus de théorie des corps finis. Il faut bien évidemment les avoir en *teetsavoirunminimumlesjustifier*.

5 - On pourrait tout aussi bien démontrer la première loi complémentaire en étudiant le morphisme $u : x \rightarrow -x$.

6 - Historiquement, ce lemme a été utilisé pour démontrer d'une nouvelle manière la loi de réciprocité quadratique.

IV - Références

[Bec] : *Objectif agrégation*, Vincent Beck, Jérôme Malick, Gabriel Peyré

[Goz] : *Théorie de Galois*, Ivan Gozard