Signature et corps finis

www.h-k.fr/publications/objectif-agregation

Motivations.

L'objectif de cette note est de donner une expression de la signature du morphisme de Frobenius sur un corps fini. Le morphisme de Frobenius est une bijection (en fait un automorphisme de corps) sur un ensemble fini (en fait un corps fini). Quel est donc la signature de cette bijection ? Cette question a été posée à l'oral de l'agrégation en 2001. Cette note fait écho à celle de Daniel Ferrand

http ://agreg-maths.univ-rennes1.fr/documentation/docs/SignFrob.pdf

et celle de Stef Graillat

http ://gala.univ-perp.fr/~graillat/papers/SignFrob.pdf .

La réponse donnée par Stef Graillat utilise une généralisation du symbole de Legendre : le symbole de Zolotarev. Celle de Daniel Ferrand repose sur l'étude du problème suivant. À une bijection f sur un ensemble X, on peut associer de façon naturelle d'autres bijections, comment relier la signature de ces nouvelles bijections à celle de f ? Par exemple, on trouvera dans la note de Daniel Ferrand une expression de la signature de la bijection induite par f sur l'ensemble des parties de cardinal k de X en fonction de celle de f.

La démonstration proposée ici aboutit à une nouvelle expression. Elle est l'occasion d'appliquer les résultats de base sur les corps finis qu'il est indispensable d'avoir vu pendant son année d'agrégatif et que l'on trouvera dans la note « Corps finis » disponible en ligne

http ://www.h-k.fr/publications/objectif-agregation .

Notations.

Soient p un nombre premier, $m, n \in \mathbb{N}^*$ et $q = p^m$. On note $\mathbb{F}_{q^n}$ « le » corps fini à q^n éléments (voir [PER, III.2.5]) et on pose

$$\mathrm{F}: \begin{cases} \mathbb{F}_{q^n} & \longrightarrow \mathbb{F}_{q^n} \\ x & \longmapsto x^q \end{cases}$$

le m-ième itéré du morphisme de Frobenius de $\mathbb{F}_{q^n}$ (voir la note « Corps finis »). Pour les besoins de la preuve on introduit, pour $d \in \mathbb{N}$, l'ensemble

$$\mu_q(d) = \{\mathrm{P} \in \mathbb{F}_q[\mathrm{X}], \quad \mathrm{P} \text{ irréductible sur } \mathbb{F}_q \text{ unitaire de degré } d\}$$

et son cardinal $m_q(d) = |\mu_q(d)|$.

Prérequis.

La preuve présentée ici utilise les résultats suivants sur les corps finis (voir les lemmes 3, 4, 5 et 9 de la note « Corps finis »).

1. Pour tout $x \in \mathbb{F}_{q^n}$, on a $x^{q^n} = x$.
2. Soient $\mathrm{P} \in \mathbb{F}_q[\mathrm{X}]$, $x \in \mathbb{F}_{q^n}$ et $s \in \mathbb{N}$, alors $\mathrm{P}(x^{q^s}) = (\mathrm{P}(x))^{q^s}$.
3. L'ensemble des points fixes de F est le sous-corps $\mathbb{F}_q$ de $\mathbb{F}_{q^n}$, autrement dit
$$\{x \in \mathbb{F}_{q^n}, \quad x^q = x\} \; = \; \mathbb{F}_q.$$
4. Sur $\mathbb{F}_q$, la décomposition de $\mathrm{X}^{q^n} - \mathrm{X}$ en polynômes irréductibles est donnée par
$$\mathrm{X}^{q^n} - \mathrm{X} = \prod_{d|n} \prod_{\mathrm{P} \in \mu_q(d)} \mathrm{P}\,.$$

Polynômes minimaux des éléments d'un corps fini.

Lemme 1 – Orbites. Soient $x, y \in \mathbb{F}_{q^n}$. Les éléments x et y ont le même polynôme minimal sur $\mathbb{F}_q$ si et seulement si x et y sont dans la même orbite sous F.

Preuve. (⇐) Soient $x \in \mathbb{F}_{q^n}$ et y dans son orbite sous F. Par hypothèse, il existe $s \in \mathbb{N}$ tel que $y = x^{q^s}$. Considérons $\mathrm{P} \in \mathbb{F}_q[\mathrm{X}]$ et montrons que l'on a alors

$$\mathrm{P}(y) = 0 \iff \mathrm{P}(x^{q^s}) = 0 \iff (\mathrm{P}(x))^{q^s} = 0 \iff \mathrm{P}(x) = 0. \qquad (*)$$

La première équivalence repose sur l'égalité $y = x^{q^s}$. La deuxième équivalence est un cas particulier du point 2 des prérequis. La troisième équivalence repose simplement sur le fait que, dans un anneau intègre (ici le corps $\mathbb{F}_{q^n}$), on dispose de l'équivalence

$$a^k = 0 \iff a = 0.$$

L'équivalence $(*)$ implique que les idéaux formés des polynômes annulateurs de x et de y coïncident. Les polynômes minimaux de x et y coïncident donc aussi.

(⇒) Soit $x \in \mathbb{F}_{q^n}$. Les éléments de $\mathbb{F}_{q^n}$ qui ont le même polynôme minimal que x sont les éléments de $\mathbb{F}_{q^n}$ qui sont racines du polynôme minimal π_x de x. On note $\mathcal{O}_x$ l'orbite de x sous F. On définit alors

$$\mathrm{P} = \prod_{y \in \mathcal{O}_x} (\mathrm{X} - y).$$

D'après **(⇐)** tout élément de l'orbite de x est racine de son polynôme minimal et donc P divise π_x. De plus, comme F induit une bijection sur $\mathcal{O}_x$, on en déduit que

$$\prod_{y \in \mathcal{O}_x} (\mathrm{X} - \mathrm{F}(y)) \;=\; \prod_{y \in \mathcal{O}_x} (\mathrm{X} - y) \;=\; \mathrm{P}.$$

Ceci signifie que les coefficients de P sont invariants sous l'action de F, ce qui montre que $\mathrm{P} \in \mathbb{F}_q[\mathrm{X}]$ grâce au point 3 des prérequis. Or $x \in \mathcal{O}_x$, donc P est un polynôme de $\mathbb{F}_q[\mathrm{X}]$ qui annule x et ainsi $\pi_x \mid \mathrm{P}$. Comme π_x et P sont unitaires, on en déduit que $\mathrm{P} = \pi_x$. Ainsi l'expression factorisée de P montre que les racines de π_x appartenant à $\mathbb{F}_{q^n}$ sont les éléments de l'orbite de x sous F, ce qui achève la preuve. ■

Remarque 2 – Inclusions. Remarquez que l'implication **(⇐)** n'utilise que l'inclusion $\mathbb{F}_q \subset \{x \in \mathbb{F}_{q^n}, \quad x^q = x\}$. De même, l'implication **(⇒)** n'utilise que l'inclusion $\{x \in \mathbb{F}_{q^n}, \quad x^q = x\} \subset \mathbb{F}_q$.

Remarque 3 – Avec le langage de la théorie de Galois. Le lemme 1 repose sur le fait que l'extension $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ est galoisienne de groupe de Galois engendré par F (voir les définitions dans [GOZ]).

Lemme 4 – Polynômes minimaux et corps finis. Soit $\mathrm{P} \in \mu_q(d)$. Le polynôme P est le polynôme minimal sur $\mathbb{F}_q$ d'un élément de $\mathbb{F}_{q^n}$ si et seulement si $d \mid n$.

Preuve. Supposons que $d \mid n$. D'après le point 4 des prérequis, le polynôme P divise $\mathrm{X}^{q^n} - \mathrm{X}$. Par ailleurs, le point 1 des prérequis appliqué au corps $\mathbb{F}_{q^n}$ montre que $\mathrm{X}^{q^n} - \mathrm{X}$ possède au moins q^n racines distinctes. Il est donc scindé à racines simples sur $\mathbb{F}_{q^n}$ et donc P aussi. Ainsi P a une racine $x \in \mathbb{F}_{q^n}$ et est donc le polynôme minimal de x sur $\mathbb{F}_q$ (car $\mathrm{P} \in \mathbb{F}_q[\mathrm{X}]$ est irréductible sur $\mathbb{F}_q$ et unitaire).

Réciproquement, soit $x \in \mathbb{F}_{q^n}$ tel que P soit le polynôme minimal de x sur $\mathbb{F}_q$. D'après le point 1 des prérequis, x est racine de $\mathrm{X}^{q^n} - \mathrm{X} \in \mathbb{F}_q[\mathrm{X}]$ et donc $\mathrm{P} \mid \mathrm{X}^{q^n} - \mathrm{X}$. Le point 4 des prérequis assure alors que $d \mid n$. ■

Le lemme précédent peut se reformuler ainsi : les polynômes minimaux sur $\mathbb{F}_q$ des éléments de $\mathbb{F}_{q^n}$ sont les polynômes à coefficients dans $\mathbb{F}_q$ unitaires irréductibles sur $\mathbb{F}_q$ et dont le degré divise n.

Signature du morphisme de Frobenius.

Proposition 5 – Signature. La signature du morphisme de Frobenius est donnée par

$$\varepsilon(\mathrm{F}) = (-1)^{q^n + \sum_{d \mid n} m_q(d)}.$$

Preuve. La preuve repose sur la décomposition d'une permutation en cycles à supports disjoints : on exhibe cette décomposition pour F. Les cycles intervenant dans la décomposition d'une permutation en cycles à supports disjoints sont déterminés par les orbites sous cette permutation [RDO1, 2.4.2 Théorème I]. Ainsi d'après le lemme 1, il suffit de déterminer les polynômes minimaux sur $\mathbb{F}_q$ des éléments de $\mathbb{F}_{q^n}$. Or d'après le lemme 4, les polynômes minimaux sur $\mathbb{F}_q$ des éléments de $\mathbb{F}_{q^n}$ sont les polynômes P unitaires irréductibles sur $\mathbb{F}_q$ dont le degré divise n. De plus, on a vu dans la preuve du lemme 4 que de tels polynômes sont scindés sur $\mathbb{F}_{q^n}$. Ainsi F induit un cycle de longueur $\deg \mathrm{P}$ sur l'ensemble des racines de P. On en déduit alors

$$\varepsilon(\mathrm{F}) = (-1)^{\sum_{d \mid n} (d+1) m_q(d)}.$$

De plus, d'après le point 4 des prérequis, on a $\sum_{d \mid n} d\, m_q(d) = q^n$. Ainsi

$$\varepsilon(\mathrm{F}) = (-1)^{q^n + \sum_{d \mid n} m_q(d)}.$$

Remarque 6 – Signature : une autre expression. Soit σ une permutation d'un ensemble à k éléments et j le nombre d'orbite de σ. On a alors $\varepsilon(\sigma) = (-1)^{k-j}$ (voir [RDO1, 2.4.3]).

Dans notre situation, on a $k = q^n$ et $j = \sum_{d|n} m_q(d)$, ce qui redonne le résultat.

Une autre expression.

Supposons à présent que p est un nombre premier impair et $m = 1$. L'automorphisme $\mathrm{F} : x \mapsto x^p$ de $\mathbb{F}_{p^n}$ est $\mathbb{F}_p$-linéaire. Ainsi, on peut utiliser le théorème de Frobenius-Zolotarev [BPM, exercice 5.4] pour obtenir la signature de cet automorphisme en fonction de son déterminant.

Proposition 7 – Signature du morphisme de Frobenius. Soient p un nombre premier impair, $n \in \mathbb{N}^*$ et

$$\mathrm{F}: \begin{cases} \mathbb{F}_{p^n} & \longrightarrow \mathbb{F}_{p^n} \\ x & \longmapsto x^p \,. \end{cases}$$

On a $$\varepsilon(\mathrm{F}) = (-1)^{\frac{(p-1)(n+1)}{2}} \,.$$

Preuve. Il s'agit donc de trouver une « bonne $\mathbb{F}_p$-base » de $\mathbb{F}_{p^n}$ pour pouvoir calculer le déterminant de F. Comme l'extension $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ est galoisienne de groupe de galois cyclique d'ordre n engendré par F [GOZ], le théorème de la base normale [GOZ] assure alors l'existence d'une base de la forme

$$\mathscr{B} = (x, \mathrm{F}(x), \ldots, \mathrm{F}^{n-1}(x)) \,.$$

Comme $\mathrm{F}^n = \mathrm{id}$, on en déduit que la matrice de F dans la base $\mathscr{B}$ est

$$\mathrm{Mat}_{\mathscr{B}}(\mathrm{F}) = \begin{bmatrix} & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{bmatrix} .$$

La matrice $\mathrm{Mat}_{\mathscr{B}}(\mathrm{F})$ est une matrice de permutation : celle d'un cycle de longueur n. On en déduit alors que $\det(\mathrm{F}) = (-1)^{n+1}$. Le théorème de Frobenius-Zolotarev donne

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

Comme $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, la multiplicativité du symbole de Legendre assure que

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

Références

[BPM] V. Beck, J. Malick, et G.Peyré. *Objectif Agrégation.* H & K, 2004.

[GOZ] I. Gozard. *Théorie de Galois.* Ellipses, 1997.

[PER] D. Perrin. *Cours d'algèbre.* Ellipses, 1996.

[RDO1] E. Ramis, C. Deschamps, et J. Odoux. *Cours de Mathématiques 1, Algèbre.* Dunod, 1998.