Corps finis

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

Cette note présente des énoncés classiques du programme de l'agrégation autour des corps finis, en particulier, l'étude des sous-corps d'un corps fini. Elle introduit les notations et les résultats nécessaires au calcul de la signature du morphisme de Frobenius (voir la note « Signature et corps finis »). À l'exception de la propriété d'« unicité » qui utilise la notion de corps de décomposition (voir [PER, III.2.5]), la difficulté de l'étude des corps finis repose sur le nombre et la variété des ingrédients auxquels elle fait appel et non sur la complexité de ces ingrédients.

Morphisme de Frobenius.

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.

Proposition-Définition 1 — Morphisme de Frobenius. Soient A un anneau commutatif unitaire de caractéristique p (voir l'exemple 5.12 [BPM]). L'application

$$\mathrm{Frob}_{\mathrm{A}} : \begin{cases} \mathrm{A} \longrightarrow \mathrm{A} \\ x \longmapsto x^p \end{cases}$$

est alors un morphisme d'anneaux unitaires appelé *morphisme de Frobenius de* A.

Preuve. On a $1^p = 1$. De plus, A est commutatif, donc $(xy)^p = x^p y^p$ pour tout $x, y \in \mathrm{A}$. Il suffit donc de montrer que $(x+y)^p = x^p + y^p$ pour tout $x, y \in \mathrm{A}$. Cette égalité se démontre grâce à la formule du binôme et au fait que $p \mid \mathrm{C}_p^i$ pour tout $i \in [\![1\,,\, p-1]\!]$ (voir [RDO1, 3.2.4.2]). ∎

Lorsqu'on travaille en caractéristique p, le morphisme de Frobenius est un instrument fondamental et omniprésent, tant à la source que dans la résolution des problèmes. Ses itérés ont tout autant d'intérêt. Pour $i \in \mathbb{N}$, le i-ième itéré de $\mathrm{Frob}_{\mathrm{A}}$ est le morphisme d'anneaux donné par

$$\mathrm{Frob}_{\mathrm{A}}{}^i = \mathrm{Frob}_{\mathrm{A}} \circ \cdots \circ \mathrm{Frob}_{\mathrm{A}} : \begin{cases} \mathrm{A} \longrightarrow \mathrm{A} \\ x \longmapsto x^{p^i} . \end{cases}$$

Exemple 2 — Le cas de $\mathbb{F}_{q^n}$. Le corps $\mathbb{F}_{q^n}$ est un anneau commutatif unitaire de caractéristique p. Pour la suite de cette note, on note F le m-ième itéré du morphisme de Frobenius de $\mathbb{F}_{q^n}$, c'est-à-dire

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

Résultats.

Le lemme 3 est le lemme fondamental pour la démonstration de « l'unicité » des corps finis. Sa preuve repose uniquement sur le théorème de Lagrange.

Lemme 3 — Corps fini et Lagrange. Soit $\mathbb{F}_q$ un corps fini à q éléments. Alors $x^q = x$ pour tout $x \in \mathbb{F}_q$.

Preuve. Soit $x \in \mathbb{F}_q$. Si $x = 0$ alors $x^q = x = 0$. Si $x \neq 0$, alors x appartient au groupe multiplicatif $\mathbb{F}_q^\times$ de cardinal $q-1$. D'après le théorème de Lagrange, l'ordre de x divise $q-1$ et donc $x^{q-1} = 1$. On en déduit que $x^q = x$. ∎

Le lemme 4 lie les valeurs d'une fonction polynomiale à coefficients dans $\mathbb{F}_q$ prise en un élément de $\mathbb{F}_{q^n}$ et en son image par F. La preuve du lemme 5.35 de [BPM] repose sur une idée similaire.

Lemme 4 — Corps fini et évaluation de polynômes. Soient $\mathrm{P} \in \mathbb{F}_q[\mathrm{X}]$ et $x \in \mathbb{F}_{q^n}$. Pour tout $s \in \mathbb{N}$, on a

$$\mathrm{P}(x^{q^s}) = (\mathrm{P}(x))^{q^s} .$$

Preuve. Écrivons

$$\mathrm{P} = \sum_{i=0}^{\ell} a_i \mathrm{X}^i \qquad \text{et} \qquad \mathrm{P}(x^{q^s}) = \sum_{i=0}^{\ell} a_i\, x^{iq^s}.$$

D'après le lemme 3, on a $a_i{}^{q^s} = a_i{}^q = a_i$ et donc

$$\mathrm{P}(x^{q^s}) = \sum_{i=0}^{\ell} a_i{}^{q^s}\, x^{iq^s} = \sum_{i=0}^{\ell} (a_i\, x^i)^{q^s}.$$

Comme F^s est un morphisme de corps, on en déduit que

$$\mathrm{P}(x^{q^s}) = \left(\sum_{i=0}^{\ell} a_i\, x^i\right)^{q^s} = \mathrm{P}(x)^{q^s}. \qquad \blacksquare$$

Le lemme 5 est à la base de l'étude des sous-corps d'un corps fini (corollaire 7). Il est aussi utilisé pour le théorème de factorisation de Berlekamp [BPM, théorème 5.36]. Sa preuve repose sur les ingrédients suivants

(i) un polynôme de degré ℓ à coefficients dans un corps a au plus ℓ racines [RDO1, 6.4.4 corollaire II] ;

(ii) tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique [DMZ, Th 3.9] et [BPM, exercice 6.9] ;

(iii) si $d \mid \ell$, un groupe cyclique de cardinal ℓ admet un unique sous-groupe de cardinal d [CAL, Th.III.3.14].

Lemme 5 — Corps fini et points fixes. L'ensemble des points fixes de F est un sous-corps à q éléments de $\mathbb{F}_{q^n}$, autrement dit

$$\{x \in \mathbb{F}_{q^n}, \quad x^q = x\} \overset{\text{corps}}{\simeq} \mathbb{F}_q\,;$$

Preuve. Comme F est un morphisme de corps, on voit aisément que l'ensemble des points fixes de F est un sous-corps de $\mathbb{F}_{q^n}$. De plus, si x est un point fixe de F, alors $x^q = x$ et donc x est racine du polynôme $\mathrm{X}^q - \mathrm{X}$. D'après la remarque ($i$), l'ensemble des points fixes de F est donc un sous-corps de $\mathbb{F}_{q^n}$ de cardinal au plus q.

Par ailleurs, d'après la remarque (ii), le groupe $\mathbb{F}_{q^n}^{\times}$ d'ordre $q^n - 1$ est cyclique. Or $q - 1 \mid q^n - 1$, puisque

$$\frac{q^n - 1}{q - 1} = \sum_{k=0}^{n-1} q^k\,.$$

Ainsi d'après la remarque (iii), $\mathbb{F}_{q^n}^{\times}$ admet un sous-groupe G d'ordre $q-1$. Le théorème de Lagrange [PER, I.0.1] assure alors que tout élément de G vérifie $x^{q-1} = 1$ et donc $x^q = x$. De plus comme $0^q = 0$ et $0 \notin \mathrm{G}$, on en déduit que F a au moins q points fixes. Finalement, l'ensemble des points fixes de F est donc un sous-corps de $\mathbb{F}_{q^n}$ de cardinal q. Par « unicité », il s'agit donc de $\mathbb{F}_q$.

Remarque 6 — $n = 1$. En faisant $n = 1$ dans le lemme 5, on retrouve le résultat du lemme 3.

Corollaire 7 — Sous-corps d'un corps fini. Soit $\mathbb{F}_{p^m}$ un corps à p^m éléments. Si K est un sous-corps de $\mathbb{F}_{p^m}$, alors K a p^d éléments où d divise m. Réciproquement, pour tout diviseur d de m, il existe un unique sous-corps de $\mathbb{F}_{p^m}$ à p^d éléments. De plus, ce sous-corps est l'ensemble des racines de $\mathrm{P} = \mathrm{X}^{p^d} - \mathrm{X}$.

Preuve. Si K est un sous-corps de $\mathbb{F}_{p^m}$, alors $\mathbb{F}_{p^m}$ est un K-espace vectoriel. De plus, $\dim_{\mathrm{K}} \mathbb{F}_{p^m}$ est finie puisque $\mathbb{F}_{p^m}$ est fini. Notons $d' = \dim_{\mathrm{K}} \mathbb{F}_{p^m}$. On a donc $(\mathrm{Card}\ \mathrm{K})^{d'} = p^m$. On en déduit que K a p^d avec $d'd = m$.

Réciproquement, si d divise m, on pose $q = p^d$ et $n = m/d$. On a alors $q^n = p^m$. Le lemme 5 montre que alors $\mathbb{F}_{p^m} = \mathbb{F}_{q^n}$ a un sous-corps à $q = p^d$ éléments. De plus, si K est un sous-corps à p^d éléments, alors d'après le lemme 3, K est un sous-ensemble des racines du polynôme P. Comme P est degré p^d, cet ensemble a au plus p^d éléments et donc K est l'ensemble des racines de P.

Exemple 8 — Sous-corps. Comme 2 divise 4 mais ne divise pas 3, $\mathbb{F}_4 = \mathbb{F}_{2^2}$ est un sous-corps de $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ mais n'est pas un sous-corps de $\mathbb{F}_8 = \mathbb{F}_{2^3}$.

Finissons par un résultat de décomposition en facteur irréductible dans $\mathbb{F}_q[\mathrm{X}]$.

Lemme 9 — Corps fini et polynômes irréductibles. Sur $\mathbb{F}_q$, la décomposition de $\mathrm{X}^{q^n} - \mathrm{X}$ en polynômes irréductibles est donnée par

$$\mathrm{X}^{q^n} - \mathrm{X} = \prod_{d \mid n} \prod_{\mathrm{P} \in \mu_q(d)} \mathrm{P}\,.$$

Preuve. Posons $\mathrm{Q} = \mathrm{X}^{q^n} - \mathrm{X}$. On remarque que $\mathrm{Q}' = q^n \mathrm{X}^{q^n-1} - 1 = -1$. On en déduit alors que $\mathrm{pgcd}\,(\mathrm{Q}, \mathrm{Q}') = 1$. La proposition 5.39 de [BPM] montre alors que les multiplicités non nulles dans la décomposition de Q en produit de polynômes irréductibles sont toutes égales à un. Ainsi Q est un produit de polynômes irréductibles deux à deux distincts. Cherchons à présent quels sont les polynômes irréductibles unitaires qui divisent Q.

Soit $\mathrm{P} \mid \mathrm{Q}$ avec P irréductible unitaire. Le lemme 3 appliqué au corps $\mathbb{F}_{q^n}$ montre que le polynôme Q a q^n racines distinctes dans $\mathbb{F}_{q^n}$. Comme Q est de degré q^n, il est scindé à racines simples. Le polynôme P l'est donc aussi. En particulier, P admet une racine $x \in \mathbb{F}_{q^n}$. Comme P est unitaire et irréductible sur $\mathbb{F}_q$, P est le polynôme minimal sur $\mathbb{F}_q$ de x. On a alors la « suite d'extension de corps »

$$\mathbb{F}_q \subset \mathbb{F}_q[x] \subset \mathbb{F}_{q^n}.$$

On en déduit par multiplicativité des degrés [PER, III.1.5],

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q[x]][\mathbb{F}_q[x] : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q[x]] \deg \mathrm{P}.$$

On a donc $\deg \mathrm{P} \mid n$. Comme tous les facteurs irréductibles sont simples, on en déduit que

$$\mathrm{Q} \ \mid \ \prod_{d \mid n} \prod_{\mathrm{P} \in \mu_q(d)} \mathrm{P}.$$

Inversement, si $d \mid n$ et P est un polynôme unitaire de degré d irréductible sur $\mathbb{F}_q$, alors $\mathbb{F}_q[\mathrm{X}]/\langle \mathrm{P} \rangle$ est un corps fini a q^d éléments. Soient $\pi : \mathbb{F}_q[\mathrm{X}] \to \mathbb{F}_q[\mathrm{X}]/\langle \mathrm{P} \rangle$ la surjection canonique et $\alpha = \pi(\mathrm{X})$. Le lemme 3 appliqué au corps $\mathbb{F}_q[\mathrm{X}]/\langle \mathrm{P} \rangle$ montre que

$$\alpha^{p^d} = \alpha \qquad \text{et comme } d \mid n, \qquad \alpha^{p^n} = \alpha^{p^d p^d \cdots p^d} = \alpha$$

donc α est racine de $\mathrm{X}^{p^n} - \mathrm{X}$. Comme le polynôme minimal de α sur $\mathbb{F}_q$ est P puisque $\mathrm{P}(\alpha) = \pi(\mathrm{P}(\mathrm{X})) = 0$ et que P est irréductible sur $\mathbb{F}_q$ (voir la note « polynôme minimal »), on en déduit que $\mathrm{P} \mid \mathrm{X}^{p^n} - \mathrm{X}$, ce qui achève la preuve.

Références

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

[CAL] J. Calais. *Éléments de théorie des groupes.* PUF, 1998.

[DMZ] M. Demazure. *Cours d'algèbre. Primalité, divisibilité, codes.* Cassini, 1997.

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

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