Dénombrement des polynômes irréductibles unitaires sur un corps fini

Geoffrey Deperle

Leçons associées :
— 123 : Corps finis. Applications.
— 125 : Extension de corps. Exemples et applications.
— 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
— 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.
— 190 : Méthodes combinatoires, problèmes de dénombrement.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *On note $\mathcal{P}_q(d)$ l'ensemble des polynômes irréductibles de degré d sur $\mathbb{F}_q$ ($q = p^\alpha$ est une puissance d'un nombre premier). Si $I(q,d)$ désigne le cardinal de $\mathcal{P}_q(d)$, on a pour $n \in \mathbb{N}^*$,*

$$I(q,d) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

Preuve :

Lemme 1. *Pour $n \in \mathbb{N}^*$, $X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$.*

Preuve : Soit $P \in \mathcal{P}_q(d)$, l'anneau $K = \mathbb{F}_q[X]/(P)$ est un corps (car $\mathbb{F}_q[X]$ est principal) de cardinal q^d donc isomorphe à $\mathbb{F}_{q^d}$, ainsi $\forall x \in K, x^{q^d} = x$.
Or, si $n = dk$, on a $x^{q^n} = x^{q^{dk}} = (x^{q^d})^{q^d \times \cdots \times q^d}$ donc par récurrence $x^{q^n} = x$ donc $\overline{X^{q^n} - X} = 0$ et P divise $X^{q^n} - X$ dans $\mathbb{F}_q[X]$. Comme les éléments de $\mathcal{P}_q(d)$ sont irréductibles, le produit $\prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$ divise $X^{q^n} - X$.
Réciproquement, soit P un facteur irréductible de degré d de $X^{q^d} - X$ dans $\mathbb{F}_q[X]$,
Comme $\mathbb{F}_{q^n}$ est un corps de décomposition de $X^{q^n} - X$, P est scindé sur $\mathbb{F}_{q^n}$,
Si x est une racine de P, on a $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, par multiplicativité des degrés, $[\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = n$. Or, comme P est irréductible, $\mathbb{F}_q(x)$ est un corps de rupture de P de degré d sur $\mathbb{F}_q$ donc $d|n$.
Montrons que $X^{q^n} - X$ n'admet pas de facteur double (ou plus), s'il existe un tel facteur, alors $X^{q^n} - X$ admet une racine double dans un corps de décomposition.
Or, $(X^{q^n} - X)' = q^n X^{q^n - 1} - 1 = -1$ car K (car caractéristique p) donc $X^{q^n} - X$ n'a pas de racine double dans un corps de décomposition. □

Lemme 2 (Inversion de Möbius)**.** *Soit $g : \mathbb{N}^* \to \mathbb{C}$, soit $G(n) = \sum_{d|n} g(d)$, on a*

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$$

où μ est la fonction de Möbius

Preuve : Soit $n \geq 2$,
Soit $p_1, \ldots, p_r$ les diviseurs de n, (on a $r \geq 2$),

$$\sum_{d|n} \mu(d) = \sum_{I \subset [\![1,r]\!]} (-1)^{|I|} = \sum_{s=0}^{r} \binom{r}{s} (-1)^s = (1-1)^r = 0$$

Donc

$$\sum_{d|n} \mu(d) = \begin{cases} 0 & \text{si } n \geq 2 \\ 1 & \text{si } n = 1 \end{cases}$$

Si $n \in \mathbb{N}^*$, $d|n$ et $d'|\frac{n}{d} \iff d'|n$ et $d|\frac{n}{d'}$, donc

$$\begin{aligned} \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} g(d') &= \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(d) g(d') \\ &= \sum_{d'|n} \sum_{d|\frac{n}{d'}} \mu(d) g(d') \\ &= \sum_{d'|n} g(d') \underbrace{\sum_{d|\frac{n}{d}} \mu(d)}_{=0 \text{ sauf pour } d'=n} = g(n) \end{aligned}$$

□

Passons à la preuve du théorème, on a

$$\deg(X^{q^n} - X) = q^n = \sum_{d|n} \sum_{P \in \mathcal{P}_q(d)} \deg(P) = \sum_{d|n} dI(q,d)$$

D'où par inversion de Möbius,

$$I(q,d) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

□

Annexe

Application. *On a* $I(q,n) \underset{n\to+\infty}{\sim} \dfrac{q^n}{n}$

Preuve : En posant $r_n = \sum_{\substack{d|n \\ d<n}} \mu\left(\frac{n}{d}\right) q^d$, on a

$$\begin{aligned} |r_n| &\leq \sum_{\substack{d|n \\ d<n}} q^d \leq \sum_{d=0}^{\lfloor \frac{n}{2} \rfloor} q^d \\ &= \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q-1} \end{aligned}$$

Donc $r_n = \underset{n\to+\infty}{O}(q^n)$, comme $I(q,d) = \frac{q^n + r_n}{n}$ on a le résultat. □

Application. *Pour tout* $n \in \mathbb{N}^*$*, il existe un polynôme irréductible sur* $\mathbb{F}_q$ *de degré* n*.*

Preuve : Comme $q^n = \sum_{d|n} dI(q,d)$,

Donc pour tout $d \in \mathbb{N}^*$, $q^d \geq dI(q,d)$ d'où

$$\begin{aligned} nI(q,n) &= q^n - \sum_{\substack{d|n \\ d\neq n}} dI(q,d) \\ &\geq q^n - \sum_{\substack{d|n \\ d\neq n}} q^d \\ &\geq q^n - \sum_{d=1}^{n-1} q^d = q^n - q\frac{q^{n-1}-1}{q-1} > 0 \end{aligned}$$

□

Quelques polynômes irréductibles

- Sur $\mathbb{F}_2$, on a
  - $\mathcal{P}_2(1) = \{X, X+1\} \to I(2,1) = 2$
  - $\mathcal{P}_2(2) = \{X^2+X+1\} \to I(2,2) = 1$
  - $\mathcal{P}_2(3) = \{X^3+X+1, X^3+X^2+1\} \to I(2,3) = 2$
- Sur $\mathbb{F}_3$, on a
  - $\mathcal{P}_3(1) = \{X, X+1, X+2\} \to I(3,1) = 3$
  - $\mathcal{P}_3(2) = \{X^2+1, X^2+X+2, X^2+2X+2\} \to I(3,2) = 3$

Références

[1] Jean Étienne Rombaldi. *Mathématiques pour l'agrégation : Algèbre Géométrie*. deboeck, 2019.