

Dénombrement des polynômes irréductibles sur un corps fini

Leçons : 123, 125, 141, 190

Références :

1. *Mathématiques pour l'agrégation : Algèbre et géométrie*, J.-E. Rombaldi, p. 424.
2. *Cours d'algèbre*, Michel Demazure, p. 220.

Soit p un nombre premier.

Proposition 1. Soit $n > 0$. Dans $\mathbb{F}_p[X]$, on a

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{U}_d(p)} P(X),$$

où $\mathcal{U}_d(p)$ est l'ensemble des polynômes unitaires irréductibles de degré d de $\mathbb{F}_p[X]$.

Démonstration. Notons $P_n = X^{p^n} - X$. Soit P un polynôme unitaire, irréductible de degré d sur $\mathbb{F}_p$.

Lemme 2. $(d \mid n) \iff (P \mid P_n)$.

Démonstration du lemme. Posons $K = \mathbb{F}_p[X]/(P) \cong \mathbb{F}_{p^d}$. Notons $\alpha = \bar{X}$ la classe de X dans ce quotient. Ainsi K est un $\mathbb{F}_p$ -espace vectoriel dont $1, \alpha, \dots, \alpha^{d-1}$ est une base.

$(\Rightarrow)$ Supposons que $d \mid n$. Montrons que $P \mid P_n$.

$\alpha \neq 0$ donc $\alpha \in \mathbb{F}_{p^d}^*$, qui est un groupe de cardinal $p^d - 1$, donc, d'après le théorème de Lagrange, $\alpha^{p^d-1} = 1$, donc $\alpha^{p^d} = \alpha$. De plus, $d \mid n$ donc $\alpha^{p^n} = \alpha$, i.e. $P_n(\alpha) = 0$.

De plus, on a, par construction, $P(\alpha) = 0$. Supposons que P ne divise pas P_n . Comme P est irréductible, cela revient à dire $\text{pgcd}(P_n, P) = 1$, donc, d'après Bézout, il existe A, B tels que

$$AP + BP_n = 1,$$

et, en évaluant en α , il vient $0 = 1$, ce qui est faux. Donc $P \mid P_n$.

$(\Leftarrow)$ Supposons $P \mid P_n$. Montrons que $d \mid n$.

$P \mid P_n$ et $P(\alpha) = 0$ donc $P_n(\alpha) = 0$. De plus, $\forall \bar{\theta} \in K$,

$$\bar{\theta} = \sum_{k=0}^{d-1} a_k \alpha^k, \quad a_k \in \mathbb{F}_p, \quad \forall k \in \llbracket 0, d-1 \rrbracket.$$

D'après le morphisme de Frobenius, on a

$$\bar{\theta}^{p^n} \underset{(*)}{=} \sum_{k=0}^{d-1} \underbrace{a_k^{p^n}}_{\text{car } a_k \in \mathbb{F}_p} \alpha^{p^n k} = \sum_{k=0}^{d-1} a_k (\alpha^{p^n})^k = \sum_{k=0}^{d-1} a_k \alpha^k = \bar{\theta},$$

où la dernière égalité utilise $\alpha^{p^n} = \alpha$ (car $P_n(\alpha) = 0$).

Or, $\mathbb{F}_{p^d}^*$ est cyclique d'ordre $p^d - 1$ (cf. annexe), donc il existe $x \in \mathbb{F}_{p^d}^*$ d'ordre $p^d - 1$. Comme $x \neq 0$, on a, d'après $(*)$, $x^{p^n-1} = 1$, donc $p^d - 1 \mid p^n - 1$, donc $d \mid n$ (cf. annexe). CQFD

Il reste à se convaincre qu'aucun des facteurs de P_n n'est carré. Mais si $P^2 \mid P_n$, alors $P \mid P'_n = -1$ (car $P'_n = p^n X^{p^n-1} - 1 = -1$ en caractéristique p).

Finalement, on a bien montré que

$$X^{p^n} - X = \prod_{d \mid n} \prod_{P \in \mathcal{U}_d(p)} P(X).$$

□

On peut maintenant passer au dénombrement des polynômes irréductibles unitaires dans $\mathbb{F}_p$.

Théorème 3. Posons $I_n(p) = \#\mathcal{U}_n(p)$. On a alors

$$0 < I_n(p) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d \underset{n \rightarrow \infty}{\sim} \frac{p^n}{n},$$

où μ est la fonction de Möbius.

Démonstration. En considérant les degrés dans le résultat précédent, on obtient

$$p^n = \sum_{d \mid n} d I_d(p). \quad (1)$$

Montrons d'abord que $I_n(p) > 0$: D'une part, on a

$$p^n = n I_n(p) + \underbrace{\sum_{\substack{d \mid n \\ d < n}} d I_d(p)}_{\geq 0},$$

donc $I_n(p) \leq \frac{p^n}{n}$.

En appliquant cette majoration dans la somme initiale, il vient

$$\begin{aligned} p^n &= n I_n(p) + \sum_{\substack{d \mid n \\ d < n}} d I_d(p) \leq n I_n(p) + \sum_{\substack{d \mid n \\ d < n}} d \frac{p^d}{d} \\ &\leq n I_n(p) + \sum_{d=0}^{\lfloor n/2 \rfloor} p^d = n I_n(p) + \frac{p^{\lfloor n/2 \rfloor + 1} - 1}{p - 1}, \end{aligned}$$

donc

$$I_n(p) \geq \frac{p^n - p^{\lfloor n/2 \rfloor + 1} + 1}{n} > 0.$$

Donc il existe des polynômes irréductibles unitaires de tout degré.

Montrons maintenant l'équivalent :

Lemme 4 (Inversion de Möbius). Soit $f : \mathbb{N}^* \rightarrow \mathbb{C}$, et $F(n) = \sum_{d \mid n} f(d)$. Alors,

$$f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) F(d).$$

Démonstration du lemme. Par définition de μ , on a $\mu * 1(n) = \delta_n$, donc $F = f * 1$, donc $F * \mu = f * 1 * \mu = f * \delta = f$. CQFD

Donc, en appliquant l'inversion de Möbius à (1), il vient

$$I_n(p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

On a alors

$$I_n(p) = \frac{p^n}{n} + \frac{1}{n} \sum_{\substack{d|n \\ d < n}} \mu\left(\frac{n}{d}\right) p^d.$$

Or,

$$\left| \frac{1}{n} \sum_{\substack{d|n \\ d < n}} \mu\left(\frac{n}{d}\right) p^d \right| \leq \frac{1}{n} \sum_{\substack{d|n \\ d < n}} \underbrace{\left| \mu\left(\frac{n}{d}\right) \right|}_{\leq 1} p^d \leq \frac{1}{n} \sum_{d=0}^{\lfloor n/2 \rfloor} p^d = \frac{1}{n} \cdot \frac{p^{\lfloor n/2 \rfloor + 1} - 1}{p - 1} \leq \frac{p^{\lfloor n/2 \rfloor + 1}}{n},$$

d'où

$$I_n(p) = \frac{p^n}{n} + O\left(\frac{p^{\lfloor n/2 \rfloor + 1}}{n}\right).$$

□

Annexes

Rappel (théorème de Lagrange) : Soit G un groupe fini, $H \leq G$ un sous-groupe. Alors :

- (1) $\#H = \#aH, \forall a \in G$;
- (2) $\forall a, b \in G, aH \cap bH = \emptyset$ ou $aH = bH$;
- (3) $G = \bigsqcup_a aH$, donc $|G| = k|H|$ (où $k = [G : H]$).

Théorème 5. Pour tout corps fini $\mathbb{F}_q$, $\mathbb{F}_q^*$ est cyclique.

Lemme 6. $n = \sum_{d|n} \varphi(d)$.

Démonstration du lemme. Considérons, pour $d | n$, C_d l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d , et Φ_d l'ensemble des générateurs de C_d . On a

$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} \Phi_d,$$

donc

$$n = \sum_{d|n} \#\Phi_d = \sum_{d|n} \varphi(d).$$

CQFD

Démonstration du théorème. Posons $q-1 = |\mathbb{F}_q^*|$. Pour $d \mid q-1$, notons N_d le nombre d'éléments de $\mathbb{F}_q^*$ d'ordre exactement d . Comme tout élément de $\mathbb{F}_q^*$ a un ordre divisant $q-1$ (Lagrange), on a $q-1 = \sum_{d \mid q-1} N_d$.

Or, pour $d \mid q-1$, les éléments d'ordre d sont racines de $X^d - 1$, qui en admet au plus d dans le corps $\mathbb{F}_q$; donc $N_d \leq \varphi(d)$ (car s'il existe un élément d'ordre d , les racines de $X^d - 1$ forment un groupe cyclique d'ordre d , dont les éléments d'ordre exactement d sont au nombre de $\varphi(d)$; sinon $N_d = 0 \leq \varphi(d)$).

Donc $q-1 = \sum_{d \mid q-1} N_d \leq \sum_{d \mid q-1} \varphi(d) = q-1$ (lemme précédent), d'où égalité terme à terme :

$N_d = \varphi(d)$ pour tout $d \mid q-1$. En particulier, $N_{q-1} = \varphi(q-1) \geq 1$, donc il existe un élément d'ordre $q-1$: $\mathbb{F}_q^*$ est cyclique. $\square$

Théorème 7. Si $p^d - 1 \mid p^n - 1$, alors $d \mid n$.

Démonstration. Notons $n = qd + r$ avec $0 \leq r \leq d-1$. Supposons $r > 0$. On a

$$\begin{aligned} p^n - 1 &= p^{qd+r} - 1 = p^{dq} p^r - 1 = (p^{dq} - 1) p^r + p^r - 1 \\ &= (p^d - 1)(p^{d(q-1)} + \dots + 1) p^r + p^r - 1. \end{aligned}$$

Donc, $p^d - 1 \mid p^n - 1$ et $r > 0$ donc $d \leq r$, ce qui est faux. Donc $d \mid n$. $\square$