# Polynômes irréductibles unitaires sur $\mathbb{F}_q$

**Théorème 1.** *Soient $p$ un nombre premier, $\alpha, n \in \mathbb{N}^\star$ et $q = p^\alpha$. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes unitaires irréductibles de degré $d$ sur $\mathbb{F}_q$. Alors :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$$

*Démonstration.*

Notons $Q(X)$ le second membre de l'égalité précédente. Le polynôme $X$ divise $X^{q^n} - X$.

Soit $d$ un diviseur de $n$, on pose $n = dk$. Soit $P \in \mathcal{P}_p(d)$. On pose $\mathbb{K} = \mathbb{F}_p[X]/(P)$. $\mathbb{K}$ est un corps de cardinal $q^d$, donc isomorphe à $\mathbb{F}_{q^d}$. Par une récurrence immédiate, on obtient, pour tout $x \in \mathbb{K}$ :

$$x^{q^n} = x^{q^{dk}} = (((x^{q^d})^{q^d}) \cdots)^{q^d} = x$$

Autrement dit, $X^{q^n} - X = 0$ dans $\mathbb{K}[X]$, donc $P$ divise $X^{q^n} - X$ dans $\mathbb{F}_q[X]$. Comme les éléments de $\mathcal{P}_q(d)$ sont irréductibles, le produit $Q(X)$ divise lui aussi $X^{q^n} - X$.

Réciproquement, soit $P$ un facteur irréductible de degré $d$ de $X^{q^n} - X$ 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 :

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)]\,[\mathbb{F}_q(x) : \mathbb{F}_q]$$

Or $P$ est irréductible, donc $\mathbb{F}_q(x)$ est un corps de rupture de $P$ de degré $d$ sur $\mathbb{F}_q$, et $d$ divise $n$. Il suffit alors de montrer que $X^{q^n} - X$ n'admet pas de facteur double (ou plus). En effet, s'il existe un tel facteur, alors $X^{q^n} - X$ admet une racine double dans un corps de décomposition. Cependant, comme le polynôme dérivé de $X^{q^n} - X$ est $q^n X^{q^n - 1} - 1 = -1$ en caractéristique $p$, $X^{q^n} - X$ n'a pas de racine double dans un corps de décomposition, ce qui termine la preuve.

□

**Proposition 2** (Inversion de Möbius)**.** *On note $\mu$ la fonction de Möbius. Soit $g : \mathbb{N}^\star \to \mathbb{C}$. On pose $G(n) = \sum_{d|n} g(d)$. Alors :*

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

*Démonstration.*

Pour $n \geqslant 2$, on a $\sum_{d|n} \mu(d) = 0$. En effet, si $n = \prod_{i=1}^r p_i^{\alpha_i}$, alors :

$$\sum_{d|n} \mu(d) = \sum_{\beta < \alpha} \mu\left(\prod_{i=1}^r p_i^{\beta_i}\right) = \sum_{\beta \in \{0,1\}^r} (-1)^\beta = \sum_{i=0}^r \binom{r}{i} (-1)^i = (1-1)^r = 0$$

Ensuite, si $n \in \mathbb{N}^\star$ et $d \mid n$, alors $d' \mid \frac{n}{d}$ si, et seulement si, $dd' \mid n$. On a donc :

$$\sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{d' \mid \frac{n}{d}} g(d') = \sum_{d|n} \mu(d) \sum_{dd'|n} g(d') = \sum_{dd'|n} \mu(d) g(d') = \sum_{d'|n} g(d') \sum_{d \mid \frac{n}{d'}} \mu(d) = g(n)$$

□

**Corollaire 3.** *Si $I(q,d)$ désigne le cardinal de $\mathcal{P}_p(d)$, alors, pour tout $n \in \mathbb{N}^\star$, on a :*

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

*Démonstration.*

On pose $g(n) = nI(q,n)$ et $G(n) = \sum_{d|n} g(d)$. On a que :

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

Par l'inversion de Möbius, on obtient :

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

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

$$|r_n| \leqslant \sum_{\substack{d|n \\ d<n}} q^d \leqslant \sum_{d=0}^{\lfloor \frac{n}{2} \rfloor} q^d = \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q-1}$$

Ainsi $r_n = \mathcal{O}(q^n)$. Or $I(q,d) = \frac{q^n + r_n}{n}$, d'où le résultat. □

# Références

[Tau] Patrice Tauvel. *Corps commutatifs et théorie de Galois.* Calvage et Mounet