Polynômes irréductibles sur $\mathbb{F}_q[X]$

Leçons : 123, 125, 141, 190

Théorème 1

On note $\mathscr{P}_q(d)$ l'ensemble des polynômes irréductibles de degré d sur $\mathbb{F}_q$. Alors si $n \in \mathbb{N}^*$,

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

Démonstration. Soit $P \in \mathscr{P}_q(d)$. Alors $K = \mathbb{F}_q[X]/(P)$ est un corps de cardinal q^d donc pour tout $x \in K$, on a $x^{q^d} = x$. Mais si $n = dk, k \in \mathbb{N}$, alors

$$x^{q^n} = x^{q^{dk}} = \underbrace{\left(\dots(x^{q^d})\dots\right)^{q^d}}_{k \text{ fois}} = x.$$

par une récurrence immédiate. Donc en particulier avec $x = \overline{X}$, on obtient $P \mid X^{q^n} - X$. Ainsi, par le lemme de Gauss, $\prod_{d|n} \prod_{P \in \mathscr{P}_q(d)} P(X) \mid X^{q^n} - X$.

Soit P un facteur irréductible de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$. Comme $\mathbb{F}_{q^n}$ est le corps de décomposition de $X^{q^n} - X$, P est scindé sur $\mathbb{F}_{q^n}$. Donc si x est une racine de P dans $\mathbb{F}_{q^n}$, selon le théorème de la base télescopique, $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q]$. Mais comme P est irréductible, P est le polynôme minimal de x sur $\mathbb{F}_q$ donc $[\mathbb{F}_q(x) : \mathbb{F}_q] = d$, de sorte que $d \mid n$.

Enfin, $X^{q^n} - X$ est à facteurs simples : si $X^{q^n} - X$ avait un facteur double, il aurait une racine double dans son corps de décomposition. Mais $(X^{q^n} - X)' = -1$ dans toute extension de $\mathbb{F}_q$ (à cause de la caractéristique de $\mathbb{F}_q$) donc $X^{q^n} - X$ est à racines simples dans son corps de décomposition [1]. $\square$

Proposition 2

Soit $g : \mathbb{N}^* \to \mathbb{C}$, alors si $G(n) = \sum_{d|n} g(d)$, on a pour tout $n \in \mathbb{N}^*$, $g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$, où μ est la fonction de Möbius.

Démonstration. On remarque que $d \mid n$ et $d' \mid \frac{n}{d}$ si et seulement si $dd' \mid n$.

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

Or, si $m \neq 1$, $\sum_{d|m} \mu(d) = 0$ [2] donc $\sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) = g(n)$. $\square$

1. Une racine double de P est une racine de P' dans un corps de caractéristique quelconque, mais la réciproque n'est vraie qu'en caractéristique nulle

2. en effet, si $m = \prod_{i=1}^r p_i^{\alpha_i}$, $\sum_{d|m} \mu(d) = \sum_{d|m} \mu(d) = \sum_{\beta \leqslant \alpha} \mu(p_1^{\beta_1} \dots p_r^{\beta_r}) = \sum_{\beta \in \{0,1\}^r} (-1)^{|\beta|} = \sum_{k=0}^r \binom{r}{k} (-1)^k$ (choix de k 1 parmi r termes) donc $\sum_{d|m} \mu(d) = 0$

Corollaire 3

Si $I(q,d) = \mathrm{Card}\mathscr{P}_q(d)$*, alors* $\forall n \in \mathbb{N}^*, I(q,n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$ *et* $I(q,n) \sim_{n\to+\infty} \frac{q^n}{n}$.

Démonstration. La première formule est une conséquence immédiate de l'inversion de Möbius. Pour la deuxième, posons $r_n = \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) q^d$. Alors

$$|r_n| \leqslant \sum_{\substack{d|n\\ d\neq n}} q^d \leqslant \sum_{d=0}^{E\left(\frac{n}{2}\right)} q^d = \frac{q^{E\left(\frac{n}{2}\right)+1}-1}{q-1} \xrightarrow[n\to+\infty]{} \frac{1}{1-q}$$

donc en particulier, $r_n = o(q^n)$.

Ainsi, comme $I(n,q) = \frac{q^n + r_n}{n}$, on a $I(n,q) \sim_{n\to+\infty} \frac{q^n}{n}$. □

Référence : Patrice TAUVEL (2008). *Corps commutatifs et théorie de Galois*. Calvage et Mounet, p. 121.