DÉVELOPPEMENT 26

POLYNÔMES IRRÉDUCTIBLES DE $\mathbb{F}_q[T]$

Soit p un nombre premier et $f \geq 1$, on note $q = p^f$ et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Il existe un unique corps $\mathbb{F}_q$ à q éléments ; il s'agit du corps de décomposition de $X^f - X$ sur $\mathbb{F}_p$. On note $\mathbb{I}$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_q[T]$.

Proposition. — *Si $\Pi(n)$ est le nombre de polynômes unitaires irréductibles sur $\mathbb{F}_q$ alors*

$$\Pi(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Démonstration. — On a $\left(X^{q^n} - X\right)' = q^n X^{q^n-1} - 1 = -1$ (puisque q est une puissance de la caractéristique) donc le polynôme $X^{q^n} - X$ n'a que des racines simples et il s'ensuit que c'est le produit des polynômes irréductibles unitaires qui le divisent.

Si P est un tel polynôme et si α est une racine de P dans une clôture algébrique de $\mathbb{F}_q$ alors $\alpha^{q^n} - \alpha = 0$ *i.e.* $\alpha^{q^n} = \alpha$ donc $\alpha \in \mathbb{F}_{q^n}$; on a $\mathbb{F}_q \leq \mathbb{F}_q(\alpha) \leq \mathbb{F}_{q^n}$ d'où

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)] \cdot [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)] \cdot (\deg P)$$

donc $\deg P$ divise n.

Réciproquement, si le degré de P divise n et si α est une racine de P dans une clôture algébrique alors $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^{\deg P}}$ est un sous-corps de $\mathbb{F}_{q^n}$ donc $\alpha \in \mathbb{F}_{q^n}$ et il s'ensuit que $\alpha^{q^n} - \alpha = 0$. Ainsi, toute racine de P (dans une clôture algébrique) est une racine de $X^{q^n} - X$ donc P divise $X^{q^n} - X$, d'où

$$X^{q^n} - X = \prod_{\substack{P \in \mathbb{I} \\ \deg P | n}} P.$$

Il en résulte que

$$q^n = \deg(X^{q^n} - X) = \deg \prod_{\substack{P \in \mathbb{I} \\ \deg P | n}} P = \sum_{d|n} \sum_{\substack{P \in \mathbb{I} \\ \deg P = d}} d = \sum_{d|n} d\Pi(d).$$

En particulier, on a $n\Pi(n) \leq q^n$.

On rappelle que la fonction de Möbius μ est la fonction multiplicative définie sur $\mathbb{N}^*$ par $\mu(1) = 1$, $\mu(n) = 0$ si n a un facteur carré et $\mu(q_1 \cdots q_r) = (-1)^r$ si les q_j sont des premiers distincts. On a alors

Lemme. — *Soit $f, g : \mathbb{N}^* \to \mathbb{C}$ alors on a équivalence entre*

(i) $g(n) = \sum_{d|n} h(d)$ *pour tout* $n \geq 1$

(ii) $h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$ *pour tout* $n \geq 1$

On applique ce lemme pour $g(k) = q^k$ et $h(k) = k\Pi(k)$, d'où

$$n\Pi(n) = h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

On note $p(n)$ le plus petit facteur premier de n. Si d est un diviseur strict de n alors $\frac{n}{d} > 1$ admet un diviseur premier r donc d divise $\frac{n}{r}$ et on a

$$q^n = n\Pi(n) + \sum_{\substack{d|n \\ d<n}} d\Pi(d) \leq n\Pi(n) + \sum_{\substack{r|n \\ r \text{ premier}}} \sum_{d|\frac{n}{r}} d\Pi(d) \leq n\Pi(n) + \sum_{\substack{r|n \\ r \text{ premier}}} q^{\frac{n}{r}}.$$

Si r est un diviseur premier de n alors $r \geq p(n)$ donc $\frac{n}{r} \leq \frac{n}{p(n)}$ d'où

$$q^n \leq n\Pi(n) + \sum_{k=1}^{\frac{n}{p(n)}} q^k \leq n\Pi(n) + q^{\frac{n}{p(n)}} \left(1 + \frac{1}{q} + \cdots + \frac{1}{q^{\frac{n}{p(n)}}}\right) \leq n\Pi(n) + q^{\frac{n}{p(n)}} \frac{q}{q-1}.$$

On a donc

$$q^n - q^{\frac{n}{p(n)}} \frac{q}{q-1} \leq n\Pi(n) \leq q^n.$$

Puisque $p(n) \geq 2$, on en déduit que

$$\Pi(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right)$$

et si n est impair, on a $p(n) \geq 3$, d'où

$$\Pi(n) = \frac{q^n}{n} + O\left(\frac{q^{n/3}}{n}\right).$$

□

Remarque. — Notons l'analogie entre la formule

$$\Pi(n) = \frac{q^n}{\log_q q^n} + O\left(\frac{q^{n/2}}{n}\right)$$

et le théorème des nombres premiers

$$\pi(x) = \frac{x}{\log x} + O\left(xe^{-\alpha\sqrt{\log x}}\right).$$

Leçons concernées

01 Méthodes combinatoires, problèmes de dnombrements

12 Corps finis. Applications

14 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications

Référence

S. Francinou et H. Gianella, *Exercices d'algèbre 1*, Masson, 1993.