Sandrine CARUSO

Polynômes irréductibles de $\mathbb{F}_q$.

Référence : Francinou-Gianella, Exercices pour l'agrégation, algèbre 1

Proposition. *Soit $\mathbb{F}_q$ un corps fini de cardinal q. Pour tout $n \in \mathbb{N}^*$, il existe un polynôme irréductible sur $\mathbb{F}_q$ de degré n. Le nombre de tel polynômes est équivalent à $\frac{q^n}{n}$ lorsque $n \to \infty$.*

On note $A(n,q)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_q$, et $I(n,q) = \operatorname{Card} A(n,q)$.

Soit d un diviseur de n et P un polynôme irréductible de degré d. Montrons que P divise $X^{q^n} - X$. Soit $K = \mathbb{F}_q[X]/(P)$ un corps de rupture de P, et notons x la classe de X dans K. Comme $[K : P] = \deg P = d$, K est isomorphe à $\mathbb{F}_{q^d}$ et donc $x^{q^d} = x$. Par récurrence, on déduit du fait que d divise n que $x^{q^n} = x$. Donc P divise $X^{q^n} - X$.

Inversement, montrons que si P est un diviseur irréductible de $X^{q^n} - X$, alors le degré d de P divise n. Le polynôme $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$, notons x une racine de P dans $\mathbb{F}_{q^n}$, et $K = \mathbb{F}_q(x)$. Le corps K est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$, et $[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K][K : \mathbb{F}_q]$. Comme $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ et $[K : \mathbb{F}_q] = d$, on en déduit que d divise n.

Ainsi,

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

et en prenant le degré de ce polynôme, on obtient

$$q^n = \sum_{d|n} dI(d,q).$$

La formule d'inversion de Möbius donne alors

$$nI(n,q) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, q^d.$$

Notons

$$r_n = \sum_{\substack{d|n \\ d<n}} \mu\Big(\frac{n}{d}\Big)\, q^d$$

de sorte que $nI(n,q) = q^n + r_n$. On a la majoration

$$|r_n| \leqslant \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = q\frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1}.$$

D'une part, $|r_n| < q^n$, donc $I(n,q) > 0$, d'autre part, $|r_n| = O(q^{\lfloor \frac{n}{2} \rfloor}) = o(q^n)$ donc

$$I(n,q) \sim \frac{q^n}{n}.$$

Lemme (Fonction de Möbius)**.** *Rappelons que la fonction de Möbius* $\mu = \mathbb{N}^* \to \{0, -1, 1\}$ *est définie par* $\mu(n) = 0$ *si* n *a un facteur carré, et* $\mu(p_1 \cdots p_r) = (-1)^r$ *si* $p_1, \ldots, p_r$ *sont des nombres premiers distincts*[1]*. Elle vérifie les propriétés suivantes :*

(i) μ *est multiplicative,* ie *si* $\text{PGCD}(n, m) = 1$ *alors* $\mu(nm) = \mu(n)\mu(m)$*,*

(ii) *pour tout* $n > 1$*,* $\sum_{d|n} \mu(d) = 0$*,*

(iii) *Formule d'inversion de Möbius : si* $g(n) = \sum_{d|n} f(d)$*, alors*

$$f(n) = \sum_{d|n} \mu(d) g\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, g(d).$$

Démonstration. (i) Soient $n, m \in \mathbb{N}^*$ tels que $\text{PGCD}(n, m) = 1$. Si n ou m a un facteur carré, alors nm aussi et $\mu(nm) = \mu(n)\mu(m) = 0$. Sinon, on décompose n et m en facteurs carrés : $n = p_1 \cdots p_r$ et $m = q_1 \cdots q_s$. Comme n et m sont premiers entre eux, les p_i et q_i sont tous distincts, et nm est donc également sans facteurs carrés. On a alors $\mu(nm) = (-1)^{r+s}$ et $\mu(n)\mu(m) = (-1)^r(-1)^s = (-1)^{r+s}$.

(ii) On décompose n en facteurs premiers : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Alors

$$\begin{aligned}\sum_{d|n} \mu(d) &= \sum_{k=0}^{r} \sum_{i_1 < \cdots < i_k} \mu(p_{i_1} \cdots p_{i_k}) = \sum_{k=0}^{r} \sum_{i_1 < \cdots < i_k} (-1)^k \\ &= \sum_{k=0}^{r} \binom{r}{k} (-1)^k = (1-1)^r = 0\end{aligned}$$

car $r > 0$. Notons que pour $n = 1$, cette somme est égale à $\mu(1) = 1$.

(iii) On a

$$\begin{aligned}\sum_{d|n} \mu(d) g\Big(\frac{n}{d}\Big) &= \sum_{d|n} \mu(d) \sum_{d' | \frac{n}{d}} f(d') \\ &= \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d | \frac{n}{d'}} \mu(d) = f(n).\end{aligned}$$

L'autre égalité s'obtient par changement de variable $d \leftrightarrow \frac{n}{d}$ dans la somme. □

[1] Éventuellement, $r = 0$ si $n = 1$.