Polynômes irréductibles sur $\mathbb{F}_q$

S. Franciou, H. Gianella, *Exercices de mathématiques pour l'agrégation : Algèbre 1*, Masson. Exercice 5.10 page 189.

Recasage : 121, 123, 125, 141, 144, 190.

Théorème 1

Pour $n \in \mathbb{N}^*$, on note $A(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré n dans $\mathbb{F}_q[X]$ et $I(n,q)$ son cardinal. On a :

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

$\triangleright$ – *Étape 1 : Montrons que $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P$.*

$\star$ Soient un diviseur d de n et $P \in A(d,q)$. Soit x une racine de P et $K = \mathbb{F}_q(x)$ un corps de rupture de P. Comme P est irréductible, $[K : \mathbb{F}_q] = \deg(P) = d$ donc, par unicité des corps finis, $K = \mathbb{F}_{q^d}$. On en déduit en particulier que $x^{q^d} = 1$. Mais alors, comme $d|n$,

$$x^{q^n} = x^{(q^d)^{\frac{n}{d}}} = \left(x^{q^d}\right)^{(q^d)^{\frac{n}{d}-1}} = x^{(q^d)^{\frac{n}{d}-1}} = \cdots = x$$

par récurrence, donc x est racine de $X^{q^n} - X$. Comme P est irréductible sur $\mathbb{F}_q$, il est à racine simple sur toute extension de $\mathbb{F}_q$ (les corps finis sont parfaits). On a donc montré que $P|X^{q^n} - X$.

$\star$ Soit P un facteur irréductible de $X^{q^n} - X$ et notons d son degré. Comme $X^{q^n} - X$ est scindé dans $\mathbb{F}_{q^n}$, on peut considérer une racine $x \in \mathbb{F}_{q^n}$ de P. Alors, $K = \mathbb{F}_q(x)$ est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ donc

$$[\mathbb{F}_{q^n} : K] \underbrace{[K : \mathbb{F}_q]}_{d} = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$$

donc $d|n$. De plus, comme les racines de $X^{q^n} - X$ sont simples, ses facteurs irréductibles ont une multiplicité égale à 1. Comme $X^{q^n} - X$ est unitaire, on a donc montré que

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

– *Étape 2 : Inversion de Möbius.* En considérant les degrés dans l'égalité précédente, on obtient :

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

donc, par la formule d'inversion de Möbius :

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

d'où le résultat. □

Remarque : Notons $I(n,q) = \dfrac{q^n + r_n}{n}$ avec $r_n = \sum_{\substack{d|n \\ d<n}} \mu\left(\frac{n}{d}\right) q^d$. Alors,

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

On en déduit :

$\star$ $|r_n| < \dfrac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{q-1} \leq \dfrac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{\frac{q}{2}} = 2q^{\lfloor \frac{n}{2} \rfloor} \leq q^n$ donc pour tout $n \geq 1$, $I(n,q) > 0$: il existe donc des polynômes irréductibles sur $\mathbb{F}_q$ de tout degré.

$\star$ $|r_n| \leq \dfrac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{q-1} = o(q^n)$ donc $I(n,q) \underset{n \to +\infty}{\sim} \dfrac{q^n}{n}$.

Lemme 2 (*Inversion de Möbius*)

Soit $g : n \in \mathbb{N}^* \mapsto \sum_{d|n} f(d)$*. On a :*

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

$\triangleright$ – *Étape 1 : Montrons que* $\sum_{d|n} \mu(d) = \delta_{1,n}$. Si $n = 1$, le résultat est évident. Supposons $n > 1$ et notons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $\alpha_i \geq 1$ et p_i premiers distincts. Si $d|n$, on a $\mu(d) \neq 0$ si et seulement si d est sans facteurs carrés *ie.* $d = p_{i_1} \cdots p_{i_1} \cdots p_{i_k}$ avec $i_1, \ldots, i_k$ distincts. Alors,

$$\begin{aligned}
\sum_{d|n} \mu(d) &= \sum_{i=1}^{r} \underbrace{\mu(p_i)}_{-1} + \sum_{i \neq j} \underbrace{\mu(p_i p_j)}_{1} + \cdots + \underbrace{\mu(p_1 \cdots p_r)}_{(-1)^r} \\
&= \sum_{i=1}^{r} \binom{n}{i} (-1)^i = (1-1)^r = 0
\end{aligned}$$

– *Conclusion.* On en déduit que

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

$\square$