Titre : **Polynômes irréductibles sur $\mathbb{F}_q$**
Recasages : 123,125,141,190
Thème : Anneaux de polynômes, corps finis, théorie des nombres.
Références : Tauvel - Corps commutatifs et théorie de Galois (p. 120)

Théorème 1. *On note $\mathcal{P}_q(d)$ l'ensemble des polynômes irréductibles de degré d sur $\mathbb{F}_q$ ($q = p^\alpha$ est une puissance d'un nombre premier). Pour $n \in \mathbb{N}^*$, on a*

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

Pour $P \in \mathcal{P}_q(d)$, alors $K = \mathbb{F}_q[X]/(P)$ est un corps ($\mathbb{F}_q[X]$ est principal), de cardinal q^d, donc isomorphe à $\mathbb{F}_{q^d}$:

$$\forall x \in K, x^{q^d} = x$$

Mais si $n = dk$ pour un $k \in \mathbb{N}^*$, on a

$$x^{q^n} = x^{q^{dk}} = (((x^{q^d})^{q^d}) \cdots)^{q^d} \quad (k \text{ fois})$$

par une récurrence immédiate sur k, ceci est égal à x. Autrement dit, $X^{q^n} - X = 0 \in K[X]$, donc P divise $X^{q^n} - X$ dans $\mathbb{F}_q[X]$. Comme les éléments de $\mathcal{P}_q(d)$ sont irréductibles, le produit $\prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$ 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 $[F_{q^n} : \mathbb{F}_q] = n = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q]$, mais comme P est irréductible, $\mathbb{F}_q(x)$ est un corps de rupture de P de degré d sur $\mathbb{F}_q$, donc d divise n.
Il suffit alors de montrer que $X^{q^n} - X$ n'admet pas de facteur double (ou plus) : si 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 $q^n X^{q^n - 1} - 1 = -1$ (à cause de la caractéristique), $X^{q^n} - X$ n'a pas de racine double dans un corps de décomposition, ce qui termine la preuve.

Proposition 2. *(Inversion de Möbius)*
Soit $g : \mathbb{N}^* \to \mathbb{C}$, en posant $G(n) := \sum_{d|n} g(d)$, on a

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

Où $\mu : N^* \to \mathbb{C}$ est la fonction de Möbius[1]

Démonstration. Commençons par remarquer que pour $n \geqslant 2$ $\sum_{d|n} \mu(d) = 0$, en effet, si $n = \prod_{i=1}^r p_i^{\alpha_i}$, alors

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

1. 0 si n est divisible par un carré parfait non trivial, sinon $(-1)^k$ ou k est le nombre de premiers distincts divisant n

Ensuite, si $n \in \mathbb{N}^*$ et $d|n$, alors $d'|\frac{n}{d}$ si et seulement si $dd'|n$, on a donc

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

$\square$

<u>Corollaire</u> 3. *Si $I(q,d)$ désigne le cardinal de $P_q(d)$, alors pour $n \in \mathbb{N}^*$, on a*

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

Équivalent, quand $n \to +\infty$, à $\frac{q^n}{n}$.

Démonstration. La première formule est conséquence directe de l'inversion de Möbius, en remarquant que

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

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

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

donc $r_n = O(q^n)$, on conclut car $I(q,d) = \frac{q^n + r_n}{n}$. $\square$