Développement: polygones irréductibles sur un corps fini

Arthur Maritch-Roy

Dans ce développement, on s'intéresse à la proportion de polynômes irréductibles de degré donné dans $\mathbb{F}_q[X]$, qui peut être pratique à connaître si on veut donner rapidement une description de $\mathbb{F}_q$ en machine comme un corps de rupture pour pouvoir faire des calculs.

Théorème 1. Soit $\mathcal{P}_q(d)$ l'ensemble des polynômes irréductibles de degré d sur $\mathbb{F}_q$. Alors pour $n \in \mathbb{N}^*$:

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

Démonstration. Soit $P \in \mathcal{P}_q(d)$ et $K := \mathbb{F}_q[X]/(P)$. C'est un corps de cardinal q^d. Si d est un diviseur de n, on a alors $x^{q^d} = x$ pour tout x élément de K. Ainsi $P|(X^{q^n} - X)$ dans $\mathbb{F}_q[X]$. On peut donc faire le produit, qui divise bien $X^{q^n} - X$.

Réciproquement, soit P un facteur irréductible de degré d de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$, P est scindé sur $\mathbb{F}_{q^n}$ par unicité du corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_q$. Ainsi pour x racine de P :

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = n = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)]\, d$$

car P est irréductible. Donc d divise n. Par ailleurs, chaque facteur ne peut apparaître qu'une fois parce que $(X^{q^n} - X)' = -1$ donc $X^{q^n} - X$ est à racines simples dans un corps de décomposition. Ainsi on a exactement l'égalité voulue. □

Corollaire 2. Si $I(q, d)$ est le nombre de polynômes irréductibles de degré d sur $\mathbb{F}_q$, on a en passant au degré :

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

d'où, par inversion de Möbius :

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

Remarque 3. Puisque $r^n := \sum_{d|n, d\neq n} \mu\left(\frac{n}{d}\right) q^d \leq \sum_{d=0}^{\lfloor n/2 \rfloor} q^d \leq \frac{q^{\lfloor n/2 \rfloor + 1} - 1}{q-1} = \mathrm{O}(q^n)$ quand q tend vers l'infini, on a

$$I_(q, n) = \frac{q^n + r_n}{n} \sim_{q\to\infty} \frac{q^n}{n}.$$

Concluons avec deux propositions utilisées et/ou en partie redémontrées.

Proposition 4. (injections des corps finis)
Soit q une puissance d'un nombre premier. Alors $\mathbb{F}_{q^d} \hookrightarrow \mathbb{F}_{q^n}$ si et seulement si $d|n$.

Démonstration. Le sens direct vient du fait que si on a l'injection alors on peut munir le grand corps d'une structure d'espace vectoriel sur le petit. Le fait qu'il soit forcément de dimension finie permet de conclure. Pour la réciproque, on utilise le fait que si $d|n$ alors $q^d - 1$ divise $q^n - 1$, et donc dans ce cas que $X^{q^d-1} - 1$ divise $X^{q^n} - 1$. En multipliant par X, on obtient le fait que les racines de $X^{q^d} - X$ sont dans $\mathbb{F}_{q^n}$, et ce sont exactement les éléments de $\mathbb{F}_{q^d}$. □

Proposition 5. Soit q une puissance d'un nombre premier. Alors $\mathbb{F}_{q^n}$ est le corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_q$.

Démonstration. Puisque $(\mathbb{F}_{q^n})^*$ est un groupe de cardinal $q^n - 1$, tous les éléments de $\mathbb{F}_{q^n}$ sont racine de $X^{q^n} - X$. Ainsi, $X^{q^n} - X$ est scindé à racines simples sur $\mathbb{F}_{q^n}$ et ses racines sont exactement les éléments de ce corps. □