Polynômes irréductibles sur $\mathbb{F}_q$

Arnaud Girand

17 juin 2012

Référence :
- [FG97], p. 189–191

Prérequis :
- formule d'inversion de Möbius.

Soit p un nombre premier et soit $r \in \mathbb{N}^*$. On pose $q := p^r$ et on s'intéresse, pour $n \geq 1$, à l'ensemble $A(n,q)$ des polynômes de degré n irréductibles sur $\mathbb{F}_q$. On pose également $I(n,q) := \text{card}(A(n,q))$.

Proposition 1
Soit $n \geq 1$. Alors :

(*i*) *on a la factorisation suivante :*

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

(*ii*) *si on note μ la fonction de Möbius on a :*

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

(*iii*) *on a l'équivalent $I(n,q) \sim_{n\to\infty} \frac{q^n}{n}$.*

Démonstration :

(*i*) – Soit $d|n$ et soit $P \in A(d,q)$, dont on fixe une racine x dans une clôture algébrique de $\mathbb{F}_q$. $\mathbb{K} := \mathbb{F}_q(x)$ est alors un corps de rupture de P et $[K : \mathbb{F}_q] = \deg(P) = d$ donc $\mathbb{K} \cong \mathbb{F}_{q^d}$ (par "unicité" des corps finis). Or tout élément de $\mathbb{F}_{q^d}$ est racine du polynôme $X^{q^d} - X$, donc $x^{q^d} = x$ et alors :

$$x^{q^n} = \left(\left(\dots \left(x^{q^d} \right)^{q^d} \dots \right)^{q^d} \right)^{q^d} = x$$

De fait x est racine de $X^{q^n} - X$ donc P divise ce dernier polynôme. Par irréductibilité on a alors $\prod_{d|n} \prod_{P \in A(d,q)} P | X^{q^n} - X$.

– Soit P un facteur irréductible de $X^{q^n} - X$, de degré $d \geq 1$ et soit $x \in \mathbb{F}_{q^n}$ une racine de ce polynôme [1]. Si on pose à nouveau $\mathbb{K} := \mathbb{F}_q(x)$ on a $[\mathbb{F}_{q^n} : \mathbb{K}][\mathbb{K} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. De fait $d = [\mathbb{K} : \mathbb{F}_q]$ divise n.
De plus, les racines de $X^{q^n} - X$ dans $\mathbb{F}_{q^n}$ sont toutes simples, de fait ce polynôme est sans facteur carrés. On a donc bien et donc $X^{q^n} - X \mid \prod_{d|n} \prod_{P \in A(d,q)} P$.

– Les deux polynômes considérés étant unitaires, on a bien l'égalité voulue.

(*ii*) Passons au degré dans le résultat du (*i*) :

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

1. Qui est scindé sur ce dernier corps

En appliquant la formule d'inversion de Möbius à $g : n \mapsto q^n$ et $f : n \mapsto nI(n,q)$ on obtient alors :

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

(*iii*) Posons :

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

Alors :

$$\begin{aligned} |r_n| &\leq \sum_{d=1}^{\lfloor n/2 \rfloor} q^d \\ &= q\frac{q^{\lfloor n/2 \rfloor} - 1}{q-1} \\ &= \frac{q^{\lfloor n/2 \rfloor + 1}}{q-1} \end{aligned}$$

Ainsi :

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

Détails supplémentaires :

– Rappelons que la fonction de Möbius est définie comme suit :

$$\begin{aligned} \mu : \mathbb{N} &\to \{-1, 0, 1\} \\ n &\mapsto \begin{cases} 0 & \text{si } n \text{ a un facteur carré} \\ (-1)^k & \text{sinon, où } k \text{ est le nombre de facteurs premiers distincts de } n \end{cases} \end{aligned}$$

On a alors le résultat suivant :

Proposition 2 (Formule d'inversion de Möbius)
Soient $f, g : \mathbb{N} \to \mathbb{C}$ telles que :

$$\forall n \geq 1, \qquad g(n) = \sum_{d|n} f(d)$$

Alors :

$$\forall n \geq 1, \qquad f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

Références

[FG97] Serge Francinou and Hervé Gianella. *Exercices de mathématiques pour l'agrégation, Algèbre 1.* Masson, 1997.