Polynômes irréductibles sur $\mathbb{F}_q$

Leçons : 125, 141, 190, *123, 144*

[FG], exercices 3.11 et 5.10

Théorème

Soit p un nombre premier et $r \in \mathbb{N}^*$; on note $q = p^r$, soit $n \in \mathbb{N}^*$.
Soit $\mathcal{A}(n,q)$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ irréductibles unitaires de degré n et $I(n,q) = \#\mathcal{A}(n,q)$.
Alors :

1. On a la factorisation suivante dans $\mathbb{F}_q[X]$: $X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{A}(d,q)} P$.
2. Notant μ la fonction de Möbius [1], on a : $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.
3. On en déduit alors l'équivalent : $I(n,q) \underset{n\to\infty}{\sim} \frac{q^n}{n}$.

Démonstration :

On commence bien évidemment par fixer une bonne fois pour toutes une clôture algébrique $\overline{\mathbb{F}_q}$ de $\mathbb{F}_q$, dans laquelle on travaillera tout le long de ce développement.

1. – Soit $d|n$ et $P \in \mathcal{A}(d,q)$; fixons x une racine de P dans $\overline{\mathbb{F}_q}$.
   Alors $K := \mathbb{F}_q(x)$ est un corps de rupture de P et $[K : \mathbb{F}_q] = \deg P = d$ et donc, par unicité des corps finis : $K = \mathbb{F}_{q^d}$.
   Comme $\mathbb{F}_{q^d}$ est l'ensemble des racines de $X^{q^d} - X$ et que ce polynôme divise $X^{q^n} - X$, x est racine de $X^{q^n} - X$. [2]
   Donc $P \Big| X^{q^n} - X$, car P étant irréductible sur un corps fini, il est à racines simples dans $\overline{\mathbb{F}_q}$. [3]
   Puis, par irréductibilité, on en déduit : $\left(\prod_{d|n} \prod_{P \in \mathcal{A}(d,q)} P\right) \Big| X^{q^n} - X$.

   – Soit P un facteur irréductible de $X^{q^n} - X$, de degré $d \geqslant 1$.
   Comme $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$, P l'est aussi.
   Soit x racine de P, qui est donc dans $\mathbb{F}_{q^n}$; $K := \mathbb{F}_q(x)$ est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$.
   On a alors : $[\mathbb{F}_{q^n} : K][K : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ et donc $d = [K : \mathbb{F}_q]$ divise n.

1. Pour $k \in \mathbb{N}^*$, on définit μ par $\mu(k) = 0$ si k possède un facteur carré et $\mu(k) = (-1)^r$ sinon, où r désigne alors le nombre de facteurs premiers distincts de k.

2. En effet, $x^{q^n} = x^{\left(q^d\right)^{\frac{n}{d}}} = x^{q^d\left(q^d\right)^{\frac{n}{d}-1}} = \left(x^{q^d}\right)^{\left(q^d\right)^{\frac{n}{d}-1}} = x^{\left(q^d\right)^{\frac{n}{d}-1}} = \ldots = x^{\left(q^d\right)^0} = x$.

3. Démontrons ce fait général :

Lemme

Si K est un corps fini ou de caractéristique nulle, et si $P \in K[X]$ est un polynôme irréductible,
Alors P est à racines simples dans la clôture algébrique $\overline{K}$ de K.

En effet, soit α une racine multiple de P, alors $\exists Q \in \overline{K}[X], P = (X-\alpha)^2 Q$.
En dérivant, on obtient ensuite $P' = (X-\alpha)(2Q + (X-\alpha)Q')$, donc $(X-\alpha)|P'$ dans $\overline{K}[X]$.
Et finalement, $(X-\alpha)|P \wedge P'$ dans $\overline{K}[X]$.
Or $P \wedge P'|P$ dans $K[X]$ et $\deg P \wedge P' \geqslant 1$, donc, par irréductibilité de P, on a : $P = P \wedge P'$, et comme $\deg P' < \deg P$: $P' = 0$.
Si K est de caractéristique nulle, alors P est une constante donc nul ou inversible donc non-irréductible. On a donc une contradiction dans ce cas.
Sinon, K est de caractéristique $p > 0$ et $P \in K\left[X^p\right]$, d'où $P(X) = R\left(X^p\right) = R(X)^p$, avec $R \in K[X]$, car le morphisme de Frobenius est un automorphisme quand le corps est fini.
Pour terminer sur ce sujet, citons un contre-exemple sur un corps infini de caractéristique positive.
Soit $P = T^2 + X \in \mathbb{F}_2(X)[T]$.
P est irréductible, car il n'admet pas de racine dans $\mathbb{F}_2(X)$ (pour des problèmes de parité) et qu'il est de degré 2.
P admet une racine $\alpha = \sqrt{-X} \in \overline{\mathbb{F}_2(X)}$ et donc $P = (T-\alpha)(T+\alpha) = (T-\alpha)^2$ car $\overline{\mathbb{F}_2(X)}$ est un corps de caractéristique 2.

Les racines de $X^{q^n} - X$ dans $\mathbb{F}_{q^n}$ sont simples donc tous les facteurs irréductibles de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$ interviennent avec une multiplicité égale à 1.

Ainsi $X^{q^n} - X \left| \left(\prod_{d|n} \prod_{P \in \mathcal{A}(d,q)} P \right) \right.$.

– Les deux polynômes considérés étant unitaires, on en déduit $X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{A}(d,q)} P$.

2. **Lemme (*Formule d'inversion de Möbius*)**

Soit $f : \mathbb{N}^* \to \mathbb{R}$ et $g : \left| \begin{array}{ccc} \mathbb{N}^* & \to & \mathbb{R} \\ n & \mapsto & \sum_{d|n} f(d) \end{array} \right.$.
Alors $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$.

Démonstration :

Soit $n \in \mathbb{N}^*$, on a : $\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{d' \left| \frac{n}{d} \right.} \mu(d) f(d') = \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \left(\sum_{d \left| \frac{n}{d'} \right.} \mu(d) \right)$.

Soit désormais $k \in \mathbb{N}^*$, $k > 1$.
On écrit $k = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa décomposition en facteurs premiers, avec $r > 0$.
On a ensuite : $\sum_{d|k} \mu(d) = \mu(1) + \sum_{i=1}^{r} \sum_{1 \leqslant \gamma_1 < \dots < \gamma_i \leqslant r} \mu\left(p_{\gamma_1} \dots p_{\gamma_i}\right) + 0 = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = (1-1)^r = 0$.
Et si $k = 1$, $\sum_{d|1} \mu(d) = \mu(1) = 1$, ce qui nous donne donc $\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = f(n)$. ■

En regardant les degrés dans la factorisation précédente, on obtient : $q^n = \sum_{d|n} dI(d,q)$.

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

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

3. On pose $r_n = \sum_{\substack{d|n \\ d<n}} \mu\left(\frac{n}{d}\right) q^d$ et alors : $|r_n| \leqslant \sum_{i=1}^{\left\lfloor \frac{n}{2} \right\rfloor} q^d = q \frac{q^{\left\lfloor \frac{n}{2} \right\rfloor} - 1}{q-1} = \mathcal{O}_{n\to\infty}\left(q^{\left\lfloor \frac{n}{2} \right\rfloor}\right)$.

Donc r_n est négligeable devant q^n, d'où : $I(n,q) = \frac{q^n + r_n}{n} \underset{n\to\infty}{\sim} \frac{q^n}{n}$. ■

Références

[FG] S. FRANCINOU et H. GIANELLA – *Exercices de mathématiques pour l'agrégation (Algèbre 1)*, 2ème éd., Masson, 1997.