Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$

Référence : [FG97] p.189-191 ([Cal06]).

Proposition 0.1 *Pour $n \in \mathbb{N}^*$, on note $A(n,q)$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ irréductibles, unitaires et de degré n. On pose $I(n,q) = card(A(n,q))$. Alors :*

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

où μ désigne la fonction de Möbius.

Démonstration

Étape 1 Soit d un diviseur de n. Soit $P \in A(d,q)$. Montrons que P divise $X^{q^n} - X$.
Soit $K = \mathbb{F}_q(x)$ un corps de rupture de P, x étant une racine de P.
On a alors $[K : \mathbb{F}_q] = \deg(P) = d$.
Par conséquent K est isomorphe à $\mathbb{F}_{q^d}$ (par unicité des corps finis) et comme $\mathbb{F}_{q^d}$ est l'ensemble des racines de $X^{q^d} - X$, on a, en particulier :

$$x^{q^d} = x$$

Et comme d divise n, on a :

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

Donc x est racine du polynôme $X^{q^n} - X$, ainsi $X^{q^n} - X$ divise P.

Étape 2 Soit P un facteur irréductible unitaire de $X^{q^n} - X$. Montrons que $\deg(P)$ divise n.
On note $d = \deg(P)$. On sait que $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$. Si on note x une racine de P dans $\mathbb{F}_{q^n}$, $K = \mathbb{F}_{q^n}(x)$ est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ de degré d sur $\mathbb{F}_q$, par multiplicativité des degrés on a :

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

Alors $d = \deg(P)$ est bien un diviseur de n.

Étape 3 Montrons que :

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

et déduisons-en la formule voulue.
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 d'après les étapes 1 et 2, on a :

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

En regardant les degrés, on obtient :

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

La première formule d'inversion de Möbius appliquée à la fonction $n \longmapsto nI(n,q)$ donne alors :

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

Étape 5 Montrons la formule d'inversion de Möbius.

Lemme 0.1 *Soit μ la fonction de Möbius. Soit :*

$$\begin{aligned} g : \mathbb{N}^* &\longrightarrow \mathbb{R} \\ n &\longmapsto \sum_{d|n} f(d) \end{aligned}$$

où $f : \mathbb{N}^* \longrightarrow \mathbb{R}$.
Alors pour tout $n \geq 1$,

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

Démonstration Soit $n \geq 1$, on a :

$$\begin{aligned} \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \left(\sum_{d'|\frac{n}{d}} f(d') \right) \quad \text{par définition de } g\,; \\ &= \sum_{dd'|n} \mu(d) f(d') \quad \text{car } d|n \text{ et } d'|\frac{n}{d} \text{ est équivalent à } dd'|n\,; \\ &= \sum_{d'|n} f(d') \left(\sum_{d|\frac{n}{d'}} \mu(d) \right) \quad \text{car } d'|n \text{ et } d|\frac{n}{d'} \text{ est équivalent à } dd'|n\,; \\ &= f(n) \end{aligned}$$

Trucs utilisés

Définition 0.1 (Corps de rupture) *Soit $\mathbb{K}$ un corps. Soit P un polynôme irréductible et unitaire sur $\mathbb{K}[X]$. On appelle corps de rupture de P sur $\mathbb{K}$ toute extension simple $\mathbb{K}(\alpha)$ de $\mathbb{K}$ telle que le polynôme minimal de α sur $\mathbb{K}$ soit P.*

Définition 0.2 (Fonction de Möbius) *On appelle fonction de Möbius, l'application $\mu : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ telle que $\mu(1) = 1$, $\mu(d) = (-1)^k$ si d est produit de k nombres premiers distincts et $\mu(d) = 0$ si d est divisible par le carré d'un nombre premier.*

Définition 0.3 (Corps intermédiaire) *On dit que $\mathbb{K}'$ est un corps intermédiaire pour une extension $\mathbb{L}$ de $\mathbb{K}$ si $\mathbb{K} \subset \mathbb{K}' \subset \mathbb{L}$.*

Proposition 0.2 (Multiplicativité des degrés) *Soit $\mathbb{L}$ un extension de $\mathbb{K}$ et $\mathbb{M}$ une extension de $\mathbb{L}$, alors :*

$$[\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}] = [\mathbb{M} : \mathbb{K}]$$

Démonstration Soit $(x_i)_{i \in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$ et $(y_j)_{j \in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$ avec I et J non vides. Montrons que $(x_i y_j)_{(i,j) \in I \times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.
Soit $z \in \mathbb{M}$, alors il existe $(\alpha_j)_{j \in J} \in \mathbb{L}$ presque tous nuls tels que :

$$z = \sum_{j \in J} \alpha_j y_j$$

Or pour tout $j \in J$, $\alpha_j \in \mathbb{L}$, donc il existe $(\beta_{i,j})_{i \in I} \in \mathbb{K}$ presque tous nuls tels que :

$$\alpha_j = \sum_{i \in I} \beta_{i,j} x_i$$

D'où :

$$z = \sum_{j \in J} \sum_{i \in I} \beta_{i,j} x_i y_j$$

Supposons maintenant que :

$$\sum_{(i,j) \in I \times J} c_{i,j} x_i y_j = 0$$

les $c_{i,j} \in \mathbb{K}$ étant presque tous nuls.
Alors :

$$\sum_{j\in J}\left(\sum_{i\in I} c_{i,j}x_i\right) y_j = 0$$

Or $(y_j)_{j\in J}$ est une base de $\mathbb{M}$ sur $\mathbb{L}$ et pour tous $j \in J$, $\sum_i c_{i,j}x_i \in \mathbb{L}$, donc :

$$\sum_{i\in I} c_{i,j}x_i = 0$$

Donc le fait que $c_{i,j} = 0$ car $(x_i)_{i\in I}$ est une base de $\mathbb{L}$ sur $\mathbb{K}$.
Ainsi, on a montré que $(x_i y_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$, de plus $card(I\times J) = card(I)\times card(J)$ d'où le résultat.

Références

[Cal06] Josette Calais. *Eléments de la théorie des anneaux.* Ellipses, 2006.

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