Dénombrement des polynômes unitaires irréductibles sur un corps fini :

I Le développement

Le but de ce développement est de déterminer le nombres de polynômes irréductibles sur un corps fini $\mathbb{F}_q$ en utilisant la fonction de Möbius.

On commence avec un résultat préliminaire sur la fonction de Möbius.

Lemme 1 : [Francinou, p.93]
Pour tout $n \in \mathbb{N}^*$, on a :

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$$

Preuve :
Soit $n \in \mathbb{N}^*$.
$*$ Si $n = 1$, alors $\sum_{d|n} \mu(d) = \mu(1) = 1$.

$*$ Sinon, en notant $n = \prod_{i=1}^r p_i^{\alpha_i}$ la décomposition en facteurs premiers de n, on a alors par la définition de la fonction de Möbius :

$$\sum_{d|n} \mu(d) = 1 + \sum_{i=1}^{r} \mu(p_i) + \sum_{\substack{1 \leq i,j \leq r \\ i \neq j}} \mu(p_i p_j) + \ldots + \mu(p_1 \ldots p_r)$$
$$= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \ldots + \binom{r}{r}(-1)^r = (1-1)^r = 0$$

Finalement, on a bien la formule voulue.

■

Théorème 2 : Formule d'inversion de Möbius [Francinou, p.93] :
Soient A un groupe abélien et $f : \mathbb{N}^* \longrightarrow A$.
Si l'on pose $g(n) = \sum_{d|n} f(d)$, alors $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.

Preuve :
Soient A un groupe abélien, $f : \mathbb{N}^* \longrightarrow A$ et $g(n) = \sum_{d|n} f(d)$.

On remarque tout d'abord que pour tous $d, d' \in \mathbb{N}^*$, on a l'équivalence entre ($d|n$ et $d'|\frac{n}{d}$) et ($d'|n$ et $d|\frac{n}{d'}$).

On a alors pour tout $n \in \mathbb{N}^*$:

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{\tilde{d}|n} \mu\left(\tilde{d}\right) g\left(\frac{n}{\tilde{d}}\right) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d)$$
$$\underset{(\text{lm.})}{=} f(n)$$

■

Théorème 3 : [Francinou, p.189]
Si l'on note $A(n,q)$ l'ensemble des polynômes irréductibles, unitaires et de degré n sur $\mathbb{F}_q$, alors on a l'égalité $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P(X)$.

Preuve :
On note $A(n,q)$ l'ensemble des polynômes unitaires irréductibles et de degré n sur le corps $\mathbb{F}_q$.
$*$ Soit $P \in A(d,q)$ un facteur irréductible (unitaire) de $X^{q^n} - X$ de degré noté d.
On considère x une racine symbolique de P et $\mathbb{F}_q(x)$ un corps de rupture de P. On a alors l'inclusion :

$$\mathbb{F}_q \subseteq \mathbb{F}_q(x) \subseteq \mathbb{F}_{q^n} \quad (\text{car } \mathbb{F}_{q^n} \text{ est le corps de décomposition de } X^{q^n} - X \text{ dans } \mathbb{F}_q)$$

Ainsi, par le théorème de la base télescopique, on a :

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

Or, on a $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ et $[\mathbb{F}_q(x) : \mathbb{F}_q] = \deg(P) = d$ (car P est irréductible), donc d divise n.

$*$ Réciproquement, soit $P \in A(d,q)$ tel que d divise n.
On considère x une racine symbolique de P et $\mathbb{K}$ un corps de rupture de P.
On a alors $[\mathbb{K} : \mathbb{F}_q] = d$ (car P est irréductible) et par unicité des corps finis à l'isomorphisme près, on a alors $\mathbb{K} \cong \mathbb{F}_{q^d}$.

Ainsi, $x \in \mathbb{K}$ peut être vu comme un élément de $\mathbb{F}_{q^d}$ et donc (puisque d divise n) :

$$x^{q^n} = x^{q^{kd}} = \left(x^{q^d}\right)^{q^{(k-1)d}} = x^{q^{(k-1)d}} = ... = x^{q^d} = x$$

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

Finalement, puisque $X^{q^n} - X$ est scindé à racines simples (donc sans facteurs carrés), on obtient donc que $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P(X)$ $(*)$.

■

Corollaire 4 : [Francinou, p.189]
En notant $I(n,q) = \mathrm{Card}(A(n,q))$, on a :

$$I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \text{ et } \forall q \geq 2,\ I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$$

Preuve :
On note $I(n,q) = \mathrm{Card}(A(n,q))$.
En regroupant les degrés dans la formule $(*)$ de la preuve précédente, on obtient que :

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

Donc en posant $g : n \longmapsto q^n$ et $f : d \longmapsto dI(n,q)$, par la formule d'inversion de Möbius, on a :

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

Ainsi, on obtient :

$$I(n,q) = \frac{q^n + r_n}{n} \text{ où } r_n = \sum_{\substack{d|n \\ d \neq n}} \mu\left(\frac{n}{d}\right) q^d$$

Or, on a :

$$|r_n| \leq \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = q\frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1} \leq \frac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{q-1} \quad (**)$$

Donc :

$$I(n,q)\frac{n}{q^n} = 1 + \frac{r_n}{q^n} \underset{n \to +\infty}{\longrightarrow} 1$$

Finalement, on en déduit que $I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$.

■

II Remarques sur le développement

II.1 Résultat(s) utilisé(s)

On a utilisé dans ce développement la fonction de Möbius dont on rappelle la définition :

Définition 5 : Fonction de Möbius [Berhuy, p.151] :
On appelle **fonction de Möbius** la fonction μ définie par :

$$\mu : \left| \begin{array}{ccl} \mathbb{N}^* & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & \begin{cases} (-1)^r & \text{si } n \text{ est produit de } r \text{ nombres premiers distincts} \\ 0 & \text{s'il existe un nombre premier } p \text{ tel que } p^2 \text{ divise } n \end{cases} \end{array} \right.$$

On a également utilisé un résultat important sur les corps finis :

Théorème 6 : [Perrin, p.73]
Soient p un nombre premier et $n \in \mathbb{N}^*$.
Si l'on pose $q = p^n$, alors il existe un corps $\mathbb{K}$ à q éléments (c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$).
En particulier, $\mathbb{K}$ est unique à isomorphisme près et on le note $\mathbb{F}_q$.

II.2 Pour aller plus loin...

$*$ Il est possible de déterminer, lorsque n et p sont petits, l'ensemble des polynômes irréductibles de degré n dans l'anneau $\mathbb{F}_q[X]$. Pour cela, on peut par exemple utiliser la méthode du crible. Par exemple, pour $q = 2$, on a :

$$A(1,2) = \{X, X+1\},\ A(2,2) = \{X^2+X+1\} \text{ et } A(3,2) = \{X^3+X+1,\ X^3+X^2+1\}$$

Si les valeurs de q ou de n sont grandes, on peut implémenter l'algorithme de Berlekamp pour factoriser le polynôme $X^{q^n} - X$ avec un ordinateur.

$*$ Le corollaire du développement possède une interprétation très profonde :
Pour tous $n, q \in \mathbb{N}^*$, $I(n,q) \geq 1$. Ainsi, il existe au moins un polynôme irréductible de degré quelconque n dans $\mathbb{F}_p$ (c'est-à-dire que $\mathbb{F}_{p^n}$ existe toujours en tant que corps).

II.3 Recasages

Recasages : 123 - 125 - 141 - 190.

III Bibliographie

— Serge Francinou, *Exercices de mathématiques pour l'agrégation, Algèbre 1*.

— Grégory Berhuy, *Algèbre : le grand combat*.

— Daniel Perrin, *Cours d'algèbre*.