Développement : Nombre de polynômes irréductibles à coefficients dans un corps fini

Algèbre & Géométrie

Référence : [BER] Berhuy G., *Algèbre : le grand combat*, **2ème édition**, Calvage & Mounet, 2018, p655. (réf exacte à vérifier)
Pour le lemme : même référence, p155.
Pour les leçons :
- 123 : Corps finis. Applications.
- 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- 190 : Méthodes combinatoires, problèmes de dénombrement.

Soit p un nombre premier, et soit $q = p^a$ avec $a \in \mathbb{N}^*$. On note $\mathbb{F}_q$ l'unique corps fini à q éléments.
Le but de ce développement est de calculer le nombre de polynômes irréductibles unitaires à coefficients dans $\mathbb{F}_q$ de degré $n \in \mathbb{N}^*$, qu'on note $I_{n,q}$. Pour tout $d \in \mathbb{N}^*$, on note $\mathcal{U}_d(q)$ l'ensemble des polynômes irréductibles unitaires à coefficients dans $\mathbb{F}_q$ de degré d. On a donc $I_{n,q} = |\mathcal{U}_d(q)|$.

Définition 1. ***Fonction de*** Möbius**.**

On appelle *fonction de* Möbius l'application définie sur $\mathbb{N}^*$ par :

$$\forall n \in \mathbb{N}^* \quad \mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \neq 1 \text{ a un facteur carré} \\ (-1)^k & \text{si } n = p_1 \cdots p_k \text{ avec les } p_i \in \mathbb{P} \text{ distincts} \end{cases}.$$

On admet le lemme suivant :

Lemme 2.

μ est multiplicative et pour tout $n \in \mathbb{N}^*$, $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geqslant 2 \end{cases}$ (la somme étant indexée sur les diviseurs positifs de n).

Preuve : On admettra le lemme au tableau (d'autant plus que le fait que μ soit multiplicative n'est pas vraiment utile), mais si le jury demande, il faut en connaître une preuve... En voici donc une.
Soient $n, m \in \mathbb{N}^*$ premiers entre eux.
$\longrightarrow$ Si $n = 1$, on a $\mu(nm) = \mu(m) = \mu(n)\mu(m)$. De même si $m = 1$.
Ensuite, si $n = 1$, l'unique diviseur positif de n est 1, donc $\sum_{d|n} \mu(d) = \mu(1) = 1$.
$\longrightarrow$ Supposons que $n \geqslant 2$ et $m \geqslant 2$. Comme $n \wedge m = 1$, n et m n'ont pas de facteur commun. On écrit donc $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $m = q_1^{\beta_1} \cdots q_s^{\beta_s}$, avec $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s \in \mathbb{N}^*$, et les p_i, q_i des nombres premiers tous distincts.
Si n ou m a un facteur carré, nm aussi donc $\mu(nm) = 0 = \mu(n)\mu(m)$.
Sinon, comme $n \wedge m = 1$, n et m n'ont pas de facteur commun nm n'a pas de facteur carré.
En outre, $\mu(nm) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(n)\mu(m)$, ce qui prouve que μ est multiplicative.
Ensuite,

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{\substack{1 \leqslant i \leqslant r \\ 0 \leqslant k_i \leqslant \alpha_i}} \mu(p_1^{k_1} \cdots p_i^{k_i}) \\ &= \sum_{\substack{1 \leqslant i \leqslant r \\ k_i \in \{0;1\}}} \mu(p_1^{k_1} \cdots p_i^{k_i}) \\ &= \sum_{j=0}^{r} \sum_{\substack{1 \leqslant i \leqslant r \\ k_i \in \{0;1\}, |k| = j}} (-1)^j \\ &= \sum_{j=0}^{r} \binom{r}{j} (-1)^j \\ &= (1 + (-1))^r \\ &= 0, \end{aligned}$$

par binôme de Newton. □

Lemme 3. ***Formule d'inversion de*** MÖBIUS**.**

Soit $f : \mathbb{N}^* \to \mathbb{R}$ une application. Pour $n \in \mathbb{N}^*$, on pose $g(n) = \sum_{d|n} f(d)$. Alors :

$$\forall n \in \mathbb{N}^* \quad f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

PREUVE : Soit $n \in \mathbb{N}^*$. D'après la définition de g, on a :

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

Or, pour tout $d, d' \geqslant 1$, on a :

$$\begin{cases} d|n \\ d'|\dfrac{n}{d} \end{cases} \iff \begin{cases} d'|n \\ d|\dfrac{n}{d'} \end{cases}.$$

(L'implication directe se démontre en revenant à la définition de la divisibilité, et l'implication réciproque est vraie par symétrie du problème).
Ainsi, d'après le lemme précédent,

$$\begin{aligned} \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d'|n} \sum_{d|\frac{n}{d'}} \mu(d) f(d') \\ &= \sum_{d'|n} f(d') \underbrace{\sum_{d|\frac{n}{d'}} \mu(d)}_{=\delta_{\frac{n}{d'},1} = \delta_{n,d'}} \\ &= f(n). \end{aligned}$$

D'où le résultat. □

Lemme 4.

Soit $n \in \mathbb{N}^*$.
[1] Pour tout $d|n$ et $P \in \mathcal{U}_d(q)$, $P | X^{q^n} - X$.
[2] Si $P \in \mathbb{F}_q[X]$ est irréductible et si $P | X^{q^n} - X$, alors $\deg(P) | n$.

PREUVE : **[1]** Soient $d|n$ et $P \in \mathcal{U}_d(q)$. Soit $\mathbb{K} = \mathbb{F}_q(x)$ un corps de rupture de P, où $x \notin \mathbb{F}_q$ est une racine de P. On a donc $[\mathbb{K} : \mathbb{F}_q] = \deg(P) = d$, puisque P est irréductible.
Par unicité des corps finis, $\mathbb{K} \cong \mathbb{F}_{q^d} = \mathrm{Rac}(X^{q^d} - X)$ (racines de $X^{q^d} - X$). En particulier, $x^{q^d} = x$ et :

$$\begin{aligned} x^{q^n} &= \underbrace{((x^{q^d})^{\cdots})^{q^d}}_{n/d \text{ fois}} \\ &= \underbrace{((x^{q^d})^{\cdots})^{q^d}}_{\frac{n}{d}-1 \text{ fois}} \\ &= \cdots = x^{q^d} \\ &= x. \end{aligned}$$

Donc x est racine de $X^{q^n} - X$. Cela prouve que P divise $X^{q^n} - X$.
[2] Soit $P \in \mathbb{F}_q[X]$ irréductible divisant $X^{q^n} - X$. Posons $d = \deg(P)$. $X^{q^n} - X$ est scindé dans $\mathbb{F}_{q^n}$, donc P aussi. Il existe donc $x \in \mathbb{F}_{q^n}$ tel que $P(x) = 0$.
Posons alors $\mathbb{K} = \mathbb{F}_q(x)$. Par multiplicativité des degrés, on a :

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

Donc $d = [\mathbb{K} : \mathbb{F}_p]$ divise n. □

Théorème 5.

Pour tout $n \in \mathbb{N}^*$, $I_{n,q} = \dfrac{1}{n} \sum_{d|n} \mu\left(\dfrac{n}{d}\right) q^d$.

Preuve : On sait que $X^{q^n} - X = \prod_{d|n} P_d$, où les P_d sont le produit des polynômes irréductibles unitaires de $\mathbb{F}_q[X]$ de degré d. Le degré de P_d est en outre $dI_{d,q}$.
Par passage au degré, on a donc $q^n = \prod_{d|n} dI_{d,q}$.

D'après la formule d'inversion de Möbius (**??**), $nI_{n,q} = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.

Cela achève la preuve. □

Corollaire 6.

$I_{n,q} \underset{n\to+\infty}{\sim} \frac{q^n}{n}$.

Preuve : Soit $n \in \mathbb{N}^*$. En majorant grossièrement, on a :

$$nI_{n,q} \leqslant \sum_{d|n} dI_{d,q} = q^n.$$

Donc $I_{n,q} \leqslant \frac{q^n}{n}$.
Ensuite, en posant $r_n = \sum_{\substack{d|n \\ d<n}} \mu\left(\frac{n}{d}\right) q^d$, on a $I_{n,q} = \frac{q^n + r_n}{n}$, donc $nI_{n,q} - q^n = r_n$. Il vient :

$$\begin{aligned} q^n - nI_{n,q} &\leqslant \sum_{\substack{d|n \\ d<n}} q^d \\ &\leqslant \sum_{d=1}^{\lfloor n/2 \rfloor} q^d \\ &\leqslant \frac{q^{\lfloor n/2 \rfloor} - 1}{q-1} \\ &\leqslant q^{\lfloor n/2 \rfloor}, \end{aligned}$$

en majorant le numérateur par $q^{\lfloor n/2 \rfloor}$ et $\frac{1}{q-1} \leqslant 1$.
Ainsi, $I_{n,q} \geqslant \frac{q^n - q^{\lfloor n/2 \rfloor}}{n}$, ce qui donne :

$$1 - q^{\lfloor n/2 \rfloor - n}. \leqslant \frac{I_{n,q}}{q^n/n} \leqslant 1.$$

Comme $\lfloor n/2 \rfloor - n < 0$, par passage à la limite, on en déduit le résultat. □