Développement : Nombre de polynômes irréductibles unitaires sur un corps fini

MATHIEU Alix - alix89.mathieu@gmail.com

Sommaire

1 Pré-requis

Définition 1.1 : (Fonction de Mobius)
On définit la Fonction de Mobius μ sur $\mathbb{N}^*$ à valeurs dans $\{-1, 0, 1\}$ par :

$$\text{si } n = \prod_{i=1}^{r} p_i^{\alpha_i},\ \mu(n) = \begin{cases} 0 \text{ s'il existe } i \in \{1, \cdots, r\}, \text{ tel que } \alpha_i > 1 \\ (-1)^r \text{ si } n = p_1 \dots p_r \end{cases}$$

2 Développement

Lemme 2.1 :

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

Preuve :
Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$,

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{r} \mu(p_i) + \sum_{1 \leq i < j \leq r} \mu(p_i p_j) + \cdots + \mu(p_1 \dots p_r) \\ &= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \cdots + \binom{r}{r}(-1)^r \\ &= (1-1)^r \text{ en reconaissant un binôme de Newton} \\ &= 0 \end{aligned}$$

■

Proposition 2.2 :

Soit $f : \mathbb{N}^* \to \mathbb{C}$. On pose $g(n) = \sum_{d|n} f(d)$. Alors

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

Preuve :
Soit $n \geq 1$, alors

$$\begin{aligned}
\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) &= \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') \\
&= \sum_{dd'|n} \mu(d) f(d') \\
&= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) \\
&= f(n) \text{ par le lemme 1}
\end{aligned}$$

■

Théorème 2.3 :
On note $A(n, q)$ l'ensemble des polynômes irréductibles et unitaire de degré n sur le corps $\mathbb{F}_q$
Alors :

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

Preuve :
On effectue la preuve par double divisiblité.

▷ Soit $d \mid n$ et $P \in A(d, q)$. Notons $K := \mathbb{F}_q(x)$ un corps de rupture de P, où x est une racine symbolique de P. Alors $[K : \mathbb{F}_q] = \deg(P) = d$ donc par unicité à isomorphisme près des corps finis, on a : $K \simeq \mathbb{F}_{q^d}$.

Or $\mathbb{F}_{q^d}$ correspond au corps de décomposition du polynôme $X^{q^d} - X$ donc en particulier, on a $x^{q^d} = x$ et comme $d \mid n$, on a :

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

Ainsi x est une racine de $X^{q^n} - X$ et donc toute racine de P est une racine de $X^{q^n} - X$. De plus, comme P est irréductible, on a donc $P \mid X^{q^n} - X$ et donc :

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

▷ Si on considère $P \in A(d,q)$ un facteur irréductible de $X^{q^n} - X$. Comme $\mathbb{F}_{q^n}$ correspond au corps de décomposition du polynôme $X^{q^n} - X$, ce polynôme est donc scindé sur $\mathbb{F}_{q^n}$. Si l'on note maintenat x une racine de P dans $\mathbb{F}_{q^n}$ et $K = \mathbb{F}_q(x)$. On a la tour d'extension suivante :

$$K \subseteq \mathbb{F}_q(x) \subseteq \mathbb{F}_{q^n}$$

Par le théorème de la base téléscopique : $\underbrace{[\mathbb{F}_{q^n} : \mathbb{F}_q]}_{=n} = [\mathbb{F}_{q^n} : K] \underbrace{[K : \mathbb{F}_q]}_{=\deg(P)=d}$ donc $d \mid n$

Or les racines de $X^{q^n} - X$ sont simples dans $\mathbb{F}_{q^n}$ (de dérivée $= 1$) et donc les facteurs irréductibles de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$ interviennent avec multiplicité 1. Ainsi :

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

d'où l'égalité par caractère unitaire. ■

COROLLAIRE 2.4 :
En notant $I(n,q) = \#(A(n,q))$, on a :

$$I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d \quad \text{et} \quad I(n,q) \sim \frac{q^n}{n}$$

PREUVE :
En considérant les degrés dans l'égalité du théorème :

$$q^n = \sum_{d \mid n} d I(d,q)$$

donc en posant $f : d \longmapsto dI(d,q)$, on a donc en posant $g(n) = q^n$ par la proposition 2.2 que :

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

i.e.

$$I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d = \frac{q^n + r_n}{n} \quad \text{où} r_n := \sum_{\substack{d \mid n \\ d \neq n}} \mu\left(\frac{n}{d}\right) q^d$$

Pour conclure, il suffit donc de montrer que $r_n = o(q^n)$. Mais on peut déjà majorer comme suit :

$$|r_n| \leq \sum_{d=1}^{E(n/2)} q^d = q \frac{q^{E(n/2)} - 1}{q - 1} \underset{q \geq 2}{\leq} q^{E(n/2)+1}$$

où $E(n/2)$ correspond à la partie entière de $n/2$. ceci montre que $r_n = o(q^n)$. On a finalement donc montré que

$$I(n,q) \sim \frac{q^n}{n}$$

■

3 Remarques et bibliographie

REMARQUE

▷ Il serait bon d'avoir des idées de preuve sur les résultats suivants utilisées dans le développement : binome de Newton, base telescopique, unicité corps finis (à isomorphisme)

▷ Dans le dernier corollaire, j'effectue une majoration dans la somme mais pourquoi y'a-t-il au plus $\frac{n}{2}$ diviseurs pour un entier n : Quels sont les diviseurs possible de n et leurs "copains de divisions" :

$$1 -> n\ ,\ 2 -> \frac{n}{2}\ ,\ 3 -> \frac{n}{3}\ , \cdots$$

On observe qu'en regardant les diviseurs de n qui ne sont pas n, le plus grand entier possible divisant n hors n est $n/2$. Il y a donc au plus $E(n/2)$ entiers.

Bibliographie : Francinou, Gianella - Exercices pour l'agrégation