Dénombrement des polynômes irréductible de $\mathbb{F}_q[X]$

Lemme . — **Formule d'inversion de Möbius.** Soient $f, g : \mathbb{N}^* \to G$ avec G un groupe abélien telles que $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d)$. Alors

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

avec μ la fonction de Möbius.

Preuve :
On introduit $S_n := \sum_{d|n} \mu(d)$. On a $S_1 = 1$. Pour $n \geq 2$, on pose P l'ensemble des diviseurs premiers de n et on a

$$S_n = \sum_{D \subset P} \mu\left(\prod_{d \in D} d\right) = \sum_{D \subset P} (-1)^{|D|} = \sum_{i=0}^{|P|} \binom{|P|}{i} (-1)^i = (1-1)^{|P|} = 0.$$

On a alors

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

□

Théorème . Le nombre de polynômes irréductible de degré n dans $\mathbb{F}_q[X]$ est

$$\frac{q-1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Preuve :
On commence par montrer que $P := X^{q^n} - X = \prod_{d|n} \prod_{D \in I_q^d} D$, où I_q^n est l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_q[X]$ de degré n.

En effet, soit D un diviseur irréductible unitaire P de degré d. Soit $\alpha \in \mathbb{F}_{q^n}$ une racine de D, car D divisant P et P étant scindé sur $\mathbb{F}_{q^n}$ par définition, les racines de D sont dans $\mathbb{F}_{q^n}$.
Alors D est irréductible sur $\mathbb{F}_q$ et $D(\alpha) = 0$ donc c'est le polynôme minimal de α sur $\mathbb{F}_q$.
D'après le théorème de la base téléscopique, on a

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

donc $d = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ divise $n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$.

Réciproquement, soient d un diviseur de n et D un polynôme irréductible unitaire de degré d. Soit $\mathbb{F}_q(\alpha)$ un corps de rupture de D. Alors

$$\mathbb{F}_q(\alpha) \simeq \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n},$$

car $d|n$, et ainsi α est aussi une racine de P. Or D est irréductible sur $\mathbb{F}_q$ donc il est à racines simples dans $\mathbb{F}_{q^n}$, donc D divise P.

Or P est scindé à racines simples sur $\mathbb{F}_{q^n}$, car $P' = -1$ dans $\mathbb{F}_{q^n}[X]$, donc chaque diviseur irréductible de P est de multiplicité 1, donc

$$P = \prod_{d|n} \prod_{D \in I_q^d} D.$$

On a alors en passant au degré

$$q^n = \sum_{d|n} d|I_q^n|.$$

Grâce à la formule d'inversion de Möbius, on en déduit

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

et la formule finale en multipliant par $q-1$ car on a compté seulement les polynômes irréductibles unitaires.

□

Remarque On utilise le fait qu'un polynôme irréductible dans $\mathbb{F}_q[X]$ est à racines simples dans un corps où il est scindé. Ici, D est scindé sur $\mathbb{F}_{q^n}$ et irréductible sur $\mathbb{F}_q$. En voici une preuve.
Supposons par l'absurde qu'il existe $\alpha \in \mathbb{F}_{q^n}$ une racine double de D. Alors D est irréductible sur $\mathbb{F}_q$ et $D(\alpha) = 0$ donc D est le polynôme minimal de α sur $\mathbb{F}_q$. Or $D'(\alpha) = 0$ et $\deg(D') < \deg(D)$ donc $D' = 0$. Ainsi, on a $D = R^p$ avec $R \in \mathbb{F}_q[X]$, ce qui est absurde car D est irréductible dans $\mathbb{F}_q[X]$.