Polynômes irréductibles sur $\mathbb{F}_q$

Théorème 1. Soient p un nombre premier, r un entier positif non nul et $q = p^r$. Notons $A(n,q)$ l'ensemble des polynômes irréductibles de $\mathbb{F}_q[X]$ unitaires de degré n et $I(n,q) = \text{Card}A(n,q)$.

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P, \;\; I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{n\to\infty}{\sim} \frac{q^n}{n}.$$

Démonstration. Soit d un diviseur de n. Soient $P \in A(d,q)$ et x une racine de P dans $\overline{\mathbb{F}_q}$. Le corps $K = \mathbb{F}_q(x)$ est un corps de rupture de P et $[K/\mathbb{F}_q] = \deg P = d$. Par unicité des corps finis, $K = \mathbb{F}_{q^d}$ l'ensemble des racines de $X^{q^d} - X$. Or, $X^{q^d} - X | X^{q^n} - X$, donc x est racine de $X^{q^n} - X$. En effet, en itérant n/d fois,

$$x^{q^n} = x^{q^d} x^{q^{n-d}} = x^{q^{n-d}} = \cdots = x.$$

Puisque P est à racines simples [1], P divise $X^{q^n} - X$. Par irréductibilité,

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

Réciproquement, soit P un facteur irréductible de $X^{q^n} - X$ de degré $d \geq 1$. Le polynôme $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$, donc P l'est aussi. Soit x une racine de P et notons comme précédemment $K = \mathbb{F}_q(x)$, corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$. Le degré d divise n car :

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

Les racines de $X^{q^n} - X$ sont simples, donc la multiplicité des facteurs irréductibles de $X^{q^n} - X$ est 1 :

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

Ces deux polynômes étant unitaires, ils sont égaux, ce qui donne le premier point du théorème. En prenant le degré, il vient :

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

La formule d'inversion de Möbius appliquée à $n \mapsto nI(n,q)$ assure alors que :

$$\forall n \in \mathbb{N}^*, \; nI(n,q) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Or, seul le dernier terme de la somme est prépondérant, puisque :

$$r_n = \sum_{d|n,\, d<n} \mu\left(\frac{n}{d}\right) q^d \leq \sum_{d=1}^{\lfloor n/2 \rfloor} q^d \underset{n\to\infty}{=} O\left(q^{\lfloor n/2 \rfloor}\right), \;\; I(n,q) = \frac{q^n + r_n}{n} \underset{n\to\infty}{\sim} \frac{q^n}{n}.$$

D'où le résultat souhaité. □

Lemme 2 (Formule d'inversion de Möbius)**.** Pour $f : \mathbb{N}^* \to \mathbb{R}$, notons $\varphi_f : n \in \mathbb{N}^* \mapsto \sum_{d|n} f(d)$. Alors,

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

1. En effet, si $P = (X-\alpha)^2 Q$, alors $X - \alpha$ divise $P \wedge P'$ donc par irréductibilité $P = P \wedge P'$. En caractéristique nulle P est constant et en caractéristique finie p, $P \in K[X^p]$, i.e. $P = R(X^p) = R(X)^p$, ce qui est absurde.

Démonstration. Commençons par calculer la somme suivante, pour $d = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, décomposition avec $r \geq 1$:

$$\sum_{d'|d} \mu(d') = \mu(1) + \sum_{k=1}^{r} \sum_{\gamma_1 < \dots < \gamma_k} \mu(p_{\gamma_1} \dots p_{\gamma_k}) + 0 = \sum_{k=0}^{r} \binom{n}{k} (-1)^k = 0.$$

Ainsi, puisque pour $k = 1$ la somme ci-dessus vaut 1, il vient :

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

□