

---

## Polynômes irréductibles sur $\mathbb{F}_q$

---

**Recasage** : 123 / 125 / 141 / 144 / 190

**Référence** : Francinou- Gianella "Exercices de mathématiques pour l'agrégation" p.189

### Théorème 1

Soit  $n \in \mathbb{N}^*$ , on note  $A(n, q)$  l'ensemble des polynômes irréductibles unitaire de degré  $n$  dans  $\mathbb{F}_q[X]$  et  $I(n, q)$  son cardinal alors on a :

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

où  $\mu$  désigne la fonction de Möbius.

**Preuve.**

► Commençons par montrer que  $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(n, q)} P$ .

- On commence par montrer que si  $d|n$  et  $P \in A(d, q)$  alors  $P|X^{q^n} - X$ . Soit  $x$  une racine de  $P$ , alors en posant  $K = \mathbb{F}_q(x)$  un corps de rupture du polynôme  $P$  on a que  $[K : \mathbb{F}_q] = d$ . Ainsi  $\mathbb{F}_{q^d}(x)$  est de cardinal  $q^d$  et donc par unicité des corps finis il est isomorphe à  $\mathbb{F}_{q^d}$ . Cependant  $\mathbb{F}_{q^d}$  est le corps de décomposition du polynôme  $X^{q^d} - X$ . Or  $\mathbb{F}_{q^d}^*$  est un groupe multiplicatif de cardinal  $q^d - 1$  en vertu du théorème de Lagrange il vient alors que  $x^{q^d} = x$ . Or comme  $d|n$  on a alors que  $n = kd$  et ainsi on peut écrire :

$$x^{q^n} = x^{q^{kd}} = \underbrace{\left( \left( \left( x^{q^d} \right)^{q^d} \dots \right)^{q^d} \right)^{q^d}}_{k \text{ fois}} = \underbrace{\left( \left( \left( x^{q^d} \right)^{q^d} \dots \right)^{q^d} \right)^{q^d}}_{k-1 \text{ fois}} = \dots = x^{q^d} = x$$

Ainsi  $x$  est une racine de  $X^{q^n} - X$  d'où  $P|X^{q^n} - X$ .

- Réciproquement montrons que si  $P$  est un diviseur irréductible (unitaire) de  $X^{q^n} - X$  alors  $d|n$ . Soit  $P$  un diviseur irréductible de  $X^{q^n} - X$ , notons alors  $d$  le degré de  $P$ . Comme dis précédemment  $\mathbb{F}_{q^n}$  est le corps de décomposition du polynôme  $X^{q^n} - X$ , il est donc scindé dans ce corps. Soit  $x$  une racine de  $P$  dans  $\mathbb{F}_{q^n}$  donc en posant  $K = \mathbb{F}_q(x)$  un corps de rupture du polynôme  $P$  et en particulier on a  $\mathbb{F}_q \subset \mathbb{F}_q(x) \subset \mathbb{F}_{q^n}$  et en vertu du théorème de la base télescopique :

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

Et en particulier  $[\mathbb{F}_q : K] = d$  donc  $d|n$

Comme les racines de  $X^{q^n} - X$  sont simples dans  $\mathbb{F}_{q^n}$  donc tous les facteurs irréductibles  $X^{q^n} - X$  interviennent avec multiplicité 1. Finalement on a bien démontré que

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

► En regardant les degrés dans la formule  $(\star)$  on obtient  $q^n = \sum_{d|n} dI(d, q)$ . En appliquant la formule d'inversion de Möbius à  $n \mapsto nI(n, q)$  on obtient alors :

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

On peut également montrer que  $I(n, q) \underset{n \rightarrow \infty}{\sim} \frac{q^n}{n}$ . En effet en écrivant :

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

On pose alors  $r_n = \sum_{\substack{d|n \\ d \neq n}} q^d \mu\left(\frac{n}{d}\right)$  et on majore on sait que  $|\mu\left(\frac{n}{d}\right)| \leq 1$  par définition et pour  $d|n$  on a  $n = kd$  ainsi  $d = \frac{n}{k} \leq \lfloor \frac{n}{2} \rfloor$  Ainsi :

$$\begin{aligned} |r_n| &= \left| \sum_{\substack{d|n \\ d \neq n}} q^d \mu\left(\frac{n}{d}\right) \right| \leq \sum_{\substack{d|n \\ d \neq n}} \left| q^d \mu\left(\frac{n}{d}\right) \right| \\ &\leq \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = q \frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q - 1} < q^{\lfloor \frac{n}{2} \rfloor + 1} \leq q^{\frac{n}{2} + 1} \end{aligned}$$

Donc  $nI(n, q) \geq q^n + q^{\frac{n}{2} + 1} \geq 0$  et donc  $\left| \frac{nI(n, q)}{q^n} - 1 \right| < \frac{q^{\frac{n}{2} + 1}}{q^n} = \frac{1}{q^{\frac{n}{2}} - 1} \xrightarrow{n \rightarrow \infty} 0$ . Finalement  $I(n, q) \underset{n \rightarrow \infty}{\sim} \frac{q^n}{n}$ . ■