FG 3.11 5.10 — Polynômes irréductibles sur $\mathbb{F}_q$. — 141, 130

Théorème : Soit p premier. Notons $q = p^r$, $r \in \mathbb{N}^*$.
Soit $A(n,q)$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ irréductibles, unitaires de degré n. Notons $I(n,q) = \#A(n,q)$.

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

Soit $d \mid n$. Soit $P \in A(d,q)$. Soit x racine de P dans $\overline{\mathbb{F}_q}$.
Le corps $K = \mathbb{F}_q(x)$ est un corps de rupture de P et $[K : \mathbb{F}_q] = \deg P = d$.
Donc par unicité des corps finis, $K = \mathbb{F}_{q^d}$, ensemble des rac. de $X^{q^d} - X$.
$X^{q^d} - X \mid X^{q^n} - X$ donc x racine de $X^{q^n} - X$
(En effet, $x^{q^n} = x^{q^d \times q^{n-d}} = x^{(q^d)^{\frac{n}{d}-1}} = \dots = x$)
Donc $P \mid X^{q^n} - X$ car P à racines simples dans $\overline{\mathbb{F}_q}$.

> En effet, si $P = (X-\alpha)^2 Q$, alors $X - \alpha \mid P \wedge P'$ donc par irréductibilité, $P = P \wedge P'$. En particulier, $P \mid P'$, donc $P' = 0$.
> → En car nulle, P constant, absurde.
> → En car. $p > 0$, $P \in K[X^p]$. $P(X) = R(X^p) = R(X)^p$, absurde.

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

- Soit P facteur irréductible de $X^{q^n} - X$ de degré $d \geq 1$.
$X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$ donc P aussi. Soit x racine de P. Posons $K = \mathbb{F}_q(x)$ corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$. $[\mathbb{F}_{q^n} : K][K : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.
d $[\mathbb{F}_{q^n} : K]$ donc $d \mid n$.

Les racines de $X^{q^n} - X$ sont simples, donc la multiplicité des facteurs irréductibles de $X^{q^n} - X$ est 1 : $X^{q^n} - X \mid \prod_{d \mid n} \prod_{P \in A(d,q)} P$.

Puisque ces deux polynômes sont unitaires : $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in A(d,q)} P$.

La formule d'inversion à $f : n \mapsto n I(n,q)$ assure, puisque $q^n = \sum_{d \mid n} d I(d,q)$ par le degré : $\forall n \in \mathbb{N}^*$, $n I(n,q) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$
$r_n = \sum_{\substack{d \mid n \\ d < n}} \mu\left(\frac{n}{d}\right) q^d$ donc $|r_n| \leq \sum_{d=1}^{\lfloor n/2 \rfloor} q^d \underset{n \to +\infty}{=} O\left(q^{\lfloor n/2 \rfloor}\right)$, donc $I(n,q) = \frac{q^n + r_n}{n} \sim \frac{q^n}{n}$