Polynômes irréductibles sur $\mathbb{F}_q$

Définitions/Notations : Dans la suite on se donne un nombre premier p et $q = p^r$ où r est un entier naturel non nul. On se donne aussi $n \in \mathbb{N}^*$. On note alors

- $\mathcal{A}(n,q) = \{\text{polynômes irréductibles unitaires de degré } n \text{ sur } \mathbb{F}_q\}$
- $I(n,q) = \#\mathcal{A}(n,q)$

Théorème : Dans $\mathbb{F}_q[X]$ on a l'égalité suivante :

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

Corollaire : On a l'équivalent suivant en $+\infty$:

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

Lemme : Soit $\mathbb{K}$ un corps fini de caractéristique p et $P \in \mathbb{K}[X]$. Si P est irréductible alors il est à racines simples dans un corps de décomposition.

Preuve du lemme : Soit $\mathbb{L}$ un corps de décomposition de P et supposons par l'absurde qu'il existe $\alpha \in \mathbb{L}$ racine double de P sur $\mathbb{L}$. On peut alors écrire $P(X) = (X-\alpha)^2 Q(X)$ où $Q \in \mathbb{L}[X]$. Mais alors

$$P'(X) = 2(X-\alpha)Q(X) + (X-\alpha)^2 Q'(X)$$

donc $(X-\alpha) | P \wedge P'$ ce qui implique que $\deg(P \wedge P') > 0$. Mais P est irréductible et $P \wedge P' | P$ donc $P \wedge P' = P$ (car non constant). Comme $\deg(P') < \deg(P)$ il vient que $P' = 0$ donc $P \in \mathbb{K}[X^p]$. Comme $\mathbb{K}$ est de caractéristique p il existe $Q(X) \in \mathbb{K}[X]$ tel que $P(X) = Q(X^p) = Q(X)^p$ d'où l'absurdité car alors P n'est pas irréductible si Q n'est pas constant.

Preuve du théorème : i) Soit $d|n$ et $P \in \mathcal{A}(d,q)$. Dans la suite on note $\mathbb{L}$ la clôture algébrique de $\mathbb{F}_q$. Soit $\alpha \in \mathbb{L}$ une racine de P. Soit $\mathbb{K} = \mathbb{F}_q(x)$ un corps de rupture de P qui contient x. On a alors $[\mathbb{K} : \mathbb{F}_q] = d$. Par unicité des corps finis $\mathbb{K}$ est isomorphe à $\mathbb{F}_q^d$. Ce dernier corps peut être vu comme l'ensemble des racines du polynôme $X^{q^d} - X$. Or ce polynôme divise $X^{q^n} - X$. En effet, il existe un réel m tel que $q^{d\frac{n}{d}} - 1 = (q^d - 1)m$ donc il existe un polynôme $R(X)$ tel que $X^{q^{d\frac{n}{d}}-1} - 1 = (X^{q^d-1} - 1)R(X)$ et finalement $X^{q^n} - X = (X^{q^d} - X)R(X)$.

Ainsi x est racine de $X^{q^n} - X$. Comme P est irréductible le lemme nous dit qu'il est à racines simples sur $\mathbb{L}$. On vient de montrer que P est à racines simples sur $\mathbb{L}$ et que toutes ses racines sont aussi racines de $X^{q^n} - X$, cela suffit à montrer que $P | X^{q^n} - X$.

ii) Soit P un diviseur de $X^{q^n}-X$ irréductible unitaire de degré d. Comme $X^{q^n}-X$ est scindé sur $\mathbb{F}_{q^n}$, P l'est aussi. On peut donc se donner une racine x de P. On a alors une tour d'extension de corps $\mathbb{F}_q \subset \mathbb{F}_q(x) \subset \mathbb{F}_{q^n}$ d'où par multiplicativité des degrés $[\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Comme P est irréductible, $[\mathbb{F}_q(x) : \mathbb{F}_q] = d$ d'où $d|n$.

iii) Les racines de $X^{q^n}-X$ sont simples dans $\mathbb{F}_{q^n}$ (son polynôme dérivé est constant égale à -1) donc si P est un diviseur irréductible de $X^{q^n}-X$ il intervient exactement une fois dans sa décomposition. On déduit alors de i) et ii) le résultat du théorème. □

Preuve du corollaire : En regardant les degrés de la décomposition précédente il vient $q^n = \sum_{d|n} dI(d,q)$ d'où $nI(n,q) \leq q^n$ pour tout n. On a alors

$$q^n \geq nI(n,q) \geq q^n - \sum_{d|n} q^d \geq q^n - \sum_{d=0}^{\lfloor \frac{n}{2} \rfloor} q^d = q^n - \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q-1} \geq q^n - q^{\frac{n}{2}+1}.$$

ce qui permet de conclure en divisant ces inégalités par q^n. □

Remarques importantes :

- Il faut être plutôt à l'aise avec les différentes considérations sur les extension de corps
- La preuve du corollaire est plutôt succinctes, n'hésitez pas à la retravailler de votre côté