Polynômes irréductibles de $\mathbb{F}_q$

Références : Francinou, Gianella, *Exercices de mathématiques pour l'agrégation - Algèbre 1*, 5.10 et 3.11

Théorème.

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

- $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P$,
- $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$,
- On a l'équivalent $I(n,q) \sim \frac{q^n}{n}$,
- Il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_q$.

Démonstration. • Soit d un diviseur de n, $P \in A(d,q)$ et x une racine de P dans $\overline{F_q}$, alors $[\mathbb{F}_q(x) : \mathbb{F}_q] = d$ et donc $\mathbb{F}_q(x)$ est isomorphe à $\mathbb{F}_{q^d}$. En particulier, x est racine de $X^{q^d} - X$ car $\mathbb{F}_{q^d}$ est le corps de décomposition de ce polynôme. Or $X^{q^d} - X | X^{q^n} - X$ car $d|n$, donc x est racine de $X^{q^n} - X$. [1]
Les polynômes irréductibles étant à racines simples sur $\overline{F_q}$, on a $P | X^{q^n} - X$. [2]
Par décomposition en irréductibles, on a donc $\prod_{d|n} \prod_{P \in A(d,q)} P | X^{q^n} - X$.

• Soit P un diviseur irréductible unitaire de $X^{q^n} - X$, on note d son degré et on choisit x une de ses racines sur $\mathbb{F}_{q^n}$ (où P est scindé). Alors on a la tour d'extensions de corps $\mathbb{F}_q \subset \mathbb{F}_q(x) \subset \mathbb{F}_{q^n}$, donc par le théorème de la base télescopique : $[\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Donc $d = [\mathbb{F}_q(x) : \mathbb{F}_q] | n$.
De plus, comme $X^{q^n} - X$ est à racines simples, chaque facteur irréductible, n'apparaît qu'une fois.
On en déduit donc que $\prod_{d|n} \prod_{P \in A(d,q)} P = X^{q^n} - X$ car notre décomposition contient bien tous les polynômes irréductibles (car il faut $d|n$ et chacun d'eux n'apparaît qu'une fois) et de plus les membres des deux côtés sont unitaires.

• En regardant les degrés dans l'égalité précédente, on voit que $q^n = \sum_{d|n} dI(d,q)$. On a besoin de la formule d'inversion de Möbius pour poursuivre. [3]

1. En effet, on sait que $X^{q^d} - X$ est à racines simples, et si x en est une racine, alors $x^{q^n} = x^{(q^d)^{\frac{n}{d}}} = x^{q^d (q^d)^{\frac{n}{d}-1}} = x^{(q^d)^{\frac{n}{d}-1}} = \ldots = x$
2. On utilise le résultat suivant :

Lemme.

Si K est un corps fini ou de caractéristique nulle, et si $P \in K[X]$ est un polynôme irréductible, alors P est à racines simples dans la clôture algébrique $\overline{K}$ de K.

Démonstration. Si P a une racine double α, alors $P = (X-\alpha)^2 Q$, donc $X - \alpha | P'$ et $X - \alpha | P \wedge P'$, donc comme P est irréductible et $P \wedge P' | P$, on a $P' = 0$.
Si K est de caractéristique nulle, cela implique $P = cste$, ce qui est absurde.
Si K est de caractéristique p, alors $P = R(X^p)$. Or si K est fini, le Frobenius est un automorphisme et $P = R_0(X)^p$ (en changeant les coefficients avec le Frobenius), ce qui est absurde.

□

En fait, on vient de prouver que les corps finis et les corps de caractéristique nulle sont parfaits, càd que toutes leurs extensions sont séparables. On peut trouver un théorème plus général dans le Calais à la page 44.

Il est bon de savoir que c'est faux en général si K est un corps infini de caractéristique p non nulle. Par exemple, $P(T) = T^p - X$ est irréductible sur le corps $\mathbb{F}_p(X)$ par un argument de degré. Mais si on prend une racine α dans une extension, alors $X = \alpha^p$ et $P(T) = T^p - \alpha^p = (T-\alpha)^p$.

3. On rappelle que la fonction de Möbius est définie par $\mu(n) = 0$ si n a un facteur irréductible carré, et $\mu(n) = (-1)^r$ si $n = p_1 \ldots p_r$ avec les p_i tous distincts et irréductibles.

Lemme (Première formule d'inversion de Möbius)**.**

Soit $f : \mathbb{N}^* \to \mathbb{R}$ et $g : n \in \mathbb{N}^* \mapsto \sum_{d|n} f(d)$, alors

$$\forall n \geqslant 1, f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Démonstration. On passe d'une somme à l'autre en posant le changement de variable $d' = \frac{n}{d}$ dans la somme.
Prouvons donc $f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$.

→ Soit $k = p_1^{\alpha_1} ... p_r^{\alpha_r}$ avec $r > 0$, alors $\sum_{d|k} \mu(d) = \mu(1) + \sum_{i=1}^{r} \sum_{1 \leqslant \gamma_1 < ... < \gamma_i \leqslant r} \mu(p_{\gamma_1} ... p_{\gamma_r}) = 1 + \sum_{i=1}^{r} \sum_{1 \leqslant \gamma_1 < ... < \gamma_i \leqslant r} (-1)^i =$
$\sum_{i=0}^{r} (-1)^i \binom{r}{i} = (1-1)^r = 0.$

→ On a $\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d)$. Or on a vu que si $\frac{n}{d'} \neq 1$,
alors $\sum_{d|\frac{n}{d'}} \mu(d) = 0$, donc $\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = f(n) \sum_{d|1} \mu(d) = f(n)$. □

• Ceci étant fait, on a $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$. Puis pour l'équivalent, on pose $r_n = \sum_{d|n, d \neq n} \mu\left(\frac{n}{d}\right) q^d$, alors
$|r_n| \leqslant \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - q}{q-1}$.
En particulier, $|r_n| \leqslant \frac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{q-1}$ donc $|r_n| = o(q^n)$. Ainsi, comme $I(n,q) = \frac{q^n + r_n}{n}$, on a l'équivalent voulu.

• On a vu que $\sum_{d|n, d \neq n} q^d < q^n$. Donc $I(n,q) > 0$.
Cela donne l'existence de polynômes irréductibles de tout degré. □

Corollaire.

Toute extension **de degré fini** sur $\mathbb{F}_q$ est une extension simple, normale et séparable.

Démonstration. • Une extension est simple si elle peut s'écrire sous la forme $\mathbb{F}_q(x)$.
Soit $\mathbb{K}$ une extension de degré fini de $\mathbb{F}_q$. Par unicité des corps finis, si n est le degré de $\mathbb{K}$, alors $\mathbb{K} = \mathbb{F}_{q^n}$. Comme il existe des polynômes irréductibles de tout degré, $\mathbb{F}_{q^n}$ est un corps de rupture d'un polynôme irréductible de degré n sur $\mathbb{F}_q$. Cela prouve le résultat.

• Une extension est normale si tout polynôme irréductible de $\mathbb{F}_q$ admettant une racine dans cette extension est scindé.
Soit P un tel polynôme et x une telle racine. Notons n le degré de P. Alors la formule du théorème montre que P est scindé sur $\mathbb{F}_{q^n}$. Or $\mathbb{F}_q(x)$ est un sous-corps de $\mathbb{F}_{q^n}$ de degré n. Donc $\mathbb{F}_q(x) = \mathbb{F}_{q^n}$ et l'extension est normale.

• Une extension $\mathbb{K}$ est séparable si le polynôme minimal sur $\mathbb{F}_q$ de tout élément α de $\mathbb{K}$ n'a que des racines simples dans un corps de décomposition.
On a vu que $\mathbb{F}_q$ est parfait. Donc toute extension de $\mathbb{F}_q$ est séparable. □