Polynômes irréductibles sur $\mathbb{F}_q$

Leçons : 123, 125, 141, 144, 190.

Énoncés :

• Lemme : pour $n \geq 1$ on pose $\mu(n) = \begin{cases} (-1)^k \text{ si } n \text{ est produit de } k \in \mathbb{N} \text{ nb premiers} \neq \\ 0 \text{ sinon} \end{cases}$:

c'est la fonction de Möbius. On a la formule d'inversion de Möbius : si $f, g : \mathbb{N}^* \to \mathbb{C}$ tq $\forall n \geq 1$, $f(n) = \sum_{d \mid n} g(d)$, alors $\forall n \geq 1$, $g(n) = \sum_{d \mid n} f(d)\, \mu\left(\frac{n}{d}\right)$.

• Prop : $\mathbb{F}_q$ un corps fini, $P \in \mathbb{F}_q[X]$ irréductible unitaire. Si L est un corps de rupture de P sur $\mathbb{F}_q$ et $\alpha \in L$ une racine de P, on a dans $L[X]$: $P = \prod_{i=0}^{\deg P - 1} (X - \alpha^{q^i})$. En particulier L est un corps de décomposition de P.

• Th : $\mathbb{F}_q$ un corps fini. Pour $n \geq 1$ on note $\mathcal{I}_n$ l'ens des polynômes de $\mathbb{F}_q[X]$ irréductibles unitaires de degré n, et $I_n = |\mathcal{I}_n|$. Si $n \geq 1$ on a $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in \mathcal{I}_d} P$.

De plus $I_n = \frac{1}{n} \sum_{d \mid n} q^d \mu\left(\frac{n}{d}\right)$ et $I_n \underset{n \to +\infty}{\sim} \frac{q^n}{n}$.

⊛ Lemme.

• D'abord on mq si $n \geq 1$, $\sum_{d \mid n} \mu(d) = \delta_{1,n}$. Si $n = 1$, bien sûr $\sum_{d \mid 1} \mu(d) = \mu(1) = 1$. Sinon soit p un facteur premier de n, de valuation $\alpha = v_p(n)$. Puisque p^α et $p^{-\alpha} n$ sont premiers entre eux et que que μ est manifestement multiplicative (cad $\mu(mn) = \mu(m)\mu(n)$ qd $m \wedge n = 1$), $\sum_{d \mid n} \mu(d) = \sum_{d_1 \mid p^\alpha} \sum_{d_2 \mid p^{-\alpha} n} \mu(d_1 d_2)$

$= \left(\sum_{d_1 \mid p^\alpha} \mu(d_1) \right) \left(\sum_{d_2 \mid p^{-\alpha} n} \mu(d_2) \right)$. Mais $\sum_{d_1 \mid p^\alpha} \mu(d_1) = \sum_{i=0}^{\alpha} \mu(p^i) = \mu(1) + \mu(p) = 1 - 1 = 0$. Donc $\sum_{d \mid n} \mu(d) = 0$.

• Montrons la formule d'inversion. Pour $n \geq 1$: $\sum_{d \mid n} f(d)\, \mu(\gamma d) = \sum_{d \mid n} \sum_{d' \mid d} g(d')\, \mu(\gamma d) = \sum_{d' \mid n} \sum_{k \mid \gamma d'} g(d')\, \mu\left(\frac{n}{k d'}\right)$

$= \sum_{d' \mid n} g(d') \sum_{k \mid \gamma d'} \mu(k)$, en effectuant le changement $d = k d'$. Mais d'après ce qui précède $\sum_{k \mid \gamma d'} \mu(k) = \delta_{1, \gamma d'} = \delta_{n d'}$

donc $\cdots = g(n)$; c'est la formule. □

⊛ Prop.

$x \mapsto x^q$ est un $\mathbb{F}_q$-automorphisme de L (ses itérées également) donc pour $i \in \mathbb{N}$, α^{q^i} est racine de P. Soit $k \geq 1$ minimal tq $\alpha^{q^k} = \alpha$. Si $0 \leq i < j \leq k-1$ vérifiant $\alpha^{q^j} = \alpha^{q^i}$, $\alpha^{q^{j-i}} = \alpha$ (en appliquant l'inverse de $x \mapsto x^{q^i}$), mais $1 \leq j - i \leq k-1$: c'est absurde. Donc $(\alpha^{q^i})_{0 \leq i \leq k-1}$ sont k racines distinctes de P. Soit $Q = \prod_{i=0}^{k-1} (X - \alpha^{q^i})$: ses coefficients sont fixés par $x \mapsto x^q$ (car $\{\alpha^{q^i} ; 0 \leq i \leq k-1\}$ l'est) donc $Q \in \mathbb{F}_q[X]$. On a $Q \mid P$, donc $P = Q$ et $k = \deg P$. □

⊛ Th.

- On note $Q = \prod_{d|n} \prod_{P \in \mathcal{I}_d} P$. Si $d|n$ et $P \in \mathcal{I}_d$. P est à racines simples et est scindé sur $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$ (d'après la prop qui précède par ex) donc $P \mid \prod_{x \in \mathbb{F}_{q^n}} (X - x) = X^{q^n} - X$. Les polynômes apparaissant dans Q sont 2à2 premiers entre eux donc $Q \mid X^{q^n} - X$.
On peut écrire $X^{q^n} - X = QR$ avec $R \in \mathbb{F}_q[X]$; soit par l'absurde S un facteur irréd de R. Si $d = \deg S$, le corps de rupture de S est inclus dans $\mathbb{F}_{q^n}$ (car $S \mid X^{q^n} - X$) donc $d|n$. Ainsi $S \in \mathcal{I}_d$, et $S^2 \mid X^{q^n} - X$. C'est absurde puisque $X^{q^n} - X$ est sans facteur carré. Donc R est constant ; puisque $X^{q^n} - X$ et Q sont unitaires, ils sont égaux.
- En passant aux degrés on obtient $q^n = \sum_{d|n} d\, I_d$. D'une part la formule d'inversion de Möbius donne $n I_n = \sum_{d|n} q^d \mu(n/d)$. D'autre part $q^n - n I_n = \sum_{\substack{d|n \\ d \neq n}} d\, I_d$. Le nb de polynômes unitaires de deg d sur $\mathbb{F}_q$ est q^d donc $I_d \leq q^d$ et $\ldots \leq \sum_{\substack{d|n \\ d \neq n}} d\, q^d \leq n \sum_{i=0}^{\lfloor n/2 \rfloor} q^i = n \dfrac{q^{\lfloor n/2 \rfloor + 1} - 1}{q - 1}$.
Mais $q^{\lfloor n/2 \rfloor + 1} - 1 \underset{n \to \infty}{=} O(q^{n/2})$ donc ce qui précède est en $O(q^n)$ quand $n \to \infty$, ce qui signifie $q^n \underset{n \to \infty}{\sim} n I_n$ et donc $I_n \underset{n \to \infty}{\sim} \dfrac{q^n}{n}$. □

Complément : corollaire de la prop : si K est une extension finie de $\mathbb{F}_q$, $\mathrm{Aut}(K/\mathbb{F}_q) \simeq \mathbb{Z}/d\mathbb{Z}$ avec $d = [K : \mathbb{F}_q]$ et est engendré par $\beta_q : x \mapsto x^q$.

Preuve. Prenons $\alpha \in K$ tq $K = \mathbb{F}_q(\alpha)$. Soit $g \in \mathrm{Aut}(K/\mathbb{F}_q)$: g est déterminé par $g(\alpha)$ (en effet tout $x \in K$ s'écrit $P(\alpha)$ avec $P \in \mathbb{F}_q[X]$ et alors $g(x) = P(g(\alpha))$). $g(\alpha)$ est racine de $\pi_\alpha \in \mathbb{F}_q[X]$ donc d'après la prop $g(\alpha) = \alpha^{q^i}$ pour un $0 \leq i \leq d-1$; ainsi $g \in \{\beta_q^0, \ldots, \beta_q^{d-1}\}$. Ces d automorphismes sont distincts et forment un groupe cyclique, dont β_q est un générateur. □

Réf : Tauvel – Corps commutatifs et théorie de Galois : p 12 (lemme), p 120 (th).

↳ Pour le lemme, plus généralement $*$ déf par $\beta * g(n) = \sum_{d|n} \beta(d) g(n/d)$ est une loi de corps interne sur $\mathbb{C}^{\mathbb{N}^*}$ qui est associative, commutative, admet δ_1 pour neutre, et stabilise l'ensemble des fonctions multiplicatives ($\beta \in \mathbb{C}^{\mathbb{N}^*}$ tq $\beta(1) = 1$ et si $m \wedge n = 1$, $\beta(mn) = \beta(m)\beta(n)$). On a mq la fonction ζ égale à 1 admet μ comme inverse. On a fait les preuves dans des cas particuliers des prop précédentes.

↳ La prop améliore le recasage dans 144 (à la fois l'énoncé et la preuve).

↳ La preuve du th est, au début, légèrement différente de celle de la réf (ici on a montré la prop donc autant l'utiliser). Pour avoir que P est scindé à racines simples sur $\mathbb{F}_{q^d}$, la réf dit grâce $P = \pi_\alpha$ pour un $\alpha \in \mathbb{F}_{q^d}$, alors $X^{q^d} - X$ annule α, et $P \mid X^{q^d} - X$.