Polynômes irréductibles de $\mathbb{F}_q$.

Réf : (• I. Gozard, Théorie de Galois)
• S. Francinou, H. Gianella, Exercices de mathématiques pour l'agrégation : Algèbre 1.

Leçons : 123, 141, 125, 144, 190

Notations : • p un nombre premier.
• $n \in \mathbb{N}^*$
• $q := p^n$, $n \in \mathbb{N}^*$.
• $\mathbb{K}(q,k)$: ensemble des polynômes irréductibles unitaires de degré k sur $\mathbb{F}_q$.
• $I(q,k) = |\mathbb{K}(q,k)|$.

Objectif : déterminer $I(p,k)$, et un équivalent lorsque $k \to +\infty$.

Théorème 1 $X^{q^m} - X = \prod_{d|m} \prod_{P \in \mathbb{K}(q,d)} P(X)$.

Démonstration

• Soit $P \in \mathbb{K}(q,d)$, $d \in \mathbb{N}^*$, $d|m$. Alors $L := \mathbb{F}_q[X]/(P)$ est un corps de cardinal $|L| = |\mathbb{F}_q|^{d^\circ P} = q^d$. Ainsi par le théorème de Lagrange, $\forall x \in L$ $x^{q^d} = x$.
($\forall x \in L^*$ $x^{q^d - 1} = 1$ et $0^{q^d} = 0$).

Si $m = dk$ pour $k \in \mathbb{N}$, alors $x^{q^m} = x^{q^{dk}} = x^{\overbrace{q^d \times \cdots \times q^d}^{k \text{ fois}}}$
$= \left(x^{\overbrace{q^d \times \cdots \times q^d}^{k-1 \text{ fois}}}\right)^{q^d}$
$= x^{\overbrace{q^d \times \cdots \times q^d}^{k-1 \text{ fois}}}$
$= \cdots$
$= x$.

En particulier, si $x \in L$ est une racine de P, alors x est une racine de $X^{q^m} - X$. Donc $P | X^{q^m} - X$. Par le lemme de Gauss, $\prod_{d|m} \prod_{P \in \mathbb{K}(q,d)} P(X) | X^{q^m} - X$.

Détail. $L = \mathbb{F}_q[X]/(P) = \mathbb{F}_q(x)$ est un corps de rupture de P où $x \in L$ est une racine de P. P unitaire / irréductible / dans $\mathbb{F}_q[X]$ $\to$ P pol. minimal de x.
$[L : \mathbb{F}_q] = \deg P = d \Rightarrow L \simeq \mathbb{F}_{q^d}$, unicité corps finis.

• Soit P un facteur irréductible de $X^{q^m} - X$ dans $\mathbb{F}_q[X]$. On sait que $X^{q^m} - X$ est scindé sur $\mathbb{F}_{q^m}$ (car $\mathbb{F}_{q^m}$ est son corps de décomposition). Donc P est scindé sur $\mathbb{F}_{q^m}$. Ainsi, si x est une racine de P dans $\mathbb{F}_{q^m}$, on a : $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m = [\mathbb{F}_{q^m} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q]$. Mais P est irréductible dans $\mathbb{F}_q[X]$, donc P est le polynôme minimal de x sur $\mathbb{F}_q$, donc $d := \deg(P) = [\mathbb{F}_q(x) : \mathbb{F}_q]$, et $d|m$. De plus $P \in \mathbb{K}(q,d)$.
Donc $X^{q^m} - X | \prod_{d|m} \prod_{P \in \mathbb{K}(q,d)} P(X)$.

Égalité car les racines de $X^{q^m} - X$ dans $\mathbb{F}_{q^m}$ sont simples donc pas de P^2.
□

Corollaire 2 $q^n = \sum_{d|n} d\,I(q,d)$.

Démonstration

Il suffit de regarder les degrés. □

Rappel sur la fonction de Möbius : pas obligé à l'oral. (même impossible je pense).

Définition 3 On définit la fonction de Möbius par :

$$\mu : \mathbb{N}^* \to \mathbb{C}$$
$$n \mapsto \begin{cases} 1 \text{ si } n=1 \\ (-1)^r \text{ si } n \text{ est le produit } r \text{ nombres premiers \underline{distincts}} \\ 0 \text{ si } n \text{ est divisible par un carré} \end{cases}$$

Définition 4 $f,g : \mathbb{N}^* \to \mathbb{C}$, on définit le produit de convolution de Dirichlet :

Il est associatif et commutatif.

$$f*g : \mathbb{N}^* \to \mathbb{C}$$
$$n \mapsto \sum_{d|n} f(d)\,g(n/d).$$

. $\delta_1 : \mathbb{N}^* \to \mathbb{C},\ n \mapsto \begin{cases} 1 \text{ si } n=1 \\ 0 \text{ sinon} \end{cases}$

. $1 : \mathbb{N}^* \to \mathbb{C},\ n \mapsto 1$

Proposition 5 $\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ si } n=1 \\ 0 \text{ sinon} \end{cases}$, ie $\boxed{1 * \mu = \delta_1}$

Démonstration

. Si $n=1$: c'est clair car $\mu(1)=1$.

. Soit $n \geq 2$. On écrit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec p_i 1er, $\alpha_i \in \mathbb{N}^*$.

Si $\alpha_i \geq 2$, alors $\mu(n)=0$ et tout diviseur de n de la forme $k p_i^{\alpha_i}$ va aussi annuler μ. On peut donc supposer que $\alpha_1 = \cdots = \alpha_r$, sans changer la valeur $\sum_{d|n} \mu(d)$. Si $n = p_1 \cdots p_r$, $d|n \Leftrightarrow d = \prod_{i\in I} p_i$, avec $I \subset [\![1,r]\!]$ (si $I=\emptyset$, $d=1$).

Alors : $\sum_{d|n} \mu(d) = \sum_{I\subset[\![1,r]\!]} (-1)^{|I|} \underset{\substack{\uparrow \\ \text{partitionne selon} \\ \text{les tailles de } I}}{=} \sum_{k=0}^{r} \binom{r}{k}(-1)^k = (1-1)^r = 0.$ □

Théorème 6 $I(q,n) = \frac{1}{n}\sum_{d|n} \mu(n/d)\, q^d$, et $I(q,n) \underset{n\to\infty}{\sim} \frac{q^n}{n}$.

Démonstration

$q^n = \sum_{d|n} d\,I(q,d)$. On note $f : \mathbb{N}^* \to \mathbb{C}$, $d \mapsto d\,I(q,d)$. Alors

$q^n = f * 1(n) \Rightarrow f * d_1(n) = (f(n)) = (n \mapsto q^n) * \mu(n)$

ie $nI(q,n) = \sum_{d|n} \mu(d/n)\, q^d$.

On pose $r_n = \sum_{\substack{d|n \\ d<n}} \mu(d/n) q^d$. Alors $|r_n| \leq \sum_{\substack{d|n \\ d<n}} q^d \leq \sum_{d=0}^{\lfloor n/2 \rfloor} q^d = \frac{1-q^{\lfloor n/2 \rfloor+1}}{1-q}$.

On a $I(n,q) = \frac{q^n + r_n}{n}$

$\Rightarrow \frac{n}{q^n} I(n,q) = \frac{q^n + r_n}{q^n} = 1 + \frac{r_n}{q^n}$, et $\frac{r_n}{q^n} = \frac{1}{1-q}\left(\frac{1}{q^n} - \frac{q^{\lfloor n/2 \rfloor+1}}{q^n}\right) \xrightarrow[n\to+\infty]{} 0$

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

$\square$

→ faire l'inversion $g(n) = \sum_{d|n} f(d) \Rightarrow f(n) = \sum_{d|n} g(n/d)\mu(d)$

à la main, si il faut prouver la déf 4 (associativité / commutativité).

On peut aussi en déduire qu'il existe un polynôme irréductible sur $\mathbb{F}_q$ de tout degré.

$n I(n,q) = q^n - \sum_{\substack{d|n \\ d<n}} d I(q,d)$ $\quad\quad (q^n = \sum_{d|n} dI(q,d))$

$\Rightarrow q^n \geq n I(q,n), \forall n$.

$\geq q^n - \sum_{k=1}^{n-1} q^{k}$

$= q^n - q\frac{1-q^n}{1-q}$

$= \frac{q^n - q^{n+1} - q + q^n}{1-q} = \frac{q^n(2-q) - q}{1-q} = \frac{q + q^n(q-2)}{q-1} > 0.$