Polynômes irréductibles sur $\mathbb{F}_q$

« Francinou, Gianella, 3.11, 5.10. (Exercices mathématiques pour l'agreg).

Réf: « Gozard, Théorie de Galois p. 89. « Perrin, Cours d'Algèbre, excc III.7).

« Cours d'algèbre de demazure « Dpt Rémi Nicaud, Antoine Mouzard

« Grand Combat, Beckuy.

On veut montrer le théorème suivant.

Théorème: Soient p premier, $r \in \mathbb{N}^*$ on pose $q = p^r$. On note $A(n,q)$ l'ensemble des polynômes irréductibles de $\mathbb{F}_q[X]$ unitaires de degrés n et $I(n,q) = \text{Card } A(n,q)$ alors

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

Définition: (fonction de Möbius) On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \mathbb{C}$:

- $\mu(1) = 1$
- $\mu(p_1 \dots p_k) = (-1)^k$ si $p_1, \dots, p_k$ sont des nbres premiers tous distincts.
- $\mu(n) = 0$ sinon

Lemme 1: On a les propriétés suivantes:

1) Si $n = n_1 n_2$ avec $n_1, n_2 \in \mathbb{N}$ et $n_1 \wedge n_2 = 1$ alors $\mu(n) = \mu(n_1)\mu(n_2)$
2) Pour $n \geq 2$, $\sum_{d \mid n} \mu(d) = 0$

Preuve:

1) **Cas 1:** $n = 1$ alors $n_1 = n_2 = 1$ donc $\mu(n) = 1 = \mu(n_1)\mu(n_2)$.

Cas 2: $\exists$ p existe p premier tel que $p^2 \mid n_1$ ou $p^2 \mid n_2$ alors $\mu(n_1) = 0$ ou $\mu(n_2) = 0$ donc $\mu(n_1)\mu(n_2) = 0$
donc $p^2 \mid n$ ainsi $\mu(n) = 0 = \mu(n_1)\mu(n_2)$

Cas 3: $n_1 = p_1 \dots p_r$ et $n_2 = p_1' \dots p_\ell'$ distincts or $n_1 \wedge n_2 = 1$ donc $p_1, \dots, p_r, p_1', \dots, p_\ell'$ distincts
$\Rightarrow n = p_1 \dots p_r p_1' \dots p_\ell'$ donc $\mu(n) = (-1)^{r+\ell}$
et $\mu(n_1) = (-1)^r$, $\mu(n_2) = (-1)^\ell$ ainsi $\mu(n) = (-1)^{r+\ell} = (-1)^r (-1)^\ell = \mu(n_1)\mu(n_2)$

2) On écrit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ ainsi

$$\sum_{d|n} \mu(d) = \sum_{\substack{d = p_1^{\beta_1} \cdots p_r^{\beta_r} \\ \beta_i \leq \alpha_i}} \mu(d) = \sum_{\substack{d = p_1^{\beta_1} \cdots p_r^{\beta_r} \\ \beta_i \in \{0,1\}}} \mu(d) = \sum_{i=0}^{r} \sum_{\substack{d = p_{j_1} \cdots p_{j_i} \\ j_1, \dots, j_i \in [\![1,r]\!]}} (-1)^i$$

↑ si $\beta_i \geq 2$ alors $p_i^2 \mid d \Rightarrow \mu(d) = 0$

$\rightarrow$ il y a $\binom{r}{i}$ choix possibles.

$$= \sum_{i=0}^{r} \binom{r}{i} (-1)^i$$

$$= (1-1)^i = 0.$$

∎

Lemme 2: (Formule d'inversion de Möbius) Soient $f, g : \mathbb{N}^* \to \mathbb{C}$ telles que $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d)$.

Alors:

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d).$$

Preuve: On sait que $\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ sinon} \end{cases}$.

Et:

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{d' \mid \frac{n}{d}} g(d') = \sum_{\substack{d|n \\ d' \mid \frac{n}{d}}} \mu(d) g(d') = \sum_{d'|n} g(d') \sum_{d \mid \frac{n}{d'}} \mu(d)$$

$dd' = n$

$= 1$ ssi $\frac{n}{d'} = 1$ ssi $n = d'$

$$= g(n).$$

Ainsi $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$.

∎

Lemme 3: Soit $P \in \mathbb{F}_q[X]$ irréductibles alors P est à racines simples dans un corps où il est scindé.

Preuve: Par l'absurde soit $\alpha \in K$ une racine double de P. Alors P est irréductible sur $\mathbb{F}_q$ et $P(\alpha) = 0$. Donc P est le polynôme minimal de α sur $\mathbb{F}_q$. Or $P'(\alpha) = 0$ et $\deg(P') < \deg(P)$ donc $P' = 0$ (sinon c'est lui le pol minimal). Ainsi on a $P = R^p$ sur $\mathbb{F}_q[X]$, absurde P étant irréductible.

car $P = R(X^p) = R(X)^p$

Le Frobenius surjectif sur les corps finis.

∎

Preuve du théorème :

Soit $f \in \mathbb{F}_q[X]$ un polynôme irréductible de degré $d \mid n$.

Alors $K = \mathbb{F}_q[X]/\langle f \rangle$ est un corps fini à q^d éléments donc :

$$X^{q^d} - X = \overline{X}^{q^d} - \overline{X} = 0$$

donc $X^{q^d} - X \in \langle f \rangle$ donc $f \mid X^{q^d} - X$ dans $\mathbb{F}_q[X]$

Or on sait que $d \mid n$ donc $X^{q^d} - X \mid X^{q^n} - X$ donc $f \mid X^{q^n} - X$, par irréductibilités, $\prod_{d \mid n} \prod_{P \in A(d,q)} P \mid X^{q^n} - X$.

Soit f un facteur irréductible de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$, on note d son degré.

Alors $K = \mathbb{F}_q[X]/\langle f \rangle$, le corps de rupture de f, est de cardinal q^d.

De plus on sait que $X^{q^n} - X$ est scindé dans $\mathbb{F}_{q^n}$ et $f \mid X^{q^n} - X$ donc f est scindé dans $\mathbb{F}_{q^n}$.

Par la propriété des corps de rupture $\mathbb{F}_{q^n}$ est une extension de K ainsi comme on a :

$$\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$$

Donc :

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K][K : \mathbb{F}_q] = d\,[\mathbb{F}_{q^n} : K]$$

i.e $d \mid n$.

Il nous reste à montrer que $f^2 \nmid X^{q^n} - X$.

En effet $(X^{q^n} - X)' = q^n X^{q^n - 1} - 1 = -1$ dans $\mathbb{F}_q[X]$ donc

$$X^{q^n} - X \wedge (X^{q^n} - X)' = -1.$$

Ainsi $X^{q^n} - X$ n'admet pas de facteur carré dans $\mathbb{F}_q[X]$ on a donc montré que :

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

et $\prod_{d \mid n} \prod_{P \in A(d,q)} P \mid X^{q^n} - X$ étant unitaires on a l'égalité voulue.

En prenant le degré on obtient que :

$$q^n = \sum_{d \mid n} d\,I(d,q).$$

D'où par la formule d'inversion de Möbeius on obtient :

$$I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d. \qquad \frac{q^n}{n} \frac{n}{q^n} + \frac{r_n}{n} \frac{n}{n}$$

Or si on note $r_n = \sum_{\substack{d \mid n \\ d \neq n}} \mu\left(\frac{n}{d}\right) q^d \leq \sum_{d=1}^{\lfloor n/2 \rfloor} q^d = \underset{q \to +\infty}{O}(q^n)$ donc $I(n,q) = \frac{q^n + r_n}{n} \underset{q \to +\infty}{\sim} \frac{q^n}{n}$

Remarque: 1) Il y a q^{n-1} polynômes unitaires de degré n sur $\mathbb{F}_q[X]$ la proportion d'irréductibles notée p_n alors

$$p_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^{d-n+1} \underset{n\to+\infty}{\sim} \frac{q}{n}$$

2) La fonction de Möebuis peut définit autrement. Pour cela on note $S = \{f : \mathbb{N}^* \to \mathbb{C}\}$ qui est un $\mathbb{C}$ espace vectoriel. On définit une loi de composition interne sur S par :

$$\forall u, v \in S,\quad u * v(n) = \sum_{ab=n} u(a)v(b) = \sum_{d|n} u\left(\frac{n}{d}\right) v(d) = \sum_{d|n} u(d)\, v\left(\frac{n}{d}\right).$$

Alors $(S, +, ., *)$ est une $\mathbb{C}$algèbre commutative unitaire où $\chi : \mathbb{N}^* \to \mathbb{C}$, $n \mapsto \begin{cases} 1 \text{ si } i=1 \\ 0 \text{ sinon} \end{cases}$ est l'élément neutre

On peut caractériser ses inverses, $f \in S$ est inversible pour $*$ <u>ssi</u> $f(1) \neq 0$.

Et on définit la fonction de Moebuis comme l'inverse de $1 : \mathbb{N} \to \mathbb{C}$, $n \mapsto 1$ $\in S$ pour la loi $*$. La formule d'inversion et alors immédiate.

Lemme: Soit A un anneau euclidien.
Soient $a \in A$, alors: $d|n \iff a^d - 1 \mid a^n - 1$.

Preuve: On a: $n = qd + r$

$$a^n - 1 = a^{qd} a^r - 1$$
$$= (a^{qd} - 1 + 1)a^r - 1$$
$$= \left((a^d)^q - 1\right)a^r + a^r - 1 \qquad \text{or} \quad b^n - 1 = (b-1)P(b).$$
$$= a^r P(a)(a^d - 1) + a^r - 1$$

Ainsi si $d|n$ alors $r = 0$ donc $a^d - 1 | a^n - 1$

si $a^d - 1 | a^n - 1$ alors $a^r - 1 = 0$ (unicité de la div euclidienne)

alors $a^r = 1$ donc $r = 0$.

□

Corollaire : Si $d \mid n$ alors $X^{q^d} - X \mid X^{q^n} - X$.

Preuve : Si $d \mid n$ alors $q^d - 1 \mid q^n - 1$

donc $X^{q^d - 1} - 1 \mid X^{q^n - 1} - 1$.

donc $X^{q^d} - X \mid X^{q^n} - X$.

∎