Polynômes irréductibles sur $\mathbb{F}_q$

Chen Thomas
t.chen.thomas1[at]gmail.com

16 mai 2024

Attention

1. Ce document contient certainement des coquilles. N'hésitez pas à me le signaler. De même si vous avez une question.
2. Pour les recasages, ce sont les miens mais ce développement se case peut-être ailleurs et je n'y ai pas réfléchi.
3. Il se peut que ce développement dure plus de 15 minutes. J'ai essayé de le découper pour faire des recollements personnalisés.

Leçons

- 123 : Corps finis. Applications.
- 125 : Extensions de corps. Exemples et applications.
- 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Références

[1] M. Demazure. *Cours d'algèbre*. Cassini, 2009.

[2] X. Gourdon. *Algèbre et Probabilités*. Ellipses, 2021.

[3] J.-E. Rombaldi. *Mathématiques pour l'agrégation : Algèbre & géométrie*. deBoeck Supérieur, 2021.

[4] S. Francinou, H. Gianella. *Exercices de mathématiques pour l'agrégation : Algèbre 1*. Masson, 1997.

Théorème 1.
Soit $n \in \mathbb{N}^*$. On note $A(n,q)$, l'ensemble des polynômes irréductibles de $\mathbb{F}_q[X]$ unitaires de degré n et $I(n,q)$ son cardinal. Alors

$$q^n = \sum_{d|n} dI(d,q) \text{ et } \frac{q^n - q^{n/2+1}}{n} \leq I(n,q) \leq \frac{q^n}{n}.$$

En particulier, sur $\mathbb{F}_q$, il existe des polynômes irréductibles unitaires de tout degré et $I(n,q) \underset{n\to+\infty}{\sim} \frac{q^n}{n}$.

Remarque : seul [4] propose une preuve pour $\mathbb{F}_q[X]$ mais les idées/arguments sont sensiblement les mêmes dans les autres ouvrages.

Démonstration

Etape 1 : Soit $P \in \mathbb{F}_q[X]$ irréductible unitaire. Alors $\deg(P)|n \iff P|X^{q^n} - X =: P_n$.

$\Longrightarrow$[1] : Soit $d|n$. Soit $P \in A(d,q)$. On regarde $\mathbb{F}_{q^d} \simeq \mathbb{F}_q[X]/(P)$ qui est un – le à isomorphisme près – corps de cardinal q^d. Alors $F_{q^d}^*$ est un groupe cyclique d'ordre $q^d - 1$. Par le théorème de Lagrange, $\overline{X}^{q^d-1} = \overline{1}$ donc $\overline{X}^{q^d} = \overline{X}$. Ainsi, $(\overline{X}^{q^d})^{q^d} = \overline{X}^{q^{2d}} = \overline{X}^{q^d} = \overline{X}$ et de proche en proche, pour tout $k \in \mathbb{N}^*$, on a $\overline{X}^{q^{kd}} = \overline{X}$. Puisque $d|n$, on en déduit donc que $\overline{X}^{p^n} = \overline{X}$. Ainsi, $\overline{P_n} = 0$ ce qui signifie que $P|P_n$.

$\Longleftarrow$[2] : Soit P, un polynôme irréductible unitaire de $\mathbb{F}_q$ divisant P_n. Notons d son degré. Puisque $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$, P admet une racine x dans $\mathbb{F}_{q^n}$. Soit $K = \mathbb{F}_q(x)$. Alors K est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$. Puisque $[K : \mathbb{F}_q] = \deg(P) = d$, et que

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

on en déduit que $d|n$.

Etape 2 : Déduire une factorisation de P_n.[3]

Puisque $P_n' = q^n X^{q^n-1} - 1 = -1$ dans $\mathbb{F}_q[X]$, un facteur carré de P_n divise -1 donc est constant ce qui signifie, en notant $\mathcal{P}$, un système de représentants irréductibles unitaires de $\mathbb{F}_q[X]$ qui divise P_n, on a

$$P_n = u \prod_{P \in \mathcal{P}} P,$$

avec u un inversible de $\mathbb{F}_q[X]$ qui vaut 1 par unitarité. Or, par l'étape 1, on a $\mathcal{P} = \bigsqcup_{d|n} A(d,q)$. On a donc

$$P_n = \prod_{d|n} \prod_{P \in A(d,q)} P.$$

Etape 3 : Conclure.[4]

En prenant les degrés, on obtient alors

$$q^n = \sum_{d|n} dI(d,q).$$

De fait, $nI(n,q) = q^n - \sum_{\substack{d|n \\ d \neq n}} dI(d,q)$ (ce qui donne un procédé algorithmique pour calculer $I(n,q)$). On en déduit

$$nI(n,q) \leq q^n.$$

Cela étant vrai pour tout $n \in \mathbb{N}^*$, on obtient $\forall d|n, dI(d,q) \leq q^d$. Cela donne

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

La quantité de droite est strictement positive lorsque $n \geq 3$. Pour $n = 1$, la formule donne $I(1,q) = q$ et pour $n = 2$, la formule donne $2I(2,q) = q^2 - q$. Ainsi, $\forall n \in \mathbb{N}^*, I(n,q) > 0$. On a donc existence de polynômes irréductibles de $\mathbb{F}_q$ de tout degré. Pour l'équivalent, par théorème d'encadrement, on a le résultat souhaité. □

Pour la formule exacte, nous avons besoin d'un lemme.[5]

1. [3], page 423, point 2.
2. [4], page 190, point 2.
3. On a le choix.
4. [1], page 220, corollaire 9.23 ou [2], page 100, 3).
5. [3], paragraphe 11.7

Lemme 2. Pour toutes suites $u, v \in \mathbb{R}^{\mathbb{N}^*}$, les assertions suivantes sont équivalentes :

1. $\forall n \in \mathbb{N}^*, u(n) = \sum_{d|n} v(d)$ (1).
2. $\forall n \in \mathbb{N}^*, v(n) = \sum_{d|n} \mu(d) u\left(\frac{n}{d}\right)$ (2).

Preuve du lemme. On va montrer plus général :

1. $(\mathbb{R}^{\mathbb{N}^*}, +, *)$ est un anneau commutatif unitaire de neutre $e : n \in \mathbb{N}^* \mapsto \delta_{n,1} \in \{0, 1\}$
2. L'inverse de μ est ω, la suite constante égale à 1.

Etape 1. On sait déjà que $(\mathbb{R}^{\mathbb{N}^*}, +)$ est un groupe abélien. $*$ est commutatif car $d \mapsto \frac{n}{d}$ est une permutation sur les diviseurs de n. La distributivité de $*$ sur $+$ provient de celle $\times_{\mathbb{R}}$ sur $+_{\mathbb{R}}$. Réglons l'associativité en remarquant que

$$\sum_{d|n} u(d) v\left(\frac{n}{d}\right) = \sum_{\substack{1 \leq d,k \leq n \\ dk = n}} u(d)v(k).$$

Cela permet d'écrire

$$\forall n \in \mathbb{N}^*, ((u * v) * w)(n) = \sum_{\substack{1 \leq d,k \leq n \\ dk = n}} \sum_{\substack{1 \leq i,j \leq n \\ ij = d}} u(i)v(j)w(k) = \sum_{\substack{1 \leq i,j,k \leq n \\ ijk = n}} u(i)v(j)w(k).$$

Enfin,

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

□

Etape 2. Déjà, $(\mu * w)(1) = \mu(1)w(1) = 1$. Ensuite, pour $n \in \mathbb{N}_{\geq 2}$, $(\mu * w)(n) = \sum_{d|n} \mu(d)$. Si l'on note $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, les diviseurs de n sont les d de la forme $\prod_{i=1}^{r} p_i^{\beta_i}$ où $\forall 1 \leq i \leq r, \beta_i \in [\![0, \alpha_i]\!]$. Automatiquement, si $\beta_i \geq 2$ pour un certain i, alors $\mu(d) = 0$ donc

$$(\mu * w)(n) = \sum_{(\beta_1, \cdots, \beta_r) \in \{0,1\}^r} \mu\left(\prod_{i=1}^{r} p_i^{\beta_i}\right).$$

On calcule la somme comme suit : on fixe le nombre de 1 dans le r-uplet, disons k. On fixe un k-uplet ayant exactement k fois 1. L'entier d construit par ce k-uplet est envoyé sur $(-1)^k$ par μ. Cette quantité ne dépend pas de l'uplet choisi. On obtient alors

$$(\mu * w)(n) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = 0$$

pour $r \in \mathbb{N}^*$. Donc $\mu * w = e$.

On en déduit la formule d'inversion de Möbius :

$$(1) \iff (u = v * w) \iff (u * \mu = v * w * \mu) \iff (u * \mu = v) \iff (2).$$

Si on ne veut pas faire la formule d'inversion, on peut conclure par le théorème de l'élément primitif mais attention, il faut avoir construit les corps finis comme Perrin et non comme Rombaldi.