Polynomes irréductibles sur $\mathbb{F}_q$: (2).

Francinou - Gianella - Exercices pour l'agrégation

Th : On note $A(n,q)$ l'ensemble des polynomes unitaires irréductibles de degré n sur $\mathbb{F}_q$ $(q = p^n)$. Alors :

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

(2) $\# A(n,q) = I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.

(3) $I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$.

Lemme (Möbius) : Soient $f : \mathbb{N}^* \to \mathbb{R}$ et $g : \begin{cases} \mathbb{N}^* \to \mathbb{R} \\ n \mapsto \sum_{d|n} f(d) \end{cases}$. Alors : $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.

---

dem Lemme : Tout d'abord par un chgment de variable $d' = \frac{n}{d}$ on a $\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$.

On a : $\sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(d) f(d') = \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d)$. (*)

Or si $k \in \mathbb{N}^*_{\geq 2}$ avec $k = \prod_{i=1}^{s} p_i^{\alpha_i}$ (sa décomposition en nombre premier) on a :

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^{s} \sum_{1 \leq \gamma_1 < \dots < \gamma_i \leq n} \mu(p_{\gamma_1} \cdots p_{\gamma_i}) + \underbrace{0}_{\sum_{d|n} \mu(d) \text{ avec } d \text{ contenant un carré}}$$

$= 1 + \sum_{i=1}^{s} \binom{s}{i} (-1)^i$ [par déf on $\mu(p_{\gamma_1} \cdots p_{\gamma_i}) = (-1)^i$ et combien il y a de terme de cette sorte ? Il y en a autant que de diviseur où exactement i facteurs premiers apparaissent dans la décomposi° de i en s facteurs 1ers donc il y en a $\binom{s}{i}$]

$= (1-1)^s$

$= 0$

Comme $\mu(1) = 1$, par (*) on trouve : $\sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) = f(n)$. ///

dem Th : (1) • Soit $P \in A(d,q)$ où $d = kn$, alors le corps $K = \mathbb{F}_q[X]/(P)$ est un corps à q^d élément. Si on note α la classe de X dans K, par Lagrange on a : $\alpha^{q^d} = \alpha$. Alors

$\alpha^{q^n} = \alpha^{q^{kd}} = \alpha^{q^{d+(k-1)d}} = \left(\alpha^{q^d}\right)^{(k-1)d} = \alpha^{(k-1)d} = \dots = \alpha$.

Ainsi $X^{q^n} - X$ annule α, mais P est le polynome minimal de α sur $\mathbb{F}_q$ donc $P | X^{q^n} - X$.

Or un ensemble de polynomes irréductibles est un ensemble où tout les polynomes sont premiers entre eux deux à deux donc $\prod_{d|n} \prod_{P \in A(d,q)} P \mid X^{q^n} - X$.

• Si P est un facteur irréductible de $X^{q^n} - X$, alors comme $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$ (car $\mathbb{F}_{q^n} = D_{\mathbb{F}_p}^{\text{rac}}(X^{q^n} - X)$), $\exists\, \alpha \in \mathbb{F}_{q^n}$ tel que $P(\alpha) = 0$. Par th de la base télescopique :

$n = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)] \underbrace{[\mathbb{F}_q(\alpha) : \mathbb{F}_q]}_{= \deg P \text{ car } \mathbb{F}_q(\alpha) \text{ corps de rupture de } P \text{ sur } \mathbb{F}_q}$ car $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

donc $\deg(P) \mid n$.

Comme $X^{q^n} - X$ est scindé à racines simples dans $\mathbb{F}_{q^n}$, il n'admets pas de carré dans sa décomposition en irréductible, i.e $X^{q^n} - X = \prod_{i=1}^{n} P_i^{\alpha_i}$, $\alpha_i = 1$ (la décomposition en irréductible de $X^{q^n} - X$ sur $\mathbb{F}_q[X]$)

donc $X^{q^n} - X \mid \prod_{d \mid n} \prod_{P \in A(d,q)} P$. Les polynômes considérés étant unitaire, on conclut à l'égalité.

(2) En regardant les degrés dans (1), on trouve :

$q^n = \sum_{d \mid n} I(d,q)\, d$ d'où par le lemme avec $g(n) = q^n$ et $f(n) = I(n,q)\, n$ on a :

$$n I(n,q) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d \Rightarrow I(n,q) = \frac{1}{n}\left[\sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d\right]$$

(3) $$I(n,q) = \frac{1}{n}\left[q^n + \underbrace{\sum_{\substack{d \mid n \\ d < n}} \mu\left(\frac{n}{d}\right) q^d}_{r_n}\right]$$

$\boxed{\text{on majore } |\mu(\tfrac{n}{d})| \leq 1 \text{ et pas de } d \mid n \text{ tq } d > \tfrac{n}{2}.}$

$$|r_n| \leq \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} q^k = q\,\frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1} \leq \frac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{q-1} = o(q^n) \text{ d'où } I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}.$$ ▨

Recasage : 123 - 125 - 141 - 144 - 190

Questions: 2:

1. Pq at-on $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$?

Tout d'abord on a bien $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ car $\mathbb{F}_q = D_{\mathbb{F}_p}(X^q - X)$ et $\mathbb{F}_{q^n} = D_{\mathbb{F}_p}(X^{q^n} - X)$
or comme $\forall (a,b) \in \mathbb{N}^{*2}$, $X^{ab} - 1 = (X^a - 1)(X^{ab-a} + \dots + X^{ab-(b-1)a} + 1)$ on a $X^a - 1 \mid X^{ab} - 1$,
donc $X^q - X \mid X^{q^n} - X$ donc $D_{\mathbb{F}_p}(X^q - X) \subset D_{\mathbb{F}_p}(X^{q^n} - X) \Leftrightarrow \mathbb{F}_q \subset \mathbb{F}_{q^n}$.
Donc $\mathbb{F}_{q^n}$ est un $\mathbb{F}_q$-e-v de dimension finie (puisque il est fini) donc $|\mathbb{F}_{q^n}| = |\mathbb{F}_q|^{[\mathbb{F}_{q^n} : \mathbb{F}_q]}$

donc $[\mathbb{F}_{q^n} ; \mathbb{F}_q] = n$.

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

2. Un autre argument pour mq dans (1). $x^{q^n} = x$?

On aurait pu utiliser que $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n} \Leftrightarrow d \mid n$ et on aurait alors directement $x^{q^n} = x$.
Démontrons l'$\Leftrightarrow$ce :

$\boxed{\Rightarrow}$ Si $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$ alors $\mathbb{F}_{q^n}$ est un $\mathbb{F}_{q^d}$-e-v-d-f et donc $|\mathbb{F}_{q^n}| = q^n = |\mathbb{F}_{q^d}|^{[\mathbb{F}_{q^n} : \mathbb{F}_{q^d}]}$
$= q^{d[\mathbb{F}_{q^n} : \mathbb{F}_{q^d}]}$

donc $d \mid n$.

$\boxed{\Leftarrow}$ Si $d \mid n$. On a $X^{q^d} - X \mid X^{q^n} - X$. On note $K = \{x \in \mathbb{F}_{q^n} \mid x^{q^d} = x\}$.
K est un sous-corps de $\mathbb{F}_{q^n}$. En effet il est clair que $0, 1 \in K$ que si $xy \in K$ alors $(xy) \in K$ et $x^{-1} \in K$. De plus $(x+y)^{q^d} = x^{q^d} + y^{q^d}$ (c'est l'automorphisme de Frobenius itéré).
Mais alors comme $(X^{q^d} - 1)' = -1$ (car $(\mathbb{F}_{q^n}) = p$) le polynome X^{q^d} est scindé à racine simple donc $|K| = q^d$ et donc $K \simeq \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$.

3. Démontrer qu'il existe des polynomes irréductibles sur $\mathbb{F}_q$ de tout degré :

Soit $n \in \mathbb{N}$, on a $q^n = \sum_{d \mid n} d I(d,q)$ donc $q^n \geq n I(n,q)$ et :

$$n I(n,q) = q^n - \sum_{\substack{d \mid n \\ d < n}} d I(d,q) \geq q^n - \sum_{d=1}^{n-1} q^d = q^n - q \frac{q^{n-1} - 1}{q-1}$$
$$= q^n - \frac{q^n - q}{q-1}$$
$$= \frac{q^{n+1} - q^n - q^n + q}{q-1}$$
$$= \frac{q^n[q-2] + q}{q-1} > 0$$

4. En déduire le théorème de l'élément primitif pour les corps finis :

On veut mq $\forall n \in \mathbb{N}$, $\exists x \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q(x)$
On peut choisir $P \in A(n,q)$ et alors $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/(P) \simeq \mathbb{F}_q(x)$ où x désigne la classe de X sur $\mathbb{F}_q[X]/(P)$.

5. Donner la valeur de $I(1,q)$, $I(2,q)$ et $I(3,q)$

$I(1,q) = q$, $I(2,q) = \frac{1}{2} \sum_{d|2} \mu\left(\frac{2}{d}\right) q^d = (-q + q^2)\frac{1}{2} = \frac{q(q-1)}{2}$

$I(3,q) = \frac{1}{3}\left[q^3 - q\right]$

Par ex : il y a : $\frac{2(2-1)}{2} = 1$ pol irreductible de degré 2 sur $\mathbb{F}_2$: $X^2 + X + 1$

$\frac{3(3-1)}{2} = 3$ pol irred de deg 2 sur $\mathbb{F}_3$: X^2+1, X^2+X+2, X^2+2X+2

$\frac{2^3-2}{3} = 2$ pol irred de deg 3 sur $\mathbb{F}_2$: X^3+X+1, X^3+X^2+1