Pol irred sur $\mathbb{F}_q$ [Francinou Gianella, Exos pour l'agreg alg 1 p 189]

Lemmes sur la fonction de Möbius

déf $\mu : \mathbb{N}^* \to \{-1,0,1\}$ est tq $\mu(n) = 0$ si n a un facteur carré

$$\mu(p_1 \cdots p_r) = (-1)^r \text{ si les } p_i \in \mathbb{P} \text{ et 2 à 2 } \neq$$

1) μ est multiplicative : $m \wedge n \Rightarrow \mu(mn) = \mu(m)\mu(n)$

2) $\forall n > 1, \quad \sum_{d|n} \mu(d) = 0$

3) Inversion de Möbius : si $g(n) = \sum_{d|n} f(d)$ alors $f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) \left(= \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) \right)$

démo lemmes

1) Si m ou n a un facteur carré, mn aussi donc $\mu(mn) = 0 = \mu(m)\mu(n)$

Sinon $n = p_1 \cdots p_r$ et $m = q_1 \cdots q_s$ et comme $m \wedge n = 1$, les p_i, q_i sont tous $\neq$

Dc $\mu(mn) = (-1)^{r+s} = \mu(m)\mu(n)$ aussi

2) On décompose n en facteurs premiers : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $r \geq 1$ car $n > 1$

Alors $\sum_{d|n} \mu(d) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k$ (les $\mu(d)$ sont tous nuls dès que $d|n$ sauf les d constitués de k p_i 2 à 2 $\neq$ choisis parmi les r possibles pour lesquels $\mu(d) = (-1)^k$

$= (1-1)^r = 0$ car $r \geq 1$

3) $\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \left(\sum_{d' | \frac{n}{d}} f(d') \right)$ par déf de g

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

$= \sum_{d'|n} \underbrace{\sum_{d | \frac{n}{d'}} \mu(d)}_{= 0 \text{ sauf pour } \frac{n}{d'} = 1 \text{ par 2}} f(d') = f(n)$

Pour l'autre $=$, on fait 1 chgmt var $d \leftrightarrow \frac{n}{d}$

Th $\mathbb{F}_q$ = corps $< \infty$. Pour tout $n \in \mathbb{N}^*$, $\exists$ 1 polynôme irred et unitaire de degré n sur $\mathbb{F}_q$ et on a m̂ que le nombre de tels polynômes est $\sim \frac{q^n}{n}$ qd $n \to +\infty$

démo On note $E(n,q) = \{ P \in \mathbb{F}_q[X] \mid P$ est de degré n et est irréductible sur $\mathbb{F}_q$ et unitaire$\}$

et $I(n,q) = |E(n,q)|$

• On mq $X^{q^n} - X = \prod_{d|n} \prod_{P \in E(d,q)} P$

Pour ce faire, on mq $\{P \in \mathbb{F}_q[X] \mid d|n \text{ et } P \in E(d,q)\}$ est exactement l'ensemble des pol irréd intervenant ds la décomposition de $X^{q^n} - X$

Cela conclura car les coeff dom sont = 1 et les racines de $X^{q^n} - X$ sont simples (dérivée = -1) donc y a pas de facteurs carrés ds cette décomp.

Or, si $d|n$ et $P \in E(d,q)$, $P \mid X^{q^n} - X$ car : on a $n = dk$

($\forall a \in \mathbb{N}, a^n - 1 \mid a^p - 1 \Leftrightarrow n \mid p$ car dans $R = \mathbb{Z}/(a^n-1)\mathbb{Z}$ on a

Soit x racine de P ds 1 clôture alg. $\mathbb{F}_q(x)$ est 1 corps de rupture de P et $[\mathbb{F}_q(x) : \mathbb{F}_q] = \deg(P) = d$ donc / unicité des corps $< \infty$, $\mathbb{F}_q(x) \simeq \mathbb{F}_{q^d}$. Comme $\mathbb{F}_{q^d}$ est "le" corps de décomposition de $X^{q^d} - X$, $\mathbb{F}_q(x) \simeq \{$racines de $X^{q^d} - X\}$. En particulier,

$x^{q^d} - x = 0$ donc $x^{q^n} = \underbrace{\left(\left(x^{q^d}\right)^{q^d} \cdots\right)^{q^d}}_{k \text{ fois}} = \underbrace{\left(\left(x^{q^d}\right)^{q^d} \cdots\right)^{q^d}}_{k-1 \text{ fois}} = \cdots = x$

Donc x est aussi racine de $X^{q^n} - X$. Comme les racines de $X^{q^d} - X$ sont tout aussi simples que celles de $X^{q^n} - X$, et que les 2 pol sont unitaires, $P \mid X^{q^n} - X$

Réciproquement, si P = pol irréd qui $| X^{q^n} - X$, il est unitaire. Reste à mq $\deg(P) \mid n$

$X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$ (donc P aussi). Notons x 1 racine de P ds $\mathbb{F}_{q^n}$ et $K = \mathbb{F}_q(x)$

Comme $\mathbb{F}_q \subset K \subset \mathbb{F}_{q^n}$, $\underbrace{[\mathbb{F}_{q^n} : \mathbb{F}_q]}_{= n} = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)] \underbrace{[\mathbb{F}_q(x) : \mathbb{F}_q]}_{= \deg(P)}$ donc $\deg(P) \mid n$.

• En prenant le degré de l'égalité précédente, on a

$q^n = \sum_{d|n} d\, I(n,q)$ donc / inversion Möbius, $n I(n,q) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$

$= q^n + \underbrace{\sum_{\substack{d|n \\ d \neq n}} \mu\left(\frac{n}{d}\right) q^d}_{= r_n}$

Or, $|r_n| \leq \sum_{d=1}^{\left[\frac{n}{2}\right]} 1 \times q^d = q \frac{q^{\left[\frac{n}{2}\right]} - 1}{q-1} \leq \frac{q^{\left[\frac{n}{2}\right]+1}}{q-1}$ ($\left[\frac{n}{2}\right]$ en fois)

On a donc $|r_n| < q^n$ donc $I(n,q) > 0$ ce qui assure l'$\exists$ d'1 pol de $E(n,q)$

et $\frac{|r_n|}{q^n} \leq \frac{q}{q-1} \frac{q^{\left[\frac{n}{2}\right]}}{q^n} = \frac{q}{q-1} \frac{1}{q^{\left[\frac{n}{2}\right]}} \xrightarrow[n \to +\infty]{} 0$ car $q > 1$ donc $|r_n| = o(q^n)$

On en déduit que $n I(n,q) = q^n + o(q^n)$ donc $I(n,q) = \frac{q^n}{n} + o\left(\frac{q^n}{n}\right)$

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