Dén. Irred ($\mathbb{F}_q[X]$)

→ Inversion de Möbius : partir de la formule et étudier les sommes de ν

→ Énoncer clairement ce qu'il faut démontrer
- Si $D \mid X^{p^n} - X$, $\deg D \mid n$ (avec $D = \pi_\alpha$, $\alpha \in \mathbb{F}_{p^n}$
- Si $d \mid n$, $D \mid X^{p^d} - X \mid X^{p^n} - X$
- chaque facteur irred est de multiplicité 1.

Prérequis

* Corps de rupture et de décomposition
* Lemme de divisibilité
* $P \wedge P' = 1 \Rightarrow P$ sans facteur carré.

Dénombrement des irréductibles de $\overline{\mathbb{F}_p}[X]$

par p premier.

(FGN Al 1) (?)
Gozard

DEV 1

Lemme - Formule d'inversion de Möbius

Soit $f, g : \mathbb{N}^* \longrightarrow G$ avec G groupe abélien tq $\forall n \in \mathbb{N}^*$, $f(n) = \sum_{d|n} g(d)$

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

preuve

Posons $S_n := \sum_{d|n} \mu(d)$ $S_1 = 1$.

Pour $n \geq 2$, on pose P_n l'ensemble des diviseurs premiers de n.

Alors $S_n = \sum_{D \subset P_n} \mu\left(\prod_{d \in D} d\right)$ en effet, $d|n \iff \exists D \subset P_n$ tq les diviseurs premiers de d sont exactement ceux de D.

Parenthèse sur la fonction de Möbius : (Gozard, p89)

Déf : $\mu(1) = 1$

$\mu(p_1 \times \cdots \times p_k) = (-1)^k$ avec les p_i premiers distincts

$\mu(n) = 0$ sinon (ie si $\exists p$ premier tq $p^2 | n$, $\mu(n) = 0$).

Rq : Prouver la formule d'inversion de Möbius revient à prouver que l'inverse de μ pour le produit de convolution $*$ est $\mathbb{1}$

$f * g(n) = \sum_{ab=n} f(a) g(b)$

En effet, on a par hypothèse $g * \mathbb{1} = f$ donc $g = f * \mathbb{1}^{-1}$ et si on a montré que $\mathbb{1}^{-1} = \mu$, on a le résultat recherché.

Donc si $d|n$ contient des facteurs carrés, $\mu(d) = 0$.

Donc on a bien $S_n = \sum_{D \subset P_n} (-1)^{|D|} = \sum_{i=0}^{|P|} \binom{|P|}{i} (-1)^i$

↑ on partitionne en fonction du cardinal de D

$= (1-1)^{|P|} = 0$

on a alors

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

$= S_{\frac{n}{\delta}}$

$= 0$ sauf si $\frac{n}{\delta} = 1$

$= g(n)$

□

Théorème

Le nombre de polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$ est :

$$I(p,n) = \frac{p-1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

Rq : Dans Gozard, on ne cherche qu'un résultat sur les irred de $\mathbb{F}_p[X]$, parce que le théorème suivant justifie leur utilité :

Soit p premier et $q = p^n$.
Alors $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.

preuve

- montrons que $X^{p^n} - X = \prod_{d|n} \prod_{D \in I_p^d} D$ où I_p^n : ensemble des irred unitaires de degré n sur $\mathbb{F}_p[X]$.

on note $P := X^{p^n} - X$

- Soit D un diviseur irréductible unitaire de P de degré d.
Soit $\alpha \in \mathbb{F}_{p^n}$ une racine de D. Existe : P est scindé sur $\mathbb{F}_{p^n}$, donc D aussi.
D est irréductible sur $\mathbb{F}_p$ et $D(\alpha) = 0$, donc D est le polynôme minimal de α.
on a donc la tour d'extensions $\mathbb{F}_p \longrightarrow \mathbb{F}_p(\alpha) \longrightarrow \mathbb{F}_{p^n}$
et la base télescopique donne $\underbrace{[\mathbb{F}_{p^n} : \mathbb{F}_p]}_{n} = [\mathbb{F}_{p^n} : \mathbb{F}_p(\alpha)]\underbrace{[\mathbb{F}_p(\alpha) : \mathbb{F}_p]}_{d}$

donc $d|n$.

(car $\mathbb{F}_{p^n}$ est un $\mathbb{F}_p$-ev, donc de dimension n) (à détailler en (*))

- Soit $d|n$ et $D \in \mathbb{F}_p[X]$ irréductible de degré d. Soit $\mathbb{F}_p(\alpha)$ un corps de rupture de D
Alors $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ (↑ car $d|n$ (*))

(bof, cf après, dans les parenthèses)

Ainsi, α est aussi une racine de P.
Or, D est irréductible sur $\mathbb{F}_p$, donc à racines simples dans $\mathbb{F}_{p^n}$. (*)
Donc $D|P$.

- De plus, chaque diviseur irréductible de P est de multiplicité 1.
En effet, $P' = -1$ dans $\mathbb{F}_{p^n}[X]$ donc $\text{pgcd}(P, P') = 1$.

Donc on a bien $P = X^{p^n} - X = \prod_{d|n} \prod_{D \in I_p^d} D$.

- On passe au degré dans cette formule :

$$\frac{p^n}{f(n)} = \sum_{d|n} \underbrace{|I_p^d|}_{g(d)} d$$

On déduit alors de l'inversion de Möbius que

$$|I_p^n| n = \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

On a compté ici seulement les polynômes unitaires, donc on peut multiplier par $q-1$ pour obtenir tous les polynômes irréductibles de degré n

□

Parenthèses

- D irréductible sur $\mathbb{F}_p$ est à racines simples sur $\overline{\mathbb{F}_{p^n}}$.

Soit α une racine de D dans $\overline{\mathbb{F}_{p^n}}$.
$\mathbb{F}_p$ est un corps donc division euclidienne sur les polynômes et donc algo d'Euclide OK.
On a D et D' premiers entre eux : Bézout donne alors U et V $\in \mathbb{F}_p[X]$ tq

$$DU + D'V = 1$$

Cette relation reste valable dans $\mathbb{F}_{p^n}$ car $\mathbb{F}_p \subset \overline{\mathbb{F}_{p^n}}$.
Donc en évaluant en α on a $D'(\alpha)V(\alpha) = 1$ donc $D'(\alpha) \neq 0$ si α n'est pas racine de D' donc racine simple de D.

variante (Antoine Touzard) :
On admet pour l'instant que D est scindé sur $\mathbb{F}_{q^n}$. On suppose que $\alpha \in \mathbb{F}_{q^n}$ est une racine double de D. Donc $D'(\alpha) = 0$. Or, D étant irréductible, il est le polynôme minimal de α. Donc $\deg D' < \deg D$ et $D'(\alpha) = 0$ contredit ça si $D' \neq 0$ Donc $D' = 0$ et comme D non constant, cela implique qu'il existe $R \in \mathbb{F}_p[X]$ tel que $D = R^p$: absurde

- preuve du théorème justifiant l'utilité

Théorème
pour p premier et $n \in \mathbb{N}^*$

$$\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(\pi)$$ où π irred quelconque de degré n sur $\mathbb{F}_p$.

preuve
- Soit π irred de degré n sur $\mathbb{F}_p$. Alors corps de rupture de π : $\mathbb{F}_p[X]/(\pi)$: extension algébrique de degré n, donc $\mathbb{F}_p$-ev de dimension n, donc un corps fini de cardinal p^n.
D'où $\mathbb{F}_p[X]/(\pi) \simeq \mathbb{F}_{p^n}$

- Réciproquement, soit ξ un générateur du groupe cyclique $\mathbb{F}_{p^n}^*$. On note π son polynôme minimal sur $\mathbb{F}_p$. Alors $\mathbb{F}_p[X]/(\pi) \simeq \mathbb{F}_p(\xi)$ + petit corps contenant $\mathbb{F}_p$ et ξ. ah bon ?? oui ok
Contient donc en particulier $\mathbb{F}_{p^n}$, et est de même cardinal, donc égalité.

Donc $\deg(\pi) = [\mathbb{F}_p(\xi) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Car $\mathbb{F}_p(\xi)$ corps de cardinal $p^{\deg \pi} = p^n$ car $\mathbb{F}_{p^n}$

Donc $\mathbb{F}_{p^n}$ peut toujours être obtenu comme quotient de $\mathbb{F}_p[X]$ par un irred de degré n

$\blacksquare$

$\longrightarrow$ en particulier, justifie que $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

($\mathbb{F}_{p^n} \simeq \mathbb{F}_p[X]/(\pi)$, donc $p^n = p^{\deg(\pi)}$ et $\deg(\pi)$ est le degré de l'extension)

Corollaire

Si π est un pol. irred de degré n sur $\mathbb{F}_p$, alors $\pi(x) \mid X^{p^n} - X$ dans $\mathbb{F}_p[X]$, donc est scindé sur $\mathbb{F}_{p^n}$

$\longrightarrow$ corps de rupture = corps de décomposition

Preuve

Soit π irred de degré n sur $\mathbb{F}_p$. (on suppose $n \geq 2$) (sinon, $\pi(X) = X - \alpha$, $\alpha \in \mathbb{F}_p$, et α est aussi racine de $X^p - X$)

Soit K un corps de décomposition de $\pi(X)$ sur $\mathbb{F}_p$ et θ une racine de π dans K.

On a $\pi(0) \neq 0$, car sinon on peut factoriser par X, mais π est irred.

Donc $\theta \neq 0$. $\theta \in \mathbb{F}_p(\theta) \simeq \mathbb{F}_p[X]/(\pi)$ (π irred $\longrightarrow$ pol. minimal de θ)

$\simeq \mathbb{F}_{p^n}$ d'après le th. précédent (ou juste égalité des cardinaux)

Donc $\theta^{p^n - 1} - 1 = 0$ par def de $\mathbb{F}_{p^n}$, et donc $\pi(X) \mid X^{p^n - 1} - X$.

Mais $X^{p^n - 1} - X$ est scindé dans $\mathbb{F}_{p^n}$, donc π aussi.

$\blacksquare$

Lemme :

Pour A euclidien (et commutatif, unitaire, intègre), $a \in A \setminus U(A)$, et $u, v \in \mathbb{N}$,

$u \mid v \iff a^u - 1 \mid a^v - 1$ (dans A).

Preuve

Div eucl de v par u : $v = uq + r$.

$$a^v - 1 = a^{uq+r} - 1 = (a^{uq} - 1)a^r + a^r - 1 = (a^u - 1)\sum_{j=0}^{q-1} a^{uj+r} + a^r - 1$$

Donc les diviseurs communs à $(a^v - 1, a^u - 1)$ sont les diviseurs communs à $(a^u - 1, a^r - 1)$

D'où $\operatorname{pgcd}(a^u - 1, a^v - 1) = a^{\operatorname{pgcd}(u,v)} - 1$.

$\blacksquare$

Donc si $d \mid n$, alors $p^d - 1 \mid p^n - 1$

Rq : on obtient ce résultat plus rapidement en écrivant

$$p^n - 1 = p^{dd'} - 1 = (p^d - 1)\sum_{j=0}^{d'-1} p^{dj}$$

On a encore, $d \mid n \Rightarrow p^d - 1 \mid p^n - 1 \Rightarrow X^{p^d - 1} - 1 \mid X^{p^n - 1} - 1$

On a vu au corollaire précédent que si π irred de degré n sur $\mathbb{F}_p$, alors $\pi \mid X^{p^n} - X$.

Donc $\forall D$ irred sur $\mathbb{F}_p[X]$ de degré $d \mid n$, $D \mid X^{p^d} - X \mid X^{p^n} - X$.

Donc $D \mid X^{p^n} - X$.

Rq : Pour ce développement, il faut savoir qu'il existe des polynômes irréductibles de haut degré sur $\mathbb{F}_p$, on ne peut pas le montrer avec la formule démontrée.

Donc il faut savoir démontrer que $\mathbb{F}_q^*$ est cyclique.

Théorème : $\mathbb{F}_q^*$ est cyclique

(Demazure)

preuve

$\mathbb{F}_q^*$ est un groupe commutatif pour $\times$ (car $\mathbb{F}_q$ commutatif et corps)

On note s son exposant. Son ordre est connu, il vaut $q-1$ on a alors $s \leq q-1$.

Or, $\forall x \in \mathbb{F}_q^*$, $x^s = 1$ donc $\mathbb{F}_q^* \subset \mathrm{Rac}(X^s - 1)$

Mais par Lagrange, $s \mid q-1$ donc $X^s - 1 \mid X^{q-1} - 1$

Donc $\underbrace{\mathbb{F}_q^*}_{\text{de cardinal } q-1} \subset \underbrace{\mathrm{Rac}_{\mathbb{F}_q}(X^{q-1} - 1)}_{\text{de cardinal au plus } q-1}$

Donc $\mathbb{F}_q^* = \mathrm{Rac}(X^{q-1} - 1) \subset \mathrm{Rac}(X^s - 1)$ avec $s \leq q-1$

Donc $s = q-1$ et il existe un élément d'ordre l'exposant, donc un générateur de $\mathbb{F}_q^*$.

□

Ex : nb d'irréductibles de degré 2 dans $\mathbb{F}_2[X]$.

$$I(2,2) = \frac{1}{2} \cdot \left(\mu(2) 2 + \mu(1) 4 \right)$$

$$= \frac{1}{2} \left(-2 + 4 \right) = 1$$

Et c'est $X^2 + X + 1$