ÉNONCÉ

p 1er. $n \in \mathbb{N}^*$.

$\mathcal{U}_n(p) = \{P \in \mathbb{F}_p[X]$, unitaire, irréduct. $\deg(P) = n\}$

$I_n(p) = \# \mathcal{U}_n(p)$.

$P_n = X^{p^n} - X$

$Q \in \mathcal{U}_d(p)$. $n \in \mathbb{N}^*$

① $Q \mid P_n \Leftrightarrow d \mid n$.

② $P_n = \prod_{p \mid n} \prod_{P \in \mathcal{U}_d(p)} P$ ds $\mathbb{F}_p[X]$ et $p^n = \sum_{d \mid n} d I_d(p)$.

③ . $\forall n \in \mathbb{N}^*$, $I_n(p) \geq 1$

. $I_n(p) \underset{n \to +\infty}{\sim} \frac{p^n}{n}$.

④ exemple de $\mathcal{U}_2(3)$

LEÇONS.

123

125

141

190

RÉFS.

inspiré de : (mais bcp modifié)

①②③ [Rb] Rombaldi alg. et géom p. 422

④ PAS DE RÉF.

RÉSULTATS ASSOCIÉS

1. $Q \in \mathcal{U}_d(p)$. $\frac{\mathbb{F}_p[X]}{(Q)}$ corps de cardinal p^d.

DÉMO

■ : à l'oral.
■ écrit au tableau.
■ : pour comprendre.

$P_n = X^{p^n} - X$

Soit $Q \in \mathcal{U}_d(p)$. $\underbrace{\mathbb{F}_p[X]/(Q)}$ c'est un corps de cardinal p^d. On note $\bar{X} = X \bmod Q$

PLAN :

1. $d | n \Leftrightarrow Q | P_n$
2. $P_n = \prod_{d|n} \prod_{R \in \mathcal{U}_d(p)} R$
3. $\forall n \geq 1$, $I_n(p) \geq 1$ et $p^n \sim n I_n(p)$.
4. ex de $\mathcal{U}_2(3)$

(1)

$\Leftarrow$ Sq $d | n$: $n = qd$ $q \in \mathbb{N}$.

But : $\bar{P}_n = \bar{0}$ mod Q.

$\bar{X} \in (\mathbb{F}_{p^d})^*$ donc par le théo Lagrange, $\bar{X}^{p^d - 1} = \bar{1}$ puis $\bar{X}^{p^d} = \bar{X}$

Or, $\bar{X}^{p^n} = \bar{X}^{p^{qd}} = \left(\bar{X}^{p^d}\right)^{p^{d(q-1)}} \overset{(*)}{=} \bar{X}^{p^{d(q-1)}} = \dots \overset{\text{récu.}}{=} \bar{X}$ donc $\overline{P_n(X)} = P_n(\bar{X}) = \bar{X}^{p^n} - \bar{X} = \bar{0}$ ie $Q | P_n$

th de Lagrange : tous sont $\surd$ et car $+ p^n$ $\surd$

$\Rightarrow$ $P_n = X^{p^n} - X = \prod_{x \in \mathbb{F}_{p^n}} (X - x)$ ds $\mathbb{F}_{p^n}[X]$ donc si $Q | P_n$, Q admet une racine x dans $\mathbb{F}_{p^n}$.

$\mathbb{F}_{p^n}$. $K = \mathbb{F}_p(x) \simeq \mathbb{F}_p[X]/(Q)$ c'est un corps supl car Q irr.

$x \in \mathbb{F}_{p^n}$ donc $\mathbb{F}_p - \mathbb{F}_p(x) - \mathbb{F}_{p^n}$

contient x et $\mathbb{F}_p$

+ petit contenant x et $\mathbb{F}_p$.

Par mul des deg : $\underbrace{[\mathbb{F}_{p^n} : \mathbb{F}_p]}_{=n} = [\mathbb{F}_{p^n} : K] \underbrace{[K : \mathbb{F}_p]}_{d}$

$\mathbb{F}_{p^n} \simeq (\mathbb{F}_p)^n$

Donc $d | n$.

(2)

Par (1),

- $\forall d | n$, $P \in \mathcal{U}_d(P)$ $P | P_n$ ĉ ils sont irr, ils sont 1ers (.) eux 2 à 2 donc $\prod_{d|n} \prod_{P \in \mathcal{U}_d(p)} P \,|\, P_n$.

Mq P_n sans facteurs carrés

car $= p$ ($P_n \in \mathbb{F}_p[X]$)

$P_n'(X) = p^n X^{p^n - 1} - 1 = -1$

Donc $P_n \wedge P_n' \sim 1$

Sq $\exists R, Q \in \mathbb{F}_p[X]$ tq $P_n = R^2 Q$.

Alors $P_n' = 2R'RQ + Q'R^2 = R(2R'Q + Q'R)$

Donc $R \,|\, P_n \wedge P_n' \sim 1$ et R non irr.

Donc $P_n = \prod_{d \mid n} \prod_{P \in \mathcal{U}_d(p)} P$ par unitarité

(3)

On passe au degré dans (2) $p^n = \sum_{d \mid n} d\, I_d(p)$.

On a déjà : $p^n \geq n I_p(n)$.

On veut obt 1 mino :

$$n I_n(p) = p^n - \sum_{\substack{d \mid n \\ d \neq n}} d\, I_d(p) \geq p^n - \sum_{\substack{d \mid n \\ d \neq n}} p^d$$

Pour $d \mid n$, $d < n$, $n = dq$, $2 \leq q \leq n$. D'où : $d = \frac{n}{q} \in [\![1, \lfloor \frac{n}{2} \rfloor]\!]$

↳ $\frac{n}{2} \geq \frac{n}{q} \geq \frac{n}{n}$ et $d \in \mathbb{N}$ donc $d \leq \lfloor \frac{n}{2} \rfloor \leq \frac{n}{2}$

$$\geq p^n - \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} p^d$$

$$= p^n - p \frac{\left(p^{\lfloor n/2 \rfloor} - 1\right)}{p-1} \to \Sigma \text{ géom.}$$

$\frac{1}{p-1} \leq 1$ donc $-\frac{1}{p-1} \geq -1$.

$$\geq p^n - p^{\lfloor n/2 \rfloor + 1}$$

et $p\left(p^{\lfloor \frac{n}{2} \rfloor} - 1\right) \leq p\, p^{\lfloor \frac{n}{2} \rfloor}$

$$\geq p^n - p^{n/2 + 1}$$

donc $-p\left(p^{\lfloor \frac{n}{2} \rfloor} - 1\right) \geq -p^{\lfloor \frac{n}{2} \rfloor + 1}$

Positivité stricte :

Pour $n \geq 3$: $n I_n(p) \geq p^n - p^{n/2 + 1} > 0$.

l'égalité préc donne 0 ou 1 : permet pas cane.

Pour $n = 1$: $I_1(p) = p$ → calcul ; $p = \sum_{d \mid 1} d\, I_d(p) = I_1(p)$.

Pour $n = 2$: $2 I_2(p) = p^2 - p > 0$.

Donc $\forall n \in \mathbb{N}^*$, $I_n(p) > 0$.

équivalent :

$$\underbrace{p^n - p^{n/2+1}}_{\sim p^n} \leq n I_n(p) \leq p^n$$

Donc $I_n(p) \sim \frac{p^n}{n}$

EXEMPLE de $\mathcal{U}_2(3)$:

$2\,I_2(3) = 3^2 - I_1(3) = 3^2 - 3 = 6$

Donc $I_2(3) = 3$.

. Soit $P \in \mathcal{U}_2(3)$: $P = X^2 + aX + b$, $a, b \in \mathbb{F}_3$.

on veut savoir qui sont les 3 irr parmi les $3 \times 3 = 9$ psb.

X^2+1	X^2	X^2+X
X^2+X+1	X^2+2	X^2+2X
X^2+2X+1	X^2+X+2	X^2

il est de deg deux irr $\Leftrightarrow$ pas de r ds $\mathbb{F}_3$.

$P(0) \neq 0$ donc $b \neq 0$ donc $b \in \{1, 2\}$.

$P(1) \neq 0$ donc $1 + a + b \neq 0$. dans $\mathbb{F}_3$.

$P(2) \neq 0$ donc $1 + 2a + b \neq 0$ dans $\mathbb{F}_3$.

si <u>$b = 1$</u> : $P = X^2 + 1$ (a est $\neq 1$ via 2^e cond , $\neq 2$ via 3^e cond)

si <u>$b = 2$</u> : $P = X^2 + X + 2$ ou $P = X^2 + 2X + 2$ ($a \neq 0$ 2^e cond).