ÉNONCÉ

NOT : Pour $x \in \mathbb{Z}$, on note P_x poly min de x sur $\mathbb{Q}$

$n \in \mathbb{N}^*$ $p \nmid n$. $\Phi_n(X) = \prod_{\alpha \in \mathbb{U}_n^*} (X-\alpha)$, $\mathbb{U}_n^* = \{$ r n^e primitives de 1 ds $\mathbb{C}\}$.

1. Φ_n n'a que des r simples dans $\mathbb{F}_p[X]$
2. $\Phi_n \in \mathbb{Z}[X]$
3. Φ_n est irr sur $\mathbb{Z}$ donc sur $\mathbb{Q}$

LEÇONS :

102

125

141

RÉFS

[P] : Perrin p. 82.

RÉSULTATS ASSOCIÉS

1. $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$. et $\Phi_n \in \mathbb{Z}[X]$
2. $\mathbb{U}_n^* = \{ \xi^p , p \wedge n = 1 \}$
3. irr de $\mathbb{Z}[X]$ = { constant irr
   ou
   primitif, irr ds $\mathbb{Q}[X]$.
4. Lemme de Gauss : $C(PG) = C(P)C(G)$

DÉMO

▪ : à l'oral. ▪ : pour comprendre.
▪ écrit au tableau. ▪ : structure

2 Veut irr : qu'est ce qu'on sait irr ? Poly min ! de quoi ? → qui a un lien avec Φ_n :

Soit $\alpha \in \mathbb{U}_n^*$.

<u>BUT</u> : mq $\Phi_n = P_\alpha$. poly min de α sur $\mathbb{Q}$

les √ de Φ_n sont exactement les √ n^e unité : on va voir à quoi ressemble poly min d'1 telle √.

Soit p 1er tq $p \nmid n$. On sait que $\gamma := \alpha^p \in \mathbb{U}_n^*$

car les √ primitives sont les ξ^m avec $m \wedge n$ commençons avec nb 1er.

<u>LEM 1</u> : $\Phi_n \in \mathbb{Z}[X]$ → on peut donc réduire mod p.

<u>LEM 2</u> : $\bar{\Phi}_n$ est sfc ds $\mathbb{F}_p[X]$.

↳ démo à la fin selon le temps.

<u>PLAN</u> : ① mq $P_\alpha, P_\gamma \mid \Phi_n$ dans $\mathbb{Z}[X]$: Relier nos 3 polynômes

② mq $P_\alpha = P_\gamma$:

③ mq $P_\alpha = \Phi_n$.

①. poly min | les poly annul.

Par définition, $\Phi_n(\alpha) = \Phi_n(\gamma) = 0$. ($\alpha \in \mathbb{U}_n^*$) $\Phi_n = \prod_{\xi \in \mathbb{U}_n^*} (X-\xi)$.

Donc f, g | Φ_n dans $\mathbb{Q}$: en fait ds $\mathbb{Z}$: on va montrer l'égalité avec des facteurs de Φ_n coeffs dans $\mathbb{Z}$ lemme.

Soit $\Phi_n = Q_1^{k_1} \cdots Q_r^{k_r}$ la décomposition de Φ_n en produit d'irréductibles ds $\mathbb{Z}[X]$.

On peut supposer les Q_i unitaires Φ_n l'est donc quitte à changer de signe

$c(\Phi_n) = 1 = \prod c(Q_i)$

$\exists\, i, j \in \{1..r\}$, $Q_i(\alpha) = Q_j(\gamma) = 0$ pour ce qui préc.

Q_i et Q_j sont irréductibles sur $\mathbb{Z}$ et unitaires, donc irréductibles sur $\mathbb{Q}$

Donc $Q_i = P_\alpha$ et $Q_j = P_\gamma \in \mathbb{Z}[X]$. → ∈ irr ils sont = aux poly min.

Donc P_α et P_γ divisent Φ_n dans $\mathbb{Z}[X]$.

② Par l'absurde, sq $P_\alpha \neq P_\gamma$

Comme ils sont irréductibles, $P_\alpha \wedge P_\gamma = 1$. Donc $P_\alpha P_\gamma \mid \Phi_n$. dans $\mathbb{Z}[X]$. → lemme euclide.

<u>mq $P_\alpha(X) \mid P_\gamma(X^p)$ dans $\mathbb{Z}[X]$</u> $h \in \mathbb{Z}[X]$.

$P_\gamma(\alpha^p) = 0$ donc $\exists\, h \in \mathbb{Q}[X]$, $P_\gamma(X^p) = h(X) P_\alpha(X)$ → on ne sait pas si $g(X^p) \in \mathbb{Z}[X]$.

$P_\gamma(X^p)$ poly annul de α.

On va voir que valable ds $\mathbb{Z}[X]$.

- On a : $h = \frac{a}{b}\tilde{h}$ $\quad a, b \in \mathbb{Z}\setminus\{0\}$, $\tilde{h} \in \mathbb{Z}[X]$ $\quad$ (met sur le même dénom → b ; facto par le contenu → a.)
- $\underbrace{C(P_\gamma)}_{=1} = \frac{1}{b} C(\tilde{h}) \underbrace{C(P_\alpha)}_{=1}$ unitaire.

  hamag pgcd

Donc $h = \frac{\tilde{h}}{C(\tilde{h})} \in \mathbb{Z}[X]$. Car $\frac{a}{b} = \frac{1}{C(\tilde{h})}$

÷ ∀ les coeffs.

On veut faire sortir le p : on projette ds $\mathbb{F}_p$. On note $\bar{\ }$ classe

On a : $\overline{P_\gamma(X^p)} = \overline{P_\gamma(X)}^p = \bar{h}(X)\,\bar{P_\alpha}(X)$ (Frobenius) dans $\mathbb{F}_p[X]$.

Donc $\bar{P_\alpha} \mid \bar{P_\gamma}^p$ mais pas psb conc $P_\alpha \mid P_\gamma$ car pas forcément irr ds $\mathbb{F}_p$!

On va regarder un facteur irr.

Soit φ facteur irr de $\bar{P_\alpha}$ ds $\mathbb{F}_p[X]$. $\varphi \mid \bar{P_\gamma}^p$ et φ irr donc $\varphi \mid \bar{P_\gamma}$

Donc $\varphi^2 \mid \overline{P_\alpha P_\gamma}$ et $\varphi^2 \mid \bar{\Phi}_n$: CONTRADICTION lemme 2..

Donc $P_\gamma = P_\alpha$

(3) Reste à mq $P_\alpha = \Phi_n$. On sait déjà que

On sait que $P_\alpha \mid \Phi_n$ et P_α, Φ_n unitaires.

Mq $\deg P_\alpha \geq \deg(\Phi_n)$

Mq $\forall \alpha' \in \mathbb{U}_n^*$, $P_\alpha(\alpha') = 0$: 2 elems de μ_n ont m̂ poly min.

Soit $\alpha' \in \mathbb{U}_n^*$: $\exists k \in \mathbb{N}$, $\alpha' = \alpha^k$ où $k \wedge n = 1$. déf √ n^e primitives.

On veut use (2).

On décompose $k = \prod_{i=1}^{R} p_i$ $\quad p_i \wedge n = 1$, p_i 1ers

appli (2) à α^{p_1} encore √ primitive.

Par (2), $P_\alpha = P_{\alpha^{p_1}} = P_{\alpha^{p_1 p_2}} = \dots = P_{\alpha^k}$

appli (2) à P_α $\quad$ Récu.

D'où : $P_\alpha = P_{\alpha^k}$

Donc $\deg(P_\alpha) \geq |\mathbb{U}_n^*| = \deg(\Phi_n)$.

Donc $P_\alpha = \Phi_n$. En particulier, Φ_n est irr sur $\mathbb{Q}$, donc sur $\mathbb{Z}$.

si le temps :

PREUVE LEM 2

Par définition, $\bar{\Phi}_n \mid X^n - 1 := P$ dans $\mathbb{F}_p[X]$.

Or, $P'(X) = nX^{n-1}$ admet 0 comme unique racine dans tt ext car $p \nmid n$ → $nX = 0 \Rightarrow X = 0$.

et elle n'est pas racine de P. P est sans facteurs carrés

pas √ commune ds tt ext à P et P' scindé ⇒ sfc.

PREUVE LEM 1 :

Par récurrence :

$n \in \mathbb{N}^*$ $\mathcal{H}(n)$: " $\Phi_n \in \mathbb{Z}[X]$ ".

(I) $n = 1$: $\Phi_1 = X - 1$: ok.

(H) Supposons $\mathcal{H}(d)$ vraie $\forall d \mid n$, $d < n$, $n \in \mathbb{N}^*$

. $X^n - 1 = \Phi_n(x) \underbrace{\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)}_{B(x).\ \in \mathbb{Z}[X] \text{ par HR.}}$ dans $\mathbb{C}[X]$

psb car on a des polynômes unitaires.

. $X^n - 1 = B(x)\,Q(x) + R(x)$ par la div euclidienne dans $\mathbb{Z}[X]$ ($\deg R < \deg B$)

D'où : $\underbrace{B(x)\left(\Phi_n(x) - Q(x)\right)}_{\deg \geq \deg B \text{ si } \Phi_n - Q \neq 0} = \underbrace{R(x)}_{\deg < B.}$

Donc $\Phi_n(x) = Q(x) \in \mathbb{Z}[X]$