

L'idée de la preuve est de montrer que $\Phi_m = \mu_{\zeta, \mathbb{Q}}$ où $\zeta \in \mu_m^*$ [PER] p.83

Pour cela on va commencer par montrer:

Pour p premier tq $p \nmid m$ $\mu_{\zeta^p, \mathbb{Q}} = \mu_{\zeta, \mathbb{Q}}$

• Montrons que $f := \mu_{\zeta, \mathbb{Q}}$ et $g := \mu_{\zeta^p, \mathbb{Q}}$ sont des facteurs irr. de Φ_m dans $\mathbb{Q}[X]$

→ Déjà, on a que $\zeta^p \in \mu_m^*$ car $\text{pgcd}(p, m) = 1$.

→ Puisque $\mathbb{Z}[X]$ est factoriel, on peut écrire:

$\Phi_m = f_1^{d_1} \dots f_r^{d_r}$ la décomposition en irréductible de $\mathbb{Z}[X]$

Φ_m est unitaire, on peut donc supposer les f_i unitaires (quitte à multiplier par -1)

→ De plus, $\Phi_m(\zeta) = 0 = \Phi_m(\zeta^p)$, donc il existe $i, j \in \{1, \dots, r\}$ tq
 $f_i(\zeta) = 0$ et $f_j(\zeta^p) = 0$.

Or f_i et f_j sont unitaire et irréductible dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$

Donc $f_i = f$ et $f_j = g$.

Il reste à but va être montrer que $f = g$, on va raisonner par l'absurde et donc supposer que $f \neq g$.

On va se servir de cette hypothèse pour,

• ¶ $\Phi_m \not\equiv 0$ a une racine double (ce qui conduira à une absurdité)

(i) ¶ $f \nmid g(X^p)$ dans $\mathbb{Z}[X]$:

$g(\zeta^p) = 0$ donc $g(X^p)$ est un annulateur de ζ donc
 $f \mid g(X^p)$ dans $\mathbb{Q}[X]$. Donc il existe $h(X) \in \mathbb{Q}[X]$ tq

$$g(X^p) = f(X)h(X)$$

notons $h(X) = \frac{a}{b} h'(X)$ où $\frac{a}{b} \in \mathbb{Q}$ tq $h'(X) \in \mathbb{Z}[X]$ et $c(h') = 1$.

Donc $\underbrace{c(g(X^p))}_{=1} = \underbrace{c(f(X))}_{=1} \frac{a}{b} \underbrace{c(h'(X))}_{=1}$ donc $\frac{a}{b} = 1$ d'où $h(X) \in \mathbb{Z}[X]$

(ii) Hg $\bar{g}(x)^p = \bar{g}(x^p) = \bar{f}(x) \bar{h}(x)$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$

Ecrivons $g(x) = a_r x^r + \dots + a_0$ où les $a_i \in \mathbb{Z}$.

Donc $\bar{g}(x^p) = a_r (x^r)^p + \dots + a_0$
 $= (a_r x^r + \dots + a_0)^p \quad \downarrow \text{morphisme de Frobenius}$
 $= \bar{g}(x)^p$

Et donc prenons φ un facteur irr. de $\bar{f}$ donc $\varphi \mid \bar{f}$

Or $\bar{g}(x)^p = \bar{f}(x) \bar{h}(x)$ donc $\varphi \mid \bar{g}$

Donc $\varphi^2 \mid \bar{f} \bar{g}$ or $\bar{f} \bar{g} \mid \bar{\Phi}_m$ car $f \equiv g$

Donc $\varphi^2 \mid \bar{\Phi}_m$

Or $\bar{\Phi}_m = \Phi_m, \mathbb{F}_p$.

Donc dans un corps de décomposition $\Phi_m, \mathbb{F}_p$ a une racine double.

• Venons en à l'absurdité

Dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$, $X^m - 1 = \prod_{d \mid m} \Phi_d, \mathbb{F}_p$.

Or $X^m - 1$ n'a que des racines simples, en effet : [PER] p. 80

$(X^m - 1)' = m X^{m-1}$ or $p \nmid m$ donc l'unique racine de $(X^m - 1)'$ est 0
 or 0 n'est pas racine de $X^m - 1$, donc $X^m - 1$ n'a que des racines simples dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$. D'où l'absurdité. (car $\Phi_m, \mathbb{F}_p$ est un fact.
 de $(X^m - 1)$ quelque 12 min (avec algèbre)

Hg $f = \Phi_m$

• Hg f admet toutes les racines m -ème primitives de l'unité comme racines:

Soit $\zeta \in \mu_m^*$ donc il existe m premier à m tq

$$\zeta' = \zeta^m$$

Or $\text{pgcd}(m, m) = 1$ donc en écrivant $m = p_1^{a_1} \dots p_r^{a_r}$ on a $p_i \nmid m$

D'après ce qu'il précède on en déduit que $\mu_{\zeta', \mathbb{Q}} = f$

Donc pour ^{tout} $\gamma' \in \mu_n^*$, $f(\gamma') = 0$

Donc $\phi_n \mid f$

or f est un facteur irr. de ϕ_n donc $f \mid \phi_n$

Donc $f = \phi_n$, or f est unitaire et irréductible dans $\mathbb{Q}[x]$

Donc dans $\mathbb{Z}[x]$.

ce qui conclut la preuve

□

Commentaires:

Il faut savoir redémontrer que $\phi_n \in \mathbb{Z}[x]$ et ϕ_n unitaire. [PER] p. 81

$\phi_n = \phi_{n, \mathbb{F}}$ [PER] p. 81

$c(PQ) = c(P)c(Q)$ [PER] p. 51

- un corollaire de ce résultat est que $\mu_{3, \mathbb{Q}} = \phi_n$ et donc $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$
(à présenter s'il reste du temps).