

Théorème Les polynômes cyclotomiques Φ_n sont irréductibles sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

Plan: 1) $\forall \xi \in \mu_n^*(K)$, $\forall p$ premier, $\Phi_n(\xi^p) = 0$ si $p \nmid n$.

2) Soient f et g polynômes minimaux de ξ et ξ^p sur $\mathbb{Q}$, on a $f \mid g$ dans $\mathbb{Z}[X]$.

3) On a $f = g$.

4) Conclusion.

1) Soit $n \in \mathbb{N}^*$, soient K un corps de décomposition de Φ_n sur $\mathbb{Q}$, $\xi \in K$ racine de Φ_n , p un nombre premier qui ne divise pas n .

Comme les générateurs de $\mu_n(K)$ sont les racines primitives ξ élevées à la puissance m avec $m \wedge n = 1$,

ξ^p est une racine primitive de 1.

donc $\Phi_n(\xi^p) = 0$.

2) Soient f et $g \in \mathbb{Q}[X]$ les polynômes minimaux de ξ et ξ^p sur $\mathbb{Q}$.

Comme $\mathbb{Z}[X]$ est factoriel, et que $\Phi_n \in \mathbb{Z}[X]$ unitaire.

On a $\Phi_n = f_1^{\alpha_1} \dots f_r^{\alpha_r}$ avec les $f_i \in \mathbb{Z}[X]$ irréductibles.

Puisque α_i multiples par $n-1$, les f_i sont unitaires.

Donc ξ est racine de l'un des f_i .

Comme f_i est irréductible et unitaire sur $\mathbb{Z}$, donc sur $\mathbb{Q}$ aussi,

$f_i = f$.

Donc $f \mid \Phi_n$ dans $\mathbb{Z}[X]$.

De même $g \mid \Phi_n$ dans $\mathbb{Z}[X]$.

3) Raisonnons par l'absurde:

Comme f et g sont irréductibles et distincts, $f \nmid g$ dans $\mathbb{Z}[X]$.

Comme $g(\xi^p) = 0$ et $f(\xi) = 0$,

ξ est racine de $g(X^p)$ et f

Comme f est le polynôme minimal de ξ sur $\mathbb{Q}$, $f \mid g(X^p)$ dans $\mathbb{Q}[X]$.

$g(X^p) = fh$ avec $h \in \mathbb{Q}[X]$,

on écrit alors $h = \frac{a}{b} h'$

Le lemme de Gauss ($c(PQ) = c(P)c(Q)$ modulo A^*) permet de se ramener à

$g(X^p) = fh$ avec $h \in \mathbb{Z}[X]$.

On projette alors cette égalité dans $(\mathbb{F}_p)$.

$g(X) = a_r X^r + \dots + a_0$ avec les $a_i \in \mathbb{Z}$

$g(X^p) = a_r X^{rp} + \dots + a_1 X^p + a_0$

mod p $\hookrightarrow g(X^p) = (\overline{a_r} X^r + \dots + \overline{a_0})^p$ par Frobenius.

Donc $\bar{g}(x^p) = (\bar{g}(x))^p$.

Soit alors $\varphi(x)$ un facteur irréductible de $\bar{f}(x)$ sur $\mathbb{F}_p$.

$$\text{On a } (\bar{g}(x))^p = \bar{f}(x) \bar{q}(x)$$

D'après le lemme d'Euler, $\varphi \mid \bar{g}$.

Comme on obtient $\Phi_n, \mathbb{F}_p$ à partir de $\Phi_n, \mathbb{Q}$ en réduisant modulo p ,

$$\bar{g} \mid \Phi_n \text{ sur } \mathbb{F}_p \Rightarrow \bar{f} \bar{g} \mid \bar{\Phi}_n = \Phi_n, \mathbb{F}_p$$

$$\text{Donc } \varphi^2 \mid \Phi_n, \mathbb{F}_p$$

Mais alors dans un corps de décomposition de Φ_n sur $\mathbb{F}_p$,

Φ_n aurait une racine double.

ABSURDE car $\text{Car}(\mathbb{F}_p) = p \nmid n$

Donc $\Phi_n, \mathbb{F}_p$ a pour racines les racines primitives de $\underbrace{x^n - 1}_{\text{de dérivée } n x^{n-1} \text{ (une racine est 0)}}$

4) si ζ' est une racine primitive n -ième de l'unité, on a

$$\zeta' = \zeta^m \text{ avec } m = p_1^{\alpha_1} \dots p_r^{\alpha_r} \text{ et } p_i \nmid n.$$

3) + petite récurrence, ζ' et ζ ont même polynôme minimal sur $\mathbb{Q}$.

$$\text{Donc } f(\zeta') = 0$$

Donc f admet toutes les racines primitives de l'unité comme racine.

$$\text{Donc } \deg(f) \geq \varphi(n)$$

$$\text{Comme } f \mid \Phi_n$$

$$\deg(f) \leq \varphi(n)$$

$$\text{Finalement } \deg(f) = \varphi(n)$$

$$\text{Donc } f = \Phi_n$$

Donc Φ_n est irréductible sur $\mathbb{Q}$.

Comme Φ_n est primitif car unitaire, Φ_n est irréductible sur $\mathbb{Z}$.