Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$ (et $\mathbb{Z}$)

Φ_n (G) V1

Leçons : 102, 125, 126, 141

Réf. : Perrin, Cours d'algèbre p 82 | Ortiz, Exercices d'algèbre p 169

Th : [Perrin]
Pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Q}$

Notations :
- $\Phi_n = \Phi_{n,\mathbb{Q}}$
- $\mu_n^* = \{$racines primitives de l'unité$\}$ dans $\mathbb{C}$, corps de décomposition de Φ_n

1) Soit $\zeta \in \mu_n^*$.

Rappel : $\zeta' \in \mu_n^*$ ssi $\exists\, m \in \mathbb{N} / \zeta' = \zeta^m$ et $m \wedge n = 1$

Soit $p \in \mathbb{N}$ un nombre premier tq $p \nmid n$. Alors $\zeta^p \in \mu_n^*$
$\Phi_n(\zeta) = \Phi_n(\zeta^p) = 0$ et $\Phi_n \in \mathbb{Q}[X]$ donc ζ et ζ^p sont algébriques sur $\mathbb{Q}$.
On note f et $g \in \mathbb{Q}[X]$ leurs polynômes minimaux respectifs.
f (et g) est alors unitaire et irréductible sur $\mathbb{Q}$

Objectif : Montrer que $f = \Phi_n$

2) Montrer que $f, g \in \mathbb{Z}[X]$: on en aura besoin pour projeter sur $\mathbb{F}_p$
On sait que $\Phi_n \in \mathbb{Z}[X]$ qui est factoriel.
Soit $\Phi_n = f_1^{\alpha_1} \dots f_r^{\alpha_r}$ sa décomposition en facteurs irréductibles dans $\mathbb{Z}[X]$. Φ_n étant unitaire, OPS f_i unitaire $\forall 1 \le i \le r$

Par conséquent, comme le contenu $c(f_i) = 1$, f_i est irréductible dans $\mathbb{Q}[X]$

On a $\Phi_n(\xi) = 0 = \prod_{i=1}^{r} (f_i(\xi))^{\alpha_i}$ (dans $\mathbb{C}$)

donc $\exists\, 1 \leq i \leq r$ tq $f_i(\xi) = 0$

et $f_i \in \mathbb{Q}[X]$ est irréductible unitaire, donc par unicité de f,

$$f = f_i \in \mathbb{Z}[X]$$ (et idem pour g)

Rq: Une fois qu'on aura m.q. $\Phi_n = f$, on aura également m.q. Φ_n est irréductible sur $\mathbb{Z}$ car f_i est irréductible sur $\mathbb{Z}$.

3) Montrer par l'absurde que $f = g$

OSP f et g sont distincts.

• f et g sont irréductibles dans $\mathbb{Z}[X]$, $f \mid \Phi_n$ et $g \mid \Phi_n$ donc par unicité de la décomposition dans un anneau factoriel, $fg \mid \Phi_n$ dans $\mathbb{Z}[X]$

• $g(\xi^p) = 0$ donc $g(X^p) \in \mathbb{Q}[X]$ divise f dans $\mathbb{Q}[X]$.

On a $g(X^p) \in \mathbb{Z}[X]$ et $f \in \mathbb{Z}[X]$ donc $g(X^p) \mid f$ dans $\mathbb{Z}[X]$

en effet, $f = g(X^p) Q_1$ dans $\mathbb{Q}[X]$.

$g(X^p) \in \mathbb{Z}[X]$ est unitaire, donc on peut effectuer la division euclidienne de f par $g(X^p)$:

$$f = g(X^p) Q_2 + R \quad \text{où} \quad Q_2, R \in \mathbb{Z}[X],\ \deg(R) < \deg(g(X^p)) \text{ ou } \deg(R) = 0$$

Alors

$$g(X^p)(Q_1 - Q_2) = R \quad \text{dans } \mathbb{Q}[X]$$

donc $Q_1 - Q_2 = 0$ (pour une raison de degré)

donc $R = 0$

donc $Q_1 = Q_2 = Q \in \mathbb{Z}[X]$ et $g(X^p) \mid f$ dans $\mathbb{Z}[X]$

Soit $h \in \mathbb{Z}[X]$ tq $g(X^p) = f h$.

En projetant cette égalité dans $\mathbb{F}_p$, on a donc

$$\overline{g(X^p)} = \bar{f}\,\bar{h}$$

"morphisme de Frobenius"

donc $\bar{g}^p = \bar{f}\,\bar{h}$

Soit φ un facteur irréductible de f dans $\mathbb{F}_p[X]$.

Alors φ est un facteur irréductible de $\bar{g}^p$

donc φ _____ $\bar{g}$

On a $f g \mid \Phi_n$ dans $\mathbb{Z}[X]$

donc $\bar{f}\,\bar{g} \mid \overline{\Phi_n} = \Phi_{n,\mathbb{F}_p}$ dans $\mathbb{F}_p[X]$.

donc $\varphi^2 \mid \Phi_{n,\mathbb{F}_p}$ dans $\mathbb{F}_p[X]$

Dans $K = D_{\mathbb{F}_p}(\Phi_{n,\mathbb{F}_p})$, $\Phi_{n,\mathbb{F}_p}$ admettrait alors une racine double.

On a, dans $\mathbb{F}_p[X]$, $P_n = X^n - 1 = \prod_{d \mid n} \Phi_{d,\mathbb{F}_p}$

et $P'_n = n X^{n-1}$, donc $P_n \wedge P'_n = 1$,

donc les racines de P_n dans K sont simples — absurde

Donc, $g = f$ et le poly. minimal de ξ^p dans $\mathbb{Q}[X]$ est le même que celui de ξ

4) Conclure que $\Phi_n = f$

Soit $\xi' \in \mu_n^*$.

$\exists\, m \in \mathbb{N}$ / $\xi' = \xi^m$, où $m \wedge n = 1$.

En écrivant $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, pour tout $1 \le i \le n$, $p_i \nmid n$.

Donc par récurrence, $f(\xi') = 0$ $\forall\, \xi' \in \mu_n^*$.

$|\mu_n^*| = \varphi(n)$, donc $\deg(f) \ge \varphi(n) = \deg \Phi_n$.

Enfin, $f \mid \Phi_n$ et f et g sont unitaires, donc $\Phi_n = f$.

Appli : [Oraux]

Soit $\mathbb{Q} \subset K$ une extension finie.

Alors K contient un nombre fini de racines de l'unité.

1) Soit ζ une racine de l'unité. Alors, ζ est une racine primitive de l'ordre donc il suffit de m.q. K contient un nb fini de racines primitives de l'unité

2) On pose $[K : \mathbb{Q}] = N$.

Soit $n \in \mathbb{N}^*$ et $\zeta \in \mu_n^* \text{ t.q } \zeta \in K$. Alors $\mathbb{Q}(\zeta) \subset K$

donc $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) \leq N$

3) Soit $X = \{n \geq 2 \ / \ \varphi(n) \leq N\}$. m.q. X est fini

a°/ Soit $n \in X$ et p premier $/ \ p \mid n$. Alors $p-1 \mid \varphi(n)$ donc $p \leq N+1$

Par conséquent, $\mathcal{P} = \{p \mid n, p \text{ premier et } n \in X\}$ est fini

b°/ Soit $n \in X$. On a alors :

$$N \geqslant \varphi(n) = n \prod_{\substack{p \mid n \\ p \in \mathcal{P}}} \underbrace{\left(1 - \frac{1}{p}\right)}_{\leq 1 \ \forall p \in \mathcal{P}} \geqslant n \times \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right)$$

donc : $\forall n \in X, \ n \leq \dfrac{N}{\prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right)}$