

102 125
 (121) 141
 (123) 144

15, 00

Gouadon
 p 97-98
 Perrin
 p. 83
 Obez p. 169

Irréductibilité des polynômes cyclotomiques

Thé: Pour tout $n \in \mathbb{N}$, Φ_n est irréductible sur $\mathbb{Q}(X)$.

Soit $\xi \in \mathbb{T}_n$ et p premier tel que $p \nmid n$. Alors $\xi^p \in \mathbb{T}_n$ et $\Phi_n(\xi) = \Phi_n(\xi^p) = 0$

Montrons que Φ_n est le polynôme minimal de ξ sur $\mathbb{Q}(X)$. Puisque $\mathbb{Z}[X]$ factoriel, on a $\Phi_n = \prod_{k=1}^r P_k^{a_k}$ où $P_k \in \mathbb{Z}[X]$ est unitaire et irréductible. Alors $\exists i, j \in \{1, \dots, r\}$ tel que

$P_i(\xi) = P_j(\xi^p) = 0$. Comme P_i, P_j sont irréductibles sur $\mathbb{Q}(X)$, ce sont les polynômes minimaux de ξ et ξ^p . Supposons $P_i \neq P_j$. On a $P_i \mid P_j(X^p)$ dans $\mathbb{Q}(X)$, donc $\exists Q \in \mathbb{Q}(X)$

tel que $P_i Q = P_j(X^p)$. On a $\frac{a}{b} \in \mathbb{Q}$ et $\tilde{Q} \in \mathbb{Z}[X]$ primitif tel que $Q = \frac{a}{b} \tilde{Q}$. Alors

$1 = \deg(P_j(X^p)) = \deg(\frac{a}{b} P_i \tilde{Q}) = \frac{a}{b}$ et $Q = \tilde{Q} \in \mathbb{Z}[X]$. En projetant dans $\mathbb{F}_p[X]$,

on a $\overline{P_i} \tilde{Q} = \overline{P_j(X^p)} = \overline{P_j}^p$ (par Fermat $a^p = a$ dans $\mathbb{F}_p$ et $\mathcal{F}: \mathbb{F}_p \rightarrow \mathbb{F}_p$ morphisme)

Soit $\bar{P} \in \mathbb{F}_p[X]$ facteur irréductible de $\bar{P_i}$, alors $\bar{P} \mid \bar{P_i}$ et $\bar{P} \mid \bar{P_j}$ dans $\mathbb{F}_p[X]$. Donc $\bar{P} \mid \Phi_n$

et $\bar{P} \mid X^n - 1$ dans $\mathbb{F}_p[X]$. En dérivant, $\bar{P} \mid nX^{n-1}$ et $\bar{P}$ divise $nX^{n-1}X - n(X^n - 1) = n$

dans $\mathbb{F}_p[X]$. Puisque $n \neq 0$, $\bar{P}$ est constant, donc $\bar{P_i}$ est constant. C'est absurde car

P_i est unitaire, et non constant. Alors $P_i = P_j$.

Donc $\forall k \in \{1, \dots, r\}$ tel que $k \nmid n$, on a $k = \prod_{i=1}^s p_i$ où p_i est premier tel que $p_i \nmid n$. Par récurrence sur s , on a que le polynôme minimal μ_{ξ} de ξ sur $\mathbb{Q}$ est celui de ξ^k .

Puisque $\mu_{\xi}(z) = 0 \forall z \in \mathbb{T}_n$, on a $\deg \mu_{\xi} \geq |\mathbb{T}_n| = \varphi(n)$. Or $\Phi_n(\xi) = 0$ donc $\mu_{\xi} \mid \Phi_n$, et $\mu_{\xi} = \Phi_n$ car unitaire et du même degré.

Appli: Soit $K/\mathbb{Q}$ de degré N . Alors contient un nombre fini de racines de l'unité.

Puisque $\forall n \in \mathbb{N}^*$, $\mathbb{Q}_n = \bigcup_{d \mid n} \mathbb{Q}_d$, il suffit de montrer que $\{n \in \mathbb{N}^* \mid \mathbb{T}_n \cap K \neq \emptyset\}$ est fini.

Soit $n \in \mathbb{N}^*$ et $\xi \in \mathbb{T}_n \cap K$, on a $\mathbb{Q} \subset \mathbb{Q}(\xi) \subset K$ donc $[\mathbb{Q}(\xi) : \mathbb{Q}] = \deg \Phi_n = \varphi(n) \leq [K : \mathbb{Q}] = N$.

On a $N \geq \varphi(n) = n \prod_{p \in \mathcal{P}} (1 - \frac{1}{p}) \geq n \prod_{p \in \mathcal{P}} (1 - \frac{1}{p})$ donc $n \leq \frac{N}{\prod_{p \in \mathcal{P}} (1 - \frac{1}{p})}$.

Rac: $n \in \mathbb{N}$ fini. On pose $P(s) = \prod_{k \in \{1, \dots, r\}, k \nmid n} \prod_{i=1}^s p_i$, $\forall \xi \in \mathbb{T}_n \mu_{\xi} = \mu_{\xi^k}$, $s \in \mathbb{N}^*$

$P(1)$: $\forall p \in \mathcal{P} \cap \mathbb{N}$, $p \nmid n$: $\mu_{\xi} = \mu_{\xi^p}$ vraie. Supp $P(s-1)$, avec $k \in \mathcal{P} \cap \mathbb{N}$, $\mu_{\xi} = \mu_{\xi^k} = \mu_{\xi^k}^{p_1} = \mu_{\xi^k}^{p_2} = \dots = \mu_{\xi^k}^{p_s}$.

- * $\xi, \xi' \in \Pi_n \rightarrow \Phi_n = \prod_{i=1}^n P_i \rightarrow P_i(\xi) = P_j(\xi')$ poly min ($P_i \nmid P_j$ ou $P_j \nmid P_i$) $\Rightarrow P_i \mid P_j(X)$ dans $\mathbb{Q}(X)$
 $\rightarrow P_i \mathbb{Q} = P_j(X)$ dans $\mathbb{Z}(X) \rightarrow P_i \mathbb{Q} = P_j \mathbb{Q} \rightarrow \overline{P_i} \mid \overline{P_j} \rightarrow \overline{P_i} \mid \overline{P_j} \rightarrow \overline{P_i}^2 \mid X^n - 1, \overline{P_i} \mid nX^{n-1}$
 $\rightarrow \overline{P_i}$ est $\nmid P_i = P_j \rightarrow$ Rec $\mu_g = \mu_{gk} \forall k \mid n-1 \rightarrow \deg \mu_g \in \varphi(n), \Phi_n \mid \mu_g \rightarrow \Phi_n = \mu_g$
- * $\Pi_n \Pi_n \rightarrow N \geq \varphi(n)$ formule degré $\rightarrow n \leq \frac{N}{\pi(1-\frac{1}{p})}$

Lemma: $\forall n \in \mathbb{N}^*, X^n - 1 = \prod_{d \mid n} \Phi_d$

On a $\Phi_n = \prod_{d \mid n} \Phi_d$ par Lagrange, $X^n - 1 = \prod_{z \in \mathbb{U}_n} (X - z) = \prod_{z \in \prod_{d \mid n} \mathbb{U}_d} (X - z) = \prod_{d \mid n} \prod_{z \in \mathbb{U}_d} (X - z) = \prod_{d \mid n} \Phi_d$

Lemma: $\forall n \in \mathbb{N}^*, \Phi_n \in \mathbb{Z}(X)$ unitaire

I Si $n=1$, $\Phi_1 = X-1 \in \mathbb{Z}(X)$ unitaire. Supp $\forall d \mid n-1$, $\Phi_d \in \mathbb{Z}(X)$ unitaire

H On a $X^n - 1 = F_n \Phi_n$, $F_n = \prod_{d \mid n, d \neq n} \Phi_d \in \mathbb{Z}(X)$ unitaire par I.H.R.

Par div eucl, $\exists Q, R \in \mathbb{Z}(X)$, $X^n - 1 = F_n Q + R$ $\deg R < \deg F_n$ or $R=0$

Donc $F_n \Phi_n = F_n Q + R$, $F_n (\Phi_n - Q) = R$. Si $\Phi_n \neq Q$, $\deg(F_n (\Phi_n - Q)) = \deg R \geq \deg F_n$

Alors $R=0$ et $Q = \Phi_n \in \mathbb{Z}(X)$ est unitaire.

Corollaire: $\forall n \in \mathbb{N}^*, [\mathbb{Q}(\mathbb{U}_n) : \mathbb{Q}] = \varphi(n)$

Soit $\xi \in \Pi_n$. On a $\Phi_n = \mu_{\xi, \mathbb{Q}}$ poly min de ξ sur $\mathbb{Q}$. Puisque $\langle \xi \rangle = \mathbb{U}_n$, on a

$[\mathbb{Q}(\mathbb{U}_n) : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}] = \deg \Phi_n = |\Pi_n| = \varphi(n)$.

Proposition: Soit $n, m \in \mathbb{N}^*$ $n \wedge m = 1$, $\alpha \in \Pi_n, \beta \in \Pi_m$. Alors $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\mathbb{U}_{nm})$, $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$

Soit $w = \alpha\beta \in \mathbb{C}^*$, on a $\text{ord}(w) = nm$ ($w^{nm} = (\alpha^n)^m (\beta^m)^n = 1$ et $w^k = 1$, ie $\alpha^k = \beta^{-k}$

or $\langle \alpha \rangle \cap \langle \beta \rangle = \{1\}$ car $|\langle \alpha \rangle \cap \langle \beta \rangle| \mid |\langle \alpha \rangle| = n$ et $|\langle \alpha \rangle \cap \langle \beta \rangle| \mid m$ donc $|\langle \alpha \rangle \cap \langle \beta \rangle| \mid n \wedge m = 1$.

Alors $\alpha^k = \beta^{-k} = 1$ et $n \mid k, m \mid k, n \wedge m = nm \mid k$. Donc $w \in \Pi_{nm}$. De plus $\mathbb{Q}(w) \subset \mathbb{Q}(\alpha, \beta)$.

On a $\alpha^m \in \Pi_n, \beta^n \in \Pi_m$, donc $\mathbb{Q}(\alpha) = \mathbb{Q}(\mathbb{U}_n) = \mathbb{Q}(\alpha^m)$, $\mathbb{Q}(\beta) = \mathbb{Q}(\mathbb{U}_m) = \mathbb{Q}(\beta^n)$.

Or $\alpha^m = w^m \in \mathbb{Q}(w)$ donc $\mathbb{Q}(\alpha) \subset \mathbb{Q}(w)$ et sym $\mathbb{Q}(\beta) \subset \mathbb{Q}(w)$, et $\mathbb{Q}(\alpha, \beta) \subset \mathbb{Q}(w)$.

Alors $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(w) = \mathbb{Q}(\mathbb{U}_{nm})$. Donc $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = \varphi(nm) = \varphi(n)\varphi(m)$ ($n \wedge m = 1$).

Alors $\varphi(n)\varphi(m) = [\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)] [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)] \varphi(n)$ car $\mathbb{Q}(\alpha) = \mathbb{Q}(\mathbb{U}_n)$

et $[\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)] = \varphi(m)$. Soit $K = \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$, alors $\varphi(m) = [\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)] \leq d$

où $d = [\mathbb{Q}(\beta) : \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)]$ (e_j base de $\mathbb{Q}(\beta)$, $\forall x \in \mathbb{Q}(\alpha)(\beta)$, $x = \sum_{j=1}^d a_j b_j$ où

$a_j \in \mathbb{Q}(\alpha)$, $b_j \in \mathbb{Q}(\beta)$ donc $b_j = \sum_{i=1}^d \lambda_{ij} e_j$, $\lambda_{ij} \in K$ et $x = \sum_{i=1}^d (\sum_{j=1}^d a_i \lambda_{ij} e_j)$ où $a_i \lambda_{ij} \in \mathbb{Q}(\alpha)$

donc e_j base de $\mathbb{Q}(\alpha)(\beta)$. Comme $\varphi(m) = [\mathbb{Q}(\beta) : \mathbb{Q}] \leq [\mathbb{Q}(\beta) : K]$

où $[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\beta) : K] [K : \mathbb{Q}]$, on a $[K : \mathbb{Q}] \leq 1$ ie $K = \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.