

Iréductibilité des polynômes cyclotomiques (Gézard)

Racines: 102, (121), (123), 125, (127) 141, 144, 142

Théorème: $\forall n \in \mathbb{N}^*$, $\phi_{n, \mathbb{Q}}(x)$ est irréductible dans $\mathbb{Q}[x]$.

Preuve: Soit ω une racine primitive n -ième de l'unité dans $\mathbb{C}$.

Notons $f(x) = \pi_{\omega, \mathbb{Q}}(x)$ le polynôme minimal de ω .

$f(x) \mid x^n - 1$ dans $\mathbb{Q}[x]$. Notons $x^n - 1 = f(x)h(x)$, $h(x) \in \mathbb{Q}[x]$.

Comme $x^n - 1 \in \mathbb{Z}[x]$ et $f(x)$ est unitaire, on a $h(x) \in \mathbb{Z}[x]$.

• Montrons que si u est une racine de f et p un nombre premier, u^p est aussi racine de f .

Comme $f(x) \mid x^n - 1$ dans $\mathbb{Q}[x]$, on a $u^n - 1 = 0$. u est une racine n -ième de l'unité dans $\mathbb{C}$ donc u^p aussi: $0 = (u^p)^n - 1 = f(u^p)h(u^p)$

Supposons $f(u^p) \neq 0$. Alors $h(u^p) = 0$. Or, u est racine de f irréductible dans $\mathbb{Q}[x]$ donc $f(x) = \pi_{u, \mathbb{Q}}(x)$. Donc $f(x) \mid h(x^p)$ dans $\mathbb{Q}[x]$.

$\exists g \in \mathbb{Q}[x]$, $f(x) = h(x^p)g(x)$ (*)

$h(x) \in \mathbb{Z}[x]$ et $f(x)$ est unitaire donc $g(x) \in \mathbb{Z}[x]$.

On réduit (*) modulo p : $\bar{h}(x)^p = \overline{h(x^p)} = \bar{f}(x) \bar{g}(x) \in \mathbb{F}_p[x]$.

Soit $\theta \in \mathbb{F}_p[x]$ un facteur irréductible de $\bar{f}$. Alors $\theta \mid \bar{h}^p$ donc $\theta \mid \bar{h}$ donc $\theta^2 \mid \bar{f} \bar{h} = \overline{x^n - 1}$ dans $\mathbb{F}_p[x]$.

Par conséquent, $x^n - 1$ possède une racine double dans $\mathbb{F}_p$ une clôture algébrique de $\mathbb{F}_p$ absurde car $x^n - 1$ est premier avec sa dérivée nx^{n-1} dans $\mathbb{F}_p[x]$: $\left(\frac{1}{n} x^n - x^{n-1} - (x^n - 1) \right) \neq 1 \rightarrow$ Bezout
Finalement $f(u^p) = 0$.

• Comme ω est une racine de f , et comme toute racine primitive n -ième de l'unité dans $\mathbb{C}$, c'est toute ω^k , k et $n-1$ peut être obtenus par itération successive de ω à des puissances où p premier, $p \nmid n$.

ω est racine de f donc $\omega^{p^2} \text{ aussi } \dots \omega^{p^{n-1}} \text{ aussi } \dots \omega^{p^n} = \omega \text{ aussi!}$
 D'après α qui précède, toute racine n -ième primitive n -de
 de l'unité dans $\mathbb{C}$ est racine de f . Donc $\deg(f) \geq \varphi(n)$.

Or, $f(x) \mid \Phi_{n,\mathbb{Q}}(x)$ dans $\mathbb{Q}[x]$, $\deg(\Phi_{n,\mathbb{Q}}) = \varphi(n)$ et f et $\Phi_{n,\mathbb{Q}}$
 tous deux unitaires. Donc $\Phi_{n,\mathbb{Q}}(x) = f(x) = \prod_{\omega \in \mathbb{Q}} (x - \omega)$.
 Ainsi, $\Phi_{n,\mathbb{Q}}$ est irréductible dans $\mathbb{Q}[x]$.

Lemme: (à démontrer AVANT): Soit P, A, B trois éléments non nuls
 de $\mathbb{Z}[X]$. On suppose que $P \in \mathbb{Z}[X]$, que $P = AB$ et P et A sont unitaires.
 Alors A et B sont dans $\mathbb{Z}[X]$.

Preuve: B est aussi unitaire. Notons $A(X) = X^m + \sum_{i=0}^{m-1} a_i X^i$, $a_i \in \mathbb{C}$.
 Pour tout i , $a_i = \frac{p_i}{q_i}$, $p_i \in \mathbb{Z}$, $q_i \in \mathbb{N}^*$ sont premiers entre eux.
 Soit q un multiple commun à $q_0, \dots, q_{m-1}$. Alors

$$A(X) = \frac{1}{q} \sum_{i=0}^{m-1} z_i X^i + X^m, \quad z_i \in \mathbb{Z}$$

Quitte à diviser $z_0, \dots, z_{m-1}$ et q par $\text{PGCD}(z_0, \dots, z_{m-1}, q)$, on peut
 supposer que $\text{PGCD}(z_0, \dots, z_{m-1}, q) = 1$.

On note $A_1(X) = qX^m + \sum_{i=0}^{m-1} z_i X^i$, $A_1(X) \in \mathbb{Z}[X]$, $A(X) = \frac{1}{q} A_1(X)$
 et $c(A_1) = 1$.

De même $\exists n \in \mathbb{N}^*$, $B(X) = \frac{1}{n} B_1(X)$ avec $B_1(X) \in \mathbb{Z}[X]$, $c(B_1) = 1$.

Or $P = A_1 B_1$ et d'après le lemme de Gauss
 $c(q) c(P) = c(A_1) c(B_1)$

$q = 1$ donc $q = 1 = 1$. D'où $A = A_1 \in \mathbb{Z}[X]$ et $B = B_1 \in \mathbb{Z}[X]$.

Lemme (Gauss): $c(PQ) = c(P)c(Q)$

Preuve: Supposons P, Q primitifs. Si $c(PQ) \neq 1$, il existe $p \in \mathbb{Z}$ premier
 qui divise $c(PQ)$ (A factoriel). Mais comme $c(P) = c(Q) = 1$, il existe
 $i_0, j_0 \in \mathbb{N}$ tels que $p \mid a_i$ $i < i_0$ et $p \nmid a_{i_0}$
 $p \mid b_j$ $j < j_0$ et $p \nmid b_{j_0}$.

Alors $p \mid c_{i_0 j_0} = \sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i < i_0 \text{ ou } j < j_0}} a_i b_j$ mais alors
 $\hookrightarrow$ avec Euclide

cas général: $d = c(P)$, $e = c(Q)$, $P' = \frac{P}{d}$ $Q' = \frac{Q}{e}$. $PQ = de$
 $c(P'Q') = 1$ donc $c(PQ) = de$