Polynômes cyclotomiques

Leçon : 102, 120, 121, 141

Ref : Perrin, Gourdon

On étudie les polynômes cyclotomiques sur $\mathbb{Q}$.

On note $\mu_n = \{\zeta \in \mathbb{C}, \zeta^n = 1\}$, $\mu_n^\times = \{\zeta \in \mu_n, o(\zeta) = n\}$
(racines primitives).

$$\Phi_n(X) := \prod_{\zeta \in \mu_n^\times} (X - \zeta).$$

Rappel : (preuve à la fin)

- Φ_n unitaire, $\deg \Phi_n = \varphi(n)$
- $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$
- $\Phi_n \in \mathbb{Z}[X]$

→ l'étude de $\Phi_{n,\mathbb{Q}}$ permet d'étudier $\Phi_{n,k}$, k corps qcq.

Théorème

$\Phi_n(X)$ est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.

Preuve

Stratégie : mq Φ_n est le polynôme minimal de $\zeta \in \mu_n^\times$, pour ζ racine primitive n-ième qcq.

Soit $\zeta \in \mathbb{C}$ une racine primitive n-ième de 1. Soit p un nombre premier ne divisant pas n. Alors $\zeta^p \in \mu_n^\times$ aussi.
(les générateurs de μ_n, ie les racines primitives, sont les ζ^m, avec $m \wedge n = 1$).

2) Soit $f \in \mathbb{Q}[X]$ le polynôme minimal de ζ, et $g \in \mathbb{Q}[X]$ celui de ζ^p. On va mq $f, g \in \mathbb{Z}[X]$.

$\mathbb{Z}[X]$ est factoriel (car $\mathbb{Z}$ l'est, c'est le lemme de Gauss).

On peut donc écrire $\Phi_m(X) = P_1(X)^{\alpha_1} \cdots P_r(X)^{\alpha_r}$ avec $P_i \in \mathbb{Z}[X]$ irréductible. Φ_m est unitaire, donc quitte à multiplier les P_i par -1, on peut supposer les P_i unitaires.

Mais alors ζ est racine de l'un des P_i, qui est <u>unitaire</u> <u>irréductible</u> sur $\mathbb{Z}$, donc sur $\mathbb{Q}$, et ainsi $f = P_i \in \mathbb{Z}[X]$.

De même, $g = P_j \in \mathbb{Z}[X]$.

De plus, f et g divisent Φ_m dans $\mathbb{Z}[X]$.

3) Mq $f = g$. Par l'absurde, on suppose que $f \neq g$.

Par irréductibilité de f et g, on a $fg \mid_{\mathbb{Z}[X]} \Phi_m$.

Par ailleurs, comme $g(\zeta^p) = 0$, ζ est racine de $g(X^p)$, donc $f(X)$ divise $g(X^p)$ dans $\mathbb{Q}[X]$. Il existe $R \in \mathbb{Q}[X]$ tq $g(X^p) = f(X) R(X)$.

On écrit $R = \frac{a}{b} R'$, avec $R' \in \mathbb{Z}[X]$ de contenu 1, alors, comme f, g sont unitaires leur contenu est 1 et par le lemme de Gauss :

$$\begin{cases} c(fR) = c(f)c(R) = 1 \times \frac{a}{b} \times c(R') = a/b \\ c(g(X^p)) = 1. \end{cases}$$

Donc $R \in \mathbb{Z}[X]$, donc $f(X)$ divise $g(X^p)$ dans $\mathbb{Z}[X]$.

On projette dans $\mathbb{F}_p$.

Si $g(X) = \sum_{i=0}^{n} a_i X^i$, $a_i \in \mathbb{Z}$, alors

$g(X^p) = \sum_{i=0}^{n} a_i X^{pi}$, donc dans $\mathbb{F}_p$, comme $\bar{a_i} = \bar{a_i}^p$:

$$\bar{g}(X^p) = \sum_{i=0}^{n} \bar{a_i}^p (X^i)^p \underset{\text{Frobenius}}{=} \left(\sum_{i=0}^{n} \bar{a_i} X^i\right)^p = \bar{g}(X)^p.$$

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

$\bar{g}(X)^p = \bar{f}(X)\,\bar{h}(X)$, donc φ divise $\bar{g}^p$ et par le lemme d'Euclide, φ divise $\bar{g}$.

fg divise Φ_m sur $\mathbb{Z}$, donc $\bar{f}\bar{g}$ divise $\overline{\Phi_m}$ sur $\mathbb{F}_p$.

Ainsi, φ^2 divise $\overline{\Phi_m}$.

Or, $X^m - 1 = \Phi_m R$, où $R = \prod_{\substack{d \mid m \\ d \neq m}} \Phi_d \in \mathbb{Z}[X]$

$\Rightarrow X^m - \bar{1} = \overline{\Phi_m}\,\bar{R} = \varphi^2 S$, où $S = \frac{\overline{\Phi_m}}{\varphi^2} \bar{R}$.

Par dérivation, $\bar{m} X^{m-1} = 2\varphi\varphi' S + \varphi^2 S'$

$\Rightarrow \varphi \mid \bar{m} X^{m-1}$. $\Rightarrow \varphi \mid \bar{m} X^m$

Or $\varphi \mid \bar{m} X^m - \bar{m}$, donc par différence

$\varphi \mid \bar{m}$, or $p \nmid m$, donc $\underline{\bar{m} \neq 0}$ et φ est constant.

On a une contradiction, donc $\boxed{f = g}$.

4) Si $\zeta' \in \mu_m^\times$, on a $\zeta' = \zeta^m$, avec $m \wedge n = 1$.

En écrivant $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, avec $p_i \nmid n$, par une récurrence immédiate, il vient que ζ' et ζ ont le m̂ pol. minimal sur $\mathbb{Q}$, donc $f(\zeta') = 0$, de sorte que f admet toutes les racines primitives de l'unité comme zéros. Donc $d^\circ f \geq \varphi(n)$, et $f \mid \Phi_n$, d'où $\boxed{f = \Phi_n}$

Donc Φ_n est irréductible sur $\mathbb{Q}$, et donc sur $\mathbb{Z}$ car son contenu est 1 (il est unitaire)

□

<u>Corollaire</u> Si $\zeta \in \mu_n^\times$, son polynôme minimal est Φ_n sur $\mathbb{Q}$, et on a $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

<u>Proposition</u> On suppose toujours $(n, \mathrm{car}(k)) = 1$.

1) $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

$$\mu_n = \bigsqcup_{d \mid n} \mu_d^\times$$

2) $\Phi_n \in \mathbb{Z}[X]$

Récurrence + DE

3) Soit k un corps qcq, $\sigma : \mathbb{Z} \to k$ l'homomorphisme canonique. On a alors

$$\Phi_{n,k}(X) = \sigma(\Phi_{n,\mathbb{Q}}(X)).$$

En particulier, $\Phi_{m,\mathbb{F}_p}$ s'obtient à partir de $\Phi_{m,\mathbb{Q}}$ par réduction modulo p.

__Preuve__ de 3).

Par récurrence. $m=1$, c'est bon.

Dans $\mathbb{Z}[X]$, on a $X^m - 1 = \prod_{d \mid m} \Phi_{d,\mathbb{Q}}(X) = \Phi_{m,\mathbb{Q}} F(X)$,

où $F(X) = \prod_{\substack{d \mid m \\ d \neq m}} \Phi_{d,\mathbb{Q}}(X)$.

On note $K_m = D_k(X^m - 1)$. On a dans $K_m[X]$,

$X^m - 1 = \sigma(X^m - 1) = \sigma(\Phi_{m,\mathbb{Q}})\sigma(F)$, par HR :

$$\sigma(F) = \prod_{\substack{d \mid m \\ d \neq m}} \sigma(\Phi_{d,\mathbb{Q}}) = \prod_{\substack{d \mid m \\ d \neq m}} \Phi_{d,k}$$

Par intégrité de $k[X]$, il vient $\Phi_{m,k} = \sigma(\Phi_{m,\mathbb{Q}})$.

$$\left(\prod_{d \mid m} \Phi_{d,k} = \left(\prod_{\substack{d \mid m \\ d \neq m}} \Phi_{d,k} \right) \sigma(\Phi_{m,\mathbb{Q}}) \right).$$

□

⚠ on perd l'irréductibilité sur le corps $\mathbb{F}_p$.

Par exemple, $\Phi_8 = X^4 + 1$ est réductible sur tous les corps $\mathbb{F}_p$.

En effet : $\cdot\, p = 2$, $X^4 + 1 = (X+1)^4$

$\cdot\, p > 2$, ⊕ de travail.

On a $X^8-1=(X^4+1)(X^4-1)$, ainsi si X^4+1 a une racine x dans un corps K, on a $x^8=1$, avec $x^4\neq 1$, ie x est un élément d'ordre 8 de K^*.

Rq : $P\in k[X]$, $d^\circ P=n>0$,

Pirréductible sur $k \iff P$ n'a pas de racines dans les extensions K de k tq $[K:k]\leq n/2$.

Pour prouver que X^4+1 est réductible sur $\mathbb{F}_p$, on va mq qu'il admet une racine dans $\mathbb{F}_{p^2}$, donc de mq $\mathbb{F}_{p^2}^*$ ~~est~~ contient un élt d'ordre 8.

Or $\mathbb{F}_{p^2}^*$ est cyclique d'ordre $p^2-1 \to$ multiple de 8

(car $p^2-1=(p-1)(p+1)$ et p impair).

On a en fait le résultat suivant :

Thm Sont équivalents :

1) il existe p premier, $(p,n)=1$, tq $\Phi_{n,\mathbb{F}_p}$ irréductible sur $\mathbb{F}_p$.
2) $(\mathbb{Z}/n\mathbb{Z})^\times$ cyclique
3) $n=1,2,4,q^\alpha,2q^\alpha$ avec q premier impair.

Rmq : Si car$(k)\mid n$, k ne possède pas de racine primitive n-ième de l'unité.

Si $p=\text{car}(k)\mid n$, $n=pm$, et $X^n-1=(X^m-1)^p$