X

IRREDUCTIBILITE DES POLYNOMES CYCLOTOMIQUES

(Calais Extension de corps, théorie de Galois p86-89)
Gozard, Théorie de Galois p68.
(Gourdon Algèbre)

14,45 sans démo lemmes
18 min pour tout.

Prérequis
- polynôme minimal
- μ_n cyclique d'ordre n
- (division euclidienne dans $\mathbb{Z}[X]$ avec coeff dominant inversible)
- Lemme de Gauss, contenu, primitif

K corps $\Rightarrow K[X]$ euclidien $\Rightarrow K[X]$ factoriel
factoriel = irred $\Leftrightarrow$ premier ?

On note μ_n l'ensemble des racines n-ièmes de l'unité sur $\mathbb{C}$.
μ_n^* l'ensemble des racines n-ièmes primitives de l'unité.
Φ_n le n-ème polynôme cyclotomique.

Théorème = $n\in\mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$ et Φ_n est irréductible dans $\mathbb{Q}[X]$. Comme il est unitaire donc primitif, il le sera dans $\mathbb{Z}[X]$.

Lemme 1 $X^n-1 = \prod_{d|n} \Phi_d(X)$ Calais p86 ou Gozard p68

Dém: μ_n est cyclique d'ordre n donc pour tout diviseur d de n, il y a exactement $\varphi(d)$ éléments d'ordre d dans μ_n. Or les éléments de μ_d^* sont au nb de $\varphi(d)$ et d'ordre d donc ce sont μ_d^*.
L'union est disjointe car tout élément a un unique ordre: $\mu_n = \bigsqcup_{d|n} \mu_d^*$

d'où $X^n-1 = \prod_{\alpha\in\mu_n}(X-\alpha) = \prod_{d|n}\left(\prod_{\alpha\in\mu_d^*}(X-\alpha)\right) = \prod_{d|n}\Phi_d$.

A priori on a seulement $\Phi_n \in \mathbb{C}[X]$

Dém: **Etape 1: Par récurrence forte $\Phi_n\in\mathbb{Z}[X]$.** ~~Calais p87~~ Goz p68

- $n=1$ $\Phi_1(X) = X-1 \in \mathbb{Z}[X]$.
- Supposons le résultat vrai jusqu'au rang n-1.

On a, par le lemme, $X^n-1 = \Phi_n F$ où $F = \prod_{\substack{d|n\\ d\neq n}} \Phi_d \in \mathbb{Z}[X]$ par hypothèse de récurrence.

on fait la div eucli de X^n-1 par F dans $\mathbb{Q}[X]$, ce qui donne $\Phi_n\in\mathbb{Q}[X]$ cf (Δ)

puis par lemme 2, $\Phi_n\in\mathbb{Z}[X]$ et $F\in\mathbb{Z}[X]$

~~X^n-1 et F sont à coefficients dans $\mathbb{Z}[X]$, et F est à coefficient dominant inversible d'où il existe $Q, R\in\mathbb{Z}[X]$ $\deg R<\deg F$ tq~~ (Lemme 6.13 Calais p85)

~~$X^n-1 = FQ+R$. D'où $F(\Phi_n - Q) = R$.~~
~~si $R\neq 0$ $\deg F + \deg(\Phi_n - Q) = \deg R < \deg F$.~~ absurde d'où $R=0$

~~D'où $\Phi_n = Q \in \mathbb{Z}[X]$.~~

Etape 2: ~~Tout~~ P_ω doit vivre dans $\mathbb{Z}[X]$

Soit $\omega\in\mu_n^*$. On note P_ω le polynôme minimal de ω sur $\mathbb{Q}$. existe car $\omega^n-1=0$. $X^n-1\in\mathbb{Q}[X]$

$\omega^n-1=0$ d'où $P_\omega | X^n-1$. : il existe $Q\in\mathbb{Q}[X]$ tq $X^n-1 = P_\omega Q$.
Comme X^n-1 et P_ω sont unitaires, on peut appliquer le lemme 2 donc $P_\omega\in\mathbb{Z}[X]$ et $Q\in\mathbb{Z}[X]$. on aura besoin plus tard de $Q\in\mathbb{Z}[X]$

On veut mq $P_\omega = \Phi_n$.

Etape 3: $P_\omega | \Phi_n$ dans ~~$\mathbb{Z}[X]$~~ $\mathbb{Q}[X]$ (P_ω et Q unitaire)

$\Phi_n(\omega)=0$ d'où $P_\omega | \Phi_n$ dans $\mathbb{Q}[X]$. et même dans $\mathbb{Z}[X]$ par le lemme 2 (pas besoin):
$\Phi_n = PR$ Φ_n unitaire et P_ω unitaire donc $P_\omega\in\mathbb{Z}[X]$ et $R\in\mathbb{Z}[X]$.
$\Phi_n \in\mathbb{Z}[X]$
donc $P_\omega | \Phi_n$ dans $\mathbb{Z}[X]$

Étape 4: Soit $u \in \mathbb{C}$ une racine de P_ω, p premier $p \wedge n$ alors u^p est une racine de P_ω

• Comme $P_\omega \mid X^n - 1$ dans $\mathbb{Q}[X]$, on a $u^n - 1 = 0$ donc $u \in \mu_n$ d'où $u^p \in \mu_n$.
↳ $\omega^n - 1 = 0$, car $\omega \in \mu_n^\times$ d'où

d'où $0 = (u^p) - 1 = P_\omega(u^p)\, Q(u^p)$ $\quad Q \in \mathbb{Z}[X]$ par étape 2.

• Supposons par l'absurde que $P_\omega(u^p) \neq 0$ alors $Q(u^p) = 0$. Mais u annule P_ω qui est irréductible sur $\mathbb{Q}$ d'où P_ω est le polynôme minimal de u sur $\mathbb{Q}$.
et donc $P_\omega \mid Q(X^p)$ dans $\mathbb{Q}[X]$.
d'où $Q(X^p) = P_\omega g$ où $g \in \mathbb{Q}[X]$
Comme $Q(X^p) \in \mathbb{Z}[X]$ unitaire et P_ω unitaire, d'après le lemme 2, $g \in \mathbb{Z}[X]$

• On a donc le droit maintenant de réduire modulo p : $\varphi : \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p\mathbb{Z}[X]$ $\quad \varphi_{X \to X}$

$p \nmid n$

$[\bar{Q}(X)]^p = \bar{Q}(X^p)$ par le morphisme de Frobenius.
$= \bar{P_\omega}\, \bar{g}$.

$\mathbb{F}_p$ corps $\Rightarrow$ $\mathbb{F}_p[X]$ euclidien donc factoriel

Soit Θ un facteur irréductible de $\bar{P_\omega}$ dans $\mathbb{F}_p[X]$. alors $\Theta \mid \bar{Q}^p$ donc $\Theta \mid \bar{Q}$ dans $\mathbb{F}_p[X]$.
car est irréductible donc premier. donc $\Theta^2 \mid \bar{P_\omega}\, \bar{Q} = X^n - \bar{1}$ dans $\mathbb{F}_p[X]$

(Mais $X^n - \bar{1}$ est sans facteur carré ds $\mathbb{F}_p$ car $\bar{n} X^{n-1} \wedge X^n - \bar{1} = 1$ puisque $p \nmid n$.
Absurde. donc $P_\omega(u^p) = 0$ $\quad \frac{1}{\bar{n}} X\, \bar{n} X^{n-1} - (X^n - \bar{1}) = \bar{1}$ Bezout

voir fin

Étape 5: $\mu_n^\times \subset \{$racines de $P_\omega\}$. Gourdon

Soit ζ une racine primitive n^e de l'unité, $\exists k$, $k \wedge n = 1$, tq $\zeta = \omega^k$.
$k = p_1 \dots p_s$ avec p_i premiers.

hyp de réc H_s = $P_\omega(\omega^{p_1 \dots p_s}) = 0$

- si $s = 1$, $k = p_1$, $p_1 \wedge n = 1$. on vient de le montrer à l'étape 4.
- Si c'est vrai jusqu'à $s-1$.
  Comme $p_1 \dots p_s \wedge n = 1$ alors $p_s \wedge n = 1$ et $p_1 \dots p_{s-1} \wedge n = 1$.

Par hypothèse de récurrence $\omega^{p_1 \dots p_{s-1}}$ est racine de P_ω or $p_s \wedge n = 1$
donc $P_\omega(\zeta) = 0$. par étape 4

Étape 6: Conclusion:

car Φ_n est à racines simples
↳ ds $\mathbb{C}$ ou ds $\mathbb{Z}$. dans $\mathbb{Q}$ suffit

D'après l'étape 5, $\Phi_n \mid P_\omega$ or $P_\omega \mid \Phi_n$. or ils sont unitaires donc $\Phi_n = P_\omega$.
et comme P_ω est irréductible sur $\mathbb{Q}$, Φ_n l'est.

Rq : En même temps, on a montré que le polynôme minimal sur $\mathbb{Q}$ de toute racine n^e primitive de l'unité est Φ_n. et donc que $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n) = \deg \Phi_n$.

Gozard

Lemme 2 : Soit $P \in \mathbb{Z}[X]$ non nul unitaire, $A, B \in \mathbb{Q}[X]$ non nuls, tq $P = AB$ et A est unitaire alors $A, B \in \mathbb{Z}[X]$.

3min

Dém : Déjà B est unitaire. On note $A(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$, $a_i = \frac{p_i}{q_i} \in \mathbb{Q}$. $p_i \in \mathbb{Z}$, $q_i \in \mathbb{N}^*$
$p_i \wedge q_i = 1$. On pose $q = \mathrm{ppcm}(q_1, \dots, q_{n-1}) \in \mathbb{N}$

mise sous forme contenu × primitif

Alors $A(X) = X^n + \frac{1}{q} \sum_{i=0}^{n-1} z_i X^i$ où $z_i \in \mathbb{Z}$. $\quad d = \mathrm{pgcd}(z_0, \dots, z_{n-1}, q) \in \mathbb{Z}$

$$= X^n + \frac{d}{q} \sum_{i=0}^{n-1} \frac{z_i}{d} X^i = X^n + \frac{1}{\tilde{q}} \sum_{i=0}^{n-1} \tilde{z}_i X^i$$

$\tilde{q} \in \mathbb{N}$, $\tilde{z}_i \in \mathbb{Z}$ et premiers entre eux

↳ on note $q = \tilde{q}$ et $z_i = \tilde{z}_i$ ensuite

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

A_1 est primitif car $\mathrm{pgcd}(z_0, \dots, z_{n-1}, q) = 1$.

De la même manière $B(X) = \frac{1}{r} B_1(X)$ où $B_1 \in \mathbb{Z}[X]$ primitif, $r \in \mathbb{N}$

d'où $qrP = A_1 B_1$ or d'après le lemme de Gauss, A_1B_1 est primitif (produit de deux polynômes primitifs)

d'où $\mathcal{C}(qrP) = \mathcal{C}(A_1B_1) = 1$
$= qr\,\mathcal{C}(P) = qr$ car P unitaire.

Donc $qr = 1$ or $q \in \mathbb{N}, r \in \mathbb{N}$ d'où $q = r = 1$. d'où $A = A_1 \in \mathbb{Z}[X]$
$B = B_1 \in \mathbb{Z}[X]$

* pour ne pas parler de "pseudo division" dans $\mathbb{Z}[X]$

(Δ) $X^n - 1$ et $F \in \mathbb{Q}[X]$, $X^{n-1} = FQ + R$ $\deg R < \deg F$, $Q, R \in \mathbb{Q}[X]$ division euclid ds $\mathbb{Q}$

or $X^{n-1} = \Phi_n F$, par unicité, $Q = \Phi_n$ et $R = 0$ donc $\underline{\Phi_n \in \mathbb{Q}[X]}$

$X^n - 1 = \Phi_n F$, $X^n - 1 \in \mathbb{Z}[X]$ unitaire, $F, \Phi_n \in \mathbb{Q}[X]$, Φ_n unitaire
d'où $F \in \mathbb{Z}[X]$ et $\Phi_n \in \mathbb{Z}[X]$ par lemme 2.

* [$P' \wedge P = 1 \Rightarrow P$ sans facteur carré ds k corps

Dém : si $P = Q^2 \times R$ $\quad P' = 2QQ'R + Q^2R'$ donc $Q \mid P'$ or $Q \mid P$
↳ Q irréductible $\quad$ ↑ ici vrai car $p \nmid n$ d'où $P' \neq 0$.
d'où $Q \mid \mathrm{pgcd}(Q, Q') = 1$ d'où Q inversible et donc non irréductible.

Méthode permettant de calculer "rapidement" Φ_n – Merci Pierre

Proposition (Formule d'inversion)

Soit G un groupe abélien noté additivement, $g : \mathbb{N}^* \longrightarrow G$ une application et $f : \mathbb{N}^* \longrightarrow G$ l'application définie par $f(n) = \sum_{d|n} g(d)$. On a

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d).$$

Preuve :

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n}\left[\mu(d)\sum_{e|\frac{n}{d}} g(e)\right] = \sum_{d|n}\left[g(e)\sum_{d|\frac{n}{e}}\mu(d)\right] = g(n). \text{ car } \sum_{d|\frac{n}{e}} \mu(d) = 0 \text{ si } n/e > 1 \text{ i.e si } e < n. \quad \blacksquare$$

En notant $G = \mathbb{C}(X)^*$ le groupe multiplicatif des fractions rationnelles à coefficients complexes, $f, g : \mathbb{N}^* \to G$ les applications définies par $f(n) = X^n - 1$ et $g(n) = \Phi_n(X)$ on a $f(n) = \prod_{d|n} g(d)$ et la formule d'inversion de Möbius (version multiplicative) donne

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$$

Exemple : $\Phi_{28}(X) = \prod_{d|28} (X^d - 1)^{\mu(28/d)}$

$$= (X^{28}-1)^{\mu(1)}(X^{14}-1)^{\mu(2)}(X^7-1)^{\mu(4)}(X^4-1)^{\mu(7)}(X^2-1)^{\mu(14)}(X-1)^{\mu(28)}$$
$$= (X^{28}-1)^1(X^{14}-1)^{-1}(X^7-1)^0(X^4-1)^{-1}(X^2-1)^1(X-1)^0$$
$$= \frac{(X^{28}-1)(X^2-1)}{(X^{14}-1)(X^4-1)} = \frac{(X^{14}+1)}{(X^2+1)} = X^{12} - X^{10} + X^8 - X^6 + X^4 - X^2 + 1.$$

$\Phi_{18} = X^6 - X^3 + 1 \in \mathbb{F}_7[X]$
$= (X^2 + 7X + 1)(X^4 - \dots)$

$P \mid Q \quad PR = Q \quad R \in \mathbb{Q}[X]$
$S \mid P \quad QS = P \quad S \in \mathbb{Q}[X]$
$PSR = P$.
$P(1 - SR) = 0$. or $P \neq 0$
↳ $SR = 1$
↳ $\deg S = 0 \quad \deg R = 0$.

un polynôme cyclo dans $\mathbb{F}_q[X]$ n'est pas forcément irréductible
↑ ou à coeff dans $\mathbb{Z}$ = $\Phi_{18}(X)$.

✓ D'une manière générale on peut définir les polynômes cyclotomiques sur un corps k quelconque : on les note $\Phi_{n,k}$. Ici on étudie les polynômes cyclotomiques sur $\mathbb{Q}$. Il faut avoir conscience à l'oral que les polynômes cyclotomiques dépendent du corps où l'on a choisi de se placer.
✓ À quoi servent ces polynômes ? Les extensions cyclotomiques (un corps de rupture d'un polynôme cyclotomique) sont très utilisées dans la résolution de certaines équations diophantiennes.