Irréductibilité des polynômes cyclotomiques

Référence : Gozard Théorie de Galois p.68
Leçons : 102,120,121,123,141.

Définition

Pour $n \in \mathbb{N}^*$, on note $\mu_n := \left\{ e^{\frac{2ik\pi}{n}} \ / \ k \in \mathbb{Z} \right\}$ l'ensemble des racines n-ièmes de l'unité et

$$\mu_n^* := \left\{ e^{\frac{2ik\pi}{n}} \ / \ k \in [\![1, n-1]\!], \ \ k \wedge n = 1 \right\}$$

l'ensemble des racines n-ièmes primitives de l'unité c'est à dire celles qui engendrent μ_n. Le n-ième polynôme cyclotomique est le polynôme défini par

$$\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi).$$

Lemme 1

On a $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Preuve :

Il suffit de montrer que $\mu_n = \bigsqcup_{d|n} \mu_d^*$.

Si $d|n$, $\mu_d^* \subset \mu_d \subset \mu_n$.

Chaque racine n-ième de l'unité a un unique ordre (multiplicatif) qui est un diviseur de n d'après le théorème de Lagrange. Autrement dit, chaque élément de μ_n appartient à un et un seul des μ_d^*. ■

Lemme 2

Soient $P \in \mathbb{Z}[X]$ non nul unitaire, A, B éléments non nuls de $\mathbb{Q}[X]$ et A unitaire.
Alors $A, B \in \mathbb{Z}[X]$.

Preuve :

Déjà, B est forcément unitaire aussi.

Notons $A(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ où $a_i \in \mathbb{Q}$. Soit $a_i = \frac{p_i}{q_i}$ sa forme factorisée ($p_i \in \mathbb{Z}$ et $q_i \in \mathbb{N}^*$).

On pose $q = \text{ppcm}(q_0, \ldots, q_{n-1})$. Ainsi, $A(X) = X^n + \frac{1}{q} \sum_{i=0}^{n-1} z_i X^i$ et les $z_i \in \mathbb{Z}$.

Quitte à diviser $z_0, \ldots, z_{n-1}$ et q par $\text{pgcd}(z_0, \ldots, z_{n-1}, q)$, on peut supposer [1] $\text{pgcd}(z_0, \ldots, z_{n-1}, q) = 1$.
Posons $A_1 = qA$. Par construction, $A_1 \in \mathbb{Z}[X]$. De plus, A_1 est primitif par la remarque si dessus. De même, on peut contruire de la même manière un polynôme $B_1 \in \mathbb{Z}[X]$ primitif tq $B_1 = rB$. Le lemme de Gauss nous dit que $A_1 B_1$ est également primitif.

1. Ca ne change rien à notre problème car le pgcd est dans $\mathbb{Z}$ donc si on doit remultiplier par lui à la fin on garde notre résultat

Mais on a $qrP = A_1B_1$ donc $c(qrP) = qrc(P) = 1$ donc $qr = 1$ et comme q et r sont naturels $q = r = 1$.
Donc $A = A_1 \in \mathbb{Z}[X]$ et $B = B_1 \in \mathbb{Z}[X]$

■

Théorème

On a $\Phi_n \in \mathbb{Z}[X]$ et Φ_n irréductible dans $\mathbb{Q}[X]$. Alors il le sera dans $\mathbb{Z}[X]$ car primitif (car unitaire).

Preuve :

Etape 1 Par récurrence forte, montrons que $\Phi_n \in \mathbb{Z}[X]$.

- Pour $n = 1$, c'est vrai car $\Phi_1(X) = X - 1$.
- Supposons le résultat vrai jusqu'au rang $n-1$ et montrons le au rang n.
  Par hypothèse de récurrence, le polynôme $F = \prod_{\substack{d|n \\ d\neq n}} \Phi_d \in \mathbb{Z}[X]$ et $X^n - 1 = \Phi_n F$ par le **Lemme 1**.

  $\mathbb{Q}$ étant un corps, $X^n - 1$ et F sont des polynômes à coefficients dans $\mathbb{Q}$. Donc on peut faire la division euclidienne (avec unicité) de $X^n - 1$ par F :

$$X^n - 1 = FQ + R \quad \text{avec } \deg(R) < \deg(F) \text{ et } Q, R \in \mathbb{Q}[X]$$

  Comme on avait déjà $X^n - 1 = \Phi_n P_0$, par unicité, on a $R = 0$ et $Q = \Phi_n$ donc $\Phi_n \in \mathbb{Q}[X]$. Le **Lemme 2** permet de conclure.

Etape 2 Soit $\omega \in \mu_n^*$. Comme $\mathbb{Q}$ est un corps, on peut avoir un polynôme minimal pour ω sur $\mathbb{Q}$. Soit f ce polynôme qui est donc irréductible sur $\mathbb{Q}$.
Comme ω annule $X^n - 1$, $f|X^n - 1$ ie il existe $h \in \mathbb{Q}[X]$ tq [2] $X^n - 1 = f(X)h(X)$. Toutes les hypothèses sont bonnes pour appliquer le **Lemme 2** qui nous dit que f et h sont dans $\mathbb{Z}[X]$.

Etape 3 Soit $u \in \mathbb{C}$ une racine de f et p un nombre premier tel que $p \nmid n$, montrons que $f(u^p) = 0$.

- Comme $f|X^n - 1$, on a $u^n - 1 = 0$ donc $u \in \mu_n$ donc $u^p \in \mu_n$. Donc

$$0 = (u^p)^n - 1 = f(u^p)h(u^p)$$

- Supposons par l'absurde $f(u^p) \neq 0$. Alors $h(u^p) = 0$.
  Comme u annule f (choisi ainsi), et que f est irréductible sur $\mathbb{Q}$, f est aussi le polynôme minimal de u sur $\mathbb{Q}$. Donc finalement $f|h(X^p)$. Il existe $g \in \mathbb{Q}[X]$ tq $h(X^p) = f(X)g(X)$. On appelle le **Lemme 2** encore une fois qui nous dit que $g \in \mathbb{Z}[X]$.

- On se place maintenant dans $\mathbb{F}_p$ et on note $\bar{\cdot}$ les classes. Par le morphisme de Frobenius (question 2/c de Gourdon Algèbre p.91 si on veut détailler), on a

$$[\overline{h}(X)]^p = \overline{h(X^p)} = \overline{f}(X)\overline{g}(X)$$

  Soit $\theta \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{f}$. Alors $\theta|\overline{h}^p$ donc $\theta|\overline{h}$ dans $\mathbb{F}_p[X]$. Donc θ^2 divise $\overline{fh} = X^n - \overline{1}$.
  Par conséquent $X^n - \overline{1}$ possède une racine double dans une clôture algébrique de $\mathbb{F}_p$. Ceci est absurde [3] car $X^n - \overline{1}$ est premier [4] avec sa dérivée $\overline{n}X^{n-1}$.
  Donc l'hypothèse de départ était fausse et $f(u^p) = 0$

2. Si on a un doute sur pk h est dans $\mathbb{Q}$ on dit que h est dans $\mathbb{C}$ puis toujours pareil unicité de la division euclidienne dans $\mathbb{Q}$.
3. On trouve une autre preuve qui revient au même dans Gourdon algèbre p.91 question 2/d

Supposons $X^n - \overline{1} = \overline{\theta}^2\overline{S}$.

On dérive cette expression : $\overline{n}X^{n-1} = 2\overline{\theta\theta' S} + \overline{\theta}^2\overline{S'}$ et donc $\overline{\theta}\big|\overline{n}X^{n-1}$. Donc $\overline{\theta}\big|\overline{n}X^n$. Or $\overline{\theta}\big|(X^n - \overline{1})$ donc $\overline{\theta}\big|(\overline{n}X^n - \overline{n})$ et finalement par différence $\overline{\theta}\big|\overline{n}$.

Or $p \nmid n$ ie $\overline{n} \neq \overline{0}$ et donc $\overline{\theta}$ est constant. Cela est absurde car alors $\overline{\theta}$ serait inversible et non irréductible dans $\mathbb{F}_p[X]$.

4. C'est le théorème de Bezout car $\frac{1}{\overline{n}}X\overline{n}X^{n-1} - (X^n - \overline{1} = 1$

Etape 4 Soit ξ une racine n-ième primitive quelconque de l'unité. On sait qu'il existe $k \wedge n = 1$ tq $\xi = \omega^k$. Par élévations successives [5] de ω à des puissances de p où p premier ne divise par n, on montre que $f(\xi) = 0$.

Etape 5 Conclusion

On a donc montré que tous les éléments de μ_n^* sont racines de f donc de Φ_n. Donc $\deg(f) \geqslant \deg(\Phi_n) = \varphi_n$. Mais $f|\Phi_n$ et ils sont tous les deux unitaires donc $f = \Phi_n$ et finalement Φ_n est irréductible dans $\mathbb{Q}[X]$!

■

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 :

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

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

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

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

$$= (X^{28} - 1)^{\mu(1)} (X^{14} - 1)^{\mu(2)} (X^7 - 1)^{\mu(4)} (X^4 - 1)^{\mu(7)} (X^2 - 1)^{\mu(14)} (X - 1)^{\mu(28)}$$

$$= (X^{28} - 1)^1 (X^{14} - 1)^{-1} (X^7 - 1)^0 (X^4 - 1)^{-1} (X^2 - 1)^1 (X - 1)^0$$

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

Notes :

✓ **A l'oral**, 14'38 tout sauf le Lemme 1. Se garder le Lemme 2 à la fin pour aller plus ou moins vite dessus.

✓ Il faut savoir que Gozard ici contourne le problème de la factorialité de $\mathbb{Z}[X]$ en la démontrant partiellement.

5. Il serait plus propre de faire ici la récurrence du Gourdon (question 2/f).
$k = p_1 \cdots p_s$ avec p_i premiers. Par récurrence sur s, mq $f(\omega^k) = 0$.

— Pour $s = 1$, c'est par construction.
— Supposons le résultat vrai au rang $s - 1$ et montrons le au rang s.
Comme $k \wedge n = 1$, on a $(p_1 \cdots p_{s-1}) \wedge n = 1$ et par hypothèse de récurrence $f(\omega^{p_1 \cdots p_{s-1}}) = 0$. Or $p_s \wedge n = 1$ donc $f\left((\omega^{p_1 \cdots p_{s-1}})^{p_s}\right) = 0$ (c'est l'étape 3) d'où le résultat.

Si ça nous gêne, il vaut mieux prendre dans Perrin.
✓ On peut remarquer que $\deg(\Phi_n) = \varphi(n)$.
✓ On peut également remarquer que pour p premier,

$$\Phi_p = \left(X - \mathrm{e}^{\frac{2\mathrm{i}\pi}{p}}\right) \dots \left(X - \mathrm{e}^{\frac{2\mathrm{i}(p-1)\pi}{p}}\right) = \frac{X^p - 1}{X - 1} = 1 + X + \dots + X^{p-1}$$

(se retrouve avec la formule d'inversion) L'irréductibilité pour p premier peut se montrer plus rapidement avec Eisenstein (exo 4p58 Gourdon)
✓ 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.
✓ A 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.
✓ Autre version : uniquement p premier + dim d'un ev FGNAl1 p.190