Développement : Irréductibilité des polynômes cyclotomiques

Référence : Algèbre et Probabilité, GOURDON page 97-98
Leçon : 102, 125, 141 et 142.

Pour tout entier naturel non nul n, on note $U_n = \{e^{2ik\pi/n} \mid k \in \mathbb{Z}\} \subset \mathbb{C}$. On dit qu'un élément $x \in U_n$ est une racine primitive n-ième de l'unité si x engendre le groupe multiplicatif U_n. On note Π_n l'ensemble des racines primitives n-ièmes de l'unité, et on définit le **polynôme cyclotomique** d'indice n par :

$$\Phi_n = \prod_{\xi \in \Pi_n} (X - \xi).$$

Proposition :
Soit $n \in \mathbb{N}^*$. On a

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Anisi, pour tout $n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.

Démonstration. Soit $\omega = e^{2i\pi/n}$. Soit k, $0 \leq k \leq n-1$. Soit d l'ordre de ω^k dans U_n. On a $d|n$. Par ailleurs $(\omega^k)^d = 1$, donc $\omega^k \in U_d$, et ω^k étant d'ordre d, on a même $\omega^k \in \Pi_d$. Ainsi, $(X - \omega^k)$ divise Φ_d donc divise $\prod_{d|n} \Phi_d$. Les valeurs ω^k $(0 \leq k \leq n-1)$ étant distinctes, on en déduit que $X^n - 1 = \prod_{k=0}^{n-1}(X - \omega^k)$ divise $\prod_{d|n} \Phi_d$. Ces polynômes étant de plus unitaires et de même degré (car $\sum_{d|n} \deg(\Phi_d) = \sum_{d|n} \varphi(d) = n$), ils sont égaux.

Montrons maintenant par récurrence sur $n \in \mathbb{N}^*$ que $\Phi_n \in \mathbb{Z}[X]$. Pour $n = 1$, c'est vrai car $\Phi_1 = X - 1$. Supposons le résultat vrai jusqu'au rang $n-1$ et montrons-le au rang n. D'après l'hypothèse de récurrence, le polynôme $P = \prod_{d|n, d \neq n} \Phi_d \in \mathbb{Z}[X]$. Par ailleurs, on a $X^n - 1 = \Phi_n P$. Comme P est unitaire, on peut effectuer la division euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$:

$$(\exists Q, R \in \mathbb{Z}[X]), \quad X^n - 1 = PQ + R \text{ avec } \deg(R) < \deg(P).$$

Il y a unicité du couple (Q, R) dans $\mathbb{C}[X]$ donc dans $\mathbb{Z}[X]$, et comme $X^n - 1 = P\Phi_n$ on en déduit $R = 0$ et $\Phi_n = Q$. Donc $\Phi_n \in \mathbb{Z}[X]$, ce qui achève le raisonnement par récurrence. □

Théorème :
Pour tout $n \in \mathbb{N}^*$ Φ_n est irréductible dans $\mathbb{Q}[X]$.

Démonstration. ⋆ **Etape n°1 :** Montrer que l'on peut écrire $\Phi_n = F_1 F_2 \cdots F_r$ avec les $F_i \in \mathbb{Z}[X]$, unitaires et irréductibles dans $\mathbb{Q}[X]$ (on pourra utiliser le lemme de Gauss).

Soit $\Phi_n = G_1 \cdots G_r$ la décomposition de Φ_n en facteurs irréductibles unitaires de $\mathbb{Q}[X]$. Pour tout i, il existe $\alpha_i \in \mathbb{N}^*$ tel que $\alpha_i G_i \in \mathbb{Z}[X]$. On a $\alpha_1 \cdots \alpha_r \Phi_n = (\alpha_1 G_1) \cdots (\alpha_r G_r)$. Utilisons le lemme de Gauss : comme $c(\Phi_n) = 1$ (car Φ_n est unitaire), on a :

$$\alpha_1 \cdots \alpha_r = c(\alpha_1 \cdots \alpha_r \Phi_n) = \prod_{i=1}^{r} c(\alpha_i G_i).$$

Pour tout i, le polynôme $F_i = \alpha_i G_i / c(\alpha_i G_i)$ est dans $\mathbb{Z}[X]$ et d'après (*), on a $\Phi_n = F_1 \cdots F_r$. Pour tout i, $F_i \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$ et est forcément unitaire puisque Φ_n est unitaire.

⋆ **Etape n°2 :** Soit ξ une racine de F_1 dans $\mathbb{C}$. Soit p un nombre premier tel que $p \nmid n$. Montrer qu'il existe $i \in \{1, \dots, r\}$ tel que $F_i(\xi^p) = 0$.

L'élément ξ est racine de F_1 donc de Φ_n, donc $\xi \in \Pi_n$. Or p est premier et $p \nmid n$, donc $p \wedge n = 1$, et donc $\xi^p \in \Pi_n$, d'où ξ^p est racine de Φ_n. Il existe donc i tel que $F_i(\xi^p) = 0$.

⋆ **Etape n°3 :** Pour tout $F = \sum_{k=0}^m a_k X^k \in \mathbb{Z}[X]$, on pose $\overline{F} = \sum_{k=0}^m \overline{a_k} X^k \in \mathbb{Z}/p\mathbb{Z}[X]$. Montrer que pour tout $F \in \mathbb{Z}[X]$, $\overline{F}(X^p) = (\overline{F}(X))^p$.

On montre cette relation par récurrence sur $m = \deg(F)$. Pour $m = 0$, c'est évident. Supposons le résultat vrai jusqu'au rang $m-1$ et montrons-le au rang m. Écrivons $F = \sum_{k=0}^m a_k X^k = G + a_m X^m$. D'après l'hypothèse de récurrence, on a $\overline{G}(X)^p = \overline{G}(X^p)$. Or

$$\overline{F}^p = (\overline{G} + \overline{a_m} X^m)^p = \overline{G}^p + \overline{a_m}^p X^{mp} + \sum_{k=1}^{p-1} C_p^k \overline{G}^k \overline{a_m}^{p-k} X^{(p-k)m}$$

et comme $\overline{a_m}^p = \overline{a_m}$ et que pour $1 \leq k \leq p-1$, $p | C_p^k$, on en déduit

$$\overline{F}(X)^p = \overline{G}(X^p) + \overline{a_m} X^{mp} = \overline{G}(X^p) + \overline{a_m}(X^p)^m = \overline{F}(X^p).$$

⋆ **Etape n°4 :** Montrer que dans $\mathbb{Z}/p\mathbb{Z}[X]$, Φ_n n'est divisible par le carré d'aucun polynôme non constant.

Supposons $\overline{\Phi_n} = \overline{Q}^2 \overline{P}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Si $R = \prod_{d|n, d \neq n} \Phi_d \in \mathbb{Z}[X]$, on a $X^n - 1 = \Phi_n R$ d'après 1/b), et donc $X^n - \overline{1} = \overline{\Phi_n R} = \overline{Q}^2 \overline{S}$ (avec $S = PR$), d'où par dérivation

$$\overline{n} X^{n-1} = 2\overline{Q Q'} \overline{S} + \overline{Q}^2 \overline{S'} \quad \text{donc} \quad \overline{Q} \mid \overline{n} X^{n-1}.$$

Donc $\overline{Q} \mid \overline{n} X^n$. Or $\overline{Q} \mid (X^n - \overline{1})$ donc $\overline{Q}$ divise la différence, c'est-à-dire $\overline{Q} \mid \overline{n}$. Or $p \nmid n$ donc $\overline{n} \neq 0$, et donc $\overline{Q}$ est constant.

⋆ **Etape n°5 :** Montrer que $i = 1$, c'est-à-dire que $F_1(\xi^p) = 0$.

On a $F_1(X)$ et $F_i(X^p)$ admettent ξ comme racine donc ne sont pas premier entre eux dans $\mathbb{Q}[X]$ (l'égalité de Bézout $U(X)F_1(X) + V(X)F_i(X^p) = 1$ avec $U, V \in \mathbb{Q}[X]$ appliquée à $X = \xi$ mène à une contradiction).

De plus F_1 est le polynôme minimal de ξ sur $\mathbb{Q}[X]$, on a déduit que $F_1(X) \mid F_i(X^p)$ dans $\mathbb{Q}[X]$.

Comme F_1 est unitaire n en déduit que $F_1(X) \mid F_i(X^p)$ dans $\mathbb{Z}[X]$. Ainsi $\overline{F_1}(X) \mid \overline{F_i}(X^p) = \overline{F_i}(X)^p$.

Soit $\overline{P}$ un facteur irréductible de $\overline{F_1}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. On a $\overline{P} \mid \overline{F_i}(X)^p$ donc $\overline{P} \mid \overline{F_i}(X)$. Par conséquent, si $i \neq 1$, on voit que $\overline{P}^2 \mid \overline{\Phi_n} = \overline{F_1} \cdots \overline{F_r}$, ce qui est impossible d'après la question précédente. On a donc $i = 1$.

⋆ **Etape n°6 :** Montrer que pour tout entier k premier avec n, $F_1(\xi^k) = 0$. Conclure.

Soit k premier avec n. Écrivons $k = p_1 p_2 \cdots p_s$, les p_i étant des nombres premiers. Nous allons prouver par récurrence sur s que $F_1(\xi^k) = 0$. Pour $s = 1$, c'est le résultat de la question précédente. Supposons le résultat vrai au rang $s-1$ et montrons-le au rang s. Comme $k \wedge n = 1$, on a $p_s \wedge n = 1$, donc d'après l'hypothèse de récurrence $F_1(\xi^{p_1 \cdots p_{s-1}}) = 0$. Or $p_s \wedge n = 1$ donc $F_1((\xi^{p_1 \cdots p_{s-1}})^{p_s}) = F_1(\xi^k) = 0$, ce qui achève le raisonnement par récurrence.

Pour tout nombre premier k premier avec n, on a donc $F_1(\xi^k) = 0$. Or $\xi \in \Pi_n$ donc $\Pi_n = \{\xi^k \mid k \wedge n = 1\}$. Tous les éléments de Π_n sont donc des racines de F_1, ce qui prouve que $\Phi_n = F_1$, donc Φ_n est irréductible dans $\mathbb{Q}[X]$.

□

Application : [ORTIZ] p.169
Soit $\mathbb{K}$ une extension finie de $\mathbb{Q}$. Alors il n'y a qu'un nombre fini de racines de l'unité dans $\mathbb{K}$.

Démonstration. Toute racine de l'unité étant aussi une racine primitive de l'unité, il suffit de montrer qu'il n'y a qu'un nombre finide racines primitives de l'unité dans $\mathbb{K}$. Soit $N = [\mathbb{K} : \mathbb{Q}]$. Si $u \in \mathbb{K}$ est une racine primitive n-ème de 1 dans $\mathbb{K}$ alors, comme $\mathbb{Q}(u) \subseteq \mathbb{K}$, par multiplicativité, $[\mathbb{Q}(u) : \mathbb{Q}]$ divise N et en particulier, $\varphi(n) \leqslant N$.
Pour conclure, il suffit de montrer que $X = \{n \geqslant 2; \varphi(n) \leqslant N\}$ est fini. Soit p un facteur premier de $n \in X$. Comme $p - 1 \mid \varphi(n)$, on a $p \leqslant N + 1$ donc l'ensemble $\mathcal{P}$ des facteurs premiers des éléments de X est fini. D'autre part, si $n \geqslant 2$ alors $\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right)$. Par suite, si $n \in X$, on a

$$n \prod_{\substack{p \mid n \\ p \in \mathcal{P}}} \left(1 - \frac{1}{p}\right) \leqslant \varphi(n) \leqslant N,$$

ce qui prouve que X est bien un ensemble majoré et donc fini. □