Étude des polynômes cyclotomiques

Proposition 1. *Pour $n \in \mathbb{N}^\star$, Φ_n est dans $\mathbb{Z}[X]$.*

Démonstration.

On raisonne par récurrence sur n.
Le résultat étant clair pour $\Phi_1(X) = X - 1$, on suppose le résultat vrai pour un diviseur d de $n \geqslant 2$. On pose :

$$F(X) = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(X)$$

F est un polynôme unitaire de $\mathbb{Z}[X]$. On effectue alors la division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{Z}[X]$:

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

Or, on sait que $X^n - 1 = F(X)\Phi_n(X)$ est dans $\mathbb{C}$[X], donc $F(X)(\Phi_n(X) - P(X)) = R(X)$. Par comparaison des degrés, on a donc $\Phi_n(X) = P(X) \in \mathbb{Z}[X]$.

□

Proposition 2. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Z}[X]$.*

Démonstration.

Soit $\zeta \in \mathbb{K}$ une racine primitive n-ième de l'unité. Soit p un nombre premier ne divisant pas n. On sait que $\zeta^p \in \mu_n^\star$. Posons f (resp. g) le polynôme minimal de ζ (resp. ζ^p).

Étape 1 : Montrons que f et g sont dans $\mathbb{Z}[X]$.

L'anneau $\mathbb{Z}[X]$ est factoriel, on peut donc écrire une décomposition de Φ_n en produit de facteurs irréductibles :

$$\Phi_n(X) = \prod_{i=1}^{r} f_i^{\alpha_i}$$

Comme Φ_n est unitaire, on peut supposer que les f_i le sont également. Ils sont alors irréductibles sur $\mathbb{Q}$. Or, ζ est racine de l'un des f_i, qui est donc égal à f par irréductibilité. Ainsi, $f = f_i$ est dans $\mathbb{Z}[X]$. On a de plus $f \mid \Phi_n$, et de même on a $g \in \mathbb{Z}[X]$ et $g \mid \Phi_n$.

Étape 2 : Montrons que $f = g$.

On suppose par l'absurde que $f \neq g$. Comme f et g sont irréductibles et distincts, on a $fg \mid \Phi_n$ dans $\mathbb{Z}[X]$. De plus, comme $g(\zeta^p) = 0$, ζ est racine du polynôme $g(X^p)$, donc $f(X)$ divise $g(X^p)$ dans $\mathbb{Q}[X]$, et donc dans $\mathbb{Z}[X]$ car $f(X)$ et $g(X^p)$ sont unitaires. Projetons l'égalité $g(X^p) = f(X)h(X)$ dans $\mathbb{F}_p$. On pose :

$$g(X) = \sum_{k=0}^{r} a_k X^k \quad \text{avec} \quad \forall\, k \in [\![0, r]\!],\ a_k \in \mathbb{Z}$$

Grâce au morphisme de Frobenius, on obtient :

$$\overline{g}(X^p) = \sum_{k=0}^{r} \overline{a_k} X^{kp} = \left(\sum_{k=0}^{r} \overline{a_k} X^k \right)^p = \overline{g}(X)^p = \overline{f}(X)\overline{h}(X)$$

Soit $\varphi(X)$ un facteur irréductible non constant de $\overline{f}(X)$ dans $\mathbb{F}_p[X]$. Par le lemme d'Euclide, φ divise $\overline{g}$. Comme fg divise Φ_n dans $\mathbb{Z}[X]$, fg divise $X^n - 1$ dans $\mathbb{Z}[X]$, donc φ^2 divise $X^n - 1$ dans $\mathbb{F}_p[X]$. Or, φ^2 admet une racine double dans $\mathbb{F}_p$, donc $X^n - 1$ aussi. Cette dernière proposition est fausse, donc $f = g$.

Étape 3 : Montrons que Φ_n est irréductible sur $\mathbb{Z}[X]$.

Soit $\zeta' \in \mu_n^\star$. On a $\zeta' = \zeta^m$ avec m un entier premier avec n, que l'on décompose comme $m = \prod_{i=1}^{r} p_i^{\alpha_i}$. Par itération des étapes précédentes, on sait que ζ et ζ' ont même polynôme minimal sur $\mathbb{Q}$. On a donc $f(\zeta') = 0$, ainsi f admet toutes les racines primitives n-ièmes de l'unité comme racine. Alors $\deg f \geqslant \varphi(n) = \deg \Phi_n$, mais comme $f \mid \Phi_n$, on a $f = \Phi_n$. Il en résulte que Φ_n est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Z}$ puisque Φ_n est unitaire. $\square$

Conclusion. Les polynômes cyclotomiques sont des polynômes sur $\mathbb{Z}$ qui sont irréductibles sur $\mathbb{Q}$ et sur $\mathbb{Z}$. $\triangleleft$

Références

[Per] Daniel Perrin. *Cours d'Algèbre.* Ellipses