Développement 20. L'irréductibilité des polynômes cyclotomiques sur l'anneau des entiers

Théorème 1. Le n-ième polynôme cyclotomique $\Phi_n \in \mathbf{Z}[X]$ sur $\mathbf{Q}$ est irréductible sur les anneaux $\mathbf{Q}$ et $\mathbf{Z}$.

On rappel le lemme de Gauss sur les contenus, ici précisés dans l'anneau des polynômes à coefficients entiers. Pour un polynôme $P \coloneqq a_n X^n + \cdots + a_0 \in \mathbf{Z}[X]$, on définit son *contenu*, noté $\operatorname{cont}(P)$, comme le PGCD des entiers a_i.

Lemme 2. Pour deux polynômes $P, Q \in \mathbf{Z}[X]$, on a $\operatorname{cont}(PQ) = \operatorname{cont}(P)\operatorname{cont}(Q)$.

Preuve Soit K un corps de décomposition du polynôme Φ_n sur $\mathbf{Q}$. Soit $\zeta \in K$ une racine n-ième primitive de l'unité. Soit p un nombre premier ne divisant pas n. Comme les entiers p et n sont alors premiers entre eux, l'élément ζ^p est aussi une racine n-ième primitive de l'unité.

On va montrer que le polynôme Φ_n est le polynôme minimal de l'élément ζ sur $\mathbf{Q}$ ce qui montrera qu'il est irréductible sur $\mathbf{Q}$. L'irréductibilité sur $\mathbf{Z}$ en découlera alors puisque le corps $\mathbf{Q}$ est le corps de fractions de l'anneau $\mathbf{Z}$.

Soient $f, g \in \mathbf{Q}[X]$ les polynômes minimaux des racines ζ et ζ^p sur $\mathbf{Q}$. Montrons que $f \in \mathbf{Z}[X]$. Comme l'anneau $\mathbf{Z}[X]$ est factoriel, on écrit

$$\Phi_n = f_1^{\alpha_1} \cdots f_r^{\alpha_r}$$

pour des polynômes irréductibles $f_i \in \mathbf{Z}[X]$ et des entiers $\alpha_i \geqslant 1$. Comme le polynôme Φ_n est unitaire, on peut supposer que les polynômes f_i le sont aussi. Ainsi ces derniers sont irréductibles sur $\mathbf{Q}$. Mais l'élément ζ est une racine du polynôme Φ_n et donc d'un des polynômes f_i, donc la minimalité implique qu'on peut écrire $f = f_{i_0}$ pour un certain indice $i \in [\![1, r]\!]$ ce qui donne $f \in \mathbf{Z}[X]$. Avec le premier paragraphe, on obtient également $g \in \mathbf{Z}[X]$. Par ailleurs, cela montre que les polynômes f et g divisent le polynôme Φ_n dans $\mathbf{Z}[X]$.

Montrons que $f = g$. Raisonnons par l'absurde et supposons $f \neq g$. Comme l'anneau $\mathbf{Z}[X]$ est factoriel, il vérifie le lemme de Gauss et, comme $f \neq g$, ce lemme montre $fg \mid \Phi_n$ dans $\mathbf{Z}[X]$. Comme l'élément ζ est une racine du polynôme $g(X^p)$, on peut écrire $f \mid g(X^p)$ dans $\mathbf{Q}[X]$. Soit $h \in \mathbf{Q}[X]$ un polynôme tel que $g(X^p) = fh$. Montrons que $h \in \mathbf{Z}[X]$. On sait qu'il existe deux entiers $\alpha \in \mathbf{Z}$ et $\beta \in \mathbf{N}^*$ et un polynôme $\tilde{h} \in \mathbf{Z}[X]$ tels que $h = \frac{a}{b}\tilde{h}$. Comme les polynômes f, g et h sont unitaires avec $\beta g(X^p) = \alpha f h$, le lemme de Gauss pour les contenus donne $\alpha = \beta$. Finalement, on a $h \in \mathbf{Z}[X]$.

Projetons alors l'égalité $g(X^p) = fh$ dans $\mathbf{F}_p[X]$. Pour un polynôme $P \in \mathbf{Z}[X]$, on note $\overline{P} \in \mathbf{F}_p[X]$ sa projection. Notons $g = a_r X^r + \cdots + a_0$ avec $a_i \in \mathbf{Z}$. Alors

$$g(X^p) = a_r X^{rp} + \cdots + a_0$$

et, comme $\overline{a_i} = \overline{a_i}^p$ pour $i \in [\![1, r]\!]$, le morphisme de Frobenius assure que

$$\overline{g}(X^p) = \overline{a_r} X^{rp} + \cdots + \overline{a}_0 = (\overline{a_r} X^r + \cdots + \overline{a_0})^p = \overline{g}(X)^p.$$

Soit $\overline{\varphi} \in \mathbf{F}_p[X]$ un facteur irréductible du polynôme $\overline{f}$. Comme $\overline{g}(X)^p = \overline{f} \times \overline{h}$, on obtient alors $\overline{\varphi} \mid \overline{g}(X)^p$ dans $\mathbf{F}_p[X]$ et, comme le polynôme $\overline{\varphi}$ est irréductible, le lemme d'Euclide fournit donc $\overline{\varphi} \mid \overline{g}$. Comme $fg \mid \Phi_n$ dans $\mathbf{Z}[X]$, on a $\overline{f}\overline{g} \mid \overline{\Phi_n}$ dans $\mathbf{F}_p[X]$, donc $\overline{\varphi}^2 \mid \overline{\Phi_n}$. Mais on sait que, comme $p \nmid n$, le polynôme $\overline{\Phi_n} = \Phi_{n, \mathbf{F}_p}$ n'a que des racines simples ce qui est impossible. D'où $f = g$.

Soit $\zeta' \in K$ une racine primitive n-ième de l'unité. Comme l'élément ζ génère le groupe $\mu_n(K)$ des racines primitives n-ième de l'unité, il existe un entier $m \in \mathbf{N}$ tel que $\zeta' = \zeta^m$. On écrit l'entier m en une produit $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ de nombres premiers p_i. Comme la racine n-ième ζ' de l'unité est primitive, on a $m \wedge n = 1$, donc aucun nombre premier p_i ne divise n. On peut alors appliquer récursivement le paragraphe précédent pour montrer que les racines ζ et ζ' ont le même polynôme minimal sur $\mathbf{Q}$. L'élément ζ' est donc une racine du polynôme f. Ceci étant vrai pour toute racine primitive n-ième de l'unité, on obtient $\deg f \geqslant \deg \Phi_n$. Comme $f \mid \Phi_n$, on en conclut l'égalité $\Phi_n = f$.

Finalement, le polynôme Φ_n est irréductible sur $\mathbf{Q}$ et, comme il est primitif, il l'est aussi sur $\mathbf{Z}$. ◁

Corollaire 3. Soient K un corps de caractéristique nulle et $\zeta \in K$ une racine n-ième de l'unité. Alors

$$[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n).$$

Preuve Le polynôme minimal de l'élément ζ sur $\mathbf{Q}$ est le polynôme cyclotomique Φ_n puisqu'il l'annule et qu'il est irréductible sur $\mathbf{Q}$. Par conséquent, l'extension $\mathbf{Q}(\zeta)/\mathbf{Q}$ est de degré $\deg \Phi_n$. Comme $\varphi(n) = \deg \Phi_n$, cela donne le corollaire. ◁

[1] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.