Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$

Leçons : 102, *120, 125*, 141, *144*

Définition 1

Soit k un corps, K_n le corps de décomposition de $P_n = X^n - 1$. On note $\mu_n(K_n)$ le groupe des racines de P_n dans k_n et $\mu_n(K_n)^*$ l'ensemble de ses générateurs. Le n-ième polynôme cyclotomique est

$$\phi_{n,k} = \prod_{\zeta \in \mu_n(K_n)^*} (X - \zeta) \in K_n[X].$$

On note $\phi_n = \phi_{n,\mathbb{Q}}$

On rappelle que $\phi_{n,k} \in k[X]$, que $X^n - 1 = \prod_{d|n} \phi_{d,k}(X)$ et que $\phi_{n,k}$ est de degré $\phi(n)$.

Proposition 2

On a $\phi_n \in \mathbb{Z}[X]$ et si k est un corps, $\sigma : \mathbb{Z} \to k$ le morphisme canonique, $\phi_{n,k} = \sigma(\phi_n)$.

Théorème 3

Le polynôme ϕ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$.

Démonstration. Soit K corps de décomposition de ϕ_n sur $\mathbb{Q}$, $\zeta \in K$ une racine primitive n-ième de l'unité. Soit p premier ne divisant pas n.

Étape 1 : ζ^p est aussi une racine primitive n-ième de l'unité. En effet, si $up + vn = 1$ est une relation de Bézout entre p et n, on a $\zeta = (\zeta^p)^u(\zeta^n)^v = (\zeta^p)^u$.

Étape 2 : Soient f et g les polynômes minimaux respectifs de ζ et ζ^p sur $\mathbb{Q}$. Ecrivons la décomposition en facteurs irréductibles de ϕ_n sur $\mathbb{Z}$: $\phi_n = \prod_{i=1}^{r} f_i^{\alpha_i}$. Comme ϕ_n est unitaire, il en va de même des f_i quitte à multiplier par -1. De plus, ζ étant racine de ϕ_n, ζ est racine d'un des f_i de sorte que $f_i = f$ par minimalité de f. En particulier $f \in \mathbb{Z}[X]$ et est unitaire et il en va de même pour g.

Étape 3 : Montrons par l'absurde que $f = g$. Si ce n'est pas le cas, f et g sont premiers entre eux donc par le lemme de Gauss, fg divise ϕ_n dans $\mathbb{Z}[X]$. De plus, $g(\zeta^p) = 0$ donc $f(X)$ divise $g(X^p)$ dans $\mathbb{Q}[X]$: $g(X^p) = f(X)h(X), h \in \mathbb{Q}[X]$. En écrivant $h = \frac{a}{b}h_1$ où h_1 polynôme entier primitif, on voit en comparant le contenu de part et d'autre de l'égalité que $h \in \mathbb{Z}[X]$.

Réduisons maintenant modulo p : si $g(X) = a_sX^s + \cdots + a_0$, alors si $\overline{g}$ est la réduction modulo p de g, on a

$$\overline{g}(X^p) = \overline{a_s}X^{ps} + \cdots + \overline{a_0} = \overline{a_s}^p X^{ps} + \cdots + \overline{a_0}^p = (\overline{g}(X))^p$$

par linéarité de l'extension du morphisme de Frobenius à $\mathbb{F}_p[X]$.

Soit φ un facteur irréductible de $\overline{f}$ dans $\mathbb{F}_p[X]$. Alors comme $\overline{g}(X)^p = \overline{f}(X)\overline{h}(X)$, on a par le lemme de Gauss, $\varphi | \overline{g}(X)$. Comme $\overline{f}(X)\overline{g}(X)$ divise $\overline{\phi_n}$, $\overline{\phi_n}$ a un facteur double dans $\mathbb{F}_p[X]$. Mais selon la proposition préliminaire, $\overline{\phi_n} = \phi_{n,\mathbb{F}_q}$ qui n'a pas de racine multiple dans son corps de décomposition donc pas de facteur double. Ayant abouti à une contradiction, on conclut que $f = g$.

Étape 4 : conclusion. Soit ζ' une racine primitive n-ième de l'unité. De même que dans l'étape 1, on a $\zeta' = \zeta^m$ où m est premier avec n. Ainsi, si $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ est la décomposition de m

en facteurs premiers, aucun des p_i ne divise n. Par une récurrence immédiate s'appuyant sur le résultat de l'étape 3, on obtient que le polynôme minimal de ζ' sur $\mathbb{Q}$ est f. En particulier, f annule toutes les racines primitives n-ièmes de l'unité donc, puisque f est unitaire entier et divise ϕ_n, $f = \phi_n$. $\square$

Il est intéressant de prolonger l'étude dans les corps finis, bien que cela dépasse le cadre du développement proprement dit.

Proposition 4

Soit $k = \mathbb{F}_q[X]$, n un entier premier avec q et r l'ordre de $[q]$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Alors $\phi_{n,k}$ est un produit de facteurs irréductibles simples, tous de degré r.

Démonstration. Le fait que $\phi_{n,k}$ est à facteurs simples a déjà été établi dans la démonstration du théorème.

Soit P un facteur irréductible de ϕ_n, s son degré. Notons $K = k[X]/(P)$ un corps de rupture de P. Celui-ci est de cardinal q^s donc $\forall x \in K, x^{q^s-1} = 1$. De plus, il contient une racine ζ de P, donc de $\phi_{n,k} = \phi_{n,K}$. Donc ζ est une racine primitive n-ième de l'unité de K, de sorte que $n \mid q^s - 1$ puisque n est l'ordre de ζ dans K^*. D'où $q^s \equiv 1[n]$ et comme r est l'ordre multiplicatif de $[q]$, r divise s.

Par ailleurs, $n \mid q^r - 1$ par définition de r donc $\zeta^{q^r} = \zeta$: ζ appartient au sous-corps L de K constitué des racines de $X^{q^r} - X$ dans K (cf construction des corps finis). Comme ζ est un générateur du groupe des racines n-ièmes de l'unité dans un corps de décomposition K_n de $X^n - 1$ et $K \subset K_n$, ζ engendre K^*, d'où $K = k[\zeta]$. De même, $L = k[\zeta]$ donc $K = L$. En particulier, $\mathrm{Card}(K) = q^s \leqslant q^r$ donc $s \leqslant r$, et finalement $s = r$. $\square$

Corollaire 5

Le polynôme $\phi_{n,\mathbb{F}_q}$ est irréductible si et seulement si q engendre $(\mathbb{Z}/n\mathbb{Z})^*$.

Remarque.
- L'exemple de $\phi_7 = 1 + X + \cdots + X^6$ montre la complexité de la situation sur les corps finis. Modulo 2, $\phi_7 = (1 + X + X^3)(1 + X^2 + X^3)$ n'est pas irréductible.
- Une première application est la description du groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ pour ζ racine primitive n-ième de l'unité. Une conséquence immédiate du théorème est que ϕ_n est le polynôme minimal de ζ et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.
  Soit le morphisme de groupes $j : \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\ [m]_n & \longmapsto & \sigma_m : \zeta \mapsto \zeta^m \end{array}$. Il est injectif car si $j([m]) = \mathrm{id}$, on a $\zeta^m = \zeta$ donc $\zeta^{m-1} = 1$ et comme ζ est primitive, $m \equiv 1[n]$. De plus, les racines de ϕ_n dans $\mathbb{Q}(\zeta) = \mathbb{Q}(\mathbb{U}_n)$ sont les ζ^k pour k premier avec n et tout $\mathbb{Q}$-automorphisme envoie une racine du polynôme minimal ϕ_n de ζ sur une autre, ce qui prouve la surjectivité. Ainsi $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.
- Pour la culture, une (lointaine) application de l'irréductibilité de ϕ_n est le théorème de la progression arithmétique de Dirichlet, et plus généralement le théorème de densité de Chebotarev qui s'appuie sur la structure du groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Références :

- Daniel Perrin (1996). *Cours d'algèbre*. Ellipses, p. 79.
- Michel Demazure (2008). *Cours d'algèbre*. Cassini, p. 206.