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

Référence : D. Perrin, *Cours d'Algèbre*, Ellipses, 1996.

Leçons concernées : 102, 122, 141, 144.

Théorème 1. *Pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.*

Démonstration. Étape 1 : soit $\zeta \in \mathbb{C}$ une racine primitive n-ème de l'unité, donc racine de Φ_n. Si p est premier et ne divise pas n, alors ζ^p est aussi une racine primitive n-ème de l'unité car $n \wedge p = 1$. Soit f, g les polynômes minimaux de ζ, ζ^p sur $\mathbb{Q}$. On décompose

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

en produit d'irréductibles sur $\mathbb{Z}[X]$, unitaires puisque Φ_n l'est. Alors ζ est racine de l'un des f_i, irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$, ainsi f_i est le polynôme minimal de ζ sur $\mathbb{Q}$, et $f = f_i$. De même il existe j tel que $g = f_j$.

Étape 2 : montrons que $f = g$: supposons par l'absurde que ce n'est pas le cas, alors puisque f et g sont irréductibles, fg divise Φ_n. D'autre part, $g(\zeta^p) = 0$ donc ζ est racine de $g(X^p)$, ainsi, $f(X) \mid g(X^p)$ dans $\mathbb{Q}[X]$: il existe $h \in \mathbb{Q}[X]$ tel que

$$g(X^p) = f(X)h(X),$$

mais si on écrit $h = \frac{a}{b}h'$ avec $h' \in \mathbb{Z}[X]$ et $c(h') = 1$ (si $h(X) = \sum_i \frac{a_i}{b_i} X^i$, on prend $b := \mathrm{ppcm}(b_i)$ de sorte que $h(X) = \frac{1}{b}\sum_i a_i' X^i$, et on pose $a := \mathrm{pgcd}(a_i)$), on a

$$bg(X^p) = af(X)h'(X)$$

et en passant au contenu, $b = a$ puisque f et g sont unitaires, ainsi $f(X) \mid g(X^p)$ dans $\mathbb{Z}[X]$. Or par le morphisme de Frobenius, dans $\mathbb{F}_p[X]$, si $g = a_r X^r + \cdots + a_0$

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

Soit maintenant φ un facteur irréductible de $\overline{f}$ sur $\mathbb{F}_p$, alors avec

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

dans $\mathbb{F}_p[X]$, φ divise $\overline{g}$ par le lemme d'Euclide. Ainsi, φ^2 divise $\overline{\Phi_n} = \Phi_{n,\mathbb{F}_p}$, qui aura donc une racine multiple dans son corps de décomposition, ce qui est impossible puisque $n \wedge p = 1$.

Étape 3 : soit maintenant ζ' une racine primitive n-ème de l'unité. Alors $\zeta' = \zeta^m$ où $m = p_1^{\beta_1} \cdots p_l^{\beta_l}$ avec $p_i \nmid n$. On a alors avec le paragraphe précédent et une récurrence immédiate que ζ' et ζ ont même polynôme minimal. Ainsi, $f(\zeta') = 0$, de sorte que toutes les racines primitives n-ème de l'unité annulent f, et donc $\deg(f) \geqslant \varphi(n)$, mais puisque $f \mid \Phi_n$, $f = \Phi_n$ et donc Φ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$.

□