38 Irréductibilité de Φ_n

ref : Perrin

THÉORÈME 38.1 *Le polynôme Φ_n est irréductible sur $\mathbb{Q}$.*

PREUVE. L'idée est de montrer que Φ_n est le polynôme minimal de ζ pour $\zeta \in \mu_n^*$ quelconque. Un polynôme minimal est toujours irréductible presque par définition et on a ce polynôme miminal divise Φ_n. Pour montrer l'autre divisibilité, la proposition clé est la suivante :

PROPOSITION 38.2 *Soit $\zeta \in \mu_n^*$ et p premier ne divisant pas n. On note f et g les polynômes minimaux de ζ et ζ^p sur $\mathbb{Q}$. Alors f et g sont dans $\mathbb{Z}[X]$ et $f = g$.*

PREUVE. On a $\zeta^n = (\zeta^p)^n = 1$ donc f et g divisent $X^n - 1$. Mais comme $\mathbb{Z}[X]$ est factoriel (Gauss), on peut décomposer ce dernier en produit de polynômes irréductibles sur $\mathbb{Z}[X]$ et unitaire :

$$X^n - 1 = P_1 \times \cdots \times P_r$$

Chaque P_i est unitaire et irréductible sur $\mathbb{Z}$ donc par Gauss, P_i est irréductible sur $\mathbb{Q}$, et par unicité, la décomposition ci-dessus est la décomposition en produits d'irréductibles dans $\mathbb{Q}[X]$. Ainsi, f et g figurent parmi les P_i et sont donc dans $\mathbb{Z}[X]$.

Si f et g étaient distincts, on aurait fg divise $X^n - 1$ puisque f et g sont premiers entre eux (irréductibles distincts). Soit $h = g(X^p)$, on a $h(\zeta) = 0$ donc f divise h dans $\mathbb{Q}[X]$, mais aussi dans $\mathbb{Z}[X]$ car f est unitaire. En réduisant modulo p, on trouve $\overline{h} = (\overline{g}(X))^p$ d'après le morphisme de Frobenius. Donc tout facteur irréductible φ de $\overline{f}$ dans $\mathbb{F}_p[X]$ (attention $\overline{f}$ n'est pas irréductible dans $\mathbb{F}_p[X]$ a priori), apparait dans $\overline{h}$ donc dans $\overline{g}$, donc φ^2 divise $X^n - \overline{1}$. Mais $X^n - \overline{1}$ est premier avec sa dérivée $\overline{n}X^{n-1} - \overline{1}$ puisque $\overline{n} \neq 0$ dans $\mathbb{F}_p$, donc n'admet pas de facteur carré. C'est contradictoire, donc $f = g$. □

A partir de la proposition, on remarque que si f est le polynôme minimal de ζ, ζ^p est aussi racine de f, et par récurrence immédiate, $\zeta^{p_1^{\alpha_1} \cdots p_m^{\alpha_m}}$ avec $p_i \not| n$ est racine de f. Autrement dit, f contient toutes les racines primitives n-ièmes de l'unité (qui sont les ζ^m avec $m \wedge n = 1$), donc $\deg f \geq \deg \Phi_n$, puis $f = \Phi_n$. □

Remarque : comme Φ_n est à coefficients entiers et unitaire, il est aussi irréductible sur $\mathbb{Z}$.

Rappel : Si $n \geq 1$ et k est un corps de caractéristique ne divisant pas n, le polynôme $P_n(X) = X^n - 1$ est séparable : ses racines dans un corps de décomposition K_n de k sont simples. En effet, $P_n' = nX^{n-1}$ donc $P_n \wedge P_n' = 1$. L'ensemble $\mu_n(K_n)$ des racines de P_n est un sous-groupe de K_n^* donc est cyclique. Il est d'ordre n car les racines de $X^n - 1$ sont simples. Ses générateurs forment une partie à $\varphi(n)$ éléments appelés racines *primitives* n-ièmes de l'unité. On définit alors

$$\Phi_{n,k} = \prod_{\zeta \in \mu_n(K_n)^*} (X - \zeta)$$

Dans le cas où $k = \mathbb{Q}$, on trouve le polynôme de $\mathbb{C}[X]$:

$$\Phi_n = \prod_{m \wedge n = 1} (X - e^{\frac{2i\pi m}{n}})$$

En partitionant $\mu_n(K_n)$ selon l'ordre de ses éléments, on trouve la formule :

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

Cette formule permet de montrer par récurrence sur n que :

- Φ_n est à coefficients entiers
- Φ_n est universel au sens où on obtient les autres (sur un corps k) comme image de Φ_n par le morphisme $\mathbb{Z}[X] \to k[X]$

Leçons concernées : groupes des nombres complexes de module 1, polynôme irréductible, anneaux Z/nZ.