# Irréductibilité des polynômes cyclotomiques

Réf :
- Cours d'algèbre, D. Perrin

Leçons : 102, 125, 141

**Théorème**

Soit $n \in \mathbb{N}^*$. Le polynôme $\Phi_n$ est irréductible dans $\mathbb{Z}[X]$.

**Preuve :**

Soit $K$ un corps de décomposition de $\Phi_n$ sur $\mathbb{Q}$.
Soit $\gamma$ une racine de $\Phi_n$ dans $K$ et $p \in \mathbb{N}$ un nombre premier ne divisant pas $n$.

* Alors $\gamma^p$ est une racine $n$-ième primitive de l'unité (aussi)
En effet, on a pour tout $k \in \mathbb{N}^*$

$$\gamma^{pk} = 1 \iff n = o(\gamma) \mid pk \iff n \mid k$$

(car $p \wedge n = 1$)

* Notons $f$ le polynôme minimal de $\gamma$ sur $\mathbb{Q}$ et $g$ celui de $\gamma^p$ sur $\mathbb{Q}$. Alors $f$ et $g$ sont éléments de $\mathbb{Z}[X]$.

En effet, comme $\mathbb{Z}[X]$ est factoriel, il existe $f_1, \dots, f_r$ des polynômes irréductibles dans $\mathbb{Z}[X]$ et $\alpha_1, \dots, \alpha_r$ des entiers naturels non nuls tels que

$$\Phi_n = f_1^{\alpha_1} \dots f_r^{\alpha_r}.$$

Comme $\Phi_n$ est unitaire, on peut supposer que tous les $f_i$ le sont aussi.
Comme $\Phi_n(\gamma) = \Phi_n(\gamma^p) = 0$, il existe $i$ et $j$ dans $[\![1, r]\!]$ tels que $f_i = f$ et $f_j = g$. On obtient alors que $f$ et $g$ sont irréductibles dans $\mathbb{Z}[X]$ et divise $\Phi_n$ dans $\mathbb{Z}[X]$.
( $f$ divise $f_i$ or $f_i$ unitaire irréductible dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$ comme $f$

* Montrons que $f$ et $g$ sont égaux.

Supposons qu'on ait $f \neq g$. Alors le produit $fg$ divise $\Phi_n$ dans $\mathbb{Z}[X]$.

Par ailleurs, $\gamma$ est racine du polynôme $g(X^p)$ donc par minimalité $f$ divise $g(X^p)$ dans $\mathbb{Q}[X]$, mais aussi dans $\mathbb{Z}[X]$ comme ce sont tous deux des polynômes de $\mathbb{Z}[X]$, et $g$ est unitaire

Soit alors $h \in \mathbb{Z}[X]$ tel que

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

Dans $\mathbb{F}_p[X]$, le morphisme de Frobenius assure qu'on a

$$\bar{g}(X^p) = \bar{g}(X)^p$$

Soit $\varphi$ un diviseur irréductible de $\bar{f}(X)$ dans $\mathbb{F}_p[X]$.
Alors $\varphi$ divise $\bar{g}(X)^p$ et comme $\varphi$ est irréductible donc premier dans l'anneau principal $\mathbb{F}_p[X]$, on a $\varphi$ divise $\bar{g}(X)$.

On en déduit alors que $\varphi^2$ divise $\bar{f}\bar{g}$ donc $\overline{\Phi}_n$ dans $\mathbb{F}_p[X]$.
Ainsi dans un corps de décomposition de $\overline{\Phi}_n$ sur $\mathbb{F}_p$, $\overline{\Phi}_n$ aura une racine double. Or $\overline{\Phi}_n = \overline{\Phi}_{n,\mathbb{F}_p}$ a des racines simples car $p \wedge n = 1$. ↯

Nécessairement $f = g$.

* Soit $\gamma'$ une racine $n$-ième primitive de l'unité. Alors il existe $k \in \mathbb{N}^*$ tel que $\gamma' = \gamma^k$ et $k \wedge n = 1$. Comme $k$ s'écrit en produit de nombres premiers ne divisant pas $n$, par récurrence à partir de ce qui précède on obtient que $\gamma'$ et $\gamma$ ont le même polynôme minimal sur $\mathbb{Q}$. Ainsi $f$ s'annule sur $\mu_n^*$ (comme $\Phi_n$) et divise $\Phi_n$ : c'est $\Phi_n$.

* Ainsi $\Phi_n$ est unitaire et irréductible dans $\mathbb{Q}[X]$ donc dans $\mathbb{Z}[X]$.