

Irréductibilité de Φ_n sur $\mathbb{Q}$

Leçons : 102, 125, 141, 144

Référence : Michel Demazure, *Cours d'algèbre*, p. 216.

Théorème 1. *Pour tout $n > 0$, le polynôme Φ_n est irréductible dans $\mathbb{Q}[X]$.*

Démonstration.

Lemme 2 (Gauss). *Soit $P, Q \in \mathbb{Q}[X]$ unitaires. Si $PQ \in \mathbb{Z}[X]$, alors $P \in \mathbb{Z}[X]$ et $Q \in \mathbb{Z}[X]$.*

Démonstration du lemme. Notons $P = \frac{1}{m}P_1$ et $Q = \frac{1}{m}Q_1$ avec $P_1 \in \mathbb{Z}[X]$ de coefficient dominant m et $Q_1 \in \mathbb{Z}[X]$ de coefficient dominant m . On a alors

$$m^2 PQ = P_1 Q_1,$$

donc

$$m^2 \underbrace{c(PQ)}_{=1} = c(P_1) c(Q_1),$$

donc $c(P_1) = m$ et $c(Q_1) = m$, donc $P \in \mathbb{Z}[X]$ et $Q \in \mathbb{Z}[X]$. CQFD

Soit maintenant $f \in \mathbb{Q}[X]$ un facteur irréductible de Φ_n . On peut supposer f unitaire. On veut montrer que $f = \Phi_n$. Pour cela, on va montrer que f et Φ_n ont les mêmes racines, à savoir les racines primitives n -ièmes de l'unité.

Soit ξ une racine primitive n -ième de l'unité. Si ξ' est une autre racine primitive n -ième de l'unité, alors $\xi' = \xi^m$ où $\text{pgcd}(m, n) = 1$. On va donc réduire le problème :

Lemme 3. $\forall p$ premier ne divisant pas n , si $f(\xi) = 0$, alors $f(\xi^p) = 0$.

Démonstration du lemme. Soit p premier tel que $p \nmid n$. Supposons que $f(\xi) = 0$. Alors f est un polynôme annulateur de ξ unitaire et irréductible sur $\mathbb{Q}$, donc f est le polynôme minimal de ξ sur $\mathbb{Q}$.

De plus, on a $\xi^n = 1$, donc il existe $g \in \mathbb{Q}[X]$ tel que

$$X^n - 1 = f(X) g(X) \in \mathbb{Z}[X],$$

donc, d'après le lemme de Gauss, $f, g \in \mathbb{Z}[X]$.

On a de plus,

$$f(\xi^p) g(\xi^p) = (\xi^p)^n - 1 = (\xi^n)^p - 1 = 0,$$

donc, pour montrer que $f(\xi^p) = 0$, il nous suffit de montrer que $g(\xi^p) \neq 0$.

Supposons donc par l'absurde que $g(\xi^p) = 0$. Donc il existe $h \in \mathbb{Q}[X]$ tel que

$$g(X^p) = f(X) h(X) \in \mathbb{Z}[X],$$

donc, d'après le lemme de Gauss, $h(X) \in \mathbb{Z}[X]$.

Réduisons alors cette égalité modulo p . On obtient

$$X^n - 1 = \bar{f}(X) \bar{g}(X) \quad \text{et} \quad \bar{g}(X^p) = \bar{f}(X) \bar{h}(X).$$

Par le morphisme de Frobenius, on a $\bar{g}(X)^p = \bar{g}(X^p)$, donc

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

Soit alors $\bar{R} \in \mathbb{F}_p[X]$ un facteur irréductible de $\bar{f}$. Alors $\bar{R} \mid \bar{g}(X)^p$, donc $\bar{R} \mid \bar{g}(X)$, donc

$$\bar{R}^2 \mid X^n - 1.$$

Comme $p \nmid n$, $X^n - 1$ n'admet pas, dans $\mathbb{F}_p[X]$, de facteurs carrés. C'est absurde.

Donc $g(\xi^p) \neq 0$, et par suite $f(\xi^p) = 0$.

CQFD

f est un facteur irréductible unitaire de Φ_n , donc f est le polynôme minimal sur $\mathbb{Q}$ d'une racine primitive n -ième de l'unité dans $\mathbb{C}$.

D'après notre lemme, toutes les racines primitives n -ièmes de l'unité sont racines de f ; il y en a $\varphi(n)$. Donc $\deg(f) \geq \varphi(n) = \deg(\Phi_n)$.

Et $f \mid \Phi_n$, donc $\deg(f) \leq \deg(\Phi_n)$, et donc $\deg(f) = \deg(\Phi_n)$, d'où $f = \Phi_n$.

On en déduit que $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$.

□