# Irréductibilité des polynômes cyclotomiques sur $\mathbb{Z}$

Manon Ruffini

[1] Référence : Perrin, Cours d'algèbre

**Théorème 1**

*Soit $n \in \mathbb{N}^*$. Le polynôme cyclotomique $\Phi_n$ est dans $\mathbb{Z}[X]$. Il est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.*

_ **Étape 1**

*Pour tout $n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.*

On fait une récurrence forte sur $n$.

$\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$

Soit $n \in \mathbb{N}^*$. Supposons que pour tout $k \in [|1, n|], \Phi_k \in \mathbb{Z}[X]$.

Soit $F = \prod_{d|n, d\neq n} \Phi_d$ . Par hypothèse de récurrence : $F \in \mathbb{Z}[X]$ et $F$ est unitaire. De plus, on sait que $F\Phi_n = X^n - 1$ [2]

et par division euclidienne :

$$X^n - 1 = F(X)P(X) + R(X) \text{ où } P, R \in \mathbb{Z}[X], \text{ et } \deg R < \deg F$$

Cette division euclidienne est aussi vraie sur $\mathbb{C}[X]$. Par unicité, on trouve $P = \Phi_n$ et $R = 0$. [3]
Finalement, comme $P \in \mathbb{Z}[X]$ : $\Phi_n \in \mathbb{Z}[X]$.

_ **Étape 2**

*Soit $\zeta$ une racine primitive $n$-ème de l'unité. Soit $p$ un nombre premier, qui ne divise pas $n$. Alors : $\omega = \zeta^p$ est aussi une racine primitive $n$-ème de l'unité.*

_ **Étape 3**

*Soient $f$ et $g$ les polynômes minimaux de $\zeta$ et $\omega$ dans $\mathbb{Q}[X]$. Alors : $f, g \in \mathbb{Z}[X]$*

L'anneau $\mathbb{Z}[X]$ est factoriel, donc on peut écrire $\Phi_n = f_1^{\alpha_1} \dots f_r^{\alpha_r}$, où les $f_i$ sont dans $\mathbb{Z}[X]$ et sont irréductibles. On peut même supposer qu'ils sont unitaire car $\Phi_n$ l'est.
Comme $\Phi_n(\zeta) = 0$, $\zeta$ est racine de l'un des $f_i$, qui est unitaire et irréductible sur $\mathbb{Z}$, donc sur $Q$. Donc

$$f = f_i \in \mathbb{Z}[X]$$

On fait pareil avec $\omega$ et finalement :

$$f, g \in \mathbb{Z}[X], \text{ et } f, g \text{ divisent } \Phi_n$$

_ **Étape 4**

*Les polynômes $f$ et $g$ sont égaux.*

1. $\Phi_n = \prod_{\zeta \in U_n^*} (X - \zeta)$, où $U_n^*$ est l'ensemble des racines primitives $n$-èmes de l'unité
2. **Proposition 1**

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

   Ce résultat vient du faire que les racines $n$-èmes de l'unité sont exactement les racines primitives $d$-èmes, où $d|n$
3. Dans $\mathbb{C}[X]$ : $F(\Phi_n - P) = R$, avec le dégré de $R$ strictement inférieur à celui de $F$. Nécessairement : $\Phi_n - P = 0$

Par l'absurde, supposons que $f \neq g$.
Alors : $fg|\Phi_n$ dans $\mathbb{Z}[X]$ (parce qu'ils sont irréductibles et distincts). Or $g(\omega) = g(\zeta^p) = 0$, donc $\zeta$ est racine du polynôme $g(X^p)$. Donc $\exists Q \in \mathbb{Q}[X], g(X^p) = f(X)Q(X)$.
Comme précédemment, comme $f$ est unitaire, par division euclidienne sur $\mathbb{Z}$, $G(X^p) = f(X)S(X)+R(X)$ ; et par unicité : $S = Q \in \mathbb{Z}[X]$, et

$$f(X)|g(X^p) \text{ dans } \mathbb{Z}[X]$$

On projette dans $\mathbb{F}_p$ : $\bar{f}(X)|\bar{g}(X^p) = \bar{g}(x)$ pas le morphisme de Frobenius. Soit $\varphi$ un facteur de $\bar{f}$ dans $\mathbb{F}_p$. D'après le lemme d'Euclide, $\varphi|\bar{g}$. Or, $fg|\Phi_n$ dans $\mathbb{Z}[X]$, donc $\bar{f}\bar{g}|\overline{\Phi_n}$ dans $\mathbb{F}_p[X]$. D'où :

$$\varphi^2|\overline{\Phi_n}|\overline{X^n-1} \text{ donc } \exists B \in \mathbb{F}_p[X], \overline{X^n-1} = \varphi^2 B$$

Ainsi, $\overline{nX^{n-1}} = \varphi(\varphi' B + \varphi B')$, donc $\varphi|\bar{n} \neq 0$ car $p \neq n$ donc $\deg \varphi = 0$.
On obtient une contradiction ($\varphi$ est irréductible). Donc $f = g$.

– **Étape 5**

$\forall s \in \mathbb{N}^*, \forall \alpha$ *racine de* $f, \forall p_1, \dots p_s$ *premiers tels que* $(p_1 \dots p_n) \wedge n = 1$ : $f(\alpha^{p_1 \cdots p_n}) = 0$

On le fait par récurrence sur $s \in \mathbb{N}^*$.

$s = 1$ **:** C'est l'étape 4.

$s \in \mathbb{N}^*$ **:** Soit $\alpha$ une racine de $f$, soit $k = p_1 \dots p_s$ premier avec $n$. Par hypothèse de récurrence

$$f(\alpha^{p_1 \cdots p_{n-1}}) = 0$$

Or $p_s \wedge n = 1$ donc d'après l'étape 4 :

$$f(\alpha^{p_1 \cdots p_n}) = 0$$

– **Conclusion :**
Toutes les racines primitives $n$-ème de l'unité sont racines de $f$. Donc $\deg f > \varphi(n) = \deg \Phi_n$. Or $f|Phi_n$, et $f$ et $\Phi_n$ sont unitaires, donc :

$$f = \Phi_n \text{ est irréductible sur } \mathbb{Q} \text{ donc sur } \mathbb{Z}\ ^4$$

4. $P\mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$ ssi
**ou bien** $P = p \in \mathbb{Z}$, $p$ irréductible
**ou bien** $P$ est irréductible dans $\mathbb{Q}[X]$, et $P$ est primitif.