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

Leçons : 102, 141, *120, 121, 144*

[Per], théorème 4.10

Théorème

Soit $n \in \mathbb{N}^*$; le polynôme cyclotomique Φ_n (qui est dans $\mathbb{Z}[X]$) est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.

Démonstration :

Étape 1 : Par récurrence forte, on va commencer par montrer que $\forall n \in \mathbb{N}^*, \Phi_n \in \mathbb{Z}[X]$.
- Si $n = 1$, on a bien $\Phi_1 = X - 1 \in \mathbb{Z}[X]$.
- Soit $n > 1$, on suppose : $\forall k \in [\![1, n-1]\!], \Phi_k \in \mathbb{Z}[X]$.
  Soit $F = \prod_{\substack{d|n \\ d \neq n}} \Phi_d$; on a $F \in \mathbb{Z}[X]$ et F unitaire. D'une part, $\Phi_n F = X^n - 1$. [1]
  Et comme F est unitaire, on peut faire la division euclidienne de $X^n - 1$ par F dans $\mathbb{Z}[X]$:
  $$X^n - 1 = PF + R \text{ avec } P, R \in \mathbb{Z}[X] \text{ et } \deg R < \deg F.$$
  Cette division euclidienne est aussi vraie dans $\mathbb{C}[X]$; elle y est même unique, et on obtient : $P = \Phi_n$ et $R = 0$.
  Conséquemment, $\Phi_n \in \mathbb{Z}[X]$.

Étape 2 : Soit $\xi \in \mathbb{C}$ une racine primitive n^{e} de l'unité ; soit p premier, avec $p \nmid n$.
Ainsi, ξ^p est aussi une racine primitive n^{e} de l'unité, on note $\omega = \xi^p$.

Étape 3 : Soit π_ξ (respectivement π_ω) le polynôme minimal de ξ (resp. ω) sur $\mathbb{Q}$.
On va montrer que π_ξ et π_ω sont des éléments de $\mathbb{Z}[X]$.
$\mathbb{Z}$ est un anneau euclidien, donc a fortiori, $\mathbb{Z}$ est factoriel, donc $\mathbb{Z}[X]$ est un anneau factoriel. [2]
Donc on peut écrire $\Phi_n = \prod_{i=1}^{r} F_i^{\alpha_i}$, où les F_i sont irréductibles dans $\mathbb{Z}[X]$ et les α_i sont dans $\mathbb{N}^*$.
Quitte à multiplier les F_i par -1, comme Φ_n est unitaire, on peut supposer que les F_i sont unitaires.
Comme $\Phi_n(\xi) = \Phi_n(\omega) = 0$; $\exists i_0 \in [\![1, r]\!], F_{i_0}(\xi) = 0$ et $\exists i_1 \in [\![1, r]\!], F_{i_1}(\omega) = 0$.
Mais comme F_{i_0} et F_{i_1} sont irréductibles dans $\mathbb{Z}[X]$ (donc dans $\mathbb{Q}[X]$) et unitaires, ce sont les polynômes minimaux de ξ et ω, sur $\mathbb{Q}$.
Conséquemment, $F_{i_0} = \pi_\xi$ et $F_{i_1} = \pi_\omega$.
Ainsi, on a montré que $\pi_\xi \big| \Phi_n$ et $\pi_\omega | \Phi_n$ dans $\mathbb{Z}[X]$.

Étape 4 : On va montrer désormais que $\pi_\xi = \pi_\omega$; supposons par l'absurde que $\pi_\xi \neq \pi_\omega$.
Comme π_ξ et π_ω sont irréductibles dans $\mathbb{Z}[X]$ et distincts, on a : $\pi_\xi \pi_\omega \big| \Phi_n$ dans $\mathbb{Z}[X]$.
Par ailleurs, comme $\pi_\omega(\xi^p) = 0$, ξ est racine de $\pi_\omega(X^p)$; ainsi, π_ξ étant le polynôme minimal de ξ sur $\mathbb{Q}$, on a : $\pi_\xi(X) \big| \pi_\omega(X^p)$ dans $\mathbb{Q}[X]$.
Autrement dit, $\exists Q \in \mathbb{Q}[X], \pi_\omega(X^p) = \pi_\xi(X)Q(X)$.
Mais $\pi_\xi \in \mathbb{Z}[X]$ est unitaire ; on a donc la division euclidienne dans $\mathbb{Z}[X]$:
$$\pi_\omega(X^p) = \pi_\xi(X)S(X) + R(X) \text{ avec } S, R \in \mathbb{Z}[X] \text{ et } \deg R < \deg \pi_\xi.$$
Par unicité de la division euclidienne dans $\mathbb{Q}[X]$, on a : $Q = S$ et $R = 0$.
En particulier, $\pi_\xi(X) \big| \pi_\omega(X^p)$ dans $\mathbb{Z}[X]$.
Dans la suite, on notera $\overline{P} \in \mathbb{F}_p[X]$ la réduction modulo p du polynôme $P \in \mathbb{Z}[X]$.
Le morphisme de Frobenius fournit alors : $\overline{\pi_\xi(X)} \Big| \overline{\pi_\omega(X^p)} = \overline{\pi_\omega(X)}^p$.
Soit A un facteur irréductible de $\overline{\pi_\xi}$ dans $\mathbb{F}_p[X]$.
Ainsi, $A | \overline{\pi_\omega}^p$, et par le lemme d'Euclide : $A | \overline{\pi_\omega}$.
Comme $\pi_\xi \pi_\omega \big| \Phi_n$ dans $\mathbb{Z}[X]$, $\overline{\pi_\xi \pi_\omega} \big| \overline{\Phi_n}$ dans $\mathbb{F}_p[X]$ et donc $A^2 \big| \overline{\Phi_n}$ dans $\mathbb{F}_p[X]$.
Ensuite, $A^2 \big| \overline{X^n - 1}$, donc $\exists B \in \mathbb{F}_p[X], \overline{X^n - 1} = A^2 B$, puis en dérivant $\overline{nX^{n-1}} = A(2A'B + AB')$.
Donc, $A \Big| \overline{nX^{n-1}}$ dans $\mathbb{F}_p[X]$.
Mais $A \Big| \overline{nX^n - n}$ dans $\mathbb{F}_p[X]$, donc $A | \overline{n} \neq 0$.

1. Cela se justifie bien en disant que les racines n^{es} de l'unité sont les racines primitives d^{es} de l'unité, avec $d | n$.
2. « Je veux bien, je les connais ces résultats-là, mais si on me demande comment ça se démontre ?
– Eh bien, tu n'as qu'à aller voir à la page **??**. »

En conséquence, $\deg A = 0$, ce qui contredit l'irréductibilité de A (car $\mathbb{F}_p$ est un corps donc les polynômes de degré nul sont inversibles dans $\mathbb{F}_p[X]$).
On obtient donc (enfin) une contradiction : ainsi $\pi_{\xi} = \pi_{\omega}$.

Étape 5 : Montrons, par récurrence sur $s \in \mathbb{N}^*$ que :

$$\forall \alpha \text{ racine de } \pi_{\xi}, \forall p_1, \dots, p_s \text{ premiers tels que } (p_1 \dots p_s) \wedge n = 1, \pi_{\xi}\left(\alpha^{p_1 \cdots p_s}\right) = 0.$$

- Si $s = 1$, on a déjà vu ça dans l'étape précédente.
- Soit $s > 1$, α une racine de π_{ξ}, et $k = p_1 \dots p_s$ où les p_i sont des nombres premiers tels que $k \wedge n = 1$.
  On a $p_1 \dots p_{s-1} \wedge n = 1$ donc $\alpha^{p_1 \cdots p_{s-1}}$ est racine de π_{ξ} par hypothèse de récurrence.
  Or, aussi $p_s \wedge n = 1$, donc $\pi_{\xi}\left((\alpha^{p_1 \cdots p_{s-1}})^{p_s}\right) = 0$, d'où $\pi_{\xi}\left(\alpha^k\right) = 0$.

Étape 6 : Ainsi, tous les éléments de μ_n^* sont racines de π_{ξ}, donc $\deg \pi_{\xi} \geqslant \varphi(n)$.
Et comme $\pi_{\xi} \big| \Phi_n$, on a $\deg \pi_{\xi} = \varphi(n)$; π_{ξ} et Φ_n étant unitaires, on obtient $\Phi_n = \pi_{\xi}$. ■

Références

[Per] D. PERRIN – *Cours d'algèbre*, Ellipses, 1996.