Irréductibilité des polynômes cyclotomiques

Perrine Jouteur

Ce développement est très classique, il se place dans les leçons 102, 125, 141 et 144, et on peut le trouver dans le livre d'Algèbre de Perrin.

Théorème 0.1 Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$, et même sur $\mathbb{Z}$.

Lemme 0.1 Soit $P \in \mathbb{Z}[X]$, et $A, B \in \mathbb{Q}[X]$, tous les trois unitaires. Si $P = AB$, alors A et B sont en fait à coefficients dans $\mathbb{Z}$.

Démonstration (du lemme)
Soit m_A le ppcm des dénominateurs des coefficients de A, et m_B pareil pour B. Alors $m_A A \in \mathbb{Z}[X]$ et $m_B B \in \mathbb{Z}[X]$, et de plus $c(m_A A) = c(m_B B) = 1$. Donc $c(m_A m_B P) = 1$, et donc $m_A m_B = 1$. Ainsi $m_A, m_B \in \{\pm 1\}$, et donc les dénominateurs de A et de B étaient égaux à 1, ce qui signifie que A et B étaient à coefficients dans $\mathbb{Z}$. ■

Démonstration (du théorème)
Soit $n \in \mathbb{N}^*$. On note ϕ_n le n-ème polynôme cyclotomique. On va montrer mieux que l'énoncé : on va montrer que ϕ_n est le polynôme minimal de n'importe quelle de ses racines.
Soit donc ξ une racine primitive n-ème de l'unité. Notons π son polynôme minimal sur $\mathbb{Q}$. On a déjà que π divise ϕ_n dans $\mathbb{Q}$, puisque ξ est racine de ϕ_n.

Montrons que π annule toutes les racines primitives n-èmes de l'unité.
Soit p un nombre premier qui ne divise pas n, et x une racine de π. Montrons que x^p est encore racine de π.
Comme $\pi | X^n - 1$, il existe un polynôme g à coefficients dans $\mathbb{Q}$ tel que $\pi(X)g(X) = X^n - 1$. Par le lemme 1, on a même que g et π sont à coefficients dans $\mathbb{Z}$. Et, en évaluant en x^p, on a

$$\pi(x^p)g(x^p) = 0.$$

Si $\pi(x^p) \neq 0$, alors $g(x^p) = 0$, donc x est racine de $g(X^p)$. Par minimalité de π, on a $\pi | g(X^p)$, dans $\mathbb{Q}[X]$: il existe $h \in \mathbb{Q}[X]$ tel que $g(X^p) = h(X)\pi(X)$. Mais par le lemme 1, on a même que $h \in \mathbb{Z}[X]$. Donc on peut réduire ça modulo p. Dans $\mathbb{F}_p[X]$, on a

$$\overline{g}(X)^p = \overline{h}(X)\overline{\pi}(X).$$

Soit θ est un facteur irréductible de $\overline{\pi}$. Alors θ divise $\overline{g}$ et donc θ^2 divise $X^n - 1$, dans $\mathbb{F}_p[X]$. Or $X^n - 1$ est sans facteur carré (par exemple avec la dérivée), contradiction.
Donc $\pi(x^p) = 0$.

Soit $\tilde{\xi}$ une racine primitive n-ème de l'unité. Il existe $r \in [\![1, n]\!]$ tel que $\xi^r = \tilde{\xi}$. Comme $\tilde{\xi}$ est primitive, r est premier avec n. Donc aucun des diviseurs premiers de r ne divise n. Écrivons $r = p_1 \cdots p_m$. Alors $\pi(\xi^{p_1}) = 0$ car ξ est racine de π et d'après ce qu'on vient de faire. Puis par récurrence, $\pi(\xi^r) = 0$.
Donc toutes les racines primitives n-èmes de l'unité sont racines de π. Ainsi ϕ_n divise π, et comme ils sont tous les deux unitaires, on a égalité $\phi_n = \pi$. ■

Remarque 0.1 Questions possible de la part du jury :
- Pourquoi les polynômes cyclotomiques sont à coefs dans $\mathbb{Z}$?
- Montrer que ϕ_8 est réductible sur tous les corps fini.