Développement : Irréductibilité des polynômes cyclotomiques

Leçons : 102, 123, 141.

Théorème. *Pour $n \in \mathbb{N}^*$, on note Π_n l'ensemble des racines primitives n-èmes de l'unité, et on définit le n-ème polynôme cyclotomique $\Phi_n = \prod_{\zeta \in \Pi_n} (X - \zeta)$. Les Φ_n sont à coefficients dans $\mathbb{Z}$, et irréductibles dans $\mathbb{Q}[X]$.*

Démonstration.
Étape 1 : $X^n - 1 = \prod_{d|n} \Phi_d$.
On remarque d'abord que $\deg(\Phi_n) = |\Pi_n| = |\{k \leq n, k \wedge n = 1\}| = \varphi(n)$.
Si n est premier, tous les éléments de $\mathbb{U}_n$ sauf 1 engendrent $\mathbb{U}_n$. Ainsi $\Phi_n = \dfrac{X^n - 1}{X - 1} = 1 + X + \cdots + X^{n-1}$.
Soit $\omega = e^{2i\pi/n}$. Soient $k \in [\![0, n-1]\!], d = \mathrm{ord}(\omega^k)$. On a $d|n$. De plus, $(\omega^k)^d = 1$ donc $\omega^k \in \mathbb{U}_d$, et comme $d = \mathrm{ord}(\omega^k)$, on a même $\omega^k \in \Pi_d$. D'où $(X - \omega^k)|\Phi_d$, et par suite, $(X - \omega^k)|\prod_{d|n} \Phi_d$. Comme les $\omega^k, 0 \leq k \leq n-1$ sont deux à deux distincts, il s'ensuit que $X^n - 1 = \prod_{k=0}^{n-1}(X - \omega^k)|\prod_{d|n} \Phi_d$. De plus, ces deux polynômes sont de même degré (car $\deg\left(\prod_{d|n} \Phi_d\right) = \sum_{d|n} \varphi(d) = n$), et unitaires, donc égaux : $X^n - 1 = \prod_{d|n} \Phi_d$.
Étape 2 : $\forall n \in \mathbb{N}^*, \Phi_n \in \mathbb{Z}[X]$.

Par récurrence. On a $\Phi_1 = X - 1$ donc c'est vrai pour $n = 1$. Si c'est vrai jusqu'à $n - 1$, on a $P := \prod_{\substack{d|n \\ d \neq n}} \Phi_d \in \mathbb{Z}[X]$, et $X^n - 1 = \Phi_n P$. Division euclidienne dans $\mathbb{Z}[X]$ (possible car P unitaire) : $X^n - 1 = PQ + R, \deg(R) < \deg(P)$. Par unicité de la division euclidienne, $R = 0, \Phi_n = Q \in \mathbb{Z}[X]$, ce qui prouve le résultat au rang n.

Étape 3 : Polynôme minimal des racines primitives.
Soit ζ une racine primitive n-ème de l'unité, soit P son polynôme minimal dans $\mathbb{Q}$. On a $P|(X^n - 1)$: il existe $Q \in \mathbb{Q}[X], X^n - 1 = PQ$, et comme précédemment (division euclidienne), $Q \in \mathbb{Z}[X]$. Soit p nombre premier qui ne divise pas n, soit u racine de P. Montrons que u^p racine de P. Comme $P|(X^n - 1)$, on a $u^n - 1 = 0$ d'où $0 = (u^p)^n - 1 = P(u^p)Q(u^p)$. Par l'absurde, si $P(u^p) \neq 0$, alors $Q(u^p) = 0$. Or u racine de P qui est unitaire et irréductible dans $\mathbb{Q}[X]$, donc P polynôme minimal de u. Ainsi, comme $Q(X^p)$ annule u, on a $P|Q(X^p)$, et $Q(X^p) = P(X)R(X)$, $R(X) \in \mathbb{Z}[X]$ comme précédemment. On réduit modulo p : $\overline{Q}(X)^p = \overline{Q}(X^p) = \overline{P}(X)\overline{R}(X)$. Soit $T \in \mathbb{F}_p[X]$ facteur irréductible de $\overline{P}$, alors $T|\overline{Q}^p \Rightarrow T|\overline{Q}$, et comme $T|\overline{P}$, on a $T^2|\overline{PQ} = (X^n - 1)$. Ainsi $X^n - 1$ a une racine double dans une clôture algébrique de $\mathbb{F}_p$, contradiction car $X^n - 1$ premier avec sa dérivée par Bézout : $(n^{-1}X)nX^{n-1} - (X^n - 1) = 1$. Donc $P(u^p) = 0$.

Étape 4 : Φ_n est un polynôme minimal.
ζ racine de P, et donc pour tout $p \in \mathbb{N}$ premier non diviseur de n, ζ^p racine de P. Il s'ensuit, par élévations successives à des puissances premières, que pour tout $k \in \mathbb{N}$ premier avec n, ζ^k racine de P, donc toutes les racines primitives n-èmes sont racines de P. Donc $\Phi_n|P$. Mais comme $\Phi_n(\zeta) = 0$, on a aussi $P|\Phi_n$. Les deux étant unitaires, $\Phi_n = P$ est irréductible dans $\mathbb{Q}[X]$. □

Références

X. Gourdon, Les maths en tête - Algèbre, Ellipses, p. 91.
I. Gozard, Théorie de Galois, Ellipses, p. 69.

Notes personnelles

Développement présenté à l'oral dans la leçon 102. La seule question qu'on m'a posé a été de prouver l'affirmation "Si $P|Q$ et qu'ils sont unitaires de même degré, ils sont égaux".