Irréductibilité des polynômes cyclotomiques.

Rémi Lajugie

On appelle Φ_n le $n-$ème polynôme cyclotomique (produit des $(X-\xi_n)$ où ξ est une racine primitive n-ème de l'unité).

Proposition 1 *On a la relation* $\Pi_{d|n}\Phi_d = X^n - 1$.

On peut alors en déduire par récurrence que les polynômes cyclotomiques sont à coefficients entiers.

Proposition 2 *Un polynôme cyclotomique* Φ_n *est irréductible dans* $\mathbb{Q}[X]$ *si, et seulement si il l'est dans* $\mathbb{Z}[X]$.

Preuve : Le sens direct est évident. Pour le sens réciproque, supposons que Φ_n admette une factorisation dans $\mathbb{Q}$, $\Phi_n = PQ$. On pose, pour $R \in \mathbb{Z}[X], c(R)$ le pgcd des coefficients de R. Cette fonction est multiplicative. Notons p le ppcm des dénominateurs de P, q celui de Q. On a alors $c(pqPQ) = c(pP)c(qQ) = pqc(\Phi_n) = pq$. Donc on en déduit que $p|c(qQ)$ et $q|c(pP)$ donc p divise tous les numérateurs des coefficients de Q et idem pour q vis à vis de ceux de P. Donc $\tilde{Q} = qQ/p$ et $\tilde{(P)} = pP/q$ sont à coefficients entiers. Et on a $\Phi_n = \tilde{Q}\tilde{P}$.

Théorème 1 *Le polynôme cyclotomique* Φ_n *est irréductible sur* $\mathbb{Q}$.

Preuve : Elle s'effectue par l'absurde.

Soit ξ une racine primitive n-ème de l'unité. *Etape 1 : montrons que si p est un nombre premier avec n,* ξ *et* ξ^p *ont le même polynôme minimal.*

Supposons que ce ne soit pas le cas. Notons P et Q les polynômes minimaux sur $\mathbb{Q}$ en question. Ils sont premiers entre eux [1].

Réduisons modulo p, on a alors $\tilde{P}(X)^p = \tilde{P}(X^p)$. Soit H un facteur irréductible non constant de Q, il y en a car le polynôme Q est unitaire comme il divise le cyclotomique. $H|\tilde{P}(X)^p$ donc $H|\tilde{P}$. Ainsi, dans $\mathbb{F}_p[X]$, on a $H^2|X^n - 1$. Or comme, p est premier avec n, ce dernier polynôme est premier avec sa dérivée. Donc, dans un corps de décomposition de H, $X^n - 1$ admet une racine double, ce qui est contradictoire.

Etape 2 : on passe au cas général. Une récurrence immédiate montre que, pour tout $k \in \mathbb{N}$ pour tout p premier avec n ξ^{p^n} a le même polynôme minimal que ξ. Une autre récurrence immédiate nous assure que toutes les racines primitives $n-$ème de l'unité auront bien pour polynôme minimal, le polynôme cyclotomique.

Références

— Perrin.
— Combes.

1. Ce sont des irréductibles sur $\mathbb{Q}$, distincts par hypothèse.