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

Leçons 102, 141(, 120, 121, 144)

Ref : [Perrin] III.4

On démontre ici l'irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$, et on en déduit celle sur $\mathbb{Z}$. Les arguments en gris peuvent suivant la leçon être à énoncer rapidement, ou bien demandent un peu plus d'attention et de détails.

On introduit le n-ième polynôme cyclotomique sur le corps $\mathbb{K}$, que l'on note $\Phi_{n,\mathbb{K}}$. Si $\mathbb{K} = \mathbb{Q}$, on notera simplement Φ_n. On note μ_n (resp. μ_n^*) l'ensemble des racines (resp. primitives) n-ième de l'unité.

Proposition 1 Φ_n est à coefficients dans $\mathbb{Z}$.

Démonstration. On procède par récurrence forte sur n. Comme $\Phi_1(X) = X - 1$, le résultat est vrai pour $n = 1$. Supposons maintenant qu'il l'est pour tout $d < n$, avec $n \geq 2$. On note $P = \prod_{d|n, d\neq n} \Phi_d$, qui est un polynôme à coefficients dans $\mathbb{Z}$ par hypothèse de récurrence. De plus, puisque tous les $\Phi_{k,\mathbb{K}}$ sont unitaires, quelquesoit l'entier k et le corps $\mathbb{K}$, P est unitaire. On peut donc effectuer la division euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$: $X^n - 1 = PQ + R$ avec $Q, R \in \mathbb{Z}[X]$ et $\deg(R) < \deg(P)$. Or on sait que $X^n - 1 = \Phi_n P$ [1], donc $R = P(\Phi_n - Q)$, et pour des raisons de degré, les deux membres de l'égalité sont nuls. Donc $\Phi_n = Q \in \mathbb{Z}[X]$. □

Théorème 2 Φ_n est irréductible sur $\mathbb{Z}$.

Démonstration.

Étape 1. Polynômes minimaux des racines primitives de l'unité sur $\mathbb{Q}$.

On se donne un corps de décomposition de Φ_n sur $\mathbb{Q}$, que l'on note $\mathbb{K}$, et une racine n-ième primitive de l'unité $\zeta \in \mathbb{K}$. On note μ le polynôme minimal de ζ sur $\mathbb{Q}$. Montrons que $\mu \in \mathbb{Z}[X]$ et μ divise Φ_n dans $\mathbb{Z}[X]$.

Comme $\mathbb{Z}[X]$ est factoriel, on écrit $\Phi_n = P_1..P_r$ la décomposition de Φ_n en produit d'irréductibles dans $\mathbb{Z}$. Puisque Φ_n est unitaire, on peut supposer (quitte à le multiplier par -1) que P_i est unitaire, pour tout $i \in [\![1, r]\!]$. Mais comme ζ est racine de l'un des P_i, et que celui-ci est irréductible unitaire sur $\mathbb{Z}$, et donc sur $\mathbb{Q}$, on a $\mu = P_i$. Donc $\mu \in \mathbb{Z}[X]$ est μ divise Φ_n dans $\mathbb{Z}$.

Étape 2. Les puissances d'une même racine primitive ont le même polynôme minimal.

Soit maintenant $p \in \mathfrak{P}$ un nombre premier ne divisant pas n. Alors ζ^p est aussi une racine primitive n-ième de l'unité dans $\mathbb{K}$. On note ν son polynôme minimal. Montrons que $\mu = \nu$. Supposons par l'absurde que c'est faux. Alors μ et ν sont deux polynômes irréductibles distincts qui divisent Φ_n dans $\mathbb{Z}$, donc leur produit le divise aussi. De plus, comme $\nu(\zeta^p) = 0$, ζ est racine de $\nu(X^p) \in \mathbb{Z}[X]$. On en déduit que μ divise $\nu(X^p)$ dans $\mathbb{Q}[X]$. Montrons que c'est aussi vrai dans $\mathbb{Z}[X]$: on se donne $P \in \mathbb{Q}[X]$ tel que $\nu(X^p) = \mu(X)P(X)$. On se donne $q \in \mathbb{Q}$ tel que $P = qQ$ et $Q \in \mathbb{Z}[X]$ soit primitif, et on applique le lemme de Gauß :

$$1 = c(\nu(X^p)) = qc(\mu)c(Q) = q,$$

car ν et μ sont unitaires, et Q primitif. Donc $q = 1$, ce qui signifie que P est bien dans $\mathbb{Z}[X]$.

On projette alors cette égalité dans $\mathbb{F}_p$. On a $\overline{\nu}(X^p) = \overline{\nu}(X)^p$.

En effet, on note $\nu(X) = \sum_{i=0}^{k} a_i X^i$, et on a $\overline{\nu}(X^p) = \sum_{i=0}^{k} \overline{a_i} X^{pi} = \left(\sum_{i=0}^{k} \overline{a_i} X^i\right)^p = \overline{\nu}(X)^p$.

Ainsi, $\overline{\nu}^p = \overline{\mu}\overline{P}$. On se donne un facteur irréductible φ de $\overline{\mu}$ sur $\mathbb{F}_p$. D'après le lemme d'Euclide, comme φ divise $\overline{\nu}^p$, alors il divise $\overline{\nu}$. Or comme $\mu\nu$ divise Φ_n sur $\mathbb{Z}$, $\overline{\mu\nu}$ divise $\overline{\Phi_n}$ sur $\mathbb{F}_p$, mais $\overline{\Phi_n}$ est en fait $\Phi_{n,\mathbb{F}_p}$ [2], donc $\overline{\mu\nu}$ divise $\Phi_{n,\mathbb{F}_p}$ sur $\mathbb{F}_p$. Donc φ^2 est un facteur carré de $\Phi_{n,\mathbb{F}_p}$, ce qui est absurde.

En effet, la dérivée de $X^n - 1$ est nX^{n-1}, qui n'admet que 0 comme racine dans $\mathbb{F}_p$, car n et p sont premiers entre eux. Donc, comme 0 n'est pas racine de $X^n - 1$, celui-ci n'a que des racines simples. On en déduit que sur $\mathbb{F}_p$, les polynômes cyclotomiques n'ont pas de facteurs carrés.

1. Cela vient de l'égalité $\mu_n(\mathbb{K}) = \bigcup_{d|n} \mu_d^*(\mathbb{K})$.

2. Cela se montre par récurrence forte en utilisant un procédé similaire à celui de la proposition précédente.

Donc $\mu = \nu$.

Étape 3. Autres racines et conclusion.

Si ζ' est une racine primitive n-ième de l'unité, on peut écrire $\zeta' = \zeta^m$, avec m premier avec n, et donc décomposable en un produit $p_1..p_r$ de nombre premiers ne divisant pas n. Par récurrence sur r [3], on montre alors en appliquant directement la seconde étape que ζ' et ζ ont le même polynôme minimal sur $\mathbb{Q}$, et que celui-ci est μ. Donc, comme μ admet les $\varphi(n)$ racines primitives de l'unité comme zéros, il est de degré au moins $\varphi(n)$. Or Φ_n est de degré $\varphi(n)$, divisible par μ, et les deux sont unitaires. Donc $\mu = \Phi_n$, et donc Φ_n est irréductible sur $\mathbb{Q}$. Comme il est unitaire et à coefficients dans $\mathbb{Z}$, il est primitif, et donc irréductible sur $\mathbb{Z}$. □

3. On applique l'étape 2 à $\widetilde{\zeta} := \zeta^{p_1 \cdots p_{r-1}}$ et $\widetilde{\zeta}^{p_r} = \zeta'$ pour montrer que leur polynôme minimal sur $\mathbb{Q}$ est le même.