P. Maurer

ENS Rennes

Recasages : 123, 125, 141, 144.

Référence : Perrin, Cours d'Algèbre

Polynômes cyclotomiques

Dans ce qui suit, K est un corps et $n \in \mathbb{N}^*$ est un entier tel que $\mathrm{car}(K) \nmid n$.

Definition 1. *On appelle groupe des racines $n^{\text{èmes}}$ de l'unité dans K, et on note $\mu_n(K)$ l'ensemble $\{\zeta \in K : \zeta^n = 1\}$. Une racine $n^{\text{ème}}$ de l'unité est dite primitive si de plus, pour tout k divisant n, on a $\zeta^k \neq 1$. On note $\mu_n^*(K)$ l'ensemble des racines primitives $n^{\text{èmes}}$ de l'unité.*

Definition 2. *Le $n^{\text{ème}}$ polynôme cyclotomique sur K est défini par :*

$$\Phi_{n,K}(X) := \prod_{\zeta \in \mu_n^*(K)} X - \zeta.$$

Lemma 3. *$\Phi_{n,K}(X)$ est unitaire, de degré $\varphi(n)$, et vérifie $X^n - 1 = \prod_{d|n} \Phi_{d,K}(X)$.*

Proof. Le polynôme $\Phi_{n,K}(X)$ est produit de polynômes unitaires de degré 1, et il y a autant de ces polynômes que d'éléments dans $\mu_n^*(K)$. On en déduit que $\Phi_{n,K}(X)$ est unitaire, de degré $|\mu_n^*(K)| = \varphi(n)$.

Pour montrer la dernière égalité, on écrit $X^n - 1 = \prod_{\zeta \in \mu_n(K)} X - \zeta$. Si d est l'ordre de ζ dans $\mu_n(K)$, alors $d|n$, et de plus, $\zeta \in \mu_d^*(K)$. Par conséquent, $X - \zeta$ divise Φ_d, donc divise $\prod_{d|n} \Phi_{d,K}(X)$.

Les valeurs de ζ dans $\mu_n(K)$ étant toutes distinctes, les polynômes $X - \zeta$ sont premiers entre eux : ainsi, leur produit divise toujours $\prod_{d|n} \Phi_{d,K}(X)$.

Les polynômes $X^n - 1$ et $\prod_{d|n} \Phi_{d,K}(X)$ étant tous deux unitaires et de même degré (via la formule $n = \sum_{d|n} \varphi(n)$), ils sont égaux. □

Theorem 4. *(Polynômes cyclotomiques rationnels)*

i. $\Phi_{n,\mathbb{Q}}(X)$ est à coefficients dans $\mathbb{Z}$.

ii. $\Phi_{n,\mathbb{Q}}(X)$ est irréductible sur $\mathbb{Z}$.

Proof.

Pour démontrer le premier point, on raisonne par récurrence forte sur $n \in \mathbb{N}$.

On a $\Phi_{1,\mathbb{Q}}(X) = X - 1$, qui est à coefficients dans $\mathbb{Z}$. Suposons que pour un certain $n \in \mathbb{N}$, on ait : $\forall k \in [\![0, n-1]\!] \quad \Phi_{k,\mathbb{Q}} \in \mathbb{Z}[X]$. D'après le lemme précédent, on a :

$$X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{Q}}(X) = \Phi_{n,\mathbb{Q}}(X) \cdot \prod_{d|n, d<n} \Phi_{d,\mathbb{Q}}(X) =: \Phi_{n,\mathbb{Q}}(X) \cdot F(X).$$

Par hypothèse de récurrence, $F(X) \in \mathbb{Z}[X]$. On peut donc effectuer la division euclidienne de $X^n - 1$ par $F(X)$: il existe $Q, R \in \mathbb{Z}[X]$ uniques tels que $X^n - 1 = F(X)Q(X) + R(X)$, avec $\deg(R) < n$.

On en déduit que $F(X)Q(X) = F(X)\Phi_{n,\mathbb{Q}}(X)$, donc par intégrité de $K[X]$, $\Phi_{n,\mathbb{Q}}(X) = Q(X) \in \mathbb{Z}[X]$.

Montrons à présent le second point. On va démontrer que $\Phi_{n,\mathbb{Q}}(X)$ est irréductible sur $\mathbb{Q}$: comme son contenu (pgcd de ses coefficients est 1), on en déduira l'irréductibilité sur $\mathbb{Z}$.

Soit K un corps de décomposition de $\Phi_n := \Phi_{n,\mathbb{Q}}(X)$. On note ζ une racine primitive $n^{\text{ème}}$ de l'unité (qui est donc racine de Φ_n dans K). Soit p un nombre premier ne divisant pas n, alors ζ^p est encore une racine primitive $n^{\text{ème}}$ de l'unité car $p \wedge n = 1$. On note f (respectivement g) le polynôme minimal de ζ (respectivement de ζ^p) sur $\mathbb{Q}$.

- **Etape 1** : f et g sont à coefficients entiers.

  Pour prouver ce résultat, on utilise la factorialité de l'anneau $\mathbb{Z}[X]$: on écrit $\Phi_n = f_1^{r_1} \cdots f_m^{r_m}$, avec $f_i \in \mathbb{Z}[X]$ irréductibles. Alors ζ est racine de l'un des f_i, qui est irréductible et unitaire (quitte à multiplier par -1) : c'est donc que $f_i = f$. De même, ζ^p est racine d'un f_j irréductible et unitaire, donc $f_j = g$. Ceci montre que $f, g \in \mathbb{Z}[X]$, et de plus que f et g divisent Φ_n.

- **Etape 2** : $f = g$.

  On raisonne par l'absurde en supposant $f \neq g$. Comme f et g sont irréductibles, on a dans ce cas $fg | \Phi_n$ dans $\mathbb{Z}[X]$.

  Par ailleurs, $g(\zeta^p) = 0$, donc ζ est aussi racine de $g(X^p)$. On en déduit que f divise $g(X^p)$ dans $\mathbb{Q}[X]$: il existe $h \in \mathbb{Q}[X]$ tel que $g(X^p) = f(X)h(X)$. En écrivant $h = \dfrac{a}{b} h'$ avec $h' \in \mathbb{Z}[X]$, on a $b g(X^p) = a f(X) h'(X)$, donc $h'(X)$ divise $g(X^p)$ (puisqu'il ne divise pas b). On a donc $g(X^p) = f(X)h'(X)$ dans $\mathbb{Z}[X]$.

  On va projeter cette égalité dans $\mathbb{F}_p$: remarquons d'abord que $\overline{g}(X^p) = \overline{g}(X)^p$. En effet, si on écrit $g(X) = a_r X^r + \cdots + a_0$, alors $\overline{g}(X)^p = (\overline{a_r} X^r + \cdots + \overline{a_0})^p = \overline{a_r}^p X^{pr} + \cdots + \overline{a_0}^p$ (c'est le morphisme de Frobenius). De plus, dans $\mathbb{F}_p$, on a $X^p = X$, donc $\overline{a_i}^p = \overline{a_i}$ pour tout i.

  La projection donne donc $\overline{g}(X)^p = \overline{f}(X)\overline{h'}(X)$. Soit φ un diviseur irréductible de $\overline{f}$ dans $\mathbb{F}_p[X]$. Alors φ divise $\overline{g}(X)^p$, donc par lemme d'Euclide, φ divise $\overline{g}(X)$. Comme fg divise Φ_n sur $\mathbb{Z}$, $\overline{f}\overline{g}$ divise $\overline{\Phi_n}$ sur $\mathbb{F}_p$, donc φ^2 divise $\overline{\Phi_n}$. Mais alors, dans un corps de décomposition, $\overline{\Phi_n}$ a une racine double, ce qui n'est pas possible lorsque la caractéristique p du corps $\mathbb{F}_p$ ne divise pas n.

- **Etape 3** : Φ_n est irréductible sur $\mathbb{Q}$.

  Soit ζ' une autre racine primitive $n^{\text{ème}}$ de Φ_n. Alors $\zeta' = \zeta^m$ avec $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où p_i ne divise pas n. Par récurrence immédiate avec le résultat de l'étape 2, on en déduit que ζ' et ζ ont même polynôme minimal sur $\mathbb{Q}$, de sorte que f admet toutes les racines primitives $n^{\text{ème}}$ de l'unité comme zéro : on a donc $f | \Phi_n$ et $\deg(f) \geq \varphi(n)$, ce qui donne $f = \Phi_n$.

  Ainsi, $\Phi_n = f$ est irréductible sur $\mathbb{Q}$. □

Theorem 5. *(Cas des corps finis)*

Les propositions suivantes sont équivalentes :

i. Il existe p premier, avec $p \wedge n = 1$, tel que $\Phi_{n,\mathbb{F}_p}(X)$ soit irréductible sur $\mathbb{F}_p$.

ii. $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.