Titre : Étude des polynômes cyclotomiques.
Recasages : 102,122,125,141,144
Thème : Anneaux de polynômes, corps finis, arithmétique.
Références : Perrin (p. 82)

D'abord quelques notations : on pose, pour $n \in \mathbb{N}^*$ $\mu_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$ et $\mu_n^* = \{z \in \mathbb{C}^* \mid o(z) = n \text{ dans } \mathbb{C}^*\}$ respectivement les racines de l'unité, et les racines primitives n-èmes de l'unité dans $\mathbb{C}$. Pour $n \in \mathbb{N}^*$, on pose également

$$\Phi_n(X) := \prod_{\zeta \in \mu_n^*} (X - \zeta)$$

On rappelle que $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Théorème 1. *Pour $n \geqslant 1$, on a $\Phi_n(X) \in \mathbb{Z}[X]$ est un polynôme irréductible et unitaire, donc irréductible dans $\mathbb{Q}[X]$ également.*

Premièrement, on montre par récurrence sur n qur Φ_n est unitaire à coefficients entiers : c'est clair pour $\phi_1(X) = X - 1$, et si le résultat est acquis pour $d|n$. Alors on pose

$$F(X) = \prod_{\substack{d|n \\ d<n}} \Phi_d(X)$$

On a $F \in \mathbb{Z}[X]$ est unitaire par hypothèse de récurrence, on peut effectuer la division euclidienne dans $\mathbb{Z}[X]$ de $X^n - 1$ par F, on obtient

$$X^n - 1 = F(X)P(X) + R(X) \text{ avec } P, R \in \mathbb{Z}[X] \text{ et } dR < dF$$

On sait par ailleurs que $X^n - 1 = F(X)\Phi_n(X)$ dans $\mathbb{C}[X]$, donc $F(X)(\Phi_n(X) - P(X)) = R(X)$, par comparaison des degrés, on a donc $\Phi_n(X) = P(X) \in \mathbb{Z}[X]$.

Pour l'irréductibilité, on pose k un corps de décomposition de $\Phi_n(X)$ sur $\mathbb{Q}$, $\zeta \in \mu_n^*$ et p un nombre premier ne divisant pas n. On sait que $\zeta^p \in \mu_n^*$. Posons f (resp g) le polynôme minimal de ζ (resp, de ζ^p) sur $\mathbb{Q}$. On a $f, g \in \mathbb{Z}[X]$, en effet, l'anneau $\mathbb{Z}[X]$ étant factoriel, on peut considérer

$$\Phi_n(X) = \prod_{i=1}^{r} f_i^{\alpha_i}$$

une décomposition de Φ_n en produit de facteur irréductibles. Comme Φ_n est unitaire, on peut supposer que les f_i le sont également (quitte à les multiplier par -1), ils sont alors irréductibles sur $\mathbb{Q}$. Mais alors ζ est racine d'un des f_i, qui est donc égal à f par irréductibilité. On obtient donc $f|\Phi_n$ et de même $g|\Phi_n$.
Montrons par l'absurde que $f = g$: dans le cas contraire, le produit fg divise Φ_n dans $\mathbb{Z}[X]$, par ailleurs, comme $g(\zeta^p) = 0$, ζ est racine de $g(X^p)$, donc $f(X)|g(X^p)$ dans $\mathbb{Q}[X]$, et donc dans $Z[X]$ car $f(X)$ et $g(X^p)$ sont unitaires. Projetons l'égalité $g(X^p) = f(X)h(X)$ dans $\mathbb{F}_p$, on pose

$$g(X) = \sum_{i=0}^{r} a_i X^i$$

on a

$$\overline{g}(X^p) = \sum_{i=0}^{r} \overline{a_i} X^{pi} = \overline{g}(X)^p$$

(morphisme de Frobenius). Soit $\varphi(X)$ un facteur irréductible de $\overline{f}(X)$ dans $\mathbb{F}_p[X]$. On a $\overline{g}(X)^p = \overline{f}(X)\overline{h}(X)$, donc par le lemme d'Euclide, φ divise $\overline{g}$. Comme fg divise Φ_n dans $\mathbb{Z}[X]$, φ^2 divise $\overline{\Phi_n}$ dans $\mathbb{F}_p[X]$. Mais dans un corps de décomposition, on obtiendrait que Φ_n a une racine double, donc $X^n - 1$ également, ce qu'on sait être faux, donc $f = g$.
Soit maintenant $\zeta' \in \mu_n^*$, on sait que ζ' s'écrit ζ^m avec m premier avec n, on décompose $m = \prod_{i=1}^r p_i^{\alpha_i}$, en itérant le résultat précédent, on trouve que ζ' et ζ ont même polynôme minimal sur $\mathbb{Q}$, égal à f, donc tous les éléments de μ_n^* sont racines de f d'où $\Phi_n | f$, $f = \Phi_n$ et le résultat.

Proposition 2. *Soient $n \in \mathbb{N}^*$, p premier ne divisant pas n, et $q = p^\alpha$. Dans $\mathbb{F}_q[X]$, les facteurs irréductibles de $\overline{\Phi_n}$ ont tous pour degré l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration. Soient P un facteur irréductible de $\overline{\Phi_n}$, on note k_0 son degré, et $k = o(q)$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Si K est un corps de rupture de P sur $\mathbb{F}_q$, on a $K \simeq F_{q^{k_0}}$, et pour $\lambda \in K$ une racine de P. On a

$$(X - \lambda) \mid P \mid \overline{\Phi_n} \mid X^n - 1$$

Donc $o(\lambda) | n$ (ordre de λ dans K^*.
Si $o(\lambda) = q < n$, alors $X - \lambda$ divise $X^q - 1$ et $(X - \lambda)^2 | (X^d - 1)\overline{\Phi_n}$ qui divise $X^n - 1$, donc $X^n - 1$ a une racine double : contradiction, donc λ est d'ordre n.
Or comme $\lambda \in K^*$, $\lambda^{q^{k_0}-1} = 1$, donc n divise $q^{k_0} - 1$: $q^{k_0} \equiv 1[n]$ et k divise k_0.
Réciproquement, regardons $\mathbb{F}_{q^k}$, on a $q^k \equiv 1[n]$, donc n divise $q^k - 1$, donc

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \mid \prod_{d|q^k-1} \Phi_d = X^{q^k-1} - 1$$

Mais $X^{q^k-1} - 1$ est scindé sur $\mathbb{F}_{q^k}$ (construction des corps finis), donc P est scindé sur $\mathbb{F}_{q^k}$. Pour $\lambda \in \mathbb{F}_{q^k}$ une racine du P, on a $\mathbb{F}_q(\lambda) \leqslant \mathbb{F}_{q^k}$. Comme $\mathbb{F}_q(\lambda) \simeq K \simeq \mathbb{F}_{q^{k_0}}$ (degré de P), on a $k_0 \leqslant k$ d'où le résultat. □