Irréductibilité des polynômes cyclotomiques

Références : Perrin, *Cours d'algèbre*, p 82

On rappelle que $\Phi_{n,k}(X) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta)$ où K_n est le corps de décomposition de $X^n - 1$ sur k, $\mu_n(K_n)$ est l'ensemble des racines de l'unité dans K_n (qui est cyclique car sous-groupe de k^* qui est cyclique) et $\mu_n^*(K_n)$ est l'ensemble des racines primitives de l'unité, c'est à dire celles qui engendrent $\mu_n(K_n)$.
On note $\Phi_n = \Phi_{n,\mathbb{Q}}$ pour simplifier.

Proposition.

Les Φ_n sont dans $\mathbb{Z}[X]$.

Démonstration. On fait la démonstration par récurrence forte.
On a $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$.
Au rang n, on pose $F(X) = \prod_{d|n, d \neq n} \Phi_d(X)$. On a $F \in \mathbb{Z}[X]$ par hypothèse.
On rappelle que $X^n - 1 = \prod_{d|n} \Phi_d(X) = \Phi_n(X)F(X)$.
Puis on fait la division euclidienne de $X^n - 1$ par F dans $\mathbb{Z}[X]$ (possible car F unitaire) : $X^n - 1 = F(X)P(X) + R(X)$. Donc $F(X)(\Phi_n(X) - P(X)) = R(X)$ et comme $\deg(R) < \deg(F)$, on a $\Phi_n = P \in \mathbb{Z}[X]$. □

Théorème.

Les polynômes cyclotomiques sont irréductibles dans $\mathbb{Z}[X]$ (et donc dans $\mathbb{Q}[X]$).

Démonstration. • On se donne un nombre premier p ne divisant pas n et ζ une racine primitive de l'unité. On sait que ζ^p est aussi une racine primitive (car ζ^m est primitive ssi $m \wedge n = 1$). On note f et g les polynômes minimaux respectifs de ζ et ζ^p. Ce sont des polynômes de $\mathbb{Q}[X]$. Montrons que f, $g \in \mathbb{Z}[X]$.
On décompose Φ_n en produit d'irréductibles $\Phi_n = f_1 ... f_r$ avec $f_i \in \mathbb{Z}[X]$ (car $\mathbb{Z}[X]$ est factoriel). Comme Φ_n est unitaire, quitte à multiplier les f_i par -1, on peut supposer que les f_i sont unitaires.
$\Phi_n(\zeta) = 0$ donc il existe i_0 tel que $f_{i_0}(\zeta) = 0$. Or f_{i_0} est irréductible et unitaire sur $\mathbb{Z}[X]$, donc sur $\mathbb{Q}[X]$, donc $f = f_{i_0} \in \mathbb{Z}[X]$ et $f | \Phi_n$.
On peut faire le même travail pour montrer que $g \in \mathbb{Z}[X]$ et $g | \Phi_n$.

• Montrons à présent que $f = g$.
Supposons f et g distincts, alors comme ils sont irréductibles, $fg | \Phi_n$ dans $\mathbb{Z}[X]$. D'autre part comme ζ est racine de $g(X^p)$, on a que $f(X) | g(X^p)$ dans $\mathbb{Q}[X]$. Il existe $h \in \mathbb{Q}[X]$ tel que $g(X^p) = f(X)h(X)$. On écrit $h = \frac{a}{b} h'$ avec $h' \in \mathbb{Z}[X]$ de contenu 1, alors comme $g(X^p)$ et $f(X)$ sont unitaires, on a $1 = \frac{a}{b}$ en passant au contenu, ce qui donne $h \in \mathbb{Z}[X]$.
On écrit $g(X) = \sum a_i X^i$, alors en réduisant dans $\mathbb{F}_p$, on a $\overline{g}(X^p) = \sum \overline{a_i} X^{pi} = \overline{g}(X)^p$ par Frobenius.
Soit φ un facteur irréductible de $\overline{f}$, alors comme $\overline{g}^p = \overline{fh}$, φ divise $\overline{g}^p$ et par le lemme d'Euclide [1], φ divise $\overline{g}$.
Comme $fg | \Phi_n$, on a $\overline{f}\,\overline{g} | \overline{\Phi_n}$ sur $\mathbb{F}_p$, donc φ^2 divise $\overline{\Phi_n} = \Phi_{n,\mathbb{F}_p}$. [2] Mais cela est absurde car alors $\Phi_{n,\mathbb{F}_p}$ aurait une racine double dans un corps de décomposition, ce qui est faux par construction des polynômes cyclotomiques.
Donc $f = g$.

• À présent, prenons ζ^m une racine primitive n-ième de l'unité, avec $m = p_1^{\alpha_1} ... p_s^{\alpha_s}$. Par le travail précédent, on a $0 = f(\zeta^{p_1}) = f((\zeta^{p_1})^{p_1}) = ... = f(\zeta^{p_1^{\alpha_1}}) = f((\zeta^{p_1^{\alpha_1}})^{p_2}) = ... = f(\zeta^m)$.
Finalement, f divise Φ_n, il admet toutes les racines primitives n-ièmes de l'unité comme racines et il est unitaire, donc $\Phi_n = f$ et Φ_n est irréductible sur $\mathbb{Q}$. Comme Φ_n est unitaire, son contenu est 1 et il est irréductible sur $\mathbb{Z}$. □

1. Si φ divise $\overline{g}^p$, alors soit φ divise $\overline{g}$, soit il divise $\overline{g}^{p-1}$...
2. On montre ça par récurrence à nouveau. On a $X^n - 1 = \overline{X^n - 1} = \overline{\Phi_n F} = \overline{\Phi_n} F$ (par hypothèse de récurrence). Donc $(\overline{\Phi_n} - \Phi_{n,\mathbb{F}_p})F = 0$ et on a le résultat par intégrité de $\mathbb{F}_p[X]$.

Remarque : • La difficulté de ce développement est de voir dans quoi on fait les divisions euclidiennes ou dans quel ensemble sont les éléments. Je rappelle donc ici (et il faut le dire à l'oral) qu'un polynôme minimal n'a de sens que sur un anneau *principal* (donc pas $\mathbb{Z}[X]$) car il est l'élément engendrant l'idéal annulateur. De même on doit faire nos divisions euclidiennes sur un anneau *euclidien* (et $A[X]$ est euclidien ssi A est un corps). Les divisions euclidiennes sont aussi possibles dans $A[X]$ si on veut diviser par un polynôme **unitaire**. On peut le montrer par récurrence en divisant tout monôme X^n par $P = \alpha X^p + P_0$. On a $X^n = \alpha^{-1} X^{n-p} P - \alpha^{-1} X^{n-p} P_0$ et on s'est ramené à un degré plus faible.
• L'application majeure de ce développement est de montrer que Φ_n est le polynôme minimal de toute racine primitive n-ième de l'unité. On déduit de cela le degré des extensions cyclotomiques et on peut faire de la théorie de Galois avec. On se sert notamment de ce résultat dans la constructibilité des polygones réguliers.