Irréductibilité des polynômes cyclotomiques

Théorème . Soit $\mathbb{K}$ un corps. On considère le corps de décomposition $\mathbb{K}_n$ de X^n-1 sur $\mathbb{K}$. On note $\mu_n(\mathbb{K}_n)$ le groupe cyclique des racines n-ième de l'unité dans $\mathbb{K}_n$ et $\mu_n^*(\mathbb{K}_n)$ l'ensemble des racines primitives n-ième de l'unité, c'est-à-dire qui engendrent $\mu_n(\mathbb{K}_n)$. On définit le n-ième polynôme cyclotomique sur $\mathbb{K}$ par

$$\Phi_{n,\mathbb{K}}(X)=\prod_{\xi\in\mu_n^*(\mathbb{K}_n)}(X-\xi).$$

Alors $\Phi_n=\Phi_{n,\mathbb{Q}}\in\mathbb{Z}[X]$ et il est irréductible dans $\mathbb{Z}[X]$.

Preuve :
On commence par montrer par récurrence que $\Phi_n\in\mathbb{Z}[X]$.
On a $\Phi_1=X-1\in\mathbb{Z}[X]$. Supposons le résultat vrai pour tout $k\in[\![1,n]\!]$ avec $n\geq 1$. On a $\mu_n(\mathbb{Q}_n)=\bigsqcup_{d|n}\mu_d^*(\mathbb{Q}_n)$, donc

$$X^n-1=\prod_{d|n}\Phi_d=\Phi_n\prod_{\substack{d|n\\ d\neq n}}\Phi_d.$$

$\prod_{\substack{d|n\\ d\neq n}}\Phi_d$ étant unitaire dans $\mathbb{Z}[X]$ par hypothèse de récurence, l'unicité de la division euclidienne dans $\mathbb{Q}[X]$ permet de conclure que $\Phi_n\in\mathbb{Z}[X]$.

Pour montrer l'irréductibilité de Φ_n, on va montrer que c'est le polynôme minimal d'une racine primitive n-ième de l'unité.
Soient $\xi\in\mu_n^*(\mathbb{Q}_n)$ et p un nombre premier ne divisant pas n. On sait alors que $\xi^p\in\mu_n^*(\mathbb{Q}_n)$ car $p\wedge n=1$. Soient f et g les polynômes minimaux respectifs de ξ et ξ^p sur $\mathbb{Q}$. On commence par montrer que $f,g\in\mathbb{Z}[X]$.
$\mathbb{Z}[X]$ étant factoriel, on peut décomposer $\Phi_n=\varphi_1\dots\varphi_r$ avec $\varphi_1,\dots,\varphi_r\in\mathbb{Z}[X]$ irréductibles, que l'on peut supposer unitaires car Φ_n l'est. Comme $\Phi_n(\xi)=\Phi_n(\xi^p)=0$, il existe $i,j\in[\![1,r]\!]$ tels que $\varphi_i(\xi)=0$ et $\varphi_j(\xi^p)=0$. Or φ_i et φ_j sont irréductibles sur $\mathbb{Z}[X]$ donc sur $\mathbb{Q}[X]$ et unitaires, on en déduit

$$f=\varphi_i\in\mathbb{Z}[X],\quad g=\varphi_j\in\mathbb{Z}[X]\quad\text{et}\quad f,g|\Phi_n.$$

On montre alors que $f=g$. Supposons par l'absurde $f\neq g$. Alors $fg|\Phi_n$ dans $\mathbb{Z}[X]$. On sait aussi que ξ est une racine de $g(X^p)$, donc f divise $g(X^p)$ dans $\mathbb{Q}[X]$, en tant que polynôme minimal de ξ sur $\mathbb{Q}$, ie $g(X^p)=h(X)f(X)$ avec $h\in\mathbb{Q}[X]$. Or $f(X),g(X^p)\in\mathbb{Z}[X]$ avec f unitaire donc l'unicité de la division euclidienne dans $\mathbb{Q}[X]$ permet de conclure que $h\in\mathbb{Z}[X]$.
On réduit alors le problème modulo p, et on a

$$\bar{h}(X)\bar{f}(X)=\bar{g}(X^p)=\Big(\bar{g}(X)\Big)^p,$$

via le morphisme de Frobenius car l'anneau $\mathbb{F}_p[X]$ est de caractéristique p. Donc $\overline{f}$ divise $\overline{g}^p$ dans $\mathbb{F}_p[X]$.

Soit $\varphi \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{f}$. Or $\overline{f}$ divise $\overline{g}^p$ donc φ divise $\overline{g}^p$. Par le lemme d'Euclide, φ divise $\overline{g}$ ou $\overline{g}^{p-1} = 1$, donc φ divise $\overline{g}$. De plus, $fg|\Phi_n$ dans $\mathbb{Z}[X]$ donc $\overline{f}\overline{g}|\overline{\Phi_n}$ dans $\mathbb{F}_p[X]$, ce qui donne finalement $\varphi^2|\overline{\Phi_n}$. On peut montrer par récurrence $\overline{\Phi_n} = \Phi_{n,\mathbb{F}_p}$. $\Phi_{n,\mathbb{F}_p}$ aurait alors une racine double dans un corps de décomposition, ce qui est impossible par contruction des polynômes cyclotomiques. Donc $f = g$.

Soit ξ^m une racine primitive de l'unité avec $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$. On sait que $m \wedge n = 1$, donc $p_i \wedge n = 1$ pour tout $i \in [\![1, s]\!]$. Par ce qui précède, on a

$$f(\xi) = 0 \implies f(\xi^{p_i}) = 0,$$

on peut donc reconstituer m pour obtenir $f(\xi^m) = 0$. Comme ξ engendre $\mu_n(\mathbb{Q}_n)$, on a $f(\xi) = 0$ pour tout $\xi \in \mu_n^*(\mathbb{Q}_n)$. On a montré $f|\Phi_n$, f unitaire et f admet comme racine toutes les racines primitives n-ième de l'unité, donc $f = \Phi_n$ et ainsi Φ_n est irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.

□