I.E Irréductibilité des polynômes cyclotomique sur $\mathbb{Q}$

Lemme 11:

1) Pour tout $n \in \mathbb{N}^*$, on a $X^n - 1 = \prod_{d|n} \phi_d$
2) Le polynôme ϕ_n est unitaire et à coefficients dans $\mathbb{Z}$ pour tout n
3) Si $P = QR$ avec $P \in \mathbb{Z}[X]$ et $Q, R \in \mathbb{Q}[X]$ unitaires, alors $Q, R \in \mathbb{Z}[X]$

Démonstration.

1) $X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mu_n^*} (X - \zeta) = \prod_{d|n} \phi_d$
2) On procède par récurrence :
si $n = 1$ alors $\phi_1 = X - 1$;
si on suppose le résultat vrai jusqu'au rang $n - 1$ alors, par le premier point :
$$X^n - 1 = \phi_n \prod_{d|n \ , \ d<n} \phi_d$$
Il s'agit de la division euclidienne de $X^n - 1$ par $\prod_{d|n \ , \ d<n} \phi_d$ qui est bien dans $\mathbb{Z}[X]$ unitaire par HR. Donc le quotient est dans $Z[X]$. Et c'est aussi la division euclidienne dans $Q[X]$, mais celle-ci est unique. D'où le deuxième point (le caractère unitaire se voit sur les coefficients dominants).
3) On note q le générateur positif de l'idéal $\{n \in \mathbb{Z} \quad / \quad nQ \in \mathbb{Z}[X]\}$. Alors $qQ \in \mathbb{Z}[X]$ et est primitif par définition de q et car Q est unitaire. En effet si $p|qQ$, alors en particulier en regardant le coefficient dominant $p|q$. Donc $\frac{q}{p}Q \in \mathbb{Z}[X]$ et par minimalité de q, on a donc $p = 1$.
On obtient de même $r \in \mathbb{Z}$ tel que $rR \in \mathbb{Z}[X]$ primitif.
Alors $qrP = qQrR$ et en passant au contenu il vient que $qr \ \mathrm{c}(P) = 1$ donc q et r sont dans $\mathbb{Z}$ inversibles. Ils valent donc tous deux ± 1.

■

Théorème 12:

Pour tout $n \in \mathbb{N}^*$, ϕ_n est irréductible sur $\mathbb{Q}$.

Démonstration. Soit $\zeta \in \mu_n^*$. On va montrer que $\phi_n = \mu_\zeta$

1. Soit $\zeta' \in \mu_n^*$.Alors il existe $m \in \{1, \dots, n-1\}$ premier avec n tel que $\zeta' = \zeta^m$, il s'écrit $m = p_1\alpha_1 \dots p_k\alpha_k$.
Quitte à raisonner par récurrence sur le nombre de diviseurs premiers de m, OPS $m = p$ est premier.
2. Montrons que $\mu_\zeta = \mu_{\zeta^p}$. On note $f = \mu_\zeta$ et $g = \mu_{\zeta^p}$. Alors on a immédiatement que $f|g(X^p)$. Donc il existe $h \in \mathbb{Q}[X]$ tel que $fh = g(X^p)$.
On a de plus que f et g sont à coefficients entiers. En effet, l'anneau $\mathbb{Z}[X]$ est factoriel, donc $\phi_n = f_1\beta_1 \dots f_r\beta_r$ en produit d'irréductibles.
Alors l'un des f_{i_0} annule ζ et est unitaire et irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$. Par minimalité du polynôme minimal, on a donc $f = f_{i_0}$. Il en est de même pour g.

Par le lemme on obtient donc que $h \in \mathbb{Z}[X]$. On a donc $fh = g(x^p)$ dans $\mathbb{Z}[X]$. On peut donc réduire cette équation modulo p.
Supposons que $f \neq g$. Alors f et g sont deux irréductibles distincts divisant ϕ_n, et donc $fg \mid \phi_n$.
Soit φ un diviseur irréductible de $\overline{f}$. Alors $\varphi \mid \overline{fh} = \overline{g(X^p)} = \overline{g(X)}^p$. Donc par le lemme d'Euclide, $\varphi \mid \overline{g}$. On a alors :
$$\varphi^2 \mid \overline{fg} \mid \overline{\phi_n} \mid \overline{X^n - 1}$$
Or le polynôme dérivé de $\overline{X^n - 1}$ est $\overline{nX^{n-1}}$ qui est non nul car p et n sont premiers entre eux. Mais alors 0 est la seule racine de $\overline{nX^{n-1}}$ sans être racine de $\overline{X^n - 1}$. Il n'a donc pas de racine multiple, c'est absurde et donc $f = g$.

3. On a donc $\mu_\zeta = f = g = \mu_{\zeta^m}$ pour tout $1 \leqslant m \leqslant n-1$ premier avec n. Donc μ_ζ admet $\varphi(n) = \deg(\phi_n)$ racines. De plus $\phi_n(\zeta) = 0$ donc ϕ_n est annulateur pour ζ et $\mu_\zeta \mid \phi_n$. Les deux polynômes sont donc associés. Comme de plus ils sont tous deux unitaires, ils sont égaux. Donc ϕ_n est un polynôme minimal et donc il est irréductible.

■