dev: Etude des polynômes cyclotomiques.

Leçons : 123, 141, 102, 144.
réf : Perrin. p82.

thm : Pour $n \geq 1$, on a $\Phi_n(X)$: * $\in \mathbb{Z}[X]$ (et donc irred dans $\mathbb{Q}[X]$)
* irréductible
* unitaire.

dem :

Ne pas faire.

① Dans $\mathbb{Z}[X]$ + unitaire :

Montrons par récurrence sur $n \in \mathbb{N}^*$ que : « $\Phi_n \in \mathbb{Z}[X]$ et Φ_n unitaire »

* ini : $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$ unitaire.
* Hér : Soit $n \in \mathbb{N}^*$. Supposons le résultat acquis pour tout $k < n$.

Par H.R : $F(X) := \prod_{\substack{d \mid n \\ d<n}} \Phi_d(X) \in \mathbb{Z}[X]$ et $F(X)$ est unitaire

Par division euclidienne dans $\mathbb{Z}[X]$ (factoriel) :
$X^n - 1 = F(X)P(X) + R(X)$ $\quad P, R \in \mathbb{Z}[X]$ et $\deg(R) < \deg(F)$.
De plus : $X^n - 1 = \Phi_n(X) F(X)$ dans $\mathbb{C}[X]$.
Donc $F(X)(\Phi_n(X) - P(X)) = R(X)$ $\Rightarrow \deg R < \deg F$
puis $\Phi_n(X) = P(X) \in \mathbb{Z}[X]$ et unitaire.

② irréductible : Soit $n \in \mathbb{N}^*$

Soit $\xi \in \mathbb{U}_n^*$ et soit p un nombre premier ne divisant pas n.
Notons P le polynôme minimal de ξ sur $\mathbb{Q}$ (pol min ξ = ann principal)
Q ______ ξ^p ____ ($\xi^p \in \mathbb{U}_n^*$ car $n \wedge p = 1$).

$Q = P_j$, $P = P_i$

* Par décomposition de Φ_n en produit de facteurs irréductibles dans $\mathbb{Z}[X]$:
$\Phi_n(X) = \prod_{i=1}^{r} P_i(X)^{\alpha_i}$ car $\mathbb{Z}[X]$ factoriel — pas sur $\mathbb{Z}$.

Φ_n est unitaire donc OPS P_i tous unitaire quitte à $\times(-1)$.

$\Phi_n(\xi) = 0$ donc : $\exists i \in [\![1, r]\!]$, $P_i(\xi) = 0$
Comme P_i est irréductible et unitaire, $P = P_i \in \mathbb{Z}[X]$
On a de même pour ξ^p donc $Q = P_j \in \mathbb{Z}[X]$, pour $j \in [\![1, r]\!]$

$Q = P$

* Supposons par l'absurde $P \neq Q$.
P et Q étant irréductible et $P \mid \Phi_n$, $Q \mid \Phi_n$ on a $PQ \mid \Phi_n$.
De plus, $Q(\xi^p) = 0$ donc $Q(X^p)$ annule ξ et $P \mid Q(X^p)$ dans $\mathbb{Q}[X]$
Il existe $(a,b) \in \mathbb{Z}^2$ et $R \in \mathbb{Z}[X]$ tq $c(R) = 1$ et $Q(X^p) = P(X) \frac{a}{b} R(X)$.
a = ppcm et b = pgcd des coeff de R
Par le lemme de Gauss : $c(Q(X^p)) = c(P(X)) \frac{a}{b} c(R(X))$
$1 = \frac{a}{b}$.
Donc $P \mid Q(X^p)$ dans $\mathbb{Z}[X]$.
modulo p, grâce au morphisme de Frobenius : $\overline{P(X)}\,\overline{R(X)} = \overline{Q(X^p)} = \overline{Q(X)}^p$
($\Leftarrow x \mapsto x^p$ est morph (car $\binom{p}{k} = 0$ si $p \neq 1$))

Soit φ un facteur irréductible de $\overline{P}$ dans $\mathbb{F}_p[X]$. On a donc $\varphi \mid \overline{Q}^p$ et par le lemme d'Euclide $\varphi \mid \overline{Q}$.
Comme $PQ \mid \Phi_n$, on a $\varphi^2 \mid \overline{\Phi_n}$.
Ainsi dans $\mathrm{Dec}_{\mathbb{F}_p}(\Phi_n)$, $\overline{\Phi_n}$ admet une racine double, donc $X^n - 1$ également : ABSURDE. $\Phi_n \times F(X)$
On en conclut que $\boxed{P = Q}$.
$\Leftarrow \varphi \mid \Phi_n$ de admet 1 rac car corps de décompo $\Rightarrow \varphi^2$ admet rac double.

* Soit $\xi' \in \mathbb{U}_n^*$: $\exists m \in [\![1, n]\!]$, $m \wedge n$, $\xi^m = \xi'$
On décompose m en facteur premier $m = \prod_{i=1}^{s} p_i^{\beta_i}$.

En utilisant le point précédent, on obtient par récurrence que ξ^m a le même polynôme minimal que ξ, i.e. P détail →

ζ, ζ^{p_1} $\tilde{m}$ pol min.

$\dots$, $\zeta^{p_1}, \zeta^{p_1p_2}$ $\tilde{m}$ pol min $\rightsquigarrow$ $\tilde{m}$ que ζ par ... point précédent avec $\zeta = \zeta^{p_1}$ et $p = p_2$

$\zeta^{p_1 \cdots p_{r-1}}, \zeta^{p_1 \cdots p_r}$ $\tilde{m}$ pol min $\rightsquigarrow$

Tous les éléments de $\mathbb{U}_n^*$ sont donc racines de P, d'où $P \mid \Phi_n$ puis $P = \Phi_n$.

P étant irréductible, Φ_n l'est également sur $\mathbb{Q}$