Irréductibilité de Φ_n [Per] p 83.

Th : $\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta)$ est irréd ds $\mathbb{Z}[X]$.

Dém :
Soit $\zeta \in \mu_n^*$ et f son polyn min sur $\mathbb{Q}$.
A voir : 1) f est irréd ds $\mathbb{Z}[X]$
2) f est le polyn min sur $\mathbb{Q}$ de tt les racines n-ième prim de 1.
Ccl : $\deg \Phi_n = \varphi(n) \leq \deg f$ mais $f \mid \Phi_n$ donc $\Phi_n = f$ (ils st unitaires) et donc Φ_n est irréd ds $\mathbb{Z}[X]$.

---

1) On décompose Φ_n ds $\mathbb{Z}[X]$ (anneau fact) :
$\Phi_n = \prod_{i=1}^{r} f_i^{\alpha_i}$ avec f_i unit et irréd ds $\mathbb{Z}[X]$.
Il existe alors $i \in \{1, \dots, r\}$ tq $f_i(\zeta) = 0$ donc $f_i = f$ (f_i est unitaire, irréd ds $\mathbb{Q}[X]$ et annule ζ) et donc f est irréd ds $\mathbb{Z}[X]$.
N.B : $f \mid \Phi_n$ ds $\mathbb{Z}[X]$.

2) $\mu_n^* = \{\zeta^m \mid m = \prod_{i=1}^{r} p_i^{\alpha_i} \in \{1, \dots, n\}$ et $p_i \nmid n\}$ donc il suffit de mq f est le polyn min sur $\mathbb{Q}$ de ζ^p pour tt p premier ne divisant pas n (car alors, f est le polyn min sur $\mathbb{Q}$ de $\zeta^{p^2}, \dots$)
Soit donc un tel p.
On note g le polyn min de ζ^p sur $\mathbb{Q}$.
Par l'abs, on supp que $g \neq f$.
Alors, $fg \mid \Phi_n$ ds $\mathbb{Z}[X]$ (d'après 1), g est irréd ds $\mathbb{Z}[X]$ et $g \mid \Phi_n$ ds $\mathbb{Z}[X]$) donc $\overline{f}\,\overline{g} \mid \overline{\Phi_n}$ ds $\mathbb{F}_p[X]$.

On considère un fact iréd φ de f ds $\mathbb{F}_p[x]$.
On rq que $\varphi \mid \overline{g}$ ds $\mathbb{F}_p[x]$. En effet, f est racine de $g(x^p)$ donc $f \mid g(x^p)$ ds $\mathbb{Q}[x]$ et ℓn ds $\mathbb{Z}[x]$ ie $g(x^p) = fh$ avec $h \in \mathbb{Z}[x]$ (si $h \in \mathbb{Q}[x]$, $h = \frac{a}{b} h'$ avec $h' \in \mathbb{Z}[x]$ primitif et $\frac{a}{b} \in \mathbb{Q}$ donc $b\, g(x^p) = a f h'$ et donc $b = a$ d'après le lemme de Gauss).
et donc $\overline{g}^p = \overline{f}\,\overline{h}$ ds $\mathbb{F}_p[x]$ ($\overline{g(x^p)} = \overline{g(x)}^p$ d'après Frobenius) d'où la rq moyennant le lemme d'Euclide.
Finalt, $\varphi^2 \mid \overline{\Phi_n}$ ds $\mathbb{F}_p[x]$ donc $\overline{\Phi_n}$ possède une racine double ds son corps de décomp sur $\mathbb{F}_p$ et donc $p \mid n$

Exple : $\Phi_8 = X^4 + 1$ est iréd ds $\mathbb{Z}[x]$ mais réd ds $\mathbb{F}_p[x]$ pour tt p 1er.

Dém :
$p = 2$: $X^4 + 1 = (X+1)^4$ d'après Frobenius.
$p > 2$: Il suffit de mq $X^4 + 1$ a une racine ds $\mathbb{F}_{p^2}$ ou encore que $\mathbb{F}_{p^2}$ a un élt d'ordre 8 (si x est un tel élt, $x^8 - 1 = 0$ et $x^4 - 1 \neq 0$ mais $x^8 - 1 = (x^4+1)(x^4-1)$ donc $x^4 + 1 = 0$).
Or, $\mathbb{F}_{p^2}^*$ est cyclique d'ordre $p^2 - 1$ et $8 \mid p^2 - 1$ ($p^2 - 1 = (p-1)(p+1)$ et $p-1, p+1$ sont 2 nbres pairs consécutifs donc l'un des 2 est multiple de 4) donc $\mathbb{F}_{p^2}^*$ a un élt d'ordre 8.