Théorème: $\forall m \in \mathbb{N}^*$, Φ_m est irréductible sur $\mathbb{Z}[X]$.

(**Def:** $U_m = \{z \in \mathbb{C} \mid z^m = 1\} \supseteq P_m(\mathbb{C}) = \{\exp(\frac{2i\pi k}{m}) \mid k \wedge m = 1, k \in [\![1, m]\!]\}$. $P_m(\mathbb{C})$ est l'ensemble des racines primitives m-ièmes de l'unité.)

Lemme 1: $\forall m \in \mathbb{N}^*$, $X^m - 1 = \prod_{d \mid m} \Phi_d(X)$.

Lemme 2: Soient $P, A, B \in \mathbb{Q}[X] \setminus \{0\}$, $P \in \mathbb{Z}[X]$, $P = AB$, P et A unitaires. Alors, $A, B \in \mathbb{Z}[X]$.

Preuve théorème: On va procéder en 5 étapes :

Étape 1: $\Phi_m(X) \in \mathbb{Z}[X]$. Procédons par récurrence :

- $m = 1$: $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. ok

- Supposons la prop vraie jusqu'au rang $n-1 \geq 1$.

Soit $F(X) = \prod_{\substack{d \mid m \\ d \neq m}} \phi_m(X)$. Alors, $F(X) \in \mathbb{Z}[X]$ par hypothèse de récurrence et est unitaire. $\forall m \in \mathbb{N}^*$, $\phi_m(X) = \prod_{\xi} (X - \xi)$ avec ξ racine primitive m-ième de l'unité.

De plus, par **Lemme 1**, $\Phi_m(X) F(X) = X^m - 1 \Rightarrow \Phi_m(X) \in \mathbb{Q}[X]$ par unicité de la division euclidienne de $X^m - 1$ par F et par **lemme 2**, $\phi_m(X) \in \mathbb{Z}[X]$ dans $\mathbb{C}[X]$

↙ Si la division euclidienne était différente dans $\mathbb{Q}[X]$, on aurait 2 division euclidienne dans $\mathbb{C}[X]$ → Contradiction.

Étape 2. Soit $\omega = \exp(\frac{2i\pi}{m}) \in P_m(\mathbb{C})$ et soit $f(X)$ son polynôme minimal unitaire sur $\mathbb{Q}[X]$. ($\exists$ car $\mathbb{Q}[X]$ euclidien et $\omega^m - 1 = 0$)

Alors, $f \mid X^m - 1 \Rightarrow \exists h(X) \in \mathbb{Q}[X]$ tel que $X^m - 1 = f(X)h(X)$ et $h(X) \in \mathbb{Q}[X]$ unitaire. $X^m - 1 \in \mathbb{Z}[X]$ donc par **Lemme 2**, $f(X), h(X) \in \mathbb{Z}[X]$.

Étape 3: - Montrons que si $f(\omega) = 0$ et p premier, $p \nmid m$, alors ω^p racine de f.

On a $f \mid X^m - 1 \Rightarrow \omega^m - 1 = 0$ et ω est une racine m-ième de l'unité dans $\mathbb{C}$. Ainsi, $(\omega^p)^m - 1 = \underbrace{(\omega^m)^p}_{=1} - 1 = 0 = f(\omega^p) h(\omega^p)$. Supposons $f(\omega^p) \neq 0$, alors $h(\omega^p) = 0$. (car $\mathbb{C}$ est intègre) Or, f étant irréductible sur $\mathbb{Q}[X]$, $f(X) \mid h(X^p)$ dans $\mathbb{Q}[X]$ et $\exists P(X) \in \mathbb{Q}[X]$ tel que $h(X^p) = f(X)P(X)$ et par le **Lemme 2**, vu que $h(X^p) \in \mathbb{Z}[X]$, $P(X) \in \mathbb{Z}[X]$.

- On se place à présent dans $\mathbb{F}_p$. On a alors $(\bar{h}(X))^p = \bar{h}(X^p) = \bar{f}(X)\bar{g}(X) \in \mathbb{F}_p[X]$. Soit $\bar{\theta}$ un facteur irréductible de $\bar{f}$, alors $\bar{\theta} \mid \bar{h}$ et

$$(\bar{h}(X))^p = \left(\sum_{i=0}^{m} \bar{\lambda}_i X^i\right)^p = \left(\sum_{i=0}^{m-1} \bar{\lambda}_i X^i + \bar{\lambda}_m X^m\right)^p = \sum_{k=0}^{p} \binom{p}{k} \left(\sum_{i=0}^{m-1} \bar{\lambda}_i X^i\right)^k (\bar{\lambda}_m X^m)^{p-k} = \bar{\lambda}_m^p X^{mp} + \left(\sum_{i=0}^{m-1} \bar{\lambda}_i X^i\right)^p = \bar{h}(X^p)$$

par itérations successives.

$\bar{\lambda}_m^p = \bar{\lambda}_m$ car on est dans $\mathbb{F}_p$ et p premier $\Rightarrow \binom{p}{k} = 0 \; \forall k \in [\![1, p-1]\!]$

$\overline{Q}^2 \mid \overline{fh} = X^m - \overline{1}$. Donc, $\exists \widetilde{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$ où $X^m - \overline{1}$ possède une racine double → Absurde car $X^m - \overline{1}$ premier avec sa dérivée

$\overline{m} X^{m-1}$ dans $\mathbb{F}_p[X]$. ($\frac{1}{\overline{m}} \times \overline{m} X^{m-1} - (X^m - \overline{1}) = \overline{1}$ et on conclut par Bézout) Donc, $f(\omega^k) = 0$.
↳ $\neq \overline{0}$ car $p \nmid m$

Étape 4: À présent, on sait que $\forall \xi_j \in \mu_m(\mathbb{C})$, $\exists k \in [\![1, m]\!]$ tel que $\xi_j = \omega^k$ avec $k = \prod_{i=1}^{n} p_i$, les p_i des facteurs premiers ne divisant pas m. Alors, par récurrence, on obtient $f(\xi_j) = f(\omega^k) = 0$ grâce à l'étape 3 $\forall \xi_j \in \mu_m(\mathbb{C})$.

Étape 5: $|\mu_m(\mathbb{C})| = \varphi(m)$ donc $\deg(f) \geq \varphi(m)$. On a $f \mid \Phi_m$ et $\deg(\Phi_m) = \varphi(m)$. Les 2 étant unitaires, $f = \Phi_m$ et Φ_m irréductible sur $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$ car unitaire. □

Preuve Lemme 2: On a forcément B unitaire. Notons $A(X) = X^m + \sum_{i=0}^{m-1} \frac{p_i}{q_i} X^i$, $p_i \in \mathbb{Z}$, $q_i \in \mathbb{N}^*$ premiers entre eux. Soit $q = \operatorname{ppcm}_i(q_i)$, alors $A(X) = X^m + \frac{1}{q} \sum_{i=0}^{m-1} z_i X^i$, $z_i \in \mathbb{Z}$. Quitte à diviser $z_0, \dots, z_{m-1}, q$ par $\operatorname{PGCD}_i(z_i, q)$, on considère $\operatorname{PGCD}_i(z_i, q) = 1$. Posons $A_1(X) = qA(X) \in \mathbb{Z}[X] \setminus \{0\}$, $A_1(X) = qX^m + \sum z_i X^i$

$c(A_1) = 1$. De la même manière, $\exists n \in \mathbb{N}^*$ tq $B_1(X) = nB(X) \in \mathbb{Z}[X]$ et $c(B_1) = 1$. Alors, $qnP = A_1 B_1$ et $qn\, c(P) = c(A_1)c(B_1)$ par le lemme de Gauss.

Enfin, $qn = 1 \Rightarrow q = n = 1$ car $q, n \in \mathbb{N}^*$. Donc, $A_1 = A$, $B_1 = B$ et $A, B \in \mathbb{Z}[X]$. □

Preuve Lemme 1: Si $d \mid m$, $P_d(\mathbb{C}) \subseteq U_d(\mathbb{C}) \subseteq U_m(\mathbb{C})$. $\forall \xi_j \in U_m(\mathbb{C})$, $|\langle \xi_j \rangle| \mid m$ par le théorème de Lagrange. Donc, ξ_j appartient à un unique $P_d(\mathbb{C})$ par unicité de l'ordre. Ainsi, $U_m(\mathbb{C}) = \bigsqcup_{d \mid m} P_d(\mathbb{C})$ et $X^m - 1 = \prod_{d \mid m} \Phi_d(X)$ par définition. □
↳ annule $U_m(\mathbb{C})$

Référence: Théorie de Galois, Ivan Gozard

Leçons: 141 - 102 - 122 - 125
↳ on utilise la division euclidienne dans $\mathbb{C}[X]$ et $\mathbb{Q}[X]$ ainsi que son unicité dans ces anneaux (ce qui n'est pas toujours le cas !!!), le fait que k corps ⇒ k[X] euclidien, Bézout, l'existence du polynôme minimal annulateur. Bref, ça se défend très bien.

Remarques:
- Faire uniquement le théorème et le lemme 1 ou 2 si le temps le permet.
- Dans une leçon, il vaut mieux définir $U_m(\mathbb{C})$ et $P_m(\mathbb{C})$ avant pour ne pas perdre de temps.