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

preuve : En mettant au même dénominateur les coefficients, $\exists m \in \mathbb{N}^*$ tq $A = \frac{1}{m} A_1$ et $B = \frac{1}{m} B_1$, avec $A_1, B_1 \in \mathbb{Z}[X]$ de coefficient dominant égal à m (A et B sont unitaires)

donc $m^2 A.B = A_1 B_1$. Par le Lemme de Gauss et homogénéité du PGCD, $\text{cont}(m^2 AB) = m^2 \times 1 = \underbrace{\text{cont}(A_1).\text{cont}(B_1)}_{\text{divisent } m.}$ (AB est unitaire ↓ ; coef dominant)

donc $m = \text{cont}(A_1) = \text{cont}(B_1)$ i.e m divise tous les coefficients de A_1 et B_1 donc $A = \frac{1}{m} A_1 \in \mathbb{Z}[X]$ et aussi B.

□

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

preuve : Soit $\omega \in \mathbb{C}$ une racine m-ième primitive de 1. On note f son polynôme minimal sur $\mathbb{Q}[X]$. Par définition, $\exists h \in \mathbb{Q}[X]$, $f(X).h(X) = X^m - 1$.
Puisque $X^m - 1 \in \mathbb{Z}[X]$ et que f est unitaire, par le Lemme f et $h \in \mathbb{Z}[X]$. (h est évidemment unitaire)

- Mq si $f(u) = 0$ et p premier tq $p \nmid m$, alors $f(u^p) = 0$:

On a alors $u^m - 1 = 0$ et donc : $0 = (u^m)^p - 1 = (u^p)^m - 1 = f(u^p) h(u^p)$
si $f(u^p) \neq 0$, alors $h(u^p) = 0$ et u étant racine de $f \in \mathbb{Q}[X]$ irréductible unitaire, f est son polynôme minimal et $f(X) \mid h(X^p) \in \mathbb{Z}[X]$: $\exists g \in \mathbb{Q}[X]$, $h(X^p) = f(X).g(X)$.
et là encore par le Lemme, $g \in \mathbb{Z}[X]$.
En réduisant mod p : (*) caractéristique p
$\bar{h}(X)^p \overset{(*)}{=} \bar{h}(X^p) = \bar{f}(X).\bar{g}(X)$ dans $\mathbb{F}_p[X]$. Soit $\theta \in \mathbb{F}_p[X]$ un facteur irréductible de $\bar{f}$ on a θ^2 qui divise $\bar{f}.\bar{h} = \bar{f}.\bar{h} = X^m - \bar{1}$.
Ainsi dans le corps de décomposition de $X^m - \bar{1}$, celui-ci admet une racine double.
ce qui est impossible car son polynôme dérivé est $\bar{m} X^{m-1}$ et annule seulement 0 (car $p \nmid m$)
Ainsi $f(u^p) = 0$.

- Mq $f = \Phi_m$: $f(\omega) = 0$ et tout élément de μ_m peut être obtenu par élévations successives de ω à des puissances p premier tq $p \nmid m$ (1) on a alors montré que tout élément de μ_m est racine de f et donc $\varphi(m) \leq \deg(f)$ et $f \mid \Phi_m$ dans $\mathbb{Q}[X]$ et sont unitaires donc $f = \Phi_m$ est irréductible sur $\mathbb{Q}[X]$.

□

À ajouter pour la leçon PPCM, PGCD :

Lemme de Gauss : Soient $A, B \in \mathbb{Z}[X] \setminus \{0\}$ on a $\text{cont}(AB) = \text{cont}(A).\text{cont}(B)$.

preuve :

- cas où A, B primitifs : Si $\text{cont}(AB) \neq 1$ soit p premier divisant tous les coefficients de AB.

On a alors $\overline{AB} = \bar{A}.\bar{B} = \bar{0}$ dans $\mathbb{F}_p[X]$ intègre donc $\bar{A}$ ou $\bar{B} = \bar{0}$ i.e p divise tous les coefficients de A ou ceux de B : donc A ou B est non primitif. Par contraposée on a le résultat.

- cas général : On a $A.B = \text{cont}(A).\text{cont}(B).\underbrace{\frac{A}{\text{cont}(A)}}_{\text{primitif par le cas 1)}}.\frac{B}{\text{cont}(B)}$ donc $\text{cont}(A.B) = \text{cont}(A)\,\text{cont}(B).1$ par homogénéité du PGCD.

□

À ajouter dans "extension de corps" :

Corollaire : Soit $n \in \mathbb{N}^*$, Le polynôme minimal de toute racine primitive n-ième de l'unité dans $\mathbb{C}$ est Φ_n.
En particulier $\forall \omega \in \mu_n$, $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$.

preuve : $\forall \omega \in \mu_n$, Φ_n est irréductible dans $\mathbb{Q}[X]$, unitaire et annule ω donc Φ_n est son polynôme minimal.
On sait que $\deg(\Phi_n) = \varphi(n)$ et que $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\Phi_n)$ d'où le résultat. □

Notations : Soit $n \in \mathbb{N}^*$, $\mathbb{U}_n := \{z \in \mathbb{C} \mid z^n = 1\}$ et $\mu_n = \{\omega \in \mathbb{U}_n \mid \langle \omega \rangle = \mathbb{U}_n\}$ les racines n-ièmes primitives de l'unité.
$\Phi_n(X) := \prod_{\omega \in \mu_n} (X - \omega)$. On prend pour acquis que $\Phi_n \in \mathbb{Z}[X]$ (récurrence en utilisant $X^n - 1 = \prod_{d \mid n} \Phi_d$ et la pseudo division euclidienne dans $\mathbb{Z}[X]$)

(1) Soit $\omega \in \mu_n$ et $\alpha \in \mu_n$. On sait que $\exists k \in [\![1;n]\!]$ tq $\alpha = \omega^k$. De plus, $k \wedge n = 1$:
$\alpha \in \mu_n$ donc $\exists u \in \mathbb{Z}$; $\alpha^u = \omega$ donc $\omega^{k.u} = \omega$ et ω est d'ordre n donc, $n \mid ku - 1$ et donc
$\exists v \in \mathbb{Z}$; $nv = ku - 1$ et $1 = ku - nv$ donc $k \wedge n = 1$.
Donc $k = \prod_{i=1}^{s} p_i^{\alpha_i}$ où p_i est premier ne divisant pas n et $\alpha_i \geq 1$ $\forall i$ (ou $k = 1$ mais dans ce cas $\omega = \mu$ est racine de f)

et on a $\omega^{p_i} \in \mu_n$ on reprend avec $\tilde{\omega} = \omega^{p_i}$ racine de f et on a $\tilde{\omega}^{p_i} \in \mu_n$ racine de f etc
on obtient $\omega^{p_i^{\alpha_i}} \in \mu_n$ est racine de f et on recommence ... on a $\omega^{p_1^{\alpha_1} \cdots p_s^{\alpha_s}} = \omega^k = \mu$ est racine de f.

On peut en déduire le Thm de dirichlet faible : $\forall n \in \mathbb{N}^*$, il existe une infinité de nombres premiers p congrus à 1 modulo n

preuve : Soit $k > n$, mq il existe $p > k$ premier tq $p \equiv 1 [n]$:

On considère $\Phi_n(k!)$. Soit p premier divisant $\Phi_n(k!)$. Puisque $\Phi_n(0) \in \mathbb{Z}$ et de module 1, $\Phi_n(0) = \pm 1$ donc

$p \nmid k!$. En particulier $\boxed{p > k > n}$ et $p \wedge n = 1$. Mq $p \equiv 1 [n]$ revient à dire $n \mid p - 1$ et donc suffit de trouver $x \in \mathbb{F}_p^*$ d'ordre n. prenons $x = \overline{k!}$.

On a $\overline{\Phi_n}(x) = \overline{\Phi_n(k!)} = \bar{0}$ donc $x^n - \bar{1} = \bar{0}$ donc si ω est l'ordre de x dans $\mathbb{F}_p^*$, $\omega \mid n$.

Si $\omega < n$, $x^\omega - \bar{1} = \bar{0}$ donc $\exists d \mid \omega$ tq $\overline{\Phi_d}(x) = 0$ (donc $d < n$)

or, $\Phi_d \cdot \Phi_n \mid X^n - 1$ donc x serait dans $(\mathbb{F}_p[X])$ racine double de $X^n - \bar{1}$: absurde. Donc $\omega = n$. □

(*) pour les futés qui auraient remarqué que peut être $\Phi_n(k!) = \pm 1$ et que donc il n'existerait pas de nombre premier p le divisant :

$\{k > n \mid \Phi_n(k!) = \pm 1\}$ est fini car sinon $\Phi_n - 1$ ou $\Phi_n + 1$ aurait une infinité de racines et serait nul : impossible.

Donc on reprend la preuve pour k assez grand.