Lemme. *Soit A un anneau factoriel. Pour $P \in A[X]$ on définit $c(P)$ un PGCD des coeffcients de P. Alors pour tout $P,\ Q \in A[X]$, $c(PQ) = c(P)c(Q)$*

Démonstration. *supposons $c(P) = c(Q) = 1$ et par l'absudre que $c(PQ) \neq 1$. Alors il existe $\pi \in A$ irréductible (car A factoriel) qui divise tous le coefficients de PQ. On note $P = \sum_{i=0}^{d_P} p_i X^i$ et $Q = \sum_{j=0}^{S} q_j X^j$. Comme $cP) = c(Q) = 1$ il existe $i_0 \in \{0, ..., d_P\}$ et $j_0 \in \{0, ..., d_q\}$ tels que pour tout $i < i_0,\ j < j_0,\ \pi | p_i,\ \pi | q_j,\ \pi \nmid p_{i_0},\ \pi \nmid q_{j_0}$. Par hypothèse $\pi | \sum\limits_{i+j=i_0+j_0} p_i q_j = p_{i_0} q_{j_0} + \sum p_i q_j$ Donc $\pi | p_{i_0} q_{j_0}$ et comme π est irrréductible, $\pi | p_{i_0}$ ou $\pi | q_{j_0}$, contradtiction avec la définition de i_0 et j_0.*

Si P et Q sont quelconques, on peut écrire $P = c(P)\tilde{P}$ et $Q = c(Q)\tilde{Q}$ avec $c(\tilde{P}) = c(\tilde{Q}) = 1$. On a montré $c(\tilde{P}\tilde{Q}) = 1$ et on a $PQ = c(P)c(Q)\tilde{P}\tilde{Q}$ donc $c(PQ) = c(P)c(Q)c(\tilde{P}\tilde{Q}) = c(P)c(Q)$

théorème. *$\forall n \in \mathbb{N}$, $\Phi_n \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}$*

Démonstration.

- *Voyons d'abord $\Phi_n \in \mathbb{Z}[X]$ par récurrence sur $n \in \mathbb{N}^*$.*
  - *$\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$*
  - *Supposons que pour tout $m \leq n$, $\Phi_m \in \mathbb{Z}[X]$. Alors $Q = \prod\limits_{d|n+1,\ d<n+1} \Phi_d \in \mathbb{Z}[X]$ et Q est unitaire.*

    Donc par la division euclidienne dans $\mathbb{Z}[X]$ Il existe $P, R \in \mathbb{Z}[X]$ tels que $X^{n+1} - 1 = PQ + R$ er $deg(R) < deg(Q)$. Or $X^{n+1} = \Phi_{n+1} Q$ Donc en faisant la différence des expressions il vient : $R = Q(\Phi_{n+1} - P)$. On a donc $deg(R) = deg(Q) + deg(\Phi_{n+1} - P) > deg(R) + deg(\Phi_{n+1} - P)$ donc $deg(\Phi_{n+1} - P) < 0$, $\Phi_{n+1} = P \in \mathbb{Z}[X]$ ce qui achève la récurrence.
- *Voyons que Φ_n est irréductible en montrant que c'est le polynôme minimal de $\xi_n = e^{\frac{2i\pi}{n}}$.*

  Soit p premier ne divisant pas n. On a alors $\xi_n^p \in \mu_n^*$. Par factorialité de $\mathbb{Z}[X]$ il existe $P_1, ..., P_k$ k polynômes irréductibles unitaires (car Φ_n l'est) de $\mathbb{Z}[X]$ et $\alpha_1, ..., \alpha_k \in \mathbb{Z}$ tels que $\Phi_n = P_1^{\alpha_1} ... P_k^{\alpha_k}$. Comme ξ_n et $\xi_n^p \in \mu_n^*$ on a $\Phi_n(\xi_n) = \Phi_n(\xi_n^p) = 0$, donc il existe $i, j \in \{1, ..., k\}$ tels que $P_i(\xi_n) = P_j(\xi_n^p) = 0$. Comme P_i et P_j sont unitaires et irréductibles sur $\mathbb{Z}$ ils sont aussi irréducibles sur $\mathbb{Q}$ donc ce sont les polynômes minimaux de ξ_n et ξ_n^p respectivement.

  Supposons $P_i \neq P_j$. On a $P_i, P_j |$ Phi_n dans $\mathbb{Z}[X]$. D'autre part $P_j(X^p)$ annule ξ_n donc $P_i(X) | P_j(X^p)$ dans $\mathbb{Q}[X]$. Il existe $H \in \mathbb{Q}[X]$ tel que $P_j(X^p) = P_i(X)H(X)$.

  Comme $H \in \mathbb{Q}[X]$ il existe $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*,\ h \in \mathbb{Z}[X]$ tel que $c(h) = 1$ et $H = \frac{a}{b}h$.

  Ainsi $P_j(X^p) = P_i(X)\frac{a}{b}h(X)$ et on a

  $$1 = c(P_j(X^p)) = c(\frac{a}{b}c(P_i(X)h(X)) = \frac{a}{b}c(P_i(X))c(h(X)) = \frac{a}{b}$$

  Donc $P_i(X) | P_j(X^p)$ dans $\mathbb{Z}[X]$. Modulo p, par le morphisme de Frobenius il vient

  $$\overline{P_i(X)h(X)} = \overline{P_j(X^p)} = \overline{P_j(X)}^p$$

  Soit φ un facteur irréducible de $\overline{P_i}$ dans $\mathbb{F}^p$. Alors par la relation précédente φ est un facteur irréductible de $\overline{P_j}$. Comme $P_i | \Phi$ et $P_j | \Phi$ on a $\varphi^2 | \overline{\Phi}$. Ainsi dans un corps de décomposition K $\overline{\Phi}$ admet une racine double. Or $\Phi_n | X^n - 1$, $\overline{\Phi_n} | \overline{X^n - 1}$ et $\overline{X^n - 1}$ n'a que des racines simples dans K. En effet $(\overline{X^n - 1})' = n\overline{X}^{n-1}$ qui n'admet que 0 comme racine car K est de caractéristique p et p et n sont premiers entre eux, 0 n'est pas racine de $\overline{X}^n - 1$. On a donc $P_i \neq P_j$ implique $\overline{\Phi}$ a un facteur irréductible carré modulo p or $\overline{\Phi}$ n'a que des racines simples, contradiction. Forcément $P_i = P_j$

  Par une récurrence immédiate, pour tout $k \leq n$ premier à n, le polynome minimale μ_{ξ_n} de ξ_n est le polynome minimale de ξ^k. En particulier toutes les racines primitives n ième de l'unité annulent μ_{ξ_n} donc $\Phi_n | \mu_{\xi_n}$. Comme $\Phi_n(\xi_n) = 0$, $\mu_{\xi_n} | \Phi_n$. Comme les deux polynomes sont unitaire, $\Phi_n = \mu_{\xi_n}$