Perrin 34-10 — Irréductibilité des cyclotomiques sur $\mathbb{Z}$ — 102, 141.

Théorème : $\forall n \in \mathbb{N}^*$, $\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi)$ est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.

Lemme. $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.

Par récurrence forte, $\Phi_1 = X - 1 \in \mathbb{Z}[X]$ et si $\forall k < n$, $\Phi_k \in \mathbb{Z}[X]$, alors
$F = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d \in \mathbb{Z}[X]$ est unitaire et $\Phi_n F = X^n - 1$ (car $\mu_n = \bigsqcup_{d \mid n} \mu_d^*$)
La div eucl dans $\mathbb{Z}[X]$ par F unitaire est licite et $X^n - 1 = PF + R$.
avec $P, F \in \mathbb{Z}[X]$, $\deg R < \deg F$.
Par unicité dans $\mathbb{C}[X]$, $P = \Phi_n$, $R = 0$. $\Phi_n \in \mathbb{Z}[X]$.

Rq : Si $\xi \in \mu_n^*$ et $p \nmid n$, alors $\xi^p \in \mu_n^*$. On note $\omega = \xi^p$.
Soient Π_ξ, Π_ω polynômes minimaux de ξ, ω sur $\mathbb{Q}$.
$\mathbb{Z}[X]$ est factoriel (car $\mathbb{Z}$ euclidien donc factoriel), donc $\Phi_n = \prod_{i=1}^{r} F_i^{\alpha_i}$ avec F_i irréd. dans $\mathbb{Z}[X]$. Puisque Φ_n est unitaire, on peut supposer les F_i unitaires.
De plus, $\Phi_n(\xi) = \Phi_n(\omega) = 0$ donc par irréductibilité, $\Pi_\xi = F_{i_0}$, $\Pi_\omega = F_{i_1}$.
Ainsi, $\Pi_\xi, \Pi_\omega \in \mathbb{Z}[X]$, $\Pi_\xi, \Pi_\omega \mid \Phi_n$.

Supposons par l'absurde $\Pi_\xi \neq \Pi_\omega$.
Par irréductibilité, $\Pi_\xi \Pi_\omega \mid \Phi_n$ dans $\mathbb{Z}[X]$.
D'autre part, $\Pi_\omega(\omega) = \Pi_\omega(\xi^p) = 0$ donc $\Pi_\xi(X) \mid \Pi_\omega(X^p)$: $\exists Q \in \mathbb{Q}[X]$, $\Pi_\omega(X^p) = \Pi_\xi(X) Q(X)$
$\Pi_\xi \in \mathbb{Z}[X]$ unitaire donc par division euclidienne, $\Pi_\omega(X^p) = \Pi_\xi(X) S(X) + R(X)$
et par unicité dans $\mathbb{Q}[X]$, $S = Q$, $R = 0$. De là, $\Pi_\xi(X) \mid \Pi_\omega(X^p)$ dans $\mathbb{Z}[X]$

· Dans $\mathbb{F}_p$, le morphisme de Frob fournit $\overline{\Pi_\xi}(X) \mid \overline{\Pi_\omega}(X)^p$
Soit A facteur irréductible de $\overline{\Pi_\xi}$ dans $\mathbb{F}_p[X]$: $A \mid \overline{\Pi_\xi}$ donc $A \mid \overline{\Pi_\omega}^p$
donc $A \mid \overline{\Pi_\omega}$.

· De plus, $\Pi_\omega \Pi_\xi \mid \Phi_n$, donc $\overline{\Pi_\omega}\,\overline{\Pi_\xi} \mid \overline{\Phi_n}$ donc $A^2 \mid \overline{\Phi_n}$ donc $A^2 \mid \overline{X^n - 1}$
$\exists B \in \mathbb{F}_p[X]$, $A^2 B = \overline{X^n - 1}$ donc en dérivant $\overline{n X^{n-1}} = A(2A'B + AB')$.
Donc $\begin{cases} A \mid \overline{n X^{n-1}} \\ A \mid \overline{n} X^n - \overline{n} \end{cases}$ donc $A \mid \overline{n}$ i.e. $\deg A = 0$ donc A inversible
$\neq 0$ car $p \nmid n$ car $\mathbb{F}_p$ corps. **absurde** : $\Pi_\xi = \Pi_\omega$

Ainsi ★ tout élément de μ_n^* est racine de Π_ξ : $\deg \Pi_\xi \geq \varphi(n) = \deg \Phi_n$.
Or $\Pi_\xi \mid \Phi_n$, donc étant unitaires, $\Pi_\xi = \Phi_n$.

verso

(*)

Par récurrence sur s, montrons que :

$\forall \alpha$ racine de π_ξ, $\forall p_1, \dots, p_s$ premiers tq $(p_1 \cdots p_s) \wedge n = 1$, $\pi_\xi(\alpha^{p_1 \cdots p_s}) = 0$.

- $s = 1$: vu ci-dessus

- $s > 1$: $(p_1 \cdots p_s) \wedge n = 1$ donc $(p_1 \cdots p_{s-1}) \wedge n = 1$ donc $\pi_\xi(\alpha^{p_1 \cdots p_{s-1}}) = 0$.

  De même $p_s \wedge n = 1$ donc si $\pi_\xi(\beta) = 0$, $\pi_\xi(\beta^{p_s}) = 0$.

  On conclut pour $\beta = \alpha^{p_1 \cdots p_{s-1}}$.