Critère d'Eisenstein et irréductibilité de Φ_p

Proposition Soit $P \in \mathbb{Z}[X]$.
Si P est irréductible dans $\mathbb{Z}[X]$, il est irréductible dans $\mathbb{Q}[X]$.

Supposons que P soit irréductible dans $\mathbb{Z}[X]$ et réductible dans $\mathbb{Q}[X]$.
Il existe alors $R, Q \in \mathbb{Q}[X]$ tels que $P = QR$, avec $\deg Q \geq 1$, $\deg R \geq 1$.
En chassant les dénominateurs,

il existe $q \in \mathbb{Z}$, $r \in \mathbb{Z}$ tels que $qQ \in \mathbb{Z}[X]$, $rR \in \mathbb{Z}[X]$

On obtient :

$$qr P = qQ \cdot rR = c(qQ)\widetilde{qQ} \; c(rR)\widetilde{rR}$$

Par le lemme des contenus de Gauss,

$$qR\, c(P) = c(qQ)c(rR) \quad \text{donc : } P = c(P)\,\widetilde{qQ}\;\widetilde{rR}$$

on remplace $c(qQ)c(rR)$ ds l'égalité précédente et on simplifie par qR

Or, $\deg(\widetilde{qQ}) \geq 1$, $\deg(\widetilde{rR}) \geq 1$, ainsi P est réductible dans $\mathbb{Z}[X]$.

puisque $\widetilde{qQ}, \widetilde{rR} \in \mathbb{Z}[X]$

Contradiction !

Proposition (Critère d'Eisenstein) Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$.
Supposons qu'il existe p premier tel que $p \mid a_0, \dots, a_{n-1}$, $p \nmid a_n$ et $p^2 \nmid a_0$. Alors P est irréductible dans $\mathbb{Q}[X]$.

Supposons que P soit réductible dans $\mathbb{Q}[X]$.
D'après ce qui précède, P est alors réductible dans $\mathbb{Z}[X]$.
Donc :

$$P = QR \quad \text{avec } Q, R \in \mathbb{Z}[X],\ \deg Q \geq 1,\ \deg R \geq 1$$

On obtient alors dans $\mathbb{Z}_p$:

$$\overline{a_n}\, X^n = \overline{P} = \overline{Q}\,\overline{R} \qquad \text{avec } Q = \sum_{k=0}^{a} q_k X^k \text{ et } R = \sum_{k=0}^{b} r_k X^k$$

ainsi :

$$\overline{Q} = \overline{q_a}\, X^a \quad \text{et} \quad \overline{R} = \overline{r_b}\, X^b$$

s'il y avait un autre $\overline{q_i} \neq 0$ par exemple alors $\overline{a_n} X_n = \overline{r_b q_a} X^n + \overline{r_b q_i} X^{i+b} + \dots$

Donc :

$$\overline{r_0} = \overline{q_0} = 0 \text{ dans } \mathbb{Z}_p \text{ d'où } p^2 \text{ divise } r_0 q_0 = a_0.$$

Contradiction !

Corollaire Soit p un nombre premier.
Alors le polynôme cyclotomique Φ_p est irréductible dans $\mathbb{Q}[X]$.

On a : $\Phi_p(X) = \prod_{\omega \in \mathbb{U}_p} (X - \omega) = \dfrac{X^p - 1}{X - 1}$.

D'où :

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}$$

Or : $\forall k \in [\![1, p-1]\!],\ p \mid \binom{p}{k}$

$p^2 \nmid \binom{p}{1} = p$

$p \nmid \binom{p}{p} = 1$

Donc, par le critère d'Eisenstein, $\Phi_p(X+1)$ est irréductible dans $\mathbb{Q}[X]$.
Il en va donc de même de Φ_p.

Corollaire
$\mathbb{Q}[X]$ admet des polynômes irréductibles de tout degré ≥ 1.

Pour tout $n \geq 1$, $X^n - p$ avec p premier est irréductible dans $\mathbb{Q}[X]$.