Étude des polynômes cyclotomiques

- Perrin, *Cours d'algèbre*. (81-83)

Pour tout $n \in \mathbb{N}^*$, on pose $\mu_n^* = \{z \in \mathbb{C},\ z^n = 1,\ \forall k < n,\ z^k \neq 1\}$ l'ensemble des racines n-ièmes primitives de l'unité et $\Phi_n(X) = \prod_{z \in \mu_n^*} (X - z)$.

Pour tout $n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$ et est un polynôme unitaire et irréductible dans $\mathbb{Z}[X]$ (donc dans $\mathbb{Q}[X]$ aussi).

Démonstration.

- Pour tout $n \in \mathbb{N}^*$, on pose $H_n : \Phi_n \in \mathbb{Z}[X]$ et est unitaire.

Pour $n = 1$, $\Phi_1(X) = X - 1$ donc H_1 est vraie.
Soit $n \in \mathbb{N}\backslash\{0, 1\}$. Supposons H_d vraie pour tout $d < n$. Posons $F(X) = \prod_{\substack{d<n \\ d|n}} \Phi_d(X)$.
D'après l'hypothèse, $F \in \mathbb{Z}[X]$ est unitaire.
On peut effectuer la division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{Z}[X]$ (effectuable sur $A[X]$ euclidien, ce n'est pas le cas de $\mathbb{Z}[X]$ mais on peut le faire car F est unitaire).

$$X^n - 1 = F(X)P(X) + R(X) \text{ avec } P, R \in \mathbb{Z}[X] \text{ et } \deg R < \deg F$$

De plus, $X^n - 1 = \prod_{d|n} \Phi_d(X) = \Phi_n(X)F(X)$ dans $\mathbb{Q}[X]$. On a donc que Φ_n est unitaire.
Et $F(X)(\Phi_n(X) - P(X)) = R(X)$.
Comme $\deg R < \deg F$, $\Phi_n = P \in \mathbb{Z}[X]$. Donc H_n est vraie.
Le principe de récurrence assure que la propriété est vraie pour tout $n \in \mathbb{N}^*$.

- Montrons que pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible.

Soit $n \in \mathbb{N}^*$. Soit $p \in \mathbb{N}$ premier tel que $p \nmid n$. Soit $z \in \mu_n^*$. Alors $z^p \in \mu_n^*$.
Notons $f, g \in \mathbb{Q}[X]$ les polynômes minimaux de z et z^p (respectivement).
Un polynôme minimal n'a de sens que sur un anneau principal (donc pas sur $\mathbb{Z}[X]$) car il engendre l'idéal annulateur.

- ⋆ Montrons que $f, g \in \mathbb{Z}[X]$.

Or $\mathbb{Z}[X]$ est factoriel donc on peut écrire $\Phi_n = f_1^{\alpha_1} \dots f_r^{\alpha_r}$ avec $f_i \in \mathbb{Z}[X]$ irréductible.
Comme Φ_n est unitaire alors quitte à multiplier les f_i par -1, on peut supposer les f_i unitaires donc irréductibles dans $\mathbb{Q}[X]$.
Comme $\Phi_n(z) = 0$ alors il existe $i \in [\![1, r]\!]$ tel que $f_i(z) = 0$. Et f_i est unitaire et irréductible, ainsi $f = f_i \in \mathbb{Z}[X]$. Donc $f \mid \Phi_n$ dans $\mathbb{Z}[X]$. De même, $g \in \mathbb{Z}[X]$ et $g \mid \Phi_n$.

- ⋆ Montrons que $f = g$. Supposons que $f \neq g$.

Comme f et g irréductibles alors $fg \mid \Phi_n$ dans $\mathbb{Z}[X]$. Et comme z est également racine de $g(X^p)$ dans $\mathbb{Q}[X]$ par définition de g, alors $f(X) \mid g(X^p)$ dans $\mathbb{Q}[X]$ i.e. il existe $h \in \mathbb{Q}[X]$ tel que $g(X^p) = f(X)h(X)$.
Si on écrit $h = \frac{a}{b}h'$ avec $h' \in \mathbb{Z}[X]$ de contenu 1, alors par le lemme de Gauss ($g(X^p)$ et $f(X)$ sont unitaires) $1 = \frac{a}{b}$. Donc $h \in \mathbb{Z}[X]$.

- ⋆ Projetons l'égalité $g(X^p) = f(X)h(X)$ dans $\mathbb{F}_p$:

Si on écrit $g(X) = \sum_{i=0}^{r} a_i X^i$ avec $a_i \in \mathbb{Z}$ alors $g(X^p) = \sum_{i=0}^{r} a_i X^{pi}$.
Or $\overline{a_i} = \overline{a_i^p}$ dans $\mathbb{F}_p$ donc par le morphisme de Frobenius ($x \mapsto x^p$ est l'identité sur $\mathbb{F}_p$),

$$\bar{g}(X^p) = (\overline{a_r}X^r + \dots + \overline{a_0})^p = \bar{g}(X)^p$$

Soit $\varphi(X)$ un facteur irréductible de $\bar{f}(X)$ sur $\mathbb{F}_p$.
Comme $\bar{g}(X)^p = \bar{f}(X)\bar{h}(X)$ alors par le lemme d'Euclide (si p est irréductible et $p \mid ab$ alors $p \mid a$ ou $p \mid b$) on a $\varphi \mid \bar{g}^p \Rightarrow \varphi \mid \bar{g}$. Comme $fg \mid \Phi_n$ alors $\bar{f}\bar{g} \mid \overline{\Phi_n}$ sur $\mathbb{F}_p$. Donc $\varphi^2 \mid \overline{\Phi_n}$.
Mais, alors dans un corps de décomposition de Φ_n sur $\mathbb{F}_p$, $\overline{\Phi_n}$ aurait une racine double, donc $X^n - 1$ également, ce qui est faux. Donc $g = f$.

⋆ Soit $z' \in \mu_n^*$ tel que $z' = z^m$ avec $m = p_1^{m_1} \dots p_k^{m_k}$ et $p_i \nmid n$ premier.
En faisant une récurrence immédiate des arguments précédents, on trouve que z et z' ont même polynôme minimal sur $\mathbb{Q}$ (i.e. f). Par conséquent, f s'annule en toutes les racines primitives de l'unité. D'où $\Phi_n \mid f$. Ainsi, $f = \Phi_n$. □