# Etude des polynômes cyclotomiques :

Référence : [Gourdon P91]

Contexte : $U_n = \{ e^{2i\pi k/n} ; k \in \mathbb{Z} \}$ $e^{2i\pi k/n} = (e^{2i\pi/n})^k$ est générateur de $U_n$ ssi $k \wedge n = 1$

On note alors $R_n = \{ e^{2i\pi k/n} ; k \in [\![0; n-1]\!], k \wedge n = 1 \}$

Énoncé : pour p premier, $\Phi_p(X) = X^{p-1} + \dots + 1$

pour $n \in \mathbb{N}^*$ $X^n - 1 = \prod_{d|n} \Phi_d(X)$ et $\Phi_n(X) \in \mathbb{Z}[X]$

pour tout $n \in \mathbb{N}^*$, $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$

Démo :

Étape 1 : cas p premier $\Phi_p(X) = X^{p-1} + \dots + 1$ et Eisenstein

Étape 2 : $\forall n \in \mathbb{N}^*$ $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Étape 3 : $\Phi_n(X) \in \mathbb{Z}[X]$

Étape 4 : on mq si $\Phi_n = F_1 \dots F_r$ avec $F_i \in \mathbb{Q}[X]$

en fait $F_i \in \mathbb{Z}[X]$ pour tout $i \in [\![1; r]\!]$

Étape 5 : on mq si $F_1(\xi) = 0$ alors $F_1(\xi^p) = 0$

Lemme : si $\overline{Q}^2 \mid \overline{\Phi_n}$ alors $\overline{Q}$ est constant

Étape 6 : on mq $\forall \xi \in R_n$, $F_1(\xi) = 0$.

# Étude des polynômes cyclotomiques :

Etape 1 : Soit p premier,

$\forall k \in [\![1; p-1]\!]$, $p \wedge k = 1$ donc $U_p = \mathbb{R}_p \setminus \{1\}$

Et $\forall w \in U_p$, $w$ est racine de $X^p - 1$. Donc

$$X^p - 1 = \prod_{\omega \in U_p} (X - \omega) = \prod_{\omega \in \mathbb{R}_p} (X - \omega) \times (X - 1)$$

Donc $\Phi_p(X) = \dfrac{X^p - 1}{X - 1}$

Or $X^p - 1 = (X-1) \sum_{k=0}^{p-1} X^k$ donc $\Phi_p(X) = X^{p-1} + \dots + 1$

Irréductibilité :

On va appliquer le critère d'Eisenstein

$(X-1)\,\Phi_p(X) = X^p - 1$

donc $X\,\Phi_p(X+1) = (X+1)^p - 1$

donc $X\,\Phi_p(X+1) = \sum_{k=0}^{p} \binom{p}{k} X^k - 1$

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

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

$$\Phi_p(X+1) = \sum_{k=0}^{p-1} \binom{p}{k+1} X^k$$

donc $p \mid \binom{p}{k+1}$ $\forall k \in [\![0, p-1]\!]$, $p \nmid \binom{p}{p} = 1$

et $\left(\frac{p}{1}\right) = p$ donc $p^2 \nmid \left(\frac{p}{1}\right)$
donc par le critère d'Eisenstein, $\Phi_p(X)$ est irréductible dans $\mathbb{Q}[X]$.

Etape 2: pour $n$ quelconque $X^n - 1 = \prod_{d|n} \Phi_d(X)$ et $\Phi_n(X) \in \mathbb{Z}[X]$

Mq les $\mathbb{R}_d$, pour $d|n$, forment une partition de $U_n$.
Soit $w \in \mathbb{R}_d$, $w^d = 1$ or $d|n$ donc $\exists u \in \mathbb{Z}$ $ud = n$.
donc $w^n = (w^d)^u = 1^u = 1$ donc $w \in U_n$.
Ainsi, $\bigcup_{d|n} \mathbb{R}_d \subset U_n$.
Soit $w \in U_n$, on veut mq il existe $d|n$ tel que $w^d = 1$ $\exists k \in \mathbb{Z}$ tq $w = e^{2ik\pi/n}$ donc $w^d = 1$ si $\frac{dk}{n} \in \mathbb{Z}$. En notant $\delta = \text{pgcd}(k \wedge n)$, et $k', n'$ tels que $k'\delta = k$ et $n'\delta = n$ on a alors comme condition nécessaire et suffisante $\frac{dk'}{n'} \in \mathbb{Z}$.
ie, $n' | dk'$ or $k' \wedge n' = 1$ donc la condition devient $n' | d$. Le plus petit entier naturel convenant est alors $d = n'$ et on a bien $d|n$. Ainsi, $w^d = 1$, $w \in \mathbb{R}_d$ donc $U_n \subset \bigcup_{d|n} \mathbb{R}_d$. Cette union est bien disjointe car $\mathbb{R}_d$ et $\mathbb{R}_{d'}$ contiennent des éléments d'ordre

différent.

Donc comme $\forall n \in \mathbb{N}^*$ $X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega)$

on a $X^n - 1 = \prod_{d|n} \prod_{\omega \in \mathbb{U}_d} (X - \omega)$ ie $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Etape 3 : On montre par récurrence sur $n$ que $\forall n \in \mathbb{N}^*$ $\Phi_n \in \mathbb{Z}[X]$

Pour $n = 1$, $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$

Soit $n \in \mathbb{N}$, $n \geq 2$. On suppose que $\forall k \in [\![1; n-1]\!]$, $\Phi_k \in \mathbb{Z}[X]$

$$X^n - 1 = \prod_{d|n} \Phi_d(X) = \Phi_n(X) \underbrace{\prod_{\substack{d|n \\ d<n}} \Phi_d(X)}_{= P \in \mathbb{Z}[X] \text{ et unitaire.}}$$

Comme $P$ est unitaire, on peut alors effectuer la la division euclidienne de $X^n - 1$ par $P$ dans $\mathbb{Z}[X]$

On a $Q \in \mathbb{Z}[X]$ et $R \in \mathbb{Z}[X]$ tel que

$$X^n - 1 = (QP + R)(X)$$

donc $QP + R = \Phi_n P$ et $\deg(R) < \deg(P)$

Valable dans $\mathbb{C}[X]$ donc par unicité de la division euclidienne dans $\mathbb{C}[X]$, $Q = \Phi_n$ et $R = 0$ donc $\Phi_n \in \mathbb{Z}[X]$.

Donc $\forall n \in \mathbb{N}^*$, $\Phi_n$ est unitaire et à coef. dans $\mathbb{Z}[X]$.

Etape 4 : Soit $G_1, \dots, G_r \in \mathbb{Q}[X]$ les polynômes de la décomposition en facteurs irréductibles de $\Phi_n$.

Mq $\exists F_1, \dots, F_r \in \mathbb{Z}[X]$ unitaires tq $\Phi_n(X) = F_1(X) \dots F_r(X)$

$\forall i \in [\![1; r]\!]$, $\exists n_i \in \mathbb{N}$ tel que $H_i = n_i G_i \in \mathbb{Z}[X]$.

On a alors $n_1 \dots n_r \Phi_n(X) = H_1(X) \dots H_r(X)$

Donc par le lemme de Gauss,

$n_1 \dots n_r \, c(\Phi_n) = c(H_1) \dots c(H_r)$

donc comme $\Phi_n$ est irréductible, $c(\Phi_n) = 1$. Donc,

en notant $G_i = c(H_i) F_i$, avec $F_i \in \mathbb{Z}[X]$ primitif

on a $\Phi_n(X) = G_1(X) \dots G_r(X)$

$$= \frac{c(H_1) \dots c(H_r)}{n_1 \dots n_r} F_1(X) \dots F_r(X) = F_1(X) \dots F_r(X).$$

Comme $\Phi_n$ est unitaire et les $F_i$ à coefficients dans $\mathbb{Z}$, ils sont également unitaires

Étape 5 : Soit $\xi$ racine de $F_1$, soit $p$ premier tel que $p \nmid n$

Mq $\xi^p$ est racine de $F_1$.

$F_1(\xi) = 0$ donc $\Phi_n(\xi) = 0$.

Donc $\xi \in \mathbb{U}_n$ donc comme $p \nmid n$, $\xi^p$ est également dans $\mathbb{U}_n$ donc $\Phi_n(\xi^p) = 0$ donc $\exists i \in [\![1; r]\!]$, $F_i(\xi^p)$

Lemme : Dans $\mathbb{Z}/p\mathbb{Z}[X]$, $\overline{\Phi_n}$, si $\overline{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$ est tq $\overline{Q}^2 \mid \overline{\Phi_n}$ alors $\overline{Q}$ est constant.

Preuve : si $\overline{\Phi_n}(X) = \overline{Q}(X)^2 \overline{S}(X)$

On a $X^n - \overline{1} = \overline{Q}(X)^2 \overline{S}(X) \overline{R}(X)$ où $R(X) = \prod_{d \mid n \, d \neq n} \Phi_d(X)$

En dérivant

$\overline{n}X^{n-} = {}^{1}2\overline{Q}\overline{Q}'(\overline{SR})(X) + \overline{Q}^2(\overline{SR})'(X)$

donc $\overline{Q} \mid \overline{n}X^{n-1}$ et $\overline{Q} \mid X^n - \overline{1}$

Donc $\overline{Q} \mid \overline{n}X^n - \overline{n}$ et $\overline{Q} \mid \overline{n}X^n$

Donc $\overline{Q} \mid \overline{n}$ or comme $p \nmid n$, $\overline{n} \neq \overline{0}$ donc $\overline{Q}$ est constant. □

$F_i(X^p)$ et $F_1(X)$ ne sont pas premiers entre eux dans $\mathbb{Q}[X]$, car $\forall U, V \in \mathbb{Q}[X]$ $U(X)F_i(X^p) + V(X)F_1(X) \neq 1$ (évalué en $\xi$). dans $\mathbb{Q}[X]$

Donc $\exists U$, facteur irréductible commun à $F_1(X)$ et $F_i(X^p)$. Or $F_1$ est irréductible. Donc $F_1(X) \mid F_i(X^p)$ dans $\mathbb{Q}[X]$ dans $\mathbb{Q}[X]$ Donc $\exists R(X) \in \mathbb{Q}[X]$ tq $F_1(X)R(X) = F_i(X^p)$ Donc $\exists R'(X) \in \mathbb{Z}[X]$ tq $F_1(X)R'(X) = F_i(X^p)$ (lemme de Gauss à nouveau) donc $F_1(X) \mid F_i(X^p)$ dans $\mathbb{Z}[X]$ donc $\overline{F_1(X)} \mid \overline{F_i(X)}^p$ donc $\exists \overline{P} \in \mathbb{F}_p[X]$ irréd tq $\overline{P}$ soit un facteur irréductible commun à $\overline{F_1}$ et $\overline{F_i}$, on a alors, si $i \neq 1$, $\overline{P}^2 \mid \overline{\Phi_n}$. Absurde.

Donc $i = 1$ Donc $F_1(\xi^p) = 0$

Etape 6 : mq $\forall k \in \mathbb{Z}$, $k \wedge n = 1$, $\xi^k$ est racine de $F_1$.

Soit $k = p_1 \dots p_s$, $p_1, \dots, p_s$ premiers.

On fait une récurrence sur le nombre de facteurs dans la décomposition de $k$.

$\underline{s=1}$ ou

$\underline{s \geq 2}$ on suppose vrai pour $s-1$

$k = p_2 \dots p_s$. Comme $k \wedge n$, $p_1 \dots p_{s-1} \wedge n$ donc comme $\xi$ est racine de $F_1$ donc $\xi^{p_1 \dots p_{s-1}}$ aussi par hypothèse de récurrence

Or $p_s$ est premier et $p_s \nmid n$ car $p_s \wedge n = 1$.

donc $(\xi^{p_1 \dots p_{s-1}})^{p_s}$ est racine de $F_1$ d'après l'étape 5

donc $\xi^k$ est racine de $F_1$.

Ainsi, $\forall k \in \mathbb{Z}$, $k \wedge n = 1$, $\xi^k$ est racine de $F_1$

donc toutes les racines primitives de l'unité sont racines de $F_1$. Donc $F_1 = \Phi_n$ et $\Phi_n$ est irréductible dans $\mathbb{Q}[X]$.