Irréductibilité des polynômes cyclotomiques

Ref : Perrin, Algèbre (p82)

Thm : $\Phi_m = \prod_{\substack{k=1 \\ k\wedge m=1}}^{m} \left(X - e^{2ik\pi/m}\right) \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$.

Lm : $X^n - 1 = \prod_{\substack{d=1 \\ d|m}}^{m} \Phi_d$ et $\deg \Phi_n = \varphi(m)$.

Dem : $\mu_n(\mathbb{C}) = \bigsqcup_{\substack{d=1 \\ d|m}}^{m} \mu_d^*(\mathbb{C})$ car pour toute racine m-ième de l'unité, son ordre divise m.

Donc : $X^m - 1 = \prod_{z\in\mu_n(\mathbb{C})} (X-z) = \prod_{\substack{d=1 \\ d|m}}^{m} \prod_{z\in\mu_d^*} (X-z) = \prod_{\substack{d=1 \\ d|m}}^{m} \Phi_d$

$\deg \Phi_n \underset{\text{def}}{=} \#\{k\in[\![1,m]\!],\ k\wedge m = 1\} = \varphi(m)$. □

Lm : Φ_m est unitaire à coeffs dans $\mathbb{Z}$.

Dem : Par rec, • $m=1$: $\Phi_1 = X-1 \in \mathbb{Z}(X)$ unitaire.

• $d\in[\![1,m-1]\!] \Rightarrow m$: Alors $P = \prod_{\substack{d=1 \\ d|m}}^{m-1} \Phi_d \in \mathbb{Z}[X]$ unitaire.

On fait la div de $X^m - 1$ par P (unitaire donc de coeff dominant inversible) dans $\mathbb{Z}[X]$: $\exists Q, R \in \mathbb{Z}[X]$ tq $X^n - 1 = PQ + R$ $\deg R < \deg P$.

Ainsi, Q est unitaire. Or dans $\mathbb{C}[X]$, $X^m - 1 \underset{Lm}{=} \Phi_m P$, donc $P(\Phi_n - Q) = R$

Or $\deg(R) < \deg P$ donc $\Phi_m = Q \in \mathbb{Z}(X)$ unitaire. □

Dem du thm : (1) Egalité des polynômes minimaux de z et z^p

Soit $z\in\mu_n^*$ et $p\in\mathcal{P}$ tq $p\nmid m$ alors $z^p\in\mu_n^*$ car $z^p = (e^{2ik\pi/m})^p = e^{2ik\pi p/m}$ avec $k\wedge m = 1$ et $p\wedge m = 1$ donc $kp\wedge m = 1$ donc $z^p\in\mu_n^*$.

Soit $(F,G)\in\mathbb{Q}[X]^2$ poly minimaux de z et z^p sur $\mathbb{Q}$.

Or $\mathbb{Z}[X]$ est factoriel et $\Phi_m\in\mathbb{Z}[X]$ donc $\exists P_i\in\mathbb{Z}[X]$ irréductible tq $\Phi_m = P_1^{\alpha_1}\cdots P_R^{\alpha_R}$.

Or Φ_m est unitaire, donc les P_i peuvent être pris unitaires. Comme z et z^p sont racines de Φ_m, $\exists i,j\in[\![1,R]\!]$ tq $P_i(z) = 0$, $P_j(z^p) = 0$ avec P_i et P_j irréductibles unitaires dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$ donc $F = P_i\in\mathbb{Z}[X]$, $G = P_j\in\mathbb{Z}[X]$. Mq $i=j$. Supposons par l'absurde $F\neq G$.

Par irréductibilité, $F\wedge G = 1$

De plus dans $\mathbb{Z}[X]$, $F, G \mid \Phi_m$ donc dans $\mathbb{Z}[X]$ $FG\mid\Phi_m$. De plus $G(z^p) = 0$ donc dans $\mathbb{Q}[X]$ $F\mid G(X^p)$ ie $\exists H\in\mathbb{Q}[X]$ tq $FH = G(X^p)$ (car F est le poly min de z)

On écrit $H = \frac{a}{b} H'$ avec $H' \in \mathbb{Z}[X]$ tq $c(H') = 1$ et $(a,b) \in \mathbb{Z} \times \mathbb{Z}\setminus\{0\}$

Donc $aFH' = bG(X^p)$. Or (par Lm de Gauss sur $\mathbb{Z}[X]$) :

$$b = c(b) \times c(G(X^p)) = c(bG(X^p)) = c(aFH') = a\,c(F)\,c(H') = a.$$

Donc $H = H' \in \mathbb{Z}[X]$ et $F \mid G(X^p)$ dans $\mathbb{Z}[X]$.

On écrit $G = a_k X^k + \dots + a_0$ donc $G(X^p) = a_k X^{kp} + \dots + a_0$

Dans $\mathbb{F}_p[X]$ par Frobenius : $\overline{G(X^p)} = \bar{a}_k X^{pk} + \dots + \bar{a}_0 = (\bar{a}_k X^k + \dots + \bar{a}_0)^p = \bar{G}^p$

Soit φ un facteur irréductible de $\bar{F}$ sur $\mathbb{F}_p$.

Or $\bar{G}^p = \overline{G(X^p)} = \overline{FH} = \bar{F}\bar{H}$. Donc, par le lemme d'Euclide, $\varphi \mid \bar{G}^p$, $\varphi \mid \bar{G}$

Or dans $\mathbb{Z}[X]$, $FG \mid \Phi_m$ donc dans $\mathbb{F}_p[X]$ $\bar{F}\bar{G} \mid \bar{\Phi}_m$ d'où $\varphi^2 \mid \bar{\Phi}_n = \Phi_{m,\mathbb{F}_p}$

Ainsi, dans un corps de décompo de Φ_m sur $\mathbb{F}_p$, $\bar{\Phi}_n$ a une racine double.

Absurde car $(X^m - 1)' = mX^{m-1} \neq 0$ et $m \wedge p = 1$ ie $X^m - 1$ sans racine double dans $\mathbb{F}_p$.

Donc $F = G$.

② Égalité des poly min de tous les $z \in \mu_n^*(\mathbb{C})$

Soit z' une racine primitive n-ième de l'unité, on note $z' = z^m$ avec $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ et $p_i \nmid n$ $\forall i$. Par ce qui précède, $0 = F(z^{p_1}) = F((z^{p_1})^{p_1}) = \dots F(z^{p_1^{\alpha_1}})$

$= F((z^{p_1^{\alpha_1}})^{p_2}) \dots = F(z^m)$

Donc z et z^m ont même poly minimal.

③ Conclusion :

Ainsi $F(z^m) = 0$ donc F admet toutes les racines n-ième primitives de l'unité comme racine d'où $\deg(F) \geq \varphi(m)$. Or $F \mid \Phi_m$ donc $\deg F \leq \deg \Phi_m = \varphi(m)$

Donc $\begin{cases} F \mid \Phi_n \\ \deg F = \deg \Phi_n \\ F \text{ et } \Phi_n \text{ unitaires} \end{cases} \Rightarrow F = \Phi_m$. En part, Φ_n est irréductible sur $\mathbb{Q}$, et comme Φ_n est unitaire son contenu est 1, Φ_n est irréductible sur $\mathbb{Z}$. ☒

Rq : ⚠ Dans qui on fait les d.e.

⚠ Un poly minimal a du sens que sur un anneau principal (donc pas $\mathbb{Z}[X]$) et les d.e sur un anneau euclidien ($A[X]$ euclidien ssi A est un corps)

Appli : Φ_n est le poly min de toute racine primitive n-ième de l'unité.
$\Rightarrow$ on en déduit le degré des extensions cyclotomiques et on peut faire de la théorie de Galois avec + constructibilité des polygones réguliers.