Irréductibilité des polynômes cyclotomiques (125, 141)

Perrin p. 81

prop : Soit $n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$ et il est unitaire

démo : Soit $n \in \mathbb{N}^*$. Montrons le par récurrence sur n.

* initialisation : $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$ et il est unitaire

* hérédité : Supposons que la propriété est vraie pour tout $d < n$.

Soit $F(X) = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(X)$. On a par HR, $F(X) \in \mathbb{Z}[X]$ et il est unitaire

On effectue la division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{Z}[X]$:

Alors il existe $(Q, R) \in \mathbb{Z}[X]^2$ tel que $d^\circ(R) < d^\circ(F)$ et

$$X^n - 1 = F(X)\,Q(X) + R(X)$$

Cependant, on a $X^n - 1 = F(X)\,\Phi_n(X)$ dans $\mathbb{Q}[X]$. donc par unicité de la division euclidienne sur $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, on a $R(X) = 0$ et $\Phi_n(X) = Q(X)$.

Ainsi $\Phi_n \in \mathbb{Z}[X]$ et il est unitaire.

thm : Soit $n \in \mathbb{N}^*$. Φ_n est irréductible sur $\mathbb{Q}[X]$ donc sur $\mathbb{Z}[X]$.

démo : Soit $\zeta \in \mathbb{C}$ une racine n-ième primitive de l'unité et p un nombre premier ne divisant pas n.
Ainsi ζ^p est aussi une racine n-ième primitive de l'unité.

Soit $f, g \in \mathbb{Q}[X]$ les polynômes minimaux de ζ et ζ^p respectivement.

Étape 1 : Montrons que $f, g \in \mathbb{Z}[X]$

Comme $\Phi_n \in \mathbb{Z}[X]$ et que $\mathbb{Z}[X]$ est factoriel, on a $\Phi_n(X) = f_1^{\alpha_1}(X) \cdots f_r^{\alpha_r}(X)$ avec

$\forall i \in [\![1, r]\!]$ $f_i(X) \in \mathbb{Z}[X]$ irréductible

Comme Φ_n est unitaire, quitte à multiplier f_i par -1, on peut supposer f_i unitaire $\forall i \in [\![1, r]\!]$.

Or $\Phi_n(\zeta) = 0$ donc il existe $i_0 \in [\![1, r]\!]$ tel que ζ est racine de f_{i_0}, qui est unitaire et irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$. D'où $f_{i_0} = f$.

Il en est de même pour g.

D'où f et g divisent Φ_n dans $\mathbb{Z}[X]$.

Étape 2 : Montrons que $f=g$, par l'absurde

Supposons que $f \neq g$. Comme ils sont irréductibles et distincts, on a fg divise Φ_n dans $\mathbb{Z}[X]$.

Par ailleurs, on a $g(\zeta^p)=0$ donc $g(X^p)$ admet ζ comme racine donc $f(X)$ divise $g(X^p)$ dans $\mathbb{Q}[X]$, mais aussi dans $\mathbb{Z}[X]$

Donc il existe $h(X) \in \mathbb{Z}[X]$ tel que $g(X^p)=f(X)h(X)$.

On projette cette égalité dans $\mathbb{F}_p$, on écrit

$g(X)=a_r X^r + \dots + a_0$ avec $a_i \in \mathbb{Z}$, $g(X^p)=a_r X^{pr} + \dots + a_1 X^p + a_0$

En réduisant modulo p, on a :

$$\overline{g}(X^p)=\overline{a_r}X^{pr}+\dots+\overline{a_1}X^p+\overline{a_0}=\left(\overline{a_r}X^r+\dots+\overline{a_1}X+\overline{a_0}\right)^p=\overline{g(X)}^p$$ par le morphisme de Frobenius.

Soit $\varphi(X)$ un facteur irréductible de $\overline{f}(X)$ sur $\mathbb{F}_p$. Comme $\overline{g(X)}^p=\overline{f}(X)\overline{h}(X)$, par le lemme d'Euclide φ divise $\overline{g}$. Comme fg divise Φ_n sur $\mathbb{Z}$, $\overline{fg}$ divise Φ_n sur $\mathbb{F}_p$ donc φ^2 divise $\overline{\Phi}_n$ ie φ^2 divise $\overline{X}^n-1$ dans $\mathbb{F}_p$.

Ainsi dans un corps de décomposition de X^n-1 sur $\mathbb{F}_p$, $\overline{X}^n-1$ aurait une racine double ce qui est absurde car p ne divise pas n.

D'où $f=g$.

Étape 3 : Montrons que $f=\Phi_n$ sur $\mathbb{Q}[X]$.

Soit ζ' une racine n-ième primitive de l'unité, on a $\zeta'=\zeta^m$ avec $m \wedge n = 1$.

On écrit $m=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ avec p_i ne divisant pas n.

En itérant l'étape 2, on obtient que ζ' et ζ ont le même polynôme minimal sur $\mathbb{Q}$

Ainsi f admet toutes racines primitives n-ième de l'unité comme zéros.

Donc on a $d^\circ f \geq \varphi(n)$. Or $f \mid \Phi_n$ qui est de degré $\varphi(n)$.

Donc $f=\Phi_n$ sur $\mathbb{Q}$.

Étape 4 : Conclusion

Comme Φ_n est unitaire et irréductible sur $\mathbb{Q}[X]$, il est irréductible sur $\mathbb{Z}[X]$.

Questions : Irréductibilité des polynômes cyclotomiques

- Division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{Z}[X]$?

Comme $F(X) \in \mathbb{Z}[X]$ et unitaire, on peut effectuer la division euclidienne par F dans $\mathbb{Z}[X]$ (coefficient dominant irréductible dans $\mathbb{Z}[X]$).

- irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$?

Soit A anneau intègre et $\mathrm{Frac}(A) = K$. Soit $P \in A[X]$ de degré ≥ 1. On a l'équivalence suivante :

P irréductible sur $A[X]$ ssi P est irréductible sur $K[X]$ et $c(P) = 1$.

Ici f_n unitaire et irréductible sur $\mathbb{Z}[X]$ donc comme $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$. Alors f_n irréductible sur $\mathbb{Q}[X]$.

- $f(X)$ divise $g(X^p)$ dans $\mathbb{Z}[X]$?

Soit $P, Q, R \in \mathbb{Q}[X]$. On suppose $P \in \mathbb{Z}[X]$ et $P = QR$ avec P et Q unitaires

Alors Q et R sont dans $\mathbb{Z}[X]$.

On a $\underbrace{g(X^p)}_{\in \mathbb{Z}[X]} = \underbrace{f(X)\,h(X)}_{\in \mathbb{Z}[X]}$ et $g(X^p)$ et $f(X)$ sont unitaires donc $h(X)$.

D'où le résultat.

- $(\bar{X}^n - 1)' = n\bar{X}^{n-1}$?

On a $(X^n - 1)' = nX^{n-1}$ or p ne divise pas n donc $(\bar{X}^n - 1)' = n\bar{X}^{n-1}$.

- Φ_n irréductible sur $\mathbb{Z}[X]$?

Φ_n irréductible sur $\mathbb{Q}[X]$ et $c(\Phi_n) = 1$ car unitaire. D'où Φ_n irréductible sur $\mathbb{Z}[X]$.