Irréductibilité des polynômes cyclotomiques

Dorian Cacitti-Holland

2020-2021

Références.

1. Cours d'algèbre de Daniel Perrin

Leçons.

1. 102 Groupe des nombres complexes de module 1, sous-groupes des racines de l'unité, applications
2. 123 Corps finis, applications
3. 125 Extension de corps, exemples et applications
4. 141 Polynômes irréductibles à une indéterminée, corps de rupture, exemples et applications
5. 144 Racines d'un polynôme, fonctions symétriques élémentaires, exemples et applications

Théorème. Soit $n \in \mathbb{N}^*$, alors le polynôme cyclotomique

$$\phi_n = \prod_{\substack{k=1 \\ k \wedge n = 1}}^{n} \left(X - e^{\frac{2ik\pi}{n}} \right) \in \mathbb{Z}[X]$$

est irréductible dans $\mathbb{Z}[X]$.

Démonstration.
Etape 1 : Egalité des polynômes minimaux de z et z^p
Soit $z \in \mu_n^*(\mathbb{C})$ et $p \in \mathcal{P}$ tel que p ne divise pas n, alors $z^p \in \mu_n^*(\mathbb{C})$ car

$$z^p = \left(e^{\frac{2ik\pi}{n}} \right)^p = e^{\frac{2ikp\pi}{n}}$$

avec $k \wedge n = 1$ et $p \wedge n = 1$, donc $kp \wedge n = 1$.
Soit $(F, G) \in \mathbb{Q}[X]^2$ polynômes minimaux de z et z^p sur $\mathbb{Q}$.
Or $\mathbb{Z}[X]$ est factoriel et $\phi_n \in \mathbb{Z}[X]$, donc il existe $P_i \in \mathbb{Z}[X]$ irréducitbles tel que

$$\phi_n = P_1^{\alpha_1} ... P_r^{\alpha_r}$$

Or ϕ_n est unitaire, donc les P_i peuvent également être choisis unitaires.
Comme z et z^p sont racines de ϕ_n, donc il existe $(i, j) \in [\![1, r]\!]$ tel que

$$P_i(z) = 0, P_j(z^p) = 0$$

avec P_i et P_j irréductibles unitaires dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$, donc

$$F = P_i \in \mathbb{Z}[X], G = P_j \in \mathbb{Z}[X]$$

On suppose par l'absurde que $F \neq G$, alors par irréductibilité $F \wedge G = 1$.
De plus dans $\mathbb{Z}[X]$, $F, G \mid \phi_n$, donc, dans $\mathbb{Z}[X]$, $FG \mid \phi_n$.
Par ailleurs $G(z^p) = 0$, donc dans $\mathbb{Q}[X]$, $F \mid G(X^p)$ ie il existe $H \in \mathbb{Q}[X]$ tel que

$$FH = G(X^p)$$

On écrit $H = \frac{a}{b}H'$ avec $H' \in \mathbb{Z}[X]$ tel que $c(H') = 1$ et $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$.
Donc

$$aFH' = bG(X^p)$$

Or par lemme de Gauss sur $\mathbb{Z}[X]$

$$b = c(b)c(G(X^p)) = c(bG(X^p)) = c(aFH') = ac(F)c(H') = a$$

D'où dans $\mathbb{Z}[X]$, $F \mid G(X^p)$ et $H \in \mathbb{Z}[X]$.
On écrit $G = a_rX^r + ... + a_0$, donc

$$G(X^p) = a_rX^{rp} + ... + a_0$$

D'où dans $\mathbb{F}_p[X]$ grâce au morphisme de Frobenius,

$$\overline{G(X^p)} = \overline{a_r}X^{pr} + ... + \overline{a_0} = \overline{a_p}^pX^{pr} + ... + \overline{a_0}^p = (\overline{a_r}X^r + ...\overline{a_0})^p = \overline{G}^p$$

Soit φ facteur irréductible de $\overline{F}$ sur $\mathbb{F}_p$.
Or

$$\overline{G}^p = \overline{G(X^p)} = \overline{FH} = \overline{F}\ \overline{H}$$

D'où par le lemme d'Euclide $\varphi \mid \overline{G}$.
Or dans $\mathbb{Z}[X]$, $FG \mid \phi_n$, donc dans $\mathbb{F}_p[X]$, $\overline{FG} \mid \overline{\phi_n}$, d'où

$$\varphi^2 \mid \overline{\phi_n} = \phi_{n,\mathbb{F}_p}$$

Ainsi dans un corps de décomposition de ϕ_n sur $\mathbb{F}_p$, $\overline{\phi}_n$ a une racine double ce qui est absurde car $(X^n - 1)' = nX^{n-1} \neq 0$ et $n \wedge p = 1$ ie $X^n - 1$ sans racine double dans $\mathbb{F}_p$.
Par conséquent

$$F = G$$

<u>Etape 2 : Egalité des polynômes minimaux de tous les $z \in \mu_n^*(\mathbb{C})$</u>
Soit z' une racine primitive n-ième de l'unité, alors $z' = z^m$, avec $m = p_1^{\alpha_1}...p_r^{\alpha_r}$ et p_i ne divisant pas n pour tout $i \in [\![1, r]\!]$.
Alors z et z^{p_1} ont même polynôme minimal d'après ce qui précède car p_1 ne divise pas n.
Or z^{p_1} est également une racine n-ième primitive de l'unité donc z^{p_1} et $(z^{p_1})^{p_1} = z^{p_1^2}$ ont même polynôme minimal. Ainsi z et $z^{p_1^2}$ ont même polynôme minimal.
Par conséquent, par itérations successives, z et $z^{p_1^{\alpha_1}}$ ont même polynôme minimal.
De même $z^{p_1^{\alpha_1}}$ est une racine n-ième primitive de l'unité et p_2 ne divise pas n, donc d'après

ce qui précède $z^{p_1^{\alpha_1}}$ et $(z^{p_1^{\alpha_1}})^{p_2^{\alpha_2}}$ ont même polynôme minimal. Ainsi z et $z^{p_1^{\alpha_1}p_2^{\alpha_2}}$ ont même polynôme minimal.
Par conséquent, par itérations successives, z et $z' = z^m = z^{p_1^{\alpha_1}\dots p_r^{\alpha_r}}$ ont même polynôme minimal.
Etape 3 : Conclusion
En particulier $F(z') = 0$, donc F admet toutes les racines n-ième primitives de l'unité, d'où

$$deg(F) \geq \phi(n)$$

Or $F \mid \phi_n$, d'où

$$F = \phi_n$$

En particulier ϕ_n est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Z}$ car unitaire. □

Proposition. (S'il reste du temps) Soit $n \in \mathbb{N}^*$, alors le polynôme cyclotomique ϕ_n est unitaire à coefficients dans $\mathbb{Z}$.

Démonstration.
On raisonne par récurrence sur $n \in \mathbb{N}^*$:
- Pour $n = 1$, on a $\phi_1 = X - 1 \in \mathbb{Z}[X]$ unitaire.
- On suppose la propriété vraie pour tout $d \in [\![1, n-1]\!]$, alors $P := \prod_{\substack{d=1 \\ d|n}}^{n-1} \phi_d \in \mathbb{Z}[X]$ unitaire.
  On effectue la division euclidienne de $X^n - 1$ par P unitaire (en particulier de coefficient dominant inversible) dans $\mathbb{Z}[X]$: il existe $(Q, R) \in \mathbb{Z}[X]^2$ tel que

  $$X^n - 1 = PQ + R \text{ et } deg(R) < deg(P)$$

  Ainsi Q est unitaire.
  Or dans $\mathbb{C}[X]$ on a $X^n - 1 = \phi_n P$, donc

  $$P(\phi_n - Q) = R$$

  Or $deg(R) < deg(P)$, d'où $\phi_n = Q \in \mathbb{Z}[X]$ unitaire.

□

Proposition. (S'il reste encore du temps) Soit $n \in \mathbb{N}^*$, alors $X^n - 1 = \prod_{\substack{d=1 \\ d|n}}^{n} \phi_d$, ainsi $deg(\phi_n) = \varphi(n)$.

Démonstration.
On a l'égalité ensembliste $\mu_n(\mathbb{C}) = \bigsqcup_{\substack{d=1 \\ d|n}}^{n} \mu_d^*(\mathbb{C})$ car pour tout racine n-ième de l'unité, son ordre divise n.
Donc

$$X^n - 1 = \prod_{z \in \mu_n(\mathbb{C})} (X - z) = \prod_{\substack{d=1 \\ d|n}}^{n} \prod_{z \in \mu_d^*(\mathbb{C})} (X - z) = \prod_{\substack{d=1 \\ d|n}}^{n} \phi_d$$

□