/

Irréductibilité de Φ_n

Leçons: 102, 141.

Enoncé: $n \geq 1$. Le n^e polynôme cyclotomique Φ_n est irréductible sur $\mathbb{Z}$ et $\mathbb{Q}$, et $\pi_\zeta^{\mathbb{Q}} = \Phi_n$ pour toute racine primitive n^e de l'unité $\zeta \in U_n'$.

Preuve.

- D'abord, $\Phi_n \in \mathbb{Z}[X]$ est unitaire et non constant donc il est irréd sur $\mathbb{Z}$ ssi irréd sur $\mathbb{Q}$.

  Soit $\zeta \in U_n'$: on note $\pi_\zeta = \pi_\zeta^{\mathbb{Q}}$ son polynôme minimal sur $\mathbb{Q}$. On écrit la décomposition en facteurs irréd (DFi) de Φ_n dans $\mathbb{Z}[X]$: $\Phi_n = P_1 \cdots P_r$ avec $P_i \in \mathbb{Z}[X]$ irréd (non nécessairement 2à2 $\neq$). Φ_n étant unitaire on peut supposer P_i unitaire pour tout $1 \leq i \leq r$. En particulier les P_i sont non constants donc irréd sur $\mathbb{Q}$. Ainsi Φ_n a les mêmes DFI dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.
  Revenons à ζ : π_ζ est irréd dans $\mathbb{Q}[X]$ et divise Φ_n dans $\mathbb{Q}[X]$, donc $\pi_\zeta = P_i$ pour un certain $1 \leq i \leq r$. En particulier $\pi_\zeta \in \mathbb{Z}[X]$ (et ζ est irréd car unitaire) et $\pi_\zeta \mid \Phi_n$ dans $\mathbb{Z}[X]$.

- On prend $\zeta \in U_n'$ et $p \nmid n$ un premier, et on note $P = \pi_\zeta$ et $Q = \pi_{\zeta^p}$. Mq $P = Q$.

  D'abord $\zeta^p \in U_n'$, donc on peut lui appliquer ce qui précède. Par l'absurde supq $P \neq Q$. Vu que $P, Q \in \mathbb{Z}[X]$ sont irréd dans $\mathbb{Z}[X]$ et divisent Φ_n dans $\mathbb{Z}[X]$, $PQ \mid \Phi_n$ dans $\mathbb{Z}[X]$.
  On cherche donc à trouver à P et Q un facteur commun (ce sera possible en jouant modulo p).
  ζ est racine de $Q(X^p)$ donc $P \mid Q(X^p)$ dans $\mathbb{Q}[X]$. En fait on vérifie que cette relation a encore lieu dans $\mathbb{Z}[X]$: soit $R \in \mathbb{Q}[X]$ tq $PR = Q(X^p)$. Il existe $h \in \mathbb{N}^*$ tq $hR \in \mathbb{Z}[X]$: on a, dans $\mathbb{Z}[X]$, $P \cdot (hR) = h\, Q(X^p)$. En passant au contenu c, $c(P)\, c(hR) = h\, c(Q)$ cad $c(hR) = h$: $R = \frac{1}{h}(hR) \in \mathbb{Z}[X]$.
  Passons dans $\mathbb{F}_p[X]$. En écrivant $Q = \sum_{i=0}^{d} a_i X^i$: $\overline{Q(X^p)} = \sum_{i=0}^{d} \overline{a_i} X^{ip} = \sum_{i=0}^{d} (\overline{a_i} X^i)^p = \left(\sum_{i=0}^{d} \overline{a_i} X^i\right)^p = \overline{Q}^p$.
  Ainsi $\overline{P} \mid \overline{Q}^p$ dans $\mathbb{F}_p[X]$. Soit $\overline{S} \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{P}$: $\overline{S} \mid \overline{Q}^p$ donc $\overline{S} \mid \overline{Q}$ par le lemme d'Euclide. Or $\overline{P}\,\overline{Q} \mid \overline{\Phi_n} \mid X^n - \overline{1}$ donc $\overline{S}^2 \mid X^n - \overline{1}$. Mais $(X^n - \overline{1})' = \overline{n} X^{n-1}$ avec $\overline{n} \neq 0$ (car $p \nmid n$) donc $X^n - \overline{1}$ est à racines simples dans son corps de décomposition, donc sans facteur carré : c'est absurde! On conclut que $P = Q$.

- Soient $\zeta, \zeta' \in U_n'$: $\zeta' = \zeta^m$ avec $m \wedge n = 1$, donc $m = p_1 \cdots p_r$ avec $p_i \nmid n$ premiers (non nécessairement 2à2 $\neq$). On montre par réc sur $r \in \mathbb{N}$ que $\pi_\zeta = \pi_{\zeta'}$. Initialisation : $r = 0$ donc $m = 1$ et $\zeta = \zeta'$. Hérédité : supq vrai pour $r \in \mathbb{N}$ fixé, mq vrai pour $r+1$. $\zeta' = (\zeta^{p_1 \cdots p_r})^{p_{r+1}}$ a même polynôme minimal que $\zeta^{p_1 \cdots p_r}$ (par le point précédent et car $\zeta^{p_1 \cdots p_r} \in U_n'$), qui a par HR le même polynôme minimal que ζ. Donc $\pi_{\zeta'} = \pi_\zeta$.
  Ainsi finalement π_ζ annule tout $\zeta' \in U_n'$: par déf de Φ_n, $\Phi_n \mid \pi_\zeta$ dans $\mathbb{Q}[X]$. Comme on sait déjà que $\pi_\zeta \mid \Phi_n$ et que π_ζ est unitaire, cela prouve que $\Phi_n = \pi_\zeta$. En particulier Φ_n est irréd sur $\mathbb{Q}$, et sur $\mathbb{Z}$.

□

Complément 1 : justification de : si $P = P_1 \cdots P_r$ DFi dans $\mathbb{Z}[X]$ avec P unitaire, on peut supposer que pour tout $1 \leq i \leq r$, P_i est unitaire.

Preuve. Réc sur $r \geq 1$. Initialisation : $r=1$ donc $P = P_1$ est unitaire. Hérédité : sq vrai pour $r \geq 1$ fixé, mq vrai pour $r+1$. S'il existe $1 \leq i \leq r+1$ tq P_i unitaire, $\prod_{j \neq i} P_j$ unitaire : par HR on peut supposer $\forall j \neq i$, P_j unitaire. Sinon il existe $i \neq i'$ tq P_i et $P_{i'}$ aient pour coef dom -1 (car $\mathbb{Z}^\times = \{-1, 1\}$) : on les remplace par leurs opposés ce qui ne change pas $P_i P_{i'}$; de plus $\prod_{j \notin \{i,i'\}} P_j$ unitaire : par HR on peut supposer $\forall j \notin \{i,i'\}$, P_j unitaire. □

Complément 2 : propriétés élémentaires de $\Phi_n = \prod_{\zeta \in U_n'} (X - \zeta)$.

(i) $\deg \Phi_n = \varphi(n)$.

(ii) Pour $\ell \in \mathbb{P}$, $\Phi_\ell = \sum_{i=0}^{\ell-1} X^i$.

(iii) $X^n - 1 = \prod_{d \mid n} \Phi_d$.

(iv) $\Phi_n \in \mathbb{Z}[X]$.

Preuve. (i) : car $|U_n'| = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.

(ii) : $U_\ell' = U_\ell \setminus \{1\}$ donc $\Phi_\ell = \frac{X^\ell - 1}{X - 1} = \sum_{i=0}^{\ell-1} X^i$.

(iii) : car $U_n = \bigsqcup_{d \mid n} U_d'$ et $X^n - 1 = \prod_{\zeta \in U_n} (X - \zeta)$.

(iv) : Réc forte sur $n \geq 1$. Initialisation : $n=1$: $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Hérédité : soit $n \geq 2$, sq vrai pour $m < n$. Par (iii), $X^n - 1 = P \Phi_n$ avec $P \in \mathbb{Z}[X]$ unitaire. Comme P unitaire on peut faire la div euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$: $X^n - 1 = PQ + R$. Par unicité de la div euclidienne dans $\mathbb{Q}[X]$, $(Q, R) = (\Phi_n, 0)$; en particulier $\Phi_n \in \mathbb{Z}[X]$. □

Complément 3 : application : un corps de nombres (cad une extension finie de $\mathbb{Q}$) ne contient qu'un nombre fini de racines de l'unité.

Preuve. Soit K un corps de nombres : on note $N = [K : \mathbb{Q}]$. Soit ζ une racine de l'unité tq $\zeta \in K$, soit $n \geq 1$ tq $\zeta \in U_n'$. $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \pi_\zeta = \deg \Phi_n = \varphi(n)$, or $\mathbb{Q}(\zeta) \subset K$ donc $\varphi(n) \leq N$. On note $A = \{ n \geq 1 \mid \varphi(n) \leq N \}$: comme U_n' est fini pour $n \geq 1$, il suffit de mq A est fini.

Soit $n \in A$: si $\ell \mid n$ est premier, $\ell - 1 \mid \varphi(n)$ donc $\ell \leq \varphi(n) + 1 \leq N + 1$. Ainsi l'ens $P = \{ \ell \in \mathbb{P} \mid \exists n \in A, \ell \mid n \}$ est fini. Alors si $n \in A$: $\varphi(n) = n \prod_{\ell \mid n} (1 - \ell^{-1}) \geq n \prod_{\ell \in P} (1 - \ell^{-1})$ car $\{ \ell \in \mathbb{P} \mid \ell \mid n \} \subset P$ et $0 < 1 - \ell^{-1} \leq 1$.

Ainsi $n \leq \dfrac{N}{\prod_{\ell \in P} (1 - \ell^{-1})}$: A est fini. □

Complément 4 : autre preuve dans le cas $n = \ell \in \mathbb{P}$, par le critère d'Eisenstein.

Preuve. $\Phi_\ell = \dfrac{X^\ell - 1}{X - 1}$ donc $\Phi_\ell(X+1) = \dfrac{(X+1)^\ell - 1}{X} = \sum_{k=1}^{\ell} \binom{\ell}{k} X^{k-1}$. Le coef dom est $\binom{\ell}{\ell} = 1$. Le coef constant est $\binom{\ell}{1} = \ell$, non multiple de ℓ^2. Pour $1 \leq k \leq \ell - 1$, $\ell \mid \binom{\ell}{k}$. Le critère d'Eisenstein s'applique : $\Phi_\ell(X+1)$ est irréductible dans $\mathbb{Q}[X]$ (donc dans $\mathbb{Z}[X]$). C'est donc aussi le cas de Φ_ℓ. □

Réf : • Perrin : ↑ 83 (dv).
• Ortiz : ↑ 169 (complément 3).

↳ Corollaire : pour $\zeta \in U_n'$, $[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n)$. Utilisé dans le complément 3 (qui est intéressant à mentionner, dans la leçon 102 notamment).

↳ Les polynômes cyclotomiques sont importants. En effet les racines de l'unité (sur $\mathbb{Q}$ ou sur un autre corps) interviennent fréquemment en algèbre. En particulier tout élément non nul d'un corps fini $x \in \mathbb{F}_q^\times$ est racine de l'unité, puisque $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ avec p sa caractéristique.

↳ Dans le dv : attention il faut mentionner à de nombreuses reprises l'anneau dans lequel une relation est vérifiée ($\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{F}_p[X]$).

↳ On utilise les trois th suivant, avec A un anneau factoriel (pour nous $A = \mathbb{Z}$) (ils se prouvent d'ailleurs les uns à partir des autres, dans cet ordre) :
- si $P, Q \in A[X]$, $c(PQ) = c(P)c(Q)$ avec c le contenu ;
- en notant $K = \mathrm{Frac}\, A$: les irréductibles de $A[X]$ sont d'une part les irréductibles de A, d'autre part les irréductibles primitifs de $K[X]$;
- $A[X]$ est factoriel.

↳ Un certain nb de questions en lien avec ce dv sont traitées dans Ortiz (en plus du complément 3).