Cours d'algèbre - Perrin (p. 82)

Étude des polynômes cyclotomiques

102 (121) 141
(108) 123 144
120 125

Soit $n\in\mathbb{N}^*$. On note $\mu_n=\{z\in\mathbb{C}^* \mid z^n=1\}$ l'ensemble des racines n-ièmes de l'unité et $\mu_n^\times=\{z\in\mathbb{C}^* \mid \forall p\wedge n=1,\ p<n \Rightarrow z^p\neq 1,\ z^n=1\}$ celui des racines primitives n-ièmes de l'unité.

On appelle n-ième polynôme cyclotomique :

$$\Phi_n(X)=\prod_{\xi\in\mu_n^\times}(X-\xi)$$

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

Théorème : Soit $n\in\mathbb{N}^*$.
Alors : Φ_n est à coefficients entiers, unitaire et irréductible dans $\mathbb{Z}[X]$

oral

Preuve :

L'idée pour montrer ce résultat est de :
1. Mq : $\Phi_n\in\mathbb{Z}[X]$ et unitaire par récurrence
2. Se préparer à montrer que Φ_n est irréductible sur $\mathbb{Q}$
3. Montrer une certaine égalité de polynômes minimaux de racines primitives n-ièmes.
4. Répéter le procédé à toutes les racines primitives n-ièmes pour montrer l'irréductibilité sur $\mathbb{Q}$.
5. Utiliser le contenu de Φ_n pour montrer son irréductibilité sur $\mathbb{Z}$.

Soit $n\in\mathbb{N}^*$.

① Montrons que Φ_n est unitaire à coeffs entiers.
Montrons-le par récurrence sur n.

* Initialisation : $\Phi_1(X)=X-1\in\mathbb{Z}[X]$ unitaire ✓
* Hérédité : Supposons que pour tout $d\in\mathbb{N}$ tel que $d<n$ et $d\mid n$, $\Phi_d\in\mathbb{Z}[X]$ unitaire.

Soit $F(X)=\prod_{\substack{d\mid n\\ d<n}}\Phi_d(X)\in\mathbb{Z}[X]$ unitaire.

Par division euclidienne, il existe $Q,R\in\mathbb{Z}[X]$ avec Q unitaire et $\deg(R)<\deg(F)$ tels que :

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

Ainsi, $F(X)\left[\Phi_n(X)-Q(X)\right]=R(X)$

Or : $\deg(R)<\deg(F)$ donc $\Phi_n-Q=0$

Alors $\Phi_n=Q\in\mathbb{Z}[X]$ unitaire.

② Soit K un corps de décomposition de Φ_n sur $\mathbb{Q}$,
ksi → $\xi\in\mu_n^\times$ et p premier tel que $p\nmid n$.
Soit f et g polynômes minimaux de ξ et ξ^p respectivement (a priori dans $\mathbb{Q}[X]$).

Or : $\mathbb{Z}[X]$ est factoriel et alors $\Phi_n=f_1^{\alpha_1}\times\dots\times f_r^{\alpha_r}$ avec f_i irréductibles et unitaires (quitte à multiplier par -1)
Ainsi, ξ est racine d'un f_i et par minimalité de f, $f=f_i$ et alors $f\mid\Phi_n$. De même, $g\mid\Phi_n$.

③ Montrons que $f=g$.
Supposons par l'absurde que $f\neq g$.
Puisque $g(\xi^p)=0$, alors ξ est racine de $g(X^p)$
Il existe alors $h\in\mathbb{Z}[X]$ tel que $g(X^p)=f(X)h(X)$
En notant $g(X)=a_rX^r+\dots+a_0$ et en projetant sur $\mathbb{F}_p$,

$$\bar{g}(X^p)=(a_rX^r+\dots+a_0)^p \text{ (par Frobenius)}$$
$$=\bar{g}(X)^p=\bar{f}(X)\bar{h}(X)$$

Soit alors φ facteur irréductible de $\bar{f}$.
Puisque $\bar{g}(X)^p=\bar{f}(X)\bar{h}(X)$, par le lemme d'Euclide, $\varphi\mid\bar{g}$ et comme $fg\mid\Phi_n$, $\varphi^2\mid\overline{\Phi_n}$.
Ainsi, dans un corps de décomposition de $\overline{\Phi_n}$ sur $\mathbb{F}_p$, $\overline{\Phi_n}$ a une racine double et alors X^n-1 aussi.
ABSURDE car $\frac{d}{dX}(X^n-1)=nX^{n-1}$ et puisque $p\nmid n$, alors la seule racine de nX^{n-1} est 0 qui n'annule pas X^n-1 qui n'a alors que des racines simples.

Alors $f=g$

④ Soit $\xi'\in\mu_n^\times$ telle que $\xi'=\xi^m$ avec $m\wedge n=1$ et $m=p_1^{\alpha_1}\times\dots\times p_r^{\alpha_r}$ et $p_i\nmid n$.
En itérant le résultat précédent, ξ' et ξ ont même polynôme minimal f.
Ceci étant valable pour tout élément de $\mu_n^\times$, tous ceux-ci sont racines de f.
donc : $\Phi_n\mid f$, d'où : $\Phi_n=f$ irréductible.

⑤ Φ_n est unitaire donc $c(\Phi_n)=1$ et irréductible sur $\mathrm{Frac}(\mathbb{Z})$ donc Φ_n est irréductible sur $\mathbb{Z}$.

Preuves des résultats utilisés :

Théorème : $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Preuve :

- Montrons que $X^n - 1 \mid \prod_{d|n} \Phi_d(X)$

  Soit α racine de X^n-1 i.e. $\alpha \in \mu_n$ et $d := \mathrm{ord}(\alpha)$. Ainsi, $\alpha \in \mu_d^\times$ (car $|\mu_d| = d$).
  Alors α est racine Φ_d.
  Par ailleurs, par le théorème de Lagrange, $d = \mathrm{ord}(\alpha) \mid |\mu_n| = n$.
  Ceci étant vrai pour toute racine de $X^n - 1$,
  $$X^n - 1 \mid \prod_{d|n} \Phi_d(X)$$

- Montrons que $\prod_{d|n} \Phi_d(X) \mid X^n - 1$

  Soit β racine de $\prod_{d|n} \Phi_d(X)$, en particulier racine de $\Phi_d(X)$ avec $d|n$.
  $$\beta^n = \beta^{d \times \frac{n}{d}} = (\beta^d)^{\frac{n}{d}} = 1$$
  donc : β est aussi racine de $X^n - 1$.
  Ceci étant vrai pour toute racine de $\prod_{d|n} \Phi_d(X)$,
  $$\prod_{d|n} \Phi_d(X) \mid X^n - 1$$

Théorème : Soit $P \in \mathbb{A}[X]$ de degré ≥ 1 et primitif $c(P) = 1$.
Alors : si P est irréductible sur $\mathrm{Frac}(\mathbb{A})$, alors il l'est sur $\mathbb{A}$ aussi.

Preuve :
Supposons $P = QR$
Puisque P est irréductible sur $\mathrm{Frac}(\mathbb{A})$,
qps $Q \in \mathrm{Frac}(\mathbb{A})(X)^\times$ i.e. $Q = a \in \mathrm{Frac}(\mathbb{A})^*$
Alors $P = aR$ et puisque $a \mid c(P) = 1$,
$a \in \{\pm 1\}$ donc $a \in \mathbb{A}^\times$ i.e. $Q \in \mathbb{A}^\times$.

Temps
13' 51''