

Réductibilité des polynômes cyclotomiques [CVA] p.220

Recherches: 120, 123, 125, 141, 127

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

Soit p premier, $p \nmid n$.

Proposition:

Soit K un corps contenant $\mathbb{F}_p$.
 $F: \sum_{i=0}^m a_i x^i \in K[X] \mapsto \sum_{i=0}^m a_i^p x^i \in K[X]$ est un morphisme d'anneaux.

Preuve:

Mg $F: \sum_{i=0}^m a_i x^i \mapsto \sum_{i=0}^m a_i^p x^i$ est un morph. d'anneaux.

Soient $P = \sum_{i=0}^m a_i x^i, Q = \sum_{i=0}^m b_i x^i \in K[X]$.

On a, pour $i \in [0, \max(m, m)]$, $(a_i + b_i)^p = a_i^p + b_i^p$
 et $(a_i b_i)^p = a_i^p b_i^p$

D'où $F(P+Q) = F(P) + F(Q)$ et $F(PQ) = F(P)F(Q)$.

D'où F est bien un morph. d'anneaux de $K[X]$ au lui-même.

$$(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k}$$

$\uparrow$
 $\binom{p}{k} \equiv 0 \pmod{p}$ pour $1 \leq k \leq p-1$
 $= a^p + b^p$

Théorème:

Soit α racine de Φ_m dans K . Soit m l'ordre de p dans $(\mathbb{Z}/m\mathbb{Z})^\times$.
 (i) $\alpha^m = \bar{1}$ (ii) m est le plus petit $k \in \mathbb{N}^*$ t.q. $\alpha^{p^k} = \alpha$.

Preuve: (i) Mg $\alpha^m = \bar{1}$.

On a: $X^m - 1 = \prod_{d|m} \Phi_d(X)$, $\Phi_d \in \mathbb{Z}[X]$

Donc, par réduction mod p : $X^m - \bar{1} = \prod_{d|m} \bar{\Phi}_d(X) \in \mathbb{F}_p[X]$
 (*)

Puisque $\mathbb{F}_p[X] \subset K[X]$, on évalue en α :

$$\alpha^m - \bar{1} = 0 \quad \text{donc} \quad \alpha^m = \bar{1}$$

Notons m l'ordre de p dans $(\mathbb{Z}/m\mathbb{Z})^\times$.

(ii) Mg m est le plus petit entier k t.q. $\alpha^{p^k} = \alpha$.

D'abord, on a $\alpha^{p^m} = 1 + mk$, $k \in \mathbb{Z}$ par construction
 donc $\alpha^{p^m} = \alpha(\alpha^m)^k = \alpha \cdot \bar{1} = \alpha$.

Montrons que m est minimal.

Pour cela, montrons que α est d'ordre m dans $K^\times$.

En effet, on a $\alpha^{p^k-1} = \bar{1}$ donc k est le plus petit t.q. $m | p^k - 1$.

xi h est le plus petit entier tq $p^h \equiv 1 \pmod{m}$, m étant minimal par construction (c'est l'ordre de p dans $(\mathbb{Z}/m\mathbb{Z})^\times$)

On a d'abord $\alpha^m = \bar{1}$ par ce qui précède.

Soit $d \mid m$, $d \neq m$. Montrons que $\alpha^d \neq \bar{1}$.

Par l'absurde

Pour cela on suppose, en vue d'une contradiction, que $\alpha^d = \bar{1}$.

Alors par (*) pour $m = d$, on a $\overline{\Phi_d'}(\alpha) = 0$ pour un $d' \mid d$.

Donc $d' \neq m$. Ainsi α annule $\overline{\Phi_{d'}}$ et $\overline{\Phi_m}$ et est une racine double du polynôme à racines simples $X^m - \bar{1}$.

Ceci étant absurde, m est minimal.

Théorème:

Si $(\mathbb{Z}/m\mathbb{Z})^\times$ n'est pas cyclique, alors pour tout $p \nmid m$, $\overline{\Phi_m}$ est irréductible sur $\mathbb{F}_p$.

Preuve:

Ng Si $m < \varphi(m)$, $\overline{\Phi_m}$ est irréductible sur $\mathbb{F}_p$.

Soit $Q = \prod_{k=0}^{m-1} (X - \alpha^{p^k})$

On a $Q \in \mathbb{F}_p[X]$ car $F(Q) = Q$.

D'autre part, on a $0 < \deg Q = m < \varphi(m) = \deg \overline{\Phi_m}$.

Ng $Q \mid \overline{\Phi_m}$

Les racines de Q sont les α^{p^k} , $k=0, \dots, m-1$.

On a α est racine de $\overline{\Phi_m}$ et pour $P \in K[X]$, si α est racine de P , α^{p^k} aussi.

D'autre part, les $\alpha^{p^0}, \alpha^{p^1}, \dots, \alpha^{p^{m-1}}$ sont distinctes par minimalité de m .

Il suit que $Q \mid \overline{\Phi_m}$ donc $\overline{\Phi_m}$ est irréductible sur $\mathbb{F}_p$.

Conclusion: Soit $p \nmid m$.

Si $(\mathbb{Z}/m\mathbb{Z})^\times$ n'est pas cyclique, nécessairement $m = o(p) < o((\mathbb{Z}/m\mathbb{Z})^\times) = \varphi(m)$.

Par ce qui précède $\overline{\Phi_m}$ est irréductible sur $\mathbb{F}_p$.

□

On aura alors un diviseur strict de $\overline{\Phi_m}$ non inversible $\rightarrow$

Soit $0 \leq h \leq h' \leq m-1$

tg $\alpha^{p^{h'}} = \alpha^{p^h}$
Alors $\alpha^{p^{h'} - h} = \bar{1}$ avec $0 \leq h' - h \leq m$ donc $h' - h$ est un min. de m .