Développement : Irréductibilité des polynômes cyclotomiques et application aux extensions finies de $\mathbb{Q}$.

RM

2022-2023

Référence :

1. Cours d'algèbre Perrin
2. Exercice d'algèbre Ortiz

Énoncé :

Soit $\Phi_{n,\mathbb{Q}}(X) = \prod_{\zeta \in \mu_n^*(K_n)}(X - \zeta)$ le n-ième polynôme cyclotomique dans $K_n[X]$ (K_n corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$, $\mu_n(K_n)$ racines de l'unité dans K_n et $\mu_n^*(K_n)$ racines primitives de l'unité dans K_n).
Alors $\Phi_n(X)$ est irréductible sur $\mathbb{Z}[X]$ (et donc dans $\mathbb{Q}[X]$).

On suppose avant que l'on connaît que :
- $X^n - 1 = \prod_{d|n} \Phi_d(X)$ (avec $\mu_n = \sqcup_{d|n}\mu_d^*$).
- $\Phi_n(X) \in \mathbb{Z}[X]$ (Par récurrence avec la division de $X^n - 1$).

Résolution :

On se place sur un corps décomposition K de Φ_n sur $\mathbb{Q}$.
Soit $\zeta \in \mu_n^*(K)$ et p un nombre premier, ne divisant pas n. On a alors que ζ^p est une autre racine primitive de 1, car $p \wedge n = 1$ (qui implique $ppcm(n, p) = np$).
Soit $f, g \in \mathbb{Q}[X]$ les polynômes minimaux de ζ et ζ^p respectivement sur $\mathbb{Q}$. Alors on a $f, g \in \mathbb{Z}[X]$. En effet, comme $\mathbb{Z}[X]$ est factoriel (car par théorème de Gauss, $A[X]$ est factoriel si A est factoriel) , on a alors

$$\Phi_n(X) = f_1(X)^{\alpha_1}...f_r(X)^{\alpha_r}$$

avec $f_i \in \mathbb{Z}[X]$ irréductible. Comme Φ_n est unitaire, il en est de même des f_i (quitte à multiplier par -1).
Mais comme ζ est une racine de Φ_n, alors il existe un i_0 tel que $f_{i_0}(\zeta) = 0$, ou f_{i_0} est un polynôme de $\mathbb{Z}[X]$ irréductible et unitaire, donc sur $\mathbb{Q}[X]$ aussi. Par définition de f, on a que $f = f_{i_0}$ et de même pour g.
On a donc que f et g sont dans $\mathbb{Z}[X]$ et divisent chacun Φ_n.
On va maintenant montrer que $f = g$.
Si ce n'est pas le cas, alors comme f, g sont irréductibles et distincts, le produit $f.g$ divise Φ_n dans $\mathbb{Z}[X]$. Par ailleurs, comme $g(\zeta^p) = 0$, ζ est racine du polynôme $g(X^p)$, donc $f(X)$ divise $g(X^p)$, a priori dans $\mathbb{Q}[X]$, mais aussi dans $\mathbb{Z}[X]$. En effet

$$g(X^p) = f(X)h(X) \text{ avec } h \in \mathbb{Q}[X].$$

On écrit $h = \frac{a}{b}h'$ ou $h' \in \mathbb{Z}[X]$ de contenue 1, et comme g et f sont unitaires, on a que $c(g) = c(f)c(\frac{a}{b}h')$ ce qui équivaut à $1 = \frac{a}{b}$. Donc $h = h'$ et donc $h \in \mathbb{Z}[X]$.

la transformation de $h = \frac{a}{b}h'$ se réalise en multipliant par b toues les coefficients de h de sorte que tous ces coefficients soient entiers, puis on calcule le contenue du polynôme bh qu'on note a, on a donc que le polynôme $\frac{b}{a}h = h'$ est un polynôme dans $\mathbb{Z}[X]$ de contenue 1.

On écrit $g(X) = \sum_{i=0}^{r} a_i X^i$, d'où $g(X^p) = \sum_{i=0}^{r} a_i X^{pi}$. Mais il est intéressant de notée que modulo p, on a $\overline{a_i} = \overline{a_i}^p$ dans $\mathbb{F}_p$. On se projette alors dans $\mathbb{F}_p$:

$$\overline{g}(X^p) = \sum_{i=0}^{r} \overline{a_i} X^{pi} = \sum_{i=0}^{r} \overline{a_i}^p X^{pi} = \sum_{i=0}^{r} (\overline{a_i} X^i)^p \underset{\text{car } car \mathbb{F}_p = p}{=} \left(\sum_{i=0}^{r} \overline{a_i} X^i \right)^p = \overline{g}(X)^p.$$

Soit alors $\varphi(X)$ un facteur irréductible de $\overline{f}(X)$ sur $\mathbb{F}_p$. On a donc que $\overline{g}(X^p) = \overline{g}(X)^p = \overline{f}(X)\overline{h}(X)$. Donc comme $\varphi(X)$ est un facteur irréductible, par le lemme d'Euclide, on en déduit que φ divise $\overline{g}$ ou $\overline{g}^{p-1}$, et en réitérant le processus sur $\overline{g}^{p-1}$, on en déduit que φ divise $\overline{g}$.
Comme fg divise Φ_n sur $\mathbb{Z}$, $\overline{f}\overline{g}$ divise $\overline{\Phi_n}$ sur $\mathbb{F}_p$, donc φ^2 divise $\overline{\Phi_n} = \Phi_{n,\mathbb{F}_p}$.

En effet, prouvons le par récurrence. On a bien $\overline{\Phi_1} = \overline{X-1} = X - 1 = \Phi_{1,\mathbb{F}_p}$. Sinon on suppose cela vrai pour $d < n$. On sait dans $\mathbb{Z}[X]$ que

$$X^n - 1 = \Phi_{n,\mathbb{Q}}(X)F(X) \text{ avec } F(X) = \prod_{d|n, d\neq n} \Phi_{d,\mathbb{Q}}(X).$$

On sait aussi que $X^n - 1 = \overline{X^n - 1} = \overline{\Phi_{n,\mathbb{Q}}(X)F(X)} = \overline{\Phi_{n,\mathbb{Q}}}\overline{F(x)}$. Or par hypothèse de récurrence, on a

$$\overline{F}(X) = \prod_{d|n, d\neq n} \overline{\Phi_{d,\mathbb{Q}}}(X) = \prod_{d|n, d\neq n} \Phi_{d,\mathbb{F}_p} = G(X)$$

Comme on a aussi $X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{F}_p} = \Phi_{n,\mathbb{F}_p} G(X) = \overline{\Phi_{n,\mathbb{Q}}} G(X)$, on a alors $(\Phi_{n,\mathbb{F}_p} - \overline{\Phi_{n,\mathbb{Q}}})G(x) = 0$ et on en conclut $\Phi_{n,\mathbb{F}_p} = \overline{\Phi_{n,\mathbb{Q}}}$ par intégrité de $\mathbb{F}_p[X]$.

Mais cela signifie que dans un corps de décomposition de Φ_n sur $\mathbb{F}_p$, $\overline{\Phi_n}$ aura une racine double. Or $P_n(X) = X^n - 1$ a pour dérivée $P_n'(X) = nX^{n-1}$ et comme p ne divise pas n, on a que la seule racine de P_n' est 0, qui n'annule pas P_n. Donc P_n n'a que des racines simples. C'est donc absurde.
On a finalement que $f = g$.
Soit ζ' une racine primitive n-ième, on a alors $\zeta' = \zeta^m$, où $m \wedge n = 1$, donc si $m = p_1^{\alpha_1} ... p_r^{\alpha_r}$, on a $p_i \not| n$. On en déduit du travail précédent que ζ et ζ' ont même polynôme minimal sur $\mathbb{Q}$, donc on a $f(\zeta') = 0$ de sorte que f admet toutes les racines primitives de l'unité comme zéros. On sait donc qu'il y a $\varphi(n)$ racines et donc $deg(f) \geq \varphi(n) = deg(\Phi_n)$. Or comme $f|\Phi_n$, on en déduit que $f = \Phi_n$. On a donc que Φ_n est irréductible sur $\mathbb{Q}$,donc sur $\mathbb{Z}$ car $c(\Phi_n) = 1$ car unitaire et $\mathbb{Q}$ corps des fractions de $\mathbb{Z}$.

Application 1 : Soit K une extension finie de $\mathbb{Q}$. Il y a alors un nombre fini de racines de l'unité dans $\mathbb{K}$.

Résolution :

Toute racine de l'unité étant aussi une racine primitive de l'unité, il suffit de montrer qu'il n'y a qu'un nombre fini de racines primitive de l'unité dans K. Soit $N = [K : \mathbb{Q}]$. Si $u \in K$ est une racine primitive n-ème de 1 dans K alors, comme $\mathbb{Q}(u) \subseteq K$, par multiplicativité, $[\mathbb{Q}(u); \mathbb{Q}]$ divise N et en particulier, $\varphi(n) \leq N$.
Pour conclure, il suffit de montrer que $X = \{n \geq 2; \varphi(n) \leq N\}$ est fini. Soit p un facteur premier de $n \in X$. Comme $p - 1|\varphi(n)$(car $\varphi(n) = \prod_{i=1}^{r}(p_i - 1)p^{\alpha_i - 1}$), on a $p \leq N + 1$ donc l'ensemble $\mathcal{P}$ des facteurs premiers des éléments de X est fini. D'autre part, si $n \geq 2$ alors on a aussi

$\varphi(n) = n\prod_{p\in\mathcal{P}p|n}(1-\frac{1}{p})$. On conclut alors que

$$n\prod_{p\in\mathcal{P}}(1-\frac{1}{p}) \leq n\prod_{p\in\mathcal{P}p|n}(1-\frac{1}{p}) = \varphi(n) \leq N$$

Finalement on a

$$n \leq \frac{N}{\prod_{p\in\mathcal{P}}(1-\frac{1}{p})}$$

et donc X est bien fini.