102
125
141
(144)

Irréductibilité des polynômes cyclotomiques

- Théorie de Galois, GOZARD, p 69
- Algèbre pour l'agreg, Rombaldi, p 384
- Cours d'Algèbre, Perrin, p 80

Notation : On note U_n l'ensemble des racines n-ièmes de l'unité, et U_n^* l'ensemble des racines primitives n-ièmes de l'unité

PER 80 **Déf :** On appelle n-ième polynôme cyclotomique le polynôme : $\Phi_n(X) = \prod_{\xi \in U_n^*} (X - \xi)$

ROM 384 **Lemme 1 :** Soit $P, Q \in \mathbb{Q}[X]$ non nuls. On suppose que $PQ \in \mathbb{Z}[X]$ ~~et que $P \neq Q$~~. On suppose que P et Q sont unitaires. Alors P et Q sont dans $\mathbb{Z}[X]$.

Dém : En posant m le PPCM des dénominateurs de P et Q, on a alors $mP = P_1 \in \mathbb{Z}[X]$ et $mQ = Q_1 \in \mathbb{Z}[X]$

Donc $m^2 PQ = P_1 Q_1$ dans $\mathbb{Z}[X]$ et en passant au contenu : $m^2 . c(PQ) = c(P_1)\, c(Q_1)$

On $c(PQ) = 1$ car PQ est unitaire dans $\mathbb{Z}[X]$

Ainsi $m^2 = c(P_1)\, c(Q_1)$, et $c(P_1)$ et $c(Q_1)$ divisent m car m est le coeff dominant de ces polynômes

Ainsi $c(P_1) = c(Q_1) = m$

Donc $P = \frac{P_1}{c(P_1)} \in \mathbb{Z}[X]$ et $Q = \frac{Q_1}{c(Q_1)} \in \mathbb{Z}[X]$.

GOZ 69 **Théorème :** pour tout $n \in \mathbb{N}^*$, $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

Dém : ~~Soit K un corps de décomposition de Φ_n sur $\mathbb{Q}$ (on peut prendre $K = \mathbb{C}$)~~

Soit $w \in \mathbb{C}$ une racine n-ième primitive de l'unité : $w \in U_n^*$.

Soit p premier qui ne divise pas n.

Alors m^p est une autre racine primitive n-ième de l'unité. En effet, les générateurs de U_n sont les m^m où $pgcd(m, n) = 1$

Soit $f \in \mathbb{Q}[x]$ le polynôme minimal de m sur $\mathbb{Q}$
~~Soit $g \in \mathbb{Q}[x]$ le polynôme minimal de m^p sur $\mathbb{Q}$~~
Alors par minimalité, f divise $x^n - 1$ dans $\mathbb{Q}[x]$:
$x^n - 1 = f(x).h(x)$ où $h(x) \in \mathbb{Q}[x]$.
On $x^n - 1 \in \mathbb{Z}[x]$ et $f(x)$ étant unitaires, d'après le lemme 1, $h(x) \in \mathbb{Z}[x]$ (et même $f(x) \in \mathbb{Z}[x]$)

Montrons que si m est racine de f, alors m^p est aussi racine de f.
Comme f divise $x^n - 1$ dans $\mathbb{Z}[x]$, on a
$m^n - 1 = 0$
Comme m est racine n-ième de l'unité, alors m^p aussi. Ainsi :
$0 = (m^p)^n - 1 = f(m^p) h(m^p)$
On suppose que $f(m^p) \neq 0$ i.e. m est racine de $h(x^p)$
Alors $h(m^p) = 0$ (par intégrité de $\mathbb{C}$)
On m est racine de f, qui est unitaire et irréductible dans $\mathbb{Q}[x]$: donc f est le poly minimal de m sur $\mathbb{Q}$
Ainsi par minimalité, f divise $h(x^p)$ dans $\mathbb{Q}[x]$: $h(x^p) = f(x)\, g(x)$ avec $g(x) \in \mathbb{Q}[x]$.
Comme $h(x^p) \in \mathbb{Z}[x]$ et que $f, h(x^p)$ sont unitaires, d'après le lemme 1, $g(x) \in \mathbb{Z}[x]$.

On réduit alors modulo p l'égalité :
$$h(x^p) = f(x)\, g(x)$$
Il vient :

(*) En effet, les racines primitives n-ièmes sont de la forme w^m où $m = \prod_{i=1}^{n} p_i^{d_i}$ et $p_i \nmid n$. Alors par rec immédiate, w^{p_1} puis $(w^{p_1})^{p_1}$ puis $w^{p_1^{d_1}}$ puis $(w^{p_1^{d_1-1}})^{p_2^{d_2}} = w^{p_1^{d_1} p_2^{d_2}}$ est racine

PER 83

On écrit $h(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$

d'où $h(x^p) = x^{pn} + a_{n-1}x^{p(n-1)} + \dots + a_1 x^p + a_0$

On d'après le morphisme de Frobenius, dans $\mathbb{F}_p$ comme $\overline{a_i} = \overline{a_i}^p$

alors $\overline{h}(x^p) = x^{pn} + \overline{a_{n-1}}x^{p(n-1)} + \dots + \overline{a_1}x^p + \overline{a_0}$

$= x^{pn} + \left(\overline{a_{n-1}}x^{n-1}\right)^p + \dots + \left(\overline{a_1}x\right)^p + \overline{a_0}^p$

$= \left(x^n + \overline{a_{n-1}}x^{n-1} + \dots + \overline{a_1}x + \overline{a_0}\right)^p$

$= \left(\overline{h(x)}\right)^p$

Ainsi :

$\left(\overline{h(x)}\right)^p = \overline{h(x^p)} = \overline{f(x)}\,\overline{g(x)}$ dans $\mathbb{F}_p[x]$.

Soit $\theta \in \mathbb{F}_p[x]$ un facteur irréductible de $\overline{f}$.

Alors θ divise $\overline{h}^p$ donc divise $\overline{h}$ dans $\mathbb{F}_p[x]$.

D'où θ^2 divise $\overline{f}\,\overline{h} = x^n - \overline{1}$ dans $\mathbb{F}_p[x]$.

Donc $x^n - \overline{1} \in \mathbb{F}_p[x]$ possède une racine double θ

Or la dérivée de $x^n - \overline{1}$ est $\overline{n}x^{n-1}$. Comme p ne divise pas n, alors 0 est la seule racine de la dérivée, et 0 n'annule pas $x^n - \overline{1}$, donc $x^n - \overline{1}$ n'admet que des racines simples.

Contradiction.

Donc $f(w^p) = 0$ pour toute racine w de f.

On w est racine de f, donc tous les w^p sont racines de f, donc toutes les racines primitives n-ièmes de l'unité sont racines de f. (*)

Ainsi $\deg(f) \geq \varphi(n)$

Or comme w est racine de $\Phi_n(x)$, alors par minimalité, $f(x)$ divise $\Phi_n(x)$ dans $\mathbb{Q}[x]$

Comme $\deg(\Phi_n) = \varphi(n)$ et que $f(x)$ et $\Phi_n(x)$ sont tous les deux unitaires, on en déduit que $f(x) = \Phi_n(x)$.

Donc Φ_n est irréductible dans $\mathbb{Q}[x]$, donc dans $\mathbb{Z}[x]$ car il est primitif (Φ_n est unitaire).

irréductible dans $\mathbb{Q}[x]$)

Remarques :

1) On en déduit que le polynôme minimal sur $\mathbb{Q}$ de toute racine primitive n-ème de l'unité w_n dans $\mathbb{C}$, est $\Phi_n(x)$. Donc $[\mathbb{Q}(w_n) : \mathbb{Q}] = \varphi(n)$.
En effet, $\Phi_n(w_n) = 0$ et Φ_n est unitaire et irréductible.

2) On a : $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$
Cela résulte du fait que : $\mu_n = \bigsqcup_{d \mid n} \mu_d^*$ car
$\subset$: Si $x \in \mu_n$, alors $x^n = 1$ et x a un ordre qui divise n d'après Lagrange, donc $x \in \mu_d^*$ pour un certain d, avec $d \mid n$.
$\supset$: Si il existe $d \mid n$ tq $x^d = 1$, alors $x^n = (x^d)^{n/d} = 1$ donc $x \in \mu_n$
Et l'union est disjointe par unicité de l'ordre
Ainsi :
$$x^n - 1 = \prod_{z \in \mu_n} (x - z) = \prod_{d \mid n} \prod_{z \in \mu_n^*} (x - z) = \prod_{d \mid n} \Phi_d(x)$$

3) On a $\Phi_n(x) \in \mathbb{Z}[x]$
On le prouve par récurrence sur n
• $n = 1$: $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$
• On suppose vrai pour $d < n$. Soit $F(x) = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x)$
Par HR, $F(x) \in \mathbb{Z}[x]$. On F unitaire donc on fait la div eucli de $x^n - 1$ par $F(x)$ dans $\mathbb{Z}[x]$:
$x^n - 1 = F(x) P(x) + R(x)$ avec $P, R \in \mathbb{Z}[x]$ et $\deg(R) < \deg(F)$
donc $R(x) = x^n - 1 - F(x) P(x)$
$= F(x)[\Phi_n(x) - P(x)]$ car $x^n - 1 = \Phi_n(x) F(x)$
Par condition sur les degrés, on a $\Phi_n(x) = P(x)$
(car Φ_n unitaire). Donc $\Phi_n(x) \in \mathbb{Z}[x]$.