DÉVELOPPEMENT 21

IRRÉDUCTIBILITÉ DE Φ_n

Lemme. — *Si $f, g \in \mathbb{Q}[X]$ sont unitaires et vérifient $fg \in \mathbb{Z}[X]$, alors $f, g \in \mathbb{Z}[X]$.*

Démonstration. — Soit $a > 0$ le plus petit entier tel que $af \in \mathbb{Z}[X]$, on pose $af = f_1$. Soit $b > 0$ le plus petit entier tel que $bg \in \mathbb{Z}[X]$, on pose $bg = g_1$. Supposons que $ab > 1$ et soit p un diviseur premier de ab, on considère alors les morphismes $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ et $\pi_P : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$. On a $f_1 g_1 = abfg \in \mathbb{Z}[X]$ d'où

$$\pi_P(f_1)\pi_P(g_1) = \pi_P(f_1 g_1) = \pi_P(ab)\pi_P(fg) = 0$$

et il en résulte (puisque $(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre) que $\pi_P(f_1) = 0$ ou $\pi_P(g_1) = 0$, par exemple $\pi_P(f_1) = 0$. On peut alors écrire $f_1 = pf_2$ où $f_2 \in \mathbb{Z}[X]$. Comme f est unitaire et puisque $f_1 = af$, a est le coefficient dominant de f_1, donc p divise a et on écrit $a = pa'$. Il vient donc $pa'f = f_1 = pf_2$ *i.e.* $a'f = f_2 \in \mathbb{Z}[X]$, ce qui est impossible puisque $a' < a$. Donc $ab = 1$ *i.e.* $a = b = 1$. □

Proposition. — *$\phi_{n,\mathbb{Q}}$ est le polynôme minimal sur $\mathbb{Q}$ d'une racine primitive n-è de l'unité. En particulier, $\phi_{n,\mathbb{Q}}$ est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. — Soit ζ une racine primitive n-ième de l'unité et montrons que $\phi_{n,\mathbb{Q}} = \mathrm{Irr}(\zeta, \mathbb{Q})$. Soit p premier ne divisant pas n alors ζ^p est aussi une racine primitive n-è de l'unité ; on pose $f = \mathrm{Irr}(\zeta, \mathbb{Q})$ et $g = \mathrm{Irr}(\zeta^p, \mathbb{Q})$.

• Puisque $\phi_{n,\mathbb{Q}}(\zeta) = 0$, $\phi_{n,\mathbb{Q}}$ est divisible par f donc on peut écrire $\phi_{n,\mathbb{Q}}(\zeta) = fq$ avec $q \in \mathbb{Q}[X]$. Comme f et $\phi_{n,\mathbb{Q}}$ sont unitaires, il en est de même de q. Puisque $\phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$, il résulte du lemme que $f \in \mathbb{Z}[X]$. On obtient de même que $g \in \mathbb{Z}[X]$.

• Puisque $g(\zeta^p) = 0$, ζ est racine de $g(X^p)$ donc $f(X)$ divise $g(X^p)$ *i.e.* $f(X)h(X) = g(X^p)$ avec $h \in \mathbb{Z}[X]$ d'après le lemme. On considère les morphismes $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ et $\pi_P : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$, alors

$$\pi_P\left(f(X)\right)\pi_P\left(h(X)\right) = \pi_P\left(f(X)h(X)\right) = \pi_P\left(g(X^p)\right).$$

Notons $g = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0$, alors

$$\pi_P\left(g(X^p)\right) = X^{dp} + \overline{a_{d-1}}X^{(d-1)p} + \cdots + \overline{a_1}X^p + \overline{a_0}$$

et d'après le théorème de Fermat on a

$$\pi_P\left(g(X^p)\right) = X^{dp} + \overline{a_{d-1}}^p X^{(d-1)p} + \cdots + \overline{a_1}^p X^p + \overline{a_0}^p$$

or l'anneau $(\mathbb{Z}/p\mathbb{Z})[X]$ est de caractéristique p donc

$$\pi_P\left(g(X^p)\right) = X^d + \overline{a_{d-1}}X^{d-1} + \cdots + \overline{a_1}X + \overline{a_0}^p = \left(\pi_P\left(g(X)\right)\right)^p$$

d'où

$$\pi_P\left(f(X)\right)\pi_P\left(h(X)\right) = \left(\pi_P\left(g(X)\right)\right)^p.$$

• Soit $\pi_P(f_1) \in (\mathbb{Z}/p\mathbb{Z})[X]$ un diviseur irréductible de $\pi_P(f(X))$, alors $\pi_P(f_1)$ divise $(\pi_P(g(X)))^p$ donc $\pi_P(f_1)$ divise $\pi_P(g(X))$. Si f et g sont distincts, alors $fg = \text{ppcm}(f,g)$ divise $\phi_{n,\mathbb{Q}}$ or $\phi_{n,\mathbb{Q}}$ divise X^n-1 donc fg divise X^n-1, on écrit $X^n-1 = fgq_1$, d'où

$$X^n - \overline{1} = \pi_P(f)\pi_P(g)\pi_P(q_1).$$

Or $\pi_P(f_1)$ divise $\pi_P(f)$ et $\pi_P(g)$ donc $(\pi_P(f_1))^2$ divise $X^n-\overline{1}$. Soit $(\mathbb{Z}/p\mathbb{Z})(\xi)$ un corps de rupture de $\pi_P(f_1)$ sur $\mathbb{Z}/p\mathbb{Z}$, alors $\pi_P(f_1)(\xi) = 0$ donc ξ est une racine multiple de $X^n-\overline{1}$. Comme p ne divise pas n, on a $\left(X^n-\overline{1}\right)' = nX^{n-1}$ *i.e.* $X^n-\overline{1}$ n'admet pas de racine multiple. Donc $f = g$ *i.e.* si p ne divise pas n, alors $\text{Irr}(\zeta,\mathbb{Q}) = \text{Irr}(\zeta^p,\mathbb{Q})$.

• Soit ζ' une autre racine primitive n-ième de l'unité alors on a $\zeta' = \zeta^m$ pour un entier m premier avec n. Ecrivons $m = p_1^{\varepsilon_1}\cdots p_r^{\varepsilon_r}$, aucun des p_i ne divise n donc on a $\text{Irr}(\zeta,\mathbb{Q}) = \text{Irr}(\zeta^{p_i},\mathbb{Q})$, puis $\text{Irr}(\zeta^{p_i},\mathbb{Q}) = \text{Irr}((\zeta^{p_i})^{p_i},\mathbb{Q})$ et par récurrence, il vient $\text{Irr}(\zeta,\mathbb{Q}) = \text{Irr}(\zeta^{p_i^{\varepsilon_i}},\mathbb{Q})$. Il vient ensuite

$$f = \text{Irr}(\zeta,\mathbb{Q}) = \text{Irr}\left(\zeta^{p_1^{\varepsilon_1}\cdots p_r^{\varepsilon_r}},\mathbb{Q}\right) = \text{Irr}(\zeta^m,\mathbb{Q}) = \text{Irr}(\zeta',\mathbb{Q}).$$

Ainsi, toutes les racines primitives n-ièmes de l'unité sont racines de f donc $\deg f \geq \varphi(n)$. Or on a $fq = \phi_{n,\mathbb{Q}}$ avec $\deg\phi_{n,\mathbb{Q}} = \varphi(n)$ et f et $\phi_{n,\mathbb{Q}}$ unitaires, donc $q = 1$ *i.e.* $\phi_{n,\mathbb{Q}} = \text{Irr}(\zeta,\mathbb{Q})$. □

Leçons concernées

14 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications

15 Groupe des nombres complexes de module 1. Applications

Références

X. Gourdon, *Algèbre*, Ellipses, 1994.

I. Gozard, *Théorie de Galois*, Ellipses, 1997.