Leçon 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Perrin
Szpirglas
Francinou

On considère A un anneau intègre et $\mathbb{K}$ un corps (commutatif).

I - Polynômes irréductibles

1. Définitions et premières propriétés [Per]

Proposition 1.1 On a : $A[X]^* = A^*$.

Définition 1.2 Un polynôme $P \in A[X]$ est dit irréductible si $P \in A^*$ et si pour tous $R, Q \in A[X]$ tels que $P = QR$, $Q \in A^*$ ou $R \in A^*$.

Proposition 1.3 Les assertions suivantes sont équivalentes :
- $A[X]$ est euclidien
- $A[X]$ principal
- A est un corps

Corollaire 1.4 Dans $\mathbb{K}[X]$, P est irréductible si et seulement si (P) est maximal.

Exemple 1.5
$\mathbb{R}[X]/(X^2+1)$ est un corps

2. Critères d'irréductibilité [Szp]

Proposition 1.6 Un polynôme P de $\mathbb{K}[X]$ de degré 2 ou 3 est irréductible si et seulement s'il n'admet pas de racines dans $\mathbb{K}$.

Contre-exemple 1.7
$(X^2+1)^2$ dans $\mathbb{R}[X]$ n'admet pas de racine et est réductible

Théorème 1.8 (critère d'Eisenstein) Soient A factoriel et $\mathbb{K}$ son corps des fractions. Considérons $P = a_0 + a_1 X + \dots + a_n X^n \in A[X]$. Supposons qu'il existe p irréductible de A tel que p ne divise pas a_n, divise tous les autres coefficients et p^2 ne divise pas a_0.
Alors P est irréductible dans $\mathbb{K}[X]$. De plus, si $c(P) = 1$ alors P est irréductible dans $A[X]$.

Lemme 1.9 Soit A un anneau factoriel, de corps des fractions $\mathbb{K}$. Soit $P \in A[X]$, si P est primitif i.e. $c(P) = 1$ alors les assertions suivantes sont équivalentes :
- P est premier dans $A[X]$
- P est irréductible dans $\mathbb{K}[X]$
- P est irréductible dans $A[X]$

Exemple 1.10
Soit $a = \pm p_1^{\alpha_1} \dots p_r^{\alpha_r} \in \mathbb{Z}$, si l'un des α_i vaut 1 alors $X^n - a$ est irréductible dans $\mathbb{Z}[X]$

Proposition 1.11 Soit $P \in \mathbb{Z}[X]$ et p un nombre premier. On note $\overline{P} \in \mathbb{F}_p[X]$ le polynôme issu de la réduction modulo p de P. Si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$ alors P est irréductible dans $\mathbb{Q}[X]$, et dans $\mathbb{Z}[X]$ si $c(P) = 1$.

Contre-exemple 1.12
Réciproque fausse : $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ et $(X+1)^4 \equiv X^4 + 1 \mod 2$

3. Nombres algébriques [Per]

Définition 1.13 Soit $\mathbb{L}/\mathbb{K}$ une extension de corps. Soient $\alpha \in \mathbb{L}$ et $\varphi : \mathbb{K}[X] \longrightarrow \mathbb{L}$ l'homomorphisme défini par $\varphi|_{\mathbb{K}} = id_{\mathbb{K}}$ et $\varphi(X) = \alpha$. Si α est non injectif, on dit que α est algébrique sur $\mathbb{K}$.

Proposition 1.14 Soient $\mathbb{L}/\mathbb{K}$ et α algébrique sur $\mathbb{K}$. Il existe alors un unique polynôme [de degré minimal] P tel que $\ker \varphi = (P)$ avec $P \neq 0$ et P unitaire. On dit que P est le polynôme minimal de α sur $\mathbb{K}$ et on le note $m_\alpha^{\mathbb{K}}$ ou m_α. De plus, $m_\alpha^{\mathbb{K}}$ est irréductible.

Exemples 1.15
$\sqrt{2}$, i, $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux $X^2 - 2$, $X^2 + 1$, $X^3 - 2$

Théorème 1.16 Soient $\mathbb{L}/\mathbb{K}$ une extension et $\alpha \in \mathbb{L}$. Alors sont équivalents :

- α algébrique sur $\mathbb{K}$
- $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$
- $[\mathbb{K}(\alpha) : \mathbb{K}] < +\infty$

Proposition 1.17 Soit $\mathbb{L}/\mathbb{K}$ une extension et notons $\mathcal{A}$ l'ensemble des nombres algébriques de $\mathbb{L}$ sur $\mathbb{K}$. Alors $\mathcal{A}$ est un corps et si $\mathbb{K}$ est dénombrable alors $\mathcal{A}$ l'est. Si $\mathbb{L}$ est algébriquement clos alors $\mathcal{A}$ aussi.

II - Extension de corps par adjonction de racines

1. Corps de rupture [Per]

Définition 2.1 Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Une extension $\mathbb{L}/\mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ s'il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$ et $P(\alpha) = 0$.

Théorème 2.2 Soit $P \in \mathbb{K}[X]$ irréductible. Alors P admet un corps de rupture, unique à isomorphisme près.

Exemples 2.3

$\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ est un corps de rupture de X^2+1

$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[X]/(X^3-2)$ est un corps de rupture de X^3-2

Remarque 2.4 Un corps de rupture de $P \in \mathbb{K}[X]$ irréductible vérifie : $[\mathbb{L} : \mathbb{K}] = \deg P$.

Remarque 2.5 Soit $P \in \mathbb{K}[X]$ irréductible de corps de rupture $\mathbb{K}(\alpha)$. Alors P n'est pas nécessairement scindé dans $\mathbb{K}(\alpha)[X]$. Par exemple, $P = X^3 - 2 \in \mathbb{Q}[X]$.

2. Corps de décomposition [Sza]

Définition 2.6 Un corps $\mathbb{L}$ est un corps de décomposition pour $P \in \mathbb{K}[X]$ si :

- $\mathbb{K} \hookrightarrow \mathbb{L}$
- P est scindé dans $\mathbb{L}$
- $\mathbb{L}$ est minimal pour cette propriété

Remarque 2.7 En notant $\lambda_1, \dots, \lambda_n$ les racines de P, la condition 3 s'écrit $\mathbb{L} = \mathbb{K}(\lambda_1, \dots, \lambda_n)$.

Exemple 2.8

$\mathbb{F}_4$ est un corps de décomposition de X^2+X+1 sur $\mathbb{F}_2$ car dans $\mathbb{F}_4[X]$, $X^2+X+1 = (X+\alpha)(X+\alpha+1)$

$\mathbb{Q}(\sqrt[3]{2})$ n'est pas un corps de décomposition de X^3-2

Théorème 2.9 Soit $P \in \mathbb{K}[X]$ (irréductible ou non) alors il existe un corps de décomposition de P, qu'on note $D_{\mathbb{K}}(P)$, unique à isomorphisme près.

Lemme 2.10 Soient $\mathbb{K} \xrightarrow{i} \mathbb{K}'$ un isomorphisme de corps, $\mathbb{L}$ corps de décomposition de $P \in \mathbb{K}[X]$ sur $\mathbb{K}$, $\mathbb{L}'$ corps de décomposition de $i(P)$ sur $\mathbb{K}'$. Alors, il existe un isomorphisme de corps $j : \mathbb{L} \longrightarrow \mathbb{L}'$ tel que $j|_{\mathbb{K}} = i$.

Théorème 2.11 (corps finis) Soient p un nombre premier et $q = p^n$. Il existe un corps de cardinal q défini comme corps de décomposition de $X^q - X$.

Ce corps est unique à isomorphisme près, et on le note $\mathbb{F}_q$.

III - Étudier de familles de polynômes irréductibles

1. Polynômes irréductibles sur un corps fini. [Fra]

Définition 3.1 On définit $\mu : \mathbb{N}^* \longrightarrow \{\pm 1, 0\}$ la fonction de Möbius qui à n associe 0 si un carré parfait divise n et $(-1)^r$ où r est le nombre de termes dans la factorisation de n en premiers, sinon.
(facteurs)

Lemme 3.2 Soit $n \in \mathbb{N}^*$ alors $\sum_{d \mid n} \mu(d)$ vaut 1 si $n = 1$, 0 sinon.

Proposition 3.3 (formule d'inversion de Möbius) Soient $f : \mathbb{N}^* \longrightarrow \mathbb{R}$ multiplicative et $g : n \in \mathbb{N}^* \longmapsto \sum_{d \mid n} f(d)$. Alors, pour tout n, $f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$.

Lemme 3.4 On note $U(n, q)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_q$

- $\forall d \mid n$, $\forall P \in U(d, q)$, $P \mid X^{q^n} - 1$
- $P \in \mathbb{F}_q[X]$ irréductible, $P \mid X^{q^n} - 1 \Longrightarrow \deg P \mid n$

Proposition 3.5 On pose $I(n, q) := \#U(n, q)$. Alors : $I(n, q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$.

développement 1

Corollaire 3.6 Pour tout $n \in \mathbb{N}^*$, il existe un polynôme irréductible dans $\mathbb{F}_q[X]$.

2. Polynômes cyclotomiques

Définition 3.7 Le n-ème polynôme cyclotomique est défini par $\Phi_n := \prod_{\omega \in \mu_n'} (X - \omega)$ où μ_n' désigne les racines n-ièmes primitives de l'unité.

Remarque 3.8 Pour tout n, Φ_n est unitaire de degré $\varphi(n)$.

Proposition 3.9 Pour tout $n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$.

Remarque 3.10 En comparant les degrés, on retrouve $n = \sum_{d \mid n} \varphi(d)$.

Proposition 3.11 Pour tout n, $\Phi_n \in \mathbb{Z}[X]$.

Lemme 3.11 Soient $q, d, n \in \mathbb{N}^*$ avec $q \geq 2$. Alors $q^d - 1$ divise $q^n - 1$ si et seulement si d divise n. De plus, le cas échéant, $\Phi_n(q) \mid \frac{q^n - 1}{q^d - 1}$ pour d diviseur strict de n.

Application 3.12 (théorème de Wedderburn) Tout anneau A tel que $A^\times = A \setminus \{0\}$ qui est fini est commutatif. Il s'agit alors d'un corps.

développement 2

Théorème 3.13 Pour tout n, Φ_n est irréductible sur $\mathbb{Q}$.

Corollaire 3.14 Soit $\omega \in \mu_n'$ alors $m_\omega = \Phi_n$ et $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$.