141

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

Cadre : A est un anneau commutatif unitaire intègre, k est un corps.

I - Notion de polynôme irréductible

1.1. Définitions et premières propriétés

[Goz] p.9

Déf 1 Un polynôme $f \in A[X]$ est irréductible s'il est non nul, non inversible, et si $\forall g, h \in A[X] : f = gh \Rightarrow g \in A^\times$ ou $h \in A^\times$.

Ex 2 Si $a \in A$, $X - a$ est irréductible dans $A[X]$.

Prop 3 $f \in k[X]$ de deg $\geqslant 1$. $k[X]/(f)$ est un corps $\Leftrightarrow$ f irréductible dans $k[X]$.

Prop 4 Il y a une infinité de polynômes irréductibles dans $k[X]$.

1.2 Lien irréductibilité - racines

[Goz] p.9

Prop 5 sur $k[X]$

(1) Tout polynôme de degré 1 est irréductible.

(2) Tout polynôme irréd. de degré > 1 n'a pas de racine dans k

(3) En degré 2 ou 3, la réciproque de (2) est vraie.

C-ex 6 $(X^2+1)^2$ n'a pas de racine réelle, mais est réductible dans $\mathbb{R}[X]$.

Rem 7 $k \subset K$ deux corps

P irréductible dans $K[X] \Rightarrow P$ irréductible dans $k[X]$.

C-ex 8 X^2+1 irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Prop 9 Si k parfait, tout polynôme irréductible sur k est premier avec sa dérivée.

1.3 Généralités sur les anneaux factoriels

A factoriel et $K = \mathrm{Frac}(A)$

[Goz] p.10

Déf 10 Le contenu de $P \in A[X] \setminus \{0\}$ est $\gamma(P) =$ pgcd de ses coefficients. P est primitif si $\gamma(P) = 1$.

Ex 11 • Tout polynôme unitaire est primitif.

• $2X+3 \in \mathbb{Z}[X]$ est primitif.

Lemme 12 (de Gauss) $\gamma(PQ) = \gamma(P)\gamma(Q)$ $\forall P, Q \in A[X] \setminus \{0\}$

Thm 13 (de Gauss) $A[X]$ factoriel $\Leftrightarrow$ A factoriel.

Dans ce cas, pour deg $P \geqslant 1$: P irréd. dans $A[X] \Leftrightarrow P$ irréductible dans $K[X]$ et $\gamma(P) = 1$

C-ex 14 $2X$ irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$.

1.4 Critères d'irréductibilité

A factoriel et $K = \mathrm{Frac}(A)$

[Goz] p.10

Thm 15 (Critère d'Eisenstein) $P = \sum_{i=0}^{n} a_i X^i$

Si p premier tel que $\begin{cases} p \mid a_0, \dots, a_{n-1} \\ p \nmid a_n \\ p^2 \nmid a_0 \end{cases}$; Alors P irréd. dans $K[X]$.

App 16 $P(X) = \sum_{i=0}^{p-1} X^i$, p premier est irréductible dans $\mathbb{Z}[X]$.

App 17 $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$, $\forall n \geqslant 1$.

[PER] p.77

Thm 18 (Critère de réduction)

Soit $I \subset A$ idéal premier, et $L = \mathrm{Frac}(A/I)$. Soit $P \in A[X]$ et $\bar{P}$ sa réduction modulo I, avec $\bar{a}_n \neq \bar{0}$ dans A/I.

Si $\bar{P}$ irréductible sur A/I ou L, alors P irréductible sur K.

Ex 19 $X^3 + 462X^2 + 2433X - 67691$ irréductible sur $\mathbb{Z}$.

C-ex 20 X^4+1 irréductible sur $\mathbb{Z}$ mais sur aucun $\mathbb{F}_p$, p premier

II - Corps de rupture et autres extensions de corps

K, L corps.

2.1. Extension algébrique et polynôme minimal

[PER] p.65

Thm 21 (Base télescopique) Si $k \subset L \subset M$ corps

$\left.\begin{array}{l} (e_i)_{i \in I} \text{ base de } L \text{ sur } k \\ (f_j)_{j \in J} \text{ base de } M \text{ sur } L \end{array}\right\} \Rightarrow (e_i f_j)_{(i,j) \in I \times J}$ base de M sur k.

Cor 22 M/k est finie ssi M/L et L/k sont finies. Dans ce cas, on a : $[M:k] = [M:L][L:k]$

[PER] p.65

Déf-Prop 23 $L|k$ extension, $a \in L$ et $ev_a : k[X] \longrightarrow L$, $X \longmapsto a$.
a est algébrique si ev_a n'est pas injectif, ie $\exists P \neq 0$ tq $P(a) = 0$.
Dans ce cas, $\ker(ev_a)$ est un idéal principal non nul (premier et maximal); son unique générateur unitaire est appelé polynôme minimal de a sur k et noté $\min(a,k)$. Il est irréductible.

Ex 24 1) $\sqrt[3]{2}$ et i sont algébriques sur $\mathbb{Q}$ de polmin X^3-2 et X^2+1.
2) X^4-10X^2+1 est le polmin de $\sqrt{2}+\sqrt{3}$ sur $\mathbb{Q}$.

[BER] p.782

Thm 25 $a \in L$ algébrique sur $k \iff [k(a):k] < \infty \iff k[a]$ corps
$\iff k[a] \simeq k(a)$.

Dans ce cas, $(1, a, \dots, a^{d-1})$ est une k-base de $k(a)$
où $d := \deg(\min(a,k)) = [k(a):k]$.

Rem 26 $\dfrac{k[X]}{\min(a,k)} \simeq k[a]$

Ex 27 $[\mathbb{R}(i):\mathbb{R}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$.

[PER] p.65

Déf 28 $L|k$ est monogène ou simple si $L = k(\alpha)$, $\alpha \in L$.

Déf 29 $L|k$ est algébrique si tous ses éléments sont algébriques sur k.

Prop 30 Toute extension finie est algébrique (la réciproque est fausse).

Thm 31 $\{x \in L$ tq x est alg^q sur $k\}$ est un sous-corps de L.

2.2. Corps des racines d'un polynôme

[GOZ] p.57

Déf 32 $P \in k[X]$ irréductible. L est un corps de rupture de P sur k si $L|k$ est simple : $L = k(\alpha)$ avec α une racine de P.

Rem 33 L est alors une extension algébrique de k.

Ex 34 Si $\deg(P) = 1$, k est un corps de rupture de P.

Thm 35 $\forall P$ irréductible $\in k[X]$, il existe un corps de rupture de P sur k, unique à isomorphisme près. [PER] p.70

C-ex 36 Si f non irréductible $\Rightarrow$ plus forcément d'unicité!
Pour $f(X) = (X^2+1)X \in \mathbb{Q}[X]$, $\mathbb{Q}|\mathbb{Q}$ et $\mathbb{Q}(i)|\mathbb{Q}$ sont des corps de rupture de f, non isomorphes. [BER] p.820

Ex 37 1) Construction de $\mathbb{C}$: X^2+1 irréductible dans $\mathbb{R}[X]$.
$\mathbb{C} = \dfrac{\mathbb{R}[X]}{(X^2+1)}$ corps de rupture de X^2+1.
2) $\mathbb{Q}(\sqrt[3]{2}) = \dfrac{\mathbb{Q}[X]}{(X^3-2)}$ corps de rupture de X^3-2.

[GOZ] p.58

Thm 38 (autre critère d'irréductibilité)
$P \in k[X]$, de degré n. P irréductible dans $k[X] \iff P$ n'a aucune racine dans les extensions de k de degré $\leq \frac{n}{2}$.

Ex 39 X^4+X+1 est irréductible dans $\mathbb{F}_2[X]$.

Thm 40 Soit P irréductible sur k (corps) et L une extension finie de k de degré premier à $\deg(P)$. Alors P est irréductible sur L. [PER] p.79

Ex 41 X^2-2 est irréductible sur toute extension de $\mathbb{Q}$ de degré impaire.

[GOZ] p.58

Déf 42 Un corps de décomposition de P sur k est une extension $L|k$ tq :
- dans $L[X]$: $P(X) = (X-\alpha_1)\dots(X-\alpha_n)$, α_i racine de P
- $L = k(\alpha_1, \dots, \alpha_n)$.

Rem 43 L est alors une extension algébrique finie de k.

Thm 44 $\forall P \in k[X]$, il existe un corps de décomposition de P sur k, unique à isomorphisme près. [PER] p.71

Ex 45
- $\mathbb{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition de X^3-2 sur $\mathbb{Q}$.
- $\mathbb{R}(i)$ est un corps de décomposition de X^2+1 sur $\mathbb{R}$.

[Goz] p. 62

2.3 Clôtures algébriques

Soit K corps.

Déf 46 K est algébriquement clos si il vérifie une des conditions équivalentes suivantes :
1) Tout pol de degré ≥ 1 est scindé sur K
2) Tout pol de degré ≥ 1 admet au moins une racine dans K
3) Les pols irréductibles de $K[X]$ sont ceux de degré $= 1$
4) Si $L \backslash K$ algébrique, alors $L = K$.

Ex 47 $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos

Thm 48 (de d'Alembert-Gauss) $\mathbb{C}$ est algébriquement clos.

Rem 49 pols irréductibles sur $\mathbb{R}$: ceux de degré 1, et ceux de degré 2 sans racine réelle.

Déf 50 $L\backslash K$ est une clôture algébrique de K si $L \backslash K$ est algébrique et L algébriquement close.

Ex 51
- $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$
- $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$
- $\{x \in \mathbb{C}$ tq x algébrique sur $\mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$.

[BER] p. 825

Thm 52 (de Steinitz) Tout corps admet une clôture algébrique, unique à isom. près.

III - Cas des corps finis

Soit p un nombre premier, n dans $\mathbb{N}^*$, et notons $q = p^n$.

3.1 - Construction des corps finis

[PER] p. 73

Thm 53 Il existe un corps K à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ (donc unique à isom près). On le note $\mathbb{F}_q$.

De plus : $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(f)$, f irréductible de degré n.

App 54 Constructions explicites : $\mathbb{F}_4 \simeq \dfrac{\mathbb{F}_2[X]}{(X^2+X+1)}$; $\mathbb{F}_9 \simeq \dfrac{\mathbb{F}_3[X]}{(X^2+X+2)}$

[GOZ] p. 89

3.2 - Dénombrement des polynômes irréductibles sur $\mathbb{F}_p$

Notons $K(n,p)$ l'ensemble des pols irréd unitaires de degré n sur $\mathbb{F}_p$.

Notons $I(n,p) = |K(n,p)|$

Déf 55 Fonction de Möbius : $\mu : \mathbb{N}^* \to \{-1,0,1\}$.
$\mu(1) = 1$; $\mu(p_1 \cdots p_k) = (-1)^k$ avec $(p_i)_i$ premiers 2 à 2 distincts ;
$\mu(n) = 0$ si n a un facteur carré.

[Goz] p. 89

Prop 56 Inversion de Möbius (ADMIS)
Si $f, g : \mathbb{N}^* \to \mathbb{C}$, tq $f(n) = \sum_{d|n} g(d)$, Alors : $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$

Thm 57 $X^{p^n} - X = \prod_{d|n} \prod_{Q \in K(d,p)} Q(X)$ — DEV 1

Cor 58 $p^n = \sum_{d|n} d \cdot I(d,p)$ et $I(p,n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$.

IV - Cyclotomie

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

4.1 Racines primitives n-ièmes de l'unité

[Goz] p. 67

Déf 59 $\mathbb{U}_n^* = \{\omega \in \mathbb{C}$ tq $\omega^n = 1$ et $\omega^d \neq 1 \ \forall 1 \leq d < n\}$ est l'ensemble des racines primitives n-ièmes de l'unité.

Rem 60 $|\mathbb{U}_n^*| = \varphi(n)$

Prop 61 Si $\omega \in \mathbb{U}_n^*$, alors $\mathbb{U}_n^* = \{\omega^k, k \leq n$ et $k \wedge n = 1\}$

4.2 Polynômes cyclotomiques

[Ber] p. 643

Déf 62 $\phi_n(X) = \prod_{\omega \in \mathbb{U}_n^*} (X - \omega)$ est le n-ième pol cyclotomique.

Ex 63 $\phi_1 = X - 1$; $\phi_2 = X + 1$; $\phi_p = X^{p-1} + \ldots + X + 1$, p premier

Prop 64 $X^n - 1 = \prod_{d|n} \phi_d(X)$

Ex 65 $\phi_4(X) = \dfrac{X^4 - 1}{\phi_1 \phi_2} = X^2 + 1$; $\phi_8(X) = X^4 + 1$

Prop 66 $\phi_n \in \mathbb{Z}[X]$

Thm 67 ϕ_n est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Z}$. — DEV 2

[PER] p. 83

Cor 68 ϕ_n est le pol minimal de toute racine primitive n-ième de l'unité sur $\mathbb{Q}$, et donc $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$, $\forall \omega \in \mathbb{U}_n^*$.

Autres notions qu'on peut aussi aborder :

- Théorème de l'élément primitif
- Algorithme de Berlekamp (pour une factorisation en facteurs irréductibles)
- comment trouver le pol min d'un élément alg ? (cela revient à trouver un polynôme annulateur)

Références :

- [PER] Cours d'Algèbre, Perrin D.
- [GOZ] Théorie de Galois, Gozard I.
- [BER] Algèbre : le grand combat, Berhuy G.
- [FRA] Exercices de mathématiques pour l'agrégation, Algèbre 1, Francinou et Gianella

Autres références possibles

- Extensions de corps, J. Calais
- Exercices Oraux X-ENS Algèbre 1, Francinou et toute sa clique
- Corps commutatifs et théorie de Galois, P. Tauvel