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

I - Définitions et constructions

1) Polynômes irréductibles

Soit A un anneau commutatif et K un corps, on rappelle que $A[X]^\times = A^\times$, A factoriel $\Rightarrow A[X]$ factoriel, $K[X]$ est euclidien.

1 **Def** : . $P \in A[X]$ est irréductible sur A si $\deg P \geq 1$ et $Q \mid P \Rightarrow Q \in A^\times$ ou $Q \in A^\times P$
. P est réductible sur A si $\deg P \geq 1$ si P n'est pas irréductible sur A

2 **Ex** : . $\forall a \in A$, $X-a$ est irréductible sur A
. $P \in A[X]$ est irréductible sur $A \Rightarrow P$ n'a pas de racines sur A et $\deg P \geq 2$.

3 **Prop** : Soit $P \in K[X]$ tel que $\deg P \in \{2,3\}$.
P est irréductible sur K ssi P n'a pas de racines dans K

4 ⚠ : $P = X^4+1 = (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$ n'a pas de racines dans $\mathbb{R}$ mais P est réductible sur $\mathbb{R}$. $(2X-1)^2 \in \mathbb{Z}[X]$ est réductible sur $\mathbb{Z}$

5 **Ex** : X^3+X+1 est irréductible sur $\mathbb{Q}$

2) Extension algébrique

6 **Def** : Soit $K \subset L$ deux corps et $a \in L$. On dit que a est algébrique sur K si $\exists P \in K[X]$, $P(a)=0$. De plus on appelle polynôme minimal de a, l'unique polynôme unitaire de plus petit degré annulant a.

7 **Ex** : Dans $\mathbb{Q} \subset \mathbb{R}$ $\Pi_{\sqrt{3}} = X^2-3$. Dans $K \subset L$ $a \in K \Leftrightarrow \Pi_a = X-a$

8 **Prop** : Soit $P \in K[X]$ et $a \in L$. $P = \Pi_a \Leftrightarrow P$ unitaire, irréductible, $P(a)=0$

9 **Ex** : $\Pi_{\sqrt{2}+\sqrt{3}} = X^4-10X^2+1$

10 **Prop** : Soit $P \in K[X]$. On a
P irréductible sur $K \Leftrightarrow \langle P \rangle$ est maximal dans $K[X]$
$\Leftrightarrow K[X]/\langle P \rangle$ est un corps

Prop : Soit $a \in L$ algébrique. $K[a] = \{P(a), P \in K[X]\} \simeq K[X]/\langle \Pi_a \rangle$ est un corps et un K-espace vectoriel de dimension $\deg \Pi_a$. 11
- Si $K[a]$ est un K-ev de dimension fini alors a est algébrique sur K

Th : L'ensemble des éléments algébriques de L sur K est un corps. 12

Application : . $\mathbb{A} = \{z \in \mathbb{C},\ z$ algébrique sur $\mathbb{Q}\}$ est un corps dénombrable 13
. L'ensemble des nombres transcendants est infini et non dénombrable

3) Adjonction de racines

Def : Soit $P \in K[X]$ irréductible sur K. On dit que L est un corps de rupture de P si $\exists \alpha \in L$ tel que $P(\alpha)=0$ et $L = K[\alpha]$. 14

Th : Soit $P \in K[X]$ irréductible sur K. 15
$K[X]/\langle P \rangle$ est un corps de rupture de P.
Si $L = K[\alpha]$ est un corps de rupture de P alors $\varphi : K[X]/\langle P \rangle \longrightarrow L$, $\overline{X} \longmapsto \alpha$ induit un K-isomorphisme de L sur $K[X]/\langle P \rangle$

Ex : $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ est le corps de rupture de X^4-10X^2+1 sur $\mathbb{Q}$ 16

Prop : Soit $P \in K[X]$ et $n = \deg P$. P est irréductible sur K ssi $\forall L$ ext de K tel que $[L:K] \leq \frac{n}{2}$, P n'a pas de racine dans L. 17

Def : Soit $P \in K[X]$, $n = \deg P$. On dit que L est un corps de décomposition de P si $\exists (\lambda, \alpha_1, \dots, \alpha_n) \in L^{n+1}$, $P = \lambda \prod_{k=1}^{n} (X-\alpha_k)$ et $L = K[\alpha_1, \dots, \alpha_n]$ 18

Th : Soit $P \in K[X]$ et $n = \deg P$. 19
. Il existe un corps de décomposition L de P. De plus $[L:K] \leq n!$
. Deux corps de décomposition de P sont K-isomorphe. 20

Rq : Il n'existe pas d'isomorphisme canonique entre les corps de décomposition.

Ex : $\mathbb{Q}[\sqrt[3]{2}, j]$ est le corps de décomposition de $P = X^3-2$ sur $\mathbb{Q}$. 21
Ce n'est pas le corps de rupture de P (qui est $\mathbb{Q}[\sqrt[3]{2}]$)

Applications : - Si $U_0 = 3$, $U_1 = 0$, $U_2 = 2$ et $U_{n+1} = U_{n-1} + U_{n-2}$ $n \geq 2$ 22
alors pour p premier $p \mid U_p$

- Th (élément primitif) : Soit K un corps fini ou de caractéristique nulle et L une extension finie de K. Alors $\exists \alpha \in L$, $L = K[\alpha]$.

3) Corps finis

Prop : Soit F un corps fini. La caractéristique p de F est un nombre premier et $\exists n \in \mathbb{N}^*$, $\mathrm{card}(F) = p^n$. F est un $\mathbb{Z}/p\mathbb{Z}$-ev.

Rq : Pour tout p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps de caractéristique p.

Prop : Soit $\varphi : \begin{array}{l} K \to K \\ x \mapsto x^p \end{array}$. Si K est un corps fini de caractéristique p alors φ est un automorphisme.

Si $K = \mathbb{Z}/p\mathbb{Z}$ alors $\varphi = id_K$

Th : Soit p premier et $n \in \mathbb{N}^*$. Il existe un corps K à p^n éléments. Si K' est un corps à p^n éléments, K et K' sont $\mathbb{Z}/p\mathbb{Z}$-isomorphe.

Rq : On note $\mathbb{F}_{p^n}$ le corps à p^n éléments.
- le corps de décomposition de $X^{p^n} - X$ est un corps à p^n éléments
- Si $Q \in \mathbb{F}_p[X]$, $\deg Q = n$ et Q irréductible sur $\mathbb{F}_p$ alors $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/\langle Q \rangle$

Ex : $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/\langle X^2+X+1 \rangle$

Prop : Si K est un corps fini alors $(K^*, \times)$ est cyclique.
De plus si $K^* = \langle g \rangle$ et $\mathrm{car}(K) = p$ alors $K \simeq \mathbb{F}_p[g]$

II - Critères d'irréductibilité

1) Critères généraux

Prop : Soit k un sous corps de K et $P \in k[X]$.
Si P est irréductible sur K alors P est irréductible sur k

⚠ Réciproque fausse avec $k = \mathbb{R}$, $K = \mathbb{C}$ et $P = X^2+1$

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

Def : Soit $P \in A[X] \setminus \{0\}$, on définit $\mathrm{cont}(A)$ comme le PGCD des coefficients de A. P est dit primitif si $\mathrm{cont}(P) = 1$

Lemme (Gauss) : $\forall (P,Q) \in (A[X]\setminus\{0\})^2$, $\mathrm{cont}(PQ) = \mathrm{cont}(P)\,\mathrm{cont}(Q)$

Th : Soit $P \in A[X]$, $\deg P \geq 1$
P est irréductible sur A ssi P est irréductible sur K et $\mathrm{cont}(P) = 1$

Ex : $2X^3+X+1$ est irréductible sur $\mathbb{Z}$
$2X$ est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Z}$

Th : (Eisenstein) : Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ avec $a_n \neq 0$
Si $\exists p \in A$ irréductible tel que $\begin{cases} \cdot\ a_n \notin pA \\ \cdot\ \forall i \in [\![0; n-1]\!],\ a_i \in pA \\ \cdot\ a_0 \notin p^2 A \end{cases}$
Alors P est irréductible sur K

Ex : $\Phi_p = \sum_{i=0}^{p-1} X^i$ (p premier) est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$

• $a_0 \notin p^2A$ est nécessaire : $X^2+4X+4 = (X+2)^2$

Th (Réduction) : Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ avec $a_n \neq 0$
Soit I un idéal premier de A, $B = A/I$ et $L = \mathrm{Frac}\, B$
Si $a_n \notin I$ et $\overline{P}$ irréductible sur L alors P est irréductible sur K

Ex : . $P = X^3 - 5X^2 + 12X - 3$ est irréductible sur $\mathbb{Z}$ ($I = 2\mathbb{Z}$)
. $P = X^4+1$ est irréductible sur $\mathbb{Z}$ et $\mathbb{Q}$ mais P est réductible sur $\mathbb{Z}/p\mathbb{Z}$ pour tout p premier

2) Critères sur les corps finis

Soit p premier, $n \in \mathbb{N}^*$ et $q = p^n$

Def : On note $K(q,j)$ l'ensemble des polynômes unitaires irréductibles sur $\mathbb{F}_q$ de degrés j et $I(q,j) = \mathrm{card}(K(q,j))$. 41

Def : On définit la fonction de Moebius $\mu : n \mapsto \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } p^2 \mid n \text{ avec } p \text{ premier} \\ (-1)^k \text{ si } n = \prod_{i=1}^{k} p_i,\ p_i \text{ premiers 2 à 2} \neq \end{cases}$ 42

Th : Dans $\mathbb{F}_q[X]$, on a pour tout $k \in \mathbb{N}^*$
$$X^{q^k} - X = \prod_{d \mid k} \prod_{Q \in K(q,d)} Q \quad \text{et} \quad \prod_{Q \in K(q,n)} Q = \prod_{d \mid n} \left(X^{q^d} - X\right)^{\mu(\frac{n}{d})}$$

44 **Application** : Test de Ben-Or : Soit $P \in \mathbb{F}_q[X]$, $\deg P = s$.
P est irréductible sur $\mathbb{F}_q$ ssi $\forall e \in [\![1 ; s-1]\!]$, $P \wedge (X^{q^e} - X) = 1$

45 **Prop** : $I(q,k) = \frac{1}{k} \sum_{d \mid k} \mu\left(\frac{k}{d}\right) q^d$

3) Le cas réel et complexe

46 **Th** : (D'Alembert-Gauss) : Tout polynôme de $\mathbb{C}[X]$ non constant admet une racine dans $\mathbb{C}$

47 **Cor** : les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

48 **Prop** : les polynômes irréductibles de $\mathbb{R}[X]$ sont :
- les polynômes de degré 1
- les polynômes de la forme $aX^2 + bX + c$ avec $\Delta = b^2 - 4ac < 0$

49 **Application** : Calcul d'intégrale :
$$\int_0^1 \frac{x^3}{1+x^3}\, dx = 1 - \frac{1}{3}\ln(2) - \frac{\pi}{3\sqrt{3}}$$

III - Factorisation

1) Polynômes cyclotomiques

50 **Déf** : On définit $\Phi_n = \prod_{\substack{k=1 \\ k \wedge n = 1}}^{n} \left(X - e^{\frac{2ik\pi}{n}}\right)$

51 **Prop** : $X^n - 1 = \prod_{d \mid n} \Phi_d$. **Cor** : $\Phi_n = \prod_{d \mid n} (X^d - 1)^{\mu(\frac{n}{d})}$

52 **Ex** : $\Phi_8 = X^4 + 1$

53 **Prop** : $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$

54 **Application** : Th de Wedderburn :
Tout corps gauche fini est commutatif.

55 **Th** : $\forall n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Z}$

56 **Ex** : Soit ξ une racine primitive n-ième de l'unité dans $\mathbb{C}$.
Alors Φ_n est le polynome minimal de ξ sur $\mathbb{Q}$ et $[\mathbb{Q}[\xi] : \mathbb{Q}] = \varphi(n)$

57 **Application** : - Théorème de Dirichlet : Soit $\lambda \in \mathbb{N}^*$.
Il existe une infinité de nombre premier de la forme $\lambda n + 1$, $n \in \mathbb{N}$

58 - $\cos\left(\frac{2\pi}{5}\right) = \frac{-1 + \sqrt{5}}{4}$

Th Soit $n \in \mathbb{N}^*$, p premier tel que $p \wedge n = 1$. Soit r l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Alors Φ_n se décompose dans $\mathbb{F}_p[X]$ en produit de polynômes unitaires irréductibles de degré r. 59

Cor : $\exists$ p premier, $p \wedge n = 1$ tel que Φ_n soit irréductible sur $\mathbb{F}_p$ si et seulement si $(\mathbb{Z}/n\mathbb{Z})^\times = \langle \bar{p} \rangle$. 60

2) Algorithme de Berlekamp

Soit p premier, $n \in \mathbb{N}^*$ et $q = p^n$.

Prop : Soit $R \in \mathbb{F}_q[X]$, $S_R : \mathbb{F}_q[X]/\langle R \rangle \longrightarrow \mathbb{F}_q[X]/\langle R \rangle$, $Q \longmapsto Q(X^p) = Q^p$ est une application linéaire 61

Algo : Entrée : $P \in \mathbb{F}_q[X]$. Sortie : Décomposition en facteurs irréductibles de P sur $\mathbb{F}_q[X]$. 62

1) Si P est constant, retourner P
2) Calculer $P \wedge P'$:
   a) Si $P \wedge P' = P$ alors $\exists R \in \mathbb{F}_q[X]$, $P = R^p$: Appliquer l'algo à R
   b) Si $P \wedge P' = P_1 \notin \{1, P\}$ alors $P = P_1 P_2$: Appliquer l'algo à P_1 et P_2
   c) Si $P \wedge P' = 1$:
   i) Calculer la matrice de $S_P - id$ dans la base $\{1, \bar{X}, \dots, \bar{X}^{\deg P - 1}\}$
   ii) Calculer $r = \dim(\mathrm{Ker}(S_P - id))$. Si $r = 1$ retourner P.
   iii) Calculer un $V \in \mathrm{Ker}(S_P - id)$ non constant.
   On a $P = \prod_{\alpha \in \mathbb{F}_q} [P \wedge (V - \alpha)]$. Appliquer le c) de l'algo à $V - \alpha$ pour $\alpha \in \mathbb{F}_q$ tq $P \wedge (V - \alpha) \neq 1$