

[Ber]
[Goz]
[Per]

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

I- Polynômes irréductibles

1) Notion d'irréductibilité [Ber] 609 [Goz] 9

- def polynôme irréductible
- lien avec racines deg 2, 3
- $\mathbb{K}[X]_{(P)}$
- racine dans $\mathbb{Q}$

2) Critères d'irréductibilité [Goz] 10

- réduction modulo
- contenu + critère d'Eisenstein

DEV 1

II- Polynômes et extensions de corps

1) Élément algébrique [Per] 66

- def
- polynôme min
- lien avec $\mathbb{K}[X]$ et $\mathbb{K}(\alpha)$

2) Corps de rupture et de décomposition [Per] 70-72

- def
- existence et unicité
- critère $\leq \frac{n}{2}$

(3) Cloture algébrique
• def alg obs + exemples

III- Applications et exemples

1) Corps finis [Per] 73 [Goz] 87

- caractérisation morphisme de Frobenius

DEV 2

existence et unicité corps fin
cyclicité

2) Polynômes cyclotomiques [Goz] 67

- Racine n-ième
- Racine primitive
- def et prop
- irréductibilité
- Dirichlet faible

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

Soit A un anneau commutatif intègre et K un corps

I- Polynômes irréductibles

1) Notion d'irréductibilité

Définition 1: Un polynôme $P \in A[x]$ est irréductible s'il est non nul, non inversible et si $P = QR$ avec $Q, R \in A[x]$ alors Q ou R est inversible.

Proposition 2: Soit $P \in K[x]$. Alors: $K[x] \mid 105$?

1) si $\deg P = 1$, P est irréductible.

2) Si P est irréductible et $\deg P > 1$ alors P n'a pas de racines dans K .

3) Si $\deg P = 2$ ou 3 alors P irréductible ssi P n'a pas de racines dans K .

Contre exemple 3: $(x^2+1)^2$ n'a pas de racines dans $\mathbb{Q}$ mais est réductible dans $\mathbb{Q}[x]$

Exemple 4: $2x$ irréductible dans $\mathbb{Q}[x]$ mais pas dans $\mathbb{Z}[x]$

Remarque 5: Si k sous-corps de K et $P \in k[x]$, alors si P irréductible dans $K[x]$, il est irréductible dans $k[x]$

Proposition 6: Soit $P \in K[x]$ de degré d . Alors $K[x]_{(P)}$ est intègre ssi P est irréductible. Dans ce cas, c'est un corps.

2) Critères d'irréductibilité

Définition 7: Soit A anneau factoriel. Soit $P \in A[x]$ avec $P \neq 0$. On appelle contenu de P , noté $c(P)$, un pgcd de ses coefficients. On dit que P est primitif si $c(P) = 1$

Lemme 8 (Gauss) Soit $P, Q \in A[x]$. On a:

$$c(PQ) = c(P)c(Q)$$

Théorème 9: Soit A anneau factoriel, $K = \text{Frac}(A)$ le corps des fractions de A . Soit P le polynôme de degré supérieur ou égal à 1 à coefficient dans A . P irréductible dans $A[x]$ ssi P irréductible dans $K[x]$ et $c(P) = 1$

Théorème 10 (critère d'Eisenstein) DEV 1

Soit A factoriel et $K = \text{Frac}(A)$. Soit $P(x) = \sum_{i=0}^n a_i x^i \in A[x]$ avec $\deg P \geq 1$.

Soit $p \in A$ irréductible de A tel que $p \nmid a_n$, $\forall i \in [1, n-1]$ $p \mid a_i$ et $p^2 \nmid a_0$.

Alors P est irréductible dans $K[x]$.

Exemple 11: Pour tout p premier, le polynôme $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ est irréductible dans $\mathbb{Z}[x]$.

Théorème 12: Soit A factoriel et $K = \text{Frac}(A)$. Soit I un idéal premier de A et $B = A/I$. Soit $P(x) = \sum_{i=0}^n a_i x^i \in A[x]$ de degré ≥ 1 . Soit $\bar{P}$ sa réduction modulo I . On suppose $\bar{a}_n \neq 0$ dans B . Alors si $\bar{P}$ est irréductible sur $B[x]$, P est irréductible dans $K[x]$

Exemple 13: $x^3 + 462x^2 + 2433x - 67691$ est irréductible

sur $\mathbb{Z}$

II - Polynômes et extensions de corps

Soit K, L, M des corps

1) Éléments algébriques

[Per]
66

Définition 14: Soit L/K et $\alpha \in L$. Soit $\varphi: K[x] \rightarrow L$ le morphisme d'évaluation en α . Alors

- 1) Si φ est injectif, on dit que α est transcendant sur K .
- 2) Sinon on dit que α est algébrique sur K . Ainsi il existe $P \in K[x]$ non nul tel que $P(\alpha) = 0$. Si α algébrique sur K , $\ker \varphi = (P)$ avec P le polynôme minimal de α sur K . Il est irréductible dans $K[x]$.

Exemple 15: e et π sont transcendants sur $\mathbb{Q}$

$\sqrt{2}$ et i sont algébriques sur $\mathbb{Q}$

Théorème 16: Soit L/K une extension et soit $\alpha \in L$. On a les équivalences:

- 1) α est algébrique sur K
- 2) $K(\alpha) = K[\alpha]$
- 3) $[K(\alpha):K] < \infty$

Si P est le polynôme minimal de α sur K on a $[K(\alpha):K] = \deg(P)$. C'est le degré de α .

2) Corps de rupture et de décomposition

Définition 17: Soit $P \in K[x]$ irréductible. Une extension L de K est appelée un corps de rupture de P sur K si L est une extension monogène $L = K(\alpha)$ avec $P(\alpha) = 0$.

Théorème 18: Soit $P \in K[x]$ irréductible. Il existe un corps de rupture P sur K , unique à isomorphisme près.

Exemple 19: $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$ est un corps de rupture de x^2+1 sur $\mathbb{R}$.

Définition 20: Soit $P \in K[x]$ de degré n . On appelle corps de décomposition de P sur K une extension L de K telle que:

- 1) P est scindé dans $L[x]$
- 2) L est minimal pour cette propriété (L est engendré par les racines de P)

Théorème 21: Pour tout $P \in K[x]$, il existe un corps de décomposition de P sur K , unique à isomorphisme près. On le note $D_K(P)$.

Exemple 22: Pour $K = \mathbb{Q}$, $P(x) = x^3 - 2$, $D_K(P) = \mathbb{Q}(\sqrt[3]{2}, j)$

Théorème 23: Soit $P \in K[x]$ de degré n . Alors P est irréductible dans $K[x]$ si P n'a pas de racines dans les extensions L de K telles que $[L:K] \leq \frac{n}{2}$.

III - Applications et exemples

1) Corps finis

Proposition 24: Soit K un corps de caractéristique $p > 0$. L'application $F: K \rightarrow K$ est un isomorphisme de corps.

$$x \mapsto x^p$$

il est appelé morphisme de Frobenius.

- si K est fini, c'est un automorphisme
- si $K = \mathbb{F}_p$ c'est l'identité.

73 Théorème 25: Soit p premier et $n \in \mathbb{N}^*$. On pose $q = p^n$. Alors il existe un corps K à q éléments. C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. Il est unique à isomorphisme près. On le note $\mathbb{F}_q$.

[602] Théorème 26: Soit p premier et $n \in \mathbb{N}^*$. Soit $q = p^n$.

87 Alors $\mathbb{F}_q = \mathbb{F}_p[X]_{(\pi)}$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.

2) Polynômes cyclotomiques

67 Définition 27: Soit $n \in \mathbb{N}^*$. On pose $\mathcal{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$.

L'ensemble des racines n -ièmes de l'unité.

On appelle racine primitive n -ième de l'unité tout générateur de $\mathcal{U}_n$, c'est à dire tout élément de $\mathcal{U}_n$ d'ordre n . On note $\mathcal{U}_n^*$ cet ensemble.

Définition 28: Soit $n \in \mathbb{N}^*$. On appelle n -ième polynôme cyclotomique le polynôme:

$$\Phi_n(X) = \prod_{\zeta \in \mathcal{U}_n^*} (X - \zeta).$$

Proposition 29: Φ_n est unitaire de degré $\varphi(n)$ où φ est l'indicatrice d'Euler.

$$\text{On a } X^n - 1 = \prod_{d \mid n} \Phi_d(X)$$

Proposition 30: $\forall n \in \mathbb{N}^* \quad \Phi_n(X) \in \mathbb{Z}[X]$

Théorème 31: $\forall n \in \mathbb{N}^* \quad \Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$

Application 32: (Théorème de Dirichlet faible) dev2

Il existe une infinité de nombres premiers congru à 1 modulo n pour $n \in \mathbb{N}^*$

Un polynôme n'admet pas forcément de racines dans un corps donné. C'est pour cela qu'on s'intéresse aux extensions de corps.

Notion d'irréductibilité?

critères

deg max 3 : pas de racines

→ réduction modulo

→ Eisenstein DEV 1

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

on introduit

Corps de rupture

Corps dans lequel P admet une racine mais P et pas forcément scindé

Corps de décomposition

P scindé

Existence et unicité

Applications

Corps finis

Morphisme de Frobenius
+ existence corps à q éléments

Polynômes cyclotomiques

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mathbb{C}^* \\ \zeta^n = 1}} (x - \zeta)$$

↓
Dichotomie faible DEV 2