

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

Cadre : A un anneau commutatif unitaire, $Fr(A)$ son corps de fractions, K un corps, A^\times les inversibles de A .

I) L'anneau $K[X]$

Définition d'un irréductible, inversibles de $A[X]$, exemple. Contenu d'un polynôme, polynôme primitif. Caractérisation des irréductibles sur $A[X]$. Exemple. Irréductibles de $K[X]$, caractérisation de la primalité de $A[X]$. Contre-exemple de $\mathbb{Z}[X]$. Caractérisation d'un quotient par un polynôme irréductible.

II) Critères d'irréductibilité

Critère EISENSTEIN, exemples. Théorème de réduction. Contre-exemple dans A . Applications.

III) Extension de corps, polynôme

A) Définitions, propriétés

Définition d'une extension, de degré, exemples. Théorème de la base télescopique, application. Définition d'un élément algébrique, transcendant, exemple. Polynôme minimal, caractérisation. Exemple du sous-corps des algébriques sur un corps.

B) Corps de rupture

Définition, exemple. Théorème d'existence et d'unicité, application à l'irréductibilité (critères dans les extensions), exemples.

C) Corps de décomposition

Définition, théorème d'existence et d'unicité, exemples.

DEV 1 : GALOIS INVERSE. Exemples.

IV) Polynômes irréductibles sur les corps finis

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

A) L'ensemble des polynômes irréductibles sur \mathbb{F}_p

Définitions de $\mathcal{P}_p(i)$ et $I_p(i)$. **DEV 2** : POLYNÔMES IRRÉDUCTIBLES SUR \mathbb{F}_p . Exemples.

B) Factorisation de polynômes

Théorème de BERLEKAMP, applications.

V) Polynômes cyclotomiques

Sous-groupes de l'unité, définition du n -ième polynôme cyclotomique $\Phi_{n,k}$, exemples. Degré de $\Phi_{n,k}$, relations avec $X^n - 1$, irréductibilité de $\Phi_{n,k} \in \mathbb{Z}[X]$, application au degré de l'extension de $\mathbb{Q} \subset \mathbb{Q}(\xi)$.

ANNEXE : Algorithme de BERLEKAMP.

Références :

- PERRIN
- TAUVEL
- BECK-MALICK-PEYRÉ