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

Références	[Gozard], [Perrin]
Section	Algèbre
Date	@18 mars 2025
Statut leçon	Plan détaillé ok
Enseignant	Lionel Fourquaux
Développements choisis	Algorithme de Berlekamp, Irréductibilité des polynômes cyclotomiques sur Q
Nb choisis	2
Développements	Algorithme de Berlekamp

Rapport de Jury

La présentation du bagage théorique permettant de définir corps de rupture, corps de décomposition, ainsi que des illustrations dans différents types de corps (réel, rationnel, corps finis) sont inévitables. Les corps finis peuvent être illustrés par des exemples de polynômes irréductibles de degré 2, 3, 4 sur F_2 ou F_3. Il est nécessaire de présenter des critères d'irréductibilité de polynômes et des polynômes minimaux de quelques nombres algébriques. Il est bon de savoir montrer que l'ensemble des nombres algébriques sur le corps $\mathbb{Q}$ des rationnels est un corps algébriquement clos. Le théorème de la base téléscopique, ainsi que les utilisations arithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes, est incontournable.

Introduction

→ polynômes irréductibles briques de bases (comme décompose les nombres en produits de nombre premiers)

→ ajout de racines utile ?

Plans

▼ ***Plan***

I. Polynômes irréductibles

1. Définitions et premières propriétés
2. Lien entre les irréductibles de A[X] et de Frac(A)[X]
3. Critères d'irréductibilité

II. Extensions de corps (et polynômes minimaux)

1. Définitions et premières propriétés
2. Éléments algébriques et polynômes minimaux

III. Adjonction de racines

1. Corps de rupture
2. Corps de décomposition
3. Clôture algébrique ??

▼ ***Plan détaillé***

▼ I.1. Définitions et premières propriétés

→ Perrin & Gozard

- def polynôme irred dans un anneau
- prop : deg 1 dans K[X] ⇒ irred
- contre-ex dans anneau pas corps : 2X dans Z[X]
- prop : tout pol de deg >1 irred dans K[X] n'a pas de racine dans K **(besoin de corps ??)**
- contre-ex réciproque : (X^2+1)^2 pas de racine dans Q mais pas irred dans Q *[Gozard]*

- prop : réciproque vraie pour deg ≤ 3 **(besoin de corps ??)**
- prop : dans K[X], P irred ssi <P> max ssi K/<P> corps
- app : construction des corps finis **sur un exemple**
- (contre-ex sans corps : Z[X]/<X^2+1> pas corps *[OA]*)

▼ I.2. Critères d'irréductibilité

→ Gozard&Perrin&OA

- def contenu
- def primitif
- lemme de Gauss
- th : lien irred dans corps des fractions et ceux dans l'anneau
- critère d'Eisenstein
- app : irred des polynômes cyclotomiques d'ordre p avec p premier *[Perrin]* (sans dire que c'est un pol cyclotomique?)
- th : critère de réduction (si place)
- ex : 55 Gozard (si place)
- Berlekamp + app irred de X^p+?? *[OA]* + rq : pas efficace et l'ordi fait pas ça + rq besoin de crops de rupture plus tard + si pas séparable?? DEV1

▼ II.1. Définitions et premières propriétés

→ Gozard

- def extension de corps
- exemples : C extension de corps de R, R de Q
- def degré + extension finie
- th de la base télescopique
- prop : multiplicativité degré

▼ II.2. Polynômes minimaux d'éléments algébriques

→ Perrin

- def élément algébrique + polynôme minimal
- prop : polynôme minimal irred
- prop : deg de l'extension = deg du pol mi
- th : a algébrique ssi K[a]=K(a) ssi K[a] extension finie
- (prop : extension finie ⇒ extension algébrique)

Polynômes cyclotomiques :

- def polynômes cyclotomiques
- prop X^n-1=prod(phi_d)
- th : irred dans Q DEV2 et donc dans Z car unitaire (prop I)
- app : Dirichlet faible (th de Wedderburn)

▼ III.1. Corps de rupture

- def Jérem
- def équivalente : K[racine]
- existence et unicité à iso K-linéaire près quand pol irred **(et quand pol pas irred??)**
- application : construction de C comme corps de rupture de X^2+1

▼ III.2. Corps de décomposition

- def Jerem (et Perrin)
- def équivalente *[Gozard]*
- exemple : le corps fini a p^n éléments est un corps de décomposition de X^(p^n)-X

- existence et unicité à iso K-linéaire près
- application : construction des corps finis (surtout unicité)
- th : il existe des polynômes irred de tout degré sur Fp (besoin du th de l'élément primitif)
- app en algèbre : dans le corps de décomposition du polynôme minimal d'un endomorphisme, cet endo est trigonalisable

▼ III.3.Clôture algébrique

→ Gozard

- def algébriquement clos
- prop : tout corps alg clos est infini
- th : C alg clos (D'Alembert-Gauss)

savoir trouver isomorphisme entre deux corps finis construits avec deux polynômes irred différents

version construction des corps finis par le dénombrement des polynômes irred sur Fp