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

Prérequis : racine d'un polynôme, les corps sont doit de caract p soit de caract 0. On admet le th de Steinitz.

L'intérêt des polynômes irréductibles est de construire des corps en quotientant K[X] par (P).

I) Polynômes irréductibles [Goz] + [FG]

1) Définitions [Goz]

Déf : irréductible sur un anneau.

Ex : polynômes de degré 1.

Prop : tout polynôme irred sur K n'a pas de racine dans K. Réciproque fausse.

2) Exemples [Goz]

Sur C, les seuls poly irred sont les poly de degré 1 (d'Alembert Gauss)

Sur R, les seuls poly irred sont les poly de degré 1 et les poly de degré 2 sans racine réelle.

Ex : X^2+1

Sur Q et Fp c'est plus compliqué.

Ex : X^2-2 est irréductible sur Q.

Sur Z : 2X est irréductible.

3) Critères d'irréductibilité [Goz]

Prop : anXn+…+a0 un polynôme à coeffs entiers, an et a0 non nuls. Si p/q est racine de P, alors p divise a0 et q divise an. En particulier, si P est unitaire, toutes les racines rationnelles sont en fait entières

Ex : X^3+X+1 est irred sur Q. En effet, un tableau de variation donne qu'il peut s'annuler qu'une fois, qu'il vaut -1 en 1 et 1 en zéro, il s'annule pas en 0, pas en 1, donc pas sur Z donc pas sur Q donc irred

Déf : contenu (que sur un anneau factoriel)

Prop : lemme de Gauss.

Th : a un anneau, K son corps des fractions. P un polynôme de A[X]. Alors P est irred sur A ssi il est irred sur K et son contenu est 1.

Eisenstein

Csq : il y a des th de tous degrés sur Q.

Th Réduction modulo p

Des exemples

4) Polynômes irréductibles sur Fq [FG]

Th : formule d'inversion de Möbius [FG 93]

Appl : lien entre les deux fonctions *(appliquer la formule d'inversion à Phi)*

Th : dénombrement des polynômes irréductibles de Fq[X] [FG 189]

II) Extensions de corps [Goz]

1) Extension algébrique [Goz]

Déf : nb algébrique, extension, extension algébrique

Prop : l'ensemble des nb algébriques est dénombrable

Déf : polynôme minimal

Exemple

Prop : le polynôme minimal est irréductible

Prop le degré de K(a)/K est le degré du polynôme minimal de a sur K

2) Corps de rupture [Goz]

Déf : extension, extensions algébriques

Déf : corps de rupture, existence, unicité à isomph près

Ex : construction de C

Prop : P irred sur K ssi P n'a pas de racine dans les extensions L de degré inférieur a n/2 *(si P est irred, et que a est une racine de P, alors a es tdans K(a) qui est de degré n. Réciproquement, si on avait P non irred, on aurait un facteur Q de degré plus petit que n/2, et si on prend une racine de ce Q, l'extension K(a)/K est de degré plus petit que n /2, et P y a une racine)*

3) Corps de décomposition [Goz]

[Goz]

III) Applications [Gourdon] + [Goz] + [Carrega]

1) Construction des corps finis [Goz]

Construction comme corps de rupture

Construction explicite (exemple : F4)

2) Polynômes cyclotomiques [Goz]

Déf

Irréductibles

Appl : th de Dirichlet

3) Constructibilité [Carr]

Th de Wantzel

Th de Gauss

4) Algèbre linéaire [Gou]

Gourdon : semi simples

Développements :
1 - Dénombrement des polynômes irréductibles sur Fq [FG 189] (***)
2 - Irréductibilité des polynômes cyclotomiques [Goz 69] (***)
3 - Endomorphismes semi-simples [Gou Alg 224] (**)
Théorème de Gauss [Carrega 48] (**)

Bibliographie :
[Goz]
[FG]
[Carr]
[Gourdon]

Rapport du jury : les applications ne concernent pas que les corps finis. Des informations sur le degré du corps de rupture et du corps de décomposition d'un polynôme irréductible de degré d sont utiles : d dans le premier cas, d! dans le second. Le candidat peuvent réfléchir à l'exercice suivant : exhiber un isomorphisme entre R[X]/(X^2 + X + 1) et R[X]/(X^2 + 1).