(123) Corps finis. Applications.

Lidl - Niederreiter
Tauvel
Caldero - Germoni

I/ Généralités sur les corps finis

1) Corps finis et nombres premiers

- Anneau intègre fini ⇒ corps
- Equivalence entre n premier ⇔ $\mathbb{Z}/n\mathbb{Z}$ intègre ⇔ $\mathbb{Z}/n\mathbb{Z}$ corps
- Critère d'Eisenstein.
- Caractéristique d'un corps fini → premier.
- Déf sous-corps premier → Thm sur le cardinal d'un corps fini ~ p^n.

2) Propriétés des corps finis

- Thm de Fermat
- Morphisme de Frobenius
- K^* cyclique.

3) Carrés dans K^*

- Thm des carrés dans un corps fini
→ infinité de nbrs premiers de la forme $4n+1$.

4) Appl: éq d'ordre 2.

$ax^2+by^2=1$.

→ appl: (CG) formes quadratiques sur un corps fini → classification.

II/ Existence et unicité d'un corps fini à p^n elts.

1) Existence

- P irréductible sur K ⇒ $K[X]/(P)$ est un corps
- fonction de Möbius
- Existence

2) Unicité

3) Critère des sous-corps.

Sous-corps de $\mathbb{F}_q$: → les sous-corps de cardinal p^m si m divise n ($q=p^n$)

→ annexe : sous-corps de $\mathbb{F}_{2^{30}}$.

4) Représentations des corps finis (racines, matrices compagnons).

III/ Polynômes sur les corps finis.

1) Corps de rupture, corps de décomposition

- Déf puis thm d'ex, unicité du corps de rupture.
- Déf décomposition

2) Polynômes cyclotomiques

- Déf corps cyclotomiques, racines de l'unité, générateurs des, polynôme cyclotomique ← racines de l'unité

Thm : $\mathbb{F}_q$ corps de décomposition de $X^{q-1}-1$

Thm de Wedderburn : algèbre de division de cardinal fini → corps.

3) Algorithme de Berlekamp.

Lemme préliminaire

→ explication de l'algorithme.