

123 - Corps finis. Applications.

➤ Références	[Perrin], [Obj_pas_chômage], [NH2G2.T1], [Griff], [UImA], [Gozard]
📁 Section	Algèbre
📅 Date	@6 novembre 2024
☰ Statut leçon	Plan détaillé ok
≡ Enseignant	Lionel Fourquaux
➤ Développement choisis	<u>Loi de réciprocité quadratique</u> , <u>Algorithme de Berlekamp</u>
🔍 Nb choisis	2
➤ Développement	<u>Algorithme de Berlekamp</u> , <u>Lemme de Fitting et dénombrement des matrices nilpotentes sur F_q</u> , <u>Loi de réciprocité quadratique</u> , <u>Corps des nombres algébriques</u>

Rapport de Jury

- construction des corps finis connus
- bonne notion calculs
- theo base télescopique
- injection
- structure groupe multiplicatif
- applications des corps finis et avec q non premier ex: polynômes à coefficients entiers et leur irréductibilité, carrés ds corps finis, résolutions équations de degré deux
- plus loin: codes correcteurs, irréductibilité polynômes à coeff ds corps finis

Introduction

- corps pas mal, corps finis mieux !
- plein de propriétés cool
- code correcteurs, crypto..

Plans

▼ Plan

- I. Construction des corps finis
- II. Structure interne
 1. Carrés
 2. Cyclicité
 3. Automorphisme
 4. Sous-corps (injection)
- III. Structure externe
 1. Anneaux $F_p[X]$
 2. Algèbre linéaire sur F_q
 3. Classification des formes quadratiques

Annexe sous corps de $F_{2^{12}}$ par exemple comme Ulmer

▼ Plan détaillé

- ▼ I.1. Construction des corps finis
 - Gozard
 - F_p pour p premier
 - caractéristique def , si K corps premier ou nul + ex ref ?
 - ° [Phase d'analyse] Si K corps fini alors
 - caractéristique est p premier
 - cardinal p^n
 - Frobenius est un automorphisme sur K fini et sur F_p c'est l'identité
 - lemme unicité corps des décompositions
 - existence et unicité corps fini, c'est le corps de décomposition + notation F_q
 - contre exemple F_4 et $\mathbb{Z}/4\mathbb{Z}$
- ▼ II. 1. Carrés dans F_q
 - Gozard
 - notations
 - cas $p=2$

- cas $p > 2$
- ex: -1 est un carré ssi $p=2$ ou congru à $1 \pmod{4}$ (comme dans théo 2 carrés)
- app des cardinaux: $ax^2+by^2=?$ admet solutions (utiles classification formes quadratiques) [Perrin]

→ NH2G2.1 ou Gozard plus loin

- symbole de Legendre + morphisme de groupes
- loi réciprocity quadratique DEV 1
- corollaire avec les deux cas
- app: un calcul
- loi complémentaire ? A maîtriser, preuve purement corps fini (plutôt H2G2)

▼ II. 2. Cyclicité de F_q^*

→ Gozard

- K corps quelconque, sous groupe fini de K^* cyclique
- Coro: F_q^* cyclique
- Théorème de l'élément primitif pour les corps fini version simple
- un exemple style $F_5[X]/(x^2+X+2)$ avec un générateur
- App ? Si jamais

▼ II. 3. Automorphismes

→ Gozard

- Groupe des auto cyclique d'ordre n engendré par Frobenius
- App ? existence de polynôme irred de tout degré dans F_p cf plus tard ?

▼ II.4 Sous corps /injection

→ Gozard

- théorème de la base télescopique (ref ??)
- Prop (théo VII.4.3): si t est un sous corps de F_q alors il existe d diviseur de n tq $\text{card } K = p^{*d} + \text{unique sous corps}$
- diagramme machin F12 en annexe ? Ulmer ou rq F64 avec F32 pas un sous corps

▼ III. 1 Anneau $F_p[X]$

→ Gozard.. ou pas. Pas très convaincue des refs, à voir si on trouve mieux

- rq: intérêt de l'étude des polynômes irred sur F_p justifié par $F_q = F_p[X]/(\pi)$ où π polynôme irred quelconque
- (Ulmer parle de: $X^{p^n} - X$ dans $F_p[X]$ est le produit de tous les polynômes irréductibles unitaires de $F_p[X]$ dont le degré divise n (Loïc et Malo l'avait mis aussi) et en déduit un test d'irréductibilité et en déduit l'existence d'un polynôme irred de tout degré)
- il existe des polynômes irréductibles de tout degré (application des automorphismes) DANS F_p (dans le Gozard pas comme applications des automorphismes je crois mais après Mobius pareil). Dans F_q ?

- nombre de poly irréductibles → donne une autre construction car utilise pas l'existence
- test d'irréductibilité: Berlekamp DEV 2 (où est ce qu'on prend l'énoncé, Objectif agreg ?) et un exemple (il y en a un dans le Ulmer si besoin), objectif agreg aussi sûrement ?!

▼ III.2. Algèbre linéaire

→ Ref ? Perrin ?

- dénombrement $GL_n(F_q)$...
- dénombrement sur les corps finis: matrices diagonalisables, nilpotentes grâce au lemme de Fitting (DEV 2) ref?
- application $GL_n(F_q) \rightarrow p$ sylow, existence des p sylow Perrin ?

▼ III.3. Algèbre bilinéaire

-classification des formes quadratiques (Griffone)

- rq application à la loi de réciprocité quadratique

- le lemme avec m divise n alors $X^{p^m} - X$ divise $X^{p^n} - X$ particulièrement utile donc vaut peut-être le coup d'être ajouté quelque part mais où ? A voir dans les démo
- polynômes cyclotomiques ?