Lecon 113 :Corps finis. Application

Plan

1 Généralités

1.1 definitions, premiere prop[Gob96] [Per]

- carcteristique. sous corp premier
- anneau (commutatif) integre fini corps
- cardinal
- frobinius

1.2 $\mathbb{Z}/p\mathbb{Z}$

- corps [Per]
- Fermat
- Wilson
- exo [Gou]

2 Structure

2.1 existence, unicité

- Wedderburn [Per] **DVP**
- Thm d'existence, uncicité
- calcul dans un corps fini [PR02]

2.2 structure de $\mathbb{F}_q^*$

- cardinal, cyclique
- sous corps

3 plynome sur $\mathbb{F} - q$

3.1 généralité [Goz97]

- il enxiste infinité de pol irreduct
- isomorphisme entre $\mathbb{F}_q$

3.2 Polynome cyclo[Per]

- def
- prop

3.3 Factorisation[Goz97] [PR02]

- sans facteur crré
- Berlekamp

3.4 equation dans $\mathbb{F}_q$

- quelque exemple avec ou sans sol [Per] [Gou]
- LRQ [Tau99]**DVP**

4 application

- p groupe et thm de la base de Burnside [Hal59]**DVP**
- structure de $\mathbb{Z}/p\mathbb{Z}^*$ et constructibilité ? ? ? [Goz97]
- criptographie [PR02]
- code correcteur BCH [**?**]**DVP**

Bibliographie

Références

[Gob96] R. Goblot, *Algèbre commutative*, Masson, 1996, 512.1 GOB.

[Gou] Xavier Gourdon, *Les maths en tête algèbre*, Ellipse.

[Goz97] I. Gozard, *Théorie de galois*, Elipse, 1997, 512.1 GOZ.

[Hal59] M. Hall, *The theory of groups*, Macmillan, 1959.

[Per] Daniel Perrin, *Cours d'algèbre*, Ellipse.

[PR02] P. Sau Picart and E. Rannou, *Cours de calcul formel*, Ellipse, 2002, 512.1 SAU.

[Tau99] P. Tauvel, *cours d'algèbre*, dunod, 1999, 512.1 TAU.

Developpement

- Wedderburn [Per] **DVP**
- LRQ [Tau99]**DVP**
- p groupe et thm de la base de Burnside [Hal59]**DVP**
- code correcteur BCH [**?**]**DVP**