

113 Corps finis. Applications.

Jonathan Loupia jonas001@free.fr <http://jonas001.free.fr/agreg/index2.htm>

Plan :

- 1) Structure des corps finis
 - caractéristique et cardinal
 - commutativité (th de Wedderburn)
 - existence et unicité des corps finis

- 2) Corps finis et polynomes
 - une autre construction des corps finis
 - polynomes irréductibles sur \mathbb{F}_p (+ Eisenstein)
 - décomposition des polynomes de \mathbb{F}_p (Berlekamp)

- 3) Carrés dans un corps fini
 - quelques propriétés
 - résidus quadratiques

- 3) Autres applications
 - théorie des groupes [P](groupe linéaire)
 - arithmétique (critères de primalité, forme faible du théorème de Dirichlet [G1])
 - cryptographie
 - algèbre linéaire [P 130]

Développements :

- Berlekamp
- Eisenstein
- Wedderburn

Bibliographie

- Perrin "Cours d'algèbre" [P]
- Gozard "Théorie de Galois" [Goz]
- Gourdon "Algèbre" [G1]
- Demazure "Cours d'algèbre : primalité, divisibilité, codes" [Dem]