

Corps finis. Applications

1 Structure des corps finis

- caractéristique, cardinalité, corps premiers [2]
- existence et unicité [2]
- Sous-corps [2]
- Wedderburn [4]

2 Groupe multiplicatif \mathbb{F}_q^*

- Automorphisme, Frobenius, études des carrés [2][5]
- Loi de réciprocité quadratique [2][5]

3 $\mathbb{F}_q[X]$

- Existence de polynômes irréductibles [2]
- Comptage, fonction de Möbius [2]
- Clôture algébrique [2]
- Algorithme de Berlekamp + contre-exemple [1, 3, 2]

4 Espace vectoriel sur \mathbb{F}_q

- Groupe simple + isomorphisme des $PSL(k, \mathbb{F}_q)$ [4]
- Cardinal de $GL_n(\mathbb{F}_q)$, théorème de Sylow [4]
- Classification des formes quadratique sur \mathbb{F}_q [5]
- Théorème de Frobenius-Zolotarev [6]

Références

- [1] M. Demazure. *Cours d'algèbre : Primalité. Divisibilité. Codes.* Cassini, 1997.
- [2] I. Gozard. *Théorie de Galois.* Ellipses, 1997.
- [3] D. E. Knuth. *The art of computer programming.* Addison-Wesley, 1999.
- [4] D. Perrin. *Cours d'algèbre.* Ellipses, 1996.
- [5] J.-P. Serre. *Cours d'arithmétique.* PUF, 1970.
- [6] G. Peyré V. Beck, J. Malick. *Objectif agrégation.* HK, 2è édition, 2005.