120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Antoine Dequay

21 septembre 2022

Notes

— Prof : .

— Références :

— Rombaldi,

— Calais, *Éléments de théorie des groupes*,

— Perrin,

— Serre, *Cours d'arithmétique*,

— Saux Picart-Rannou, *Cours de calcul formel, tome 2*,

— Gozard, *Théorie de* Galois.

Table des matières

1 Structure de groupe

Cf Rombaldi.

1.1 Lien avec les groupes cycliques

1.2 Groupes abéliens de type fini

+ *Cf* Calais.

⇝ Calais pour def torsion (8.36) et théorème général.

2 Structure d'anneau

Cf Rombaldi.

2.1 Groupe multiplicatif et propriétés

2.2 Restes chinois et application

3 Utilisation des propriétés de corps

Cf Rombaldi.

3.1 Résidus quadratiques et recherche de nombres premiers

Cf Serre, Perrin *et* Saux Picart–Rannou.

⇝ Symbole de Legendre, propriétés, réciprocité quadratique,

⇝ **[DEV]** Primalité des nombres de Mersenne + ce qui va autour.

3.2 Polynômes irréductibles et corps finis

Cf Gozard *et* Perrin.

⇝ Construction, unicité, groupe linéaire sur les corps finis,

⇝ **[DEV]** pour groupe orthogonal : Le groupe $\mathcal{SO}_2(\mathbb{F}_q)$.