

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

Matei Lefebvre

2025/2026

1 Construction et propriétés de $\mathbb{Z}/n\mathbb{Z}$.

1.1 Structure de $\mathbb{Z}/n\mathbb{Z}$.

[Rom21], X.1

~ 10-15 items.

Suivre le Rombaldi en ajoutant que tous les groupes cycliques sont isomorphes à un $\mathbb{Z}/n\mathbb{Z}$ pour introduire le dev 1.

D1

Théorème. *Si p est impair alors :*

$$SO_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \in \mathbb{F}_q^{*2} \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{si } -1 \notin \mathbb{F}_q^{*2} \end{cases}$$

De plus, $SO_2(\mathbb{F}_{2^n}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$.

[CG18], VIII.3

1.2 $(\mathbb{Z}/n\mathbb{Z})^\times$ et indicatrice d'Euler.

[Rom21], X.2

~ 10 items.

Suivre le Rombaldi. (Ne pas oublier de mettre en application que les sous-groupes finis de $\mathbb{K}^\times$ sont cycliques.)

1.3 Théorème des restes chinois.

[Rom21], X.3-4

~ 5 items.

Suivre le Rombaldi en mettant au moins un exemple de résolution de système d'équations diophantiennes (peut-être en annexe).

2 Carrés dans $\mathbb{Z}/n\mathbb{Z}$.

2.1 Carrés dans $\mathbb{Z}/p\mathbb{Z}$, réciprocity quadratique.

[Goz09], VII.7 et XII.2 et [Dem09], V.3

~ 15 items.

$\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n premier ssi $\varphi(n) = n - 1$ (Rombaldi XI.5 par exemple) | :

Carrés dans $\mathbb{F}_p$ pour $p = 2$ et $p > 2$ | Carrés = noyau de $x \mapsto x^{\frac{p-1}{2}}$ | -1 est un carré ssi $p \equiv 1[4]$ (Gozard VII.7) : | : définition symbole de Legendre | $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ | définition sommes de Gauss | DEV 2 : réciprocity quadratique | exemple en annexe (Gozard XII.2) : | : définition symbole de Jacobi | propriétés symbole de Jacobi | remarque : ne caractérise pas les carrés dans $\mathbb{Z}/n\mathbb{Z}$ (uniquement un sens) | loi de réciprocity quadratique symboles Jacobi (Demazure V.3) :

D2

Proposition. On a $s(a) = \left(\frac{a}{p}\right) s(1) \forall a \in \mathbb{F}_p^*$ et $s(1)^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p \in \mathbb{K}$.

Théorème (Loi de réciprocity quadratique et deuxième loi complémentaire). .

1. $\left(\frac{p}{p'}\right) \left(\frac{p'}{p}\right) = (-1)^{\frac{(p-1)(p'-1)}{4}}$
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

[Goz09], XII.2 et [Zav13], II.6

Remarque : besoin de définir les sommes de Gauss.

2.2 Calcul effectif d'une racine carré dans $\mathbb{Z}/p\mathbb{Z}$.

[Dem09], V.1.3

~ 3 items.

Cas où $p \equiv -1[4]$ | algorithme dans le cas général (peut-être en annexe) | remarque : comment trouver le z tq $z^{2^r} \equiv -1[p]$.

2.3 Cas de $\mathbb{Z}/n\mathbb{Z}$

[Dem09], V.1.4 et [Ber20], XVI.3

~ 3 items.

On se ramène au cas $n = p^\alpha$ par le théorème chinois | cas de $p = 2$ | cas de $p \geq 3$

3 Applications.

3.1 Aux nombres premiers.

[Rom21], XI.5-6, [Dem09], II.3.6-7 et [App24], XIX.4

~ 5 items.

Théorème de Wilson (Rombaldi XI.5) | : critère de Fermat, témoins de Fermat | exemple avec $F_5 = 2^{2^5} + 1 = 2^{32} + 1$ | critère de Miller-Rabin, témoins de Miller | nombre de témoins de Miller (Demazure II.3.6-7) : | test probabiliste de primalité (Appel) | (Dirichlet faible)

3.2 Structure des groupes abéliens finis.

[Ber20], XII.5

~ 5 items.

Références

- [Dem09] M. DEMAZURE. *Cours d'algèbre*. CASSINI, 2009. ISBN : 9782842251277.
- [Goz09] I. GOZARD. *Théorie de Galois : Niveau L3-M1*. ELLIPSES, 2009. ISBN : 9782729842772.
- [Zav13] M. ZAVIDOVIQUE. *Un max de math*. CALVAGE&MOUNET, 2013. ISBN : 9782916352299.
- [CG18] P. CALDERO et J. GERMONI. *Nouvelles histoires hédonistes de groupes et de géométries Tome 2*. CALVAGE&MOUNET, 2018. ISBN : 9782916352671.
- [Ber20] G. BERHUY. *Algèbre : le grand combat*. CALVAGE&MOUNET, 2020. ISBN : 9782916352831.
- [Rom21] J.E. ROMBALDI. *Mathématiques pour l'agrégation - Algèbre et géométrie*. DEBOECK, 2021. ISBN : 9782807332201.
- [App24] W. APPEL. *Mathématiques pour l'agrégation externe. Probabilités*. DEBOECK, 2024. ISBN : 9782807361669.