

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

Soit $n \geq 2$ un entier.

I - L'anneau $\mathbb{Z}/n\mathbb{Z}$

1. Construction

Théorème 1 (Division euclidienne dans \mathbb{Z}).

$$\forall (a, b) \in \mathbb{Z}^2, \exists!(q, r) \in \mathbb{Z}^2 \text{ tel que } a = bq + r \text{ et } r \in \llbracket 0, |b| \rrbracket$$

[GOU21]
p. 9

Définition 2. Soient $a, b \in \mathbb{Z}$. On dit que a est **congru** à b modulo n si $n \mid b - a$. On note cela $a \equiv b \pmod{n}$.

[ROM21]
p. 279

Proposition 3. Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$. Alors :

- (i) $a + c \equiv b + d \pmod{n}$.
- (ii) $ac \equiv bd \pmod{n}$

Lemme 4. Tout idéal de \mathbb{Z} est principal, de la forme $(n) = n\mathbb{Z}$.

Définition 5. Le quotient de l'anneau \mathbb{Z} par son idéal $n\mathbb{Z}$ est l'anneau noté $\mathbb{Z}/n\mathbb{Z}$. On note $\bar{a} = \{a + qn \mid q \in \mathbb{Z}\}$ l'image d'un élément $a \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Remarque 6. Soient $a, b \in \mathbb{Z}$.

$$\bar{a} = \bar{b} \iff a \equiv b \pmod{n}$$

Proposition 7. (i) $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$.

(ii) La compatibilité de \equiv avec les lois $+$ et \times sur \mathbb{Z} conjuguée à la remarque précédente transporte la structure d'anneau à $\mathbb{Z}/n\mathbb{Z}$ en posant, pour tout $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$:

- $\bar{a} + \bar{b} = \overline{a + b}$.
- $\bar{a}\bar{b} = \overline{ab}$.

2. Le groupe additif

a. Générateurs

Théorème 8. Soit $a \in \mathbb{Z}$. Les assertions suivantes sont équivalentes :

- (i) $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- (ii) $\text{pgcd}(a, n) = 1$.
- (iii) a est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exemple 9. $(\mathbb{Z}/4\mathbb{Z})^\times = \{\pm\bar{1}\}$.

p. 301

Proposition 10. (i) \mathbb{Z} est monogène, l'ensemble de ses générateurs est $\mathbb{Z}^\times = \{\pm 1\}$.

p. 14

(ii) $\mathbb{Z}/n\mathbb{Z}$, l'ensemble de ses générateurs est $(\mathbb{Z}/n\mathbb{Z})^\times$.

Corollaire 11. Soit G un groupe.

- (i) Si G est monogène infini, alors $G \cong \mathbb{Z}$.
- (ii) Si G est cyclique d'ordre n , alors $G \cong \mathbb{Z}/n\mathbb{Z}$.

Exemple 12. Le groupe des racines n -ièmes de l'unité, μ_n , est isomorphe $\mathbb{Z}/n\mathbb{Z}$ via

$$\bar{k} \mapsto e^{\frac{2ik\pi}{n}}$$

b. Sous-groupes additifs et idéaux

Théorème 13. Les sous-groupes additifs de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre divisant n . Réciproquement, pour tout diviseur d de n , il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, c'est le groupe cyclique engendré par $\frac{\bar{n}}{d}$.

p. 281

Théorème 14. (i) Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont ses sous-groupes additifs.

p. 255

(ii) Les idéaux premiers de $\mathbb{Z}/n\mathbb{Z}$ sont les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$: ce sont les idéaux engendrés par (\bar{p}) où p est un diviseur premier de n .

3. Indicatrice d'Euler

Définition 15. L'indicatrice d'Euler φ est la fonction qui à un entier k , associe le nombre d'entiers compris entre 1 et n qui sont premiers avec k .

p. 283

Remarque 16. D'après le Théorème 8, $\varphi(n)$ est le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$ et est également le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exemple 17. — Si n est premier, $\varphi(n) = n - 1$.
— $\varphi(4) = 2$ d'après l'Exemple 9.

Proposition 18. Pour tout p premier et pour tout entier n ,

$$\varphi(p^n) = p^n - p^{n-1}$$

[GOZ]
p. 4

Théorème 19 (Chinois). Soient n et m deux entiers premiers entre eux. Alors,

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Corollaire 20. $\forall m, n \in \mathbb{Z}$ premiers entre eux,

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Proposition 21 (Théorème Euler). Pour tout entier relatif a premier avec n , $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proposition 22 (Petit théorème de Fermat). Pour tout entier relatif a , pour tout p premier, $a^{p-1} \equiv 1 \pmod{p}$.

Proposition 23. Pour tout entier naturel n ,

$$\sum_{d|n} \varphi(d) = n$$

II - Cas où n est premier

1. Structure de corps

Proposition 24. Les assertions suivantes sont équivalentes.

- (i) n est un nombre premier.
- (ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre.
- (iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Théorème 25. Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

p. 83

Corollaire 26. Si p désigne un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Remarque 27. On a un résultat encore plus fort : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 2, 4, p^\alpha$ ou $2p^\alpha$ avec p premier impair et $\alpha \geq 1$.

[ROM21]
p. 294

2. Carrés

Remarque 28. Tout élément de $\mathbb{Z}/2\mathbb{Z}$ est un carré.

p. 427

Soit p un nombre premier impair.

Théorème 29. (i) Il y a $\frac{p-1}{2}$ carrés et autant de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

(ii) Les carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ sont les racines de $X^{\frac{p-1}{2}} - 1$ et les non carrés celles de $X^{\frac{p-1}{2}} + 1$.

Corollaire 30. -1 est un carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si $p \equiv 1 \pmod{4}$.

III - Applications

1. Systèmes de congruences

Proposition 31. Soit a un entier non nul. L'équation

$$ax \equiv 1 \pmod{n}$$

admet des solutions si et seulement si $\text{pgcd}(a, n) = 1$.

p. 289

Corollaire 32. Soient a un entier non nul et b un entier relatif. L'équation

$$ax \equiv b \pmod{n}$$

a des solutions si et seulement si $d = \text{pgcd}(a, n) \mid b$. Dans ce cas, l'ensemble des solutions est

$$\left\{ \frac{b}{d}x_0 + k\frac{n}{d} \mid k \in \mathbb{Z} \right\}$$

où x_0 est une solution de l'équation $\frac{a}{n}x \equiv 1 \pmod{n}$.

Pour résoudre des systèmes de congruences, on va préciser le Théorème 19.

p. 285

Théorème 33 (Chinois). Soient $n_1, \dots, n_r \geq 2$ des entiers. On note $n = \prod_{i=1}^r n_i$ et $\pi_k = \pi_{n_k\mathbb{Z}}$ la surjection canonique de \mathbb{Z} sur $\mathbb{Z}/k\mathbb{Z}$ pour tout $k \in \llbracket 1, r \rrbracket$.

Les entiers n_1, \dots, n_r sont premiers entre eux si et seulement si les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ sont isomorphes. Dans ce cas, l'isomorphisme est explicité par l'application

$$\psi: \begin{array}{l} \mathbb{Z}/n\mathbb{Z} \rightarrow \prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z} \\ \pi_n k \rightarrow (\pi_i(k))_{i \in \llbracket 1, r \rrbracket} \end{array}$$

Exemple 34.

$$\begin{cases} k \equiv 2 \pmod{4} \\ k \equiv 3 \pmod{5} \\ k \equiv 1 \pmod{9} \end{cases}$$

admet pour ensemble de solutions $\{838 + 180q \mid q \in \mathbb{Z}\}$.

p. 291

2. Étude d'équations diophantiennes

a. Entiers sommes de deux carrés

Notation 35. On note

$$N: \begin{array}{l} \mathbb{Z}[i] \rightarrow \mathbb{N} \\ a + ib \rightarrow a^2 + b^2 \end{array}$$

et Σ l'ensemble des entiers qui sont somme de deux carrés.

[I-P]
p. 137

Remarque 36. $n \in \Sigma \iff \exists z \in \mathbb{Z}[i]$ tel que $N(z) = n$.

Théorème 37 (Deux carrés de Fermat). Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \pmod{4}$ (où $v_p(n)$ désigne la valuation p -adique de n).

b. Premiers congrus à 1 modulo n

Notation 38. On note Φ_n le n -ième polynôme cyclotomique.

[GOU21]
p. 99

Lemme 39. Soient $a \in \mathbb{N}$ et p premier tels que $p \mid \Phi_n(a)$ mais $p \nmid \Phi_d(a)$ pour tout diviseur strict d de n . Alors $p \equiv 1 \pmod{n}$.

Théorème 40 (Dirichlet faible). Pour tout entier n , il existe une infinité de nombres premiers congrus à 1 modulo n .

3. Irréductibilité de polynômes

Lemme 41 (Gauss). (i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est égal à 1).

(ii) $\forall P, Q \in \mathbb{Z}[X] \setminus \{0\}, \gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

[GOZ]
p. 10

Théorème 42 (Critère d'Eisenstein). Soit $P = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. On suppose qu'il existe p premier tel que :

(i) $p \mid a_i, \forall i \in \llbracket 0, n-1 \rrbracket$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$.

[DEV]

Application 43. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur \mathbb{Z} .

[PER]
p. 67

Théorème 44 (Critère d'irréductibilité modulo p). Soit $P = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. Soit p un premier. On suppose $p \nmid a_n$.

Si \bar{P} est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

[GOZ]
p. 12

Exemple 45. Le polynôme $X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$.

4. Chiffrement RSA

Définition 46. Afin de chiffrer un **message** (tout entier découpé en séquence d'entiers de taille bornée) en utilisant RSA, on doit a besoin de deux clés :

- Une **clé privée**, qui est un couple de nombres premiers (p, q) .
- La **clé publique** correspondante, qui est le couple (n, e) où $n = pq$ et e est l'inverse de d modulo $\phi(n)$ où d désigne un nombre premier à $\phi(n)$.

[ULM18]
p. 62

Nous conserverons ces notations pour la suite.

Théorème 47 (Chiffrement RSA). Soit $m = (m_i)_{i \in \llbracket 1, r \rrbracket}$ un message où pour tout i , $m_i < n$.

(i) Possédant la clé publique, on peut *chiffrer* ce message en un message m' :

$$m' = (m_i^e)_{i \in \llbracket 1, r \rrbracket}$$

(ii) Possédant la clé privée, on peut *déchiffrer* le message m' pour reconstituer m :

$$\forall i \in \llbracket 1, r \rrbracket, (m_i^e)^d \equiv m_i \pmod{n}$$

Remarque 48. — L'intérêt vient pour des premiers p et q très grands : il devient alors très compliqué de factoriser n et d'obtenir la clé privée.

— Les inverses peuvent se calculer à l'aide de l'algorithme de Bézout.

Bibliographie

Les maths en tête

[GOU21]

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3^e éd. Ellipses, 13 juill. 2021.

<https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html>.

Théorie de Galois

[GOZ]

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1*. 2^e éd. Ellipses, 1^{er} avr. 2009.

<https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html>.

L'oral à l'agrégation de mathématiques

[I-P]

Lucas ISENMANN et Timothée PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2^e éd. Ellipses, 26 mars 2024.

<https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html>.

Cours d'algèbre

[PER]

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.

<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.

Mathématiques pour l'agrégation

[ROM21]

Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2^e éd. De Boeck Supérieur, 20 avr. 2021.

<https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie>.

Anneaux, corps, résultants

[ULM18]

Felix ULMER. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation*. Ellipses, 28 août 2018.

<https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-l3-m1-agregation-9782340025752.html>.