

Chapter 19 Anneaux, corps

19.1 La structure d'anneau

Exercice 19.1 Étude d'un ensemble de fonctions

Soit A l'ensemble des fonctions définies sur \mathbb{R} telles que $f(0) = f(1)$. Démontrer que A est un anneau.

Exercice 19.2 (*)

L'anneau $\mathbb{R}^{\mathbb{R}}$ est-il intègre? Déterminer $U(\mathbb{R}^{\mathbb{R}})$.

Exercice 19.3 (**)

Soit \mathbb{D} l'ensemble des nombre décimaux *i.e.*

$$\mathbb{D} = \left\{ \frac{a}{10^n} \mid a \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}.$$

1. Montrer que $(\mathbb{D}, +, \times)$ est un anneau où $+$ et \times sont les lois usuelles.
2. Déterminer le groupe des éléments inversibles de \mathbb{D} .

Exercice 19.4 (*)

On pose

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}.$$

1. Montrer que A est un anneau pour les lois d'addition et de multiplication matricielles.
2. Déterminer $U(A)$.

Exercice 19.5

Montrer que $\mathbb{Q}[i\sqrt{3}] = \left\{ a + bi\sqrt{3} \mid (a, b) \in \mathbb{Q}^2 \right\}$ est un corps.

Exercice 19.6 Études d'inversibilités dans un anneau

Soit $(A, +, \cdot)$ un anneau.

1. Soit $a \in A$ tel que $a^2 = 0$. Démontrer que $1 - a$ et $1 + a$ sont inversibles et expliciter leurs inverses.
2. Généraliser pour $a \in A$ tel qu'il existe $n \in \mathbb{N}^*$ pour lequel $a^n = 0$.

Exercice 19.7 Éléments nilpotents

Soit $(A, +, \cdot)$ un anneau. Un élément x de A est dit **nilpotent** s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$.

1. Démontrer que si xy est nilpotent, alors yx l'est aussi.
2. Démontrer que si x et y sont nilpotents et commutent, alors, xy et $x + y$ sont nilpotents.

Exercice 19.8

Soit A un anneau commutatif. Pour $x \in A$ et $n \in \mathbb{N}^*$, on note

$$x^{(0)} = 1, \quad x^{(1)} = x, \quad x^{(2)} = x(x-1), \quad \dots \dots \quad x^{(n)} = x(x-1) \dots (x-n+1).$$

Montrer

$$\forall (x, y) \in A^2, (x+y)^{(n)} = \sum_{k=0}^n \binom{n}{k} x^{(n-k)} y^{(k)}.$$

19.2 Sous-structures

Exercice 19.9

Soit

$$M = \{ aI_2 + bJ \in \mathcal{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R} \}$$

$$\text{où } I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ et } J = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}.$$

1. Calculer J^2 et montrer que si $a, b \in \mathbb{R}$ et $aI_2 + bJ = 0$ alors $a = b = 0$.
2. Montrer que, muni des lois usuelles sur $\mathcal{M}_2(\mathbb{R})$, M est un anneau.
Cet anneau est-il commutatif, intègre ?
3. M est-il un corps ?

Exercice 19.10 Nilradical d'un anneau

On appelle nilradical d'un anneau commutatif $(A, +, \times)$ l'ensemble N formé des éléments nilpotents de A , c'est-à-dire des $x \in A$ tels qu'il existe $n \in \mathbb{N}^*$ vérifiant $x^n = 0_A$.

Montrer que N est un idéal de A .

Exercice 19.11 Radical d'un idéal

Soit I un idéal d'un anneau commutatif A . On appelle **radical** de l'idéal I l'ensemble $R(I)$ des éléments x de A pour lesquels il existe $q \in \mathbb{N}^*$ tel que $x^q \in I$.

1. Montrer que $R(I)$ est un idéal de A contenant I .
2. Soient I et J deux idéaux. Vérifier

$$R(I \cap J) = R(I) \cap R(J).$$

3. On suppose que $A = \mathbb{Z}$. Déterminer le radical de $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

19.3 Morphismes d'anneaux

Exercice 19.12

Soit a un élément d'un ensemble X . Montrer que l'application

$$\begin{aligned} E_a : \mathcal{F}(X, \mathbb{R}) &\rightarrow \mathbb{R} \\ f &\mapsto f(a) \end{aligned}$$

est un morphisme d'anneaux.

Exercice 19.13

Pour tout couple (a, b) de \mathbb{R}^2 , on pose

$$M_{a,b} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Soit

$$S = \{ M_{a,b} \mid (a, b) \in \mathbb{R}^2 \}, \quad S^* = S \setminus \{ M_{0,0} \}, \quad \text{et} \quad f : \begin{array}{ccc} S & \rightarrow & \mathbb{C} \\ M_{a,b} & \mapsto & a + ib \end{array}.$$

1. (a) Montrer que S est un sous-anneau de l'anneau usuel $\mathcal{M}_2(\mathbb{R})$.
(b) Montrer que S^* est un sous-groupe multiplicatif de $\mathbf{GL}_2(\mathbb{R})$.
2. Montrer que f est un isomorphisme de l'anneau $(S, +, \cdot)$ sur l'anneau $(\mathbb{C}, +, \cdot)$.
3. En déduire que $(S, +, \cdot)$ est un corps.

19.4 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Exercice 19.14 (*)

Résoudre les équations suivantes:

1. $\bar{3}x = \bar{7}$ d'inconnue $x \in \mathbb{Z}/13\mathbb{Z}$.
2. $\bar{2}x = \bar{5}$ d'inconnue $x \in \mathbb{Z}/12\mathbb{Z}$.
3. $\bar{6}x = \bar{21}$ d'inconnue $x \in \mathbb{Z}/45\mathbb{Z}$.

Exercice 19.15 (**)

Soit p un nombre premier impair, $(a, b, c) \in \mathbb{Z}/p\mathbb{Z}$ avec $a \neq \bar{0}$.

Montrer que l'équation

$$ax^2 + bx + c = \bar{0}$$

d'inconnue $x \in \mathbb{Z}/p\mathbb{Z}$ possède au plus 2 solutions. À quelle condition nécessaire et suffisante sur a, b et c en possède-t-elle au moins une?

Exercice 19.16 (***)

On désigne par F_p le corps $\mathbb{Z}/p\mathbb{Z}$ pour p premier.

On munit l'ensemble $E = F_{11} \times F_{11}$ des deux lois de composition données par les formules suivantes

$$(u, v) + (x, y) = (u + x, v + y) \quad \text{et} \quad (u, v) \cdot (x, y) = (ux + 7vy, uy + vx).$$

Montrer que l'on obtient de cette façon un corps à 121 éléments.

Exercice 19.17 (****)

Soit $(m, n) \in (\mathbb{N}^*)^2$. On notera ici $\bar{x}_{(n\mathbb{Z})}$ la classe de l'entier relatif x modulo n .

1. Montrer que l'application

$$\begin{aligned} \mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar{x}_{(mn\mathbb{Z})} &\mapsto (\bar{x}_{(m\mathbb{Z})}, \bar{x}_{(n\mathbb{Z})}) \end{aligned}$$

est bien définie et que c'est un morphisme d'anneaux.

2. Montrer que si m et n sont premiers entre eux, alors cette application est un isomorphisme d'anneaux.
3. Généraliser ce dernier résultat. En déduire le *théorème chinois*: soit $(n_1, \dots, n_k) \in (\mathbb{N}^*)^k$ des entiers premiers entre eux deux à deux, et soit $(a_1, \dots, a_k) \in \mathbb{Z}^k$. Alors il existe $x \in \mathbb{Z}$ tel que

$$\forall i \in \llbracket 1, k \rrbracket, x \equiv a_i \pmod{n_i}.$$

Que dire de l'ensemble des solutions de ce système de congruences?

4. Application. Déterminer toutes les solutions du système

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 1 \pmod{9} \\ x \equiv -1 \pmod{25}. \end{cases}$$

Pour cela, on pourra chercher

- x_1 une solution du système $x \equiv 3 \pmod{8}$ et $x \equiv 0 \pmod{9 \times 25}$,
- x_2 une solution du système $x \equiv 1 \pmod{9}$ et $x \equiv 0 \pmod{8 \times 25}$,
- x_3 une solution du système $x \equiv -1 \pmod{25}$ et $x \equiv 0 \pmod{8 \times 9}$.

5. Soient p premier, $p \geq 3$ et $n \in \mathbb{N}^*$. Résoudre dans $\mathbb{Z}/p^n\mathbb{Z}$ l'équation

$$(\bar{x}_{(p^n\mathbb{Z})})^2 = \bar{1}_{(p^n\mathbb{Z})}.$$

Traiter le même problème pour $p = 2$.

6. Quel est le nombre de solutions de l'équation

$$(\bar{x}_{(1800\mathbb{Z})})^2 = \bar{1}_{(1800\mathbb{Z})}?$$

Indiquer comment on pourrait déterminer ces solutions.