EXERCICES – CHAPITRE 5

STRUCTURES ALGÉBRIQUES

Anneaux : définition et calculs

EXERCICE 1 ⋆

Les ensembles suivants, munis des deux lois indiquées, sont-ils des anneaux ? Le cas échéant, préciser s'ils sont commutatifs ; sinon, indiquer quel axiome échoue.

1. $(\mathbb{N}\,;+\,;\times)$
2. $(\mathbb{Z}\,;+\,;\times)$
3. $(2\mathbb{Z}\,;+\,;\times)$
4. $(\mathbb{Q}\,;+\,;\times)$
5. $(\mathbb{R}^{\mathbb{R}}\,;+\,;\times)$, les opérations étant définies point par point.
6. $(\mathbb{R}^2\,;+\,;\times)$, les opérations étant définies coordonnée par coordonnée.
7. $(\mathcal{P}(E)\,;\Delta\,;\cap)$, où Δ désigne la différence symétrique du chapitre 1.

EXERCICE 2 ⋆

Soit $(A\,;+\,;\times)$ un anneau, de neutres 0_A et 1_A, et soient x et y deux éléments de A.

1. Démontrer que $0_A \times x = 0_A$. On pourra partir de $0_A = 0_A + 0_A$.
2. Démontrer que $(-x)y = -(xy)$, puis que $(-x)(-y) = xy$.
3. Développer $(x+y)^2$, puis $(x+y)(x-y)$.
4. À quelle condition retrouve-t-on les identités remarquables habituelles ?

EXERCICE 3 ⋆⋆

On rappelle qu'un élément x non nul d'un anneau A est un *diviseur de zéro* lorsqu'il existe y non nul dans A tel que $xy = 0_A$.

1. Exhiber deux diviseurs de zéro dans $(\mathbb{R}^2\,;+\,;\times)$.
2. Vérifier que les fonctions $f : x \mapsto |x| + x$ et $g : x \mapsto |x| - x$ sont des diviseurs de zéro de $(\mathbb{R}^{\mathbb{R}}\,;+\,;\times)$.
3. Exhiber deux diviseurs de zéro dans $\mathbb{Z}/6\mathbb{Z}$.
4. Démontrer qu'un élément inversible d'un anneau n'est jamais un diviseur de zéro.
5. En déduire qu'un corps ne possède aucun diviseur de zéro.

EXERCICE 4 ⋆⋆

Soit A un anneau dans lequel $x^2 = x$ pour tout $x \in A$. Un tel anneau est dit *de Boole*.

1. En développant $(x+x)^2$, démontrer que $x + x = 0_A$ pour tout $x \in A$, c'est-à-dire $-x = x$.
2. En développant $(x+y)^2$, démontrer que $xy + yx = 0_A$.
3. En déduire que A est commutatif.
4. Vérifier que $(\mathcal{P}(E)\,;\Delta\,;\cap)$ est un anneau de Boole.

EXERCICE 5 ⋆⋆⋆

Un élément x d'un anneau A est dit *nilpotent* lorsqu'il existe un entier $n \geqslant 1$ tel que $x^n = 0_A$. Dans les trois premières questions, l'anneau A est supposé **commutatif**, et x et y désignent deux éléments nilpotents de A.

1. Démontrer que xy est nilpotent.
2. Démontrer que $x + y$ est nilpotent. On pourra utiliser la formule du binôme, valable dans un anneau commutatif.
3. Démontrer que $1_A - x$ est inversible, et préciser son inverse.
4. Dans cette question, l'anneau A n'est plus supposé commutatif. Soient u et v deux éléments de A tels que uv soit nilpotent. Démontrer que vu l'est également.

Sous-anneaux

EXERCICE 6 ⋆

Dans chaque cas, déterminer si la partie B est un sous-anneau de l'anneau A. On utilisera la caractérisation de la proposition 1.

1. $A = \mathbb{Z}$ et $B = 2\mathbb{Z}$.
2. $A = \mathbb{Q}$ et $B = \mathbb{Z}$.
3. $A = \mathbb{R}$ et $B = \mathbb{Q}$.
4. $A = \mathbb{R}$ et $B = \left\{a + b\sqrt{3} \mid (a\,;b) \in \mathbb{Z}^2\right\}$.
5. $A = \mathbb{R}^{\mathbb{R}}$ et B est l'ensemble des fonctions continues sur $\mathbb{R}$.
6. $A = \mathbb{R}^{\mathbb{R}}$ et $B = \left\{f \in \mathbb{R}^{\mathbb{R}} \mid f(0) = 0\right\}$.
7. $A = \mathbb{R}^{\mathbb{R}}$ et $B = \left\{f \in \mathbb{R}^{\mathbb{R}} \mid f(1) = f(2)\right\}$.

EXERCICE 7 ⋆⋆

On appelle *entiers de Gauss* les nombres complexes de la forme $a + \mathrm{i}b$ avec $(a\,;b) \in \mathbb{Z}^2$, et l'on note $\mathbb{Z}[\mathrm{i}]$ leur ensemble.

1. Démontrer que $(\mathbb{Z}[\mathrm{i}]\,;+\,;\times)$ est un sous-anneau de $(\mathbb{C}\,;+\,;\times)$.
2. Pour tout nombre complexe z, on pose $N(z) = z\overline{z}$.
   (a) Démontrer que $N(z)N(z') = N(zz')$ pour tous complexes z et z'.
   (b) Démontrer que $N(z)$ est un entier naturel pour tout entier de Gauss z.
   (c) Soit z un entier de Gauss inversible *dans* $\mathbb{Z}[\mathrm{i}]$. Déduire des questions précédentes que $N(z) = 1$.
   (d) Déterminer tous les éléments inversibles de $\mathbb{Z}[\mathrm{i}]$.

EXERCICE 8 ⋆⋆

On considère l'ensemble des rationnels admettant une écriture à dénominateur impair :

$$A = \left\{\frac{m}{n} \;\middle|\; m \in \mathbb{Z},\ n \in 2\mathbb{N} + 1\right\}$$

1. Démontrer que A est un sous-anneau de $(\mathbb{Q}\,;+\,;\times)$.
2. Déterminer les éléments inversibles de $(A\,;+\,;\times)$.

EXERCICE 9 ⋆⋆

Soient B et C deux sous-anneaux d'un anneau A.

1. Démontrer que $B \cap C$ est un sous-anneau de A.
2. On prend $A = \mathbb{Q}^2$, muni des lois coordonnée par coordonnée, $B = \mathbb{Q} \times \mathbb{Z}$ et $C = \mathbb{Z} \times \mathbb{Q}$. Vérifier que B et C sont deux sous-anneaux de A, puis démontrer que $B \cup C$ n'en est pas un.
3. L'intersection d'une famille quelconque de sous-anneaux de A est-elle un sous-anneau ? Justifier.

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

EXERCICE 10 ⋆

1. Effectuer les calculs suivants dans $\mathbb{Z}/7\mathbb{Z}$:

   (a) $\overline{5} + \overline{4}$ (b) $\overline{3} \times \overline{5}$ (c) $\overline{6}^2$ (d) $\overline{2}^5$

2. Effectuer les calculs suivants dans $\mathbb{Z}/12\mathbb{Z}$:

   (a) $\overline{7} + \overline{8}$ (b) $\overline{5} \times \overline{9}$ (c) $\overline{4} \times \overline{3}$ (d) l'opposé de $\overline{1}$

3. Déterminer le reste de la division euclidienne de 3^{100} par 7. On pourra commencer par calculer les puissances successives de $\overline{3}$ dans $\mathbb{Z}/7\mathbb{Z}$.

EXERCICE 11 ⋆

1. Dresser la table de multiplication de $\mathbb{Z}/8\mathbb{Z}$.
2. En déduire la liste des éléments inversibles de $\mathbb{Z}/8\mathbb{Z}$, ainsi que l'inverse de chacun. Que remarque-t-on ?
3. En déduire la liste des diviseurs de zéro de $\mathbb{Z}/8\mathbb{Z}$.
4. L'anneau $\mathbb{Z}/8\mathbb{Z}$ est-il un corps ? Le théorème 1 permettait-il de le prévoir ?

EXERCICE 12 ⋆⋆

Résoudre les équations suivantes, d'inconnue $\overline{x}$.

1. $\overline{3}\,\overline{x} = \overline{2}$ dans $\mathbb{Z}/7\mathbb{Z}$
2. $\overline{3}\,\overline{x} = \overline{0}$ dans $\mathbb{Z}/12\mathbb{Z}$
3. $\overline{x}^2 = \overline{1}$ dans $\mathbb{Z}/5\mathbb{Z}$
4. $\overline{x}^2 = \overline{1}$ dans $\mathbb{Z}/8\mathbb{Z}$

Comparer les deux dernières réponses, et expliquer l'écart à l'aide du théorème 1.

EXERCICE 13 ⋆⋆

1. Donner la liste des éléments de $\mathbb{Z}/7\mathbb{Z}$ qui sont des carrés. Combien y en a-t-il ?
2. Soit $\overline{a}$ un élément de $\mathbb{Z}/7\mathbb{Z}$. Déterminer le nombre d'éléments de l'ensemble :

$$\mathcal{A} = \{ -\overline{x}^2 + \overline{a} \mid \overline{x} \in \mathbb{Z}/7\mathbb{Z} \}$$

3. En comparant le nombre d'éléments de $\mathcal{A}$ et celui de l'ensemble des carrés, démontrer que l'équation $\overline{x}^2 + \overline{y}^2 = \overline{a}$ admet toujours une solution dans $\mathbb{Z}/7\mathbb{Z}$.
4. Donner explicitement un couple $(u\,;v)$ d'entiers relatifs tel que $u^2 + v^2 \equiv -1\ [7]$.

Corps

EXERCICE 14 ⋆

Les anneaux suivants sont-ils des corps ? Justifier, en exhibant le cas échéant un élément non nul non inversible.

1. $(\mathbb{Z}\,;+\,;\times)$
2. $(\mathbb{Q}\,;+\,;\times)$
3. $\mathbb{Z}/5\mathbb{Z}$
4. $\mathbb{Z}/6\mathbb{Z}$
5. $\mathbb{Z}/11\mathbb{Z}$
6. $\mathbb{Z}/12\mathbb{Z}$
7. $(\mathbb{R}^2\,;+\,;\times)$
8. $(\mathbb{R}^{\mathbb{R}}\,;+\,;\times)$

EXERCICE 15 ⋆⋆

Démontrer que les deux ensembles suivants, munis de l'addition et de la multiplication usuelles, sont des corps.

1. $\mathbb{Q}[\mathrm{i}] = \{a + \mathrm{i}b \mid (a\,;b) \in \mathbb{Q}^2\}$.
2. $\mathbb{Q}[\sqrt{d}\,] = \{a + b\sqrt{d} \mid (a\,;b) \in \mathbb{Q}^2\}$, où d est un entier naturel tel que $\sqrt{d} \notin \mathbb{Q}$.

Pour la seconde question, on prendra garde à justifier que le dénominateur intervenant dans l'inverse ne s'annule pas.

EXERCICE 16 ⋆⋆

Soit $n \geqslant 2$ un entier. On admet le théorème de Bézout : deux entiers x et n sont premiers entre eux si et seulement s'il existe $(u\,;v) \in \mathbb{Z}^2$ tel que $xu + nv = 1$.

1. Démontrer que $\overline{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si x et n sont premiers entre eux.
2. Application : déterminer les éléments inversibles de $\mathbb{Z}/10\mathbb{Z}$, ainsi que l'inverse de chacun.
3. Soit $\overline{x}$ un élément non nul de $\mathbb{Z}/n\mathbb{Z}$ non inversible. Démontrer que $\overline{x}$ est un diviseur de zéro.
4. Retrouver le théorème 1 du cours à l'aide de la question 1.

Morphismes d'anneaux

EXERCICE 17 ⋆

Les applications suivantes sont-elles des morphismes d'anneaux ? Justifier, en précisant le cas échéant laquelle des trois conditions échoue.

1. $z \mapsto \overline{z}$ de $\mathbb{C}$ dans $\mathbb{C}$.
2. $x \mapsto \overline{x}$ de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.
3. $f \mapsto f(a)$ de $\mathbb{R}^{\mathbb{R}}$ dans $\mathbb{R}$, où a est un réel fixé.
4. $x \mapsto 2x$ de $\mathbb{Z}$ dans $\mathbb{Z}$.
5. $z \mapsto |z|$ de $\mathbb{C}$ dans $\mathbb{R}$.
6. $x \mapsto (x\,;x)$ de $\mathbb{Z}$ dans $\mathbb{Z}^2$.
7. $x \mapsto (x\,;0)$ de $\mathbb{Z}$ dans $\mathbb{Z}^2$.
8. $x \mapsto x^2$ de $\mathbb{Z}$ dans $\mathbb{Z}$.

EXERCICE 18 ⋆⋆

Soit $\varphi : (A\,;+\,;\times) \longrightarrow (B\,;\oplus\,;\otimes)$ un morphisme d'anneaux, et $\operatorname{Ker}\varphi = \{x \in A \mid \varphi(x) = 0_B\}$.

1. Démontrer que $\operatorname{Ker}\varphi$ est un sous-groupe de $(A\,;+)$.
2. Démontrer que pour tout $x \in \operatorname{Ker}\varphi$ et tout $a \in A$, les éléments ax et xa appartiennent à $\operatorname{Ker}\varphi$.
3. Démontrer que $\operatorname{Ker}\varphi$ n'est jamais un sous-anneau de A.
4. Déterminer le noyau de la réduction modulo n, puis celui de l'évaluation en a.

EXERCICE 19 ⋆⋆

Soit $(A\,;+\,;\times)$ un anneau, et $\varphi : \mathbb{Z} \to A$ un morphisme d'anneaux. Pour $n \in \mathbb{N}$, on note $n \cdot 1_A$ la somme $1_A + \cdots + 1_A$ comportant n termes, avec la convention $0 \cdot 1_A = 0_A$.

1. Démontrer par récurrence que $\varphi(n) = n \cdot 1_A$ pour tout $n \in \mathbb{N}$, puis étendre à $n \in \mathbb{Z}$.
2. En déduire qu'il existe *au plus* un morphisme d'anneaux de $\mathbb{Z}$ dans A.
3. Déterminer le noyau de ce morphisme dans le cas $A = \mathbb{Z}/n\mathbb{Z}$, puis dans le cas $A = \mathbb{R}$.

Exercices de synthèse

EXERCICE 20 : VRAI OU FAUX

Pour chaque affirmation, dire si elle est vraie ou fausse en justifiant la réponse.

1. Dans un anneau, un produit peut être nul sans qu'aucun de ses facteurs ne le soit.
2. Un anneau n'est pas nécessairement commutatif.
3. L'ensemble $2\mathbb{Z}$ est un sous-anneau de $(\mathbb{Z}\,;+\,;\times)$.
4. Un corps est un anneau commutatif non nul dont tout élément non nul est inversible.
5. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
6. Un corps ne possède aucun diviseur de zéro.
7. Pour un morphisme d'anneaux, la condition $\varphi(1_A) = 1_B$ se déduit des autres conditions.
8. Le noyau d'un morphisme d'anneaux est un sous-anneau de l'anneau de départ.
9. Dans un anneau commutatif, $(x+y)^2 = x^2 + 2xy + y^2$ pour tous x et y.
10. Tout sous-anneau d'un corps est un corps.

EXERCICE 21 ⋆⋆⋆

On note $\mathcal{M}$ l'ensemble des matrices carrées de taille 2 à coefficients réels, muni de l'addition terme à terme et du produit défini par :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

On admet que $(\mathcal{M}\,;+\,;\times)$ est un anneau non commutatif, de neutres la matrice nulle et la matrice identité. On considère alors :

$$\mathcal{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; (a\,;b) \in \mathbb{R}^2 \right\}$$

1. Démontrer que $\mathcal{C}$ est un sous-anneau de $\mathcal{M}$.
2. Démontrer que $\mathcal{C}$ est commutatif.

3. Démontrer que tout élément non nul de $\mathcal{C}$ est inversible, et conclure que $\mathcal{C}$ est un corps.
4. Démontrer que l'application ci-dessous est un isomorphisme d'anneaux :

$$\phi : \left| \begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathbb{C} \\ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} & \longmapsto & a + \mathrm{i}b \end{array} \right.$$

EXERCICE 22 ⋆⋆⋆

Soit A un anneau commutatif **fini**, ne possédant aucun diviseur de zéro.

1. Soit a un élément non nul de A. Démontrer que l'application $m_a : x \mapsto ax$, de A dans A, est injective.
2. En déduire que m_a est surjective. On pourra invoquer la question 4 de l'exercice 17 du chapitre 4.
3. En déduire que a est inversible, puis que A est un corps.
4. On admet le lemme d'Euclide : si un nombre premier p divise un produit xy, alors il divise x ou y. Démontrer que $\mathbb{Z}/p\mathbb{Z}$ ne possède aucun diviseur de zéro lorsque p est premier.
5. En déduire une seconde démonstration du sens réciproque du théorème 1.