Anneaux, corps

Anneaux

Autocorrection A.

Dans cet exercice, B désigne à chaque fois une partie d'un anneau A (muni des lois d'addition et de multiplication usuelles). Déterminer si B est un sous-anneau de A.

(i) $A = \mathbb{Z}$, $B = \mathbb{N}$;

(ii) $A = \mathbb{R}$, $B = \left\{ \frac{k}{10^n} \,\middle|\, k \in \mathbb{Z}, n \in \mathbb{N} \right\}$ est l'ensemble des nombres décimaux ;

(iii) $A = M_2(\mathbb{R})$, $B = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \,\middle|\, a \in \mathbb{Z} \right\}$;

(iv) $A = M_n(\mathbb{R})$, $B = S_n(\mathbb{R})$;

(v) $A = M_n(\mathbb{C})$, $B = M_n(\mathbb{R})$;

(vi) $A = \mathbb{R}^{\mathbb{N}}$, B est l'ensemble des suites convergeant vers 0 ;

(vii) $A = \mathbb{R}^{\mathbb{N}}$, B est l'ensemble des suites convergeant vers 1 ;

(viii) $A = \mathbb{R}^{\mathbb{N}}$, B est l'ensemble des suites convergentes ;

(ix) $A = \mathbb{R}^{\mathbb{R}}$, B est l'ensemble des fonctions paires.

Autocorrection B.

Soit A un anneau et B un sous-anneau.

1. A-t-on en général $B^\times \subseteq A^\times$?
2. A-t-on en général $B^\times = A^\times \cap B$?

Exercice 1$^+$.

Soit A un anneau tel que $\forall x, y \in A, (xy)^2 = x^2y^2$.

1. Montrer $\forall x, y \in A, x^2y = xyx = yx^2$.
2. Montrer que A est commutatif.

Exercice 2.

Soit A un anneau et $a, b \in A$.

On suppose que ab est inversible et que b n'est pas un diviseur de zéro.

Montrer que a et b sont inversibles.

Exercice 3.

Dans un anneau A, une *racine carrée* de $a \in A$ est un élément $r \in A$ tel que $r^2 = a$.

1. Montrer que, dans un anneau intègre, un élément possède au plus deux racines carrées.
2. Donner un exemple de situation où un élément d'un anneau possède strictement plus de deux racines carrées.

Exercice 4^{+}.

Soit A un anneau tel que $\forall x, y \in A, xy = \pm yx$. Montrer que A est commutatif.

Exercice 5.

On rappelle qu'un élément $x \in A$ est dit *nilpotent* si $\exists n \in \mathbb{N} : x^n = 0_A$.

Dans toute la suite, A est un anneau et $x, y \in A$.

1. Donner un exemple d'élément (non nul) nilpotent dans un anneau commutatif, et un autre dans un anneau non commutatif.
2. Un anneau est dit *réduit* si 0_A est son seul élément nilpotent.
   Montrer que tout anneau intègre est réduit et donner un exemple d'anneau réduit non intègre.
3. (a) On suppose xy nilpotent. Montrer que yx l'est.
   (b) Trouver un exemple de situation où l'on a, pour un certain $n \in \mathbb{N}$, $(xy)^n = 0_A \neq (yx)^n$.
4. (a) On suppose A commutatif et x, y nilpotents. Montrer que xy et $x + y$ sont nilpotents.
   (b) Donner un exemple de situation où x et y sont nilpotents mais ni xy ni $x + y$ ne le sont.

Exercice 6^{+} (L'arnaque d'Eilenberg-Mazur).

Soit A un anneau.

1. Soit $x \in A$ nilpotent. Donner un sens à l'élément $\sum_{k \in \mathbb{N}} x^k$ et montrer que $1 - x$ est inversible.
2. Soit $x, y \in A$ nilpotents. Montrer $1 - xy \in A^\times \Rightarrow 1 - yx \in A^\times$.
3. Montrer à nouveau le résultat de la question précédente sans supposer x et y nilpotents.

Exercice 7.

Soit A un anneau.

1. Montrer que si l'entier $n \in \mathbb{N}^*$ vérifie $n\,1_A = 0_A$, alors $\forall x \in A, n\,x = 0_A$.
2. En déduire qu'il n'existe pas d'anneau A dont le groupe additif soit isomorphe au groupe $\mathbb{Q}/\mathbb{Z}$ des rationnels quotienté par la relation de congruence modulo 1 (qui est bien un groupe pour l'addition « usuelle »).

Exercice 8^{++}.

Montrer qu'il n'existe pas d'anneau dont le groupe additif soit isomorphe au groupe $(\mathbb{R}/2\pi\mathbb{Z}, +)$.

Morphismes

Exercice 9.

1. Soit A un anneau. Déterminer tous les morphismes d'anneaux $\mathbb{Z} \to A$.
2. Donner un exemple d'anneau tel qu'il n'existe pas de morphisme $A \to \mathbb{Z}$.

Exercice 10.

1. Montrer que tout endomorphisme de l'anneau $\mathbb{Z}$ est l'identité. Même question pour $\mathbb{Q}$.
2. Soit φ un endomorphisme d'anneaux $\mathbb{R} \to \mathbb{R}$.
   (a) Montrer que $\forall x \in \mathbb{Q}, \varphi(x) = x$.
   (b) Montrer que $\varphi[\mathbb{R}_+^*] \subseteq \mathbb{R}_+^*$ et en déduire que φ est une application croissante.
   (c) En déduire que $\varphi = \mathrm{id}_{\mathbb{R}}$.
3. Montrer qu'il y a exactement deux endomorphismes φ de $\mathbb{C}$ tels que $\forall x \in \mathbb{R}, \varphi(x) = x$.

Exercice 11$^+$.

Une fonction $\mathbb{R} \to \mathbb{R}$ est dite *polynomiale à coefficients entiers* s'il existe $d \in \mathbb{N}$ et $a_0, \dots, a_d \in \mathbb{Z}$ tels que l'on ait $f : x \mapsto \sum_{k=0}^{d} a_k \, x^k$.

1. Montrer que l'ensemble $\mathcal{P}$ des fonctions polynomiales à coefficients entiers est un sous-anneau de $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$.
2. Soit A un anneau.
   Montrer que l'ensemble des morphismes d'anneaux $\mathcal{P} \to A$ est en bijection avec A.

Exercice 12$^+$.

Déterminer les anneaux A tels qu'il existe à la fois un morphisme d'anneaux $\mathbb{Q} \to A$ et un morphisme d'anneaux $\mathbb{Z}/2\mathbb{Z} \to A$.

Exemples

Exercice 13.

Pour tout $d \in \mathbb{N}$, on note

$$A_d = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \,\middle|\, x \equiv y \pmod{d} \right\}.$$

Montrer que tout sous-anneau de $\mathbb{Z}^2$ est égal à A_d, pour un certain $d \in \mathbb{N}$.

Exercice 14 (Entiers de Gauss et d'Eisenstein). ☑

1. Soit $A = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ l'ensemble des *entiers de Gauss*.
   (a) Montrer que A est un sous-anneau de $\mathbb{C}$.
   (b) Montrer que $\forall z \in A, |z|^2 \in \mathbb{N}$ et en déduire l'égalité $A^\times = A \cap \mathbb{U}$, puis la description complète de $A^\times$.
   (c) Identifier le corps des fractions $\mathrm{Frac}(A)$, en tant que sous-corps de $\mathbb{C}$.
2. Reprendre toutes les questions avec l'ensemble $\mathbb{Z}[j] = \{a + jb \mid a, b \in \mathbb{Z}\}$ des *entiers d'Eisenstein.*

Exercice 15$^+$.

Soit $A = \left\{ a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Z} \right\}$.

1. Montrer que A est un sous-anneau de $\mathbb{R}$.
2. En montrant au passage qu'un tel endomorphisme doit nécessairement envoyer $\sqrt{2}$ sur $\pm\sqrt{2}$, montrer que l'anneau A n'a que deux endomorphismes : id_A et un endomorphisme non trivial que l'on notera c.
3. Montrer que pour tout $x \in A$, on a $x + c(x) \in \mathbb{Z}$ et $x\,c(x) \in \mathbb{Z}$.
4. En déduire que $A^\times = \{x \in A \mid x\,c(x) = \pm 1\}$.
5. Montrer que $A^\times$ est infini.

Mélange

Exercice 16 (Anneaux connexes).

Dans tout l'exercice, A désigne un anneau commutatif non nul.

- Un élément $p \in A$ est dit *idempotent* si $p^2 = p$.
- L'anneau A est dit *connexe* si, étant donné deux anneaux R et S et un isomorphisme $A \to R \times S$, on a R ou S nul.

1. Montrer que A est connexe si et seulement s'il possède exactement deux idempotents : 0_A et 1_A.
2. En déduire que tout anneau intègre est connexe.
3. Montrer que $C^0(\mathbb{R})$ est connexe mais que $C^0(\mathbb{R}^*)$ ne l'est pas.
4. Soit $r, s \in \mathbb{N}^*$. Montrer que les anneaux produits $\mathbb{Z}^r$ et $\mathbb{Z}^s$ ne sont isomorphes que si $r = s$.

Exercice 17$^+$ (Anneaux booléiens).

Un anneau $(A, +, \cdot)$ est dit *booléien* si $\forall x \in A, x^2 = x$.

1. Pour tout ensemble E, montrer que $(\mathcal{P}(E), \triangle, \cap)$ est un anneau booléien.
2. Quels sont les anneaux booléiens intègres ?
3. Montrer qu'un anneau booléien est commutatif.
4. **Anneaux booléiens finis.** Soit A un anneau booléien fini non nul. Le but de cette question est de construire un ensemble fini E tel que A soit isomorphe à l'anneau $\mathcal{P}(E)$ de la première question.
   (a) Montrer que la relation $\preccurlyeq$ définie sur A par
   $$\forall x, y \in A, x \preccurlyeq y \Leftrightarrow xy = x$$
   est une relation d'ordre.
   (b) Montrer que l'ensemble $\mathcal{M}$ des éléments minimaux de $(A \setminus \{0\}, \preccurlyeq)$ est non vide, et que l'on a $\forall x \in A \setminus \{0\}, \exists m \in \mathcal{M} : m \preccurlyeq x$.
   (c) Montrer $\forall x \in A, \forall m \in \mathcal{M}, mx \in \{m, 0_A\}$.
   (d) Montrer que l'application suivante est un isomorphisme d'anneaux :
   $$\varphi : \begin{cases} A \to & \mathcal{P}(\mathcal{M}) \\ x \mapsto & \{m \in \mathcal{M} \,|\, m \preccurlyeq x\} \end{cases}.$$

5.$^{++}$ Donner un exemple d'anneau booléien qui ne soit isomorphe à aucun $\mathcal{P}(E)$.

Corps

Autocorrection C.

Les anneaux commutatifs suivants (tous munis des lois usuelles) sont-ils des corps ?

(i) L'anneau produit $\mathbb{R}^2$;

(ii) L'anneau $D = \left\{ \frac{k}{10^n} \,\middle|\, k \in \mathbb{Z}, n \in \mathbb{N} \right\}$ des nombres décimaux ;

(iii) L'anneau de matrices $\left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$;

(iv) L'anneau de matrices $\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{C} \right\}$;

(v) L'anneau de matrices $\left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$;

(vi) L'anneau de matrices $\left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{Q} \right\}$.

Exercice 18.

Soit $d \in \mathbb{Z} \backslash \{0, 1\}$ un entier *quadratfrei* (ou *sans facteur carré*, c'est-à-dire que le seul carré parfait divisant d est 1, ou encore que $|d|$ est un produit de nombres premiers tous différents).

On note alors

$$\rho_d = \begin{cases} \sqrt{d} & \text{si } d > 0 \\ i\sqrt{|d|} & \text{si } d < 0 \end{cases} \qquad \text{et} \qquad K_d = \{a + b\rho_d \mid a, b \in \mathbb{Q}\}.$$

1. Montrer que K_d est un sous-corps de $\mathbb{C}$.
2. Montrer que tout élément de K_d s'écrit de manière unique sous la forme $a+b\rho_d$, pour un certain couple $(a, b) \in \mathbb{Q}^2$.
3. Soit $\delta \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei.
   Montrer que l'équation $x^2 = \delta$ possède une solution dans K_d si et seulement si $\delta = d$.
4. Soit $d, \delta \in \mathbb{Z} \backslash \{0, 1\}$ deux entiers quadratfrei différents. Montrer $K_d \neq K_\delta$, et même que les corps K_d et K_δ ne sont pas isomorphes.
5. Montrer que K_d admet deux morphismes $K_d \to \mathbb{C}$, et deux automorphismes, que l'on précisera à chaque fois.

Exercice 19$^+$.

Soit $K = \mathbb{Q}[\sqrt[3]{2}] = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \,\middle|\, a, b, c \in \mathbb{Q} \right\}$.

1. Montrer que K est un sous-corps de $\mathbb{C}$.
2. Montrer qu'il existe exactement trois morphismes de corps $K \to \mathbb{C}$, que l'on précisera.
3. Déduire de ce qui précède que id_K est le seul automorphisme de K.

Exercice 20.

On admet l'existence d'un corps à quatre éléments $\mathbb{F}_4 = \{0, 1, a, b\}$.

1. Montrer que $ab = 1$.
2. Déterminer la caractéristique de $\mathbb{F}_4$.
3. En déduire les tables d'addition et de multiplication de $\mathbb{F}_4$.
4. À quels groupes connus sont isomorphes les groupes additif $(\mathbb{F}_4, +)$ et multiplicatif $(\mathbb{F}_4^\times, \cdot)$?

Exercice 21.

Dans cet exercice, K est $\mathbb{R}$ ou $\mathbb{C}$. On fixe $M \in M_2(K)$ et on note

$$A = K[M] = \{a + bM \mid a, b \in K\}.$$

1. Montrer que $M^2 \in A$ et en déduire que A est un sous-anneau commutatif de $M_2(K)$.
2. Que vaut A si M est scalaire ? De manière générale, montrer $\forall \lambda \in K, K[M] = K[M - \lambda I_2]$.
3. On suppose maintenant M non scalaire.
   (a) Montrer que si M et $N \in M_2(K)$ sont deux matrices semblables, alors les anneaux $K[M]$ et $K[N]$ sont isomorphes.
   (b) Montrer que si M admet une valeur propre double dans K, alors A n'est pas réduit, c'est-à-dire qu'il contient un élément nilpotent non nul.
   (c) Montrer que si M admet une valeur propre dans K, alors A n'est pas intègre.
   (d) Montrer que si $K = \mathbb{R}$ et que $\mathrm{Sp}_{\mathbb{R}}(M) = \varnothing$, alors A est un corps.
   À quel corps connu est-il isomorphe ?

Morphismes

Exercice 22.

Soit K et L deux corps de caractéristiques différentes.

Montrer qu'il n'existe pas de morphismes de corps $K \to L$.

Exercice 23.

Montrer que les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont deux à deux non isomorphes.

Exercice 24$^+$ (Morphisme de Frobenius).

Soit p un nombre premier.

1. Montrer que, pour tout $k \in [\![1, p-1]\!]$, p divise le coefficient binomial $\binom{p}{k}$.
2. Soit K un corps de caractéristique p. Montrer que

$$F : \begin{cases} K \to K \\ x \mapsto x^p \end{cases}$$

   est un morphisme de corps, appelé *morphisme de Frobenius*.

Exercice 25^{++}.

Soit K un corps. Montrer que les groupes $(K, +)$ et $(K^*, \cdot)$ ne sont pas isomorphes.