Université d'Angers – 2023/2024

Théorie des anneaux

CC du 29/01/2024.

Aucun document ou appareil électronique n'est autorisé.
*Vous devez **justifier toutes vos réponses**. La note tiendra compte de la qualité et de la concision de la rédaction.*
Vous pouvez utiliser tous les résultats du cours. Ces résultats doivent être cités correctement.

Exercice 1. *Les questions de cet exercice sont indépendantes les unes des autres.*

(1) Qu'est-ce qu'un anneau intègre ?
On ne demande pas de rappeler la définition d'anneau, mais seulement les conditions que doit vérifier un anneau pour être intègre.

(2) Soient A un anneau et $a \in A$. On suppose qu'il existe $b, c \in A$ tels que $ab = ca = 1$.
Montrer que a est inversible.

(3) Est-ce que l'application trace $\mathrm{tr} : M_2(\mathbb{R}) \to \mathbb{R}$ est un morphisme d'anneaux ?

(4) Est-ce que l'application déterminant $\det : M_2(\mathbb{R}) \to \mathbb{R}$ est un morphisme d'anneaux ?

(5) On considère $C^0([0,1])$ l'anneau des fonctions $f : [0,1] \to \mathbb{R}$ continues.
Est-ce que $I \coloneqq \left\{ f \in C^0([0,1]) \ : \ f(0) = 0 \right\}$ est un idéal de $C^0([0,1])$?

Exercice 2.

On considère $A \coloneqq \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \ : \ a, b \in \mathbb{Z} \right\}$.

(1) Montrer que A est un sous-anneau de $M_2(\mathbb{Z})$.

(2) Est-ce que A est commutatif ?

(3) Déterminer A^*.
On rappelle que A^* dénote l'ensemble des inversibles de A.

(4) Montrer que $J \coloneqq \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \ : \ b \in \mathbb{Z} \right\}$ est un idéal de A.

(5) Montrer que A/J et $\mathbb{Z}$ sont isomorphes.

Exercice 3.

(1)
  a. Montrer que $\forall a, b \in \mathbb{Z},\ a + b\sqrt{2} = 0 \Leftrightarrow a = b = 0$.
  b. En déduire que $\forall a, b, c, d \in \mathbb{Z},\ a + b\sqrt{2} = c + d\sqrt{2} \Leftrightarrow a = c$ et $b = d$.

(2) On considère $A \coloneqq \left\{ a + b\sqrt{2} \ : \ a, b \in \mathbb{Z} \right\}$ et, pour $a, b \in \mathbb{Z}$, on note $N\left(a + b\sqrt{2}\right) \coloneqq a^2 - 2b^2$.
  a. Montrer que A est le plus petit sous-anneau de $\mathbb{R}$ contenant $\sqrt{2}$.
  b. Montrer que $\forall z, z' \in A,\ N(zz') = N(z)N(z')$.
  c. Montrer que $\forall z \in A,\ z \in A^* \Leftrightarrow |N(z)| = 1$.
  d. On définit $W \coloneqq \left\{ z \in A^* \ : \ z > 1 \right\}$.
  Montrer que si $a + b\sqrt{2} \in W$ alors $-1 < a - b\sqrt{2} < 1$.
  e. En déduire que si $a + b\sqrt{2} \in W$ alors $a, b > 0$.
  f. Montrer que W admet un plus petit élément, que l'on note $\omega \coloneqq \min(W)$ dans la suite.
  g. Soit $z \in A^* \cap]0, +\infty[$.
    i. Montrer qu'il existe un entier $n \in \mathbb{Z}$ tel que $\omega^{n-1} < z \leq \omega^n$.
    ii. Montrer que $z = \omega^n$.
  h. Déterminer A^*.
  Commentaire : vous pouvez décrire A^* en termes de ω si vous n'avez pas réussi à déterminer ω.

Solution de l'exercice 1.

(1) Un anneau intègre est un anneau non-trivial, commutatif et sans diviseur de zéro.

(2) Soient $a, b, c \in A$ tels que $ab = ca = 1$.
Alors $b = 1 \cdot b = cab = c \cdot 1 = c$. Ainsi $ab = ba = 1$, et donc a est inversible.

(3) *Méthode 1.* Non puisque $\mathrm{tr}(I_2) = 2 \neq 1$.
Méthode 2. Non, puisque l'application trace n'est pas compatible avec la multiplication :

$$\mathrm{tr}\left(\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\right)\mathrm{tr}\left(\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\right) = 4 \neq 2 = \mathrm{tr}\left(\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\right)$$

(4) Non, puisque l'application déterminant n'est pas compatible avec l'addition :

$$\det\left(\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\right) + \det\left(\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\right) = 2 \neq 4 = \det\left(\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} + \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\right)$$

(5) *Méthode 1.* Montrons d'abord que I est un sous-groupe de $C^0([0,1])$.

- $I \subset C^0([0,1])$.
- $0 \in I$ donc I est non-vide.
- Soient $f, g \in I$ alors $(f-g)(0) = f(0) - g(0) = 0 - 0 = 0$ donc $f - g \in I$.

Soient $f \in I$ et $g \in C^0([0,1])$ alors $(fg)(0) = f(0)g(0) = 0g(0) = 0$. Donc $fg \in I$ et $gf = fg \in I$.
Ainsi I est bien un idéal de $C^0([0,1])$.

Méthode 2.

- $I \subset C^0([0,1])$.
- $0 \in I$ donc I est non-vide.
- Soient $f, g \in I$ et $h \in C^0([0,1])$. Alors $(f+gh)(0) = f(0) + g(0)h(0) = 0$ et donc $f + gh \in I$.

Ainsi I est bien un idéal de $C^0([0,1])$.
Remarque : puisque $C^0([0,1])$ est commutatif, il n'est pas nécessaire de considérer $f + kgh$ où $f, g \in I$ et $k, h \in C^0([0,1])$.

Méthode 3. Considérons $\mathrm{ev}_0 : C^0([0,1]) \to \mathbb{R}$ définie par $\mathrm{ev}_0(f) = f(0)$.
Alors $\mathrm{ev}_0(1) = 1$ et, pour $f, g \in C^0([0,1])$, $\mathrm{ev}_0(f+g) = (f+g)(0) = f(0) + g(0) = \mathrm{ev}_0(f) + \mathrm{ev}_0(g)$ et $\mathrm{ev}_0(fg) = (fg)(0) = f(0)g(0) = \mathrm{ev}_0(f)\,\mathrm{ev}_0(g)$.
Donc ev_0 est un morphisme d'anneaux.
Remarquons que $I = \ker(\mathrm{ev}_0)$, donc I est bien un idéal comme noyau d'un morphisme d'anneaux.

Solution de l'exercice 2.

(1)
- $A \subset M_2(\mathbb{Z})$
- $I_2 \in A$
- Soient $M := \begin{pmatrix}a & b\\0 & a\end{pmatrix}, N := \begin{pmatrix}c & d\\0 & c\end{pmatrix} \in A$ alors

$$M - N = \begin{pmatrix}a-c & b-d\\0 & a-c\end{pmatrix} \in A \quad \text{et} \quad MN = \begin{pmatrix}ac & ad+bc\\0 & ac\end{pmatrix} \in A.$$

Donc A est un sous-anneau de $M_2(\mathbb{Z})$.

(2) Soient $M := \begin{pmatrix}a & b\\0 & a\end{pmatrix}, N := \begin{pmatrix}c & d\\0 & c\end{pmatrix} \in A$. Alors $MN = \begin{pmatrix}ac & ad+bc\\0 & ac\end{pmatrix}$ et $NM = \begin{pmatrix}ac & ad+bc\\0 & ac\end{pmatrix}$.
Donc A est un anneau commutatif.

(3) *Méthode 1* (*en utilisant le déterminant*).
Soit $M := \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in A^*$ alors $\det(M) = a^2 \in \mathbb{Z}^* = \{\pm 1\}$, donc $a = \pm 1$.
Réciproquement, soit $M := \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in A$ avec $a = \pm 1$. Posons $N := \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix} \in A$ alors

$$MN = \begin{pmatrix} a^2 & -ab+ab \\ 0 & a^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

et $NM = MN = I_2$. Donc $M \in A^*$.

Ainsi $A^* = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \ : \ a \in \{-1, 1\},\, b \in \mathbb{Z} \right\}$.

Méthode 2 (*à la main*).
Soit $M := \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in A^*$ alors il existe $N := \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in A$ tel que $MN = I_2$,

$$\text{i.e.} \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ainsi $ac = 1$, d'où $a|1$, et donc $a = \pm 1$.
Réciproquement, soit $M := \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in A$ avec $a = \pm 1$. Posons $N := \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix} \in A$ alors

$$MN = \begin{pmatrix} a^2 & -ab+ab \\ 0 & a^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

et $NM = MN = I_2$. Donc $M \in A^*$.

Ainsi $A^* = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \ : \ a \in \{-1, 1\},\, b \in \mathbb{Z} \right\}$.

(4) *Méthode 1 :*

- $J \subset A$
- $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in J$ donc $J \neq \varnothing$
- Soient $M := \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, N := \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \in J$ alors $M - N = \begin{pmatrix} 0 & b-c \\ 0 & 0 \end{pmatrix} \in J$.
- Soient $M := \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in A$ et $N := \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \in J$ alors $MN = NM = \begin{pmatrix} 0 & ac \\ 0 & 0 \end{pmatrix} \in J$.

Donc J est un idéal de A.

Méthode 2 :

- $J \subset A$
- $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in J$ donc $J \neq \varnothing$
- Soient $M := \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}, N := \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \in J$ et $P := \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in A$.
  Alors $M + PN = \begin{pmatrix} 0 & c+ad \\ 0 & 0 \end{pmatrix}$.

Donc J est un idéal de A.
Remarque : puisque A est commutatif, il n'est pas nécessaire de considérer $M+PNQ$ *où* $M, N \in J$ *et* $P, Q \in A$.

Méthode 3 :
On considère $\varphi : A \to \mathbb{Z}$ définie par $\varphi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) = a$.

- $\varphi(I_2) = 1$
- Soient $M := \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, N := \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in A$ alors

$$\varphi(M+N) = \varphi\left(\begin{pmatrix} a+c & b+d \\ 0 & a+c \end{pmatrix}\right) = a + c = \varphi(M) + \varphi(N)$$

et

$$\varphi(MN) = \varphi\left(\begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix}\right) = ac = \varphi(M)\varphi(N).$$

Donc φ est un morphisme d'anneaux.
On remarque que $\ker(\varphi) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \ : \ a = 0,\ b \in \mathbb{Z} \right\} = J$.
Donc J est un idéal comme noyau d'un morphisme d'anneaux.

(5) On considère $\varphi : A \to \mathbb{Z}$ définie par $\varphi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) = a$.

- $\varphi(I_2) = 1$
- Soient $M := \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, N := \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in A$ alors

$$\varphi(M+N) = \varphi\left(\begin{pmatrix} a+c & b+d \\ 0 & a+c \end{pmatrix}\right) = a + c = \varphi(M) + \varphi(N)$$

et

$$\varphi(MN) = \varphi\left(\begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix}\right) = ac = \varphi(M)\varphi(N).$$

- Soit $a \in \mathbb{Z}$ alors $M := \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in A$ et $\varphi(M) = a$.

Donc φ est un morphisme d'anneaux surjectif.
On remarque que $\ker(\varphi) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \ : \ a = 0,\ b \in \mathbb{Z} \right\} = J$.
Donc, d'après le premier théorème d'isomorphisme, φ induit un isomorphisme $A/J \simeq \mathbb{Z}$.

Solution de l'exercice 3.

(1) a. Soient $a, b \in \mathbb{Z}$ tels que $a + b\sqrt{2} = 0$.
Si $b \neq 0$ alors $\sqrt{2} = -\frac{a}{b} \in \mathbb{Q}$, d'où une contradiction.
Donc $b = 0$ et $a = -b\sqrt{2} = 0$.

Réciproquement, si $a = b = 0$ alors $a + b\sqrt{2} = 0$.

b. Soient $a, b, c, d \in \mathbb{Z}$ alors

$$\begin{aligned} a + b\sqrt{2} = c + d\sqrt{2} &\Leftrightarrow (a-c) + (b-d)\sqrt{2} = 0 \\ &\Leftrightarrow a - c = 0 \text{ et } b - d = 0 \text{ d'après la question précédente} \\ &\Leftrightarrow a = c \text{ et } b = d \end{aligned}$$

(2) a.
- $A \subset \mathbb{R}$
- $1 = 1 + 0\sqrt{2} \in A$
- Soient $x \coloneqq a + b\sqrt{2}$, $y \coloneqq c + d\sqrt{2} \in A$ alors

$$x - y = (a - c) + (b - d)\sqrt{2} \in A$$

et

$$xy = \left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = (ac + 2bd) + (ad + bc)\sqrt{2} \in A.$$

Donc A est un sous-anneau de $\mathbb{R}$ et $\sqrt{2} = 0 + 1\sqrt{2} \in A$.

Soit B un sous-anneau de $\mathbb{R}$ contenant $\sqrt{2}$.
Soit $n \in \mathbb{N}$ alors $n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ fois}} \in B$.
Soit $m \in \mathbb{Z} \setminus \mathbb{N}$ alors $-m \in \mathbb{N}$ et donc $m = -(-m) \in B$.
Soit $z \in A$, alors il existe $a, b \in \mathbb{Z}$ tels que $z = a + b\sqrt{2}$. Puisque $a, b, \sqrt{2} \in B$, on a $z = a + b\sqrt{2} \in B$.
On a donc bien montré que $A \subset B$.

Donc A est le plus petit sous-anneau de $\mathbb{R}$ contenant $\sqrt{2}$.

b. Soient $z, z' \in A$. Alors il existe $a, b, c, d \in \mathbb{Z}$ tels que $z = a + b\sqrt{2}$ et $z' = c + d\sqrt{2}$.
On a alors

$$N(z)N(z') = (a^2 - 2b^2)(c^2 - 2d^2) = a^2c^2 - 2b^2c^2 - 2a^2d^2 + 4b^2d^2$$

et

$$N(zz') = N\left(ac + 2bd + (ad + bc)\sqrt{2}\right) = (ac + 2bd)^2 - 2(ad + bc)^2 = a^2c^2 + 4b^2d^2 - 2a^2d^2 - 2b^2c^2.$$

Donc $N(zz') = N(z)N(z')$.

c. Soit $z \in A^*$ alors il existe $z' \in A$ tel que $zz' = 1$.
D'après la question précédente $N(z)N(z') = N(zz') = N(1) = 1$, donc $N(z)$ divise 1.
Ainsi $N(z) = \pm 1$.

Réciproquemment, soit $z \in A$ tel que $|N(z)| = 1$. Il existe $a, b \in \mathbb{Z}$ tels que $z = a + b\sqrt{2}$.
Premier cas : $N(z) = 1$. Posons $z' = a - b\sqrt{2}$.
Alors $zz' = \left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right) = a^2 - 2b^2 = N(z) = 1$ et $z'z = zz' = 1$.
Donc z est inversible.
Second cas : $N(z) = -1$. Posons $z' = -a + b\sqrt{2}$.
Alors $zz' = -\left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right) = -a^2 + 2b^2 = -N(z) = 1$ et $z'z = zz' = 1$.
Donc z est inversible.

On a bien montré que $\forall z \in A,\ z \in A^* \Leftrightarrow |N(z)| = 1$.

d. Soit $z \in W$. Il existe $a, b \in \mathbb{Z}$ tels que $z = a + b\sqrt{2}$.
Alors $1 = |N(z)| = |a^2 - 2b^2| = \left|a + b\sqrt{2}\right|\left|a - b\sqrt{2}\right| = z\left|a - b\sqrt{2}\right| > \left|a - b\sqrt{2}\right|$ car $z > 1$ et $a - b\sqrt{2} \neq 0$ (sinon $a = b = 0$ et $z = 0$).
Donc $-1 < a - b\sqrt{2} < 1$.

e. Soit $a+b\sqrt{2} \in W$ alors
   - $a+b\sqrt{2} > 1$ par définition de W, et
   - $a-b\sqrt{2} > -1$ d'après la question précédente.

   Donc, en sommant les inégalités, $2a > 0$ et $a > 0$.

   De même,
   - $a+b\sqrt{2} > 1$ par définition de W, et
   - $-a+b\sqrt{2} > -1$ d'après la question précédente.

   Donc $2\sqrt{2}b > 0$ et $b > 0$.

   On a bien montré que si $a+b\sqrt{2} \in W$ alors $a, b > 0$.

f. Posons $\omega \coloneqq 1+\sqrt{2}$ alors $\omega > 1$ et $N(\omega) = 1-2 = -1$ d'où $\omega \in A^*$ d'après la question c.
   Ainsi $\omega \in W$.
   Soit $z \coloneqq a+b\sqrt{2} \in W$ alors, d'après la question précédente, $z = a+b\sqrt{2} \geq 1+\sqrt{2} = \omega$.
   Donc ω est le plus petit élément de W.

g. i. *Premier cas : $z > 1$.*
   Considérons $E \coloneqq \left\{k \in \mathbb{N} \ : \ \omega^k \geq z\right\}$.
   Puisque $\omega > 1$, $\lim\limits_{k\to+\infty} \omega^k = +\infty$ et E est non-vide.
   Donc $n \coloneqq \min(E)$ est bien défini et vérifie $\omega^n \geq z$.
   Puisque $\omega^0 = 1$, on a $n \geq 1$. Ainsi $n-1 \in \mathbb{N} \setminus E$, et donc $\omega^{n-1} < z$.
   On a bien $\omega^{n-1} < z \leq \omega^n$.

   Second cas : $z \leq 1$.
   Considérons $F \coloneqq \left\{k \in \mathbb{N} \ : \ \omega^{-k} < z\right\}$.
   Puisque $\omega > 1$, $\lim\limits_{k\to+\infty} \omega^{-k} = 0$ et F est non-vide.
   Donc $m \coloneqq \min(F)$ est bien défini et vérifie $\omega^{-m} < z$.
   Puisque $\omega^0 = 1$, on a $m \geq 1$. Ainsi $m-1 \in \mathbb{N} \setminus F$, et donc $\omega^{-m+1} \geq z$.
   En posant $n \coloneqq -m+1 \in \mathbb{Z}$, on a bien $\omega^{n-1} < z \leq \omega^n$.

   ii. On considère $n \in \mathbb{Z}$ comme dans la question précédente, i.e. tel que $\omega^{n-1} < z \leq \omega^n$.
   Alors $1 < z\omega^{-n+1} \leq \omega$.
   Puisque $z, \omega \in A^*$, on a $z\omega^{-n+1} \in A^*$ et donc $z\omega^{-n+1} \in W$ puisque $z\omega^{-n+1} > 1$.
   Or $z\omega^{-n+1} \leq \omega$ et ω est le plus petit élément de W, donc $z\omega^{-n+1} = \omega$ d'où $z = \omega^n$.

h. Soit $n \in \mathbb{Z}$ alors $\omega^n \in A^*$ et $-\omega^n \in A^*$ puisque ω est inversible.

   Soit $z \in A^*$.
   Premier cas : si $z > 0$. Alors, d'après la question précédente, il existe $n \in \mathbb{Z}$ tel que $z = \omega^n$.
   Premier cas : si $z < 0$. Alors, d'après la question précédente, il existe $n \in \mathbb{Z}$ tel que $-z = \omega^n$.

   Donc $A^* = \left\{\pm\omega^n \ : \ n \in \mathbb{Z}\right\} = \left\{\pm\left(1+\sqrt{2}\right)^n \ : \ n \in \mathbb{Z}\right\} = \left\{\pm\left(1\pm\sqrt{2}\right)^n \ : \ n \in \mathbb{N}\right\}$.
   Pour la dernière égalité, on a utilisé que $\left(1+\sqrt{2}\right)^{-1} = -1+\sqrt{2}$.