Série 4 (Corrigé)

L'exercice 1 sera discuté pendant le cours du lundi 17 octobre.
L'exercice 3 ($\star$) peut être rendu le jeudi 20 octobre aux assistants jusqu'à 15h.

Exercice 1 - QCM

(a) Déterminer si les énoncés proposés sont vrais ou faux.

- Il existe un anneau $(A, +, \cdot)$ tel que A contient un seul élément.
  ◯ vrai ◯ faux
- Il existe un corps $(K, +, \cdot)$ tel que K contient un seul élément.
  ◯ vrai ◯ faux
- Dans l'anneau des polynômes $A[t]$, les polynômes de degré pair avec le polynôme zéro forment un sous-anneau.
  ◯ vrai ◯ faux
- Dans l'anneau des polynômes $A[t]$, les polynômes de degré impair avec le polynôme zéro forment un sous-anneau.
  ◯ vrai ◯ faux
- Soit $D = \{z \in \mathbb{C} | \, |z| = 1\}$. Alors $(D, \cdot)$ et $(SO(2), \cdot)$ sont isomorphes.
  ◯ vrai ◯ faux
- Pour chaque $z \in \mathbb{C}$ il existe $k \in \mathbb{N}\backslash\{0\}$ tel que $z^k \in \mathbb{R}$.
  ◯ vrai ◯ faux

(b) Déterminer les énoncés corrects.

1. Supposons que $a^2 = a$ pour tous les éléments a d'un anneau A. Lesquelles des assertions suivantes sont correctes ?
   ◯ $a^3 = a$, pour tout a.
   ◯ L'anneau est commutatif.
   ◯ $a^3 = 0$, pour tout a.
2. Combien de solutions a l'équation $z^{-1} = z$ dans $\mathbb{C}$?
   ◯ 0.
   ◯ 1.
   ◯ 2.
   ◯ ∞.
3. Combien de solutions a l'équation $z^{-1} = \bar{z}$ dans $\mathbb{C}$?
   ◯ 0.

◯ 1.
◯ 2.
◯ ∞.

4. Combien de solutions a l'équation $\exp(z) = -1$ dans $\mathbb{C}$?
   ◯ 0.
   ◯ 1.
   ◯ ∞.
5. Combien de solutions a l'équation $\exp(z) = -1 + \mathrm{i}$ dans $\mathbb{C}$?
   ◯ 0.
   ◯ 1.
   ◯ ∞.

Sol.:

(a) Determiner si les énoncés proposés sont vrais ou faux.

- *Il existe un anneau $(A, +, \cdot)$ tel que A contient un seul élément.*
  ● *vrai* ◯ *faux*
- *Il existe un corps $(K, +, \cdot)$ tel que K contient un seul élément.*
  ◯ *vrai* ● *faux*
- *Dans l'anneau des polynômes $A[t]$, les polynômes de degré pair avec le polynôme zéro forment un sous-anneau.*
  ◯ *vrai* ● *faux*
- *Dans l'anneau des polynômes $A[t]$, les polynômes de degré impair avec le polynôme zéro forment un sous-anneau.*
  ◯ *vrai* ● *faux*
- *Soit $D = \{z \in \mathbb{C} || z| = 1\}$. Alors $(D, \cdot)$ et $(SO(2), \cdot)$ sont isomorphes.*
  ● *vrai* ◯ *faux*
- *Pour chaque $z \in \mathbb{C}$, il existe $k \in \mathbb{N}\backslash\{0\}$ tel que $z^k \in \mathbb{R}$.*
  ◯ *vrai* ● *faux*

(b) Determiner les énoncés corrects.

1. *Soit $a^2 = a$ pour tous les éléments a dans un anneau A. Lequelles des assertions suivantes sont correctes ?*
   ● *$a^3 = a$, pour tous a.*
   ● *L'anneau est commutatif.*
   ◯ *$a^3 = 0$, pour tout a.*

2. *Combien de solutions a l'équation $z^{-1} = z$ dans $\mathbb{C}$?*
   ◯ 0.
   ◯ 1.
   ● 2.
   ◯ ∞.

3. *Combien de solutions a l'équation* $z^{-1} = \bar{z}$ *a dans* $\mathbb{C}$ *?*
   ◯ 0.
   ◯ 1.
   ◯ 2.
   ● ∞.

4. *Combien de solutions a l'équation* $\exp(z) = -1$ *dans* $\mathbb{C}$ *?*
   ◯ 0.
   ◯ 1.
   ● ∞.

5. *Combien de solutions a l'équation* $\exp(z) = -1 + \mathrm{i}$ *dans* $\mathbb{C}$ *?*
   ◯ 0.
   ◯ 1.
   ● ∞.

Exercice 2
Montrer que $(M_{n\times n}(K), +, \cdot)$, $n > 1$, est un anneau non-commutatif, où K est un corps, $+$ l'addition matricelle et $\cdot$ la multiplication matricelle.
Remarque : Vous pouvez utiliser le matériel déjà montré dans le polycopié et les exercices. Par exemple, il ne faut pas montrer que $(M_{n\times n}(K), +)$ est un groupe abélien.
Sol.:

— *On a montré que* $(M_{n\times n}(K), +)$ *est un groupe abélien (voir Chapitre* 2 *du cours).*

— *L'associativité de* $\cdot$ *et la distributivité de* $\cdot$ *par rapport à* $+$ *sont données par le Lemme* 1.19 *et (partiellement) démontrées dans l'exercice* 10 *de la série 2.*

— *Il reste à montrer qu'il existe un élément neutre par rapport à la multiplication* $\cdot$*. Ceci est donné par* I_n *; voir l'équation* 1.9 *du cours.*

— *Pour finir, on a vu dans la série 2 qu'en général pour deux matrices* $A, B \in M_{n\times n}(K)$ *on a* $AB \neq BA$*, donc l'anneau n'est pas commutatif.*

Exercice 3 ($\star$)
Montrer que $\Big(\mathbb{R} \cup \{\infty\}, \oplus, \odot\Big)$ n'est pas un anneau, où les opérations $\oplus$ et $\odot$ sont définies par

$$a \oplus b = \min\{a, b\}, \quad a \odot b = a + b, \quad a, b \in \mathbb{R} \cup \{\infty\}.$$

En testant tous les axiomes, déterminer lesquels sont satisfaits et lesquels ne le sont pas.

Sol.: *D'abord on note que les opérations sont définies dans*

$$\oplus : \mathbb{R} \cup \{\infty\} \times \mathbb{R} \cup \{\infty\} \to \mathbb{R} \cup \{\infty\},$$
$$\odot : \mathbb{R} \cup \{\infty\} \times \mathbb{R} \cup \{\infty\} \to \mathbb{R} \cup \{\infty\}.$$

Soit $a, b, c \in \mathbb{R} \cup \{\infty\}$*. Ensuite, on teste tous les axiomes :*

1) $a \oplus b = \min\{a, b\} = \min\{b, a\} = b \oplus a$*, donc la commutativité de* $\oplus$ *est satisfaite.*

2) $(a \oplus b) \oplus c = \min\{\min\{a, b\}, c\} = \min\{a, b, c\} = \min\{a, \min\{b, c\}\} = a \oplus (b \oplus c)$*, donc la associativité de* $\oplus$ *est satisfaite.*

3) L'élément neutre pour $\oplus$ est ∞, parce que $a \oplus \infty = \min\{a, \infty\} = a, \forall a \in \mathbb{R} \cup \{\infty\}$.

4) Soit $a \in \mathbb{R} \cup \{\infty\}$. Si l'existe, l'élément inverse doit satisfaire $a \oplus b = \min\{a, b\} = \infty$. Cette assertion est vrai seulement quand $a = b = \infty$. Donc, en général il n'existe pas l'élément inverse pour $\oplus$.

5) $(a \odot b) \odot c = (a + b) + c = a + (b + c) = a \odot (b \odot c)$, donc la associativité de $\odot$ est satisfaite.

6) L'élément neutre pour $\odot$ est $0 \in \mathbb{R}$.

7) Supposons sans perte de généralité que $a \leq b$. Donc $a + c \leq b + c$. D'où

$$(a \oplus b) \odot c = \min\{a, b\} + c = a + c = \min\{a + c, b + c\} = (a \odot c) \oplus (b \odot c).$$

8) De la même façon que 7), on obtient que $a + \min\{b, c\} = \min\{a + b, a + c\}$.

Exercice 4

Montrer que l'ensemble $A[t]$ avec les opérations $+$ et $\cdot$, définies dans le cours, est un anneau. Montrer de plus que si A est un anneau commutatif, alors $A[t]$ est aussi un anneau commutatif.

Sol.:

Nous allons vérifier que $(A[t], +, \cdot)$ les propriétés d'un anneau.

1. *L'opération $+$ est définie dans $+ : A[t] \times A[t] \to A[t]$, comme sommer deux polynômes revient à additionnant les coefficients des monômes correspondants.*
2. *L'opération $\cdot$ est définie dans $\cdot : A[t] \times A[t] \to A[t]$, comme pour $p(t) = \sum_{i=0}^{m} a_i t^i, q(t) = \sum_{j=0}^{n} b_j t^j \in A[t]$, on a $p(t) \cdot q(t) = \sum_{j=0}^{m+n} \left(\sum_{i=0}^{j} a_i b_{j-i} \right) t^j \in A[t]$.*
3. *$(A[t], +)$ est un groupe abélien :*
   - *L'associativité et la commutativité de $+$ sur $A[t]$ découle de la commutativité et de l'associativité de l'addition sur A.*
   - *L'élément neutre de $(A[t], +)$ est $0t^0$, où 0 est l'élément neutre de $(A, +)$.*
   - *Soit $p(t) = \sum_{i=0}^{n} a_i t^i \in A[t]$. Son inverse $-p(t)$ est $\sum_{i=0}^{n} (-a_i) t^i \in A[t]$, où $-a_i$ est l'inverse de a_i dans $(A, +)$ pour $i = 0, 1, \ldots n$.*
4. *$(A[t], +, \cdot)$ est distributive par rapport au $+$:*
   - *Soient $p(t)$, $q(t)$, $r(t) \in A[t]$ et*

$$p(t) = \sum_{i=0}^{m} a_i t^i, \qquad q(t) = \sum_{j=0}^{n} b_j t^j, \qquad r(t) = \sum_{k=0}^{p} c_k t^k. \tag{1}$$

En notant $N = \max\{m, n, p\}$ *on a*

$$\begin{aligned}
(p(t) + q(t)) \cdot r(t) &= \Big(\sum_{i=0}^{N}(a_i + b_i)t^i\Big) \cdot \Big(\sum_{k=0}^{p} c_k t^k\Big) && \textit{définition de } + \\
&= \sum_{k=0}^{N+p}\Big(\sum_{i=0}^{k}(a_i + b_i)c_{k-i}\Big)t^k && \textit{définition de } \cdot \\
&= \sum_{k=0}^{N+p}\Big(\sum_{i=0}^{k} a_i c_{k-i} + \sum_{i=0}^{k} b_i c_{k-i}\Big)t^k && \textit{distrib. de } (A, +, \cdot) \\
&= \sum_{k=0}^{N+p}\Big(\sum_{i=0}^{k} a_i c_{k-i}\Big)t^k + \sum_{k=0}^{N+p}\Big(\sum_{i=0}^{k} b_i c_{k-i}\Big)t^k && \textit{définition de } + \\
&= p(t) \cdot r(t) + q(t) \cdot r(t). && \textit{définition de } \cdot
\end{aligned}$$

De manière analogue, nous montrons que $p(t)\cdot(q(t)+r(t)) = p(t)\cdot r(t)+q(t)\cdot r(t)$.

5. $(A[t], \cdot)$ *est associative :*
   — *Soient* $p(t)$, $q(t)$, $r(t) \in A[t]$ *comme* (1). *On va utiliser une autre façon d'exprimer un produit de deux polynômes :*

$$\begin{aligned}
p(t) \cdot q(t) &= \Big(\sum_{i=0}^{m}(a_i t^i)\Big) \cdot \Big(\sum_{j=0}^{n}(b_j t^j)\Big) && \textit{définition de } \cdot \\
&= \sum_{i=0}^{m}\sum_{j=0}^{n}(a_i t^i) \cdot (b_j t^j) && \textit{distrib. de } (A[t], +, \cdot) \\
&= \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j t^{i+j}. && \textit{définition de } \cdot
\end{aligned}$$

On note que

$$p(t) \cdot q(t) = \sum_{j=0}^{m+n}\Big(\sum_{i=0}^{j} a_i b_{j-i}\Big)t^j = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j t^{i+j}.$$

Alors, on a

$$\begin{aligned}
(p(t) \cdot q(t)) \cdot r(t) &= \Big(\sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j t^{i+j}\Big) \cdot \Big(\sum_{k=0}^{p} c_k t^k\Big) = \sum_{i=0}^{m}\sum_{j=0}^{n}\sum_{k=0}^{p} a_i b_j c_k t^{i+j+k}, \\
p(t) \cdot (q(t)\dot{r}(t)) &= \Big(\sum_{i=0}^{m} a_i t^i\Big) \cdot \Big(\sum_{j=0}^{n}\sum_{k=0}^{p} b_j c_k t^{j+k}\Big) = \sum_{i=0}^{m}\sum_{j=0}^{n}\sum_{k=0}^{p} a_i b_j c_k t^{i+j+k}.
\end{aligned}$$

6. *Il existe un élément neutre dans* $(A[t], \cdot)$.
   On a

$$p(t) \cdot 1t^0 = \sum_{i=0}^{m}(a_0 0 + a_1 0 + \cdots + a_{i-1} 0 + a_i 1)t^i = \sum_{i=0}^{m} a_i t^i = p(t).$$

De manière similaire nous montrons que $1t^0 \cdot p(t) = p(t)$ *donc* $1t^0$ *est l'élément neutre dans* $(A[t], \cdot)$.

Si $(A,+,\cdot)$ est commutatif alors on a $\sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} b_{k-i}a_i = \sum_{i=0}^{k} b_i a_{k-i}$ donc $p(t)\cdot q(t) = q(t)\cdot p(t)$.

Exercice 5

a) Soient $u = -2+\mathrm{i}$, $v = 2+3\mathrm{i}$ et $w = 7-11\mathrm{i}$. Calculer

$$u+v, \qquad u+\overline{v}+w, \qquad u\cdot v, \qquad v\cdot w\cdot \mathrm{i}, \qquad \frac{w}{v}, \qquad \frac{v}{u}.$$

b) Pour chacun des nombres complexes suivants, déterminer la partie réelle, la partie imaginaire, le module et l'argument :

$$\sqrt{5}+2\mathrm{i}, \qquad (3+3\mathrm{i})^9, \qquad \frac{5-\mathrm{i}}{3+2\mathrm{i}}, \qquad \Big(\frac{-1}{\mathrm{i}}\Big)^{57}.$$

Sol.:

i) On obtient

$$\begin{aligned}
u+v &= (-2+i)+(2+3i) = 0+4i = 4i,\\
u+\overline{v}+w &= (-2+i)+(2-3i)+(7-11i) = -2i+(7-11i) = 7-13i,\\
u\cdot v &= (-2+i)\cdot(2+3i) = -4-6i+2i-3 = -7-4i,\\
v\cdot w\cdot i &= (-2+3i)\cdot(7-11i)\cdot i = (14-22i+21i+33)\cdot i = (47-i)\cdot i\\
&= 1+47\cdot i,\\
\frac{w}{v} &= \frac{7-11i}{2+3i} = \frac{(7-11i)\cdot(2-3i)}{(2+3i)\cdot(2-3i)} = \frac{14-21i-22i-33}{4-6i+6i+9} = \frac{-19-43i}{13},\\
\frac{v}{u} &= \frac{2+3i}{-2+i} = \frac{(2+3i)\cdot(-2-i)}{(-2+i)\cdot(-2-i)} = \frac{-4-2i-6i+3}{4+i-i+1} = \frac{-1-8i}{5},\\
|v| &= \sqrt{v\overline{v}} = \sqrt{(2+3i)\cdot(2-3i)} = \sqrt{4+9} = \sqrt{13}.
\end{aligned}$$

ii) Pour le premier nombre $\sqrt{5}+2i$, on a :

$$\mathrm{Re}(\sqrt{5}+2i) = \sqrt{5}, \quad \mathrm{Im}\,(\sqrt{5}+2i) = 2, \quad |\sqrt{5}+2i| = \sqrt{\sqrt{5}^2+2^2} = 3,$$
$$\arg(\sqrt{5}+2i) = \mathrm{Arctg}(\frac{2\sqrt{5}}{5}) \quad (car\ \ \mathrm{Re}(\sqrt{5}+2i) > 0).$$

Pour le deuxième nombre $(3+3i)^9$, on va utiliser la formule de Moivre. D'abord on calcule

$$|3+3i| = \sqrt{3^2+3^2} = 3\sqrt{2}, \qquad \arg(3+3i) = \frac{\pi}{4}, (car\ \mathrm{Re}(3+3\mathrm{i}) > 0).$$

Donc,

$$\begin{aligned}
(3+3i)^9 &= (3\sqrt{2})^9\Big(\cos\frac{9\pi}{4}+i\sin\frac{9\pi}{4}\Big) = (3\sqrt{2})^9\Big(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\Big)\\
&= (3\sqrt{2})^9\Big(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\Big),
\end{aligned}$$

$$|(3+3i)^9| = (3\sqrt{2})^9, \mathrm{Re}((3+3\mathrm{i})^9) = \mathrm{Im}((3+3\mathrm{i})^9) = (3\sqrt{2})^9\cdot\frac{\sqrt{2}}{2}, \arg((3+3\mathrm{i})^9) = \frac{\pi}{4}.$$

Pour le troisième nombre, on rend le dénominateur réel et on obtient :

$$\frac{5-i}{3+2i} = \frac{(5-i)(3-2i)}{(3+2i)(3-2i)} = \frac{13-13i}{13} = 1-i.$$

On a $|1-i| = \sqrt{2}$, $\mathrm{Re}(1-i) = 1$, $\mathrm{Im}\,(1-i) = -1$, $\arg(1-i) = -\frac{\pi}{4}$.

Enfin, $\frac{-1}{i} = i$ *et* $i^4 = 1$, *donc* $\left(\frac{-1}{i}\right)^{57} = i^{57} = i^{4\cdot 14+1} = (i^4)^{14} \cdot i = 1 \cdot i = i$. *On obtient*

$$\mathrm{Re}(i) = 0, \quad \mathrm{Im}\,(i) = 1, \quad |i| = 1, \quad \arg(i) = \frac{\pi}{2}\,.$$

Exercice 6

On considère le sous-ensemble $H = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} ; a, b \in \mathbb{C} \right\}$ de $M_{2\times 2}(\mathbb{C})$.

i) Montrer que $(H, +, \cdot)$ est un sous-anneau de $(M_{2\times 2}(\mathbb{C}), +, \cdot)$, où $+$ et $\cdot$ sont l'addition et la multiplication usuelle des matrices.

ii) Montrer que tous les éléments de $H \setminus \{0\}$ sont inversibles pour la multiplication. Est-ce que $(H, +, \cdot)$ est un corps ?

iii) (**optionnel**) Construire un isomorphisme entre $(H, +, \cdot)$ et un sous-anneau de $(M_{4\times 4}(\mathbb{R}), +, \cdot)$.

Indice : Pour l'inverse d'un élément non nul de H, on a une formule similaire (mais pas identique) à l'inverse d'une matrice réelle 2×2 inversible.
NB : L'ensemble H muni des opérations $+$ et $\cdot$ s'appelle l'ensemble des quaternions.
Sol.:

i) Pour montrer que H est un sous-anneau, on utilise le Lemme 2.19. Soient $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}, B = \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} \in H$. *On voit facilement que* $A - B \in H$ *aussi. On montre que H est stable pour la multiplication :*

$$AB = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} = \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -\overline{b}c - \overline{a}\overline{d} & -\overline{b}d + \overline{a}\overline{c} \end{pmatrix} = \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -\overline{(ad + b\overline{c})} & \overline{ac - b\overline{d}} \end{pmatrix} \in H.$$

Et pour finir l'élément neutre pour la multiplication I_2 appartient à H aussi. D'ápres Lemme 2.19, $(H, +, \cdot)$ est un sous anneau de $(M_{2\times 2}(\mathbb{C}), +, \cdot)$.

ii) Soit $A \in H \setminus \{0\}$, *donc* $a \neq 0$ *ou* $b \neq 0$. *Supposons* $a \neq 0$. *On cherche B telle que* $AB = I_2$.

$$AB = \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -\overline{b}c - \overline{a}\overline{d} & -\overline{b}d + \overline{a}\overline{c} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

La première ligne donne le système d'équations $ac - b\overline{d} = 1$ *et* $ad + b\overline{c} = 0$. *Ce qui donne*

$$c = (1 + b\overline{d})/a \qquad et \qquad ad + b(1 + \overline{b}d)/\overline{a} = 0,$$

en développant on obtient $d = -b/(|a|^2 + |b|^2)$ *et* $c = \overline{a}/(|a|^2 + |b|^2)$. *Si* $a = 0$ *et* $b \neq 0$ *on trouve les mêmes solutions pour c, d. Ainsi A possède l'inverse*

$$A^{-1} = \frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix} \in H.$$

On a que $(H,+,\cdot)$ est un anneau dont tout élément non nul possède une inverse multiplicative dans H.

Mais, la multiplication dans H n'est pas commutative, comme en général

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}\begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} \neq \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix}\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}.$$

Donc $(H,+,\cdot)$ n'est pas un corps.

Remarque : si on multiplie $ac - b\overline{d} = 1$ par $\overline{a}$ et $ad + b\overline{c} = 0$ par $\overline{b}$ on peut trouver c et d sans effectuer divisions par a ni b, il n'est donc pas necessaire que $a \neq 0$ ou $b \neq 0$ mais il suffit que $|a|^2 + |b|^2 \neq 0$.

iii) D'abord on note que un nombre complex $a = a_1 + ia_2$ peut être representé par

$$a_1 + ia_2 \longmapsto \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix}.$$

On définit l'application $f : H \to M_{4\times 4}(\mathbb{R})$

$$f\Big(\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}\Big) = \begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ -a_2 & a_1 & -b_2 & b_1 \\ -b_1 & b_2 & a_1 & -a_2 \\ -b_2 & -b_1 & a_2 & a_1 \end{pmatrix},$$

où $a = a_1 + ia_2$ et $b = b_1 + ib_2$. Donc, on considère le sous-ensemble S de matrices $M_{4\times 4}(\mathbb{R})$ définie par $S = \left\{B \in M_{4\times 4}(\mathbb{R}) \middle| B = \begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ -a_2 & a_1 & -b_2 & b_1 \\ -b_1 & b_2 & a_1 & -a_2 \\ -b_2 & -b_1 & a_2 & a_1 \end{pmatrix}\right\}$. Il faut vérifier que S est un sous-anneau de H. On utilise le Lemme 2.19 :

- *l'élément neutre pour $\cdot$ dans $M_{4\times 4}(\mathbb{R})$ est la matrice identité I_4. Si on prend $a_2 = b_1 = b_2 = 0$, on obtient que $I_4 \in S$.*
- *Soitent $B = \begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ -a_2 & a_1 & -b_2 & b_1 \\ -b_1 & b_2 & a_1 & -a_2 \\ -b_2 & -b_1 & a_2 & a_1 \end{pmatrix}, C = \begin{pmatrix} c_1 & c_2 & d_1 & d_2 \\ -c_2 & c_1 & -d_2 & d_1 \\ -d_1 & d_2 & c_1 & -c_2 \\ -d_2 & -d_1 & c_2 & c_1 \end{pmatrix} \in S$. On voit facilement que $B - C \in S$ aussi. De plus, en multipliant B et C, on vérifie que $B \cdot C \in S$.*

  Donc, S est un sous-anneau de $(M_{4\times 4}(\mathbb{R}),+,\cdot)$.

L'application $f : H \to S$ est bijective :

- *$(\forall B \in S)$ $(\exists A \in H)$ t.q. $f(A) = B$;*
- *si $f(A_1) = f(A_2)$ pour $A_1, A_2 \in H$, donc $A_1 = A_2$.*

Maintenant, il faut montrer que f est un morphisme d'anneaux. Soient $a = a_1 + ia_2, b = b_1 + ib_2, c = c_1 + ic_2$ et $d = d_1 + id_2$. Donc,

$$f\Big(\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} + \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix}\Big) = f\Big(\begin{pmatrix} a+c & b+d \\ -\overline{b+d} & \overline{a+c} \end{pmatrix}\Big)$$
$$= \begin{pmatrix} a_1+c_1 & a_2+c_2 & b_1+d_1 & b_2+d_2 \\ -(a_2+c_2) & a_1+c_1 & -(b_2+d_2) & b_1+d_1 \\ -(b_1+d_1) & (b_2+d_2) & a_1+c_1 & -(a_2+c_2) \\ -(b_2+d_2) & -(b_1+d_1) & a_2+c_2 & a_1+c_1 \end{pmatrix}$$
$$= f\Big(\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}\Big) + f\Big(\begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix}\Big).$$

D'une manière similaire on montre que

$$f\Big(\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix}\Big) = f\Big(\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}\Big) \cdot f\Big(\begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix}\Big).$$

Enfin, on voit que $f(I_2) = I_4$, donc f est un isomorphisme entre H et S.

Exercice 7

Soit $G = \{a, b, c, x, y, z\}$ et $\circ : G \times G \to G$ une loi de composition donnée par la table de Cayley (incomplète)

$\circ$	a	b	c	x	y	z
a					c	b
b		x	z			
c		y				
x				x		
y						
z		a			x	

Par exemple, si y est dans la ligne c et la colonne b, cela signifie que $c \circ b = y$. Tous les éléments de G apparaissent au plus une fois dans chaque ligne et dans chaque colonne (la règle du Sudoku).

Compléter la table afin que $(G\,, \circ)$ soit un groupe, c-à-d vérifier

- la stabilité de G,
- l'associativité de $\circ$,
- l'existence de l'élément neutre,
- l'inversibilité.

Remarque : Vous pouvez compléter la table de sorte à ce que les 4 points ci-dessus soient vérifiés. Vous n'avez alors pas besoin à la fin de vérifier si, par exemple, l'associativité est satisfaite pour toutes les paires d'éléments de G.

Sol.: *Tout d'abord, on essaye d'identifier l'élément neutre e du groupe qui satisfait $u \circ e = u$ ou $e \circ u = u$ pour tout $u \in G$. Donc, si on trouve l'entrée $u \circ w = u$ en ligne u, alors w doit être l'élément neutre, parce que si w n'est pas l'élément neutre, il y a une contradiction avec la règle du Sudoku. De manière analogue, on peut aussi procéder pour les colonnes.*

On trouve l'entrée $x \circ x = x$ dans le tableau, donc $e = x$ doit être l'élément neutre. Maintenant, on utilise la définition de l'élément neutre ($u \circ e = u$ ou $e \circ u = u$) et on peut remplir la ligne x et la colonne x :

$\circ$	a	b	c	x	y	z
a				a	c	b
b		x	z	b		
c		y		c		
x	a	b	c	x	y	z
y				y		
z		a		z	x	

Maintenant, on utilise la définition de l'inverse élément v de u : $u \circ v = e = v \circ u$. On trouve l'entrée $z \circ y = x$, de sorte que on peut ajouter $y \circ z = x$.

Pour procéder, on doit utiliser associativité : $(u \circ v) \circ w = u \circ (v \circ w)$. Afin de créer une entrée en utilisant l'associativité, on a besoin d'utiliser trois entrées déjà existantes dans le tableau. Trouver de telles combinaisons est un peu fastidieux, mais il y a par exemple les combinaisons suivantes :

$$
\begin{aligned}
a \circ b &= \underbrace{(z \circ b)}_{a} \circ b = z \circ \underbrace{(b \circ b)}_{x} = z, \\
x &= \underbrace{(a \circ z)}_{b} \circ b = a \circ \underbrace{(z \circ b)}_{a} = a \circ a, \\
y \circ b &= \underbrace{(c \circ b)}_{y} \circ b = c \circ \underbrace{(b \circ b)}_{x} = c, \\
z \circ c &= \underbrace{(a \circ b)}_{z} \circ c = a \circ \underbrace{(b \circ c)}_{z} = b.
\end{aligned}
$$

Ensuite

$\circ$	a	b	c	x	y	z
a	x	z		a	c	b
b		x	z	b		
c		y		c		
x	a	b	c	x	y	z
y		c		y		
z		a	b	z	x	

Maintenant, on peut créer rapidement des entrées avec la Sudoku règle :

$$
\begin{aligned}
a \circ x &= a \\
c \circ c &= x \\
y \circ c &= a \\
c \circ y &= b \\
c \circ z &= a \\
y \circ y &= z \\
b \circ y &= a \\
y \circ a &= b
\end{aligned}
$$

et on obtient

$\circ$	a	b	c	x	y	z
a	x	z	y	a	c	b
b		x	z	b	a	
c	z	y	x	c	b	a
x	a	b	c	x	y	z
y	b	c	a	y	z	x
z		a	b	z	x	

Maintenant, il y a encore quatre domaines où soit x ou y doivent être disponibles. Ici, on utilise à nouveau l'associativité et reconnaît

$$y = \underbrace{(b \circ b)}_{x} \circ y = b \circ \underbrace{(b \circ y)}_{a} = b \circ a.$$

Maintenant, on utilise la Sudoku règle trois fois et ensuite obtient le tableau complet

$\circ$	a	b	c	x	y	z
a	x	z	y	a	c	b
b	y	x	z	b	a	c
c	z	y	x	c	b	a
x	a	b	c	x	y	z
y	b	c	a	y	z	x
z	c	a	b	z	x	y

Est-ce un groupe maintenant ? Comme nous l'avons appliqué des règles obligatoires à chaque étape, nous pouvons supposer cela. Si cette fin est pas un groupe, alors il n'y a pas d'achèvement de la table du tout parce que la table doit contenir une contradiction avec les règles du groupe au début.