Corrigé série 14

Exercice 1 (10 points)

a) On calcule

$$\begin{aligned}
\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \cdot \left[\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} + \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix} \right] &= \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \begin{pmatrix} y_{11}+z_{11} & y_{12}+z_{12} \\ y_{21}+z_{21} & y_{22}+z_{22} \end{pmatrix} \\
&= \begin{pmatrix} x_{11}y_{11}+x_{11}z_{11}+x_{12}y_{21}+x_{12}z_{21} & x_{11}y_{12}+x_{11}z_{12}+x_{12}y_{22}+x_{12}z_{22} \\ x_{21}y_{11}+x_{21}z_{11}+x_{22}y_{21}+x_{22}z_{21} & x_{21}y_{12}+x_{21}z_{12}+x_{22}y_{22}+x_{22}z_{22} \end{pmatrix} \\
&= \begin{pmatrix} x_{11}y_{11}+x_{12}y_{21} & x_{11}y_{12}+x_{12}y_{22} \\ x_{21}y_{11}+x_{22}y_{21} & x_{21}y_{12}+x_{22}y_{22} \end{pmatrix} + \begin{pmatrix} x_{11}z_{11}+x_{12}z_{21} & x_{11}z_{12}+x_{12}z_{22} \\ x_{21}z_{11}+x_{22}z_{21} & x_{21}z_{12}+x_{22}z_{22} \end{pmatrix} \\
&= \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \cdot \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} + \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \cdot \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix}
\end{aligned}$$

b) Il est facile de montrer que les matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ne commutent pas.

c) La matrice $\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$ est un diviseur de zéro, comme

$$\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Comme un corps n'a aucun diviseur de zéro, $M_2(\mathbb{R})$ n'est pas un corps.

d) Le sous-anneau B est un corps comme chaque élément non-nul a un inverse dans B :

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

e) On peut identifier B et $\mathbb{C}$ comme suit : pour tout $a, b \in \mathbb{R}$, on identifie

$$a + bi \longleftrightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Avec cette identification, il est clair que l'addition est préservée. Pour voir que la multiplication est préservée, on calcule $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$ et

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & bc+ad \\ -(bc+ad) & ac-bd \end{pmatrix}.$$

Par la dernière partie, les inverses sont aussi préservés.

f) L'ensemble des matrices de la forme $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ est fermé sous l'addition (c'est clair) et la multiplication :

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix}.$$

Cet ensemble n'est pas un corps, comme il contient des diviseurs de zéro :

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Exercice 2 (5 points)

Par les définitions de la somme et de la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ et en utilisant le fait que la distributivité est vérifiée dans $\mathbb{Z}$, on a pour tout $[a],[b],[c] \in \mathbb{Z}/n\mathbb{Z}$,

$$[a]([b]+[c]) = [a][b+c] = [a(b+c)] = [ab+ac] = [ab]+[ac],$$

Exercice 3 (5 points)

Les éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$ sont $[1],[5],[7],[11]$.
Les diviseurs de zéro sont $[2],[3],[4],[6],[8],[9]$ et $[10]$.

Exercice 4 (10 points)

a) $[7]\cdot[7] = [14]$.

b) $[7]+[7] = [14]$ et $[20]+[20] = [5]$.

c) L'inverse additif (appelé “opposé") de $[-1]$ est $[1]$. L'inverse multiplicatif de $[-1]$ est $[-1]$.

d) L'inverse additif de $[18]$ est $[17]$. L'inverse multiplicatif de $[18]$ est $[2]$.

e) L'inverse additif de $[14]$ est $[21]$. $[14]$ n'a pas d'inverse multiplicatif.

f) L'inverse additif de $[5]$ est $[30]$. $[5]$ n'a pas d'inverse multiplicatif.

g) L'inverse additif de $[17]$ est $[18]$. L'inverse multiplicatif de $[17]$ est $[33]$.

h) L'inverse additif de $[4]$ est $[31]$. L'inverse multiplicatif de $[4]$ est $[9]$.

Exercice 5 (10 points)

a) Comme l'addition de $\mathbb{Z}/2\mathbb{Z}$ est commutative et associative, il est clair que l'addition dans l'anneau $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ comme défini est aussi commutative et associative.

b) On calcule
$$([a],[b]) \cdot ([c],[d]) = ([ad+bc+ac],[ac+bd])$$
et
$$([c],[d]) \cdot ([a],[b]) = ([cb+da+ca],[ca+db]).$$
Les deux expressions sont égales, donc la multiplication est commutative.

De même, on calcule
$$\begin{aligned}
(\,([a],[b]) \cdot ([c],[d])\,) \cdot ([e],[f]) &= ([ad+bc+ac],[ac+bd]) \cdot ([e],[f]) \\
&= ([(ad+bc+ac)f+(ac+bd)e+(ad+bc+ac)e],[(ad+bc+ac)e+(ac+bd)f]) \\
&= ([adf+bcf+acf+2ace+bde+ade+bce],[ade+bce+ace+acf+bdf])
\end{aligned}$$
et
$$\begin{aligned}
([a],[b]) \cdot (\,([c],[d]) \cdot ([e],[f])\,) &= ([a],[b]) \cdot ([cf+de+ce],[ce+df]) \\
&= ([a(ce+df)+b(cf+de+ce)+a(cf+de+ce)],[a(cf+de+ce)+b(ce+df)]) \\
&= ([2ace+adf+bcf+bde+bce+acf+ade],[acf+ade+ace+bce+bdf])
\end{aligned}$$
Les deux expressions sont égales, donc la multiplication est associative.

On vérifie encore la distributivité :
$$\begin{aligned}
([a],[b]) \cdot (\,([c],[d]) + \cdot([e],[f])\,) &= ([a],[b]) \cdot ([c+e],[d+f]) \\
&= ([a(d+f)+b(c+e)+a(c+e)],[a(c+e)+b(d+f)]) \\
&= ([ad+af+bc+be+ac+ae)],[ac+ae+bd+bf])
\end{aligned}$$
et
$$\begin{aligned}
([a],[b]) \cdot ([c],[d]) + ([a],[b]) \cdot ([e],[f]) &= ([ad+bc+ac],[ac+bd]) + ([af+be+ae],[ae+bf]) \\
&= ([ad+bc+ac+af+be+ae)],[ac+bd+ae+bf])
\end{aligned}$$
Les deux expressions sont égales : la multiplication est distributive relativement à l'addition.

L'élément neutre 0 pour l'addition est $([0],[0])$.

L'élément neutre 1 pour la multiplication est $([0],[1])$.

c) Soient $a := ([1],[0])$ et $b := ([1],[1])$. Alors, la table de multiplication est

$*$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

d) Cet anneau est un corps, puisque chaque élément a un inverse multiplicatif.

Exercice 6 (5 points)
Soit $K := \{r + si \mid r, s \in \mathbb{Q}\}$. Pour $r, r', s, s' \in \mathbb{Q}$, on a que

$$(r + si)(r' + s'i) = (rr' - ss') + (rs' + sr')i \in K,$$

comme $\mathbb{Q}$ est un corps.
Il est facile de voir que K est un anneau commutatif, en utilisant le fait que $\mathbb{Q}$ est un corps. Il reste à montrer que tout $0 \neq r + si \in K$ a un inverse multiplicatif. On peut vérifier facilement que l'inverse est

$$(r + si)^{-1} = \frac{r}{r^2 + s^2} - \frac{s}{r^2 + s^2} i.$$

Exercice 7 (5 points)

a) **Faux.** Par exemple, $1 + 1 = 2$ est pair.

b) **Vrai.** Soit

$$(\mathbb{Z}/2\mathbb{Z})^n := \underbrace{\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}}_{n \text{ fois}}$$

l'anneau muni de la multiplication et de l'addition suivantes :

$$([a_1], \ldots, [a_n]) \cdot ([b_1], \ldots, [b_n]) := ([a_1 b_1], \ldots, [a_n b_n])$$

et

$$([a_1], \ldots, [a_n]) + ([b_1], \ldots, [b_n]) := ([a_1 + b_1], \ldots, [a_n + b_n]).$$

Alors, il n'est pas difficile de voir que $(\mathbb{Z}/2\mathbb{Z})^n$ contient 2^n éléments et que, pour tout $n \geq 1$, l'élément neutre $\mathbf{1} := ([1], \ldots, [1])$ de la multiplication est le seul élément inversible.

c) **Vrai.** $[a - b] = [a + (-b)] = [a] + [-b] = [a] - [b]$.

d) **Faux.** Il existe un corps à quatre éléments. Soit ω un élément de $\mathbb{C}$ qui satisfait $\omega^2 + \omega + 1 = 0$. Considère l'espace vectoriel K sur $\mathbb{Z}/2\mathbb{Z}$ avec base de $\{1, \omega\}$. (Notons que $1 + \omega = \omega^2$ dans cet espace vectoriel.) Alors, avec la multiplication ci-dessous, K est un corps :

*	0	1	ω	ω^2
0	0	0	0	0
1	0	1	ω	ω^2
ω	0	ω	ω^2	1
ω^2	0	ω^2	1	ω

Remarque. En fait, cette construction est différente de la construction donnée dans l'exercice 5, mais les corps sont *isomorphes*. C'est-à-dire, les corps ont les mêmes tables d'addition et de multiplication (à permutation près).

Exercice 8 (5 points)

Comme $\mathbb{R}$ est un anneau commutatif, beaucoup des propriétés d'un anneau sont trivialement vérifiées par A. Notons que la fonction

$$\mathbf{1}(x) = 1 \quad \forall x \in [0, 1]$$

est l'unité de A. La fonction

$$\mathbf{0}(x) = 0 \quad \forall x \in [0, 1]$$

est l'élément de zéro de A. Aussi, si $f \in A$, alors $-f \in A$ aussi.

On vérifie que A est fermé sous l'addition et la multiplication. Soient $f, g \in A$. Alors,

$$(f+g)(0) = f(0) + g(0) = f(1) + g(1) = (f+g)(1)$$

et

$$(f \cdot g)(0) = f(0)g(0) = f(1)g(1) = (f \cdot g)(1).$$

Exercice 9 (10 points)

a) La caractéristique de $\mathbb{Q}$ et de $\mathbb{R}$ sont nulles. La caractéristique de $\mathbb{F}_7$ est 7.

b) Si p est premier, la caractéristique de $\mathbb{F}_p$ est p.

c) Soit $n > 0$ la caractéristique de K. Supposons que n n'est pas premier. On peut donc considérer $1 < d < n$ un diviseur non-trivial de n. Alors,

$$0 = \underbrace{1 + \cdots + 1}_{n \text{ fois}} = \underbrace{\left(\underbrace{1 + \cdots + 1}_{d \text{ fois}}\right) + \cdots + \left(\underbrace{1 + \cdots + 1}_{d \text{ fois}}\right)}_{\frac{n}{d} \text{ fois}} = a\left(\underbrace{1 + \cdots + 1}_{\frac{n}{d} \text{ fois}}\right),$$

où $a = \underbrace{1 + \cdots + 1}_{d \text{ fois}}$.

Mais cela est une contradiction, comme K n'a pas de diviseurs de zéro, et $d < n$ et $\dfrac{n}{d} < n$. Donc, n est premier.

d) Si K est un corps de caractéristique nulle, les éléments

$$1, 1+1, 1+1+1, 1+1+1+1, \ldots$$

sont distincts. (Sinon, il existerait $n > m > 0$ tels que

$$0 = \left(\underbrace{1 + \cdots + 1}_{n \text{ fois}}\right) - \left(\underbrace{1 + \cdots + 1}_{m \text{ fois}}\right) = \underbrace{1 + \cdots + 1}_{n-m \text{ fois}},$$

ce qui est une contradiction.) Donc, K est infini.

Exercice 10 (5 points)

Si $A = (A, +_A, \cdot_A)$ et $B = (B, +_B, \cdot_B)$ sont deux anneaux, on peut munir l'ensemble $A \times B$ d'une structure d'anneau $(A \times B, +, \cdot)$ comme suit :
Pour tout $a \in A$, $b \in B$, on définit

$$(a, b) \cdot (a', b') := (a \cdot_A a', b \cdot_B b')$$

et

$$(a,b)+(a',b') := (a +_A a', b +_B b').$$

L'élément zéro est $(0_A, 0_B)$, où 0_A et 0_B sont les éléments zéro de A et B, respectivement. L'identité de $A \times B$ est $(1_A, 1_B)$, où 1_A et 0_B sont les identités de A et B, respectivement. Il est facile de vérifier que $A \times B$ est un anneau.

Exercice 11 (10 points)

a) Soient $z, z' \in Z(A)$. Alors, pour tout $a \in A$,

$$(z+z')a = za + z'a = az + az' = a(z+z')$$

et

$$(zz')a = z(z'a) = z(az') = (za)z' = (az)z' = a(zz').$$

De plus, $1 \in Z(A)$, et si $z \in Z(A)$, on a aussi que $-z \in Z(A)$. Cela montre que $Z(A)$ est un sous-anneau de A.

b) Comme $A := \mathbb{Z}/n\mathbb{Z}$ est commutatif, il est clair que $Z(A) = A$.

c) On montre que

$$Z(M_2(\mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R} \right\}.$$

Supposons que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(M_2(\mathbb{R}))$.

Alors, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, donc $\begin{pmatrix} b & a \\ d & c \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$, ce qui implique que $a = d$ et $b = c$. De plus,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ donc } \begin{pmatrix} -b & a \\ -d & c \end{pmatrix} = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix},$$

ce qui implique que $-b = c$. Donc, $b = c = 0$. Cela montre que $Z(M_2(\mathbb{R})) \subseteq B$, où

$$B := \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R} \right\}.$$

Mais, il est clair que chaque $b \in B$ commute avec chaque matrice de $M_2(\mathbb{R})$, comme chaque $b \in B$ est un multiple réel de l'identité. Donc, $Z(M_2(\mathbb{R})) = B$.