Université Constantine 2
Faculté des NTIC
Tronc commun «MI»
Algèbre I
Année 2015–2016

Solution de la quatrième série d'exercices

Structures Algébrique

Exercice 1

1. Montrons que $\circ$ est associative, c'est à dire $\forall f, g, h \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : (f \circ g) \circ h = f \circ (g \circ h)$.
   Soit $f, g, h \in \mathcal{F}(\mathbb{R}, \mathbb{R})$. On a

$$\begin{aligned} \forall x \in \mathbb{R} : ((f \circ g) \circ h)(x) &= (f \circ g)(h(x)) \\ &= f(g(h(x)) \\ (f \circ (g \circ h))(x) &= f((g \circ h)(x)) \\ &= f(g(h(x)) \end{aligned}$$

   Donc la composition d'application est associative.
2. Soit $f, g, h \in \mathcal{F}(\mathbb{R}, \mathbb{R})$.

$$\begin{aligned} \forall x \in \mathbb{R} : (f \circ (g + h))(x) &= f((g + h)(x)) \\ &= f(g(x) + h(x)) \\ ((f \circ g) + (g \circ h))(x) &= (f \circ g)(x) + (f \circ g)(x) \\ &= f(g(x)) + f(h(x)) \end{aligned}$$

   En général, $f(g(x) + h(x)) \neq f(g(x)) + f(h(x))$, donc la composition d'application n'est pas distributive par rapport à l'addition.
3. Soit $f, g, h \in \mathcal{F}(\mathbb{R}, \mathbb{R})$.

$$\begin{aligned} \forall x \in \mathbb{R} : (f.(g + h))(x) &= f(x)(g + h)(x)) \\ &= f(x)(g(x) + h(x)) \\ &= f(x)g(x) + f(x)h(x)) \\ &= (f.g)(x) + (f.h)(x)) \\ &= (f.g + f.h)(x)) \end{aligned}$$

   Donc la multiplication d'applications est distributive par rapport à l'addition.

Exercice 2

1. (a) Soit $x, y, z \in \mathbb{R}$.

$$\begin{aligned}(x \oplus y) \oplus z &= (x + y - 1) \oplus z \\ &= (x + y - 1) + z - 1 \\ &= x + y + z - 2 \\ x \oplus (y \oplus z) &= x \oplus (y + z - 1) \\ &= x + (y + z - 1) - 1 \\ &= x + y + z - 2\end{aligned}$$

On a $(x \oplus y) \oplus z = x \oplus (y \oplus z)$, donc $\oplus$ est associative.

(b) Soit $x, y \in \mathbb{R}$. On a $x \oplus y = x + y - 1 = y + x - 1 = y \oplus x$. Donc $\oplus$ est commutative.

(c) Soit $e \in R$.
e est un élément neutre pour $\oplus \iff \forall x \in \mathbb{R} : x \oplus e = e \oplus x = x$.
Comme $\oplus$ est commutative, il suffit de montrer que $x \oplus e = x$.

$$\begin{aligned}x \oplus e = x &\iff x + e - 1 = x \\ &\iff e = 1\end{aligned}$$

Donc $e = 1$ est un élément neutre pour $\oplus$.

2. (a) Soit $x, y, z \in \mathbb{R}$.

$$\begin{aligned}(x \otimes y) \otimes z &= (x + y - xy) \otimes z \\ &= (x + y - xy) + z - (x + y - xy)z \\ &= x + y - xy + z - xz - yz + xyz \\ &= x + y + z - xy - xz - yz + xyz \\ x \otimes (y \otimes z) &= x \otimes (y + z - yz) \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x + y + z - yz - xy - xz + xyz \\ &= x + y + z - xy - xz - yz + xyz\end{aligned}$$

On a $(x \otimes y) \otimes z = x \otimes (y \otimes z)$, donc $\otimes$ est associative.

(b) Soit $x, y \in \mathbb{R}$. On a $x \otimes y = x + y - xy = y + x - yx = y \otimes x$.
Donc $\otimes$ est commutative.

(c) Soit $e' \in R$.
e' est un élément neutre pour $\otimes \iff \forall x \in \mathbb{R} : x \otimes e' = e' \otimes x = x$.
Comme $\otimes$ est commutative, il suffit de montrer que $x \otimes e' = x$.

$$\begin{aligned} x \otimes e' = x &\iff x + e' - xe' = x \\ &\iff e'(1-x) = 0 \\ &\iff e' = 0 \end{aligned}$$

Donc $e' = 0$ est un élément neutre pour $\otimes$.

3. $(\mathbb{R}, \oplus)$ est un groupe commutatif $\iff$ $\oplus$ est commutative, associative, admet un élément neutre, et tous les éléments de $\mathbb{R}$ sont symétrisables.
Il reste donc à montrer que tous les éléments de $\mathbb{R}$ sont symétrisables. Soit $x \in \mathbb{R}$.
x est symétrisable $\iff \exists x' \in \mathbb{R} : x \oplus x' = x' \oplus x = 1$
Comme $\oplus$ est commutative il suffit d'étudier $x \oplus x' = 1$.

$$\begin{aligned} x \oplus x' = 1 &\iff x + x' - 1 = 1 \\ &\iff x + x' = 0 \\ &\iff x' = -x \end{aligned}$$

Donc tous les éléments de $\mathbb{R}$ sont symétrisables pour $\oplus$. Donc $(\mathbb{R}, \oplus)$ est un groupe commutatif.

4. $(\mathbb{R}, \otimes)$ est un groupe commutatif $\iff$ $\otimes$ est commutative, associative, admet un élément neutre, et tous les éléments de $\mathbb{R}$ sont symétrisables.
Il reste donc à voir si tous les éléments de $\mathbb{R}$ sont symétrisables. Soit $x \in \mathbb{R}$. x est symétrisable $\iff \exists x' \in \mathbb{R} : x \otimes x' = x' \otimes x = 0$
Comme $\otimes$ est commutative il suffit d'étudier $x \oplus x' = 1$.

$$\begin{aligned} x \otimes x' = 0 &\iff x + x' - xx' = 0 \\ &\iff x'(1-x) = -x \\ &\iff x' = -x/(1-x) \quad \text{si } x \neq 1 \end{aligned}$$

Donc 1 n'est pas symétrisable pour $\otimes$. Donc $(\mathbb{R}, \otimes)$ n'est pas un groupe.

5. Soit $x, y, z \in \mathbb{R}$. Comme $\otimes$ est commutative, il suffit d'étudier

$$\begin{aligned} x \otimes (y \oplus z) &= x \otimes (y + z - 1) \\ &= x + (y + z - 1) - x(y + z - 1) \\ &= x + y + z - 1 - xy - xz + x \\ &= 2x + y + z - xy - xz - 1 \\ (x \otimes y) \oplus (x \otimes z) &= (x + y - xy) \oplus (x + z - xz) \\ &= (x + y - xy) + (x + z - xz) - 1 \\ &= 2x + y + z - xy - xz - 1 \end{aligned}$$

$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$, donc $\otimes$ est distributive par rapport à $\oplus$.

Exercice 3

1. Pour montrer que f est un endomorphisme de $(\mathbb{R}^*, \times)$, on montre que $\forall x, y \in \mathbb{R}^*$: $f(xy) = f(x)f(y)$.
   Soit $x, y \in \mathbb{R}^*$.
   $$f(xy) = (xy)^n = x^n y^n = f(x)f(y)$$
   Donc f est un endomorphisme de $(\mathbb{R}^*, \times)$.
2. $\operatorname{Im} f = \{y \in \mathbb{R}^* / \exists x \in \mathbb{R}^* : y = f(x)\}$.
   On distingue deux cas :
   — Si n est pair : l'équation $y = x^n$ n'a pas de solution si $y < 0$, et elle a deux solutions si $y > 0$. Donc $\operatorname{Im} f = \mathbb{R}_+^*$.
   — Si n est impair : l'équation $y = x^n$ admet une solution quelque soit y. Donc $\operatorname{Im} f = \mathbb{R}^*$.
   $\ker f = \{x \in \mathbb{R}^* / f(x) = 1\}$.
   On distingue deux cas :
   — Si n est pair : l'équation $x^n = 1$ a deux solutions $x = 1$ et $x = -1$. Donc $\ker f = \{-1, 1\}$.
   — Si n est impair : l'équation $x^n = 1$ admet une seule solution $x = 1$. Donc $\ker f = \{1\}$.

Exercice 4

1. Pour montrer que A est un sous anneau de Q, on montre que : A n'est pas vide, $\forall x, y \in A : x - y \in A$, et $\forall x, y \in A : xy \in A$.
   — On a $0 = \frac{0}{2} \in A$. Donc $A \neq \emptyset$.
   — Soit $x, y \in A$. Alors il existe $m, m' \in \mathbb{Z}$ et $n, n' \in \mathbb{N}$ tels que $x = \frac{m}{2^n}$ et $y = \frac{m'}{2^{n'}}$. On a alors : $x - y = \frac{m}{2^n} - \frac{m'}{2^{n'}} = \frac{m2^{n'} - m'2^n}{2^{n+n'}}$, avec $m2^{n'} - m'2^n \in \mathbb{Z}$ et $n + n' \in \mathbb{N}$. Donc $x - y \in A$.
   — Soit $x, y \in A$. Alors il existe $m, m' \in \mathbb{Z}$ et $n, n' \in \mathbb{N}$ tels que $x = \frac{m}{2^n}$ et $y = \frac{m'}{2^{n'}}$. On a alors : $xy = \frac{m}{2^n} \times \frac{m'}{2^{n'}} = \frac{mm'}{2^{n+n'}}$. Donc $xy \in A$.
   Donc A est un sous anneau de Q.
2. Soit $x = \frac{m}{2^n} \in A$. Pour que $x^{-1} = \frac{2^n}{m}$ appartienne à A, il faut et il suffit que $m = \pm 2^k$ avec $k \in \mathbb{N}$.