WRITTEN ASSIGNMENT 2

McGill university

nicholas hayek

CONTENTS

QUESTION 1

By axiom:

1. $(a + b\varepsilon) + (c + d\varepsilon) = (a + c) + (b + d)\varepsilon$

   $(c + d\varepsilon) + (a + b\varepsilon) = (c + a) + (d + b)\varepsilon$

   $= (a + c) + (b + d)\varepsilon$ since $\mathbb{R}$ commutative

   $\implies x + y = y + x \; \forall x, y \in R$

2.
$$\begin{aligned}(x + y) + z &= [(a + b\varepsilon) + (c + d\varepsilon)] + (e + f\varepsilon) \\ &= [(a + c) + (b + d)\varepsilon] + (e + f\varepsilon) \\ &= (a + c) + e + [(b + d) + f]\varepsilon \\ &= a + (c + e) + [b + (d + f)]\varepsilon \\ &= (a + b\varepsilon) + [(c + d\varepsilon) + (e + f\varepsilon)] \quad = x + (y + z)\end{aligned}$$

3. Let $\mathbb{0}$, our zero element, be $\mathbb{0} := (0 + 0\varepsilon)$. Then, for $x = (a + b\varepsilon) \in R$, we have

   $x + \mathbb{0} = (0 + 0\varepsilon) + (a + b\varepsilon) = (a + 0) + (0 + b)\varepsilon = a + b\varepsilon$

4. Let the additive inverse of x, $-x$, be defined as $-x = -a - b\varepsilon$. Then, for $x \in R$, we have $x + (-x) = a - a + (b - b)\varepsilon = 0 + 0\varepsilon = \mathbb{0}$

5. Consider $x(yz)$.

$$\begin{aligned}x(yz) &= (a + b\varepsilon)[(c + d\varepsilon)(e + f\varepsilon)] \\ &= (a + b\varepsilon)[ce + (cf + de)\varepsilon] \\ &= ace + [a(cf + de) + bce]\varepsilon \\ &\implies ace + (acf + ade + bce)\varepsilon\end{aligned}$$

$$\begin{aligned}(xy)z &= [(a + b\varepsilon)(c + d\varepsilon)](e + f\varepsilon \\ &= [ac + (ad + bc)\varepsilon](e + f\varepsilon) \\ &= ace + [acf + e(ad + bc)]\varepsilon \\ &\implies ace + (acf + ead + ebc)\varepsilon\end{aligned}$$

   Using distributive property of the reals.

6. Let $\mathbb{1} := 1 + 0\varepsilon$. Then, for $x \in R$, we have

   $\mathbb{1} \cdot x = (1 + 0\varepsilon)(a + b\varepsilon) = a(1) + [a(0) + b(1)]\varepsilon = a + b\varepsilon = x$

   and

   $x \cdot \mathbb{1} = (a + b\varepsilon)(1 + 0\varepsilon) = a(1) + [b(1) + a(0)]\varepsilon = a + b\varepsilon = x$

7. Consider $x(y+z)$ for $x, y, z \in R$.

$$\begin{aligned}
x(y+z) &= (a+b\varepsilon)[(c+d\varepsilon)+(e+f\varepsilon)] \\
&= (a+b\varepsilon)[(c+e)+(d+f)\varepsilon] \\
&= a(c+e)+[a(d+f)+b(c+e)]\varepsilon \\
&= ac+ae+[(ad+bc)+(af+be)]\varepsilon \\
&= ac+(ad+bc)\varepsilon+ae+(af+be)\varepsilon \\
&= (a+b\varepsilon)(c+d\varepsilon)+(a+b\varepsilon)(e+f\varepsilon) \qquad = xy+xz \\
(y+z)x &= [(c+e\varepsilon)+(e+f\varepsilon)](a+b\varepsilon) \\
&= [(c+e)+(d+f)\varepsilon](a+b\varepsilon) \\
&= (c+e)a+[(c+e)b+(d+f)a]\varepsilon \\
&= ca+ea+[(cb+da)+(eb+fa)]\varepsilon \\
&= [ca+(cb+da)\varepsilon]+[ea+(eb+fa)\varepsilon] \\
&= (c+d\varepsilon)(a+b\varepsilon)+(e+f\varepsilon)(a+b\varepsilon) \qquad = yx+zx
\end{aligned}$$

Consider an inverse x^{-1} such that $x \cdot x^{-1} = \mathbb{1}$, where $x = (a+b\varepsilon)$, $x^{-1} = (X+Y\varepsilon)$, and $\mathbb{1} = (1+0\varepsilon)$ as above. Then we need $(a+b\varepsilon)(X+Y\varepsilon) = (1+0\varepsilon)$.

$\implies aX + (aY+bX)\varepsilon = 1 + 0\varepsilon$

$\implies aX = 1 \implies X = \frac{1}{a}$. Thus, we need $aY + \frac{b}{a} = 0 \implies Y = \frac{-b}{a^2}$.

$X + Y\varepsilon = x^{-1}$ only exists, then, if $a \neq 0$ (or else we will be dividing by 0).

We can conclude, since $q \in R := r\varepsilon$ is non-zero, for which we've shown there's no inverse, that R is not a field.

QUESTION 2

Let $a \oplus b = a + b - 1$ and $a \otimes b = ab - a - b - 2$. Once again, we'll show all 7 axioms:

1. $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$

2.
$$\begin{aligned} a \oplus (b \oplus c) &= a \oplus (b + c - 1) \\ &= a + b + c - 2 = (a + b - 1) + (c - 1) \\ &= (a \oplus b) + c - 1 \\ &= (a \oplus b) \oplus c \end{aligned}$$

3. Let $\mathbb{0} = 1$. Then $a \oplus \mathbb{0} = a + 1 - 1 = \boxed{a} = 1 + a - 1 = \mathbb{0} \oplus a$

4. Let $-a := 2 + (-1)a$. Then $a \oplus -a = a + 2 - a - 1 = 1 = \mathbb{0}$ from above

5.
$$\begin{aligned} a \otimes (b \otimes c) &= a \otimes (bc - b - c + 2) \\ &= a(bc - b - c + 2) - a - (bc - b - c + 2) + 2 \\ &= abc - ab - ac + 2a - a - bc + b + c - 2 + 2 \\ &= abc - ab - ac - bc + a + b + c \quad \star \\ (a \otimes b) \otimes c &= (ab - a - b + 2) \otimes c \\ &= (ab - a - b + 2)c - (ab - a - b + 2) - c + 2 \\ &= abc - ac - bc + 2c - ab + a + b - 2 - c + 2 \\ &= abc - ab - ac - bc + a + b + c \quad \star \end{aligned}$$

6. Let $\mathbb{1} = 2$. Then, for any $a \in R$, we have

   $a \otimes \mathbb{1} = a(2) - a - 2 + 2 = a$

   Additionally, $\mathbb{1} \otimes a = 2a - 2 - a + 2 = a$, as desired

7. Lastly, for any $a, b, c \in R$

$$\begin{aligned} a \otimes (b \oplus c) &= a(b \oplus c) - a - (b \oplus c) + 2 \\ &= a(b + c - 1) - a - (b + c - 1) + 2 \\ &= ab + ac - a - a - b - c + 1 + 2 \\ &= (ab - a - b + 2) + (ac - a - c + 2) - 1 \\ &= (a \otimes b) \oplus (a \otimes c) \end{aligned}$$

$$\begin{aligned} (b \oplus c) \otimes a &= (b \oplus c)a - (b \oplus c) - a + 2 \\ &= (b + c - 1)a - (b + c - 1) - a + 2 \\ &= ba + ca - a - b - c + 1 - a + 2 \\ &= (ba - b - a + 2) + (ca - c - a + 2) - 1 \\ &= (b \otimes a) \oplus (c \otimes a) \end{aligned}$$

Thus, R is a ring. To show that R is also a field, we need to find b such that $a \otimes b = \mathbb{1} = 2$ as above:

$\implies ab - a - b + 2 = 2$

$\implies b(a-1) = a$

$\implies b = \frac{a}{a-1}$

Note that our inverse does not exist for $a = 1$. However, from (3), $\mathbb{0} = 1$, and so our inverse *does* exist for all non-zero elements of R.

Lastly, we need to show that $a \otimes b = b \otimes a$:

$$a \otimes b = ab - a - b + 2 = ba - b - a + 2 = b \otimes a$$

$\implies \mathbb{R}$ under $\otimes$ and $\oplus$ is a field

QUESTION 4

Lemma: if $a \in R$, $a \cdot \mathbb{0} = \mathbb{0}$.

Since $a + \mathbb{0} = \mathbb{0}$, we have $\mathbb{0} = \mathbb{0} + \mathbb{0}$

$\implies a \cdot \mathbb{0} = a \cdot \mathbb{0} + a \cdot \mathbb{0}$

$\implies \mathbb{0} = a \cdot \mathbb{0}$ 👍

From here, let $\mathbb{1} = \mathbb{0}$. Then we have

$$a = a \cdot \mathbb{1} = a \cdot \mathbb{0} = \mathbb{0} \quad \forall a \in R \implies R = \{\mathbb{0}\}$$

$\square$

Question 5

Let R be a ring with exactly two elements. Per set theory (and the previous question), $a \neq b$. However, we require R to have both a $\mathbb{0}$ and $\mathbb{1}$ element, and so WLOG assume $a = \mathbb{0}$, $b = \mathbb{1}$.

For all non-zero elements of R, i.e. for $\mathbb{1}$, we have

$\mathbb{1} \cdot \mathbb{1} = \mathbb{1}$

Thus all non-zero elements in R have a multiplicative inverse.

$\mathbb{1} \cdot \mathbb{0} = \mathbb{0} = \mathbb{0} \cdot \mathbb{1}$, and so R is commutative under multiplication.

$\implies R$ is a field $\square$

QUESTION 6

Let R have exactly 3 elements. By the same logic used above, $R := \{\mathbb{0}, \mathbb{1}, a\}$, where a is distinct from both $\mathbb{0}$ and $\mathbb{1}$.

There exists 2 non-zero elements of R, $\mathbb{1}$ and a.

For a, we have $a \cdot a =$ "something," which itself is contained in R. It cannot equal $\mathbb{0}$, since that would imply that $a = \mathbb{0}$. It cannot equal a, because that would imply that $a = \mathbb{1}$. Thus, it must equal $\mathbb{1}$, and so a is its own inverse.

As before, $\mathbb{1}$ is its own multiplicative inverse.

$\forall x \in R$, with $x \neq \mathbb{0}$, $\exists y : xy = yx = \mathbb{1}$.

As before, $\mathbb{1}$ and $\mathbb{0}$ act commutativity under multiplication, and further $x \cdot x = x \cdot x \; \forall x \in R$, trivially. Then, we only need to consider:

$$a \cdot 1 = \boxed{a} = \mathbb{1} \cdot a \quad \text{and} \quad a \cdot \mathbb{0} = \boxed{\mathbb{0}} = \mathbb{0} \cdot a$$

$\implies R$ is a field.