1. Let $R$ be a ring, with additive and multiplicative neutral elements $0_R, 1_R$. Prove that $0_R, 1_R$ are unique.

Suppose there were some other additive neutral element $0'_R$. Consider $X = 0_R + 0'_R$. On one hand, $X = 0'_R$ since $0_R$ is neutral. On the other hand, $X = 0_R$ since $0'_R$ is neutral. Hence $0_R = 0'_R$.

Suppose there were some other multiplicative neutral element $1'_R$. Consider $Y = 1_R1'_R$. On one hand, $Y = 1'_R$ since $1_R$ is neutral. On the other hand, $Y = 1_R$ since $1'_R$ is neutral. Hence $1_R = 1'_R$.

2. For prime $p$, set $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}$. Prove that $\mathbb{Z}[\sqrt{p}]$ is a subring of $\mathbb{R}$.

There are four things to check. First, $0_R = 0 + 0\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. Second, let $a + b\sqrt{p}, a' + b'\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. We have $(a + b\sqrt{p}) + (a' + b'\sqrt{p}) = (a + a') + (b + b')\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. Third, let $a + b\sqrt{p}, a' + b'\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. We have $(a + b\sqrt{p})(a' + b'\sqrt{p}) = (aa' + pbb') + (ab' + ba')\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. Fourth, let $a + b\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. Now, $-(a + b\sqrt{p}) = (-a) + (-b)\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$.

3. For prime $p$, set $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$. Prove that $\mathbb{Q}[\sqrt{p}]$ is a subfield of $\mathbb{R}$.

There are five things to check, four of which are very similar to problem #2. First, $0_R = 0 + 0\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Second, let $a + b\sqrt{p}, a' + b'\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. We have $(a + b\sqrt{p}) + (a' + b'\sqrt{p}) = (a + a') + (b + b')\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Third, let $a + b\sqrt{p}, a' + b'\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. We have $(a + b\sqrt{p})(a' + b'\sqrt{p}) = (aa' + pbb') + (ab' + ba')\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Fourth, let $a + b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Now, $-(a + b\sqrt{p}) = (-a) + (-b)\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$.

Fifth, let $a + b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$ be nonzero. We calculate $\frac{1}{a + b\sqrt{p}} = \frac{a-b\sqrt{p}}{a^2-pb^2} = \frac{a-b\sqrt{p}}{a}\frac{a-b\sqrt{p}}{a-pb} = (\frac{a}{a^2-pb^2}) + (\frac{-b}{a^2-pb^2})\sqrt{p}$. Now, to show the result is in $\mathbb{Q}[\sqrt{p}]$, we need to prove that $a^2 - pb^2 \neq 0$. Fortunately this was done on the first exam, provided $a, b$ are both nonzero. If just one is zero, that contradicts $a^2 - pb^2 = 0$; if both are zero, that contradicts $a + b\sqrt{p}$ being nonzero.

4. For $k \in \mathbb{Z}$, define object $R_k$, which has ground set $Z$, and operations $\oplus, \odot$ defined as:

$$a \oplus b = a + b, \quad a \odot b = k$$

Determine for which $k$, if any, $R_k$ is a ring.

First consider $k \neq 0$ and suppose $R_k$ were a ring. Then for any $a, b, c$ we have $k = a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) = k \oplus k = k + k = 2k$. Hence $k = 2k$, so $0 = k$, a contradiction. Thus $R_k$ is not a ring for $k \neq 0$.

If $k = 0$ we will prove that $R_k$ is a ring.

1: $a + b, 0$ are each in $Z$, so $\oplus, \odot$ are closed.

2: $a \oplus (b \oplus c) = a \oplus (b + c) = a + (b + c) = (a + b) + c = (a + b) \odot c \oplus a \odot b \odot c$, so $\odot$ is associative.

3: $a \odot b = a + b = b + a = b \odot a$, so $\odot$ is commutative.

4: $0 \odot a = 0 + a = a + 0 = a \odot 0$, so $0_{R_k} = 0$ is neutral under $\odot$.

5: Let $a \in Z$. Then $a \odot (-a) = a + (-a) = 0$, so inverses exist under $\odot$.

6: $a \odot (b \odot c) = a \odot 0 = 0 \circ c = (a \odot b) \circ c$, so $\odot$ is associative.

8: $a \odot b = b \odot a$, so $\odot$ is commutative. This is optional, but makes 7 easier.

7: $a \odot (b \odot c) = a \odot (b + c) = 0 \circ 0 = 0 \circ (a \odot b) + (a \odot c) = (a \odot b) \odot (a \odot c)$. This proves the distributive property from the left; the distributive property from the right follows by 8, i.e. commutativity of $\odot$.

5. Prove or disprove: If $R, S$ are fields, then $R \times S$ is an integral domain.

We saw a counterexample in HW3. $Z_2$ and $Z_3$ are both fields, since 2, 5 are prime (and, by Thm 2.8, all nonzero elements of these rings are units). But $Z_2 \times Z_3$ has zero divisors, e.g. $(\{1\}, \{0\}) \odot (\{0\}, \{1\}) = (\{0\}, \{0\}) = 0_R$.

6. Define $R$, an object with ground set $Z$, and operations $\oplus, \odot$ defined as:

$$a \oplus b = a + b - 1, \quad a \odot b = a + b - ab$$

Prove that $R$ is an integral domain.

1. $a + b - 1, a + b - ab$ are both integers, so $\oplus, \odot$ are closed.

2. $a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + (b + c - 1) - 1 = (a + b - 1) + c - 1 = (a \odot b) + c - 1 = (a \oplus b) \odot c$, so $\odot$
is associative.
3. \( a \oplus b = a + b - 1 = b + a - 1 = b \oplus a \), so \( \oplus \) is commutative.
4. \( a \oplus 1 = a + 1 - 1 = a = 1 + a - 1 = 1 \oplus a \), so \( 0_R = 1 \) is neutral under \( \oplus \).
5. Let \( a \in Z \). Then \( a \oplus (2 - a) = a + (2 - a) - 1 = 0_R \), so inverses exist under \( \oplus \).
6. \( a \oplus (b \oplus c) = a \oplus ((b - c) - 2) = a - (b + c - 2) + 2 = (a + b + c - 2) + 2 = (a + b + c) + a - b + c = (a + b) \oplus c = (a \oplus b) \oplus c \), so \( \oplus \) is associative.
7. \( a \oplus (b \oplus c) = a \oplus b \oplus c = a \oplus (b + c) = (a + b - c) - 2 = (a + b + c - 2) \oplus 2 = a \oplus b + a - c + 2 = a - b + a - 2 = b \oplus a \), so \( \oplus \) is commutative.
8. \( a \oplus (b \oplus c) = a \oplus b \oplus c = a \oplus (b + c) = a + b + c = (a + b) \oplus c = (a \oplus b) \oplus c \), so \( \oplus \) is associative.

Define \( R \), an object with ground set \( Z \), and operations \( \oplus, \odot \) defined as:

\[
\begin{align*}
\alpha \oplus b &= a + b - 1, \\
\alpha \odot b &= ab - a - b + 2
\end{align*}
\]

Prove that \( R \) is an integral domain.

1. \( a + b - 1, ab - (a + b) + 2 \) are both integers, so \( \oplus, \odot \) are closed.
2. \( \odot (b \ominus c) = a \odot (b - c - 2) = a - (b + c - 2) + 2 = (a + b + c) + a - b + c = (a + b) \odot c = (a \odot b) \odot c \), so \( \odot \) is associative.
3. \( \alpha \odot 0 = a = 0, a - 2 = 0 \cdot a, \) so \( 0_R = 0 \) is neutral under \( \odot \).
4. \( \alpha \odot (x + y) = x \odot y = \infty \odot a \), so \( 0_R = \infty \) is neutral under \( \oplus \).
5. Inverses under \( \oplus \) do not exist. As proof, consider the counterexample of 7. There is no additive inverse to 7, because there is no \( x \in R \) with 7 = -x. In fact, only \( \infty \) has an additive inverse.
6. \( a \odot (b \ominus c) = a \odot (b - c - 2) = a - (b + c - 2) + 2 = (a + b + c) + a - b + c = (a + b) \odot c = (a \odot b) \odot c \), so \( \odot \) is associative.
7. \( a \odot (b \ominus c) = a \odot (b - c - 2) = a - (b + c - 2) + 2 = (a + b + c) + a - b + c = (a + b) \odot c = (a \odot b) \odot c \), so \( \odot \) is associative.

Define \( R \), an object with ground set \( Z \setminus \{+\infty\} \), and operations \( \oplus, \odot \) defined as:

\[
\begin{align*}
\alpha \oplus b &= \min(a, b), \\
\alpha \odot b &= a + b
\end{align*}
\]

Prove that \( R \) satisfies every field axiom except one, and prove that \( R \) fails to satisfy that one.

1. \( \min(a, b) \), \( a + b \) are both integers, so \( \oplus, \odot \) are closed.
2. \( \alpha \odot (b \ominus c) = a \odot (b - c) = \min(a, b - c) = (a, b, c) = \min(a, b) \odot c = (a \odot b) \odot c \), so \( \odot \) is associative.
3. \( \alpha \odot b = \min(a, b) = b \oplus a \), so \( \oplus \) is commutative.
4. \( \alpha \oplus \infty = \min(a, \infty) = a = \infty \oplus a \), so \( 0_R = \infty \) is neutral under \( \oplus \).
5. Inverses under \( \oplus \) do not exist. As proof, consider the counterexample of 7. There is no additive inverse to 7, because there is no \( x \in R \) with 7 = -x. In fact, only \( \infty \) has an additive inverse.
6. \( a \odot (b \ominus c) = a \odot (b - c - 2) = a - (b + c - 2) + 2 = (a + b + c) + a - b + c = (a + b) \odot c = (a \odot b) \odot c \), so \( \odot \) is associative.
7. \( a \odot (b \ominus c) = a \odot (b - c - 2) = a - (b + c - 2) + 2 = (a + b + c) + a - b + c = (a + b) \odot c = (a \odot b) \odot c \), so \( \odot \) is associative.

This proves the distributive property from the left; the distributive property from the right follows by 8, i.e. commutativity of \( \odot \).
9. \( a \odot 0 = a + 0 - a = 0 + a = 0 \odot a \), so \( 0_R = 0 \) is neutral under \( \odot \).
10. \( 0_R = \infty \neq 1 = 1_R \). Suppose now that \( a \odot b = 0_R = 1 \). Then \( a + b - ab = 1 \), which rearranges to \( ab - a - b + 1 = 0 \) or \( (a - 1)(b - 1) = 0 \). Hence either \( a = 1 = 0_R \) or \( b = 1 = 0_R \). Thus \( R \) has no zero divisors.
11. Let \( a \in R \) satisfy \( a \neq 0_R \), i.e. \( a \neq \infty \). We have \( a \odot (-a) = a + (-a) = 0 = 1_R \). Hence every nonzero element of \( R \) is a unit.