Problem 1 Prompt: Let R be the set of positive real numbers and define addition, denoted by $\oplus$, and multiplication, denoted by $\otimes$, as follows. For every $a, b \in R$, $a \oplus b = ab$, and $a \otimes b = a^{\log b}$. Please prove or disprove $(R, \oplus, \otimes)$ is a field.

Problem 1 Response: In proving/disproving that the set R is a field, we define a set of properties and definitions that are used in the following set of proofs.

Logrithmic Properties

$$a = c^{\log_c a} \ \forall a \in \mathbb{R}, \ c \in R \setminus \{1_\mathbb{R}\}. \tag{1}$$

$$\log : R \to \mathbb{R}. \tag{2}$$

$$a = c^{\log_c a}, \ \forall c \in R \setminus \{1_\mathbb{R}\}, \ a \in R \tag{3}$$

$$\log a^{\log b} = \log a \log b \tag{4}$$

$$\log_d d = 1_\mathbb{R} \forall d \in \{R \setminus 1_\mathbb{R}\} \tag{5}$$

$$a = b \Rightarrow \log a = \log b \tag{6}$$

$$\log_a b = \frac{\log_c b}{\log_c a} \ \forall c \in \{a \mid a \in R, \ a > 1\} \tag{7}$$

$$\log_c a + \log_c b = \log_c ab \ \ \forall a, b \in R, \ c \in \{d \mid d \in R, \ d > 1\} \tag{8}$$

Exponential Properties

$$a^x \in R \ \forall a \in R, \ x \in \mathbb{R} \tag{9}$$

$$\left(a^b\right)^c = a^{bc} \tag{10}$$

$$a = b \Rightarrow c^a = c^b \ \forall a, b, c \ \in \mathbb{R}. \tag{11}$$

$$a^b a^c = a^{b+c} \ \forall a, b, c \in \mathbb{R} \tag{12}$$

Definitions for R

The set of all real numbers, denoted $\mathbb{R}$ is a field with additive identity $0_\mathbb{R}$ and multiplicative identity $1_\mathbb{R}$. (13)

The product of two positive real numbers is also positive (14)

$$R \subset \mathbb{R} \tag{15}$$

$$a, b \in R \Rightarrow a \oplus b = ab \tag{16}$$

$$a, b \in R \Rightarrow a \otimes b = a^{\log b} \tag{17}$$

$$1_\mathbb{R} > 0_\mathbb{R} \tag{18}$$

$$\frac{a}{b} \in \mathbb{R} \ \forall a, b \in \mathbb{R} \tag{19}$$

Claim 1: The set R is a field.

Proof 1: Thet set R is a field if R satisfies the following: The set R is closed under addition, denoted $\oplus$, associative under addition, commutative under addition, contains an additive identity, denoted 0_R, contains an additive inverse $\forall a \in R$, is closed under multiplication, denoted $\otimes$, is commutative under multiplication, is associative under multiplication, contains a multiplicative identity, denoted 1_R, contains a multiplicative inverse for each non-zero element in R, and is distributive. The following sub-claims and sub-proofs verify each of these conditions.

1. **Claim 1-1:** R must be closed under addition such that $a, b \in R \Rightarrow a \oplus b \in R$

    Proof 1-1: Recall that $a \in R, b \in R \Rightarrow a \in \mathbb{R}, b \in \mathbb{R}$, per assumption (15). The set $\mathbb{R}$ is also a field (13), so $a, b \in \mathbb{R} \Rightarrow ab \in \mathbb{R}$ as $\mathbb{R}$ must necessarily be closed under multiplication. Recall also that R is the set of positive real numbers, and that the product of two positive numbers in $\mathbb{R}$ is also positive (14). Therefore, $a, b \in R \Rightarrow ab \in \mathbb{R}$ and $ab > 0$, which implies that $ab \in R$. Hence, $a, b \ \in R \Rightarrow a \oplus b \in R$.

    $$(15) \Rightarrow a, b \in R \Rightarrow a, b \in \mathbb{R} \quad \text{Statement 1}$$
    $$\text{Statement 1 and } (13) \Rightarrow a, b \in R \Rightarrow ab \in \mathbb{R} \quad \text{Statement 2}$$
    $$\text{Statement 2 and } (14) \Rightarrow a, b \in R \Rightarrow ab \in R$$

    Logic for Proof 1-1

2. **Claim 1-2:** The elements in R must be associative under addition such that $a, b, c \in R \Rightarrow (a \oplus b) \oplus c = a \oplus (b \oplus c)$

Proof 1-2: The elements of $\mathbb{R}$ are associative under multiplication because $\mathbb{R}$ is a field (13). Additionally, the elements in R are also elements of $\mathbb{R}$ because R is a subset of $\mathbb{R}$ (15), implying that R is associative under multiplication as defined in $\mathbb{R}$. Finally, the operator $\oplus$ from R is equivalent to multiplication in $\mathbb{R}$, therefore because R is associative under multiplication from $\mathbb{R}$, R must also be associative under $\oplus$.

$$(15) \Rightarrow a, b, c \in R \Rightarrow a, b \in \mathbb{R} \qquad \text{Statement 1}$$
$$\text{Statement 1 and } (13) \Rightarrow a, b, c \in R \Rightarrow (ab)c = a(bc) \qquad \text{Statement 2}$$
$$\text{Statement 2 and } (16) \Rightarrow a, b, c \in R \Rightarrow (a \oplus b) \oplus c = a \oplus (b \oplus c)$$

Logic for Proof 1-2

3. **Claim 1-3:** The elements in R must be commutative under addition such that $a, b \in R \Rightarrow a \oplus b = b \oplus a$

Proof 1-3: The elements in $\mathbb{R}$ are commutative under multiplication because $\mathbb{R}$ is a field (13). Additionally, the elements in R are also elements of $\mathbb{R}$ because R is a subset of $\mathbb{R}$ (15), implying that R is commutative under multiplication as defined in $\mathbb{R}$. Finally, the operator $\oplus$ from R is equivalent to multiplication in $\mathbb{R}$, therefore because R is commutative under multiplication from $\mathbb{R}$, R must also be commutative under $\oplus$.

$$(15) \Rightarrow a, b \in R \Rightarrow a, b \in \mathbb{R} \qquad \text{Statement 1}$$
$$\text{Statement 1 and } (13) \Rightarrow a, b \in R \Rightarrow ab = ba \qquad \text{Statement 2}$$
$$\text{Statement 2 and } (16) \Rightarrow a, b \in R \Rightarrow a \oplus b = b \oplus a$$

Logic for Proof 1-3

4. **Claim 1-4:** The set R must contain an additive identity, 0_R, such that $a \in R \Rightarrow a \oplus 0_R = a$.

Proof 1-4: There exists a multiplicative inverse in $\mathbb{R}$ because $\mathbb{R}$ is a field (13). From (18), we also know that the multiplicative identity from $\mathbb{R}$ is greater than zero, and therefore an element of R. Additionally, multiplication from $\mathbb{R}$ has been redefined as $\oplus$ in R (16). Therefore, $1_\mathbb{R}$ is the additive identity in R, implying that there exists an additive identity in R.

$$(13) \Rightarrow \exists 1_\mathbb{R} \in \mathbb{R} \ni 1_\mathbb{R} a = a \ \forall a \in \mathbb{R} \qquad \text{Statement 1}$$
$$\text{Statement 1 and } (15) \Rightarrow 1_\mathbb{R} a = a \ \forall a \in R \qquad \text{Statement 2}$$
$$\text{Statement 2 and } (18) \Rightarrow 1_\mathbb{R} \in R \qquad \text{Statement 3}$$
$$\text{Statement 3 and } (16) \Rightarrow 1_\mathbb{R} \oplus a = a \ \forall a \in R \qquad \text{Statement 4}$$
$$\text{Statement 4 and definition of } 0_R \Rightarrow 1_\mathbb{R} = 0_R \qquad \text{Statement 5}$$
$$\text{Statement 5} \Rightarrow \exists \ 0_\mathbb{R} \in R \ni a \oplus 0_R = a \ \forall a \in R$$

Logic for Proof 1-4

5. **Claim 1-5:** For each element in R, there must also exist an additive inverse in R such that $a \oplus a^{-1} = 0_R$.

Proof 1-5: Each element in $\mathbb{R}$ has a multiplicative inverse in $\mathbb{R}$ because $\mathbb{R}$ is a field (13) but because R is a subset of $\mathbb{R}$, then each element in R has a multiplicative inverse in $\mathbb{R}$. Furthermore, because the product of two real numbers is positive (14) and the multiplicative identity in $\mathbb{R}$ is positive (18), then the multiplicative inverse that corresponds to an element in R must also be positive, making the multiplicative inverse an element of R. We also know that addition in R and multiplication in $\mathbb{R}$ are equivalent (16), making each multiplicative inverse in $\mathbb{R}$ the additive inverse in R. Therefore, for each element in R, there exists an additive inverse in R such that $a \otimes a^{-1} = 0_R$

$$(15) \Rightarrow a \in R \Rightarrow a \in \mathbb{R} \qquad\qquad \text{Statement 1}$$
$$\text{Statement 1 and } (13) \Rightarrow \forall a \in R, \ \exists a^{-1} \in \mathbb{R} \ni aa^{-1} = 1_{\mathbb{R}} \qquad \text{Statement 2}$$
$$\text{Statement 2 and } (14) \Rightarrow \forall a \in R, \ a^{-1} \in \mathbb{R}, \ aa^{-1} = 1_{\mathbb{R}} \Rightarrow a^{-1} > 0 \quad \text{Statement 3}$$
$$\text{Statements 2 and 3} \Rightarrow \forall a \in R, \ \exists a^{-1} \in R, \ni aa^{-1} = 1_{\mathbb{R}} \qquad \text{Statement 4}$$
$$\text{Statement 4, Proof 1-4, and } (16) \Rightarrow \forall a \in R, \ \exists a^{-1} \in R, \ni a \oplus a^{-1} = 0_R$$

Logic for Proof 1-5

6. **Claim 1-6:** The set R must be closed under multiplication such that $a \otimes b \in R \ \forall a, b \in R$.

   Proof 1-6: The log of a positive real number is an element in the set of real numbers (2). When an element from the set of positive real number exponentiates another element from the set of postive real numbers, the result lies within the set of positive real numbers (9). Because the operator $\otimes$ is defined as a binary operator, where the first input exponentiates the log of the second, if both inputs are elements in the set of positive real numbers, then the $\otimes$ operator necessarily maps from the set of positive real numbers to the set of positive real numbers, making R closed under $\otimes$.

$$(2) \Rightarrow \log b \in \mathbb{R} \ \forall b \in R \qquad \text{Statement 1}$$
$$\text{Statement 1 and } (9) \Rightarrow a^{\log b} \in R \ \forall a, b \in R \qquad \text{Statement 2}$$
$$\text{Statement 2 and } (17) \Rightarrow a \otimes b \in R \ \forall a, b \in R$$

Logic for Proof 1-6

7. **Claim 1-7:** The elements in R must be commutative under multiplication such that $a \otimes b = b \otimes a$

   Proof 1-7: In Proof 1-7, we desire to show that $a \otimes b = b \otimes a \ \forall a, b \in R$. The definition of $\otimes$ in (17) can be expanded to show that
   $$a \otimes b = a^{\log_c b}.$$
   Next, because $b = d^{\log_d b}$ (3), we can also say that
   $$a^{\log_c b} = c^{\log_c a^{\log_c b}}.$$
   Additionally, a property of logrithms which states that $\log_c a^b = b \log_c a$ (4), implies that
   $$c^{\log_c a^{\log_c b}} = c^{\log_c a \log_c b}$$
   and also that
   $$c^{\log_c a \log_c b} = c^{\log_c b^{\log_c a}}$$
   which can be reexpressed as
   $$c^{\log_c b^{\log_c a}} = b^{\log_c a}$$
   by exercising (3). Note finally, that by the definition of $\otimes$ from (17),
   $$b^{\log_c a} = b \otimes a.$$
   Therefore, $a \otimes b = b \otimes a \ \forall a, b \in R$ making R commutative under $\otimes$.

$$(17) \Rightarrow a \otimes b = a^{\log_c b} \qquad\qquad \text{Statement 1}$$
$$\text{Statement 1 and } (3) \Rightarrow a \otimes b = c^{\log_c a^{\log_c b}} \qquad \text{Statement 2}$$
$$\text{Statement 2 and } (4) \Rightarrow a \otimes b = c^{\log_c b \log_c a} \qquad \text{Statement 3}$$
$$\text{Statement 3 and } (4) \Rightarrow a \otimes b = c^{\log_c b^{\log_c a}} \qquad \text{Statement 4}$$
$$\text{Statement 4 and } (3) \Rightarrow a \otimes b = b^{\log_c a} \qquad\qquad \text{Statement 5}$$
$$\text{Statements 5 and 1} \Rightarrow a \otimes b = b \otimes a$$

Logic for Proof 1-7

8. **Claim 1-8:** The elements in R must be associative under multiplication

   Proof 1-8: The objective of Proof 1-8 is to show that R is associative under multiplication, or that $a(b \otimes c) = (a \otimes b) \otimes c \ \forall a, b, c \in R$. In Proof 1-8, we begin with a true statement and use equality relationships from properties that have been previously defined to show that R is associative. By observation, we assert that

$$a^{\log_c c \log_c b} = a^{\log_c c \log_c b},$$

   or that $a^{\log_c c \log_c b}$ is equal to itself. A property of logrithms which states that $\log_c a^b = b \log_c a$ is applied to show that

$$a^{\log_c c \log_c b} = a^{\log_c b^{\log_c c}}.$$

   The next step is to apply an exponential property from (10) which states that $(a^b)^c = a^{bc}$ to obtain

$$a^{\log_c c \log_c b} = a^{\log_c b^{\log_c c}}.$$

   Because $a^{\log_c c \log_c b}$ is equal to both $a^{\log_c b^{\log_c c}}$ and $\left(a^{\log_c b}\right)^{\log_c c}$, then $a^{\log_c b^{\log_c c}}$ must be equal to $a^{\log_c b^{\log_c c}}$, yielding

$$a^{\log_c b^{\log_c c}} = \left(a^{\log_c b}\right)^{\log_c c}.$$

   By applying the definition of $\otimes$ from (17), we know that $b^{\log_c c} = b \otimes c$ and $a^{\log_c b} = a \otimes b$, which can be substituted in the previos expression to obtain

$$a^{\log_c b \otimes c} = (a \otimes b)^{\log_c c}.$$

   The definition for $\otimes$ can be applied again to obtain

$$a \otimes (b \otimes c) = (a \otimes b) \otimes c$$

   which proves that the set R is commutative under $\otimes$.

$$
\begin{aligned}
\text{Inspection} &\Rightarrow a^{\log_c c \log_c b} = a^{\log_c c \log_c b} & \text{Statement 1} \\
\text{Statement 1 and (4)} &\Rightarrow a^{\log_c c \log_c b} = a^{\log_c b^{\log_c c}} & \text{Statement 2} \\
\text{Statement 1 and (10)} &\Rightarrow a^{\log_c c \log_c b} = \left(a^{\log_c b}\right)^{\log_c c} & \text{Statement 3} \\
\text{Statements 1, 2, and 3} &\Rightarrow a^{\log_c b^{\log_c c}} = \left(a^{\log_c b}\right)^{\log_c c} & \text{Statement 4} \\
\text{Statement 4 and (17)} &\Rightarrow a^{\log_c(b \otimes c)} = (a \otimes b)^{\log_c c} & \text{Statement 5} \\
\text{Statement 5 and (17)} &\Rightarrow a \otimes (b \otimes c) = (a \otimes b) \otimes c &
\end{aligned}
$$

   Logic for Proof 1-8

9. **Claim 1-9:** The set R must contain a multiplicative identity, 1_R such that $a \otimes 1_R = 1 \forall a \in R$

   Proof 1-9: Proof 1-9 will show taht R contains a multiplicative identity under $\otimes$. From the definition of $\otimes$, we know that

$$a \otimes c = a^{\log_c c}$$

   A property of logrithms also tells us that $\log_c c = 1$, which can be substituted into the previous expression to obtain

$$a^{\log_c c} = a^1.$$

   Finally, upon inspection, $a^1 = a$, indicating that c is the multiplicative identity for R. c is also defined as an element in the set of all real numbers greater than 1, making it an element in R. Therefore there exists an element in R that satisfies the conditions of a multiplicative identity under $\otimes$.

$$
\begin{aligned}
(17) &\Rightarrow a \otimes c = a^{\log_c c} & \text{Statement 1} \\
\text{Statement 1 and (5)} &\Rightarrow a \otimes c = a^1 & \text{Statement 2} \\
\text{Statement 2 with inspection} &\Rightarrow a \otimes c = a &
\end{aligned}
$$

   Logic for Proof 1-9

10. **Claim 1-10:** The set R must contain a multiplicative inverse for each non-zero element such that $\exists a^{-1} \in R \ni aa^{-1} = 1_R \ \forall a \in R \setminus \{0_R\}$.

Proof 1-10: Proof 1-10 will demonstrate that the multiplicative inverse of any non-zero value a is R is $c^{\frac{1}{\log_c a}}$. The definition of $\otimes$ from (17) implies that

$$a \otimes c^{\frac{1}{\log_c a}} = a^{\log_c c^{\frac{1}{\log_c a}}}.$$

Furthermore, two properties of logrithms state that $1 = \log_c c$ (5) and $\frac{\log_c c}{\log_c a} = \log_a c$ (7) and can be applied to the previous statement in showing that

$$a^{\log_c c^{\frac{1}{\log_c a}}} = a^{\log_c c^{\log_a c}}.$$

Another property of logrithms also states that $\log_c c^a = a \log_c c$ (4) which allows us to reexpress the previous statement as

$$a^{\log_c c^{\log_a c}} = a^{\log_a c \log_c c}$$

which can be used in conjunction with (5) to show that

$$a^{\log_c c^{\log_a c}} = a^{\log_a c}.$$

Finally, the property of logrithms which states that $a = c^{\log_c a}$ (5) can be used to express the statement given above as

$$a^{\log_a c} = c$$

and because c is the multiplicative identity in R, we can conclude that $c^{\frac{1}{\log_c a}}$ is the multiplicative inverse of a in R. Next, we must show that $c^{\frac{1}{\log_c a}}$ is an element of R. We know that 1 is an element of R because $1 \in \mathbb{R}$ and $1 > 0$. We also know that $\log_c a \in \mathbb{R}$ because $a \in R$ and $\log : R \to \mathbb{R}$ (2). We also know that $\frac{1}{\log_c a} \in \mathbb{R}$ because $\frac{a}{b} \in \mathbb{R} \ \forall a, b \in \mathbb{R}$ (19). Finally, $\frac{1}{\log_c a} \in \mathbb{R}$ and the exponential property which states that $a^b \in R \ \forall a \in R, b \in \mathbb{R}$ (9) shows that $c^{\frac{1}{\log_a c}} \in R$. Hence, $a \otimes c^{\frac{1}{\log_a c}} = 1_R \ \forall a \in R$ and $c^{\frac{1}{\log_a c} \in R}$, showing that for every element in R, there exists a multiplicative inverse in R such that $aa^{-1} = 1_R$.

$$(17) \Rightarrow a \otimes c^{\frac{1}{\log_c a}} = a^{\log_c c^{\frac{1}{\log_c a}}} \qquad \text{Statement 1}$$

$$\text{Statement 1 and } (5) \Rightarrow a \otimes c^{\frac{1}{\log_c a}} = a^{\log_c c^{\frac{\log_c c}{\log_c a}}} \qquad \text{Statement 2}$$

$$\text{Statement 2 and } (7) \Rightarrow a \otimes c^{\frac{1}{\log_c a}} = a^{\log_c c^{\log_a c}} \qquad \text{Statement 3}$$

$$\text{Statement 3 and } (3) \Rightarrow a \otimes c^{\frac{1}{\log_c a}} = a^{\log_a c} \qquad \text{Statement 4}$$

$$\text{Statement 4 and } (3) \Rightarrow a \otimes c^{\frac{1}{\log_c a}} = c \qquad \text{Statement 5}$$

$$\text{Statement 5 and Proof 1-9} \Rightarrow a \otimes c^{\frac{1}{\log_c a}} = 1_R \qquad \text{Statement 6}$$

$$(19), (2), \text{ and } (9) \Rightarrow c^{\frac{1}{\log_c a}} \in R \qquad \text{Statement 7}$$

$$\text{Statements 6 and 7} \Rightarrow \forall a \in R, \ \exists b \in R \ni a \otimes b = 1_R$$

Logic for Proof 1-10

11. **Claim 1-11:** The set R must be distributive such that $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c \ \forall a, b, c \in R$.

Proof 1-11: Proof 1-11 will demonstrate that $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c \ \forall a, b, c \in R$. Begin by applying the definitions of $\oplus$ and $\otimes$ to $a \otimes b \oplus a \otimes c$

$$a \otimes b \oplus a \otimes c = a^{\log b} a^{\log c}.$$

The expression above can be reexpressed using an exponential property which states $a^b a^c = a^{b+c}$ (12) such that

$$a^{\log b} a^{\log c} = a^{\log b + \log c}.$$

Next, we apply the logrithmic property which states $\log_c a + \log_c b = \log_c ab$ (8) to show that

$$a^{\log b + \log c} = a^{\log bc}.$$

Finally, we apply the definition of $\otimes$ and $\oplus$ to show that

$$a^{\log bc} = a \otimes (b \oplus c)$$

Therefore, because $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c \; \forall a, b, c \in R$, R is distributive.

(17) and (18) $\Rightarrow a \otimes b \oplus a \otimes d = a^{\log b} a^{\log c}$.	Statement 1
Statement 1 and (12) $\Rightarrow a \otimes b \oplus a \otimes d = a^{\log b + \log c}$	Statement 2
Statement 2 and (8) $\Rightarrow a \otimes b \oplus a \otimes d = a^{\log bc}$	Statement 3
Statement 3, (17), and (18) $\Rightarrow a \otimes b \oplus a \otimes d = a \otimes (b \oplus c)$	

Logic for Proof 1-11

Because $(R, \oplus, \otimes)$ contains all behavioral traits of a field, we can conclude that R is a field.

Problem 2 Prompt: Denote the set $\{0, 1, 2, 3\}$ by $\mathbb{Z}_4$, and define addition, denoted $+$, and multiplication, denoted by $\cdot$ or juxtaposition, via the following tables:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Please prove or disprove $(\mathbb{Z}_4, +, \cdot)$ is a field.

Claim 2: The set $\mathbb{Z}_4$ is not a field.

Proof 2: For a set to be a field, every non-zero element must have a multiplicative inverse, or $a \in R \setminus \{0_R\}, \Rightarrow \exists\, a^{-1} \in R \;\ni\; aa^{-1} = 1_R$. In this case, $(\mathbb{Z}_4, +, \cdot)$ is not a field because $2 \in \mathbb{Z}_4$, but does not have an accompanying multiplicative inverse. This can be proven by inspection. The multiplication table implies that 1 is the multiplicative identity for $\mathbb{Z}_4$ however, 1 is not the result of any value multiplied by 2. Hence, 2 does not have a multiplicative inverse, and $(\mathbb{Z}, +, \cdot)$ cannot be a field.

Problem 3 Prompt: Denote the set $\{0, 1\}$ by $\mathbb{Z}_2$, and define addition, denoted $+$, and multiplication, denoted by $\cdot$ or juxtaposition, via the following tables:

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Please prove or disprove $(\mathbb{Z}_2, +, \cdot)$ is a field.

Problem 3 Response: We will show that $\mathbb{Z}_2$ contains all the properties of a field:

1. **Claim 3-1:** $\mathbb{Z}_2$ must be closed under addition such that $a + b \in \mathbb{Z} \forall a, b \in \mathbb{Z}$.

   Proof 3-1: By inspection, the addition table only contains elements in $\mathbb{Z}_2$. Therefore, the sum of any two element in $\mathbb{Z}_2$ yields another element in $\mathbb{Z}_2$, implying that $\mathbb{Z}_2$ is closed under addition.

2. **Claim 3-2:** The elements in $\mathbb{Z}_2$ must be commutative under addition such that $a + b = b + a \forall a, b \in \mathbb{Z}$.

   Proof 3-2: By inspection, the addition table is symmetric which implies that $a, b \in \mathbb{Z}_2 \Rightarrow a + b = b + a$ and hence, $\mathbb{Z}_2$ is commutative under addition.

3. **Claim 3-3:** The elements in $\mathbb{Z}_2$ must be associative under addition such that $(a+b)+c = a+(b+c) \forall a, b, c \in \mathbb{Z}_2$

Proof 3-3: We prove that $\mathbb{Z}_2$ is associative under addition by computing the sum of all possible combinations for $a, b, c \in \mathbb{Z}_2$.

a	b	c	$a + (b + c)$	$(a + b) + c$
0	0	0	0	0
1	0	0	1	1
0	1	0	1	1
1	1	0	0	0
0	0	1	1	1
1	0	1	0	0
0	1	1	0	0
1	1	1	1	1

$$(20)$$

4. **Claim 3-4:** The set $\mathbb{Z}_2$ must contain an additive identity, $0_{\mathbb{Z}_2}$ such that $a + 0_{\mathbb{Z}_2} = a \forall a \in \mathbb{Z}_2$.

   Proof 3-4: By inspection, the addition table indicates that $0 + a = a \forall a \in \mathbb{Z}_2$. Therefore, the additive identity of $\mathbb{Z}_2$ is 0... shocker.

5. **Claim 3-5:** The set $\mathbb{Z}_2$ must contain an additive inverse for each element in $\mathbb{Z}_2$ such that $\exists b \in \mathbb{Z}_2 \ni a + b = 0_{\mathbb{Z}_2} \ \forall a \in \mathbb{Z}_2$.

   Proof 3-5: The additive inverse for $1 \in \mathbb{Z}_2$ is 1, and the additive inverse for $0 \in \mathbb{Z}_2$ is 0. Therefore each element in $\mathbb{Z}_2$ has an additive inverse.

6. **Claim 3-6:** The set $\mathbb{Z}_2$ must be closed under multiplication such that $ab \in \mathbb{Z}_2 \ \forall a, b \in \mathbb{Z}_2$

   Proof 3-6: By inspection, all elements in the multiplication table are elements of $\mathbb{Z}_2$, which implies that $\mathbb{Z}_2$ is closed under multiplication.

7. **Claim 3-7:** The set $\mathbb{Z}_2$ must be commutative under multiplication such that $ab = ba \forall a, b \in \mathbb{Z}_2$.

   Proof 3-7: By inspection, the multiplication table is symmetric, implying that $ab = ba \ \forall a, b \in \mathbb{Z}_2$. Hence, $\mathbb{Z}_2$ is commutative under multiplication.

8. **Claim 3-8:** The set $\mathbb{Z}_2$ must be associative under multiplication such that $(ab)c = a(bc) \forall a, b, c \in \mathbb{Z}_2$.

   Proof 3-8: The definition of associativity under multiplication is $\forall a, b, c \in \mathbb{Z}_2, \ (ab)c = a(bc)$, which we can show by making an exhaustive table that demonstrates that the associative property holds for all possible combinations of $a, b, c \in \mathbb{Z}_2$.

a	b	c	$a \cdot (b \cdot c)$	$a \cdot (b \cdot c)$
0	0	0	0	0
1	0	0	0	0
0	1	0	0	0
1	1	0	0	0
0	0	1	0	0
1	0	1	0	0
0	1	1	0	0
1	1	1	1	1

$$(21)$$

9. **Claim 3-9:** The set $\mathbb{Z}_2$ must contain a multiplicative identity, $1_{\mathbb{Z}_2}$ such that $a1_{\mathbb{Z}_2} = a \ \forall a \in \mathbb{Z}_2$.

   Proof 3-9: According to the multiplication table, $1 \cdot 0 = 0$, and $1 \cdot 1 = 1$. Because $\{0, 1\}$ makes up all elements in $\mathbb{Z}_2$, we can infer that 1 behaves as a multiplicative identity. Therefore, because $\mathbb{Z}_2$ contains 1, $\mathbb{Z}_2$ contains a multiplicative identity.

10. **Claim 3-10:** The set $\mathbb{Z}_2$ must contain a multiplicative inverse for each non-zero element in $\mathbb{Z}_2$ such that $\exists b \in \mathbb{Z}_2 \ni ab = 1_{\mathbb{Z}_2} \ \forall a \in \mathbb{Z}_2 \setminus \{0_{\mathbb{Z}_2}\}$.

    Proof 3-10: The only non-zero element in $\mathbb{Z}_2$ is 1, which is self-inverse (as shown in the multiplication table). Therefore, all non-zero elements in $\mathbb{Z}_2$ have a multiplicative inverse.

11. **Claim 3-11:** The elements in $\mathbb{Z}_2$ must be distributive under addition and multiplication such that $a(b + c) = ab + ac \ \forall a, b, c \in \mathbb{Z}_2$.

Proof 3-11: We show that $\mathbb{Z}_2$ is distributive by making an exhaustive table that demonstrates how the distributive property holds for all possible combinations of $a, b, c \in \mathbb{Z}_2$.

$$
\begin{array}{ccc|c|c}
a & b & c & a \cdot (b + c) & a \cdot b + a \cdot c \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 \\
\end{array}
\tag{22}
$$