

Math 4310 Homework #2 Solutions

1. Prove, step by step, using *only* the field axioms on pp. 19–20, the following propositions:

- (a) $0 \cdot a = 0$ for every $a \in F$

Solution:

$$\begin{aligned} 0 + 0 &= 0 && \text{by definition of additive identity} \\ a \cdot (0 + 0) &= a \cdot 0 \\ a \cdot 0 + a \cdot 0 &= a \cdot 0 && \text{by the distributive law} \\ (a \cdot 0 + a \cdot 0) + (-a \cdot 0) &= a \cdot 0 + (-a \cdot 0) && \text{by existence of additive inverses} \\ a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) &= a \cdot 0 + (-a \cdot 0) && \text{by associativity of addition} \\ a \cdot 0 + 0 &= 0 && \text{by definition of additive inverse} \\ a \cdot 0 &= 0 && \text{since } 0 \text{ is the additive identity.} \end{aligned}$$

- (b) If $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

Solution: Suppose $a \cdot b = 0$. Then either $a = 0$ or $a \neq 0$. If $a = 0$, we are done. If $a \neq 0$, then there exists $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$. Therefore we have

$$\begin{aligned} a \cdot b &= 0 && \text{by assumption} \\ b \cdot a &= 0 && \text{by commutativity of multiplication} \\ (b \cdot a) \cdot a^{-1} &= 0 \cdot a^{-1} \\ (b \cdot a) \cdot a^{-1} &= 0 && \text{by problem 1(a)} \\ b \cdot (a \cdot a^{-1}) &= 0 && \text{by associativity of multiplication} \\ b \cdot 1 &= 0 && \text{by definition of multiplicative inverse} \\ b &= 0 && \text{since } 1 \text{ is the multiplicative identity.} \end{aligned}$$

Thus if $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

- (c) If -1 is the additive inverse of 1 , then $(-1)^2 = 1$.

Solution:

$$\begin{aligned} 1 + (-1) &= 0 && \text{by definition of } (-1) \\ (-1) \cdot (1 + (-1)) &= (-1) \cdot 0 \\ (-1) \cdot (1 + (-1)) &= 0 \cdot (-1) && \text{by commutativity of multiplication} \\ (-1) \cdot (1 + (-1)) &= 0 && \text{by problem 1(a)} \\ (-1) \cdot 1 + (-1)^2 &= 0 && \text{by the distributive law} \\ (-1) + (-1)^2 &= 0 && \text{since } 1 \text{ is the multiplicative identity} \\ (-1)^2 + (-1) &= 0 && \text{by commutativity of addition} \\ ((-1)^2 + (-1)) + 1 &= 0 + 1 \\ (-1)^2 + ((-1) + 1) &= 0 + 1 && \text{by associativity of addition} \\ (-1)^2 + 0 &= 0 + 1 && \text{by definition of } (-1) \\ (-1)^2 &= 1 && \text{since } 0 \text{ is the additive identity} \end{aligned}$$

2. Prove that \mathbb{Z}_2 , consisting of the elements $\{0, 1\}$ with laws

$$\begin{array}{cccc} 0 + 0 = 0 & 0 + 1 = 1 & 1 + 0 = 1 & 1 + 1 = 0 \\ 0 \cdot 0 = 0 & 0 \cdot 1 = 0 & 1 \cdot 0 = 0 & 1 \cdot 1 = 1 \end{array}$$

is a field. (Check each of the field axioms explicitly.)

Solution:

(These operations represent the arithmetic of even and odd numbers, with 0 being even numbers and 1 being odd numbers.)

(a) Commutativity of addition: $1 + 1 = 1 + 1$ and $0 + 0 = 0 + 0$ obviously, so the only thing to check is $1 + 0 = 0 + 1$, which is true.

(b) Associativity of addition:

- $0 + (0 + 0) = 0 + 0 = 0$, $(0 + 0) + 0 = 0 + 0 = 0$
- $0 + (0 + 1) = 0 + 1 = 1$, $(0 + 0) + 1 = 0 + 1 = 1$
- $0 + (1 + 0) = 0 + 1 = 1$, $(0 + 1) + 0 = 1 + 0 = 1$
- $0 + (1 + 1) = 0 + 0 = 0$, $(0 + 1) + 1 = 1 + 1 = 0$
- $1 + (0 + 0) = 1 + 0 = 1$, $(1 + 0) + 0 = 1 + 0 = 1$
- $1 + (0 + 1) = 1 + 1 = 0$, $(1 + 0) + 1 = 1 + 1 = 0$
- $1 + (1 + 0) = 1 + 1 = 0$, $(1 + 1) + 0 = 0 + 0 = 0$
- $1 + (1 + 1) = 1 + 0 = 1$, $(1 + 1) + 1 = 0 + 1 = 1$

(c) Commutativity of multiplication: $1 \cdot 1 = 1 \cdot 1$ and $0 \cdot 0 = 0 \cdot 0$ obviously, so just check $1 \cdot 0 = 0 \cdot 1$, which is true.

(d) Associativity of multiplication:

- $0 \cdot (0 \cdot 0) = 0 \cdot 0 = 0$, $(0 \cdot 0) \cdot 0 = 0 \cdot 0 = 0$
- $0 \cdot (0 \cdot 1) = 0 \cdot 0 = 0$, $(0 \cdot 0) \cdot 1 = 0 \cdot 1 = 0$
- $0 \cdot (1 \cdot 0) = 0 \cdot 0 = 0$, $(0 \cdot 1) \cdot 0 = 0 \cdot 0 = 0$
- $0 \cdot (1 \cdot 1) = 0 \cdot 1 = 0$, $(0 \cdot 1) \cdot 1 = 0 \cdot 1 = 0$
- $1 \cdot (0 \cdot 0) = 1 \cdot 0 = 0$, $(1 \cdot 0) \cdot 0 = 0 \cdot 0 = 0$
- $1 \cdot (0 \cdot 1) = 1 \cdot 0 = 0$, $(1 \cdot 0) \cdot 1 = 0 \cdot 1 = 0$
- $1 \cdot (1 \cdot 0) = 1 \cdot 0 = 0$, $(1 \cdot 1) \cdot 0 = 1 \cdot 0 = 0$
- $1 \cdot (1 \cdot 1) = 1 \cdot 1 = 1$, $(1 \cdot 1) \cdot 1 = 1 \cdot 1 = 1$

(e) Existence of additive identity 0:

$$0 + 0 = 0 \quad \text{and} \quad 1 + 0 = 1.$$

(f) Existence of multiplicative identity 1:

$$0 \cdot 1 = 0 \quad \text{and} \quad 1 \cdot 1 = 1.$$

(g) Distributive law:

- $0 \cdot (0 + 0) = 0 \cdot 0 = 0, 0 \cdot 0 + 0 \cdot 0 = 0 + 0 = 0$
- $0 \cdot (0 + 1) = 0 \cdot 1 = 0, 0 \cdot 0 + 0 \cdot 1 = 0 + 0 = 0$
- $0 \cdot (1 + 0) = 0 \cdot 1 = 0, 0 \cdot 1 + 0 \cdot 0 = 0 + 0 = 0$
- $0 \cdot (1 + 1) = 0 \cdot 0 = 0, 0 \cdot 1 + 0 \cdot 1 = 0 + 0 = 0$
- $1 \cdot (0 + 0) = 1 \cdot 0 = 0, 1 \cdot 0 + 1 \cdot 0 = 0 + 0 = 0$
- $1 \cdot (0 + 1) = 1 \cdot 1 = 1, 1 \cdot 0 + 1 \cdot 1 = 0 + 1 = 1$
- $1 \cdot (1 + 0) = 1 \cdot 1 = 1, 1 \cdot 1 + 1 \cdot 0 = 1 + 0 = 1$
- $1 \cdot (1 + 1) = 1 \cdot 0 = 0, 1 \cdot 1 + 1 \cdot 1 = 1 + 1 = 0$

(h) Existence of additive inverse: Use $(-0) = 0$ and $(-1) = 1$, since $0 + 0 = 0$ and $1 + 1 = 0$.

(i) Existence of multiplicative inverse for nonzero elements: Use $1^{-1} = 1$, since $1 \cdot 1 = 1$.

3. Prove that \mathbb{Z}_2 with laws

$$\begin{array}{cccc} 0 + 0 = 0 & 0 + 1 = 1 & 1 + 0 = 1 & 1 + 1 = 1 \\ 0 \cdot 0 = 0 & 0 \cdot 1 = 0 & 1 \cdot 0 = 0 & 1 \cdot 1 = 1 \end{array}$$

is not a field. (Which axioms are not valid?)

Solution:

(These operations represent Boolean arithmetic, with 0 being “true” and 1 being “false,” where $+$ is “or” and \cdot is “and.”)

By going through the same computations as above, we can see that all the axioms are valid except for the existence of an additive inverse for 1: since $0 + 1 = 1$ and $1 + 1 = 1$, there is no element that can be added to 1 to obtain 0.

4. Prove step by step that for any ordered field F , and any element $a \in F$ with $a \neq 0$, we have $a^2 > 0$. Conclude that \mathbb{C} cannot be an ordered field.

Solution: Take any element $a \in F$ with $a \neq 0$. Then by the first order axiom, we know either $a > 0$ or $0 < a$.

If $a > 0$, then by the multiplication axiom, we know $a \cdot a > 0 \cdot a$ so that $a^2 > 0$ (by problem 1(a)). If $a < 0$, then by the multiplication axiom we know $a \cdot a > 0 \cdot a$ so that $a^2 > 0$ (again by problem 1(a)).

Now for \mathbb{C} we have $i^2 = -1$, and we also have $1^2 = 1$. Thus if \mathbb{C} were an ordered field, we would have both $-1 > 0$ and $1 > 0$. But if we add 1 to both sides of $-1 > 0$, we get $0 > 1$, which contradicts $1 > 0$. Hence \mathbb{C} cannot be an ordered field.