1 Let $(F, +, \cdot, <)$ be an ordered field and let $a, b, c \in F$. Show that

$$2ab \leq a^2 + b^2$$

and

$$ab + bc + ca \leq a^2 + b^2 + c^2.$$

Specify what axioms you are using at each step.

Solution Since F is a field, $-b \in F \implies a + (-b) = a - b \in F$. By a proposition proved in class, $a - b \neq 0 \implies (a-b)^2 > 0$. If $a - b = 0$, then $(a-b)^2 = (a-b)\cdot(a-b) = 0 \cdot 0 = 0$. Combining both statements yields $(a-b)^2 \geq 0$ for any $a, b \in F$. Thus

$$\begin{aligned}
(a-b)^2 &= (a-b)\cdot(a-b) \\
&\overset{\text{(D)}}{=} a(a-b) - b(a-b) \\
&\overset{\text{(D)}}{=} a\cdot a + a\cdot(-b) - (b\cdot a - b\cdot b) \\
&= a^2 - ab - (ba - b^2) \\
&\underset{\text{(M2)}}{\overset{\text{(D)}}{=}} a^2 - ab - ab + b^2 \\
&= a^2 - 2ab + b^2 \\
&\overset{\text{(A2)}}{=} a^2 + b^2 - 2ab
\end{aligned}$$

Then

$$a^2 + b^2 - 2ab \geq 0$$
$$a^2 + b^2 - 2ab + 2ab \overset{\text{(A5)}}{=} a^2 + b^2 \overset{\text{(O1)}}{\geq} 0 + 2ab \overset{\text{(A4)}}{=} 2ab.$$

Thus, $2ab \leq a^2 + b^2$ as desired.

For the second inequality, we start by proving a lemma: if $a \leq b$ and $c \leq d$, then $a + c \leq b + d$ if $a, b, c, d \in F$. Since F is an ordered field, we can use (O1) and (A2):

$$a + c \leq a + d = d + a \leq d + b = b + d$$

In other words, we can add inequalities as long as they are both in the same direction.

Using the first inequality, we can write

$$\begin{aligned}
2ab &\leq a^2 + b^2 \\
2ac &\leq a^2 + c^2 \\
2bc &\leq b^2 + c^2
\end{aligned}$$

for $a, b, c \in F$. Then using the lemma proved above, we get

$$2ab + 2ac + 2bc \leq 2a^2 + 2b^2 + 2c^2.$$

Since $0 < 2$, by a proposition proved in class, we have $0 < 2^{-1}$, so we can use another proposition we proved in class, (A2), (M2), (M5), and (D) to get the desired result:

$$\begin{aligned}
2^{-1}\cdot(2ab + 2ac + 2bc) &\leq 2^{-1}\cdot(2a^2 + 2b^2 + 2c^2) \\
ab + bc + ca &\leq a^2 + b^2 + c^2
\end{aligned}$$

2 Let $(F, +, \cdot)$ be a field with exactly four distinct elements $F = \{0, 1, a, b\}$ where 0 and 1 denote the identities for $+$ and $\cdot$, respectively, and a, b denote the remaining two elements of F. Fill in the addition and multiplication tables below. Use the axioms to justify your answer. (Note that for each table entry there is a *unique* correct solution.)

$+$	0	1	a	b
0				
1				
a				
b				

$\cdot$	0	1	a	b
0				
1				
a				
b				

Hint: Show that in the addition table, each row and each column contains every element of F exactly once (as in Sudoku). Show that the same is true for the rows and columns of the multiplication table that are not identically zero.

Solution 0 is the additive identity of F, so $0 + c = c \ \forall c \in F$, by axiom (A4). The identity is also unique. Suppose 0' is another additive identity of F. Then by (A4), $0 + 0' = 0$. It follows from a proposition proved in class that $0' = 0$, so 0 is unique. Thus in each row and column, the element being added appears exactly once.

Next consider $a+1 = 1+a$. The sum cannot be a because it would imply that $1 = 0$, and the sum cannot be 1 because then a would be 0. So, the sum is equal to 0 or b. Suppose $a + 1 = 0$. Then $-a = 1$ and $-1 = a$. But then b will have no additive inverse, which violates (A4). This means $a + 1 = b$. Similarly, $b + 1 = a$.

Using (A5), $a + 1 + (-1) = b + (-1) \implies a = b - 1$. Combining that with $b + 1 = a$, we get $b - 1 = b + 1$, which by a proposition we proved in class gives $-1 = 1$, which means 1 is its own inverse. It follows that $-a = a$ and $-b = b$ by multiplying both sides by a and b, respectively.

Since $b = a + 1$, we can add a to both sides to get $a + b = a + a + 1$. Since the inverse of each element is itself, we get $a + b \overset{(A2)}{=} b + a = 1$.

Thus, the addition table is

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

By a proposition we proved in class, $0c = 0 \ \forall c \in F$, so the first row and column are all 0. By (M4), $1c = c \ \forall c \in F$, so the second row and column will be the element multiplied with 1. So, there are three products left to determine: $a \cdot a$, $b \cdot b$, and $a \cdot b \overset{(M2)}{=} b \cdot a$.

Similarly to addition, the multiplicative identity 1 is unique. Suppose otherwise, and that 1' is also a multiplicative inverse. Then $1 \cdot 1' = 1 = 1'$, so 1 is unique. That means $a \cdot b \neq a$ and $a \cdot b \neq b$. $a \cdot b \neq 0$, too since, by a proposition proved in class, that would imply that $a = 0$ or $b = 0$. Since $a \cdot b \in F$ by (M2), the only possibility left is $a \cdot b = 1$. Thus, a and b are multiplicative inverses to each other.

a^2 cannot be equal to 0 because that would mean $a = 0$, and a^2 cannot equal a because the multiplicative identity is unique. a^2 cannot equal 1 either since the multiplicative inverse of a is b. Thus, a^2 must be b. By a similar argument, $b^2 = a$. So, the multiplication table is

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

3 Define two internal laws of composition on $R = \mathbb{Z} \times \mathbb{Z}$ as follows

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1 + 2a_2 b_2, a_1 b_2 + a_2 b_1).$$

a. Show that with these operations R is a ring.

b. Define an order relation $\leq$ on R as follows: we write $(a_1, a_2) \leq (a_2, b_2)$ if $a_1 + a_2\sqrt{2} \leq b_1 + b_2\sqrt{2}$ in the usual sense on $\mathbb{R}$. Prove that this is an order relation on R and that with it, R is an ordered ring.

Solution a. In this problem, I will use the fact that $\mathbb{Z}$ is a ring. The axioms I use will be applied to elements of $\mathbb{Z}$.

(A1) $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$. $a_1, b_1, a_2, b_2 \in \mathbb{Z} \overset{\text{(A1)}}{\Longrightarrow} a_1 + b_1 \in \mathbb{Z}$ and $a_2 + b_2 \in \mathbb{Z} \Longrightarrow (a_1 + b_1, a_2 + b_2) \in \mathbb{Z} \times \mathbb{Z}$.

(A2) $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \overset{\text{(A2)}}{=} (b_1 + a_1, b_2 + a_2) = (b_1, b_2) + (a_1, a_2)$.

(A3) $(a_1, a_2) + [(b_1, b_2) + (c_1, c_2)] = (a_1, a_2) + (b_1 + c_1, b_2 + c_2) = (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2)) \overset{\text{(A3)}}{=} ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2) = (a_1 + b_1, a_2 + b_2) + (c_1, c_2) = [(a_1, a_2) + (b_1, b_2)] + (c_1, c_2)$

(A4) $(a_1, a_2) + (0, 0) = (a_1 + 0, a_2 + 0) \overset{\text{(A4)}}{=} (a_1, a_2) \Longrightarrow (0, 0)$ is the identity.

(A5) $(a_1, a_2) + (-a_1, -a_2) = (a_1 + (-a_1), a_2 + (-a_2)) \overset{\text{(A5)}}{=} (0, 0) \Longrightarrow -(a_1, a_2) = (-a_1, -a_2)$ is the inverse.

(M1) $\mathbb{Z}$ is closed under scalar multiplication and addition, so $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1 + 2a_2 b_2, a_1 b_2 + a_2 b_1) \in \mathbb{Z} \times \mathbb{Z}$.

(M2) $(b_1, b_2) \cdot (a_1, a_2) = (b_1 a_1 + 2b_2 a_2, b_1 a_2 + b_2 a_1) \overset{\text{(M2)}}{=} (a_1 b_1 + 2a_2 b_2, a_1 b_2 + a_2 b_1) = (a_1, a_2) \cdot (b_1, b_2)$.

(M3)
$$\begin{aligned}
(a_1, a_2) \cdot [(b_1, b_2) \cdot (c_1, c_2)] &= (a_1, a_2) \cdot (b_1 c_1 + 2b_2 c_2, b_1 c_2 + b_2 c_1) \\
&= (a_1(b_1 c_1 + 2b_2 c_2) + 2a_2(b_1 c_2 + b_2 c_1), a_1(b_1 c_2 + b_2 c_1) + a_2(b_1 c_1 + 2b_2 c_2)) \\
&\overset{\text{(D)}}{=} (a_1 b_1 c_1 + 2a_1 b_2 c_2 + 2a_2 b_1 c_2 + 2a_2 b_2 c_1, a_1 b_1 c_2 + a_1 b_2 c_1 + a_2 b_1 c_1 + 2a_2 b_2 c_2) \\
[(a_1, a_2) \cdot (b_1, b_2)] \cdot (c_1, c_2) &= (a_1 b_1 + 2a_2 b_2, a_1 b_2 + a_2 b_1) \cdot (c_1, c_2) \\
&= ((a_1 b_1 + 2a_2 b_2)c_1 + 2(a_1 b_2 + a_2 b_1)c_2, (a_1 b_1 + 2a_2 b_2)c_2 + (a_1 b_2 + a_2 b_1)c_1) \\
&\overset{\text{(D)}}{=} (a_1 b_1 c_1 + 2a_2 b_2 c_1 + 2a_1 b_2 c_2 + 2a_2 b_1 c_2, a_1 b_1 c_2 + 2a_2 b_2 c_2 + a_1 b_2 c_1 + a_2 b_1 c_1) \\
&\overset{\text{(A3)}}{=} (a_1 b_1 c_1 + 2a_1 b_2 c_2 + 2a_2 b_1 c_2 + 2a_2 b_2 c_1, a_1 b_1 c_2 + a_1 b_2 c_1 + a_2 b_1 c_1 + 2a_2 b_2 c_2) \\
&= (a_1, a_2) \cdot [(b_1, b_2) \cdot (c_1, c_2)]
\end{aligned}$$

(M4) $(a_1, a_2) \cdot (1, 0) = (a_1 \cdot 1 + 2a_2 \cdot 0, a_1 \cdot 0 + a_2 \cdot 1) \underset{\text{(A4)}}{\overset{\text{(M5)}}{=}} (a_1, a_2) \Longrightarrow (1, 0)$ is the identity.

(D)
$$\begin{aligned}
(a_1, a_2) \cdot [(b_1, b_2) + (c_1, c_2)] &= (a_1, a_2) \cdot (b_1 + c_1, b_2 + c_2) \\
&= (a_1(b_1 + c_1) + 2a_2(b_2 + c_2), a_1(b_2 + c_2) + a_2(b_1 + c_1)) \\
&\overset{\text{(D)}}{=} (a_1 b_1 + a_1 c_1 + 2a_2 b_2 + 2a_2 c_2, a_1 b_2 + a_1 c_2 + a_2 b_1 + a_2 c_1) \\
&\underset{\text{(A3)}}{\overset{\text{(A2)}}{=}} ((a_1 b_1 + 2a_2 b_2) + (a_1 c_1 + 2a_2 c_2), (a_1 b_2 + a_2 b_1) + (a_1 c_2 + a_2 c_1)) \\
&= (a_1 b_1 + 2a_2 b_2, a_1 b_2 + a_2 b_1) + (a_1 c_1 + 2a_2 c_2, a_1 c_2 + a_2 c_1) \\
&= (a_1, a_2) \cdot (b_1, b_2) + (a_1, a_2) \cdot (b_1, b_2)
\end{aligned}$$

b. Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in \mathbb{Z} \times \mathbb{Z}$ such that $(a_1, a_2) \leq (b_1, b_2)$.

(O1) By definition, $a_1 + a_2\sqrt{2} \leq b_1 + b_2\sqrt{2}$. We wish to show that $(a_1, a_2) + (c_1, c_2) = (a_1 + c_1, a_2 + c_2) \leq (b_1 + c_1, b_2 + c_2) = (b_1, b_2) + (c_1, c_2)$. That is, we wish to show that $(a_1 + c_1) + (a_2 + c_2)\sqrt{2} \leq (b_1 + c_1) + (b_2 + c_2)\sqrt{2}$.

Note that $a_1 + a_2\sqrt{2}, b_1 + b_2\sqrt{2}, c_1 + c_2\sqrt{2} \in \mathbb{R}$, which is an ordered field. Then we can use (O1), (A2), and (A3) to get

$$
\begin{aligned}
(a_1 + a_2\sqrt{2}) + (c_1 + c_2\sqrt{2}) &\leq (b_1 + b_2\sqrt{2}) + (c_1 + c_2\sqrt{2}) \\
(a_1 + c_1) + (a_2 + c_2)\sqrt{2} &\leq (b_1 + c_1) + (b_2 + c_2)\sqrt{2} \\
\iff (a_1, a_2) + (c_1, c_2) &\leq (b_1, b_2) + (c_1, c_2)
\end{aligned}
$$

Thus, (O1) holds on R.

(O2) Let (a_1, a_2) and (b_1, b_2) be as described above, and let $(c_1, c_2) \geq 0 \iff c_1 + c_2\sqrt{2} \geq 0$. We wish to show that $(a_1, a_2) \cdot (c_1, c_2) \leq (b_1, b_2) \cdot (c_1, c_2)$.
Once again, note that $a_1 + a_2\sqrt{2}, b_1 + b_2\sqrt{2}, c_1 + c_2\sqrt{2} \in \mathbb{R}$, and $\mathbb{R}$ is an ordered field. By assumption, $a_1 + a_2\sqrt{2} \leq b_1 + b_2\sqrt{2}$. Since $c_1 + c_2\sqrt{2} \geq 0$ as well, we can use (O2), (A2), (A3), (M3), and (D), which gives us

$$
\begin{aligned}
(a_1 + a_2\sqrt{2})(c_1 + c_2\sqrt{2}) &\leq (b_1 + b_2\sqrt{2})(c_1 + c_2\sqrt{2}) \\
a_1c_1 + a_1c_2\sqrt{2} + a_2c_1\sqrt{2} + (\sqrt{2})^2 a_2c_2 &\leq b_1c_1 + b_1c_2\sqrt{2} + b_2c_1\sqrt{2} + (\sqrt{2})^2 b_2c_2 \\
a_1c_1 + a_1c_2\sqrt{2} + a_2c_1\sqrt{2} + 2a_2c_2 &\leq b_1c_1 + b_1c_2\sqrt{2} + b_2c_1\sqrt{2} + 2b_2c_2 \\
(a_1c_1 + 2a_2c_2) + (a_1c_2 + a_2c_1)\sqrt{2} &\leq (b_1c_1 + 2b_2c_2) + (b_1c_2 + b_2c_1)\sqrt{2} \\
\iff (a_1c_1 + 2a_2c_2, a_1c_2 + a_2c_1) &\leq (b_1c_1 + 2b_2c_2, b_1c_2 + b_2c_1) \\
\iff (a_1, a_2) \cdot (c_1, c_2) &\leq (b_1, b_2) \cdot (c_1, c_2)
\end{aligned}
$$

Thus (O2) holds on R.

(O1) and (O2) holds on R, and R is a ring, so R is an ordered ring.

---

4 Let S be a non-empty bounded subset of $\mathbb{R}$.

a. Prove that $\inf S \leq \sup S$

b. What can you say about S if $\inf S = \sup S$?

Solution a. Let $s \in S$. Then by definition, $\inf S \leq s \leq \sup S \implies \inf S \leq \sup S$.

b. Let $M = \inf S = \sup S$. Then by definition, for all $s \in S$, $M = \inf S \leq s \leq \sup S = M$. Then $s = M$ for all s. In other words, $S = \{M\}$.

---

5 Let S and T be two non-empty bounded subsets of $\mathbb{R}$.

a. Prove that if $S \subseteq T$, then $\inf T \leq \inf S \leq \sup S \leq \sup T$.

b. Prove that $\sup(S \cup T) = \max\{\sup S, \sup T\}$.

Solution a. From exercise (4a), we have $\inf S \leq \sup S$ and $\inf T \leq \sup T$. All that's left is to show that $\inf T \leq \inf S$ and $\sup S \leq \sup T$.

Since S and T are non-empty bounded subsets of $\mathbb{R}$ and $\mathbb{R}$ has the least-upper-bound property, $\sup S, \sup T \in \mathbb{R}$. Suppose $\sup T < \sup S$. By definition, $\sup S \geq \ \forall s \in S$. Since $S \subseteq T$, then for all $s \in S$, we have $s \in T$ also, so $s \leq \sup T < \sup S$. Thus, $\sup T$ is an upper bound for S, but less than $\sup S$, which is a contradiction. Hence, we must have $\sup T \geq \sup S$.

Similarly, $\inf S, \inf T \in \mathbb{R}$ since $\mathbb{R}$ also has the greatest-lower-bound property. Suppose $\inf S < \inf T$ and let $s \in S$. Then by definition, $s \leq \inf S < \inf T$. Thus, $\inf T$ is a lower bound for S greater than $\inf S$, but $\inf S$ is the greatest lower bound. We have a contradiction, so $\inf S \geq \inf T$.

Taking the above parts, we have $\inf T \leq \inf S \leq \sup S \leq \sup T$ as desired.

b. $\sup S$ and $\sup T$ both exist and belong to $\mathbb{R}$ since $\mathbb{R}$ has the least-upper-bound property. Since $\mathbb{R}$ is an ordered field, there are three cases to consider:

$\sup S < \sup T$:

Suppose $\sup S < \sup T$ and let $a \in S \cup T$. If $a \in S$, then $a \leq \sup S < \sup T$. If $a \in T$, then $a \leq \sup T$. Thus, for any element a in $S \cup T$, we have $a \leq \sup T \implies \sup(S \cup T) = \sup T$.

$\sup T < \sup S$:

The same argument can be made as the above, but with S and T switched. So, in this case, $\sup(S \cup T) = \sup S$.

$\sup S = \sup T$:

Let $a \in S \cup T$. Then if $a \in S$, then $a \leq \sup S = \sup T$. Otherwise, if $a \in T$, then $a \leq \sup T = \sup S$. Thus, $\sup(S \cup T) = \sup S = \sup T$.

In all three cases, we take the larger of $\sup S$ and $\sup T$, unless they are the same, then we can take either. Thus, $\sup S \cup T = \max\{\sup S, \sup T\}$.

---

6 Let A be a non-empty subset of $\mathbb{R}$ which is bounded below and let

$$-A = \{-a \mid a \in A\}.$$

Prove that $\inf A = -\sup(-A)$.

Solution Let $a \in A$. Then by definition, $\inf A \leq a$. By a proposition proved in class, we multiply both sides by -1 to get $-a \leq -\inf A$. $-a \in -A$ by definition, and the inequality holds for any $-a \in -A$, so $-\inf A$ is the supremum of $-A$. That is, $-\inf A = \sup(-A) \implies \inf A = -\sup(-A)$.

---

7 Let A and B be two non-empty bounded subsets of $\mathbb{R}$ and let

$$S = \{a + b \mid a \in A \text{ and } b \in B\}$$

a. Prove that $\sup S = \sup A + \sup B$

b. Prove that $\inf S = \inf A + \inf B$

Solution a. Let $s \in S$. Then we can find $a \in A$ and $b \in B$ such that $s = a + b$. Then by definition, $a \leq \sup A$ and $b \leq \sup B$. By a lemma proved in problem (1), we can add these inequalities to get

$$s = a + b \leq \sup A + \sup B.$$

This inequality holds for every $s \in S$ we choose, so by definition, $\sup S = \sup A + \sup B$.

b. Let s, a, and b be as described above. By definition, we have $\inf A \leq a$ and $\inf B \leq b$. Using the same lemma, we get $\inf A + \inf B \leq a + b = s$ $\forall s \in S$, so by definition, $\inf S = \inf A + \inf B$.

---

8 Show that

$$\sup\{r \in \mathbb{Q} \mid r < a\} = a \quad \text{for all} \quad a \in \mathbb{R}.$$

Solution By the definition of the set, all elements in the set are less than a. Thus, a is an upper bound for it. We only need to show that it is the least upper bound of the set.

Suppose a is not the least upper bound, and that there exists an upper bound $M \in \mathbb{R}$ such that $M < a$. Since the rationals are dense on $\mathbb{R}$, we can find $r \in \mathbb{Q}$ such that $M < r < a \implies r \in \{r \in \mathbb{Q} \mid r < a\}$. However, this is a contradiction since M is supposed to be an upper bound for that set. Thus, no such M exists, and a must be the least upper bound for the set, so we have $\sup\{r \in \mathbb{Q} \mid r < a\} = a$ $\forall a \in \mathbb{R}$.