Problem 1: **Lemma:** For all $a \in F$, $a^2 \geq 0$.

Proof: Let $a \in F$.

Case 1: Assume $a = 0$. Then $a^2 = 0 \cdot 0 = 0$ by Proposition 4.5.1.

Case 2: Assume $a \neq 0$. Then $a^2 > 0$ by Proposition 5.1.3.

Hence, $a^2 \geq 0$.

(a) Let $a, b \in F$. By the field axioms, $-b \in F$ and $a + (-b) = a - b \in F$. So, using the lemma, $(a-b)^2 \geq 0$. Using the field axioms to expand the left hand side and add the additive inverse of $-2ab$,

$$\begin{aligned} (a-b)^2 = a^2 - 2ab + b^2 &\geq 0 \\ a^2 - 2ab + b^2 + 2ab &\geq 0 + 2ab \\ a^2 + b^2 &\geq 2ab \end{aligned}$$

(b) Let $a, b, c \in F$. By the Field Axioms, $a-b, b-c, c-a \in F$. Hence, $(a-b)^2 \geq 0$, $(b-c)^2 \geq 0$, and $(c-a)^2 \geq 0$.
From ordered field axiom 1, we get the following inequality,

$$0 \leq (a-b)^2 + 0 + 0 \leq (a-b)^2 + (b-a)^2 + 0 \leq (a-b)^2 + (b-a)^2 + (c-a)^2$$

Expanding $(a-b)^2 + (b-a)^2 + (c-a)^2$ with the Field axioms, we get

$$(a-b)^2 + (b-a)^2 + (c-a)^2 = 2(a^2 + b^2 + c^2 - ab - bc - ca) \geq 0$$

Lemma: In the ordered field F, $2 \neq 0$.
Proof: We know that $0 < 1$ from Proposition 5.1.3. From Ordered Field Axiom 1, $0 < 1 + 0 < 1 + 1 = 2$. By Trichtomy of Order Relations, $0 \neq 2$.
Since, $2 \neq 0$, $2^{-1} \in F$. Note that $0 \cdot 2^{-1} = 0$ by a proposition.
So, using the field axioms

$$\begin{aligned} 2^{-1} \cdot 2(a^2 + b^2 + c^2 - ab - bc - ca) &\geq 2^{-1} \cdot 0 \\ a^2 + b^2 + c^2 - ab - bc - ca &\geq 0 \\ a^2 + b^2 + c^2 &\geq ab + bc + ca \end{aligned}$$

Problem 2: Note that both tables must be symmetric because fields are commutative both for addition and multplication.

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Multiplication: From the propositions, $0 \cdot a = 0$ for all $a \in F$. From the axioms, $1 \cdot a = a$ for all $a \in F$. This explains the first two rows and columns. Additionally, the table is evidentally closed under multiplication. Moreover, all of the multiplicative inverses of the non-zero elements are also non-zero.

Next, we can verify that it is associative. It is trivial to check for products with 0 or 1.

$$\begin{aligned} a(a \cdot a) &= a(b) = 1 \\ (a \cdot a)a &= b(a) = 1 \\ a(a \cdot b) &= a(1) = a \\ (a \cdot a)b &= bb = a \\ a(b \cdot a) &= a(1) = a \\ (a \cdot b)a &= (1)a = a \\ b(a \cdot b) &= b(1) = b \\ (b \cdot a)b &= (1)b = b \\ b(b \cdot b) &= b(a) = 1 \\ (b \cdot b)b &= a(b) = 1 \end{aligned}$$

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

Addition: The first row and column follow the axiom of the additive identity. Evidentally, addition is closed as well and every element has an additive inverse. Associativity of addition can be verified the same way as multiplication.

There are too many cases to check for distributivity, but trust that I have verified them, and that it works.

Problem 3: (a) Let $q \geq 2$ be a prime number. Let $n, m, n', m' \in \mathbb{Z}$ where n n' and m m'. We want to show that $C(n + m) = C(n' + m')$.

So, we know that $C(n) = C(n')$ and $C(m) = C(m')$. This means $n - n' = kq$ for some $k \in \mathbb{Z}$ and $m - m' = lq$ for some $l \in \mathbb{Z}$.

Adding these two equations together, we get

$$n - n' + m - m' = kq + lq$$

Moving around terms, we find

$$(m+n)-(m'+n)=(k+l)q$$

Note that $k+l \in \mathbb{Z}$. Hence, $C(m+n)=C(m'+n')$ and addtion is well defined.

To show that multiplication is well defined, we want to show that $C(n \cdot m)=C(n' \cdot m')$, or $n \cdot m - n' \cdot m' = cq$ for some $c \in \mathbb{Z}$

We can obtain the left hand side of the previous equation from

$$n \cdot m - n' \cdot m' = n \cdot (m-m') + m' \cdot (n-n')$$

Using the same variables as the addition check,

$$n \cdot (m-m') + m' \cdot (n-n') = n \cdot lq + m' \cdot kq$$

Distributing,

$$n \cdot lq + m' \cdot kq = q(nl + m'k)$$

Since $\mathbb{Z}$ is closed under addition and multiplication, $nl+m'k \in \mathbb{Z}$. Hence, $n \cdot m - n' \cdot m' = q(nl+m'k)$ and $C(mn)=C(m'n')$.

(b)

- Additive Closure. Let $C(n), C(m) \in \mathbb{Z}/q\mathbb{Z}$. We know that $n+m \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under addition. Therefore, $C(n+m)$ is an equivalence class by definition, so $C(m+n) \in \mathbb{Z}/q\mathbb{Z}$.
- Additive Commutativity. Let $C(n), C(m) \in \mathbb{Z}/q\mathbb{Z}$. We know that $C(n)+C(m)=C(n+m)$. Using the additive commutativity of $\mathbb{Z}$, we find $C(n+m)=C(m+n)$. We know that $C(m+n)=C(m)+C(n)$. Hence, $C(m)+C(n)=C(n)+C(m)$
- Additive Associativity. Let $C(n), C(m), C(p) \in \mathbb{Z}/q\mathbb{Z}$. We know that $(C(n)+C(m))+C(p)=C(n+m)+C(p)=C((n+m)+p)$. Using the associativity of $\mathbb{Z}$, $C((n+m)+p)=C(n+(m+p))=C(n)+C(m+p)=C(n)+(C(m)+C(p))$. Ergo, $(C(n)+C(m))+C(p)=C(n)+(C(m)+C(p))$
- Additive Identity. Let $C(n) \in \mathbb{Z}/q\mathbb{Z}$. Using the additive identity of $\mathbb{Z}$, we know that $n+0=n=0+n$. So, $C(n)=C(n+0)=C(n)+C(0)$ and $C(n)=C(0+n)=C(0)+C(n)$. Hence, there exists an additive identity and it is $C(0)$.
- Additive Inverse. Let $C(n) \in \mathbb{Z}/q\mathbb{Z}$. We know that $-n$ exists in $\mathbb{Z}$. So, $C(0)=C(n+(-n))=C(n)+C(-n)$. Hence, the additive inverse of $C(n)$ exists and it is $C(-n)$ since their sum is the additive identity $C(0)$.
- Multiplicative Closure. Let $C(n), C(m) \in \mathbb{Z}/q\mathbb{Z}$. We know $nm \in \mathbb{Z}$ since it is closed under multiplication. Hence, $C(nm)$ is an equivalence class and $C(n) \cdot C(m) \in \mathbb{Z}/q\mathbb{Z}$.

- Multiplicative Commutativity. Let $C(n), C(m) \in \mathbb{Z}/q\mathbb{Z}$. We know that $C(n) \cdot C(m) = C(n \cdot m)$. Using the additive commutativity of $\mathbb{Z}$, we find $C(n \cdot m) = C(m \cdot n)$. We know that $C(m \cdot n) = C(m) \cdot C(n)$. Hence, $C(m) \cdot C(n) = C(n) \cdot C(m)$
- Multiplicative Associativity. Let $C(n), C(m), C(p) \in \mathbb{Z}/q\mathbb{Z}$. We know that $(C(n) \cdot C(m)) \cdot C(p) = C(n \cdot m) \cdot C(p) = C((n \cdot m) \cdot p)$. Using the associativity of $\mathbb{Z}$, $C((n \cdot m) \cdot p) = C(n \cdot (m \cdot p)) = C(n) \cdot C(m \cdot p) = C(n) \cdot (C(m) \cdot C(p))$. Therefore, $(C(n) \cdot C(m)) \cdot C(p) = C(n) \cdot (C(m) \cdot C(p))$
- Multiplicative Identity. Let $C(n) \in \mathbb{Z}/q\mathbb{Z}$ and assume $C(n) \neq C(0)$. Using the multiplicative identity of $\mathbb{Z}$, we know that $n \cdot 1 = n = 1 \cdot n$. So, $C(n) = C(n \cdot 1) = C(n) \cdot C(1)$ and $C(n) = C(1 \cdot n) = C(1) \cdot C(n)$. Hence, there exists an additive identity and it is $C(1)$.
- Multiplicative Inverse. Let $C(n) \in \mathbb{Z}/q\mathbb{Z}$. We want to show that there exists a $C(m) \in \mathbb{Z}/q\mathbb{Z}$ such that $C(m) \cdot C(n) = C(1)$.
  Assume that $C(mn) = C(1)$. So, $mn - 1 = kq$ for some $k \in \mathbb{Z}$. This is equivalent to finding an multiplicative inverse for the field $\mathbb{Z}$ mod q. By pigeonhole principle, we can show that every element $1, ..., q-1$ has a multiplicative inverse because q is prime. Note that by pigeonhole principle n must share an equivalence class with some $x \in \{1, ...q-1\}$ because $C(n) \neq C(0)$. Let m be the multiplicative inverse of x. m is also the multiplicative inverse of n. Hence, there exists a $C(m)$ such that $C(m) \cdot C(n) = C(mn) = C(1)$.
- Distributivity. Let $C(n), C(m), C(p) \in \mathbb{Z}/q\mathbb{Z}$.

$$\begin{aligned}(C(n) + C(m)) \cdot C(p) &= C(n+m) \cdot C(p) \\ &= C((n+m) \cdot p) \\ &= C(n \cdot p + m \cdot p) \\ &= C(n \cdot p) + C(m \cdot p)\end{aligned}$$

  Hence, $\mathbb{Z}/q\mathbb{Z}$ is distributive

Since, $\mathbb{Z}/q\mathbb{Z}$ fulfills all of the axioms, it is a field.

(c) Assume there exists an order relation $<$ on $\mathbb{Z}/q\mathbb{Z}$.

We know that $C(q) = C(0)$. By proposition 5.1, we know that $C(1)$ the multiplicative identity must be greater than $C(0)$ in any order relation; so $C(0) < C(1)$. Since $C(1) > C(0)$, if we add $C(1)$ $q-1$ times to both sides of the inequality we get, $C(1) < C(q-1) < C(q)$. However, $C(q) = C(0)$, so $C(1) < C(q-1) < C(0)$. This leads to a contradiction since $C(1) > C(0)$ in all ordered fields. Hence, there cannot be an ordered relation on $\mathbb{Z}/q\mathbb{Z}$

Problem 4: (a)

- Let $(a_1, a_2), (b_1, b_2) \in F$. We know that $\mathbb{R}$ is closed under addition, so $a_1 + b_1, a_2 + b_2 \in \mathbb{Z}$ So, $(a_1, a_2), (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \in F$.

- Let $(a_1, a_2), (b_1, b_2) \in F$. Using additive commutativity of $\mathbb{R}$

$$\begin{aligned}(a_1, a_2) + (b_1, b_2) &= (a_1 + b_1, a_2 + b_2) \\ &= (b_1 + a_1, b_2 + a_2) \\ &= (b_1, b_2) + (a_1, a_2)\end{aligned}$$

- Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in F$. Using additive associativity of $\mathbb{R}$

$$\begin{aligned}((a_1, a_2) + (b_1, b_2)) + (c_1, c_2) &= (a_1 + b_1, a_2 + b_2) + (c_1, c_2) \\ &= ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2) \\ &= (a_1 + (b_1 + c_1), a_2 + (b_2) + c_2) \\ &= (a_1, a_2) + (b_1 + c_1, b_2 + c_2) \\ &= (a_1, a_2) + ((b_1, b_2) + (c_1, c_2))\end{aligned}$$

- Let $(a_1, a_2) \in F$. We know that for all $c \in \mathbb{R}$, $c + 0 = c$ and $0 + c = c$. So, $(0, 0) + (a_1, a_2) = (0 + a_1, 0 + a_2) = (a_1, a_2)$ and $(a_1, a_2) + (0, 0) = (a_1 + 0, a_2 + 0) = (a_1, a_2)$. Hence, there exists an additive identity in F and it is $(0, 0)$
- Let $(a_1, a_2) \in F$. We know that for all $c \in \mathbb{R}$, there exists a $-c$ such that $c + (-c) = 0$. So, $(a_1, a_2) + (-a_1, -a_2) = (a_1 + (-a_1), a_2 + (-a_2)) = (0, 0)$ and $(-a_1, -a_2) + (a_1, a_2) = (-a_1 + a_1, -a_2 + a_2) = (0, 0)$. Hence, there exists an additive inverse for every element in F.
- Let $(a_1, a_2), (b_1, b_2) \in F$. Since $\mathbb{R}$ is closed under multiplication, $a_1b_1, a_2b_2, a_1b_2, a_2b_1 \in \mathbb{R}$. The sums of these elements are also elements of $\mathbb{R}$ because it is closed under addition as well. So, $(a_1, a_2) \cdot (b_1, b_2) = (a_1b_1 - a_2b_2, a_1b_2 + b_2a_1) \in F$.
- Let $(a_1, a_2), (b_1, b_2) \in F$. Since $\mathbb{R}$ is a field, it has multiplicative and additive commutativity. So,

$$\begin{aligned}(a_1, a_2) \cdot (b_1, b_2) &= (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1) \\ &= (b_1a_1 - b_2a_2, b_1a_2 + b_2a_1) \\ &= (b_1, b_2) \cdot (a_1, a_2)\end{aligned}$$

- Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in F$. Using the field axioms of $\mathbb{R}$,

$$\begin{aligned}((a_1, a_2) \cdot (b_1, b_2)) \cdot (c_1, c_2) &= (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1) \cdot (c_1, c_2) \\ &= ((a_1b_1 - a_2b_2)c_1 - (a_1b_2 + a_2b_1)c_2, \\ &\quad (a_1b_1 - a_2b_2)c_2 + (a_1b_2 + a_2b_1)c_1) \\ &= (a_1b_1c_1 - a_2b_2c_1 - a_1b_2c_2 - a_2b_1c_2, \\ &\quad a_1b_1c_2 - a_2b_2c_2 + a_1b_2c_1 + a_2b_1c_1) \\ &= ((b_1c_1 - b_2c_2)a_1 - (b_1c_2 + b_2c_1)a_1, \\ &\quad (b_1c_1 - b_2c_2)a_2 + (b_1c_2 + b_2c_1)a_1) \\ &= (b_1c_1 - b_2c_2, b_1c_2 + b_2c_2) \cdot (a_1, a_2) \\ &= ((b_1, b_2) \cdot (c_1, c_2)) \cdot (a_1, a_2) \\ &= (a_1, a_2) \cdot ((b_1, b_2) \cdot (c_1, c_2))\end{aligned}$$

- Let $(a_1, a_2) \in F$. $(1, 0)$ is the multiplicative identity in F.
  Proof: $(a_1, a_2) \cdot (1, 0) = (a_1 \cdot 1 - a_2 \cdot 0, a_1 \cdot 0 + a_2 \cdot 1) = (a_1, a_2)$. Using multiplicative commutativity, we know that $(1, 0) \cdot (a_1, a_2) = (a_1, a_2)$ as well.
- Let $(a_1, a_2) \in F$ and assume that $(a_1, a_2) \neq (0, 0)$. The multiplciative inverse of (a_1, a_2) is $(\frac{a_1}{a_1^2+a_2^2}, -\frac{a_2}{a_1^2+a_2^2})$. This is well defined since $a_1 \neq 0$ and $a_2 \neq 0$, so the denominator can never be zero in $\mathbb{R}$
- Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in F$.

$$\begin{aligned}((a_1, a_2) + (b_1, b_2)) \cdot (c_1, c_2) &= (a_1 + b_1, a_2 + b_2) \cdot (c_1, c_2) \\ &\vdots \\ &= (a_1, a_2) \cdot (c_1, c_2) + (b_1, b_2) \cdot (c_1, c_2)\end{aligned}$$

Hence, F is a field.

(b) Let $<$ be an order relation on F. Take $(0, 1) \in F$ and note that $(0, 1) \neq (0, 0)$.

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

Since $(1, 0)$ is the multiplicative identity in F, $(1, 0) > (0, 0)$ by proposition 5.1. Also, notice that $(1, 0) + (-1, 0) = (0, 0)$. This means that $(-1, 0) = -(1, 0)$. By proposition 5.1, $-(1, 0) < 0$ because $(1, 0) > 0$. So, $(0, 1)^2 < 0$. However, by proposition 5.1, the square of any non-zero element in an ordered element must be greater than zero. Hence, this leads to a contradiction. Therefore, there cannot exist an order relation on F.

Problem 5: (a)

- Additive Closure. let $(a_1, a_2), (b_1, b_2) \in R$. Since $\mathbb{Z}$ is closed under addition, we know that $a_1 + b_1, a_2 + b_2 \in \mathbb{R}$. Hence, $(a_1, a_2) + (b_1 + b_2) = (a_1 + b_1, a_2 + b_2) \in F$
- Additive Commutativity. Let $(a_1, a_2), (b_1, b_2) \in R$. $\mathbb{Z}$ has additive commutativity so, $a_1 + b_1 = b_1 + a_1$ and $a_2 + b_2 = b_2 + a_2$. Therefore, $(a_1, b_1) + (a_2, b_2) = (a_1 + b_1, a_2 + b_2) = (b_1 + a_1, b_2 + b_1) = (b_1, b_2) + (a_1, a_2)$
- Additive Associativity. Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in R$. $\mathbb{R}$ has additive associativity, so $(a_1 + b_1) + c_1 = a_1 + (b_1 + c_1)$ and $(a_2 + b_2) + c_2 = a_2 + (b_2 + c_2)$. So,

$$\begin{aligned}((a_1, a_2) + (b_1, b_2)) + (c_1, c_2) &= (a_1 + b_1, a_2 + b_2) + (c_1, c_2) \\ &= ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2) \\ &= (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2)) \\ &= (a_1, a_2) + (b_1 + c_1, b_2 + c_2) \\ &= (a_1, a_2) + ((b_1, b_2) + (c_1, c_2))\end{aligned}$$

- Additive Identity. Let $(a_1, a_2) \in R$. We know that for all $x \in \mathbb{Z}$ that $x + 0 = x$. So, $(0, 0)$ is the additive identity in F since $(a_1, a_2) + (0, 0) = (a_1 + 0, a_2 + 0) = (a_1, a_2)$.
- Additive Inverse. Let $(a_1, a_2) \in R$. We know that for all $x \in \mathbb{Z}$ there exists a $-x$ such that $0 = x + (-x)$. So, the additive inverse of (a_1, a_2) is $(-a_1, -a_2)$.
- Multiplicative Closure. Let $(a_1, a_2), (b_1, b_2) \in R$. Since $\mathbb{R}$ is a field, $a_1b_1, a_2b_2, a_1b_2, a_2b_1 \in \mathbb{R}$ and any of their sums are also in $\mathbb{R}$.
  So, $a_1b_1 + 2a_2b_2, a_1b_2 + a_2b_1 \in \mathbb{Z}$. Thus, $(a_1, a_2) \cdot (b_1, b_2) = (a_1b_1 + 2a_1b_2, a_1b_2 + a_2b_1) \in F$.
- Multiplciative Commutativity. Let $(a_1, a_2), (b_1, b_2) \in R$. Using the commutativity of addition and multiplication in $\mathbb{Z}$, we know that $a_1b_1 + 2a_2b_2 = b_1a_1 + 2b_2a_2$ and $a_1b_2 + b_1a_2 = b_1a_2 + b_2a_1$. So,

$$\begin{aligned}(a_1, a_2) \cdot (b_1, b_2) &= (a_1b_1 + 2a_2b_2, a_1b_2 + b_1a_2) \\ &= (b_1a_1 + 2b_2a_2, b_1a_2 + b_2a_1) \\ &= (b_1, b_2) \cdot (a_1, a_2)\end{aligned}$$

- Multiplicative Associativity. Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in R$. Using the fact that $\mathbb{Z}$ is a ring, we can use the properties to expand $((a_1, a_2) \cdot (b_1, b_2)) \cdot (c_1, c_2)$ to show that it is equal to $(a_1, a_2) \cdot ((b_1, b_2) \cdot (c_1, c_2))$
- Distributivity. Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in R$. Similarly, we can use the axioms of $\mathbb{Z}$ being a ring to show that $((a_1, a_2)+(b_1, b_2)) \cdot (c_1, c_2) = (a_1, a_2) \cdot (c_1, c_2) + (b_1, b_2) \cdot (c_1, c_2)$.

(b)

- Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in R$. Assume that $(a_1, a_2) < (b_1, b_2)$. We want to show that $(a_1, a_2) + (c_1, c_2) < (b_1, b_2) + (c_1, c_2)$.
  By definition of the order relation, we know that $a_1 + a_2\sqrt{2} < b_1 + b_2\sqrt{2}$. Using the order relation of $\mathbb{R}$, we also know that for all $x \in \mathbb{R}$,

$$a_1 + a_2\sqrt{2} + x < b_1 + b_2\sqrt{2} + x$$

  Note that $c_1 + c_2\sqrt{2} \in \mathbb{R}$. So,

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

- Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in R$. Assume that $(a_1, a_2) < (b_1, b_2)$ and that $(c_1, c_2) > (0, 0)$. This means that $a_1 + a_2\sqrt{2} < b_1 + b_2\sqrt{2}$ and $c_1 + c_2\sqrt{2} > 0$.
  Multiplying (c_1, c_2), we get

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

We want to show that

$$(a_1c_1 + 2a_2c_2) + (a_1c_2 + a_2c_1)\sqrt{2} < (b_1c_1 + 2b_2c_2) + (b_1c_2 + b_2c_1)\sqrt{2}$$

With the use of associativity, commutativity, and distributivity in $\mathbb{R}$, we find that

$$(a_1c_1 + 2a_2c_2) + (a_1c_2 + a_2c_1)\sqrt{2} = (a_1 + a_2\sqrt{2})(c_1 + c_2\sqrt{2})$$
$$(b_1c_1 + 2b_2c_2) + (b_1c_2 + b_2c_1)\sqrt{2} = (b_1 + b_2\sqrt{2})(c_1 + c_2\sqrt{2})$$

By assumption we know that $a_1+a_2\sqrt{2} < b_1+b_2\sqrt{2}$ and $c_1+c_2\sqrt{2} > 0$. So, using the order relation on $\mathbb{R}$, we know that

$$(a_1 + a_2\sqrt{2})(c_1 + c_2\sqrt{2}) < (b_1 + b_2\sqrt{2})(c_1 + c_2\sqrt{2})$$

Therefore,

$$(a_1c_1 + 2a_2c_2) + (a_1c_2 + a_2c_1)\sqrt{2} < (b_1c_1 + 2b_2c_2) + (b_1c_2 + b_2c_1)\sqrt{2}$$

and $<$ is an order relation on R.

Problem 6: Let S be a nonempty subset of $\mathbb{R}$.

(a) Using the definitions of both, we know that $\inf S \leq s \leq \sup S$ for all $s \in S$.

Since S is nonempty, there exists at least one element $s \in S$. Therefore, $\inf S \leq s \leq \sup S$ holds for at least one $s \in S$.

Therefore, by transitivity $\inf S \leq \sup S$.

(b) Assume that $\inf S = \sup S$.

We know that $\inf S \leq s \leq \sup S$ for all $s \in S$. Substituting the asusmption, $\sup S \leq s \leq \sup S$. Since, S is non empty, $s = \sup S = \inf S$. Hence, $S = \{\sup S\}$

Problem 7: Let S and T be two non-empty bounded subsets of $\mathbb{R}$.

(a) Assume that $S \subseteq T$. From question 6, we know that $\inf S \leq \sup S$ and $\inf T \leq \sup T$, so it is sufficient to show that $\inf T \leq \inf S$ and $\sup S \leq \sup T$.

Since $S \subseteq T$, we know that for all $s \in S$, $s \in T$. So, $\inf T \leq s$ for all $s \in S$. Therefore, $\inf T$ is a lower bound for S. By definition, $\inf S$ is the greatest lower bound of S, so $\inf S \geq \inf T$.

Similarly, we can apply the definition of $\sup S$ and the greatest upper bound to show that $\sup S \leq \sup T$.

Therefore, $\inf T \leq \inf S \leq \sup S \leq \sup T$.

(b) Let $m = \max\{\sup S, \sup T\}$. Then $\sup S \leq m$ and $\sup T \leq m$. So for all $x \in S$, $x \leq \sup S \leq m$, and for all $x \in T$, $x \leq \sup T \leq m$. Hence, for all $y \in S \cup T$, $y \leq m$. Therefore, m is an upper bound for $S \cup T$.

Assume that $m = \sup S$ (the same can be done with $\sup T$). Then, $\sup T \leq \sup S = m$. Assume that l is a lower bound of $S \cup T$ and $l < m$. Then d would be an an upper bound of S, and $l < \sup S$. However, this is a contradiction because $\sup S$ is the least upper bound of S. Thus, there cannot exist an upper bound of $S \cup T$ less than m. Therefore, $\max\{\sup S, \sup T\} = \sup(S \cup T)$

Problem 8: Let A be a nonempty subset of $\mathbb{R}$ which is bounded below and let $-A = \{-a \colon a \in A\}$

- We know that $\inf A \leq a$ for all $a \in A$. So, $-\inf A \geq -a$, for all $a \in A$. In other words, $-infA \geq b$, for all $b \in -A$. Thus, $-\inf A$ is an upper bound for $-A$.
- We want to show that $-infA$ is the least upper bound. Assume that there exists an l such that l is an upper bound for $-A$ and $l < -\inf A$. Then, for all $b \in -A$, $l \geq b$ and $-l \leq -b$. Note that $-(-A) = A$ and that $\inf A < l$. So, l is a lower bound for A. However, this leads to a contradiction, because $\inf A$ is the greatest lower bound of A. Therefore, there cannot exist an upper bound l of $-A$ that is lesser than $-\inf A$. Therefore, $-\inf A = \sup -A$ and $\inf A = -\sup -A$.