Problem Set 2

Math 255: Analysis I

Due: Thursday, Feb 1st at 11:59pm EST

Problem 1.

1. Using the Peano axioms and our subsequent definitions of addition and multiplication on $\mathbb{N}$ prove: Note that by lemma proved in class, we can induct on $\mathbb{N}_0$ instead of $\mathbb{N}$ for the following proofs.

   (a) Commutativity of addition, $\forall a, b \in \mathbb{N} \quad a + b = b + a$.

   Proof. We will prove by induction on a.
   Base Case: Consider $a = 0$.

$$\begin{aligned} a + b &= 0 + b \\ &= b && \text{(by definition of addition)} \\ &= b + 0 && \text{(proven earlier through induction in class)} \\ &= b + a \end{aligned}$$

   Thus, the base case holds since $a + b = b + a$.
   Inductive Step: Assume the statement is true for some natural number a, i.e., $a + b = b + a$. We need to show it holds for $S(a)$.

$$\begin{aligned} S(a) + b &= S(a + b) && \text{(by definition of addition)} \\ &= S(b + a) && \text{(by the inductive hypothesis)} \\ &= b + S(a) && \text{(proven earlier through induction in class)} \end{aligned}$$

   Therefore, the inductive case also holds, completing the proof. □

   (b) Associativity of addition. $\forall a, b, c \in \mathbb{N} \quad (a + b) + c = a + (b + c)$.

   Proof. We will prove this by induction on a.
   Base Case: Consider $a = 0$.

$$\begin{aligned} (a + b) + c &= (0 + b) + c \\ &= b + c && \text{(by definition of addition)} \\ &= 0 + (b + c) && \text{(by definition of addition)} \\ &= a + (b + c) && \text{(since } a = 0) \end{aligned}$$

   Thus, the base case holds.
   Inductive Step: Assume the statement is true for some natural number a, i.e., $(a + b) + c = a + (b + c)$. We need to show it holds for $S(a)$. Consider $(S(a) + b) + c$.

$$\begin{aligned} (S(a) + b) + c &= S(a + b) + c && \text{(by the definition of addition)} \\ &= S((a + b) + c) && \text{(by the definition of addition)} \\ &= S(a + (b + c)) && \text{(by the inductive hypothesis)} \\ &= S(a) + (b + c) && \text{(by the definition of addition)} \end{aligned}$$

   Therefore, the inductive step holds, completing the proof. □

   (c) Commutativity of multiplication. $\forall a, b \in \mathbb{N} \quad a \times b = b \times a$.

Proof. We will prove this by induction on a.
Base Case: Consider $a = 0$.

$$\begin{aligned}
a \times b &= 0 \times b \\
&= 0 && \text{(by definition of multiplication)} \\
b \times a &= b \times 0 \\
&= 0 && \text{(we will prove this below)}
\end{aligned}$$

We will prove $b \times 0 = 0$ by induction on b.
Base Case': Consider $b = 0$.

$$\begin{aligned}
b \times 0 &= 0 \times 0 \\
&= 0 && \text{(by definition of multiplication)}
\end{aligned}$$

Inductive Step': Assume the statement is true for some natural number b, i.e., $b \times 0 = 0$. We need to show it holds for $S(b)$.

$$\begin{aligned}
S(b) \times 0 &= b \times 0 + 0 \\
&= 0 + 0 && \text{(by the inductive hypothesis)} \\
&= 0 && \text{(by definition of addition)}
\end{aligned}$$

Therefore, the base case holds.
Inductive Step: Assume the statement is true for some natural number a, i.e., $a \times b = b \times a$. We need to show it holds for $S(a)$. Consider $S(a) \times b$.

$$\begin{aligned}
S(a) \times b &= (a \times b) + b && \text{(by definition of multiplication)} \\
&= (b \times a) + b && \text{(by the inductive hypothesis)} \\
&= b \times S(a) && \text{(we will prove this below)}
\end{aligned}$$

We will prove $(b \times a) + b = b \times S(a)$ by induction on b.
Base Case": Consider $b = 0$.

$$\begin{aligned}
(b \times a) + b &= (0 \times a) + 0 \\
&= 0 + 0 && \text{(by definition of multiplication)} \\
&= 0 && \text{(by definition of addition)} \\
&= 0 \times S(a) && \text{(by definition of multiplication)} \\
&= b \times S(a)
\end{aligned}$$

Inductive Step": Assume the statement is true for some natural number b, i.e., $(b \times a) + b = b \times S(a)$. We need to show it holds for $S(b)$.

$$\begin{aligned}
(S(b) \times a) + S(b) &= ((b \times a) + a) + S(b) && \text{(by definition of multiplication)} \\
&= S(b) + ((b \times a) + a) && \text{(by commutativity of addition)} \\
&= S(b + ((b \times a) + a)) && \text{(by definition of addition)} \\
&= S((b + (b \times a)) + a) && \text{(by associativity of addition)} \\
&= S(b + (b \times a)) + S(a) && \text{(by definition of addition)} \\
&= S((b \times a) + b) + S(a) && \text{(by commutativity of addition)} \\
&= S(b \times S(a)) + S(a) && \text{(by the inductive hypothesis)} \\
&= S(b) \times S(a) && \text{(by definition of multiplication)}
\end{aligned}$$

Therefore, the inductive step holds, completing the proof.

$\square$

(d) Associativity of multiplication. $\forall a, b, c \in \mathbb{N}$, $(a \times b) \times c = a \times (b \times c)$.

Before we prove associativity of multiplication, we will first prove distributivity holds in $\mathbb{N}$, i.e. that $\forall a, b, c \in \mathbb{N}$, $(a + b) \times c = (a \times c) + (b \times c)$.

Proof. We will prove this by induction on a.
Base Case: Consider $a = 0$.

$$\begin{aligned}
(a + b) \times c &= (0 + b) \times c \\
&= b \times c && \text{(by definition of addition)} \\
&= 0 + (b \times c) && \text{(by definition of addition)} \\
&= (0 \times c) + (b \times c) && \text{(by definition of multiplication)}
\end{aligned}$$

Inductive Step: Assume the statement is true for some natural number a, i.e., $(a + b) \times c = (a \times c) + (b \times c)$. We need to show it holds for $S(a)$.

$$\begin{aligned}
(S(a) + b) \times c &= S(a + b) \times c && \text{(by definition of addition)} \\
&= ((a + b) \times c) + c && \text{(by definition of multiplication)} \\
&= ((a \times c) + (b \times c)) + c && \text{(by the inductive hypothesis)} \\
&= ((a \times c) + c) + (b \times c) && \text{(by asso. and comm. of addition)} \\
&= (S(a) \times c) + (b \times c) && \text{(by definition of multiplication)}
\end{aligned}$$

Therefore, the inductive step holds, completing the proof. □

No we return to the proof of associativity of multiplication.

Proof. We will prove this by induction on a.
Base Case: Consider $a = 0$.

$$\begin{aligned}
(a \times b) \times c &= (0 \times b) \times c \\
&= 0 \times c && \text{(by definition of multiplication)} \\
&= 0 && \text{(by definition of multiplication)} \\
&= 0 \times (b \times c) && \text{(by definition of multiplication)} \\
&= a \times (b \times c) && \text{(since } a = 0\text{)}
\end{aligned}$$

Inductive Step: Assume the statement is true for some natural number a, i.e., $(a \times b) \times c = a \times (b \times c)$. We need to show it holds for $S(a)$.

$$\begin{aligned}
(S(a) \times b) \times c &= ((a \times b) + b) \times c && \text{(by definition of multiplication)} \\
&= ((a \times b) \times c) + (b \times c) && \text{(by distributivity in } \mathbb{N}\text{)} \\
&= (a \times (b \times c)) + (b \times c) && \text{(by the inductive hypothesis)} \\
&= S(a) \times (b \times c) && \text{(by definition of multiplication)}
\end{aligned}$$

□

Note that we have assumed $\forall a, b \in \mathbb{N}$, $a \times b \in \mathbb{N}$ in our application of distributivity. We will prove that addition and multiplication are well defined in $\mathbb{N}$, i.e. $\forall a, b \in \mathbb{N}$, $a + b \in N$ and $a \times b \in \mathbb{N}$.

Proof. We will prove that addition and multiplication are well defined in $\mathbb{N}$ by induction on a. First, addition.
Base Case: Consider $a = 0$.

$$\begin{aligned}
a + b &= 0 + b \\
&= b && \text{(by definition of addition)} \\
&\in \mathbb{N} && \text{(since } b \in \mathbb{N}\text{)}
\end{aligned}$$

Inductive Step: Assume the statement is true for some natural number a, i.e., $a + b \in \mathbb{N}$. We need to show it holds for $S(a)$.

$$\begin{aligned} S(a) + b &= S(a + b) && \text{(by definition of addition)} \\ &\in \mathbb{N} && (a + b \in \mathbb{N} \text{ by inductive step and Peano Axiom (II)}) \end{aligned}$$

Therefore, addition is well defined in $\mathbb{N}$.
Now, multiplication.
Base Case: Consider $a = 0$.

$$\begin{aligned} a \times b &= 0 \times b \\ &= 0 && \text{(by definition of multiplication)} \\ &\in \mathbb{N} && (\text{since } 0 \in \mathbb{N}\text{, in this case } \mathbb{N}_0\text{, but can treat the same because of lemma in class}) \end{aligned}$$

Inductive Step: Assume the statement is true for some natural number a, i.e., $a \times b \in \mathbb{N}$. We need to show it holds for $S(a)$.

$$\begin{aligned} S(a) \times b &= (a \times b) + b && \text{(by definition of multiplication)} \\ &\in \mathbb{N} && (a \times b \in \mathbb{N} \text{ by inductive step and addition well-defined}) \end{aligned}$$

Therefore, multiplication is well defined in $\mathbb{N}$. □

2. Using our formal construction of $\mathbb{Z}$ from $\mathbb{N}$ and the subsequent definition of addition on $\mathbb{Z}$ - prove the commutativity of addition in $\mathbb{Z}$.

   Proof. We will prove that $\forall [n - m], [k - l] \in \mathbb{Z}$, $[n - m] + [k - l] = [k - l] + [n - m]$.

$$\begin{aligned} [n - m] + [k - l] &= [(n + k) - (m + l)] && \text{(by definition of addition on } \mathbb{Z}) \\ &= [(k + n) - (l + m)] && \text{(by commutativity of addition in } \mathbb{N}) \\ &= [k - l] + [n - m] && \text{(by definition of addition on } \mathbb{Z}) \end{aligned}$$

   Therefore, the commutativity of addition in $\mathbb{Z}$ holds. □

3. Using our formal construction of $\mathbb{Q}$ from $\mathbb{Z}$ and the subsequent definition of addition on $\mathbb{Z}$ - prove the commutativity of addition in $\mathbb{Q}$.[1]

   Proof. Before proving the commutativity of addition in $\mathbb{Q}$, we will prove the commutativity of multiplication in $\mathbb{Z}$. We will prove that $\forall [n - m], [k - l] \in \mathbb{Z}$, $[n - m] \times [k - l] = [k - l] \times [n - m]$.

$$\begin{aligned} [n - m] \times [k - l] &= [(n \times k + m \times l) - (m \times k + n \times l)] && \text{(by definition of multiplication on } \mathbb{Z}) \\ &= [(k \times n + l \times m) - (k \times m + l \times n)] && \text{(by commutativity of multiplication in } \mathbb{N}) \\ &= [(k \times n + l \times m) - (l \times n + k \times m)] && \text{(by commutativity of addition in } \mathbb{N}) \\ &= [k - l] \times [n - m] && \text{(by definition of multiplication on } \mathbb{Z}) \end{aligned}$$

   □

   Proof. We will prove that $\forall [p//q], [r//s] \in \mathbb{Q}$, $[p//q] + [r//s] = [r//s] + [p//q]$.

$$\begin{aligned} [p//q] + [r//s] &= [(p \times s + q \times r)//q \times s] && \text{(by definition of addition on } \mathbb{Q}) \\ &= [(r \times q + s \times p)//q \times s] && \text{(by commutativity of addition in } \mathbb{Z}) \\ &= [(r \times q + s \times p)//s \times q] && \text{(by commutativity of multiplication in } \mathbb{Z}) \\ &= [r//s] + [p//q] && \text{(by definition of addition on } \mathbb{Q}) \end{aligned}$$

   Therefore, the commutativity of addition in $\mathbb{Q}$ holds. □

[1] Try to convince yourselves that one can indeed prove all the properties of a field on $\mathbb{Q}$ using our constructions.

Problem 2. Using induction on $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ and the definition of addition prove the following:

1. Cancellation law: $\forall n, m, k \in \mathbb{N}_0$ if $n + k = n + m$ then $k = m$.

   Proof. We will prove this by induction on n.

   Base Case: Consider $n = 0$.

   $$\begin{aligned} n + k = n + m &\implies 0 + k = 0 + m \\ &\implies k = m && \text{(by definition of addition)} \end{aligned}$$

   Thus, the base case holds.

   Inductive Step: Assume the statement is true for some natural number n, i.e., $n+k = n+m$ implies $k = m$. We need to show it holds for $S(n)$.

   $$\begin{aligned} S(n) + k = S(n) + m &\implies S(n + k) = S(n + m) && \text{(by definition of addition)} \\ &\implies S(k) = S(m) && \text{(by the inductive hypothesis)} \\ &\implies k = m && \text{(by Peano Axiom (IV), i.e., } S \text{ is surjective)} \end{aligned}$$

   Therefore, the inductive step holds, completing the proof. □

2. If $k_1, k_2 \in \mathbb{N}_0$ satisfy $k_1 + k_2 = 0$ then $k_1 = k_2 = 0$.

   Proof. We will prove the contrapositive statement: If $k_1 \neq 0$ or $k_2 \neq 0$, then $k_1 + k_2 \neq 0$.

   Suppose, for the sake of contradiction, that $k_1 \neq 0$ or $k_2 \neq 0$ and $k_1 + k_2 = 0$. Without loss of generality, assume $k_1 \neq 0$. This means k_1 is a successor of some number in $\mathbb{N}_0$, say $k_1 = S(p)$ for some $p \in \mathbb{N}_0$.

   By the definition of addition:

   $$k_1 + k_2 = S(p) + k_2 = S(p + k_2)$$

   Since $S(p)$ is the successor of p, $S(p+k_2)$ cannot be 0 by the properties of natural numbers (specifically, no natural number's successor is 0).

   Hence, $k_1 + k_2 = S(p + k_2) \neq 0$, which contradicts our assumption. Therefore, if $k_1 + k_2 = 0$, it must be the case that $k_1 = k_2 = 0$. □

Problem 3. Recall that for all $n, m \in \mathbb{N}_0$ we defined $n < m$ if and only if $m = n + k$ for some $k \in \mathbb{N}$. Prove that $\mathbb{N}_0$ with this relation is an ordered set, i.e. prove:

1. Trichotomy: $\forall n, m \in \mathbb{N}_0$ **exactly one** of the following holds

$$n < m \quad \text{or} \quad n = m \quad \text{or} \quad m < n.$$

Proof. We consider the following cases:

- If $n = m$, then neither $n < m$ nor $m < n$ can be true by the definition of $<$ in $\mathbb{N}_0$.
- If $n < m$, i.e., $m = n + k$ for some $k \in \mathbb{N}$, then $n \neq m$ and $m \neq n + k'$ for any $k' \in \mathbb{N}$, hence $m < n$ cannot be true.
- Similarly, if $m < n$, then neither $n < m$ nor $n = m$ can be true.

Thus, exactly one of $n < m$, $n = m$, or $m < n$ holds for any $n, m \in \mathbb{N}_0$. □

2. Transitivity: $\forall n, m, k \in N_0$ if $n \leq m$ and $m \leq k$ then $n \leq k$.

Proof. We consider the following cases:

- If $n = m$ and $m = k$, then clearly $n = k$.
- If $n = m$ and $m < k$, i.e., $k = m + r$ for some $r \in \mathbb{N}$, then $k = n + r$, implying $n < k$.
- If $n < m$ and $m = k$, i.e., $m = n + q$ for some $q \in \mathbb{N}$, then $k = n + q$, implying $n < k$.
- If $n < m$ and $m < k$, i.e., $m = n + q$ and $k = m + r$ for some $q, r \in \mathbb{N}$, then $k = n + q + r$. Since $q + r \in \mathbb{N}$, we have $n < k$.

In all cases, $n \leq k$. □

Problem 4.

1. Prove that $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, together with the usual addition and multiplication operations, is a field.

   Proof. For any two elements $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we define addition and multiplication as follows:

$$
\begin{aligned}
(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \\
(a + b\sqrt{2}) \times (c + d\sqrt{2}) &= (ac + 2(bd)) + (ad + bc)\sqrt{2}
\end{aligned}
$$

   Note: We will use the shorthand for multiplication in $\mathbb{Q}$, i.e., $a \times b = ab$.

   We will prove that $\mathbb{Q}(\sqrt{2})$ is a field by showing that it satisfies all the properties of a field.

   Commutativity of addition: $\forall a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have

$$
\begin{aligned}
(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} && \text{(by definition of addition)} \\
&= (c + a) + (d + b)\sqrt{2} && \text{(by commutativity of addition in } \mathbb{Q}) \\
&= (c + d\sqrt{2}) + (a + b\sqrt{2}) && \text{(by definition of addition)}
\end{aligned}
$$

   Associativity of addition: $\forall a + b\sqrt{2}, c + d\sqrt{2}, e + f\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have

$$
\begin{aligned}
&((a + b\sqrt{2}) + (c + d\sqrt{2})) + (e + f\sqrt{2}) \\
&= ((a + c) + (b + d)\sqrt{2}) + (e + f\sqrt{2}) && \text{(by def. of add.)} \\
&= ((a + c) + e) + ((b + d) + f)\sqrt{2} && \text{(by def. of add.)} \\
&= (a + (c + e)) + (b + (d + f))\sqrt{2} && \text{(by asso. of addition in } \mathbb{Q}) \\
&= (a + b\sqrt{2}) + ((c + e) + (d + f)\sqrt{2}) && \text{(by def. of add.)} \\
&= (a + b\sqrt{2}) + ((c + d\sqrt{2}) + (e + f\sqrt{2})) && \text{(by def. of add.)}
\end{aligned}
$$

   Existence of neutral element for addition: $\exists 0 + 0\sqrt{2} \in \mathbb{F} \colon \forall a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have

$$
\begin{aligned}
(a + b\sqrt{2}) + (0 + 0\sqrt{2}) &= (a + 0) + (b + 0)\sqrt{2} && \text{(by definition of addition)} \\
&= a + b\sqrt{2} && \text{(by } \mathbb{Q} \text{ is field, add. neutral element)}
\end{aligned}
$$

   Existence of additive inverse: $\forall a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have

$$
\begin{aligned}
(a + b\sqrt{2}) + ((-a) + (-b)\sqrt{2}) &= (a + (-a)) + (b + (-b))\sqrt{2} && \text{(by definition of addition)} \\
&= 0 + 0\sqrt{2} && \text{(by } \mathbb{Q} \text{ is field, additive inverse)} \\
&= 0 && \text{(by definition of addition in } \mathbb{Q})
\end{aligned}
$$

   Commutativity of multiplication: $\forall a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have

$$
\begin{aligned}
(a + b\sqrt{2}) \times (c + d\sqrt{2}) &= (ac + 2(bd)) + (ad + bc)\sqrt{2} && \text{(by definition of multiplication)} \\
&= (ca + 2(db)) + (da + cb)\sqrt{2} && \text{(by commutativity of multiplication in } \mathbb{Q}) \\
&= (ca + 2(db)) + (cb + da)\sqrt{2} && \text{(by commutativity of addition in } \mathbb{Q}) \\
&= (c + d\sqrt{2}) \times (a + b\sqrt{2}) && \text{(by definition of multiplication)}
\end{aligned}
$$

Associativity of multiplication: $\forall a+b\sqrt{2}, c+d\sqrt{2}, e+f\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have

$$\begin{aligned}
&((a+b\sqrt{2}) \times (c+d\sqrt{2})) \times (e+f\sqrt{2}) \\
&= ((ac+2(bd)) + (ad+bc)\sqrt{2}) \times (e+f\sqrt{2}) && \text{(by def. of multi.)} \\
&= ((ac+2bd)e + 2(ad+bc)f) + ((ac+2(bd))f + (ad+bc)e)\sqrt{2} && \text{(by def. of multi.)} \\
&= (ace+2bde+2adf+2bcf) + (acf+2bdf+ade+bce)\sqrt{2} && \text{(by distr. in } \mathbb{Q}\text{, field)} \\
&= (ace+2adf+2bde+2bcf) + (acf+ade+bce+2bdf)\sqrt{2} && \text{(by comm. of add. in } \mathbb{Q}\text{)} \\
&= (a(ce+2(df)) + 2b(cf+de)) + (a(cf+de) + b(ce+2(df)))\sqrt{2} && \text{(by distr. in } \mathbb{Q}\text{, field)} \\
&= (a+b\sqrt{2}) \times ((ce+2(df)) + (cf+de\sqrt{2})) && \text{(by def. of multi.)} \\
&= (a+b\sqrt{2}) \times ((c+d\sqrt{2}) \times (e+f\sqrt{2})) && \text{(by def. of multi.)}
\end{aligned}$$

Existence of neutral element for multiplication: $\exists 1+0\sqrt{2} \in \mathbb{F}$: $\forall a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have

$$\begin{aligned}
(a+b\sqrt{2}) \times (1+0\sqrt{2}) &= (a \times 1 + 2b \times 0) + (a \times 0 + b \times 1)\sqrt{2} && \text{(by definition of multiplication)} \\
&= a+b\sqrt{2} && \text{(by definition of multiplication in } \mathbb{Q}\text{)}
\end{aligned}$$

Existence of multiplicative inverse: $\forall a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have

$$\begin{aligned}
&(a+b\sqrt{2}) \times \left(\frac{a}{a^2-2b^2} + \left(-\frac{b}{a^2-2b^2}\right)\sqrt{2}\right) \\
&= \left(a\frac{a}{a^2-2b^2} + 2\left(b\left(-\frac{b}{a^2-2b^2}\right)\right)\right) + \left(a\left(-\frac{b}{a^2-2b^2}\right) + b\frac{a}{a^2-2b^2}\right)\sqrt{2} \\
&\text{(by definition of multiplication)} \\
&= \left(\frac{a^2}{a^2-2b^2} + \frac{-2b^2}{a^2-2b^2}\right) + \left(\frac{-ab}{a^2-2b^2} + \frac{ab}{a^2-2b^2}\right)\sqrt{2} \\
&\text{(by definition of multiplication in } \mathbb{Q}\text{)} \\
&= \frac{a^2-2b^2}{a^2-2b^2} + 0\sqrt{2} \\
&\text{(by definition of addition in } \mathbb{Q}\text{)} \\
&= 1 \\
&\text{(by definition of multiplication in } \mathbb{Q}\text{)}
\end{aligned}$$

Distributivity of multiplication over addition: $\forall a+b\sqrt{2}, c+d\sqrt{2}, e+f\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have

$$\begin{aligned}
&(a+b\sqrt{2}) \times ((c+d\sqrt{2}) + (e+f\sqrt{2})) \\
&= (a+b\sqrt{2}) \times ((c+e) + (d+f)\sqrt{2}) && \text{(by definition of addition)} \\
&= (a(c+e) + 2b(d+f)) + (a(d+f) + b(c+e))\sqrt{2} && \text{(by definition of multiplication)} \\
&= (ac+ae+2bd+2bf) + (ad+af+bc+be)\sqrt{2} && \text{(by distributivity in } \mathbb{Q}\text{)} \\
&= (ac+ae+2bd+2bf) + (ad+bc)\sqrt{2} + (bc+be)\sqrt{2} && \text{(by distributivity in } \mathbb{Q}\text{)} \\
&= (ac+2bd) + (ad+bc)\sqrt{2} + (ae+2bf) + (af+be)\sqrt{2} && \text{(by asso., comm., in } \mathbb{Q}\text{)} \\
&= (a+b\sqrt{2}) \times (c+d\sqrt{2}) + (a+b\sqrt{2}) \times (e+f\sqrt{2}) && \text{(by definition of multiplication)}
\end{aligned}$$

Therefore, $\mathbb{Q}(\sqrt{2})$ is a field.

$\square$

2. Verify that in $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ together with multiplication mod 5, every non-zero element has a multiplicative inverse.[2]

   Proof. Here is the multiplication mod 5 table for $\mathbb{F}_5$:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

   We can see that every non-zero element has a multiplicative inverse, i.e., $1 \cdot 1 = 1$, $2 \cdot 3 = 1$, $3 \cdot 2 = 1$, and $4 \cdot 4 = 1$. $\square$

[2] This is indeed a field.

Problem 5.

1. Let $\mathbb{F}$ be any field and let $x, y \in \mathbb{F}$. Prove that if $x \cdot y = 0$ then $x = 0$ or $y = 0$.

   Proof. Suppose, towards a contradiction, that both $x \neq 0$ and $y \neq 0$. In a field $\mathbb{F}$, every non-zero element has a multiplicative inverse. Thus, there exist elements x^{-1} and y^{-1} in $\mathbb{F}$ such that $x \cdot x^{-1} = 1$ and $y \cdot y^{-1} = 1$.

   Multiply both sides of the equation $x \cdot y = 0$ by x^{-1} on the left and y^{-1} on the right:

   $$x^{-1} \cdot (x \cdot y) \cdot y^{-1} = x^{-1} \cdot 0 \cdot y^{-1}.$$

   Using the associativity of multiplication in fields, we have:

   $$(x^{-1} \cdot x) \cdot y \cdot y^{-1} = 0.$$

   Substituting the identity elements, we get:

   $$1 \cdot y \cdot y^{-1} = 0.$$

   $$1 \cdot 1 = 0.$$

   $$1 = 0.$$

   This is a contradiction because in a field, the identity elements for addition and multiplication are distinct. Therefore, either $x = 0$ or $y = 0$. □

2. Let $\mathbb{F}_m = \{0, 1, 2, ..., m-1\}$ together with addition and multiplication mod m. Prove that if m is not prime then $\mathbb{F}_m$ is not a field.

   Proof. Suppose, towards a contradiction, that $\mathbb{F}_m$ is a field and m not prime. Then there exist $x, y \in \mathbb{F}_m$ such that $x \neq 0$, $y \neq 0$, and $a \cdot b = m \mod m = 0$. By Problem 5.1, this implies that $x = 0$ or $y = 0$, which is a contradiction. Therefore, $\mathbb{F}_m$ is not a field. □

Problem 6. Let S be an ordered set and let A and B be two subsets of S. Prove the following:

1. If A has a maximum then it also has a supremum and $\sup A = \max A$.

   Proof. Let $\max A = m$ be the maximum element of A. By definition, for all $a \in A$, $a \leq m$. To show m is the supremum of A, we must prove that m is an upper bound of A and that any other upper bound of A is greater than or equal to m.

   Since m is the maximum, it is an upper bound of A (no element in A is greater than m). Now suppose there is another upper bound u of A. Since $m \in A$ and u is an upper bound, it must be that $m \leq u$.

   Therefore, m is the least upper bound or supremum of A, and hence $\sup A = \max A$. $\square$

2. Assume there exists a supremum for A in S and a supremum for B in S. If for all $a \in A$ there exists $b \in B$ satisfying $a \leq b$ then $\sup A \leq \sup B$.

   Proof. Let $\sup A = s_A$ and $\sup B = s_B$. By assumption, for each $a \in A$, there exists a $b \in B$ such that $a \leq b$. Since s_B is an upper bound of B, it must be that $b \leq s_B$ for all $b \in B$. Combining these inequalities, we have $a \leq b \leq s_B$ for all $a \in A$. (By transitivity of order, shown in problem 3, part 2.)

   This means s_B is an upper bound of A. Since s_A is the least upper bound of A, it follows that $s_A \leq s_B$. $\square$

3. Assume as in (2) that $\sup A, \sup B$ exist and assume further that for all $a \in A$ there exists $b \in B$ satisfying $a < b$. Does this necessarily mean that $\sup A < \sup B$?

   Proof. No, consider the following counterexample. Let $A = \{\frac{n}{n+1} : n \in \mathbb{N}\}$ and $B = \{\frac{n}{n+1} : n \in \mathbb{N}\} \cup \{1\}$. Then for all $a \in A$, there exists $b \in B$ such that $a < b$, i.e. $1 \in B$. However, $\sup A = \sup B = 1$. $\square$