The most first numbers every considered were the whole numbers:

1, 2, 3, ...
The most first numbers every considered were the whole numbers:

$$1, 2, 3, \ldots$$

Then someone realized that it was important to include a number representing “nothing”. This then gave us the natural numbers:

$$\mathbb{N} = 1, 2, 3, \ldots$$
Then people noticed that addition worked better if there were negative numbers. This led us to the integers

$$\mathbb{Z} = \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$
Then people noticed that addition worked better if there were negative numbers. This led us to the integers

\[ \mathbb{Z} = \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \]

After dealing with the integers for a while people began to notice the usefulness of fractions and the rational numbers were born:

\[ \mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \right\} \]
Square Root of Two

What is next...?
Square Root of Two

What is next...?

Theorem

*There is no rational number* $p$ *such that* $p^2 = 2$. 
Definition of a Set

Definition
A set is a collection of objects. If a set has at least one element we say it is *non-empty*. If a set has no objects we say it is *empty*.

Definition
Suppose $A$ is a set
- If $x$ is a member of $A$ we write $x \in A$.
- If $x$ is not a member of $A$ we write $x \notin A$. 
Definition of a Set

Suppose $A$ and $B$ are sets

- If every element of $A$ is an element of $B$ we say $A$ is a subset of $B$ and write $A \subseteq B$ or $B \supseteq A$.
- If $A$ is a subset of $B$ and not equal to $B$ we say $A$ is a proper subset of $B$.
- If $A \subseteq B$ and $B \subseteq A$ then we say the sets are equal and write $A = B$. 
Ordered Sets

Definition

Let $S$ be a set. An order on $S$ is a relation, denoted by $<$, such that the following two properties hold

(i) If $x \in S$ and $y \in S$ then one and only one of the following is true

- $x < y$
- $x = y$
- $y < x$

(ii) For all $x, y, z \in S$, if $x < y$ and $y < z$ then $x < z$
Definition

An *ordered set* is a set $S$ in which an order is defined.

Definition

If $S$ is an ordered set with $<$ and $x < y$, we often say $x$ is *less than* $y$. We also often use $y > x$ in place of $x < y$ when convenient.

We will use $x \leq y$ as a shorthand for $x < y$ or $x = y$. i.e. $x \leq y$ if and only if (NOT $y < x$)
Examples of Ordered Sets

Here are some examples

- The one point set \{\ast\} with nothing satisfying \(<\)
Examples of Ordered Sets

Here are some examples

- The one point set \{\star\} with nothing satisfying \( < \)
- \( \mathbb{Z} \) with the order \( a < b \) if and only if \( b - a \) is positive.
Examples of Ordered Sets

Here are some examples

- The one point set \( \{\ast\} \) with nothing satisfying \(<\).
- \( \mathbb{Z} \) with the order \( a < b \) if and only if \( b - a \) is positive.
- \( \mathbb{Z} \) with the order \( a < b \) if either
  - \( |a| < |b| \)
  - \( |a| = |b| \), \( a \) is negative and \( b \) is positive.

Notice that if \( S \) is an ordered set with \(<\) and \( E \subseteq S \) then \( E \) is an ordered set with \(<\).
Definition

Suppose $S$ is an ordered set and $E \subseteq S$.

- If there exists $\beta \in S$ such that $x \leq \beta$ for all $x \in E$ then we say $E$ is bounded above and call $\beta$ an upper bound.
- If there exists $\beta \in S$ such that $x \geq \beta$ for all $x \in E$ then we say $E$ is bounded below and call $\beta$ an lower bound.
Least Upper and Greatest Lower Bounds

Definition

Suppose $S$ is an ordered set and $E \subseteq S$.

- Suppose there exists an $\alpha \in S$ such that
  1. $\alpha$ is an upper bound of $E$
  2. If $\gamma < \alpha$ then $\gamma$ is not an upper bound of $E$

  We then say $\alpha$ is the least upper bound of $E$ or the supremum of $E$ and write $\alpha = \sup E$

- Suppose there exists an $\alpha \in S$ such that
  1. $\alpha$ is a lower bound of $E$
  2. If $\gamma > \alpha$ then $\gamma$ is not a lower bound of $E$

  We then say $\alpha$ is the greatest lower bound of $E$ or the infimum of $E$ and write $\alpha = \inf E$
Examples

Let's consider the set $\mathbb{Q}$ with the standard ordering.

- Let $X = \{ q \in \mathbb{Q} : q \geq 0 \text{ and } q \leq 1 \}$
Examples

Let's consider the set $\mathbb{Q}$ with the standard ordering.

- Let $X = \{ q \in \mathbb{Q} : q \geq 0 \text{ and } q \leq 1 \}$
  
  $X$ has a greatest lower bound and a least upper bound in $X$. 
Examples

Let $X = \{q \in \mathbb{Q} : q \geq 0 \text{ and } q \leq 1\}$
- $X$ has a greatest lower bound and a least upper bound in $X$

Let $X = \{q \in \mathbb{Q} : q > 0 \text{ and } q < 1\}$
Examples

Let's consider the set $\mathbb{Q}$ with the standard ordering.

- Let $X = \{q \in \mathbb{Q} : q \geq 0 \text{ and } q \leq 1\}$
  $X$ has a greatest lower bound and a least upper bound in $X$

- Let $X = \{q \in \mathbb{Q} : q > 0 \text{ and } q < 1\}$
  $X$ has a greatest lower bound and a least upper bound in $\mathbb{Q}$
  but not in $X$. 

- Let $X = \{n \in \mathbb{Z} : n \geq 0\}$
  $X$ has a least upper bound

- Let $X = \{q \in \mathbb{Q} : 2 \leq q^2 \text{ and } q^2 \leq 3\}$
  $X$ is bounded above and below but does not have a least upper bound or a greatest lower bound in $\mathbb{Q}$. 

Examples

Let's consider the set $\mathbb{Q}$ with the standard ordering.

- Let $X = \{q \in \mathbb{Q} : q \geq 0 \text{ and } q \leq 1\}$
  $X$ has a greatest lower bound and a least upper bound in $X$

- Let $X = \{q \in \mathbb{Q} : q > 0 \text{ and } q < 1\}$
  $X$ has a greatest lower bound and a least upper bound in $\mathbb{Q}$
  but not in $X$.

- Let $X = \{q \in \mathbb{Q} : q \geq 0\}$
Examples

Let's consider the set \( \mathbb{Q} \) with the standard ordering.

- Let \( X = \{ q \in \mathbb{Q} : q \geq 0 \text{ and } q \leq 1 \} \)
  \( X \) has a greatest lower bound and a least upper bound in \( X \)

- Let \( X = \{ q \in \mathbb{Q} : q > 0 \text{ and } q < 1 \} \)
  \( X \) has a greatest lower bound and a least upper bound in \( \mathbb{Q} \) but not in \( X \).

- Let \( X = \{ q \in \mathbb{Q} : q \geq 0 \} \)
  \( X \) has a greatest lower bound in \( X \) but is not bounded above.
Examples

Let's consider the set $\mathbb{Q}$ with the standard ordering.

- Let $X = \{q \in \mathbb{Q} : q \geq 0 \text{ and } q \leq 1\}$
  $X$ has a greatest lower bound and a least upper bound in $X$.
- Let $X = \{q \in \mathbb{Q} : q > 0 \text{ and } q < 1\}$
  $X$ has a greatest lower bound and a least upper bound in $\mathbb{Q}$ but not in $X$.
- Let $X = \{q \in \mathbb{Q} : q \geq 0\}$
  $X$ has a greatest lower bound in $X$ but is not bounded above.
- Let $X = \{n : n \in \mathbb{Z}\}$
Examples

Let’s consider the set $\mathbb{Q}$ with the standard ordering.

- Let $X = \{ q \in \mathbb{Q} : q \geq 0 \text{ and } q \leq 1 \}$
  $X$ has a greatest lower bound and a least upper bound in $X$

- Let $X = \{ q \in \mathbb{Q} : q > 0 \text{ and } q < 1 \}$
  $X$ has a greatest lower bound and a least upper bound in $\mathbb{Q}$ but not in $X$.

- Let $X = \{ q \in \mathbb{Q} : q \geq 0 \}$
  $X$ has a greatest lower bound in $X$ but is not bounded above.

- Let $X = \{ n : n \in \mathbb{Z} \}$
  $X$ is not bounded above or below.
Examples

Let’s consider the set $\mathbb{Q}$ with the standard ordering.

- Let $X = \{q \in \mathbb{Q} : q \geq 0 \text{ and } q \leq 1\}$
  $X$ has a greatest lower bound and a least upper bound in $X$.

- Let $X = \{q \in \mathbb{Q} : q > 0 \text{ and } q < 1\}$
  $X$ has a greatest lower bound and a least upper bound in $\mathbb{Q}$ but not in $X$.

- Let $X = \{q \in \mathbb{Q} : q \geq 0\}$
  $X$ has a greatest lower bound in $X$ but is not bounded above.

- Let $X = \{n : n \in \mathbb{Z}\}$
  $X$ is not bounded above or below.

- Let $X = \{q \in \mathbb{Q} : 2 \leq q^2 \text{ and } q^2 \leq 3\}$
Examples

Let's consider the set $\mathbb{Q}$ with the standard ordering.

- Let $X = \{ q \in \mathbb{Q} : q \geq 0 \text{ and } q \leq 1 \}$
  $X$ has a greatest lower bound and a least upper bound in $X$.

- Let $X = \{ q \in \mathbb{Q} : q > 0 \text{ and } q < 1 \}$
  $X$ has a greatest lower bound and a least upper bound in $\mathbb{Q}$ but not in $X$.

- Let $X = \{ q \in \mathbb{Q} : q \geq 0 \}$
  $X$ has a greatest lower bound in $X$ but is not bounded above.

- Let $X = \{ n : n \in \mathbb{Z} \}$
  $X$ is not bounded above or below.

- Let $X = \{ q \in \mathbb{Q} : 2 \leq q^2 \text{ and } q^2 \leq 3 \}$
  $X$ bounded above and below but does not have a least upper bound or a greatest lower bound in $\mathbb{Q}$.
Definition

An ordered set $S$ has the Least Upper Bound Property if for all $E \subseteq S$ such that

- $E$ is non-empty
- $E$ is bounded above

we have $\sup E$ exists in $S$. 
Theorem

Suppose $S$ is an ordered set with the least upper bound property, $B \subseteq S$ with $B$ non-empty and bounded below. Let $L$ be the set of all lower bounds of $B$. Then

$$\alpha = \sup L$$

exists in $S$ and $\alpha = \inf B$. In particular $\inf B$ exists in $S$. 
Definition

A Field is a set $F$ with two operations called addition (denoted by $+$) and multiplication (denoted by $\cdot$) which satisfy the following field axioms

(A) Axioms for addition

(A1) If $x, y \in F$ then $x + y \in F$
(A2) Addition is commutative: For all $x, y \in F$, $x + y = y + x$
(A3) Addition is associative: For all $x, y, z \in F$, $x + (y + z) = (x + y) + z$
(A4) $F$ contains a constant 0 such that for all $x \in F$ $0 + x = x$
(A5) For every element $x \in F$ there is an element $-x \in F$ such that $x + (-x) = 0$. 
Definition of a Field

(M) Axioms for multiplication

(M1) If $x, y \in F$ then $x \cdot y \in F$

(M2) Multiplication is commutative: For all $x, y \in F$, $x \cdot y = y \cdot x$

(M3) Multiplication is associative: For all $x, y, z \in F$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

(M4) $F$ contains a constant $1 \neq 0$ such that for all $x \in F$ $1 \cdot x = x$

(M5) If $x \in F$ and $x \neq 0$ then there is an element $1/x \in F$ such that $x \cdot (1/x) = 1$.
Definition of a Field

**Definition**

(M) Axioms for multiplication

(M1) If \( x, y \in F \) then \( x \cdot y \in F \)

(M2) Multiplication is commutative: For all \( x, y \in F \), \( x \cdot y = y \cdot x \)

(M3) Multiplication is associative: For all \( x, y, z \in F \),
\[
x \cdot (y \cdot z) = (x \cdot y) \cdot z
\]

(M4) \( F \) contains a constant \( 1 \neq 0 \) such that for all \( x \in F \), \( 1 \cdot x = x \)

(M5) If \( x \in F \) and \( x \neq 0 \) then there is an element \( 1/x \in F \) such that \( x \cdot (1/x) = 1 \).

(D) The distributive law

\[
x \cdot (y + z) = x \cdot y + x \cdot z
\]

for all \( x, y, z \in F \).
Examples of Fields

The following are some examples of fields

- The rational numbers: $\mathbb{Q}$
- The real numbers: $\mathbb{R}$
- The Complex numbers: $\mathbb{C}$
- Integers mod a prime $p$: $\mathbb{Z}/(p)$. 
Examples of Fields

The following are some examples of fields

- The rational numbers: $\mathbb{Q}$
- The real numbers: $\mathbb{R}$
- The Complex numbers: $\mathbb{C}$
- Integers mod a prime $p$: $\mathbb{Z}/(p)$.

The following are not fields

- The non-negative rational numbers $\{x \in \mathbb{Q} : x \geq 0\}$
- Integers mod a composite $n$: $\mathbb{Z}/(n)$. 
The axioms of addition imply the following

(a) If \( x + y = x + z \) then \( y = z \)
(b) If \( x + y = x \) then \( y = 0 \)
(c) If \( x + y = 0 \) then \( x = (-y) \)
(d) If \( -(−x) = x \)
The field axioms imply the following for all $x, y, z \in F$.

(a) $0x = 0$

(b) If $x \neq 0$ and $y \neq 0$ then $xy \neq 0$

(c) If $(-x)y = x(-y) = -(xy)$

(d) If $(-x)(-y) = xy$
An **Ordered Field** is a field $F$ which is also an ordered set (with $<$) such that

- $x + y < x + z$ if $x, y, z \in F$ and $y < z$
- $xy > 0$ if $x, y \in F$, $x > 0$ and $y > 0$

If $x > 0$ then we say $x$ is **positive**.
The following are some examples of ordered fields

- The rational numbers: \( \mathbb{Q} \)
- The real numbers: \( \mathbb{R} \)
The following are some examples of ordered fields

- The rational numbers: \( \mathbb{Q} \)
- The real numbers: \( \mathbb{R} \)

The following are fields which can not be made into ordered fields.

- The Complex numbers: \( \mathbb{C} \)
- Integers mod a prime \( p \): \( \mathbb{Z}/(p) \).
The following are true in every ordered field.

(a) If $x > 0$ then $-x < 0$ and vice versa
(b) If $x > 0$ and $y < z$ then $xy < xz$
(c) If $x < 0$ and $y < z$ then $xy > xz$
(d) If $x \neq 0$ then $x^2 > 0$. In particular $1 > 0$
(e) If $0 < x < y$ then $0 < 1/y < 1/x$