The Reals
Outline

As we have seen, the set of real numbers, \( \mathbb{R} \), has cardinality \( c \). This doesn't tell us very much about the reals, since there are many sets with this cardinality and cardinality doesn't tell us anything about the structure of a set.

We will now investigate the structure of this important set.

To do this we will look at the axiomatic construction of the reals. Starting with the axioms for the natural numbers, we will build up to the reals.

Our investigation will be superficial, since going through all the details would take up most of a full semester course.
Binary Operations on a Set

One of the obvious features of the reals is that we can perform algebraic operations on them (addition, multiplication, etc.) We start by reviewing some of the general terminology associated with these operations.

A binary operation on a set $S$ is a function : $S \times S \to S$.

Many binary operations can be defined on the same set. We will use a generic symbol for a binary operation, namely $\odot$, but this could stand for addition or multiplication or any other binary operation. So, for $a, b \in S$, the binary operation maps

$(a,b) \to a \odot b \in S.$
Properties of Binary Operations

A binary operation on a set $S$ may (but does not have to) satisfy any of these properties.

**Associative Law:** $a \odot (b \odot c) = (a \odot b) \odot c$ for all $a,b,c \in S$.

**Commutative Law:** $a \odot b = b \odot a$ for all $a,b \in S$.

**Closure on a set.** Let $A \subseteq S$. If for all $a,b \in A$, $a \odot b \in A$, then we say that the binary operation is *closed* on $A$.

*Example:* Let $S$ be the set of natural numbers with binary operation of addition ($+$). If $A$ is the subset of even natural numbers then $+$ is closed on $A$. On the other hand, if $B$ is the subset of odd natural numbers, then $+$ is not closed on $B$. 
Properties of Binary Operations

Identity elements: If there exists an element \( i \in S \) such that for all \( a \in S \), \( i \odot a = a \odot i = a \), then we say that \( i \) is an identity element for \( \odot \).

Example: For \( S = \mathbb{R} \), 0 is the identity element for addition and 1 is the identity element for multiplication.

Inverse elements: If a set \( S \) has a binary operation with an identity element \( i \), then for \( a \) in \( S \), the inverse of \( a \) with respect to the binary operation is an element \( b \in S \) with the property that
\[
 a \odot b = b \odot a = i .
\]

Example: For \( S = \mathbb{R} \), the inverse of 5 with respect to addition is -5, while the inverse of 5 with respect to multiplication is \( 1/5 \). -5 is called the additive inverse and \( 1/5 \) is called the multiplicative inverse in this case.
Peano's Axioms

We start with a set of objects, called "numbers" satisfying:

**Peano's Axioms**

a. 1 is a number.

b. For each number n, there is another number n' called the **successor** of n.

c. For each number n, n' does not equal 1.

d. For all numbers m and n, if m' = n' then m = n.

e. **Inductive Property**: If a set S of numbers has the properties:

   1. 1 is in S,
   2. If for each n ∈ S, n' ∈ S, then S contains all of the numbers.

All models of Peano's Axioms are isomorphic.

We will call such a model the set of natural numbers, \( \mathbb{N} \).
Arithmetic in a Peano System

We now define two binary operations inductively:

**Addition:** Let \( n \) be a natural number. Then
1) \( n + 1 = n' \)
2) For all natural numbers \( m \), \( n + m' = (n + m)' \)

It can be shown that the binary operation of addition is associative and commutative. There is no identity element for \(+\).

**Multiplication:** Let \( n \) be a natural number. Then
1) \( n \times 1 = n \),
2) For all natural numbers \( m \), \( mn' = mn + m \).

It can be shown that the binary operation of multiplication is associative and commutative. \( 1 \) is the identity element for \( \times \).
Extending the Naturals

Having defined the natural numbers axiomatically we now start to extend the set by adding new elements so that certain conditions are satisfied.

We first add an element called 0 to \(\mathbb{N}\) and define addition and multiplication involving this new element by:

\[
\begin{align*}
    n + 0 &= 0 + n = n & \text{for all } n \in \mathbb{N} \\
    0 + 0 &= 0 \\
    n \times 0 &= 0 \times n = 0 & \text{for all } n \in \mathbb{N} \\
    0 \times 0 &= 0
\end{align*}
\]

Our next extension is to add new elements which will be additive inverses of the elements of \(\mathbb{N}\). That is, for each \(n \in \mathbb{N}\), we define an element \(-n\) so that \(n + (-n) = (-n) + n = 0\). We also extend the multiplication operation to include these new elements by defining:

\[
\begin{align*}
    m \times (-n) &= (-n) \times m = -(m \times n) \quad \text{and} \quad (-m) \times (-n) &= (-n) \times (-m) = n \times m.
\end{align*}
\]
Finally, defining \( 0 \times (-n) = (-n) \times 0 = 0 \), we have extended the natural numbers to the set of integers \( \mathbb{Z} \). \( \mathbb{Z} \) has two binary operations which are the extensions of the binary operations defined on the natural numbers.

Except for 1, no element of \( \mathbb{Z} \) has a multiplicative inverse. Our next extension will add these missing elements. It turns out that we need to add more than just the multiplicative inverses in order to be able to extend our two binary operations to the larger set.

We define the "field of fractions" of \( \mathbb{Z} \) by:

\[
F = \{(a,b) \in \mathbb{Z} \times \mathbb{Z}: b \neq 0\}
\]

and extend the binary operations by:

\[
(a,b) + (c,d) = (a \times d + b \times c, b \times d) \quad \text{and} \quad (a,b) \times (c,d) = (a \times c, b \times d).
\]
The Rationals

It can be shown that these extended operations have the same properties that operations in $\mathbb{Z}$ have.

We now define an equivalence relation $R$ on $F$ by:

$$(a,b) R (c,d) \iff a \times d = b \times c.$$  

The equivalence classes of this equivalence relation are called rational numbers and the set of all rational numbers is denoted by $\mathbb{Q}$.

Addition and multiplication of elements of $\mathbb{Q}$ is defined by:

$$[(a,b)] + [(c,d)] = [(a,b) + (c,d)] \text{ and } [(a,b)] \times [(c,d)] = [(a,b) \times (c,d)]$$

With these definitions (which must be shown to be well defined) $\mathbb{Q}$ forms an algebraic object known as a field.
Fields

A field is a set $F$ together with two binary operations, called addition and multiplication, which satisfy the following axioms:

1. $F$ under addition is an abelian group.
   This means that
   
   a) $a + (b + c) = (a + b) + c \quad \forall a, b, c \in F$ (The Associative Law for Addition)
   
   b) $a + b = b + a \quad \forall a, b \in F$ (The Commutative Law for Addition)

   c) $\exists$ an element, called 0, which satisfies $a + 0 = 0 + a = a \quad \forall a \in F$ (Additive Identity)

   d) For every element $a \in F$, there exists an element denoted $-a$ which satisfies $a + (-a) = (-a) + a = 0$. (Additive Inverse)
Fields

2. $F - \{0\}$ under multiplication is an abelian group. This means that

a) $a(bc) = (ab)c \quad \forall a, b, c \in F - \{0\}$ \textit{(The Associative Law for Multiplication)}

b) $ab = ba \quad \forall a, b \in F - \{0\}$ \textit{(The Commutative Law for Multiplication)}

c) $\exists$ an element, called 1, which satisfies $a1 = 1a = a \quad \forall a \in F - \{0\}$ \textit{(Multiplicative Identity)}

d) For every element $a \in F - \{0\}$, there exists an element denoted $a^{-1}$ which satisfies $a(a^{-1}) = (a^{-1})a = 1$. \textit{(Multiplicative Inverse)}

3. $\forall a, b, c \in F$ we have $a(b + c) = ab + ac$ \textit{(The distributive law of multiplication over addition)}.

4. $0a = a0 = 0 \quad \forall a \in F$. 
Examples

Examples of fields are given by the reals, the rationals, the complex numbers and the integers modulo $p$ where $p$ is a prime.

The first three examples above are infinite fields (the sets on which they are based are infinite sets) while the last examples are finite fields.

There are other finite fields besides the integers mod $p$, in fact there is one of each size $q$ where $q$ is a power of a prime. These however are not the integers modulo $q$ and their construction is more complicated.
Before continuing our construction of the reals we pause to consider some other properties that the reals have.

These properties are needed to distinguish the reals from the other fields.
Ordered Fields

A field $F$ is *ordered* if there is a relation $<$ on $F$ such that for all $x, y, z \in F$,

1. $x < x$ is never true. (*irreflexivity*).
2. If $x < y$ and $y < z$ then $x < z$ (*transitivity*)
3. Either $x < y$, $x = y$ or $y < x$ (*trichotomy*)
4. If $x < y$, then $x + z < y + z$
5. If $x < y$ and $0 < z$, then $xz < yz$

Examples of ordered fields are given by the reals and the rationals. The complex numbers and the finite fields cannot be ordered.
Bounds Again

Let A be a subset of an ordered field F. We say that \( u \in F \) is an **upper bound** for A iff \( a \leq u \) for all \( a \in A \). If A has an upper bound, A is **bounded from above**. Likewise, \( l \in F \) is a **lower bound** for A iff \( l \leq a \) for all \( a \in A \). A is **bounded from below** if any lower bound for A exists. The set A is **bounded** iff A is both bounded from above and bounded from below.
Complete Fields

In some fields bounded sets may not have sup's or inf's. For example in $\mathbb{Q}$, the set \{x | x^2 < 2\} is bounded but does not have a least upper bound nor a greatest lower bound in $\mathbb{Q}$.

This set is the set of rational numbers x where $-\sqrt{2} < x < \sqrt{2}$.

This set is bounded above by 3 and bounded below by -3, so it is a bounded set. However, there is no rational number which is, for instance, an upper bound which is smaller than every upper bound of the set, i.e., no least upper bound.

An ordered field $F$ is complete iff every nonempty subset of $F$ that has an upper bound in $F$ has a supremum that is in $F$. 
The Reals

The rationals are not complete, but the reals form a complete ordered field. In fact, it can be shown that any complete ordered field is just a copy (with the elements renamed) of the reals, so in this sense there is only one complete ordered field.

Back to our construction. We have at this point obtained the field of rationals. To move on to the reals we need to construct a complete ordered field based on $\mathbb{Q}$. To do this we first need to define a partial order on $\mathbb{Q}$ that will turn it into an ordered field. The next step would be to extend $\mathbb{Q}$ so that it becomes a complete ordered field.
Orders

To define the order relation on $\mathbb{Q}$ we start with the integers $\mathbb{Z}$.

By our construction, we know that $\mathbb{N} \subseteq \mathbb{Z}$.

We define an element $b \in \mathbb{Z}$ to be *positive* if $b \in \mathbb{N}$.
If $b$ is positive we write $0 < b$.

**Note:** If $0 < a$ and $0 < b$ then we have $0 < a + b$ and $0 < a \times b$.

**Definition:** For any $a$ and $b \in \mathbb{Z}$ we now define
\[
a < b \text{  iff  } 0 < b + (-a).
\]

We write $a \leq b$ if either $a < b$ or $a = b$.
It can now be shown that $\leq$ is a linear (total) order on $\mathbb{Z}$.
Orders

We can now extend this linear order to $\mathbb{Q}$ by defining:

$$[(a,b)] < [(c,d)] \text{ iff } a\times d < b\times c \text{ when } 0 < b \text{ and } 0 < d.$$ 

We can now verify that $\mathbb{Q}$ is an ordered field with this definition of $<$.

The next step is to extend this ordered field to a complete ordered field.

The completeness property is not as familiar as the other properties that we have studied. So, before we make this last extension, we will study this property in detail.