Real Numbers

Mark Dean +

Lecture Notes for Fall 2014 PhD Class - Brown University

1 Introduction

As a warm-up exercise, we are going to begin discussing what we mean by 'real numbers'. This will be useful for two reasons – one of which is that real numbers are pretty foundational to what we do, so it is useful for you to know a bit more about them. Second, it will help us to highlight the difference between various 'types' of numbers; natural numbers, integers, rationals and reals. For the remainder of the course I'll be assuming that you know what these are, and their properties, so it is worth refreshing our memory in this regard. We are not going to go through a formal construction of the various number systems (we don't have time). Rather, we are going to give some notion of where they come from, and define some of these properties. For more information, see Ok Chapter A part 2.

2 Ordered Fields

To start with we are going to define the *algebraic structure* of the number system. Roughly speaking, an algebraic structure is a set of objects, and a set of operations defined on these objects. First, a couple of definitions:

Definition 1 *Let X be a non-empty set. A **binary operation** is a function $\bullet : X \times X \to X$. For convenience, we will write $x \bullet y$ rather than $\bullet(x, y)$ for any $x, y \in X$.*

For the natural numbers (i.e the counting numbers $1, 2, 3, 4...$) obvious binary operations include addition and multiplication, but *not* subtraction (why not?).

Now we can define the concept of a field.

Definition 2 *A **field** is a non-empty set X and two binary operations, $+$ and $\times$, that obey the following rules:*

- ***Commutativity:*** $x + y = y + x$ *and* $x \times y = y \times x$ *for all* $x, y \in X$
- ***Associativity :*** $(x + y) + z = x + (y + z)$ *and* $(x \times y) \times z = x \times (y \times z)$ *for all* $x, y \in X$
- ***Distributivity:*** $x \times (y + z) = x \times y + x \times z$
- ***Existence of Identity Elements:*** *There exist elements* 0 *and* 1 *in* X *such that* $0 + x = x$ *and* $1x = x$ *for all* $x \in X$
- ***Existence of Inverse Elements:*** *For each element* $x \in X$ *there exists an element* $-x \in X$ *such that* $x + (-x) = 0$ ***(the additive inverse)*** *and for each* $x \in X/0$ *there exists an element* x^{-1} *such that* $x \times x^{-1} = 1$ ***(the multiplicative inverse)***.

Of course, you are used to dealing with addition and multiplication operations since you were about 4 years old, so much so that they are probably second nature to you. There is, in that sense, nothing really new here. However, there are two points worth noting.

1. A field is a general concept - the set X does not have to be numbers, and the concepts of addition and multiplication do not have to be defined as we are used to.
2. To do most of the standard algebra we usually do, we only need these properties.

To see this second point, we can use the above structure to define the concepts of 'subtraction' and 'division', as $x - y := x + (-y)$ and $x/y = x \times (y^{-1})$ (assuming $y \neq 0$). Furthermore, we can derive other algebraic laws from these results, such as:

- $x + y = x + z$ if and only if $y = z$
- $-(-x) = x$
- $-(x + y) = -x + -y$

These results are relatively easy to prove (you should check you can do it). We will do the first one as an example:

Proof ($(x+y) = (x+z)$ if and only if $y = z$). Note that there are two things to prove. However, the 'if' part is trivial, so we concentrate on the ' only if' part. First, note that

$$\begin{aligned} y &= 0 + y \text{ (Existence of Identity Element)} \\ &= (-x + x) + y \text{ (Existence of Inverse Element)} \\ &= -x + (x + y) \text{ (Associativity)} \end{aligned}$$

So, if $(x + y) = (x + z)$ we have that

$$\begin{aligned} y &= -x + (x + y) \\ &= -x + (x + z) \text{ (by assumption)} \\ &= (-x + x) + z \text{ (Associativity)} \\ &= 0 + z \text{ (Inverse Element)} \\ &= z \text{ (Identity Element)} \end{aligned}$$

■

The concept of a field gives us the *algebraic structure* that we associate with numbers.[1] However, numbers have something else - an *order structure*. We 'know' that 1 is smaller than 2, 700 is bigger that 600 and so on. However, there is nothing in the definition of a field that captures this notion (remember that X may not be numbers, they could be anything - types of fruit, for example). To introduce the concept of ordering, we need to introduce the notion of a binary relation.

Definition 3 *Let X be a non-empty set. A **binary relation** R on X is a subset of $X \times X$. We write xRy to indicate that $(x, y) \in R$.*

You will have used binary relations before. In fact, the binary relation that you will be most used to is the 'greater than' relation for numbers. The binary relation defines a "property", and all pairs in R possess this property, while the pairs not in R do not.

[1] Of course, a field is only one type of algebraic structure. We could demand less structure - for example we could drop the requirement of inverses for multiplication. This is called an integral domain. We could additionally drop the requirement of multiplicative inverse and identity element, which gives us a ring.

We can also have algebraic structures that have more properties, as we will see below.

Definition 4 *A **linear order** $\succeq$ is a binary relation on a set X which is*

1. *Transitive: $x \succeq y \succeq z$ implies $x \succeq z$*
2. *Complete: $x \succeq y$ or $y \succeq x$ for all $y, x \in X$*
3. *Antisymmetric: $x \succeq y$ and $y \succeq x$ implies that $x = y$*

Note that completeness implies $x \succeq x$ (reflexivity). An order that satisfies only reflexivity but not completeness is called a *partial order*. The standard 'weakly greater than' relation on the real numbers is a linear order. However, one could think of other binary relations that have the same properties.

We are now in a position to define the concept of an ordered field.

Definition 5 *An ordered field consists of a field $(X, +, \times)$ and a linear order $\geq$ that is consistent with the field operations $+$ and $\times$:*

1. *$x \geq y$ implies $x + z \geq y + z$ for all $x, y, z \in X$*
2. *$x \geq y$ implies $xz \geq yz$ for $x, y, z \in X$ and $z \geq 0$*

We also define the following sets:

$$\begin{aligned} X_+ &= \{x \in X | x \geq 0\} \\ X_{++} &= \{x \in X/0 | x \geq 0\} \\ X_- &= \{x \in X | 0 \geq x\} \\ X_{--} &= \{x \in X/0 | 0 \geq x\} \end{aligned}$$

An ordered field is rich enough to establish pretty much all the algebraic properties that we use. In other words, most of the algebraic results we use derive from the fact that we have a number system that has well behaved addition and multiplication properties, and a linear order that respects these operations. For example, the definition of an ordered field implies things such

as

$$\begin{aligned} -x &\leq 0 \leq x \text{ or } x \leq 0 \leq -x \text{ for all } x \in X \\ x &\geq y \text{ implies } xz \leq yz \text{ for all } z \leq 0 \\ 0x &= 0 \ \forall \ x \in X \end{aligned}$$

A slightly richer example is the following.

Example 1 *Let* $(X, +, \times, \geq)$ *be an ordered field. The* absolute value function $|.| : X \to X$ *is defined as*

$$\begin{aligned} |x| &= x \text{ if } x \geq 0 \\ |x| &= -x \text{ if } x \leq 0 \end{aligned}$$

Then the ***triangle inequality*** *must hold:*

$$|x + y| \leq |x| + |y|.$$

Proof. *Homework* ■

3 Natural Numbers, Integers and Rationals

We can now start describing the properties of some of the number sets that we are interested in. First, the natural numbers, denoted by $\mathbb{N}$. These are sometimes called the 'counting numbers', because they are the numbers $1, 2, 3, ...$etc. A formal basis for these numbers was provided by Giuseppe Peano. Informally, the Peano axioms define the concept of a *successor relation,* which defines the immediate successor of each natural number. The axioms then state that (i) there is an element 1 that is not the successor of any element (ii) if $i \in \mathbb{N}$, then the successor to $i \in \mathbb{N}$ and (iii) if x and y have the same successor, then $x = y$. Addition, multiplication and ordering are defined using this successor relation.

The property of natural numbers that we are most interested in is the Axiom of Induction:

Definition 6 ***The Axiom of Induction:*** *If* S *is a subset of* $\mathbb{N}$ *such that* $1 \in S$ *and* $i + 1 \in S$ *whenever* $i \in S$ *then* $S = \mathbb{N}$.

Consider a sequence of propositions $P_1, P_2, P_3, ...$ If we can show that P_1 is true, and that, if P_i is true then so is P_{i+1}, the we can use the principle of mathematical induction to conclude that each proposition in the sequence is true.

Now note that $\mathbb{N}$ is not an ordered field with the standard addition and multiplication operations (why?). What about the integers? In order to get from the natural numbers to the integers, we need to do two things:

1. Add a zero. We define the resulting set as $\mathbb{Z}_+ = \{0, 1, 2, 3, ..\}$
2. Add negative numbers. We define the resulting set as $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ..\}$

Is $\mathbb{Z}$ an ordered field? Unfortunately not - it does not contain multiplicative inverse elements (e.g. there is no integer such that $x2 = 1$). Thus, if we want to be able to solve such equations (which often we do) we are going to have to extend $\mathbb{Z}$ to be a field. The minimal way of doing this (i.e. the smallest field that contains $\mathbb{Z}$) are the **Rational Numbers $\mathbb{Q}$.** This set is constructed based on the multiplication operation.

$$\mathbb{Q} = \left\{ x = \frac{m}{n} | m \in \mathbb{Z}, n \in \mathbb{Z}/0 \right\}$$

We can extend addition and multiplication to $\mathbb{Q}$ in the standard way (i.e. using the rules you learned in high school, plus the rules of arithmetic on the integers), and we can also extend our ordering, in the sense than $\frac{m}{n} \geq \frac{k}{l}$ iff $ml \geq nk$. Note that this definition is a little informal, as the function / (division) is not defined on $\mathbb{Z}$, but we can get round this with some simple tricks. Now we have an ordered field.

Proposition 1 *$\mathbb{Q}$ is an ordered field.*

We don't have enough information to prove this formally, but it should feel true. That means we can perform many of the algebraic operations that we would like to do using just the rational numbers.

4 Real Numbers

Unfortunately, while the rational structure is quite rich, it is not rich enough for all the things that we would like to do, as the following example shows.

Example 2 *Imagine we want a number system that will allow us to consider the length of the hypotenuse of a right angled triangle where the length of each other side is 1. As we know, this means the length of the hypotenuse is given by* $r^2 = 2$. *Can* r *be a rational number? The answer is no, and we can show this as follows. If* r *is a rational number, then it can be written as* $\frac{m}{n}$ *where* m *and* n *are integers without a common factor. But as* $m^2 = 2n^2$, *we know that* m^2 *is even, and so* m *is even, meaning* $m = 2k$ *for some* $k \in \mathbb{Z}$. *But as*

$$\begin{aligned} m^2 &= 2n^2 \\ 4k^2 &= 2n^2 \\ &\Rightarrow \quad 2k^2 = n^2; \end{aligned}$$

implying that n^2 *is even, and so* n *is even. Thus,* 2 *is a common factor of* m *and* n, *a contradiction.*

This shows that there are 'holes' in the rational numbers. Informally, what we want to do is 'complete' the rational numbers to include numbers like r above. We call numbers in $\mathbb{R}/\mathbb{Q}$ **irrational numbers.**

There are two broad approaches to this. One is to define the reals as an ordered field that satisfies one more property, which we will define below. It turns out that all such ordered fields are the 'same' in the sense that they are isomorphic to each other. The other is to generate the real numbers from the rationals and extend the additive, multiplicative and order elements in a nice way. We will not pursue either approach here, just note the following.

Proposition 2 $\mathbb{R}$ *is an ordered field.*

In order to define the property that separates $\mathbb{R}$ from $\mathbb{Q}$, we need to introduce the concept of an upper bound and a supremum.

Definition 7 *An **upper bound** of the subset S of an ordered set X is an element $x \in X$ such that*

$$s \leq x \ \forall \ s \in S$$

Definition 8 *A set is **bounded from above** if it has an upper bound.*

Definition 9 *The **supremum** of the subset S of an ordered set X is the least upper bound of S. i.e. it is an element $x \in X$ such that*

1. *x is an upper bound of S*
2. *$x \leq y$ for all other upper bounds y of S*

We write $x = \sup S$.

The key thing about $\mathbb{R}$ is that any subset that is bounded from above will have a supremum. This is the Completeness axiom.

Definition 10 ***The Completeness Axiom:*** *For any non-empty subset S of $\mathbb{R}$ that is bounded from above, there exists $s \in \mathbb{R}$ such that $s = \sup S$.*

An immediate corollary are the following (very useful) properties of the set $\mathbb{R}$.

Proposition 3 *The completeness axiom implies the following two properties*

1. ***(The Archimedean Property)*** *For any $\{a, b\} \in \mathbb{R}_{++} \times \mathbb{R}$ there is an $m \in \mathbb{N}$ such that $b < ma$*
2. *For any $a, b \in \mathbb{R}$, such that $a < b$, there exists a $q \in \mathbb{Q}$ such that $a < q < b$ (this is sometimes described as $\mathbb{Q}$ being order-dense in $\mathbb{R}$).*

Proof. *We will do each in turn*

1. *Assume not, then for some a, the set $\{ma | m \in \mathbb{N}\}$ is bounded from above by b. As this is a set of real numbers, this implies that this set has a sup s. Thus $s - a$ is not an upper bound of $\{ma | m \in \mathbb{N}\}$, implying there exists an m such that $ma > s - a$. But this implies that $(m + 1)a > s$, a contradiction.*

■

Without giving a formal proof (this is an exercise in Ok), note that the completeness axiom also implies that the irrational numbers are order-dense in $\mathbb{R}$, that is, for any two numbers in $\mathbb{R}$, there exists a number in $\mathbb{R}/\mathbb{Q}$ between them.

We will use both properties in proposition 3 during the course. In fact, we can use them here to show that $\mathbb{Q}$ is not complete. We first prove the following claim:

Claim 1 *Consider the set $S = \{q \in \mathbb{Q} | q^2 < 2\}$. This is a subset of $\mathbb{R}$ that is bounded from above and therefore has a supremum $s = \sup S$. We claim that $s^2 = 2$.*

Proof. *Step 1: suppose $s^2 > 2$. Then $s^2 - 2 > 0$, and so, by the Archimedean property, there exists an $m \in \mathbb{N}$ such that $m(s^2 - 2) > 2s$. Then*

$$\begin{aligned}\left(s - \frac{1}{m}\right)^2 &= s^2 - \frac{2s}{m} + \frac{1}{m^2} \\ &> s^2 - (s^2 - 2) + \frac{1}{m^2} \\ &> s^2 - (s^2 - 2) = 2\end{aligned}$$

So $s - \frac{1}{m}$ is a lower upper bound, a contradiction.

Step 2: now assume that $s^2 < 2$, and use the Archimedean property to find an $m \in \mathbb{N}$ such that $m(2 - s^2) > 4s$ and $m > \frac{1}{2s}$. This implies that

$$\begin{aligned}\left(s + \frac{1}{m}\right)^2 &= s^2 + \frac{2s}{m} + \frac{1}{m^2} \\ &< s^2 + \frac{2s}{m} + \frac{2s}{m} \\ &< s^2 + 2 - s^2 \\ &= 2\end{aligned}$$

But, by the second part of proposition 3, there must exist $q \in \mathbb{Q}$ such that $s < q < (s + \frac{1}{m})$, and so $q^2 < (s + \frac{1}{m})^2 < 2$. This is a contradiction of the fact that s is an upper bound. Thus we conclude that $s^2 = 2$. ■

We can now use this result to show that there is no supremum of S within the rational numbers.

Claim 2 *There is no $\bar{q} \in \mathbb{Q}$ such that*

1. *$\bar{q}$ is an upper bound of $\left\{q \in \mathbb{Q} | q^2 < 2\right\}$*
2. *for any $r \in \mathbb{Q}$ such that r is an upper bound of $\left\{q \in \mathbb{Q} | q^2 < 2\right\}$, $\bar{q} \leq r$*

Proof. *Assume that such a $\bar{q}$ exists. We already know that $\bar{q}^2 \neq 2$, and Step 2 above showed that it cannot be that $\bar{q}^2 < 2$. We also know that there exists a real number s s.t. $s^2 = 2$. Suppose $\bar{q}^2 > 2$; then there is a $q \in \mathbb{Q}$ such that $s < q < \bar{q}$, and $q^2 > 2$. Thus $\bar{q}$ is not a least upper bound.* ■

Note the difference between the sup of a set and the maximum of a set (which you are probably already familiar with). The maximum of a set is defined as follows

Definition 11 *The **maximum** of a set $S \subset \mathbb{R}$ is*

$$\max S = \{x \in S | x \geq y \ \forall \ y \in S\}$$

Note that, unlike the sup operator, not every S that is bounded above has a max (for example, the set $S = \{x \in \mathbb{R} | x < 2\}$ has a sup but not a max). However, if the max does exist for a set S, then it will be the case that $\max S = \sup S$ (can you prove this?).

The preceding discussion should suggest in an informal way that the set of real numbers is 'bigger' than the set of rational (and indeed natural) numbers. There is a formal sense in which this is true (though we are not going to have time to go into the details - see OK Chapter B for more). In order to state this, we need to define the concept of countability.

Definition 12 *A set is **countably infinite** if there exists a bijective function (i.e. one to one mapping) between that set and the natural numbers. A set is **countable** if there exists an injective function from the set to the natural numbers (i.e. each element in the set can be mapped to a different number).*

Any countably infinite set can therefore be enumerated as $X = \{x_1, x_2, ..., \}$. Moreover

- any subset of a countable set is countable, and
- any countable union of countable sets is countable.

In terms of the sets we have come across, clearly $\mathbb{N}$ and $\mathbb{Z}$ are countable. Perhaps more surprisingly, $\mathbb{Q}$ is countable. This comes from the fact that we can describe $\mathbb{Q}$ as a countable union of countable sets. This is a very important result, particularly when combined with the second part of proposition 3, as we will see. One immediate corollary of this is the following:

Theorem 3 *Let $\mathcal{I}$ be a set of non-degenerate intervals on $\mathbb{R}$ such that $|I \cap J| \leq 1$ for any $I, J \in \mathcal{I}$. Then $\mathcal{I}$ is countable.*

We will not go through the proof formally here, but you should get an intuitive idea of how it works. These are intervals that do not overlap. Each of them must contain a distinct rational number, thus if we have an uncountable number of intervals, then there would be an uncountable number of distinct rational numbers, which we know we do not have.

Finally, the most important result here (that we will not prove) is that the real numbers are *not* countable - i.e. there is no bijection between the real and natural numbers.

Proposition 4 *The real numbers are not countable.*

This is the sense in which there are 'more' real numbers than rationals.

As a last note, observe that not all the properties of the number system we typically use are determined by the properties given by an ordered field. For example, the decimal system that we use to label our numbers is an added property (something that should be clear from the fact that we could equivalently use a binary system or other base). We also assume that there are no duplicates, that is, there are no "redundant" real numbers that act exactly the same as the "original" numbers with respect to the various operations we allow, but are distinct.

5 Intervals and Extended Reals

Some notation that you are probably already used to is the following. Let a, b be real numbers such that $a < b$. Then

- $(a, b) = \{t \in \mathbb{R} | a < t < b\}$
- $[a, b) = (a, b) \cup a$
- $(a, b] = (a, b) \cup b$
- $[a, b] = \{t \in \mathbb{R} | a \leq t \leq b\}$

These define **bounded intervals.** Note that we may also want to consider unbounded intervals, for example of the form $\{t \in \mathbb{R} | t > a\}$. Such sets are not bounded from above, and so do not have a sup in $\mathbb{R}$. We may sometimes use the notation (a, ∞) to describe such sets, but at the moment, this is just notational convenience, as ∞ is not a real number.

It is possible to make the concept of ∞ more than just notation, and extend the notion of the real numbers to include ∞ and $-\infty$. We call such a set the **extended real line,** and denote it by $\bar{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$. In order to do this (moderately) formally, we need to extend the order relation we have on $\mathbb{R}$ to ∞ and $-\infty$ in the following way.

$$\infty > -\infty \text{ and } \infty > t > -\infty \ \forall \ t \in \mathbb{R}$$

Thus, we have a complete partial (linear) order of $\bar{\mathbb{R}}$. Moreover, $\bar{\mathbb{R}}$ obeys the completeness axiom, and now *every* set in $\bar{\mathbb{R}}$ has a sup (if S is not bounded above in $\mathbb{R}$, then the above means that $\sup S = \infty$).

We need to do one more thing in order to make the extended reals useful – we need to define arithmetic operations involving $-\infty$ and ∞. We do this as follows for any $t \in \mathbb{R}$

- $t + \infty = \infty + t = \infty$
- $t + -\infty = -\infty + t = -\infty$
- $\infty + \infty = \infty$
- $-\infty + -\infty = -\infty$
- $t \times \infty = \infty \times t = \begin{Bmatrix} \infty \text{ if } 0 < t \leq \infty \\ -\infty \text{ if } -\infty \leq t < 0 \end{Bmatrix}$

- $t \times -\infty = -\infty \times t = \left\{ \begin{array}{l} -\infty \text{ if } 0 < t \leq \infty \\ \infty \text{ if } -\infty \leq t < 0 \end{array} \right\}$

Does this make the extended reals a field? Unfortunately not, as we have not defined all the various operations, such as $\infty \times 0$.