Axioms

Herein begins the rigorous foundations of our course.
In this chapter we shall work to construct an axiomatic description of what the real numbers *ought to be*, that is, we will attempt to write down (and justify!) a collection of necessary conditions for a mathematical object to be called “a number line”. We will then see (but the proof will be beyond the scope of this first course), that there is indeed a single *unique* mathematical object satisfying these axioms; and define **the** real numbers to be this object. All subsequent developments in this course will spring forth from this firm foundation: that is, we will use these axioms, and only these axioms (and their consequences) in all rigorous claims that follow, from the discussion of decimals to the theory of calculus.

Perhaps first we should embark on a brief discussion of what the point of axioms are in the first place. What are we trying to do, when we describe a mathematical object or theory by some finite list of rules?

Chapter 1
Axioms

Section 1.1
Fields

We begin not directly with our goal of axiomatizing the number line, but with the rather more modest goal of axiomatizing the concept of “number”. If axioms are to give an operational definition of numbers, to begin we should not ask ourselves the philosophically loaded question *what are numbers*, but rather the much more mundane *what can you do with numbers, if you have them?*

The origins[1] of abstract numeracy lie deep in antiquity, hidden from us moderns by the relatively short written history our species has left behind (though recent discoveries point towards a robust and abstract concept of number pre-dating written speech by tens of thousands of years).

From our most distant ancestors to the modern day, numbers are "for" counting, and measuring things. Numbers are things you can do arithmetic to - they're things where you can add (concatenate two counted lists), subtract (remove one counted list from another), multiply (measure an area given two measurements of lengths), and divide (infer a rectangle's side length given its area and the length of a complementary side).

Thus, to axiomatize numbers as "the things you can do arithmetic to", we have a concrete path forwards: we need only axiomatize the four operations of $+, -, \times, \div$.

Binary Operations

In the slow but sure style of a careful mathematician, we begin by asking ourselves "what is an operation, anyway?" From the four examples we wish to axiomatize, we see a single commonality: they are all processes that take in two numbers and perform some process, before returning the result (which is a third number). In mathematics, processes are formally encoded as *functions*, so we may say that an operation is a function that takes in two numbers as input, and returns a single as output. Of course, we do not yet have an axiomatic definition of "number" itself, so we will define operations more generally as functions on a set.

Recall for the definition below that if A, B are two sets, the cartesian product $A \times B$ is the set of all ordered pairs where there first element comes from A and the second comes from B.

> **Definition :** Let S be a set. A *binary operation* on S is a function $f\colon S \times S \to S$. While the usual function notation for evaluation of f on a pair (s, t) would be $f(s, t)$, it is customary when talking of operations to write sft instead.
>
> > **Example :** Addition is a binary operation on the integers $+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, and
> >
> > $$+(2, 7) := 2 + 7 = 9$$

There are many properties one may wish to investigate for operations. Among these, two of the most important are (1) does the order you feed in elements affect the result and (2) does where you put grouping parentheses affect the result? These properties are called *commutativity* and *associativity* respectively.

> **Definition :** An operation $\star S \times S \to S$ is commutative if for every pair $s, t \in S$ we have $s \star t = t \star s$. The operation $\star$ is associative if for every triple s, t, u we have $s \star (t \star u) = (s \star t) \star u$.
>
> > **Example :** Addition, and multiplication are both commutative and associative operations, as $a + b = b + a$, $ab = ba$ and $a + (b + c) = (a + b) + c$, $a(bc) = (ab)c$. However exponentiation $(x, y) \mapsto x^y$ is neither commutative nor associative: $2^3 = 8$ whereas $3^2 = 9$, and $(2^3)^4 = 8^4 = 4096$ whereas
> >
> > $$2^{(3^4)} = 2^{81} = 2417851639229258349412352$$

To single out from the wide space of possible operations things we wish to call addition and multiplication, we need to think more deeply about the properties they enjoy. Indeed, one important thing stands out - in both operations theres a ‘special number’ which does nothing: for addition this is zero, and for multiplication this is 1:

$$0 + x = x \qquad 1x = 1$$

An element with this property is said to be an *identity element* for the given operation.

> **Definition :** An element $e \in S$ of a set S equipped with an operation $\star\colon S \times S \to S$ is an identity for that operation if for all $s \in S$, the following is true:
>
> $$e \star s = s \star e = s$$
>
> > **Example :** Zero is the identity for the operation of $+$ on the integers. The function $f(x) = x$ is the identity for the operation of composition on the set of functions from $\mathbb{R} \to \mathbb{R}$.

> **Exercise :** Prove that if an operation $\star$ on a set S has an identity, that this identity is unique (that is, there cannot be two distinct elements of S which both satisfy the definition above).

> **Exercise :** True or false: there is an identity for the operation $(x, y) \mapsto x^y$ of exponentiation on the positive integers $\mathbb{N} = 1, 2, 3, \ldots,$

So, addition and multiplication are not just any old operations, but now we have precise definitions to describe some of the properties they enjoy: both are commutative and associative operations, and both have an identity element. While this is great theoretical progress, one might worry that we aren't even half way to our goal: after all, we haven't said anything at all about subtraction or division! (And at first glance these may seem as though they'll require significant thought: indeed, is subtraction even commutative or associative?)

However, we are actually much closer to our goal than it may look: subtraction and division are not wholly independent operations from addition and multiplication, but rather are *defined as inverses to them*. So, instead of codifying two additional operations, it will instead suffice to write down a single additional property, that of invertibility, that elements may posess with respect to a given operation.

> **Definition :** If S is a set with operation $\star$, and assume this operation has an identity $e \in S$. Then an element $s \in S$ is said to have $t \in S$ as an inverse if $s \star t = e$. An element $s \in S$ is said to be invertible if it has an inverse. The operation $\star$ is said to be invertible if every element of S is invertible.

> **Exercise :** Is addition invertible on the integers? Is multiplication? How about the same questions, but on the rational numbers instead?

Starting from our common, but non-rigorous experience with addition and multiplication, we have rigorously spelled out several properties each of these operations has: they are commutative, associative, and invertible.

> **Definition :** A group is a set G with an associative invertible operation $\star$ with identity e. If $\star$ is commutative, G is called a commutative group, or an 'abelian group' [^2]

The abstract study of groups - that is, understanding *all possible* associative invertible operations is a foundational topic in the modern field of abstract algebra. Much beyond our humble goals of axiomatizing the number line, from this simple theory springs forth a wealth of examples which have completely transformed the landscape of modern mathematics and theoretical physics over the past century. Along our journey, we will not have the need to explore deep into the mysterious jungle of groups, but will rather be content having the term 'group' a means of succinctly collecting together (some may say....'grouping') operations which are particularly 'nice'. To continue the jungle analogy, we will be less concerned with our ability to classify all species of panthers than we are with our ability to recognize ‘oh- that is a cat’.

Fields

The group concept does an excellent job of formalizing each of the operations of addition and multiplication individually, but to get the full power of arithmetic we need to combine them into a single, coherent whole.

What is this relationship between addition and multiplication? These operations find their original home on the set of positive whole numbers, where addition measures concatenation of lengths and multiplication measures areas. Here, the relationship between the two is geometrically both beautiful and transparent: multiplication is repeated addition! Indeed, given any rectangular array of dots, one can disassemble the rectangle into lines, and concatenate these lines end to end, to get a single line with the same number of dots as the rectangle:

While clarifying, this is not a property we wish to take as “the” defining relationship between addition and multiplication: it’s too specific! After all, we know our goal is to understand the real numbers eventually, and it seems difficult to make sense of multiplication like $\pi\sqrt{2}$ as saying to “add $\sqrt{2}$ to itself π times”. Instead, we look for a property that is true when one operation is a repetition of another, but that makes sense for arbitrary operations. Thinking operationally once again leads us in the right direction: what is it that we *do* with the fact that multiplication is repeated addition, after all? We use it to justify expressions such as

$$3\star(4+5)=3\times 4+3\times 5$$

saying something like “repeatedly 4+5 three times is the same as repeatedly adding 4 three times and then adding to that the sum of repeated addition of 5 three times”. Abstractly, we say that we have *distributed* the multiplication across both of the terms of the sum:

> **Definition :** The distributive law is a relationship between two commutative operations, here denoted $+$ and $\star$ on the same underlying set S. We say that $\star$ distributes over $+$ if for every triple of elements $a, b, c\in S$ the following is satisfied
>
> $$a\star(b+c)=(a\star b)+(a\star c)$$

It turns out that this distributive law completely distills the essence of how addition is connected to multiplication, and the entirety of arithmetic is encoded by the commutative group axioms for $+$, the commutative group axioms for $\times, and the distributive law relating them. A mathematical object satisfying all of these is called a *field*.

> **Definition :** A Field is a set F together with two binary operations $+, \star$ such that (1) $(F, +)$ is a commutative group. We write the identity element as 0. (2) $(F \setminus 0, \times)$ is a commutative group. We write the identity element as 1. (3) $\star$ distributes over $+$.

> **Remark :** While the symbol $+$ is universally agreed on as the standard notation for the first operation in a field, there isn't quite as strong a convention for the operation which distributes over this (that we call multiplication). Indeed, people often freely switch between $\times$, a raised dot $\cdot$, and no symbol at all - with the juxtaposition of two field elements implicitly denoting their multiplication.
>
> $$a \times b = a \cdot b = ab$$

> **Exercise :** What mathematical structures that you already know are fields? Which are not?

Fields are the abstraction of the ideas of arithmetic: they are the true distillation of the minimal requirements for a collection of objects to possess operations worthy of being called addition, subtraction multiplication and division. For us then, we have reached our goal: to be a ‘number’ will mean to be an element of a field.

> **Example :** Some example fields:

> **Example :** While it will be useful to introduce more notation before we prove many things about fields, can you explain now how from the axioms we know that $0 \neq 1$?

Arithmetic Notation

How do we get from these austere beginnings to the usual theory of arithmetic we learned in childhood? What is the mathematical content of statements such as $1 + 1 = 2$ or $2 \star 2 = 4$? Indeed, what do the symbols 0,1,2,3,4 mean, anyway?

If we look at the field axioms, we see that $(F, +)$ is a commutative group. Since groups have an identity, this means there is some element in F which is the identity of $+$. A priori we know nothing else about this element, but since we know it exists, we might as well give it a name. The traditional name is 0, so we will stick wtih that. So, every field contains at least one element, which we denote with the symbol 0.

But the field axioms also say that after removing this element 0 (“you can’t divide by zero”!) second operation $\star$ turns the remaining elements of F into a commutative group as well. This means there must be some identity element for $\star$, and so we will call this identity element 1. Thus, every field contains at least two distinct elements, which we call 0 and 1.

Positive Integers

Now, since 1 is an element of F and $+$ is an operation, it makes sense to apply this operation to 1 and itself, and in doing so we get another element of the field $1 + 1$. This precisely and uniquely defines the element, but is a rather cumbersome name to carry around: we dont wish to say “the sum of the multiplicative identity and itself” or even “one plus one” over and over. Instead, we will invent a new symbol[2] to represent this concept, to make our writing shorter:

> **Definition :** 1+1=2

> **Remark :** This element $1 + 1$ is certainly an element of the field, but it need to be a "new" element: if you are familiar with modular arithmetic, you may recall that addition modulo 2 has the property that $1 + 1 = 0$. So while we can add 1 to itself, we do not get a new distinct element of the field, but rather we return to an element we already knew about! In light of the above definition, we say that in the field of modular arithmetic mod 2, we have $2 = 0$.

How wonderful is this, to be able to say something as short and sweet as “two”! It’s so wonderful, that it might inspire us to continue down this path, and make an *infinite list of shorthand definitions* to prevent ourselves from ever having to say $1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$ and the like aloud.

> **Definition :** 1+2=3, 1+3=4, 1+4=5, and so on...

We will actually not have use for many of these definitions throughout the class, as we will rarely speak of specific numbers unless we are just doing an example. You’ll be fine so long as you remember the definitions of 2, 3, and 4, and that the variable symbol n means[3] “The result of adding 1 to itself n times”

The Negative Sign

By the field axioms, $+$ is invertible so every elememnt x has some inverse y where $x + y = 0$. Since phrases like “the additive inverse of x” will come up often, it will be useful to have a symbol for it. Thus, we introduce as a shorthand the dash $-$:

> **Definition :** If x is an element of a field, we write $-x$ to denote the inverse of x. As a further shorthand, if we are to write the result of adding a field element z to the additive inverse of x, we allow ourselves to omit the $+$ sign and write
>
> $$z + (-x) := z - x$$

We should be careful when making up a notaiton like this: while it seems innocent there's a hidden assumption we must check. Namely, what would happen if a certain field element had three different inverses? How would we decide which one should be called $-x$? (We certainly should not call all three of them by the same symbol! That would lead to hopeless confusion)

> **Proposition :** Additive inverses are unique: if $y \in F$ and $z \in F$ are both inverses of $x \in F$ then $y = z$.

So far, so good. The dash is an unambiguous notation choice.

Can we say anything about the additive inverse of 1? You might think it would be easy to prove that $-1 \neq 1$, but in fact this is not possible from the field axioms alone! The field axioms do not pick out a single mathematical object but rather a wide and varied class of structures, and in some fields it is the case that $-1 \neq 1$ whereas in others $-1 = 1$! Of course, on the number line we know these two numbers are not equal, and so we will need to prove this at some point: this is a hint that we will *require* further axioms down the road.

> **Example :** (For those who have seen some abstract algebra) Can you give an example of a field where $-1 = 1$?

> **Example :** For those who have seen modular arithmetic, what is -3 in $\mathbb{Z}_7$?

Multiplicative Inverse

Just as we use a dash to denote the additive inverse, it will also prove extremely convenient to have a notation decorating a field element x to denote *the multiplicative inverse of* x. Following standard convention, we denote this inverse with a superscript -1 (this fits well with the notation for powers, to be introduced shortly). Similarly to the case for $+$, such a notation only makes sense if there is a unique inverse for each element: can you apply the same idea as in the proof there to confirm this? [4]

> **Definition :** If F is a field and $x \in F$ we write x^{-1} to denote the multiplicative inverse of x.

Just as for addition where it is often useful to omit the $+$ sign when adding an inverse (and write directly $x - y$ which we tend to call 'subtraction' in our youth), it is similalrly useful to come up for a noation which omits the multiplication sign when multiplying by an inverse: for this, we use the slash

> **Definition :** As a shorthand notation for the product $a \cdot b^{-1}$ we write a/b, or $\frac{a}{b}$.

Thus, since $x^{-1} = 1 \cdot x^{-1}$ (1 is the multiplicative identity, after all) using this convention we may write

$$x^{-1} = 1 \cdot x^{-1} = \frac{1}{x}$$

Powers

We will need to do a lot of work before we can talk generally about exponentation (even for real numbers), but much like for multiplication the story simplifies drastically for *positive integer* exponents, where we may rigorously define exponentation as repeated multiplication.

> **Definition :** Let F be any field and $x \in F$. The symbol x^2 denotes the product xx, the symbol x^3 denotes xxx and so on, with the symbol x^n being a short hand for the product of n copies of x.

From our rigorous mindset, we should be a little nervous about introducing this meaning of superscripts, given we already have a definition of superscript -1 which means multiplicative inverse, seeming nothing to do with repeated multiplication! Do these notations fit together well, or conflict with one another? Indeed, x^{-3} is currently defined to mean the multiplicative inverse of x^3 (usually seen as the identity $x^{-3} = 1/x^3$ in high-school algebra classes). But it could also plausibly mean the result of repeated multiplying x^{-1} by itself three times. But this poses no issues

> **Proposition :** $x^{-3} = x^{-1}x^{-1}x^{-1}$

Of course there is nothing special about "3" in the proposition above, and one can prove by induction that the multiplicative inverse of x^n is the product of n copies of x^{-1}.

Convention: if there is a "simpler" symbol in a field to denote an element, we use it (eg lowest term fractions, or use 0 instead of 2 in binary…)

Properties of Fields

> **Proposition :** $2 + 2 = 4$
>
> > **Proof :** This proof is essentially a suffling of definitions and the field axioms: since $2 = 1 + 1$, we can rewrite the left hand side as $(1 + 1) + (1 + 1)$ And since $4 = 3 + 1$ and $3 = 2 + 1$ we can re-write the right hand side as $1 + (1 + (1 + 1))$. Now that these definitions have been unpacked, we just need to use the field axioms to move the parentheses from one of these configurations to the other. This can be done in a single step starting on the left side, were associativity of $+$ allows us to take $(1 + 1) + x$ to $1 + (1 + x)$ for any x. Substituting $x = 1 + 1$ gives

> > $$(1+1)+(1+1)=1+(1+(1+1))$$
> >
> > as required.

> **Proposition :** $2 \star 2 = 4$
>
> > **Proof :** Since $2=1+1$ by definition, we expand the second 2 in the expression above to give $2 \star (1+1)$. Next, we use the distributive axiom which implies $2 \star (1+1) = (2 \star 1) + (2 \star 1)$. Recalling that 1 is by definition the identity of the operation $\star$, we see that $2 \star 1 = 1$ and so $(2 \star 1) + (2 \star 1) = 2 + 2$. Using our previous proposition in which we proved $2+2=4$, we see that this is then equal to 4. Thus, as claimed $2 \star 2 = 4$.

In fact more generally we can show that twice repeated addition, in any field, is the same as multiplication by 2.

> **Exercise :** Let F be any field, and $x \in F$ an arbitrary element. Then $x + x = 2 \star x$.

> **Theorem :** In any field, $-0=0$ and $1^{-1}=1$.

> **Theorem :** In every field, $0 \cdot x = 0$

> **Theorem :** In every field, $-x = -1 \cdot x$

> **Theorem :** In any field $p/(-q) = (-p)/q = -(p/q)$.

> **Theorem :** In every field $(xy)^{-1} = x^{-1}y^{-1}$.

> **Theorem :** If F is any field and $a, b \in F$ are any two numbers, then $(a+b)(a-b) = a^2 - b^2$

> **Theorem :** If F is any field and $a, b \in F$ are any two numbers, then $(a+b)^2 = a^2 + 2ab + b^2$ (recall the symbol 2 is by definition $1+1$ so $2=0$ in $\mathbb{Z}_2$)

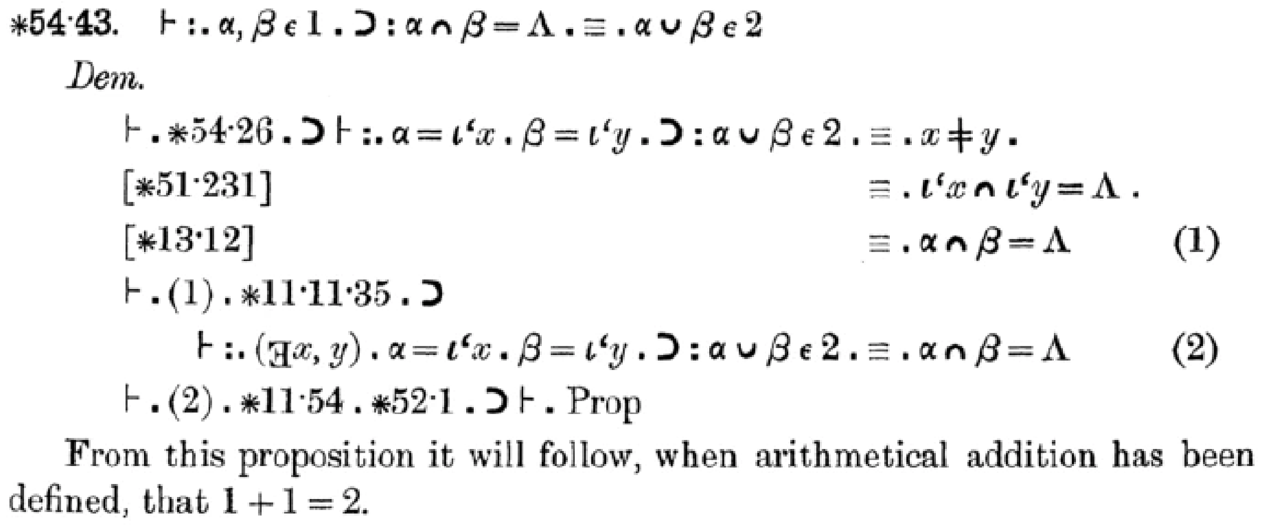
What can we say about division by zero? The field axioms do not *require* one to be able to divide by zero, but they do not directly *prohibit it* (they simply require that $(F \smallsetminus 0, \star)$ is a group, but perhaps for certain special fields, $(F, \star)$ could be a group as well?)

> **Theorem :** Zero does not have a multiplicative inverse in any field.
>
> > **Proof :** Assume for the sake of contradiction that 0 has an inverse, and use this to deduce a contradiction.

---

1. Direct uses of numbers for counting have of course been around much longer than even our species: there is good evidence that even relatively simple insects such as bees and ants have sophisticated neural circuits designed to count. See for example this article on bees ↩

2. From our perspective, this is a definition (of field theory) rather than a theorem. However, if you peer deep enough into mathematical logic, there are many subtlties left to uncover. See this site for a brief look at a purely logical proof of $1+1=2$ originally appearing in Whitehead and Russel's *Principia Mathematica*, published in 1910. To get to the proof takes approximately 1,000 pages of dense mathematical logic, but the "core" idea is here (expressed in their unfortuantely inpenetrable notation)



*54·43. $\vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . {*}54{\cdot}26 . \supset \vdash :. \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

[*51·231] $\equiv . \iota`x \cap \iota`y = \Lambda .$

[*13·12] $\equiv . \alpha \cap \beta = \Lambda$ (1)

$\vdash . (1) . {*}11{\cdot}11{\cdot}35 . \supset$

$\vdash :. (\exists x, y) . \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda$ (2)

$\vdash . (2) . {*}11{\cdot}54 . {*}52{\cdot}1 . \supset \vdash .$ Prop

From this proposition it will follow, when arithmetical addition has been defined, that $1+1=2$.

↩

3. As stated, this sounds circular! But do not worry: the symbols 2,3...n will have no rigorous roll in our course other than to save us from writing impossible-to-read strings like $(1+1+1+1+1+1+1)/(1+1+1+1)$. So long as you understand what p/q means in terms of the field axioms, you are fine! ↩

4. This is actually a result that is common to all groups: inverses are unique! So the argument goes through unchanged simply swapping out the symbol $+$ for the symbol $\times$. ↩

Section 1.2

Orders

We are trying to axiomatize the idea of the real numbers: these are used for measuring things! So, we need a way to tell when one number is "bigger" than another. In the real world we use inequality: but what is an inequality?

Order Axioms

The textbook for our class directly axiomatizes the concept of inequality, but we are going to depart from that and take one step further back: we are going to axiomatize what it means to be *positive*, and then *derive* the concept of inequality from that. If F is a field, we wish to describe the subset $P \subset F$ of positive numbers by axioms; that is, by how positive numbers behave. What are some basic properties we know to be true of positive numbers?

- Every number is either positive, negative, or zero
- Adding two positive numbers gives a positive number
- Multiplying two positive numbers gives a positive number.

Turning these into axioms, we have

> **Definition :** An order on a field F is a subset $P \subset F$ satisfying the following three properties. 1) For each $x \in F$, exactly one of the following holds: $x = 0$, $x \in P$, or $-x \in P$. 2) If $a, b \in P$ then $a + b \in P$ 3) If $a, b \in P$ then $ab \in P$.

If a field F has a subset P satisfying these properties, we call the pair (F, P) an ordered field, and say F has ordering given by P. We call the elements of P *positive numbers*, and the nonzero elements of $F \setminus P$ the *negative numbers*.

> **Remark :** Not all fields admit an ordering (as we will see soon, with $\mathbb{C}$). And of fields that do admit an ordering, it is not always unique (as we will optionally see later, with a field called $\mathbb{Q}[\sqrt{2}]$).

Inequality

While it may not seem sufficient at first, having only determined which numbers to call positive is actually enough to order the entire field along a line! For the rest of this section, we will fix a field F and an ordering P on F. If a, b are in our ordered field, how do we use P to determine which is bigger? Again it is best to think back to what we are used to doing from grade school, so that we can formalize that as a definition.

> **Definition :** If a, b are elements of an ordered field, we write $a < b$ as a shorthand for the statement that $b - a \in P$. Similarly, we write $a \leq b$ if either $a = b$, or $a < b$. To make things easier

> in natural writing, we allow ourselves to write $b > a$ as a synonym for $a < b$, and $b \geq a$ for $a \leq b$.

> **Remark :** If $x \in P$ then $x > 0$ since $x - 0 = x \in P$, following the definition above.

Definitions

Given the concept of positive, we can press on further and rigorously define not just inequality, but also the familiar concepts of absolute value and the square root, which will show up throughout our course.

Absolute Value

> **Definition :** The absolute value of an element x of an ordered field F is defined as
>
> $$|x| = x \text{ if } x \in P$$
>
> $$|x| = -x \text{ if } x \notin P$$

Note this definition says that we define $|0|$ as -0 since $0 \notin P$. But we have previously shown thatn $-0 = 0$ so together this shows $|0| = 0$ as we are more accustomed to writing.

> **Proposition :** $||x|| = |x|$ Taking the absolute value a second time does not change anything.

> **Proposition :** In an ordered field $x^2 = |x|^2 = |x^2|$ for all x.

The Triangle Inequality

The triangle inequality is an extremely useful tool for producing inequalities in analysis. Its statement uses the absolute value, and its proof requires only the order axioms, so it is true in every ordered field.

> **Theorem :** If a, b are elements of an ordered field F then
>
> $$|a + b| \leq |a| + |b|$$

Square Root

> **Definition :** Let $x \in F$ be a field element. If there exists some $y \in F$ with $y^2 = F$ we call y *a square root of x*.

> **Proposition :** The unique square root of 0 in a field is 0. If $x \neq 0$ has a square root in a field F, then it has exactly two distinct square roots.

Because the two square roots are additive inverses of one another, the order axioms require that exactly one of them be positive and the other must not be. This allows us to define a unique *positive square root*, and a symbol to go with it.

> **Definition :** Let F be an ordered field, and $x \in F$ a nonzero element which has a square root. We then define the symbol $\sqrt{x}$ to denote the unique element of F which is both (1) in P, and (2) squares to x.

Note that the field axioms certainly do not require that square roots exist: we are *only* allowed to write $\sqrt{x}$ once we are already sure that x has *some* square root in F (at this point, the symbol just disambiguates the positive root from the negative one).

Properties of Ordered Fields

Some basic proofs that will be useful in the future go here.

> **Proposition :** In any ordered field, 1 is positive.

> **Proposition :** In any ordered field, no finite sum of 1's is equal to zero.

> **Theorem :** Every ordered field contains the natural numbers as a subset

> **Theorem :** Every ordered field contains all the rational numbers as a subset.

> **Theorem :** The complex numbers do not admit any ordering.

Section 1.3

Gaps

Constructing the Ordered Field $\mathbb{Q}$

We have shown that $\mathbb{Q}$ has a unique ordering (coming from the necessity that $1 \in P$) but it's nice to stop for a minute and see how to actually *realize* this ordering by assigning the elements of $\mathbb{Q}$ to points on a line.

There's a nice construction of this dating back to ancient greece requiring only a ruler and a compass, that represents one of the first hints at the deep connection between the *algebraic* study of numbers and the *geometric* study of lines, curves, and figures in the plane.

First, given a straightedge, we choose a fixed length that we will call 1 (this is just picking a unit, be it inches, feet, centimeters, or whatever you like). From here one can immediately construct the integers, by successively laying out this length, from a starting point we label "zero".

The relation of *less than* is instantiated geometrically as *to the left of*: that is, given our assignment of integers to the line, the phrase $a < b$ translates directly to a *is to the left of* b. But how can we extend this to all rational numbers? How can we determine a rule that lets us place all numbers (including things like $12432/57384920287$) along the number line in a precise position, so that this remains true?

The first simplifying assumption is to notice that if we can figure out where the number $1/q$ goes along the number line for any positive integer q, that will be sufficient, as just like we constructed the number n by repeatedly laying out copies of the already-known length 1, we can then construct p/q by repeatedly laying out copies of $1/q$. So, how do we find $1/q$'s position along the line?

Finding this point is easy so long as you can construct a line of slope q: if this line intesects the vertical (y-axis) through the point you've called zero at a distance of 1 below 0, then it intersects the number line at $1/q$. The greeks had no troubles constructing such a line exactly, using a combination of a ruler and compass to (provably) draw a parallel line to the original at height -1, construct a right angle at $(-1, 1)$, and then measure a distance of q vertically to reach the point $(1, q-1)$. Connecting this point to $(0, -1)$ using the straight-edge produces the point $1/q$.

PICTURE

Remark: one can actually do the same thing for general p/q by constructing a rectangle of size $p \times q$, shifting it down by 1, and marking the intersection of the diagonal with the number line.

This seems to be a fundamental triumph: we have precisely algebraically described what numbers *are* in terms of their operations, precisely defined their ordering, and managed to identify them with the points of a line, producing the familiar *numbr line* picture we all imagine in our minds.
But unfortunately, the story is far from over.

The square root of 2.

Having such an explicit construction of the number line in front of us, it is easy to make the implicit assumption that not only is every (rational) number assigned a point on the line, but in fact that every point along the line has been assigned to some rational number. Indeed, experimentally this is all but true: given any point on the line, to within the precision of any measuring device you like you will find that that point to be indistinguishable from some rational p/q.

But we should not be satisfied with any heuristic argument, and neither were the greeks. We would like a proof one way or another, that the ordered field of the rationals in fact captures all the points of the number line.
This problem met its resolution almost 2500 years ago, through an ingeniously simple argument that has been handed down to us all the way until today.

The fact that the square root of two is a number is indisputable following Pythagoras if numbers are supposed to be *the things that measure magnitudes*, as is the length of the diagonal of the unit square.

But there's other ways to see that it must occupy some point along the real line as well. The greeks had a geometric understanding of continuity, which today we might think of as an axiom that if one curve starts below a given line and ends up above it, then it must have intersected that line at some point (we will prove this from our modern axioms later, in a guise known as the *intermediate value theorem*). Starting from the parabola $y = x^2$ (well known to the greeks), simply shift it down by 2 units: now it starts below the real line, and ends above, so it must have intersected at some point. But what is this point? It's a number which must square to two!

Of course, no one knew *which* (implicitly assumed rational) number this was, but it was the length of a straight line segment so geometrically it is as good a number as any. However in the century following Pythagoras, an incredible discovery was made:

> **Theorem :** The length of the diagonal of a square is not rationally related to the length of its sides.

In modern terminology, we would say "there is no rational number which squares to 2". To prove this rigorously, we need a useful property of the natural numbers called Euclids lemma: we have not proven this formally from our axioms but that is OK, as we are only doing an example right now anyway:

> **Lemma :** If p is a prime number and p divides the product ab then either p divides a or p divides b.

> **Theorem :** There is no rational number whose square is 2.
>
> > **Proof :**

Filling this Gap

How are we to come back from the devastating discovery that while there are rational numbers seemingly *everywhere* on the line, there are yet more numbers to be discovered? A first thought is that we should simply add $\sqrt{2}$ to our number system, forming perhaps $\mathbb{Q} \cup \sqrt{2}$. But this immediately runs into trouble! This collection is no loger a field, as the sum of 1 and $\sqrt{2}$ is undefined. So, we may wish instead to add all terms of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$.

> **Definition :** The Field $\mathbb{Q}[\sqrt{2}]$ is the set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ together with the operations of addition defined 'componentwise', and multiplication defined by multiplying out the terms, and using $\sqrt{2}^2 = 2$.

It may be surprising this is a field: forced it to be closed under addition, but why is it closed under multiplication or division? Why don’t we need to add numbers like

$$\frac{1 + 2\sqrt{2} + 3\sqrt{2}^5}{3 - \sqrt{2} + 17\sqrt{2}^{14}}$$

> **Proposition :** $\mathbb{Q}[\sqrt{2}]$ is indeed a field: in particular, the multiplicative inverse of $a + b\sqrt{2}$ is of the form $c + d\sqrt{2}$ for some c, d.

Oh no.....

It would be optimistic to hope this has solved our problem: we discovered a number that was missed by the rationals, and successfully added it to our field. However, far from the end of the story this is just the beginning:

> **Theorem :** $\sqrt{3}$ is not an element of $\mathbb{Q}[\sqrt{2}]$.

You’ll prove this on your homework. What if we try to add both $\sqrt{2}$ and $\sqrt{3}$ to the rational numbers, and then throw in everything that is necessary for it to be a field? While the set $a + b\sqrt{2} + c\sqrt{3}$ is closed under addition, to make a field we need to also include multiples of $\sqrt{2}\sqrt{3} = \sqrt{6}$ so that it is closed under multiplication. But then, by a similar argument to the proposition (exercise) above, this is enough to make a field

> **Definition :** The field $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$ is the smallest field containing the rationals as well as $\sqrt{2}$ and $\sqrt{3}$.

Unfortunately, you probably see where this is going....

> **Proposition :** $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$

A bolder move might be to attempt to add *all square roots of all rational numbers* to make some new, much much larger field. Let's call this field $\mathcal{S}$ for *square roots*. Then, while we have solved all the problems disovered so far by filling all the "square root shaped gaps" in the line, we are still far from done:

> **Theorem :** $\sqrt[4]{2} \notin \mathcal{S}$.

Constructible Numbers

Level 0 = Rationals

Level 1 = Use circles with rational radii, lines with rational slopes

Level 2 = Use circles with level 1 radii and level 1 slopes....

Etc....implicit assumption: we got all the numbers on the line now!

Remaining questions: cube root of 2 and pi?

The gaps abound

It took until 1837, but Pierre Wanzel proved that $\sqrt[3]{2}$ is *not constructible* - its a gap in the Greek number system! And, in 1887, the last of the greek problems fell when π (and hence, $\sqrt{\pi}$) is not the solution to *any* polynomial equation whatsoever. Since circles are quadratic curves and straight lines are *linear*, all constructible numbers are some (very complicated) iterated combination of square roots, and thus are the solution to some (very high degree, very complicated) polynomial. In the intervening years, a new gap was also discovered, Euler's number e was proven to not solve any polynomial in 1873 by Charles Hermite.

Of course, just like the first time, the discovery of new gaps opens the floodgates: since π solves no polynomial equation neither does $3 + 2\pi$ or $\pi^3 - 8\pi^{17}$, etc.....

{

> **Remark :** While it is known that π, e are not the solutions to any polynomial equations (called, algebraic numbers), it is unknown whether or not $\pi + e$ or πe are algebraic. In fact, it is unknown if either of these are rational! (But it is known, that at least one of them must not be...can you see why?)

Section 1.4
Completeness

What is a "gap" formally? If we have a field like $\mathbb{Q}$, we've been using *gap* when we find a number that is not in the field, like after proving $\sqrt{2} \notin \mathbb{Q}$ we said that "$\sqrt{2}$ is a gap in $\mathbb{Q}$". But now that we are going to try and be axiomatic about it, we need to be much more precise: for instance, $\sqrt{-1}$ is also not rational number, but we don't want to imply that it represents a *gap*: indeed we do not expect there to be any point on the line which squares to -1, as we showed such a number cannot exist in an ordered field.

So, 'gap' should mean something like 'x is not in the field, but x *should be* on the number line'. But axiomatic mathematics has no room for a concept like *should*! We are in the business of making precise statements about numbers, not moral judgements of them. So, what does *should be on the number line* really mean? Better (remember how we came up with the axioms of arithmetic), how could one operationally tell what counts as a gap and what does not?

It's easiest to start if we look at a number that's not a gap. What happens if you try to cut the number line in half at the number 0? Once you've cut it in two, the number 0 itself is an endpoint of one of the pieces (its either the largest number of the left piece, or the smallest number of the right piece).

Contrast this with $\sqrt{2}$, where there is a point along the number line that we can split $\mathbb{Q}$ into two disjoint sets, the smaller of which has no maximum element **and** the larger of which has no minimum. (This is of course because such min or max would be $\sqrt{2}$, which is not a rational number).

It is *this* distinction that we wish to axiomatize: how do we say concisely (and precisely) that any way of splitting the number line like this leads to a max or a min, so that there was no gap there? To do so, we need to introduce some terminology. First, an essential part of our *cutting process* is that each cut 'ends' at some finite point along the line (the trick is, of course, we can't say *where* the cuts end because we are trying to *axiomatize* the existence of a number at that location).

To stay truest to our picture, we could define rays (where we may say a positive ray is a subset R of a field F such that if $s \in R$ and $t > s$ then $t \in R$, and a negative ray is the reverse, where $s \in R$ and $t < s$ implies $t \in R$), and then define what it means for a ray to stop, or be bounded at some finite distance. But for future purposes, it will be easier to not bother with this added complexity, and just defined *bounded* for arbitrary sets directly.

> **Definition :** Let F be an ordered field, and $S \subset F$ a subset. We say that $u \in S$ is an upper bound for S if $s \leq b$ for all $s \in S$. When there exists an upper bound, we say that S is \emph{bounded above}. Similarly, $\ell \in F$ is a lower bound if $\ell \leq s$ for all $s \in S$, and S is bounded below if there exists a lower bound. A set S is called *bounded* if its bounded above and below.

Any subset of the line that could be the lower part of a cut will be bounded above (any point in the upper cut will be an upper bound), and likewise the upper cut is bounded below (any point in the lower cut is a lower bound). So, how do we now say that such cuts result in either one of the sets having a minimum or the other having a maximum? We would prefer to do this without an *or statement* as we are trying to write an axiom, and simpler is always better.

> **Definition :** Given a nonempty subset $S \subset F$ of an ordered field which is bounded above, we say that an upper bound b is the *least upper bound* if for every other upper bound u of S, we have $b \leq u$. When such a least upper bound exists, we call it the *supremum* of S and write $b = \sup S$ to denote it.

The supremum of a set does exactly the job we want: it specifies the maximum of S when there is one, and if S has no maximum, it is the *minimum* of the set of points $T = \{x \mid x > s, , \forall s \in \S\}$.

> **Lemma :** Prove this: if $S \subset F$ is a nonempty subset of an ordered field which has a supremum σ, then either (1) σ is the maximal element of S, or (2) σ is the minimal number larger than all elements of S.

We can define an analogous concept for sets bounded below: the greatest lower bound, or the infimum. This is the definition focusing on the 'upper cut' versus the 'lower cut'.

> **Definition :** Let S be a nonempty subset of an ordered field F which is bounded below. A lower bound b is the greatest lower bound if for every other lower bound ℓ of S, we have $\ell \leq b$. When such a b exists, we call it the infimum and denote it by $\inf S$.

To say that a particular way of cutting the number line does not hit a gap, we may say that the lower cut has a supremum, or that the upper cut has an infimum. To say that the number line has no gaps at all, we might say that *every possible cut* has a supremum (or infimum). This is the spirit of the **completeness axiom**

> **Definition :** *The Completeness Axiom*: Every nonempty subset $S \subset F$ which is bounded above has a supremum.

If an ordered field F satisfies the completeness axiom, we say that field is complete.

> **Example :** The rational numbers are not complete.
>
> > **Idea :** Let $S = s \in \mathbb{Q} \mid s^2 < 2\}$. Then S is a nonempty subset of $\mathbb{Q}$ (note that $1 \in S$, for instance), and that S is bounded above (this needs proof, but for example 2 is an upper bound for S because everything bigger than 2 squares to something bigger than 4, and so cannot be in S). Next, we need to see this set has no least upper bound: can you show that if u is some upper bound, then there exists a natural number N where $u - \frac{1}{N}$ is also an upper bound?

One natural question to ask here is: why focus on supremum? Could we also have defined the completeness axiom using infima instead?

> **Proposition :** If an ordered field F is complete, then every nonempty set which is bounded below has an infimum.

Section 1.5
The Real Numbers

We finally have the correct axiom set to describe the number line: its an object known as a *complete ordered field*.

> **Definition :** A complete ordered field is a set F equipped with two operations $+\star$ such that $(F, +, \star)$ satisfies the field axioms, and a subset $P \subset F$ satisfying the order axioms (making (F, P)

> into an ordered field), which also satisfies the completeness axiom for ordered fields.

That is, F is a set which has the operations that allow us to call it *numbers*, and an order that allows us to place it onto a line, and furthermore, a certificate of assurance that once it's been placed onto a line, there are no gaps. A natural question to ask at this point is, what are some complete ordered fields? In each previous incarnation of the axioms, we've seen that adding more axioms makes smaller and smaller the collection of objects that satisfy them. We have $\mathbb{Q}, \mathbb{Z}_3, \mathbb{C}, \mathbb{Q}[\sqrt{2}]$ as fields, but of these, only $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{2}]$ are *ordered fields*. Which ordered fields are complete? The completeness axiom is a different beast then the rest: instead of slowly building up from the simplest ordered field ($\mathbb{Q}$) by adding each new gap we found, instead we have jumped over the whole process into the unknown, and simply defined what it means to be "done". This makes it hard to write down any examples at all of a complete ordered field.
Indeed, how do we know there even are any at all?
While the proof of the following is beyond our current abilities,

This theorem should (finally!) bring comfort to us along our quest. We truly have fully captured the notion of the number line in a precise axiomatic system (existence), and there is no ambiguity given these axioms, what we could mean (uniqueness). While we will not prove this theorem now, nor use it in our rigorous development (since we have not proved it, we should not do so), we *will* use it to justify one piece of sloppy language we will find incredibly useful.

Instead of constantly saying "a complete ordered field", we will say "the real numbers", where the switch from the indefinite *a* to the definite *the* is justified by us knowing that there truly is only one field in all the mathematical universe which satisfies the axioms we have written down.

Consequences of Completeness

As a complete ordered field, the real numbers enjoy any property that we have already shown that all ordered fiels must have. In particular:

> **Theorem :** The rational numbers are a subset of $\mathbb{R}$.

> **Theorem :** There is no real number which squares to -1.

But with the extremely powerful axiom of completeness now in our hands, we can go much further. The first thing we shall do is show that the real numbers share an important property with the rationals, called the \emph{Archimedean property}. (You prove the rationals have this on the homework).

> **Definition :** An ordered field is said to be Archimedean, or to have the Archimedean property if for every positive $a, b \in F$ there exists some natural number $n \in F$ (remember, the natural numbers are a subset of any ordered field) with $na > b$,

The way I think of this property is saying that the field elements a, b aren't too far apart: their difference can be quantified by some natural number. More colloquially, I remember this by the phrase "you can empty even the oceans with a teaspoon": if b is the volume of the ocean, and a is the volume of a teaspoon, there is some large integer n where if you take n scoops out of the ocean, you'll empty it (na is bigger than b). While the ocean is gigantic, its not *immeasurably larger* than a teaspoon. The same holds for any two numbers in an archimedean field: no positive element is *immeasurably larger* than any other.

> **Theorem :** The real numbers are archimedean.
>
>> **Proof :** Assume for the sake of contradiction, that this property fails. Then there is some particular positive $a, b \in \mathbb{R}$ where for *no possible* $n \in \mathbb{N}$ do we have $na > b$. Equivalently, for *every natural number n* we must have $na \leq b$. If $S = \{na \mid n \in \mathbb{N}\}$ this is just the definition of the statement "b is an upper bound for S". The set S is nonempty (for instance, since $1 \in \mathbb{N}$ we have $1a \in S$), and bounded above (b is an upper bound, as we just saw). Thus, the completeness axiom **requires** that S have some least upper bound σ. What properties can we tease out of σ to reach a contradiction? Since $a > 0$, we can prove from the order axioms that $\sigma - a < \sigma$. But σ is supposed to be the *least upper bound* for our set S. Thus, $\sigma - a$ cannot be an upper bound, which means there must be some element $na \in S$ with $na > \sigma - a$ (if there were not, it would be larger than all elements, and so would in fact be an upper bound). But this immediately puts us into trouble: adding a to both sides shows $na + a > \sigma$, and some easy work from the field axioms allows us to simplify the left hand side to $(n+1)a$. Since n was a natural number, so is $n+1$, so $(n+1)a$ is an element of S by definition. That means we managed to find an element of S which is larger than σ! So σ cannot be an upper bound at all, much less the supremum. This is our contradiction, and so there could not have been such a pair a, b in the first place.

This property will prove particularly useful to us as we continue on our real analysis journey. Indeed, it immediately unlocks a few secrets of the real numbers that are worth dwelling on before we push forwards.

Infinities and Infinitesimals

Remember in the non-rigorous history of calculus, we discussed several imagined propreties that numbers might have to make a certain argument work:

> **Definition :** A nonzero number x is said to be *nilpotent* if some power $x^n = 0$. (This is often used in non-rigorous arguments saying something like dx is so small that $dx^2 = 0$...).

> **Definition :** A number x is called *infinitesmial* if it is positive, but is smaller than every rational number. Such numbers are used non-rigorously when thinking $dx = 0.0000.\ldots.01$ as something

> smaller than $1/10^n$ for any n....

> **Definition :** A number N is called *infinite* if it is an upper bound for the natural numbers: if $n

Now that we have spent some serious energy tracking things back to the very beginning, we can rigorously investigate the sensibility of these various ideas.

> **Theorem :** There are no nilpotent real numbers.
>
> > **Proof :** $\mathbb{R}$ is a field, and so in particular $(\mathbb{R} \smallsetminus 0, \times)$ is a commutative group. That means if $x \in \mathbb{R}$ is nonzero, xx is nonzero. This is the base case for an argument by induction that $x^n \neq 0$ for any n.

> **Theorem :** There are no infinitesimal real numbers.
>
> > **Proof :**
>
> Think about what would have to be the case if there *were* an infinitesimal $\varepsilon \in \mathbb{R}$. Then ε is smaller than every positive rational, so in particular for every $n \in \mathbb{N}$, we have $0 < \varepsilon < 1/n$. Multiplying this inequality through by n we see that
>
> $$\forall n \in \mathbb{N} \text{ we have } 0 < n\varepsilon < 1$$
>
> But this contradicts the Archimedean property: as ϵ and 1 are both positive numbers and ϵ is so small that no natural number multiple of it exceeds 1.

This statement of the non-existence of infinitesimals is very useful as a positive statement as well, we record it as an important corollary of the Archimedean property:

> **Corollary :** If ϵ is any positive real number, there exists a natural number n with $0 < \frac{1}{n} < \epsilon$.

This has a second important corollary (which is in fact equivalent):

> **Theorem :** There are no infinite real numbers.
>
> > **Proof :** Again, assume for the sake of contradiction that some infinite number exists in $\mathbb{R}$, call this number I. Then since $I > n$ for all natural numbers n we may invert this inequality to see that $1/I < 1/n$: that is, $1/I$ (which is a perfectly well-defined field element, since $I \neq 0$) is infinitesimal, contradicting the theorem above.

Thus, any intuitive proofs of calculus type concepts using these sort of numbers are *wrong*: no such numbers exist on the real line! Much of the work of real analysis is to put all of this mathematics on a true, rigorous footing.

> **Remark :** Arguments using infinitesimals are both so intuitive and convincing that people wondered for about a century if there was any means of finding *some* number system which had them, in which one could attempt to salvage the old arguments of calculus. Of course, after the uniqueness theorem was proved for complete ordered fields, it was clear that this would be impossible, without giving up one of the properties of (1) field, (2) ordered, or (3) complete. In the 1960's Robinson discovered (using a significant amount of mathematical logic) that one can indeed

> build an ordered field that *contains* $\mathbb{R}$ as a proper subset, but also contains infinitesimals! Of course, this field (called the *hyperreals*) is no longer complete.....

A note on the symbol ∞.

While we have just proved that there do not exist any infinite real numbers, the concept of *potential infinity* is extremely useful as a shorthand. Consider the following completely rigorous sentences:

“The set of all numbers greater than 1”

“S is not bounded above”

We will use the symbol ∞ as a shorthand for statements like this. But it is extremely important to remember **infinity is not a number, and these statements are only shorthands**. We will add more of these shorthands as the course progresses, but for now we will write things like

$$(a, \infty) \iff \{x \in \mathbb{R} \mid x > a\}$$

$$(-\infty, a) \iff \{x \in \mathbb{R} \mid x < a\}$$

$$\sup S = \infty \iff \text{S is not bounded above.}$$

$$\inf S = -\infty \iff \text{S is not bounded below.}$$

The Existence of an Irrational Number

As we will keep talking about this set of new numbers, it’s useful to give them a name:

> **Definition :** An irrational number is an element of the real numbers $\mathbb{R}$ which is not rational.

We defined the real numbers to solve the problem of gaps in the rationals. But our completeness axiom only asserts something about the *existence* of certain suprema, but does not actually guarantee that we’ve added any new numbers: maybe all of these suprema are rational numbers after all! So, we should work to prove this is not the case:

> **Theorem :** Irrational numbers exist.
>
> > **Proof :** We are proving an existence statement, so it's enough to give an example. Happily, there's a natural candidate to try for: if we can prove that there is a real number that squares to 2, then we are done, as we have already proven there is no rational number which squares to 2. This is the result of the following proposition.

> **Proposition :** There is a real number which squares to 2.
>
> > **Sketch :** Let S be the set of real numbers whose square is less than 2. We can show this set is nonempty and bounded, so that $s = \sup S$ exists by the completeness axiom. Since $s \in \mathbb{R}$ we know that $s^2 \in \mathbb{R}$, and what wen need is that $s^2 = 2$. We can prove this using trichotomy, by showing that $s^2 < 2$ and $s^2 > 2$ both lead to contradiction.

Density of Rationals and Irrationals

We have seen, via the nonexistence of infinite numbers, there are no real numbers "beyond" the rationals: all the real numbers are *bounded* by rationals, in the sense that there's some rational bigger, and some smaller than any given real. But *how* exactly the reals are distributed amongst the rationals is still unknown to us.
Could it be that there are entire intervals of real numbers that were added into the number line? Are there gaps between every pair of rational numbers, or just some? With the help of the archimedean property of $\mathbb{R}$, we can come to a complete understanding of these deep questions.

First, a bit of terminology that is standard when discussing questions such as these across mathematics.

> **Definition :** Let F be an ordered field, and $S \subset F$ a subset. We say that S is dense in F if for every pair $a, b \in F$ with $a

If a set S is dense, we may think of that as meaning the set S is *everywhere*: no matter how far you zoom in, and no matter how closely you look, there's some element of S hiding there. Thus, the question of *did we ever insert a whole chunk of new numbers into the line when expanding from* $\mathbb{Q}$ *to* $\mathbb{R}$ is the same as asking *is* $\mathbb{Q}$ *dense in* $\mathbb{R}$? If it is - there's no interval of only non-rationals, any interval $[a, b]$ must contain a rational number r with $a < r < b!$.

> **Theorem :** The rational numbers are dense in the real numbers.
>
> > **Proof :** Let a, b be any two real numbers with $a < b$: we seek a rational number m/n between them. Let $\epsilon = b - a$, so ϵ is positive, and by our corollary to the Archimedean property we have that there exists a natural number n with $0 < \frac{1}{n} < \epsilon$. Multiplying through by n we see $0 < 1 < nb - na$ which means that na and nb are real numbers at a distance of 1 apart. Since na and nb differ by more than 1, there must be some integer m between them (proven below). And since $na < m < nb$, dividing through by n gives
> >
> > $$a < \frac{m}{n} < b$$

The final step of this proof seems "obvious", that between any two real numbers x, y which differ by more than 1 its possible to find an integer. But in our rigorous development, requires its own proof! And, in fact, this statement must require the archimedean property somewhere, as if there were some infinite number I greater than all integers, then there'd be no integer between I and $I+2$, even though they differ by more than 1! It will be easiest for us to divide up the logic of this argument into several simple steps:

> **Proposition :** Every nonempty set of natural numbers has a smallest element.
>
> > **Proof :** Can you prove this?

The above argument involves induction in an important way: and indeed this is necessary. One can show that this proposition is actually *equivalent* to the existence of mathematical induction. (As a challenge, can you prove that if you assume this proposition, that induction works?) Next, we extend this to the integers:

> **Corollary :** If S is a nonempty set of integers which is bounded below, it has a minimum element.
>
> > **Proof :** Can you prove this?

To put this to use for our application, we need a new idea. We want to show that if $x<y$ are separated by more than 1, that there's an integer between them: and it turns out that studying the set of integers greater than x proves the key:

> **Theorem :** If x, y are real numbers with $y-x>1$ then there exists an integer m with $x<m<y$.
>
> > **Proof :** Let $S=\{n\in\mathbb{Z}\mid n>x\}$. Then S is nonempty (this needs the Archimedean property of $\mathbb{R}$!), and S is bounded below (for example, x is a lower bound). By the previous proposition, this implies that S has a minimal element. Call this element m. Then $m>x$ as its in S, but since its the minimal integer with this property, $m-1$ must be less than x. That is $x>m-1$ so $x+1>m$. But $y-x>1$ so $y>x+1$. Thus $x<m<x+1<y$ so we have found an m between x and y as required!

Now that we know the rational numbers are dense, its straightforward to *use* that result to help us discover the irrationals are as well. A starting point to this is to prove that there is an irrational number between every pair of rationals.

> **Theorem :** For any two rational numbers p, q with $p<q$, there is an irrational number x with $p<x<q$.
>
> > **Sketch :** If p, q are rational, find an irrational between p and q by first finding an irrational between 0 and $q-p$...

> **Corollary :** The irrational numbers are dense in the real numbers.
>
> > **Sketch :** If a, b are any two real numbers, we are looking for an irrational between them. If a, b are both rational, we are done by the above argument, so we only need to worry about what happens when at least one of a, b are irrational themselves. When a is irrational, we

> > can find some N with $a + a/N$ in-between a and b, and prove that its irrational. Similarly if b's irrational theres some irrational of the form $b - b/N$ in-between a and b, so we are done.