

The Real Number System

Some time ago, we looked at algebraic systems called fields. A field is an algebraic system that satisfies the following axioms.

F1) There are elements $0 \in F$ and $1 \in F$ (and $0 \neq 1$)
(so the system has at least two elements)

F2) $\forall x \forall y \forall z (x + y) + z = x + (y + z)$ F2') $\forall x \forall y \forall z (x \cdot y) \cdot z = x \cdot (y \cdot z)$
(addition and multiplication are associative)

F3) $\forall x \forall y x + y = y + x$ F3') $\forall x \forall y x \cdot y = y \cdot x$
(addition and multiplication are commutative)

F4) $\forall x \forall y \forall z x \cdot (y + z) = x \cdot y + x \cdot z$
(the distributive law connects addition and multiplication)

F5) $\forall x x + 0 = x$ F5') $\forall x x \cdot 1 = x$
(0 and 1 are “neutral” elements for addition and multiplication. 0 is called the additive identity element and 1 is called the multiplicative identity element in F)

F6) $\forall x \exists y x + y = 0$ F6') $(\forall x)x \neq 0 \Rightarrow (\exists y) y \cdot x = 1$
(such a y is called an additive inverse of x) (such a y is called a multiplicative inverse for x)

The system of integers, \mathbb{Z} , is not a field (because axiom F6' is not true in \mathbb{Z}). We proved that the systems \mathbb{Z}_p are fields iff p is a prime.

The (informal) system of rational numbers, \mathbb{Q} , is a field, and so is the (informal) system \mathbb{R} of real numbers. As far as this set of axioms goes, there is no difference between \mathbb{Q} and \mathbb{R} : any theorem that can be proved from these axioms is true in both \mathbb{Q} and \mathbb{R} since both are fields.

In the lecture supplement about the construction of \mathbb{Q} (*not discussed in class*) it is shown how to construct the rational numbers from the integers: each rational number is an equivalence class of pairs of integers.

In a nutshell, if $a, b \in \mathbb{Z}$ and $b \neq 0$, then we can write the ordered pair (a, b) : it is in the set $\mathbb{Z} \times (\mathbb{Z} - \{0\})$. We want to think of this ordered pair as being the rational number $\frac{a}{b}$, but we realize that certain ordered pairs should represent the same rational number: for example, we want to think of $(1, 2)$ and $(2, 4)$ as representing the same rational (since $\frac{1}{2} = \frac{2}{4}$). More generally: in the informal system \mathbb{Q} we have that $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$; therefore we want to think of the pairs (a, b) and (c, d) as representing the same rational iff $ad = bc$.

So we make an equivalence relation on the set $\mathbb{Z} \times (\mathbb{Z} - \{0\})$: $(a, b) \simeq (c, d)$ iff $ad = bc$. The set of all equivalence classes for this relation is called \mathbb{Q} :

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} - \{0\}) / \simeq .$$

Each equivalence class is called a rational number: for example, the equivalence class

$$[(1, 2)] = \{ \dots, (-3, -6), \dots, (-1, -2), (1, 2), (2, 4), (*3, 6), (4, 8), \dots \}$$

is a rational number (it is the rational that, in the usual informal system we denote by $\frac{1}{2}$ (or $\frac{2}{4}$ or $\frac{-3}{-6}$ or ...)

In the supplementary notes, definitions are given for how to add and multiply these equivalence classes (rationals) and then one can prove that all the axioms F1...F6' are satisfied in this system: that we, we can prove that the formal system \mathbb{Q} constructed in this way is a field. Based on this and other theorems that we can prove in \mathbb{Q} , we convince ourselves that the formal system \mathbb{Q} "acts just like" the informal system of rationals. Therefore we are will to all accept the formal definition for \mathbb{Q} : $\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} - \{0\}) / \simeq$.

Using the formal system \mathbb{Q} , it is then possible to construct a formal definition for the real number system \mathbb{R} . We will not have time to do this: the construction is a little more complicated than the constructions for $\omega, \mathbb{Z}, \mathbb{Q}$ and it would take 2-3 lectures just to do a worthwhile introduction.

We will only say here that there are different (equivalent) ways to formally construct \mathbb{R} and, in one version, a real number turns out to be a pair (L, R) where L, R are certain special subsets of \mathbb{Q} .

However, we do want to say a few things about the real number system \mathbb{R} . These comments, necessarily, will just refer to the informal real number system, \mathbb{R} , but all of the comments could be proved if we took the time to construct the real number system formally.

Ordered Fields

An ordered field is an algebraic structure where "positive" and "negative" can be defined. This lets us introduce relations $<$ and \leq (by saying $x < y$ iff $y - x$ is "positive"). To be a little more formal:

Definition A field F is called an ordered field if there is a designated subset $P \subseteq F$ (called the "positive" elements in F) that satisfies the following axioms (*these are numbered, here, as additions to the list of field axioms F1-...-F6'*):

O7) If $x, y \in P$, then $x + y \in P$ and $xy \in P$
 ("the sum and product of two positive elements is positive")

O8) For every $x \in F$, either $x \in P$ or $-x \in P$, but not both are in P .

O9) $0 \notin P$

For example, in \mathbb{Z} we defined P to be the set containing those integers of the form $[(k, 0)]$ and, with that definition O7-O9 turned out to be true (*this comment is just to illustrate O7-O8; \mathbb{Z} is not an ordered field because it's not even a field: Axiom F6' isn't true in \mathbb{Z}*).

In the supplementary notes on constructing \mathbb{Q} , it is shown how we can define “positive” in \mathbb{Q} in such a way that O7-O9 are true. In other words, \mathbb{Q} is an ordered field.

And although we have not formally constructed \mathbb{R} , it is clear that the informal system \mathbb{R} of real numbers is an ordered field: P is just that set of real numbers that (informally) we have always called positive.

In an ordered field, we can use the axioms to prove theorems that say that all the “standard” rules for manipulating inequalities are true. As far as the ordered field axioms are concerned, there is no difference between \mathbb{Q} and \mathbb{R} : all the standard rules for the algebra involving addition, subtraction, multiplication, division and manipulating inequalities are identical in \mathbb{Q} and \mathbb{R} .

Yet (informally) we know that

- i) in \mathbb{Q} there is no x for which $x^2 = 2$
- ii) in \mathbb{R} , there are solutions for the equation $x^2 = 2$.

Since we believe (informally) in this difference between \mathbb{Q} and \mathbb{R} , it must be true that the statement

$$“ (\exists x) x^2 = 2 ”$$

is unprovable from the ordered field axioms *(otherwise it would be true in all ordered fields: $\mathbb{Q}, \mathbb{R}, \dots$)*

and also the statement

$$“ \sim (\exists x) x^2 = 2 ”$$

is unprovable from the ordered field axioms *(otherwise it would be true in all ordered fields: $\mathbb{Q}, \mathbb{R}, \dots$)*

In other words, the statement “ $(\exists x) x^2 = 2$ ” is undecidable from the ordered field axioms: neither the statement nor its negation can be proved.

If we want to understand the real number system, there must be some other special property about \mathbb{R} , one not “captured” by the ordered field axioms: this special property of \mathbb{R} is what makes it different from \mathbb{Q} .

The missing property, it turns out, is one called the Completeness Axiom. We will discuss this axiom soon. The real number system, \mathbb{R} satisfies this axiom but \mathbb{Q} , it turns out, does not – and therein lies the crucial difference between \mathbb{Q} and \mathbb{R} . \mathbb{R} is called a complete ordered field because it's an ordered field that also satisfies this additional “Completeness Axiom.”

Before we can state the Completeness Axiom, we need to define some terms and think about what they mean.

Definition Suppose X is an ordered field (for example, you can think $X = \mathbb{R}$ or $X = \mathbb{Q}$) and that $A \subseteq X$. Let $x \in X$.

i) x is called an upper bound for the set A iff

$$(\forall a \in A) a \leq x.$$

ii) x is called a least upper bound (= lub) for the set A if

a) x is an upper bound for the set A , and in addition,

b) If $y < x$, then y is not an upper bound for A

The contrapositive equivalent for condition b)

is: if y is an upper bound for the set A , then $x \leq y$.

iii) If A has an upper bound in X , we say that A is bounded above.

If A has no upper bounds, we say A is unbounded above.

Exercise: Write the negations of the definitions:

i) x is not an upper bound for the set A iff ...

ii) x is not a least upper bound for the set A iff ...

iii) A is not unbounded above iff ...

Examples In the ordered field \mathbb{R} (as we informally understand it):

i) $A = \mathbb{N}$ has no upper bound in \mathbb{R} : it is unbounded above. Since \mathbb{N} has no upper bounds, it has no least upper bound.

Note: we could also think of \mathbb{N} as a subset of \mathbb{Q} . In \mathbb{Q} it is also true that \mathbb{N} is unbounded above.

ii) If $A = \emptyset$, then every real number r is an upper bound for A .

Why? If r were not an upper bound for A , that would mean ...? (See the exercise above.)

Note: as in i), we could also think of \emptyset as a subset of \mathbb{Q} . In \mathbb{Q} it is also true that every rational number q is an upper bound for \emptyset .

Therefore $A = \emptyset$ has no least upper bound because, if r is an upper bound then (for example) $r - 1$ is also an upper bound.

iii) In \mathbb{R} : a) if $A = (0, 1)$, then r is an upper bound for A iff $r \geq 1$

b) if $B = [0, 1]$, then r is an upper bound for B iff $r \geq 1$.

Just for example, 15 is an upper bound for both A and B . So is 137. In fact, there are infinitely many other upper bounds for both sets because each number larger than an upper bound (15, say) must also be an upper bound.

Of course, A and B also have upper bounds smaller than 15. For example, $\frac{5}{2}$ and 1.00000000000001.

For both sets A and B , the least upper bound is 1 because

- i) 1 is an upper bound, and
- ii) If $s < 1$, then s is not an upper bound.

Notice from this example: a least upper bound for a set (if one exists) might or might not actually be in the set.

iv) If A has a largest member s , then s is a least upper bound for A (*carefully explain why!*).

Conversely, if s is a least upper bound for A and $s \in A$, then s must be the largest element in A (*carefully explain why!*).

v) $A = \{0.1, 0.11, 0.111, 0.1111, \dots\}$. Note that every decimal in this set A has only finitely many digits. Since $\frac{1}{9}$ is given by the infinite repeating decimal $0.1\bar{1}\dots$, it is easy to see that each number in A is $< \frac{1}{9}$ and that $\frac{1}{9}$ is a least upper bound for A .

Theorem Suppose $A \subseteq X$ where X is an ordered field. If r and s are both least upper bounds for A , then $r = s$. *In other words: a least upper bound for A , if it exists, is unique. Therefore when a least upper bound for A exists, we are justified to call it the least upper bound of A .*

Proof By definition of least upper bound, both r and s are upper bounds for A . Since r is a least upper bound, it is \leq every other upper bound – so $r \leq s$. Similarly, since s is a least upper bound, $s \leq r$. Therefore $r = s$. •

Notation In an ordered field X : if a set A has a least upper bound s , we write $s = \text{lub } A$. *Note: in many books – especially more advanced mathematics texts – the least upper bound of A is instead called the supremum of A ; these books would write $s = \text{sup } A$.*

Now we can state the Completeness Axiom. Notice that this is an axiom that not every ordered field satisfies.

For example, the Completeness Axiom is false in \mathbb{Q} , as we will indicate below. It turns out to be true in \mathbb{R} .

The Completeness Axiom Suppose $A \subseteq X$ and that $A \neq \emptyset$. If A has an upper bound in X , then A has a least upper bound in X .
 (Paraphrased: “the Completeness Axiom for X ” = “a nonempty subset of X that is bounded above has a least upper bound in X .” Why do we need the word “nonempty” in the statement?)

Example The Completeness Axiom is not true in \mathbb{Q} .

We proved long ago that $\sqrt{2}$ must be irrational – that is, there is no rational number x for which $x^2 = 2$. Let $A = \{x \in \mathbb{Q} : x^2 < 2\} \subseteq \mathbb{Q}$.

A has an upper bound in \mathbb{Q} – for example, 4 is an upper bound (if $x \in A$, then $x^2 < 2$, so certainly $x \leq 4$). We will show that if $q \in \mathbb{Q}$, then q is not a least upper bound for A – that is, A has no least upper bound in \mathbb{Q} .

Let $q \in \mathbb{Q}$. We know $q^2 = 2$ is impossible, so either $q^2 < 2$ or $q^2 > 2$.

i) Suppose $q^2 < 2$. Then $\epsilon = 2 - q^2 > 0$.

(The idea is to show that we can find a rational number y slightly larger than q for which $y^2 < 2$; this means $y \in A$ and $y > q$ so that q is not an upper bound for A .)

We can pick an $n \in \mathbb{N}$ large enough that $\frac{9}{n} < \epsilon = 2 - q^2$. (This move was motivated by some offline scratchwork.) Since $2 - q^2 > \frac{9}{n}$,

$$\begin{aligned} 2 > q^2 + \frac{9}{n} &= q^2 + \frac{1}{n}(9) \geq q^2 + \frac{1}{n}(2q + 1) \geq q^2 + \frac{1}{n}(2q + \frac{1}{n}) \\ &\quad \uparrow \text{since } q \leq 4 \\ &= q^2 + \frac{1}{n}2q + \frac{1}{n^2} = (q + \frac{1}{n})^2. \end{aligned}$$

Let $y = q + \frac{1}{n}$. Then $y^2 < 2$ so $y \in A$, and $q < y$. So q is not an upper bound for A (and therefore q certainly is not a least upper bound for A).

ii) Suppose $q^2 > 2$. Then $\epsilon = q^2 - 2 > 0$.

(The idea is to show that we can find a rational number y slightly smaller than q such that $y^2 > 2$. This means that $y \geq x$ for every x in A – making y an upper bound for A . Since $y < q$, q cannot be the least upper bound for A . The moves below were motivated by some offline scratchwork.)

Pick an $n \in \mathbb{N}$ big enough that $\frac{1}{n} < \frac{\epsilon}{2q}$. Then $\frac{1}{n}2q < \epsilon = q^2 - 2$, so, for this n ,

$$\begin{aligned} \frac{1}{n}2q &< q^2 - 2 && \Rightarrow \\ \frac{1}{n}(2q - \frac{1}{n}) &< q^2 - 2 && \Rightarrow \\ \frac{1}{n}2q - \frac{1}{n^2} &< q^2 - 2 && \Rightarrow \\ -2q\frac{1}{n} + \frac{1}{n^2} &> 2 - q^2 && \Rightarrow \\ q^2 - 2q\frac{1}{n} + \frac{1}{n^2} &> 2 && \Rightarrow \\ (q - \frac{1}{n})^2 &> 2 && \Rightarrow \end{aligned}$$

Let $y = q - \frac{1}{n}$. Then $y^2 > 2$ and $y < q$ which, as noted above, means that q is not a least upper bound for A .

Informally, imagine taking the real number line and “throwing away” all the irrational numbers (such as $\sqrt{2}$, for example). What's left sitting in a line is the set of rational numbers, \mathbb{Q} , but the line is no longer “complete”: there is a “hole” where each irrational used to sit. Of course, these are not “wide” holes because, between any two rationals, another rational still remains. The holes are like “pinpricks” of width 0.

In the preceding example, the set A consists of all rationals to the left of the “hole” where $\sqrt{2}$ ought to be. The rationals in A are all too small to be a lub for A , and the other rationals are all too large to be a lub for A . A lub for A would need to be a number that “plugs the hole.”

Informally, we can think of starting with \mathbb{Q} and somehow constructing “new numbers” (the irrationals) to plug all the “holes” in \mathbb{Q} so that the end result, the set \mathbb{R} , is “complete” in the sense that it “has no holes.” Informally, that's why \mathbb{R} satisfies the Completeness Axiom.

We did not have the time to show carefully how to start with \mathbb{Q} and formally define the system \mathbb{R} of real numbers – in the formal system, each real number turns out to be some set containing sets of rational numbers. But had we done so, we could then prove that what is described in the last few paragraphs is what actually, rigorously happens: we could prove that the Completeness Axiom is really a theorem in the formal, “official” system \mathbb{R} .

In order to illustrate some of the power of the Completeness Axiom, we will simply need here to

assume that the Completeness Axiom is true in \mathbb{R}

that is, we assume here that \mathbb{R} is a complete ordered field.

With that assumption we can prove some facts that we already believe, informally, about \mathbb{R} . Part of the point of the remaining examples and theorems is to show how some “familiar facts” about \mathbb{R} are actually consequences of the Completeness Axiom.

Theorem \mathbb{N} has no upper bound in \mathbb{R} .

Proof Suppose, to the contrary, that \mathbb{N} did have an upper bound, x , in \mathbb{R} . Since $\mathbb{N} \neq \emptyset$, the Completeness Axiom would then imply that \mathbb{N} has a least upper bound in \mathbb{R} : call it s . Since s is the least upper bound of \mathbb{N} , the number $s - 1$ is not an upper bound for \mathbb{N} . That means that $\exists k \in \mathbb{N}$ such that $k > s - 1$. Then $k + 1 \in \mathbb{N}$ and $k + 1 > s$; this is a contradiction – since s is an upper bound for \mathbb{N} . •

Corollary (the “Archimedean Property” of \mathbb{R}) Suppose $y \in \mathbb{R}$. If $x > 0$, then $\exists n \in \mathbb{N}$ for which $nx > y$.

Proof We do an argument by contradiction: suppose the corollary is false. Then $nx \leq y$ for every $n \in \mathbb{N}$, that is, $\forall n \in \mathbb{N}, n \leq \frac{y}{x}$. This means that $\frac{y}{x}$ is an upper bound for \mathbb{N} , which contradicts the theorem. •

Corollary If $x > 0$, then $\exists n \in \mathbb{N}$ for which $0 < \frac{1}{n} < x$.

Proof According to the preceding corollary (with $y = 1$), there is an $n \in \mathbb{N}$ for which $nx > 1$, that is, $0 < x < \frac{1}{n}$. •

Corollary (“Squeeze Theorem”) If $a \leq x \leq a + \frac{y}{n}$ for all $n \in \mathbb{N}$, then $x = a$.

Proof We know that $x \geq a$. If $x \neq a$, then $x > a$, so $x - a > 0$. Therefore, by the Archimedean Property, $\exists n \in \mathbb{N}$ for which $n(x - a) > y$. But that would mean $x > a + \frac{y}{n}$, contrary to the hypothesis. •

Example 2 has a square root in \mathbb{R} , that is, $\exists x \in \mathbb{R} \ x^2 = 2$

Interestingly, essentially the same algebra used in the earlier example to show that $A = \{q \in \mathbb{Q} : q < 2\}$ has no lub in \mathbb{Q} can be used here: but watch how it fits into a different logical framework.

Let $A = \{r \in \mathbb{R} : r^2 < 2\}$. A has upper bound in \mathbb{R} (for example., 4 is an upper bound). By the Completeness Axiom (**), A has a least upper bound s in \mathbb{R} , and there are only 3 possibilities about s : $s^2 < 2$, $s^2 = 2$ or $s^2 > 2$.

As before, for \mathbb{Q} : if $s^2 < 2$, then we can find an $n \in \mathbb{N}$ such that $(s + \frac{1}{n})^2 < 2$. This means that $s < s + \frac{1}{n} \in A$, and this contradicts that s is an upper bound for A .

As before, for \mathbb{Q} : if $s^2 > 2$, then we can find an n such that $(s - \frac{1}{n})^2 > 2$. If $a \in A$, then $a > s - \frac{1}{n}$ would give that $a^2 > 2$. Therefore, for every $a \in A$, $a \leq s - \frac{1}{n} < s$. This means that $s - \frac{1}{n}$ is an upper bound for A , and this contradicts that s is the least upper bound for A .

Since the alternatives $s^2 > 2$ and $s^2 < 2$, both lead to a contradictions the only remaining possibility must be true: $s^2 = 2$. So s is a square root for 2 in \mathbb{R} .

A side comment: Suppose a is a member of any ordered field ($\mathbb{Q}, \mathbb{R}, \dots$):

i) if $a < 0$, then a has no square roots: because $a = x^2 < 0$ is impossible.

ii) if $a = 0$, then a has exactly one square root: $a = 0 = x^2$ iff $x = 0$.

iii) if $a > 0$, then a has either no square roots or exactly two square roots.

a) if a has a square root $x \neq 0$, then $-x$ is also a square root because $a = x^2 = (-x)^2$

b) if x and y are both square roots of a , then $x^2 = a$ and $y^2 = a$.
Therefore $0 = x^2 - y^2 = (x - y)(x + y)$ and so $y = \pm x$.

The Completeness Axiom is used in analysis to prove the Intermediate Value Theorem which you should have seen earlier, almost certainly without proof, in Calculus I.

Intermediate Value Theorem Suppose $f : [a, b] \rightarrow \mathbb{R}$ is continuous. If $f(a)$ and $f(b)$ have opposite signs (one positive, the other negative) then there must exist a $c \in (a, b)$ for which $f(c) = 0$.

The proof depends on a careful definition of “continuous function” and on the Completeness Axiom. The idea behind the proof is that the graph of a continuous function f is “all in one piece” (so the graph can’t simply “jump” across the x -axis) and there are “no holes in \mathbb{R} ” (for the graph could “slip through” and get from the positive to the negative side of the x -axis without intersecting the x -axis).

Once the Intermediate Value Theorem is proven, it allows mathematicians to prove that square roots exist in \mathbb{R} for all positive real numbers d without going through a detailed argument such as we used when $d = 2$.

If $d > 0$, then let $f(x) = x^2 - d$. Pick any b for which $b^2 > d$. Because f is continuous on $[0, b]$, and because $f(0) = -d < 0$ and $f(b) = b^2 - d > 0$, the Intermediate Value Theorem guarantees that there is a $c \in (0, b)$, for which $f(c) = c^2 - d = 0$, that is, for which $d = c^2$. So c is a square root for d .

In fact, we can use the Intermediate Value Theorem to prove that lots of other roots exist in \mathbb{R} , too. For example, in the preceding argument, we could replace $f(x) = x^2 - d$ with, say, $f(x) = x^{28} - d$ and use the Intermediate Value Theorem in the same way to show that d must have a 28th root in \mathbb{R} .

We conclude with a few final observations about lub's in \mathbb{R} .

Suppose $\text{lub } A = s$.

i) As we observed earlier, it could happen that $s \in A$ or that $s \notin A$. For example:

a) If $A = \{1 - \frac{1}{n} : n \in \mathbb{N}\}$, then $\text{lub } A = 1$ (explain carefully why!) but $1 \notin A$.

b) If $A = \{1\} \cup \{1 - \frac{1}{n} : n \in \mathbb{N}\}$, then $\text{lub } A = 1$ and $1 \in A$.

ii) Whether or not $s \in A$, s is “just the right size” to indicate the “upper limit” of the set A :

If $s = \text{lub } A$, then no matter how tiny we choose $\epsilon > 0$:

$s + \epsilon$ is too big to be the least upper bound for A . There are many smaller upper bounds for the set A smaller than $s + \epsilon$: for example, $s + \frac{\epsilon}{2}$, or, say, $s + \frac{\epsilon}{1000}$, or s itself (*the smallest possible choice of upper bound for A*)

$s - \epsilon$ is too small to be an upper bound for A : so, for any $\epsilon > 0$ (*no matter how tiny!*) there must be an $a \in A$ for which $s - \epsilon \geq a$ is false: that is, an a for which $a > s - \epsilon$. (In part a) or b) above, there must be a number $1 - \frac{1}{n} \in A$ for which $1 - \frac{1}{n} > 1 - 10^{-100}$.