

CHAPTER 1

Number Systems and Mathematical Induction

Counting is so basic that it can't really be called mathematics. Infants playing with toys seem to have a notion of counting. The concept is much more elementary than any arithmetic operations.

If we're going to examine counting, we might as well ask where we should start. We actually could start with any whole number but experience tells us that we should start either with zero or one. In current mathematics, it doesn't much matter whether the set of whole numbers includes zero or not, but historically and philosophically, it meant a great deal.

0.1. Much ado about nothing. If you look up zero on the web, you'll find lots of information which is often contradictory. Even scientists working at the same U. S. government laboratory, don't seem to agree.

Here's my understanding of the history. The origins of zero were not as a number but rather as a placeholder in positional notation for numbers. The Babylonians did that, using a symbol, in the 3rd century or so BC. Earlier, their placeholder for zero was a blank space. The Romans didn't use it, although Greek astronomers did. To write a number like 1024, a Roman would have have used MXXII. The Mayans in Mexico and Central America were into long-term calendars, hence needed to write big numbers; they developed positional notation out of necessity.

The source of the modern use of zero seems to come from Fifth Century AD India. It spread first east then, possibly through China, to the Arabic countries. As Arabic numerals were adopted throughout the world, the use of the placeholder zero spread.

Some examples of the historic numerals is given in

<http://www.mediatinker.com/blog/archives/008821.html>

As a number, zero has a more interesting history, in

<http://www-groups.dcs.st-and.ac.uk/history/HistTopics/Zero.html>

a seventh century AD reference is given for arithmetic using zero; to wit, zero is being treated as a number. By 1200 or so, it was in common use in Arabic and other Islamic countries. However it had a harder time gaining a foothold in Europe before the late Renaissance. One reason I heard a long time ago — and whose source I don't recall — is that there was philosophical and religious resistance to the notion of zero. Zero, as a number, connotes "nothingness." In the Judeo-Christian tradition, some aspect of the deity is omnipresent, hence there is no such thing as nothingness.

1. Counting

Just to be specific, we'll start counting with the number 1. Most of what we write is equally valid if we start with zero or any positive whole number. The fundamental notion of counting is not of adding one — addition is a much more subtle algebraic notion — but rather of "the next number" or successor. So 2 is the successor of 1, 3 the successor of 2, etc. In fact, the only way we know a counting number, other than one, is to know what number it succeeds. A number $\neq 1$, is the successor to only one number and every number is succeeded by exactly one number.

We define the set of natural number as 1 and all of its successors.

This collection of properties of natural numbers was formalized, probably first by Dedekind but named after Peano, as the definition of the natural numbers. We follow the notation and basic properties in Joyce's web posting:

<http://aleph0.clarku.edu/~djoyce/numbers/peano.pdf>

The Peano Axioms

We define *the natural numbers*, as a set \mathbb{N} with a distinguished element 1 and a function

$$\begin{aligned} \sigma : \mathbb{N} &\rightarrow \mathbb{N} \\ &: n \mapsto \sigma(n) \end{aligned}$$

with the following properties:

- (1) $1 \notin \sigma(\mathbb{N})$.
- (2) σ is injective i.e. if $\sigma(n) = \sigma(m)$ then $n = m$.

- (3) If T is any subset of \mathbb{N} and $1 \in T$ and T is closed under σ , i.e. for any $n \in T$, $\sigma(n) \in T$.

Notice that the axioms don't say that such a set exists; however, preschoolers know it when they see it.

2. Mathematical Induction

The Principle of Mathematical Induction uses the third axiom to create proofs that a given set T contains all natural numbers. I like to think of it informally in two ways:

First, it is the words *et cetera* in mathematical arguments. For example, a statement is true for $n = 1$, true for $n = 2$, etc. Here the *et cetera* means that the same argument, that worked for a number n , will work for the successor of n .

Second, the successor function allows us to reach any number by using the successor function a finite number of times. So a statement that is true for $n = 1$ and is true for $\sigma(n)$, whenever it is true for n , will be true for any number k since the truth of the statement comes from applying Mathematical Induction $k - 1$ to the truth of the statement for $n = 1$.

EXAMPLE 2.1. (due to Gauss)

Supposedly, he was a noisy little lad so, to keep him busy, his schoolteacher told him to add the first 100 numbers. He thought for a moment, came up with the answer 5050 and went back to being noisy. Gauss' argument is quite elegant — even if this telling of the story is a more than a bit exaggerated. He grouped the numbers. The first and last add up to 101, the second and next-to-last also add up to 101 and keep going. He got 50 pairs of numbers, all of which add up to 101.

The previous example is true in much greater generality.

EXAMPLE 2.2.

$$(1) \quad 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Here's a proof. It is typical of proofs by induction.

PROOF. We use Mathematical Induction. Let T be the set of $n \in \mathbb{N}$ for which Equation 1 is true.

First we need show that $1 \in T$. $1 = 1 \cdot 2/2$, hence $1 \in T$.

Next, we assume $k \in T$. We must show that $k + 1 = \sigma(k) \in T$.

Since $k \in T$, we know that

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Now add k_1 to both sides of the previous equation to get

$$1 + 2 + \cdots + k + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.$$

The previous line is Equation 1 when $n = k + 1 = \sigma(k)$. So $\sigma(k)$ also lies in T and we have shown that $T = \mathbb{N}$. \square

One key feature of proofs by induction is that you have to have guess the statement that you want to prove true. That statement may come from experiments, wishful thinking, a textbook writer, or some other source of inspiration.

Here's a similar example.

EXAMPLE 2.3. What is the sum of the first n squares, i.e. $1^2 + 2^2 + \cdots + n^2$?

There's a standard formula for this, but let's try to guess it. The formula for summing first powers gave a quadratic polynomial in n . The average number was about $n/2$ and there were n numbers, which roughly gives a quadratic. Now we have n squares; the "average" one is $n^2/4$. So a first guess might be that the sum should be a cubic polynomial. Even if that guess is correct, which one should it be? We don't know *a priori* so we try to figure it out.

Let's experiment with a general cubic, $P(x) = Ax^3 + Bx^2 + Cx + D$. If this is the right polynomial, it should give us the right answer for every value of n . So $P(1) = 1 = A + B + C + D$. $P(2) = 5 = 8A + 4B + 2C + D$. Hopefully, $P(3)$ and $P(4)$ will give us enough equations to solve for the unknown coefficients A, B, C, D .

- EXERCISES 2.1.
- (1) Finish the guess and prove, using induction, that it is correct. It is Exercise 3 on p. 10 in the text.
 - (2) Try to construct an argument, using induction, to prove that all horses have the same color.
 - (3) Read the Joyce posting.

3. Arithmetic in \mathbb{N} and inductive definitions

The Peano Axioms give us a means of proving that a subset $T \subset \mathbb{N}$ is actually all of \mathbb{N} . We would like to do arithmetic in \mathbb{N} . We can use induction here again to give the definitions.

Here's the idea. Both addition and multiplication take any two natural numbers and output a third number. Alternatively, they are functions from $\mathbb{N} \times \mathbb{N}$ to \mathbb{N} with special properties. Here are the definitions.

DEFINITION 3.1. We define a function

$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} &\rightarrow \mathbb{N} \\ &: (n, m) \mapsto + (n, m) \end{aligned}$$

as follows:

- (1) $+(n, 1) = \sigma(n)$ for every n
- (2) $+(n, \sigma(m)) = \sigma(+(n, m))$ for every n and m

We write $n + m := +(n, m)$ and call it the *sum* of n and m . The function is called *addition*

Note that we can now write $\sigma(n)$ as $n + 1$.

Addition of two natural numbers satisfies

PROPOSITION 3.1. *If $k, n, m \in \mathbb{N}$ then*

- (*associative law*) $(k + n) + m = k + (n + m)$, and
- (*commutative law*) $n + m = m + n$.
- (*cancellation*) if $k + n = k + m$ then $n = m$.

Proof is homework.

We can do the same for multiplication.

DEFINITION 3.2. We define a function

$$\begin{aligned} \cdot : \mathbb{N} \times \mathbb{N} &\rightarrow \mathbb{N} \\ &: (n, m) \mapsto \cdot (n, m) \end{aligned}$$

as follows:

- (1) $\cdot(n, 1) = n$ for every n

$$(2) \cdot(n, \sigma(m)) = \cdot(n, m) + n \text{ for every } n \text{ and } m$$

We write $n \cdot m := \cdot(n, m)$ and call it the *product* of n and m . The function is called *multiplication*

The three properties of addition, as given above, have analogs for multiplication — just change $+$ to \cdot . Formulate them and prove one or two.

Another property is the distributive law:

For any $k, n, m \in \mathbb{N}, k \cdot (n + m) = kn + km$. You might want to try to prove this too.

A sequence in a set X is a special type of function.

DEFINITION 3.3. Let X be any set and let

$$\begin{aligned} () : \mathbb{N} &\rightarrow X \\ &: n \mapsto x_n; = ()(n) \end{aligned}$$

is called a *sequence* in X and is usually denoted (x_n) .

EXAMPLE 3.1. Let's define an infinite decimal. First we form a sequence of 0's and 1's. $a_1 = 1$. $a_2 = 0$. $a_3 = 1$. The next two digits are zeroes, then a one, then three zeroes, then a one, etc. Next form an infinite decimal as $.a_1a_2a_3 \dots$. This decimal is an irrational number (Why?) but is much easier to describe than most rationals.

There is also a natural ordering on \mathbb{N} .

DEFINITION 3.4. Given $n, m \in \mathbb{N}$. If there is a $k \in \mathbb{N}$ so that $n = m + k$, then we write $n > m$ or $m < n$ and use the usual terminology *bigger than* and *less than*.

Here is a list of the major properties of this ordering.

PROPOSITION 3.2. Suppose $k, n, m \in \mathbb{N}$, then

- exactly one of $n < m$, $n = m$ or $m < n$ is valid. (This is the trichotomy property of an ordering).
- if $n < m$ and $m < k$ then $n < k$. (This is the transitivity property of an ordering.)
- if $n < m$ then $n + k < m + k$.
- if $n < m$ then $kn < km$.

We can also write

$$n = m - k \quad \text{whenever } m = n + k.$$

Arithmetic in \mathbb{N} is not very powerful; we lack an additive identity, zero, and also negative numbers and fractions. Now it is time to define them.

0 is a new symbol or numeral. We define addition in the set $\mathbb{N} \cup \{0\}$, by

$$0 + n = n + 0 = n$$

for any $n \in \mathbb{N} \cup \{0\}$. Also $0 < n$ for any $n \in \mathbb{N}$.

We also define the set of *negative integers* $\mathbb{Z}^- := \{-n \mid n \in \mathbb{N}\}$. We also often use the symbol \mathbb{Z}^+ for \mathbb{N} when we think of them as the positive integers. By the way, the *set of integers* is

$$\mathbb{Z} := \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+.$$

It has the usual addition, multiplication and ordering with all the usual properties. We'll develop them in them at the end of the next section after we've shown how fractions lead naturally to rational numbers.

4. The Rational Numbers

First we start with *fractions* which are numbers of the form p/q with p and q integers and $q \neq 0$. This isn't good enough. We want to think of $1/2$ as the same number as $2/4$.

DEFINITION 4.1. Two fractions p/q and p'/q' are called *equivalent* if $p \cdot q' = p' \cdot q$. A *rational number* $r = [p/q]$ or more usually and more sloppily just p/q is the set of all fractions equivalent to p/q ; that set is called the *equivalence class* of p/q . The set of rational numbers is denoted \mathbb{Q} .

The equivalence class of p/q has a few properties that make it look like it is an equality — we've actually forced that.

PROPOSITION 4.1.

- (1) p/q is equivalent to itself.
- (2) If p/q is equivalent to r/s then r/s is equivalent to p/q .
- (3) If p/q is equivalent to r/s and r/s is equivalent to u/v then p/q is equivalent to u/v .

You can prove the Proposition directly from the definition of equivalence. We don't like to use the term equality in this kind of situation. Equality means *is the same as*. Two fractions like $2/4$ and $1/2$ are not the same as fractions but they have the same value as numbers.

The first property is called *reflexivity*, the second is called *symmetry* and the third is called *transitivity*.

I trust that everyone can do arithmetic in the rationals. \mathbb{Q} is an example of a field. We've actually one, \mathbb{Z}_2 , already.

The definition of a field, given as a set of axioms, is on Page 2 of the text.

The rationals also have an ordering, using the usual symbol $<$ and its variants. It is easy to define. Any rational r can be written with a positive denominator. So do it for p/q and r/s . Then $p/q < r/s$ if $ps < rq$. Notice that the second inequality is taken among integers; so the ordering of the rationals is derived from the ordering of the integers. It is an exercise to show that replacing a fractions by an equivalent ones doesn't change the ordering.

The positive rationals is the $\mathbb{Q}^+ := \{r = p/q \mid p, q \in \mathbb{Z}^+\}$. Notice that, when $r \in \mathbb{Q}^+$, $0 < r$. The ordering can be defined in an equivalent fashion. If $r, s \in \mathbb{Q}$, then $r < s$ if $s - r \in \mathbb{Q}^+$.

Show that the two definitions are equivalent. (Actually showing two definitions are equivalent is a theorem.)

DEFINITION 4.2. Given an ordering on some collection X of numbers and two numbers x and y , with $x < y$. We say that $z \in X$ is *between* x and y , if $x < z$ and $z < y$. The set

$$(x, y) := \{z \in X \mid z \text{ between } x \text{ and } y\}$$

is the open interval in X with endpoints x and y . The set

$$[x, y] := \{z \in X \mid z \text{ between } x \text{ and } y\} \cup \{x, y\}$$

is the closed interval in X with endpoints x and y .

PROPOSITION 4.2. *Between any two distinct rationals, there is a third one.*

PROOF. Suppose $[p/q] < [r/s]$ are rationals. Then

$$t := \frac{1}{2} \left[\frac{p}{q} + \frac{r}{s} \right] = \left[\frac{ps + qr}{2qs} \right]$$

is the average of the two rationals and $(ps + qr)s < 2s(qr)$ or, equivalently, $t < [r/s]$. The other inequality is an exercise. \square

4.1. A stage aside — Equivalence relations and orderings. We've more than touched on two fundamental mathematical concepts — equivalence and order. We might as well make them explicit.

The first one is a distillation of our concept of things being equal. In mathematics, two things are equal if there's no way that we can distinguish them — they are, in any possible sense, indistinguishable. However, we sometimes like to think of objects as being the same within the context under discussion. So fractions, in the context of rational numbers, are "the same" if they define the same rational number. Triangles are the same, in Euclidean geometry, if they are congruent. The same idea appears in physics and, indeed, in all of science. Something we observe is an essential (the technical term is *intrinsic*) property of an object if no valid experiment can result in a different interpretation or evaluation of that property.

Now we'll turn all of that prose into mathematics.

DEFINITION 4.3. Let S be any set. Two elements $x, y \in S$ are called *equivalent*, written xRy if:

- (ER-1)** xRx for any $x \in S$.
- (ER-2)** If xRy then yRx for any two $x, y \in S$.
- (ER-3)** Suppose $x, y, z \in S$ and xRy and yRz , then xRz .

The first property is *reflexivity*; the second is symmetry and the third is transitivity.

For $x \in S$, the set of $y \in S$ for which xRy is called the equivalence class of x and is (often) denoted $[x]$.

- EXAMPLE 4.1.**
- (1) equality of numbers or functions, in any sense, is an equivalence relation.
 - (2) congruence of geometric objects is an equivalence relation.
 - (3) citizenship in the same country is an equivalence relation.

If R is an equivalence relation on a set S , we can graph it.

DEFINITION 4.4. Suppose S is a set and R is an equivalence relation on S . The *graph* of R is the subset $graph(R)$ of $S \times S$ defined by $(x, y) \in graph(R)$ if and only if xRy .

An ordering is also a relation on a set. It is quite different from an equivalence relation. For example, we're very happy that $2 = 2$; we wouldn't be too happy to discover that $2 < 2$. So we don't expect that reflexivity is a property of an ordering. Symmetry would be even worse

— it would dictate that $2 < 3$ implies $3 < 2$. We really don't want symmetry as a property of an ordering. Transitivity is not so bad. We can accept that $2 < 3$ and $3 < 4$. And $2 < 4$ is pretty appealing.

There's also a contest aspect to an ordering — think of it as a pecking ordering. You go before me, I go before you or we're really the same person. There are three possibilities and no pair of them can hold simultaneously. That describes a division into three possibilities or a *trichotomy*. Now an ordering defines itself.

DEFINITION 4.5. Let S be any set. On ordering $<$ on S is a relationship between pairs of elements $x, y \in S$ so that

(O-1) For any $x, y \in S$ exactly one of $x < y$, $x = y$ or $y < x$ holds true.

(O-2) For any $x, y, z \in S$, if $x < y$ and $y < z$, then $x < z$.

The *graph* of the ordering $<$ is the subset $Graph(<)$ consisting of the points (x, y) for which $x < y$.

The ordering of the natural or rational numbers is a good example of an ordering. On the other hand, proper set containment is rarely an ordering. Why?

4.2. An approach to defining the integers. We just finished deriving the rational numbers from the integers. There is a similar method for defining the integers and their ordering and arithmetic from pairs of natural numbers. It is less intuitive than defining rationals in terms of equivalent fractions, but is still straightforward.

DEFINITION 4.6. In $\mathbb{N} \times \mathbb{N}$, define $(n, m) \sim (n', m')$ if $n + m' = n' + m$. We then say that (n, m) is equivalent to (n', m') . An *integer* k is the set $[n, m] := \{(n', m') \mid (n', m') \sim (n, m)\}$. The set of integers is denoted \mathbb{Z} .

We can think of an integer (n, m) intuitively as $n - m$ which, of course, we have not defined for all natural numbers n and m .

PROPOSITION 4.3. *If $(n, m), (p, q)$ and (r, s) lie in $\mathbb{N} \times \mathbb{N}$ and \sim is the equivalence defined above, then*

- (1) (n, m) is equivalent to itself.
- (2) If (n, m) is equivalent to (p, q) then (p, q) is equivalent to (n, m) .
- (3) If (n, m) is equivalent to (p, q) and (p, q) is equivalent to (r, s) then (n, m) is equivalent to (r, s) .

The proof is an exercise.

There is an ordering in \mathbb{Z} which is defined by $[n, m] < [p, q]$ if $n + q < p + m$. As defined here, we don't know that the property of being "less than" is characteristic of the integer $[n, m]$, i.e. we need to show that, whenever $(n', m') \sim (n, m)$ then $[n', m']$ remains "less than" $[p, q]$. Here's the computation.

We first write $(n, m) < (p, q)$ if $n + q < p + m$. We need to show that when we replace the pairs by equivalent ones, the ordering remains valid.

PROPOSITION 4.4. *Assume $(n, m) \sim (n', m')$ and $(p, q) \sim (p', q')$. If $(n, m) < (p, q)$ then $(n', m') < (p', q')$.*

PROOF. Since $(n, m) < (p, q)$, we have $n + q < p + m$. Add $q' + m'$ to both sides of the inequality and replace $m' + n$ by $m + n'$ and, similarly, replace $p + q'$ by $p' + q$. Cancel the common summand $m + q$ from both sides to get $n' + q' < p' + m'$ which is equivalent to $(n', m') < (p', q')$. \square

We can now define an ordering in \mathbb{Z} by $[n, m] < [p, q]$ if $n + q < p + m$. The Proposition tells us that it does not depend on the choice of elements of the sets $[n, m]$ and $[p, q]$.

DEFINITION 4.7. Suppose P is a statement about one or more collections or sets of objects given in terms of a choice of element of the collections or sets. P is called *well-defined* if its truth (or falsehood) does not depend on which choice of elements we have made.

We have already proved

THEOREM 4.1. *$<$ is an ordering of the integers \mathbb{Z} .*

We've been using the arithmetic of integers since we were puppies but, in this context, we need a definition. It is based on the simple formulas for $(m - n)$ plus or times $(p - q)$.

DEFINITION 4.8. Suppose $[n, m], [p, q] \in \mathbb{Z}$.

We define *integer sum* to be the map

$$\begin{aligned} + : \quad \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} \\ &: ([n, m], [p, q]) \mapsto [n, m] + [p, q] := +([n, m], [p, q]) \end{aligned}$$

by

$$[n, m] + [p, q] := [n + p, m + q].$$

Similarly, we define the *integer product* to be the map

$$\begin{aligned} \cdot : \quad \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} \\ :([n, m], [p, q]) &\mapsto [n, m] \cdot [p, q] := \cdot([n, m], [p, q]) \end{aligned}$$

by

$$[n, m] \cdot [p, q] := [np + mq, mp + qn].$$

EXERCISES 4.1. Show that addition and multiplication of integers are well-defined and commutative operations.

There are two special integers.

$$0 := [(1, 1)]$$

and

$$1 := [(2, 1)].$$

It is an exercise to show that, if n is any integer, $n + 0 = n$, $n \cdot 0 = 0$ and $n \cdot 1 = n$.

DEFINITION 4.9. An integer $n = [n + 1, 1]$ is called *positive*.

An integer $-n := [1, n + 1]$ is called *negative*.

THEOREM 4.2. An integer $[n, m]$ is positive if and only if $0 < n + (-m)$.

5. The Real Numbers

This whole section needs a lot of illustrations using rational rays — much like the ones that students liked in class.

The real numbers were originally conceived to make limits exist; so far as I know there was no formal theory even though limits were assumed to exist. There are several ways to define the real numbers, we will follow Dedekind. His approach has the same kind of naturality that our descriptions of other number systems have had.

$\sqrt{2}$ shows us the problem — \mathbb{Q} has a hole at $\sqrt{2}$. There are rationals bigger than and less than $\sqrt{2}$ and we can get arbitrarily close to $\sqrt{2}$ using rationals. That suffices to tell us what

we mean by a hole. We do have to be careful to make sure that the "non-holes" at the rationals are filled but by the correct rational.

DEFINITION 5.1. Let $L \subset \mathbb{Q}$ have the following properties:

- (1) $\exists r \in L$.
- (2) $\exists r' \notin L$.
- (3) If $s \in L$ and $r < s$ then $r \in L$
- (4) If $s \in L$, $\exists r \in L$ with $r > s$. L is called a *real number* or *Dedekind cut*. The set of real numbers is denoted \mathbb{R} .

The hole at the point L is defined by all rational numbers less than L . Think of the number L as the infinite open interval of rationals lying to the left of L . You could also think of L as an open ray pointing left with two properties: it only contains rational points and the real number it defines is the initial point. L also defines, and is defined by, all the rationals bigger than the hole. Those bigger rationals, we'll soon give it the name R , will be a necessary part of our further discussion.

It seems to be useful to introduce the following notation. If L is a real number or Dedekind cut, we can write x for the number and L_x for the interval. In fact, they are exactly the same. By using different symbols in different contexts, we seem to be able to make the presentation clearer.

EXAMPLE 5.1. The rationals live in \mathbb{R} . Take any $r \in \mathbb{Q}$ and let

$$\bar{r} := \{p/q \in \mathbb{Q} \mid p/q < r\}.$$

It has all the desired properties, so it *is* a real number. We will identify \bar{r} with r . The identification is an injection or embedding

$$i : \mathbb{Q} \hookrightarrow \mathbb{R}.$$

A real number which is not rational is called *irrational*.

The ordering on \mathbb{R} is particularly easy to define.

DEFINITION 5.2. If $x, y \in \mathbb{R}$, then $x < y$ if $x \subset y$ but $x \neq y$. Equivalently, x is a *proper subset* of y written $x \subsetneq y$.

THEOREM 5.1. $<$ is an order relation on \mathbb{R} .

PROOF. We first show transitivity. So, assume $x < y$ and $y < z$. In terms of sets, our assumption is $L_x \subset L_y$ and $L_y \subset L_z$. It is a basic property of sets that $L_x \subset L_z$ or, equivalently, $x < z$. So $<$ is transitive.

Next assume x and y are real numbers. If $x = y$, then we are done. If not, then $L_x \neq L_y$ and one of these sets, say L_y contains a rational $r = p/q$ which does not lie in L_x . By definition of L_y , every rational s, r must also lie in L_y . Then L_y contains every rational in L_x hence $x < y$. It is an exercise to show that $x < y$ and $y < x$ cannot occur simultaneously. \square

We also get a notion of positivity.

DEFINITION 5.3. A real number x is *positive* if $0 < x$. x is *negative* if $x < 0$.

One easy way to check the ordering is to note that a real number x is less than a rational real number \bar{q} if $q \notin x$. From now on, we wont generally distinguish between q and \bar{q} .

THEOREM 5.2. *Between any two real numbers, there is an rational number.*

PROOF. Let $x < y$ be any two real numbers. Then there is a rational $r \in y \setminus x$. \bar{r} then lies between x and y . \square

DEFINITION 5.4. Suppose X is an ordered set of numbers with ordering $<$ and $A \subset X$. An element $b \in X$ is called an *upper* (respectively, *lower*) *bound* for A if, $\forall x \in A, x \leq b$ (respectively, $b \leq x$). A number $l \in X$ is called a *least upper bound* or *supremum* of A if $l \leq b$ for every upper bound b of A . A similar definition holds for *greatest lower bound* or *infimum*. These are denoted \sup and \inf respectively.

The most important single property of the real numbers is the following theorem. It shows that we have gotten rid of holes and taking limits is a meaningful operation.

THEOREM 5.3 (The Completeness of \mathbb{R}). *Suppose $A \subset \mathbb{R}$ is non-empty and has an upper bound. Then it has a least upper bound given by*

$$\sup(A) = \cup\{x \mid x \in A\}.$$

PROOF. Assume, for the moment that $s = \cup\{x \mid x \in A\}$. s is a union of subsets of \mathbb{Q} , hence $s \subset \mathbb{Q}$. Since A has some upper bound $b \in \mathbb{R}$, there is an element $b' \in \mathbb{Q}$ which does not lie in b . Thus $b' \notin x$ for any $x \in a$ and $b' \notin s$ by definition of s . Since $A \neq \emptyset$, there is some $x \in A$ which contains a rational r ; r also lies in s . If $r \in s$, then r is a rational in some $x \in A$. It follows from the definition of the real number x , that every rational $r' < r$ also lies in x hence $r' \in s$. Similarly, given any $r \in s, r \in x$ for some $x \in A$. From the definition, there is some $r' \in x$ with $r < r'$. It follows that $r' \in s$. We have shown that $s \in \mathbb{R}$.

s is an upper bound for A since $s \supset x$ for all $x \in A$. . If b is any other upper bound for A , then $x \leq b$ for any $x \in A$. From the definition, it follows that $x \subset b$ for all $x \in A$. Thus

$s = \cup\{x \mid x \in A\} \leq b$. It follows that $s \leq b$ for any which is precisely the condition that $s = \sup(A)$. \square

5.1. The arithmetic of real numbers. Real numbers are sets. Therefore if we want to define addition and multiplication, we need to define sets of rationals with specific properties. Since we now have an ordering, we can define any real number x as $\{r \in \mathbb{Q} \mid r < x\}$.

DEFINITION 5.5. Given two real numbers x and y , The *sum* of x and y is the set

$$x + y := \{r + s \mid r \in x, s \in y\}.$$

The product is not so easy to define precisely because the product of two large negative rational is a large positive number.

It is convenient to define the negative of a number first. Suppose $x \in \mathbb{R}$. Then x is a set of rationals, which it is convenient to denote $L_x := \{r \in \mathbb{Q} \mid r < x\}$. We can also define $R_x := \{\{r \in \mathbb{Q} \mid r < x\}\}$. These are rational rays emanating from x . Each determines the other. When we take the negative of rational numbers, we know that we interchange the class of right and left rays. So we have

DEFINITION 5.6. We use the above notation. If $x \in \mathbb{R}$, then the *negative* of x is the number

$$-x := \{-r \mid r \in R_x\}.$$

For $A \subset \mathbb{R}$, define $-A := \{-x \mid x \in A\}$.

The *difference* of two real numbers x and y is

$$x - y := x + (-y).$$

EXERCISES 5.1.

- (1) Show $-x = -R_x$.
- (2) Show that $-(-x) = x$.
- (3) show that $x + (-x) = 0$.
- (4) Show that $x + y = 0$ implies that $y = -x$.
- (5) Show that $x < y$ implies $-y < -x$.
- (6) Show that a finite set X subset \mathbb{R} has both an infimum and a supremum and both $\inf(X)$ and $\sup(X)$ are elements of X .
- (7) Prove the following Corollary to the Completeness Theorem.

COROLLARY 5.1. *If A is a set of real numbers having a lower bound, then $\inf(A)$ exists.*

(Hint: Think of the set $-A$.)

DEFINITION 5.7. Suppose $X \subset \mathbb{R}$. If $\sup(X) \in X$ (respective, $\inf(X) \in X$), then $\sup(X)$ is called the *maximum* of X (respectively, $\inf(X)$ is called the *minimum* of X).

To define multiplication, notice that multiplication by -1 should send s to $-x$. So we have to expect that R_{-x} will play a role in defining multiplication.

DEFINITION 5.8. Given two sets $A, B \subset \mathbb{Q}$, define

$$AB := \{a \cdot b \mid a \in A, b \in B\}.$$

Suppose $x, y \in \mathbb{R}$. Then the product of x and y , denoted $x \cdot y$ or, simply xy is defined as follows:

- (1) if $x = y = 0$, then $x \cdot y = L_0 R_0 (= (-R_0)R_0 = \{p/q \in \mathbb{Q} \mid P/Q < 0\})$.
- (2) if $x > 0$ and $y > 0$, $R_{x \cdot y} = R_x R_y$.
- (3) if $x > 0$ and $y < 0$, $R_{x \cdot y} = -R_x R_{-y}$.
- (4) if $x < 0$ and $y > 0$, $R_{x \cdot y} = -R_{-x} R_y$.
- (5) if $x < 0$ and $y < 0$, $R_{x \cdot y} = R_{-x} R_{-y}$.

One must show that these definitions make sense. The first thing we must do is show that $x + y$ and xy are real numbers. Next we must show that these arithmetic notions, when applied to rationals, give the same results as rational arithmetic. We would like \mathbb{R} to be a field and we still don't have the multiplicative inverses x^{-1} for all $x \neq 0$.

Again, we can get the idea for taking the inverse of a real number from inequalities. L_x is the set of all rational $p/q < x$. At least for real, positive x and positive p/q , taking inverses reverses the sense of inequalities, i.e. $x^{-1} < q/p$. But those rationals are precisely the ones we need in $R_{x^{-1}}$. It is the key to giving us the definition for $x > 0$.

DEFINITION 5.9. For $x \in \mathbb{R}^+$, the *inverse* of x , written x^{-1} is the set for which

$$R_{x^{-1}} = \left\{ \frac{q}{p} \mid \frac{p}{q} \in L_x \cap \mathbb{Q}^+ \right\}.$$

For $x \in \mathbb{R}^-$, $-x > 0$, and we define $x^{-1} = -(-x)^{-1}$.

You now have the option to show that the real numbers, with the above operations, form a field or just accept it.

EXERCISES 5.2.

- (1) Show that the sum or product of a rational and an irrational must be irrational.

- (2) Show that between any two distinct real numbers, there are two rationals.
- (3) Use the previous results to show that there is an irrational between any two distinct real numbers.
- (4) Show that addition and multiplication of real numbers, which are rationals, agrees with addition and multiplication as defined for rationals.
- (5) Using any reference you'd like, compare this construction of the real numbers to one based on infinite decimals. (I'd like you to hand this in next week and think of it as half a project.)

The Archimedean Property of Real Numbers

The idea of the Archimedean Property is that there are no infinitesimal real numbers. More formally, it is the statement that, given any real number $x > 0$, there is a natural number $n \in \mathbb{N}$, so that $1/n < x$.

THEOREM 5.4 (The Archimedean Property of the Real Numbers). *Suppose $x \in \mathbb{R}$ is positive. Then there exists $n \in \mathbb{N}$ so that*

$$\frac{1}{n} < x.$$

PROOF. Let $y = 1/x$. Since taking multiplicative inverses of positive reals reverses the sense of inequalities, it suffices to find some natural number $n > y$. Since $y \in \mathbb{R}$, the definition of a real number tells us that there is a rational p/q so that $y < p/q$ and we can assume that both p and q are positive. If $q = 1$, then p/q is a natural number bigger than y . Otherwise, $p/q < p$ and $y < p/q < p$ and we're done. \square

In the process of proving the Theorem, we have shown

COROLLARY 5.2. *For any $x \in \mathbb{R}^+$, there is a positive integer n so that $x < n$.*

THEOREM 5.5. *For any $x \in \mathbb{R}$, there exists exactly one integer n so that $n \in [x, x + 1)$.*

PROOF. First we show that there is at most one $n \in \mathbb{Z}$ so that $n \in [x, x + 1)$. Suppose that there are two such integers n and m with $n < m$. Then

$$x \leq n < m < x + 1.$$

We can subtract n from each term and get

$$x \leq 0 < m - n < x + 1 - n < 1$$

which contradicts the ordering of the integers.

Next assume that there is no integer in $[x, x + 1)$. By induction, it follows that there is no integer in $[x + k, x + k + 1)$ for all $k \in \mathbb{N}$. So there is no integer in R_x . If $x > 0$, this contradicts the Archimedean Property of the real numbers. If $x = 0$, then $0 \in [0, 1)$. If $x < 0$ then $R_x \supset \mathbb{Q}^+ \supset \mathbb{N}$ and again we get a contradiction. \square

THEOREM 5.6. *Given any pair of real numbers, there is an irrational between them.*

PROOF. Choose any two real numbers $a < b$. We have already seen, in theorem ?????, that there is a rational r so that $r \in (a, b)$. The interval (r, b) must also contain a rational, call it s . Then the interval $(r, s) \subset (a, b)$.

We next show that there is an irrational in the open interval $(0, 2)$. A good example is $\sqrt{2}$.

Since a rational multiple of an irrational is irrational,

$$\frac{1}{2(s-r)}\sqrt{2} \in (0, s-r).$$

So we have found an irrational x in the interval $(0, s-r)$. Since the sum of a rational and an irrational is irrational, $x+r$ is both an irrational and an element of (r, s) hence an element of (a, b) . \square

DEFINITION 5.10. A set $X \subset \mathbb{R}$ is called *dense in \mathbb{R}* if, given any two distinct reals $a < b$, there is some $x \in X$ so that $x \in (a, b)$.

THEOREM 5.7. *Both \mathbb{Q} and $\mathbb{R} \setminus \mathbb{Q}$ are dense in \mathbb{R} .*

PROOF. Let a and b be any real numbers with $a < b$. We have already shown that there is both a rational and an irrational in the interval (a, b) . That's exactly what the definition of density requires. \square