The Theory of Single-Variable Calculus

Math 421, Section 001, Spring 2021

May 5, 2021

Abstract

These are collaboratively TeXed notes for our section of Math 421 at UW-Madison this semester. Each student will volunteer to be the official notetaker for one week. When it's your turn, please feel free to consult with each-other and with Alex if you need help getting started with LaTeX.

Contents

1 Introduction to sets, logic, and proofs

1.1 Introduction to set theory (Jan 26)

A **set** is simply a collection of **elements**.

Example 1.1.1. Consider the set

$$S = \{0, 1, \pi, \text{tomato}\}.$$

We write

$$1 \in S$$

to say that the element "1" *belongs to* S. On the other hand, we write

$$\text{carrot} \notin S$$

to say that the element "carrot" does *not* belong to S.

We say that two sets are **equal** if they contain the same elements. The order in which elements are listed, and any repetitions, do not matter. For instance, the set

$$S = \{1, 1, 0, \pi, \text{tomato}, \pi\}$$

is equal to the set of Example 1.1.1 above.

Example 1.1.2. Consider the two sets

$$A = \{\text{Utah, Arizona, Colorado, New Mexico}\}$$

and

$$B = \{\text{states in the U.S.A. that share a corner with three other states}\}.$$

By consulting a map, one can observe that every element of the set A shares a corner with three other states (indeed, with the other three elements of A). Hence, every element of A belongs to B. By studying the rest of the map exhaustively, one checks that none of the remaining 46 states has a 4-way corner. Therefore $A = B$.

But what is a state? And, more importantly, what is a tomato? (Vegetable? Fruit? Berry?) These questions are outside the purview of this class.

In mathematics, we generally restrict ourselves to a very limited "universe" of sets. In fact, we will start with only the following two sets: the **natural numbers**

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$$

and the **integers**

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Everything else we need (rational numbers, real numbers, limits, derivatives), we will construct from these raw ingredients.[1]

Let's continue discussing basic set terminology.

Definition 1.1.3. Let S and T be sets. We say that S is a **subset** of T if every element of S also belongs to T. In this case, we write

$$S \subset T.$$

For example, we have

$$\{0, 2, 4\} \subset \{0, 1, 2, 3, 4, 5\}.$$

Also, notice that the natural numbers form a subset of the integers:

$$\mathbb{N} \subset \mathbb{Z}.$$

In fact, the former is precisely the set of "positive integers." We can thus specify the subset of natural numbers using the following notation:

$$\mathbb{N} = \{n \in \mathbb{Z} \mid n > 0\}.$$

[1] In fact, I encourage you not even to take the familiar properties of the natural numbers ($a + b = b + a$, $a(b + c) = ab + ac$, *etc*) for granted. These are consequences of *Peano's axioms* — see Wikipedia.

Example 1.1.4. Consider the subset of $\mathbb{Z}$ defined by

$$E = \{n \in \mathbb{Z} \mid n = 2m \text{ for some } m \in \mathbb{Z}\}.$$

In English, this reads:

"E is the set of all integers, n, such that $n = 2m$ for some natural number, m."

In fact, this is just the set of *even integers*:

$$E = \{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}.$$

For instance, why is $0 \in E$? Because there does exist an integer (namely, $m = 0$) such that $2 \cdot m = 0$.

Example 1.1.5. The set of *odd integers* is given by

$$E' = \{n \in \mathbb{Z} \mid n = 2m + 1 \text{ for some } m \in \mathbb{Z}\}.$$

Definition 1.1.6. We say that an integer p **divides** an integer n if and only if there exists an integer m such that

$$n = p \cdot m.$$

For instance, given an integer $n \in \mathbb{Z}$, we have $n \in E$ if and only if 2 divides n. (In this case, $m = n/2$ is an integer).

Example 1.1.7. Consider the subset of $\mathbb{N}$ defined by

$$Q = \{n \in \mathbb{N} \mid m \text{ divides } n \Rightarrow m = 1 \text{ or } m = n\}.$$

The symbol $\Rightarrow$ means "implies;" in other words, the set Q is defined to be "the set of all positive integers such that if m divides n, then $m = 1$ or $m = n$." (See Section 1.2.2 below for more on implications.)

What precisely is the set Q? Let's translate the definition into more familiar terms. An integer that divides n is also called a "factor." So the statement is that "if" m is a factor of n, then m must equal either 1 or n itself. In other words:

"the only factors of n are 1 and n itself."

Hence

$$Q = \{1, 2, 3, 5, 7, 11, 13, 17, 19, \dots\}$$

is just the set of all prime numbers (including 1).

Next week, we will continue discussing "set operations," *i.e.*, things one can do with sets (or collections of sets) to obtain new sets. But first, we need to discuss logical statements and implications, and go over what it means to *prove* a statement mathematically.

1.2 Logical statements, implications, and quantifiers (Jan 28)

References for this section and the next are Hutchings's notes and Chapter 3 of "Transition to higher math," both available on Canvas.

1.2.1 Statements

A **statement** is a sentence that is either true or false, but not both.

Examples 1.2.1.

1. P = "6 is an even integer". True.
2. Q = "3 is an even integer". False.
3. "The time has come." (The time for what, exactly?) Not a statement, at least as far as math is concerned.

Given one or more statements, there are several standard logical "operations" that we can perform on them. These are:

Negation: $\neg P$ = "6 is *not* an even integer" (False.)

The negation of a statement is true if and only if its negation is false. A double negation gives us back the original statement:

$$\neg(\neg P) = \text{"6 is not not an even integer "} = P \quad (\underline{\text{true}}).$$

Conjunction: $P \wedge Q$ = "6 is an even integer *and* 3 is an even integer" (false).

Disjunction: $P \vee Q$ = "6 is an even integer *or* 3 is an even integer" (true).

Here is a "truth table" summarizing the above:

P	Q	$\neg P$	$P \vee Q$	$P \wedge Q$
T	T	F	T	T
F	T	T	T	F
T	F	F	T	F
F	F	T	F	F

It's also important to know how to negate statements involving and/or.

Example 1.2.2. Consider the two statements:

$$P = \text{"Liz is taking math"}$$

$$Q = \text{"Liz is taking organic chemistry."}$$

The conjunction of these would be:

$$P \wedge Q = \text{"Liz is taking math and o. chem"}$$

whereas the disjunction would be:

$$P \vee Q = \text{"Liz is taking either math or o. chem."}$$

Then the statement

$$\neg(P \wedge Q) = \text{"Liz is } \textit{not} \text{ taking math and o. chem"}$$

is logically equivalent to:

$$\text{"Liz is not taking math } \textit{or} \text{ not taking o. chem"} = (\neg P) \vee (\neg Q).$$

On the other hand, the statement

$$\neg(P \vee Q) = \text{"Liz is } \textit{not} \text{ taking either math or o. chem"}$$

would be phrased in better English as:

$$\text{"Liz is taking } \textit{neither} \text{ math nor o. chem"}$$

which is just the same as saying:

$$\text{"Liz is not taking math } \textit{and} \text{ not taking o. chem"} = (\neg P) \wedge (\neg Q).$$

We have just demonstrated what are know as "DeMorgan's Laws:"

$$\neg(P \wedge Q) = (\neg P) \vee (\neg Q)$$

$$\neg(P \vee Q) = (\neg P) \wedge (\neg Q).$$

Note: Although it's good to write them down once for clarity, it's not at all necessary to memorize these kinds of formal logical rules; you will become very familiar with them just by doing your homework over the next few weeks.

1.2.2 Implications

Suppose that P and Q are two separate statements (as above). We say P **implies** Q, and write

$$P \Rightarrow Q$$

to mean

"if P, then Q"

or, in other words,

"P is true only if Q is true."

Example 1.2.3. Let

$$P = \text{“Harry is a Packers fan”}$$

$$Q = \text{“Harry is a human being.”}$$

Does P imply Q? Certainly....if Harry is a Packers fan, then he must be a human being. If Harry is a household cat, he might potentially be a mascot, but calling him a "fan" would be difficult to justify. In other words, Harry can be a Packers fan *only if* he is also a human being.

On the other hand, does Q imply P? In other words, if Harry is a human being, does it follow that he is a Packers fan? Blasphemous as it may sound, there do exist human beings that do *not* actively root for the Packers. So for all we know, Harry may think and breathe, but not be a Packers fan. Therefore Q does *not* imply P, in which case we write

$$Q \not\Rightarrow P.$$

So here, $P \Rightarrow Q$ is an example of a true implication whose **converse** implication, $Q \Rightarrow P$, is false.

Lastly, let's suppose that Harry is *not* a Packers fan, and is also *not* a human being (for instance, Harry is a cat). Does the implication $P \Rightarrow Q$ hold true in this case? Well, it certainly isn't false: since Harry is not a Packers fan, the fact that he is a cat is completely irrelevant. Therefore $P \Rightarrow Q$ is *vacuously true* in this case. Here's another example:

Example 1.2.4. "If you're the king of France, then I'll be a monkey's uncle."

Notice that both claims—that you're the king of France, and that I could ever have a niece or nephew not belonging to *homo sapiens*—are patently false. (The last king of France met his end in 1793, so we needn't check the identity of the "you" in the statement.) But is the whole sentence, *i.e.* the "if, then" implication, a true statement? Yes....in fact, it is *vacuously* true, since the "P" statement can never be true.

Now, back to Harry of Example 1.2.3 for a minute. Let's consider the implication

$$\neg Q \Rightarrow \neg P = \text{“If Harry is not a human being, then Harry is not a Packers fan.”}$$

This is known as the **contrapositive** of the implication $P \Rightarrow Q$.

Is the statement true? Quite certainly...in fact, we already used it above to justify $P \Rightarrow Q$. A funny (and convenient) fact about implications is that **an implication and its contrapositive are always logically equivalent.**[2] In other words, the statement "if Harry is a Packers fan, then Harry is a human being" is completely equivalent to the statement "if Harry is not a human being, then Harry can hardly be a Packers fan." (Both implications happen to be true, in this case.)

[2] *i.e.*, they are either both true or both false.

Example 1.2.5. Let S and T be sets. The statement:

$$\text{"If } x \in S \text{, then } x \in T\text{"}$$

is logically equivalent to the statement:

$$\text{"If } x \notin T \text{, then } x \notin S\text{".}$$

Why? Because if the first one is true, then the second one is definitely true. On the other hand, if the first one is false (*i.e.* there does exist an $x \in S$ such that $x \notin T$), then the second one is also obviously false. Indeed, both implications are equivalent to the statement that S is a *subset* of T (*i.e.* $S \subset T$)—see Definition 1.1.3 above.

It takes some getting-used-to; but once we've been doing proofs for a little while, the freedom to change between an implication ($P \Rightarrow Q$) and its contrapositive ($\neg Q \Rightarrow \neg P$) will become second nature.

This discussion can be summarized in the following truth table:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(\neg Q) \Rightarrow (\neg P)$
T	T	T	T	T
F	T	T	F	T
T	F	F	T	F
F	F	T	T	T

1.2.3 Quantifiers

Things get more interesting when we combine logic with set theory (as we have already begun to do in Example 1.2.5 above).

Let S be a set (for instance, $S = \mathbb{Z}$ is the set of integers), and suppose that $P(x)$ is a sentence about some element $x \in S$. For example, we might take the sentence

$$R(x) = \text{"}x > 0 \Rightarrow x^2 + 1 > 0.\text{"}$$

This isn't quite a statement (yet), because we don't know which x we're talking about. But there are two common ways to make it into a statement:

$$\forall x \in S, R(x) = \text{"For all } x \in S\text{, if } x > 0 \text{ then } x^2 + 1 > 0\text{"}$$

and

$$\exists x \in S, R(x) = \text{"There exists an } x \in S\text{, (such that) if } x > 0 \text{ then } x^2 + 1 > 0.\text{"}$$

The two symbols $\forall$ ("for all") and $\exists$ ("for some," or, "there exists") are known as **quantifiers**. They determine the range of x's that a statement needs to be true for: either for all of them, or just for one.

The two statements above are both true for $S = \mathbb{Z}$ (in fact, the first one implies the second one). But here is another example:

Example 1.2.6. Consider the statement

$$P = \text{“}\forall x \in \mathbb{Z},\ x^2 + 2x + 1 > 0.\text{”}$$

Is this statement true or false? It's a bit more difficult to tell...because of the "$\forall$" symbol, we are somehow asked to check all possible integers x. But in fact the statement is *false*, because for $x = -1$, we have

$$(-1)^2 + 2(-1) + 1 = 0 \not> 0.$$

Since P is false, we have established that the negation $\neg P$ is true.

Notice that to establish $\neg P$, for a statement involving "$\forall$," we had to show that there "$\exists$" an x for which it fails. (Such an x is sometimes called a **counterexample.**)

Example 1.2.7. Consider the statement

$$\exists x \in \mathbb{Z}, x^2 + 2x + 1 > 0.$$

This statement is clearly true: for instance, we can just take $x = 1$, and note that $1^2 + 2 + 1 = 4 > 0$.

Example 1.2.8. Consider the statement:

$$\exists x \in \mathbb{Z},\ x^2 = 2.$$

This statement asserts that there exists an integer whose square is 2; but of course, this is false, since $\sqrt{2}$ is not an integer (indeed, not even a rational number....to be proved later). To show this, we can check that the set

$$\{y \in \mathbb{Z} \mid y = x^2 \text{ for some } x \in \mathbb{Z}\} = \{0, 1, 4, 9, 16, 25, \ldots\}$$

does not contain 2, or in other words, that

$$\forall x \in \mathbb{Z}, x^2 \neq 2.$$

In other words, the negation of a "$\exists$" statement is a "$\forall$" statement.

The moral of the story is that negation changes "$\forall$" to "$\exists$," and vice-versa (much as in DeMorgan's laws, where negation changes $\wedge$ to $\vee$). In short:

$$\neg\left(\forall x, P(x)\right) = \exists x, \neg P(x)$$

$$\neg\left(\exists x, P(x)\right) = \forall x, \neg P(x).$$

Again, it's not wise to try and memorize these rules; we're planning to "learn by doing." Which raises the question: what do we plan on doing for the rest of the class?

1.3 Proofs (Feb 2)

A **proof** is a translation of statements that we know (or assume) to be true into a new true statement, using the rules of logic discussed above. As our first example, we read a dramatic dialogue from Hutchings's notes, in which the following proposition[3] and its proof were "discovered."

Proposition 1.3.1. *If $x \in \mathbb{Z}$ is an even number, then x^2 is also even.*

Proof. If x is even, then we know by definition that

$$x = 2y$$

for some integer y. Squaring both sides, we obtain

$$x^2 = (2y)^2 = 4y^2.$$

Now, let $z = 2y^2$, which is again an integer. By the last equation, we have

$$x^2 = 4y^2 = 2(2y^2) = 2z.$$

Therefore $x^2 = 2z$, so x^2 is even. □

In this section, we'll discuss several different proof "techniques."

1.3.1 Direct proof

A direct proof is usually carried out by starting from a true statement, P, and establishing a chain of implications

$$P \Rightarrow P_1 \Rightarrow P_2 \Rightarrow P_2 \Rightarrow \cdots \Rightarrow Q,$$

from which we conclude that Q is also true.

The above proposition was our first example of a direct proof. Here is another one:

Proposition 1.3.2. *For every $x \in \mathbb{Z}$, if x is odd then $x+1$ is even.*

Proof. Let $x \in \mathbb{Z}$.[4] If x is odd, then by definition,

$$x = 2y + 1$$

for some integer $y \in \mathbb{Z}$. Adding 1 to both sides, we obtain:

$$\begin{aligned} x + 1 &= (2y+1) + 1 \\ &= 2y + 2 \qquad (1.1) \\ &= 2(y+1). \end{aligned}$$

Therefore $x + 1$ is also even. □

[3] A *proposition* is a true statement that, while not completely obvious, is not quite as deep or universal as a theorem.

[4] This is how to begin the proof of a "for all" or "for every" statement.

Here is another example, this time involving set theory instead of arithmetic.

Proposition 1.3.3. *Let A, B, and C be sets. If $A \subset B$ and $B \subset C$, then $A \subset C$.*

Proof. We need to show that if $x \in A$, then $x \in C$; *i.e.*, for all $x \in A$, $x \in C$.

Let $x \in A$. Since $A \subset B, x \in A \Rightarrow x \in B$. So $x \in B$.

Since $B \subset C, x \in B \Rightarrow x \in C$. So $x \in C$.

Since $x \in A$ was arbitrary, we're done. □

1.3.2 Proof by cases

Proof by "cases" is a technique that one does very often in combination with the other proof techniques.

Proposition 1.3.4. *For any integer x, $x(x+1)$ is even.*

Proof. Let x be an integer. Then x is either even or odd.

Case 1. If x is even, then $x = 2y$ for some $y \in \mathbb{Z}$. So

$$\begin{aligned} x(x+1) &= 2y(2y+1) \\ &= 2\left(y(2y+1)\right). \end{aligned} \tag{1.2}$$

Therefore $x(x+1)$ is even.

Case 2. If x is odd, then by Proposition 1.3.4, $x+1$ is even. So

$$x + 1 = 2z$$

for some $z \in \mathbb{Z}$. Multiplying both sides by x, we obtain

$$x(x+1) = x(2z) = 2(xz).$$

So $x(x+1)$ is even.

Since we've covered both cases, we're done.[5] □

1.3.3 Proof by contrapositive

This is where instead of proving an implication $P \Rightarrow Q$ directly, we instead prove its contrapositive $\neg Q \Rightarrow \neg P$. As discussed above, we are free to do this, since the contrapositive of any statement is always logically equivalent to it (*i.e.* if one is true then the other is true, and vice-versa).

Proposition 1.3.5. *For all integers $a, b \in \mathbb{Z}$, if $ab \neq 0$, then both $a \neq 0$ and $b \neq 0$.*

[5] Technically, we did not show that every integer is either even or odd. This can be proved by induction—see Example 2.3.2 below.

Proof. We prove the contrapositive of the statement, namely:

"If $a = 0$ or $b = 0$, then $ab = 0$".

This also breaks up into cases:

Case 1. If $a = 0$, then $ab = 0 \cdot b = 0$ and we're done.

Case 2. If $b = 0$, then $ab = a \cdot 0 = 0$ and we're also done. $\square$

Here is a more interesting example.

Proposition 1.3.6. *If the average of four distinct integers is* 10, *then at least one of them is greater than* 11.

Proof. We show the contrapositive. Note that the negation of the statement "$x > 11$" is "$x \leq 11$." So the contrapositive, as a whole, is:

$$\text{For distinct integers } a, b, c, d, \text{ if } a, b, c, d \leq 11 \text{ then } \operatorname{Avg}(a, b, c, d) \neq 10.$$

Now, since a, b, c, and d are distinct, we may assume without loss of generality[6] that

$$a < b < c < d.$$

Otherwise, we could relabel the four integers so that they are ordered in this way, without changing their average.

Then, since $d \leq 11$ and $c < d$, we have

$$c \leq d - 1 \leq 10$$

so $c \leq 10$. But then

$$b \leq c - 1 \leq 9$$

and

$$a \leq b - 1 \leq 8.$$

So we have shown that in fact

$$a \leq 8, \quad b \leq 9, \quad c \leq 10, \quad \text{and} \quad d \leq 11.$$

Adding together these four inequalities, we obtain

$$a + b + c + d \leq 8 + 9 + 10 + 11 = 38.$$

Dividing by 4, we get

$$\frac{a + b + c + d}{4} \leq \frac{38}{4} < \frac{40}{4} = 10.$$

In particular, we have

$$\operatorname{Avg}(a, b, c, d) < 10.$$

But this is precisely the desired statement. $\square$

[6] This phrase means that we will prove a special case that actually covers the general case of the statement, with a little more thought.

1.3.4 Proof by induction

Suppose that $P(n)$ is a statement that involves a natural number $n \in \mathbb{N}$. The **Principle of Mathematical Induction** (PMI) states that:

<u>if</u>

1. $P(1)$ is true ("*base case*"), and
2. For all $n \in \mathbb{N}$, the implication $P(n) \Rightarrow P(n+1)$ is true ("*inductive step*")

<u>then</u>

$$P(n) \text{ is true for all } n \in \mathbb{N}.$$

The logic behind the principle is as follows. Suppose that the above two assumptions are true; we claim that $P(n)$ must be true for all $n \in \mathbb{N}$.

Let $n \in \mathbb{N}$. First, we know that $P(1)$ is true, by (1). Then, by (2), we know that if $P(1)$ is true then $P(2)$ is also true. But if $P(2)$ is true, then by (2), $P(3)$ is also true. Continuing in the same fashion, we obtain a chain of implications:

$$P(1) \Rightarrow P(2) \Rightarrow \cdots \Rightarrow P(n-1) \Rightarrow P(n)$$

that eventually gets us all the way up to $P(n)$; so $P(n)$ is true.

But since $n \in \mathbb{N}$ was arbitrary, we get to conclude that $P(n)$ is actually true *for all* $n \in \mathbb{N}$.

The wonderful thing about induction is that you avoid having to check the statement $P(n)$ separately for $n = 1, 2, 3, 4, \ldots$; instead, you just have to establish (1) and (2) above, and you're done.

Proposition 1.3.7. *If $a_1, \ldots, a_n \in \mathbb{Z}$ are such that the product $a_1 \cdots a_n = 0$, then $a_i = 0$ for some i with $1 \leq i \leq n$.*

Proof. We use induction on n.

For the base case ($n = 1$), we have only one number, so the assumption is that $a_1 = 0$. Then the conclusion is a tautology.

For the inductive step, assume that the claim is true for n (this is known as the *inductive hypothesis*). To prove it for $n+1$, let $a_1, \ldots, a_{n+1}$ be integers such that

$$a_1 \cdots a_{n+1} = 0.$$

We may rewrite this as

$$(a_1 \cdots a_n) \cdot a_{n+1} = 0.$$

By Proposition 1.3.5, we know that either $a_1 \cdots a_n = 0$ or $a_{n+1} = 0$.

Case 1. If $a_1 \cdots a_n = 0$, then by the inductive hypothesis, we know that $a_i = 0$ for some $1 \le i \le n$, so we're done.

Case 2. If $a_{n+1} = 0$, then we're also done.

In either case, we have established the claim for $n+1$, completing the inductive step. By the PMI, it follows that the proposition is true for all $n \in \mathbb{N}$, as desired. □

Here's another example:

Proposition 1.3.8. *The formula*

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

holds for all $n \in \mathbb{N}$.

Proof. For the base case, we have

$$1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

so the formula is true.

For the inductive step, suppose that the formula is true for n. We need to show that the left-hand side (LHS) of the formula with $n+1$ equals the right-hand side (RHS). The LHS is:

$$1 + 2 + \cdots + n + (n+1).$$

By the induction hypothesis, we have:

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + n + 1 \\ &= (n+1)\left(\frac{n}{2} + 1\right) \\ &= (n+1)\left(\frac{n+2}{2}\right) \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned} \tag{1.3}$$

But this is precisely the RHS of the formula for $n+1$, completing the inductive step. By the PMI, the formula holds for all $n \in \mathbb{N}$, as desired. □

1.3.5 Proof by contradiction

Proof by contradiction is similar to proof by contrapositive, but the hypothesis "P" can be any true statement. What you do is assume $\neg Q$, *i.e.*, that your desired conclusion fails, and use this to show $\neg P$. But if P is *a priori* a true statement, then $\neg P$ is a "contradiction," and you get to conclude that $\neg Q$ must be false, *i.e.*, Q is true.

Contradiction arguments should only be used as a "method of last resort," when a direct proof or proof by contrapositive is infeasible. When you do get to do one, though, it can be quite fun.

Below, we will use a contradiction argument to prove a *very* famous theorem. First we need the following lemma.[7]

Lemma 1.3.9. *Let $p \in \mathbb{N}$ be a natural number, and $n \in \mathbb{Z}$ be an integer. If $p > 1$, then p does not divide both n and $n+1$.*

Proof. We will prove the contrapositive statement: supposing that $p \in \mathbb{N}$ divides both n and $n+1$, then $p = 1$.

If p divides both n and $n+1$, then there exist integers $m, m' \in \mathbb{Z}$ such that

$$n = p \cdot m \quad \text{and} \quad n + 1 = p \cdot m'.$$

Subtracting these two equations, we obtain

$$\begin{aligned} 1 = (n+1) - n &= pm' - pm \\ &= p(m' - m). \end{aligned} \tag{1.4}$$

But then p divides 1, which implies that $p = 1$. □

Theorem 1.3.10 (Euclid, *ca.* 300BC)**.** *There exist infinitely many prime numbers.*

Proof. Suppose the contrary. Then there exist only finitely many prime numbers, which we label as

$$p_1, p_2, \ldots, p_m$$

for some $m \in \mathbb{N}$. Here, we assume that $p_i \geq 2$ by definition.

Consider the number

$$n = p_1 p_2 \cdots p_m.$$

By construction, n is divisible by *every* prime number p_i. By Lemma 1.3.9, it follows that $n+1$ is not divisible by *any* prime numbers. But since $n+1 > 1$, it must have at least one prime factor. This is a contradiction.

It follows that our assumption must have been false, *i.e.*, infinitely many prime numbers exist. □

Note: Later on, we will discuss what it means for a set to be "finite" or "infinite" in much greater detail.

[7] A *lemma* is a "simple" proposition that will be used afterwards to prove a theorem.

2 Set operations and functions

2.1 Intersection and union (Feb 4)

Definition 2.1.1. Let A and B be sets.

- The **union** $A \cup B$ is the set of all elements belonging either to A or to B (or both).
- The **intersection** $A \cap B$ is the set of all elements belonging to both A and B.

Example 2.1.2.

- $\{1, 2\} \cup \{2, 3, 4\} = \{1, 2, 3, 4\}$
- $\{1, 2\} \cap \{2, 3, 4\} = \{2\}$
- $\{0, 2, 4\} \cap \{1, 3\} = \{\} = \varnothing$. This set, which has no elements at all, is known as the **empty set.**
- $\{n \in \mathbb{Z} \mid n \text{ is divisible by } 2\} \cap \{n \in \mathbb{Z} \mid n \text{ is divisible by } 5\} = \{n \in \mathbb{Z} \mid n \text{ is divisible by } 10\}$. This follows by considering the last digit in the decimal expansion of n.

Proposition 2.1.3. *Here are several basic properties of intersection and union.*

1. $A \cup \varnothing = A$
2. $A \cap \varnothing = \varnothing$
3. $A \cap B \subset A \subset A \cup B$
4. $A \cup B = B \cup A, \ A \cap B = B \cap A$ (commutativity)
5. $A \cup (B \cup C) = (A \cup B) \cup C, \ A \cap (B \cap C) = (A \cap B) \cap C$ (associativity)
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributivity)
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof. We will prove #6.

Recall that two sets are equal if every element of one is also an element of the other, and vice-versa. Equivalently, we will show that

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$$

and

$$A \cap (B \cup C) \supset (A \cap B) \cup (A \cap C).$$

($\subset$) Let $x \in A \cap (B \cup C)$. Then x is in A, and x is either in B or in C. If $x \in B$, then $x \in A \cap B$, so $x \in (A \cap B) \cup (A \cap C)$. If $x \in C$, then $x \in C \cap A = A \cap C$, so $x \in (A \cap B) \cup (A \cap C)$. This shows that $x \in (A \cap B) \cup (A \cap C)$, as desired.

($\supset$) Let $x \in (A \cap B) \cup (A \cap C)$. Then either $x \in A \cap B$ or $x \in A \cap C$. In the first case, we have $x \in A$ and $x \in B$, so $x \in B \cup C$. So $x \in A \cap (B \cup C)$. In the second case, we have $x \in A$ and $x \in C$, so $x \in C \cup B = B \cup C$. This shows that $x \in A \cap (B \cup C)$, as desired.

Since each set is a subset of the other, they are equal. □

It is actually easy to picture the above result using Venn Diagrams; still, at the end of the day, one has to write out the proof formally.

2.2 Collections of sets (Feb 4)

This seems like a good time to discuss the following point about sets and set theory. Sometimes, the elements of a set are themselves sets, as in the following example:

Example 2.2.1. Let $S = \{\{1,2\},\{3,4\}\}$. This set has two elements, $\{1,2\}$ and $\{3,4\}$.

A set whose elements are also sets is sometimes called a **collection of sets**, although not always.

Question. Is 1 an element of S?

Answer. No. S has only the two elements listed above. □

Question. Is $\{1,2\}$ a subset of S?

Answer. No; it is an element. □

Question. Is $\{\{1,2\}\}$ a subset of S?

Answer. Yes. This is a set with the single element $\{1,2\}$, which is also an element of S. Therefore, every element of $\{\{1,2\}\}$ is also an element of S. □

Question. Is $\varnothing$ a subset of S?

Answer. Yes; in fact the empty set is a subset of any set. (Why?) □

Example 2.2.2. Let S be as above and consider $T = \{\{1,2\},3\}$. We have:

- $S \cup T = \{\{1,2\},\{3,4\},3\}$.
- $S \cap T = \{\{1,2\}\}$.
- $S \cup \{S\} = \{\{1,2\},\{3,4\},\{\{1,2,\},\{3,4\}\}\}$.

Question. Is 2 an element of $S \cup T$?

Answer. No; but 3 is. $\square$

Question. Is $\{1,2\}$ a subset of $S \cap T$?

Answer. No; but it is an element of it. $\square$

Question. Is S a subset of $S \cup \{S\}$?

Answer. Yes; by construction, $S \cup \{S\}$ contains every element of S. $\square$

2.2.1 A word of caution

Now that we have started making collections of sets, it is tempting to become a bit too grandiose, as follows.

Example 2.2.3 (Russell's Paradox)**.** Let U be the set of all sets. Define the subset

$$R = \{S \in U \mid S \notin S\}.$$

Question. Is R an element of R?

Answer? Suppose that $R \in R$. Then by the definition of R, $R \notin R$, which is a contradiction.

But if $R \notin R$, then R is not an element of itself. By the definition of R, we have $R \in R$, which is again a contradiction.

Therefore, both the statement $R \in R$ and its negation $R \notin R$ are false, *i.e.*, $R \in R$ is both true and false. $\square$

It is possible to avoid these kinds of problems by being more strict about what kinds of sets one allows in one's theory: this is called *axiomatic set theory* (as opposed to *naive set theory*, which we have been practicing). But for everyday use, naive set theory is almost always good enough.

2.3 More on set operations (Feb 9)

Definition 2.3.1. Suppose A is a subset of a larger "universal" set U. Then

$$A^{\mathsf{C}} = \{x \in U \mid x \notin A\}$$

is called the **complement** of A.

Example 2.3.2. Let $A = \{\text{even integers}\}$, $U = \mathbb{Z}$. Then $A^{\mathsf{C}} = \{\text{odd integers}\}$.

Proof. We need to show that each $x \in \mathbb{Z}$ is either even or odd. We assume without loss of generality that $x \geq 0$ and use induction.
Base Case: $x = 0$ is even since $0 = 2 \cdot 0$.
Inductive Step: assume that all integers up to $n = k$ are either even or odd. We want to show that $n = k + 1$ is either even or odd.

Case 1: $k = 2m, m \in \mathbb{Z}$ is even. Then $k + 1 = 2m + 1$ is odd.

Case 2: $k = 2m + 1, m \in \mathbb{Z}$ is odd. Then $k + 1 = 2m + 1 + 1 = 2m + 2 = 2(m + 1)$ is even. This completes the inductive step, and the proof. □

Theorem 2.3.3. *Suppose A and B are subsets of U. Then* $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$

Proof. ($\subset$) Let $x \in (A \cup B)^{\complement}$. Then $x \notin A$ and $x \notin B$ (otherwise $x \in A$ or $x \in B$, hence $x \in A \cup B$). But this just means $x \in A^{\complement} \cap B^{\complement}$.

($\supset$) Let $x \in A^{\complement} \cap B^{\complement}$. Then $x \notin A$ and $x \notin B \implies x \notin A \cup B$ (otherwise, $x \in A$ or $x \in B$). □

Note: This is "the same" as De Morgan's Law!

Now, what about $A \cap B \cap C$? We have:

$$A \cap B \cap C = \{x \mid x \in A \text{ and } B \text{ and } C\}.$$

Similarly,

$$A \cup B \cup C = \{x \mid x \in A \text{ or } B \text{ or } C\}.$$

Suppose we have a collection of sets $\{A_1, A_2, A_3, \cdots\}$. We normally don't use $\{\}$ and simply write

$$A_1, A_2, A_3, \cdots$$

We say that this collection is "indexed" by the natural numbers $\mathbb{N}$. Their intersection is

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap A_3 \cap \cdots = \{x \mid x \in A_n \forall n\}.$$

Their union is

$$\bigcup_{n=1}^{\infty} A_n = A_1 \cup A_2 \cup A_3 \cup \cdots = \{x \mid x \in A_n \text{ for some } n\}.$$

Example 2.3.4. For each $n \in \mathbb{N}$, let

$$A_n = \{1, 2, 3, \ldots, n\} = \{x \in \mathbb{N} \mid x \leq n\}$$

Question. What is $\bigcup_{n=1}^{\infty} A_n$?

Answer. $\bigcup_{n=1}^{\infty} A_n = \mathbb{N}$. Why? Because given $m \in \mathbb{N}$, $m \in A_n$ for any $n \geq m$. So $m \in \bigcup_{n=1}^{\infty} A_n$. Since $m \in \mathbb{N}$ was arbitrary,

$$\bigcup_{n=1}^{\infty} A_n \subset \mathbb{N}, \quad \bigcup_{n=1}^{\infty} A_n \supset \mathbb{N}.$$

Therefore, $\bigcup_{n=1}^{\infty} A_n = \mathbb{N}$. □

Question. What is $\bigcap_{n=1}^{\infty} A_n$?

Answer. $\bigcap_{n=1}^{\infty} A_n = \{1\}$. □

2.4 Functions (Feb 11)

Consider two sets A (the domain) and B (the codomain). A *function* (written $f : A \to B$) is an assignment of a value $f(x) \in B$ for each element $x \in A$. A "function" can also be called a "map". The set of all outputs

$$f(A) = \{y \in B \mid y = f(x) \text{ for some } x \in A\}$$

is called the **image** of f (*Note*: the image of f is a subset of B, i.e. $f(A) \subset B$).

Given a subset $Y \subset B$, the **pre-image** (or inverse image) is the set of all points that map to Y. I.e.

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}.$$

Note that the image of a subset of A is a subset of B, and the pre-image of a subset of B is a subset of A.

Example 2.4.1. Let $A = \{1, 2, 3\}$, $B = \{0, 2, 4, 6, 8\}$. Let

$$\begin{aligned} f : A &\to B \\ x &\longmapsto 2x. \end{aligned}$$

Question. What is $f(A)$?

Answer: $f(A) = f(\{1, 2, 3\}) = \{2, 4, 6\}$ □

Question. What is $f(\{1, 3\})$?

Answer: $\{2, 6\}$ □

Question. What is $f^{-1}(\{4, 6\})$?

Answer: $\{2, 3\}$ □

Question. What is $f^{-1}(\{8\})$?

Answer: $\varnothing$, because $4 \notin A$. □

Example 2.4.2. Let

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ x &\longmapsto x^2 \end{aligned}$$

Using the same sets A and B as above,

$$f(\{1, 2, 3\}) = \{f(1), f(2), f(3)\} = \{1, 4, 9\}$$

$$f(\{-2, -1, 0, 1, 2\}) = \{0, 1, 4\}$$

Question. What is $f^{-1}(\{1\})$? What about $f^{-1}(\{-1\})$? $f^{-1}(\{2,3,5\})$?

Answer: $f^{-1}(\{1\}) = \{x \in \mathbb{Z} \mid x^2 = 1\} = \{-1, 1\}$
$f^{-1}(\{-1\}) = \varnothing$,
$f^{-1}(\{2,3,5\}) = \varnothing$ $\square$

Question. What is $f^{-1}(\{\mathbb{N}\})$?

Answer: The pre-image of $\mathbb{N}$ is the set of all numbers $x \in \mathbb{Z}$ such that $x^2 \in \mathbb{N}$. This is every integer except 0. So $f^{-1}(\{\mathbb{N}\}) = \mathbb{Z} \setminus \{0\}$. $\square$

Note: We will sometimes use the **set difference** between two sets:

$$A \setminus B = \{x \in A \mid x \notin B\} = A \cap B^{\complement}.$$

Definition 2.4.3. A function f is **injective** (one to one) if f maps distinct elements of the domain to distinct elements of the codomain. *I.e.* for each $y \in B$, there is <u>at most</u> one $x \in A$ such that $f(x) = y$.

If a function f is injective, we can say that if $x_1, x_2 \in A$ and that $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$. Example 2.4.1 is injective but Example 2.4.2 is <u>NOT</u> injective (because $f(n) = f(-n)$ for all $n \neq 0$).

Definition 2.4.4. A function is **surjective** (onto) if $f(A) = B$ (the image of the domain equals the codomain). I.e. for <u>every</u> $y \in B$, there exists at least one $x \in A$ such that $f(x) = y$.

$$f(A) = B \iff f^{-1}(y) \neq \varnothing$$

for all $y \in B$. Neither Example 2.4.1 nor Example 2.4.2 is surjective.

Example 2.4.5. $f : \mathbb{Z} \longrightarrow \mathbb{N} \cup \{0\}$, $x \mapsto |x+2|$. Is this surjective? Yes!

Proof. Given $y \in \mathbb{N} \cup \{0\}$, we let $x = y - 2$. Clearly $x \in \mathbb{Z}$.
Furthermore,

$$f(x) = f(y-2) = |y - 2 + 2| = |y| = y.$$

Since $y \in \mathbb{N} \cup \{0\}$ was arbitrary, f is surjective. $\square$

While f is surjective, it is not injective. Why?

Proof. Consider $y = 1$. Clearly, $y \in \mathbb{N} \cup \{0\}$. $f(-3) = 1$, and $f(-1) = 1$. But $-3 \neq -1$. So f is not injective. $\square$

Definition 2.4.6. A function f is **bijective** if it is <u>both</u> injective and surjective.

Example 2.4.7. Construct a bijection $f : \mathbb{Z} \longrightarrow \mathbb{N}$. Is this possible?

Yes!

$$f(x) = \begin{cases} 0 & x = 0 \\ 2x+1 & x > 0 \\ 2|x| & x < 0 \end{cases}$$

Although $\mathbb{Z}$ seems to have more elements than $\mathbb{N}$, we can map every element in $\mathbb{Z}$ to every element of $\mathbb{N}$. Interesting... $\square$

If a function f is bijective, there exists a unique **inverse map** f^{-1} such that

$$f^{-1}(y) = x \iff f(x) = y.$$

Since f is surjective, for any y, there exists an x such that $f(x) = y$. Since f is injective, that x is unique. Consequently, $(f \circ f^{-1})(x) = x$, and $(f^{-1} \circ f)(x) = x$.

Note: The notation "f^{-1}" has two different meanings! It is both used to denote the "inverse image" of a set, and to denote the "inverse function" of a bijective function. It should always be clear from the context which one we mean.

2.5 Cartesian product and graphs of functions (Feb 16)

Definition 2.5.1. Given two sets, S and T, the **Cartesian Product** is

$$S \times T = \{(x,y) \mid x \in S \text{ and } y \in T\}$$

Example 2.5.2.

$$S = \{0,1,2\}$$
$$T = \{3,4\}$$

$$S \times T = \{(0,3),(0,4),(1,3),(1,4),(2,3),(2,4)\}$$

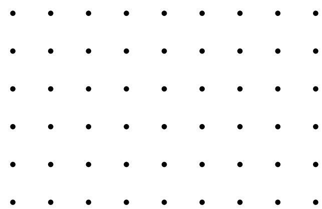
$$S \times T \neq T \times S$$

Example 2.5.3. $\mathbb{N} \times \mathbb{N} =$

$$\{(x,y) \mid x \in \mathbb{N}, y \in \mathbb{N}\}$$

$$\left\{\begin{matrix} (1,1) & (1,2) & (1,3) & (1,4) & ... \\ (2,1) & (2,2) & (2,3) & (2,4) & ... \\ & \vdots & & & \\ & \vdots & & & \end{matrix}\right\}$$

$\mathbb{N} \times \mathbb{N} =$



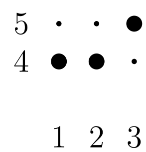
Definition 2.5.4. Given a function $f : S \mapsto T$, the graph of f is the subset of $S \times T$ given by $\{(x, y) \in S \times T \mid y = f(x) \text{ for some } x\}$.

Example 2.5.5. Graph of $\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{N} \\ x &\longmapsto x^2 \end{aligned}$

$$\{(1,2), (2,4), (3,9), (4,16), \cdots\}$$

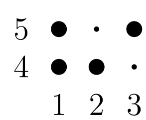
Question. Let $S = \{1,2,3\}$ and $T = \{4,5\}$. Which of the following subsets of $S \times T$ are equal to the graph of some function $f : S \longrightarrow T$?

Example 2.5.6. $\{(1,4), (2,4), (3,5)\}$



Answer: Yes... b/c every $x \in S$ is mapped to exactly one value $y \in T$.
$f(1) = 4$
$f(2) = 4$
$f(3) = 5$

Example 2.5.7. $\{(1,4), (1,5), (2,4), (3,5)\}$
Answer:

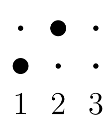


No! $f(1) = 4$, $f(1) = 5$???

$$\Rightarrow f \text{ is not a function!}$$

FAILS THE VERTICAL LINE TEST!

Example 2.5.8. $\{(1,4), (2,5)\}$



$f(3) = ???$
Answer: Not a function, since $f(3) =$ "undefined."

3 Infinity

3.1 Finite and infinite sets (Feb 16)

Let
$$\mathcal{P}_n = \{1, 2, 3, \ldots, n\} \subset \mathbb{N}$$
be the set of all integers from 1 to n.

Definition 3.1.1. We say that a set is **finite** if there exits a bijection from $\mathcal{P}_n$ to S, for some $n \in \mathbb{N}$. In this case, we write
$$|S| = n,$$
and say "the *order* of S is n."

Otherwise, we say that S is infinite.

Example 3.1.2. Consider the set
$$S = \{*, \dagger, @, x, \text{Ivanka Trump}, \text{potato}\}$$
Is S finite? Let's define a map as follows:
$$\begin{aligned} 1 &\longmapsto * \\ 2 &\longmapsto @ \\ 3 &\longmapsto \dagger \\ 4 &\longmapsto \text{Ivanka} \\ 5 &\longmapsto x \\ 6 &\longmapsto \text{potato.} \end{aligned} \tag{3.1}$$
This gives us a bijection
$$\mathcal{P}_6 \xrightarrow{\sim} S.$$
We conclude that S is a finite set of order 6 (*i.e.* $|S| = 6$).

Note: We will sometimes use the following notation for maps:
$\hookrightarrow$ = injection
$\twoheadrightarrow$ = surjection
$\xrightarrow{\sim}$ = bijection

Example 3.1.3. The sets
$$\mathbb{N}, \ \mathbb{N} \times \mathbb{N}, \ \mathbb{N} \times \mathbb{Z}, \ \mathbb{Z} \times \mathbb{N}, \ \text{and } \mathbb{Z} \times \mathbb{Z}$$
are all infinite.

Example 3.1.4. If A and B are finite, and

$$|A| = n = |B|,$$

then there exists bijections

$$\mathcal{P}_n \xrightarrow{\sim} A$$

$$\mathcal{P}_n \xrightarrow{\sim} B.$$

But any bijection is <u>invertible</u>. So we also have $A \xrightarrow{\sim} \mathcal{P}_n$, and the composition

$$A \xrightarrow{\sim} \mathcal{P}_n \xrightarrow{\sim} B$$

is a bijection.

Informal definition. Two sets S and T have "*the same size*" if there exists a bijection (*i.e.* a 1-1 correspondence) between them.

Example 3.1.5. $\mathbb{Z}$ $\mathbb{N}$
Do these have the same size?

$$\{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$$

$$\{1, 2, 3, 4, ...\}$$

We saw last time that there <u>does</u> exist a bijection:

$$\mathbb{Z} \xrightarrow{\sim} \mathbb{N}$$

$$\text{and } \mathbb{Z} \xleftarrow{\sim} \mathbb{N}$$

<u>So they have the same size</u>!

Question. Do all the sets of Example 3.1.3 have the "same size?" I.e., is it possible to construct bijections between them?

More generally, are all infinite sets the "<u>same size</u>?"

3.2 Countable sets (Feb 18)

Definition 3.2.1. Suppose that S is an infinite set. We say that S is **countably infinite** if there exists a bijection $\mathbb{N} \xrightarrow{\sim} \mathbb{S}$ (or $S \xrightarrow{\sim} \mathbb{N}$).

The reason for this definition is as follows. If we are given a bijection $f : \mathbb{N} \to S$, this gives us the ability to label each element of S as

$$s_n = f(n).$$

Then we can list all the elements of S as:

$$S = \{s_1, s_2, s_3, s_4, ...\}.$$

So, a countably infinite set is precisely one whose elements can be "counted" (*i.e.*, indexed) using the natural numbers.

Definition 3.2.2. We say that a set S is **countable** if it is either finite or countably infinite.

Example 3.2.3. We saw last time that there is a bijection $g : \mathbb{N} \xrightarrow{\sim} \mathbb{Z}$ (specifically, the inverse of the bijection $\mathbb{Z} \xrightarrow{\sim} \mathbb{N}$ of Example 2.4.7). Therefore $\mathbb{Z}$ is countably infinite.

Example 3.2.4. Let

$$E = \{x \in \mathbb{Z} \mid x = 2n \text{ for some } n \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

be the set of even integers. To show that E is countable, we just need to construct a bijection

$$\mathbb{N} \xrightarrow{\sim} E.$$

To do this, we first write down a bijection:

$$\begin{aligned} f : \mathbb{Z} &\to E \\ n &\mapsto 2n. \end{aligned} \tag{3.2}$$

To obtain a bijection $\mathbb{N} \to E$, we just take the composition with the map g of the previous example:

$$\mathbb{N} \xrightarrow{g} \mathbb{Z} \xrightarrow{f} E.$$

Since the composition of two bijections is a bijection, $f \circ g : \mathbb{N} \to E$ is the required bijection.

We will now prove a few lemmas that will save us from having to construct bijections explicitly every time we want to show that a set is countable.

Lemma 3.2.5. *Any subset $A \subset \mathbb{N}$ is countable.*

Proof. Let's order the elements of A :

$$a_1 < a_2 < a_3 < \ldots$$

Either A contains a largest element, or not.

Case 1. A contains a largest element. Then the list above

$$a_1 < a_2 < a_3 < \ldots < a_k$$

ends at the k'th element, a_k. The map

$$\mathcal{P}_k \to A$$

$$n \longmapsto a_n$$

is a bijection, so A is finite ($\Rightarrow$ *countable*).

Case 2. A does not contain a largest element (i.e $\forall a \in A, \exists\, a' \in A$ $s.t$ $a' > a$). Then the above list

$$a_1 < a_2 < a_3 < \ldots$$

goes on forever. So the map

$$\begin{aligned} \mathbb{N} &\longrightarrow A \\ n &\longmapsto a_n \end{aligned}$$

is a bijection. $\Rightarrow A$ is countably infinite ($\Rightarrow$ *countable*). $\square$

Example 3.2.6. Let

$$\begin{aligned} Q &= \{m \in \mathbb{N} \mid m \in \mathbb{N} \text{ divides } n \Rightarrow m = 1 \textit{ or } m = n\} \\ &= \{1, 2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots\}. \end{aligned}$$

This is the set of all prime numbers (including 1). We proved in Theorem 1.3.10 above that this set is infinite! By the previous Lemma, Q is in fact countably infinite.

Lemma 3.2.7. *Suppose there exists an injective map $f : S \hookrightarrow \mathbb{N}$. Then S is countable.*

Proof. Define the subset $A = f(S) \subset \mathbb{N}$. By the previous Lemma, A is countable. But we can define a map

$$\begin{aligned} g : S &\longrightarrow A \\ x &\longmapsto f(x). \end{aligned}$$

Since f is injective, g is also injective. Since $A = f(S)$, g is also surjective. Therefore g is a bijection. Since A is countable, S is also countable. $\square$

Lemma 3.2.8. *Let $A \subset S$ be a subset of a countable set S. Then A is countable.*

Proof. Since S is countable, there exists an injection $f : S \hookrightarrow \mathbb{N}$. (If S is finite, we have $S \xrightarrow{\sim} \mathcal{P}_n \subset \mathbb{N}$, which is an injection; if S is countably infinite, we have a bijection $S \xrightarrow{\sim} \mathbb{N}$.) But then the "restriction"

$$\begin{aligned} f|_A : A &\to \mathbb{N} \\ x &\mapsto f(x) \end{aligned}$$

is also an injection. So, by the previous lemma, A is countable. $\square$

Lemma 3.2.9. *Suppose that there exists a surjective map $\mathbb{N} \twoheadrightarrow A$. Then A is countable.*

Proof. Given $f : \mathbb{N} \twoheadrightarrow S$, we can choose a subset $M \subset \mathbb{N}$ such that the restriction

$$\begin{aligned} f|_M : M &\to A \\ x &\mapsto f(x) \end{aligned} \tag{3.3}$$

is bijective. (For each $y \in S$, choose exactly one $x \in f^{-1}(\{y\})$, and let $x \in M$.)

Case 1. M is finite. $\mathcal{P}_n \xrightarrow{\sim} M \xrightarrow{\sim} S$ is bijective $\Rightarrow S$ is finite.

Case 2. M is infinite. $\mathbb{N} \xrightarrow{\sim} M \xrightarrow{\sim} S$ is a bijection. $\Rightarrow S$ is countably infinite. $\square$

Theorem 3.2.10. *Let A and B be countable sets. Then $A \cup B$ is countable.*

Proof. We may assume without loss of generality that $A \cap B = \varnothing$. (If not, replace B by $B \setminus A$, which is countable by Lemma 3.2.8.)

Since A and B are countable, there exist injective maps

$$f : A \hookrightarrow \mathbb{N}$$

$$g : B \hookrightarrow \mathbb{N}.$$

Consider the map

$$h : A \cup B \longrightarrow \mathbb{Z}$$

$$h(x) = \begin{cases} f(x) & x \in A \\ -g(x) & x \in B. \end{cases}$$

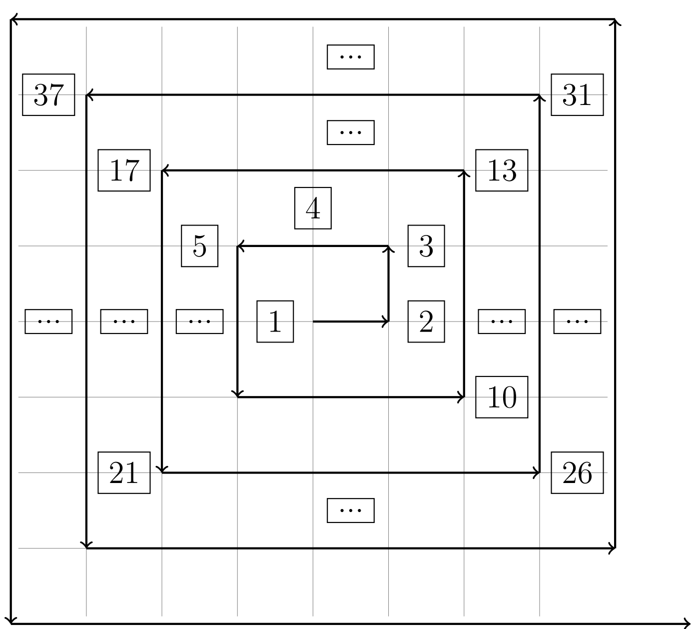
Then h is injective. So the composition $A \cup B \hookrightarrow \mathbb{Z} \xrightarrow{\sim} \mathbb{N}$ is a composition of injective maps, so is injective.

Therefore, by the lemma above, $A \cup B$ is countable. $\square$

Question. Is $\mathbb{N} \times \mathbb{N}$ countable?

Answer: Yes. We showed two ways to "count" the points...either by using "boxes," or by using "diagonals."

We also showed how to count $\mathbb{Z} \times \mathbb{Z}$. In the picture below, we label the 1st, 2nd, 3rd, ..., 37th dot, etc.



More generally, we have the following result.

Theorem 3.2.11. *Let A and B be countable sets. Then the Cartesian product $A \times B$ is* *countable.*

Proof of Theorem 3.2.11. Since A and B are countable, there exist surjective maps

$$f : \mathbb{N} \twoheadrightarrow A$$

$$g : \mathbb{N} \twoheadrightarrow B.$$

(Why?) Consider the "product map"

$$f \times g : \mathbb{N} \times \mathbb{N} \longrightarrow A \times B$$

$$(x, y) \mapsto (f(x), g(y)).$$

We claim that this is surjective. Given $(z, w) \in A \times B$, there exists $x \in A$ such that $f(x) = z$ and $y \in B$ such that $f(y) = w$. Then, by definition, we have

$$(f \times g)(x, y) = (z, w).$$

Since $(z, w) \in A \times B$ was arbitrary, this shows that $f \times g$ is surjective.

But then the composition

$$\mathbb{N} \xrightarrow{\sim} \mathbb{N} \times \mathbb{N} \xrightarrow{f \times g} A \times B$$

is surjective. Therefore, by the lemma, $A \times B$ is countable. □

Corollary 3.2.12. *Let $A_1, \ldots, A_n$ be a finite collection of countable sets. Then the cartesian product*

$$A_1 \times A_2 \times \cdots \times A_n$$

is countable.

Proof. This follows by induction from the previous theorem (see homework). □

Example 3.2.13. We now know that the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Z} \times \mathbb{N}, \mathbb{Z} \times \mathbb{Z}, \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}$, *etc.*, are *all countable.*

Question: Do there exist uncountable sets??

3.3 Uncountable sets (Feb 23)

Above we discussed *countable sets.* An infinite set S is said to be **uncountable** if it is not countable, *i.e.*, there *does not exist any* bijection from $\mathbb{N}$ to S. The goal of this section is to show that indeed, uncountable sets exist. This fact was discovered by Georg Cantor in 1878.

Given a set S and a positive integer $n \in \mathbb{N}$, we shall denote the *n-fold cartesian product* by

$$\begin{aligned} S^n &= \overbrace{S \times S \times S \times \cdots \times S}^{n \text{ times}} \\ &= \{(a_1, a_2, \ldots, a_n) \mid a_i \in S \text{ for } i = 1, \ldots, n\}. \end{aligned}$$

The elements of this set are sometimes called "n-tuples." (For $n = 2$, we say "pairs," and for $n = 3$ we say "triples," *etc.*)

Example 3.3.1. Take $S = \{0, 1\}$. Then $|S| = 2$. It was shown on homework that $|S \times S| = 4$, by constructing an explicit bijection with $\mathcal{P}_4$. More generally, we have:

Proposition 3.3.2. *For $S = \{0, 1\}$, $|S^n| = 2^n$.*

Proof. The base case is clear. For induction, assume the result for n. We have

$$\begin{aligned} S^{n+1} = S^n \times S &= \{0,1\}^n \times \{0,1\} \\ &= \{0,1\}^n \times \{0\} \cup \{0,1\}^n \times \{1\} \\ &= \{(a_1, a_2, \ldots, a_n, 0\} \cup \{b_1, b_2, \ldots, b_n, 1\}. \end{aligned}$$

Since the union is "disjoint," *i.e.* the sets do not overlap, we have:

$$\begin{aligned} |S^{n+1}| &= |\{0,1\}^n \times \{0\}| + |\{0,1\}^n \times \{1\}| \\ &= 2^n + 2^n \\ &= 2^{n+1}. \end{aligned}$$

This completes the induction. □

Notice that the order of this set grows "exponentially" with n; although of course if S is finite, then S^n is still finite for each $n \in \mathbb{N}$. What we need is a much bigger set.

Definition 3.3.3. Given any set S, we denote the "infinite" cartesian product by

$$\begin{aligned} S^{\mathbb{N}} &= S \times S \times S \times \cdots \\ &= \{(a_1, a_2, a_3, \cdots) \mid a_i \in S \text{ for } i \in \mathbb{N}\}. \end{aligned}$$

An element of $S^{\mathbb{N}}$ is an "infinite string" or "**sequence**" of elements of S.

Example 3.3.4. Let $S = \{0, 1\}$. Then the set $S^{\mathbb{N}}$ is the set of all infinite binary sequences. Here are a few examples of elements of this set.

- $(0, 0, 0, 0, 0, \ldots)$ = sequence of all 0's
- $(1, 1, 1, 1, 1, \ldots)$ = sequence of all 1's

- $(1,0,0,1,0,0,1,0,0,\ldots)$ sequence of $1,0,0$ repeating ad infinitum
- $(1,1,1,0,1,0,1,0,0,0,1,0,1,0,0,0,1,0,1,0,0,0,1,\ldots)$ = the sequence defined by

$$a_n = \begin{cases} 1 & n \text{ is prime} \\ 0 & n \text{ is composite.} \end{cases}$$

- $(1,1,0,0,1,0,0,1,0,0,0,0,\ldots)$ = digits in the binary expansion of π (essentially a random sequence of 0's and 1's).
- $(1,0,0,1,0,1,0,0,0,1,1,0,\ldots)$ = transmission data of Thursday's lecture video over the internet...

The point here is that the set $\{0,1\}^{\mathbb{N}}$ contains an absolutely vast array of possible sequences....in fact, it turns out to be even bigger than the set of natural numbers $\mathbb{N}$.

Theorem 3.3.5 (G. Cantor, 1878)**.** *The set* $\{0,1\}^{\mathbb{N}}$ *is uncountable.*

Proof. Suppose, on the contrary, that $\{0,1\}^{\mathbb{N}}$ is countable. Then it is possible to list (*i.e.* index) all of its elements by the natural numbers, as follows:

$$\{0,1\}^{\mathbb{N}} = \{s_1, s_2, s_3, \ldots\}.$$

For example, our list might consist of the following sequences:

$$\begin{array}{llllll} s_1 = 0, & 1, & 0, & 1, & 0, & \cdots \\ s_2 = 1, & 0, & 1, & 0, & 0, & \cdots \\ s_3 = 1, & 1, & 1, & 0, & 1, & \cdots \\ s_4 = 0, & 1, & 1, & 0, & 0, & \cdots \\ s_5 = 1, & 0, & 0, & 1, & 1, & \cdots \\ \quad\vdots & & \vdots & & & \ddots \end{array}$$

We now construct a new sequence, s, as follows. If the first digit of s_1 is 0, let the first digit of s be 1, and vice-versa. If the second digit of s_2 is 1, let the second digit of s be 0, and vice-versa. Continuing, if the n'th digit of s_n is 0, let the n'th digit of s be 1, and vice-versa. So, in the above example, we would change each digit on the diagonal,

$$\begin{array}{rlllll} s = 1, & 1, & 0, & 1, & 0, & \cdots \\ 1, & 1, & 1, & 0, & 0, & \cdots \\ 1, & 1, & 0, & 0, & 1, & \cdots \\ 0, & 1, & 1, & 1, & 0, & \cdots \\ 1, & 0, & 0, & 1, & 0, & \cdots, \end{array}$$

to obtain the sequence $s = (1, 1, 0, 1, 0, \ldots)$.

By construction, the n'th element of s is different from the n'th element of s_n, for each $n \in \mathbb{N}$. Therefore, as elements of $\{0,1\}^{\mathbb{N}}$, we have

$$s \neq s_n \text{ for all } n \in \mathbb{N}.$$

But this means that the sequence s appears nowhere on the list $s_1, s_2, s_3, \ldots$, which contradicts our assumption.

We conclude that no such list can include all the elements of $\{0,1\}^{\mathbb{N}}$, *i.e.*, this set is uncountable. □

3.4 Another look at Cantor's proof (Feb 25)

Above, we viewed the set

$$\{0,1\}^{\mathbb{N}} = \{(a_1, a_2, a_3, \ldots)\}$$

as the set of all sequences of 0's and 1's. Equivently, we may think of any such sequence as a *function* from $\mathbb{N}$ to $\{0,1\}$: given such a sequence, we can define a function by

$$f(n) = a_n \in \{0,1\}$$

and vice-versa. So it is completely equivalent to define:

$$\{0,1\}^{\mathbb{N}} = \{f : \mathbb{N} \to \{0,1\}\}$$

as the set of all possible functions from $\mathbb{N}$ to $\{0,1\}$. More generally, given two sets S and T, we can define

$$T^S = \{\text{set of all functions from } S \text{ to } T\}.$$

We should note that two functions f and g are *equal* if and only if

$$f(x) = g(x) \; \forall \, x \in S.$$

So, to show that $f \neq g$, you just have to make sure that there exists at least one $x \in S$ such that

$$f(x) \neq g(x).$$

(Above, we treated sequences in the same way.)

It's worth reviewing the proof of Cantor's theorem from this perspective.

Proof of Theorem 3.3.5, *redux.* Assume that the set of all functions from $\mathbb{N} \to \{0,1\}$ can be indexed by the natural numbers:

$$\{0,1\}^{\mathbb{N}} = \{f_1, f_2, f_3, \ldots\}.$$

Define a new function by

$$\begin{aligned} f : \mathbb{N} &\to \{0,1\} \\ n &\mapsto \begin{cases} 0 & \text{if } f(n) = 1 \\ 1 & \text{if } f(n) = 0. \end{cases} \end{aligned}$$

Since each $n \in \mathbb{N}$ is mapped to exactly one value, this is a function. And, by construction, we have

$$f(n) \neq f_n(n) \; \forall \, n \in \mathbb{N},$$

and so

$$f \neq f_n$$

as functions, for all $n \in \mathbb{N}$. But this contradicts our assumption. □

This proof can easily be adapted to show that for any set S with $|S| \geq 2$, the set $S^{\mathbb{N}}$ is uncountable. For instance, with $S = \{0,1,2,3,4,5,6,7,8,9\}$, we could just define

$$f(n) = \begin{cases} 1 & \text{if } f_n(n) = 0 \\ 2 & \text{if } f_n(n) = 1 \\ & \vdots \\ 9 & \text{if } f_n(n) = 8 \\ 0 & \text{if } f_n(n) = 9. \end{cases}$$

In fact, any choice so that $f(n) \neq f_n(n)$ works.

The next question one might ask is if there exist *even bigger* sets than $\{0,1\}^{\mathbb{N}}$. In fact, we have the following:

Theorem 3.4.1. *For any set S, there does not exist a bijection between S and $\{0,1\}^S$.*

Proof. Adapt the proof of Cantor's theorem (exercise!). □

So, given any set S, one can always make a *strictly larger* set just by taking the set of all functions from S to $\{0,1\}$. This shows that "infinity" actually comes in infinitely many different sizes.

4 Number systems

4.1 Rules of Arithmetic (March 9)

Below is the set of all integers

$$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

This is more than just a set, it comes equipped with arithmetical operations.

4.1.1 Addition

What is "addition"? It is a map:

$$f_+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$(a, b) \longmapsto f_+(a, b) = \text{“}a + b\text{”} (\textit{Just a notation})$$

This map satisfies the following **axioms**, for any $a, b, c \in \mathbb{Z}$.

A1: $a + b = b + a$ i.e. $f_+(a, b) = f_+(b, a)$
A2: $(a + b) + c = a + (b + c)$ i.e. $f_+(f_+(a, b), c) = f_+(a, f_+(b, c))$
A3: $a + 0 = a$
A4: $a + (-a) = 0$

Note: $-(-a) = a$ by definition

. Note: You can prove these axioms by induction from even simpler axioms (Peano's axioms). It is good to see how to prove the familiar laws of arithmetic from the above axioms.

Proposition 4.1.1. *if $a + x = a$, then $x = 0$.*

Proof. if $x + a = a$, then,
$(-a) + (x + a) = (-a) + a$ (Because f_+ is a function). But

$$\begin{aligned} (-a) + a &= a + (-a) && (A1) \\ &= 0 && (A4) \end{aligned}$$

Therefore

$$\begin{aligned} (-a) + (x + a) &= 0 \\ &= (-a) + (a + x) && (A1) \\ &= ((-a) + a) + x && (A3) \\ &= 0 + x && (A4) \\ &= x + 0 && (A1) \\ &= x && (A3) \end{aligned}$$

$\therefore \quad x = 0.$ □

Definition 4.1.2. "$a - b$" $= a + (-b)$. In the last proof, we just "subtracted a from both sides".

4.1.2 Multiplication

We can also "multiply" two integers together: It is a map:

$$f_{\cdot} : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$(a, b) \longmapsto f_{\cdot}(a, b) = \text{``}a \cdot b\text{''}$$

This map satisfies the following axioms, for any $a, b, c \in \mathbb{Z}$.

M1: $a \cdot b = b \cdot a$ i.e. $f_{\cdot}(a, b) = f_{\cdot}(b, a)$
M2: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
M3: $1 \cdot a = a (= a \cdot 1)$
M4: $a \cdot (b + c) = a \cdot b + a \cdot c$ i.e. $f_{\cdot}(a, f_{+}(b, c)) = f_{+}(f_{\cdot}(a, b), f_{\cdot}(a, c))$
M5: If $x \cdot y = x \cdot z$ and $x \neq 0$, then $y = z$

Note: You can also prove these by induction using addition.

$$1 \cdot a = a$$
$$2 \cdot a = a + a$$
$$3 \cdot a = 2a + a$$
$$\cdots$$
$$(n + 1) \cdot a = n \cdot a + a$$

Proposition 4.1.3. $a \cdot 0 = 0$.

Proof.

$$\begin{aligned} a \cdot 0 + a \cdot 0 &= a \cdot (0 + 0) \qquad (M4) \\ &= a \cdot 0 \qquad (A3) \end{aligned}$$

Subtracting $a \cdot 0$ from both sides, we obtain

$$a \cdot 0 = 0 \qquad (M4)$$

$\square$

Proposition 4.1.4. $(-a) \cdot (-b) = a \cdot b$.

Proof. We first show that

$$(-a) \cdot b = -(a \cdot b)$$

$$\begin{aligned}
(-a) \cdot b + a \cdot b &= ((-a) + a) \cdot b \qquad (M4) \\
&= 0 \cdot b \qquad (A3) \\
&= 0 \qquad \text{(last proposition)}
\end{aligned}$$

Subtracting $-(a \cdot b)$ from both sides, we now calculate

$$\begin{aligned}
(-a) \cdot (-b) - (a \cdot b) &= (-a) \cdot (-b) + [-(a \cdot b)] \\
&= (-a) \cdot (-b) + (-a) \cdot b \qquad \text{(just showed)} \\
&= (-a) \cdot ((-b) + b) \\
&= (-a) \cdot 0 \\
&= 0
\end{aligned}$$

$\therefore \quad (-a) \cdot (-b) = a \cdot b$ □

Note: we just showed that the product of two negative numbers is positive!

4.1.3 Ordering

In addition to "+" and "·", $\mathbb{Z}$ comes with an "ordering", $<$ or $>$.

O1: $\forall a, b \in \mathbb{Z}$, exactly one of the following is true:
$a < b$, or
$a > b$, or
$a = b$
O2: if $a < b$ and $b < c$, then $a < c$
O3: if $b < c$, then $a + b < a + c$
O4: if $a, b > 0$, then $a \cdot b > 0$

We write $a \leq b$ if $a < b$ or $a = b$, etc. Note: Rather than a function on $\mathbb{Z} \times \mathbb{Z}$, "$<$" is represented as a subset

$$S_< \subset \mathbb{Z} \times \mathbb{Z}$$

where

$$(a, b) \in S_< \text{ iff "} a < b \text{"}.$$

Rewriting O2 and O3 from before:

O2: if $(a, b) \in S_<$ and $(b, c) \in S_<$, then $(a, c) \in S_<$

O3: if $(b, c) \in S_<$, then $(f_+(a, b), f_+(a, c)) \in S_<$

Proposition 4.1.5. *The following properties are true of "<".*

i) *if $x > 0$ and $y < z$, then $x \cdot y < x \cdot z$*

ii) *if $x < 0$ and $y < z$, then $x \cdot y > x \cdot z$*

iii) *if $x \neq 0$, then $x^2 > 0$*

Proof. **i)** if $z > y$ then

$$z + (-y) > y + (-y) = 0 \qquad \text{(O3)}$$
$$\Rightarrow z - y > 0$$

Since $x > 0$,

$$x \cdot (z - y) > 0 \qquad \text{(O4)}$$
$$\Rightarrow x \cdot z - x \cdot y > 0 \qquad \text{(M4)}$$
$$\Rightarrow x \cdot z - x \cdot y + x \cdot y > x \cdot y \qquad \text{(A2, A3, A4)}$$
$$\Rightarrow x \cdot z > x \cdot y.$$

ii) if $x < 0$ and $z > y$, then

$$-[x \cdot (z - y)]$$
$$= (-x) \cdot (z - y) \qquad \text{(by proof of proposition above)}$$

Since $x > 0$, $-x < 0$

So by (i), we have:

$$(-x) \cdot (z - y) > 0$$
$$\Rightarrow -[x \cdot (z - y)] > 0$$
$$\Rightarrow 0 > x(z - y)$$
$$\Rightarrow 0 > xz - xy$$
$$\Rightarrow xy > xz.$$

iii) By 01, either $x > 0$ or $x < 0$ (because $x \neq 0$)

if $x > 0$, then $x^2 = x \cdot x > 0$ by **O4**

if $x < 0$, then

$$x^2 = (-x) \cdot (-x) > 0 \qquad \text{(by proposition above)}$$

since $-x > 0$. □

4.1.4 Division

We now want to "extend" $\mathbb{Z}$ to contain fractions $\frac{p}{q}$, where $p, q \in \mathbb{Z}$.

We want to build a set that contains these elements. Notice that $\frac{p}{q}$ is a pair of integers, where $q \neq 0$.

First Attempt: take the Cartesian product:

$$\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\}).$$

We think of a pair (p, q) as a fraction $\frac{p}{q}$. How do we add, subtract, multiply these pairs?

Definition 4.1.6. $\frac{p}{q} + \frac{p'}{q'} = \frac{pq' + qp'}{qq'}$

$$(p, q) + (p', q') = (pq' + qp', qq') \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$$

Does this "+" equation also satisfy A1 - A4 above? Yes.

$$\textbf{A1:} \quad \begin{aligned} (p, q) + (p', q') &= (pq' + qp', qq') \\ &= (p'q + q'p, q'q) \\ &= (p', q') + (p, q) \qquad \text{(by the axioms for } \mathbb{Z}) \end{aligned}$$

$$\textbf{A2:} \quad \begin{aligned} ((p, q) + (p', q')) + (p'', q'') &= (pq' + qp', qq') + (p'', q'') \\ &= (p'q + q'p, qq') + (p'', q'') \\ &= ((pq', qp')q'' + qq'p'', qq'q'') \\ &= (pq'q'' + p'q''q + q'p''q, qq'q'') \end{aligned}$$

In fact, all axioms work!

Definition 4.1.7. $\frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp''}{qq'''}$.

$$(p, q) \cdot (p', q') = (pp', qq')$$

But we want: $p \cdot \frac{1}{p} = 1$

whereas, in $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$, we have $p \cdot \frac{1}{p} = (p, 1) \cdot (1, p) = (p, p)$. But in the set $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$, $(p, p) \neq (1, 1)$.

So what we need to do is define a new set, called $\mathbb{Q}$, the rational numbers, by "declaring" that $(p, p) = (1, 1)$. And more generally, that $(p, q) = (p', q')$ if and only if $\exists r \in \mathbb{Z}$ s.t.

$$p \cdot r = p' \text{ and } q \cdot r = q'$$

or

$$p = r \cdot p' \text{ and } q = r \cdot q'.$$

4.2 Equivalence relations (Mar 11)

Goal: construct the set of rational numbers, $\mathbb{Q}$. This should be composed of pairs of integers (p,q), with $q > 0$, representing a fraction $\frac{p}{q}$.

We need to declare that

$$(2,3),(4,6),(6,9), etc.$$

all represent the same number. (Because $\frac{2}{3} = \frac{4}{6} = \frac{6}{9} = \dots$)

We're going to write this as:

$$(2,3) \sim (4,6)$$

but:

$$(5,8) \nsim (16,30).$$

Why? Because

$$(30 \cdot 5 = 150) \neq (16 \cdot 8 = 128).$$

We're now going to describe a new set operation that allows us to "declare different elements to be the same."

Definition 4.2.1. We say that a relation $\sim$ is "an equivalence relation" if

1) $\forall x \in S, x \sim x$(reflexive)

2) $\forall x, y \in S$, if $x \sim y$ then $y \sim x$(symmetric)

3) $\forall x, y, z \in S$, if $x \sim y$ and $y \sim z$, then $x \sim z$(transitive)

Example 4.2.2. Consider the relation on $\mathbb{Z}$ given by

$$x \sim y \iff x^2 = y^2.$$

Is this an equivalence relation? Need to check 3 properties:

1) $x \sim x$? $x^2 = x^2$ (reflexive)

2) $x \sim y \Rightarrow x^2 = y^2$

$\Rightarrow y^2 = x^2$

$\Rightarrow y \sim x$ (symmetric)

3) $x \sim y, y \sim z$

$\Rightarrow x^2 = y^2$ and $y^2 = z^2$

$\Rightarrow x^2 = z^2$
$\Rightarrow x \sim z$ (transitive)

This is an equivalence relation.

$$1 \sim -1$$
$$2 \sim -2$$
$$\cdots$$
$$n \sim -n$$
$$0 \sim 0$$

Example 4.2.3. Consider the relation on $\mathbb{Z}$ defined by:

$$x \sim y \iff x \leq y$$

<u>Reflexive:</u> $x \sim x$?
$x \leq x$.

<u>Transitive:</u> if $x \leq y$ and $y \leq z$, then $x \leq z$.
by O3, this is true.

<u>Symmetric:</u> if $x \leq y$, is $y \leq x$?
$2 \leq 3$ but $3 \nleq 2$.

So this <u>is not</u> an equivalence relation!

Example 4.2.4. Let S be a course with 9 students, sitting in a lecture hall. The relation "a is sitting next to b".
Symmetric? Yes.
Reflexive? Yes.
Transitive? No.
This <u>is not</u> an equivalence relation.
However, let's try: "a is sitting in the same row as b".

$$\begin{array}{ccc} a & f & i \\ e & b & d \\ g & h & c \end{array}$$

Symmetric? Yes.
Reflexive? Yes.
Transitive? Yes.
So this <u>is</u> an equivalence relation!

Definition 4.2.5. Given an equivalence relation on a set, and an element $a \in S$, we write

$$[a] = \{b \in S \mid a \sim b\}$$

to denote the equivalence class of a.

$$[a] \subset S.$$

Sometimes, a is called a "representative" of $[a]$.

In example 1, $x \sim y \iff x^2 = y^2$.
We have:

$$[1] = \{1, -1\}$$

$$[2] = \{2, -2\}$$

$$\dots$$

$$[n] = \{n, -n\}$$

$$[0] = \{0\}$$

In example 4.2.4 (lecture hall),

$$[a] = \{a, f, i\}$$

$$[f] = \{f, a, i\} = [a]$$

$$[g] = \{g, h, c\}$$

Proposition 4.2.6. *Suppose that $\sim$ is an equivalence relation on a set S.*

- **i)** *if $x \sim y$, then $[x] = [y]$ as a subset of S.*
- **ii)** *if $x \nsim y$, then $[x] \cap [y] = \varnothing$.*

Proof. **i)** Assume $x \sim y$. Let us show that $[x] \subset [y]$.
Given $z \in [x]$, we have $z \sim x$.
By transitivity, this is the same as $x \sim y$,
$z \sim x \sim y \Rightarrow z \sim y \Rightarrow z \in [y]$.
Since $z \in [x]$ was arbitrary, we're done.

ii) We show the contrapositive:
Assume $[x] \cap [y] \neq \varnothing$.
Then let $z \in [x] \cap [y]$. Then $z \sim x$, and $z \sim y$.
But then by transitivity, $x \sim z \sim y \Rightarrow x \sim y$. □

Definition 4.2.7. We write $S/\sim$ to denote "S modulo $\sim$", the set of all equivalence classes of $\sim$ on S. This is a collection of disjoint subsets of S.

$$\text{if } A \in X/\sim \text{ and } B \in X/\sim,$$

$$\text{then if } A \neq B, \text{ then}$$

$$A \cap B = \varnothing$$

Also,

$$\bigcup_{A \in S/\sim} A = S$$

(because every element $x \in S$ is contained in its own equivalence class, $A = [x]$).

In example 1, we have

$$\mathbb{Z}/\sim = \{\{0\}, \{1, -1\}, \{2-, -2\}, \dots\}$$

We could write

$$\{[0], [1], [2], [3], \dots\}$$

There is an obvious bijection

$$\mathbb{N} \cup \{0\} \longmapsto \mathbb{Z}/\sim$$

$$n \longmapsto [n]$$

$\mathbb{Z}/\sim$ is countably infinite. In example 4.2.4 (lecture hall), we had

$$S/\sim = \{\{a, i, f\}, \{g, h, c\}, \{e, b, d\}\}$$
$$= \{[a], [b], [c]\}$$

In $S/\sim$, we have:

$$[a] = [f], \text{ and}$$

$$[g] = [c], \text{ etc.}$$

4.3 The rational numbers (Mar 11)

Now, consider the following relation on $\mathbb{Z} \times \mathbb{N}$

$$(p, q) \sim (p', q') \iff pq' = p'q.$$

Note in particular that if $p' = q \cdot r$, for $r \in \mathbb{N}$, then

$$p \cdot q' = p \cdot (q \cdot r) = (p \cdot r) \cdot q = p' \cdot q.$$

So $[(p, q)] = [(p', q')]$. (This corresponds to "cross-multiplication!")

$$\frac{p}{q} = \frac{p'}{q'} \iff pq' = p'q$$

Proposition 4.3.1. $\sim$ *is an* *equivalence relation.*

Proof.

1) $(p,q) \sim (p,q)$? Yes.

2) if $(p,q) \sim (p',q')$, does $(p',q') \sim (p,q)$?

$pq' = p'q$

$\Rightarrow p'q = pq'$ (M1)

$\Rightarrow (p',q') \sim (p,q)$

3) if $(p,q) \sim (p',q')$ and $(p',q') \sim (p'',q'')$, does (p,q) (p'',q'')?

Have: $pq' = p'q$ and $p'q'' = p''q'$.

Need: $pq'' = p''q$.

$pq'q'' = p'qq''$

$\Rightarrow pq''q' = q(p'q'')$

$\Rightarrow pq'' = qp''$

Since $q' \neq 0$, by (M5), we have $pq'' = qp''$

$\Rightarrow (p,q) \sim (p'',q'')$ □

Definition 4.3.2. The rational numbers, $\mathbb{Q}$, are defined as:

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{N}) / \sim$$

where $\sim$ is the equivalence relation:

$$(p,q) \sim (p',q') \iff pq' = p'q$$

So a natural number is an equivalence class of pairs

$$[(p,q)] = \{(p,q),(2p,2q),(3p,3q),\dots\}$$

These all represent the "fraction" $\dfrac{p}{q}$.

We can define the equations "+" and "·", and the order "<", as follows:

$$[(p,q)] + [(p',q')] = [\frac{pq'+p'q}{qq'}]$$

$$[(p,q)] \cdot [(p',q')] = [(pp',qq')]$$

$$[(p,q)] < [(p',q')] \text{ if } pq' < qp'.$$

Moreover, if $p \neq 0$, we can also define the inverse:

$$[(p,q)]^{-1} = \begin{cases} (q,p) & p > 0 \\ (-q,-p) & p < 0. \end{cases}$$

This satisfies:

$$[(p,q)]\cdot[(p,q)]^{-1} = \begin{cases} [(p,q)\cdot(q,p)] = [(pq,pq)] = [(1,1)] & p > 0 \\ [(p,q)\cdot(-q,-p)] = [(-pq,-pq)] = [(1,1)] & p < 0 \end{cases}$$

Note: Strictly speaking, we need to check that these operations are "well-defined", i.e. if

$$[(p,q)] = [(p',q')],$$

then

$$[(p,q)] + [(p'',q'')] = [(p',q')] + [(p'',q'')].$$

i.e, that "f_+" is a function on $\mathbb{Q}$. I encourage you to check this as an exercise.

Theorem 4.3.3. *The rational numbers, $\mathbb{Q}$, also satisfy the axioms A1-A4, M1-M5, O1-O4.*

Proof. We actually checked A1 and A2 already last class, and you have M4 and O3 on your homework. The rest can be checked in a similar way. □

4.4 Properties of $\mathbb{Q}$ (Mar 16)

From last lecture, we defined the set of rational numbers, $\mathbb{Q}$. We know that this number system satisfies the same axioms as $\mathbb{Z}$.

Proposition 4.4.1. *The map*

$$\mathbb{Z} \longrightarrow \mathbb{Q}$$

$$n \longmapsto [(n,1)]$$

is injective.

Proof. We have to check that if $m \neq n$, then $[(n,1)] \neq [(m,1)]$, i.e. $(m,1) \sim (n,1)$. But if $m \neq n$, then $m\cdot 1 \neq n\cdot 1$, so by definition of $\sim$,

$$(n,1) \nsim (m,1).$$

Therefore the above map is injective. □

We will now switch to the following "standard" notation for rational numbers:

$$\frac{p}{q} = [(p,q)]$$

$$\frac{p}{q} = [(2p,2q)]$$

$$\frac{p}{q} = [(100p,100q)]$$

$$\frac{p}{q} = \left[\left(\frac{p}{2}, \frac{q}{2}\right)\right] \text{ if } p \text{ and } q \text{ are both even.}$$

$$n = \frac{n}{1} = [(n,1)]$$

$$0 = \frac{0}{1} = [(0,1)]$$

$$1 = \frac{1}{1} = [(1,1)].$$

Theorem 4.4.2. *Let $x, y \in \mathbb{Q}$ with $x < y$. There exist infinitely many rational numbers, $z \in \mathbb{Q}$, with*

$$x < z < y.$$

Proof. Take the average of the x and y values:

$$z = \frac{x+y}{2} \in \mathbb{Q}$$

Then, since $x < y$, we can write:

$$x + x < x + y < y + y$$

$$2x < x + y < 2y$$

$$x < \frac{x+y}{2} < y$$

$$x < z < y.$$

If we continue this method for more z-values, we can choose:

$$z' = \frac{x+z}{2}$$

Thus, we know that

$$x < z' < z < y.$$

Continuing, we write

$$z'' = \frac{x+z'}{2}$$

$$\Rightarrow x < z'' < z' < z < y$$

$$\Rightarrow x < \ldots < z'' < z' < z < \ldots < y.$$

$\square$

Question: How big is the set $\mathbb{Q}$? Is it countably infinite or uncountably infinite?

Proposition 4.4.3. *$\mathbb{Q}$ is countably infinite.*

Proof. $\mathbb{Q}$ is certainly infinite, since there is an injective map from $\mathbb{Z}$ to $\mathbb{Q}$ (by the last proposition).

Note that $\mathbb{Z} \times \mathbb{N}$ is countable, and there exists a surjective map:

$$\mathbb{Z} \times \mathbb{N} \twoheadrightarrow \mathbb{Q}$$

$$(p, q) \longmapsto [(p, q)]$$

Therefore, $\mathbb{Q}$ is countable. $\square$

Problem: $\mathbb{Q}$ is full of holes!

Theorem 4.4.4. *There does not exist $x \in \mathbb{Q}$ such that $x^2 = 2$.*

Proof. Suppose that $x = \frac{p}{q}$ satisfies the equation $x^2 = 2$. We may assume, without loss of generality, that p and q are not both even. (This can be achieved this by cancelling their common factors of 2). We can write:

$$\begin{aligned} x^2 = 2 \iff & p^2 = 2q^2 \\ & \implies \text{p is even} \\ & \implies p = 2r \text{ for some } r \in \mathbb{Z}. \end{aligned}$$

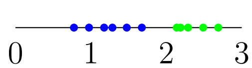
But then

$$\begin{aligned} p^2 &= (2r)^2 \\ &= 4r^2, \text{ and so} \\ 4r^2 &= 2q^2. \end{aligned}$$

Cancelling a factor of 2, we obtain:

$$\begin{aligned} 2r^2 &= q^2 \\ &\implies q^2 \text{ is also even} \\ &\implies q \text{ is even.} \end{aligned}$$

But, this contradicts our assumption that p and q are not both even. $\square$



The blue set of numbers satisfy $r^2 < 2$. The green set of numbers satisfy $r^2 > 2$. Between these two sets, there should exist a number called "$\sqrt{2}$." But we do not yet know that such a number exists!

We need to define a number system in which $\sqrt{2}$ exists. This number system will be called the real numbers, $\mathbb{R}$. More generally, we want $\mathbb{R}$ to have the following special property.

Definition 4.4.5. (i) Given a set E, we say that M is an **upper bound** for E if for all $x \in E$, $x \leq M$.

(ii) We say that E is **bounded above** if an upper bound exists.

(iii) We say that $\overline{M}$ is the **least upper bound** for E if $\overline{M}$ is itself an upper bound for E and for any given upper bound, M, we have $\overline{M} \leq M$.

(iv) We say that a number system (for instance, $\mathbb{R}$) has the **least upper bound property** if, for any subset E that is bounded above, there exists a least upper bound $\overline{M}$ for E. In this case,

$$\overline{M} = \sup E$$

is called the **supremum** of E.

Example 4.4.6. Let $E = \{x \in \mathbb{Q} \mid x^2 < 2\}$. Is this set bounded above? Yes. Let $M = 2$.

$$\text{If } x^2 < 2, \text{then } x < 2$$

$$\implies M = 2 \text{ is an upper bound for } E.$$

BUT there does *not* exist a least upper bound for E within the natural numbers, $\mathbb{Q}$. This is because, given any $x \in \mathbb{Q}$ with $x^2 < 2$, there exists $y \in \mathbb{Q}$ with $y > x$ and $x^2 < y^2 < 2$...see homework.

$$\implies \mathbb{Q} \text{ does not have the least upper bound property!}$$

Idea: Instead of just rational numbers, we will consider entire subsets of $\mathbb{Q}$ and make a number system out of those!

4.5 The real numbers (Mar 18)

Goal: Construct a number system, $\mathbb{R}$, that has the least upper bound property.

Recall that given any subset $E \subset \mathbb{R}$, if E is bounded above, then there exists a least upper bound (supremum) for E, in $\mathbb{R}$.

Then for any upper bound M, $\overline{M} \leq M$.

Note that this is not true for the set $\mathbb{Q}$. We can consider the set $E = \{r \in \mathbb{Q} \mid r^2 < 2\}$.

Definition 4.5.1. A subset $\alpha \subset \mathbb{Q}$ is said to be a Dedekind Cut if it satisfies the following three properties:
1. α is a proper subset of $\mathbb{Q}$ (i.e. $\alpha \neq 0, \mathbb{Q}$)
2. If $r \in \alpha$ and $s < r$, where $s \in \mathbb{Q}$, then $s \in \alpha$
3. If $s \in \alpha$, $\exists r \in \alpha$ with $s < r$.

Example 4.5.2. Let $0^* = \{r \in \mathbb{Q} \mid r < 0\}$ Is this a Dedekind cut?
1. $-1 \in 0^*$, $1 \neq 0^*$, therefore $0^* \neq 0$, $0^* = \mathbb{Q}$✓
2. Let $r \in 0^*$. Then $r < 0$. Given $s < r$, $s < 0$

$$\implies s \in 0^* ✓$$

3. Let $s \in 0^*$. Then $s < 0$. Let $r = \frac{s}{2}$. Then,

$$s < \frac{s}{2} < 0$$

$$\implies s < r \text{ and } r \in 0^*.\checkmark$$

Therefore, 0^* is a Dedekind cut.

Example 4.5.3. Given any rational number $t \in \mathbb{Q}$, we define

$$t^* = \{r \in \mathbb{Q} \mid r < t\}.$$

This is called a "rational" Dedekind cut. Then we must check if this set follows the parameters of a Dedekind cut:
1. $t - 1 \in t^*$ and $t + 1 \neq t*$

$$\implies t \neq 0, \mathbb{Q}$$

2. Given $r \in t^*$, we have $r < t$. So if $s < r$, then $s < r < t$

$$\implies s \in t^* \checkmark$$

3. Given $s \in t^*$, we take

$$r = \frac{s+t}{2}.$$

Since we have $s < t$, we write

$$s < r < t$$

$$\implies r \in t^* \text{ and } r > s.\checkmark$$

So this is in fact a Dedekind cut!

Example 4.5.4. Let $\alpha = \{r \in \mathbb{Q} \mid r^2 < 2\} \cup 0^*$ This is a Dedekind cut (this will be proved on HW). But, it does not equal t^* for <u>any</u> rational number t! This is true since $\sqrt{2}$ is not rational. This would be called an <u>irrational</u> Dedekind cut.

Example 4.5.5. The set $\{r \in \mathbb{Q} \mid r \leq 1\}$ is <u>not</u> a Dedekind cut. Why is this the case? Property (III) fails for $s = 1$.

Definition 4.5.6. Given two cuts α and β, we define the "sum"

$$\alpha + \beta = \{r + s \mid r \in \alpha, s \in \beta\}$$

Is this a Dedekind cut?
1. If $\alpha \neq 0$ and $\beta \neq 0$, then $\alpha + \beta \neq 0$. Given $r \notin \alpha$ and $s \notin \beta$, we must have

$$r + s \neq \alpha + \beta$$

If $r \neq \alpha$, then $\forall\ r' \in \alpha$, we have $r' < r$. This is true since if $\mathbf{r} \leq \mathbf{r'}$, then $r \in \alpha$ by property (2.). Also, if $s \notin \beta$, then $\forall\ s' \in \beta$, we have $\mathbf{s'} < \mathbf{s}$. So, $\forall\ r' \in \alpha$ and $s' \in \beta$, we have

$$r' + s\text{"} < r + s$$

$$\implies r + s \notin \alpha + \beta$$

$$\implies \alpha + \beta \neq \mathbb{Q}\checkmark$$

2. Given $r \in \alpha + \beta$, we have $r = t + t'$, for $t \in \alpha$, $t' \in \beta$. Given that $s < r$, let $t'' = t' + s - r < t'$

$$\implies t'' \in \beta$$

But then, we see

$$t + t'' = t + t' + s - r$$

$$= r + s - r$$

$$= s$$

$$\implies s \in \alpha + \beta\checkmark$$

3. Given that $s \in \alpha + \beta$, we have $s = t + t'$ and $t \in \alpha, t' \in \beta$. By property (2.), for β, $\exists t'' \in \beta$ such that $t'' > t'$. Then,

$$t + t'' \in \alpha + \beta$$

and

$$t + t'' > t + t' > s$$

Therefore

$$r = t + t'' > s$$

and

$$r \in \alpha + \beta\checkmark$$

Therefore, we conclude that $\alpha + \beta$ is a Dedekind cut!

Next, we define the order "<" on two Dedekind cuts by:

$$\alpha < \beta \iff \alpha \subsetneq \beta.$$

This means that α is a proper subset of β. We can also write that

$$\alpha > \beta \iff \alpha \supsetneq \beta$$

$$\alpha = \beta \iff \alpha \text{ and } \beta \text{ are equal and subsets of } \mathbb{Q}.$$

Definition 4.5.7. The real number system, $\mathbb{R}$, is defined to be the set of all Dedekind cuts, with the operation "+" and the order "<" defined above.

We have the following inclusions:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

$$n \in \mathbb{Z} \mapsto [(n,1)] \in \mathbb{Q}$$

$$r \in \mathbb{Q} \mapsto r^* \in \mathbb{R}$$

Theorem 4.5.8. *$\mathbb{R}$ satisfies all of the axioms A1-A4, M1-M5, O1-O4.*

Proof. (A1)

$$\alpha + \beta = \{r + s \mid r \in \alpha, s \in \beta\}$$

$$= \{s + r \mid s \in \beta, r \in \alpha\}$$

$$= \beta + \alpha \checkmark$$

(A2) Same

(A3) We need to show:

$$\alpha + 0^* = \alpha$$

($\subset$) Given that $r \in \alpha + 0^*$, we have that $r = t + t'$ for $t \in \alpha, t' \in 0^*$

$$\implies t' < 0$$

$$\implies r < t$$

$$\implies r \in \alpha \text{ (by (2.))} \checkmark$$

($\supset$) Given that $r \in \alpha$, by (3.), $\exists E \in \alpha$ with $r < t$. Then, $r - t < 0$

$$\implies r - t \in 0^*.$$

But then, we have,

$$r = t + r - t \in \alpha + 0^*.$$

$$\implies r \in \alpha + 0^*. \checkmark$$

(A4) Define the following:

$$-\alpha = \{s \in \mathbb{Q} \mid \exists t > 0, -s - t \notin \alpha\}$$

<u>Claim</u>: $\alpha + (-\alpha) = 0^*$

($\subset$) Given that $r \in \alpha$ and $s \in -\alpha$, $\exists t > 0$ such that $-s - t \notin \alpha$

$$-s - t > r$$

$$\implies 0 > r + s + t$$

$$\Longrightarrow 0 > r + s$$

$$\Longrightarrow r + s \in 0^* \checkmark$$

($\supset$) Given $q > 0$, we must show that

$$-q \in \alpha + (-\alpha)$$

Let $t = \frac{q}{2}$. We choose $n \in \mathbb{N}$ such that

$$n \cdot t \in \alpha \text{ but,}$$

$$(n+1) \cdot t \notin \alpha$$

Next, let $r = -(n+2)t$

$$\begin{aligned} \Longrightarrow -r - t &= (n+2)t - t \\ &= (n+1)t \notin \alpha \\ \Longrightarrow r &\in -\alpha. \end{aligned}$$

But then, we see that

$$\begin{aligned} r + (n \cdot t) &= -(n+2)t + nt \\ &= -2t = -q \end{aligned}$$

$$\Longrightarrow \text{Since } r \in -\alpha \text{ and } nt \in \alpha, \text{ we conclude that } -q \in \alpha + -(\alpha) \checkmark$$

The rest of the axioms can be proved similarly. □

Note that

$$\mathbb{Q} \subset \mathbb{R}$$

$$r \longmapsto r^*$$

$$(r+s)^* = r^* + s^*$$

$$r < s \Longrightarrow r^* < s^*.$$

The real numbers fill the "holes" in the number system $\mathbb{Q}$! In fact, we have:

Theorem 4.5.9. $\mathbb{R}$ *satisfies the least upper bound property.*

Proof. Let $E \subset \mathbb{R}$ be a nonempty subset that is bounded above (i.e. $\exists \beta \in \mathbb{R}, \forall \gamma \in E, \gamma < \beta$). We need to construct the least upper bound of E. We write

$$\alpha = \bigcup_{\gamma \in E} \gamma \subset \mathbb{Q}.$$

We claim that α is a Dedekind cut, and is the least upper bound of E.
(1.) $\alpha \neq 0$ since $\gamma \in E$ is a Dedekind cut, and then it is nonempty as a subset of $\mathbb{Q}$. Since $\gamma \subset \beta, \forall \gamma \in E$, we see that $\alpha \subset \beta \subsetneq \mathbb{Q}$

$$\implies \alpha \subsetneq \mathbb{Q} \checkmark$$

(2.) If $r \in \alpha$, then $r \in \gamma$ for some $\gamma \in E$. Given that $s < r, s \in r$

$$\implies s \in \alpha \checkmark$$

(3.) Same as (2.) ✓ Therefore α is the least upper bound!
- α is an upper bound for E, because given any $\gamma \in E$, we have $\gamma \subset \bigcup \gamma = \alpha$

$$\implies \gamma \subset \alpha$$

$$\implies \gamma < \alpha \checkmark$$

-Let α' be any other upper bound for E. We need to show that $\alpha \leq \alpha'$, meaning that $\alpha \subset \alpha'$
Let $r \in \alpha$. Then, $r \in \gamma$ for some $\gamma \in E$. Since α' is an upper bound for E, $\gamma \subset \alpha$!

$$\implies r \in \alpha'$$

Since $r \in \alpha$ was arbitrary, we know that $\alpha \subset \alpha'$. □

4.6 Properties of $\mathbb{R}$ (Mar 23)

We proved above that $\mathbb{R}$ satisfies the least-upper-bound property. This will be crucial to developing limits, calculus, etc. There are two more properties of $\mathbb{R}$ that are easy to prove from the above construction.

Theorem 4.6.1. *(i) Given any $\alpha > 0^*$ in $\mathbb{R}$, and $\beta \in \mathbb{R}$, there exists $n \in \mathbb{N}$ such that*

$$n \cdot \alpha > \beta$$

This is called the **Archimedean property** *of* $\mathbb{R}$.
(ii) Given any $\alpha, \beta \in \mathbb{R}$ such that $\alpha < \beta$, there exists some $r \in \mathbb{Q}$ such that

$$\alpha < r^* < \beta$$

This is sometimes referred to as the **density of $\mathbb{Q}$ in $\mathbb{R}$.**

Proof. (i) Pick a rational number s $\in \alpha$ with $s > 0$. Then

$$s = \frac{p}{q} \text{ for } p, q \in \mathbb{N}.$$

Pick $r = \frac{p'}{q'} \notin \beta$, and let $n = q \cdot p' \in \mathbb{N}$.

Claim: $n \cdot s \notin \beta$

For,

$$n \cdot s = (q \cdot p') \cdot \frac{p}{q} = pp' > \frac{p'}{q'} = r.$$

Since $r \notin \beta$ and $n \cdot s > r$, $n \cdot s \notin \beta$ (by contrapositive of (II)) but $n \cdot s \in n \cdot \alpha$.

$$\implies n \cdot \alpha \supset \beta$$

$$\implies n \cdot \alpha > \beta$$

as real numbers.

(ii) If $\alpha < \beta$, then $\alpha \subsetneq \beta$ by definition. So $\exists r \in \beta, r \notin \alpha$, so $\alpha \subset r^*$ (by contrapositive of (II)). Also $r^* \subsetneq \beta$ (because $r \in \beta$, but $r \notin r^*$)).

So $\alpha \subsetneq r^* \subsetneq \beta$ i.e. $\alpha < r^* < \beta$ as real numbers. $\square$

Also, for any $\alpha > 0$, we can define $\sqrt[n]{\alpha} = \{t \in \mathbb{Q} \mid t > 0, t^n \in \alpha\} \cup 0^*$.

Question: How big is $\mathbb{R}$? Is it countably infinite or uncountably infinite?

Recall that $\{0, 1, 2, ..., 9\}^{\mathbb{N}}$ is the set of all sequences with digits 0 through 9. Given $\underline{a} = (a_1, a_2, a_3, ...)$, we want to define

$$\text{“}.a_1a_2a_3a_4...,\text{''}$$

i.e., the real number with decimal expansion $\underline{a}$.

Given $n \in \mathbb{N}$, we first define the *rational* number

$$s_n = \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + ... + \frac{a_n}{10^n}$$

$$\text{“} = .a_1a_2...a_n''.$$

To get the whole string as a real number, define:

$$f(\underline{a}) = \{t \in \mathbb{Q} \mid t < s_n \text{ for some} n \in \mathbb{N}\}.$$

It's not hard to see that this is a Dedekind cut!

Moreover, the only way for two sequences $\underline{a}$ and $\underline{a'}$ to have $f(\underline{a}) = f(\underline{a'})$ is if

$$\underline{a} = .a_1a_2...a_n1000...$$

and

$$\underline{a'} = .a_1a_2...a_n0999,$$

or vice versa.

Theorem 4.6.2. *The set* $\mathbb{R}$ *is uncountable.*

Proof. Assume, for contradiction, that $\mathbb{R}$ is countable. Above, we defined a map

$$f : \{0, 1, ..., 9\}^{\mathbb{N}} \to \mathbb{R}$$

$$\underline{a} \mapsto .a_1 a_2 a_3 ...$$

Given $y \in \mathbb{R}$, there exist at most two sequences, $\underline{a}$ and $\underline{a'}$, with $f(\underline{a}) = f(\underline{a'})$. Therefore

$$| f^{-1}(\{y\}) | \leq 2 \quad \forall y \in \mathbb{R}.$$

In particular, $f^{-1}(\{y\})$ is countable. But, by definition, we have $\{0, ..., 9\}^{\mathbb{N}} = \bigcup_{y \in \mathbb{R}} f^{-1}(\{y\})$. So if $\mathbb{R}$ were countable, this would be a countable union of countable sets $\implies$ countable. But this contradicts Cantor's theorem that $\{0, 1, ..., 9\}^{\mathbb{N}}$ is uncountable. $\square$

4.7 Supremum and infimum (Mar 23)

We will now stop using Dedekind cut notation. We'll write 0 instead of 0^*, $\alpha < \beta$ instead of $\alpha \subsetneq \beta$, etc.

Definition 4.7.1. $[0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ and $(0, 1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$.

Recall that $\sup E$ = least upper bound of a set E that is bounded above.

If E is not bounded above, we write $\sup E = \infty$. This is just a notation to say that E is *not* bounded above.

Definition 4.7.2. Given a subset $E \subset \mathbb{R}$ that is bounded below, we write

$\inf E$ = "infimum of E" = greatest lower bound of E.

(In other words, this is a number $\underline{N} \in \mathbb{R}$ such that $N \leq x$ $\forall x \in E$ and, given $N \in \mathbb{R}$ with $N \leq x$ $\forall x \in E$, $N \leq \underline{N} = \inf E$.)

If E is not bounded below, then we write $\inf E = -\infty$.

Example 4.7.3.

$$\sup(0, 1) = 1 = \sup[0, 1]$$

$$\inf(0, 1) = 0 = inf[0, 1].$$

Example 4.7.4. $\sup \mathbb{N} = \infty$ (because $\mathbb{N}$ is not bounded above).

Example 4.7.5. Fix $x > 0$. Let $E = \{n \cdot x \mid n \in \mathbb{N}\}$. Then $\sup E = \infty$.

Proof. Let $m \in \mathbb{R}$. By the Archimedean property, $\exists n \in \mathbb{N}$ such that $n \cdot x > M$. Therefore, M is not an upper bound for E. Since $M \in \mathbb{R}$ was arbitrary, E is not bounded above. $\square$

Example 4.7.6. $\sup \mathbb{Z} = \infty$, $\inf \mathbb{Z} = -\infty$ (because $\mathbb{Z}$ is bounded neither above nor below.)

Theorem 4.7.7. *For any set $E \subset \mathbb{R}$ such that E is bounded below, the infimum* $\inf E \in \mathbb{R}$ *exists ($\infty \notin \mathbb{R}$).*

Proof. Let $-E = \{x \in \mathbb{R} \mid -x \in E\}$ then $-E$ is bounded above. Let $\underline{N} = -\sup(-E)$. One can check that this is the infimum of E! $\square$

5 Sequences and limits

5.1 The definition of a limit (Mar 25)

Definition 5.1.1. A **sequence** is an infinite string of real numbers $\underline{a} = (a_1, a_2, a_3, ...)$. In our earlier notation, this is just an element of $\mathbb{R}^{\mathbb{N}} = \{\text{functions from } \mathbb{N} \text{ to } \mathbb{R}\}$, where we write $f(n) = a_n$.

Example 5.1.2. $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, ...$

$a_n = \frac{1}{n}$

Example 5.1.3. 1, 2, 3, 4, 5, 6, ...

$a_n = n \ \forall n \in \mathbb{N}$

Example 5.1.4. 1, 0, 1, 0, 1, 0, 1, 0, ...

$$a_n = \begin{cases} 1 & \text{n odd} \\ 0 & \text{n even} \end{cases}$$

Example 5.1.5. 1, 1.4, 1.41, 1.414, 1.4142, 1.41425, ...

This is the decimal expansion of $\sqrt{2}$.

Example 5.1.6. 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, ...

Example 5.1.7. 3, 1, 4, 1, 5, 9, 2, 6, ...

This is the sequence of digits in the decimal expansion of π. (Essentially just a random sequence of integers in $\{0, ..., 9\}$.)

Let L be a real number. *Informally,* a sequence $\underline{a}$ converges to L if a_n "becomes arbitrarily close to L as n becomes arbitrarily large." In the above examples:

Example 5.1.2: $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, ...$ This converges to $L = 0$.

Example 5.1.3: $1, 2, 3, 4, 5, ...$ This diverges to infinity.

Example 5.1.4: $1, 0, 1, 0, 1, 0, ...$ This diverges (all of the points have to get close to the same L).

Example 5.1.5: $1, 1.4, 1.41, 1.414, ...$ This converges to $\sqrt{2}$.

Example 5.1.6: $1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, ...$ Diverges.

We now make the *formal* definition of a limit, as follows.

Definition 5.1.8. We write $a_n \to L$, or

$$\lim_{n \to \infty} a_n = L$$

if the following statement is true: for each $\varepsilon > 0$, $\exists N \in \mathbb{N}$ such that

$$|a_n - L| < \epsilon$$

for all $n > N$.

If no such $L \in \mathbb{R}$ exists, we say that $\underline{a}$ diverges.

Note: Order of quantifiers is essential.

Proposition 5.1.9. *The sequence* $a_n = \frac{1}{n}$ *converges to* $L = 0$, *i.e.*

$$\lim_{n\to\infty} \frac{1}{n} = 0.$$

Proof. Let $\varepsilon > 0$. We need to find N such that $\forall n \geq N$, $|a_n - 0| < \varepsilon$.

We have:

$$|a_n - 0| = |a_n| = \frac{1}{n}$$

$$\text{and } \frac{1}{n} < \varepsilon \Leftrightarrow 1 < n \cdot \varepsilon.$$

By the Archimedean property of $\mathbb{R}$ (Theorem 4.6.1i), $\exists N \in \mathbb{N}$ such that $1 < N \cdot \epsilon$. Then for any $n > N$, we have

$$1 < N \cdot \varepsilon < n \cdot \varepsilon \implies 1 < n \cdot \varepsilon \implies \frac{1}{n} < \varepsilon,$$

which is the desired inequality. Therefore, N has the required property.

Since $\varepsilon > 0$ was arbitrary, we're done. $\square$

Note: By a similar proof, one can show

$$\lim_{n\to\infty} \frac{1}{n^p} = 0 \quad \forall p > 0.$$

Proposition 5.1.10. *The sequence* $a_n = 1 + \frac{(-1)^n}{n}$ *converges to* $L = 1$.

$0, \frac{3}{2}, \frac{2}{3}, \frac{5}{4}, \frac{4}{5}, \frac{7}{6}, \frac{6}{7}, \ldots$

Proof. Let $\varepsilon > 0$. We have

$$|a_n - 1| = \left|\frac{(-1)^n}{n}\right| = \frac{1}{n}.$$

By the proof of the previous proposition, we know $\exists N > 0$ such that $\frac{1}{n} < \varepsilon$ $\forall n > N$

$$\implies |a_n - 1| = \frac{1}{n} < \varepsilon,$$

which is the desired statement. Since $\varepsilon > 0$ was arbitrary, we're done. $\square$

Proposition 5.1.11. *The sequence*

$$a_n = \begin{cases} 0 & n \text{ even} \\ 1 & n \text{ odd} \end{cases}$$

is **divergent**.

Proof. To prove that $\underline{a}$ diverges, we need to show that no possible $N \in \mathbb{R}$ can satisfy the definition, let $L \in \mathbb{R}$. We must show that $a_n \nrightarrow L$, i.e. in $\exists \varepsilon > 0$ such that $\forall N \in \mathbb{R}$, $\exists n > N$ with $| a_n - L | \geq \varepsilon$. In this case, we let $\varepsilon = \frac{1}{2}$.

Case 1: $L \geq \frac{1}{2}$

For n even, we have $a_n = 0 \implies | a_n - L | = | 0 - L | = | L | \geq \frac{1}{2} = \varepsilon$. So $| a_n - L | \nless \varepsilon$ $\forall$n even. Since, for any N, $\exists n > N$ that are even, this shows that $a_n \nrightarrow L$

Case 2: $L < \frac{1}{2}$

For n odd, we have $a_n = 1 \implies | a_n - L | = | 1 - L | > \frac{1}{2}$.

Since $L < \frac{1}{2} \implies -L > \frac{1}{2} \implies 1 - L > \frac{1}{2} \implies | a_n - L | \nless \frac{1}{2} = \varepsilon$. Since $\forall N, \exists n > N$ with n odd, this shows that $a_n \nrightarrow L$

This covers all possible L, so we're done. □

The following simple lemma is very useful for doing limits.

Lemma 5.1.12 (Triangle inequality)**.** *For $x, y,$ and $z \in \mathbb{R}$ we have*

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

Proof. Let $a = x - y$, $b = y - z$

$a + b = x - y + y - z = x - z$ so the above inequality is equivalent to:

$$|a + b| \leq |a| + |b|$$

.

Case 1: $a, b \geq 0$. Then

$$|a + b| = a + b = |a| + |b|$$

so we're done.

Case 2: $a, b \leq 0$. Then

$$|a + b| = -(a + b) = -a - b = |a| + |b|$$

so we're done.

Case 3: $a < 0, b > 0$ and $0 < -a \leq b$. This implies that $a + b > 0$. So we have:

$$|a + b| = a + b = -|a| + |b| < |a| + |b|$$

and we're done.

There are a few more similar cases, which we omit. □

Theorem 5.1.13. *The limit of any convergent sequence is unique.*

Proof. Suppose that $a_n \to L$, but also $a_n \to L'$.

We need to show that $L = L'$.

Let $\varepsilon > 0$. We know that there exists N such that if $n > N$ then $| a_n - L | < \frac{\varepsilon}{2}$, and $\exists N'$ such that $\forall n > N'$, $| a_n - L' | < \frac{\varepsilon}{2}$. But then by the triangle inequality,

$|L - L'| \leq |L - a_n| + |a_n - L'| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$, for $n >$ max (N, N') $\implies |L - L'| < \varepsilon$

Since $\varepsilon > 0$ was arbitrary, this implies that $L = L'$ □

Definition 5.1.14. We say that a sequence is bounded above (and respectively below) if the set $\{a_n \mid n \in \mathbb{N}\}$ is bounded above.

Note: A sequence can be bounded above (and below) and still diverge.

Proposition 5.1.15. *Any convergent sequence is bounded above (and below).*

Note: In other words, boundedness is a *necessary, but not sufficient* condition for convergence.

Proof. Let $L \in \mathbb{R}$ such that $a_n \to L$. Let $\epsilon = 1$. Since $a_n \to L$, there exists N such that $\forall n > N$, $|a_n - L| < 1$. Since $a_n - L + L = a_n$, $|a_n| \leq |a_n - L| + |L|$ by the triangle inequality for
$n > N \implies |a_n| < 1 + |L| \implies \{|a_n| \mid n > N\}$ is bounded above.
But the set $\{|a_n| \mid n \leq N\}$ is also bounded above, since this is a finite set.
So $\{|a_n| \mid n \in \mathbb{N}\} = \{|a_n| \mid n \leq N\} \cup \{|a_n| \mid n > N\}$ is also bounded above.
If $\{|a_n| \mid n \in \mathbb{N}\}$ is bounded above, then $\{a_n \mid n \in \mathbb{N}\}$ is bounded. □

5.2 Limit rules (Mar 30)

Theorem 5.2.1. *Suppose that $\underline{a}$ and $\underline{b}$ are convergent sequences with $a_n \to a$ and $b_n \to b$. Then*
1.$a_n + b_n \to a + b$
2.$ca_n \to ca$
3.$a_n * b_n \to a * b$
4.If $b_n \neq 0 \forall n$, and $b \neq 0$, then $a_n/b_n \to a/b$.

Proof of 1. Given $\varepsilon > 0, \exists N_1, N_2$ such that

$$n \geq N_1 \Rightarrow |a_n - a| < \varepsilon/2$$

and

$$n \geq N_2 \Rightarrow |b_n - b| < \varepsilon/2.$$

Let $N = \max(N_1, N_2)$.
Then for $n \geq N$, we have

$$|a_n + b_n - (a + b)| = |(a_n - a) + (b_n - b)|.$$

By the Triangle Theorem,

$$\leq |a_n - a| + |b_n + b| < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

by construction. Since $\varepsilon > 0$ was arbitrary, we are done. □

Proof of 2. Given $\varepsilon > 0$, choose N such that, $|a_n - a| < \varepsilon/c$, for $n > N$,

$$\begin{aligned} &|c * a_n - c * a| \\ &= |c * (a_n - a)| \\ = |c||a_n - a| < &|c| * \varepsilon/|c| \\ &= \varepsilon. \end{aligned}$$

Since $\varepsilon > 0$ and was arbitrary, we're done. □

Proof of 3.

$$a_n * b_n \to a * b$$

We first do the special case that $a = 0$. We need to show that

$$a_n * b_n \to 0 * b = 0$$

$$\Rightarrow$$

$$a_n * b_n \to 0.$$

Let $\varepsilon > 0$. By last class, since b_n is convergent, it is bounded by some number $B > 0$.

$$\Rightarrow$$

$$|b_n| < B, \forall n \in N$$

Since $a_n \to 0$ by assumption, Choose N such that

$$|a_n - 0| = |a_n| < \varepsilon/B$$

$\forall n > N$. But then,

$$\begin{aligned} |a_n b_n - 0| = |a_n b_n| &= |a_n||b_n| \\ &< \frac{\varepsilon}{B} B = \varepsilon. \end{aligned}$$

Since $\varepsilon > 0$ was arbitrary, we are done with this case.

So, if $a_n \to 0$ and $b_n \to b$, then $a_n b_n \to 0$.

For the general case, consider the sequence

$$(a_n - a) b_n.$$

Note that $a_n - a \to a - a = 0$ by the first property. By the previous case, we have

$$(a_n - a) * b \to 0.$$

By the second property, we also have

$$a b_n \to ab$$

(because a is just a constant). Therefore, the sequence

$$a_nb_n = a_nb_n - ab_n + ab_n = (a_n - a)b_n + ab_n.$$

By the first property,

$$a_nb_n \to 0 + ab = ab$$

as desired.

The proof for number 4 is skipped. □

Example 5.2.2. $a_n = 1 + ((-1)^n)/n$

$\lim_{n\to\infty} 1 = 1$ and

$\lim_{n\to\infty}(-1^n)/n = 0$

So, $\lim_{n\to\infty} a_n = 1 + 0 = 1$.

Example 5.2.3. $\lim_{n\to\infty}(100/n^2) * (5 + 10/\sqrt{n} + 8/\sqrt[3]{n})$

The limits all exist, so the limit of it is

$$0 * |5 + 0 + 0| = 0.$$

Example 5.2.4.

$$a_n = \frac{1 + (-1)^n}{n} = (1 + (-1)^n)\frac{1}{n}.$$

We can show directly that $\lim_{n\to\infty} a_n = 0$ or use the Squeeze Theorem:

if $0 < a_n < \frac{2}{n}$ as $0 \to 0$

as $\frac{2}{n} \to 0$

$a_n \to 0$.

5.3 Monotone sequences (Mar 30)

Recall that being bounded is a necessary but not sufficient condition for a general sequence to converge. However, there IS an important exception.

Definition 5.3.1. A sequence $\underline{a}$ is **monotonically increasing** if $a_n \le a_n + 1 \forall n$.

A sequence $\underline{a}$ is **monotonically decreasing** if $a_n \ge a_n + 1 \forall n$.

A sequence $\underline{a}$ is **monotone** if it is either monotonically increasing or decreasing.

Theorem 5.3.2. *Suppose that a sequence $\underline{a}$ is monotone and bounded, then $\underline{a}$ is convergent.*

Proof. Suppose $\underline{a}$ is monotonically increasing and bounded above. Let $E = a_n | n \in N$. Since a_n is bounded, E is bounded. We may therefore let $a = \sup E$.

We now claim that

$$a_n \to a.$$

By definition, we have

$$a_n \le a \forall n$$

since a is an upper bound for E. Let $\varepsilon > 0$. Since a is the least upper bound, there must exist N such that

$$a_n > a - \varepsilon.$$

But since $\underline{a}$ is monotone, we have

$$a_N \le a_n$$

$$\forall n \ge N.$$

$$a - \varepsilon \le a_N \le a_n \le a$$

$$\Rightarrow a - \varepsilon < a_n \le a$$

$$\Rightarrow a - a_n < \varepsilon,$$

$$a_n - a \le 0 < \varepsilon$$

$$|a - a_n| < \varepsilon$$

Since $\varepsilon > 0$ was arbitrary, we are done. $\square$

Example 5.3.3. Consider the sequence

$$a_n = (1 + \frac{1}{n})^n.$$

We have

$$a_n = (1 + \frac{1}{n})^n$$

$$= (\frac{n+1}{n})^n$$

$$a_n + 1 = (\frac{n+2}{n+1})^n + 1$$

So,

$$\frac{a_n + 1}{a_n} = \frac{(n+2)^n + 1}{(n+1)^n + 1} * \frac{(n+1)^n}{n^n}$$

$$= \frac{(n+2)^n + 1}{(n+1) * n^n}$$

$$= (\frac{n+1}{n})^n \times \frac{n+2}{n+1}$$

$$\frac{n+2}{n} > 1 \Rightarrow (\frac{n+2}{n})^n > 1$$

$$\frac{n+2}{n+1} > 1$$
$$\Rightarrow \frac{a_{n+1}}{a_n} > 1$$

Therefore, the sequence a_n is monotonically increasing. We will see later that a_n is bounded. Therefore, the previous Theorem implies that

$$\lim_{n \to \infty} a_n$$

exists!

This limit is just the number "e" (by definition).

5.4 $\limsup$ and $\liminf$ (Apr 1)

In the last class we proved the following theorem.

Theorem 5.4.1. *A bounded, monotone sequence is convergent.*

Proof. Let $L = \sup\{a_n \mid n \in \mathbb{N}\}$.

Then for each $\varepsilon > 0$, $\exists a_N$ such that

$$L - \varepsilon < a_N \leq L.$$

(If not, $L - \varepsilon$ is an upper bound; but then L is not the least upper bound!)

Since a_n is increasing, if $n > N$, then

$$L - \varepsilon < a_N \leq a_n \leq L$$

$$\Rightarrow |a_n - L| < \varepsilon.$$

□

What about a sequence that is bounded, but not necessarily monotone? We want to compare such a sequence with a monotone sequence (in fact, two of them.)

Let

$$E_n = \{a_n \mid m \geq n\}.$$

Define

$$A_n = \sup E_n = \sup_{m \geq n} a_m.$$

Lemma 5.4.2. *A_n is a decreasing sequence.*

Proof. Since $E_{n+1} \subset E_n$, the number $A_n = \sup E_n$ is an upper bound for E_{n+1}. Since A_{n+1} is the *least* upper bound of E_{n+1} (by definition), we have

$$A_n \geq A_{n+1}$$

as desired. □

Similarly, one has,

$$B_n \leq B_n + 1$$

$\Rightarrow B_n$ is an *increasing* sequence.

By the previous theorem, both sequences A_n, B_n are convergent! We can therefore make the following definition:

Definition 5.4.3.

$$\limsup_{n\to\infty} a_n = \lim_{n\to\infty} A_n$$

$$\liminf_{n\to\infty} a_n = \lim_{n\to\infty} B_n.$$

Example 5.4.4. $\underline{a} = (1, 0, 1, 0, 1, 0, ...)$

$$\limsup_{n\to\infty} a_n = 1$$

$$\liminf_{n\to\infty} a_n = 0.$$

Example 5.4.5. $a_n = (-1)^n * (1 + 1/n)$

$$\limsup_{n\to\infty} a_n = 1$$

$$\liminf_{n\to\infty} a_n = -1.$$

Example 5.4.6. $\underline{a} = (1, 0, 2, 0, 3, 0, 4...)$

$$A_n = \sup_{m\geq n} a_m = \infty \, \forall n,$$

$$A_n = (\infty, \infty, ...)$$

$$\lim_{n\to\infty} A_n = \infty$$

$$\limsup_{n\to\infty} a_n = \infty.$$

On the other hand, we have,

$$\liminf_{n\to\infty} a_n = 0.$$

Example 5.4.7. (0, -1, 0, -2, 0, -3...)

$$\limsup_{n\to\infty} a_n = 0$$

$$\liminf_{n\to\infty} a_n = -\infty.$$

Example 5.4.8. Let $a_n = \frac{(-1)^n}{n}$. Then

$$\limsup_{n\to\infty} a_n = 0 = \liminf_{n\to\infty} a_n.$$

In fact, this is just a convergent sequence, with $\lim_{n\to\infty} a_n = 0$.

More generally, we have the following:

Theorem 5.4.9. *Let $\underline{a}$ be a bounded sequence. Then $\underline{a}$ is convergent if and only if*

$$\limsup_{n\to\infty} a_n = \liminf_{n\to\infty} a_n.$$

In this case, we have

$$\lim_{n\to\infty} a_n = \limsup_{n\to\infty} a_n = \liminf_{n\to\infty} a_n.$$

Proof. We shall write

$$\bar{L} = \limsup_{n\to\infty} a_n$$
$$\underline{L} = \liminf_{n\to\infty} a_n.$$

($\Rightarrow$) Suppose that $\underline{a}$ is convergent, with $\lim_{n\to\infty} a_n = L$. Then, given $\varepsilon > 0$, $\exists$ N such that

$$\begin{aligned}
|a_n - L| &< \varepsilon \\
(\forall n &> N) \\
\Rightarrow a_n - L &< \varepsilon \\
\Rightarrow a_n &< L + \varepsilon \\
(\forall n &> N) \\
\Rightarrow \sup_{n\geq N+1} a_n &\leq L + \varepsilon \\
\Rightarrow \lim_{N\to\infty} \sup_{n\geq N+1} a_n &\leq L + \varepsilon \\
\bar{L} &\leq L + \varepsilon.
\end{aligned}$$

But also,

$$\begin{aligned}
L - a_n &< \varepsilon \\
\Rightarrow L - \varepsilon &< a_n \\
(\forall n &> N) \\
\Rightarrow L - \varepsilon &< \inf_{n\geq N+1} a_n \\
\Rightarrow L - \varepsilon &\leq \lim_{N\to\infty} \inf_{n\geq N+1} a_n \\
\Rightarrow L - \varepsilon &\leq \underline{L}.
\end{aligned}$$

Therefore,

$$\bar{L} \leq L + \varepsilon = (L - \varepsilon) + 2\varepsilon$$
$$\bar{L} \leq \underline{L} + 2\varepsilon.$$

By homework, we always have

$$\begin{aligned} \underline{L} &\le \bar{L} \\ \Rightarrow \underline{L} &\le \bar{L} \le \underline{L} + 2\varepsilon \\ \Rightarrow |\bar{L} - \underline{L}| &\le 2\varepsilon. \end{aligned}$$

Since $\varepsilon > 0$ is arbitrary, we conclude that $\underline{L} = \bar{L}$

($\Leftarrow$) Suppose that

$$\underline{L} = \bar{L}.$$

Let $L = \underline{L} = \bar{L}$. We will show that

$$\lim_{n\to\infty} a_n = L.$$

Let $\varepsilon > 0$. By definition of the limsup, $\exists N_1$ such that

$$\sup_{m\ge N_1} a_m < \bar{L} + \varepsilon.$$

By definition of the liminf, there exists N_2 such that

$$\underline{L} - \varepsilon < \inf_{m\ge N_2} a_m.$$

For $n > N = \max(N_1, N_2)$, we have

$$\inf_{m\ge N} a_m \le a_n \le \sup_{m\ge N} a_m.$$

Combining with the above, we have

$$\underline{L} - \varepsilon < \inf_{m\ge n} \le a_n \le \sup_{m\ge n} a_n.$$

But

$$\begin{aligned} \underline{L} = \bar{L} &= L \\ L - \varepsilon < a_n < L + \varepsilon &\quad \forall n > N \\ \Rightarrow |a_n - L| &< \varepsilon. \end{aligned}$$

Since $\varepsilon > 0$ was arbitrary, we are done. □

5.5 Subsequences and the Bolzano-Weierstrass Theorem (Apr 8)

The following notion can be very helpful for dealing with sequences.

Definition 5.5.1. Given a sequence a_n and an increasing sequence of positive integers

$$n_1 < n_2 < n_3 < \cdots,$$

the sequence a_{n_i}, *i.e.*

$$a_{n_1}, a_{n_2}, a_{n_3}, \cdots$$

is called a **subsequence** of a_n.

Example 5.5.2. $a_n = \begin{cases} 0 & n \text{ even} \\ 1 & n \text{ odd} \end{cases}$. This has two obvious subsequences:

$$(a_1, a_3, a_5, \ldots) = (1, 1, 1, \ldots)$$

and

$$(a_2, a_4, a_6, \ldots) = (0, 0, 0, \ldots).$$

Note that while the original sequence is divergent, each of these subsequences is *convergent*. In this way, passing to a subsequence can help you "fix" the divergence of a sequence. In fact, for *bounded* sequences, this is always possible.

Theorem 5.5.3 (Bolzano-Weierstrass)**.** *Any bounded sequence has a convergent subsequence.*

This is a very well-known theorem, and there are many different ways to prove it. Fortunately, with the technology we have already developed, we can give a very fast proof. In fact, we shall prove the following more precise theorem, which clearly implies Bolzano-Weierstrass as a corollary.

Theorem 5.5.4. *Given any bounded sequence a_n, there exists a subsequence a_{n_i} such that*

$$\lim_{i\to\infty} a_{n_i} = \limsup_{n\to\infty} a_n.$$

There also exists a subsequence a_{m_j} such that

$$\lim_{j\to\infty} a_{n_j} = \liminf_{n\to\infty} a_n.$$

Proof. Let $\overline{L} = \limsup_{n\to\infty} a_n$. We know that the sequence

$$A_n = \sup_{m\geq n} a_n$$

converges to $\overline{L}$.

Let $\varepsilon = \frac{1}{2i}$. Since $A_n \to \overline{L}$, there exists N such that

$$|A_N - \overline{L}| < \frac{1}{2i}.$$

Since $A_N = \sup_{m\geq N} a_m$, there must exist $m \geq N$ such that

$$|a_m - A_N| < \frac{1}{2i}.$$

Let $n_i = m$. By the triangle inequality, we have

$$|a_{n_i} - \overline{L}| < |a_{n_i} - A_N| + |A_N - \overline{L}| < \frac{1}{2i} + \frac{1}{2i}$$

and

$$|a_{n_i} - \overline{L}| < \frac{1}{i}.$$

But $\frac{1}{i} \to 0$ as $i \to \infty$. Therefore (by HW), the sequence a_{n_i} satisfies

$$\lim_{i\to\infty} a_{n_i} \to \overline{L}.$$

So, a_{n_i} is the desired subsequence.

The subsequence a_{m_j} converging to $\liminf_{n\to\infty} a_n$ is obtained in a similar way. □

Note that the Bolzano-Weierstrass Theorem follows immediately from this theorem (since the lim sup and lim inf of any bounded sequence exists as a real number). We can also make the following corollary:

Corollary 5.5.5. *A bounded sequence a_n is divergent if and only if there exist two (or more) convergent subsequences, a_{n_i} and a_{m_j}, such that*

$$\lim_{i\to\infty} a_{n_i} \neq \lim_{j\to\infty} a_{m_j}.$$

Proof. This follows from Theorem 5.4.9 and the previous theorem. □

Note: This corollary applies only to *bounded* sequences. If a sequence is unbounded, it may not have *any* convergent subsequences (see HW).

Example 5.5.6. Consider the sequence of integers $\underline{a} = (3, 1, 4, 1, 5, 9, 2, 6, 2, 7, \ldots)$. This is the sequence of digits of π, so a_n lies in the finite set $[0, 9] \cap \mathbb{Z}$ for each n. In particular, the sequence is bounded, so we know from the Bolzano-Weierstrass Theorem that it must have a convergent subsequence. In this case, however, this is obvious. Why? Because there are only 10 digits, at least one of them (say d) must occur infinitely many times. Then

$$d, d, d, d, d, \ldots$$

is a subsequence of a_n, which (clearly) converges to d.

Example 5.5.7. Consider the following sequence of real numbers:

$$a_1 = \pi = 3.141592\ldots$$

$$a_2 = 1.415926\ldots$$

$$a_3 = 4.1519262\ldots$$

$$a_4 = 1.5192627\ldots$$

$$\vdots$$

This is a sequence of real number between 0 and 10. By the Bolzano-Weierstrass Theorem, it must have a convergent subsequence. We discussed a somewhat more explicit way to construct such a subsequence, by "freezing" one digit at a time:

$$d_1. *****$$

$$d_1.d_2 *****$$

$$d_1.d_2d_3 ****$$

$$d_1.d_2d_3d_4 ***.$$

This is Frank Morgan's (very informal) proof of Bolzano-Weierstrass, on p. 38 of the text.

5.6 Accumulation points (Apr 13)

Let $E \subset \mathbb{R}$ be a subset and $p \in \mathbb{R}$.

Definition 5.6.1. We say p is an accumulation point of E, if there exists a sequence $a_n \in E$ with $a_n \to p$, $a_n \neq p, \forall n$. We denote by E' the set of all accumulation points of E.

Example 5.6.2. $E = \mathbb{Q}$, $E' = \mathbb{R}$!

Formal proof. Let $x \in \mathbb{R}$, we need to construct a sequence of rationals: $a_n \to x$ (with $a_n \neq x$). By density of $\mathbb{Q}$ in $\mathbb{R}$, for any $\varepsilon > 0$, $\exists\ r \in \mathbb{Q}$, such that

$$x - \varepsilon < r < x.$$

Choose $\varepsilon = \frac{1}{n}$. There exists $r = a_n$, such that

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

Do this for each $n \in \mathbb{N}$, we obtain a sequence a_n with

$$|a_n - x| < \frac{1}{n},$$

$$\Rightarrow\ a_n \to x,$$

$$(\text{also, } a_n < x \Rightarrow a_n \neq x, \forall n)$$

□

Informal proof. Take the decimal expansion of x:

$$x = d_1d_2.d_3d_4d_5d_6\dots$$

Let

$$a_1 = d_1 0.0000\dots$$

$$a_2 = d_1 d_2.0\dots$$
$$a_3 = d_1 d_2.d_3 0\dots$$
$$a_4 = d_1 d_2.d_3 d_4 00\dots$$

$$\Rightarrow a_n = 10.d_1 + d_2 + \frac{d_3}{10} + \frac{d_4}{100} + \cdots + \frac{d_n}{10^{n-1}}$$
$$= \frac{10^n d_1 + 10^{n-1} d_2 + \cdots + 10 d_{n-1} + d_n}{10^{n-1}}$$

$$\Rightarrow a_n \in \mathbb{Q} \text{ for each } n,\ |a_n - x| = 00.00000 d_{n+1} d_{n+2} \cdots < .000001$$
$$\Rightarrow a_n \to x!$$

□

Example 5.6.3 (From Homework). $E = \{r^2 \mid r \in \mathbb{Q}\}$, $E' = [0, \infty)$. Let $x \geq 0$. How to construct a sequence $a_n \in \mathbb{Q}$ s.t. $a_n^2 \to x$?

Proof. By the previous example, we know that there exists a sequence $a_n \in \mathbb{Q}$, s.t. $a_n \to \sqrt{x} \in \mathbb{R}$!
By limit rules, $a_n^2 = a_n \cdot a_n \to \sqrt{x} \cdot \sqrt{x} = x! \Rightarrow a_n^2$ is a sequence of element of E that tends to x.
On the other hand, if $x < 0$, I claim there is no sequence $a_n \in \mathbb{Q}$ with $a_n^2 \to x$, $a_n^2 \geq 0 = b_n$, $\forall n$. By problem 3 of Homework 8,

$$\lim_{n\to\infty} a_n^2 \geq 0 > x \Rightarrow \lim_{n\to\infty} a_n^2 \neq x,\ x \notin E',\ \forall x < 0.$$
$$E' = [0, \infty).$$

□

Theorem 5.6.4. *Let $E \subset \mathbb{R}$ and $p \in \mathbb{R}$, then p is an accumulation point of E if and only if for every $\varepsilon > 0$, the set $E \cap ((p - \varepsilon, p + \varepsilon) \setminus p)$ is nonempty.*

Proof. ($\Rightarrow$) If $P \in E'$, then there exists a sequence $a_n \in E$, such that $a_n \to p$. Given $\varepsilon > 0$, $|a_n - p| < \varepsilon$, for n sufficiently large, i.e. $\exists\ N$, such that true for $n \geq N$, particularly, $(p - \varepsilon, p + \varepsilon)$ contains a_n. Since $a_n \neq p$,

$$((p - \varepsilon, p + \varepsilon) \setminus p) \ni a_n, \text{ but } a_n \in E$$

$$\Rightarrow E \cap ((p - \varepsilon, p + \varepsilon) \setminus p) \neq \varnothing.$$

($\Leftarrow$) Let $\varepsilon = \frac{1}{n}$. By assumption, $\exists\ x \in E$, such that

$$p - \varepsilon < x < p + \varepsilon, \quad x \neq p.$$

Let $a_n = x$. Do this for each $n \in \mathbb{N}$,

$$\Rightarrow 0 < |a_n - x| < \frac{1}{n}$$

$$\Rightarrow a_n \to x.$$

$\square$

Example 5.6.5. $E = \mathbb{Z}$ (set of integers), $E' = \varnothing$.

Proof. <u>Case 1</u>: $p \in \mathbb{Z}$. Let $\varepsilon = \frac{1}{2}, \left(p - \frac{1}{2}, p + \frac{1}{2}\right) \cap \mathbb{Z} = p$. $\Rightarrow \left(p - \frac{1}{2}, p + \frac{1}{2}\right) \smallsetminus p = \varnothing$. By previous theorem, $p \notin \mathbb{Z}$.
<u>Case 2</u>: $p \notin \mathbb{Z}$. Then $p \in (n, n+1)$, for some integer n, $\varepsilon_1 = p - n > 0$ and $\varepsilon_2 = p - (n+1) > 0$.
Let $\varepsilon = \min(\varepsilon_1, \varepsilon_2) \Rightarrow (p - \varepsilon, p + \varepsilon) \cap \mathbb{Z} = \varnothing$
$\Rightarrow p$ is <u>not</u> an accumulation point of $\mathbb{Z}$!
Overall, we get $\mathbb{Z}' = \varnothing$. $\square$

Example 5.6.6. $E = \left\{\frac{1}{n} \mid n \in \mathbb{N}\right\}, E' = \{0\}$, clearly, $0 \in E'$.

Theorem 5.6.7. *Let a_n be a convergent sequence with $a_n \to L$, $a_n \neq L$ for all n. Let $E = \{a_n \mid n \in \mathbb{N}\} \Rightarrow E' = \{L\}$.*

Proof. Proof is on Homework. $\square$

Compare with "Extra Credit" from this week's homework, how to construct a sequence with subsequences tending to any $x \in R$?
Idea: Make a sequence out of $\mathbb{Q}$!

$$\{a_n \mid n \in \mathbb{N}\} = \mathbb{Q}.$$
$$\mathbb{Q}' = \mathbb{R}.$$

Accumulation points of this set are just limits of subsequence.
$\Rightarrow$ A divergent sequence can have all manners of subsequence limits! (i.e. accumulation points of $\{a_n \mid n \in \mathbb{N}\}$). Whereas, convergent sequences have <u>only one</u> accumulation point.

6 Functions and limits

6.1 Limits of functions (Apr 13)

Let $E \subset \mathbb{R}$ be a subset and $p \in E'$ (an accumulation point of E). Consider a function

$$f : E \to \mathbb{R} \text{ with domain } E.$$

Definition 6.1.1. We say $\lim_{x \to p} f(x) = L$, if for any $\varepsilon > 0$, there exists $\delta > 0$, such that $|f(x) - L| < \varepsilon$, for all $x \in E$ with $0 < |x - p| < \delta$.

Note: p may not be a point of E. This is why we put

$$0 < |x - p|$$

in the definition. You only have to consider $x \neq p$.

Example 6.1.2. $f(x) = 2x$. Claim: for all $p \in \mathbb{R}$, $\lim_{x \to p} f(x) = 2p = L$.

Proof. Given $\varepsilon > 0$, let $\delta = \frac{\varepsilon}{2}$, if $|x - p| < \delta = \frac{\varepsilon}{2}$, then $|f(x) - L| = |2x - 2p| = 2|x - p| < 2\delta = \varepsilon$, definition is satisfied. □

Example 6.1.3. $f(x) = x^2$. Claim: $\lim_{x \to 1} f(x) = 1$.

Proof. Side Calculation:

$$f(x) - 1 = x^2 - 1 = (x - 1)(x + 1).$$

If $|x - 1| < \delta$, then

$$\begin{aligned} \left|x^2 - 1\right| &= |x + 1|\,|x - 1| \\ &< \delta\,|x + 1|. \end{aligned}$$

If $\delta < 1$, then

$$\begin{aligned} |x - 1| < 1 &\Rightarrow 0 \leqslant x \leqslant 2 \\ &\Rightarrow |x + 1| \leqslant 3 \\ &\Rightarrow \left|x^2 - 1\right| < 3\delta. \end{aligned}$$

Let $\varepsilon > 0$, if $\varepsilon \geq 3$, choose $\delta = \frac{1}{2}$; if $\varepsilon < 3$, choose $\delta = \frac{\varepsilon}{3}$. By the previous side calculation, since $\delta < 1$, we have

$$|f(x) - 1| = \left|x^2 - 1\right| < 3\delta = 3 \cdot \frac{\varepsilon}{3} = \varepsilon, \text{ if } \varepsilon < 3.$$

If $\varepsilon \geq 3$, then $\delta = \frac{1}{2} \Rightarrow 3\delta = \frac{3}{2} < 3 \leq \varepsilon$.
In either case, we have $|x^2 - 1| < \varepsilon$. □

Note: We could make an equivalent definition of Limits, where we only consider $0 < \varepsilon < 1$.

$$\text{"}\forall 0 < \varepsilon < 1, \exists\ \delta ...\text{"},\ |f(x) - L| < \frac{1}{2} < 1 < \varepsilon, \text{ if } \varepsilon > 1.$$

Or, we could have, at the beginning of the proof, said: "Without loss of generality, we assume that $\varepsilon < 1$."

Example 6.1.4. $f(x) = \frac{x^2-4}{x-2}$, $E = \mathbb{R} \setminus \{2\}$, $p = 2$ is accumulation point of $\mathbb{R} \setminus \{2\}$(*i.e.* $\underline{E}$), $a_n = 2 + \frac{1}{n} \Rightarrow$ It makes sense to write $\lim_{x\to 2} f(x) = ?$

Proof. Side Calculation:

$$\begin{aligned}\frac{x^2-4}{x-2} &= \frac{(x-2)(x+2)}{x-2} \\ &= x+2, \text{ for } x \neq 2\end{aligned}$$

But since $|x-2| > 0$ in the definition, we get

$$\lim_{x\to 2} f(x) = \lim_{x\to 2}(x+2) = 4.$$

□

Definition 6.1.5. Suppose that $p \in E$, we say that $f(x)$ is continuous at p if either $\lim_{x\to p} f(x) = f(p)$; or p is not an accumulation point of E. $E =$ domain of $f \Rightarrow f$ is continuous on E.

Example 6.1.6. $f(x) = x^n$ is continuous everywhere, for all $p \in \mathbb{R}$.

Example 6.1.7. $\sin(x), \cos(x), a^x(a > 0)$ are also continuous everywhere.

Example 6.1.8.

$$f(x) = \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \notin \mathbb{Q} \end{cases}$$

$E = \mathbb{R}$. But $f(x)$ is discontinuous everywhere. ($\forall p \in \mathbb{R}$, $f(x)$ is discontinuous at P).

Recall from last time: Let $E \subset \mathbb{R}$, and $p \in E'$ (set of all accumulation points of E). Given a function $f : E \to \mathbb{R}$, we say $f(x) \to L$ as $x \to p$, or $\lim_{x\to p} f(x) = L$, if: $\forall\ \varepsilon > 0, \exists\ \delta > 0$ such that $0 < |x-p| < \delta \Rightarrow |f(x) - L| < \varepsilon$, we say $f(x)$ is continuous at $x = p \in E$ if either

$$\begin{aligned}&\lim_{x\to p} f(x) = f(p), \text{ or} \\ &p \notin E'.\end{aligned}$$

Example 6.1.9. $x, x^2, \cdots$ are all continuous. $\sin(x)$, $\cos(x)$, $a^x(a > 0)$ are continuous everywhere (i.e. on $E = \mathbb{R}$).

Example 6.1.10.

$$f(x) = \begin{cases} x & x < 0. \\ x+1 & x \geq 0. \end{cases}$$

Claim 1: $f(x)$ is continuous at any $p \neq 0$.

Proof. Let $p \neq 0$ and $\varepsilon > 0$, we may assume without loss of generality that $\varepsilon \leq |p|$. (If $\varepsilon \geq |p|$, use the δ that works for $\varepsilon = |p|$.)
Case 1: $p > 0$, we choose $\delta = \varepsilon$. if $|x-p| < \delta = \varepsilon \leq |p|$, i.e. $|x-p| \leq |p|$.

$$\Rightarrow x \geq 0$$

$$\Rightarrow f(x) = x + 1$$

$$\Rightarrow |f(x) - f(p)| = |x + 1 - (p + 1)| = |x - p| < \delta = \varepsilon$$

$$\Rightarrow |f(x) - f(p)| < \varepsilon.$$

<u>Case 2</u>: $p < 0$, choose $\delta = \varepsilon$, if $|x - p| < \delta \leq |p|$, then $x < 0$.

$$\Rightarrow f(x) = x$$

$$\Rightarrow |f(x) - f(p)| = |x - p| < \delta = \varepsilon$$

$$\Rightarrow |f(x) - f(p)| < \varepsilon.$$

□

<u>Claim 2</u>: $f(x)$ is discontinuous at $x = 0$.

Proof. We choose $\varepsilon = 1$, we must show $\nexists\ \delta > 0$, s.t. $\cdots$, i.e. $\forall \delta > 0,\ 0 < |x - 0| < \delta \not\Rightarrow |f(x) - f(0)| < \varepsilon$. i.e. $\forall\ \delta > 0, \exists\ x$ with $0 < |x| < \delta$ such that $|f(x) - 1| \geq \varepsilon$. Given $\delta > 0$, let $x = -\frac{\delta}{2}$,

$$\Rightarrow 0 < |x| < \delta \text{ and } f(x) = f\left(-\frac{\delta}{2}\right) = -\frac{\delta}{2} \text{ because } -\frac{\delta}{2} < 0$$

$$\Rightarrow |f(x) - 1| = \left|-\frac{\delta}{2} - 1\right| = \left|1 + \frac{\delta}{2}\right| = 1 + \frac{\delta}{2} \geq \varepsilon.$$

□

<u>Question</u>: How discontinuous can a function be?

Proposition 6.1.11. *The function* $f(x) = \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \notin \mathbb{Q} \end{cases}$ *is discontinuous everywhere. (Domain of* $f : E = \mathbb{R}$*!)*

Proof. Let $p \in \mathbb{R}$, we'll show that for $\varepsilon = 1$, $\nexists\ \delta$ as required by definition.
<u>Case 1</u>: $p \in \mathbb{Q}$, then $f(p) = 1$. Given $\delta > 0$. denote $x \notin \mathbb{Q}$, such that $|x - p| < \delta$,

$$\Rightarrow |f(x) - f(p)| = |0 - 1| = 1 \geq \varepsilon.$$

But $\mathbb{R} \setminus \mathbb{Q}$ is dense in $\mathbb{R}$, so such an x must exist.
<u>Case 2</u>: $p \notin \mathbb{Q}$, then $f(p) = 0$. Given $\delta > 0$, $\exists\ x \in \mathbb{Q}$, such that $p - \delta < x < p$ by density of $\mathbb{Q}$. But then

$$f(x) = 1 \Rightarrow |f(x) - f(p)| = |1 - 0| = 1 \geq \varepsilon.$$

□

6.2 Continuity of functions using sequences (Apr 15)

You can test for whether a function is continuous using sequences, in the following way:

Theorem 6.2.1. *A function $f\colon E \to \mathbb{R}$ is continuous at a point if and only if: for any sequence $a_n \in E$ with $a_n \to p$ as $n \to \infty$, we have $f(a_n) \to f(p)$ as $n \to \infty$.*

Proof. First note that if $p \notin E'$, then there are no sequences $a_n \to p$ with $a_n \in E$. So the Theorem is vacuously true. So we can assume without loss of generality (i.e. "Wlog") that $p \in E'$.

($\Rightarrow$) Assume that $f(x)$ is continuous at $x = p$. Given $a_n \to p$ as $n \to \infty$, we need to show that $f(a_n) \to f(p)$. Let $\varepsilon > 0$, since $\lim_{x \to p} f(x) = f(p)$, there exists $\delta > 0$. such that

$$|x - p| < \delta \Rightarrow |f(x) - f(p)| < \varepsilon.$$

Since $a_n \to p$ as $n \to \infty$, $\exists\ N$ such that $|a_n - p| < \delta$ for all $n \geq N$. $\Rightarrow |f(a_n) - f(p)| < \varepsilon$ for all $n \geq N$. Since $\varepsilon > 0$ was arbitrary, we conclude that $f(a_n) \to f(p)$ as $n \to \infty$.

($\Leftarrow$) We'll show that if $f(x)$ is discontinuous at $x = p$, then there exists a sequence $a_n \to p$ with $f(a_n) \nrightarrow f(p)$. Since $f(x)$ is discontinuous at $x = p$, $\exists\ \varepsilon > 0$, such that $\forall\ \delta > 0. \exists\ x \in E$ with $0 < |x - p| < \delta$ but $|f(x) - f(p)| \geq \varepsilon$. Let $\delta = \frac{1}{n}$, choose $a_n = x$ for this δ, so: $0 < |a_n - p| < \frac{1}{n}$, but $|f(a_n) - f(p)| \geq \varepsilon > 0$. Then clearly $a_n \to p$, but $f(a_n) \nrightarrow f(p)$. □

Corollary 6.2.2. *Let $f(x)$ and $g(x)$ be continuous function at $x = p$. Then:*
(i) $f(x) + g(x)$ is continuous at $x = p$.
(ii) $f(x) \cdot g(x)$ is continuous at $x = p$.
(iii) $f(x)/g(x)$ is continuous at $x = p$, if $g(p) \neq 0$.

Proof. Just need to check an arbitrary sequence $a_n \to p$. Since f and g are continuous, $f(a_n) \to f(p)$, $g(a_n) \to g(p)$. By the limit rules for sequences, we have

$$f(a_n) + g(a_n) \to f(p) + g(p)$$

$$f(a_n) \cdot g(a_n) \to f(p) \cdot g(p)$$
$$\frac{f(a_n)}{g(a_n)} \to \frac{f(p)}{g(p)}, \text{ if } g(p) \neq 0.$$

Since $a_n \to p$ was arbitrary, by the previous Theorem, we are done. □

Corollary 6.2.3. *Let f, g, h be 3 functions with $f(x) \leq g(x) \leq h(x)$, $\forall x \in E$, if $\lim_{x \to p} f(x) = L = \lim_{x \to p} h(x)$, then $\lim_{x \to p} g(x) = L$.*

Proof. Let $a_n \to p$ with $a_n \in E$, $\Rightarrow f(a_n) \to L$ and $h(a_n) \to L$. By "squeeze Theorem" for sequences, $g(a_n) \to L$. □

Corollary 6.2.4. *Let $g : E \to \mathbb{R}$, $f : H \to \mathbb{R}$ with $g(E) \subset H$. ($f \circ g : E \to \mathbb{R}$ is a well-defined function). Suppose that $g(x)$ is continuous at $x = p$ and $f(u)$ is continuous at $u = g(p)$. Then $f \circ g$ is continuous at $x = p$.*

Proof. Let $a_n \to p$ with $a_n \in E$, since g is continuous at $x = p \Rightarrow g(a_n) = g(p)$; since f is continuous at $u = g(p) \Rightarrow f[g(a_n)] \to f[g(p)]$. □

Example 6.2.5. Show that $\sqrt{\sin x}$ is continuous on $E = [0, \pi]$.

Proof.

$$\text{Let } g(x) = \sin x \quad f(u) = \sqrt{u}$$

$$(f \circ g)(x) = \sqrt{\sin x}$$

$$\sin(x) \text{ is continuous on } [0, \pi]$$

$$\sin([0, \pi]) = [0, 1]$$

Domain of $f(u) = [0, \infty)$ and $f(u)$ is continuous on $[0, \infty)$. Since $[0, 1] \subset [0, \infty)$, the previous theorem applies.

$$\Rightarrow \sqrt{\sin x} \text{ is continuous on } E = [0, \pi).$$

□

Note: Yon can also use the above theorem to prove discontinuity! You just need to find $a_n \to p$, such that

$$f(a_n) \nrightarrow f(p),$$

prove that $f(x)$ is discontinuous.

Proof. Case 1: $p \in \mathbb{Q}$. Can I find $a_n \to p$, such that $f(a_n) \nrightarrow p$?
Let $a_n = p + \frac{\pi}{n}$. Since $\pi \notin \mathbb{Q}$, $\frac{\pi}{n} \notin \mathbb{Q}$

$$\Rightarrow p + \frac{\pi}{n} \notin \mathbb{Q} \text{ (since } p \in \mathbb{Q})$$

$$\Rightarrow a_n \in \mathbb{R} \setminus \mathbb{Q}$$

$$\Rightarrow f(a_n) = 0.$$

But $a_n = p + \frac{\pi}{n} \to p$ because $\frac{\pi}{n} \to 0$ as $n \to \infty$. So $f(a_n) = 0 \nrightarrow f(p) = 1$, $\Rightarrow$ f is discontinuous at p.
Case 2: $p \notin \mathbb{Q}$. One can make a similar argument. □

6.3 Extreme values (Apr 20)

Next topic: max's and min's of function.

Definition 6.3.1. Let $f : E \to \mathbb{R}$.
(a) $f(x)$ is **bounded above** if $f(x) < M$ for some $M \in \mathbb{R}$, and for all $x \in E$. (Bounded below is similar).
If $f(x)$ is bounded above, we write

$$\sup_{x \in E} f(x) = \sup f(E),$$

where $f(E) = \{f(x) \mid x \in E\}$. This is a real number! (Similarly, if f is bounded below, $\inf_{x\in E} f(x) = \inf f(E)$.)
(b) Suppose that $f(x)$ is bounded above. We say that $f(x)$ **attains its supremum** if $\exists\ p \in E$, $s.t. f(p) = \sup_{x\in E} f(x)$.
(Similarly, "attains its infimum".)

Example 6.3.2.

$$f(x) = 1 - x^2, E = [-1, 1]$$

Then $\sup_{x\in E} f(x) = 1$. (Why? $f(x) = 1 - x^2 \leq 1, \forall\ x \in E$ and $f(0) = 1$)
$\inf_{x\in E} f(x) = 0$. (Why? If $-1 \leq x \leq 1$, then

$$1 - x^2 = (1 - x)(1 + x) \geq 0$$

$$\Rightarrow \inf_{x\in E} f(x) \geq 0$$

But $f(-1) = f(1) = 0 \Rightarrow \inf_{x\in E} f(x) = 0$ and is attained at $x = -1$ (and $x = +1$).)
Note: If $E = \mathbb{R}$, then $f(x)$ would not be bounded below!

$$\Rightarrow \inf_{x\in E} f(x) = -\infty$$

$\Rightarrow$ inf can never be attained!

Example 6.3.3.

$$f(x) = \frac{1}{x^2}$$

$$E = (-\infty, 0) \cup (0, +\infty) = \mathbb{R} \setminus \{0\}.$$

$\sup_{x\in E} f(x) = +\infty$, $f(x)$ is not bounded above! $\inf_{x\in E} f(x) = 0$.
(Why?

$$\frac{1}{x^2} > 0, \forall x \in E$$

$$\Rightarrow \inf_{x\in E} f(x) \geq 0$$

In fact, $\inf_{x \in E} f(x) = 0$, because $\lim_{x \to +/-\infty} = 0!$)
Given any $N > 0, \exists x$ s.t. $\frac{1}{x^2} < N$
(E.g. $x = \frac{2}{\sqrt{N}} \Rightarrow \frac{1}{x^2} = \frac{N}{4} < N$).
Is the infimum <u>attained</u> on E?
<u>No!</u> $\inf f(x) = 0, x \in E$, but $f(x) = \frac{1}{x^2} > 0, \forall x \in E$

$$\Rightarrow \nexists\, p \in E \text{ s.t. } f(p) = \inf_{x \in E} f(x).$$

Example 6.3.4.

$$f(x) = \arctan(x), E = \mathbb{R}.$$

Domain of $\arctan(x) = \mathbb{R}$! But values of $\arctan(x)$ are always between $-\frac{\pi}{2}$ and $\frac{\pi}{2}$.

$$\sup_{x \in \mathbb{R}} \arctan(x) = \frac{\pi}{2}$$

$$\inf_{x \in \mathbb{R}} \arctan(x) = -\frac{\pi}{2}$$

$$\Rightarrow \arctan(x) \text{ is bounded } \underline{\text{above}} \text{ and } \underline{\text{below}} \text{ !}$$

<u>But</u> neither the sup nor the inf are attained!

Example 6.3.5.

$$f(x) = \arctan(x), E = [-1, 1] \text{ (different domain from previous example!)}$$

$$\Rightarrow \sup_{x \in E} f(x) = f(1) = \frac{\pi}{4}$$

$$\Rightarrow \inf_{x \in E} f(x) = f(-1) = -\frac{\pi}{4}$$

<u>Moral</u>: Attainment of sup and inf depend both on continuity of $f(x)$ and on the domain E.

Theorem 6.3.6. *(Extreme Value Theorem). Let $f(x)$ be a continuous function on a <u>closed</u> interval $E = [a, b]$. Then $f(x)$ is bounded both above and below, <u>and attains</u> both its* sup *and its* inf *on E.*
<u>Note</u>: In common language, $\sup_{x \in [a,b]} f(x)$ = "absolute max" and $\inf_{x \in [a,b]} f(x)$ = "absolute min".

Proof. Let

$$\overline{L} = \sup_{x \in [a,b]} f(x) = \sup\{f(x) \mid a \le x \le b\}.$$

We choose a sequence $a_n \in [a, b]$ s.t. $f(a_n) \to \overline{L}$, as follows:
If $\overline{L} < \infty$, then for each n, let a_n be s.t.

$$\overline{L} - \frac{1}{n} < f(a_n) \le \overline{L}.$$

If $\overline{L} = \infty$, then for each n, choose a_n s.t.

$$f(a_n) > n.$$

In either case, we have:

$$a \le a_n \le b, \text{ and}$$

$$f(a_n) \to \overline{L}$$

(We don't know if a_n is convergent or not!)
By the Bolzano–Weierstrass Theorem, since a_n is a bounded sequence of real numbers, it has a convergent sub-sequence, a_{n_i} s.t.

$$a_{n_i} \to p \text{ as } i \to \infty, \text{ for some } a \le p \le b.$$

This still satisfies

$$f(a_{n_i}) \to \overline{L} \text{ as } i \to \infty!$$

But since $p \in [a,b]$ and $f(x)$ is continuous at p,
By Definition 2 of continuity, we have

$$\lim_{i\to\infty} f(a_{n_i}) = f(p).$$

Since the limit of any sequence is unique, and

$$\lim_{n\to\infty} f(a_n) = \overline{L} = \lim_{i\to\infty} (a_{n_i})$$

$$\Rightarrow \overline{L} = f(\delta).$$

Therefore, $f(x)$ is bounded above ($\overline{L} < \infty$), and attains its supremum at $x = p$.
The argument for inf is similar. $\square$

More Examples:

Example 6.3.7.

$$f(x) = \sqrt{\sin^4(x) + \cos^{18}(x) + 16x^4} \text{ on } E = [-1000, 1000].$$

(a) Is $f(x)$ bounded on E?
(b) If so, does $f(x)$ attain its sup/inf?
Answer: Let's do (a) and (b) together.
By the Theorem, we just have to check:

- Is E a closed interval? (Yes! Since $E = [-1000, 1000]$)

- Is $f(x)$ continuous on E?

$$\sqrt{g(x)} \text{ is on } [0,\infty)$$

$$g(x) = \sin^4(x) + \cos^{18}(x) + 16x^4 \geq 0 \text{ (since } \sin^4(x) \geq 0,\ \cos^{18}(x) \geq 0, \text{ and } 16x^4 \geq 0).$$

$$\Rightarrow g(x) \text{ is on } \mathbb{R}, \text{ and } g([-1000,1000]) \subset [0,\infty)$$

By Corollary 6.2.4, we conclude that

$$f(x) = \sqrt{g(x)} \text{ is continuous on } E!$$

By the Extreme Value Theorem, it must be bounded <u>and</u> attain its sup / inf somewhere on E!

Example 6.3.8.

$$f(x) = \begin{cases} x & x \in \mathbb{Q} \\ 0 & x \notin \mathbb{Q} \end{cases}$$

<u>Claim 1</u>: $p = 0$, use squeeze theorem!

$$-|x| \leq f|x| \leq |x|$$

<u>Claim 2</u>: $p \neq 0$, looks like

$$f(x) = \begin{cases} 1 \text{ on } \mathbb{Q} \\ 0 \text{ on } \mathbb{Q}^c \end{cases}$$

Example 6.3.9. Consider $f(x) = \begin{cases} x & x \in \mathbb{R} \\ 0 & x \notin \mathbb{R} \end{cases}$, and $E = [-\pi, \pi]$.
(a) Is $f(x)$ bounded?
(b) Does it attain inf / sup?
Can we apply the *Theorem*? $\Rightarrow$ <u>No!</u> $f(x)$ needs to be for <u>all</u> $p \in [-\pi,\pi](E)$! It is only at $p = 0$!
<u>Answer</u>:
<u>(a)</u> $-\pi \leq f(x) \leq \pi$ is <u>bounded</u>!
<u>(b)</u>

$$\sup_{x \in [-\pi,\pi]} f(x) = \pi$$

$$\inf_{x \in [-\pi,\pi]} f(x) = -\pi$$

<u>But</u> there are <u>not</u> attained!
Because π is <u>irrational</u>, so $f(\pi) = 0$, $f(-\pi) = 0$.

6.4 A word or two about calculus (Apr 22)

Recall the main theorem of last class:

Theorem 6.4.1 (Extreme Value Theorem)**.** *Let $f(x)$ be a continuous function on a closed interval $E = [a,b]$ (i.e. "$\forall p \in [a,b]$, $f(x)$ is continuous at $x = p$"). Then $f(x)$ is bounded and attains its supremum and infimum.*

In other words,

$$\exists p \in [a,b] \ s.t.\ f(p) = \sup_{x\in[a,b]} f(x),$$

$$\text{and } \exists q \in [a,b] \ s.t.\ f(q) = \inf_{x\in[a,b]} f(x).$$

How to find these points p and q explicitly?

Definition 6.4.2. Let $f : E \to \mathbb{R}$ and $p \in E'$. We say that $f(x)$ differentiable of $x = p$ if the limit

$$\lim_{x\to p} \frac{f(x) - f(p)}{x - p}$$

exists. In this case, the limit is denoted by $f'(p)$, and is called the derivative of $f(x)$ at $x = p$.

Example 6.4.3.

$$f(x) = x^2$$

Answer:

$$f'(p) = \lim_{x\to p} \frac{x^2 - p^2}{x - p}$$

$$= \lim_{x\to p} \frac{(x-p)(x+p)}{(x-p)}$$

$$= \lim_{x\to p}(x+p) = p + p = 2p.$$

Thus, $f'(x) = 2x$.

Theorem 6.4.4. *If $f(x)$ is differentiable at p, then $f(x)$ is continuous at p.*

Proof. Note that $f(x)$ is continuous at p iff

$$\lim_{x\to p}[f(x) - f(p)] = 0.$$

But we know that

$$\lim_{x\to p} \frac{f(x) - f(p)}{x - p}$$

exists.

Applying limit rule, we get

$$\lim_{x\to p} (f(x) - f(p)) \frac{x - p}{x - p}$$

$$= \lim_{x\to p} \frac{f(x) - f(p)}{x - p} \cdot \lim_{x\to p} x - p$$

$$= 0 \cdot f'(p) = 0. \text{ (Since } \lim_{x\to p} x - p = p - p = 0)$$

$\square$

Note: Continuity is a necessary, but not sufficient condition for differentiability.

$$\text{differentiability} \Rightarrow \text{continuity},$$

but

$$\text{differentiability} \nLeftarrow \text{continuity}.$$

In other words, there exist continuous functions that are *not* differentiable.

Example 6.4.5.

$$f(x) = |x|$$

Answer: This is continuous at $x = 0$.

$$f(x) = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases} .$$

Then,

$$\lim_{x \to 0} \frac{|x| - 0}{x}$$
$$= \lim_{x \to 0} \frac{|x|}{x}$$

For $x > 0$, let $a_n = \frac{1}{n}$, then

$$\lim_{n \to \infty} a_n = 1.$$

For $x < 0$, let $b_n = -\frac{1}{n}$, then

$$\lim_{n \to \infty} b_n = -1.$$

Therefore, the limit in the definition of $f'(0)$ does not exist! So the $f(x)$ is not differentiable at $x = 0$.

Question: How non-differentiable can a continuous function be?
More specifically, can $f'(x)$ fail to exist for infinitely many points $x \in [a, b]$?

Example 6.4.6.

$$x \cdot \sin \frac{1}{x} = f(x)$$

We have:

$$f'(x) = \sin \frac{1}{x} - \frac{x}{x^2} \cdot \cos \frac{1}{x}$$
$$= \sin \frac{1}{x} - \frac{\cos \frac{1}{x}}{x}$$

By imitating this example, it is possible to construct a function that fails to be differentiable on a whole sequence $a_n \to 0$!

$$f'(a_n) = dne.$$

$\Rightarrow$ Can get a countably infinite set of x where

$$f'(x) = dne.$$

In fact, one can construct a function $f(x)$ that is continuous everehere, but differentiable nowhere. (Preview of Math 521.)

Let's say that $f(x)$ *is* differentiable at all points on E. How can we use this fact in finding min's and max's?

Definition 6.4.7. We say that $f(x)$ has a local maximum at p if $\exists\delta > 0$ s.t. $\forall x \in (p-\delta, p+\delta), f(x) \leq f(p)$. Local minimum: $f(x) \geq f(p)$.
local max $\neq$ absolute max

Theorem 6.4.8 (Fermat's Theorem)**.** *Let $f : (a,b) \to \mathbb{R}$. If $f(x)$ has a local maximum/minimum at $p \in (a,b)$, and $f(x)$ is differentiable at $x = p$, then $f'(p) = 0$.*
Note: If the derivative at $x = p$ does not exist, then the Theorem does not apply.

Corollary 6.4.9 ("Closed interval method")**.** *If $f(x)$ is a continuous function on $[a,b]$, then the absolute maximum and minimum can be found among the set of points $a \leq x \leq b$ where:*

- $x = a$ *or* $x = b$
- $f(x) = 0$
- $f'(x) = DNE$.

Point: we reduce from checking an infinity of points $x \in [a,b]$ to (usually) a finite list!

Proof of Fermat's Theorem. Since $f'(p) = \lim_{x\to p} \frac{f(x)-f(p)}{x-p}$ exists, we can use any sequence $a_n \to p$ to compute it.
Recall that a local maximum satisfies $f(x) \leq f(p)$ $\forall p-\delta \leq x \leq p+\delta$ (for some δ).
Let $a_n = p - \frac{1}{n}$

$$\Rightarrow a_n \to p, p - \delta < a_n < p$$

$$\Rightarrow f(a_n) \leq f(x), f(a_n) - f(x) \leq 0.$$

But $a_n - x < 0$, so

$$\frac{1}{a_n - x} < 0$$

$$\Rightarrow \frac{f(a_n) - f(p)}{a_n - p} \geq 0$$

$$\Rightarrow \lim_{n\to\infty} \frac{f(a_n) - f(p)}{a_n - p} \geq 0 \text{ (we assume that this exists!)}$$

$$\Rightarrow f'(p) \geq 0.$$

Next, let $b_n = p + \frac{\delta}{n}$.

$$b_n - p = \frac{\delta}{n} > 0, f(b_n) - f(p) \leq 0$$

$$\Rightarrow \frac{f(b_n) - f(p)}{b_n - p} \leq 0$$

$$\Rightarrow \lim_{n\to\infty} \frac{f(b_n) - f(p)}{b_n - p} \leq 0$$

$$\Rightarrow f'(p) \leq 0$$

Since,

$$0 \leq f'(p) \leq 0,$$

Thus,

$$f'(p) = 0$$

□

Corollary 6.4.10 (Rolle's Theorem)**.** *If $f(x)$ is on $[a,b]$ and differentiable on (a,b), and $f(a) = f(b)$, then $\exists x \in (a,b)$ s.t. $f'(x) = 0$.*

Proof. Since $f(x)$ is on $[a,b]$, it has a maximum and minimum.
Case 1: The absolute maximum is attained at $x \in (a,b)$. By $Fermat$, $f'(x) = 0$.
Case 2: The absolute minimum is attained at $x \in (a,b)$.
Case 3: Both the maximum and minimum occur at the end points.
Then $f(a)$ and $f(b)$ are the maximum/minimum, on vice-versa.
But $f(a) = f(b)$!
So $f(a) \leq f(x) \leq f(b) = f(a)$ $\forall x \in [a,b]$.

$$\Rightarrow f(x) = constant$$

$$\Rightarrow f'(x) = 0, \forall x \in [a,b].$$

□

Corollary 6.4.11 (Mean Value Theorem)**.** *Let $f(x)$ be on $[a,b]$ and differentiable on (a,b). $\exists x \in (a,b)$ s.t.*

$$f'(x) = \frac{f(b) - f(a)}{b - a}.$$

Proof. Let

$$g(x) = f(x) - (x - a) \cdot \frac{f(b) - f(a)}{b - a}.$$

Then $g(x)$ is differentiable on (a,b). And,

$$g(a) = f(a) - (a - a)\frac{f(b) - f(a)}{b - a} = f(a) - 0 = f(a)$$

$$g(b) = f(b) - (b-a) \cdot \frac{f(b)-f(a)}{b-a} = f(b) - (f(b)-f(a)) = f(b) - f(b) + f(a) = f(a) = g(a)$$

$$\Rightarrow g(a) = g(b)!$$

By *Rolle's*, $\exists x \in (a,b)$ s.t. $g'(x) = 0$.
But

$$0 = g'(x) = f'(x) - \frac{f(b)-f(a)}{b-a}.$$

Thus,

$$f'(x) = \frac{f(b)-f(a)}{b-a}.$$

□

Corollary 6.4.12. *Let $f(x)$ be continuous on $[a,b]$ and differentiable on (a,b). If $f'(x) = 0$ for all $x \in [a,b]$, then $f(x)$ is constant on $[a,b]$.*

Proof. If $f(x) \neq f(a)$ for some $x \in [a,b]$, then $\exists y \in (a,x)$ s.t. $f'(y) = \frac{f(x)-f(a)}{x-a} \neq 0$.

$$\Rightarrow f'(y) \neq 0.$$

But this is the contrapositive. □

Note: This last result is used in an essential way during the proof of the Fundamental Theorem of Calculus.