MATH 215: NOTES

Contents

1. Jan 8: Syllabus day

- Go through syllabus
- Finish with mathematical warmup: what is an even number ($x = 2k$ with $k \in \mathbb{Z}$), what is an odd number ($y = 2k + 1$ with $k \in \mathbb{Z}$). Must every number be even or odd? (Yes, but to prove this will require later material). Idea is to get students thinking about precise, useful definitions and how to prove facts they are used to assuming.

Here $\in$ is read "in" and $\mathbb{Z}$ denotes the set of integers (i.e. the set $\{\dots, -3, -2, -, 1, 0, 1, 2, 3, \dots\}$ of positive whole numbers, zero, negative whole numbers). "$k \in \mathbb{Z}$" therefore means that k is an integer.

2. Jan 10: Statements

- Introduction to *statements* in the mathematical sense (declarative statement that can be assigned a truth value: it is either True or False, not both).
- Building statements from new statements. Negation, and, or. Truth tables below.

P	$\neg P$
T	F
F	T

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

- Use examples to motivate logical equivalences. Two things are logically equivalent if they always have the same truth value. This means they can be swapped for one another in statements, expressions, etc. DeMorgan's laws:

$$\neg(A \wedge B) \text{ logically equiv to } \neg A \vee \neg B$$
$$\neg(A \vee B) \text{ logically equiv to } \neg A \wedge \neg B$$

as well as distributive properties:

$$A \wedge (B \vee C) \text{ logically equiv to } (A \wedge B) \vee (A \wedge C)$$
$$A \vee (B \wedge C) \text{ logically equiv to } (A \vee B) \wedge (A \vee C)$$

3. Jan 17: Conditionals

Another example of building new statements from old ones. Given P, Q statements we can form $P \Rightarrow Q$. It has the following truth assignments, depending on those of P, Q.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

We discuss what it means to "prove" a statement of the form $P \Rightarrow Q$: this means, show it is always true. Looking at the table above, we only need to worry about landing in the case of $T \Rightarrow F$. So proving a conditional means assuming P is true, and trying to use logical arguments to deduce that Q is true. We see that, for x an integer,

$$x \text{ is a multiple of } 4 \Rightarrow x \text{ is a multiple of } 2$$

is true (information on the left always implies information on the right) , but

$$x^2 > 0 \Rightarrow x > 0$$

is not true (there are situations where $x^2 > 0$ and $x < 0$).

From the conditional $P \Rightarrow Q$, we can define the inverse $(\neg P \Rightarrow \neg Q)$ as well as the converse $(Q \Rightarrow P)$ and the contrapositive $(\neg Q \Rightarrow \neg P)$. We then go through writing their truth values:

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

From there we see the original $P \Rightarrow Q$ is logically equivalent to the contrapositive. We also see the inverse, converse are logically equivalent to eachother (note that the inverse is the contrapositive of the converse). We discuss how this will be useful: sometimes the contrapositive is way easier to prove than the original statement.

Lastly, if $P \Rightarrow Q$ and $Q \Rightarrow P$ are true, then we say $P \iff Q$ (read "P if and only if Q). This means P is true exactly when Q is true and vice versa: i.e. this means P, Q are logically equivalent. So from now on we write P, Q logically equivalent as $P \iff Q$. If trying to prove $P \iff Q$ on a HW/in class: there should be two parts: showing $P \Rightarrow Q, Q \Rightarrow P$.

Direct students to Taylor 1.4 for $\forall$ (for all/any) and $\exists$ (there exists) quantifiers.

4. Jan 19: Proof methods part 1 (direct proofs)

Three major proof methods when trying to show $P \Rightarrow Q$

- Direct proof: assume P true, use logical deductions, algebra, lemmas (small results) and theorems from class to try to show Q is true.
- Contradiction: assume P is true but Q is false. Show that this yields a logical contradiction (say, contradict a part of the assumption, or run into a logical fallacy like $0 = 1$). Then the original assumption must have been wrong, and Q is true.
  - Good to start these proofs with "Assume, for the sake of contradiction" or "Suppose P is true but Q were false." Something to indicate to the reader that you are doing a contradiction proof.
  - Colloquially, this also gets used for: if you're trying to show a statement A is true, you assume $\neg A$ is true instead and run into a contradiction.
- Contrapositive: show $\neg Q \Rightarrow \neg P$.

We focus on direct proof today.

Two exercises:

- **Show that x even, y odd $\Rightarrow x + y$ odd.**
- **Show that x odd $\iff x + 2$ odd.**

Proof of the first result: Since x even, y odd: by definition we have

$$x = 2k$$
$$y = 2\ell + 1$$

with k, ℓ integers. Then $x + y = 2k + 2\ell + 1 = 2(k + \ell) + 1$. $k + \ell$ is an integer since k, ℓ are integers. Thus, by definition, $x + y$ is odd. □

Similar definition unwinding yields the second result.

Things to note: using separate variables for writing $x = 2k$, $y = 2\ell + 1$. At each point we are clear about what results/definitions/information/etc we are using. Note that for the second result: make sure proof has two parts.

5. Jan 22: Contradiction, contrapos

This lesson we focus more on contradiction, contrapositive: i.e. the methods that involve some sort of negation.

Warmup: you may assume every integer is exactly one of even or odd. Show that x^2 even $\Rightarrow$ x even.

Proof. (Note that this is hard to do directly! Contrapositive helps flip this into turning info about x into info about x^2 in a pretty straightforward manner.) We use proof by contradiction: we will show x not even $\Rightarrow$ x^2 not even. Equivalently, this means showing x odd $\Rightarrow$ x^2 odd. If x is odd, then $x = 2k + 1$ for some k an integer. Then:

$$x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

$2k^2 + 2k$ is an integer because k is an integer. So by definition, x^2 is odd and we are done. □

Next, some definitions. A number x is **rational** provided that it can be written as $x = \frac{p}{q}$ where p, q are integers and $q \neq 0$. A number is **irrational** if it is not rational.

Show: if x is rational, y irrational, then $x + y$ is irrational.

One thing that jumps out: hard to do this directly. Contrapositive seems difficult because negative the left side seems tedious. So let's try contradiction. That will turn $x + y$ irrational into $x + y$ rational, which will be nice to work with.

Proof. Suppose, for the sake of contradiction, that x is rational, y irrational, $x + y$ irrational. Then $x = \frac{p}{q}$ and $x + y = \frac{a}{b}$ with p, q, a, b integers and q, b nonzero. Then:

$$y = (x + y) - x = \tfrac{a}{b} - \tfrac{p}{q} = \frac{aq - pb}{bq}.$$

The numerator and denominator are integers since a, b, p, q are. bq is nonzero because b, q are nonzero. But that means y is rational, which contradicts y being irrational. Hence our assumption is false, and $x + y$ must be irrational. □

We end by trying to prove the following: **Show $\sqrt{2}$ irrational.** Start by supposing, for the sake of contradiction, that $\sqrt{2}$ is rational. Then:

$$\sqrt{2} = \frac{p}{q}.$$

Square both sides, get $2 = p^2/q^2$, equivalently $2q^2 = p^2$. Try messing with even-ness, odd-ness to see if can get a contradiction.

(Another fun result one can do with contradiction: $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k}$ is never an integer).

6. Jan 24: Finish contradiction. Casework

We finish the proof of $\sqrt{2}$ irrational. Intuitively: look at $2q^2 = p^2$. Look at the prime factorization of each. The number of 2's on the left is odd, the number of 2's in the right is even (because the primes in the factorization of a square all have even power).

Proof that $\sqrt{2}$ irrational. Suppose, for the sake of contradiction, that $\sqrt{2}$ is irrational. Then

$$\sqrt{2} = \frac{p}{q}$$

We shall assume that p, q are in lowest terms. Squaring both sides and rearranging, we get

$$2q^2 = p^2$$

Looking at this equation, p^2 is even. By a result from last class, this means p is even. Write $p = 2k$, k an integer. Then:

$$2q^2 = (2k)^2 = 4k^2.$$

Cancelling a factor of 2, we see

$$q^2 = 2k^2,$$

hence q is even. But if p, q are both even: the fraction couldn't have been in lowest terms! We could cancel a factor of 2 from top and bottom! So we've arrived at a contradiction. Our assumption must be false, and so $\sqrt{2}$ is irrational. □

The heart of what's going on is factorization issues. We'll see more about factorization in the number theory section of the course.

A nice bookend to the proof methods chunk is to cover proof by cases. We show that $n^2 - n$ is always even by looking at even, odd cases. This and proof of $\sqrt{2}$ help motivate induction. Time permitting, show multiple proofs of $n^2 - n$.

7. Jan 26: Induction

Results like:

- all fractions can be put in least terms
- all integers are even or odd

rely on induction (or one of its equivalent formulations: strong induction, well ordering principle). It is an axiom, and a very useful and major method. Likened to "mathematical dominos."

Idea of induction: if a property holds for $k = 1$, and a property holding for k implies it holds for $k + 1$, then we can start at 1 and "domino effect" down to get a property holds for all natural numbers ($\{1, 2, 3, 4, \dots\}$). Good for proving a fact holds for all natural numbers.

Proofs by induction always have two parts: base case (the $k = 1$ part) and inductive step (showing the property holds for k implies the property holds for $k + 1$).

Examples of proofs by induction:

- Show that every integer is even or odd. (casework + induction)
- Show that
$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$
for all natural numbers n Note: provides a fun proof that $n^2 - n$ is even as a corollary.
- Show that $k^3 + 2k$ is always divisible by 3.
- Show that
$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$
for all natural numbers n
- Show that
$$\sum_{k=1}^{n} k(k+1) = (1 \times 2) + (2 \times 3) + (3 \times 4) + \cdots + (n \times (n+1)) = \frac{n(n+1)(n+2)}{3}$$
for all natural numbers n.

Proof of the second statement. We use proof by induction. Base case: note that $1 = \frac{1(2)}{2}$ so the formula holds for $k = 1$.

Inductive step: suppose the formula is true for k. Then:

$$\begin{aligned} 1 + 2 + \cdots + k + k + 1 = \frac{k(k+1)}{2} + (k+1) &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+2)(k+1)}{2} \\ &= \frac{(k+1)((k+1)+1)}{2}, \end{aligned}$$

which means the formula is true for $k+1$. So, by induction, the formula is true for all natural numbers n. □

8. Jan 29: Induction part 2

Start with note about for all, there exists. $P(x)$ being some property of x, etc. Recall $\mathbb{N} = \{1, 2, 3, 4, \dots\}$.

Go over

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

more slowly.

Induction

- Useful for proving things about the natural numbers (and this sometimes lets you yield statements about $\mathbb{Z}, \mathbb{Q}$)
- Useful in situations with *recursive structure* or properties that can "build up"

Let's get some motivation for why this might be true:

- $n = 1$: Well, $1 = 1(1+1)/2$.
- $n = 2$ Well, $1 + 2 = 3 = 2(2+1)/2$.
- $n = 3$ Well, $1 + 2 + 3 = 6 = 3(3+1)/2$.

Grouping trick: first and last add to $n+1$. Second and penultimate add to $n+1$. And so on, and there will be $n/2$ such pairs (if n even get $n/2$ pairs and if n odd get $(n-1)/2$ pairs and a loner with the value of $(n+1)/2$).

Then: circle back to induction and formal proof Say you want a property P to hold for all natural numbers, so write $P(k)$ to denote the property for the natural number k. (ex: $P(k)$ is the property that $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$).

Induction says that if you have the following:

- $P(1)$ is true
- $P(k)$ is true implies $P(k+1)$ is true

then $P(k)$ is true for all natural numbers k. That is, your desired property is true for every natural number. (With our example choice of P, this would mean the formula for $1 + \cdots + n$ always holds.

Proof. We use proof by induction. Base case: note that $1 = \frac{1(2)}{2}$ so the formula holds for $k = 1$.

Inductive step: suppose the formula is true for k. Then:

$$\begin{aligned} 1 + 2 + \cdots + k + k + 1 = \frac{k(k+1)}{2} + (k+1) &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+2)(k+1)}{2} \\ &= \frac{(k+1)((k+1)+1)}{2}, \end{aligned}$$

which means the formula is true for $k+1$. So, by induction, the formula is true for all natural numbers n. □

9. Jan 31: Induction, some more examples, strong induction (if time)

Use induction to show all integers are even or odd. The main thing is that we need to start by doing this for all *natural numbers* n, and then handle 0 and negatives separately. The last part is either done by some slightly tedious algebra or just checking that (-1) is odd and citing that odd $\times$ odd, even is odd, even respectively.

This is a special case of the *division algorithm*, which we will see in the next unit (number theory). This is saying we can divide a number by 2 with remainder, and the remainder has the usual size constraints $0 \leq r < b - 1$ with $b = 2$ here.

10. Feb 2: Strong induction

Suppose we want some property P to hold for all natural numbers n. Let $P(n)$ to denote the property for the natural number n. Strong induction says: if you have the following

- $P(1)$ is true
- ($P(k)$ true for $1 \leq k < n \Rightarrow P(n)$ true) is true

then $P(n)$ is true for all natural numbers n.

One of the first applications of this is showing every fraction can be put in least terms. Another classical application is showing the fundamental theorem of arithmetic (every integer decomposes as a unique product of primes. We'll see this later).

For our first application, we'll do that every natural number is 1 or splits as a product of primes. (Main part: in inductive step, you'll have n. If it is prime, done. If it splits, write $n = ab$ with $1 \leq a, b < n$. Then can apply the inductive hypothesis to get a, b are products of primes (and so n is a product of primes).

End on an example of finding an error in a proof:

False theorem: if the sum of two integers is even, then both integers are even ($m+n$ even $\Rightarrow m, n$ even).

Proof. Assume, for the sake of contradiction, that the result is false, i.e. either m or n is odd. Then $m = 2k + 1$ and $n = 2j$ with $j, k \in \mathbb{Z}$ (swap the label of m and n as needed). Then:

$$m + n = 2(k + \ell) + 1$$

is odd. Contradicts our assumption that $m+n$ is even. So our assumption is false and the theorem is true. □

Where is the error? (Where: in the contradiction setup, assumed *either* m or n is odd. Why: it's assumed precisely one odd one even, when the failure could come from both odd. In failing to account for this, they miss the phenomena that m odd and n odd will yield $m + n$ even, which is where this theorem fails).

Can also write a proof of $\sqrt{m}\sqrt{n}$ an integer, then $\sqrt{m}/\sqrt{n}$ is rational.

Can also do a strong induction example or take HW 1/ HW 2 questions. Strong induction example: We will define a sequence of numbers. Let $a_1 = 1, a_2 = 2$, and then for $n \geq 3$ we set

$$a_n := a_{n-1} + a_{n-2}.$$

Use strong induction to show that $a_n < 2^n$ for all $n \in \mathbb{N}$. (Need two base cases!)

11. Feb 5 (Putting fractions into least terms)

We'll show that every fraction can be put into least terms. Let $P(n)$ be the property that

For every $m \in \mathbb{Z}$, m/n can be put in least terms.

(This is saying that any fraction that can be written with a denominator of n can be written in least terms) We first show that $P(1)$ holds. Certainly $m/1 = 1$ is in least terms; the only factors 1 has is $1, -1$, so we can't do any cancellation from the top and bottom.

Next we show $P(k)$ true for $1 \leq k < n$ implies that $P(n)$ is true (n is an arbitrary natural number). Boils down to: if you can put fractions with denominator $< n$ in least terms, can you put fractions with denominator $= n$ in least terms?

Assume that indeed, $P(k)$ is true for $1 \leq k < n$. Note that our goal is to show every m/n can be put in least terms. Well, either m/n is in least terms (and we are fine), or it is not. In that case,

$$\frac{m}{n} = \frac{m'}{n'}$$

with $1 \leq n' < n$. Note that the fraction on the right has a smaller denominator, so $P(n')$ is true. In particular, m'/n' can be put in least terms. So $m/n = m'/n'$ can be put in least terms. No matter what, we can always put m/n in least terms. So $P(n)$ holds. By strong induction, $P(n)$ holds for all n, and so all fractions can be put in least terms.

(Rephrase to students: we're saying: need to show: if we can put m/k in least terms for every $k < n$, then m/n can always be put in least terms).

12. Feb 7 (Division algorithm cont.)

Hamkins 3 material.

Talk about division with remainder: put as many copies of b into a, get a leftover bit. The remainder should be $o \leq r < b$, otherwise I could shrink it.

For $a \in \mathbb{Z}, b \in \mathbb{N}$ with b nonzero, can find *unique* q, r such that $a = bq + r$ with $0 \leq r < b$. This is the division algorithm. It is division with remainder. q is the quotient, and r is the remainder.

So, with $a = 12, b = 5$ performing the division algorithm is $12 = 5 \cdot 2 + 2$, i.e. we put as many copies of 5 as we can into 12, and then we have a remainder that is non-neg and strictly less than the thing we're dividing with.

With $a = 27, b = 8$, performing the division algorithm yields $27 = 8 \cdot 3 + 3$. When $a = 16, b = 8$ we get $16 = 8 \cdot 2 + 0$.

In fact, can let a just be an integer, no necessarily positive. Still get that $a = bq + r$ with $0 \leq r < b$.

Restrict to $b = 2$ case: Note that diving by 2 always gets a remainder of 0 or 1. i.e. division algorithm being true $\Rightarrow$ every natural number even or odd.

So splitting into even and odd cases in proofs was like splitting into cases based on remainder when dividing by 2. Leads us to another example of useful cases: we can split into cases based on remainder when dividing by, say, 3 or 5.

Example: Can split into cases by remainder ($3k$, $3k + 1$, $3k + 2$) to show that $n(n + 1)(n + 2)$ is always divisible by 3. (You could do this with induction too, but it's a little painful and less intuitive).

Start proof of division algorithm.

13. Feb 9 (Division algorithm cont.)

Prove the division algorithm. Handle $b = 1$ case separately. Fix b. We'll show that division works for $a \in \mathbb{N}$, but holds for $a \in \mathbb{Z}$ in general. For fixed b, we then induct on a:

$$P(n): \text{ there exists } q, r \in \mathbb{Z} \text{ such that } n = bq + r \text{ with } 0 \leq r < b.$$

(i.e. $P(n)$ is the property that n can be divided by b with remainder). Do scratch work on side with $b = 4$ to see:

$$5 = 4 \cdot 1 + 1$$
$$6 = 4 \cdot 1 + 2$$
$$7 = 4 \cdot 1 + 3$$
$$8 = 4 \cdot 2 + 0$$
$$9 = 4 \cdot 2 + 1$$
$$10 = 4 \cdot 2 + 2$$

In general, seems like we increment remainder by 1 unless $r = b - 1$, in which case we have to be careful. Suggests that we need to split proof into cases. Back to the proof:

Base case: $1 = b \cdot 0 + 1$. $0 \leq 1 < b$ since we can assume $b \geq 2$ (as we handled $b = 1$ separately).

Inductive step: We need to show $P(n) \Rightarrow P(n+1)$. We know we can write $n = bq + r$, $0 \leq r < b$.

Case 1: $r < b - 1$. Then $n + 1 = bq + (r + 1)$ and $0 \leq r + 1 < b$.

Case 2: $r = b - 1$. Then $n + 1 = b(q + 1)$, and $r = 0$.

End on proving $n(n+1)(n+2)$ is always a multiple of 3 for any $n \in \mathbb{Z}$. This comes from casework: div algorithm says you can split into $n = 3k$ or $n = 3k + 1$ or $n = 3k + 2$. Have students observe: in this case, better to not try to expand the product.

14. Feb 12 (Least number principle/Well ordering principle)

Natural numbers: has smallest element + discreteness means **any nonempty subset of $\mathbb{N}$ has smallest element**. This is LNP.

So: If you look at the collection of natural numbers with a certain property P (and that collection isn't empty) then there is a smallest natural number with that property P.

Strong induction, induction, LNP all equivalent. Some slightly nicer in certain proofs, LNP sometimes "picks out" a number we want with a certain property (good for minimizing/inequality conditions). But in the end the three tools are equivalent. We now reprove some old results with the LNP.

- **Example 1:** Show that for all $n \in \mathbb{N}$ we have $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

  Look at collection of natural numbers such that the formula doesn't hold. We want to show this collection is empty. Suppose, for sake of contradiction, that collection isn't empty. Then it has a least element k. Note: $1 = \frac{1(1+1)}{2}$, so 1 not in the set. So $k \geq 2$. Then $k - 1$ a natural number and not in the set so:

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

  Adding k to both sides:

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

  Contradiction, so assumption was false and collection was empty. So formula holds for all $n \in \mathbb{N}$.

  (Note how you get something like a base case and an inductive step here).
- **Example 2:** Show that all fractions can be put in least terms.

  Take an arbitrary fraction $\frac{a}{b}$. We'll show it can be put in least terms. We may assume $b \in \mathbb{N}$. Look at all the different expressions $\frac{a'}{b'}$ that are equal to $\frac{a}{b}$ and look at the collection of (natural number) denominators b' that appear. Take the smallest one using LNP, call

it b''. There is some associated a'' such that $\frac{a''}{b''} = \frac{a}{b}$, by definition of how we formed this collection.

Can show that $\frac{a''}{b''}$ is in least terms.

- **Example 3:** We'll show the division algorithm works. Fix $b \in \mathbb{N}$ and $a \in \mathbb{Z}$. Look at the collection of non-negative numbers r' that can be written as $r' = a - bq$ for some q. This collection is nonempty (take q to be negative with large absolute value to get *an* example of a $a - bq$ non-negative). Use LNP to take the smallest element, call it r. Can show that $0 \leq r < b$.

  (Remind students: using a slight variant of LNP so that we can work with $\mathbb{N} \cup \{0\}$, but it still works).

15. Feb 14 (Set theory 1)

Today is the first day of set theory. All about collections of objects, and some basic operations you can do on them. Very useful in a "building foundations" sense, since lots of things in math/STEM are phrased in terms of sets. Implicitly you've likely worked with some notion of them in the past, today we talk about them more in detail.

Rigorous definition is... difficult to do! We will not worry too much about it– a colloquial idea is enough, and we understand the operations well enough.

A set is a(n unordered) collection of objects. We usually denoted sets with capital letters. An object a in a set S is called an **element** of that set, and is denoted $a \in S$. We've seen this with, e.g., $2 \in \mathbb{Z}$ and $\frac{3}{4} \in \mathbb{Q}$.

There are two ways we usually denote them. First: There is the **roster method**: just list elements.

$$S = \{\text{red}, \text{green}, \text{blue}\},$$
$$P = \{1, 2, 7, 9\}$$

(The first being a set with three elements: red, green blue. The second being a set with four distinct elements: the numbers 1,2,7,9).

Before we do the second: note that we have some "stock" sets already: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. This will help us with the second method: **set builder** notation, where you characterize the elements of your set as having some shared property. For example:

$$\{x \in \mathbb{N} : 4 \leq x \leq 7\}$$

Read "x in $\mathbb{N}$ such that $4 \leq x \leq 7$". In set builder notation, this set is $\{4, 5, 6, 7\}$, because those are all the x in $\mathbb{N}$ that satisfy the condition after the colon: $4 \leq x \leq 7$.

Another example: $\{x \in \mathbb{R} : |x| < 1\}$ is the interval $(-1, 1)$. (Draw this).

Examples for the class: Draw the following sets on the number line.

- $\{x \in \mathbb{Z} : |x| \leq 2\}$
- $\{x \in \mathbb{R} : x^2 = -1\}$
- $\{x \in \mathbb{R} : x^2 = 4\}$
- $\{x \in \mathbb{R} : x = \frac{n}{2}, n \in \mathbb{Z}\}$

The middle one leads us to: $\varnothing$: the empty set. The set that contains no elements. We use $a \mid b$, read "a divides b," to denote that b is a multiple of a, i.e. $a = bk$ for some $k \in \mathbb{Z}$. Describe the following sets in words.

- $\{x \in \mathbb{Z} : x = 2k,\ k \in \mathbb{Z}\}$
- $\{x \in \mathbb{Z} : a \mid x \Rightarrow a \in \{1, -1, x, -x\}\}$
- $\{x \in \mathbb{R} : x \notin \mathbb{Q}\}$

Some more notation: for two sets A, B, **we say that $A \subseteq B$ if every element of A is an element of B.** (That is: $a \in A \Rightarrow a \in B$ is always true). (So, set theory analogue of implication). Draw venn diagram, possibilities, this is same as containment. Examples:

$$\{1,3\} \subseteq \{1,2,3,4\}, \quad \mathbb{Q} \subseteq \mathbb{R}.$$

If you are trying to show $A \subseteq B$ in a proof: it basically follows the same format always: you fix an arbitrary element a of A. Show that it is in B. Since your choice of a was arbitrary, it works for any element of A. So any element of A is an element of B, and $A \subseteq B$

Let's do a practice problem. We'll show: $\mathbb{Z} \subseteq \mathbb{Q}$. Let n be an element of $\mathbb{Z}$. Then $n = \frac{n}{1}$, and we satisfy the usual conditions for a rational number: $n, 1 \in \mathbb{Z}$ and $1 \neq 0$. So $n \in \mathbb{Q}$. So $n \in \mathbb{Z} \Rightarrow n \in \mathbb{Q}$. Therefore, $\mathbb{Z} \subseteq \mathbb{Q}$. (In practice you don't need to prove "obvious" containments between stock sets, but it's good practice).

(Note: this means that LNP is saying: if $S \subseteq \mathbb{N}$ and $S \neq \varnothing$, then S has a smallest element).

Two sets are equal if $A \subseteq B$ and $B \subseteq A$ (set theory analog of a biconditional). Therefore, showing an equality of two sets has two parts: showing $A \subseteq B$ (so $a \in A \Rightarrow a \in B$) and showing $B \subseteq A$ (so $b \in B \Rightarrow b \in A$). For example:

$$\{x \in \mathbb{Z} : x \text{ is even}\} = \{x \in \mathbb{Z} : x/2 \in \mathbb{Z}\}$$

(Run through proof). In practice, you can just say x is even $\iff x/2 \in \mathbb{Z}$, so the two sets above are equal. But we needed a nice simple problem to practice the idea on.

16. Feb 16 (Set theory 2)

Set operations! Union (or) and intersection (and). Set complement. Demorgan's law. Do concrete examples with finite amounts of numbers. Remind them at start: sets are just unordered collections of objects. So the elements don't have to be numbers. $\{[0,1],[2,3]\}$ is a valid two element set. $\{\varnothing\}$ is a valid one element set. Refresh on terminology from other day.

Run through containment proofs: We'll show: $\mathbb{Z} \subseteq \mathbb{Q}$. Let n be an element of $\mathbb{Z}$. Then $n = \frac{n}{1}$, and we satisfy the usual conditions for a rational number: $n, 1 \in \mathbb{Z}$ and $1 \neq 0$. So $n \in \mathbb{Q}$. So $n \in \mathbb{Z} \Rightarrow n \in \mathbb{Q}$. Therefore, $\mathbb{Z} \subseteq \mathbb{Q}$. (In practice you don't need to prove "obvious" containments between stock sets, but it's good practice).

(Note: this means that LNP is saying: if $S \subseteq \mathbb{N}$ and $S \neq \varnothing$, then S has a smallest element).

Two sets are equal if $A \subseteq B$ and $B \subseteq A$ (set theory analog of a biconditional). Therefore, showing an equality of two sets has two parts: showing $A \subseteq B$ (so $a \in A \Rightarrow a \in B$) and showing $B \subseteq A$ (so $b \in B \Rightarrow b \in A$). For example:

$$\{x \in \mathbb{Z} : x \text{ is even}\} = \{x \in \mathbb{Z} : x/2 \in \mathbb{Z}\}$$

(Run through proof). In practice, you can just say x is even $\iff x/2 \in \mathbb{Z}$, so the two sets above are

Use venn diagram analogy: define $A \cup B$. Analogue of "or" in that:

$$x \in A \cup B \iff (x \in A \text{ or } x \in B)$$

The formulation on the right is quite useful in proofs.

Use venn diagram analogy: define $A \cap B$. Analogue of "and" in that:

$$x \in A \cap B \iff (x \in A \text{ and } x \in B)$$

Define set difference: $A \setminus B$. (Read: A cut B, A minus B, A setminus B). It consists of all elements of A that aren't in B. i.e.

$$x \in A \setminus B \iff x \in A \text{ and } x \notin B$$

Example time! Say we have $A = \{1, 2, 3, 6\}$ and $B = \{3, 6, 9, 10\}$ and $C = [1, 2]$.

- What is $A \cup B$?
- What is $A \cap B$?
- What is $A \setminus B$?
- What is $B \setminus A$?
- What is $B \cap C$?
- What is $A \cap C$?
- What is $C \setminus A$?

Quick proof: for any two sets A, B, we have that $A \subseteq A \cup B$:

$$x \in A \Rightarrow x \in A \text{ or } x \in B \Rightarrow x \in A \cup B$$

You'll be asked to prove some more complicated facts on your homework. For now, we note a few more:

- $A, B \subseteq A \cup B$
- $A \cap B \subseteq A, B$
- $A \setminus B \subseteq A$.

17. Feb 19 (Set theory 3)

Products and power sets. Indexed unions

Products. Given sets X, Y, we define the set product (or product set, or cross product):

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

i.e. it's the set of **ordered pairs** (x, y) with the first entry being X and the second being in Y.

$$(x, y) \in X \times Y \iff x \in X, y \in Y$$

Examples: If $X = \{a, b, c\}$ and $Y = \{1, 2\}$ then

$$\{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)$$

Notice the number of elements. If $|X|, |Y|$ finite then $|X \times Y| = |X||Y|$.

Example: $\mathbb{R} \times \mathbb{R}$, also denoted $\mathbb{R}^2$, is visualized as the usual x, y plane. Draw that and $[1, 2] \times [3, 4]$ to motivate cross/set product.

Consider the intervals $[0, 1], [3, 5]$ and $[2, 3], [-1, 0]$

- Draw $[0, 1]$ and $[0, 1] \cup [3, 5]$
- Draw $[0, 1] \times [2, 3]$
- Draw $([0, 1] \cup [3, 5]) \times [2, 3]$
- Draw $[0, 1] \times ([2, 3] \cup [-1, 0])$

What pattern do we notice? What do you think $([0, 1] \cup [3, 5]) \times ([2, 3] \cup [-1, 0])$ would look like?

Proposition: (A distributivity-type law) Show that $(A \cup B) \times C = A \times C \cup B \times C$.

Proof.

$$\begin{aligned}
(x, y) \in (A \cup B) \times C &\iff x \in (A \cup B) \wedge y \in C \\
&\iff (x \in A \vee x \in B) \wedge y \in C \\
&\iff (x \in A \wedge y \in C) \vee (x \in B \wedge y \in C) \\
&\iff (x, y) \in A \times C \vee (x, y) \in B \times C
\end{aligned}$$

The second-to-last bit comes from the distributive property in logic: $(Q \vee R) \wedge P = (Q \wedge P) \vee (R \wedge P)$. Our chain of biconditionals implies that $(A \cup B) \times C = (A \times C) \cup (B \times C)$. □

Being able to reason out some of these set theory equations and their logic equivalents is useful for things like probability.

Power sets. Given a set A, it has a *power set*, denoted $\mathscr{P}(A)$. (Different from $P(k)$ in induction!!) $\mathscr{P}(A)$ **is the set of all subsets of** A**.**

Example: (count by number of elements)

$$\mathscr{P}(\{1,2,3\}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$$

Yes, the empty set counts! Every element of the empty set is an element of $\{1,2,3\}$. This is *vacuously* true. We can never pick any elements; all zero of the elements in $\varnothing$ are in $\{1,2,3\}$. As in, $x \in \varnothing \Rightarrow x \in \{1,2,3\}$ is true, because the first part is always F. So $\varnothing \subseteq \{1,2,3\}$.

And then ask: what should this be?

$$\mathscr{P}(\varnothing) = \{\varnothing\}$$

Can also ask:

- Is $\{\varnothing\} \subseteq \mathscr{P}(\varnothing)$? (yes)
- Is $\{\varnothing\} \in \mathscr{P}(\varnothing)$? (no)
- Is $\varnothing \in \mathscr{P}(\varnothing)$? (yes)
- Is $\varnothing \subseteq \mathscr{P}(\varnothing)$? (yes)

— If time, cover indexing sets. Likely not. So give sufficient characterization to do the HW and expound next class. $A_i = \{1, 2, \ldots, n\}$.

$$x \in \bigcup_{i \in \mathbb{N}} A_i \iff x \in A_n \text{ for some } n \in \mathbb{N} (\iff \exists n \text{ s.t. } x \in A_n)$$

$$x \in \bigcap_{i \in \mathbb{N}} A_i \iff x \in A_n \text{ for every } n \in \mathbb{N} (\iff \forall n \in \mathbb{N}, x \in A_n)$$

18. Feb 21 (Set theory 4)

First, let's talk about unions indexed over $\mathbb{N}$. (Might want to motivate with sigma notation. $1^2 + 2^2 + \cdots + n^2$ clunky so could write as $\sum_{i=1}^{n} i^2$ instead).

Could take union of two sets A_1, A_2. Drag venn diagram. Maybe union with a third set A_3.

$$x \in A_1 \cup A_2 \cup A_3 \iff x \in A_1 \text{ or } A_2 \text{ o r} A_3$$

Similarly with A_4. Can do with A_n.

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i \left(= \bigcup_{i \in \{1,2,\ldots,n\}} A_i \right)$$

Analogous to sigma notation. The i is the indexing variable, start at 1, iterate to get n. The right most is thoguht of as: take every choice of i in the set $\{1, 2, \ldots, n\}$ and add the corresponding A_i to the union.

But sometimes we want to take unions of infinity many sets!

$$\bigcup_{i=1}^{\infty} A_i = (A_1 \cup A_2 \cup \ldots) \left(= \bigcup_{i \in \mathbb{N}} A_i \right)$$

Again: rightmost says you union all the sets A_i with i in the prescribed indexing set.

$$x \in \bigcup_{i=1}^{\infty} A_i = \bigcup_{i \in \mathbb{N}} A_i \iff x \in \text{at least one of the } A_i$$

Above: It's an existence statement

Example: let $A_i = \{2i, 4i\}$ for $i \in \mathbb{N}$. What is $\cup_{i\in\mathbb{N}} A_i$?

Next, sometimes we want unions over index sets that aren't like $\mathbb{N}$. Maybe want them indexed by the real numbers instead. Suppose you have an indexing set I, and for each choice of $i \in I$, you have a set B_i. So you have a family of sets $\{B_i : i \in I\}$. Then you can form a new set $\cup_{i\in I} B_i$. It is characterized by:

$$x \in \bigcup_{i\in I} B_i \iff \text{there exists an } i \in I \text{ such that } x \in B_I$$

i.e. the elements of the union are elements that appear in at least one B_i.
Example: for $r \in \mathbb{R}$, let $B_r = \{r\}$. Then:

$$\bigcup_{r\in R} B_r = \mathbb{R}$$

A similar idea extends to intersections.

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

where x is in this set if and only if it's in all of them. Likewise:

$$x \in \bigcap_{i=1}^{\infty} A_i = \bigcap_{i\in\mathbb{N}} \iff x \in A_i \text{ for all } i \in \mathbb{N}$$

and then we can do intersections with any sort of indexing set. I an indexing set, have a B_i for each $i \in I$. Then:

$$x \in \bigcap_{i\in I} B_i \iff x \in B_i \text{ for } \underline{\text{every}}\ i \in I$$

Example: let's use $\mathbb{R}$ as an indexing set again. For $r \in \mathbb{R}$, set $B_r = \{0, r\}$. Then

$$\bigcap_{r\in\mathbb{R}} B_r = \{0\}.$$

If $B_r = \{r\}$, then $\cap_{r\in\mathbb{R}} = \varnothing$.
If time, do power set counting stuff. Or ask: is $\mathscr{P}(A \cup B) = \mathscr{P}(A) \cup \mathscr{P}(B)$?
If time, could also do $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

19. Feb 23 (Set theory 5)

We'll do examples of indexed unions, intersections. Key formulas: if $I \subseteq J$ then:

$$\bigcap_{i\in I} B_i \supseteq \bigcap_{j\in J} B_j$$

(makes sense: intersecting more sets should make the intersection smaller). If $I \subseteq J$ then:

$$\bigcup_{i\in I} C_i \subseteq \bigcup_{j\in J} C_j$$

(makes sense: unioning more sets should make the union bigger).

- **Example 1**:

$$\bigcap_{r\in\mathbb{R}} [r^2 - 1, r^2 + 1] = \varnothing$$

Note: each individual $[r^2-1, r^2+1]$ is an interval with length 2, and as r ranges they can be very far apart! In particular, if we pick, say, $r = 0$ and $r = 10$ we get

$$\bigcap_{r\in\mathbb{R}} [r^2-1, r^2+1] \subseteq [-1,1] \cap [99,100] = \varnothing$$

which means this intersection must be $\varnothing$.

- **Example 2**:

$$\bigcap_{r\in\mathbb{R}} [-r^2-1, r^2+1] = [-1,1]$$

Intuitively: as we increase the size of $|r|$, get a window "growing" around $[-1,1]$. Minimum at $r = 0$, which is $[-1,1]$. So intersection is $[-1,1]$.

More formally: every $[-r^2-1, r^2+1]$ contains $[-1,1]$ so, since the intersection consists of elements common to each "piece," we get

$$[-1,1] \subseteq \bigcap_{r\in\mathbb{R}} [-r^2-1, r^2+1]$$

On the other hand, the intersection is a subset of any $[-r^2-1, r^2+1]$ piece. Pick $r = 0$ to get:

$$\bigcap_{r\in\mathbb{R}} [-r^2-1, r^2+1] \subseteq [-1,1]$$

Hence we have both containments and the two sets are equal.

- **Example 3**:

$$\bigcup_{n\in\mathbb{Z}} ([-2,|n|] \cap \mathbb{Z}) = [-2,\infty) \cap \mathbb{Z}$$

Note: our final answer definitely needs to be a subset of $\mathbb{Z}$ since every $[-2,|n|] \cap \mathbb{Z}$ is a subset of $\mathbb{Z}$. As we increase $|n|$ we can get arbitrarily large integers in this union, and all the integers below until -2.

- **Example 4**:

$$\begin{aligned}\bigcup_{n\in\mathbb{N}} (n-1, n) &= (0,\infty) \setminus \mathbb{N} \\ &= (0,\infty) \setminus \mathbb{Z} \\ &= \{x \in \mathbb{R} : x > 0 \wedge x \notin \mathbb{Z}\}\end{aligned}$$

Best way to see this is to draw the first few terms in this union: $(0,1), (1,2)$, etc. Get all positive numbers, except the positive integers.

20. Feb 26: Exam review

Do practice problems from sheet, discuss proof strategies.

21. Feb 28: N/A due to exam

Administer exam.

22. March 1 (Relations 1)

(Reference: Hamkins chapter 11, Taylor chapter 5)

Math and real life full of relations: a way to associate certain pairs of objects, numbers, people, etc usually based on some property. Examples of relations:

aSb we write this if person a is a sibling of b. $x = y$: we write this if the two numbers are the same $x < y$: write if y is bigger than x (i.e. $y - x$ is positive)

In general, a relation on a set S is a subset of $S \times S$. If $R \subseteq S \times S$ is our relation subset, we say s is related to t if and only if $(s, t) \in R$. For shorthand, we'd usually write $s \sim t$. If we have multiple relations running around in a problem, we might do $\sim_1, \sim_2$ to differentiate them.

(Can also define a relation between X and Y: it is again a subset of $X \times Y$ and is meant to relate objects of X to objects of Y, often under some nice rule. For now we focus on binary relations, i.e. between a set and itself.).

- If the relation is equals, the associated subset of, say, $\mathbb{R} \times \mathbb{R}$ is $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x = y\}$
- If the relation is $x < y$, the associated subset of $\mathbb{R} \times \mathbb{R}$ if $R = \{(x, y) : y - x \text{ is positive}\}$.

Example: If $S = \{1, 2, 3\}$ and we have the relation $R = \{(1, 1), (1, 2), (2, 1), (1, 3), (3, 1)\}$. Which of the following is true?

- $1 \sim 1$? (Yes)
- $3 \sim 1$? (Yes)
- $3 \sim 2$? (No)

We often like relations with some nice properties. Suppose R is a relation on a set S.

- A relation R is **reflexive** if $s \sim s$ for all $s \in S$,
- R is **symmetric** if, whenever $s \sim t$, then also $t \sim s$. (So, for all $s, t \in S$: $s \sim t \Rightarrow t \sim s$).
- R is **transitive** if, whenever $s \sim t$ and $t \sim u$, then also $s \sim u$). (So, for all $s, t, u \in S$: $s \sim t$ and $t \sim u \Rightarrow s \sim u$).

Is our example relation reflexive? Symmetric? Transitive? Asking for a relation on some fixed set that is some number of reflexive, symmetric, transitive is a common question, so want to become comfortable with such problems as you go through this unit.

Let's do more examples: recall the divides symbol $|$. $|$ is a relation on $\mathbb{Z}$: we say $a \mid b$ if and only if $b = ak$ for some $k \in \mathbb{Z}$.

Question: is $|$ reflexive? Symmetric? Transitive?

23. March 4 (Relations 2)

Review equivalence relations, reflexive/symmetric/transitive. One use of equivalence relations is they split a set into *equivalence classes*. Sometimes it is useful to consider equality up to equivalence classes.

If R is an equivalence relation on a set S, then for any element $s \in S$, we can define its equivalence class.

$$[s] = \{t \in s : s \sim t\}$$

Because $R, \sim$ is an equivalence relation, the set of equivalence classes form a *partition* of S. That is, it is a collection of sets that are pairwise *disjoint* (i.e. if $[s_1] \neq [s_2]$, then $[s_1] \cap [s_2] = \varnothing$) and the union of all the equivalence classes is the whole set S. Note that this means if $[s_1] \cap [s_2] \neq \varnothing$, then $[s_1] = [s_2]$. See Hamkins 11.3 for more details.

Do an example: a relation on the integers $\mathbb{Z}$, where $x \sim y \iff x, y$ have the same parity. (Parity is the even-ness or odd-ness of a number. For example the parity of 2 is 'even' and the parity of 7 is 'odd.' $f(n) = (-1)^n$ is a function that depends only on the *parity* of the number n).

Show reflexive, symmetric, transitive. Demonstrate that this splits the integers into two equivalence classes (not infinitely many! Because lots of equiv classes the same!)

End by talking about how a partition yields an equiv relation.

24. March 6 (Functions 1)

Taylor 5 a little more comprehensive in terminology.

A *function* f from a set A to a set B ($f : A \to B$) does the following: for each $x \in A$, it assigns some $u \in B$ (and assigns only *one* value!). That element y is denoted by $f(x)$.

Example: functions from real numbers to real numbers, $f(x) = x^2$, $g(x) = \sin x$, $h(x) = -x$.

Example: $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7, 8\}$, sending

$$1 \mapsto 5$$
$$2 \mapsto 8 \quad 3 \mapsto 6$$

A way that mathematicians are fond of packaging all this info is:

$$\begin{aligned} f : A &\to B \\ x &\mapsto f(x) \end{aligned}$$

for example, the squaring function:

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

Now, there are a lot of new definitions/terminology when we talk about functions! We'll get used to them as we use them, feel free to stop and ask me about any of these new words.

Another word for a function is a **map**, and we say f is a **map** from A to B. A is the **domain**, B is the **codomain**. The **range** or **image (of A)** is

$$f(A) = \{y \in B : y = f(a) \text{ for some } a \in A\} = \{f(a) \in B : a \in A\}$$

i.e. all the things actually "hit" by the map/function. Note that $f(A) \subseteq B$, but is not necessarily equal to B.

Graph the following functions. What are the domains, codomains, and images of the following:

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \\ g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \sin x \\ h : \mathbb{Z} &\to \mathbb{N} \\ x &\mapsto |-x| \\ \alpha : \mathbb{N} &\to \mathbb{N} \\ x &\mapsto 2x \end{aligned}$$

If we have a function $f : A \to B$, and $A' \subseteq A$, then we can also look at the image of A', i.e.

$$f(A') = \{y \in B : y = f(a) \text{ for some } a \in A'\} = \{f(a) \in B : a \in A'\}$$

that is, you just look at the elements getting mapped to from stuff *specifically in* A'.

Relatedly, we can define the **restriction** to A:

$$\begin{aligned} f|_{A'} : A' &\to B \\ a &\mapsto f(a) \end{aligned}$$

i.e., the function rule is the same, you just consider the function on fewer elements. Ex: graph $f|_{[0,\infty)}$ with f as above (the squaring map). Or $g|_{[0,2\pi]}$. Or $h|_{2\mathbb{Z}}$ (the even integers). They will look like a smaller portion of the full graph.

25. March 8 (Functions 2)

Finish up restriction from last time. Talk about image in general. And then define the preimage. $f : A \to B$, then for $B' \subseteq B$ we define

$$f^{-1}(B') = \{a \in A : f(a) \in B'\}$$

that is, it's a subset of A consisting of all elements that land in B' after you apply the function f.

Demonstrate with $g(x) = \sin x$. Take $g^{-1}(\{0\})$ and $g^{-1}([-1, 0])$.

- $g^{-1}(\{0\}) = \{\dots, -2\pi, -\pi, 0, \pi, 2\pi, 3\pi, \dots\}$
- $g^{-1}([-1, 0]) = \bigcup_{n\in\mathbb{Z}}[2(n-1)\pi, 2n\pi]$
- $f^{-1}([0, 1/4]) = [-1/2, 1/2]$.

Time for even more definitions!

- A function $f : A \to B$ is **injective** if $f(x) = f(y) \Rightarrow x = y$. That is, no two elements of A map to the same element of B.
- A function $f : A \to B$ is **surjective** if, for any $y \in B$, you can find some $x \in A$ such that $f(x) = y$, That is, you can hit everything in B. i.e., $f(A) = B$.
- A function $f : A \to B$ is **bijective** if it is both injective and surjective.

[Draw arrow diagrams of the usual injective/surjective/bijective]

If A, B are finite sets, then an injection $A \to B$ means $|A| \leq |B|$. A surjection means $|A| \geq |B|$. And a bijection means $|A| = |B|$ (so sometimes a clever way to show two numbers are equal is to relate the two quantities to sizes of sets, and write down a bijection). We'll prove some of these in class and some in HW.

The idea is that bijections pair up elements: nice and *invertible*.

For f, g, h, α as they are above:

- f is not injective and not surjective. $f(-1) = f(1)$. $f|_{[0,\infty)}$ is injective, though. And $f : [0, \infty) \to [0, \infty)$ is injective and surjective.
- g is not injective and not surjective. $g(0) = g(2\pi)$.
- h is surjective, but not injective. $h(-1) = h(1)$.
- α is injective, but not surjective.

26. March 11 (Functions 3)

We should do an example of proving something is a bijection.

Proposition 26.1. The function

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ n &\mapsto n + 1 \end{aligned}$$

is a bijection.

Proof. First, we show the function is injective. Suppose $f(x) = f(y)$. That means that $x+1 = y+1$. Subtracting 1 from both sides, we get $x = y$ as desired.

Next, we show the function is surjective. Let $y \in \mathbb{Z}$. We want to show there is some $x \in Z$ such that $f(x) = y$. Well, pick $x = y - 1$. Then $f(x) = (y - 1) + 1 = y$, and we are done.

Since f is injective and surjective, it is bijective. □

(Note: some of this extra exposition written for the benefit of students, but could be trimmed down in an exam situation).

Next, let's talk about some nice properties of injections. Nice prop of surjection done on HW.

Function composition: $f : A \to B$ and $g : B \to C$, can define:

$$g \circ f : A \to C$$
$$x \mapsto g(f(x))$$

i.e. $g \circ f(x) = g(f(x))$.

Proposition 26.2. If $f : A \to B$ is injective and $g : B \to C$ is injective, then $g \circ f : A \to C$ is injective.

Proof. We'll show $g \circ f : A \to C$ injective. (This means: whenever $g(f(x)) = g(f(y))$, we need $x = y$).

Well, take $g(f(x)) = g(f(y))$. Since g is injective, we get $f(x) = f(y)$. Since f is injective, we get $x = y$. □

Proposition 26.3. If A is a finite set, then there does not exist an injection $f : A \to B$ with $|B| < |A|$.

Proof. We induct on the size of the set. First, note that the above is true for a set with 0 elements, i.e. $A = \varnothing$, then this easily holds because there is no set with number of elements < 0.

We now handle the case of $1 \leq |A| < \infty$. Define $P(k)$ to be the property that:

> Any set with k elements cannot inject into a smaller set.
>
> That is, for any A with $|A| = k$, and any B with $|B| < k$, there is no injection $A \to B$.

It is enough to show that $P(k)$ is true for all k (as we range over k, get all finite sets).

Base case: $P(1)$ is true, can't have an injection to the empty set (can't have a function, in fact).

Inductive step: Suppose $P(k)$ true. We'll show $P(k+1)$ true.

To show $P(k+1)$ true, let A be an arbitrary set with $k+1$ elements. Let B be an arbitrary set with fewer than $k+1$ elements. We need to show there is no injection $f : A \to B$.

Suppose such an injection f exists. Pick $a \in A$. We know it maps to some $f(a) \in B$, and we know it's the only element of A that maps to it. So we get a well-defined function (draw picture):

$$f' : A \setminus \{a\} \to B \setminus \{f(a)\}$$
$$x \mapsto f(x)$$

this is essentially a restriction of f with the codomain adjusted. Then f' is well-defined, and still injective. And:

$$k + 1 = |A| > |B| \Rightarrow k = |A \setminus \{a\}| = |A| - 1 > |B| - 1 = |B \setminus \{f(a)\}|.$$

But then we have an injection from a set with k elements to a set with fewer than k elements. This contradicts $P(k)$. So our assumption must be false, and no such f exists. This means $P(k+1)$ is true.

Then by induction, we get that a finite set cannot inject into a smaller set. □

27. March 13 (Functions 4)

Suppose $f : X \to Y$. Then f is invertible if there exists $g : Y \to X$ such that $(f \circ g)(y) = y$ for all $y \in Y$ and $(g \circ f)(x) = x$ for all $x \in X$.

For example: $f : \mathbb{R} \to \mathbb{R}$ given by $x \mapsto x + 1$ has inverse $x \mapsto x - 1$.

Key idea: invertible $\iff$ bijective. It is part of why we like bijections so much. (Draw picture: pair up elements, track back up the arrow).

Invertible $\Rightarrow$ bijective: Suppose $f(x_1) = f(x_2)$. Then $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$, so injective. And for any $y \in Y$, note that $f(g(y)) = y$, so f surjective.

Bijective $\Rightarrow$ invertible: Define the inverse as follows: for $y \in Y$, define $g(y)$ to be the unique x mapping to it (which has to exist for a bijection). One can check that $f(g(y)) = y$ and $g(f(x)) = x$.

(Can also view through relation perspective. A relation on $A \times B$ with the property that for every $a \in A$, unique b such that $(a, b) \in R$. Can flip $R' \subseteq B \times A$ – see Hamkins. If this has function property above, get that this functions as inverse. This perspective less stressed in this course.)

Give examples of computing inverses $y = f(x)$ and solve for x in terms of y.

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ x &\mapsto x + 1 \end{aligned}$$

Set $y = f(x) = x + 1$. Like one might do in Calc I/II, we solve for x in terms of y to see what the unique x mapping to a given y in the codomain is. This should be the inverse, if we look above at the bijective $\Rightarrow$ invertible paragraph.

$$y = x + 1 \Rightarrow x = y - 1$$

so the inverse is $g : \mathbb{Z} \to \mathbb{Z}, y \mapsto y - 1$.

Now consider

$$\begin{aligned} F : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^3 \end{aligned}$$

Set $y = x^3$. Then $x = y^{1/3}$. And one can indeed check that $G : \mathbb{R} \to \mathbb{R}, y \mapsto y^{1/3}$ is the inverse of F.

28. March 15 (Combinatorics 1)

We now shift to combinatorics. The reference for this is Hamkins 5.6. If any additional texts are needed, I will either provide notes or link a free source.

Combinatorics is an area of math that concerns *counting*. Nice applications such as: if I have to compute...

$$\begin{aligned} (x + y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3 \\ (x + y)^4 &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \end{aligned}$$

I can perform this computation quite quickly, without doing the extremely tedious work of expanding out the 4-term multiplication. How is this possible? Through a result of combinatorics.

As we'll see after the break, many results in combinatorics have two proofs with two distinct flavors: a proof involving careful algebra to manipulate an algebraic formula (like the factorial formula for $\binom{n}{k}$ seen below) *or* a clever counting argument that shortens the proof to a couple lines.

We first concern ourselves with choosing objects when caring about order, i.e. permutations.

- How many ways to choose an object from 3 objects? 3
- How many ways to choose two objects from three objects (while caring about the order in which we choose them)? There are 6. If you label the objects A, B, C, the possibilities are:

  $$AB, AC, BA, BC, CA, CB$$

  Another way to see it is 6: note that $6 = 3 \cdot 2$. When picking the objects: think about your three objects being in a bucket, and pulling out one object and then another. There are three options for the first choice. Then two options for the second choice. So there are $3 \cdot 2$ options.

What about picking 3 objects from a collection of 4 objects (caring about order)? Again we can imaging picking them out of a bucket. There are 4 choices when we pick the first object. Then 3 choices for the second. And then 2 choices for the next. So there are $\mathbf{24} = 4 \cdot 3 \cdot 2$ ways to choose three objects from four when caring about order.

This motivates a definition. We define the symbol $n!$ to be the quantity...

$$n! = n(n-1)(n-2)\dots 2 \cdot 1$$

In order for some formulas to work out, we define

$$0! = 1$$

And do note that:

$$(n+1)! = (n+1) \cdot (n!)$$

Let's return to our discussion of choose objects. As we see from out previous examples, the number of ways to choose k objects from a collection of n objects (when caring about the order we choose them in) is:

$$n(n-1)(n-2)\dots(n-(k-1)) = n(n-1)(n-2)\dots(n-k+1)$$

We can express this as:

$$\frac{n!}{(n-k)!}$$

Note that this means the number of permutations of n objects (i.e. the number of ways to rearrange n objects) is $n!$.

Now: what if we don't care about the order of the objects? So now things like AB are considered the same as BA. (Think about picking groceries and tossing them in a cart: don't really care what order you put them in. Mathematically, there are lots of scenarios where you're picking objects but don't care about the order).

Consider two objects, A and B. If we picked two objects from these two objects and cared about order: there would be two options: AB and BA. If we don't care about order, then there is only one option.

Consider three objects: A, B, C. If we picked two objects from these three and cared about order: there would be six options. But remember those options are AB, AC, BA, BC, CA, CB. If we don't care about order, then stuff like AC and CA should be considered the same. i.e. this list double counts if we're not caring about order. **So:** if we pick two objects from three objects and don't care about order, there are **three options**. The best way to think about this is $\frac{3\cdot 2}{2}$. There are $3 \cdot 2$ ways to pick when caring about order, and then we divide by 2 to account for the double-counting.

Consider four objects: A, B, C, D. If we pick three objects from this and care about order, there are $24 = \frac{4!}{(4-1)!}$ options. But like we discussed before: this number over-counts if we don't care about order. We need to divide by something to account for that. Specifically, we want to divide by the number of ways to re-arrange 3 objects. Because if we have a choice like ABC then the permutations

$$ABC, CAB, BCA, BAC, CBA, ACB$$

all correspond to the same thing. There are $6 = 3 \cdot 2 \cdot 1$ ways to permute three objects. So there are:

$$\frac{24}{6} = \frac{(4!/(4-1)!)}{3!} = 4$$

ways to pick three objects from four when not caring about order.

In general, we can obtain a formula for the number of ways to choose k objects from n objects. This quantity is denoted by $\binom{n}{k}$ and read aloud as "n choose k." We start by looking at the $\frac{n}{(n-k)!}$ ways to choose k objects with order, and then divide out by the number of ways to rearrange the k objects. In the end we get:

$$\begin{aligned}\binom{n}{k} &= \text{number of ways to choose } k \text{ objects from } n \text{ objects without order} \\ &= \frac{n!}{(n-k)!k!}\end{aligned}$$

These are also known as **binomial coefficients**.

One really fun thing to note: this means the fraction $\frac{n!}{(n-k)!k!}$, which at first just looks like some element of $\mathbb{Q}$, in fact has to be an integer! That's because it's counting an integer quantity.

29. March 25

Today: the fun of combinatorics: can bash things out with algebra, or do clever proofs with words!!

Do Pascal's triangle $\binom{n}{k}$ with $n \geq k \geq 0$. Row number is index of n on top. Observe an additive pattern. Then: two proofs!

One way: note that

$$\binom{n+1}{k} = \frac{(n+1)!}{(n+1-k)!k!}$$

$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(n-(k-1))!(k-1)!} + \frac{n!}{(n-k)!k!} + \\ &= \frac{n!}{(n-k+1)!(k-1)!} + \frac{n!}{(n-k)!k!} \\ &= \frac{n!k}{(n-k+1)!k!} + \frac{n!(n-k+1)}{(n-k+1)!k!} \\ &= \frac{n!(n+1)}{(n-k+1)!k!} \\ &= \frac{(n+1)!}{((n+1)-k)!k!} \\ &= \binom{n+1}{k}.\end{aligned}$$

But perhaps an easier way to see it is: $\binom{n+1}{k}$ counts the number of ways to choose k objects from $n+1$. Consider this new added $n+1$-th object. When you pick the k objects, you can include this new object or not. If you do, you are picking the remaining $k-1$ objects from the remaining n objects. If you do not pick it, you are choosing k objects from the n original objects. These two scenarios are disjoint and cover everything. Hence you get Pascal's formula.

(Draw this with circles and dot-dot-dots)

30. March 27

More combinatorics

31. March 29

More combinatorics

32. April 1

Return to number theory

33. April 3

Number theory

34. April 5

Number theory

35. April 8

Number theory

36. April 10

Graph theory

37. April 12

Graph theory

38. April 15

Graph theory

39. April 17

Graph theory

40. April 19

Finite games

41. April 22

Finite games

42. April 24

Finite games

43. April 26: Review for final exam

Go over practice problems and strategies