Every Reference in "Finite Simple Group (of Order Two)"

(And Possibly, Math (But No Promises))

CJ Quines

July–August 2022

These are notes for a Summer HSSP 2022° class aimed at high schoolers. Its ambitious goal is to cover every reference used in the Klein Four's song, "Finite Simple Group (of Order Two)". Because of that ambitious goal, we will throw rigorous math out the window, and everything will be at the mercy of intuition and incorrect explanations.

These notes will be more detailed than explanations we'll have in class, but in class I can draw pictures and answer questions much more easily.

1 Functions (July 9)

If I know my high school curriculum right, then it's likely you know some of these.

relation, well-defined. *Also: ill-defined.* Given two sets X and Y, a (binary) **relation** is a set of some ordered pairs (x, y), where $x \in X$ and $y \in Y$. In other words, a relation over X and Y is a subset of $X \times Y$.

This is a concept you've probably heard about before, we're now just giving it a name. Many things in math are relations. Chances are, if you use the phrase "x is (something) of y" or "x is (something) to y", you're describing a relation. For example:

- "is a factor of" is a relation over the sets $\mathbb{Z}$ and $\mathbb{Z}$. It's the set of all (x, y) such that x is a factor of y. The pairs $(2, 4)$ and $(-4, 8)$ are in the relation, while $(3, 8)$ and $(0, 3)$ aren't.
- "is the square root of" is another relation over the sets $\mathbb{Z}$ and $\mathbb{Z}$. It's the set of all (x, y) such that $x = y^2$, which includes $(2, 4)$ and $(-2, 4)$. As we can guess from here, it's a common case that X and Y are the same—in which case, we can drop Y, and just say it's a relation over X.
- "is double" is a third relation over $\mathbb{Z}$. It's the set of all (x, y) such that $x = 2y$. Note that not every x has a y that relates to it—that doesn't stop it from being a relation.
- "is equal to" is another relation over $\mathbb{Z}$. It can also be a relation over $\mathbb{R}$, or over $\mathbb{Q}$, or a relation between $\mathbb{Z}$ and $\mathbb{R}$, and so on. These are all different relations, because they have different sets. It's not enough to say something is a relation, you have to say which set it's a relation over.
- "has the Social Security number" is a relation over the set of people and nine-digit numbers. It's the set of all (x, y) such that x has the Social Security number y. Like the previous example, not every person has a Social Security number, but it's still a relation.

All relations we've talked about are **well-defined**: there's a unique way to interpret it. The opposite of well-defined is **ill-defined**. An example of an ill-defined relation is "is friends with" over the set of people. There's no clear definition of what friends means. There are more subtle examples of ill-defined relations. Consider the relation "has the last digit", over the real numbers. That's not well-defined: what's the last digit of $\frac{1}{11}$?

Remark 1.1. Even if you only considered terminating decimals, "has the last digit" still isn't well-defined. For example, 1 can also be written as $0.999\ldots$.

domain, image. *Also: codomain, preimage.* Given a relation over X and Y, we call X the **domain** of the relation and Y the **codomain** of the relation.

Let's consider the relation "has the Social Security number". We defined its domain as the set of all people, and its codomain as the set of all nine-digit numbers. But not all nine-digit numbers° are Social Security numbers, like 000-00-0000. The codomain of this relation is thus larger than its "active" codomain, or the nine-digit numbers that are actually *used*.

The image is the set of the codomain's elements that are "used". More precisely, the **image** of a relation is the set of all y such that (x, y) is in the relation, for some x.

Remark 1.2. You might have heard the word "range" before. We'll never use that word, because it's ambiguous: does it mean codomain or image?

You might be wondering what the "opposite" of an image is. What's the set of all x such that (x, y) is in the relation, for some y? There's no widely agreed name for this, but we'll call it the **preimage**. The preimage of the "has the Social Security number" relation is the set of all people who have Social Security numbers.

Exercise 1.3. What are the domains and images of the relations we gave as examples?

function. You're probably familiar with the concept of a function as a machine: it takes an input, and produces an output. More precisely, a **function** from X to Y is a relation over X and Y, such that for any x, there is *exactly* one y such that (x, y) is in the relation. Exactly one means that:

- it can't be less than one. The relation "is double" over $\mathbb{Z}$ is not a function, because, for example, there's no y such that $(1, y)$ is in the relation.
- it can't be more than one. The relation "is a factor of" over $\mathbb{Z}$ is not a function, because, for example, both $(1, 2)$ and $(1, 3)$ are in the relation.

Of the examples we mentioned earlier, "is the square root of" over $\mathbb{Z}$ and "is equal to" over $\mathbb{Z}$ were functions.

Functions appear so often that we have special notation for them. We often represent functions with letters like f, and say $f : X \to Y$. Instead of saying (x, y) is in the function, we say $f(x) = y$. That way, we can think of f as the "machine": it takes an input, x, and returns an output, y. We'll talk about functions with this language moving forward.

Note that this notation is only *well-defined* for functions:

- for the relation "is double" over $\mathbb{Z}$, the notation isn't defined for some xs. What's $f(3)$?
- for the relation "is a factor of" over $\mathbb{Z}$, the notation is ambiguous for some xs. What's $f(1)$?

This shows us another meaning of the term *well-defined*. A notation is well-defined if it means something, and exactly one thing, for any way you can write it.

Exercise 1.4. Of the relations we talked about that weren't functions, some of them could be "made into" functions. For example, "has the Social Security number" can be turned into a function, if we considered it as a relation over a different domain and image. Which of the relations can be turned to functions this way?

Exercise 1.5. Two of the lines of the song are "But lately our relation's not so well-defined / And I just can't function without you". How are these two lines related to each other? Do you find this funny?

one-to-one. *Also: transpose, injective, surjective, bijective, inverse function.* Here's one important difference between "is the square root of" and "is equal to". The function "is the square root of" over $\mathbb{Z}$ isn't a function the "other way around".

Given any relation over X and Y, we can construct a new relation over Y and X, by flipping the (x, y)s to (y, x)s. We call this the **transpose** of the relation. When is the transpose of a function still a function? Remember that for a relation to be a function, it needs to follow two rules:

- Every x has to be related to *at most one* y. Because $(2, 4)$ and $(-2, 4)$ are in the relation, then both $(4, 2)$ and $(4, -2)$ are in the transpose relation.
- Every x has to be related to *at least one* y. There's no x such that $(x, -1)$ is in the relation. Thus, there's no y such that $(-1, y)$ is in the transpose relation.

A function that *does* follow these two rules for its transpose relation has a special name. If a function's transpose follows the first rule, we call the original function **injective**. If a function's transpose follows the second rule, we call the original function **surjective**.

A function that is both injective and surjective is called **bijective**. That means that its transpose is also a function, which we call its **inverse**. In a bijective function, every x is related to exactly one y, and every y is related to exactly one x.

Exercise 1.6. Stop and think about these definitions! If you've seen these words before, then they're probably different definitions than what you're used to. In that case, convince yourself they're the same definition.

Another word for injective is **one-to-one**, and another word for bijective is **one-to-one correspondence**. Due to the potential for confusion, mathematicians avoid using them in practice. That means we're stuck using the names injective, surjective, and bijective, although at least those names are consistent. I also pronounce them with the abbreviations "inj", "surj", and "bij", and I personally find those pronunciations hilarious.

2 Group theory (July 9–16)

group, associative, identity, order. *Also: operation, inverse, subgroup.* A (binary) **operation** over a set G is a function that takes two elements of G and returns another element of G. Some examples are $+$ and $\cdot$ over $\mathbb{Q}$. While we could write them with the function notation of $+(2, 3) = 5$, we write them with the symbol in between instead, like $2 + 3 = 5$.

A **group** consists of a set and an operation with some properties. Some examples:

- The operation $+$ over $\mathbb{Z}$ forms a group.
  - It's **associative**, meaning $a + (b + c) = (a + b) + c$.
  - There's an **identity**, 0, which means $a + 0 = 0 + a = a$.
  - There's also an **inverse** for each a, called $-a$, which means $a + (-a) = (-a) + a = 0$.
- The operation $\cdot$ over the non-zero rational numbers $\mathbb{Q}^*$ forms a group.
  - It's *associative*, meaning $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
  - There's an *identity*, 1, which means $a \cdot 1 = 1 \cdot a = a$.
  - There's also an *inverse* for each a, called a^{-1}, which means $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

We'll name the first group $\mathbb{Z}^+$ and the second group $\mathbb{Q}^\times$. Read out, these are "the additive group of integers" and "the multiplicative group of rationals".

Here are some things that are not groups. Why?

- The operation $-$ over $\mathbb{Z}$.
- The operation $\cdot$ over (all) the rational numbers $\mathbb{Q}$.
- The operation $\cdot$ over $\mathbb{Z}$.

Here are some things that are groups. Convince yourself that they are groups.

- The operation "addition, then divide by n and take the remainder" over the set $\{0, 1, \ldots, n-1\}$ is a group. We call this $\mathbb{Z}/n\mathbb{Z}$, or "the additive group of integers modulo n".
  - We'll write its operation as $+$, because it's kinda like addition. In the group $\mathbb{Z}/5\mathbb{Z}$, $2 + 4 = 1$. But note that this is a different operation than normal addition. When we want to emphasize the difference, we'll use different symbols.
  - Another name for this group is "the cyclic group of order n". The **order** of a group is the number of elements in its set, and the set of $\mathbb{Z}/n\mathbb{Z}$ has n elements.

Remark 2.1. Note that we write $\mathbb{Z}/n\mathbb{Z}$ for both the set and the group. Unfortunately, it's common to write the group and the set using the same symbols. This can be confusing, but we'll try to make it clear what we mean.

- The operation "multiplication, then divide by n and take the remainder" over the set $\{1, 2, \ldots, p-1\}$ is a group, if p is a prime. We call this $(\mathbb{Z}/p\mathbb{Z})^\times$, or the "multiplicative group of integers modulo p".
  - It's not obvious that every element has an inverse, but it's true! For example, if $p = 7$, then you can check that $2 \cdot 4 = 3 \cdot 5 = 6 \cdot 6 = 1$.

Exercise 2.2. For small groups, we can draw its "operation table", which is a table that shows the results of applying its operations on any pair of elements. We write its elements across the rows, and then write it again across the columns. In each entry of the table, the one in the row a and column b, we write the result of the operation on a and b. Draw the operation table for $(\mathbb{Z}/7\mathbb{Z})^\times$.

Exercise 2.3. Why does p have to be prime?

- Consider this sheet of paper. Rotate it however you want, as long as it stays in portrait. Each rotation can be an element of a set. There are four rotations: don't rotate, turn upside-down, flip, and flip and turn upside-down. This is a group with the operation "apply the second rotation, and then the first one".
  - It might be weird thinking of a set whose elements are rotations. But you can think of the previous groups as having elements that also "apply" to something. For example, an element n of $\mathbb{Z}^+$ can be thought of as adding $2n$ to 42. The identity doesn't change the number you're working with, and inverses "return" to the same number.

    Remark 2.4. This is called a *group action*, because its elements "act" on an object. I think it's the right way to think of many groups. All groups have a group action.

  - This group has many names. This is called the "dihedral group of order 4", or D_4. This is also called the "group of symmetries of a rectangle". This is also known as the Klein four-group. The Klein Four, the people who wrote the song we're studying, is named after this group.

Exercise 2.5. What are the inverses of each element in the Klein-four group? Draw its operation table. What about the group of symmetries of a square: how many elements does it have? Can you draw its operation table?

Exercise 2.6. Prove that a group has only one identity element. To start, suppose that, instead, you had two different ones called e and f. Then, what is ef? Similarly, can an element have more than one inverse?

A **subgroup** of a group is a subset of its elements that forms a group under the same operation. For example, a subgroup of $\mathbb{Z}$ is $3\mathbb{Z}$, the group with operation $+$ and elements $\{\ldots, -3, 0, 3, \ldots\}$. Another subgroup is the trivial group, the group with only the element 0. (There's not much choice for what the operation should be!)

Exercise 2.7. There are five subgroups of the Klein-four group. One of them is the group itself. Another is the subgroup containing just its identity element. What are the other three?

kernel, quotient. *Also: homomorphism, isomorphism.* We care about how groups talk to each other. In fact, we care about this far more than groups themselves.

Consider the function $f : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, that's "divide by 3 then take the remainder". For example, $f(5) = 2$, and $f(7) = 1$. Let's consider the groups $\mathbb{Z}^+$ and $\mathbb{Z}/3\mathbb{Z}$. For clarity, we'll write the operation of the first group as $+$, and the operation of the second group as $\oplus$.

How does f interact with our two groups? Well, a group is about its operations, so let's see how it affects the two operations $+$ and $\oplus$. Consider an operation like $5 + 7$. One way to apply f is to

do $f(5+7)$. Another way is $f(5) \oplus f(7)$. In the first case, we get $f(12) = 0$. In the second case, we get $2 \oplus 1 = 0$. And we get the same result!

In a sense, f is a function that *maintains the operation*. You could also say that it *commutes* with the operation: it doesn't matter whether you apply $+$ and then f, or f and then $\oplus$. If we have an group with operation $+$ over set G, and a group with operation $\oplus$ over set H, then a **homomorphism** $f : G \to H$ is a function such that $f(a+b) = f(a) \oplus f(b)$.

An important kind of homomorphism is an **isomorphism**, which is a homomorphism that is also a bijection. We say that two groups that have an isomorphism are actually the same group. An example is how $\mathbb{Z}$ is isomorphic to $3\mathbb{Z}$, with the isomorphism being "multiply by three".

Exercise 2.8. Convince yourself that $\mathbb{Z}/6\mathbb{Z}$ has an isomorphism to $(\mathbb{Z}/7\mathbb{Z})^\times$.

We now define **kernel** and **quotient**, but I already have a nice writeup about this called Canonical decomposition and the first isomorphism theorem°, so I won't repeat it here.

Exercise 2.9. Two of the lines of the song are "I'm living in the kernel of a rank-one map / From my domain its image looks so blue". If you're in the kernel, why would your image "look blue"? Do you find this funny?

simple group, finite. *Also: normal, abelian.* Let's say $f : G \to H$ is a homomorphism. We've talked about the set of elements $\ker f$. Not only is it a subset of the elements of G, it's actually a *subgroup* of G!

Exercise 2.10. Convince yourself that $\ker f$ is a subgroup of G. Does the operation stay in $\ker f$? Does it have an identity? Does it have inverses? The only information we have about $\ker f$ is that it's the kernel of a homomorphism, but homomorphisms are a lot of information.

Not only is $\ker f$ a subgroup of G, but it's a special kind of subgroup called a normal subgroup. A **normal subgroup** is a subgroup that is the kernel of some homomorphism. Non-normal subgroups exist, but not in **abelian groups**, a group where $a \cdot b = b \cdot a$ for all a and b.

Remark 2.11. The smallest example of a non-normal subgroup is in the group of symmetries of an equilateral triangle, D_6. Any subgroup of order two is a non-normal subgroup. One way to check this is to try to look for a homomorphism $D_6 \to \mathbb{Z}/3\mathbb{Z}$.

A **simple group** is a non-trivial group whose only normal subgroups are the trivial group and itself. If this sounds a lot like the definition of "prime", then you're right. The cyclic groups of prime order are all simple groups.

A group is **finite** if its order is finite. In a sense, a finite simple group is like a prime number, in that they're the "building blocks" of finite groups. If a finite group isn't simple, then it has a simple subgroup. The counterpart of the statement that all positive integers have a unique prime factorization would be the Jordan–Hölder theorem.

Finite simple groups are pretty deep. One of the big projects of mathematics, spanning roughly from the 1950s to the 2010s, was to find all the finite simple groups. We know that the cyclic groups of prime order are simple, and in fact, they're the only finite simple abelian groups.

Exercise 2.12. The refrain of the song mentions a "finite simple group of order two". How many groups of order two are there? Try to construct these groups, by starting with two elements, and going over the possibilities for what the operation could be.

3 Metric topology (July 16–23)

open. *Also: metric space, metric, subspace.* If a group consists of a set and an operation, a metric space consists of a set and a **metric**. A metric over a set M is a function $d : M \times M \to \mathbb{R}_{\geq 0}$. The metric function should be interpreted as the "distance" between two elements in M, which we call *points*.

A **metric space** consists of a set and a metric with some properties:

- It is symmetric, so $d(x, y) = d(y, x)$.
- It is positive definite, so $d(x, y) = 0$ if and only if $x = y$.
- It has the triangle inequality, so $d(x, y) + d(y, z) \geq d(x, z)$.

Here are some things that are metric spaces. Convince yourself that they are metric spaces.

- The normal distance function over $\mathbb{R}^2$ gives a metric space. The metric is

$$d((x_1, x_2), (y_1, y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

  - In fact, any $\mathbb{R}^n$ is a metric space with this distance. Further, any subset of $\mathbb{R}^n$ can be made into a metric space, with the same distance.
  - In the case of $\mathbb{R}$, the metric becomes "absolute difference".
  - A subspace of $\mathbb{R}$ is $\mathbb{Q}$, with the same metric of absolute difference.

Remark 3.1. We'll overload notation, just like we did with groups, by writing $\mathbb{R}^2$ for both the set of points and the metric space, but we'll be claer which is which.

- The taxicab distance function over $\mathbb{R}^2$ also gives a metric space, where the distance function is

$$d((x_1, x_2), (y_1, y_2)) = |x_1 - x_2| + |y_1 - y_2|.$$

- There's the discrete metric, where given any set, define $d(x, y) = 1$ if $x \neq y$ and $d(x, y) = 0$ if $x = y$.

Remark 3.2. This is a specific case of a metric space on a connected simple graph, where the metric is the length of the shortest path between two vertices.

- Let p be a prime. There's the p-adic metric over $\mathbb{Q}$, where $d(x, y) = p^{-i}$, and i is defined such that $p^i(x - y)$, in simplest form, has neither numerator nor denominator divisible by p. For example, when $p = 2$, the 2-adic distance between $\frac{3}{8}$ and $\frac{1}{4}$ is 8.

Exercise 3.3. Check that the triangle inequality is satisfied for the p-adic metric. This is actually somewhat hard, but at least convince yourself that it's a metric.

Remark 3.4. Although the last two examples of metrics don't feel really "distance-y", you can still think of a metric as a distance and follow along pretty well. You can get pretty far thinking about metric spaces just by considering $\mathbb{R}^2$. Compare this to groups, where we didn't even discuss non-abelian groups that much, which are completely different from abelian groups.

A **subspace** of a metric space is a subset of its points, with the same metric. This is always a metric space, unlike subgroups.

Finally, an **open subset** of a metric space is a subset of its points such that, for any x in the subset, all points that are "close enough" to x are in the subset too. Specifically, if you want to prove to me that something is an open subset, I'll name a point x in the open set. Then you'll show me a ball around x, one that has "radius ϵ", and show me this ball is contained in the open set.

Remark 3.5. We're going to begin using interval notation° here.

Let's think of $\mathbb{R}$, and the set $(-1, 1)$. If you want to show me this is open, I'll name a point in the subset, like 0.8. Then you can show me a ball, like the ball of radius 0.1. "Look at every point with distance less than 0.1 to 0.8," you'll say. "See that all of those points are in the subset." An example of a set that *isn't* open is the set of all x such that $(-1, 1]$. If I name the point 1 in the subset, you can't give me a ball that contains it, that's also in the subset.

Exercise 3.6. Here are two sets in $\mathbb{R}^2$: a circle, with its boundary, and a circle without its boundary. Which of these two are open? What are the open sets in the discrete metric space? What are all the open sets in $\mathbb{Q}$?

dense. *Also: converge, closed, closure.* There are also these things called closed sets. A closed subset is, unlike what the name suggests, *not* the opposite of an open subset. There are, in fact, sets that are both closed and open. And most sets are *neither* closed nor open! I want to say this now, before we get into definitions, because it's that important.

Consider an infinite sequence of points in a metric space, say, $x_1, x_2, \ldots$. We say that the sequence **converges** to x, for some x also in the metric space, if the sequence gets permanently as close to x as we want to go. You can think of this as another ϵ thing. If you want to show me a sequence converges to x, I'll name a distance ϵ, and you'll have to give me an N, such that all of $x_N, x_{N+1}, \ldots$ are distance at most ϵ to x.

As an example, think of the sequence $3, 3.1, 3.14, 3.141, \ldots$. Considered as a sequence over $\mathbb{R}$, this converges to π. If I say an ϵ like 0.01, you could say, "well, all the things from $3.14, 3.141, \ldots$ have distance at most 0.01 to π." But it doesn't converge over $\mathbb{Q}$!

Now, a **closed subset** of a metric space is a subset of its points such that, for any sequence of points in the subset that does converge, the point it converges to is in the subset. Typical examples are circles in $\mathbb{R}^2$, with their boundary, and in $\mathbb{R}$, things like the set of all x such that $[0, 1]$.

Exercise 3.7. In $\mathbb{R}$, with the usual metric space, think of the set of all x such that $(0, 1]$. Is this open, closed, neither, both? What about the empty set? Now that I've given you reasons why these names are bad, here's the only reason they're good: a subset is open if its complement is closed, and vice versa. Convince yourself this is true by drawing.

Another way to think about closed subsets is through its closure. Say you did take a subset, find all the convergent sequences, and take the set of points they converge to. That set is the **closure** of the original subset, the smallest closed set containing a subset. A set is closed if it's its own closure.

Finally, a set of a metric space is **dense** if its closure is the whole metric space. The typical example is that $\mathbb{Q}$ is dense in the metric space $\mathbb{R}$. To see why every point in $\mathbb{R}$ is the result of a convergent sequence, think of the π example we had earlier. The much harder part to prove is that these are the *only* points that sequences in $\mathbb{Q}$ converge to, although depending on how you define $\mathbb{R}$, you could say that it's the closure of $\mathbb{Q}$.

Exercise 3.8. One line of the song mentions "My heart was open but too dense." We just mentioned that $\mathbb{Q}$ is dense in $\mathbb{R}$, but is it open in $\mathbb{R}$?

continuous, mirror pair. *Also: homeomorphic.* Groups talk to each other through homomorphisms. Metric spaces talk to each other through **continuous functions**. Homomorphisms maintain the group operation: a function f is a homomorphism if $f(a + b) = f(a) \oplus f(b)$. Continuous functions maintain convergence: a function f is continuous if $x_1, x_2, \ldots$ converges to x means that $f(x_1), f(x_2), \ldots$ converges to $f(x)$.

Two groups that are the same are isomorphic. Two metric spaces that are the same are **homeomorphic**. An isomorphism is a bijective homomorphism. A homeomorphism is a bijective continuous function... whose inverse function is also continuous. As an example, the square's boundary is homeomorphic to a circle's boundary. The old joke is that donuts and coffee cups are homeomorphic. An object is always homeomorphic to its **mirror pair**—which just means what you think it means.

Remark 3.9. The "inverse function is also continuous" is an important condition. For example, consider these two metric spaces. The first is the subspace $[0, 1)$ in $\mathbb{R}$. The second set is a circle's boundary, a subspace of $\mathbb{R}^2$. There's bijective continuous functions, but no matter which you pick, their inverses aren't continuous.

path, smooth. A continuous function p from $[0, 1]$ to a metric space is called a **path** in that metric space. It should line up with your intuition about what a path is: a curve connecting one point, $p(0)$, to another, $p(1)$. The fact that it's a continuous means that the path doesn't jump.

The song mentions a "path to love" that's "never smooth". I don't think there's actually a definition for what a smooth path is. The most common definition of smooth comes from calculus. A function is **smooth** if you can take its derivative infinitely many times. There's a notion of taking a derivative of a path, called the *metric derivative*, which is the instantaneous distance traveled at a given point, but I've never heard of it outside this one Wikipedia article I read.

Exercise 3.10. The second line of the song says that, even though the narrator's path to love isn't smooth, it's continuous. If you know what a derivative is, convince yourself that being continuous is

a far cry from being smooth. Is it funny yet?

simply connected. *Also: clopen, connected, path-connected, homotopy.* A set that is both closed and open is called **clopen**. We say a space is **connected** if it has no non-empty clopen sets.

Most of the spaces we've seen so far are connected, but one exception is $\mathbb{Q}$ with the absolute distance metric. Consider the set of numbers in $\mathbb{Q}$ less than $\sqrt{2}$. Seeing that it's open shouldn't be too hard. Seeing that it's closed might be a bit harder, but remember that we're in the metric space $\mathbb{Q}$, and not $\mathbb{R}$, so for it to be closed, we only have to consider sequences that converge in $\mathbb{Q}$. Thus, this set is clopen, and $\mathbb{Q}$ is disconnected.

Exercise 3.11. Consider the absolute distance metric and the set of real numbers in $[0,1] \cup [2,3]$. This is a metric space. Convince yourself that $[0,1]$ is a clopen set in this space. Thus, this space is disconnected. Does this definition match what you imagine it means for a space to be "connected"?

A **path-connected** space is one that has a path joining any two points in it. The metric space $\mathbb{R}$ is path-connected, but not the metric space $[0,1] \cup [2,3]$, over the same metric.

Remark 3.12. All path-connected spaces are connected, but not vice-versa! My favorite example is to think about the comb space. We'll use the fact that if L is a subspace of M, which is a subspace of the closure of L, and L and its closure are both connected, then so is M. We won't prove this, but think about why it feels true.

Consider the comb, which is a subspace of $\mathbb{R}^2$ with the usual distance metric. It consists of the line joining $(0,0)$ to $(1,0)$, which is its shaft, and a bunch of lines joining $\left(\frac{1}{n}, 0\right)$ to $\left(\frac{1}{n}, 1\right)$, and a line joining $(0,0)$ to $(0,1)$. This is connected. Now remove the last line; this is still connected, and its closure is the comb space. If we add back the point $(0,1)$, it follows that it's still connected. But this last space isn't path-connected, as there's no path from $(0,0)$ to $(0,1)$.

A **homotopy** between two paths is a continuous deformation from one path to the other. The formal definition involves a continuous function from $[0,1]$ to paths in the metric space, such that at 0 it's the first path and at 1 it's the last path. There's no good way of explaining this without a picture°, and I'll draw more in class.

A space is **simply connected** if it's path-connected, and, for any two points, all the paths joining them have homotopies between them. The space $\mathbb{R}^2$ is simply connected. If you take out a hole in the middle, it isn't, because there's no homotopy between two paths that go around the hole in different ways.

Remark 3.13. One of the lines of the song is "When we first met, we simply connected". There's no math joke here, it's just a pun.

4 Set theory (July 23–30)

separable. *Also: countable.* Consider the statement "the intersection of any number of open sets is open." We can try to prove this by induction on the number of sets. When you have $n = 1$ set, then it's open. Otherwise, you can take the intersection of the first $n - 1$ sets, which is open by inductive hypothesis, and you only need to show that the intersection of two open sets is open.

Exercise 4.1. Prove that the intersection of two open sets is open! Think of the "challenge" definition. Let's say I pick a point in the intersection of two open sets, and you need to give me an ϵ that works. How can you use the fact that the original sets were open, to find one that works?

Of course, this statement isn't actually true, because it's not true for an infinite number of sets! Indeed, the sets $\left(-\frac{1}{n}, \frac{1}{n}\right)$ are all open, but their intersection is just $\{0\}$, which isn't open.

This example shows that things get tricky when we jump from finite to infinite. A large part of set theory is about dealing with infinity, and what happens when you deal with really large things. And part of that is counting, and labeling the sizes of sets. We say a set is **countable** if it is finite, or if there is a bijection between it and the natural numbers.

As an example, the integers and the rational numbers are all countable, and so is "all numbers that can be described with a single sentence". We'll explain why fully in class, but the basis of the proof is why the rationals are countable°. The real numbers are uncoutable, which we'll show later.

And completely unrelated to any of that, but because I have to define it anyway, a metric space is **separable** if it contains a countable, dense subset. The space $\mathbb{R}$ with the absolute distance metric is separable because it contains $\mathbb{Q}$. The discrete space is never separable, no matter how big you make it.

Remark 4.2. The reason it's called "separable" is because you can imagine this countable, dense subset, as "separating" the space. For example, in $\mathbb{R}$, any two real numbers are "separated" by a rational number.

Remark 4.3. This is somewhat ingenious, as I'm pretty sure the "purely inseparable" in the song refers to a purely separable extension°, as in field theory. But I don't have time to develop fields, and this is close enough, that I'm fine with the lie.

class. *Also: power set.* As I said, a large part of set theory is about dealing with infinities. Part of the reason why that's tricky is because dealing with infinities can lead to weird questions about "what is a set?"

I promised a proof of why the real numbers aren't countable, and the reason is Cantor's paradox. Given a set S, let 2^S be its **power set**, or the set of its subsets. Cantor's diagonal argument says that there's never a surjective function $f : S \to 2^S$. If we did, what goes wrong?

The idea is to imagine a table, with the elements of S going down the rows and columns. Each row corresponds to applying f to that element, say x. It results in a subset of S, so across that row we write 1s or 0s, corresponding to whether the element in the column appears in $f(x)$ or not. Then we "invert" the diagonal to get a new subset, which can't be in this list by construction. A similar argument shows that there's no surjective function from $\mathbb{N}$ to $\mathbb{R}$, which shows that the real numbers aren't countable.

Why is this important? This means that we can't just define a set as "any collection of objects". Because if this was a set, which we can call V, then V would contain each of its subsets. But that would mean that there's a surjective function from V to 2^V, contradiction! That means V can't be a set. This is Cantor's paradox.

If V isn't a set, does it even exist at all? Well, we can clearly *define* V, so it has to, right? And if it's not a set, what is it? For convenience, we call it a **class**. It's the collection of sets which satisfy some property, in this case, being a set. It's not a set itself, as that leads to the size issues we talked about, but set theorists find the need to work with classes anyway.

axiom of choice. *Also: axiom, well-ordering theorem.* We just talked about how we can't just say sets are collections of objects. If so, then what *are* sets? In the twentieth century, mathematicians working on foundations gave the widely-agreed upon answer that we use today: a set is something that can be built from a certain list of rules, which we call **axioms**.

These include rules like "the empty set is a set" and "we can take unions of sets" and so on. The list of axioms most mathematicians agree to use is called ZFC, which stands for the Zermelo–Fraenkel with choice. As you can tell from the name alone, this "choice" axiom is apparently important enough to get its own letter in the acronym! We use ZF to refer to the ZFC axioms without choice.

The **axiom of choice** says that given a set of non-empty sets, you can pick an element out of each set, and make a new set. The typical example is to imagine lots of drawers with socks. The axiom of choice says that you can pick a sock from each drawer. If it sounds simple to you, then in a sense, it is—it only gets complicated when you deal with infinite things.

That's because the axiom of choice is equivalent to this axiom called the **well-ordering theorem**. A well-ordering of a set is a way to define "less than" on its elements, such that every subset of the set has a least element, according to this "less than". The well-ordering theorem says that every set has a well-ordering.

Remark 4.4. Here, equivalent means that you can prove one given the other. More precisely, if you take the axioms of ZF, you can prove that the well-ordering theorem implies the axiom of choice, and that the axiom of choice implies the well-ordering theorem.

The natural numbers, for example, have a well-ordering given by $<$. The integers aren't well-ordered by $<$, because the set of negative integers doesn't have a least element. On the other hand, they *are* well-ordered by an ordering like "the smallest absolute value, but in the event of a tie, the negative number is smaller". Those make sense—but what about something like the real numbers? The well-ordering theorem tells us that *this* is well-ordered too, which I find harder to believe.

Exercise 4.5. The axiom of choice and well-ordering theorem aren't as controversial on countable sets. Convince yourself that the rational numbers are well-ordered by coming up with a well-ordering. But don't try too hard to come up with one for the real numbers—it can be proven that there's no formula that describes one, even if one exists.

chain, upper bound. *Also: poset, maximal element, Zorn's lemma.* The axiom of choice and well-ordering theorem are both equivalent to a third theorem, called Zorn's lemma. The statement is a bit complicated: "if every chain in a poset has an upper bound, then it has a maximal element." We'll explain what those words mean.

Remark 4.6. There's a classic joke about how the three are equivalent, which I've heard attributed to Jerry Bona: "The axiom of choice is obviously true, the well-ordering thoerem is obviously false, and who can tell about Zorn's lemma?"

A **poset**, short for partially-ordered set, is a set with a relation satisfying certain properties. The relation has to be reflexive, so (x, x) is always in the relation. It must be anti-symmetric, which means that if (x, y) and (y, x) are both in the relation, then (x, x) is too. And it must be transitive: if (x, y) and (y, z) are in the relation, so is (x, z). We typically write this relation with a $\leq$ sign, but note that it's not exactly the same as $\leq$ over numbers.

The typical example of a poset is the "is a factor of" relation on the positive integers, that we talked about way, way earlier. It's not necessary that, given two integers, one is a factor of the other—that's what puts the "partial" in "partially-ordered". Other examples are "is less than or equal to" over the real numbers, or the "is a subset of" relation, over the subsets of a given set. We'll talk about the "is a factor of" poset as an example for the rest of this section, but in class, we'll draw pictures of *Hasse diagrams*, which are a way to visualize smaller posets.

A **chain** is a subset of a poset, whose elements can all be compared with each other. For example, $\{2, 8, 24, 1, 72\}$ is a chain. Chains can be infinite, like $\{1, 2, 4, 8, \dots\}$. An **upper bound** of a chain is an element u, such that for each element c in the chain, (c, u) is in the relation. The second chain we gave doesn't have an upper bound, but the first chain has several, like 72 or 144.

A **maximal element** of a poset is an element m, such that (m, M) isn't in the relation for any M. Our "is a factor of" poset doesn't have any maximal elements. Finally, **Zorn's lemma** says that if every chain in a poset has an upper bound, then there has to be some maximal element.

Exercise 4.7. Two lines of the song are "You're the upper bound in the chains of my heart / You're my axiom of choice, you know it's true". What's the joke here? Do you find it funny?

5 Linear algebra (July 30–August 6)

map, operator. *Also: vector space, linear, vector, scalar.* A **vector space** (over $\mathbb{R}$) is a set where you can add any two elements, and you multiply them by real numbers.

An example are the real polynomials with degree at most two. You can add two quadratics to get another quadratic, and you can multiply a quadratic by a real number to get another quadratic. The important property is that these *commute*, so that $2(x^2 + 2x + 4) + 2(-3x + 1)$ is the same as $2(x^2 + 2x + 4 - 3x + 1)$.

Specifically, a vector space is an operation $+$ that makes the set V an abelian group, and a function $\cdot : \mathbb{R} \times V \to V$ such that, for $k, \ell \in \mathbb{R}$ and $u, v \in V$:

- $k(u + v) = ku + kv$ and $k(\ell v) = \ell(kv)$,
- $(k + \ell)v = kv + \ell v$,
- $1v = v$ and $0v = 0$. The 0 on the right is the identity for the group over V.

The elements of a vector space are called **vectors**, and the real numbers are called **scalars**. The important condition is the first one, which means that multiplication is **linear**.

The most important vector space over $\mathbb{R}$ is $\mathbb{R}^n$, which is n copies of $\mathbb{R}$. The vector $(1, 2, 4)$ is an element of $\mathbb{R}^3$. Adding it to the vector $(2, -3, 5)$ gives the vector $(3, -1, 9)$. Multiplying this sum by $\frac{1}{3}$ gives us the vector $(1, -\frac{1}{3}, 3)$. Note that this is kinda the same as our vector space of quadratics earlier, but written differently.

Remark 5.1. In a deep sense, $\mathbb{R}^n$ is the only "finite-dimensional" vector space over $\mathbb{R}$. There are many infinite-dimensional vector spaces, like the polynomials with real coefficients, or the functions from $\mathbb{R} \to \mathbb{R}$.

A **linear map** is a function from one vector space to another that is also linear. That means that if $f : U \to V$ is a linear map, then for any $u, v \in U$ and $k \in \mathbb{R}$,

$$f(u + v) = f(u) + f(v) \text{ and } f(kv) = kf(v).$$

An example of a linear map from $\mathbb{R}^3 \to \mathbb{R}^2$ takes (a, b, c) to $(a + 2b + 4c, 0)$. Another example is from the quadratic polynomial vector space earlier to itself, which takes $ax^2 + bx + c$ to $cx^2 + bx + a$. When the domain and codomain of the map are the same, we call it a linear **operator**.

Remark 5.2. The terms *map* and *operator* are, in general, other names for *function*. The continuous functions between metric spaces are better known as *continuous maps*. Another word that's a synonym is *morphism*, and homomorphisms, isomorphisms, and homeomorphisms, are all kinds of morphisms. Some people will make distinctions, but I think they all mean the same thing. That's why when the song mentions the "smoothest operator", it just refers to a smooth function.

rank. *Also: subspace, dimension.* A **subspace** is, you guessed it, a subset of a vector space that's also a vector space. An example of a subspace in $\mathbb{R}^3$ is the set of all $(0, k, 0)$ vectors for $k \in \mathbb{R}$. Check that it's a vector space: you can add two vectors, and you can multiply by scalars. (We don't need to check for linearity, as that's covered by the parent space.)

A subtler example of a subspace is the set of all (a, b, c) vectors such that $a + 2b + 4c = 0$. Agan, you can check that adding two vectors in this subspace stays in the subspace, and so does multiplying by scalars. Another important fact is that this is the kernel of the linear map taking (a, b, c) to $a + 2b + 4c$, and in general, the kernel of a linear map is always a subspace.

The **dimension** of a vector space is how many $\mathbb{R}$-subspaces it's made out of. $\mathbb{R}^3$ has dimension 3, and so does the quadratic polynomial vector space. The space of all $(0, k, 0)$ vectors, for $k \in \mathbb{R}$, has dimension 1. The space of vectors (a, b, c) satisfying $a + 2b + 4c = 0$ has dimension 2, because it's made out of the space of all $(-4c, 0, c)$ and $(-2b, b, 0)$ vectors.

A linear map gives us two important subspaces. We've already seen that the kernel is a subspace, but so is the image, from the fact that a linear map is linear. The **rank** of a linear map is the dimension of its image. We'll draw a nice picture in class of the important *rank-nullity theorem*, which will be useful for this exercise:

Exercise 5.3. Three lines of the song go "I'm living in the kernel of a rank-one map / From my domain, its image looks so blue / Cause all I see are zeroes, it's a cruel trap". If you're in a rank-one map, why would its image look so blue (at least compared to maps with higher ranks)? If you're in the kernel of a map, why would you only see zeroes?

tensor, complexification. *Also: tensor product, dual space.* A **tensor product** is a way to glue two vector spaces V and W together. The elements of $V \otimes W$ are just the set of elements $v \otimes w$, treated as a vector space. The elements are only different up to multiplication by a scalar, so for $k \in \mathbb{R}$, $k(v \otimes w) = (kv) \otimes w = v \otimes (kw)$.

Consider the vector space V of polynomials that are at most degree 2, and the vector space W of polynomials that are at most degree 1. The tensor product is also linear in both of its arguments, which allows us to do calculations like this:

$$\begin{aligned}(x^2 + 2x + 3) \otimes (2x + 1) &= x^2 \otimes (2x + 1) + 2x \otimes (2x + 1) + 3 \otimes (2x + 1) \\ &= x^2 \otimes 2x + x^2 \otimes 1 + 2x \otimes 2x + 2x \otimes 1 + 3 \otimes 2x + 3 \otimes 1 \\ &= 2(x^2 \otimes x) + (x^2 \otimes 1) + 2(x \otimes x) + 2(x \otimes 1) + 6(1 \otimes x) + 3(1 \otimes 1).\end{aligned}$$

If this looks an awful lot like polynomial multiplication, you'd be right! The difference is that the tensor product doesn't care about what V and W actually *mean*. The only property of the tensor

product is that it's linear and it floats scalars. For example, $x \otimes 1 \neq 1 \otimes x$.

The elements of a tensor product are called **tensors**. The point of tensors is that they represent linear maps. As an example, note that the set of linear maps $\mathbb{R}^3 \to \mathbb{R}$ is also a vector space. We call this the **dual space** of $\mathbb{R}^3$, and write it as $(\mathbb{R}^3)^\vee$

Exercise 5.4. Convince yourself this is true! Every linear map $\mathbb{R}^3 \to \mathbb{R}$ takes (a, b, c) to $ka + \ell b + mc$, for some $k, \ell, m \in \mathbb{R}$. How do you add two linear maps? How do you multiply by scalars? Is multiplication linear?

Now consider the linear map $\mathbb{R}^3 \to \mathbb{R}^2$ that takes (a, b, c) to $(a + 2b + 4c, 4a + 2b + c)$. This is really just two linear maps $\mathbb{R}^3 \to \mathbb{R}$, one that goes (a, b, c) to $a + 2b + 4c$, and another that goes (a, b, c) to $4a + 2b + c$, but glued together. If you tensor the first linear map with $(1, 0)$ and the second linear map with $(0, 1)$, you end up with a linear map from $\mathbb{R}^3 \to \mathbb{R}^2$.

The **complexification** of a vector space V is $V \otimes \mathbb{C}$, but instead of multiplying by just real numbers, we also allow multiplying by complex numbers. Complexifying $\mathbb{R}^n$ gives the vector space $\mathbb{C}^n$, where you can add two vectors and multiply vectors by complex numbers.

6 Differential geometry (August 6)

wedge, form. The **wedge product** of a space V with itself is $V \otimes V$, except instead of $\otimes$ we write $\wedge$, and we have one extra condition: $v \wedge v = 0$. We write it as $\Lambda^2(V)$.

Exercise 6.1. Using this condition, show that $v \wedge w = -w \wedge v$. To do this, start with $(v+w) \wedge (v+w) = 0$, then use the fact that $\wedge$ is linear on both sides.

Here's the reason why we care about the wedge product. Consider $\mathbb{R}^2$, and let's rewrite the wedge product of two vectors $(a, b) \wedge (c, d)$ in terms of just $(1, 0) \wedge (0, 1)$:

$$\begin{aligned}(a, b) \wedge (c, d) &= ac((1, 0) \wedge (1, 0)) + ad((1, 0) \wedge (0, 1)) + bc((0, 1) \wedge (1, 0)) + bd((0, 1) \wedge (0, 1)) \\ &= (ad - bc)((1, 0) \wedge (0, 1)).\end{aligned}$$

What is $ad - bc$? It's the area of a parallelogram formed by the vectors (a, b) and (c, d). I'd add a picture here, but I'm not going to draw pictures, go to class!

Exercise 6.2. Fill in the missing steps in the above calculation.

We can also generalize the wedge product to $\Lambda^n(V)$ in general, but that won't be important to us. The important cases are $n = 0$, which is the empty vector space, $n = 1$, which is V, and $n = 2$, which we saw.

An **n-form** over a vector space V is a smooth function from $V \to \Lambda^n(V^\vee)$, where here, $V^\vee$ is the dual space. Let's take $V = \mathbb{R}^3$. Recall that the dual space is the space of functions $\mathbb{R}^3 \to \mathbb{R}$. So a 1-form over $\mathbb{R}^3$ takes each point in the space and maps it to a function from $\mathbb{R}^3$ to $\mathbb{R}$. And a 2-form maps each point to something that can be represented as the "area" spanned by two such functions. It's, uh, the algebraic definition isn't great without more details.

Exercise 6.3. At least this explains the pun "But then you drove a wedge between our 2-forms". Attempt to find humor in this line.

The geometric definition is better. A differential form is something you can sum over. If you have a 0-form on $\mathbb{R}^3$, and you have a bunch of points, the 0-form takes each point to a real number, and then you can sum over them.

If you have a 1-form on $\mathbb{R}^3$, and you're walking along a curve, then along each point in the curve you have a vector representing where you're facing. That vector is also in $\mathbb{R}^3$. The 1-form takes where you're standing to a function from $\mathbb{R}^3$ to $\mathbb{R}$, so by plugging in the direction you're facing, you get a real number. There are a bunch of real numbers along the path you walk, and you can sum over them. And then a 2-form allows you to sum over a tiny area.

Remark 6.4. Technically, I should be saying "integrate over" instead of "sum over". A 1-form is something like $f(x)\,dx$, which takes a point x and returns a function that takes a facing direction, dx, and returns a real number, $f(x)\,dx$. Except, not really. I don't understand it myself.

principal bundle. *Also: vector bundle, frame bundle.* We've now thought about a 1-form, which we can think of as assigning each point in V a vector in $V^\vee$. Really, an n-form is a way to take a vector space as a "geometric" object, and to each point attach something "algebraic" on it, in this case, a function in the wedge product of the dual space. This is similar to the idea behind bundles.

A **vector bundle** is a bundle involving vector spaces. It takes a geometric object, in our case, a metric space, and to each point in the metric space attaches a whole *vector space*. Yes, that's right, an entire vector space. The requirement is that the vector space changes continuously along the metric space, whatever that means.

For example, consider the boundary of the unit circle in $\mathbb{R}^2$ as a metric space. We can attach to each point of the unit circle a copy of $\mathbb{R}$, pointed in different directions. There are two different ways to do so: one gives a cylinder-like thing, and one gives a Möbius-strip-like thing. Another important example of vector bundles are tangent bundles, like attaching $\mathbb{R}^2$ to each point on the surface of a sphere in a way that doesn't intersect the sphere again.

In a **principal G-bundle**, the algebraic thing we attach is a group G. "But CJ," you ask, "how is it possible to place a group in space?" Well, if you follow along each element of the group, you get a copy of the original metric space. The group is important because it allows us to "multiply" each of these copies with an element of the group, mapping it to another copy.

Consider the group $\mathbb{Z}/2\mathbb{Z}$, and let's think about possible $\mathbb{Z}/2\mathbb{Z}$-bundles over the boundary of the unit circle. You have two circles. Applying the identity to each circle gives the same circle, applying the other element maps it to the other one. How are the circles related? They can "twist" around each other in space, as long as it's continuous. This leads to two possible structures again: a cylinder-like thing, and a Möbius-strip-like thing. I promise this will make more sense once we make some drawings in class. This kind of principal bundle is called a **frame bundle**, and in particular, it's the frame bundle of the vector bundle we talked about earlier.

Exercise 6.5. One line of the song goes "A principal love bundle sitting deep inside". This implies that the narrator's love for the other person forms a group. Which group would it be? What do you think a principal love bundle over a metric space would look like?

stable equivalence. Recall what it means to take the tensor prodcut of two vector spaces: it's gluing them together. In a similar way, we can take the tensor product of two vector bundles over the same metric space, by taking the tensor product of vector spaces at each point in the metric space. Two vector bundles are in a **stable equivalence** if, after tensoring them by $\mathbb{R}^k$ for some k, they become isomorphic.

Remark 6.6. If it wasn't already clear since the beginning of this section, I don't actually know any differential geometry, and so I don't know how to explain this well. Oops! As the title of the class said, no promises about the math.

7 Category theory (August 6–August 13)

directed system. *Also: category, compose.* The point of category theory is to take many different mathematical objects we've been studying, and find a way to describe them that generalizes over them all. It comes from the realization that, in many cases, we care just as much, if not more, about *how* objects talk to each other, rather than the objects themselves. For example, consider the isomorphism: it's a concept that applies in multiple places, and in each place, it's kinda the same thing. In fact, isomorphisms aren't really about the objects; they're about the maps between them.

In a **category**, we have a class of objects, and for any pair of objects, a class of maps between them. (I'm using *class* to be technical, but you can replace it with *set* if you want.) Further, we can **compose** maps: if you have a map $f\colon A \to B$ and a map $g\colon B \to C$, you can make a map $gf\colon A \to C$. Each object has an identity map to itself, and composing a function with any identity map gives the same function.

Note that we're defining an identity map with respect to how it works with other maps. In fact, that's the *only* way to define an identity map, because we can't look "inside" the objects to find out what an identity is. Again, that's the point of category theory: we're looking at the maps, not the objects.

Some examples:

- There's a category of objects, called Grp. The objects are groups, the maps are homomorphisms, and composition is function composition.
- There's a category of metric spaces, called Met. The objects are metric spaces, the maps are continuous functions, and composiiton is function composition.
- There's a category of vector spaces, called Vect. The objects are metric spaces, the maps are linear maps, and composition is function composition.
- There's a category of sets, called Set. The objects are sets, the maps are *any* functions, and composition is function composition.

Now, an *isomorphism* between two objects A and B, in *any* category, is a map $f\colon A \to B$, such that there exists a map $g\colon B \to A$, such that gf is the identity on A, and fg is the identity on B. See how we unified so many definitions into a single, category-theoretic construction?

Note that the information in a category isn't just the objects and their maps. The most important information is actually how they compose! Composition gives us information: we can specify that two maps compose to a given map.

Exercise 7.1. The classic joke about this is that any group is a one-object category where every map is an isomorphism: the elements of the group corresond to the maps. Convince yourself that this is true.

For completion's sake, I also have to give the definition of a directed system, but it won't be super relevant to our discussion. Suppose you had a poset S and a category C. A **directed system** is a set of objects A_i, where i ranges over S, with a morphism $f_{ij} \colon A_i \to A_j$, such that if $i \leq j \leq k$ then they compose in the way you'd expect them to.

free. *Also: commutative diagram, universal construction.* If for some reason you wanted to think about the "inside" of an object, there's a way around that. It's to consider maps between a special kind of object to that object. For example, consider the set with one element in Set. (There are many sets with one element, but they are all isomorphic.) A map from the set with one element "points to" a single element in another set.

Or as another example, consider $\mathbb{Z}$ in Grp. How do you construct a homomorphism from $\mathbb{Z}$ to a group? Well, 0 has to go to the identity. And 1 has to go to some element. But as soon as you've decided where 1 goes, you've decided where every other element in $\mathbb{Z}$ goes to. Thus, a map from $\mathbb{Z}$ to a group is determined by a single element in the group, and we can think of this as "pointing to" a single element.

As another example, think of the discrete space with one element, in Met. These kinds of objects, which point to a "single thing" inside an object, are all **free** objects.

Exercise 7.2. What about the discrete space with two elements? What are the continuous maps from that space to another metric space?

What do all these free objects have in common, however? Let's think about $\mathbb{Z}$ in Grp again. Consider a diagram, where we draw a set with one element, a map from this set to $\mathbb{Z}$, and a map from this set to some group G. Here, these are maps in Set, but don't worry about that just yet.

We want to interpret the second map as "pointing to" a single element in G. But we can only talk about maps, right? So what's the corresponding map in Grp that goes from $\mathbb{Z}$ to G? There are several, but there's only one that composes with the inclusion to give the same result. There's only one map that makes this a **commutative diagram**. That's what makes $\mathbb{Z}$ a free object: there's only one map that makes the compositions the same no matter what. If there were two elements, the corresponding free object is called F_2, "the free group generated by two elements".

In general, we can draw diagrams and say that they *commute* if, no matter what order you follow the arrows in, you get the same result. Thinking about making things commute allows us to specify some kinds of properties nicely. For example, if you had a set S in Set, and a map $f \colon S \times S \to S$, you can draw a diagram expressing what it means for f to be *associative*. So now, associativity, which we used to talk about with respect to elements, can actually be defined just in terms of arrows! That's why commutative diagrams are so important in category theory: forcing things to commute is what allows us to define things more specifically, especially when we have "so little" to work with.

To make an object by showing it's something that makes a diagram commute, in a specific way, is to do a **universal construction**. We just showed the universal construction for free objects. We can also do a universal construction of what a product is, which allows us to talk about $A \times B$ in more categories than just Set.

The idea is that we care about the projections of $A \times B$ to A and B. These projections are maps, p_A and p_B, that take a pair and return the first or second element. If we can only talk about maps, how do we characterize the maps that go through $A \times B$? Suppose we had a set S and a map $f\colon S \to A \times B$. Well, we have a map $p_A\colon A \times B \to A$, so we have a map $p_A f\colon S \to A$, and similarly a map $p_B f\colon S \to B$. Of course, given any set S, there are always going to be maps to A and maps to B. But $A \times B$ has a special property that you can go *in reverse*: if you had S with maps $q_A\colon S \to A$ and $q_B\colon S \to B$, then there's only one way to map from S to $A \times B$ to make everything commute nicely. In a way, that's the "most universal way" to map to A and B, the way to do it without losing information.

We can call an object $A \times B$ if it has two maps, $p_A\colon A \times B \to A$ and $p_B\colon A \times B \to B$, such that for any other object S with maps $q_A\colon S \to A$ and $q_B\colon S \to B$, there exists a *unique* map $f\colon S \to A \times B$ such that everything commutes.

Exercise 7.3. Prove that all the objects that satisfy these properties are ismoprhic. The proof is similar to what we did to show a group has only one identity element. Thus, we can always talk about "the" product.

functor, forgetful, faithful. We earlier wanted to talk about mapping *between two categories*, when defining free objects. The way to do this is a **functor**, which is a map between two categories. We can make a functor $F\colon \mathsf{Grp} \to \mathsf{Set}$. This functor takes objects in Grp to objects in Set, and maps in Grp to maps in Set. This means functors also carry diagrams to diagrams. So now, we can talk about "a map between $\mathbb{Z}$ to G in Set", which corresponds to a map between $\mathbb{Z}$ to G in Grp, that the functor takes to a map to their images in Set.

Now in Set we can draw what we want to happen. We have a set S with one element, we have $F(\mathbb{Z})$, and we have $F(G)$. We also have a map from S to $F(\mathbb{Z})$, and a map from S to $F(G)$. Once again, there are multiple maps between $F(\mathbb{Z})$ to $F(G)$, except this time, there are multiple maps that even make the diagram commute. But only one of these maps is in the image of F. That's the universal property that free objects have: they're an object such that there's only one map that makes this diagram commute.

Our map from Grp to Set is an example of a **forgetful** functor: it "forgets" some of the information in Grp. There's no formal definition for a forgetful functor. Another kind of functor is a **faithful** functor, which is a functor that's surjective on diagrams.

Exercise 7.4. One line of the song goes "The faithful image that I map into". If you were a faithful functor, what would your image map into? The line before that talks about "quotienting out" this image. If you quotient out a faithful image, what's left?

limit. *Also: n-category, natural transformation, discrete category, cone.* If you thought category theory was already pretty meta, it's about to get more meta.

Remark 7.5. Here, "meta" is an adjective that describe something that describes itself, or is somehow self-referential. I can write essays about penguins, and that's just an essay. If I write an essay about how I write essays, that's meta. Category theory is doing math on math, which is pretty meta.

Remember when we talked about homotopy? You have points, and then you have paths between

points. Then you also have homotopies, which are like paths between paths. Well, in a 2-category, you have objects, and you have maps between objects. But you also have 2-maps, which are maps between maps.

In an n**-category**, not only do we have objects and maps, but we have 2-maps between maps, and 3-maps between 2-maps, and so on up to n. A 0-category just has objects and no maps, a 1-category is what we've been discussing so far.

Now, the class of categories actually forms a category in itself, called Cat. The objects are categories and the maps are functors between them, and each category has an identity functor. In the 2-category version of Cat, we have maps between maps, and those maps are called **natural transformations**. Then 3-maps in Cat are called modifications, which is a name I've barely heard used. There are no more names after that, because mathematicians don't count higher than 3.

What do natural transformations look like? A natural transformation n must be between one functor and another, let's say $F\colon \mathsf{C} \to \mathsf{D}$ and $G\colon \mathsf{C} \to \mathsf{D}$. Then these functors would, say, take a map $f\colon A \to B$, in C, to two maps in D, which are $F(f)\colon F(A) \to F(B)$ and $G(f)\colon G(a) \to G(b)$. Then a natural transformation takes $F(A)$ to $G(A)$, and $F(B)$ to $G(B)$, and it must commute in the natural way. In other words, a natural transformation specifies maps between images of functors, and require them to commute.

What are the free objects in Cat? Let's think about the one pointed to by a one-element set for now. It's a category that'll have one object. It has one map, the identity. And that's it. This category is called $\mathsf{1}$. Now the way we can talk about a specific object in a category is by giving a functor from $\mathsf{1}$ to this category. Similarly, we have the categories $\mathsf{2}, \mathsf{3}, \ldots$. These are called **discrete categories**, in analogy to discrete space.

Consider two functors from $\mathsf{2}$ to Set. The first, F, has each object in $\mathsf{2}$ point to two distinct sets A and B, respectively. The second, Δ_S, has both objects point to some set S. Now, is there a natural transformation between these two functors? Well, it would have two parts: a map $q_A\colon S \to A$ and a map $q_B\colon S \to B$. This is now similar to the setup of the universal construction for a product.

Say you replaced $\mathsf{2}$ with a different category, say J, and you have a functor $F\colon \mathsf{J} \to \mathsf{C}$ and a functor $\Delta_S\colon \mathsf{J} \to \mathsf{C}$, and a natural transformation that works. This is called a **cone**. A **limit** is a universal cone, so you can think of it as a big generalization of a product. I refuse to explain further, mostly because I don't understand any of this myself.

Remark 7.6. Two of the lines in the song go "Our system was already directed / To have a finite limit in some sense". Now that we've seen what a directed system and a limit are, we can understand that these two line didn't refer to anything mathematically, they were just puns on their names.

8 Proof (August 13)

proof. Believe it or not, we're done with the mathematical content of this course. For some parting words, I'll talk a bit about the philosophy behind math.

What is a **proof**? It's not enough to say it's just a convincing argument, because then you have to ask: convincing to whom? One might go all the way and just say a proof is just a matter of convincing the person you're talking to that something is true. That perhaps proof, in math, is just like science, which is a continuous process of updating our knowledge and broadcasting our results to each other and replicating results when we aren't convinced. But that's not enough to account for how the mathematics community, as a whole, disagrees on so little things, compared to other fields.

On the completely opposite side, one might say that a proof is a series of steps that a computer

can follow along step-by-step to check that something is true. We can imagine a computer that's loaded all the definitions and rules, and whenever you write a proof you have to specify which rule you're applying and how, much like the boring two-column proofs I did in geometry back in high school. But that's not how we write proofs, isn't it?

I won't answer this question fully here, but that's something to think about.

without loss of generality. Mathematicians like repeating certain phrases, like **without loss of generality**. We've used this phrase ourselves, several times. For example, when we talked about groups with two elements, which are named a and b, we said, "without loss of generality, assume the identity element is a." This means that even if we're assuming that it's a, and not b, it'd still work the other way around—we'd just have to swap a and b through our proof. As another example, if we wanted to prove something like $x^2 + y^2 \geq 2xy$ for all real numbers x and y, we could say, "without loss of generality, assume $x \geq y$."

We like abbreviations, so sometimes we abbreviate that with WLOG, especially when writing on blackboards. Other abbreviations include FTSOC or FSOC, "for the sake of contradiction", NTS or WTS or WTP or whatever variation, which is "need to show" or "want to show" or "want to prove", TFAE, "the following are equivalent", and WRT, "with respect to".

QED. One abbreviation is **QED**, short for *quod erat demonstrandum*, Latin for "which was to be demonstrated". It's a way to say, "I've proven what I needed to prove, and I'm done," mic drop. It's rarely used in actual writing these days, even on blackboards. Instead, people end proofs with things like □ or ■, a symbol called the halmos. These days, you only say QED if you're trying to sound fancy after ending an argument. Although if you're trying to be funny, I like WWWWW instead, for "which was what we wanted".

proposition, corollary. *Also: theorem, lemma.* The trifecta of higher math classes and textbooks is definition, **theorem**, proof. You go over a definition, you go over a theorem, you go over its proof, and then repeat. We've talked about being well-defined (all the way in the first week!) and we just talked about proof. A theorem is just a statement that can be proved.

But perhaps I'd classify them as **propositions** instead. A proposition is what some people use to refer to a smaller theorem. It's a result that's not quite as important, not enough to get the big "theorem" title. But it stands alone, and is important in its own right.

An even smaller proposition would be a **lemma**. These results are small enough that they're often used in the proof of a proposition or two, and then not referred to again. On the other hand, the naming for these vary a lot. Some things are called lemmas only because their proof is short. While other things are called lemmas because their result is useful for *much* more than a proof or two. The ones that come to my mind include Bézout's lemma, the Borel–Cantelli lemma, Farkas's lemma, the fixed-point lemma, the Lovász local lemma, Schur's lemma, the snake lemma, the Yoneda lemma, and of course Zorn's lemma.

A **corollary** is a statement that follows directly-ish from a theorem, but is useful or notable enough to be called out in its own right. The Pythagorean theorem, for example, could be considered a corollary of the law of cosines. What is considered to be "directly-ish" following from a theorem is not clear-cut, though.

Exercise 8.1. The last stanza mentions "I've proved my proposition now, as you can see / [...] / And by corollary, this shows you and I to be / Purely inseparable, QED." Why is this funny?

9 Conclusion (August 13)

There's so many things I wanted to cover, which I didn't not only because we didn't have the time, but also because I don't know about them myself. If you took the time to fully understand every concept we dicussed in class, you'd be well on your way to getting a higher math education. If you're interested in learning more, here's some references.

- General:
  - An Infinitely Large Napkin°. Roughly follows the same philosophy of higher math for high-school students. Using the chapter numbering in v1.5.20220708, our group theory covers chapters 1 and 3, and a bit of 17. Our topology covers chapter 2, and a bit of 6 and 7. Our set theory overlaps with chapter 81. Our linear algebra covers chapters 9, 11, and a bit of 12. Our differential geometry kinda covers chapter 43, but not really? Our category theory kinda covers chapters 60 to 62.
  - The Princeton Companion to Mathematics°. A fantastic book I wish I'd read earlier, and the one I wish I'd written. You should now be familiar with enough to read around half of the book. I find it way more accessible than other general math texts like Wikipedia or MathWorld. Both are great, it's just that this book is outstanding.
- Group theory:
  - Visual Group Theory°. The one book that finally got me understanding quotients. If you only read one book in this list, read this one, please! To discuss groups without drawing pictures is to not do it justice.
  - Tim Gowers's posts on quotient groups° and group actions°. These are pretty good.
  - Algebra, Artin°. It's the book I first learned much of my abstract algebra from, because it's a standard textbook. It's okay.
- Metric topology:
  - Real Mathematical Analysis°. Despite the name, I've only ever read this book for the topology parts, and never the analysis parts. You have my permission to only read chapter 2.
  - A Course in Metric Geometry°. Has grad students as an audience, but the first two chapters are relatively accessible.
  - Topology, Munkres°. Like Artin, it's a textbook. It's okay. It starts with general point-set topology rather than the metric topology we've developed. This is more standard, but I also find it harder to draw pictures of.
- Set theory:
  - Logic as Mathematics. This is an upcoming textbook by Henry Cohn. It is the best undergraduate math textbook I've ever read, and its first chapter is among the best first chapters across all math books I've ever read. I realize it's weird to recommend a book that hasn't come out yet, but it's great.
  - Naive Set Theory°. If Cohn's book is the best set theory textbook I've read, this is second best. Doesn't have as much about logic, but it does cover the set theory stuff we've discussed.
- Linear algebra:

  - Linear Algebra Done Wrong°, Linear Algebra Done Right°. As their titles suggest, the two books complement each other well. If you like the abstractness of group theory, and want more abstract stuff, read LADR first. If you're literally anyone else, read LADW first. But I'd recommend reading both.
  - A (Terse) Introduction to Linear Algebra°. If not for its prerequisites, this would be my top recommendation. A little knowledge in abstract algebra makes studying linear algebra a bit more motivated, which this book follows in stride.

- Differential geometry:
  - I don't actually know any differential geometry, and can't make recommendations here. Maybe check this MathOverflow question°? I might read Introduction to Smooth Manifolds° next.

- Category theory:
  - Conceptual Mathematics°. Get the second edition if you can. If you don't have the prerequisites for my other recommendations, then read this.
  - Basic Category Theory°. My top recommendation if you *do* have the prerequisites for it. I think category theory might be better learned after you know enough algebra anyway.
  - Category Theory for Programmers°. Probably my favorite treatment of categories... if there weren't so many examples in C++. Best if you have more programming than math experience.

- Philosophy of mathematics:
  - The Mathematical Experience°. This is a big book, but it's one of the few on this list I've read cover to cover. I still read it again, from time to time. It's just that good.
  - Letters to a Young Mathematician°. You might've heard of Hardy's A Mathematician's Apology. I think this is the better version.

10 Lyrics

The path° of love is never smooth°
But mine's continuous° for you
You're the upper bound° in the chains° of my heart
You're my axiom of choice,° you know it's true

But lately our relation's° not so well-defined°
And I just can't function° without you
I'll prove° my proposition° and I'm sure you'll find
We're a finite° simple° group° of order° two

I'm losing my identity°
I'm getting tensor° every day
And without loss of generality°
I will assume that you feel the same way

Since every time I see you, you just quotient° out
The faithful° image° that I map° into
But when we're one-to-one° you'll see what I'm about
Cause we're a finite simple group of order two

Our equivalence was stable°
A principal love bundle° sitting deep inside
But then you drove a wedge° between our two-forms°
Now everything is so complexified°

When we first met, we simply connected°
My heart was open° but too dense°
Our system was already directed°
To have a finite limit°, in some sense

I'm living in the kernel° of a rank-one° map
From my domain°, its image looks so blue
Cause all I see are zeroes, it's a cruel trap
But we're a finite simple group of order two

I'm not the smoothest operator° in my class°
But we're a mirror pair°, me and you
So let's apply forgetful° functors° to the past
And be a finite simple group, a finite simple group
Let's be a finite simple group of order two
(Why not three?)

I've proved my proposition now, as you can see
So let's both be associative° and free°
And by corollary,° this shows you and I to be
Purely inseparable,° QED°