Last time, given a set of sets, for example the set $\{\{1,2,3\},\{4,5,6\},\{7,8\}\}$ or the set $\{\mathbb{Z}_{\geq 1},\mathbb{Z}_{\geq 0},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}\}$, I defined a binary relation $\leftrightarrow$ on this set by $X \leftrightarrow Y$ iff there exists a bijection from X to Y. I spent the entire lecture proving that this binary relation was an equivalence relation.

That means that we can talk about the equivalence classes, which is what we'll talk about today.

So let's consider the set whose elements are $X := \{1,2,3\}$, $Y := \{4,5,6\}$ and $Z := \{7,8\}$. Which pairs of sets are related via this equivalence relation? In other words, which pairs of these sets X, Y and Z biject with each other?

Claim. X and Y biject with each other.

Proof. Define $f : X \to Y$ by $f(a) = a + 3$ and define $g : Y \to X$ by $g(b) = b - 3$ (it is trivial to check that these functions are well-defined, i.e. that $a \in X$ implies $a + 3 \in Y$ and $b \in Y$ implies $b - 3 \in X$) and two-sided inverses of each other. By Theorem 9.4 we deduce that f is a bijection, and hence $X \leftrightarrow Y$.

But how do we prove that $\{1,2,3\}$ does not biject with $\{7,8\}$? We could try all the maps from $\{1,2,3\}$ to $\{7,8\}$ (exercise: how many are there?) and check that none of them are bijections. But there is a better way.

We define a set to be *finite* if there exists some $n \in \mathbb{Z}_{\geq 0}$ such that the set bijects with the set $\{1,2,3,\ldots,n\}$, and if a set bijects with $\{1,2,3,\ldots,n\}$ we define its *cardinality* to be n.

[one can check that n is well-defined, i.e. that if $\{1,2,3,\ldots,n\}$ bijects with $\{1,2,\ldots,m\}$ then $n=m$, but it's a slightly messy proof by induction and I will skip it. It is done in Lean's maths library though!]

Once this is out of the way, one can prove

Theorem 9.8 If X and Y are finite sets, then $X \leftrightarrow Y$ if and only if X and Y have the same cardinality.

Theorem 9.8 If X and Y are finite sets, then $X \leftrightarrow Y$ if and only if X and Y have the same cardinality.

Proof. If X has cardinality n then $X \leftrightarrow \{1, 2, 3, \ldots, n\}$ and if Y has cardinality m then $Y \leftrightarrow \{1, 2, 3, \ldots, m\}$.

So

$$\begin{aligned} X \leftrightarrow Y &\iff X \leftrightarrow \{1, 2, 3, \ldots, m\} \\ &\iff \{1, 2, 3, \ldots, n\} \leftrightarrow \{1, 2, 3, \ldots, m\} \\ &\iff n = m \end{aligned}$$

$\square$

[answering Michael's question about proving $\iff$ statements directly]

So for finite sets this $\leftrightarrow$ equivalence relation is easy to understand – two finite sets are equivalent if and only if their cardinalities (which are elements of $\mathbb{Z}_{\geq 0}$) are equal.

The problem is that infinity is not a number, and so you can't extend that grotty induction proof to cover the case of infinite cardinalities.

What is even worse, is that it turns out that (a) there are sets which look like they should not biject because one is strictly contained in the other, but they biject anyway, and (b) conversely, there are infinite sets, i.e. sets having "size infinity", which do not biject with each other. There is a *countable* infinity, and also some *uncountable* infinities.

This is what I'll be doing for the rest of M1F. This is an extremely abstract part of M1F and to be quite frank this sort of stuff does not come up much in "normal" mathematics – however it is occasionally useful to know.

It's clear to many of you that $\{1, 2, 3\}$ bijects with $\{4, 5, 6\}$ and that it does not biject with $\{7, 8\}$ becuase you have an intuitive notion of "being smaller than" (by which I mean "being strictly less than in size").

The problem with the idea of "being smaller than" for infinite sets.

Let $N := \mathbb{Z}_{\geq 1}$ be the set of positive integers $\{1, 2, 3, 4, 5, \ldots\}$ and let $E := \{2, 4, 6, 8, 10, \ldots\}$ be the set of positive even integers.

"Clearly" E is smaller than N, because there is a really obvious injection from E into N, sending a positive even integer n to n, and this injection is far from being a surjection.

However there is also an injection from N into E which is far from being a surjection; we simply define $f : N \to E$ by $f(n) = 4n$; this is clearly a well-defined injection which misses half of the positive even integers.

$N := \{1, 2, 3, 4, 5, \dots\}$ and $E := \{2, 4, 6, 8, 10, \dots\}$.

In fact, N and E biject with each other: the function $f : N \to E$ sending n to $2n$ is a bijection, with two-sided inverse $g : E \to N$ sending m to $m/2$ (one easily checks that these functions are well-defined and that g is a two-sided inverse for f).

So we need to think more carefully about what it means for two sets to biject with each other – it could happen even if one is "obviously" smaller than the other!

Lemma 9.9. The sets $\mathbb{Z}_{\geq 1}$ and $\mathbb{Z}_{\geq 0}$ biject with each other.

Proof. It is easily checked that $f : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 1}$ defined by $f(n) = n + 1$ is a bijection, with inverse $g(m) = m - 1$. $\square$

But what about $\mathbb{Z}_{\geq 1}$ and $\mathbb{Z}$? Before I start on this, let us see a helpful way to think about maps from $\mathbb{Z}_{\geq 1}$ to any set X.

Definition 9.10 Let X be a set. By an *infinite sequence* $x_1, x_2, \ldots, x_n, \ldots$ of elements of X, or more precisely an *infinite sequence indexed by* $\mathbb{Z}_{\geq 1}$, I just mean a map $\mathbb{Z}_{\geq 1} \to X$, where the notation we use for the map is $d \mapsto x_d$.

I just *defined* "$\ldots$"!

For example the infinite sequence of prime numbers $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ and so on corresponds to the map $\mathbb{Z}_{\geq 1} \to \mathbb{Z}$ sending 1 to 2, 2 to 3, 3 to 5 and so on.

Another example: the infinite sequence $2, 4, 6, 8, 10, \dots$ corresponds to the function sending $n \in \mathbb{Z}_{\geq 1}$ to $2n$.

Now to give a *bijection* $\mathbb{Z}_{\geq 1} \to X$ is just to list its elements $X = \{x_1, x_2, x_3, \dots\}$ in such a way that every element shows up *exactly once* in the list. Why is this? Injectivity of the map says that every element shows up *at most once*, and surjectivity says that every element shows up *at least once*, so bijectivity says that every element shows up exactly once.

Example: the positive even integers $2, 4, 6, 8, \dots$ – every positive even integer shows up exactly once in this list, and this is because the map $f(n) = 2n$ from $\mathbb{Z}_{\geq 1}$ to the set of positive even integers is a bijection.

Lemma 9.11. The sets $\mathbb{Z}_{\geq 1}$ and $\mathbb{Z}$ biject with each other.

Lemma 9.11. The sets $\mathbb{Z}_{\geq 1}$ and $\mathbb{Z}$ biject with each other.

If you are surprised by this, because $\mathbb{Z}$ looks “twice as big” as $\mathbb{Z}_{\geq 1}$, then remember that $\mathbb{Z}_{\geq 1}$ looks “twice as big” as the set E of positive even integers, but they bijected.

Proof. Here is a list of all the elements of $\mathbb{Z}$:

$$0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots.$$

This list contains every single integer exactly once, so it gives rise to a bijection from $\mathbb{Z}_{\geq 1}$ to $\mathbb{Z}$.

$\square$

Think about this claim for a while, that every integer appears exactly once, and if you are convinced you can see why it’s true then try explaining it to the person next to you, and if you are not convinced then ask the person next to you to see if they can explain it.

A formal proof would be a lot more boring, one would need to explicitly write down the formula for the nth term of $0, 1, -1, 2, -2, \ldots$ and then probably write down the inverse function too and check everything worked out. I guess $f : \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ would be defined by $f(n) = n/2$ if n is even and $f(n) = (1-n)/2$ if n is odd, and $g : \mathbb{Z} \to \mathbb{Z}_{\geq 1}$ would be defined by $g(m) = 2m$ if m is positive and $g(m) = 1 - 2m$ if $m \leq 0$. And now it would be a slightly tedious case by case check to see that g was a two-sided inverse for f. I put it on the example sheet, so if you want to convince yourself that $\mathbb{Z}_{\geq 1} \leftrightarrow \mathbb{Z}$ then do that question!

Definition 9.12. A set is *countably infinite* if it bijects with $\mathbb{Z}_{\geq 1}$.

So Lemma 9.9 (which said $\mathbb{Z}_{\geq 1} \leftrightarrow \mathbb{Z}_{\geq 0}$) can be restated as "$\mathbb{Z}_{\geq 0}$ is countably infinite", and Lemma 9.11 can be restated as "$\mathbb{Z}$ is countably infinite".

Remember that to prove that a set X is countably infinite, mathematicians are generally happy if you write down an list $x_1, x_2, x_3, \ldots$ of elements of X, such that the list contains each element of that set exactly once.

Proposition 9.13. If X and Y are disjoint countably infinite sets, then $X \cup Y$ is countably infinite.

Proof. Let's count X as $X = \{x_1, x_2, x_3, \ldots\}$ and let's count Y as $Y = \{y_1, y_2, y_3, \ldots\}$. Then we can count $X \cup Y$ as $x_1, y_1, x_2, y_2, x_3, y_3, \ldots$. □

Definition. If X and Y are sets, then the *product* $X \times Y$ of X and Y is defined to be the set of ordered pairs (x, y) with $x \in X$ and $y \in Y$.

For example $\mathbb{R} \times \mathbb{R}$ is the set of ordered pairs (x, y) of real numbers, so $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. It's sensible notation!

If A is a finite set of size m, and B is a finite set of size n, then to give an element of $A \times B$ is to give an ordered pair (a, b) with $a \in A$ and $b \in B$. There are m choices for a, and n choices for b, so by the multiplication principle there are $m \times n$ choices for (a, b), meaning that the size of $A \times B$ is $m \times n$. It's sensible notation!

What is infinity times infinity?

Proposition 9.14. If X and Y are countably infinite sets, then $X \times Y$ is countably infinite.

Proof. Set $X = \{x_1, x_2, x_3, \ldots\}$ and $Y = \{y_1, y_2, y_3, \ldots\}$. Then $X \times Y =$

$$\{(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_1, y_3), (x_2, y_2), (x_3, y_1), (x_1, y_4), \ldots\}.$$

What is going on here? I am listing all the elements of $X \times Y$ in the following way. I let $m = 2, 3, 4, 5, 6, \ldots$. For each m I look at the finite list of solutions to $i + j = m$ with $i, j \geq 1$ (arranged so that the i's increase), and I add (x_i, y_j) to the list.

Slightly tedious exercise: The bijection $\mathbb{Z}_{\geq 1} \to X \times Y$ sends n to $(x_{f(n)}, y_{g(n)})$. Work out $f(n)$ and $g(n)$ explicitly, and check that $n \mapsto (f(n), g(n))$ is a bijection $\mathbb{Z}_{\geq 1} \to (\mathbb{Z}_{\geq 1})^2$ by writing down a map the other way and proving it is a two-sided inverse.

At the end of the last lecture, and the beginning of this lecture, I mentioned the set $\{\mathbb{Z}_{\geq 1}, \mathbb{Z}_{\geq 0}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Each of these sets is obviously "smaller than the next one". And yet we have seen that the second and third sets biject with $\mathbb{Z}_{\geq 1}$, the first one!

It gets worse!
Proposition 9.15. $\mathbb{Q}$ is countably infinite.

In other words, $\mathbb{Z}_{\geq 1}$ bijects with $\mathbb{Q}$.
Proof. First I'll prove that the positive rationals are countably infinite. Here they are in a list.

$$\{1/1, 1/2, 2/1, 1/3, 3/1, 1/4, 2/3, 3/2, 4/1, 1/5, 5/1, 1/6, \ldots\}$$

$$\{1/1, 1/2, 2/1, 1/3, 3/1, 1/4, 2/3, 3/2, 4/1, 1/5, 5/1, 1/6, \ldots\}$$

What's going on here? If $m \in \mathbb{Z}_{\geq 2}$, then the number of rationals n/d in lowest terms, with $n, d \geq 1$ and $n + d = m$, is finite. So I just list the solutions to $n + d = m$ for $m = 2, 3, 4, 5, 6, \ldots$ (ordered so that n increases) and for each solution (n, d) I add the rational n/d to the list *if it is in lowest terms*. For example when $m = 4$ I threw in $1/3$ and $3/1$ but not $2/2$.

Are you convinced that every positive rational is on this list exactly once? I myself am convinced that there is not really any sensible "formula" for the underlying bijection from $\mathbb{Z}_{\geq 1}$ to $\mathbb{Q}_{>0}$. However there is certainly an *algorithm* which produces this function, and that's good enough for me.

We have just defined a bijection $F : \mathbb{Z}_{\geq 1} \to \mathbb{Q}_{>0}$. We can also define a bijection G from the negative integers $\mathbb{Z}_{\leq -1}$ to the negative rationals $\mathbb{Q}_{<0}$ by setting $G(n) = -F(-n)$. And now we can define a bijection from $\mathbb{Z}$ to $\mathbb{Q}$ by sending 0 to 0, sending a positive integer n to the positive rational $F(n)$ and sending the negative integer m to the negative rational $G(m) = -F(-m)$. This is easily checked to be a bijection.

Hence $\mathbb{Z} \leftrightarrow \mathbb{Q}$, and because $\mathbb{Z}_{\geq 1} \leftrightarrow \mathbb{Z}$ and $\leftrightarrow$ is transitive, we have $\mathbb{Z}_{\geq 1} \leftrightarrow \mathbb{Q}$, and so $\mathbb{Q}$ is countable.

$\square$

I should say that this $\leftrightarrow$ notation is not standard – I just needed a convenient piece of notation for “bijects with” and this notation looks like a good choice to me.

So far in this lecture: $\mathbb{Z}_{\geq 1} \leftrightarrow \mathbb{Z}_{\geq 0} \leftrightarrow \mathbb{Z} \leftrightarrow \mathbb{Q}$. The other two sets we have spent quite some time thinking about in M1F are $\mathbb{R}$ and $\mathbb{C}$. Are they also countably infinite? In fact is *every* set either finite or countably infinite? This question was not even raised until 1874, when it was simultaneously raised and solved by the early hipster Georg Cantor.

Remember when we were talking about decimal expansions? If X is a subset of $\mathbb{Z}_{\geq 1}$ then let's construct a real number $r(X)$ between 0 and 1, such that the nth digit in the decimal expansion of $r(X)$ is 0 if $n \notin X$ and is 1 if $n \in X$.

For example if $X = \{2, 5, 6\}$ then $r(X) = 0.010011$ and if $X = \{1, 3, 5, 7, 9, 11, \ldots\}$ is the odd positive integers then $r(X) = 0.1010101010\ldots$. What do I mean by saying a real number is "equal" to a decimal expansion? I mean the trick I explained earlier in the course – $r(X)$ is the supremum of the set of rational numbers obtained by truncating the sum in the Nth place, for all $N \in \mathbb{Z}_{\geq 1}$.

Formally, for $X \subseteq \mathbb{Z}_{\geq 1}$, let's define $r_N(X) = \sum_{i \in X, i \leq N} 10^{-i}$ (the rational number obtained by writing down the decimal expansion up to the Nth decimal place) and let $r(X)$ be the supremum of the non-empty bounded set $\{r_1(X), r_2(X), r_3(X), \ldots\}$.

For example if $X = \{1, 3, 5, 7, 9, 11, \ldots\}$ then we define $r(X)$ to be the supremum of the set $\{0.1, 0.10, 0.101, 0.1010, 0.10101, 0.101010, \ldots\}$. This is a formal definition of $0.1010101010\ldots$. I am defining $\ldots$ again, in a different context.

It will not surprise you to know that if X and Y are different subsets of $\mathbb{Z}_{\geq 1}$ then $r(X) \neq r(Y)$ – they have "different decimal expansions".