Lecture 23

The well-ordering principle, and from $\mathbb{N}$ to $\mathbb{Q}$

23.1 The well-ordering principle

So, here is a fact about the set of natural numbers:

Theorem 23.1.1 (The well-ordering principle, or WOP)**.** Let $T \subset \mathbb{N}$ be a non-empty subset. Then T has a least element.

Proof. Let us assume that T is a set that has no least element. The rest of the proof is dedicated to concluding that T is empty, proving the theorem by proving the contrapositive.[1]

Let $S = \mathbb{N} \setminus T$ be the complement.

(i) Then $0 \in S$. Why? Well, if $0 \in T$, then T would have a least element. But by assumption T has no least element. Thus, $0 \notin T$, meaning $0 \in S$.

(ii) For every natural number n such that every element from 0 to n is contained in S, then $n + 1 \in S$. Why? Well, if we know none of 0 to n is in T, but that $n + 1$ is in T, then $n + 1$ would be the least element of T. This contradicts the assumption that T has no least element.[2]

Thus, S satisfies the hypotheses of Peano's axioms—this means $S = \mathbb{N}$. But this means $T = \emptyset$. □

[1] In other words, the proof of this theorem will be a proof by proving the contrapositive. The theorem is proving the statement "If p then q" where p is "T is non-empty," and the q is "T has a least element." Remember that $p \implies q$ is equivalent to proving the contrapositive: If not q, then not p.

[2] Proofs of both (i) and (ii) were proofs by contradiction.

You will recognize that the above is a proof of one of your writing assignments! The above is not the only proof of the theorem, but it gave me an excuse to demonstrate the use of a contrapositive.

Remark 23.1.2. The well-ordering principle is often used to prove that there are *not* any numbers that satisfy some property.

For example, imagine you have a property BLAH, and you want to prove there are not any natural numbers satisfying BLAH.

Well, let T be the set of all natural numbers satisfying BLAH. If you can prove that T has no least element (or, equivalently, derive a contradiction from assuming there is a small element in T) then you have proven that T is empty—i.e., there are no elements satisfying BLAH.

23.2 Countability

We are unfortunately running out of time in this course. I have claimed to you the following:

Theorem 23.2.1. $\mathbb{N}$ and $\mathbb{Q}$ have the same cardinality.

Remember, this means there exists some bijection from $\mathbb{N}$ to $\mathbb{Q}$ (or, equivalently, from $\mathbb{Q}$ to $\mathbb{N}$).

Very roughly speaking, there are two kinds of infinite sets that appear frequently: Those that have the same cardinality as $\mathbb{N}$, and those that do not. This dichotomy is so useful that we give a term for having the same cardinality as $\mathbb{N}$:

Definition 23.2.2 (Countable)**.** We say that a set S is *countable* if it is finite, or if it has the same cardinality as $\mathbb{N}$.

Remark 23.2.3. Sometimes, people say “enumerable” or “denumerable” instead of countable.

Example 23.2.4. So we can rephrase our main theorem as saying: $\mathbb{Q}$ is a countable set.

And on the last day of class, we will see that $\mathbb{R}$ is not a countable set.

23.3 The lemmas we'll need

So, we'd like to see a proof of the theorem. This requires some build-up, including some lemmas.[3]

Proposition 23.3.1. $\mathbb{Z}$ is countable.

Theorem 23.3.2. $\mathbb{N} \times \mathbb{N}$ is countable.

Proposition 23.3.3. If A and A' have the same cardinality, and if B and B' have the same cardinality, then $A \times B$ and $A' \times B'$ have the same cardinality.

Lemma 23.3.4. There exists a surjection from $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ to $\mathbb{Q}$.

23.4 Proof of countability of $\mathbb{Q}$

Proof. We will assume that the lemmas are true, for the moment.

Invoking the lemmas, we are guaranteed functions:

$$\begin{tikzcd}
\mathbb{N} \arrow[r, "\cong", "\mathit{Thm}\ 23.7.1"'] & \mathbb{N} \times \mathbb{N} \arrow[r, "\cong", "23.3.1,\ 23.3.3"'] & \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \arrow[r, two heads, "\mathit{Lem}\ 23.3.4"'] & \mathbb{Q}
\end{tikzcd}$$

As indicated, the first arrows (functions) are bijections, and the last arrow is a surjection. Note that every function above is therefore a surjection. We conclude that the composite function $\mathbb{N} \to \mathbb{Q}$ is therefore a surjection.[4]

We proved in Proposition 17.2.1 that if there is a surjection from a set A to a set B, then there is automatically an injection from B to A. In other words, setting $A = \mathbb{N}$ and $B = \mathbb{Q}$, we may conclude that there exists an injection from $\mathbb{Q}$ to $\mathbb{N}$.

On the other hand, because $\mathbb{N}$ is a subset of $\mathbb{Q}$, there is an injection from $\mathbb{N}$ to $\mathbb{Q}$.

So we see that there is an injection from $\mathbb{N}$ to $\mathbb{Q}$, and an injection from $\mathbb{Q}$ to $\mathbb{N}$. By the Cantor-Schroder-Bernstein Theorem (Theorem 18.1.1), we conclude there exists a bijection from $\mathbb{N}$ to $\mathbb{Q}$. □

[3] Recall that a *lemma* is a technical statement we prove in order to prove another statement that we're interested in. Technically, the plural of lemma is lemmata, but it is common to write "lemmas" for the plural.

[4] Because composition of surjections is again a surjection.

Remark 23.4.1. It is very common in math to "believe some statements" and then, based on those statements, prove a big theorem. (Here, we proved the countability of $\mathbb{Q}$ by first believing the three lemmas.

Now, it is our job to go from "believing some statements" to "proving that the statements are true." In other words, if we prove the lemmas, then we have proved the theorem.

Notice that this form of proving something makes it *easier* to digest a complicated proof. If I had just written five pages of a proof without compartmentalizing different parts of the proof into lemmas, you'd have no idea how to follow the "big picture." So lemmas are not presented just to confuse you; they are presented to let the reader know where the technicalities are, and to make the proof of the theorem more digestible.

23.5 Proof of Lemma 23.3.4

The proof that there exists a surjection[5] from $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ to $\mathbb{Q}$ is actually not so bad.

So what is an element of $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$? By definition of Cartesian product, an element of this set is an ordered pair

$$(a, b)$$

where $a \in \mathbb{Z}$, and $b \in \mathbb{Z} \setminus \{0\}$. In other words, a is an integer, and b is any integer aside from 0.

To define a function from $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ to $\mathbb{Q}$, we need to assign a rational number to every pair (a, b) where a and b are integers, and $b \neq 0$. Can you think of a way to do such a thing? Probably! In fact, let's define our function by

$$(a, b) \mapsto \frac{a}{b}.$$

Let's call the function q. To summarize, we have

$$\begin{aligned} q : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) &\to \mathbb{Q} \\ (a, b) &\mapsto \frac{a}{b}. \end{aligned}$$

Then q is a surjection—given any rational number, you know you can write it as a fraction m/n for some integers m and n (with $n \neq 0$). Then $q(m, n) = m/n$, so q is a surjection.

[5] Lemma 23.3.4

23.6 ℕ and ℤ

Proof of Proposition 23.3.1. Define a function $f : \mathbb{N} \to \mathbb{Z}$ as follows:

$$f(x) = \begin{cases} x/2 & \text{if } x \text{ is even} \\ -(x+1)/2 & \text{if } x \text{ is odd.} \end{cases}$$

I will leave it to you to verify that this is a bijection. □

Remark 23.6.1. Note that $f(0) = 0$. So in fact, this f induces a bijection

$$\mathbb{N} \setminus \{0\} \cong \mathbb{Z} \setminus \{0\}.$$

23.7 ℕ × ℕ and ℕ

Last time, we talked about direct products of sets. When X and Y are finite, we saw that $\#(X \times Y) = \#(X) \times \#(Y)$. Here is a surprising fact:

Theorem 23.7.1. There exists a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$.

Remark 23.7.2. For the proof of the theorem, we will use some facts about even and odd numbers.

Recall that a natural number is called even if it is divisible by two. Equivalently, a natural number is called even if its unit digit is 0, 2, 4, 6, or 8.

Recall that a natural number is called odd if it is not divisible by two. Equivalently, a natural number is called odd if its unit digit is 1, 3, 5, 7, or 9.

If m is any even number, there exists some integer a so that $m = 2a$.

If m is an odd number, there exists some integer a so that $m = 2a + 1$.

Remark 23.7.3. As usual, I will provide footnotes in the proof to justify some non-obvious claims and make some commentary. However, keep in mind that the writing without the footnotes is a concisely written proof.

Proof of Theorem 23.7.1. We must exhibit a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. For this, define a function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by the formula

$$f(a, b) = -1 + 2^a(2b + 1)$$

To see that f is a surjection, fix $n \in \mathbb{N}$, and consider the integer $n' = n + 1$. Note $n' \geq 1$.[6] Thus there is some largest power of 2, call it 2^a, that divides n'.[7] In fact, $n'/(2^a)$ must be odd (else it could be divided by 2 again, contradicting the maximality of 2^a). So we know that

$$n'/(2^a) = 2b + 1$$

for some b.[8] We have chosen a and b so that $f(a, b) = n$.[9]

Now let us see that f is an injection. Suppose $f(a, b) = f(a', b')$, which implies

$$2^a(2b + 1) = 2^{a'}(2b' + 1).$$

If $a \neq a'$, we are led to a contradiction. For example, if $a < a'$, we may divide both sides by 2^a to conclude that $2b + 1$ is equal to an even number.[10]

Thus it must be that $a = a'$. Dividing both sides by 2^a, we see that $2b + 1 = 2b' + 1$, hence $b = b'$. This shows that if $f(a, b) = f(a', b')$, then $(a, b) = (a', b')$. Therefore f is an injection. □

Remark 23.7.4. Recall that any bijection $f : X \to Y$ defines an inverse bijection. So the above theorem tells us that there also exists a bijection from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$.

Remark 23.7.5. There are many bijections from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$. Here is a commonly drawn bijection; it is *not* the inverse to the bijection from Theo-

[6] Because $n \in \mathbb{N}$, we know that $n \geq 0$. So $n + 1 \geq 0$. Using $n' = n + 1$, we see that $n' \geq 1$.

[7] If $n' = 0$, there would be no largest a. This is because any number divides zero. Note also that when n' is an odd number, $a = 0$.

[8] Every odd number can be expressed as "some even number +1." $2b$ is this even number.

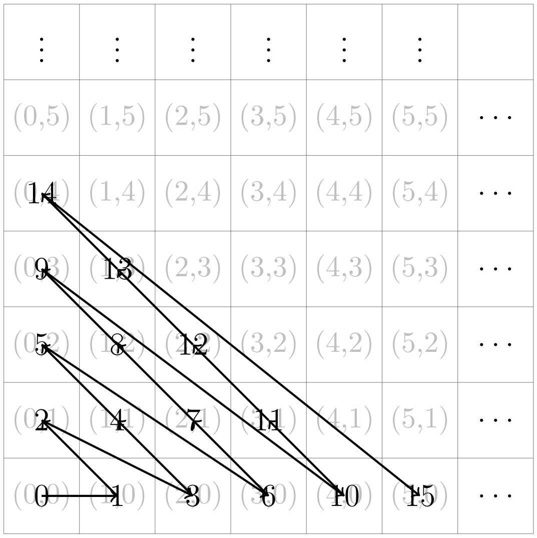
[9] Because we chose a and b so that $n'/(2^a) = 2b + 1$, we conclude that $n' = 2^a(2b + 1)$. Using that $n' = n+1$, we conclude that $n = -1+2^a(2b+1)$. This last expression is $f(a, b)$ by definition of f.

[10] A similar argument for the case $a > a'$ leads to a similar conclusion that $2b' + 1$ is even. In situations like this where there is a clear "symmetry" to the argument dealing with multiple cases, mathematicians often write "without loss of generality, assume that $a < a'$." (And it is common to make no further commentary on the case $a > a'$.)

rem 23.7.1. If we draw ℕ × ℕ as follows:

⋮	⋮	⋮	⋮	⋮	⋮	
(0,5)	(1,5)	(2,5)	(3,5)	(4,5)	(5,5)	⋯
(0,4)	(1,4)	(2,4)	(3,4)	(4,4)	(5,4)	⋯
(0,3)	(1,3)	(2,3)	(3,3)	(4,3)	(5,3)	⋯
(0,2)	(1,2)	(2,2)	(3,2)	(4,2)	(5,2)	⋯
(0,1)	(1,1)	(2,1)	(3,1)	(4,1)	(5,1)	⋯
(0,0)	(1,0)	(2,0)	(3,0)	(4,0)	(5,0)	⋯

Then we can overlay a path as follows:



Or, less clunkily, consider the assignment

$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
(0,5)	(1,5)	(2,5)	(3,5)	(4,5)	(5,5)	$\cdots$
14 (0,4)	(1,4)	(2,4)	(3,4)	(4,4)	(5,4)	$\cdots$
9 (0,3)	13 (1,3)	(2,3)	(3,3)	(4,3)	(5,3)	$\cdots$
5 (0,2)	8 (1,2)	12 (2,2)	(3,2)	(4,2)	(5,2)	$\cdots$
2 (0,1)	4 (1,1)	7 (2,1)	11 (3,1)	$\ddots$ (4,1)	(5,1)	$\cdots$
0 (0,0)	1 (1,0)	3 (2,0)	6 (3,0)	10 (4,0)	15 (5,0)	$\cdots$

While this "proof by picture" should not be accepted as a proof, I promise you can turn this picture into a function—in fact, a function with a formula—from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$ that happens to be a bijection.

23.8 Proposition 23.3.3

Proof of Proposition 23.3.3. Let $f : A \to A'$ and $g : B \to B'$ be bijections. Then the function

$$f \times g : A \times B \to A' \times B', \qquad (a, b) \mapsto (f(a), g(b))$$

is a bijection. I leave the verification to you. □