Lecture 11

Unique Uniqueness of natural numbers (equipped with nextness)

Recall that Peano's axioms posit the existence of a set N, and a function t from N to N, satisfying the following:

(PA1) N is a non-empty set.

(PA2) t is an injection.

(PA3) There is a unique element of N that is not hit by t. We will call this unique element z.

(PA4) Finally, suppose that S is some subset of N for which (i) $z \in S$, and (ii) Whenever $n \in N$, then $t(n) \in N$. Then $S = N$.

I asked you last time: What if there exist more than one set and function satisfying the above properties?

Theorem 11.0.1. Suppose that M is a set, and s is a function from M to itself, satisfying the above axioms.

Then there is a natural bijection from N to M compatible with s. More precisely, there is a bijection $f : N \to M$ so that $f \circ t = s \circ f$.

Moreover, this bijection is itself unique. This means if there is another bijection $f' : N \to M$ satisfying $f' \circ t = s \circ f'$, then $f = f'$.

Remark 11.0.2. The above theorem says that any two sets satisfying Peano's axioms must look "the same," in that there is a bijection between them (so, up to relabeling the elements of N by elements of M, N and M look the same) that also respects t and s (so that this relabeling also respects "nextness").

In fact, the theorem says even more: The bijection itself is unique if you demand that the bijection respects "nextness."

This is a very important point! Remember, if you want to exhibit a bijection between two sets, there are many, many ways to do so. (For example, there are 5! bijections between two sets with 5 elements.) But the theorem says that there is only *one* bijection that respects nextness.

We have not talked yet about what it means for two *functions* to be equal.

Definition 11.0.3 (Equality of functions)**.** Two functions f and f' are called equal if

1. They have the same domain and the same codomain, and
2. For every element x of the domain, $f(x) = f(x')$ (note this is an equality of elements of the codomain).

Remark 11.0.4. In other words, the data of N and t is not unique—there may be another M and s satisfying the same axioms—but there is exactly one may to "make N and M look the same;" or to "relabel N by M" while respecting nextness (i.e., while respecting t and s).

This kind of thing is very common in mathematics. The lingo is that any set satisfying Peano's axioms is "unique up to unique isomorphism."

Here, "up to" means "not the same, but there is a bijection between them respecting the relevant structure (i.e., nextness)."

The proof of the theorem is quite involved, so we'll take things one step at a time.

11.1 Aside: Theorems and Lemmas

Definition 11.1.1. A *theorem* is a statement that has been proven, and for which (i) The statement is supposed to be either deep, useful, or surprising, and (ii) The proof is "difficult."

Note that these are all very subjective criteria; math is done by humans, and humans are subjective.

Sometimes, when we prove a big theorem, it's best for both the reader and the writer to break up the proof into small, digestible chunks. And in doing so, we may sometimes prove a statement that is technical, but useful or necessary for proving the theorem. Such a statement is called a *lemma*.

Definition 11.1.2. A *lemma* is a statement that has been proven, and which (i) involves a technical proof and (ii) is used to prove another statement (such as a theorem).

11.2 Proving uniqueness of f

We'll start off with something fun: Even if we do not know that f exists, we'll show that if f exists, it is unique. In other words, if f and f' both satisfy the properties guaranteed by the conclusion of the theorem, then $f = f'$.

Lemma 11.2.1. Suppose that f' is another bijection from N to M for which $f' \circ t = s \circ f$. Then $f = f'$.

Proof. Let $S \subset N$ be the collection of those n for which $f(n) = f'(n)$.

First, I claim $z \in S$. In fact, I claim $f(z) = z_M$ and $f'(z) = z_M$ (where $z_M \in M$ is the unique element not hit by s, guaranteed to exist by Peano's third axiom applied to M). For if $f(z) \neq z_M$, then $f(z) = s(m)$ for some $m \in M$ by Peano's third axiom. Because f is assumed to be a bijection, then $m = f(n)$ for some n. Therefore, $f(z) = s(m) = s(f(n))$, and by the demand that $f \circ t = s \circ f$, we thus see that $f(z) = f(t(n))$. Because f is an injection, this means $z = t(n)$, which violates Peano's third axiom for N. Therefore, it must be that $f(z) = z_M$.

Now, if $n \in S$, then $t(n) \in S$. This is because $f(t(n)) = s(f(n)) = s(f'(n))$ by the assumptino that $n \in S$, and hence $s(f'(n)) = f'(t(n))$, so stringing the equalities together, we see $f(t(n)) = f'(t(n))$.

By Peano's axioms, this means $S = N$. $\square$

11.3 Constructing f

Next, let's construct the function f that the theorem claims exists.

Construction 11.3.1. Given N, there is a unique element z not hit by t.

Likewise, there is a unique element $z_M \in M$ not hit by s.

Let us define a function f from N to M as follows:

1. $f(z) = z_M$.
2. Let S be the set of elements for which f is defined. Then for any $n \in S$, we define $f(t(n))$ to be $s(f(n))$.

In particular, we see that $S = N$ by the inductive axiom, so f indeed has domain equal to N.

Remark 11.3.2. Note that, by definition, $f \circ t = s \circ f$.

11.4 Proving Theorem 11.0.1

Lemma 11.4.1. Let f be the function from Construction 11.3.1. Then for every $m \in M$, there exists an $n \in N$ for which $f(n) = m$. Put another way, every element of M is hit by f.

We'll give a proof of the lemma in a moment. But first: At this point, we've seen in this class (many times) the idea of how much a function "hits" of the codomain. My philosophy has always been concepts first, terms second. At this point, I think we can agree that it'll be useful to have a term for the things that f "hits." Here it is:

Definition 11.4.2. Let f be a function with domain X and codomain Y. The *image* of f is the set

$$\{y \in Y \mid \text{there exists some } x \in X \text{ for which } f(x) = y\}.$$

The image of f will often be written image(f).

Thus, informally speaking, f is the set of all elements of Y that are hit by f. Another way to phrase Lemma 11.4.1 is: the image of f is M.

Proof of Lemma 11.4.1. Let $R \subset M$ be the set of elements hit by f. (That is, let $R = \text{image}(f)$.)

(i) We know that $z_M \in R$ by (1) of Construction 11.3.1.

(ii) Next, suppose that $m \in R$ so that $m = f(n)$ for some n. Then $s(m) \in R$ because $s(m) = s(f(n)) = f(t(n))$, where the last equality is by (2) of Construction 11.3.1.

By the inductive axiom, $R = M$. (In other words, every element of M is hit by f.) $\square$

We prove another lemma.

Lemma 11.4.3. Let f be the function from Construction 11.3.1. Then f is an injection.

Proof. Let $R \subset M$ be the set of all m for which *at most* one element of N hits m. More precisely, we define

$$R := \{m \,|\, \text{If } f(n) = m \text{ and } f(n') = m, \text{ then } n = n'\}.\}$$

First, I claim $z_M \in R$. Here is the proof. We know $f(z) = z_M$. At the same time, suppose there is another element $n' \in N$ for which $f(n') = z_M$. If $n' \neq z$, then we know $n' = t(a)$ for some $a \in N$ (by the third of Peano's axioms, applied to N). Then we would have that $f(n') = f(t(a)) = s(f(a))$ (where the last equality is by (2) of Construction 11.3.1). But that $f(n') = s(f(a))$ contradicts our knowledge that $f(n') = z_M$. (z_M cannot equal s of anything, again by the third of Peano's axioms, applied to M.) Therefore, we conclude that $n' = z$.

Next, I claim that if $m \in R$, then so is $s(m)$. So, suppose $s(m) = f(n) = f(n')$. We must show $n = n'$. Well, because $s(m) \neq z_M$ (by Peano's third axiom applied to M) we know that neither n nor n' equal z (because we defined $f(z) = z'$ in Construction 11.3.1). Then, by Peano's third axiom applied to N, we know that $n = t(l)$ and $n' = t(l')$ for some l and l'. Putting this all together, we see that

$$s(m) = f(t(l)) = f(t(l')).$$

By (2) of Construction 11.3.1, we thus see

$$s(m) = s(f(l)) = s(f(l')).$$

But s is an injection by Peano's second axiom, so we see that

$$m = f(l) = f(l').$$

Because $m \in S'$, we conclude that $l = l'$, and hence that $t(l) = t(l')$; in other words, $n = n'$, as we sought to show. □

Now we can prove our main theorem:

Proof of Theorem 11.0.1. Let f be the function from Construction 11.3.1.

By Remark 11.3.2, f satisfies $f \circ t = s \circ f$.

By Lemma 11.4.3, f is an injection. By Lemma 11.4.1, $\text{image}(f) = M$. Therefore, f is a bijection. □

11.5 Exercises

Exercise 11.5.1. Which of the following is guaranteed by Peano's axioms?

(a) There exists a set N and a function t satisfying Peano's axioms.

(b) There exists *at most one set* N and *at most one function* t from N to N satisfying Peano's axioms.

(c) There exists *at most one set* N and *at least one* function t from N to N satisfying Peano's axioms.

(d) There exists *at least one set* N and *at least one* function t from N to N satisfying Peano's axioms.

(e) There exists *at least one set* N and, for every such N, *exactly one* function t from N to N satisfying Peano's axioms.

Exercise 11.5.2. Which of the following terms are used in Peano's axioms?

(a) Number

(b) Natural number

(c) 1

(d) Addition

(e) +1

(f) Subset

(g) Function

(h) Injection