The Recursion Theorem

https://noatmeal.github.io/

A useful item to have in one's toolbox while working in ZFC set theory[1] is the ability to create inductive definitions. My goal in this post is to prove a theorem that allows us to do exactly that whenever the proper conditions are present. We'll also work out a couple of fun examples at the end.

1 Preliminaries

If the following material doesn't make much sense, then a great review can be found in the first half of [1]. A proof for the main theorem of this post can be found in that text as well.

1.1 Natural Numbers

Definition 1.1. A set I is inductive if and only if $\emptyset \in I$ and $\forall y \in I(y \cup \{y\} \in I)$.

Example 1.1. Here are some elements one would find in an inductive set

- $\emptyset$
- $\emptyset \cup \{\emptyset\} = \{\emptyset\}$
- $\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$
- $\{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

Axiom 1.1 (Infinity)**.** $\exists I(I$ *is inductive*$)$

Axiom 1.2 (Comprehension)**.** $\forall v \exists y \forall x(x \in y \Leftrightarrow x \in v \land \phi(x))$ *where* ϕ *is a formula that* y *is not free in.*

Definition 1.2. Let I be a set who's existence is guaranteed by Axiom 1.1. We use Axiom 1.2 to form the set

$$\mathbb{N} = \{y \in I : \forall J(J \text{ is inductive} \Rightarrow y \in J)\}$$

One should think of $\mathbb{N}$ as the "smallest" inductive set[2]. An element of $\mathbb{N}$ is called a *natural number*.

[1] Short for Zermelo–Fraenkel set theory. See https://en.wikipedia.org/wiki/Zermelo-Fraenkel_set_theory for more information.

[2] We will prove this in Theorem 1.3

Example 1.2. Figure 1 shows a few compact names for natural numbers that are often used in place of the set theory notation[3].

Element of $\mathbb{N}$	Compact Name
$\emptyset$	1
$\{\emptyset\}$	2
$\{\emptyset, \{\emptyset\}\}$	3
$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$	4

Figure 1: Compact names for elements of $\mathbb{N}$.

Definition 1.3. The function $S : \mathbb{N} \to \mathbb{N}$ defined by $S(n) = n \cup \{n\}$ for all $n \in \mathbb{N}$ is called the *successor function on* $\mathbb{N}$. For $n \in \mathbb{N}$, we will refer $S(n)$ as n^+.

Example 1.3. Recall Example 1.1 and Example 1.2. One can deduce that

- $1^+ = 2$
- $2^+ = 3$
- $3^+ = 4$

and we'll define two more compact names here to be used in an informative example at the end of the post:

- $4^+ = 5$
- $5^+ = 6$

1.2 Peano Axioms

While we prove and refer to the following as theorems, it is common nomenclature to refer to these as *The Five Peano Axioms*.

Theorem 1.1. $1 \in \mathbb{N}$

Proof. Since 1 is in every inductive set, then $1 \in \mathbb{N}$. $\square$

Theorem 1.2. *If $n \in \mathbb{N}$, then $n^+ \in \mathbb{N}$.*

Proof. Let $n \in \mathbb{N}$. By definition $\forall I(I \text{ is inductive} \Rightarrow n \in I)$, and so for any inductive set K we can conclude that $n^+ \in K$ since $n \in K$. Recall that $n \in I$ from Definition 1.2. By defintion, $n^+ \in I$. So we conclude from these two facts that $n^+ \in \mathbb{N}$. $\square$

[3]Note that 1 is considered the first natural number in this post.

Theorem 1.3 (Principle of Mathematical Induction)**.** *If S is an inductive subset of $\mathbb{N}$, then $S = \mathbb{N}$.*

Proof. We will argue by subset inclusions that $S = \mathbb{N}$. By hypothesis, we are given that $S \subseteq \mathbb{N}$. Now suppose that $n \in \mathbb{N}$. By hypothesis, S is an inductive set and so by definition of $\mathbb{N}$, $n \in S$. Hence, $S = \mathbb{N}$. $\square$

Definition 1.4. We refer to invoking Theorem 1.3 as an *argument by induction.*

Theorem 1.4. *For all $n \in \mathbb{N}$, we have that $n^+ \neq 1$.*

Proof. Let $n \in \mathbb{N}$. Recall that $n^+ = n \cup \{n\}$ and so $n \in n^+$. Well $n \notin \emptyset$ and so it cannot be the case that $n^+ = 1$. Therefore $n^+ \neq 1$. $\square$

Definition 1.5. A set T is transitive if and only if $x \in T \Rightarrow x \subseteq T$.

Lemma 1.1. *Every natural number is transitive.*

Proof. We argue by induction. Let S be the set of all transitive natural numbers. $1 \in S$ trivially. Suppose $n \in S$. Since $n^+ = n \cup \{n\}$, then for all $x \in n^+$ either $x \in n$ or $x = n$. If $x \in n$, then by our inductive hypothesis that $n \in S$, we know that $x \subseteq n$ which allows us to conclude that $x \subseteq n^+$. If $x = n$, then we also conclude that $x \subseteq n^+$. Therefore, $n^+ \in S$ which completes the inductive argument. $\square$

Theorem 1.5. *If $n, m \in \mathbb{N}$ and $n^+ = m^+$, then $n = m$.*

Proof. Suppose the hypothesis is true. Well then $n \in n^+ \Rightarrow n \in m^+$ and so either $n \in m$ or $n = m$. By the same type of observation, either $m \in n$ or $m = n$. If $n \neq m$, then $m \in n$ and $n \in m$. Well then Lemma 1.1 tells us that $m \subseteq n$ and $n \subseteq m$ and so $n = m$, a contradiction. Therefore it must be the case that $n = m$. $\square$

2 Existence and Uniqueness

Theorem 2.1 (Recursion)**.** *For any set X, if $a \in X$ and $f : X \to X$, then there exists a function $u : \mathbb{N} \to X$ such that $u(1) = a$ and $u(n^+) = f(u(n))$ for all other natural numbers n.*

Proof. Let $\mathcal{C} \subseteq \mathcal{P}(\mathbb{N} \times X)$ be defined such that $(1, a) \in c$ and $(n^+, f(x)) \in c$ whenever $(n, x) \in c$ for all $c \in \mathcal{C}$. It's clear to see that $\mathcal{C}$ is nonempty since $\mathbb{N} \times X \in C$ and so we can form the intersection of all sets in $\mathcal{C}$ which we'll call u.

Let S be the set of all natural numbers such that if $n \in S$ then there exists $(n, x) \in u$ and if $(n, w), (n, y) \in u$ then $w = y$. We will prove inductively that $S = \mathbb{N}$ which establishes that u is a function. Furthermore, given how u is constructed, such a proof gives us exactly the kind of function we are looking for.

Suppose that $(1, b) \in u$, $a \neq b$, and consider the set $M = u \setminus \{(1, b)\}$. We claim that $(n^+, f(x)) \in M$ whenever $(n, x) \in M$. Since $(1, a) \in M$, this will give us that $M \in \mathcal{C}$ and $u \nsubseteq M$ which is a contradiction to u being the intersection of all members of $\mathcal{C}$. That will then allow us to say that $(1, a) \in u$ and for all $(1, b) \in u$ it would be the case that $a = b$.

So suppose that $(n^+, f(x))$ is not present in M for some $(n, x) \in M$. Well by the definition of M, for all α we have that $(\alpha \in u \wedge \alpha \neq (1, b)) \rightarrow \alpha \in M$ which implies by contraposition that if $\alpha \notin M$, then $\alpha \notin u \vee \alpha = (1, b)$. Well it can't be the case that $(n^+, f(x)) = (1, b)$ by Theorem 1.4. So then we must conclude that $(n^+, f(x)) \notin u$ which contradicts u's construction since $(n, x) \in u$ by the assumption that $(n, x) \in M$. We now must conclude that $M \in \mathcal{C}$ which gives us the base case for our inductive argument as discussed in the previous paragraph.

Now suppose that $n \in S$ which implies that there is an $(n, x) \in u$ for at most one x. It follows from the definition of u that $(n^+, f(x)) \in u$. Now if n^+ isn't in S, then there exists $(n^+, y) \in u$ such that $f(x) \neq y$. Suppose that this is the case and consider the set $J = u \setminus \{(n^+, y)\}$ with some element $(m, t) \in J$.

If $m = n$, then $t = x$ since $n \in S$ and so $(n^+, f(x)) = (m^+, f(t)) \in J$. By construction of J, we note that $\alpha \notin J \rightarrow (\alpha \notin u \vee \alpha = (n^+, y))$ for all α. So if $m \neq n$, then we know that $m^+ \neq n^+$ by Theorem 1.5 which means that if $(m^+, f(t)) \notin J$ then we must conclude that $(m^+, f(t)) \notin u$ which is a contradiction to the construction of u and so $(m^+, f(t)) \in J$.

Therefore in every case, $(m^+, f(t)) \in J$ whenever $(m, t) \in J$. Since it also the case that $(1, a) \in J$ since $n^+ \neq 1$ by Theorem 1.4, we conclude that $J \in \mathcal{C}$ and $u \nsubseteq J$ which is a contradiction to u's construction as being the intersection of all members of $\mathcal{C}$.

So $n^+ \in S$ and by the principal of mathematical induction we conclude that $\mathbb{N} = S$. $\square$

Corollary 2.1. *The function defined in Theorem 2.1 is unique.*

Proof. Let $a \in X$ and $f : X \rightarrow X$ for some set X. Suppose that there are two functions $F : \mathbb{N} \rightarrow \mathbb{X}$ and $G : \mathbb{N} \rightarrow \mathbb{X}$ given by Theorem 2.1
where $F(1) = G(1) = a$ and for all other natural numbers n we have that $F(n^+) = f(F(n))$ and $G(n^+) = f(G(n))$. Let $F(1) = G(1)$ be the base case for an inductive proof and suppose that $F(n) = G(n)$ for some natural number n. Well then $F(n^+) = f(F(n)) = f(G(n)) = G(n^+)$ by the inductive hypothesis. So by the principle of mathematical induction, F and G are the same function. $\square$

3 Examples

Let's define a couple of familiar concepts using what we've shown.

Definition 3.1. For any natural number $n \in \mathbb{N}$, we have $n^+ \in \mathbb{N}$ by Theorem 1.2. If we apply n^+ and the successor function on $\mathbb{N}$ to Theorem 2.1 and Corollary 2.1, we can define a unique function $s_n : \mathbb{N} \to \mathbb{N}$ where $s_n(1) = n^+$ and $s_n(m^+) = s_n(m)^+$ for all $m \in \mathbb{N}$.

Definition 3.2 (Addition)**.** Let $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the function that maps $+(n, m)$ to $s_n(m)$ for all $n, m \in \mathbb{N}$. We almost always write this using inline notation as $n + m$ and call it the *sum of* n *and* m.

Preliminary Remark: In an effort to recover some familiar looking calculations we prove the following lemma and theorem.

Lemma 3.1. $n + 1 = n^+$

Proof. $n + 1 = s_n(1) = n^+$ □

Theorem 3.1. $n + (m + 1) = (n + m) + 1$

Proof.

$$\begin{aligned} n + (m + 1) &= s_n(m + 1) \text{ by Definition 3.2} \\ &= s_n(m^+) \text{ by Lemma 3.1} \\ &= (s_n(m))^+ \text{ by Definition 3.1} \\ &= s_n(m) + 1 \text{ by Lemma 3.1} \\ &= (n + m) + 1 \text{ by Definition 3.2} \end{aligned}$$

□

Example 3.1. Recall Example 1.3. One can deduce that

- $2 = 1^+ = 1 + 1$
- $3 = 2^+ = 2 + 1$
- $4 = 3^+ = 3 + 1$
- $5 = 4^+ = 4 + 1$
- $6 = 5^+ = 5 + 1$

Example 3.2. Recall Example 3.1. We can see that

$$2 + 2 = 2 + (1 + 1) = (2 + 1) + 1 = 3 + 1 = 4$$

Definition 3.3. For every $n \in \mathbb{N}$, we take $s_n : \mathbb{N} \to \mathbb{N}$ from Definition 3.2 and define $p_n : \mathbb{N} \to \mathbb{N}$ where $p_n(1) = n$ and $p_n(m^+) = n + p_n(m)$.

Definition 3.4 (Multiplication)**.** Let $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the function that maps $\cdot(n, m)$ to $p_n(m)$ for all $n, m \in \mathbb{N}$. We almost always write this using inline notation as $n \cdot m$ and call it the *product of* n *and* m.

Preliminary Remark: In an effort to recover some familiar looking calculations we prove the following lemma and theorem.

Lemma 3.2. $n \cdot 1 = n$

Proof. $n \cdot 1 = p_n(1) = n$ □

Theorem 3.2. $n \cdot (m + 1) = n + (n \cdot m)$

Proof.

$$\begin{aligned} n \cdot (m+1) &= p_n(m+1) \text{ by Definition 3.4} \\ &= p_n(m^+) \text{ by Lemma 3.1} \\ &= n + p_n(m) \text{ by Definition 3.3} \\ &= n + (n \cdot m) \text{ by Definition 3.4} \end{aligned}$$

□

Example 3.3. Recall Example 3.1 once more. We can see that

$$\begin{aligned} 2 \cdot 3 &= 2 \cdot (2 + 1) \\ &= 2 + (2 \cdot 2) \\ &= 2 + (2 \cdot (1 + 1)) \\ &= 2 + (2 + (2 \cdot 1)) \\ &= 2 + (2 + 2) \\ &= 2 + 4 \text{ by Example 3.2} \\ &= 2 + (3 + 1) \\ &= (2 + 3) + 1 \\ &= (2 + (2 + 1)) + 1 \\ &= ((2 + 2) + 1) + 1 \\ &= (4 + 1) + 1 \\ &= 5 + 1 = 6 \end{aligned}$$

References

[1] Paul R. Halmos. *Naive Set Theory.* Springer New York, NY, 1998.