

## CHAPTER FOUR: THE NATURAL NUMBERS, INDUCTION, AND RECURSIVE DEFINITION

### 1 The Natural Numbers

In Chapter 1, we introduced 0 (aka  $\emptyset$ ), its successor  $1 = s(0) = 0 \cup \{0\} = \{0\}$ , 1's successor  $2 = s(1) = 1 \cup \{1\} = \{0, 1\}$ , and 2's successor  $3 = s(2) = 2 \cup \{2\} = \{0, 1, 2\}$ . This is how the first four natural numbers are usually modelled within set theory; it's intuitively obvious that we could go on in the same way to model as many of the natural numbers as time would permit. Note that  $0 \in 1 \in 2 \in 3 \in \dots$  and  $0 \subseteq 1 \subseteq 2 \subseteq 3 \dots$ . Is there a set consisting of *all* the natural numbers? The assumptions we made in Chapter 1 do not seem to enable us to draw this conclusion. It would be most useful to have such a set, but we are not yet quite in a position to add the assumption that there is a set whose members are precisely the natural numbers, since so far we haven't said what a natural number is! But we are about to.

A set  $A$  is called **inductive** iff it contains the successor of each of its members and it contains 0, i.e. iff

$$0 \in A \wedge \forall x(x \in A \rightarrow s(x) \in A)$$

We then define a **natural number** to be a set which belongs to every inductive set. It is not hard to show that 0, 1, 2, and 3 are all natural numbers. But at this stage, for all we know, *every* set might be a natural number. After all, even though we defined what it means for a set to be inductive, at this point we don't know that there *are* any inductive sets! What if there weren't any? In that case, it's easy to see that indeed every set would be a natural number. And then, since (as we already know) there is no set of all sets, there could not be a set of all the natural numbers. So if we want there to be a set of all natural numbers, there better be at least one inductive set.

We now add to our assumptions about sets the following:

**Assumption 7 (Natural Numbers)** There is a set whose members are the natural numbers.

By Extensionality, there can only be one such set. We call it  $\omega$ . With the help of this assumption, it is now easy to prove the following two theorems:<sup>1</sup>

---

<sup>1</sup>A **theorem** is just something important that we can prove. More generally, something that we can prove is usually called a **proposition**. (Note: this is a different use of the term *proposition* than in linguistic semantics, where it refers to the interpretation of a

**Theorem:**  $\omega$  is inductive.

**Proof:** Exercise.

**Theorem:**  $\omega$  is a subset of every inductive set.

**Proof:** Exercise.

The relation  $<$  (read **less than**) on  $\omega$  is defined by  $n < m$  iff  $n \in m$ , and the relation  $\leq$  (read **less than or equal to**) by  $n \leq m$  iff  $n < m$  or  $n = m$ . (So  $\leq$  is the reflexive closure of  $<$ .)<sup>2</sup> The terminology “less than or equal to” is justified, since in fact  $\leq$  is an order, as we will show. In fact we will show more, namely that  $\leq$  is a well-ordering (and in particular a linear order).

## 2 Induction and Recursive Definition

The following theorem is a corollary of the preceding one:

**Theorem (Principle of Mathematical Induction):** The only inductive subset of  $\omega$  is  $\omega$ .

**Proof:** Exercise.

The Principle of Mathematical Induction (PMI) is one of the mathematician’s most important resources for proving theorems. It is applicable any time we want to prove that a condition  $\phi[n]$  is true for every natural number  $n$ . The trick is to consider the set  $\{n \in \omega \mid \phi[n]\}$  and show that it is inductive. To put it another way, we first prove  $\phi[0]$  (this is called the **base case** of the proof) and then prove that, if we assume  $\phi[k]$  for an arbitrary natural number  $k$  (the so-called **inductive hypothesis**), then  $\phi[s(k)]$  follows (the so-called **inductive step**). By way of illustration, we prove the following:

**Proposition:** Let  $\text{suc} : \omega \rightarrow \omega$  be the function that maps each natural number to its successor. Then  $\text{ran}(\text{suc}) = \omega \setminus \{0\}$ .

**Proof:** Obviously  $0 \notin \text{ran}(\text{suc})$ . Let  $T$  be the set of all natural numbers that are either 0 or else the successor of some natural number. We must show that  $T$  is inductive, that is that (1)  $0 \in T$  and (2) for each  $n \in T$ ,  $\text{suc}(n) \in T$ . But both of these are immediate consequences of the definition of  $T$ .  $\square$

Why do we persist in saying “ $\text{suc}(n)$ ” instead of “ $1+n$ ”? Answer: because the operation of addition for natural numbers has not been defined

---

declarative sentence utterance.) So a theorem is an important proposition. A **lemma** is a proposition which is not so important in and of itself, but which is used in order to prove a theorem. And a **corollary** of a proposition is another proposition which is easily proved from it.

<sup>2</sup>Later we will be able to prove that, for any two natural numbers  $n$  and  $m$ ,  $n < m$  iff  $n \subsetneq m$ , and  $n \leq m$  iff  $n \subseteq m$ .

yet. Yet it seems clear how addition works: for any natural number  $m$ ,  $m+0$  should be  $m$ ; and if  $k$  is nonzero (so that it is the successor of some other natural number  $n$ ), then  $m+k$  should be the successor of  $m+n$ . That is, for each  $m \in \omega$  we would like to *define* addition by the equations

$$m + 0 = m$$

and

$$m + \text{suc}(n) = \text{suc}(m + n)$$

Definitions of this kind are called **recursive**. But how do we know recursive definitions make sense? The answer is provided by the Recursion Theorem, henceforth abbreviated RT:

**Theorem (RT):** Let  $X$  be a set,  $x \in X$ , and  $F: X \rightarrow X$ . Then there exists a unique function  $h: \omega \rightarrow X$  such that (1)  $h(0) = x$ , and (2) for every  $n \in \omega$ ,  $h(\text{suc}(n)) = F(h(n))$ .

RT is not hard to prove, but the proof is a bit long. So we relegate it to an appendix, and turn straightaway to some applications.

### 3 Arithmetic

#### 3.1 Addition

As our first application of RT, let's show that the informal recursive definition of addition given above actually makes sense.

To get started, suppose  $m \in \omega$ . We'll use RT to show there is a function  $A_m$  such that  $A_m(0) = m$  and  $A_m(\text{suc}(n)) = \text{suc}(A_m(n))$ . The trick, as always when applying RT, is to find the right instantiations of  $X$ ,  $x$ , and  $F$ . In the present case the happy choices are  $X = \omega$ ,  $x = m$ , and  $F = \text{suc}$ ; with these choices, the function  $h$  whose unique existence is guaranteed by RT has just the properties we want for  $A_m$ . We then define the **addition** operation  $+: \omega^{(2)} \rightarrow \omega$  such that, for all  $m, n \in \omega$ ,  $m + n =_{\text{def}} A_m(n)$ . It follows from this definition that  $m + 0 = m$  for all  $m \in \omega$  and  $m + \text{suc}(n) = \text{suc}(m + n)$  for all  $m, n \in \omega$ , as desired.

**Theorem:** For every natural number  $n$ ,  $1 + n = \text{suc}(n)$ .

**Proof:** Exercise.

## 3.2 Multiplication

Turning next to multiplication, we first use RT to define multiplication by a fixed natural number  $m$ . We want a function  $M_m$  such that (1)  $M_m(0) = 0$ , and (2) for every  $n \in \omega$ ,  $M_m(\text{suc}(n)) = m + M_m(n)$ . To this end, we apply RT again, this time with  $X = \omega$ ,  $x = 0$ , and  $F = A_m$ . We then define the **multiplication** operation  $\cdot : \omega^{(2)} \rightarrow \omega$  such that  $m \cdot n =_{\text{def}} M_m(n)$ . So  $m \cdot 0 = 0$  and  $m \cdot (1 + n) = m + m \cdot n$ , which is as it should be.

**Theorem:** For every  $n \in \omega$ ,  $1 \cdot n = n$ .

**Proof:** Exercise.

With more time and ambition, one can also prove the familiar Five Laws of Arithmetic (hereafter we omit the “.” for multiplication):

1. Associativity of Addition:  $m + (n + p) = (m + n) + p$
2. Commutativity of Addition:  $m + n = n + m$
3. Distributivity of Multiplication Over Addition:  $m(n + p) = mn + mp$
4. Associativity of Multiplication:  $m(np) = (mn)p$
5. Commutativity of Multiplication:  $mn = nm$

Yet another good exercise is to give a recursive definition of the **exponentiation** operation  $m \star n = m^n$  and prove that the definition makes sense. Hint: define  $m \star n$  to be  $E_m(n)$  where  $E_m(0) = 1$  and  $E_m(\text{suc}(n)) = m \cdot E_m(n)$ . This establishes the first two of the following three general properties of exponentiation:

1.  $m^0 = 1$
2.  $m^{1+n} = m(m^n)$
3.  $m^{n+p} = (m^n)(m^p)$

Note that the second is a special case of the third, which is usually called the **Law of Exponents**.

### 3.3 The Infinitude of the Natural Numbers

Everyone knows that there is an infinite number of natural numbers, but what exactly does that mean? A set is called **finite** if it is in one-to-one correspondence with a natural number, and **infinite** otherwise. A set is called **Dedekind infinite** if it is in one-to-one correspondence with a proper subset of itself. On the basis of the assumptions we've made so far about sets, it's possible to prove (see Chapter 5) that any Dedekind-infinite set is infinite.<sup>3</sup> Since we already know that  $\text{ran}(\text{suc}) = \omega \setminus \{0\}$ , we could then show  $\omega$  is infinite if we could show that  $\text{suc}: \omega \rightarrow \omega$  is injective. This is of course the case; a sketch of a proof follows.

First, we define a set  $A$  to be **transitive** iff every member of a member of  $A$  is itself a member of  $A$ . It is easy to see that all three of the following conditions on a set  $A$  are equivalent to transitivity:

1.  $(\bigcup A) \subseteq A$ ;
2. every member of  $A$  is a subset of  $A$ ; and
3.  $A \subseteq \wp(A)$ .

The proof that  $\text{suc}$  is injective requires a couple of preliminary results:

**Lemma 1:** If  $A$  is transitive, then  $\bigcup s(A) = A$ .

**Proof:** We use the (easily proved) general fact about union that

$$\bigcup (x \cup y) = \left( \bigcup x \right) \cup \left( \bigcup y \right)$$

and reason as follows:

$$\begin{aligned} \bigcup s(A) &= \bigcup (A \cup \{A\}) \\ &= \left( \bigcup A \right) \cup \left( \bigcup \{A\} \right) \\ &= \left( \bigcup A \right) \cup A \\ &= A \quad \square \end{aligned}$$

---

<sup>3</sup>To prove the converse, however, we need an additional assumption, viz. the Assumption of Choice (AC, Chapter 5). AC also enables us to prove that  $\omega$  is the "smallest" infinite set, in the sense of being in one-to-one correspondence with a subset of any other infinite set.

The last step follows from the fact that  $\bigcup A \subseteq A$  for transitive  $A$ .  $\square$

**Lemma 2:** Every natural number is transitive.

**Proof:** Exercise.

**Theorem:**  $\text{suc}$  is injective.

**Proof:** Suppose  $\text{suc}(m) = \text{suc}(n)$ . Then  $\bigcup \text{suc}(m) = \bigcup \text{suc}(n)$ . But  $m$  and  $n$  are transitive (by Lemma 2), so (by Lemma 1)  $\bigcup \text{suc}(m) = m$  and  $\bigcup \text{suc}(n) = n$ . Therefore  $m = n$ .  $\square$

As noted above, the infinitude of  $\omega$  is a corollary of this.

### 3.4 The Well-Ordering of $\omega$

We now have the resources to establish that the relation  $\leq$  on  $\omega$  is an order, indeed a well-ordering (i.e. a chain such that every nonempty subset of  $\omega$  has a least member). Given how obvious this seems, the argumentation required is surprisingly intricate and too long to reproduce in full detail here, so we content ourselves with an outline, including key lemmata and proof sketches.

Recall that by definition  $m < n$  iff  $m \in n$ , and  $m \leq n$  iff  $m < n$  or  $m = n$ .

**Theorem:** For all  $n \in \omega$ ,  $n = \{m \in \omega \mid m < n\}$ .

**Proof:** To show inclusion, suppose  $m \in n$ . Since  $\omega$  is transitive,  $m \in \omega$ . Then  $m < n$ . To show the reverse inclusion, suppose  $m < n$ . Then by definition,  $m \in n$ .  $\square$

**Lemma 3:** For all  $m, n \in \omega$ ,  $m < \text{suc}(n)$  iff  $m \leq n$ .

**Proof:**  $m < \text{suc}(n)$  iff  $m \in \text{suc}(n)$  iff  $m \in n \cup \{n\}$  iff  $m \in n$  or  $m \in \{n\}$  iff  $(m \in n \text{ or } m = n)$  iff  $m \leq n$ .  $\square$

**Lemma 4:** For all  $m, n \in \omega$ ,  $m \in n$  iff  $\text{suc}(m) \in \text{suc}(n)$ .

**Proof:** For the only-if direction, assume  $\text{suc}(m) \in \text{suc}(n)$ . Then  $\text{suc}(m) < \text{suc}(n)$ , so by Lemma 3,  $\text{suc}(m) \leq n$ , i.e. either  $\text{suc}(m) \in n$  or  $\text{suc}(m) = n$ . If  $\text{suc}(m) \in n$ , then  $m \in \text{suc}(m) \in n$ , so  $m \in n$  by transitivity. Otherwise  $\text{suc}(m) = n$ ; but  $\text{suc}(m) = m \cup \{m\}$ , from which it follows easily that  $m \in n$ .

For the if direction, we use PMI. Let  $T = \{n \in \omega \mid \forall m \in n, \text{suc}(m) \in \text{suc}(n)\}$ . It is sufficient to show that  $T$  is inductive. This is left as an exercise.  $\square$

**Lemma 5:** For all  $n \in \omega$ ,  $n \notin n$ .

**Proof:** This is another inductive proof. Let  $T = \{n \in \omega \mid n \notin n\}$ . It suffices to show  $T$  is inductive. The base case is trivial, and the inductive step is an easy consequence of Lemma 4.  $\square$

**Theorem:**  $<$  is transitive, irreflexive, and connex.

**Proof:** Transitivity follows readily from Lemma 2 and irreflexivity from Lemma 5. Connexity is proved inductively, by showing that the set  $T = \{n \in \omega \mid \forall m \in \omega \mid m \neq n \rightarrow (n \in m \vee m \in n)\}$  is inductive; the inductive step of the proof appeals to both Lemma 4 and Lemma 3.  $\square$

As two easy consequences of this theorem, we have the following

**Corollary 1:** For all  $m, n \in \omega$ ,  $m \in n$  iff  $m \subsetneq n$ .

**Corollary 2:**  $\leq$  is a chain.

And finally:

**Theorem:**  $\leq$  is a well-ordering.

**Proof:** Suppose  $A \subseteq \omega$  has no least element, It suffices to show  $A = \emptyset$ . To this end, let  $B$  be the set of all natural numbers  $n$  such that no natural number less than  $n$  belongs to  $A$ . All that is required is to show  $B$  is inductive. This is left as an exercise. (Hint: use Lemma 3 in the inductive step.)  $\square$

## 4 Transitive Closure and Reflexive Transitive Closure

Let  $R$  be a binary relation on  $A$ . Then informally, the **transitive closure** of  $R$ , written  $R^+$ , is usually “defined” as follows: For all  $n \in \omega$ , recursively define  $h(n)$  by  $h(0) = \text{id}_A$ ,  $h(1) = R$ , and  $h(n+1) = h(n) \circ R$ . Then  $R^+ =_{\text{def}} \bigcup_{n>0} h(n)$ . We leave as an exercise the formal justification of this definition using RT. Similarly, the **reflexive transitive closure** of  $R$ , written  $R^*$ , is  $\bigcup_{n \in \omega} h(n)$ . Note that  $R^* = R^+ \cup \text{id}_A$ .

**Lemma 6:** The intersection of a set of transitive relations is itself transitive.

**Proof:** Exercise.

**Theorem:** The transitive closure of  $R$  is the intersection of all the transitive relations of which  $R$  is a subset, i.e.

$$R^+ = \bigcap \{S \subseteq A^{(2)} \mid R \subseteq S \text{ and } S \text{ is transitive}\}$$

**Proof:** Exercise.

**Corollary:**  $R^+$  is transitive.

**Proof:** Exercise.

## 5 Hasse Diagrams

A **Hasse diagram** is a kind of textual (paper or blackboard) diagrammatic representation of a preorder  $\sqsubseteq$  on a set  $A$ , made up of dots and straight line segments directly connecting two dots (here “directly” means there are no dots on the line segment other than the two being connected). The line segments are of two kinds: (1) nonhorizontal (i.e. either slanting or vertical) single line segments, and (2) horizontal double line segments. The interpretation is as follows: the dots represent the members of  $A$ ; if (the dots representing)  $b$  and  $a$  are connected by a single nonhorizontal line segment and  $b$  is higher (on the page or board) than  $a$ , then  $a < b$ ; and if  $a$  and  $b$  are connected by a horizontal double line segment, then  $a$  and  $b$  are ‘tied’, i.e.  $a \sqsubseteq b$  and  $b \sqsubseteq a$ . (So if  $\sqsubseteq$  is an order, there will be no horizontal double line segments.)

Any finite preorder can be represented by a Hasse diagram, but not every infinite one can. (There can be infinite Hasse diagrams, but there is not enough time to draw all of one! Sometimes the gist of an infinite Hasse diagram can be conveyed with judicious use of ellipsis (“and so on”) dots, though.) For antisymmetric preorders (i.e. orders) the property of being representable by a Hasse diagram is easy to express precisely in set-theoretic terms: it is the property of being the reflexive transitive closure of its own covering relation. It can be shown (though the details are a bit tedious) that any finite order has this property.

## Appendix: Proving the Recursion Theorem