6. Natural numbers and finite sets

January 25, 2007

Here we develop the basic facts about natural numbers, and about finite sets. We expect that most of these facts will be familiar to the reader, but their rigorous development may be new. Once the basic facts are developed, we prove the important recursion theorem, which forms the basis for many "definitions by induction". Then we give the definition and elementary properties of addition, multiplication, and exponentiation; this is something that may be very familiar to the reader. The basic facts about finite sets are then given; most of these facts should be known to the reader, but they are carefully proven. Then we give an important theorem about the closure of a set under operations. Here we expect that the reader may be familiar only with special cases of the theorem.

The definition of the natural numbers depends on another axiom.

Axiom 8. (*Infinity*) **There is a set A such that $\emptyset \in A$, and for every $a \in A$, also $a \cup \{a\} \in A$.**

The infinity axiom gives us the set of natural numbers, according to the following theorem. The intuition is helped by noting that later it will turn out that $m + 1 = m \cup \{m\}$ for every natural number m.

Theorem 6.1. *There is exactly one set B with the following properties:*
(i) $\emptyset \in B$.
(ii) For all $x \in B$, $x \cup \{x\} \in B$.
(iii) For every subset C of B, if C satisfies (i) and (ii), i.e., if
(a) $\emptyset \in C$,
(b) for all $x \in C$, also $x \cup \{x\} \in C$,

then $C = B$.

Proof. Let A be given by the infinity axiom. Thus $\emptyset \in A$, and for all $x \in A$, also $x \cup \{x\} \in A$. We define

$$B = \bigcap \{C \subseteq A : \emptyset \in C \text{ and for all } x \in C[x \cup \{x\} \in C]\}.$$

Note that A satisfies the condition on C, so we are taking the intersection of a nonempty collection. For brevity, let

$$\mathscr{C} = \{C \subseteq A : \emptyset \in C \text{ and for all } x \in C[x \cup \{x\} \in C]\}.$$

Note that $B \subseteq A$ since $A \in \mathscr{C}$. Since $\emptyset \in C$ for all $C \in \mathscr{C}$, it follows that $\emptyset \in B$. Suppose that $x \in B$. Then for any $C \in \mathscr{C}$ we have $x \in C$, hence $x \cup \{x\} \in C$ by the definition of $\mathscr{C}$. So $x \cup \{x\} \in B$.

Now suppose that (iii)(a),(b) hold for C, where $C \subseteq B$. This means that $C \in \mathscr{C}$. Hence $B \subseteq C$, so $B = C$.

The argument so far shows that B exists as in the theorem. If B' also satisfies the conditions of the theorem, then $B \cap B'$ satisfies (iii)(a),(b),and hence $B \cap B' = B$ since the

conditions of the theorem hold for B, and $B \cap B' = B'$ since the conditions of the theorem hold for B'. Thus $B = B'$. □

The set indicated in Theorem 4.1 is denoted by ω; this is the *set of all natural numbers.* We usually use letters like i, j, k, l, m, n for members of ω. Note that different notations are used in many mathematics books; $\mathbb{N}$ is an example. We also define

• $0 = \emptyset$; $1 = 0 \cup \{0\}$, $2 = 1 \cup \{1\}$, $3 = 2 \cup \{2\}$.

Note that the number 0 is *defined* to be the empty set. Nevertheless, it is standard mathematical usage to continue to use "$\emptyset$" when we are really thinking of the empty set, and to use "0" when we are thinking of the number. Working out the definitions of 1,2,3, we have

$$\begin{aligned} 1 &= 0 \cup \{0\} \\ &= \{0\}; \\ 2 &= 1 \cup \{1\} = \{0\} \cup \{1\} \\ &= \{0, 1\}; \\ 3 &= 2 \cup \{2\} = \{0, 1\} \cup \{2\} \\ &= \{0, 1, 2\}. \end{aligned}$$

So each of 1,2,3 is the set of all previous natural numbers. After we define $<$ on ω we will see that this is a general fact: each natural number is the set of all previous natural numbers.

The usual induction principle follows immediately from the definition:

Theorem 6.2. *Suppose that $C \subseteq \omega$ and the following two conditions hold:*
(i) $0 \in C$.
(ii) $\forall m \in C[m \cup \{m\} \in C]$.

Then $C = \omega$. □

Our next goal is to describe some peculiar features of our notion of natural number, and to introduce the usual order on ω.

Proposition 6.3. *If $m \in \omega$, then $m \subseteq \omega$. In words: every member of a natural number is also a natural number.*

Proof. We prove this by induction. For our first few applications of induction, we explicitly use Theorem 6.2. Later we shall, as is usual, be less formal about this. Let

$$C = \{m \in \omega : m \subseteq \omega\}.$$

Since $0 \subseteq A$ for every set A, obviously $0 \in C$. Now suppose that $m \in C$. Then $m \subseteq \omega$ and $C \subseteq \omega$, so $m \cup \{m\} \subseteq \omega$. So $m \cup \{m\} \in C$.

It follows from 6.2 that $C = \omega$. □

Proposition 6.4. *If $m \in \omega$ and $n \in m$, then $n \subseteq m$.*

Proof. Again we proceed by induction. Let

$$C = \{m \in \omega : \text{ for all } n \in m[n \subseteq m]\}.$$

Then $0 \in C$, trivially. Suppose that $m \in C$. Then $m \in \omega$, hence $m \cup \{m\} \in \omega$. To show that $m \cup \{m\} \in C$, suppose that $n \in m \cup \{m\}$. If $n \in m$, then $n \subseteq m \subseteq m \cup \{m\}$ because $m \in C$. If $n = m$, trivially $n \subseteq m \cup \{m\}$. Hence $m \cup \{m\} \in C$.

It follows from 6.2 that $C = \omega$. □

Proposition 6.5. *If $m, n \in \omega$, then $m \subset n$ iff $m \in n$.*

Proof. Fix $m \in \omega$; we prove the desired result by induction on n. Let

$$C = \{n \in \omega : m \subset n \text{ iff } m \in n\}.$$

Then $0 \in C$ since both $m \subset 0$ and $m \in 0$ are false. Now suppose that $n \in C$.

If $m \subset n \cup \{n\}$, then $n \notin m$; otherwise, $n \subseteq m$ by 6.4, hence $n \cup \{n\} \subseteq m$, hence $n \cup \{n\} = m$, contradiction. It follows that $m \subseteq n$. If $m = n$, then $m \in n \cup \{n\}$, as desired. If $m \neq n$, then $m \subset n$, so $m \in n \subseteq n \cup \{n\}$ because $n \in C$.

Conversely, suppose that $m \in n \cup \{n\}$. If $m \in n$, then $m \subset n$ because $n \in C$, so $m \subset n \cup \{n\}$. If $m = n$, then clearly $m \subset n \cup \{n\}$.

This proves that $n \cup \{n\} \in C$. Hence $C = \omega$. □

Proposition 6.6. *For all $m, n \in \omega$ we have $m \in n$, $m = n$, or $n \in m$.*

Proof. Let

$$C = \{m \in \omega : \text{for all } n \in \omega[m \in n \text{ or } m = n \text{ or } n \in m]\}.$$

First, $0 \in C$. In fact, suppose that $n \in \omega$. If $n \neq 0$, then $0 \subset n$, and so $0 \in n$ by 6.6. This shows that $0 \in C$.

Now suppose that $m \in C$. Take any $n \in \omega$; we want to show that

$$(*) \qquad m \cup \{m\} \in n \text{ or } m \cup \{m\} = n \text{ or } n \in m \cup \{m\}.$$

Using the fact that $m \in C$, we have three cases.

Case 1. $m \in n$. Now $m \subset n$ by 6.5, so $m \cup \{m\} \subseteq n$. Hence either $m \cup \{m\} = n$, or else $m \cup \{m\} \subset n$ and consequently $m \cup \{m\} \in n$ by 6.5. At any rate, $(*)$ holds.

Case 2. $m = n$. Then $n \in m \cup \{m\}$, so $(*)$ holds.

Case 3. $n \in m$. Then $n \in m \cup \{m\}$, so $(*)$ holds.

So, we have proved $(*)$. Hence $m \cup \{m\} \in C$.

Now $C = \omega$ by the induction principle. □

We have proved enough properies of membership between natural numbers to intuitively justify using the notation $m < n$ instead of $m \in n$ between natural numbers. In fact, so far we know, for all $m, n, p \in \omega$,

- $m \notin m$ (by 3.14)

- if $m \in n$ and $n \in p$, then $m \in p$ (by 6.4, since $n \in p$ implies that $n \subseteq p$);
- $m \in n$ or $m = n$ or $n \in m$ (by 6.6).

So, using $<$ in place of $\in$ (*only* for natural numbers), we get the usual irreflexivity, transitivity, and trichotomy laws for order. That is, we now have a linear order on ω. In accordance with our general notation for partial orders, we also define $m \leq n$ to mean that $m < n$ or $m = n$.

Proposition 6.7. *For any $m, n \in \omega$ we have $n \in m \cup \{m\}$ iff $n \leq m$.* □

Now we can prove the principle of complete induction:

Theorem 6.8. *Suppose that $C \subseteq \omega$, and the following condition holds:*

(*) For every $m \in \omega$, if every natural number less than m is in C, then $m \in C$.

Then $C = \omega$.

Proof. Let $D = \{m \in \omega : n \in C \text{ for every } n < m\}$. Thus vacuously $0 \in D$. Suppose that $m \in D$. To show that $m \cup \{m\} \in D$, assume that $n < m \cup \{m\}$. Thus $n < m$ or $n = m$. If $n < m$, the assumption $m \in D$ implies that $n \in C$. If $n = m$, then for every $p \in \omega$, if $p < m$ then $p \in C$ because $m \in D$, and by $(*)$ it follows that $n = m \in C$. Thus $n \in C$ under each possibility. This proves that $m \cup \{m\} \in D$.

By the induction principle it follows that $D = \omega$. Now given $m \in \omega$ we have $m \cup \{m\} \in \omega$, hence $m \cup \{m\} \in D$. Since $m < m \cup \{m\}$, it follows from the definition of D that $m \in C$. So $C = \omega$. □

There are three principles related to induction: induction itself, complete induction, and the least element principle, which we now give:

Theorem 6.9. *Any nonempty set of natural numbers has a least element.*

Proof. Suppose that A is a nonempty set of natural numbers without a least element. We prove then that $\omega \backslash A = \omega$, from which it follows that $A = \emptyset$, a contradiction. To prove this, we use complete induction, Theorem 6.8. Thus assume that $m \in \omega$, and every natural number less than m is a member of $\omega \backslash A$. If $m \in A$, then obviously m is the least element of A. So $m \in \omega \backslash A$. Thus by the complete induction principle, $\omega \backslash A = \omega$. □

Thus we have now shown that $(\omega, <)$ is a well-ordering.

A *finite sequence* is a function whose domain is a natural number. This notion will be used frequently in what follows. If f is a finite sequence, with domain $m \in \omega$, we sometimes denote f by $\langle f_0, \ldots, f_{m-1} \rangle$.

We next turn to the important fact that definitions can be made by induction; such definitions are called *recursive definitions*.

Theorem 6.10. (Recursion theorem for ω) *Suppose that A is a set. Let $B = \bigcup_{m \in \omega} {}^m A$. Assume that $g : B \to A$. Then there is a unique function $f : \omega \to A$ such that $f(m) = g(f \restriction m)$ for every $m \in \omega$.*

Proof. The idea of the proof is to build up the function f from approximations to it. The collection of all approximations is the following set.

$$\mathscr{F} = \{h : \text{ there is an } m \in \omega \text{ such that } h : m \to A \text{ and for all } n < m[h(n) = g(h \restriction n)]\}.$$

Since any h mentioned in this definition is a member of B, this is a legal definition. We are going to show that any two approximations are comparable under $\subseteq$; then Corollary 3.6 applies to show that their union is a function, and then we show that the union is a function as desired in the theorem. Uniqueness is proved separately.

(1) If $h, k \in \mathscr{F}$, $h : m \to A$, $k : n \to A$, and $m \leq n$, then $h = k \restriction m$.

In fact, we really just need to show that $h(i) = k(i)$ for all $i < m$. Suppose that this fails, and let $i < m$ be minimum such that $h(i) \neq k(i)$. Then $h \restriction i = k \restriction i$ and hence $h(i) = g(h \restriction i) = g(k \restriction i) = k(i)$, contradiction.

(2) For every $m \in \omega$ there is an $h \in \mathscr{F}$ such that $\mathrm{dmn}(h) = m$.

We prove this by induction on m. Clearly $\emptyset \in \mathscr{F}$, so it holds for $m = 0$. Suppose it is true for m, and let $h \in \mathscr{F}$ be such that $\mathrm{dmn}(h) = m$. Define $k = h \cup \{(m, g(h))\}$. Clearly then $k : m \cup \{m\} \to A$. If $n < m$, then $h(i) = k(i)$ for each $i \leq n$, and so $h \restriction n = k \restriction n$ and consequently

$$k(n) = h(n) = g(h \restriction n) = g(k \restriction n).$$

Also, $k \restriction m = h$ and $k(m) = g(h) = g(k \restriction m)$. Thus $k \in \mathscr{F}$ and $\mathrm{dmn}(k) = m \cup \{m\}$. This finishes the inductive proof of (2).

Let $f = \bigcup_{h \in \mathscr{F}} h$. We claim that h is the desired function. It is a function by (1) and Corollary 3.6. Its domain is ω by (2). Finally, if $m \in \omega$, choose $h \in \mathscr{F}$ such that $\mathrm{dmn}(h) = m \cup \{m\}$. Then

$$f(m) = h(m) = g(h \restriction m) = g(f \restriction m).$$

This finishes the proof of existence of f.

Suppose that l also satisfies the conditions of the theorem. We prove that $f(m) = l(m)$ for all $m \in \omega$ by complete induction (hence $f = l$). Suppose that $f(m) = l(m)$ for all $m < n$. Then $f \restriction n = l \restriction n$, and so

$$f(n) = g(f \restriction n) = g(l \restriction n) = l(n). \qquad \square$$

Our first application of 6.10 is to define addition of natural numbers.

Lemma 6.11. *For every natural number m there is a unique function $f : \omega \to \omega$ such that $f(0) = m$ and for every natural number n, $f(n \cup \{n\}) = f(n) \cup \{f(n)\}$.*

Proof. Let m be given, and define $B = \bigcup_{n \in \omega} {}^n\omega$. Define $g : B \to \omega$ by setting

$$g(\emptyset) = m;$$
$$g(k) = k(n) \cup \{k(n)\} \quad \text{if } k \in B \text{ and } \mathrm{dmn}(k) = n \cup \{n\}.$$

Then obtain $f : \omega \to \omega$ by 6.10. Thus for every natural nunber n, $f(n) = g(f \restriction n)$. Hence for every natural number n,

$$\begin{aligned} f(0) &= g(f \restriction 0) = g(\emptyset) = m; \\ f(n \cup \{n\}) &= g(f \restriction (n \cup \{n\})) \\ &= (f \restriction (n \cup \{n\}))(n) \cup \{(f \restriction (n \cup \{n\}))(n)\} \\ &= f(n) \cup \{f(n)\}. \end{aligned}$$

This proves the existence of f as wanted in the lemma. For uniqueness, suppose that h also works: $h(0) = m$ and for every natural number n, $h(n \cup \{n\}) = h(n) \cup \{h(n)\}$. We prove that $f(n) = h(n)$ for every $n \in \omega$ by induction on n. We have $f(0) = m = h(0)$. Suppose that $f(n) = h(n)$. Then

$$f(n \cup \{n\}) = f(n) \cup \{f(n)\} = h(n) \cup \{h(n)\} = h(n \cup \{n\}),$$

finishing the inductive proof. So $f = h$. □

We denote by pl_m the unique function given by 6.11. Then we define, for any $m, n \in \omega$,

$$m + n = \mathrm{pl}_m(n).$$

Thus the crucial properties of addition are that for any natural numbers m, n,

$$\begin{aligned} m + 0 &= m, \\ m + (n \cup \{n\}) &= (m + n) \cup \{m + n\}. \end{aligned}$$

Lemma 6.12. $m + 1 = m \cup \{m\}$.

Proof. $m + 1 = (m + 0) \cup \{m + 0\} = m \cup \{m\}$. □

Lemma 6.12 is the result promised earlier. Using it and the definition of $<$, earlier results can be given a more familiar form. For example:

• Theorem 6.2 (induction principle): *Suppose that $C \subseteq \omega$ and the following two conditions hold:*

(i) $0 \in C$.

(ii) $\forall m \in C[m + 1 \in C]$.

Then $C = \omega$.

• Proposition 6.7: *For any $m, n \in \omega$ we have $n < m + 1$ iff $n \leq m$.*

Theorem 6.13. *Let $m, n \in \omega$. Then:*

(i) $m + 0 = m$;

(ii) $m + (n + 1) = (m + n) + 1$. □

This theorem is what we have been aiming for, and is all that we shall use in the future from the definition of addition.

Basic properties of addition now follow by induction:

Theorem 6.14. *Let $m, n, p \in \omega$. Then*
(i) $m + (n + p) = (m + n) + p$.
(ii) $0 + m = m$.
(iii) $m + 1 = 1 + m$.
(iv) $m + n = n + m$.

These are all easy inductions using 6.13, and we do only (i) and (iv), leaving the others to an exercise.

$$(m + (n + 0) = m + n = (m + n) + 0;$$

assume that $m + (n + p) = (m + n) + p$. Then

$$m+(n+(p+1)) = m+((n+p)+1) = (m+(n+p))+1 = ((m+n)+p)+1 = (m+n)+(p+1);$$

so (i) holds.

For (iv), $m + 0 = m = 0 + m$ using (ii). Assume that $m + n = n + m$. Then

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

So (iv) holds. □

Proposition 6.15. *(i) For any nonzero natural number m there is a natural number n such that $m = n + 1$.*
(ii) If $m, n \in \omega$ and $m + n = 0$, then $m = 0$ and $n = 0$.
(iii) If $m, n, p \in \omega$ and $m + p = n + p$, then $m = n$.

Proof. (i): This can be proved by a trivial induction on m.

(ii): Assume that $m + n = 0$ but $n \neq 0$. By (i), write $n = p + 1$ with $p \in \omega$. Then $m+n = m+(p+1) = (m+p)+1$. But obviously $(m+p)+1 \neq 0$, contradiction. Similarly if $m \neq 0$.

(iii): An easy induction on p. □

The next results indicate connections between ordering and addition.

Proposition 6.16. *Assume that $m, n \in \omega$.*
(i) $m < n + 1$ iff $m \leq n$.
(ii) $m \leq n$ iff there is a $p \in \omega$ such that $m + p = n$.
(iii) $m < n$ iff there is a nonzero $p \in \omega$ such that $m + p = n$.

Proof. For (i), since $n+1 = n\cup\{n\}$ this is obvious by the way the ordering is defined.

For (ii), we first prove

(1) If $m, p \in \omega$ and $p \neq 0$, then $m < m + p$.

We prove this by induction on p. It is vacuously true for $p = 0$. (The hypothesis is false.) Assume it for p. If $p = 0$, then $m \in m \cup \{m\} = m + 1$, so the conclusion holds for 1, which is $p + 1$. Suppose that $p \neq 0$. Then by the induction assumption we have $m < m + p$. Clearly $m + p < m + p + 1$ (by the argument for $p = 0$). So $m < m + p + 1$, finishing the inductive proof of (1).

Now the direction $\Leftarrow$ in (iii) follows from (1). Since $m + 0 = m$, the direction $\Leftarrow$ in (ii) follows from (1).

Now for a fixed m we prove by induction on n that

(2) If $m \leq n$, then there is a p such that $m + p = n$.

For $n = 0$, note that $m \leq 0$ implies that $m = 0$, so we can take $p = 0$. Now assume that the implication holds for n. Suppose that $m \leq n+1$. If $m = n+1$, then again we can take $p = 0$. Suppose that $m < n + 1$. Then by (i), $m \leq n$, so the induction hypothesis applies, and we get p such that $m + p = n$. Hence $m + p + 1 = n + 1$, finishing the inductive proof of (2).

Of course, (2) is the direction $\Rightarrow$ in (ii). For the direction $\Rightarrow$ in (iii), by (ii) we get p such that $m + p = n$, and we must have $p \neq 0$ since $m \neq n$. □

Proposition 6.17. *For any natural numbers m, n, p, q, if $m \leq p$ and $n \leq q$ then $m + n \leq p + q$. Moreover, if one of the inequalities in the hypothesis is strict, then so is the inequality in the conclustion.*

Proof. Assume the hypothesis. By 6.16(ii) there are natural number s, t such that $m + s = p$ and $n + t = q$. Hence $m + n + s + t = m + s + n + t = p + q$, so $m + n \leq p + q$ by 6.16(ii).

If one of the inequalities in the hypothesis is strict, then $s \neq 0$ or $t \neq 0$. Hence by 6.15(ii), $s + t \neq 0$, and hence $m + n < p + q$ by 6.16(iii). □

Proposition 6.18. *For any natural numbers m, n, p, $m + n < m + p$ iff $n < p$.*

Proof. For $\Rightarrow$, choose $q \neq 0$ so that $m + n + q = m + p$. Then $n + q = p$, so $n < p$.
For $\Leftarrow$, choose $q \neq 0$ so that $n+q = p$. Then $m+n+q = m+p$, so $m+n < m+p$. □

Next we define multiplication. The definition is carried out similarly to that of addition, and it depends on the following lemma.

Lemma 6.19. *For every natural number m there is a unique function $f : \omega \to \omega$ such that $f(0) = 0$ and for every natural number n, $f(n + 1) = f(n) + m$.*

Proof. Let m be given, and define $B = \bigcup_{n\in\omega} {}^n\omega$. Define $g : B \to \omega$ by setting

$$\begin{aligned} &g(\emptyset) = 0; \\ &g(k) = k(n) + m \quad \text{if } k \in B \text{ and } \mathrm{dmn}(k) = n + 1. \end{aligned}$$

Then obtain $f : \omega \to \omega$ by 6.10. Thus for every natural number n, $f(n) = g(f \restriction n)$. Hence for every natural number n,

$$\begin{aligned} f(0) &= g(f \restriction 0) = g(\emptyset) = 0; \\ f(n+1) &= g(f \restriction (n+1)) \\ &= (f \restriction (n+1))(n) + m \\ &= f(n) + m. \end{aligned}$$

This proves the existence of f as wanted in the lemma. For uniqueness, suppose that h also works: $h(0) = 0$ and for every natural number n, $h(n+1) = h(n)+m$. We prove that

$f(n) = h(n)$ for every $n \in \omega$ by induction on n. We have $f(0) = 0 = h(0)$. Suppose that $f(n) = h(n)$. Then

$$f(n+1) = f(n) + m = h(n) + m = h(n+1),$$

finishing the inductive proof. So $f = h$. □

We denote by ti_m the unique function given in 6.18. Then we define, for any $m, n \in \omega$,

$$m \cdot n = \mathrm{ti}_m(n).$$

The essential part of the definition of multiplication is summarized in the following theorem.

Theorem 6.20. *Let $m, n \in \omega$. Then:*
(i) $m \cdot 0 = 0$;
(ii) $m \cdot (n+1) = m \cdot n + m$. □

Now we can prove some simple properties of multiplication:

Theorem 6.21. *Let $m, n, p \in \omega$. Then:*
(i) $m \cdot (n+p) = m \cdot n + m \cdot p$;
(ii) $m \cdot (n \cdot p) = (m \cdot n) \cdot p$;
(iii) $0 \cdot m = 0$;
(iv) $1 \cdot m = m$;
(v) $(m+n) \cdot p = m \cdot p + n \cdot p$;
(vi) $m \cdot n = n \cdot m$;
(vii) If $m \cdot n = 0$ then $m = 0$ or $n = 0$.
(viii) If $m \neq 0$ and $m \cdot n = m \cdot p$, then $n = p$.

Proof. (i)–(vi) are easily proved by induction, in order, on p, p, m, m, p, n respectively. For (vii), assume that $m \cdot n = 0$ and $n \neq 0$. By 6.15(i) write $n = p + 1$ with $p \in \omega$. Then

$$0 = m \cdot n = m \cdot (p+1) = m \cdot p + m,$$

so $m = 0$ by 6.15(ii).

For (viii), assume that $m \neq 0$ and $m \cdot n = m \cdot p$. By symmetry say $n \leq p$. By 6.16(ii) let q be a natural number such that $n + q = p$. Then $m \cdot n = m \cdot p = m \cdot (n+q) = m \cdot n + m \cdot q$, so by 6.15(iii) we get $0 = m \cdot q$. Then by (vii), since $m \neq 0$ we have $q = 0$, and so $n = p$, as desired. □

Proposition 6.22. *Suppose that m, n, p, q are natural numbers.*
(i) If $m < n$ and $p \neq 0$, then $m \cdot p < n \cdot p$.
(ii) If $m \leq p$ and $n \leq q$, then $m \cdot n \leq p \cdot q$.
(iii) If $m < p$ and $n \leq q \neq 0$, then $m \cdot n < p \cdot q$.
(iv) If $m \leq p \neq 0$ and $n < q$, then $m \cdot n < p \cdot q$.

Proof. (i): There is an $s \neq 0$ such that $m + s = n$, by 6.16(iii). Then $n \cdot p = (m+s) \cdot p = m \cdot p + s \cdot p$, and $s \cdot p \neq 0$ by 6.21(vii). So $m \cdot p < n \cdot p$ by 6.16(iii).

(ii): There are s, t such that $m + s = p$ and $n + t = q$. Hence

$$\begin{aligned} p \cdot q &= (m + s) \cdot (n + t) \\ &= m \cdot n + m \cdot t + s \cdot n + s \cdot t; \end{aligned} \tag{1}$$

hence $m \cdot n \leq p \cdot q$ by 6.16(ii).

(iii): Under the hypotheses here, with s, t as in the proof of (ii), we have $s \neq 0$. From $q \neq 0$ we get $n \neq 0$ or $t \neq 0$ by 6.15(ii). So $s \cdot n \neq 0$ or $s \cdot t \neq 0$. Hence by 6.15(ii) again, $m \cdot t + s \cdot n + s \cdot t \neq 0$, so from (1) we get $m \cdot n < p \cdot q$, using 6.16(iii).

(iv): Similar to (iii). □

Exponentiation is defined similarly to addition and multiplication. We leave the details to exercises, since they involve similar proofs to the above.

Lemma 6.23. *For every natural number m there is a unique function $f : \omega \to \omega$ such that, for any $n \in \omega$,*
(i) $f(0) = 1$;
(ii) $f(n + 1) = f(n) \cdot m$.

Proof. Exercise.

We denote the function given in 6.23 by ex_m. Now we define for any natural numbers m, n the exponent: $m^n = \mathrm{ex}_m(n)$. Basic properties of the exponent are given in the next theorem.

Theorem 6.24. *(i) $0^0 = 1$.*
(ii) $0^m = 0$ for all $m > 0$.
(iii) $m^{n+p} = m^n \cdot m^p$.
(iv) $(m \cdot n)^p = m^p \cdot n^p$.
(v) $(m^n)^p = m^{n \cdot p}$.

Proof. Exercise.

We now turn to the discussion of finite sets. First we give a general definition which will be explored more fully when we discuss the cardinality of arbitrary sets.

Two sets A and B are *equipotent*, in symbols $A \sim_{\mathrm{ep}} B$, iff there is a one-one function mapping A onto B.

Proposition 6.25. *If m and n are natural numbers and $m \sim_{\mathrm{ep}} n$, then $m = n$.*

Proof. We prove this by induction on m. If $m = 0$, clearly also $n = 0$. Now suppose that it is true for m (for any n), and suppose that $m + 1$ is equipotent with n. Say that f is a one-one function mapping $m+1$ onto n. Clearly then $n \neq 0$, so we can write $n = p+1$. Now we define $g : n \to n$. If $f(m) = p$, we let $g = \mathrm{Id}_n$. Suppose that $f(m) \neq p$. Then for any $i < m + 1$ we define

$$g(i) = \begin{cases} p & \text{if } i = f(m), \\ f(m) & \text{if } i = p, \\ i & \text{otherwise.} \end{cases}$$

Thus g interchanges $f(m)$ and p, and fixes all other elements of n. Clearly then g is one-one and maps n onto n. Hence we can consider $g \circ f$, which is a one-one function mapping m onto n. Note that $(g \circ f)(m) = g(f(m)) = p$. Let $h = g \restriction m$. Then h is a one-one function mapping m onto p. Thus $m \sim_{\text{ep}} p$, and the induction hypothesis gives $m = p$, hence $m + 1 = p + 1 = n$. This finishes the inductive proof. □

Now we define a set A to be *finite* iff it is equipotent with some natural number m. By Proposition 6.25, that natural number m is uniquely determined by A and is called *the number of elements of* A, or the *cardinality of* A, or *size of* A, denoted by $|A|$. Later we shall extend this notation $|A|$ to infinite sets A, i.e., to sets A which are not finite. Of course, for this we need to have some more general notion of number, which we will call *cardinal numbers*.

The following proposition is rather obvious.

Proposition 6.26. *If A is a finite set with n elements and $a \notin A$, then $A \cup \{a\}$ has $n + 1$ elements.*

Proof. By hypothesis there is a bijection f from A to n. We get a bijection from $A \cup \{a\}$ to $n + 1$ by extending f, mapping a to n. (Recall that $n + 1 = n \cup \{n\}$.)

Proposition 6.27. *If A is a finite set with $n+1$ elements, $n \in \omega$, and if $a \in A$, then there is a one-one function mapping A onto $n + 1$ taking a to n, and $A\backslash\{a\}$ is finite, with n elements.*

Proof. Since A has $n + 1$ elements, there is a one-one function f mapping A onto $n+1$. As in the proof of 6.25, let g be the one-one function mapping $n+1$ onto $n+1$ which interchanges n and $f(a)$ (which may be the same) and leaves other elements of $n+1$ fixed. Then $g \circ f$ takes a to n, as desired in the proposition, and $(g \circ f) \restriction (A\backslash\{a\}$ is a one-one function from $A\backslash\{a\}$ onto n, proving that $A\backslash\{a\}$ is finite, with n elements. □

Proposition 6.28. *Every subset of a finite set is finite. In fact, if A is finite with n elements and B is a subset of A, then B has at most n elements.*

Proof. We prove by induction on n that for any set A, if A has n elements, then every subset of A has at most n elements. This is obvious for $n = 0$. Assume it for n, and suppose that A has $n + 1$ elements. Suppose that $B \subseteq A$; we want to show that B has at most $n+1$ elements. If $B = A$ this is given. So suppose that $B \neq A$, and choose $a \in A\backslash B$. By 6.27 the set $A\backslash\{a\}$ has n elements. Since clearly $B \subseteq A\backslash\{a\}$, the inductive hypothesis gives that B has at most n elements. This finishes the inductive proof. □

Corollary 6.29. *If $f : A \to B$ is one-one and B is finite, then A is finite, and $|A| \leq |B|$.*

Proof. Let $n = |B|$. Now $\text{rng}(f) \subseteq B$, so by 6.28, $\text{rng}(f)$ is finite, and has at most n elements. Since A and $\text{rng}(f)$ are equipotent, as shown by f itself, the same applies to A. □

Corollary 6.30. *If $f : A \to B$ maps onto B and A is finite, then B is finite, and $|B| \leq |A|$.*

Proof. Let g be a one-one function mapping A onto $|A|$. We define $h : B \to |A|$ by letting $h(b)$ be the least $i < |A|$ such that $f(g^{-1}(i)) = b$; this i exists since f maps onto B; thus there is an $a \in A$ such that $f(a) = b$, and we can let $i = g(a)$. Now h is one-one, for if $h(b) = h(c)$ with $b, c \in B$, let $i = h(b)$ (also it is equal to $h(c)$). Then $b = f(g^{-1}(i)) = c$. Hence B is finite by 6.29, and $|B| \leq |A|$. □

Theorem 6.31. *A finite set is not equipotent with any of its proper subsets.*

Proof. Suppose that A is finite, $B \subset A$, and A is equipotent with B. Let $f : A \to B$ be a bijection. Choose $a \in A\backslash B$. Then $f : A \to A\backslash\{a\}$, and $A\backslash\{a\}$ is finite by 6.28, so by 6.29, $|A| \leq |A\backslash\{a\}| < |A|$ using 6.27, contradiction. □

Theorem 6.32. (Finite onto=1-1 Theorem). *Suppose that A and B are finite sets with $|A| = |B|$, and $f : A \to B$. Then f is one-one iff f maps onto B.*

Proof. $\Rightarrow$: Suppose that f is one-one, but does not map onto B. Choose $b \in B\backslash\mathrm{rng}(f)$. Then $f : A \to B\backslash\{b\}$, and $B\backslash\{b\}$ is finite by 6.28, and so by 6.29, $|B| = |A| \leq |B\backslash\{b\}| < |B|$, using 6.27, contradiction.

$\Leftarrow$: Suppose that f maps onto B but is not one-one. Then there are distinct $a, a' \in A$ such that $f(a) = f(a')$. Hence $f \restriction (A\backslash\{a\})$ maps onto B. By 6.30 it follows that $|B| \leq |A\backslash\{a\}| < |A| = |B|$, using 6.27 again, contradiction. □

Theorem 6.32 gives an easy proof that ω itself is infinite:

Theorem 6.33. *ω is infinite; in fact, ω is equipotent to a proper subset of itself.*

Proof. It suffices to prove the second statement. Let $f(m) = m + 1$ for all $m \in \omega$. Then $0 \notin \mathrm{rng}(f)$, since every member of the range of f is nonempty. (Using $0 = \emptyset$ and $m + 1 = m \cup \{m\}$.) If $f(m) = f(n)$, then $m = n$ by 5.15(iii). Thus f is one-one, and it shows that ω is equipotent to a proper subset of itself. □

The following simple proposition will be useful later.

Proposition 6.34. *If A is a nonempty finite set simply ordered by a relation $<$, then A has a greatest element under $<$, i.e., there is an element $a \in A$ such that $b \leq a$ for all $b \in A$.*

Proof. We prove this by induction on $|A|$. It is clear if $|A| = 1$. Assume that it is true when $|A| = m$, and suppose now that $|A| = m + 1$. Fix $a \in A$ and let $B = A\backslash\{a\}$. Then $|B| = m$ by 6.27. By the inductive hypothesis, with B simply ordered by $(B \times B) \cap <$, B has a largest element b. Now a and b are comparable, and the largest element of A is clearly the maximum of a and b. This finishes the inductive proof. □

The relationship of finite sets to the operations addition and multiplication will be discussed when dealing with cardinal numbers in general.

Now we prove an important theorem concerning the closure of a set under finitary operations. This theorem is implicitly used in much of mathematics, and will be used several times later in these notes.

Let m be a natural number, $m \neq 0$. A *partial* m-ary operation on a set A is a function whose domain is a subset of ${}^mA$ and whose range is a subset of A. A *finitary partial*

operation on A is a function which is, for some $m \in \omega \backslash 1$, a partial m-ary operation on A. If f is a partial m-ary operation on A and $B \subseteq A$, we say that B is *closed* under f provided that for every $b \in \mathrm{dmn}(f) \cap {}^m B$ we have $f(b) \in B$. Finally, let F be a set of finitary partial operations on A, and let $X \subseteq A$. The *closure* of X under F is

$$\bigcap \{B \subseteq A : B \text{ is closed under each } f \in F\}.$$

The set we are taking the intersection of is nonempty because A is a member of it. We denote the closure by $\mathrm{Cl}_F(X)$.

Proposition 6.35. *Suppose that F is a set of finitary operations on A and $X \subseteq A$. Then $X \subseteq \mathrm{Cl}_F(X)$, and $\mathrm{Cl}_F(X)$ is closed under each $f \in F$.*

Proof. Let $\mathscr{B} = \{B \subseteq A : X \subseteq B \text{ and } B \text{ is closed under each } f \in F\}$; so $\mathrm{Cl}_F(X) = \bigcap \mathscr{B}$, and $\mathscr{B}$ is nonempty. If $B \in \mathscr{B}$, then $X \subseteq B$. Hence $X \subseteq \mathrm{Cl}_F(X)$. Now suppose that $f \in F$ and $b \in \mathrm{dmn}(f) \cap {}^m \mathrm{Cl}_F(X)$. Now for any $B \in \mathscr{B}$ we have $\mathrm{Cl}_F(X) \subseteq B$, and hence $b \in \mathrm{dmn}(f) \cap B$. It follows that $f(b) \in B$, since $B \in \mathscr{B}$ and hence it is closed under f. Since B was arbitrary, this shows that $f(b) \in \bigcap \mathscr{B} = \mathrm{Cl}_F(X)$. Hence $\mathrm{Cl}_F(X)$ is closed under each $f \in F$. □

Our theorem gives alternative constructions of this closure.

Theorem 6.36. (Closure theorem) *Let F be a set of finitary partial operations on a set A and let $X \subseteq A$. Then the following conditions are equivalent:*

(i) $a \in \mathrm{Cl}_F(X)$.

(ii) $a \in \bigcup_{m \in \omega} D_m$, where the sets D_i for $i \in \omega$ are defined by recursion as follows:

$$D_0 = X;$$
$$D_{m+1} = D_m \cup \{f(b) : f \in F,\ b \in \mathrm{dmn}(f),\ \mathrm{rng}(b) \subseteq D_m\}.$$

(iii) There exist $m \in \omega$ and $b \in {}^{m+1}A$ such that $b(m) = a$ and for each $i \leq m$ one of the following conditions holds:

(a) $b(i) \in X$;

(b) there exist $f \in F$, a positive integer n, and a $j \in {}^n i$ such that $\mathrm{dmn}(f) \subseteq {}^n A$, $b \circ j \in \mathrm{dmn}(f)$, and $b(i) = f(b \circ j)$.

Proof. (i)⇒(ii): It suffices to show that $\bigcup_{m \in \omega} D_m$ contains X and is closed under each $f \in F$. Since $D_0 = X$, obviously it contains X. Now suppose that $b \in \mathrm{dmn}(f) \cap \bigcup_{m \in \omega} D_m$. Say that $b \in {}^n A$. For each $i < m$ let $k(i)$ be the least $m \in \omega$ such that $b(i) \in D_{k(i)}$. Let n be the maximum of all $k(i)$ for $i < m$. Then $\mathrm{rng}(b) \subseteq D_n$, and so $f(b) \in D_{n+1} \subseteq \bigcup_{m \in \omega} D_m$, as desired. Here the fact that n exists can easily be shown by induction on m.

(ii)⇒(iii): It suffices to show by induction on k that for each $k \in \omega$ and each $c \in D_k$, a pair m, b exists as in (iii) with c in place of a. For $k = 0$ we have $D_0 = X$, so $c \in X$, and we can take $m = 0$ and $b = \{(0, c)\}$. Now suppose that our statement is true for D_k, and suppose now that $c \in D_{k+1}$. We may assume that $c \notin D_k$. Hence there exist $f \in F$ and $d \in \mathrm{dmn}(f)$ with $\mathrm{rng}(d) \subseteq D_k$ such that $c = f(d)$. Say $d \in {}^p D_k$. By the inductive

hypothesis, for each $i < p$ let $m(i) \in \omega$ and $e_i \in {}^{m(i)+1}A$ be such that $e_i(m(i)) = d(i)$ and for each $s \leq m(i)$ one of the following holds:

(a) $e_i(s) \in X$;

(b) there exist $g \in F$, a positive integer t, and a $j \in {}^t s$ such that $\mathrm{dmn}(g) \subseteq {}^t A$, $e_i \circ j \in \mathrm{dmn}(g)$, and $e_i(s) = g(e_i \circ j)$.

Now the idea is to string all of the e_i's together and put c at the end. Precisely, we first introduce a general notion of *concatenation* of two finite sequences u, v. Say $u \in {}^\alpha A$ and $v \in {}^\beta A$ with α and β natural numbers. Then $u^\frown v$ is the function with domain $\alpha + \beta$ such that $u \subseteq (u^\frown v)$, and $(u^\frown v)(\alpha + \gamma) = v(\gamma)$ for each $\gamma \in \beta$. Then we define by recursion

$$h_0 = e_0;$$
$$h_{x+1} = h_x^\frown e_{x+1}$$

whenever $x + 1 < p$. Then let $k = h_{p'}$, where $p = p' + 1$, and let our final function l extend k by setting $l(p) = c$. Then it is clear that this shows that (iii) holds for c.

(iii)⇒(i): Let c satisfy (iii), and choose m and b accordingly. By induction on i it is clear that $b(i) \in C$ for each $i \leq m$. In particular, $c = b(m) \in C$, as desired. □

To conclude this section we make some remarks without proofs about the construction of integers, rationals, reals. The construction of the integers from the natural numbers is rarely given in detail in textbooks. The construction of the rationals from the integers is usually given in a more general form in books on abstract algebra (any integral domain can be embedded in a field). The construction of the real numbers from the rationals is usually just sketched without full details in analysis books.

Here we give the precise constructions, with no details. In the appendices we give the full details.

• $\mathbb{Z}$: Let $A = \omega \times \omega$. We define a relation $\sim$ on A by setting, for any $m, n, p, q \in \omega$,

$$(m, n) \sim (p, q) \quad \text{iff} \quad m + q = n + p.$$

It is easy to check that $\sim$ is an equivalence relation on A. Let $\mathbb{Z}'$ be the collection of all equivalence classes under this relation. (Intuitively we think of $[(m, n)]$ as $m - n$.) Then one can define binary operations $+$ and $\cdot$ on $\mathbb{Z}'$ such that, for any $m, n, p, q \in \omega$,

$$[(m, n)] + [(p, q)] = [(m + p, n + q)]$$
$$[(m, n)] \cdot [(p, q)] = [(m \cdot p + n \cdot q, m \cdot q + n \cdot p)].$$

We also can define $<$ on $\mathbb{Z}'$ so that

$$[(m, n)] < [(p, q)] \quad \text{iff} \quad m + q < p + r.$$

Various familiar properties of the integers can be proved for elements of $\mathbb{Z}'$. For any $m \in \omega$, let $f(m) = [(m, 0)]$. Then f is a one-one function mapping ω into $\mathbb{Z}'$. We define

$$\mathbb{Z} = \omega \cup \{(\omega, a) : a \in \mathbb{Z}' \backslash \mathrm{rng}(f)\}.$$

According to Theorem 3.22 and its proof, there is a one-one function g from $\mathbb{Z}$ onto $\mathbb{Z}'$ which extends f. Now for any $a, b \in \mathbb{Z}$ we define

$$\begin{aligned} a + b &= g^{-1}(g(a) + g(b)) \\ a \cdot b &= g^{-1}(g(a) \cdot g(b)) \\ a < b \quad &\text{iff} \quad g(a) < g(b). \end{aligned}$$

The usual properties of addition, multiplication, and order of integers can now be proved.

• $\mathbb{Q}$: the construction of the rationals from the integers is a special case of an algebraic construction treated in undergraduate algebra courses. Let $A = \mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$. We define a relation $\equiv$ on A by setting, for any $(r, s), (t, u) \in A$,

$$(r, s) \equiv (t, u) \quad \text{iff} \quad r \cdot u = s \cdot t.$$

It is easily checked that this is an equivalence relation on A. We let $\mathbb{Q}'$ be the set of all equivalence classes. (Intuitively we think of $[(r, s)]$ as r/s.) Then one can define binary operations $+$ and $\cdot$ on $\mathbb{Q}'$ such that for any $(r, s), (t, u) \in A$,

$$\begin{aligned} [(r, s)] + [(t, u)] &= [(r \cdot u + s \cdot t, s \cdot u)]; \\ [(r, s)] \cdot [(t, u)] &= [r \cdot t, s \cdot u)]. \end{aligned}$$

We can also define $<$ on $\mathbb{Q}'$ so that for any $(r, s), (t, u) \in A$ with $s, u > 0$,

$$[(r, s)] < [(t, u)] \quad \text{iff} \quad r \cdot u < t \cdot s.$$

Various familiar properties of the rationals can be proved for elements of $\mathbb{Q}'$. For any $a \in \mathbb{Z}$ let $h(a) = [(a, 1)]$. Then h is a one-one function mapping $\mathbb{Z}$ into $\mathbb{Q}'$. We define

$$\mathbb{Q} = \mathbb{Z} \cup \{(\mathbb{Z}, r) : r \in \mathbb{Q}' \backslash \text{rng}(h)\}.$$

According to Theorem 3.22 and its proof, there is a one-one function k from $\mathbb{Q}$ onto $\mathbb{Q}'$ which extends h. Now for any $a, b \in \mathbb{Q}$ we define

$$\begin{aligned} a + b &= k^{-1}(k(a) + k(b)) \\ a \cdot b &= k^{-1}(k(a) \cdot k(b)) \\ a < b \quad &\text{iff} \quad k(a) < k(b). \end{aligned}$$

The usual properties of addition, multiplication, and order of rationals can now be proved.

• $\mathbb{R}$: A subset A of $\mathbb{Q}$ is a *Dedekind cut* provided the following conditions hold:

(1) $\mathbb{Q} \neq A \neq \emptyset$;
(2) For all $r, s \in \mathbb{Q}$, if $r < s$ and $s \in A$, then $r \in A$.
(3) A has no largest element.

Let $\mathbb{R}'$ be the set of all Dedekind cuts.

Let $Z = \{r \in \mathbb{Q} : r < 0\}$. So Z is a Dedekind cut.

A Dedekind cut A is *positive* if it has some positive rational number as a member.

For any Dedekind cut A we define

$$-A = \{r \in \mathbb{Q} : \exists s(r < s \wedge -s \notin A)\}.$$

It is easy to check that $-A$ is a Dedekind cut. Moreover, for any Dedekind cut A, if $A \neq Z$, then exactly one of $A, -A$ is positive; the positive one is denoted by $|A|$.

Now one can define binary operations $+$ and $\cdot$ on $\mathbb{R}'$ so that, for any $A, B \in \mathbb{R}'$,

$A + B = \{a + b : a \in A, b \in B\}$

$A \cdot B = \{r \in \mathbb{Q} : \exists s \in A \exists t \in B(0 < s \wedge 0 < t \wedge r < s \cdot t)\}$ if A and B are positive,

$A \cdot B = Z$ if $A = Z$ or $B = Z$,

$A \cdot B = -(|A| \cdot |B|)$ if $A \neq Z \neq B$ and exactly one of A, B is positive

$A \cdot B = |A| \cdot |B|$ if $-A$ and $-B$ are both positive.

Furthermore, we define $A < B$ iff $A \subset B$.

Various familiar properties of the reals can be proved for elements of $\mathbb{R}'$. For any $a \in \mathbb{Q}$ let $s(a) = \{r \in \mathbb{Q} : r < a\}$. Then s is a one-one function mapping $\mathbb{Q}$ into $\mathbb{R}'$. We define

$$\mathbb{R} = \mathbb{Q} \cup \{(\mathbb{Q}, r) : r \in \mathbb{R}' \backslash \mathrm{rng}(a)\}.$$

According to Theorem 3.22 and its proof, there is a one-one function t from $\mathbb{R}$ onto $\mathbb{R}'$ which extends s. Now for any $a, b \in \mathbb{R}$ we define

$$\begin{aligned} a + b &= t^{-1}(t(a) + t(b)) \\ a \cdot b &= t^{-1}(t(a) \cdot t(b)) \\ a < b \quad &\text{iff} \quad t(a) < t(b). \end{aligned}$$

The usual properties of addition, multiplication, and order of reals can now be proved.

Note that $\omega \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

Exercises, chapter 6

1. Finish the proof of Theorem 6.14.

2. Finish the proof of Lemma 6.21.

3. Prove Theorem 6.23.

4. Prove Theorem 6.24.

5. Prove that for any natural numbers m, n the following conditions are equivalent:
   (i) $m + n < m \cdot n$.
   (ii) m and n are both greater than 1, and at least one of them is greater than 2.

6. Prove that for any natural numbers m, n, p with $m > 0$, if $n \leq p$ then $m^n \leq m^p$, and if $m > 1$ and $n < p$ then $m^n < m^p$.

7. Prove that if A is an infinite set, then there is an injection from ω into A. Hint: Let $B = \bigcup_{m\in\omega} {}^m A$, and set

$$C = \{(k, a) : k \in B \text{ and } a \in A\backslash\mathrm{rng}(k)\}.$$

For each $(k, a) \in C$ let $f(k, a) = k$. Show that f maps onto B. Then apply the axiom of choice to get a function $g : B \to C$ such that $f \circ g = \mathrm{Id}_B$. For each $k \in B$ let $h(k) = 2^{\mathrm{nd}}(g(k))$. Apply the recursion theorem to get a function $l : \omega \to A$ such that $l(m) = h(l \restriction m)$ for all $m \in \omega$. Show that l is the desired injection.

8. A set is finite iff it is not equipotent to any of its proper subsets. Hint: use exercise 7 in the harder direction.

9. A set A is finite iff for every nonempty collection $\mathscr{A}$ of subsets of A there is a $B \in \mathscr{A}$ such that there is no $C \in \mathscr{A}$ such that $C \subset B$. Hint: again exercise 7 is useful.

10. Suppose that $A \subseteq \omega$, $m \in A$, and $\forall n \in A(n + 1 \in A)$. Prove that $\forall n \in \omega(m \leq n \Rightarrow m \in A)$.

11. Define a nonempty subset A of ω such that $\forall n \in A(n + 1 \in A)$ while $A \neq \omega$.

12. Show that A is finite iff every proper subset of A is finite.

13. Suppose that $s : \omega \to \omega$. Use the recursion theorem to show that there is a unique function $l : \omega \to \omega$ such that $l(0) = s(1)$ and for any $n \in \omega$, $l(n + 1) = s(l(n))$. Informally we could say that $l(n) = s^{n+1}(1)$ for all $n \in \omega$.

14. For each $s : \omega \to \omega$ let $t(s)$ be the unique function l of exercise 12. (That function depends on s.) Let $h(n) = n + 1$ for all $n \in \omega$. Use the recursion theorem to show that there is a unique function k with domain ω such that $k(0) = h$, and for any $m \in \omega$, $k(m + 1) = t(k(m))$. Note that for each $m \in \omega$, $k(m)$ is itself a function mapping ω into ω. Informally, if $m, n \in \omega$, then $(k(m + 1))(n) = (k(m))^{n+1}(1)$.

15. (The Ackermann function) Prove that there is a function $f : \omega \times \omega \to \omega$ such that the following conditions hold for any $m, n \in \omega$:

(i) $f(0, n) = n + 1$;
(ii) $f(m + 1, 0) = f(m, 1)$;
(iii) $f(m + 1, n + 1) = f(m, f(m + 1, n))$.

Hint: use exercise 14.

16. With f as in exercise 15, show that $n < f(m, n)$ for all $m, n \in \omega$. Hint: prove "for all m, forall n, $n < f(m, n)$" by induction on m; in the inductive step, use induction on n.

17. With f as in exercise 15, show that $f(m, n) < f(m, n + 1)$ for all $m, n \in \omega$.

18. With f as in exercise 15, show that $f(m, n) < f(m, p)$ for all $m, n, p \in \omega$ such that $n < p$.

19. With f as in exercise 15, show that $f(m, n + 1) \leq f(m + 1, n)$ for all $m, n \in \omega$.

20. With f as in exercise 15, show that $f(m, n) < f(m + 1, n)$ for all $m, n \in \omega$.

21. Prove that if y is a nonzero natural number, then $\bigcup y$ is a natural number, and $y = \bigcup y \cup \{\bigcup y\}$. Hint: proceed by induction.

22. Show that a set x is a natural number iff for every $y \in x \cup \{x\}$, if $y \neq \emptyset$, then $y = \bigcup y \cup \{\bigcup y\}$. Hint: in the direction $\Leftarrow$, suppose that $x \notin \omega$ and apply the foundation axiom to $\{w \in x \cup \{x\} : w \notin \omega\}$.

23. Assuming the usual meaning of the notions involved, prove by induction that for every positive integer n one has

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6} n(n+1)(2n+1).$$

24. Assuming the usual meaning of the notions involved, prove by induction that for every positive integer n one has

$$1^3 + 2^3 + \cdots + n^3 = \frac{1}{4} n^2 (n+1)^2.$$