6 Order Relations

Definition 6.1. Let A be a set. A *linear order* on A is a binary relation on A which satisfies the following properties:

- R is transitive.
- R satisfies *trichotomy*; *ie* if $x, y \in A$ then *exactly one* of the three alternatives

$$xRy, \quad x = y, \quad yRx$$

  holds.

Example 6.2. $R = \{\langle a, b\rangle \mid a, b \in \mathbb{N} \text{ and } a < b\}$ is a linear order on $\mathbb{N}$.

Example 6.3. $S = \{\langle a, b\rangle \mid a, b \in \mathbb{N} \text{ and } a > b\}$ is a linear order on $\mathbb{N}$.

Example 6.4. $T = \{\langle a, b\rangle \mid a, b \in \mathbb{N} \text{ and } a \leq b\}$ is *not* a linear order on $\mathbb{N}$, since $0 = 0$ and OTO. Thus T does not satisfy trichotomy.

Example 6.5. Define a binary relation $<_L$ on $\mathbb{N}\times\mathbb{N}$ by

$$\langle a, b\rangle <_L \langle c, d\rangle \iff \text{either } a < c \text{ or } (a = c \text{ and } b < d).$$

Then $<_L$ is a linear order on $\mathbb{N}\times\mathbb{N}$

Proof. We check that $<_L$ is transitive and satisfies trichotomy.

(a) Suppose that $\langle a, b\rangle <_L \langle c, d\rangle$ and $\langle c, d\rangle <_L \langle e, f\rangle$. There are four cases to consider.

Case 1 Suppose that $a < c$ and $c < e$. Then $a < e$ and so $\langle a, b\rangle <_L \langle e, f\rangle$.

Case 2 Suppose that $a < c$ and $(c = e$ and $d < f)$. Then $a < e$ and so $\langle a, b\rangle <_L \langle e, f\rangle$.

Case 3 Suppose that $(a = c$ and $b < d)$ and $c < e$. Then $a < e$ and so $\langle a, b\rangle <_L \langle e, f\rangle$.

Case 4 Suppose that $(a = c$ and $b < d)$ and $(c = e$ and $d < f)$. Then $a = e$ and $b < f$. Hence $\langle a, b\rangle <_L \langle e, f\rangle$.

(b) Suppose that $\langle a, b\rangle \neq \langle c, d\rangle$. If $a < c$ then $\langle a, b\rangle <_L \langle c, d\rangle$; and if $c < a$, then $\langle c, d\rangle \neq \langle a, b\rangle$. On the other hand, if $a = c$, then either $b < d$ or $d < b$; and so either $\langle a, b\rangle <_L \langle c, d\rangle$ or $\langle c, d\rangle \neq \langle a, b\rangle$.

Hence *at least one* alternative always holds.

Suppose that two of the alternatives hold for $\langle a, b\rangle, \langle c, d\rangle$. Then clearly $\langle a, b\rangle \neq \langle c, d\rangle$. Hence we must have that

$$\langle a, b\rangle <_L \langle c, d\rangle \quad \text{and} \quad \langle c, d\rangle <_L \langle a, b\rangle.$$

Clearly this rules out both $a < c$ and $c < a$. Thus $a = c$. BBut then we must have $b < d$ and $d < b$, which is impossible. $\square$

Exercise 6.6. Show that $<_L$ is a well-ordering.

7 The Natural Numbers

In this section, we shall define each natural number to be a suitable set. It will turn out that

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{\emptyset\} \\ 2 &= \{\emptyset, \{\emptyset\}\} \\ 3 &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\} \\ &\mathit{etc} \end{aligned}$$

In particular, we shall have

$$0 \in 1 \in 2 \in 3 \in \dots$$

and

$$0 \subseteq 1 \subseteq 2 \subseteq 3 \subseteq \dots$$

Notice also that

$$n < m \quad \text{iff} \quad n \in m$$

Definition 7.1. If a is any set, then its *successor* is defined to be

$$a^+ = a \cup \{a\}.$$

Example 7.2.

$$\begin{aligned} \emptyset^+ &= \emptyset \cup \{\emptyset\} = \{\emptyset\} \\ \{\emptyset\}^+ &= \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} \end{aligned}$$

Notation We shall write $0 = \emptyset$ and $n = \overbrace{(\dots((\emptyset^+)^+)\dots)^+}^{n \text{ times}}$

Example 7.3. $2 = (\emptyset^+)^+$

Definition 7.4. A set A in *inductive* iff the following conditions are satisfied:

1. $\emptyset \in A$

2. If $a \in A$, then $a^+ \in A$.

Remark 7.5. If A is inductive, then $n \in A$ for all n. In particular, A is infinite. So we cannot prove the existence of an inductive set using our current axioms.

Axiom 7.6 (Infinity). *There exists an inductive set.*

Definition 7.7. A *natural number* is a set that belongs to every inductive set.

Theorem 7.8. *There exists a set B such that for all x,*

$$x \in B \text{ iff } x \text{ is a natural number.}$$

Proof. By the Infinity Axiom, there exists an inductive set A. By the Subset Axiom, there exists a set B such that for all x,

$$x \in B \text{ iff } x \in A \text{ and } x \text{ belongs to every inductive set.}$$

Clearly B satisfies our requirements. □

Definition 7.9.

$$\omega = \{x \mid x \text{ is a natural number}\}$$

Short discussion of the ordinals...

Theorem 7.10.

1. *ω is inductive.*
2. *If A is inductive, then $\omega \subseteq A$.*

Proof.

1. Since $\emptyset$ belongs to every inductive set, it follows that $\emptyset \in \omega$. Next suppose that $a \in \omega$. Then a belongs to every inductive set and so a^+ belongs to every inductive set. Hence $a^+ \in \omega$. Thus ω is inductive.
2. Let A be any inductive set. If $a \in \omega$, then a belongs to every inductive set. In particular, $a \in A$. Thus $\omega \subseteq A$.

□

Question 7.11. Does there exist an inductive set $A \neq \omega$?

Answer. Yes...

Theorem 7.12 (Induction principle for ω). *If T is an inductive subset of ω, then $T = \omega$.*

Proof. Suppose that T is an inductive subset of ω. Then clearly $T \subseteq \omega$. By the previous theorem, since T is inductive, $\omega \subseteq T$. Hence $T = \omega$. □

Application. If $n \in \omega$, then either $n = 0$ or there exists $m \in \omega$ such that $n = m^+$.

Proof. Let $T = \{n \in \omega \mid n = 0 \text{ or } (\exists m \in \omega)\ n = m^+\}$. We claim that T is inductive. Clearly $0 \in T$. Next suppose that $k \in T$. Then clearly $k^+ \in T$. Hence T is an inductive subset of ω. By Induction, $T = \omega$. □

Next we would like to define the usual arithmetic operations on ω.

Definition 7.13.

1. f is a *unary operation* on A iff $f \colon A \to A$.
2. g is a *binary operation* on A iff $f \colon A \times A \to A$.

Example 7.14. The successor operation on ω is the unary operation $\sigma \colon \omega \to \omega$ defined by $\sigma(n) = n^+$. In other words,

$$\sigma = \{\langle n, m\rangle \mid \langle n, m\rangle \in \omega \times \omega \text{ and } m = n^+\}.$$

Next we would like to define a binary operation

$$a \colon \omega \times \omega \to \omega$$

such that

$$a(m, n) = m + n.$$

We shall define a by *recursion* on ω, using the successor operation, as follows:

$$\begin{aligned} m + 0 &= m \\ m + n^+ &= (m + n)^+ \end{aligned}$$

In other words, we shall define a by:

$$\begin{aligned} a(m, 0) &= m \\ a(m, n^+) &= \sigma(a(m, n)) \end{aligned}$$

Slight Problem At first glance, we appear to be defining a in terms of a.

More Serious Problem

1. Can we prove that a function $a \colon \omega \times \omega \to \omega$ satisfying the above properties exists, using our current axioms of set theory?
2. If so, can we prove that there exists a *unique* such function?

Theorem 7.15 (Recursion on ω). *Suppose that A is a set, $a \in A$ and $F\colon A \to A$ is a function. Then there exists a unique function $h\colon \omega \to A$ satisfying the following conditions:*

(i) $h(0) = a$

(ii) *for every* $n \in \omega$, $h(n^+) = F(h(n))$.

Proof. We break the proof up into a series of claims.

Claim. There exists *at most one* such function $h\colon \omega \to A$.

Proof. Suppose that $h_1\colon \omega \to A$ and $h_2\colon \omega \to A$ both satisfy conditions (i) and (ii). We must prove that $h_1 = h_2$. Let

$$S = \{n \in \omega \mid h_1(n) = h_2(n)\}.$$

We shall prove that S is inductive. By condition (i),

$$h_1(0) = a = h_2(0).$$

Hence $0 \in S$. Now suppose that $n \in S$. Then $h_1(n) = h_2(n)$. By condition (ii),

$$h_1(n^+) = F(h_1(n)) = F(h_2(n)) = h_2(n^+).$$

Thus $n^+ \in S$. By induction, $S = \omega$ and so $h_1 = h_2$. □

Now we show that there is *at least one* such function.

Definition 7.16. A function v is *acceptable* if $\operatorname{dom} v \subseteq \omega$, $\operatorname{ran} v \subseteq A$, and the following conditions hold:

(a) If $0 \in \operatorname{dom} v$, then $v(0) = a$.

(b) If $n^+ \in \operatorname{dom} v$, then $n \in \operatorname{dom} v$ and $v(n^+) = F(v(n))$.

Example 7.17.

$$v = \{\langle 0, a\rangle\} \text{ is acceptable.}$$

$$v = \{\langle 0, a\rangle, \langle 1, F(a)\rangle\} \text{ is acceptable.}$$

Let $K \subseteq \mathcal{P}(\omega \times A)$ be the set of acceptable functions. Then we define

$$h = \bigcup K.$$

Clearly $h \subseteq \omega \times A$. In particular, h is a set of ordered pairs.

Claim. h is a function.

Proof. We must prove that for each $n \in \operatorname{dom} h$, there exists a unique $y \in A$ such that $\langle n, y \rangle \in h$. (Note that we are *not* yet proving that $\operatorname{dom} h = \omega$.) Let

$$T = \{n \in \omega \mid \text{there exists } \textit{at most} \text{ one } y \text{ so that } \langle n, y \rangle \in h\}$$

We shall prove that T is inductive. First suppose that $\langle 0, y_1 \rangle, \langle 0, y_2 \rangle \in h$. Then there exists acceptable functions $v_1 m v_2$ so that $v_1(0) = y_1$ and $v_2(0) = y_2$. By condition (a),

$$v_1(0) = a = v_2(0)$$

Thus $0 \in T$. Next suppose that $n \in T$. To see that $n^+ \in T$. suppose that $\langle n^+, y_1 \rangle, \langle n^+, y_2 \rangle \in h$. Then there exist acceptable functions v_1, v_2 such that $v_1(n^+) = y_1$ and $v_2(n^+) = y_2$. By condition (b), we have that

$$n \in \operatorname{dom} v_1 \quad \text{and} \quad v_1(n^+) = F(v_1(n))$$

$$n \in \operatorname{dom} v_2 \quad \text{and} \quad v_2(n^+) = F(v_2(n))$$

Since $n \in T$, we have that $v_1(n) = v_2(n)$. Hence $v_1(n^+) = v_2(n^+)$ and so $n^+ \in T$. By induction, $T = \omega$ and so h *is* a function. □

Claim. h is acceptable.

Proof. Clearly $\operatorname{dom} h \subseteq \omega$ and $\operatorname{ran} h \subseteq A$. Suppose that $0 \in \operatorname{dom} h$. Then there exists an acceptable function v such that $h(0) = v(0) = a$. Thus (a) holds.

Now suppose that $n^+ \in \operatorname{dom} h$. Then there exists an acceptable function v such that $h(n^+) = v(n^+)$. Futhermore, $n \in \operatorname{dom} v$ and $h(n) = v(n)$. Also,

$$h(n^+) = v(n^+) = F(v(n)) = F(h(n))$$

and so (b) also holds. □

Claim. $\operatorname{dom} h = \omega$

Proof. We shall prove that $\operatorname{dom} h$ is inductive. First note that $v = \{\langle 0, a \rangle\}$ is acceptable and so $0 \in \operatorname{dom} h$. Next suppose that $n \in \operatorname{dom} h$. Thus there exists an acceptable function v such that $v(n) = h(n)$. If $n^+ \in \operatorname{dom} v$, then $n^+ \in \operatorname{dom} h$. If $n^+ \notin \operatorname{dom} v$, then

$$u = v \cup \{\langle n^+, F(v(n)) \rangle\}$$

is acceptable and so $n^+ \in \operatorname{dom} h$. By induction, $\operatorname{dom} h = \omega$. □

This completes the proof of the Recursion Theorem. □

Now we are ready to define the various arithmetic operations on ω.

Addition

First for each $m \in \omega$, the Recursion Theorem gives a unique function $A_m \colon \omega \to \omega$ such that

$$\begin{aligned} A_m(0) &= m \\ A_m(n^+) &= A_m(n)^+ \end{aligned}$$

Now we can define addition to be the binary operation on ω defined by

$$A(m,n) = A_m(n).$$

Thus

$$A = \{\langle\langle m,n\rangle,p\rangle \mid \langle\langle m,n\rangle,p\rangle \in (\omega\times\omega)\times\omega \text{ and } p = A_m(n)\}.$$

Notation We shall write $m + n = A(m,n)$.

Thus the above equations can be rewritten as

$$\begin{aligned} m + 0 &= m \\ m + n^+ &= (m+n)^+ \end{aligned}$$

Multiplication

Our plan is to define multiplication recursively in terms of addition, so that:

$$\begin{aligned} m \cdot 0 &= 0 \\ m \cdot n^+ &= m + m \cdot n \end{aligned}$$

Once again, first for each $m \in \omega$, the Recursion Theorem gives a unique function $M_m \colon \omega \to \omega$ such that

$$\begin{aligned} M_m(0) &= 0 \\ M_m(n^+) &= m + M_m(n) \end{aligned}$$

Now we can define multiplication to be the binary operation on ω defined by $M(m,n) = M_m(n)$.

Notation We shall write $m \cdot n = M_m(n)$. As desired, the above equations can now be rewritten as

$$\begin{aligned} m \cdot 0 &= 0 \\ m \cdot n^+ &= m + m \cdot n \end{aligned}$$

Summary We have the following identities.

$$\begin{array}{rrcl} (A1) & m+0 & = & m \\ (A2) & m+n^+ & = & (m+n)^+ \\ (M1) & m\cdot 0 & = & 0 \\ (M2) & m\cdot n^+ & = & m+m\cdot n \end{array}$$

When functions are defined by recursion, properties of the functions are usually proved by induction.

Theorem 7.18. *For all $m, n \in \omega$,*

$$m+n=n+m.$$

We first need to prove two lemmas,

Lemma 7.19. *For all $n \in \omega$, $0+n=n$.*

Proof. It is enough to prove that the set

$$A = \{n \in \omega \mid 0+n=n\}$$

is inductive. By (A1), $0+0=0$ and so $0 \in A$. Next suppose that $k \in A$. Then

$$0+k=k \quad (*)$$

and so

$$\begin{array}{rcll} 0+k^+ & = & (0+k)^+ & \text{by (A2)} \\ & = & k^+ & \text{by (*)} \end{array}$$

Thus $k^+ \in A$. Hence A is inductive. □

Lemma 7.20. *For all $m, n \in \omega$, $m^+ + n = (m+n)^+$.*

Proof. Fix some $m \in \omega$. Then it is enough to show that

$$B = \{n \in \omega \mid m^+ + n = (m+n)^+\}$$

is inductive. Applying (A1) twice, we see that

$$m^+ + 0 = m^+ = (m+0)^+$$

and so $0 \in B$. Next suppose that $k \in B$. Then

$$m^+ + k = (m+k)^+ \quad (**).$$

Hence

$$\begin{array}{rcll} m^+ + k^+ & = & (m^+ + k)^+ & \text{by (A2)} \\ & = & (m+k)^{++} & \text{by (**)} \\ & = & (m+k^+)^+ & \text{by (A2)} \end{array}$$

Thus $k^+ \in B$. Hence B is inductive. □

Proof of Theorem 7.18. Fix some $n \in \omega$. Then it is enough to show that

$$C = \{m \in \omega \mid m + n = n + m\}$$

is inductive. By Lemma 7.19 and (A1),

$$0 + n = n = n + 0$$

and so $0 \in C$. Next suppose that $k \in C$. Then

$$k + n = n + k \quad (***)$$

Hence

$$\begin{aligned} k^+ + n &= (k+n)^+ \quad \text{by Lemma 7.20} \\ &= (n+k)^+ \quad \text{by (***)} \\ &= n + k^+ \quad \text{by (A2)} \end{aligned}$$

Thus $k^+ \in C$. Hence C is inductive. □

Theorem 7.21. *The following identities hold for all natural numbers*

1. $m + (n + p) = (m + n) + p$
2. $m + n = n + m$
3. $m \cdot (n + p) = m \cdot n + m \cdot p$
4. $m \cdot (n \cdot p) = (m \cdot n) \cdot p$
5. $m \cdot n = n \cdot m$

Proof. Reading exercise. Enderton p. 81. □

Remark 7.22. Note that, as expected, we have that

$$n^+ \overset{(A1)}{=} (n + 0)^+ \overset{(A2)}{=} n + 0^+ = n + 1.$$

Exercise 7.23. Prove that $m \cdot 1 = m$.