

# C1 Set Theory

Robin Adams

August 21, 2022

## 1 Primitive Notions

Let there be *sets*.

Let there be a binary relation called *membership*,  $\in$ . When  $x \in y$  holds, we say  $x$  is a *member* or *element* of  $y$ . We write  $x \notin y$  iff  $x$  is not a member of  $y$ .

## 2 The Axioms

**Axiom 1** (Extensionality). *If two sets have exactly the same members, then they are equal.*

As a consequence of this axiom, we may identify a set  $A$  with the class  $\{x : x \in A\}$ . The use of the symbols  $\in$  and  $=$  is consistent.

**Definition 2.** We say that a class  $\mathbf{A}$  is a *set* iff there exists a set  $A$  such that  $A = \mathbf{A}$ . That is, the class  $\{x : P(x)\}$  is a set iff

$$\exists A. \forall x (x \in A \leftrightarrow P(x)) .$$

Otherwise,  $\mathbf{A}$  is a *proper class*.

**Definition 3** (Subset). If  $A$  is a set and  $\mathbf{B}$  is a class, we say  $A$  is a *subset* of  $\mathbf{B}$  iff  $A \subseteq \mathbf{B}$ .

**Axiom 4** (Empty Set). *The empty class is a set, called the empty set.*

**Axiom 5** (Pairing). *For any objects  $a$  and  $b$ , the class  $\{a, b\}$  is a set, called a pair set.*

**Definition 6** (Union). For any class of sets  $\mathbf{A}$ , the *union*  $\bigcup \mathbf{A}$  is the class  $\{x : \exists A \in \mathbf{A}. x \in A\}$ .

We write  $\bigcup_{P[x_1, \dots, x_n]} t[x_1, \dots, x_n]$  for  $\bigcup \{t[x_1, \dots, x_n] : P[x_1, \dots, x_n]\}$ .

**Proposition 7.** *If  $\mathbf{A} \subseteq \mathbf{B}$  then  $\bigcup \mathbf{A} \subseteq \bigcup \mathbf{B}$ .*

PROOF: Easy.  $\square$

**Axiom 8** (Union). *For any set  $A$ , the union  $\bigcup A$  is a set.*

**Proposition 9.** *For any sets  $A$  and  $B$ , the class  $A \cup B$  is a set.*

PROOF: It is  $\bigcup\{A, B\}$ .  $\square$

**Proposition Schema 10.** *For any objects  $a_1, \dots, a_n$ , the class  $\{a_1, \dots, a_n\}$  is a set.*

PROOF: By repeated application of the Pairing and Union axioms.  $\square$

**Definition 11** (Power Set). For any set  $A$ , the *power set* of  $A$ ,  $\mathcal{P}A$ , is the class of all subsets of  $A$ .

**Axiom 12** (Power Set). *For any set  $A$ , the class  $\mathcal{P}A$  is a set.*

**Axiom 13** (Subset, Aussonderung). *For any class  $\mathbf{A}$  and set  $B$ , if  $\mathbf{A} \subseteq B$  then  $\mathbf{A}$  is a set.*

**Proposition 14.** *For any set  $A$  and class  $\mathbf{B}$ , the intersection  $A \cap \mathbf{B}$  is a set.*

PROOF: By the Subset Axiom since it is a subclass of  $A$ .  $\square$

**Proposition 15.** *For any set  $A$  and class  $\mathbf{B}$ , the relative complement  $A - \mathbf{B}$  is a set.*

PROOF: By the Subset Axiom since it is a subclass of  $A$ .  $\square$

**Theorem 16.** *The universal class  $\mathbf{V}$  is a proper class.*

PROOF:

$\langle 1 \rangle 1$ . ASSUME:  $\mathbf{V}$  is a set.

$\langle 1 \rangle 2$ . LET:  $R = \{x : x \notin x\}$

$\langle 1 \rangle 3$ .  $R$  is a set.

PROOF: By the Subset Axiom.

$\langle 1 \rangle 4$ .  $R \in R$  if and only if  $R \notin R$

$\langle 1 \rangle 5$ . Q.E.D.

PROOF: This is a contradiction.

$\square$

**Definition 17** (Intersection). For any class of sets  $\mathbf{A}$ , the *intersection*  $\bigcap \mathbf{A}$  is the class  $\{x : \forall A \in \mathbf{A}. x \in A\}$ .

We write  $\bigcap_{P[x_1, \dots, x_n]} t[x_1, \dots, x_n]$  for  $\bigcap \{t[x_1, \dots, x_n] : P[x_1, \dots, x_n]\}$ .

**Proposition 18.** *For any nonempty class of sets  $\mathbf{A}$ , the class  $\bigcap \mathbf{A}$  is a set.*

PROOF: Pick  $A \in \mathbf{A}$ . Then  $\bigcap \mathbf{A} \subseteq A$ .  $\square$

**Proposition 19.** *If  $\mathbf{A} \subseteq \mathbf{B}$  then  $\bigcap \mathbf{B} \subseteq \bigcap \mathbf{A}$ .*

PROOF: Easy.  $\square$

**Proposition 20.** *For any set  $A$  and class of sets  $\mathbf{B}$ , we have*

$$A \cup \bigcap \mathbf{B} = \bigcap \{A \cup X \mid X \in \mathbf{B}\}$$

PROOF: Easy.  $\square$

**Proposition 21.** *For any set  $A$  and class of sets  $\mathbf{B}$ , we have*

$$A \cap \bigcup \mathbf{B} = \bigcup \{A \cap X \mid X \in \mathbf{B}\}$$

PROOF: Easy.  $\square$

**Proposition 22.** *For any set  $C$  and class of sets  $\mathbf{A}$ , we have*

$$C - \bigcup \mathbf{A} = \bigcap \{C - X \mid X \in \mathbf{A}\} .$$

PROOF: Easy.  $\square$

**Proposition 23.** *For any set  $C$  and class of sets  $\mathbf{A}$ , we have*

$$C - \bigcap \mathbf{A} = \bigcup \{C - X \mid X \in \mathbf{A}\} .$$

PROOF: Easy.  $\square$

### 3 Ordered Pairs

**Definition 24** (Ordered Pair). For any objects  $a$  and  $b$ , the *ordered pair*  $(a, b)$  is  $\{\{a\}, \{a, b\}\}$ . We call  $a$  its *first coordinate* and  $b$  its *second coordinate*.

**Theorem 25.** *For any objects  $(a, b)$ , we have  $(a, b) = (c, d)$  if and only if  $a = c$  and  $b = d$ .*

PROOF:

$\langle 1 \rangle 1$ . If  $(a, b) = (c, d)$  then  $a = c$  and  $b = d$

$\langle 2 \rangle 1$ . ASSUME:  $(a, b) = (c, d)$

$\langle 2 \rangle 2$ .  $a = c$

PROOF: Since  $\{a\} = \bigcap(a, b) = \bigcap(c, d) = \{c\}$ .

$\langle 2 \rangle 3$ .  $\{a, b\} = \{c, d\}$

PROOF:  $\{a, b\} = \bigcup(a, b) = \bigcup(c, d) = \{c, d\}$ .

$\langle 2 \rangle 4$ .  $b = c$  or  $b = d$

$\langle 2 \rangle 5$ . CASE:  $b = c$

$\langle 3 \rangle 1$ .  $a = b$

$\langle 3 \rangle 2$ .  $\{c, d\} = \{a\}$

$\langle 3 \rangle 3$ .  $b = d$

$\langle 2 \rangle 6$ . CASE:  $b = d$

PROOF: We have  $a = c$  and  $b = d$  as required.

$\langle 1 \rangle 2$ . If  $a = c$  and  $b = d$  then  $(a, b) = (c, d)$

PROOF: Trivial.

$\square$

**Definition 26** (Cartesian Product). The *Cartesian product* of classes  $\mathbf{A}$  and  $\mathbf{B}$  is the class

$$\mathbf{A} \times \mathbf{B} = \{(x, y) : x \in \mathbf{A}, y \in \mathbf{B}\} .$$

**Lemma 27.** For any objects  $x$  and  $y$  and set  $C$ , if  $x \in C$  and  $y \in C$  then  $(x, y) \in \mathcal{PPC}$ .

PROOF: Easy.  $\square$

**Corollary 27.1.** For any sets  $A$  and  $B$ , the Cartesian product  $A \times B$  is a set.

PROOF: By the Subset Axiom applied to  $\mathcal{PP}(A \cup B)$ .  $\square$

**Lemma 28.** If  $(x, y) \in \mathbf{A}$  then  $x, y \in \bigcup \bigcup \mathbf{A}$ .

PROOF: Easy.  $\square$

## 4 Relations

**Definition 29** (Relation). A *relation* is a class of ordered pairs. It is *small* iff it is a set.

When  $\mathbf{R}$  is a relation, we write  $x\mathbf{R}y$  for  $(x, y) \in \mathbf{R}$ .

**Definition 30** (Domain). The *domain* of a class  $\mathbf{R}$  is  $\text{dom } \mathbf{R} = \{x : \exists y.(x, y) \in \mathbf{R}\}$ .

**Definition 31** (Range). The *range* of a class  $\mathbf{R}$  is  $\text{ran } \mathbf{R} = \{y : \exists x.(x, y) \in \mathbf{R}\}$ .

**Definition 32** (Field). The *field* of a class  $\mathbf{R}$  is  $\text{fld } \mathbf{R} = \text{dom } \mathbf{R} \cup \text{ran } \mathbf{R}$ .

**Proposition 33.** If  $R$  is a set then  $\text{dom } R$ ,  $\text{ran } R$  and  $\text{fld } R$  are sets.

PROOF: Apply the Subset Axiom to  $\bigcup \bigcup R$ .  $\square$

**Definition 34** (Single-Rooted). A class  $\mathbf{R}$  is *single-rooted* iff, for all  $y \in \text{ran } \mathbf{R}$ , there is only one  $x$  such that  $x\mathbf{R}y$ .

**Definition 35** (Inverse). The *inverse* of a class  $\mathbf{F}$  is the class  $\mathbf{F}^{-1} = \{(y, x) \mid (x, y) \in \mathbf{F}\}$ .

**Theorem 36.** For any class  $\mathbf{F}$ , we have  $\text{dom } \mathbf{F}^{-1} = \text{ran } \mathbf{F}$  and  $\text{ran } \mathbf{F}^{-1} = \text{dom } \mathbf{F}$ .

PROOF: Easy.  $\square$

**Theorem 37.** For a relation  $\mathbf{F}$ ,  $(\mathbf{F}^{-1})^{-1} = \mathbf{F}$ .

PROOF: Easy.  $\square$

**Definition 38** (Composition). The *composition* of classes  $\mathbf{F}$  and  $\mathbf{G}$  is the class  $\mathbf{G} \circ \mathbf{F} = \{(x, z) \mid \exists y.(x, y) \in \mathbf{F} \wedge (y, z) \in \mathbf{G}\}$ .

**Theorem 39.** For any classes  $\mathbf{F}$  and  $\mathbf{G}$ ,  $(\mathbf{F} \circ \mathbf{G})^{-1} = \mathbf{G}^{-1} \circ \mathbf{F}^{-1}$ .

PROOF: Easy.  $\square$

**Definition 40** (Restriction). The *restriction* of the class  $\mathbf{F}$  to the class  $\mathbf{A}$  is the class  $\mathbf{F} \upharpoonright \mathbf{A} = \{(x, y) : x \in \mathbf{A} \wedge (x, y) \in \mathbf{F}\}$ .

**Definition 41** (Image). The *image* of the class  $\mathbf{A}$  under the class  $\mathbf{F}$  is the class  $\mathbf{F}(\mathbf{A}) = \{y : \exists x \in \mathbf{A}. (x, y) \in \mathbf{F}\}$ .

**Theorem 42.**

$$\mathbf{F}(\mathbf{A} \cup \mathbf{B}) = \mathbf{F}(\mathbf{A}) \cup \mathbf{F}(\mathbf{B})$$

PROOF: Easy.  $\square$

**Theorem 43.**

$$\mathbf{F}\left(\bigcup \mathbf{A}\right) = \bigcup \{\mathbf{F}(X) : X \in \mathbf{A}\}$$

PROOF: Easy.  $\square$

**Theorem 44.**

$$\mathbf{F}(\mathbf{A} \cap \mathbf{B}) \subseteq \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B})$$

*Equality holds if  $\mathbf{F}$  is single-rooted.*

PROOF: Easy.  $\square$

**Theorem 45.**

$$\mathbf{F}\left(\bigcap \mathbf{A}\right) \subseteq \bigcap \{\mathbf{F}(X) : X \in \mathbf{A}\}$$

*Equality holds if  $\mathbf{F}$  is single-rooted.*

PROOF: Easy.  $\square$

**Theorem 46.**

$$\mathbf{F}(\mathbf{A}) - \mathbf{F}(\mathbf{B}) \subseteq \mathbf{F}(\mathbf{A} - \mathbf{B})$$

*Equality holds if  $\mathbf{F}$  is single-rooted.*

PROOF: Easy.  $\square$

**Definition 47** (Reflexive). A binary relation  $\mathbf{R}$  on  $\mathbf{A}$  is *reflexive* on  $\mathbf{A}$  if and only if  $\forall x \in \mathbf{A}. x\mathbf{R}x$ .

**Definition 48** (Symmetric). A binary relation  $\mathbf{R}$  is *symmetric* iff, whenever  $x\mathbf{R}y$ , then  $y\mathbf{R}x$ .

**Definition 49** (Transitive). A binary relation  $\mathbf{R}$  is *transitive* iff, whenever  $x\mathbf{R}y$  and  $y\mathbf{R}z$ , then  $x\mathbf{R}z$ .

## 5 $n$ -ary Relations

**Definition 50.** Given objects  $a, b, c$ , define the *ordered triple*  $(a, b, c)$  to be  $((a, b), c)$ .

Define  $(a, b, c, d) = ((a, b, c), d)$ , etc.

Define the *1-tuple*  $(a)$  to be  $a$ .

**Definition 51** ( $n$ -ary Relation). Given a class  $\mathbf{A}$ , an  *$n$ -ary relation* on  $\mathbf{A}$  is a class of ordered  $n$ -tuples, all of whose components are in  $\mathbf{A}$ .

## 6 Functions

**Definition 52** (Function). A *function* is a relation  $\mathbf{F}$  such that, for all  $x \in \text{dom } \mathbf{F}$ , there is only one  $y$  such that  $x\mathbf{F}y$ . We call this unique  $y$  the *value* of  $\mathbf{F}$  at  $x$  and denote it by  $\mathbf{F}(x)$ .

We say  $\mathbf{F}$  is a function *from*  $\mathbf{A}$  *into*  $\mathbf{B}$ , or  $\mathbf{F}$  *maps*  $\mathbf{A}$  *into*  $\mathbf{B}$ , and write  $\mathbf{F} : \mathbf{A} \rightarrow \mathbf{B}$ , iff  $\mathbf{F}$  is a function,  $\text{dom } \mathbf{F} = \mathbf{A}$ , and  $\text{ran } \mathbf{F} \subseteq \mathbf{B}$ .

If, in addition,  $\text{ran } \mathbf{F} = \mathbf{B}$ , we say  $\mathbf{F}$  is a function from  $\mathbf{A}$  *onto*  $\mathbf{B}$ .

**Theorem 53.** For a class  $\mathbf{F}$ ,  $\mathbf{F}^{-1}$  is a function if and only if  $\mathbf{F}$  is single-rooted.

PROOF: Easy.  $\square$

**Theorem 54.** A relation  $\mathbf{F}$  is a function if and only if  $\mathbf{F}^{-1}$  is single-rooted.

PROOF: Easy.  $\square$

**Theorem 55.** For any function  $\mathbf{G}$  and classes  $\mathbf{A}$  and  $\mathbf{B}$ ,

$$\begin{aligned}\mathbf{G}^{-1}\left(\bigcup \mathbf{A}\right) &= \bigcup \{\mathbf{G}^{-1}(X) : X \in \mathbf{A}\} \\ \mathbf{G}^{-1}\left(\bigcap \mathbf{A}\right) &= \bigcap \{\mathbf{G}^{-1}(X) : X \in \mathbf{A}\} \quad (\text{if } \mathbf{A} \neq \emptyset) \\ \mathbf{G}^{-1}(\mathbf{A} - \mathbf{B}) &= \mathbf{G}^{-1}(\mathbf{A}) - \mathbf{G}^{-1}(\mathbf{B})\end{aligned}$$

PROOF: Easy.  $\square$

**Theorem 56.** Assume that  $\mathbf{F}$  and  $\mathbf{G}$  are functions. Then  $\mathbf{F} \circ \mathbf{G}$  is a function, its domain is  $\{x \in \text{dom } \mathbf{G} : \mathbf{G}(x) \in \text{dom } \mathbf{F}\}$ , and for  $x$  in its domain,

$$(\mathbf{F} \circ \mathbf{G})(x) = \mathbf{F}(\mathbf{G}(x)) .$$

PROOF: Easy.  $\square$

**Definition 57** (One-to-one). A function  $\mathbf{F}$  is *one-to-one* or an *injection* iff it is single-rooted.

**Theorem 58.** Let  $\mathbf{F}$  be a one-to-one function. For  $x \in \text{dom } \mathbf{F}$ ,  $\mathbf{F}^{-1}(\mathbf{F}(x)) = x$ .

PROOF: Easy.  $\square$

**Theorem 59.** Let  $\mathbf{F}$  be a one-to-one function. For  $y \in \text{ran } \mathbf{F}$ ,  $\mathbf{F}(\mathbf{F}^{-1}(y)) = y$ .

PROOF: Easy.  $\square$

**Definition 60** (Identity Function). For any class  $\mathbf{A}$ , the *identity* function on  $\mathbf{A}$  is  $\text{id}_{\mathbf{A}} = \{(x, x) \mid x \in \mathbf{A}\}$ .

**Theorem 61.** Let  $F : A \rightarrow B$ . Assume  $A \neq \emptyset$ . Then  $F$  has a left inverse (i.e. there exists  $G : B \rightarrow A$  such that  $G \circ F = \text{id}_A$ ) if and only if  $F$  is one-to-one.

PROOF:

$\langle 1 \rangle$ 1. If  $F$  is one-to-one then  $F$  has a left inverse.

⟨2⟩1. ASSUME:  $F$  is one-to-one.

⟨2⟩2.  $F^{-1} : \text{ran } F \rightarrow A$

⟨2⟩3. PICK  $a \in A$

⟨2⟩4. Define  $G : B \rightarrow A$  by:

$$G(x) = \begin{cases} F^{-1}(x) & \text{if } x \in \text{ran } F \\ a & \text{if } x \in B - \text{ran } F \end{cases}$$

⟨2⟩5.  $\forall x \in A. G(F(x)) = x$

⟨1⟩2. If  $F$  has a left inverse then  $F$  is one-to-one.

⟨2⟩1. ASSUME:  $F$  has a left inverse  $G$ .

⟨2⟩2. LET:  $x, y \in A$  with  $F(x) = F(y)$

⟨2⟩3.  $x = y$

PROOF:  $x = G(F(x)) = G(F(y)) = y$ .

□

**Definition 62** (Binary Operation). A *binary operation* on a set  $A$  is a function from  $A \times A$  into  $A$ .

## 7 The Axiom of Choice

**Axiom 63** (Choice). For any relation  $R$  there exists a function  $H \subseteq R$  with  $\text{dom } H = \text{dom } R$ .

**Theorem 64.** Let  $F : A \rightarrow B$ . Then  $F$  has a right inverse if and only if  $F$  maps  $A$  onto  $B$ .

PROOF:

⟨1⟩1. If  $F$  has a right inverse then  $F$  maps  $A$  onto  $B$ .

PROOF: If  $H : B \rightarrow A$  is a right inverse, then for any  $y$  in  $B$ , we have  $y = F(H(y))$ .

⟨1⟩2. If  $F$  maps  $A$  onto  $B$  then  $F$  has a right inverse.

⟨2⟩1. ASSUME:  $F$  maps  $A$  onto  $B$ .

⟨2⟩2. PICK a function  $H$  with  $H \subseteq F^{-1}$  and  $\text{dom } H = \text{dom } F^{-1}$

PROOF: By the Axiom of Choice.

⟨2⟩3.  $\text{dom } H = B$

PROOF:  $\text{dom } H = \text{dom } F^{-1} = \text{ran } F = B$  by ⟨2⟩1.

⟨2⟩4. For all  $y \in B$  we have  $F(H(y)) = y$

⟨3⟩1. LET:  $y \in B$

⟨3⟩2.  $(y, H(y)) \in F^{-1}$

⟨3⟩3.  $F(H(y)) = y$

□

## 8 Sets of Functions

**Definition 65.** Let  $A$  be a set and  $\mathbf{B}$  be a class. Then  $\mathbf{B}^A$  is the class of all functions  $A \rightarrow \mathbf{B}$ .

## 9 Dependent Products

**Definition 66.** Let  $I$  be a set and  $H_i$  a set for all  $i \in I$ . Define

$$\prod_{i \in I} H_i = \{f : f \text{ is a function, } \text{dom } f = I, \forall i \in I. f(i) \in H_i\} .$$

**Theorem 67.** *The Axiom of Choice is equivalent to the statement: For any set  $I$  and any function  $H$  with domain  $I$ , if  $H(i) \neq \emptyset$  for all  $i \in I$ , then  $\prod_{i \in I} H(i) \neq \emptyset$*

PROOF:

- ⟨1⟩1. If the Axiom of Choice is true then, for any set  $I$  and any function  $H$  with domain  $I$ , if  $H(i) \neq \emptyset$  for all  $i \in I$ , then  $\prod_{i \in I} H(i) \neq \emptyset$ .
- ⟨2⟩1. ASSUME: The Axiom of Choice.
- ⟨2⟩2. LET:  $I$  be a set.
- ⟨2⟩3. LET:  $H$  be a function with domain  $I$ .
- ⟨2⟩4. ASSUME:  $H(i) \neq \emptyset$  for all  $i \in I$ .
- ⟨2⟩5. LET:  $R = \{(i, x) : i \in I, x \in H(i)\}$
- ⟨2⟩6. PICK a function  $F \subseteq R$  with  $\text{dom } F = \text{dom } R$   
 PROVE:  $F \in \prod_{i \in I} H(i)$   
 PROOF: By the Axiom of Choice.
- ⟨2⟩7.  $\text{dom } H = I$   
 PROOF: We have  $\text{dom } R = I$  since for all  $i \in I$  there exists  $x$  such that  $x \in H(i)$ .
- ⟨2⟩8.  $\forall i \in I. F(i) \in H(i)$   
 PROOF: Since  $iRF(i)$ .
- ⟨1⟩2. If, for any set  $I$  and any function  $H$  with domain  $I$ , if  $H(i) \neq \emptyset$  for all  $i \in I$ , then  $\prod_{i \in I} H(i) \neq \emptyset$ , then the Axiom of Choice is true.
- ⟨2⟩1. ASSUME: For any set  $I$  and any function  $H$  with domain  $I$ , if  $H(i) \neq \emptyset$  for all  $i \in I$ , then  $\prod_{i \in I} H(i) \neq \emptyset$
- ⟨2⟩2. LET:  $R$  be a relation
- ⟨2⟩3. LET:  $I = \text{dom } R$
- ⟨2⟩4. Define the function  $H$  with domain  $I$  by: for  $i \in I$ ,  $H(i) = \{y : iRy\}$
- ⟨2⟩5.  $H(i) \neq \emptyset$  for all  $i \in I$
- ⟨2⟩6. PICK  $F \in \prod_{i \in I} H(i)$   
 PROOF: By ⟨2⟩1
- ⟨2⟩7.  $F$  is a function
- ⟨2⟩8.  $F \subseteq R$   
 PROOF: For all  $i \in I$  we have  $F(i) \in H(i)$  and so  $iRF(i)$ .
- ⟨2⟩9.  $\text{dom } F = \text{dom } R$

□

## 10 Equivalence Relations

**Definition 68** (Equivalence Relation). An *equivalence relation* on  $\mathbf{A}$  is a binary relation on  $\mathbf{A}$  that is reflexive on  $\mathbf{A}$ , symmetric and transitive.



**Theorem 69.** *If  $\mathbf{R}$  is a symmetric and transitive relation then  $\mathbf{R}$  is an equivalence relation on  $\text{fld } \mathbf{R}$ .*

PROOF:

- $\langle 1 \rangle 1.$  LET:  $x \in \text{fld } \mathbf{R}$
- $\langle 1 \rangle 2.$  PICK  $y$  such that either  $x\mathbf{R}y$  or  $y\mathbf{R}x$
- $\langle 1 \rangle 3.$   $x\mathbf{R}y$  and  $y\mathbf{R}x$

PROOF: Since  $\mathbf{R}$  is symmetric.

- $\langle 1 \rangle 4.$   $x\mathbf{R}x$

PROOF: Since  $\mathbf{R}$  is transitive.

□

**Definition 70** (Equivalence Class). If  $\mathbf{R}$  is an equivalence relation and  $x \in \text{fld } \mathbf{R}$ , the *equivalence class* of  $x$  modulo  $\mathbf{R}$  is

$$[x]_{\mathbf{R}} = \{t : x\mathbf{R}t\} .$$

**Lemma 71.** *Assume that  $\mathbf{R}$  is an equivalence relation on  $\mathbf{A}$  and that  $x$  and  $y$  belong to  $\mathbf{A}$ . Then*

$$[x]_{\mathbf{R}} = [y]_{\mathbf{R}} \text{ iff } x\mathbf{R}y .$$

PROOF:

- $\langle 1 \rangle 1.$  If  $[x]_{\mathbf{R}} = [y]_{\mathbf{R}}$  then  $x\mathbf{R}y$ 
  - $\langle 2 \rangle 1.$  ASSUME:  $[x]_{\mathbf{R}} = [y]_{\mathbf{R}}$
  - $\langle 2 \rangle 2.$   $y \in [y]_{\mathbf{R}}$
  - PROOF: Since  $\mathbf{R}$  is reflexive on  $\mathbf{A}$ .
  - $\langle 2 \rangle 3.$   $y \in [x]_{\mathbf{R}}$
  - $\langle 2 \rangle 4.$   $x\mathbf{R}y$
- $\langle 1 \rangle 2.$  If  $x\mathbf{R}y$  then  $[x]_{\mathbf{R}} = [y]_{\mathbf{R}}$ 
  - $\langle 2 \rangle 1.$  ASSUME:  $x\mathbf{R}y$
  - $\langle 2 \rangle 2.$   $[y]_{\mathbf{R}} \subseteq [x]_{\mathbf{R}}$ 
    - $\langle 3 \rangle 1.$  LET:  $z \in [y]_{\mathbf{R}}$
    - $\langle 3 \rangle 2.$   $y\mathbf{R}z$
    - $\langle 3 \rangle 3.$   $x\mathbf{R}z$

PROOF: Since  $\mathbf{R}$  is transitive.

- $\langle 3 \rangle 4.$   $z \in [x]_{\mathbf{R}}$

- $\langle 2 \rangle 3.$   $y\mathbf{R}x$

PROOF: Since  $\mathbf{R}$  is symmetric.

- $\langle 2 \rangle 4.$   $[x]_{\mathbf{R}} \subseteq [y]_{\mathbf{R}}$

PROOF: Similar.

□

**Definition 72** (Partition). A *partition* of a set  $A$  is a set  $P \subseteq \mathcal{P}A$  such that:

- Every member of  $P$  is nonempty.
- Any two distinct members of  $P$  are disjoint.
- $A = \bigcup P$

**Theorem 73.** *Let  $R$  be an equivalence relation on the set  $A$ . Then the set of all equivalence classes is a partition of  $A$ .*

PROOF:

⟨1⟩1. Every equivalence class is nonempty.

PROOF: For any  $x \in A$  we have  $x \in [x]_R$ .

⟨1⟩2. Any two distinct equivalence classes are disjoint.

⟨2⟩1. LET:  $x, y \in A$

⟨2⟩2. ASSUME:  $z \in [x]_R \cap [y]_R$

PROVE:  $[x]_R = [y]_R$

⟨2⟩3.  $xRy$

⟨3⟩1.  $xRz$

⟨3⟩2.  $yRz$

⟨3⟩3.  $zRy$

PROOF: By ⟨3⟩2 and symmetry.

⟨3⟩4.  $xRy$

PROOF: By ⟨3⟩1, ⟨3⟩3 and transitivity.

⟨2⟩4.  $[x]_R = [y]_R$

PROOF: By Lemma 3N.

⟨1⟩3.  $A$  is the union of all the equivalence classes.

PROOF: For any  $x \in A$  we have  $x \in [x]_R$ .

□

**Definition 74** (Quotient Set). If  $R$  is an equivalence relation on the set  $A$ , then the *quotient set*  $A/R$  is the set of all equivalence classes, and the *natural map* or *canonical map*  $\phi : A \rightarrow A/R$  is defined by  $\phi(x) = [x]_R$ .

**Theorem 75.** *Assume that  $R$  is an equivalence relation on  $A$  and that  $F : A \rightarrow B$ . Assume that  $F$  is compatible with  $R$ ; that is, whenever  $xRy$ , then  $F(x) = F(y)$ . Then there exists a unique  $\bar{F} : A/R \rightarrow B$  such that  $F = \bar{F} \circ \phi$ .*

PROOF: The unique such  $\bar{F}$  is  $\{([x], F(x)) : x \in A\}$ . □

## 11 Linear Orders

**Definition 76** (Linear Ordering). Let  $\mathbf{A}$  be a class. A *linear ordering* or *total ordering* on  $\mathbf{A}$  is a relation  $\mathbf{R}$  on  $\mathbf{A}$  such that:

- $\mathbf{R}$  is transitive.
- $\mathbf{R}$  satisfies *trichotomy* on  $\mathbf{A}$ ; i.e. for any  $x, y \in \mathbf{A}$ , exactly one of

$$x\mathbf{R}y, x = y, y\mathbf{R}x$$

holds.

**Theorem 77.** *Let  $\mathbf{R}$  be a linear ordering on  $\mathbf{A}$ .*

1. *There is no  $x$  such that  $x\mathbf{R}x$ .*

2. For distinct  $x$  and  $y$  in  $\mathbf{A}$ , either  $x\mathbf{R}y$  or  $y\mathbf{R}x$ .

PROOF: Immediate from trichotomy.  $\square$

**Definition 78** (Strictly Monotone Functions). Let  $A$  and  $B$  be linearly ordered sets. A function  $f : A \rightarrow B$  is *strictly monotone* iff, for all  $x, y \in A$ , if  $x < y$  then  $f(x) < f(y)$ .

**Theorem 79.** Let  $A$  and  $B$  be linearly ordered sets and  $f : A \rightarrow B$  be strictly monotone. For all  $x, y \in A$ , if  $f(x) < f(y)$  then  $x < y$ .

PROOF: We have  $f(x) \neq f(y)$  and  $f(y) \not< f(x)$  by trichotomy, hence  $x \neq y$  and  $y \not< x$  since  $f$  is strictly monotone, hence  $x < y$  by trichotomy.  $\square$

**Theorem 80.** Every strictly monotone function is injective.

PROOF: If  $f(x) = f(y)$ , then we have  $f(x) \not< f(y)$  and  $f(y) \not< f(x)$  by trichotomy, hence  $x \not< y$  and  $y \not< x$  since  $f$  is strictly monotone, hence  $x = y$  by trichotomy.  $\square$

## 12 Natural Numbers

**Definition 81** (Successor). The *successor* of a set  $a$  is the set  $a^+ = a \cup \{a\}$ .

**Definition 82** (Inductive). A class  $\mathbf{A}$  is *inductive* iff  $\emptyset \in \mathbf{A}$  and  $\forall a \in \mathbf{A}. a^+ \in \mathbf{A}$ .

**Axiom 83** (Infinity). *There exists an inductive set.*

**Definition 84** (Natural Number). A *natural number* is a set that belongs to every inductive set.

We write  $\omega$  for the class of all natural numbers.

**Theorem 85.** The class  $\omega$  is a set.

PROOF: Pick an inductive set  $I$  (by the Axiom of Infinity), then apply a Subset Axiom to  $I$ .  $\square$

**Theorem 86.** The set  $\omega$  is inductive, and is a subset of every inductive set.

PROOF: Easy.  $\square$

**Corollary 86.1** (Proof by Induction). Any inductive subclass of  $\omega$  is equal to  $\omega$ .

**Theorem 87.** Every natural number except 0 is the successor of some natural number.

PROOF: Easy proof by induction.  $\square$

**Definition 88** (Peano System). A *Peano system* is a triple  $\langle N, S, e \rangle$  consisting of a set  $N$ , a function  $S : N \rightarrow N$  and an element  $e \in N$  such that:

1.  $e \notin \text{ran } S$
2.  $S$  is one-to-one
3. Any subset  $A \subseteq N$  that contains  $e$  and is closed under  $S$  equals  $N$ .

**Definition 89** (Transitive Set). A set  $A$  is a *transitive set* iff every member of a member of  $A$  is a member of  $A$ .

**Theorem 90.** For any transitive set  $a$ ,  $\bigcup(a^+) = a$ .

PROOF:

$$\begin{aligned}
 \bigcup(a^+) &= \bigcup(a \cup \{a\}) \\
 &= \bigcup a \cup \bigcup \{a\} \\
 &= \bigcup a \cup a \\
 &= a
 \end{aligned}$$

since  $\bigcup a \subseteq a$ .  $\square$

**Theorem 91.** Every natural number is a transitive set.

PROOF:

$\langle 1 \rangle 1$ . 0 is a transitive set.

PROOF: Vacuous.

$\langle 1 \rangle 2$ . For any natural number  $n$ , if  $n$  is a transitive set then  $n^+$  is a transitive set.

$\langle 2 \rangle 1$ . LET:  $n$  be a natural number that is a transitive set.

$\langle 2 \rangle 2$ .  $\bigcup(n^+) \subseteq n^+$

PROOF: Theorem 90.

$\square$

**Theorem 92.**  $\langle \omega, \sigma, 0 \rangle$  is a Peano system, where  $0 = \emptyset$  and  $\sigma = \{ \langle n, n^+ \rangle : n \in \omega \}$ .

PROOF:

$\langle 1 \rangle 1$ .  $0 \notin \text{ran } \sigma$

PROOF: For any  $n \in \omega$  we have  $0 \neq n^+$  since  $n \in n^+$  and  $n \notin 0$ .

$\langle 1 \rangle 2$ .  $\sigma$  is one-to-one.

PROOF: If  $m^+ = n^+$  then  $m = \bigcup(m^+) = \bigcup(n^+) = n$  using Theorems 90 and 91.

$\langle 1 \rangle 3$ . Any subset  $A \subseteq \omega$  that contains 0 and is closed under  $\sigma$  equals  $\omega$ .

$\square$

**Theorem 93.** The set  $\omega$  is a transitive set.

PROOF:

$\langle 1 \rangle 1$ . For every natural number  $n$  we have  $\forall m \in n$ .  $m$  is a natural number.

$\langle 2 \rangle 1$ .  $\forall m \in 0$ .  $m$  is a natural number.

PROOF: Vacuous.

⟨2⟩2. If  $n$  is a natural number and  $\forall m \in n$ .  $m$  is a natural number, then  $\forall m \in n^+$ .  $m$  is a natural number.

PROOF: Since if  $m \in n^+$  we have either  $m \in n$  or  $m = n$ , and  $m$  is a natural number in either case.

□

**Theorem 94** (Recursion Theorem on  $\omega$ ). *Let  $A$  be a set,  $a \in A$  and  $F : A \rightarrow A$ . Then there exists a unique function  $h : \omega \rightarrow A$  such that*

$$h(0) = a ,$$

and for every  $n$  in  $\omega$ ,

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

PROOF:

⟨1⟩1. Let us call a function  $v$  *acceptable* iff  $\text{dom } v \subseteq \omega$ ,  $\text{ran } v \subseteq A$  and:

1. If  $0 \in \text{dom } v$  then  $v(0) = a$
2. For all  $n \in \omega$ , if  $n^+ \in \text{dom } v$  then  $n \in \text{dom } v$  and  $v(n^+) = F(v(n))$ .

⟨1⟩2. LET:  $\mathcal{K}$  be the set of acceptable functions.

⟨1⟩3. LET:  $h = \bigcup \mathcal{K}$

⟨1⟩4.  $h$  is a function.

⟨2⟩1. LET:  $S = \{n \in \omega : \text{for at most one } y, (n, y) \in h\}$

⟨2⟩2.  $S$  is inductive.

⟨3⟩1.  $0 \in S$

⟨4⟩1. LET:  $\langle 0, y_1 \rangle, \langle 0, y_2 \rangle \in h$

⟨4⟩2. PICK acceptable  $v_1$  and  $v_2$  such that  $v_1(0) = y_1$  and  $v_2(0) = y_2$

⟨4⟩3.  $y_1 = a$

⟨4⟩4.  $y_2 = a$

⟨4⟩5.  $y_1 = y_2$

⟨3⟩2.  $\forall k \in S. k^+ \in S$

⟨4⟩1. LET:  $k \in S$

⟨4⟩2. LET:  $(k^+, y_1), (k^+, y_2) \in h$

⟨4⟩3. PICK acceptable  $v_1, v_2$  such that  $v_1(k^+) = y_1$  and  $v_2(k^+) = y_2$

⟨4⟩4.  $y_1 = F(v_1(k))$

⟨4⟩5.  $y_2 = F(v_2(k))$

⟨4⟩6.  $v_1(k) = v_2(k)$

⟨5⟩1.  $(k, v_1(k)), (k, v_2(k)) \in h$

⟨5⟩2. Q.E.D.

PROOF: By ⟨4⟩1

⟨4⟩7.  $y_1 = y_2$

⟨2⟩3.  $S = \omega$

⟨1⟩5.  $h$  is acceptable.

⟨2⟩1. If  $0 \in \text{dom } h$  then  $h(0) = a$

⟨3⟩1. ASSUME:  $0 \in \text{dom } h$

⟨3⟩2. PICK  $v$  acceptable with  $v(0) = h(0)$

⟨3⟩3.  $v(0) = a$

- ⟨3⟩4.  $h(0) = a$
- ⟨2⟩2. For all  $n \in \omega$ , if  $n^+ \in \text{dom } h$  then  $n \in \text{dom } h$  and  $h(n^+) = F(h(n))$
- ⟨3⟩1. LET:  $n \in \omega$  with  $n^+ \in \text{dom } h$
- ⟨3⟩2. PICK  $v$  acceptable with  $v(n^+) = h(n^+)$
- ⟨3⟩3.  $n \in \text{dom } v$
- ⟨3⟩4.  $v(n) = h(n)$
- ⟨3⟩5.  $h(n^+) = F(h(n))$

PROOF:

$$\begin{aligned}
 h(n^+) &= v(n^+) \\
 &= F(v(n)) \\
 &= F(h(n))
 \end{aligned}$$

- ⟨1⟩6.  $\text{dom } h = \omega$
- ⟨2⟩1.  $0 \in \text{dom } h$
- PROOF: Since  $\{(0, a)\}$  is an acceptable function.
- ⟨2⟩2.  $\forall n \in \text{dom } h. n^+ \in \text{dom } h$
- ⟨3⟩1. LET:  $n \in \text{dom } h$
- ⟨3⟩2. PICK an acceptable  $v$  such that  $n \in \text{dom } v$
- ⟨3⟩3. ASSUME: w.l.o.g.  $n^+ \notin \text{dom } v$
- ⟨3⟩4.  $v \cup \{(n^+, F(v(n)))\}$  is acceptable.
- ⟨1⟩7. For any acceptable function  $h' : \omega \rightarrow A$  we have  $h' = h$
- ⟨2⟩1. LET:  $h' : \omega \rightarrow A$  be acceptable.
- ⟨2⟩2.  $h'(0) = h(0)$
- PROOF:  $h'(0) = h(0) = a$
- ⟨2⟩3.  $\forall n \in \omega. h'(n) = h(n) \Rightarrow h'(n^+) = h(n^+)$
- PROOF: We have  $h'(n^+) = F(h'(n)) = F(h(n)) = h(n^+)$ .

□

**Theorem 95.** *Let  $(N, S, e)$  be a Peano system. Then  $(\omega, \sigma, 0)$  is isomorphic to  $(N, S, e)$ , i.e. there is a function  $h$  mapping  $\omega$  one-to-one onto  $N$  in a way that preserves the successor operation*

$$h(\sigma(n)) = S(h(n))$$

and the zero element

$$h(0) = e .$$

PROOF:

- ⟨1⟩1. There exists a function  $h$  that satisfies those two conditions.
- PROOF: By the Recursion Theorem.
- ⟨1⟩2. For all  $m, n \in \omega$ , if  $m \neq n$  then  $h(m) \neq h(n)$
- ⟨2⟩1. For all  $n \in \omega$ , if  $n \neq 0$  then  $h(n) \neq h(0)$
- ⟨3⟩1. LET:  $n \in \omega$
- ⟨3⟩2. ASSUME:  $n \neq 0$
- ⟨3⟩3. PICK  $p$  such that  $n = p^+$
- ⟨3⟩4.  $h(n) \neq h(0)$
- PROOF:  $h(n) = S(h(p)) \neq e = h(0)$ .

$\langle 2 \rangle 2$ . For all  $m \in \omega$ , if  $\forall n(m \neq n \Rightarrow h(m) \neq h(n))$  then  $\forall n(m^+ \neq n \Rightarrow h(m^+) \neq h(n))$   
 $\langle 3 \rangle 1$ . LET:  $m \in \omega$   
 $\langle 3 \rangle 2$ . ASSUME:  $\forall n(m \neq n \Rightarrow h(m) \neq h(n))$   
 $\langle 3 \rangle 3$ . LET:  $n \in \omega$   
 $\langle 3 \rangle 4$ . ASSUME:  $m^+ \neq n$   
PROVE:  $h(m^+) \neq h(n)$   
 $\langle 3 \rangle 5$ . CASE:  $n = 0$   
PROOF:  $h(m^+) = S(h(m)) \neq e = h(n)$   
 $\langle 3 \rangle 6$ . CASE:  $n = p^+$   
 $\langle 4 \rangle 1$ .  $m \neq p$   
 $\langle 4 \rangle 2$ .  $h(m) \neq h(p)$   
 $\langle 4 \rangle 3$ .  $S(h(m)) \neq S(h(p))$   
 $\langle 4 \rangle 4$ .  $h(m^+) \neq h(p^+)$   
 $\langle 1 \rangle 3$ . For all  $x \in N$ , there exists  $n \in \omega$  such that  $h(n) = x$   
PROOF: An easy induction on  $x$ .  
□

## 13 Arithmetic

**Definition 96** (Addition). *Addition*  $+$  is the binary operation on  $\omega$  such that, for all  $m, n \in \omega$ ,

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

**Theorem 97** (Associative Law for Addition).

$$\forall m, n, p \in \omega. m + (n + p) = (m + n) + p$$

PROOF:

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

□

**Theorem 98** (Commutative Law for Addition).

$$\forall m, n \in \omega. m + n = n + m$$

PROOF:

$$\begin{aligned}
\langle 1 \rangle 1. \forall n \in \omega. 0 + n &= n + 0 \\
\langle 2 \rangle 1. 0 + 0 &= 0 + 0
\end{aligned}$$

$\langle 2 \rangle 2$ . For all  $n \in \omega$ , if  $0 + n = n + 0$  then  $0 + n^+ = n^+ + 0$

PROOF:

$$\begin{aligned} 0 + n^+ &= (0 + n)^+ \\ &= n^+ && \text{(induction hypothesis)} \\ &= n^+ + 0 \end{aligned}$$

$\langle 1 \rangle 2$ . For all  $m \in \omega$ , if  $\forall n. m + n = n + m$  then  $\forall n. m^+ + n = n + m^+$

$\langle 2 \rangle 1$ . LET:  $m \in \omega$

$\langle 2 \rangle 2$ . ASSUME:  $\forall n. m + n = n + m$

$\langle 2 \rangle 3$ .  $m^+ + 0 = 0 + m^+$

PROOF: From  $\langle 1 \rangle 1$

$\langle 2 \rangle 4$ . For all  $n \in \omega$ , if  $m^+ + n = n + m^+$  then  $m^+ + n^+ = n^+ + m^+$

PROOF:

$$\begin{aligned} m^+ + n^+ &= (m^+ + n)^+ \\ &= (n + m^+)^+ \\ &= (n + m)^{++} \\ &= (m + n)^{++} && (\langle 2 \rangle 2) \\ &= (m + n^+)^+ \\ &= (n^+ + m)^+ && (\langle 2 \rangle 2) \\ &= n^+ + m^+ \end{aligned}$$

□

**Definition 99** (Multiplication). *Multiplication*  $\cdot$  is the binary operation on  $\omega$  such that, for all  $m, n \in \omega$ ,

$$\begin{aligned} m0 &= 0 \\ m \cdot n^+ &= mn + m \end{aligned}$$

**Theorem 100** (Distributive Law).

$$\forall m, n, p \in \omega. m(n + p) = mn + mp$$

PROOF:

$\langle 1 \rangle 1$ .  $\forall m, n \in \omega. m(n + 0) = mn + m0$

PROOF:

$$\begin{aligned} m(n + 0) &= mn \\ &= mn + 0 \\ &= mn + m0 \end{aligned}$$

$\langle 1 \rangle 2$ . For all  $p \in \omega$ , if  $m(n + p) = mn + mp$  then  $m(n + p^+) = mn + mp^+$



PROOF:

$$\begin{aligned}
m(n + p^+) &= m(n + p)^+ \\
&= m(n + p) + m \\
&= (mn + mp) + m \\
&= mn + (mp + m) \quad (\text{Associative Law for Addition}) \\
&= mn + mp^+
\end{aligned}$$

□

**Theorem 101** (Associative Law for Multiplication).

$$\forall m, n, p \in \omega. m(np) = (mn)p$$

PROOF:

$$\langle 1 \rangle 1. \forall m, n \in \omega. m(n0) = (mn)0$$

PROOF: Both are equal to 0.

$$\langle 1 \rangle 2. \text{ For all } m, n, p \in \omega, \text{ if } m(np) = (mn)p \text{ then } m(np^+) = (mn)p^+$$

PROOF:

$$\begin{aligned}
m(np^+) &= m(np + n) \\
&= m(np) + mn \quad (\text{Distributive Law}) \\
&= (mn)p + mn \\
&= (mn)p^+
\end{aligned}$$

□

**Theorem 102** (Commutative Law for Multiplication).

$$\forall m, n \in \omega. mn = nm$$

PROOF:

$$\langle 1 \rangle 1. \forall n \in \omega. 0n = n0$$

$$\langle 2 \rangle 1. 0 \cdot 0 = 0 \cdot 0$$

$$\langle 2 \rangle 2. \text{ For all } n \in \omega, \text{ if } 0n = n0 \text{ then } 0n^+ = n^+0$$

PROOF:

$$\begin{aligned}
0n^+ &= 0n + 0 \\
&= 0n \\
&= n0 \\
&= 0 \\
&= n^+0
\end{aligned}$$

$$\langle 1 \rangle 2. \text{ For all } m \in \omega, \text{ if } \forall n \in \omega. mn = nm \text{ then } \forall n \in \omega. m^+n = nm^+$$

$$\langle 2 \rangle 1. \text{ LET: } m \in \omega$$

$$\langle 2 \rangle 2. \text{ ASSUME: } \forall n \in \omega. mn = nm$$

$$\langle 2 \rangle 3. m^+0 = 0m^+$$

PROOF: By  $\langle 1 \rangle 1$ .

$$\langle 2 \rangle 4. \text{ For all } n \in \omega, \text{ if } m^+n = nm^+ \text{ then } m^+n^+ = n^+m^+$$

PROOF:

$$\begin{aligned}
m^+n^+ &= m^+n + m^+ \\
&= (m^+n + m)^+ \\
&= (nm^+ + m)^+ \\
&= (nm + n + m)^+ \\
&= (mn + n + m)^+ & (\langle 2 \rangle 2) \\
&= (mn + m + n)^+ & (\text{Associative and Commutative Laws for Addition}) \\
&= (mn^+ + n)^+ \\
&= (n^+m + n)^+ & (\langle 2 \rangle 2) \\
&= n^+m + n^+ \\
&= n^+m^+
\end{aligned}$$

□

## 14 Ordering on the Natural Numbers

**Lemma 103.** *For any natural numbers  $m$  and  $n$ ,  $m \in n$  if and only if  $m^+ \in n^+$ .*

PROOF:

$\langle 1 \rangle 1.$   $\forall m, n \in \omega (m \in n \Rightarrow m^+ \in n^+)$

$\langle 2 \rangle 1.$   $\forall m \in \omega (m \in 0 \Rightarrow m^+ \in 0^+)$

PROOF: Vacuous.

$\langle 2 \rangle 2.$  For all  $n \in \omega$ , if  $\forall m \in n. m^+ \in n^+$  then  $\forall m \in n^+. m^+ \in n^{++}$

$\langle 3 \rangle 1.$  LET:  $n \in \omega$

$\langle 3 \rangle 2.$  ASSUME:  $\forall m \in n. m^+ \in n^+$

$\langle 3 \rangle 3.$  LET:  $m \in n^+$

$\langle 3 \rangle 4.$  CASE:  $m \in n$

$\langle 4 \rangle 1.$   $m^+ \in n^+$

PROOF: By  $\langle 3 \rangle 2$

$\langle 4 \rangle 2.$   $m^+ \in n^{++}$

$\langle 3 \rangle 5.$  CASE:  $m = n$

PROOF:  $m^+ = n^+ \in n^{++}$

$\langle 1 \rangle 2.$   $\forall m, n \in \omega (m^+ \in n^+ \Rightarrow m \in n)$

$\langle 2 \rangle 1.$  LET:  $m, n \in \omega$

$\langle 2 \rangle 2.$  ASSUME:  $m^+ \in n^+$

$\langle 2 \rangle 3.$   $m \in m^+$

$\langle 2 \rangle 4.$   $m^+ \in n$  or  $m^+ = n$

$\langle 2 \rangle 5.$   $m \in n$

PROOF: If  $m^+ \in n$  this follows because  $n$  is transitive (Theorem 91).

□

**Lemma 104.** *For any natural number  $n$  we have  $n \notin n$ .*

PROOF:

- ⟨1⟩1.  $0 \notin 0$
  - ⟨1⟩2. For all  $n \in \omega$ , if  $n \notin n$  then  $n^+ \notin n^+$ 
    - ⟨2⟩1. LET:  $n \in \omega$
    - ⟨2⟩2. ASSUME:  $n^+ \in n^+$ 
      - PROVE:  $n \in n$
    - ⟨2⟩3.  $n^+ \in n$  or  $n^+ = n$
    - ⟨2⟩4.  $n \in n^+$
    - ⟨2⟩5.  $n \in n$
- PROOF: If  $n^+ \in n$  this follows because  $n$  is transitive (Theorem 91).

□

**Theorem 105** (Trichotomy Law for  $\omega$ ). *For any natural numbers  $m$  and  $n$ , exactly one of*

$$m \in n, m = n, n \in m$$

*holds.*

PROOF:

- ⟨1⟩1. For any  $m, n \in \omega$ , at most one of  $m \in n, m = n, n \in m$  holds.
  - PROOF: If  $m \in n$  and  $m = n$  then  $m \in m$  contradicting Lemma 104.
  - If  $m \in n$  and  $n \in m$  then  $m \in m$  by Theorem 91, contradicting Lemma 104.
- ⟨1⟩2. For any  $m, n \in \omega$ , at least one of  $m \in n, m = n, n \in m$  holds.
  - ⟨2⟩1. For all  $n \in \omega$ , either  $0 \in n$  or  $0 = n$ 
    - ⟨3⟩1.  $0 = 0$
    - ⟨3⟩2. For all  $n \in \omega$ , if  $0 \in n$  or  $0 = n$  then  $0 \in n^+$
  - ⟨2⟩2. For all  $m \in \omega$ , if  $\forall n \in \omega (m \in n \vee m = n \vee n \in m)$  then  $\forall n \in \omega (m^+ \in n \vee m^+ = n \vee n \in m^+)$ 
    - ⟨3⟩1. LET:  $m \in \omega$
    - ⟨3⟩2. ASSUME:  $\forall n \in \omega (m \in n \vee m = n \vee n \in m)$
    - ⟨3⟩3. LET:  $n \in \omega$
    - ⟨3⟩4. CASE:  $m \in n$ 
      - PROOF: Then  $m \in n^+$
    - ⟨3⟩5. CASE:  $m = n$ 
      - PROOF: Then  $m \in n^+$
    - ⟨3⟩6. CASE:  $n \in m$ 
      - PROOF: Then  $n^+ \in m^+$  by Lemma 103 so  $n^+ \in m$  or  $n^+ = m$ .

□

**Corollary 105.1.** *The relation  $\in$  is a linear ordering on  $\omega$ .*

**Corollary 105.2.** *For any natural numbers  $m$  and  $n$ ,*

$$m \in n \Leftrightarrow m \subset n .$$

PROOF:

- ⟨1⟩1. LET:  $m, n \in \omega$
- ⟨1⟩2. If  $m \in n$  then  $m \subset n$ .
  - ⟨2⟩1. ASSUME:  $m \in n$

$\langle 2 \rangle 2. m \subseteq n$

PROOF: Theorem 91.

$\langle 2 \rangle 3. m \neq n$

PROOF: Lemma 104.

$\langle 1 \rangle 3. \text{ If } m \subset n \text{ then } m \in n.$

PROOF: We have  $m \neq n$  and  $n \notin m$  by  $\langle 1 \rangle 2$ , hence  $m \in n$  by trichotomy.

□

**Theorem 106.** *For any natural number  $p$ , the function that maps  $n$  to  $n + p$  is strictly monotone. For any natural numbers  $m$ ,  $n$  and  $p$ , we have  $m \in n$  if and only if  $m + p \in n + p$ .*

PROOF: We prove that  $m \in n \Rightarrow m + p \in n + p$ . This is an easy induction on  $p$  using Lemma 103. □

**Theorem 107.** *For any non-zero natural number  $p$ , the function that maps  $n$  to  $np$  is strictly monotone.*

PROOF: Easy induction on  $p$  using Theorem 106. □

**Theorem 108** (Strong Induction). *Let  $A$  be a subset of  $\omega$  and suppose that, for all  $n \in \omega$ , we have*

$$(\forall m < n. m \in A) \Rightarrow n \in A .$$

*Then  $A = \omega$ .*

PROOF: Prove  $\forall n \in \omega. \forall m < n. m \in A$  by induction on  $n$ . □

**Theorem 109** (Well-Ordering of  $\omega$ ). *Every nonempty subset of  $\omega$  has a least element.*

PROOF: If  $A$  is a subset of  $\omega$  with no least element, we prove  $\forall n \in \omega. n \notin A$  by strong induction on  $n$ . □

**Corollary 109.1.** *There is no function  $f : \omega \rightarrow \omega$  such that  $f(n + 1) < f(n)$  for every  $n$ .*

**Lemma 110.** *For any natural numbers  $m$  and  $n$ , we have  $m \in n$  if and only if there exists a natural number  $p$  such that  $n = m + p^+$ .*

PROOF:

$\langle 1 \rangle 1. \text{ For all } m, p, \text{ we have } m \in m + p^+$

PROOF:  $m = m + 0 \in m + p^+$

$\langle 1 \rangle 2. \text{ For all } m, n, \text{ if } m \in n \text{ then there exists } p \text{ such that } n = m + p^+$

$\langle 2 \rangle 1. \text{ For all } m, \text{ if } m \in 0 \text{ then there exists } p \text{ such that } 0 = m + p^+$

PROOF: Vacuous.

$\langle 2 \rangle 2. \text{ For all } n \in \omega, \text{ if } \forall m \in n. \exists p \in \omega. n = m + p^+ \text{ then } \forall m \in n^+. \exists p \in \omega. n^+ = m + p^+$

$\langle 3 \rangle 1. \text{ LET: } n \in \omega$

- ⟨3⟩2. ASSUME:  $\forall m \in n. \exists p \in \omega. n = m + p^+$
  - ⟨3⟩3. LET:  $m \in n^+$
  - ⟨3⟩4. CASE:  $m \in n$ 
    - ⟨4⟩1. PICK  $p$  such that  $n = m + p^+$
    - ⟨4⟩2.  $n^+ = m + p^{++}$
  - ⟨3⟩5. CASE:  $m = n$
- PROOF:  $n^+ = m + 0^+$

□

**Lemma 111.** *For natural numbers  $m, n, p$  and  $q$ , if  $m \in n$  and  $p \in q$  then  $mp + nq \in mq + np$ .*

- ⟨1⟩1. PICK natural numbers  $a$  and  $b$  such that  $n = m + a^+$  and  $q = p + b^+$
- PROOF: Lemma 110.
- ⟨1⟩2.  $mp + nq = mq + np + (a^+ + b)^+$
  - ⟨1⟩3.  $mp + nq \in mq + np$
- PROOF: Lemma 110.

## 15 The Integers

**Theorem 112.** *The relation  $\sim$  is an equivalence relation on  $\omega \times \omega$ , where  $(m, n) \sim (p, q)$  iff  $m + q = n + p$ .*

PROOF:

- ⟨1⟩1. The relation  $\sim$  is reflexive on  $\omega^2$
- PROOF: For any  $m, n$ , we have  $m + n = m + n$  and so  $(m, n) \sim (m, n)$ .
- ⟨1⟩2. The relation  $\sim$  is symmetric.
- PROOF: If  $m + q = n + p$  then  $p + n = q + m$ .
- ⟨1⟩3. The relation  $\sim$  is transitive.
- ⟨2⟩1. ASSUME:  $(m, n) \sim (p, q) \sim (r, s)$
  - ⟨2⟩2.  $m + q = n + p$
  - ⟨2⟩3.  $p + s = q + r$
  - ⟨2⟩4.  $m + p + q + s = n + p + q + r$
  - ⟨2⟩5.  $m + s = n + r$

PROOF: By cancellation of addition in  $\omega$ .

□

**Definition 113.** The set  $\mathbb{Z}$  of *integers* is the quotient set  $(\omega \times \omega) / \sim$ .

**Lemma 114.** *If  $(m, n) \sim (m', n')$  and  $(p, q) \sim (p', q')$  then  $(m + p, n + q) \sim (m' + p', n' + q')$ .*

PROOF: Assume  $m + n' = m' + n$  and  $p + q' = p' + q$ . Then  $m + p + n' + q' = m' + p' + n + q$ . □

**Definition 115 (Addition).** Addition  $+$  on  $\mathbb{Z}$  is the binary operation such that

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

**Theorem 116.** *Addition on  $\mathbb{Z}$  is commutative.*

PROOF: From the definition.  $\square$

**Theorem 117.** *Addition on  $\mathbb{Z}$  is associative.*

PROOF: Easy.  $\square$

**Definition 118 (Zero).** The zero in the integers is  $0 = [(0, 0)]$ .

**Theorem 119.** *For any integer  $a$  we have  $a + 0 = a$ .*

PROOF: Easy.  $\square$

**Theorem 120.** *For any integer  $a$ , there exists an integer  $b$  such that  $a + b = 0$ .*

PROOF: If  $a = [(m, n)]$  take  $b = [(n, m)]$ .  $\square$

**Lemma 121.** *If  $(m, n) \sim (m', n')$  and  $(p, q) \sim (p', q')$  then  $(mp + nq, mq + np) \sim (m'p' + n'q', m'q' + n'p')$ .*

PROOF:

$\langle 1 \rangle 1.$  ASSUME:  $m + n' = m' + n$  and  $p + q' = p' + q$

$\langle 1 \rangle 2.$   $mp + n'p = m'p + np$

$\langle 1 \rangle 3.$   $m'q + nq = mq + n'q$

$\langle 1 \rangle 4.$   $mp + mq' = m'p' + mq$

$\langle 1 \rangle 5.$   $n'p' + n'q = n'p + n'q'$

$\langle 1 \rangle 6.$   $mp + n'p + m'q + nq + mp + mq' + n'p' + n'q = m'p + np + mq + n'q + mp' + mq + n'p + n'q'$

$\langle 1 \rangle 7.$   $mp + nq + m'q' + n'p' = mq + np + m'p' + n'q'$

$\square$

**Definition 122 (Multiplication).** *Multiplication  $\cdot$  is the binary operation on  $\mathbb{Z}$  such that*

$$[(m, n)][(p, q)] = [(mp + nq, mq + np)]$$

**Theorem 123.** *Multiplication is commutative.*

PROOF: Easy.  $\square$

**Theorem 124.** *Multiplication is associative.*

PROOF: Easy.  $\square$

**Theorem 125.** *Multiplication is distributive over addition.*

PROOF: Easy.  $\square$

**Definition 126.** The integer one is  $1 = [(1, 0)]$ .

**Theorem 127.** *For any integer  $a$  we have  $a1 = a$ .*

PROOF: Easy.  $\square$

**Theorem 128.**  $0 \neq 1$

PROOF: Easy.  $\square$

**Lemma 129.** *If  $(m, n) \sim (m', n')$  and  $(p, q) \sim (p', q')$  then  $m + q \in p + n$  iff  $m' + q' \in p' + n'$ .*

PROOF:

$$\begin{aligned} m + q \in p + n &\Leftrightarrow m + q + n' + q' \in p + n + n' + q' \\ &\Leftrightarrow m' + n + q + q' \in p' + n + n' + q \\ &\Leftrightarrow m' + q' \in p' + n' \end{aligned} \quad \square$$

**Definition 130** (Ordering). The ordering  $<$  on  $\mathbb{Z}$  is defined by:  $[(m, n)] < [(p, q)]$  iff  $m + q \in n + p$ .

**Theorem 131.** *The relation  $<$  is a linear ordering on  $\mathbb{Z}$ .*

PROOF:

- $\langle 1 \rangle 1.$   $<$  is transitive.
  - $\langle 2 \rangle 1.$  ASSUME:  $[(m, n)] < [(p, q)]$  and  $[(p, q)] < [(r, s)]$
  - $\langle 2 \rangle 2.$   $m + q \in n + p$  and  $p + s \in q + r$
  - $\langle 2 \rangle 3.$   $m + q + s \in n + p + s$
  - $\langle 2 \rangle 4.$   $n + p + s \in n + q + r$
  - $\langle 2 \rangle 5.$   $m + q + s \in n + q + r$
  - $\langle 2 \rangle 6.$   $m + s \in n + r$
- $\langle 1 \rangle 2.$   $<$  satisfies trichotomy.

PROOF: From trichotomy on  $\omega$ .

$\square$

**Theorem 132.** *For any integers  $a, b$  and  $c$ , we have  $a < b$  iff  $a + c < b + c$ .*

PROOF: An easy consequence of the corresponding property in  $\omega$ .

**Corollary 132.1.** *If  $a + c = b + c$  then  $a = b$ .*

**Theorem 133.** *If  $0 < c$ , then the function that maps an integer  $a$  to  $ac$  is strictly monotone.*

PROOF:

- $\langle 1 \rangle 1.$  LET:  $a, b$  and  $c$  be integers.
- $\langle 1 \rangle 2.$  ASSUME:  $0 < c$  and  $a < b$
- $\langle 1 \rangle 3.$  LET:  $a = [(m, n)]$
- $\langle 1 \rangle 4.$  LET:  $b = [(p, q)]$
- $\langle 1 \rangle 5.$  LET:  $c = [(r, s)]$
- $\langle 1 \rangle 6.$   $s \in r$
- $\langle 1 \rangle 7.$   $m + q \in p + n$
- $\langle 1 \rangle 8.$   $(m + q)r + (p + n)s \in (m + q)s + (p + n)r$

PROOF: Lemma 111.

- $\langle 1 \rangle 9.$   $ac < bc$

□

**Lemma 134.** For integers  $a$  and  $b$ ,  $a(-b) = -(ab)$

PROOF: This follows from the fact that  $ab + a(-b) = a(b + (-b)) = a0 = 0$ . □

**Theorem 135.** For integers  $a$ ,  $b$  and  $c$ , if  $a < b$  and  $c < 0$  then  $ac > bc$ .

PROOF: We have  $0 < -c$  so  $a(-c) < b(-c)$  hence  $-(ac) < -(bc)$  so  $bc < ac$ . □

**Theorem 136.** For any integers  $a$  and  $b$ , if  $ab = 0$  then  $a = 0$  or  $b = 0$ .

PROOF: We prove if  $a \neq 0$  and  $b \neq 0$  then  $ab \neq 0$ .

If  $a > 0$  and  $b > 0$  then  $ab > 0$ . Similarly for the other four cases. □

**Theorem 137.** If  $ac = bc$  and  $c \neq 0$  then  $a = b$ .

PROOF: We have  $(a - b)c = 0$  so  $a - b = 0$  hence  $a = b$ . □

**Definition 138** (Positive). An integer  $a$  is *positive* iff  $0 < a$ .

**Theorem 139.** Define  $E : \omega \rightarrow \mathbb{Z}$  by  $E(n) = [(n, 0)]$ . Then  $E$  maps  $\omega$  one-to-one into  $\mathbb{Z}$ , and:

1.  $E(m + n) = E(m) + E(n)$
2.  $E(mn) = E(m)E(n)$
3.  $m \in n$  if and only if  $E(m) < E(n)$ .

PROOF: Routine calculations. □

## 16 Equinumerosity

**Definition 140** (Equinumerous). Two sets  $A$  and  $B$  are *equinumerous*,  $A \approx B$ , iff there exists a bijection between them.

**Theorem 141.** *Equinumerosity is an equivalence relation on the class of sets.*

PROOF: Easy. □

**Theorem 142** (Cantor 1873). *No set is equinumerous with its power set.*

PROOF:

⟨1⟩1. LET:  $g : A \rightarrow \mathcal{P}A$

PROVE:  $g$  is not surjective.

⟨1⟩2. LET:  $B = \{x \in A : x \notin g(x)\}$

⟨1⟩3.  $\forall x \in A. g(x) \neq B$

PROOF: Because  $x \in B$  iff  $x \notin g(x)$ .

□