C1 Set Theory

Robin Adams

August 18, 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

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

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

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

PROOF: Easy. □

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 $\bigcup\{A, B\}$. □

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

PROOF: By repeated application of the Pairing and Union axioms. □

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. □

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. □

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.
□

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

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 $\bigcap \mathbf{A} \subseteq A$. □

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

PROOF: Easy. □

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. □

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. □

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

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

PROOF: Easy. □

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

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

PROOF: Easy. □

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.
□

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

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

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

PROOF: Easy. □

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 $\mathcal{P}\mathcal{P}(A \cup B)$. □

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

PROOF: Easy. □

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 $\mathrm{dom}\,\mathbf{R} = \{x : \exists y.(x, y) \in \mathbf{R}\}$.

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

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

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

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

Definition 34 (Single-Rooted)**.** A class $\mathbf{R}$ is *single-rooted* iff, for all $y \in \mathrm{ran}\,\mathbf{R}$, 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 $\mathrm{dom}\,\mathbf{F}^{-1} = \mathrm{ran}\,\mathbf{F}$ and $\mathrm{ran}\,\mathbf{F}^{-1} = \mathrm{dom}\,\mathbf{F}$.*

PROOF: Easy. □

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

PROOF: Easy. □

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. □

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

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. □

Theorem 43.

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

Proof: Easy. □

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. □

Theorem 45.

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

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

Proof: Easy. □

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. □

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 $x \in \operatorname{dom} \mathbf{F}$, 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 $\mathbf{F} : \mathbf{A} \to \mathbf{B}$, iff $\mathbf{F}$ is a function, $\operatorname{dom} \mathbf{F} = \mathbf{A}$, and $\operatorname{ran} \mathbf{F} \subseteq \mathbf{B}$.

If, in addition, $\operatorname{ran} \mathbf{F} = \mathbf{B}$, 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. □

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

Proof: Easy. □

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

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

Proof: Easy. □

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

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

Proof: Easy. □

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* $x \in \operatorname{dom} \mathbf{F}$*,* $\mathbf{F}^{-1}(\mathbf{F}(x)) = x$*.*

Proof: Easy. □

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

Proof: Easy. □

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

Theorem 61. *Let* $F : A \to B$*. Assume* $A \neq \emptyset$*. Then* F *has a left inverse (i.e. there exists* $G : B \to A$ *such that* $G \circ F = \mathrm{id}_A$*) 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.

$\langle 2 \rangle 1$. Assume: F is one-to-one.
$\langle 2 \rangle 2$. $F^{-1} : \operatorname{ran} F \to A$
$\langle 2 \rangle 3$. Pick $a \in A$
$\langle 2 \rangle 4$. Define $G : B \to A$ by:

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

$\langle 2 \rangle 5$. $\forall x \in A . G(F(x)) = x$
$\langle 1 \rangle 2$. If F has a left inverse then F is one-to-one.
$\langle 2 \rangle 1$. Assume: F has a left inverse G.
$\langle 2 \rangle 2$. Let: $x, y \in A$ with $F(x) = F(y)$
$\langle 2 \rangle 3$. $x = y$
Proof: $x = G(F(x)) = G(F(y)) = y$.
$\square$

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 $\operatorname{dom} H = \operatorname{dom} R$.*

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

Proof:
$\langle 1 \rangle 1$. If F has a right inverse then F maps A onto B.
Proof: If $H : B \to A$ is a right inverse, then for any y in B, we have $y = F(H(y))$.
$\langle 1 \rangle 2$. If F maps A onto B then F has a right inverse.
$\langle 2 \rangle 1$. Assume: F maps A onto B.
$\langle 2 \rangle 2$. Pick a function H with $H \subseteq F^{-1}$ and $\operatorname{dom} H = \operatorname{dom} F^{-1}$
Proof: By the Axiom of Choice.
$\langle 2 \rangle 3$. $\operatorname{dom} H = B$
Proof: $\operatorname{dom} H = \operatorname{dom} F^{-1} = \operatorname{ran} F = B$ by $\langle 2 \rangle 1$.
$\langle 2 \rangle 4$. For all $y \in B$ we have $F(H(y)) = y$
$\langle 3 \rangle 1$. Let: $y \in B$
$\langle 3 \rangle 2$. $(y, H(y)) \in F^{-1}$
$\langle 3 \rangle 3$. $F(H(y)) = y$
$\square$

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 $A \to \mathbf{B}$.

9 Dependent Products

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

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

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

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* $\operatorname{fld}\mathbf{R}$*.*

PROOF:
$\langle 1 \rangle 1.$ LET: $x \in \operatorname{fld}\mathbf{R}$
$\langle 1 \rangle 2.$ 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 $x \in \operatorname{fld}\mathbf{R}$, the *equivalence class* of x modulo $\mathbf{R}$ is

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

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

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

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:
$\langle 1 \rangle 1$. Every equivalence class is nonempty.
PROOF: For any $x \in A$ we have $x \in [x]_R$.
$\langle 1 \rangle 2$. Any two distinct equivalence classes are disjoint.
$\langle 2 \rangle 1$. LET: $x, y \in A$
$\langle 2 \rangle 2$. ASSUME: $z \in [x]_R \cap [y]_R$
PROVE: $[x]_R = [y]_R$
$\langle 2 \rangle 3$. xRy
$\langle 3 \rangle 1$. xRz
$\langle 3 \rangle 2$. yRz
$\langle 3 \rangle 3$. zRy
PROOF: By $\langle 3 \rangle 2$ and symmetry.
$\langle 3 \rangle 4$. xRy
PROOF: By $\langle 3 \rangle 1$, $\langle 3 \rangle 3$ and transitivity.
$\langle 2 \rangle 4$. $[x]_R = [y]_R$
PROOF: By Lemma 3N.
$\langle 1 \rangle 3$. A is the union of all the equivalence classes.
PROOF: For any $x \in A$ we have $x \in [x]_R$.
$\square$

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* $\phi : A \to A/R$ is defined by $\phi(x) = [x]_R$.

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

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

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. □

12 Natural Numbers

Definition 78 (Successor)**.** The *successor* of a set a is the set $a^+ = a \cup \{a\}$.

Definition 79 (Inductive)**.** A class $\mathbf{A}$ is *inductive* iff $\emptyset \in \mathbf{A}$ and $\forall a \in \mathbf{A}.a^+ \in \mathbf{A}$.

Axiom 80 (Infinity)**.** *There exists an inductive set.*

Definition 81 (Natural Number)**.** A *natural number* is a set that belongs to every inductive set.

We write ω for the class of all natural numbers.

Theorem 82. *The class ω is a set.*

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

Theorem 83. *The set ω is inductive, and is a subset of every inductive set.*

PROOF: Easy. □

Corollary 83.1 (Proof by Induction)**.** *Any inductive subclass of ω is equal to ω.*

Theorem 84. *Every natural number except 0 is the successor of some natural number.*

PROOF: Easy proof by induction. □

Definition 85 (Peano System)**.** A *Peano system* is a triple $\langle N, S, e \rangle$ consisting of a set N, a function $S : N \to N$ and an element $e \in N$ such that:

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

Definition 86 (Transitive Set)**.** A set A is a *transitive set* iff every member of a member of A is a member of A.

Theorem 87. *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 $\bigcup a \subseteq a$. □

Theorem 88. *Every natural number is a transitive set.*

PROOF:
⟨1⟩1. 0 is a transitive set.
  PROOF: Vacuous.
⟨1⟩2. For any natural number n, if n is a transitive set then n^+ is a transitive set.
  ⟨2⟩1. LET: n be a natural number that is a transitive set.
  ⟨2⟩2. $\bigcup(n^+) \subseteq n^+$
    PROOF: Theorem 87.
□

Theorem 89. $\langle \omega, \sigma, 0 \rangle$ *is a Peano system, where* $0 = \emptyset$ *and* $\sigma = \{\langle n, n^+ \rangle : n \in \omega\}$.

PROOF:
⟨1⟩1. $0 \notin \operatorname{ran} \sigma$
  PROOF: For any $n \in \omega$ we have $0 \neq n^+$ since $n \in n^+$ and $n \notin 0$.
⟨1⟩2. σ is one-to-one.
  PROOF: If $m^+ = n^+$ then $m = \bigcup(m^+) = \bigcup(n^+) = n$ using Theorems 87 and 88.
⟨1⟩3. Any subset $A \subseteq \omega$ that contains 0 and is closed under σ equals ω.
□

Theorem 90. *The set* ω *is a transitive set.*

PROOF:
⟨1⟩1. For every natural number n we have $\forall m \in n.\ m$ is a natural number.
  ⟨2⟩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 91 (Recursion Theorem on ω)**.** *Let* A *be a set,* $a \in A$ *and* $F : A \to A$. *Then there exists a unique function* $h : \omega \to A$ *such that*

$$h(0) = a \ ,$$

and for every n *in* ω,

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

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

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

$\langle 1 \rangle 2$. LET: $\mathcal{K}$ be the set of acceptable functions.
$\langle 1 \rangle 3$. LET: $h = \bigcup \mathcal{K}$
$\langle 1 \rangle 4$. h is a function.
  $\langle 2 \rangle 1$. LET: $S = \{n \in \omega : \text{for at most one } y, (n, y) \in h\}$
  $\langle 2 \rangle 2$. S is inductive.
    $\langle 3 \rangle 1$. $0 \in S$
      $\langle 4 \rangle 1$. LET: $\langle 0, y_1 \rangle, \langle 0, y_2 \rangle \in h$
      $\langle 4 \rangle 2$. PICK acceptable v_1 and v_2 such that $v_1(0) = y_1$ and $v_2(0) = y_2$
      $\langle 4 \rangle 3$. $y_1 = a$
      $\langle 4 \rangle 4$. $y_2 = a$
      $\langle 4 \rangle 5$. $y_1 = y_2$
    $\langle 3 \rangle 2$. $\forall k \in S. k^+ \in S$
      $\langle 4 \rangle 1$. LET: $k \in S$
      $\langle 4 \rangle 2$. LET: $(k^+, y_1), (k^+, y_2) \in h$
      $\langle 4 \rangle 3$. PICK acceptable v_1, v_2 such that $v_1(k^+) = y_1$ and $v_2(k^+) = y_2$
      $\langle 4 \rangle 4$. $y_1 = F(v_1(k))$
      $\langle 4 \rangle 5$. $f_2 = F(v_2(k))$
      $\langle 4 \rangle 6$. $v_1(k) = v_2(k)$
        $\langle 5 \rangle 1$. $(k, v_1(k)), (k, v_2(k)) \in h$
        $\langle 5 \rangle 2$. Q.E.D.
          PROOF: By $\langle 4 \rangle 1$
      $\langle 4 \rangle 7$. $y_1 = y_2$
  $\langle 2 \rangle 3$. $S = \omega$
$\langle 1 \rangle 5$. h is acceptable.
  $\langle 2 \rangle 1$. If $0 \in \operatorname{dom} h$ then $h(0) = a$
    $\langle 3 \rangle 1$. ASSUME: $0 \in \operatorname{dom} h$
    $\langle 3 \rangle 2$. PICK v acceptable with $v(0) = h(0)$
    $\langle 3 \rangle 3$. $v(0) = a$
    $\langle 3 \rangle 4$. $h(0) = a$
  $\langle 2 \rangle 2$. For all $n \in \omega$, if $n^+ \in \operatorname{dom} h$ then $n \in \operatorname{dom} h$ and $h(n^+) = F(h(n))$
    $\langle 3 \rangle 1$. LET: $n \in \omega$ with $n^+ \in \operatorname{dom} h$
    $\langle 3 \rangle 2$. PICK v acceptable with $v(n^+) = h(n^+)$
    $\langle 3 \rangle 3$. $n \in \operatorname{dom} v$
    $\langle 3 \rangle 4$. $v(n) = h(n)$
    $\langle 3 \rangle 5$. $h(n^+) = F(h(n))$
      PROOF:

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

$\langle 1 \rangle 6$. $\operatorname{dom} h = \omega$
  $\langle 2 \rangle 1$. $0 \in \operatorname{dom} h$
    PROOF: Since $\{(0, a)\}$ is an acceptable function.
  $\langle 2 \rangle 2$. $\forall n \in \operatorname{dom} h. n^+ \in \operatorname{dom} h$
    $\langle 3 \rangle 1$. LET: $n \in \operatorname{dom} h$
    $\langle 3 \rangle 2$. PICK an acceptable v such that $n \in \operatorname{dom} v$

$\langle 3\rangle 3.$ ASSUME: w.l.o.g. $n^+ \notin \operatorname{dom} v$
$\langle 3\rangle 4.$ $v \cup \{(n^+, F(v(n)))\}$ is acceptable.
$\langle 1\rangle 7.$ For any acceptable function $h' : \omega \to A$ we have $h' = h$
$\langle 2\rangle 1.$ LET: $h' : \omega \to A$ be acceptable.
$\langle 2\rangle 2.$ $h'(0) = h(0)$
PROOF: $h'(0) = h(0) = a$
$\langle 2\rangle 3.$ $\forall n \in \omega . h'(n) = h(n) \Rightarrow h'(n^+) = h(n^+)$
PROOF: We have $h'(n^+) = F(h'(n)) = F(h(n)) = h(n^+)$.
$\square$

Theorem 92. *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 ω 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:
$\langle 1\rangle 1.$ There exists a function h that satisfies those two conditions.
PROOF: By the Recursion Theorem.
$\langle 1\rangle 2.$ For all $m, n \in \omega$, if $m \neq n$ then $h(m) \neq h(n)$
$\langle 2\rangle 1.$ For all $n \in \omega$, if $n \neq 0$ then $h(n) \neq h(0)$
$\langle 3\rangle 1.$ LET: $n \in \omega$
$\langle 3\rangle 2.$ ASSUME: $n \neq 0$
$\langle 3\rangle 3.$ PICK p such that $n = p^+$
$\langle 3\rangle 4.$ $h(n) \neq h(0)$
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.
$\square$

13 Arithmetic

Definition 93 (Addition)**.** *Addition* $+$ is the binary operation on ω such that, for all $m, n \in \omega$,

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

Theorem 94 (Associative Law for Addition)**.**

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

Proof:

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

If $m + (n + p) = (m + n) + p$ then

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

□

Theorem 95 (Commutative Law for Addition)**.**

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

Proof:

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

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

$\langle 2 \rangle 2$. 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 96 (Multiplication)**.** *Multiplication* $\cdot$ is the binary operation on ω such that, for all $m, n \in \omega$,

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

Theorem 97 (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:

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

□

Theorem 98 (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.

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

PROOF:

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

□

Theorem 99 (Commutative Law for Multiplication)**.**

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

PROOF:
⟨1⟩1. $\forall n \in \omega . 0n = n0$
⟨2⟩1. $0 \cdot 0 = 0 \cdot 0$
⟨2⟩2. For all $n \in \omega$, if $0n = n0$ then $0n^+ = n^+0$
PROOF:

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

⟨1⟩2. For all $m \in \omega$, if $\forall n \in \omega . mn = nm$ then $\forall n \in \omega . m^+n = nm^+$
⟨2⟩1. LET: $m \in \omega$
⟨2⟩2. ASSUME: $\forall n \in \omega . mn = nm$
⟨2⟩3. $m^+0 = 0m^+$
PROOF: By ⟨1⟩1.
⟨2⟩4. For all $n \in \omega$, if $m^+n = nm^+$ 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 100. *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 88).
$\square$

Lemma 101. *For any natural number n we have $n \notin n$.*

PROOF:
$\langle 1 \rangle 1.$ $0 \notin 0$
$\langle 1 \rangle 2.$ For all $n \in \omega$, if $n \notin n$ then $n^+ \notin n^+$
  $\langle 2 \rangle 1.$ LET: $n \in \omega$
  $\langle 2 \rangle 2.$ ASSUME: $n^+ \in n^+$
    PROVE: $n \in n$
  $\langle 2 \rangle 3.$ $n^+ \in n$ or $n^+ = n$
  $\langle 2 \rangle 4.$ $n \in n^+$
  $\langle 2 \rangle 5.$ $n \in n$
    PROOF: If $n^+ \in n$ this follows because n is transitive (Theorem 88).
$\square$

Theorem 102 (Trichotomy Law for ω)**.** *For any natural numbers m and n, exactly one of*

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

holds.

PROOF:

$\langle 1 \rangle 1$. 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 101.
If $m \in n$ and $n \in m$ then $m \in m$ by Theorem 88, contradicting Lemma 101.
$\langle 1 \rangle 2$. For any $m, n \in \omega$, at least one of $m \in n$, $m = n$, $n \in m$ holds.
$\langle 2 \rangle 1$. For all $n \in \omega$, either $0 \in n$ or $0 = n$
$\langle 3 \rangle 1$. $0 = 0$
$\langle 3 \rangle 2$. For all $n \in \omega$, if $0 \in n$ or $0 = n$ then $0 \in n^+$
$\langle 2 \rangle 2$. For all $m \in \omega$, if $\forall n \in \omega(m \in n \vee m = n \vee n \in m)$ then $\forall n \in \omega(m^+ \in n \vee m^+ = n \vee n \in m^+)$
$\langle 3 \rangle 1$. LET: $m \in \omega$
$\langle 3 \rangle 2$. ASSUME: $\forall n \in \omega(m \in n \vee m = n \vee n \in m)$
$\langle 3 \rangle 3$. LET: $n \in \omega$
$\langle 3 \rangle 4$. CASE: $m \in n$
PROOF: Then $m \in n^+$
$\langle 3 \rangle 5$. CASE: $m = n$
PROOF: Then $m \in n^+$
$\langle 3 \rangle 6$. CASE: $n \in m$
PROOF: Then $n^+ \in m^+$ by Lemma 100 so $n^+ \in m$ or $n^+ = m$.
□

Corollary 102.1. *For any natural numbers m and n,*

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

PROOF:
$\langle 1 \rangle 1$. LET: $m, n \in \omega$
$\langle 1 \rangle 2$. If $m \in n$ then $m \subset n$.
$\langle 2 \rangle 1$. ASSUME: $m \in n$
$\langle 2 \rangle 2$. $m \subseteq n$
PROOF: Theorem 88.
$\langle 2 \rangle 3$. $m \neq n$
PROOF: Lemma 101.
$\langle 1 \rangle 3$. If $m \subset n$ 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 103. *For any natural numbers m, n and p, we have $m \in n$ if and only if $m + p \in n + p$.*

PROOF:
$\langle 1 \rangle 1$. $\forall m, n, p \in \omega.(m \in n \Rightarrow m + p \in n + p)$
PROOF: Easy induction on p using Lemma 100.
$\langle 1 \rangle 2$. $\forall m, n, p \in \omega.(m + p \in n + p \Rightarrow m \in n)$
PROOF: If $m + p \in n + p$ then we have $m + p \neq n + p$ and $n + p \notin m + p$ by trichotomy, hence $m \neq n$ and $n \notin m$ by $\langle 1 \rangle 1$, hence $m \in n$ by trichotomy.
□

Corollary 103.1 (Cancellation Law)**.** *For any natural numbers m, n and p, if $m + p = n + p$ then $m = n$.*

Theorem 104. *For any natural numbers m, n and p, if $p \neq 0$ then we have $m \in n$ iff $mp \in np$.*

PROOF:
$\langle 1 \rangle 1.$ $\forall m, n, p \in \omega . m \in n \wedge p \neq 0 \Rightarrow mp \in np$
PROOF: Easy induction on p using Theorem 103.
$\langle 1 \rangle 2.$ $\forall m, n, p \in \omega . mp \in np \wedge p \neq 0 \Rightarrow m \in n$
PROOF: We have $mp \neq np$ and $np \notin mp$ by trichotomy, so $m \neq n$ and $n \notin m$ by $\langle 1 \rangle 1$, hence $m \in n$ by trichotomy.
$\square$

Corollary 104.1 (Cancellation Law)**.** *For any natural numbers m, n and p, if $mp = np$ and $p \neq 0$ then $m = n$.*