C1 Set Theory

Robin Adams

August 27, 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 (Replacement)**.** *For any property $P(x, y)$, the following is an axiom:*

Let A be a set. Assume that, for all $x \in A$, there is at most one y such that $P(x, y)$. Then $\{y : \exists x \in A.P(x, y)\}$ is a set.

Definition 6 (Power Set)**.** For any set A, the *power set* of A, $\mathcal{P}A$, is the class of all subsets of A.

Axiom 7 (Power Set)**.** *For any set A, the class $\mathcal{P}A$ is a set.*

Theorem 8 (Pairing)**.** *For any objects a and b, the class $\{a, b\}$ is a set, called a* pair set*.*

PROOF: Let a and b be sets. Let $P(x, y)$ be the formula $(x = \emptyset \;\&\; y = a)$ or $(x = \mathcal{P}\emptyset \;\&\; y = b)$. Then we have $(\forall x \in \mathcal{P}\mathcal{P}\emptyset)\forall y_1 \forall y_2 (P(x, y_1) \;\&\; P(x, y_2) \Rightarrow y_1 = y_2)$, hence there exists a set c such that

$$\forall y(y \in c \Leftrightarrow (\exists x \in \mathcal{P}\mathcal{P}\emptyset)P(x, y))$$

The members of c are just a and b. $\square$

Definition 9 (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 10. *If* $\mathbf{A} \subseteq \mathbf{B}$ *then* $\bigcup \mathbf{A} \subseteq \bigcup \mathbf{B}$.

PROOF: Easy. $\square$

Axiom 11 (Union)**.** *For any set A, the union $\bigcup A$ is a set.*

Proposition 12. *For any sets A and B, the class $A \cup B$ is a set.*

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

Proposition Schema 13. *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. $\square$

Theorem 14 (Subset Axioms, Aussonderung)**.** *For any class* $\mathbf{A}$ *and set B, if* $\mathbf{A} \subseteq B$ *then* $\mathbf{A}$ *is a set.*

PROOF: Let $Q(x, y)$ be the formula $x \in \mathbf{A} \wedge y = x$. Now we reason as follows. Let c be any set. Then we have

$$(\forall x \in B)\forall y_1 \forall y_2 (Q(x, y_1) \;\&\; Q(x, y_2) \Rightarrow y_1 = y_2)$$

Then, by a Replacement Axiom, there exists a set c such that

$$\forall y(y \in c \Leftrightarrow (\exists x \in B)Q(x, y)) \ .$$

This is equivalent to $\forall x(x \in c \Leftrightarrow x \in \mathbf{A})$. $\square$

Proposition 15. *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 16. *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 17. *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 18 (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 19. *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 20. *If $\mathbf{A} \subseteq \mathbf{B}$ then $\bigcap \mathbf{B} \subseteq \bigcap \mathbf{A}$.*

PROOF: Easy. $\square$

Proposition 21. *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 22. *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 23. *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 24. *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 25 (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 26. *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 27 (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 28. *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. $\square$

Corollary 28.1. *For any sets A and B, the Cartesian product $A\times B$ is a set.*

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

Lemma 29. *If $(x,y)\in\mathbf{A}$ then $x,y\in\bigcup\bigcup\mathbf{A}$.*

Proof: Easy. $\square$

4 Relations

Definition 30 (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 31 (Domain)**.** The *domain* of a class $\mathbf{R}$ is $\operatorname{dom}\mathbf{R}=\{x:\exists y.(x,y)\in\mathbf{R}\}$.

Definition 32 (Range)**.** The *range* of a class $\mathbf{R}$ is $\operatorname{ran}\mathbf{R}=\{y:\exists x.(x,y)\in\mathbf{R}\}$.

Definition 33 (Field)**.** The *field* of a class $\mathbf{R}$ is $\operatorname{fld}\mathbf{R}=\operatorname{dom}\mathbf{R}\cup\operatorname{ran}\mathbf{R}$.

Proposition 34. *If R is a set then $\operatorname{dom}R$, $\operatorname{ran}R$ and $\operatorname{fld}R$ are sets.*

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

Definition 35 (Single-Rooted)**.** A class $\mathbf{R}$ is *single-rooted* iff, for all $y \in \operatorname{ran}\mathbf{R}$, there is only one x such that $x\mathbf{R}y$.

Definition 36 (Inverse)**.** The *inverse* of a class $\mathbf{F}$ is the class $\mathbf{F}^{-1} = \{(y,x) \mid (x,y) \in \mathbf{F}\}$.

Theorem 37. *For any class* $\mathbf{F}$*, we have* $\operatorname{dom}\mathbf{F}^{-1} = \operatorname{ran}\mathbf{F}$ *and* $\operatorname{ran}\mathbf{F}^{-1} = \operatorname{dom}\mathbf{F}$*.*

PROOF: Easy. □

Theorem 38. *For a relation* $\mathbf{F}$*,* $(\mathbf{F}^{-1})^{-1} = \mathbf{F}$*.*

PROOF: Easy. □

Definition 39 (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 40. *For any classes* $\mathbf{F}$ *and* $\mathbf{G}$*,* $(\mathbf{F} \circ \mathbf{G})^{-1} = \mathbf{G}^{-1} \circ \mathbf{F}^{-1}$*.*

PROOF: Easy. □

Definition 41 (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 42 (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 43.

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

PROOF: Easy. □

Theorem 44.

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

PROOF: Easy. □

Theorem 45.

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

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

PROOF: Easy. □

Theorem 46.

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

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

PROOF: Easy. □

Theorem 47.

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

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

PROOF: Easy. □

Definition 48 (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 49 (Symmetric)**.** A binary relation $\mathbf{R}$ is *symmetric* iff, whenever $x\mathbf{R}y$, then $y\mathbf{R}x$.

Definition 50 (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 51. 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 52 (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 53 (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 54. *For a class* $\mathbf{F}$*,* $\mathbf{F}^{-1}$ *is a function if and only if* $\mathbf{F}$ *is single-rooted.*

PROOF: Easy. □

Theorem 55. *A relation* $\mathbf{F}$ *is a function if and only if* $\mathbf{F}^{-1}$ *is single-rooted.*

PROOF: Easy. □

Theorem 56. *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 57. *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,*

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

PROOF: Easy. □

Definition 58 (One-to-one)**.** A function $\mathbf{F}$ is *one-to-one* or an *injection* iff it is single-rooted.

Theorem 59. *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 60. *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 61 (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 62. *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:
⟨1⟩1. If F is one-to-one then F has a left inverse.
 ⟨2⟩1. ASSUME: F is one-to-one.
 ⟨2⟩2. $F^{-1} : \operatorname{ran} F \to A$
 ⟨2⟩3. PICK $a \in A$
 ⟨2⟩4. Define $G : B \to A$ by:

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

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

7 The Axiom of Choice

Axiom 64 (Choice)**.** *For any relation* R *there exists a function* $H \subseteq R$ *with* $\operatorname{dom} H = \operatorname{dom} R$*.*

Theorem 65. *Let $F : A \to B$. 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 $H : B \to A$ 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 $\operatorname{dom} H = \operatorname{dom} F^{-1}$
    Proof: By the Axiom of Choice.
  ⟨2⟩3. $\operatorname{dom} H = B$
    Proof: $\operatorname{dom} H = \operatorname{dom} F^{-1} = \operatorname{ran} F = B$ 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 66. 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 67. Let I be a set and H_i a set for all $i \in I$. Define

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

Theorem 68. *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 $\operatorname{dom} F = \operatorname{dom} R$
      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 $iRF(i)$.

$\langle 2\rangle 9$. $\operatorname{dom} F = \operatorname{dom} R$

$\square$

Theorem 69. *The following are equivalent.*

1. *The Axiom of Choice.*
2. *Let $\mathcal{A}$ be a set such that (a) every member of $\mathcal{A}$ is a nonempty set, and (b) any two distinct members of $\mathcal{A}$ are disjoint. Then there exists a set C such that, for all $B \in \mathcal{A}$, we have $C \cap B$ is a singleton.*
3. *For any set A, there exists a function $F : \mathcal{P}A - \{\emptyset\} \to A$ such that $F(X) \in X$ for all $X \in \mathcal{P}A - \{\emptyset\}$.*

PROOF:

$\langle 1\rangle 1$. $1 \Rightarrow 2$

PROOF: Let $\mathcal{A}$ be a set matching the two condtions. By the Multiplicative Axiom, pick a function $f \in \prod_{B \in \mathcal{A}} B$. Let $C = \operatorname{ran} f$. Then $C \cap B = \{f(B)\}$ for all $B \in \mathcal{A}$.

$\langle 1\rangle 2$. $2 \Rightarrow 3$

$\langle 2\rangle 1$. ASSUME: 2

$\langle 2\rangle 2$. LET: A be a set.

$\langle 2\rangle 3$. LET: $\mathcal{A} = \{\{B\} \times B : B \in \mathcal{P}A - \{\emptyset\}\}$

$\langle 2\rangle 4$. PICK a set C such that $C \cap (\{B\} \times B)$ is a singleton for all $B \in \mathcal{P}A - \{\emptyset\}$

$\langle 2\rangle 5$. LET: $F = C \cap \bigcup \mathcal{A}$

$\langle 2\rangle 6$. $F : \mathcal{P}A - \{\emptyset\} \to A$ is a function and $F(X) \in X$ for all X

$\langle 1\rangle 3$. $3 \Rightarrow 1$

$\langle 2\rangle 1$. ASSUME: 3

$\langle 2\rangle 2$. LET: R be a relation

$\langle 2\rangle 3$. PICK a choice function G for $\operatorname{ran} R$

⟨2⟩4. Define $F : \operatorname{dom} R \to \operatorname{ran} R$ by $F(x) = G(R(x))$
⟨2⟩5. $F \subseteq R$
□

10 Equivalence Relations

Definition 70 (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 71. *If* $\mathbf{R}$ *is a symmetric and transitive relation then* $\mathbf{R}$ *is an equivalence relation on* $\operatorname{fld} \mathbf{R}$.

Proof:
⟨1⟩1. Let: $x \in \operatorname{fld} \mathbf{R}$
⟨1⟩2. Pick y such that either $x\mathbf{R}y$ or $y\mathbf{R}x$
⟨1⟩3. $x\mathbf{R}y$ and $y\mathbf{R}x$
Proof: Since $\mathbf{R}$ is symmetric.
⟨1⟩4. $x\mathbf{R}x$
Proof: Since $\mathbf{R}$ is transitive.
□

Definition 72 (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

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

Lemma 73. *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:
⟨1⟩1. If $[x]_{\mathbf{R}} = [y]_{\mathbf{R}}$ then $x\mathbf{R}y$
⟨2⟩1. Assume: $[x]_{\mathbf{R}} = [y]_{\mathbf{R}}$
⟨2⟩2. $y \in [y]_{\mathbf{R}}$
Proof: Since $\mathbf{R}$ is reflexive on $\mathbf{A}$.
⟨2⟩3. $y \in [x]_{\mathbf{R}}$
⟨2⟩4. $x\mathbf{R}y$
⟨1⟩2. If $x\mathbf{R}y$ then $[x]_{\mathbf{R}} = [y]_{\mathbf{R}}$
⟨2⟩1. Assume: $x\mathbf{R}y$
⟨2⟩2. $[y]_{\mathbf{R}} \subseteq [x]_{\mathbf{R}}$
⟨3⟩1. Let: $z \in [y]_{\mathbf{R}}$
⟨3⟩2. $y\mathbf{R}z$
⟨3⟩3. $x\mathbf{R}z$
Proof: Since $\mathbf{R}$ is transitive.
⟨3⟩4. $z \in [x]_{\mathbf{R}}$
⟨2⟩3. $y\mathbf{R}x$
Proof: Since $\mathbf{R}$ is symmetric.

⟨2⟩4. $[x]_{\mathbf{R}} \subseteq [y]_{\mathbf{R}}$
PROOF: Similar.
□

Definition 74 (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 75. *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 76 (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 77. *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 $\{([x], F(x)) : x \in A\}$. □

11 Partial Orders

Definition 78 (Strict Partial Order)**.** A *strict partial order* is an irreflexive, transitive relation.

If $<$ is a strict partial order, we write $x \leq y$ for $x < y \lor x = y$.

Theorem 79. *Assume that $<$ is a partial order. Then for any x, y and z:*

1. At most *one of the three alternatives,*

$$x < y, x = y, y < x,$$

can hold.

2. $x \leq y \leq x \Rightarrow x = y$.

PROOF: Easy. □

Definition 80 (Minimal)**.** Let $<$ be a partial order on D. An element $m \in D$ is *minimal* iff there is no $x \in D$ such that $x < m$.

Definition 81 (Maximal)**.** Let $<$ be a partial order on D. An element $m \in D$ is *maximal* iff there is no $x \in D$ such that $m < x$.

Definition 82 (Least)**.** Let $<$ be a partial order on D. An element $m \in D$ is *least*, *smallest* or the *minimum* iff $\forall x \in D.m \leq x$.

Definition 83 (Greatest)**.** Let $<$ be a partial order on D. An element $m \in D$ is *greatest*, *largest* or the *maximum* iff $\forall x \in D.x \leq m$.

Proposition 84. *If R is a partial ordering on D then so is R^{-1}.*

PROOF: Easy. □

Definition 85 (Upper Bound)**.** Let $<$ be a partial order on A and $C \subseteq A$. An *upper bound* for C is an element $b \in A$ such that $\forall x \in C.x \leq b$.

Definition 86 (Least Upper Bound)**.** Let $<$ be a partial order on A and $C \subseteq A$. The *least upper bound* or *supremum* for C is the least element in the set of upper bounds for C.

Definition 87 (Lower Bound)**.** Let $<$ be a partial order on A and $C \subseteq A$. A *lower bound* for C is an element $b \in A$ such that $\forall x \in C.b \leq x$.

Definition 88 (Greatest Lower Bound)**.** Let $<$ be a partial order on A and $C \subseteq A$. The *greatest lower bound* or *infimum* for C is the greatest element in the set of lower bounds for C.

Definition 89 (Initial Segment)**.** Let $<$ be a partial order on A and $t \in A$. The *initial segment* up to t is

$$\operatorname{seg} t = \{x \in A : x < t\} \ .$$

12 Linear Orders

Definition 90 (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 91. *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. □

Definition 92 (Strictly Monotone Functions)**.** Let A and B be linearly ordered sets. A function $f : A \to B$ is *strictly monotone* iff, for all $x, y \in A$, if $x < y$ then $f(x) < f(y)$.

Theorem 93. *Let A and B be linearly ordered sets and $f : A \to B$ 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. □

Theorem 94. *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. □

13 Well Orderings

Definition 95 (Well Ordering)**.** A *well ordering* on a set A is a linear ordering on A such that every nonempty subset of A has a least element.

Theorem 96 (Transfinite Induction Principle)**.** *Let $<$ be a well ordering on A. Let $B \subseteq A$. Suppose that*

$$\forall x \in A(\operatorname{seg} x \subseteq B \Rightarrow x \in B) \enspace .$$

Then $B = A$.

PROOF:
$\langle 1 \rangle 1$. ASSUME: for a contradiction $B \neq A$

$\langle 1\rangle 2.$ Let: t be the least element of $A - B$
$\langle 1\rangle 3.$ $\operatorname{seg} t \subseteq B$
$\langle 1\rangle 4.$ $t \notin B$
$\langle 1\rangle 5.$ Q.E.D.
Proof: This is a contradiction.
$\square$

Theorem 97. *Assume that $<$ is a linear ordering on A. Assume that the only $<$-inductive subset of A is A itself. Then $<$ is a well ordering on A.*

Proof:
$\langle 1\rangle 1.$ Assume: for a contradiction $B \subseteq A$ has no least element.
$\langle 1\rangle 2.$ $A - B$ is $<$-inductive.
$\langle 2\rangle 1.$ Let: $t \in A$
$\langle 2\rangle 2.$ Assume: $\operatorname{seg} t \subseteq A - B$
$\langle 2\rangle 3.$ $t \notin B$
Proof: If it were, it would be the least element of B.
$\langle 2\rangle 4.$ $t \in A - B$
$\langle 1\rangle 3.$ $A - B = A$
$\langle 1\rangle 4.$ $B = \emptyset$
$\square$

Theorem 98 (Transfinite Recursion Theorem Schema)**.** *For any property $P(x, y)$ the following is a theorem:*

Assume that $<$ is a well ordering on A. Assume that $\forall x \exists! y P(x, y)$. Then there exists a unique function F with domain A such that

$$\forall t \in A . P(F \upharpoonright \operatorname{seg} t, F(t)) \ .$$

Proof:
$\langle 1\rangle 1.$ Given $t \in A$, let us say that a function v is *P-constructed up to t* iff $\operatorname{dom} v = \{x \in A : x \leq t\}$ and $\forall x \in \operatorname{dom} v . P(v \upharpoonright \operatorname{seg} x, v(x))$
$\langle 1\rangle 2.$ Let $t_1, t_2 \in A$ with $t_1 \leq t_2$. Let v_1 be a function that is P-constructed up to t_1, and v_2 a function that is P-constructed up to t_2. Then $\forall x \leq t_1 . v_1(x) = v_2(x)$
$\langle 2\rangle 1.$ Let: $x \leq t_1$
$\langle 2\rangle 2.$ Assume: $\forall y < x . v_1(y) = v_2(y)$
$\langle 2\rangle 3.$ $v_1 \upharpoonright \operatorname{seg} x = v_2 \upharpoonright \operatorname{seg} x$
$\langle 2\rangle 4.$ $P(v_1 \upharpoonright \operatorname{seg} x, v_1(x))$
$\langle 2\rangle 5.$ $P(v_2 \upharpoonright \operatorname{seg} x, v_2(x))$
$\langle 2\rangle 6.$ $v_1(x) = v_2(x)$
Proof: Since there is only one y such that $P(v_1 \upharpoonright \operatorname{seg} x, y)$.
$\langle 2\rangle 7.$ Q.E.D.
Proof: By transfinite induction.
$\langle 1\rangle 3.$ Let: $\mathcal{H} = \{v : \exists t \in A . v \text{ is } P\text{-constructed up to } t\}$
$\langle 1\rangle 4.$ $\mathcal{H}$ is a set.
Proof: By a Replacement Axiom since, if v_1 and v_2 are both P-constructed up to t then $v_1 = v_2$ by $\langle 1\rangle 2$.

$\langle 1 \rangle 5$. LET: $F = \bigcup \mathcal{H}$
$\langle 1 \rangle 6$. F is a function
$\langle 2 \rangle 1$. ASSUME: tFx and tFy
$\langle 2 \rangle 2$. PICK $v_1, v_2 \in \mathcal{H}$ such that $v_1(t) = x$ and $v_2(t) = y$
$\langle 2 \rangle 3$. PICK $t_1, t_2 \in A$ such that v_1 is P-constructed up to t_1 and v_2 is P-constructed up to t_2
$\langle 2 \rangle 4$. ASSUME: w.l.o.g. $t_1 \leq t_2$
$\langle 2 \rangle 5$. $v_1(t) = v_2(t)$
PROOF: By $\langle 1 \rangle 2$
$\langle 2 \rangle 6$. $x = y$
$\langle 1 \rangle 7$. $\forall x \in \operatorname{dom} F . P(F \upharpoonright \operatorname{seg} x, F(x))$
$\langle 2 \rangle 1$. LET: $x \in \operatorname{dom} F$
$\langle 2 \rangle 2$. PICK $v \in \mathcal{H}$ such that $x \in \operatorname{dom} v$
$\langle 2 \rangle 3$. $P(v \upharpoonright \operatorname{seg} x, v(x))$
$\langle 2 \rangle 4$. $v \upharpoonright \operatorname{seg} x = F \upharpoonright \operatorname{seg} x$
PROOF: $\forall y < x.(y, v(y)) \in \bigcup \mathcal{H} = F$
$\langle 2 \rangle 5$. $v(x) = F(x)$
PROOF: $(x, v(x)) \in \bigcup \mathcal{H} = F$
$\langle 1 \rangle 8$. $\operatorname{dom} F = A$
$\langle 2 \rangle 1$. LET: $x \in A$
$\langle 2 \rangle 2$. ASSUME: $\forall y < x . y \in \operatorname{dom} F$
$\langle 2 \rangle 3$. LET: z be the object such that $P(F \upharpoonright \operatorname{seg} x, z)$
$\langle 2 \rangle 4$. $F \upharpoonright \operatorname{seg} x \cup \{(x, z)\}$ is P-constructed up to x
$\langle 2 \rangle 5$. $x \in \operatorname{dom} F$
$\langle 2 \rangle 6$. Q.E.D.
PROOF: By transfinite induction, this proves $\forall x \in A . x \in \operatorname{dom} F$.
$\langle 1 \rangle 9$. F is unique.
$\langle 2 \rangle 1$. LET: G be a function with domain A such that $\forall x \in A . P(G \upharpoonright \operatorname{seg} x, G(x))$
PROVE: $\forall x \in A . F(x) = G(x)$
$\langle 2 \rangle 2$. LET: $x \in A$
$\langle 2 \rangle 3$. ASSUME: $\forall y < x . F(y) = G(y)$
$\langle 2 \rangle 4$. $F \upharpoonright \operatorname{seg} x = G \upharpoonright \operatorname{seg} x$
$\langle 2 \rangle 5$. $F(x) = G(x)$
$\langle 2 \rangle 6$. Q.E.D.
PROOF: This completes the proof by transfinite induction.
$\square$

14 Epsilon-Images

Lemma 99. *Let $<$ be a well ordering on A. Let E be the function on A defined by transfinite recursion thus:*

$$E(t) = \{E(x) : x < t\} \qquad (t \in A) \ .$$

Let $\alpha = \operatorname{ran} E$. Then:

1. $\forall t \in A . E(t) \notin E(t)$

2. E *is injective.*

3. $\forall s, t \in A.(s < t \Leftrightarrow E(s) \in E(t))$

4. α *is a transitive set.*

PROOF:
$\langle 1 \rangle 1$. $\forall t \in A.E(t) \notin E(t)$
  $\langle 2 \rangle 1$. LET: $t \in A$
  $\langle 2 \rangle 2$. ASSUME: $\forall s < t.E(s) \notin E(s)$
  $\langle 2 \rangle 3$. ASSUME: for a contradiction $E(t) \in E(t)$
  $\langle 2 \rangle 4$. PICK $x < t$ such that $E(t) = E(x)$
  $\langle 2 \rangle 5$. $E(x) \in E(x)$
  $\langle 2 \rangle 6$. Q.E.D.
    PROOF: This is a contradiction. The result follows by transfinite induction.
$\langle 1 \rangle 2$. E is injective.
  $\langle 2 \rangle 1$. ASSUME: for a contradiction $E(x) = E(y)$ where $x \neq y$
  $\langle 2 \rangle 2$. ASSUME: w.l.o.g. $x < y$
  $\langle 2 \rangle 3$. $E(x) \in E(y)$
  $\langle 2 \rangle 4$. Q.E.D.
    PROOF: This contradicts $\langle 1 \rangle 1$.
$\langle 1 \rangle 3$. $\forall s, t \in A(s < t \Leftrightarrow E(s) \in E(t))$
  $\langle 2 \rangle 1$. LET: $s, t \in A$
  $\langle 2 \rangle 2$. If $s < t$ then $E(s) \in E(t)$
    PROOF: Immediate from definition of E.
  $\langle 2 \rangle 3$. If $E(s) \in E(t)$ then $s < t$
    $\langle 3 \rangle 1$. ASSUME: $E(s) \in E(t)$
    $\langle 3 \rangle 2$. PICK $x < t$ such that $E(s) = E(x)$
    $\langle 3 \rangle 3$. $s = x$
      PROOF: $\langle 1 \rangle 2$.
    $\langle 3 \rangle 4$. $s < t$
$\langle 1 \rangle 4$. α is a transitive set.
  PROOF: From definition of E.

15 Natural Numbers

Definition 100 (Successor)**.** The *successor* of a set a is the set $a^+ = a \cup \{a\}$.

Definition 101 (Inductive)**.** A class $\mathbf{A}$ is *inductive* iff $\emptyset \in \mathbf{A}$ and $\forall a \in \mathbf{A}.a^+ \in \mathbf{A}$.

Axiom 102 (Infinity)**.** *There exists an inductive set.*

Definition 103 (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 104. *The class* ω *is a set.*

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

Theorem 105. *The set ω is inductive, and is a subset of every inductive set.*

PROOF: Easy. $\square$

Corollary 105.1 (Proof by Induction)**.** *Any inductive subclass of ω is equal to ω.*

Theorem 106. *Every natural number except 0 is the successor of some natural number.*

PROOF: Easy proof by induction. $\square$

Definition 107 (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 108 (Transitive Set)**.** A set A is a *transitive set* iff every member of a member of A is a member of A.

Theorem 109. *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 110. *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 109.
$\square$

Theorem 111. *$\langle \omega, \sigma, 0\rangle$ is a Peano system, where $0 = \emptyset$ and $\sigma = \{\langle n, n^+\rangle : n \in \omega\}$.*

PROOF:
$\langle 1\rangle 1.$ $0 \notin \operatorname{ran} \sigma$
PROOF: For any $n \in \omega$ we have $0 \neq n^+$ since $n \in n^+$ and $n \notin 0$.
$\langle 1\rangle 2.$ σ is one-to-one.
PROOF: If $m^+ = n^+$ then $m = \bigcup(m^+) = \bigcup(n^+) = n$ using Theorems 109 and 110.
$\langle 1\rangle 3.$ Any subset $A \subseteq \omega$ that contains 0 and is closed under σ equals ω.
$\square$

Theorem 112. *The set ω 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.
$\langle 2\rangle 2.$ 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.
$\square$

Theorem 113 (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:
$\langle 1\rangle 1.$ 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: $S = \{n \in \omega :$ 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 114. *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.
$\square$

16 Finite Sets

Definition 115 (Finite)**.** A set is *finite* iff it is equinumerous with a natural number. Otherwise it is infinite.

Theorem 116. *No natural number is equinumerous with a proper subset of itself.*

PROOF:
$\langle 1\rangle 1$. Any injective function $f : 0 \to 0$ has range 0.
PROOF: Since the only such function is $\emptyset$.
$\langle 1\rangle 2$. For any natural number n, if every injective function $f : n \to n$ has range n, then every injective function $f : n^+ \to n^+$ has range n^+.
$\langle 2\rangle 1$. LET: $n \in \omega$
$\langle 2\rangle 2$. ASSUME: Every injective function $f : n \to n$ has range n.

⟨2⟩3. LET: $f : n^+ \to n^+$ be injective.
⟨2⟩4. Define $g : n \to n$ by

$$g(k) = \begin{cases} f(k) & \text{if } f(k) \in n \\ f(n) & \text{if } f(k) = n \end{cases}$$

PROOF: If $k \in n$ and $f(k) = n$ then $f(n) \in n$ since f is injective.
⟨2⟩5. g is injective.
⟨3⟩1. LET: $i, j \in n$
⟨3⟩2. ASSUME: $g(i) = g(j)$
⟨3⟩3. CASE: $f(i) \in n$, $f(j) \in n$
PROOF: Then $f(i) = f(j)$ so $i = j$
⟨3⟩4. CASE: $f(i) \in n$, $f(j) \notin n$
PROOF: Then $f(i) = f(n)$ which is impossible as f is injective.
⟨3⟩5. CASE: $f(i) \notin n$, $f(j) \in n$
PROOF: Then $f(n) = f(j)$ which is impossible as f is injective.
⟨3⟩6. CASE: $f(i) \notin n$, $f(j) \notin n$
PROOF: Then $f(i) = f(j) = n$ so $i = j$.
⟨2⟩6. $\operatorname{ran} g = n$
PROOF: By ⟨2⟩2.
⟨2⟩7. $\operatorname{ran} f = n^+$
⟨3⟩1. $\forall k \in n . k \in \operatorname{ran} f$
PROOF: Since $\operatorname{ran} g \subseteq \operatorname{ran} f$.
⟨3⟩2. $n \in \operatorname{ran} f$
⟨4⟩1. CASE: $f(n) \in n$
⟨5⟩1. PICK k such that $g(k) = f(n)$
⟨5⟩2. $f(k) = n$
⟨4⟩2. CASE: $f(n) = n$
PROOF: Then $n \in \operatorname{ran} f$.
□

Corollary 116.1. *No finite set is equinumerous with a proper subset of itself.*

Corollary 116.2. *The set ω is infinite.*

PROOF: Since the function that maps n to $n + 1$ is a bijection between ω and the proper subset $\omega - \{0\}$. □

Corollary 116.3. *Every finite set is equinumerous with a unique natural number.*

Lemma 117. *Let n be a natural number and $C \subseteq n$. Then there exists $m \underline{\in} n$ such that $C \approx m$.*

PROOF:
⟨1⟩1. For all $C \subseteq 0$, there exists $m \underline{\in} 0$ such that $C \approx m$.
PROOF: In this case $C = \emptyset$ and so $C \approx 0$.
⟨1⟩2. Let $n \in \omega$. Assume that, for all $C \subseteq n$, there exists $m \underline{\in} n$ such that $C \approx m$. Let $C \subseteq n^+$. Then there exists $m \underline{\in} n^+$ such that $C \approx m$.

$\langle 2\rangle 1$. LET: $n \in \omega$
$\langle 2\rangle 2$. ASSUME: For all $C \subseteq n$, there exists $m \underline{\in} n$ such that $C \approx m$.
$\langle 2\rangle 3$. LET: $C \subseteq n^+$
$\langle 2\rangle 4$. CASE: $n \in C$
$\langle 3\rangle 1$. PICK $m \underline{\in} n$ such that $C - \{n\} \approx m$
$\langle 3\rangle 2$. $C \approx m^+$
$\langle 2\rangle 5$. CASE: $n \notin C$
PROOF: Then $C \subseteq n$ so $C \approx m$ for some $m \underline{\in} n$.
□

Corollary 117.1. *Any subset of a finite set is finite.*

17 Cardinal Numbers

Definition 118 (Cardinality)**.** TODO

Theorem 119. *For any sets A and B, $|A| = |B|$ if and only if $A \approx B$.*

PROOF: TODO □

Theorem 120. *For any finite set A, $|A|$ is the natural number such that $A \approx |A|$.*

PROOF: TODO □

Definition 121. We write $\aleph_0$ for $|\omega$.

18 Cardinal Arithmetic

Definition 122 (Addition)**.** Let κ and λ be any cardinal numbers. Then $\kappa+\lambda = |K \cup L|$, where K and L are any disjoint sets of cardinality κ and λ respectively.

To show this is well-defined, we must prove that, if $K_1 \approx K_2$, $L_1 \approx L_2$, and $K_1 \cap L_1 = K_2 \cap L_2 = \emptyset$, then $K_1 \cup L_1 \approx K_2 \cup L_2$.

PROOF: Easy.

Lemma 123. *For any cardinal number κ we have $\kappa + 0 = \kappa$.*

PROOF: Since for any set K we have $K \cup \emptyset = K$.

Lemma 124. *For any natural number n we have $n + \aleph_0 = \aleph_0$.*

PROOF: Easy. □

Lemma 125.

$$\aleph_0 + \aleph_0 = \aleph_0$$

PROOF: Define $f : (\omega \times \{0\}) \cup (\omega \times \{1\}) \to \omega$ by $f(n, 0) = 2n$ and $f(n, 1) = 2n+1$. Then f is a bijection. □

Theorem 126.

$$\kappa + \lambda = \lambda + \kappa$$

PROOF: Easy. □

Theorem 127.

$$\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$$

PROOF: Easy. □

Definition 128 (Multiplication)**.** Let κ and λ be any cardinal numbers. Then $\kappa\lambda = |K \times L|$, where K and L are any sets of cardinality κ and λ respectively.

It is easy to prove this well-defined.

Lemma 129. *For any cardinal number κ we have $\kappa 0 = 0$.*

PROOF: For any set K we have $K \times \emptyset = \emptyset$. □

Lemma 130. *For any natural number n we have $n\aleph_0 = \aleph_0$.*

PROOF: Induction on n using Lemma 125. □

Lemma 131.

$$\aleph_0\aleph_0 = \aleph_0$$

PROOF: Define $f : \omega \times \omega \to \omega$ by $f(m, n) = 2^m(2n + 1) - 1$. Then f is a bijection. □

Lemma 132.

$$\kappa 1 = \kappa$$

PROOF: Easy. □

Theorem 133.

$$\kappa\lambda = \lambda\kappa$$

PROOF: Easy. □

Theorem 134.

$$\kappa(\lambda\mu) = (\kappa\lambda)\mu$$

PROOF: Easy. □

Theorem 135.

$$\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu$$

PROOF: Easy. □

Definition 136 (Exponentiation)**.** Let κ and λ be any cardinal numbers. Then $\kappa^\lambda = |K^L|$, where K and L are any sets of cardinality κ and λ respectively.

It is easy to prove this well-defined.

Theorem 137. *For any cardinal κ, $\kappa^0 = 1$.*

PROOF: For any set K, there is only one function $\emptyset \to K$, namely $\emptyset$. $\square$

Theorem 138. *For any non-zero cardinal κ, we have $0^\kappa = 0$.*

PROOF: For any nonempty set K, there is no function $K \to \emptyset$. $\square$

Theorem 139. *For any set A, $|\mathcal{P}A| = 2^{|A|}$.*

PROOF: Define the bijection $f : \mathcal{P}A \to 2^A$ by $f(S)(a) = 1$ if $a \in S$, 0 if $a \notin S$. $\square$

Corollary 139.1. *For any cardinal κ, we have $\kappa \neq 2^\kappa$.*

Theorem 140.

$$\kappa^{\lambda+\mu} = \kappa^\lambda \kappa^\mu$$

PROOF: Easy. $\square$

Theorem 141.

$$(\kappa\lambda)^\mu = \kappa^\mu \lambda^\mu$$

PROOF: Easy. $\square$

Theorem 142.

$$(\kappa^\lambda)^\mu = \kappa^{\lambda\mu}$$

PROOF: Easy. $\square$

19 Arithmetic

Lemma 143. *For any natural numbers m and n, we have $m + n^+ = (m + n)^+$.*

PROOF: Easy. $\square$

Corollary 143.1. *The union of two finite sets is finite.*

Lemma 144. *For any natural numbers m and n we have $mn^+ = mn + m$.*

PROOF: Easy. $\square$

Corollary 144.1. *The Cartesian product of two finite sets is finite.*

Lemma 145. *For any natural numbers m and n we have $m^{n^+} = m^n m$.*

PROOF: Easy. $\square$

Corollary 145.1. *If A and B are finite sets then A^B is finite.*

20 Ordering on the Natural Numbers

Lemma 146. *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 110).
□

Lemma 147. *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 110).
□

Theorem 148 (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 147.
If $m \in n$ and $n \in m$ then $m \in m$ by Theorem 110, contradicting Lemma 147.
$\langle 1\rangle 2$. 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 146 so $n^+ \in m$ or $n^+ = m$.
□

Corollary 148.1. *The relation $\in$ is a linear ordering on ω.*

Corollary 148.2. *For any natural numbers m and n,*

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

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 110.
$\langle 2\rangle 3$. $m \neq n$
PROOF: Lemma 147.
$\langle 1\rangle 3$. 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 149. *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 146. □

Theorem 150. *For any non-zero natural number p, the function that maps n to np is strictly monotone.*

PROOF: Easy induction on p using Theorem 149. □

Theorem 151 (Strong Induction)**.** *Let A be a subset of ω 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. $\square$

Theorem 152 (Well-Ordering of ω)**.** *The ordering $<$ on ω is a well-ordering.*

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

Theorem 153 (Choice)**.** *Let $<$ be a linear ordering on A. Then $<$ is a well-ordering on A iff there does not exist any function $f : \omega \to \omega$ such that $f(n+1) < f(n)$ for all $n \in \omega$.*

PROOF:
⟨1⟩1. If $<$ is a well-ordering on A then there does not exist any function $f : \omega \to \omega$ such that $f(n+1) < f(n)$ for all $n \in \omega$.
 PROOF: If there is such a function f then $\operatorname{ran} f$ is a nonempty subset of A with no least element.
⟨1⟩2. If there does not exist any function $f : \omega \to A$ such that $f(n+1) < f(n)$ for all $n \in \omega$ then $<$ is a well-ordering on A.
 ⟨2⟩1. LET: $X \subseteq A$ be a nonempty subset of A with no least element.
  PROVE: There exists a function $f : \omega \to A$ such that $f(n+1) < f(n)$ for all $n \in \omega$
 ⟨2⟩2. PICK $a_0 \in X$
 ⟨2⟩3. $\forall x \in X . \exists y \in X . y < x$
 ⟨2⟩4. PICK a function $g : X \to X$ such that $\forall x \in X . g(x) < x$
  PROOF: By the Axiom of Choice.
 ⟨2⟩5. Define $f : \omega \to A$ recursively by:

$$f(0) = a_0$$
$$f(n^+) = g(f(n))$$

 ⟨2⟩6. $\forall n \in \omega . f(n^+) < f(n)$

$\square$

Lemma 154. *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:
⟨1⟩1. For all m, p, we have $m \in m + p^+$
 PROOF: $m = m + 0 \in m + p^+$
⟨1⟩2. For all m, n, if $m \in n$ then there exists p such that $n = m + p^+$
 ⟨2⟩1. For all m, if $m \in 0$ then there exists p such that $0 = m + p^+$
  PROOF: Vacuous.
 ⟨2⟩2. For all $n \in \omega$, if $\forall m \in n . \exists p \in \omega . n = m + p^+$ then $\forall m \in n^+ . \exists p \in \omega . n^+ = m + p^+$

⟨3⟩1. 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 155. *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 154.
⟨1⟩2. $mp + nq = mq + np + (a^+ + b)^+$
⟨1⟩3. $mp + nq \in mq + np$
Proof: Lemma 154.

21 The Integers

Theorem 156. *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 ω^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 ω.
□

Definition 157. The set $\mathbb{Z}$ of *integers* is the quotient set $(\omega \times \omega)/\sim$.

Lemma 158. *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 159 (Addition)**.** Addition $+$ on $\mathbb{Z}$ is the binary operation such that

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

Theorem 160. *Addition on $\mathbb{Z}$ is commutative.*

PROOF: From the definition. □

Theorem 161. *Addition on $\mathbb{Z}$ is associtative.*

PROOF: Easy. □

Definition 162 (Zero)**.** The zero in the integers is $0 = [(0, 0)]$.

Theorem 163. *For any integer a we have $a + 0 = 0$.*

PROOF: Easy. □

Theorem 164. *For any integer a, there exists an integer b such that $a + b = 0$.*

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

Lemma 165. *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:
⟨1⟩1. ASSUME: $m + n' = m' + n$ and $p + q' = p' + q$
⟨1⟩2. $mp + n'p = m'p + np$
⟨1⟩3. $m'q + nq = mq + n'q$
⟨1⟩4. $mp + mq' = mp' + mq$
⟨1⟩5. $n'p' + n'q = n'p + n'q'$
⟨1⟩6. $mp + n'p + m'q + nq + mp + mq' + n'p' + n'q = m'p + np + mq + n'q + mp' + mq + n'p + n'q'$
⟨1⟩7. $mp + nq + m'q' + n'p' = mq + np + m'p' + n'q'$
□

Definition 166 (Multiplication)**.** *Multiplication* $\cdot$ is the binary operation on $\mathbb{Z}$ such that

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

Theorem 167. *Multiplication is commutative.*

PROOF: Easy. □

Theorem 168. *Multiplication is associative.*

PROOF: Easy. □

Theorem 169. *Multiplication is distributive over addition.*

PROOF: Easy. □

Definition 170. The integer one is $1 = [(1, 0)]$.

Theorem 171. *For any integer a we have $a1 = a$.*

PROOF: Easy. □

Theorem 172. $0 \neq 1$

Proof: Easy. $\square$

Lemma 173. *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:

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

Definition 174 (Ordering)**.** The ordering $<$ on $\mathbb{Z}$ is defined by: $[(m, n)] < [(p, q)]$ iff $m + q \in n + p$.

Theorem 175. *The relation $<$ is a linear ordering on $\mathbb{Z}$.*

Proof:
⟨1⟩1. $<$ is transitive.
  ⟨2⟩1. Assume: $[(m, n)] < [(p, q)]$ and $[(p, q)] < [(r, s)]$
  ⟨2⟩2. $m + q \in n + p$ and $p + s \in q + r$
  ⟨2⟩3. $m + q + s \in n + p + s$
  ⟨2⟩4. $n + p + s \in n + q + r$
  ⟨2⟩5. $m + q + s \in n + q + r$
  ⟨2⟩6. $m + s \in n + r$
⟨1⟩2. $<$ satisfies trichotomy.
  Proof: From trichotomy on ω.
$\square$

Theorem 176. *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 ω.

Corollary 176.1. *If $a + c = b + c$ then $a = b$.*

Theorem 177. *If $0 < c$, then the function that maps an integer a to ac is strictly monotone.*

Proof:
⟨1⟩1. Let: a, b and c be integers.
⟨1⟩2. Assume: $0 < c$ and $a < b$
⟨1⟩3. Let: $a = [(m, n)]$
⟨1⟩4. Let: $b = [(p, q)]$
⟨1⟩5. Let: $c = [(r, s)]$
⟨1⟩6. $s \in r$
⟨1⟩7. $m + q \in p + n$
⟨1⟩8. $(m + q)r + (p + n)s \in (m + q)s + (p + n)r$
  Proof: Lemma 155.
⟨1⟩9. $ac < bc$

□

Lemma 178. *For integers a and b, $a(-b) = -(ab)$*

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

Theorem 179. *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 180. *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 181. *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 182 (Positive)**.** An integer a is *positive* iff $0 < a$.

Theorem 183. *Define $E : \omega \to \mathbb{Z}$ by $E(n) = [(n, 0)]$. Then E maps ω 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. □

22 Equinumerosity

Definition 184 (Equinumerous)**.** Two sets A and B are *equinumerous*, $A \approx B$, iff there exists a bijection between them.

Theorem 185. *Equinumerosity is an equivalence relation on the class of sets.*

PROOF: Easy. □

Theorem 186 (Cantor 1873)**.** *No set is equinumerous with its power set.*

PROOF:
$\langle 1 \rangle 1$. LET: $g : A \to \mathcal{P}A$
    PROVE: g is not surjective.
$\langle 1 \rangle 2$. LET: $B = \{x \in A : x \notin g(x)\}$
$\langle 1 \rangle 3$. $\forall x \in A . g(x) \neq B$
  PROOF: Because $x \in B$ iff $x \notin g(x)$.
□

23 Ordering Cardinal Numbers

Definition 187 (Dominated)**.** A set A is *dominated* by a set B, $A \preccurlyeq B$, iff there exists an injection $f : A \to B$.

Lemma 188. *Domination is a preorder on the class of sets.*

PROOF: Easy. $\square$

Lemma 189. *If $A \subseteq B$ then $A \preccurlyeq B$.*

PROOF: The inclusion from A to B is an injection. $\square$

Lemma 190. *If $A \preccurlyeq B$, $A \approx A'$ and $B \approx B'$ then $A' \preccurlyeq B'$.*

PROOF: Easy. $\square$

Definition 191. Given cardinal numbers κ and λ, we write $\kappa \leq \lambda$ iff $K \preccurlyeq L$, where K is any set of cardinality κ and L is any set of cardinality λ.

We write $\kappa < \lambda$ iff $\kappa \leq \lambda$ and $\kappa \neq \lambda$.

Theorem 192 (Schröder-Bernstein)**.** *If $A \preccurlyeq B$ and $B \preccurlyeq A$ then $A \approx B$.*

PROOF:
⟨1⟩1. LET: $f : A \to B$ and $g : B \to A$ be one-to-one.
⟨1⟩2. Define the sequence of sets $C_n \subseteq A$ by:

$$C_0 = A - \operatorname{ran} g$$
$$C_{n+1} = g(f(C_n))$$

⟨1⟩3. Define $h : A \to B$ by

$$h(x) = \begin{cases} f(x) & \text{if } \exists n \in \mathbb{N}. x \in C_n \\ g^{-1}(x) & \text{otherwise} \end{cases}$$

⟨1⟩4. h is injective.
 ⟨2⟩1. LET: $x, y \in A$
 ⟨2⟩2. ASSUME: $h(x) = h(y)$
 ⟨2⟩3. CASE: $x \in C_m$, $y \in C_n$
  PROOF: We have $f(x) = f(y)$ so $x = y$
 ⟨2⟩4. CASE: $x \in C_m$, $y \notin \bigcup_n C_n$
  PROOF: This case is impossible because we would have $y = g(f(x))$ and so $y \in C_{m+1}$.
 ⟨2⟩5. CASE: $x, y \notin \bigcup_n C_n$
  PROOF: We have $g^{-1}(x) = g^{-1}(y)$ so $x = y$.
⟨1⟩5. h is surjective.
 ⟨2⟩1. LET: $y \in B$
 ⟨2⟩2. ASSUME: $y \notin f(C_n)$ for all n
 ⟨2⟩3. $g(y) \notin C_n$ for all n
 ⟨2⟩4. $y = h(g(y))$
$\square$

Corollary 192.1. *The relation $\leq$ is a partial order on the class of cardinal numbers.*

Theorem 193. *Let κ, λ and μ be cardinal numbers.*

1. $\kappa \leq \lambda \Rightarrow \kappa + \mu \leq \lambda + \mu$
2. $\kappa \leq \lambda \Rightarrow \kappa\mu \leq \lambda\mu$
3. $\kappa \leq \lambda \Rightarrow \kappa^\mu \leq \lambda^\mu$
4. $\kappa \leq \lambda \Rightarrow \mu^\kappa \leq \mu^\lambda$ *if κ and μ are not both zero.*

Proof: Parts 1–3 are easy. For part 4:
Let $|K| = \kappa$, $|L| = \lambda$ and $|M| = \mu$ with $K \subseteq L$.
If $M = \emptyset$ then $\kappa \neq 0$ so $\mu^\kappa = 0 \leq \mu^\lambda$.
Otherwise, pick $a \in M$. Define $\Phi : M^K \to M^L$ by:

$$\Phi(f)(x) = \begin{cases} f(x) & \text{if } x \in K \\ a & \text{if } x \notin K \end{cases}$$

Then Φ is an injection. $\square$

Theorem 194 (Zorn's Lemma)**.** *The Axiom of Choice is equivalent to this statement:*

Let $\mathcal{A}$ be a set such that, for every chain $\mathcal{B} \subseteq \mathcal{A}$, we have $\bigcup \mathcal{B} \in \mathcal{A}$. Then $\mathcal{A}$ has a maximal element.

Proof:
$\langle 1 \rangle$1. If the Axiom of Choice then Zorn's Lemma.
  Proof: TODO
$\langle 1 \rangle$2. If Zorn's Lemma then the Axiom of Choice.
  $\langle 2 \rangle$1. Assume: Zorn's Lemma
  $\langle 2 \rangle$2. Let: R be a relation.
  $\langle 2 \rangle$3. Let: $\mathcal{A}$ be the set of all functions that are subsets of R.
  $\langle 2 \rangle$4. For any chain $\mathcal{B} \subseteq \mathcal{A}$ we have $\bigcup \mathcal{B} \in \mathcal{A}$
  $\langle 2 \rangle$5. Pick $F \in \mathcal{A}$ maximal.
  $\langle 2 \rangle$6. $\operatorname{dom} F = \operatorname{dom} R$

$\square$

Theorem 195 (Cardinal Comparability)**.** *The Axiom of Choice is equivalent to the statement: for any sets C and D, either $C \preccurlyeq D$ or $D \preccurlyeq C$.*

Proof:
$\langle 1 \rangle$1. If Zorn's Lemma then Cardinal Comparability.
  $\langle 2 \rangle$1. Assume: Zorn's Lemma
  $\langle 2 \rangle$2. Let: C and D be sets.
  $\langle 2 \rangle$3. Let: $\mathcal{A}$ be the set of all injective functions f with $\operatorname{dom} f \subseteq C$ and $\operatorname{ran} f \subseteq D$
  $\langle 2 \rangle$4. For every chain $\mathcal{B} \subseteq \mathcal{A}$ we have $\bigcup \mathcal{B} \in \mathcal{A}$
  $\langle 2 \rangle$5. Let: $f \in \mathcal{A}$ be maximal
  $\langle 2 \rangle$6. $\operatorname{dom} f = C$ or $\operatorname{ran} f = D$
  $\langle 2 \rangle$7. f is an injective function $C \to D$ or f^{-1} is an injective function $D \to C$

⟨1⟩2. If Cardinal Comparability then the Axiom of Choice.
PROOF: TODO
□

Theorem 196 (Choice)**.** *For any infinite set A, we have $\omega \preccurlyeq A$.*

PROOF:
⟨1⟩1. LET: A be an infinite set.
⟨1⟩2. PICK a choice function F for A
⟨1⟩3. Define $f : \omega \to A$ by recursion by: $f(n) = F(A - \{f(0), f(1), \ldots, f(n-1)\})$
PROOF: $A - \{f(0), f(1), \ldots, f(n-1)\}$ is nonempty because A is infinite.
⟨1⟩4. f is injective.
□

Corollary 196.1 (Choice)**.** *For any infinite cardinal κ we have $\aleph_0 \leq \kappa$.*

Corollary 196.2 (Choice)**.** *A set is infinite iff it is equinumerous to a proper subset of itself.*

Proposition 197 (Choice)**.** *If there exists a surjection $A \to B$ then $B \preccurlyeq A$.*

PROOF: Any surjection $A \to B$ has a right inverse which is an injection $B \to A$.

24 Countable Sets

Definition 198 (Countable)**.** A set is *countable* iff it is dominated by ω.

Proposition 199. *Any subset of a countable set is countable.*

PROOF: Easy. □

The union of two countable sets is countable.

PROOF: Because $\aleph_0 + \aleph_0 = \aleph_0$ □

Proposition 200. *The product of two countable sets is countable.*

PROOF: Because $\aleph_0 \aleph_0 = \aleph_0$. □

Proposition 201 (Choice)**.** *For any infinite set A, the set $\mathcal{P}A$ is uncountable.*

PROOF: If $|A| \geq \aleph_0$ then $|\mathcal{P}A| \geq 2^{\aleph_0}$. □

Theorem 202 (Choice)**.** *A countable union of countable sets is countable.*

PROOF:
⟨1⟩1. LET: $\mathcal{A}$ be a countable set of countable sets.
⟨1⟩2. ASSUME: w.l.o.g. $\mathcal{A} \neq \emptyset$ and $\emptyset \notin \mathcal{A}$
⟨1⟩3. PICK a surjection $G : \omega \to A$
⟨1⟩4. PICK a function F with domain ω such that, for all m, $F(m)$ is a surjection $\omega \to G(m)$
PROOF: By the Axiom of Choice.
⟨1⟩5. Define $f : \omega \times \omega \to \bigcup A$ by $f(m, n) = F(m)(n)$
⟨1⟩6. f is surjective.
⟨1⟩7. $A \preccurlyeq \omega \times \omega$
□

25 Arithmetic of Infinite Cardinals

Lemma 203 (Choice). *For any infinite cardinal κ we have $\kappa \cdot \kappa = \kappa$.*

PROOF:
$\langle 1 \rangle 1$. LET: κ be an infinite cardinal.
$\langle 1 \rangle 2$. LET: B be a set of cardinality κ.
$\langle 1 \rangle 3$. LET: $\mathcal{H} = \{f : f = \emptyset$ or for some infinite $A \subseteq B, f$ is a bijection between $A \times A$ and $A\}$
$\langle 1 \rangle 4$. For any chain $\mathcal{C} \subseteq \mathcal{H}$, we have $\bigcup \mathcal{C} \in \mathcal{H}$
  $\langle 2 \rangle 1$. LET: $\mathcal{C} \subseteq \mathcal{H}$ be a chain.
  $\langle 2 \rangle 2$. ASSUME: w.l.o.g. $\mathcal{C}$ has a nonempty element.
    PROOF: Otherwise $\bigcup \mathcal{C} = \emptyset \in \mathcal{H}$.
  $\langle 2 \rangle 3$. $\bigcup \mathcal{C}$ is an injective function.
  $\langle 2 \rangle 4$. LET: $A = \operatorname{ran} \bigcup \mathcal{C}$
  $\langle 2 \rangle 5$. A is infinite.
  $\langle 2 \rangle 6$. $\bigcup \mathcal{C}$ is a bijection between $A \times A$ and A.
    $\langle 3 \rangle 1$. LET: $a_1, a_2 \in A$
    $\langle 3 \rangle 2$. PICK $f_1, f_2 \in \mathcal{C}$ such that $a_1 \in \operatorname{ran} f_1$ and $a_2 \in \operatorname{ran} f_2$
    $\langle 3 \rangle 3$. ASSUME: w.l.o.g. $f_1 \subseteq f_2$
    $\langle 3 \rangle 4$. $\langle a_1, a_2 \rangle \in \operatorname{dom} f_2$
    $\langle 3 \rangle 5$. $\langle a_1, a_2 \rangle \in \operatorname{dom} \bigcup \mathcal{C}$
$\langle 1 \rangle 5$. PICK a maximal $f_0 \in \mathcal{H}$
  PROOF: Zorn's Lemma.
$\langle 1 \rangle 6$. $f_0 \neq \emptyset$
  PROOF: B has a countable subset A, say, and $A \times A \approx A$.
$\langle 1 \rangle 7$. PICK $A_0 \subseteq B$ infinite such that f_0 is a bijection between $A_0 \times A_0$ and A_0.
$\langle 1 \rangle 8$. LET: $\lambda = |A_0|$
$\langle 1 \rangle 9$. λ is infinite
$\langle 1 \rangle 10$. $\lambda = \lambda \cdot \lambda$
$\langle 1 \rangle 11$. $\lambda = \kappa$
  $\langle 2 \rangle 1$. $|B - A_0| < \lambda$
    $\langle 3 \rangle 1$. ASSUME: for a contradiction $\lambda \leq |B - A_0|$
    $\langle 3 \rangle 2$. PICK $D \subseteq B - A_0$ with $|D| = \lambda$
    $\langle 3 \rangle 3$. $(A_0 \cup D) \times (A_0 \cup D) = (A_0 \times A_0) \cup (A_0 \times D) \cup (D \times A_0) \cup (D \times D)$
    $\langle 3 \rangle 4$. $f_0 : A_0 \times A_0 \approx A_0$
    $\langle 3 \rangle 5$. $|(A_0 \times D) \cup (D \times A_0) \cup (D \times D)| = \lambda$
      PROOF:

$$\begin{aligned} |(A_0 \times D) \cup (D \times A_0) \cup (D \times D)| &= \lambda \cdot \lambda + \lambda \cdot \lambda + \lambda \cdot \lambda \\ &= \lambda + \lambda + \lambda && (\langle 1 \rangle 10) \\ &= 3 \cdot \lambda \\ &\leq \lambda \cdot \lambda \\ &= \lambda && (\langle 1 \rangle 10) \end{aligned}$$

    $\langle 3 \rangle 6$. PICK a bijection $g : (A_0 \times D) \cup (D \times A_0) \cup (D \times D) \approx D$
    $\langle 3 \rangle 7$. $f_0 \cup g : (A_0 \cup D) \times (A_0 \cup D) \approx A_0 \cup D$
    $\langle 3 \rangle 8$. Q.E.D.

PROOF: This contradicts the maximality of f_0.
⟨2⟩2. $\lambda = \kappa$
PROOF:

$$\begin{aligned}
\kappa &= |B| \\
&= |A_0| + |B - A_0| \\
&\leq \lambda + \lambda \\
&= 2 \cdot \lambda \\
&\leq \lambda \cdot \lambda \\
&= \lambda \\
&\leq \kappa
\end{aligned}$$

□

Corollary 203.1 (Absorption Law of Cardinal Arithmetic (Choice))**.** *Let κ and λ be cardinal numbers, the larger of which is infinite and the smaller of which is nonzero. Then*

$$\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda) \ .$$

PROOF:
⟨1⟩1. ASSUME: w.l.o.g. $\kappa \leq \lambda$
⟨1⟩2. $\kappa + \lambda = \lambda$
PROOF:

$$\begin{aligned}
\lambda &\leq \kappa + \lambda \\
&\leq \lambda + \lambda \\
&= 2 \cdot \lambda \\
&\leq \lambda \cdot \lambda \\
&= \lambda
\end{aligned}$$

⟨1⟩3. $\kappa \cdot \lambda = \lambda$
PROOF:

$$\begin{aligned}
\lambda &= 1 \cdot \lambda \\
&\leq \kappa \cdot \lambda \\
&\leq \lambda \cdot \lambda \\
&= \lambda
\end{aligned}$$

□