

C1 Set Theory

Robin Adams

August 28, 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 $\bigcup_{P[x_1, \dots, x_n]} t[x_1, \dots, x_n]$ for $\bigcup \{t[x_1, \dots, x_n] : P[x_1, \dots, x_n]\}$.

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, \dots, a_n , the class $\{a_1, \dots, a_n\}$ 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 $R \notin R$

⟨1⟩5. Q.E.D.

PROOF: This is a contradiction.

□

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

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 $\bigcap \mathbf{A} \subseteq A$. □

Proposition 20. *If $\mathbf{A} \subseteq \mathbf{B}$ then $\bigcap \mathbf{B} \subseteq \bigcap \mathbf{A}$.*

PROOF: Easy. □

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. □

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. □

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. □

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. □

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.

□

Definition 27 (Cartesian Product). The *Cartesian product* of classes **A** and **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 $(x, y) \in \mathcal{PP}C$.

PROOF: Easy. □

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 $\mathcal{PP}(A \cup B)$. □

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

PROOF: Easy. □

4 Relations

Definition 30 (Relation). A *relation* is a class of ordered pairs. It is *small* iff it is a set.

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

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

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

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

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

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

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

Definition 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 $\text{dom } \mathbf{F}^{-1} = \text{ran } \mathbf{F}$ and $\text{ran } \mathbf{F}^{-1} = \text{dom } \mathbf{F}$.

PROOF: Easy. \square

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

PROOF: Easy. \square

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. \square

Definition 41 (Restriction). The *restriction* of the class \mathbf{F} to the class \mathbf{A} is the class $\mathbf{F} \upharpoonright \mathbf{A} = \{(x, y) : x \in \mathbf{A} \wedge (x, y) \in \mathbf{F}\}$.

Definition 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. \square

Theorem 44.

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

PROOF: Easy. \square

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. \square

Theorem 46.

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

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

PROOF: Easy. \square

Theorem 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. \square

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 $x \in \text{dom } \mathbf{F}$, there is only one y such that $x\mathbf{F}y$. We call this unique y the *value* of \mathbf{F} at x and denote it by $\mathbf{F}(x)$.

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

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

Theorem 54. For a class \mathbf{F} , \mathbf{F}^{-1} is a function if and only if \mathbf{F} is single-rooted.

PROOF: Easy. \square

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

PROOF: Easy. \square

Theorem 56. For any function \mathbf{G} and classes \mathbf{A} and \mathbf{B} ,

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

PROOF: Easy. \square

Theorem 57. Assume that \mathbf{F} and \mathbf{G} are functions. Then $\mathbf{F} \circ \mathbf{G}$ is a function, its domain is $\{x \in \text{dom } \mathbf{G} : \mathbf{G}(x) \in \text{dom } \mathbf{F}\}$, and for x in its domain,

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

PROOF: Easy. \square

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

PROOF: Easy. \square

Theorem 60. Let \mathbf{F} be a one-to-one function. For $y \in \text{ran } \mathbf{F}$, $\mathbf{F}(\mathbf{F}^{-1}(y)) = y$.

PROOF: Easy. \square

Definition 61 (Identity Function). For any class \mathbf{A} , the *identity* function on \mathbf{A} is $\text{id}_{\mathbf{A}} = \{(x, x) \mid x \in \mathbf{A}\}$.

Theorem 62. Let $F : A \rightarrow B$. Assume $A \neq \emptyset$. Then F has a left inverse (i.e. there exists $G : B \rightarrow A$ such that $G \circ F = \text{id}_A$) if and only if F is one-to-one.

PROOF:

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

$\langle 2 \rangle 1$. ASSUME: F is one-to-one.

$\langle 2 \rangle 2$. $F^{-1} : \text{ran } F \rightarrow A$

$\langle 2 \rangle 3$. PICK $a \in A$

$\langle 2 \rangle 4$. Define $G : B \rightarrow A$ by:

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

$\langle 2 \rangle 5$. $\forall x \in A. G(F(x)) = x$

$\langle 1 \rangle 2$. 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 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 $\text{dom } H = \text{dom } R$.

Theorem 65. *Let $F : A \rightarrow B$. 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 $H : B \rightarrow A$ 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 $\text{dom } H = \text{dom } F^{-1}$

PROOF: By the Axiom of Choice.

$\langle 2 \rangle 3$. $\text{dom } H = B$

PROOF: $\text{dom } H = \text{dom } F^{-1} = \text{ran } F = B$ 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: $y \in B$

$\langle 3 \rangle 2$. $(y, H(y)) \in F^{-1}$

$\langle 3 \rangle 3$. $F(H(y)) = y$

□

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 $A \rightarrow \mathbf{B}$.

9 Dependent Products

Definition 67. Let I be a set and H_i a set for all $i \in I$. Define

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

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:

$\langle 1 \rangle 1$. 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 $\text{dom } F = \text{dom } R$

PROVE: $F \in \prod_{i \in I} H(i)$

PROOF: By the Axiom of Choice.

⟨2⟩7. $\text{dom } H = I$

PROOF: We have $\text{dom } R = I$ since for all $i \in I$ there exists x such that $x \in H(i)$.

⟨2⟩8. $\forall i \in I. F(i) \in H(i)$

PROOF: Since $iRF(i)$.

⟨1⟩2. If, for any set I and any function H with domain I , if $H(i) \neq \emptyset$ for all $i \in I$, then $\prod_{i \in I} H(i) \neq \emptyset$, then the Axiom of Choice is true.

⟨2⟩1. ASSUME: For any set I and any function H with domain I , if $H(i) \neq \emptyset$ for all $i \in I$, then $\prod_{i \in I} H(i) \neq \emptyset$

⟨2⟩2. LET: R be a relation

⟨2⟩3. LET: $I = \text{dom } R$

⟨2⟩4. Define the function H with domain I by: for $i \in I$, $H(i) = \{y : iRy\}$

⟨2⟩5. $H(i) \neq \emptyset$ for all $i \in I$

⟨2⟩6. PICK $F \in \prod_{i \in I} H(i)$

PROOF: By ⟨2⟩1

⟨2⟩7. F is a function

⟨2⟩8. $F \subseteq R$

PROOF: For all $i \in I$ we have $F(i) \in H(i)$ and so $iRF(i)$.

⟨2⟩9. $\text{dom } F = \text{dom } R$

□

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 $F : \mathcal{P}A - \{\emptyset\} \rightarrow A$ such that $F(X) \in X$ for all $X \in \mathcal{P}A - \{\emptyset\}$.*

PROOF:

⟨1⟩1. $1 \Rightarrow 2$

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

⟨1⟩2. $2 \Rightarrow 3$

⟨2⟩1. ASSUME: 2

⟨2⟩2. LET: \mathcal{A} be a set.

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

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

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

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

⟨1⟩3. $3 \Rightarrow 1$

⟨2⟩1. ASSUME: 3

⟨2⟩2. LET: R be a relation

⟨2⟩3. PICK a choice function G for $\text{ran } R$

- $\langle 2 \rangle 4$. Define $F : \text{dom } R \rightarrow \text{ran } R$ by $F(x) = G(R(x))$
 $\langle 2 \rangle 5$. $F \subseteq R$

□

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 $\text{fld } \mathbf{R}$.

PROOF:

- $\langle 1 \rangle 1$. LET: $x \in \text{fld } \mathbf{R}$
 $\langle 1 \rangle 2$. PICK y such that either $x\mathbf{R}y$ or $y\mathbf{R}x$
 $\langle 1 \rangle 3$. $x\mathbf{R}y$ and $y\mathbf{R}x$
 PROOF: Since \mathbf{R} is symmetric.
 $\langle 1 \rangle 4$. $x\mathbf{R}x$
 PROOF: Since \mathbf{R} is transitive.

□

Definition 72 (Equivalence Class). If \mathbf{R} is an equivalence relation and $x \in \text{fld } \mathbf{R}$, the *equivalence class* of x modulo \mathbf{R} is

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

Lemma 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:

- $\langle 1 \rangle 1$. 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.

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

Theorem 77. Assume that R is an equivalence relation on A and that $F : A \rightarrow B$. Assume that F is compatible with R ; that is, whenever xRy , then $F(x) = F(y)$. Then there exists a unique $\bar{F} : A/R \rightarrow B$ such that $F = \bar{F} \circ \phi$.

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

11 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 $x < y \vee x = y$.

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. \square

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. \square

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

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

Definition 90 (Isomorphism). Let A and B be posets. An *isomorphism* between A and B is a bijection f between A and B such that, for all $x, y \in A$, we have $x < y$ if and only if $f(x) < f(y)$.

Proposition 91. Isomorphism is an equivalence relation on the class of posets.

PROOF: Easy. \square

Proposition 92. Let $(A, <)$ be a poset and $B \subseteq A$. Then $< \cap B^2$ is a partial order on B .

PROOF: Easy. \square

12 Linear Orders

Definition 93 (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 94. Let \mathbf{R} be a linear ordering on \mathbf{A} .

1. There is no x such that $x\mathbf{R}x$.
2. For distinct x and y in \mathbf{A} , either $x\mathbf{R}y$ or $y\mathbf{R}x$.

PROOF: Immediate from trichotomy. \square

Definition 95 (Strictly Monotone Functions). Let A and B be linearly ordered sets. A function $f : A \rightarrow B$ is *strictly monotone* iff, for all $x, y \in A$, if $x < y$ then $f(x) < f(y)$.

Theorem 96. Let A and B be linearly ordered sets and $f : A \rightarrow B$ be strictly monotone. For all $x, y \in A$, if $f(x) < f(y)$ then $x < y$.

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

Theorem 97. Every strictly monotone function is injective.

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

Proposition 98. Let $(A, <)$ be a linearly ordered set and $B \subseteq A$. Then $< \cap B^2$ is a linear order on B .

PROOF: Easy. \square

13 Well Orderings

Definition 99 (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 100 (Transfinite Induction Principle). Let $<$ be a well ordering on A . Let $B \subseteq A$. Suppose that

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

Then $B = A$.

PROOF:

- ⟨1⟩1. ASSUME: for a contradiction $B \neq A$
- ⟨1⟩2. LET: t be the least element of $A - B$
- ⟨1⟩3. $\text{seg } t \subseteq B$
- ⟨1⟩4. $t \notin B$
- ⟨1⟩5. Q.E.D.

PROOF: This is a contradiction.

□

Theorem 101. *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:

- ⟨1⟩1. ASSUME: for a contradiction $B \subseteq A$ has no least element.
- ⟨1⟩2. $A - B$ is $<$ -inductive.
 - ⟨2⟩1. LET: $t \in A$
 - ⟨2⟩2. ASSUME: $\text{seg } t \subseteq A - B$
 - ⟨2⟩3. $t \notin B$
- PROOF: If it were, it would be the least element of B .
- ⟨2⟩4. $t \in A - B$
- ⟨1⟩3. $A - B = A$
- ⟨1⟩4. $B = \emptyset$

□

Theorem 102 (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

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

PROOF:

- ⟨1⟩1. Given $t \in A$, let us say that a function v is P -constructed up to t iff $\text{dom } v = \{x \in A : x \leq t\}$ and $\forall x \in \text{dom } v. P(v \upharpoonright \text{seg } x, v(x))$
- ⟨1⟩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 $\forall x \leq t_1. v_1(x) = v_2(x)$
 - ⟨2⟩1. LET: $x \leq t_1$
 - ⟨2⟩2. ASSUME: $\forall y < x. v_1(y) = v_2(y)$
 - ⟨2⟩3. $v_1 \upharpoonright \text{seg } x = v_2 \upharpoonright \text{seg } x$
 - ⟨2⟩4. $P(v_1 \upharpoonright \text{seg } x, v_1(x))$
 - ⟨2⟩5. $P(v_2 \upharpoonright \text{seg } x, v_2(x))$
 - ⟨2⟩6. $v_1(x) = v_2(x)$

PROOF: Since there is only one y such that $P(v_1 \upharpoonright \text{seg } x, y)$.

⟨2⟩7. Q.E.D.

PROOF: By transfinite induction.

- ⟨1⟩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 $\langle 1 \rangle 2$

$\langle 2 \rangle 6.$ $x = y$

$\langle 1 \rangle 7.$ $\forall x \in \text{dom } F. P(F \upharpoonright \text{seg } x, F(x))$

$\langle 2 \rangle 1.$ LET: $x \in \text{dom } F$

$\langle 2 \rangle 2.$ PICK $v \in \mathcal{H}$ such that $x \in \text{dom } v$

$\langle 2 \rangle 3.$ $P(v \upharpoonright \text{seg } x, v(x))$

$\langle 2 \rangle 4.$ $v \upharpoonright \text{seg } x = F \upharpoonright \text{seg } x$

PROOF: $\forall y < x. (y, v(y)) \in \bigcup \mathcal{H} = F$

$\langle 2 \rangle 5.$ $v(x) = F(x)$

PROOF: $(x, v(x)) \in \bigcup \mathcal{H} = F$

$\langle 1 \rangle 8.$ $\text{dom } F = A$

$\langle 2 \rangle 1.$ LET: $x \in A$

$\langle 2 \rangle 2.$ ASSUME: $\forall y < x. y \in \text{dom } F$

$\langle 2 \rangle 3.$ LET: z be the object such that $P(F \upharpoonright \text{seg } x, z)$

$\langle 2 \rangle 4.$ $F \upharpoonright \text{seg } x \cup \{(x, z)\}$ is P -constructed up to x

$\langle 2 \rangle 5.$ $x \in \text{dom } F$

$\langle 2 \rangle 6.$ Q.E.D.

PROOF: By transfinite induction, this proves $\forall x \in A. x \in \text{dom } F$.

$\langle 1 \rangle 9.$ F is unique.

$\langle 2 \rangle 1.$ LET: G be a function with domain A such that $\forall x \in A. P(G \upharpoonright \text{seg } x, G(x))$

PROVE: $\forall x \in A. F(x) = G(x)$

$\langle 2 \rangle 2.$ LET: $x \in A$

$\langle 2 \rangle 3.$ ASSUME: $\forall y < x. F(y) = G(y)$

$\langle 2 \rangle 4.$ $F \upharpoonright \text{seg } x = G \upharpoonright \text{seg } x$

$\langle 2 \rangle 5.$ $F(x) = G(x)$

$\langle 2 \rangle 6.$ Q.E.D.

PROOF: This completes the proof by transfinite induction.

□

Proposition 103. Let $(A, <)$ be a well ordered set and $B \subseteq A$. Then $< \cap B^2$ is a well order on B .

PROOF: Easy. □

Theorem 104. Let A and B be well-ordered sets. Then one of the following holds:

- $A \cong B$
- $\exists b \in B. A \cong \text{seg } b$
- $\exists a \in A. \text{seg } a \cong B$

PROOF:

$\langle 1 \rangle 1$. PICK e that is not a member of A or B

$\langle 1 \rangle 2$. Define $F : A \rightarrow B \cup \{e\}$ by:

$$F(t) = \begin{cases} \text{the least element of } B - F(\text{seg } t) & \text{if } B - F(\text{seg } t) \neq \emptyset \\ e & \text{if } B - F(\text{seg } t) = \emptyset \end{cases}$$

$\langle 1 \rangle 3$. CASE: $e \in \text{ran } F$

$\langle 2 \rangle 1$. LET: $a \in A$ be least such that $B - F(\text{seg } a) = \emptyset$

$\langle 2 \rangle 2$. $F \upharpoonright \text{seg } a : \text{seg } a \cong B$

$\langle 1 \rangle 4$. CASE: $\text{ran } F = B$

PROOF: In this case $F : A \cong B$.

$\langle 1 \rangle 5$. CASE: $\text{ran } F \subset B$

$\langle 2 \rangle 1$. LET: $b \in B$ be least such that $b \notin \text{ran } F$

$\langle 2 \rangle 2$. $F : A \cong \text{seg } b$

□

14 Epsilon-Images

Lemma 105. *Let $<$ be a well ordering on A . Let E be the function on A defined by transfinite recursion thus:*

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

Let $\alpha = \text{ran } E$. 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 .

Corollary 105.1. *For any well-ordered set $(A, <)$, if α is its epsilon-image, then $(A, <)$ is isomorphic to (α, \in) .*

Corollary 105.2. *The epsilon-image of any well-ordered set is well ordered by \in .*

Theorem 106. *Two well-ordered sets are isomorphic iff they have the same ϵ -image.*

PROOF:

$\langle 1 \rangle 1$. LET: A and B be well-ordered sets.

$\langle 1 \rangle 2$. If A and B have the same ϵ -image then they are isomorphic.

PROOF: From Corollary 105.1.

$\langle 1 \rangle 3$. If $A \cong B$ then A and B have the same epsilon-image.

$\langle 2 \rangle 1$. LET: $f : A \cong B$

$\langle 2 \rangle 2$. LET: $E : A \cong \alpha$ and $F : B \cong \beta$ be the canonical isomorphisms between A and B and their epsilon-images.

$\langle 2 \rangle 3$. $\forall x \in A. E(x) = F(f(x))$

$\langle 3 \rangle 1$. LET: $x \in A$

$\langle 3 \rangle 2$. ASSUME: $\forall y < x. E(y) = F(f(y))$

$\langle 3 \rangle 3$. $E(x) = F(f(x))$

PROOF:

$$\begin{aligned} E(x) &= \{E(y) : y < x\} \\ &= \{F(f(y)) : y < x\} \\ &= \{F(z) : z < f(x)\} \\ &= F(f(x)) \end{aligned}$$

$\langle 2 \rangle 4$. $\alpha = \beta$

□

15 Ordinal Numbers

Definition 107 (Ordinal Number). The *ordinal number* of a well-ordered set is its epsilon-image.

Definition 108 (Well-ordered by Epsilon). A set A is *well-ordered by epsilon* iff $\{(x, y) : x, y \in A, x \in y\}$ is a well ordering on A .

Theorem 109. *A set is an ordinal number if and only if it is a transitive set that is well-ordered by epsilon.*

PROOF:

$\langle 1 \rangle 1$. Every ordinal number is a transitive set.

PROOF: Lemma 105.

$\langle 1 \rangle 2$. Every ordinal number is well-ordered by epsilon.

PROOF: Corollary 105.2.

$\langle 1 \rangle 3$. Every transitive set that is well-ordered by epsilon is an ordinal number.

$\langle 2 \rangle 1$. LET: α be a transitive set well-ordered by epsilon.

$\langle 2 \rangle 2$. LET: β be the epsilon-image of (α, \in) with $E : \alpha \cong \beta$ the canonical isomorphism.

$\langle 2 \rangle 3$. $\forall x \in \alpha. E(x) = x$

$\langle 3 \rangle 1$. LET: $x \in \alpha$

$\langle 3 \rangle 2$. ASSUME: $\forall y < x. E(y) = y$

$\langle 3 \rangle 3$. $E(x) = x$

PROOF:

$$\begin{aligned} E(x) &= \{E(y) : y \in \alpha, y \in x\} \\ &= \{E(y) : y \in x\} && (\alpha \text{ is a transitive set}) \\ &= \{y : y \in x\} && (\langle 3 \rangle 2) \\ &= x \end{aligned}$$

$\langle 2 \rangle 4$. $\alpha = \beta$

□

16 Natural Numbers

Definition 110 (Successor). The *successor* of a set a is the set $a^+ = a \cup \{a\}$.

Definition 111 (Inductive). A class \mathbf{A} is *inductive* iff $\emptyset \in \mathbf{A}$ and $\forall a \in \mathbf{A}. a^+ \in \mathbf{A}$.

Axiom 112 (Infinity). *There exists an inductive set.*

Definition 113 (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 114. *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 115. *The set ω is inductive, and is a subset of every inductive set.*

PROOF: Easy. \square

Corollary 115.1 (Proof by Induction). *Any inductive subclass of ω is equal to ω .*

Theorem 116. *Every natural number except 0 is the successor of some natural number.*

PROOF: Easy proof by induction. \square

Definition 117 (Peano System). A *Peano system* is a triple $\langle N, S, e \rangle$ consisting of a set N , a function $S : N \rightarrow N$ and an element $e \in N$ such that:

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

Definition 118 (Transitive Set). A set A is a *transitive set* iff every member of a member of A is a member of A .

Theorem 119. *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 120. *Every natural number is a transitive set.*

PROOF:

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

PROOF: Vacuous.

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

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

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

PROOF: Theorem 119.

\square

Theorem 121. $\langle \omega, \sigma, 0 \rangle$ is a Peano system, where $0 = \emptyset$ and $\sigma = \{ \langle n, n^+ \rangle : n \in \omega \}$.

PROOF:

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

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

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

PROOF: If $m^+ = n^+$ then $m = \bigcup(m^+) = \bigcup(n^+) = n$ using Theorems 119 and 120.

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

□

Theorem 122. *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.

□

Theorem 123 (Recursion Theorem on ω). *Let A be a set, $a \in A$ and $F : A \rightarrow A$. Then there exists a unique function $h : \omega \rightarrow A$ such that*

$$h(0) = a ,$$

and for every n in ω ,

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

PROOF:

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

1. If $0 \in \text{dom } v$ then $v(0) = a$

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

$\langle 1 \rangle 2.$ 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: $(k^+, y_1), (k^+, y_2) \in h$

and the zero element

$$h(0) = e .$$

PROOF:

⟨1⟩1. There exists a function h that satisfies those two conditions.

PROOF: By the Recursion Theorem.

⟨1⟩2. For all $m, n \in \omega$, if $m \neq n$ then $h(m) \neq h(n)$

⟨2⟩1. For all $n \in \omega$, if $n \neq 0$ then $h(n) \neq h(0)$

⟨3⟩1. LET: $n \in \omega$

⟨3⟩2. ASSUME: $n \neq 0$

⟨3⟩3. PICK p such that $n = p^+$

⟨3⟩4. $h(n) \neq h(0)$

PROOF: $h(n) = S(h(p)) \neq e = h(0)$.

⟨2⟩2. For all $m \in \omega$, if $\forall n(m \neq n \Rightarrow h(m) \neq h(n))$ then $\forall n(m^+ \neq n \Rightarrow h(m^+) \neq h(n))$

⟨3⟩1. LET: $m \in \omega$

⟨3⟩2. ASSUME: $\forall n(m \neq n \Rightarrow h(m) \neq h(n))$

⟨3⟩3. LET: $n \in \omega$

⟨3⟩4. ASSUME: $m^+ \neq n$

PROVE: $h(m^+) \neq h(n)$

⟨3⟩5. CASE: $n = 0$

PROOF: $h(m^+) = S(h(m)) \neq e = h(n)$

⟨3⟩6. CASE: $n = p^+$

⟨4⟩1. $m \neq p$

⟨4⟩2. $h(m) \neq h(p)$

⟨4⟩3. $S(h(m)) \neq S(h(p))$

⟨4⟩4. $h(m^+) \neq h(p^+)$

⟨1⟩3. For all $x \in N$, there exists $n \in \omega$ such that $h(n) = x$

PROOF: An easy induction on x .

□

17 Finite Sets

Definition 125 (Finite). A set is *finite* iff it is equinumerous with a natural number. Otherwise it is infinite.

Theorem 126. No natural number is equinumerous with a proper subset of itself.

PROOF:

⟨1⟩1. Any injective function $f : 0 \rightarrow 0$ has range 0.

PROOF: Since the only such function is \emptyset .

⟨1⟩2. For any natural number n , if every injective function $f : n \rightarrow n$ has range n , then every injective function $f : n^+ \rightarrow n^+$ has range n^+ .

⟨2⟩1. LET: $n \in \omega$

⟨2⟩2. ASSUME: Every injective function $f : n \rightarrow n$ has range n .

⟨2⟩3. LET: $f : n^+ \rightarrow n^+$ be injective.

⟨2⟩4. Define $g : n \rightarrow n$ 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. $\text{ran } g = n$

PROOF: By ⟨2⟩2.

⟨2⟩7. $\text{ran } f = n^+$

⟨3⟩1. $\forall k \in n. k \in \text{ran } f$

PROOF: Since $\text{ran } g \subseteq \text{ran } f$.

⟨3⟩2. $n \in \text{ran } f$

⟨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 $n \in \text{ran } f$.

□

Corollary 126.1. *No finite set is equinumerous with a proper subset of itself.*

Corollary 126.2. *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 126.3. *Every finite set is equinumerous with a unique natural number.*

Lemma 127. *Let n be a natural number and $C \subseteq n$. Then there exists $m \in n$ such that $C \approx m$.*

PROOF:

⟨1⟩1. For all $C \subseteq 0$, there exists $m \in 0$ 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 $m \in n$ such that $C \approx m$.

Let $C \subseteq n^+$. Then there exists $m \in n^+$ 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 $m \subseteq n$ 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 $m \subseteq n$ 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 $m \subseteq n$.

□

Corollary 127.1. *Any subset of a finite set is finite.*

18 Cardinal Numbers

Definition 128 (Cardinality). TODO

Theorem 129. *For any sets A and B , $|A| = |B|$ if and only if $A \approx B$.*

PROOF: TODO □

Theorem 130. *For any finite set A , $|A|$ is the natural number such that $A \approx |A|$.*

PROOF: TODO □

Definition 131. We write \aleph_0 for $|\omega|$.

19 Cardinal Arithmetic

Definition 132 (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 133. *For any cardinal number κ we have $\kappa + 0 = \kappa$.*

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

Lemma 134. *For any natural number n we have $n + \aleph_0 = \aleph_0$.*

PROOF: Easy. □

Lemma 135.

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

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

Theorem 136.

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

PROOF: Easy. \square

Theorem 137.

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

PROOF: Easy. \square

Definition 138 (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 139. *For any cardinal number κ we have $\kappa 0 = 0$.*

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

Lemma 140. *For any natural number n we have $n\aleph_0 = \aleph_0$.*

PROOF: Induction on n using Lemma 135. \square

Lemma 141.

$$\aleph_0 \aleph_0 = \aleph_0$$

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

Lemma 142.

$$\kappa 1 = \kappa$$

PROOF: Easy. \square

Theorem 143.

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

PROOF: Easy. \square

Theorem 144.

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

PROOF: Easy. \square

Theorem 145.

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

PROOF: Easy. \square

Definition 146 (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 147. *For any cardinal κ , $\kappa^0 = 1$.*

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

Theorem 148. *For any non-zero cardinal κ , we have $0^\kappa = 0$.*

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

Theorem 149. *For any set A , $|\mathcal{P}A| = 2^{|A|}$.*

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

Corollary 149.1. *For any cardinal κ , we have $\kappa \neq 2^\kappa$.*

Theorem 150.

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

PROOF: Easy. \square

Theorem 151.

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

PROOF: Easy. \square

Theorem 152.

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

PROOF: Easy. \square

20 Arithmetic

Lemma 153. *For any natural numbers m and n , we have $m+n^+ = (m+n)^+$.*

PROOF: Easy. \square

Corollary 153.1. *The union of two finite sets is finite.*

Lemma 154. *For any natural numbers m and n we have $mn^+ = mn + m$.*

PROOF: Easy. \square

Corollary 154.1. *The Cartesian product of two finite sets is finite.*

Lemma 155. *For any natural numbers m and n we have $m^{n^+} = m^n m$.*

PROOF: Easy. \square

Corollary 155.1. *If A and B are finite sets then A^B is finite.*

21 Ordering on the Natural Numbers

Lemma 156. *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 120).

□

Lemma 157. *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 120).

□

Theorem 158 (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 157.
 If $m \in n$ and $n \in m$ then $m \in m$ by Theorem 120, contradicting Lemma 157.
- $\langle 1 \rangle 2$. 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 156 so $n^+ \in m$ or $n^+ = m$.

□

Corollary 158.1. *The relation \in is a linear ordering on ω .*

Corollary 158.2. *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 120.
- $\langle 2 \rangle 3$. $m \neq n$
 PROOF: Lemma 157.
- $\langle 1 \rangle 3$. 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 159. *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 156. □

Theorem 160. *For any non-zero natural number p , the function that maps n to np is strictly monotone.*

PROOF: Easy induction on p using Theorem 159. □

Theorem 161 (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 162 (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 163 (Choice). *Let $<$ be a linear ordering on A . Then $<$ is a well-ordering on A iff there does not exist any function $f : \omega \rightarrow \omega$ such that $f(n+1) < f(n)$ for all $n \in \omega$.*

PROOF:

$\langle 1 \rangle 1$. If $<$ is a well-ordering on A then there does not exist any function $f : \omega \rightarrow \omega$ such that $f(n+1) < f(n)$ for all $n \in \omega$.

PROOF: If there is such a function f then $\text{ran } f$ is a nonempty subset of A with no least element.

$\langle 1 \rangle 2$. If there does not exist any function $f : \omega \rightarrow A$ such that $f(n+1) < f(n)$ for all $n \in \omega$ then $<$ is a well-ordering on A .

$\langle 2 \rangle 1$. LET: $X \subseteq A$ be a nonempty subset of A with no least element.

PROVE: There exists a function $f : \omega \rightarrow A$ such that $f(n+1) < f(n)$ for all $n \in \omega$

$\langle 2 \rangle 2$. PICK $a_0 \in X$

$\langle 2 \rangle 3$. $\forall x \in X. \exists y \in X. y < x$

$\langle 2 \rangle 4$. PICK a function $g : X \rightarrow X$ such that $\forall x \in X. g(x) < x$

PROOF: By the Axiom of Choice.

$\langle 2 \rangle 5$. Define $f : \omega \rightarrow A$ recursively by:

$$f(0) = a_0$$

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

$\langle 2 \rangle 6$. $\forall n \in \omega. f(n^+) < f(n)$

\square

Lemma 164. *For any natural numbers m and n , we have $m \in n$ if and only if there exists a natural number p such that $n = m + p^+$.*

PROOF:

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

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

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

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

PROOF: Vacuous.

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

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

□

Lemma 165. For natural numbers m, n, p and q , if $m \in n$ and $p \in q$ then $mp + nq \in mq + np$.

- $\langle 1 \rangle 1.$ PICK natural numbers a and b such that $n = m + a^+$ and $q = p + b^+$
- PROOF: Lemma 164.
- $\langle 1 \rangle 2.$ $mp + nq = mq + np + (a^+ + b)^+$
- $\langle 1 \rangle 3.$ $mp + nq \in mq + np$
- PROOF: Lemma 164.

22 The Integers

Theorem 166. The relation \sim is an equivalence relation on $\omega \times \omega$, where $(m, n) \sim (p, q)$ iff $m + q = n + p$.

PROOF:

- $\langle 1 \rangle 1.$ The relation \sim is reflexive on ω^2
- PROOF: For any m, n , we have $m + n = m + n$ and so $(m, n) \sim (m, n)$.
- $\langle 1 \rangle 2.$ The relation \sim is symmetric.
- PROOF: If $m + q = n + p$ then $p + n = q + m$.
- $\langle 1 \rangle 3.$ The relation \sim is transitive.
- $\langle 2 \rangle 1.$ ASSUME: $(m, n) \sim (p, q) \sim (r, s)$
- $\langle 2 \rangle 2.$ $m + q = n + p$
- $\langle 2 \rangle 3.$ $p + s = q + r$
- $\langle 2 \rangle 4.$ $m + p + q + s = n + p + q + r$
- $\langle 2 \rangle 5.$ $m + s = n + r$
- PROOF: By cancellation of addition in ω .

□

Definition 167. The set \mathbb{Z} of integers is the quotient set $(\omega \times \omega) / \sim$.

Lemma 168. 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 169 (Addition). Addition $+$ on \mathbb{Z} is the binary operation such that

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

Theorem 170. *Addition on \mathbb{Z} is commutative.*

PROOF: From the definition. \square

Theorem 171. *Addition on \mathbb{Z} is associative.*

PROOF: Easy. \square

Definition 172 (Zero). The zero in the integers is $0 = [(0, 0)]$.

Theorem 173. *For any integer a we have $a + 0 = a$.*

PROOF: Easy. \square

Theorem 174. *For any integer a , there exists an integer b such that $a + b = 0$.*

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

Lemma 175. *If $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$ then $(mp + nq, mq + np) \sim (m'p' + n'q', m'q' + n'p')$.*

PROOF:

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

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

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

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

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

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

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

\square

Definition 176 (Multiplication). *Multiplication \cdot is the binary operation on \mathbb{Z} such that*

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

Theorem 177. *Multiplication is commutative.*

PROOF: Easy. \square

Theorem 178. *Multiplication is associative.*

PROOF: Easy. \square

Theorem 179. *Multiplication is distributive over addition.*

PROOF: Easy. \square

Definition 180. The integer one is $1 = [(1, 0)]$.

Theorem 181. *For any integer a we have $a1 = a$.*

PROOF: Easy. \square

Theorem 182. $0 \neq 1$

PROOF: Easy. \square

Lemma 183. *If $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$ then $m + q \in p + n$ iff $m' + q' \in p' + n'$.*

PROOF:

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

Definition 184 (Ordering). The ordering $<$ on \mathbb{Z} is defined by: $[(m, n)] < [(p, q)]$ iff $m + q \in n + p$.

Theorem 185. *The relation $<$ is a linear ordering on \mathbb{Z} .*

PROOF:

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

PROOF: From trichotomy on ω .

\square

Theorem 186. *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 186.1. *If $a + c = b + c$ then $a = b$.*

Theorem 187. *If $0 < c$, then the function that maps an integer a to ac is strictly monotone.*

PROOF:

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

PROOF: Lemma 165.

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

□

Lemma 188. For integers a and b , $a(-b) = -(ab)$

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

Theorem 189. 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 190. 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 191. 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 192 (Positive). An integer a is *positive* iff $0 < a$.

Theorem 193. Define $E : \omega \rightarrow \mathbb{Z}$ 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. □

23 Equinumerosity

Definition 194 (Equinumerous). Two sets A and B are *equinumerous*, $A \approx B$, iff there exists a bijection between them.

Theorem 195. *Equinumerosity is an equivalence relation on the class of sets.*

PROOF: Easy. □

Theorem 196 (Cantor 1873). *No set is equinumerous with its power set.*

PROOF:

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

PROVE: g is not surjective.

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

⟨1⟩3. $\forall x \in A. g(x) \neq B$

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

□

24 Ordering Cardinal Numbers

Definition 197 (Dominated). A set A is *dominated* by a set B , $A \preceq B$, iff there exists an injection $f : A \rightarrow B$.

Lemma 198. *Domination is a preorder on the class of sets.*

PROOF: Easy. \square

Lemma 199. *If $A \subseteq B$ then $A \preceq B$.*

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

Lemma 200. *If $A \preceq B$, $A \approx A'$ and $B \approx B'$ then $A' \preceq B'$.*

PROOF: Easy. \square

Definition 201. Given cardinal numbers κ and λ , we write $\kappa \leq \lambda$ iff $K \preceq L$, 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 202 (Schröder-Bernstein). *If $A \preceq B$ and $B \preceq A$ then $A \approx B$.*

PROOF:

$\langle 1 \rangle 1$. LET: $f : A \rightarrow B$ and $g : B \rightarrow A$ be one-to-one.

$\langle 1 \rangle 2$. Define the sequence of sets $C_n \subseteq A$ by:

$$C_0 = A - \text{ran } g$$

$$C_{n+1} = g(f(C_n))$$

$\langle 1 \rangle 3$. Define $h : A \rightarrow B$ by

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

$\langle 1 \rangle 4$. h is injective.

$\langle 2 \rangle 1$. LET: $x, y \in A$

$\langle 2 \rangle 2$. ASSUME: $h(x) = h(y)$

$\langle 2 \rangle 3$. CASE: $x \in C_m, y \in C_n$

PROOF: We have $f(x) = f(y)$ so $x = y$

$\langle 2 \rangle 4$. 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 $y \in C_{m+1}$.

$\langle 2 \rangle 5$. CASE: $x, y \notin \bigcup_n C_n$

PROOF: We have $g^{-1}(x) = g^{-1}(y)$ so $x = y$.

$\langle 1 \rangle 5$. h is surjective.

$\langle 2 \rangle 1$. LET: $y \in B$

$\langle 2 \rangle 2$. ASSUME: $y \notin f(C_n)$ for all n

$\langle 2 \rangle 3$. $g(y) \notin C_n$ for all n

$\langle 2 \rangle 4$. $y = h(g(y))$

\square

Corollary 202.1. *The relation \leq is a partial order on the class of cardinal numbers.*

Theorem 203. *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 $\Phi : M^K \rightarrow M^L$ 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 204 (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.

$\langle 2 \rangle 6$. $\text{dom } F = \text{dom } R$

\square

Theorem 205 (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 $\text{dom } f \subseteq C$ and $\text{ran } f \subseteq D$

$\langle 2 \rangle 4$. 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

$\langle 2 \rangle 6$. $\text{dom } f = C$ or $\text{ran } f = D$

$\langle 2 \rangle 7$. f is an injective function $C \rightarrow D$ or f^{-1} is an injective function $D \rightarrow C$

⟨1⟩2. If Cardinal Comparability then the Axiom of Choice.

PROOF: TODO

□

Theorem 206 (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 $f : \omega \rightarrow A$ by recursion by: $f(n) = F(A - \{f(0), f(1), \dots, f(n-1)\})$

PROOF: $A - \{f(0), f(1), \dots, f(n-1)\}$ is nonempty because A is infinite.

⟨1⟩4. f is injective.

□

Corollary 206.1 (Choice). *For any infinite cardinal κ we have $\aleph_0 \leq \kappa$.*

Corollary 206.2 (Choice). *A set is infinite iff it is equinumerous to a proper subset of itself.*

Proposition 207 (Choice). *If there exists a surjection $A \rightarrow B$ then $B \preccurlyeq A$.*

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

25 Countable Sets

Definition 208 (Countable). A set is *countable* iff it is dominated by ω .

Proposition 209. *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 210. *The product of two countable sets is countable.*

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

Proposition 211 (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 212 (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 $G : \omega \rightarrow \mathcal{A}$

⟨1⟩4. PICK a function F with domain ω such that, for all m , $F(m)$ is a surjection $\omega \rightarrow G(m)$

PROOF: By the Axiom of Choice.

⟨1⟩5. Define $f : \omega \times \omega \rightarrow \bigcup \mathcal{A}$ by $f(m, n) = F(m)(n)$

⟨1⟩6. f is surjective.

⟨1⟩7. $A \preccurlyeq \omega \times \omega$

□

26 Arithmetic of Infinite Cardinals

Lemma 213 (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: $\mathcal{H} = \{f : f = \emptyset \text{ or for some infinite } A \subseteq B, f \text{ is a bijection between } A \times A \text{ and } A\}$
- $\langle 1 \rangle 4$. 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: $A = \text{ran } \bigcup \mathcal{C}$
 - $\langle 2 \rangle 5$. 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 $a_1 \in \text{ran } f_1$ and $a_2 \in \text{ran } f_2$
 - $\langle 3 \rangle 3$. ASSUME: w.l.o.g. $f_1 \subseteq f_2$
 - $\langle 3 \rangle 4$. $\langle a_1, a_2 \rangle \in \text{dom } f_2$
 - $\langle 3 \rangle 5$. $\langle a_1, a_2 \rangle \in \text{dom } \bigcup \mathcal{C}$
- $\langle 1 \rangle 5$. 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 .
 $\langle 2 \rangle 2. \lambda = \kappa$
 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 213.1 (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:
 $\langle 1 \rangle 1.$ ASSUME: w.l.o.g. $\kappa \leq \lambda$
 $\langle 1 \rangle 2. \kappa + \lambda = \lambda$
 PROOF:

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

$\langle 1 \rangle 3. \kappa \cdot \lambda = \lambda$
 PROOF:

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

□