

Summary of Halmos' Naive Set Theory

Robin Adams

August 23, 2023

Contents

1	Primitive Terms and Axioms	2
2	The Subset Relation	3
3	Comprehension Notation	4
4	Unordered Pairs	5
5	Unions	6
6	Intersections	7
7	Unordered Triples	9
8	Relative Complements	10
9	Symmetric Difference	13
10	Power Sets	14
11	Ordered Pairs	16
12	Relations	18
13	Functions	21
14	Families	23
15	Inverses and Composites	25
16	Numbers	27
17	The Peano Axioms	29
18	Arithmetic	33

Chapter 1

Primitive Terms and Axioms

Let there be *sets*. We assume that everything is a set.

Let there be a binary relation of *membership*, \in . If $x \in A$ we say that x *belongs to* A , x is an *element* of A , or x is *contained in* A . If this does not hold we write $x \notin A$.

Axiom 1.1 (Axiom of Extensionality). *Two sets are equal if and only if they have the same elements.*

Axiom 1.2 (Axiom of Comprehension, Aussonderungsaxiom). *To every set A and to every condition $S(x)$ there corresponds a set B whose elements are exactly those elements x of A for which $S(x)$ holds.*

Axiom 1.3 (Axiom of Pairing). *For any two sets, there exists a set that they both belong to.*

Axiom 1.4 (Union Axiom). *For every set A , there exists a set that contains all the elements that belong to at least one element of A .*

Definition 1.5 (Subset). Let A and B be sets. We say that A is a *subset* of B , or B *includes* A , and write $A \subseteq B$ or $B \supseteq A$, iff every element of A is an element of B .

Axiom 1.6 (Power Set Axiom). *For any set A , there exists a set that contains all the subsets of A .*

Axiom 1.7 (Axiom of Infinity). *There exists a set I such that:*

- I has an element that has no elements
- for all $x \in I$, there exists $y \in I$ such that the elements of y are exactly x and the elements of x .

Chapter 2

The Subset Relation

Theorem 2.1. *For any set A , we have $A \subseteq A$.*

PROOF: Every element of A is an element of A . \square

Theorem 2.2. *For any sets A , B and C , if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.*

PROOF: If every element of A is an element of B , and every element of B is an element of C , then every element of A is an element of C . \square

Theorem 2.3. *For any sets A and B , if $A \subseteq B$ and $B \subseteq A$ then $A = B$.*

PROOF: If every element of A is an element of B , and every element of B is an element of A , then A and B have the same elements, and therefore are equal by the Axiom of Extensionality. \square

Definition 2.4 (Proper Subset). Let A and B be sets. We say that A is a *proper* subset of B , or B *properly* includes A , and write $A \subsetneq B$ or $B \supsetneq A$, iff $A \subseteq B$ and $A \neq B$.

Chapter 3

Comprehension Notation

Definition 3.1. Given a set A and a condition $S(x)$, we write $\{x \in A : S(x)\}$ for the set whose elements are exactly those elements x of A for which $S(x)$ holds.

PROOF: This exists by the Axiom of Comprehension and is unique by the Axiom of Extensionality. \square

Theorem 3.2. *There is no set that contains every set.*

PROOF:

$\langle 1 \rangle 1.$ LET: A be a set.

PROVE: There exists a set B such that $B \notin A$.

$\langle 1 \rangle 2.$ LET: $B = \{x \in A : x \notin x\}$

$\langle 1 \rangle 3.$ If $B \in A$ then we have $B \in B$ if and only if $B \notin B$.

$\langle 1 \rangle 4.$ $B \notin A$

\square

Chapter 4

Unordered Pairs

Theorem 4.1. *There exists a set with no elements.*

PROOF: Immediate from the Axiom of Infinity. \square

Definition 4.2 (Empty Set). The *empty set* \emptyset is the set with no elements.

Theorem 4.3. *For any set A we have $\emptyset \subset A$.*

PROOF: Vacuous. \square

Definition 4.4 ((Unordered) Pair). For any sets a and b , the *(unordered) pair* $\{a, b\}$ is the set whose elements are just a and b .

PROOF: This exists by the Axioms of Pairing and Comprehension, and is unique by the Axiom of Extensionality. \square

Definition 4.5 (Singleton). For any set a , the *singleton* $\{a\}$ is defined to be $\{a, a\}$.

Chapter 5

Unions

Definition 5.1 (Union). For any set \mathcal{C} , the *union* of \mathcal{C} , $\bigcup \mathcal{C}$, is the set whose elements are the elements of the elements of \mathcal{C} .

We write $\bigcup_{X \in \mathcal{A}} t[X]$ for $\bigcup \{t[X] \mid X \in \mathcal{A}\}$.

PROOF: This exists by the Union Axiom and Comprehension Axiom, and is unique by the Axiom of Extensionality. \square

Proposition 5.2.

$$\bigcup \emptyset = \emptyset$$

PROOF: There is no set that is an element of an element of \emptyset . \square

Proposition 5.3. *For any set A , we have $\bigcup \{A\} = A$.*

PROOF: For any x , we have x is an element of an element of $\{A\}$ if and only if x is an element of A . \square

Definition 5.4. We write $A \cup B$ for $\bigcup \{A, B\}$.

Proposition 5.5. *For any set A , we have $A \cup \emptyset = A$.*

PROOF: $x \in A \cup \emptyset$ iff $x \in A$ or $x \in \emptyset$, iff $x \in A$. \square

Proposition 5.6 (Idempotence). *For any set A , we have $A \cup A = A$.*

PROOF: $x \in A$ or $x \in A$ is equivalent to $x \in A$. \square

Proposition 5.7. *For any sets A and B , we have $A \subseteq B$ if and only if $A \cup B = B$.*

PROOF: For any x , the statement "if $x \in A$ then $x \in B$ " is equivalent to " $x \in A$ or $x \in B$ if and only if $x \in B$ ". \square

Proposition 5.8. *For any sets a and b , we have $\{a\} \cup \{b\} = \{a, b\}$.*

PROOF: Immediate from definitions. \square

Chapter 6

Intersections

Definition 6.1 (Intersection). For any sets A and B , the *intersection* $A \cap B$ is defined to be $\{x \in A : x \in B\}$.

Proposition 6.2. For any set A , we have $A \cap \emptyset = \emptyset$.

PROOF: There is no x such that $x \in A$ and $x \in \emptyset$. \square

Proposition 6.3. For any set A , we have

$$A \cap A = A .$$

PROOF: We have $x \in A$ and $x \in A$ if and only if $x \in A$. \square

Proposition 6.4. For any sets A and B , we have $A \subseteq B$ if and only if $A \cap B = A$.

PROOF: For any x , the statement "if $x \in A$ then $x \in B$ " is equivalent to " $x \in A$ and $x \in B$ if and only if $x \in A$ ". \square

Proposition 6.5. For any sets A , B and C , we have $C \subseteq A$ if and only if $(A \cap B) \cup C = A \cap (B \cup C)$.

PROOF: The statement "if $x \in C$ then $x \in A$ " is equivalent to the statement " $((x \in A \wedge x \in B) \vee x \in C) \Leftrightarrow (x \in A \wedge (x \in B \vee x \in C))$ ". \square

Definition 6.6 (Disjoint). Two sets A and B are *disjoint* if and only if $A \cap B = \emptyset$.

Definition 6.7 (Pairwise Disjoint). Let A be a set. We say the elements of A are *pairwise disjoint* if and only if, for all $x, y \in A$, if $x \cap y \neq \emptyset$ then $x = y$.

Definition 6.8 (Intersection). For any nonempty set \mathcal{C} , the *intersection* of \mathcal{C} , $\bigcap \mathcal{C}$, is the set that contains exactly those sets that belong to every element of \mathcal{C} .

We write $\bigcap_{X \in \mathcal{A}} t[X]$ for $\bigcap \{t[X] \mid X \in \mathcal{A}\}$.

PROOF:

$\langle 1 \rangle 1$. LET: \mathcal{C} be a nonempty set.

$\langle 1 \rangle 2$. There exists a set I whose elements are exactly the sets that belong to every element of \mathcal{C} .

PROOF: Pick $A \in \mathcal{C}$, and take $I = \{x \in A : \forall X \in \mathcal{C}. x \in X\}$.

$\langle 1 \rangle 3$. For any sets I, J , if the elements of I and J are exactly the sets that belong to every element of \mathcal{C} then $I = J$.

PROOF: Axiom of Extensionality.

□

Chapter 7

Unordered Triples

Definition 7.1 ((Unordered) Triple). Given sets a_1, \dots, a_n , define the (*unordered*) *n*-tuple $\{a_1, \dots, a_n\}$ to be

$$\{a_1, \dots, a_n\} := \{a_1\} \cup \dots \cup \{a_n\} \ .$$

Chapter 8

Relative Complements

Definition 8.1 (Relative Complement). For any sets A and B , the *difference* or *relative complement* $A - B$ is defined to be

$$A - B := \{x \in A : x \notin B\} .$$

Proposition 8.2. For any sets A and E , we have $A \subseteq E$ if and only if

$$E - (E - A) = A$$

PROOF:

$\langle 1 \rangle 1$. LET: A and E be sets.

$\langle 1 \rangle 2$. If $A \subseteq E$ then $E - (E - A) = A$

$\langle 2 \rangle 1$. ASSUME: $A \subseteq E$

$\langle 2 \rangle 2$. $E - (E - A) \subseteq A$

PROOF: If $x \in E$ and $x \notin E - A$ then $x \in A$.

$\langle 2 \rangle 3$. $A \subseteq E - (E - A)$

PROOF: If $x \in A$ then $x \in E$ and $x \notin E - A$.

$\langle 1 \rangle 3$. If $E - (E - A) = A$ then $A \subseteq E$.

PROOF: Since $E - (E - A) \subseteq E$.

□

Proposition 8.3. For any set E we have

$$E - \emptyset = E$$

PROOF: $x \in E$ if and only if $x \in E$ and $x \notin \emptyset$. □

Proposition 8.4. For any set E we have

$$E - E = \emptyset .$$

PROOF: There is no x such that $x \in E$ and $x \notin E$. □

Proposition 8.5. For any sets A and E , we have

$$A \cap (E - A) = \emptyset .$$

PROOF: There is no x such that $x \in A$ and $x \in E - A$. \square

Proposition 8.6. *Let A and E be sets. Then $A \subseteq E$ if and only if*

$$A \cup (E - A) = E .$$

PROOF:

$\langle 1 \rangle 1$. LET: A and E be sets.

$\langle 1 \rangle 2$. If $A \subseteq E$ then $A \cup (E - A) = E$.

$\langle 2 \rangle 1$. ASSUME: $A \subseteq E$

$\langle 2 \rangle 2$. $A \cup (E - A) \subseteq E$

PROOF: If $x \in A$ or $x \in E - A$ then $x \in E$.

$\langle 2 \rangle 3$. $E \subseteq A \cup (E - A)$

PROOF: If $x \in E$ then either $x \in A$ or $x \notin A$. In the latter case, $x \in E - A$.

$\langle 1 \rangle 3$. If $A \cup (E - A) = E$ then $A \subseteq E$

PROOF: Since $A \subseteq A \cup (E - A)$.

\square

Proposition 8.7. *Let A , B and E be sets. Then:*

1. *If $A \subseteq B$ then $E - B \subseteq E - A$.*

2. *If $A \subseteq E$ and $E - B \subseteq E - A$ then $A \subseteq B$.*

PROOF:

$\langle 1 \rangle 1$. LET: A , B and E be sets.

$\langle 1 \rangle 2$. If $A \subseteq B$ then $E - B \subseteq E - A$.

PROOF: If $A \subseteq B$, $x \in E$ and $x \notin B$, then we have $x \in E$ and $x \notin A$.

$\langle 1 \rangle 3$. If $A \subseteq E$ and $E - B \subseteq E - A$ then $A \subseteq B$.

$\langle 2 \rangle 1$. ASSUME: $A \subseteq E$

$\langle 2 \rangle 2$. ASSUME: $E - B \subseteq E - A$

$\langle 2 \rangle 3$. LET: $x \in A$

$\langle 2 \rangle 4$. $x \in E$

$\langle 2 \rangle 5$. $x \notin E - A$

$\langle 2 \rangle 6$. $x \notin E - B$

$\langle 2 \rangle 7$. $x \in B$

\square

Example 8.8. We cannot remove the hypothesis $A \subseteq E$ in item 2 above. Let $E = \emptyset$, $A = \{\emptyset\}$ and $B = \emptyset$. Then $E - B = E - A = \emptyset$ but $A \not\subseteq B$.

Proposition 8.9 (De Morgan's Law). *For any sets A , B and E , we have $E - (A \cup B) = (E - A) \cap (E - B)$.*

PROOF: $(x \in E \wedge \neg(x \in A \vee x \in B)) \Leftrightarrow (x \in E \wedge x \notin A \wedge x \in E \wedge x \notin B)$. \square

Proposition 8.10 (De Morgan's Law). *For any sets A , B and E , we have $E - (A \cap B) = (E - A) \cup (E - B)$.*

PROOF: $(x \in E \vee \neg(x \in A \wedge x \in B)) \Leftrightarrow (x \in E \wedge x \notin A) \vee (x \in E \wedge x \notin B)$. \square

Proposition 8.11. *For any sets A , B and E , if $A \subseteq E$ then*

$$A - B = A \cap (E - B) .$$

PROOF: If $A \subseteq E$ then we have $(x \in A \wedge x \notin B) \Leftrightarrow (x \in A \wedge x \in E \wedge x \notin B)$. \square

Proposition 8.12. *For any sets A and B , we have $A \subseteq B$ if and only if $A - B = \emptyset$.*

PROOF: Both are equivalent to the statement that there is no x such that $x \in A$ and $x \notin B$. \square

Proposition 8.13. *For any sets A and B , we have*

$$A - (A - B) = A \cap B .$$

PROOF: $(x \in A \wedge \neg(x \in A \wedge x \notin B)) \Leftrightarrow x \in A \wedge x \in B$. \square

Proposition 8.14. *For any sets A , B and C , we have*

$$A \cap (B - C) = (A \cap B) - (A \cap C) .$$

PROOF: $(x \in A \wedge x \in B \wedge x \notin C) \Leftrightarrow (x \in A \wedge x \in B \wedge \neg(x \in A \wedge x \in C))$. \square

Proposition 8.15. *For any sets A , B , C and E , if $(A \cap B) - C \subseteq E$ then we have*

$$A \cap B \subseteq (A \cap C) \cup (B \cap (E - C)) .$$

PROOF:

$\langle 1 \rangle 1$. LET: $x \in A \cap B$

PROVE: $x \in (A \cap C) \cup (B \cap (E - C))$

$\langle 1 \rangle 2$. CASE: $x \in C$

PROOF: Then $x \in A \cap C$.

$\langle 1 \rangle 3$. CASE: $x \notin C$

PROOF: Then $x \in E$ and so $x \in B \cap (E - C)$.

\square

Proposition 8.16. *For any sets A , B , C and E , we have*

$$(A \cup C) \cap (B \cup (E - C)) \subseteq A \cup B .$$

PROOF: The statement $(x \in A \vee x \in C) \wedge (x \in B \vee (x \in E \wedge x \notin C))$ implies $x \in A \vee x \in B$. \square

Proposition 8.17 (De Morgan's Law). *Let E be a set and \mathcal{C} a nonempty set. Then*

$$E - \bigcup_{X \in \mathcal{C}} X = \bigcap_{X \in \mathcal{C}} (E - X) .$$

PROOF: Easy. \square

Proposition 8.18 (De Morgan's Law). *Let E be a set and \mathcal{C} a nonempty set. Then*

$$E - \bigcap_{X \in \mathcal{C}} X = \bigcup_{X \in \mathcal{C}} (E - X) .$$

PROOF: Easy. \square

Chapter 9

Symmetric Difference

Definition 9.1 (Symmetric Difference). For any sets A and B , the *symmetric difference* $A + B$ is defined to be

$$A + B := (A - B) \cup (B - A) .$$

Proposition 9.2. For any sets A and B , we have

$$A + B = B + A$$

PROOF: From the commutativity of union. \square

Proposition 9.3. For any sets A , B and C , we have

$$A + (B + C) = (A + B) + C .$$

PROOF: Each is the set of all x that belong to either exactly one or all three of A , B and C . \square

Proposition 9.4. For any set A , we have

$$A + \emptyset = A .$$

PROOF:

$$\begin{aligned} A + \emptyset &= (A - \emptyset) \cup (\emptyset - A) \\ &= A \cup \emptyset \\ &= A \end{aligned}$$

\square

Proposition 9.5. For any set A we have

$$A + A = \emptyset .$$

PROOF:

$$\begin{aligned} A + A &= (A - A) \cup (A - A) \\ &= \emptyset \cup \emptyset \\ &= \emptyset \end{aligned}$$

\square

Chapter 10

Power Sets

Definition 10.1 (Power Set). For any set A , the *power set* of A , $\mathcal{P}A$, is the set whose elements are exactly the subsets of A .

PROOF: This exists by the Power Set Axiom and Axiom of Comprehension, and is unique by the Axiom of Extensionality. \square

Proposition 10.2.

$$\mathcal{P}\emptyset = \{\emptyset\}$$

PROOF: The only subset of \emptyset is \emptyset . \square

Proposition 10.3. For any set a , we have

$$\mathcal{P}\{a\} = \{\emptyset, \{a\}\} .$$

PROOF: The only subsets of $\{a\}$ are \emptyset and $\{a\}$. \square

Proposition 10.4. For any sets a and b , we have

$$\mathcal{P}\{a, b\} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\} .$$

PROOF: The only subsets of $\{a, b\}$ are \emptyset , $\{a\}$, $\{b\}$ and $\{a, b\}$. \square

Proposition 10.5. For any nonempty set \mathcal{C} we have

$$\bigcap_{X \in \mathcal{C}} \mathcal{P}X = \mathcal{P}\left(\bigcap \mathcal{C}\right) .$$

PROOF:

$$x \in \bigcup_{X \in \mathcal{C}} \mathcal{P}X \Leftrightarrow \forall X \in \mathcal{C}. x \subseteq X$$

$$\Leftrightarrow \forall X \in \mathcal{C}. \forall y \in x. y \in X$$

$$\Leftrightarrow \forall y \in x. \forall X \in \mathcal{C}. y \in X$$

$$\Leftrightarrow x \subseteq \bigcap \mathcal{C}$$

\square

Proposition 10.6. *For any set \mathcal{C} we have*

$$\bigcup_{X \in \mathcal{C}} \mathcal{P}X \subseteq \mathcal{P} \bigcup \mathcal{C} .$$

PROOF: If there exists $X \in \mathcal{C}$ such that $x \subseteq X$ then $x \subseteq \bigcup \mathcal{C}$. \square

Proposition 10.7. *For any set E , we have*

$$\bigcap \mathcal{P}E = \emptyset .$$

PROOF: Since $\emptyset \in \mathcal{P}E$. \square

Proposition 10.8. *For any sets E and F , if $E \subseteq F$ then $\mathcal{P}E \subseteq \mathcal{P}F$.*

PROOF: If $E \subseteq F$ and $X \subseteq E$ then $X \subseteq F$. \square

Chapter 11

Ordered Pairs

Definition 11.1 (Ordered Pair). For any sets a and b , the *ordered pair* (a, b) is defined by

$$(a, b) := \{\{a\}, \{a, b\}\} .$$

Proposition 11.2. For any sets a, b, x and y , if $(a, b) = (x, y)$ then $a = x$ and $b = y$.

PROOF:

$\langle 1 \rangle 1$. LET: a, b, x and y be sets.

$\langle 1 \rangle 2$. ASSUME: $(a, b) = (x, y)$

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

PROOF: $\{a\} = \bigcap(a, b) = \bigcap(x, y) = \{x\}$.

$\langle 1 \rangle 4$. $\{a, b\} = \{x, y\}$

$\langle 1 \rangle 5$. CASE: $a = b$

$\langle 2 \rangle 1$. $x = y$

PROOF: Since $\{x, y\} = \{a, b\}$ is a singleton.

$\langle 2 \rangle 2$. $b = y$

PROOF: $b = a = x = y$

$\langle 1 \rangle 6$. CASE: $a \neq b$

$\langle 2 \rangle 1$. $x \neq y$

PROOF: Since $\{x, y\} = \{a, b\}$ is not a singleton.

$\langle 2 \rangle 2$. $b = y$

PROOF: $\{b\} = \{a, b\} - \{a\} = \{x, y\} - \{x\} = \{y\}$.

□

Definition 11.3 (Cartesian Product). For any sets A and B , the *Cartesian product* $A \times B$ is

$$A \times B := \{p \in \mathcal{PP}(A \cup B) : \exists a \in A. \exists b \in B. p = (a, b)\} .$$

Proposition 11.4. For any sets A, B and X , we have

$$(A - B) \times X = (A \times X) - (B \times X) .$$

PROOF: Easy. \square

Proposition 11.5. *For any sets A and B , we have $A \times B = \emptyset$ if and only if $A = \emptyset$ or $B = \emptyset$.*

PROOF: Easy. \square

Proposition 11.6. *For any sets A , B , X and Y , if $A \subseteq X$ and $B \subseteq Y$ then $A \times B \subseteq X \times Y$. The converse holds assuming $A \neq \emptyset$ and $B \neq \emptyset$.*

PROOF: Easy. \square

Chapter 12

Relations

Definition 12.1 (Relation). A *relation* is a set of ordered pairs.

If R is a relation, we write xRy for $(x, y) \in R$.

Given sets X and Y , a relation *between X and Y* is a subset of $X \times Y$.

Given a set X , a relation *on X* is a relation between X and X .

Definition 12.2 (Domain). The *domain* of a relation R is the set

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

Definition 12.3 (Range). The *range* of a relation R is the set

$$\text{ran } R := \{y \in \bigcup \bigcup R : \exists x. (x, y) \in R\} .$$

Definition 12.4 (Reflexive). Let R be a relation on X . Then R is *reflexive* iff, for all $x \in X$, we have xRx .

Definition 12.5 (Symmetric). Let R be a relation on X . Then R is *symmetric* iff, whenever xRy , then yRx .

Definition 12.6 (Transitive). Let R be a relation on X . Then R is *transitive* iff, whenever xRy and yRz , then xRz .

Definition 12.7 (Equivalence Relation). Let R be a relation on X . Then R is an *equivalence relation* iff it is reflexive, symmetric and transitive.

Definition 12.8 (Partition). Let X be a set. A *partition* of X is a pairwise disjoint set of nonempty subsets of X whose union is X .

Definition 12.9 (Equivalence Class). Let R be an equivalence relation on X . Let $x \in X$. The *equivalence class* of x with respect to R is

$$x/R := \{y \in X : xRy\} .$$

We write X/R for the set of all equivalence classes with respect to R .

Definition 12.10 (Induced). Let P be a partition of X . The relation *induced* by P is X/P where $x(X/P)y$ iff there exists $X \in P$ such that $x \in X$ and $y \in X$.

Theorem 12.11. Let R be an equivalence relation on X . Then X/R is a partition of X that induces the relation R .

PROOF: Easy. \square

Theorem 12.12. Let P be a partition of X . Then X/P is an equivalence relation on X , and $P = X/(X/P)$.

PROOF: Easy. \square

Definition 12.13 (Composition). Let R be a relation between X and Y , and S a relation between Y and Z . The *composite* or *relative product* $S \circ R = SR$ is the relation between X and Z defined by

$$x(S \circ R)z \Leftrightarrow \exists y \in Y (xRy \wedge ySz) .$$

Proposition 12.14. Let R be a relation between X and Y , S a relation between Y and Z , and T a relation between Z and W . Then

$$T(SR) = (TS)R .$$

PROOF: Easy. \square

Example 12.15. Composition of relations is not commutative in general. Let $X = \{a, b\}$ where $a \neq b$. Let $R = \{(a, a), (b, a)\}$ and $S = \{(a, b), (b, b)\}$. Then $SR = S$ but $RS = R \neq S$.

Proposition 12.16. A relation R is transitive if and only if $RR \subseteq R$.

PROOF: Easy. \square

Definition 12.17 (Inverse). Let R be a relation between X and Y . The *inverse* or *converse* R^{-1} is the relation between Y and X defined by

$$yR^{-1}x \Leftrightarrow xRy .$$

Proposition 12.18. For any relation R , we have

$$\text{dom } R^{-1} = \text{ran } R .$$

PROOF: Easy. \square

Proposition 12.19. For any relation R , we have

$$\text{ran } R^{-1} = \text{dom } R .$$

PROOF: Easy. \square

Proposition 12.20. *Let R be a relation between X and Y , and S a relation between Y and Z . Then*

$$(SR)^{-1} = R^{-1}S^{-1} .$$

PROOF: Easy. \square

Proposition 12.21. *A relation R is symmetric if and only if $R \subseteq R^{-1}$.*

PROOF: Easy. \square

Definition 12.22 (Identity Relation). For any set X , the *identity relation* I_X on X is

$$I_X = \{(x, x) : x \in X\} .$$

Proposition 12.23. *Let R be a relation between X and Y . Then*

$$I_Y R = R I_X = R .$$

PROOF: Easy. \square

Proposition 12.24. *A relation R on a set X is reflexive if and only if $I_X \subseteq R$.*

PROOF: Easy. \square

Chapter 13

Functions

Definition 13.1 (Function). Let X and Y be sets. A *function*, *map*, *mapping*, *transformation* or *operator* f from X to Y , $f : X \rightarrow Y$, is a relation f between X and Y such that, for all $x \in X$, there exists a unique $f(x) \in Y$, called the *value* of f at the *argument* x , such that $(x, f(x)) \in f$.

Definition 13.2 (Onto). Let $f : X \rightarrow Y$. We say f maps X *onto* Y iff $\text{ran } f = Y$.

Definition 13.3 (Image). Let $f : X \rightarrow Y$ and $A \subseteq X$. The *image* of A under f is

$$f(A) := \{f(x) : x \in A\} .$$

Definition 13.4 (Inclusion Map). Let Y be a set and $X \subseteq Y$. Then the *inclusion map* $i : X \hookrightarrow Y$ is the function defined by $i(x) = x$ for all $x \in X$.

Proposition 13.5. *For any set X , the identity relation I_X is a function $X \rightarrow X$.*

PROOF: Easy. \square

Definition 13.6 (Restriction). Let $f : Y \rightarrow Z$ and $X \subseteq Y$. The *restriction* of f to X is the function $f \upharpoonright X : X \rightarrow Z$ defined by

$$(f \upharpoonright X)(x) = f(x) \quad (x \in X) .$$

Given sets X , Y and Z with $X \subseteq Y$, if $f : X \rightarrow Z$ and $g : Y \rightarrow Z$, we say g is an *extension* of f to Y iff $f = g \upharpoonright X$.

Definition 13.7 (Projection). Given sets X and Y , the *projection* maps $\pi_1 : X \times Y \rightarrow X$ and $\pi_2 : X \times Y \rightarrow Y$ are defined by

$$\pi_1(x, y) = x, \quad \pi_2(x, y) = y \quad (x \in X, y \in Y) .$$

Definition 13.8 (Canonical Map). Let X be a set and R an equivalence relation on X . The *canonical map* $\pi : X \rightarrow X/R$ is the map defined by $\pi(x) = x/R$.

Definition 13.9 (One-to-One). A function $f : X \rightarrow Y$ is *one-to-one*, or a *one-to-one correspondence*, iff, for all $x, y \in X$, if $f(x) = f(y)$ then $x = y$.

Proposition 13.10. Let $f : X \rightarrow Y$. Then the following are equivalent:

1. f is one-to-one.
2. For all $A, B \subseteq X$, we have $f(A \cap B) = f(A) \cap f(B)$.
3. For all $A \subseteq X$, we have $f(X - A) \subseteq Y - f(A)$.

PROOF: Easy. \square

Proposition 13.11. Let $f : X \rightarrow Y$. Then f maps X onto Y if and only if, for all $A \subseteq X$, we have $Y - f(A) \subseteq f(X - A)$.

PROOF: Easy. \square

Chapter 14

Families

Definition 14.1 (Family). Let I and X be sets. A *family* of elements of X indexed by I is a function $a : I \rightarrow X$. We write a_i for $a(i)$, and $\{a_i\}_{i \in I}$ for a .

Proposition 14.2 (Generalized Associative Law for Unions). Let $\{I_j\}_{j \in J}$ be a family of sets. Let $K = \bigcup_{j \in J} I_j$. Let $\{A_k\}_{k \in K}$ be a family of sets indexed by K . Then

$$\bigcup_{k \in K} A_k = \bigcup_{j \in J} \bigcup_{i \in I_j} A_i .$$

PROOF: Easy. \square

Proposition 14.3 (Generalized Commutative Law for Unions). Let $\{I_j\}_{j \in J}$ be a family of sets. Let $f : J \rightarrow J$ be a one-to-one correspondence from J onto J . Then

$$\bigcup_{j \in J} I_j = \bigcup_{j \in J} I_{f(j)} .$$

PROOF: Easy. \square

Proposition 14.4 (Generalized Associative Law for Intersections). Let $\{I_j\}_{j \in J}$ be a nonempty family of nonempty sets. Let $K = \bigcup_{j \in J} I_j$. Let $\{A_k\}_{k \in K}$ be a family of sets indexed by K . Then

$$\bigcap_{k \in K} A_k = \bigcap_{j \in J} \bigcap_{i \in I_j} A_i .$$

PROOF: Easy. \square

Proposition 14.5 (Generalized Commutative Law for Intersections). Let $\{I_j\}_{j \in J}$ be a nonempty family of sets. Let $f : J \rightarrow J$ be a one-to-one correspondence from J onto J . Then

$$\bigcap_{j \in J} I_j = \bigcap_{j \in J} I_{f(j)} .$$

PROOF: Easy. \square

Proposition 14.6. *Let B be a set and $\{A_i\}_{i \in I}$ a family of sets. Then*

$$B \cap \bigcup_{i \in I} A_i = \bigcup_{i \in I} (B \cap A_i)$$

PROOF: Easy. \square

Proposition 14.7. *Let B be a set and $\{A_i\}_{i \in I}$ a nonempty family of sets. Then*

$$B \cup \bigcap_{i \in I} A_i = \bigcap_{i \in I} (B \cup A_i)$$

PROOF: Easy. \square

Definition 14.8 (Cartesian Product of a Family of Sets). Let $\{A_i\}_{i \in I}$ be a family of sets. The *Cartesian product* $\times_{i \in I} A_i$ is the set of all families $\{a_i\}_{i \in I}$ such that $\forall i \in I. a_i \in A_i$.

We write A^I for $\times_{i \in I} A$.

Definition 14.9 (Projection). Let $\{A_i\}_{i \in I}$ be a family of sets and $i \in I$. The *projection* function $\pi_i : \times_{i \in I} A_i \rightarrow A_i$ is defined by $\pi_i(a) = a_i$.

Proposition 14.10. *Let $\{A_i\}_{i \in I}$ and $\{B_j\}_{j \in J}$ be families of sets. Then*

$$\left(\bigcup_{i \in I} A_i \right) \times \left(\bigcup_{j \in J} B_j \right) = \bigcup_{i \in I} \bigcup_{j \in J} (A_i \times B_j) .$$

PROOF: Easy. \square

Proposition 14.11. *Let $\{A_i\}_{i \in I}$ and $\{B_j\}_{j \in J}$ be nonempty families of sets. Then*

$$\left(\bigcap_{i \in I} A_i \right) \times \left(\bigcap_{j \in J} B_j \right) = \bigcap_{i \in I} \bigcap_{j \in J} (A_i \times B_j) .$$

PROOF: Easy. \square

Proposition 14.12. *Let $f : X \rightarrow Y$. Let $\{A_i\}_{i \in I}$ be a family of subsets of X . Then*

$$f \left(\bigcup_{i \in I} A_i \right) = \bigcup_{i \in I} f(A_i) .$$

PROOF: Easy. \square

Example 14.13. It is not true in general that, if $f : X \rightarrow Y$ and $\{A_i\}_{i \in I}$ is a nonempty family of subsets of X , then $f(\bigcap_{i \in I} A_i) = \bigcap_{i \in I} f(A_i)$.

Take $X = \{a, b\}$ and $Y = \{c\}$ where $a \neq b$. Take $I = \{i, j\}$ with $i \neq j$. Let $A_i = \{a\}$ and $A_j = \{b\}$. Let f be the unique function $X \rightarrow Y$. Then $f(\bigcap_{i \in I} A_i) = f(\emptyset) = \emptyset$ but $\bigcap_{i \in I} f(A_i) = \{c\}$.

Chapter 15

Inverses and Composites

Definition 15.1 (Inverse). Given a function $f : X \rightarrow Y$, the *inverse* of f is the function $f^{-1} : \mathcal{P}Y \rightarrow \mathcal{P}X$ defined by

$$f^{-1}(B) = \{x \in X : f(x) \in B\} \ .$$

We call $f^{-1}(B)$ the *inverse image* of B under f .

Proposition 15.2. *Let $f : X \rightarrow Y$. Then f maps X onto Y if and only if the inverse image of any nonempty subset of Y is nonempty.*

PROOF: Easy. \square

Proposition 15.3. *Let $f : X \rightarrow Y$. Then f is one-to-one if and only if the inverse image of any singleton subset of Y is a singleton.*

PROOF: Easy. \square

Proposition 15.4. *Let $f : X \rightarrow Y$. Let $B \subseteq Y$. Then*

$$f(f^{-1}(B)) \subseteq B \ .$$

PROOF: Easy. \square

Proposition 15.5. *Let $f : X \rightarrow Y$. Let $A \subseteq X$. Then*

$$A \subseteq f^{-1}(f(A)) \ .$$

Equality holds if f is one-to-one.

PROOF: Easy. \square

Proposition 15.6. *Let $f : X \rightarrow Y$. Let $\{B_i\}_{i \in I}$ be a family of subsets of Y . Then*

$$f^{-1}\left(\bigcup_{i \in I} B_i\right) = \bigcup_{i \in I} f^{-1}(B_i) \ .$$

PROOF: Easy. \square

Proposition 15.7. *Let $f : X \rightarrow Y$. Let $\{B_i\}_{i \in I}$ be a nonempty family of subsets of Y . Then*

$$f^{-1} \left(\bigcap_{i \in I} B_i \right) = \bigcap_{i \in I} f^{-1}(B_i) .$$

PROOF: Easy. \square

Proposition 15.8. *Let $f : X \rightarrow Y$ and $B \subseteq Y$. Then $f^{-1}(Y - B) = X - f^{-1}(B)$.*

PROOF: Easy. \square

Proposition 15.9. *Let $f : X \rightarrow Y$ be one-to-one. Then the inverse of f as a relation, f^{-1} , is a function $f^{-1} : \text{ran } f \rightarrow X$, and for all $y \in \text{ran } f$, we have $f^{-1}(y)$ is the unique x such that $f(x) = y$.*

PROOF: Easy. \square

Proposition 15.10. *Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$. Then $gf : X \rightarrow Z$ and, for all $x \in X$, we have*

$$(g \circ f)(x) = g(f(x)) .$$

PROOF: Easy. \square

Example 15.11. Example 12.15 shows that function composition is not commutative in general.

Proposition 15.12. *Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$. Then*

$$(gf)^{-1} = f^{-1}g^{-1} : \mathcal{P}Z \rightarrow \mathcal{P}X .$$

PROOF: Easy. \square

Proposition 15.13. *Let $f : X \rightarrow Y$ and $g : Y \rightarrow X$. If $gf = I_X$ then f is one-to-one and g maps Y onto X .*

PROOF: Easy. \square

Chapter 16

Numbers

Definition 16.1 (Successor). The *successor* of a set x , x^+ , is defined by

$$x^+ := x \cup \{x\} .$$

Definition 16.2. We define

$$0 = \emptyset$$

$$1 = 0^+$$

$$2 = 1^+$$

etc.

Definition 16.3 (Characteristic Function). Let X be a set and $A \subseteq X$. The *characteristic function* of A is the function $\chi_A : X \rightarrow 2$ defined by

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

Theorem 16.4. Let X be a set. The function $\chi : \mathcal{P}X \rightarrow 2^X$ that maps a subset A of X to χ_A is a one-to-one correspondence.

PROOF: Easy. \square

Definition 16.5. The set ω of *natural numbers* is the set such that:

- $0 \in \omega$
- For all $n \in \omega$ we have $n^+ \in \omega$
- For any set X , if $0 \in X$ and $\forall n \in X. n^+ \in X$ then $\omega \subseteq X$

PROOF: To show this exists, pick a set A such that $0 \in A$ and $\forall n \in A. n^+ \in A$ (by the Axiom of Infinity), and let $\omega = \bigcap \{X \in \mathcal{P}A : 0 \in X \wedge \forall n \in X. n^+ \in X\}$.
 \square

Definition 16.6 (Sequence). A *finite sequence* is a family whose index set is a natural number. An *infinite sequence* is a family whose index set is ω .

Given a finite sequence of sets $\{A_i\}_{i \in n^+}$, we write $\bigcup_{i=0}^n A_i$ for $\bigcup_{i \in n^+} A_i$. Given an infinite sequence of sets $\{A_i\}_{i \in \omega}$, we write $\bigcup_{i=0}^{\infty} A_i$ for $\bigcup_{i \in \omega} A_i$.

We make similar definitions for \bigcap and \times .

Chapter 17

The Peano Axioms

Theorem 17.1 (Principle of Mathematical Induction). *For any subset S of ω , if $0 \in S$ and $\forall n \in S. n^+ \in S$, then $S = \omega$.*

PROOF: From the definition of ω . \square

Proposition 17.2.

$$\forall n \in \omega. \forall x \in n. n \not\subseteq x$$

PROOF:

$\langle 1 \rangle 1.$ $\forall x \in 0. 0 \not\subseteq x$

PROOF: Vacuous.

$\langle 1 \rangle 2.$ For any natural number n , if $\forall x \in n. n \not\subseteq x$ then $\forall x \in n^+. n^+ \not\subseteq x$.

$\langle 2 \rangle 1.$ LET: n be a natural number.

$\langle 2 \rangle 2.$ ASSUME: $\forall x \in n. n \not\subseteq x$

$\langle 2 \rangle 3.$ LET: $x \in n^+$

$\langle 2 \rangle 4.$ ASSUME: for a contradiction $n^+ \subseteq x$

$\langle 2 \rangle 5.$ $x \in n$ or $x = n$

$\langle 2 \rangle 6.$ CASE: $x \in n$

PROOF: Then we have $n \subseteq n^+ \subseteq x$ contradicting $\langle 2 \rangle 2$.

$\langle 2 \rangle 7.$ CASE: $x = n$

PROOF: Then we have $n \in n^+ \subseteq x = n$ and $n \subseteq n$ contradicting $\langle 2 \rangle 2$.

\square

Corollary 17.2.1. *For any natural number n we have $n \notin n$.*

Corollary 17.2.2. *For any natural number n we have $n \neq n^+$.*

Definition 17.3 (Transitive Set). A set E is a *transitive* set iff, whenever $x \in y \in E$, then $x \in E$.

Proposition 17.4. *Every natural number is a transitive set.*

PROOF:

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

PROOF: Vacuously, if $x \in y \in 0$ then $x \in 0$.

$\langle 1 \rangle 2$. 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.

$\langle 2 \rangle 2$. ASSUME: n is a transitive set.

$\langle 2 \rangle 3$. LET: $x \in y \in n^+$

$\langle 2 \rangle 4$. $y \in n$ or $y = n$

$\langle 2 \rangle 5$. CASE: $y \in n$

$\langle 3 \rangle 1$. $x \in n$

PROOF: $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 5$.

$\langle 3 \rangle 2$. $x \in n^+$

$\langle 2 \rangle 6$. CASE: $y = n$

$\langle 3 \rangle 1$. $x \in n$

PROOF: $\langle 2 \rangle 3$, $\langle 2 \rangle 6$

$\langle 3 \rangle 2$. $x \in n^+$

□

Proposition 17.5. *For any natural numbers m and n , if $m^+ = n^+$ then $m = n$.*

PROOF:

$\langle 1 \rangle 1$. LET: m and n be natural numbers.

$\langle 1 \rangle 2$. ASSUME: $m^+ = n^+$

$\langle 1 \rangle 3$. $m \in m^+ = n^+$

$\langle 1 \rangle 4$. $m \in n$ or $m = n$

$\langle 1 \rangle 5$. $n \in n^+ = m^+$

$\langle 1 \rangle 6$. $n \in m$ or $n = m$

$\langle 1 \rangle 7$. We cannot have $m \in n$ and $n \in m$

$\langle 2 \rangle 1$. ASSUME: for a contradiction $m \in n$ and $n \in m$

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

PROOF: Since m is a transitive set (Proposition 17.4).

$\langle 2 \rangle 3$. Q.E.D.

PROOF: This contradicts Proposition 17.2.

$\langle 1 \rangle 8$. $m = n$

□

Theorem 17.6 (Recursion Theorem). *Let X be a set. Let $a \in X$. Let $f : X \rightarrow X$. There exists a function $u : \omega \rightarrow X$ such that $u(0) = a$ and, for all $n \in \omega$, we have $u(n^+) = f(u(n))$.*

PROOF:

$\langle 1 \rangle 1$. LET: $\mathcal{C} = \{A \in \mathcal{P}(\omega \times X) : (0, a) \in A \wedge \forall n \in \omega. \forall x \in X. (n, x) \in A \Rightarrow (n^+, f(x)) \in A\}$

$\langle 1 \rangle 2$. $\mathcal{C} \neq \emptyset$

PROOF: $\omega \times X \in \mathcal{C}$

$\langle 1 \rangle 3$. LET: $u = \bigcap \mathcal{C}$

$\langle 1 \rangle 4$. $u \in \mathcal{C}$

$\langle 1 \rangle 5$. u is a function.

$\langle 2 \rangle 1$. LET: $P(n)$ be the property: $\forall x, y \in X. (n, x) \in u \wedge (n, y) \in u \Rightarrow x = y$
 $\langle 2 \rangle 2$. $P(0)$
 $\langle 3 \rangle 1$. $\forall x \in X. (0, x) \in u \Rightarrow x = a$
 PROOF: If $(0, x) \in u$ and $x \neq a$ then $u - \{(0, x)\} \in \mathcal{C}$ and so $u - \{(0, x)\} \subseteq u$, which is impossible.
 $\langle 2 \rangle 3$. For every natural number n , if $P(n)$ then $P(n^+)$.
 $\langle 3 \rangle 1$. LET: n be a natural number.
 $\langle 3 \rangle 2$. ASSUME: $P(n)$
 $\langle 3 \rangle 3$. LET: $x, y \in X$
 $\langle 3 \rangle 4$. ASSUME: $(n^+, x), (n^+, y) \in u$
 $\langle 3 \rangle 5$. PICK $x', y' \in X$ such that $(n, x') \in u, (n, y') \in u$ and $f(x') = x$ and $f(y') = y$
 PROOF: If no such x' exists then $u - \{(n^+, x)\} \in \mathcal{C}$ and so $u - \{(n^+, x)\} \subseteq u$ which is impossible. Similarly for y' .
 $\langle 3 \rangle 6$. $x' = y'$
 PROOF: $\langle 3 \rangle 2$
 $\langle 3 \rangle 7$. $x = y$

□

Proposition 17.7. *For any natural number n , either $n = 0$ or there exists a natural number m such that $n = m^+$.*

PROOF: Easy induction on n . □

Proposition 17.8. *ω is a transitive set.*

PROOF:

$\langle 1 \rangle 1$. LET: $P(n)$ be the property $\forall x \in n. x \in \omega$
 $\langle 1 \rangle 2$. $P(0)$
 PROOF: Vacuous.
 $\langle 1 \rangle 3$. For any natural number n , if $P(n)$ then $P(n^+)$.
 $\langle 2 \rangle 1$. LET: n be a natural number.
 $\langle 2 \rangle 2$. ASSUME: $P(n)$
 $\langle 2 \rangle 3$. LET: $x \in n^+$
 $\langle 2 \rangle 4$. $x \in n$ or $x = n$
 $\langle 2 \rangle 5$. CASE: $x \in n$
 PROOF: Then $x \in \omega$ by $\langle 2 \rangle 2$.
 $\langle 2 \rangle 6$. CASE: $x = n$
 PROOF: Then $x \in \omega$ by $\langle 2 \rangle 1$.

□

Proposition 17.9. *For any natural number n and any nonempty subset $E \subseteq n$, there exists $k \in E$ such that $\forall m \in E. k = m \vee k \in m$.*

PROOF:

$\langle 1 \rangle 1$. LET: $P(n)$ be the property: for any nonempty subset $E \subseteq n$, there exists $k \in E$ such that $\forall m \in E. k = m \vee k \in m$
 $\langle 1 \rangle 2$. $P(0)$

PROOF: Vacuous as there is no nonempty subset of 0.

$\langle 1 \rangle 3$. For any natural number n , if $P(n)$ then $P(n^+)$.

$\langle 2 \rangle 1$. LET: n be a natural number.

$\langle 2 \rangle 2$. ASSUME: $P(n)$

$\langle 2 \rangle 3$. LET: E be a nonempty subset of n^+

$\langle 2 \rangle 4$. CASE: $E - \{n\} = \emptyset$
PROOF: Then $E = \{n\}$ so take $k = n$.

$\langle 2 \rangle 5$. CASE: $E - \{n\} \neq \emptyset$

$\langle 3 \rangle 1$. PICK $k \in E - \{n\}$ such that $\forall m \in E - \{n\}. k = m \vee k \in m$
PROOF: By $\langle 2 \rangle 2$.

$\langle 3 \rangle 2$. $\forall m \in E. k = m \vee k \in m$
PROOF: Since $k \in n$.

□

Chapter 18

Arithmetic

Definition 18.1 (Addition). Define *addition* $+$ on ω by recursion thus:

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

Proposition 18.2. *For all $m, n, p \in \omega$ we have*

$$m + (n + p) = (m + n) + p .$$

PROOF:

$\langle 1 \rangle 1$. LET: $P(p)$ be the property $\forall m, n \in \omega. m + (n + p) = (m + n) + p$

$\langle 1 \rangle 2$. $P(0)$

PROOF: $m + (n + 0) = m + n = (m + n) + 0$.

$\langle 1 \rangle 3$. $\forall p \in \omega. P(p) \Rightarrow P(p^+)$

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

$\langle 2 \rangle 2$. ASSUME: $P(p)$

$\langle 2 \rangle 3$. LET: $m, n \in \omega$

$\langle 2 \rangle 4$. $m + (n + p^+) = (m + n) + p^+$

PROOF:

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

□

Proposition 18.3. *For all $m, n \in \omega$, we have*

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

PROOF:

$\langle 1 \rangle 1$. LET: $P(m)$ be the property $\forall n \in \omega. m + n = n + m$

$\langle 1 \rangle 2. P(0)$
 $\langle 2 \rangle 1. \text{ LET: } Q(n) \text{ be the property } 0 + n = n + 0$
 $\langle 2 \rangle 2. Q(0)$
 PROOF: Trivial.
 $\langle 2 \rangle 3. \forall n \in \omega. Q(n) \Rightarrow Q(n^+)$
 $\langle 3 \rangle 1. \text{ LET: } n \in \omega$
 $\langle 3 \rangle 2. \text{ ASSUME: } Q(n)$
 $\langle 3 \rangle 3. 0 + n^+ = n^+ + 0$
 PROOF:

$$\begin{aligned}
 0 + n^+ &= (0 + n)^+ \\
 &= (n + 0)^+ & (\langle 3 \rangle 2) \\
 &= n^+ \\
 &= n^+ + 0
 \end{aligned}$$

$\langle 1 \rangle 3. \forall m \in \omega. P(m) \Rightarrow P(m^+)$
 $\langle 2 \rangle 1. \text{ LET: } m \in \omega$
 $\langle 2 \rangle 2. \text{ ASSUME: } P(m)$
 $\langle 2 \rangle 3. \text{ LET: } Q(n) \text{ be the property } m^+ + n = n + m^+$
 $\langle 2 \rangle 4. Q(0)$
 PROOF: $\langle 1 \rangle 2$
 $\langle 2 \rangle 5. \forall n \in \omega. Q(n) \Rightarrow Q(n^+)$
 $\langle 3 \rangle 1. \text{ LET: } n \in \omega$
 $\langle 3 \rangle 2. \text{ ASSUME: } Q(n)$
 $\langle 3 \rangle 3. Q(n^+)$
 PROOF:

$$\begin{aligned}
 m^+ + n^+ &= (m^+ + n)^+ \\
 &= (n + m^+)^+ & (\langle 3 \rangle 2) \\
 &= (n + m)^{++} \\
 &= (m + n)^{++} & (\langle 2 \rangle 2) \\
 &= (m + n^+)^+ \\
 &= (n^+ + m)^+ & (\langle 2 \rangle 2) \\
 &= n^+ + m^+
 \end{aligned}$$

□

Definition 18.4 (Multiplication). Define *multiplication* \cdot on ω by

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

Proposition 18.5. For all $m, n, p \in \omega$, we have

$$m(n + p) = mn + mp .$$

PROOF:

$\langle 1 \rangle 1. \text{ LET: } P(p) \text{ be the statement } \forall m, n \in \omega. m(n + p) = mn + mp$

⟨1⟩2. $P(0)$

PROOF:

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

⟨1⟩3. $\forall p \in \omega. P(p) \Rightarrow P(p^+)$

⟨2⟩1. LET: $p \in \omega$

⟨2⟩2. ASSUME: $P(p)$

⟨2⟩3. LET: $m, n \in \omega$

⟨2⟩4. $m(n+p^+) = mn + mp^+$

PROOF:

$$\begin{aligned} m(n+p^+) &= m(n+p)^+ \\ &= m(n+p) + m \\ &= (mn+mp) + m && (\langle 2 \rangle 2) \\ &= mn + (mp+m) && (\text{Proposition 18.2}) \\ &= mn + mp^+ \end{aligned}$$

□

Proposition 18.6. *For all $m, n, p \in \omega$ we have*

$$m(np) = (mn)p .$$

PROOF:

⟨1⟩1. LET: $P(p)$ be the statement $\forall m, n \in \omega. m(np) = (mn)p$

⟨1⟩2. $P(0)$

PROOF:

$$\begin{aligned} m(n0) &= m0 \\ &= 0 \\ &= (mn)0 \end{aligned}$$

⟨1⟩3. $\forall p \in \omega. P(p) \Rightarrow P(p^+)$

⟨2⟩1. LET: $p \in \omega$

⟨2⟩2. ASSUME: $P(p)$

⟨2⟩3. LET: $m, n \in \omega$

⟨2⟩4. $m(np^+) = (mn)p^+$

PROOF:

$$\begin{aligned} m(np^+) &= m(np+n) \\ &= m(np) + mn && (\text{Proposition 18.5}) \\ &= (mn)p + mn && (\langle 2 \rangle 2) \\ &= (mn)p^+ \end{aligned}$$

□

Proposition 18.7. *For all $m, n \in \omega$, we have*

$$mn = nm .$$

PROOF:

$\langle 1 \rangle 1$. LET: $P(m)$ be the statement $\forall n \in \omega. mn = nm$

$\langle 1 \rangle 2$. $P(0)$

$\langle 2 \rangle 1$. LET: $Q(n)$ be the statement $0n = n0$

$\langle 2 \rangle 2$. $Q(0)$

PROOF: Trivial.

$\langle 2 \rangle 3$. $\forall n \in \omega. Q(n) \Rightarrow Q(n^+)$

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

$\langle 3 \rangle 2$. ASSUME: $Q(n)$

$\langle 3 \rangle 3$. $Q(n^+)$

PROOF:

$$\begin{aligned}
 0n^+ &= 0n + 0 \\
 &= 0n \\
 &= n0 & (\langle 3 \rangle 2) \\
 &= 0 \\
 &= n^+0
 \end{aligned}$$

$\langle 1 \rangle 3$. $\forall m \in \omega. P(m) \Rightarrow P(m^+)$

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

$\langle 2 \rangle 2$. ASSUME: $P(m)$

$\langle 2 \rangle 3$. LET: $Q(n)$ be the statement $m^+n = nm^+$

$\langle 2 \rangle 4$. $Q(0)$

PROOF: $\langle 1 \rangle 2$

$\langle 2 \rangle 5$. $\forall n \in \omega. Q(n) \Rightarrow Q(n^+)$

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

$\langle 3 \rangle 2$. ASSUME: $Q(n)$

$\langle 3 \rangle 3$. $Q(n^+)$

PROOF:

$$\begin{aligned}
 m^+n^+ &= m^+n + m^+ \\
 &= (m^+n + m)^+ \\
 &= (nm^+ + m)^+ & (\langle 3 \rangle 2) \\
 &= (nm + n + m)^+ \\
 &= (mn + m + n)^+ & (\langle 2 \rangle 2, \text{Proposition 18.2, Proposition 18.3}) \\
 &= (mn^+ + n)^+ \\
 &= (n^+m + n)^+ & (\langle 2 \rangle 2) \\
 &= n^+m + n^+ \\
 &= n^+m^+
 \end{aligned}$$

□

Definition 18.8 (Exponentiation). Define *exponentiation* on ω by recursion:

$$\begin{aligned}
 m^0 &= 1 \\
 m^{n^+} &= m^n m
 \end{aligned}$$

Proposition 18.9. *For all $m, n, p \in \omega$ we have*

$$m^{n+p} = m^n m^p .$$

PROOF:

$$\langle 1 \rangle 1. m^{n+0} = m^n m^0$$

PROOF:

$$\begin{aligned} m^{n+0} &= m^n \\ &= m^n 1 \\ &= m^n m^0 \end{aligned}$$

$$\langle 1 \rangle 2. \text{ If } m^{n+p} = m^n m^p \text{ then } m^{n+p^+} = m^n m^{p^+}$$

PROOF:

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

□

Proposition 18.10. *For all $m, n, p \in \omega$ we have*

$$(m^n)^p = m^{np} .$$

PROOF:

$$\langle 1 \rangle 1. (m^n)^0 = m^{n0}$$

PROOF: Both are equal to 1.

$$\langle 1 \rangle 2. \text{ If } (m^n)^p = m^{np} \text{ then } (m^n)^{p^+} = m^{np^+}$$

PROOF:

$$\begin{aligned} (m^n)^{p^+} &= (m^n)^p m^n \\ &= m^{np} m^n \\ &= m^{np+n} && \text{(Proposition 18.9)} \\ &= m^{np^+} \end{aligned}$$

□

Proposition 18.11. *For any natural numbers m and n , if $m \in n$ then $m^+ \in n^+$.*

PROOF:

$$\langle 1 \rangle 1. \text{ LET: } P(n) \text{ be the property } \forall m \in n. m^+ \in n^+$$

$$\langle 1 \rangle 2. P(0)$$

PROOF: Vacuous.

$$\langle 1 \rangle 3. \text{ For any natural number } n, \text{ if } P(n) \text{ then } P(n^+).$$

$$\langle 2 \rangle 1. \text{ LET: } n \text{ be a natural number.}$$

$$\langle 2 \rangle 2. \text{ ASSUME: } P(n)$$

$$\langle 2 \rangle 3. \text{ LET: } m \in n^+$$

$$\langle 2 \rangle 4. m \in n \text{ or } m = n$$

$$\langle 2 \rangle 5. m^+ \in n^+ \text{ or } m^+ = n^+$$

PROOF: $\langle 2 \rangle 2$

□ $\langle 2 \rangle 6$. CASE: $m^+ \in n^{++}$

Proposition 18.12. *For any natural numbers m and n , either $m \in n$ or $m = n$ or $n \in m$.*

PROOF:

$\langle 1 \rangle 1$. LET: $P(n)$ be the property: for all $m \in \omega$, either $m \in n$ or $m = n$ or $n \in m$

$\langle 1 \rangle 2$. $P(0)$

$\langle 2 \rangle 1$. LET: $Q(m)$ be the property: either $m = 0$ or $0 \in m$

$\langle 2 \rangle 2$. $Q(0)$

PROOF: Since $0 = 0$.

$\langle 2 \rangle 3$. For all $m \in \omega$, if $Q(m)$ then $Q(m^+)$

PROOF: If $m = 0$ or $0 \in m$ then $0 \in m^+$.

$\langle 1 \rangle 3$. For any natural number n , if $P(n)$ then $P(n^+)$

$\langle 2 \rangle 1$. LET: n be a natural number.

$\langle 2 \rangle 2$. ASSUME: $P(n)$

$\langle 2 \rangle 3$. LET: $m \in \omega$

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

PROOF: $\langle 2 \rangle 2$

$\langle 2 \rangle 5$. CASE: $m \in n$ or $m = n$

PROOF: Then $m \in n^+$.

$\langle 2 \rangle 6$. CASE: $n \in m$

$\langle 3 \rangle 1$. PICK p such that $m = p^+$

$\langle 3 \rangle 2$. $n \in p$ or $n = p$

$\langle 3 \rangle 3$. CASE: $n \in p$

PROOF: Then $n^+ \in p^+ = m$ by Proposition 18.11.

$\langle 3 \rangle 4$. CASE: $n = p$

PROOF: Then $m = n^+$.

□

Corollary 18.12.1 (Trichotomy). *For any natural numbers m and n , exactly one of $m \in n$, $m = n$, $n \in m$ holds.*

PROOF:

$\langle 1 \rangle 1$. We never have $m \in n$ and $m = n$.

PROOF: By Corollary 17.2.1.

$\langle 1 \rangle 2$. We never have $m \in n$ and $n \in m$.

PROOF: Since m is a transitive set this would imply $m \in m$ contradicting Corollary 17.2.1.

$\langle 1 \rangle 3$. We never have $m = n$ and $n \in m$.

PROOF: By Corollary 17.2.1.

□

Proposition 18.13. *For any natural numbers m and n , we have $m \in n$ if and only if $m \subsetneq n$.*

PROOF:

$\langle 1 \rangle 1$. LET: m and n be natural numbers.
 $\langle 1 \rangle 2$. If $m \in n$ then $m \subsetneq n$.
 PROOF: Since n is a transitive set, and $m \neq n$ by Corollary 17.2.1.
 $\langle 1 \rangle 3$. If $m \subsetneq n$ then $m \in n$.
 $\langle 2 \rangle 1$. ASSUME: $m \subsetneq n$
 $\langle 2 \rangle 2$. $n \notin m$
 PROOF: Proposition 17.2.
 $\langle 2 \rangle 3$. $m \neq n$
 $\langle 2 \rangle 4$. $m \in n$
 PROOF: Trichotomy.
 \square

Definition 18.14. Given natural numbers m and n , we write $m < n$ iff $m \in n$.
 We write $m \leq n$ iff $m < n \vee m = n$.

Proposition 18.15. For natural numbers m and n , if $m \leq n$ and $n \leq m$ then $m = n$.

PROOF: We cannot have $m < n$ and $n < m$ by trichotomy. \square

Proposition 18.16. For natural numbers m , n and k , if $m < n$ then $m + k < n + k$.

PROOF:
 $\langle 1 \rangle 1$. LET: $m, n \in \omega$
 $\langle 1 \rangle 2$. ASSUME: $m < n$
 $\langle 1 \rangle 3$. $m + 0 < n + 0$
 $\langle 1 \rangle 4$. $\forall k \in \omega. m + k < n + k \Rightarrow m + k^+ < n + k^+$
 PROOF: By Proposition 18.11.
 \square

Proposition 18.17. For natural numbers m , n and k , if $m < n$ and $k \neq 0$ then $mk < nk$.

PROOF:
 $\langle 1 \rangle 1$. LET: $m, n \in \omega$
 $\langle 1 \rangle 2$. ASSUME: $m < n$
 $\langle 1 \rangle 3$. $m1 < n1$
 $\langle 1 \rangle 4$. For all $k \in \omega$, if $k \neq 0$ and $mk < nk$ then $m(k + 1) < n(k + 1)$
 PROOF:

$$\begin{aligned}
 m(k + 1) &= mk + m \\
 &< mk + n && \text{(Proposition 18.16)} \\
 &< nk + n && \text{(Proposition 18.16)} \\
 &= n(k + 1)
 \end{aligned}$$

\square

Proposition 18.18. For any nonempty set of natural numbers E , there exists $k \in E$ such that $\forall m \in E. k \leq m$.

PROOF:

- $\langle 1 \rangle 1$. LET: $E \subseteq \omega$
- $\langle 1 \rangle 2$. ASSUME: there is no $k \in E$ such that $\forall m \in E. k \leq m$.
PROVE: $E = \emptyset$
- $\langle 1 \rangle 3$. $\forall n \in \omega. n \notin E$
 - $\langle 2 \rangle 1$. LET: $P(n)$ be the property: $\forall m < n. m \notin E$
 - $\langle 2 \rangle 2$. $P(0)$
PROOF: Vacuous.
 - $\langle 2 \rangle 3$. $\forall n \in \omega. P(n) \Rightarrow P(n+1)$
 - $\langle 3 \rangle 1$. LET: $n \in \omega$
 - $\langle 3 \rangle 2$. ASSUME: $\forall m < n. m \notin E$
 - $\langle 3 \rangle 3$. $n \notin E$
PROOF: From $\langle 1 \rangle 2$.
 - $\langle 3 \rangle 4$. $\forall m < n+1. m \notin E$

□

Definition 18.19 (Equivalent). Sets E and F are *equivalent*, $E \sim F$, iff there exists a one-to-one correspondence between them.

Proposition 18.20. For any set X , equivalence is an equivalence relation on $\mathcal{P}X$.

PROOF: Easy.

Proposition 18.21. Let n be a natural number. Let X be a proper subset of n . Then there exists $m < n$ such that $X \sim m$.

PROOF:

- $\langle 1 \rangle 1$. LET: $P(n)$ be the property: for every proper subset $X \subsetneq n$, there exists $m < n$ such that $X \sim m$.
- $\langle 1 \rangle 2$. $P(0)$
PROOF: Vacuous.
- $\langle 1 \rangle 3$. $\forall n \in \omega. P(n) \Rightarrow P(n+1)$
 - $\langle 2 \rangle 1$. LET: $n \in \omega$
 - $\langle 2 \rangle 2$. ASSUME: $P(n)$
 - $\langle 2 \rangle 3$. LET: X be a proper subset of $n+1$
 - $\langle 2 \rangle 4$. CASE: $X - \{n\} = n$
PROOF: Then $X = n$ so $X \sim n < n+1$.
 - $\langle 2 \rangle 5$. CASE: $X - \{n\} \subsetneq n$
 - $\langle 3 \rangle 1$. PICK $m < n$ such that $X - \{n\} \sim m$
 - $\langle 3 \rangle 2$. $X \sim m$ or $X \sim m+1$
PROOF: If $n \in X$ then $X \sim m+1$. If $n \notin X$ then $X \sim m$.

□

Proposition 18.22. For every natural number n , we have n is not equivalent to a proper subset of n .

PROOF:

⟨1⟩1. LET: $P(n)$ be the property: every one-to-one function $n \rightarrow n$ is onto.

⟨1⟩2. $P(0)$

PROOF: The only function $0 \rightarrow 0$ is \emptyset .

⟨1⟩3. $\forall n \in \omega. P(n) \Rightarrow P(n+1)$

⟨2⟩1. LET: $n \in \omega$

⟨2⟩2. ASSUME: $P(n)$

⟨2⟩3. ASSUME: $f : n+1 \rightarrow n+1$ is one-to-one.

⟨2⟩4. LET: $g : n \rightarrow n$ be the function

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

PROOF: If $k < n$ and $f(k) = n$ then $f(n) < n$ since f is one-to-one.

⟨2⟩5. g is one-to-one.

⟨3⟩1. LET: $k, l < n$

⟨3⟩2. ASSUME: $g(k) = g(l)$

⟨3⟩3. CASE: $f(k) < n$ and $f(l) < n$

PROOF: Then $f(k) = g(k) = g(l) = f(l)$ so $k = l$ since f is one-to-one.

⟨3⟩4. CASE: $f(k) < n$ and $f(l) = n$

PROOF: Then $f(k) = g(k) = g(l) = f(n)$ contradicting the fact that f is one-to-one.

⟨3⟩5. CASE: $f(k) = n$ and $f(l) < n$

PROOF: Similar.

⟨3⟩6. CASE: $f(k) = n$ and $f(l) = n$

PROOF: Then $k = l$ since f is one-to-one.

⟨2⟩6. g maps n onto n .

PROOF: ⟨2⟩2

⟨2⟩7. f maps $n+1$ onto $n+1$.

⟨3⟩1. LET: $l < n+1$

⟨3⟩2. CASE: $l < n$

⟨4⟩1. PICK $k < n$ such that $g(k) = l$

⟨4⟩2. $f(k) = l$ or $f(n) = l$

⟨3⟩3. CASE: $l = n$

⟨4⟩1. CASE: $f(n) = n$

PROOF: Then $l \in \text{ran } f$ as required.

⟨4⟩2. CASE: $f(n) < n$

⟨5⟩1. PICK $k < n$ such that $g(k) = f(n)$

⟨5⟩2. $f(k) = n$

□