Summary of Halmos' Naive Set Theory

Robin Adams

August 24, 2023

Contents

1 Primitive Terms and Axioms **2**

2 Basic Properties and Operations on Sets **4**
2.1 The Subset Relation 4
2.2 Comprehension Notation 4
2.3 The Empty Set 5
2.4 Unordered Pairs 5
2.5 Unions 5
2.6 Intersections 6
2.7 Unordered Triples 6
2.8 Relative Complements 7
2.9 Symmetric Difference 9
2.10 Power Sets 10

3 Relations and Functions **12**
3.1 Ordered Pairs 12
3.2 Relations 13
3.3 Composition 13
3.4 Inverses 14
3.5 Equivalence Relations 14
3.6 Functions 15
3.7 Families 16
3.8 Inverses and Composites of Functions 18
3.9 Choice Functions 19

4 Equivalence **20**

5 Order **21**

6 Natural Numbers **24**
6.1 Natural Numbers 24
6.2 Arithmetic 28
6.3 Order on the Natural Numbers 33
6.4 Finite Sets 36

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.*

Definition 1.3. 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. □

Axiom 1.4 (Axiom of Pairing)**.** *For any two sets, there exists a set that they both belong to.*

Definition 1.5 ((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. □

Axiom 1.6 (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 1.7 (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 1.8 (Power Set Axiom)**.** *For any set A, there exists a set that contains all the subsets of A.*

Definition 1.9 (Empty)**.** A set is *empty* iff it has no elements; otherwise it is *non-empty*.

Axiom 1.10 (Axiom of Infinity)**.** *There exists a set I such that:*

- *I has an element that is empty*
- *for all $x \in I$, there exists $y \in I$ such that the elements of y are exactly x and the elements of x.*

Definition 1.11 (Ordered Pair)**.** For any sets a and b, the *ordered pair* (a, b) is defined by

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

Definition 1.12 (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. □

Definition 1.13 (Cartesian Product)**.** For any sets A and B, the *Cartesian product* $A \times B$ is

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

Definition 1.14 (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 1.15 (Function)**.** Let X and Y be sets. A *function, map, mapping, transformation* or *operator f from X to Y*, $f : X \to Y$, 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 1.16 (Family)**.** Let I and X be sets. A *family* of elements of X *indexed* by I is a function $a : I \to X$. We write a_i for $a(i)$, and $\{a_i\}_{i \in I}$ for a.

Definition 1.17 (Cartesian Product of a Family of Sets)**.** Let $\{A_i\}_{i \in I}$ be a family of sets. The *Cartesian product* $\bigtimes_{i \in I} A_i$ 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 $\bigtimes_{i \in I} A$.

Axiom 1.18 (Axiom of Choice)**.** *The Cartesian product of a non-empty family of non-empty sets is non-empty.*

Chapter 2

Basic Properties and Operations on Sets

2.1 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. ∎

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. ∎

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. ∎

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 $A \neq B$.

2.2 Comprehension Notation

Theorem 2.5. *There is no set that contains every set.*

PROOF:
⟨1⟩1. LET: A be a set.
PROVE: There exists a set B such that $B \notin A$.
⟨1⟩2. LET: $B = \{x \in A : x \notin x\}$
⟨1⟩3. If $B \in A$ then we have $B \in B$ if and only if $B \notin B$.
⟨1⟩4. $B \notin A$
∎

2.3 The Empty Set

Theorem 2.6. *There exists a set with no elements.*

PROOF: Immediate from the Axiom of Infinity. ∎

Definition 2.7 (Empty Set)**.** The *empty set* $\emptyset$ is the set with no elements.

Theorem 2.8. *For any set A we have $\emptyset \subset A$.*

PROOF: Vacuous. ∎

2.4 Unordered Pairs

Definition 2.9 (Singleton)**.** For any set a, the *singleton* $\{a\}$ is defined to be $\{a, a\}$.

2.5 Unions

Definition 2.10 (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. ∎

Proposition 2.11.

$$\bigcup \emptyset = \emptyset$$

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

Proposition 2.12. *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. ∎

Definition 2.13. We write $A \cup B$ for $\bigcup \{A, B\}$.

Proposition 2.14. *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 $x \in A$. ∎

Proposition 2.15 (Idempotence)**.** *For any set A, we have $A \cup A = A$.*

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

Proposition 2.16. *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 $x \in B$". ∎

Proposition 2.17. *For any sets a and b, we have $\{a\} \cup \{b\} = \{a, b\}$.*

PROOF: Immediate from definitions. ∎

2.6 Intersections

Definition 2.18 (Intersection)**.** For any sets A and B, the *intersection* $A \cap B$ is defined to be $\{x \in A : x \in B\}$.

Proposition 2.19. *For any set A, we have $A \cap \emptyset = \emptyset$.*

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

Proposition 2.20. *For any set A, we have*

$$A \cap A = A \ .$$

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

Proposition 2.21. *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 $x \in A$". □

Proposition 2.22. *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 "$((x \in A \wedge x \in B) \vee x \in C) \Leftrightarrow (x \in A \wedge (x \in B \vee x \in C))$". □

Definition 2.23 (Disjoint)**.** Two sets A and B are *disjoint* if and only if $A \cap B = \emptyset$.

Definition 2.24 (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 2.25 (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:
⟨1⟩1. LET: $\mathcal{C}$ be a nonempty set.
⟨1⟩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 $I = \{x \in A : \forall X \in \mathcal{C}. x \in X\}$.
⟨1⟩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.
□

2.7 Unordered Triples

Definition 2.26 ((Unordered) Triple)**.** Given sets $a_1, \ldots, a_n$, define the *(unordered) n-tuple* $\{a_1, \ldots, a_n\}$ to be

$$\{a_1, \ldots, a_n\} := \{a_1\} \cup \cdots \cup \{a_n\} \ .$$

2.8 Relative Complements

Definition 2.27 (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 2.28. *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 $E - (E - A) \subseteq E$.
$\square$

Proposition 2.29. *For any set E we have*

$$E - \emptyset = E$$

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

Proposition 2.30. *For any set E we have*

$$E - E = \emptyset \ .$$

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

Proposition 2.31. *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 2.32. *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 $x \in E$.
⟨2⟩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, $x \in E - A$.
⟨1⟩3. If $A \cup (E - A) = E$ then $A \subseteq E$
Proof: Since $A \subseteq A \cup (E - A)$.
□

Proposition 2.33. *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:
⟨1⟩1. Let: A, B and E be sets.
⟨1⟩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 $x \notin A$.
⟨1⟩3. If $A \subseteq E$ and $E - B \subseteq E - A$ then $A \subseteq B$.
⟨2⟩1. Assume: $A \subseteq E$
⟨2⟩2. Assume: $E - B \subseteq E - A$
⟨2⟩3. Let: $x \in A$
⟨2⟩4. $x \in E$
⟨2⟩5. $x \notin E - A$
⟨2⟩6. $x \notin E - B$
⟨2⟩7. $x \in B$
□

Example 2.34. 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 $A \nsubseteq B$.

Proposition 2.35 (De Morgan's Law)**.** *For any sets A, B and E, we have $E - (A \cup B) = (E - A) \cap (E - B)$.*

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

Proposition 2.36 (De Morgan's Law)**.** *For any sets A, B and E, we have $E - (A \cap B) = (E - A) \cup (E - B)$.*

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

Proposition 2.37. *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 $(x \in A \wedge x \notin B) \Leftrightarrow (x \in A \wedge x \in E \wedge x \notin B)$. □

Proposition 2.38. *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 $x \notin B$. □

Proposition 2.39. *For any sets A and B, we have*

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

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

Proposition 2.40. *For any sets A, B and C, we have*

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

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

Proposition 2.41. *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:
⟨1⟩1. LET: $x \in A \cap B$
PROVE: $x \in (A \cap C) \cup (B \cap (E - C))$
⟨1⟩2. CASE: $x \in C$
PROOF: Then $x \in A \cap C$.
⟨1⟩3. CASE: $x \notin C$
PROOF: Then $x \in E$ and so $x \in B \cap (E - C)$.
□

Proposition 2.42. *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 $x \in A \vee x \in B$. □

Proposition 2.43 (De Morgan's Law)**.** *Let E be a set and $\mathcal{C}$ a nonempty set. Then*

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

PROOF: Easy. □

Proposition 2.44 (De Morgan's Law)**.** *Let E be a set and $\mathcal{C}$ a nonempty set. Then*

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

PROOF: Easy. □

2.9 Symmetric Difference

Definition 2.45 (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 2.46. *For any sets A and B, we have*

$$A + B = B + A$$

Proof: From the commutativity of union. □

Proposition 2.47. *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. □

Proposition 2.48. *For any set A, we have*

$$A + \varnothing = A \ .$$

Proof:

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

□

Proposition 2.49. *For any set A we have*

$$A + A = \varnothing \ .$$

Proof:

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

□

2.10 Power Sets

Proposition 2.50.

$$\mathcal{P}\varnothing = \{\varnothing\}$$

Proof: The only subset of $\varnothing$ is $\varnothing$. □

Proposition 2.51. *For any set a, we have*

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

Proof: The only subsets of $\{a\}$ are $\varnothing$ and $\{a\}$. □

Proposition 2.52. *For any sets a and b, we have*

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

Proof: The only subsets of $\{a, b\}$ are $\varnothing$, $\{a\}$, $\{b\}$ and $\{a, b\}$. □

Proposition 2.53. *For any nonempty set $\mathcal{C}$ we have*

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

Proof:

$$\begin{aligned} x \in \bigcup_{X \in \mathcal{C}} \mathcal{P}X &\Leftrightarrow \forall X \in \mathcal{C}. x \subseteq X \\ &\Leftrightarrow \forall X \in \mathcal{C}. \forall y \in x. y \in X \\ &\Leftrightarrow \forall y \in x. \forall X \in mathcalC. y \in X \\ &\Leftrightarrow x \subseteq \bigcap \mathcal{C} \end{aligned}$$

∎

Proposition 2.54. *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 $x \subseteq \bigcup \mathcal{C}$. ∎

Proposition 2.55. *For any set E, we have*

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

Proof: Since $\emptyset \in \mathcal{P}E$. ∎

Proposition 2.56. *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 $X \subseteq F$. ∎

Chapter 3

Relations and Functions

3.1 Ordered Pairs

Proposition 3.1. *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: $\{b\} = \{a, b\} - \{a\} = \{x, y\} - \{x\} = \{y\}$.
□

Proposition 3.2. *For any sets A, B and X, we have*

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

PROOF: Easy. □

Proposition 3.3. *For any sets A and B, we have $A \times B = \emptyset$ if and only if $A = \emptyset$ or $B = \emptyset$.*

PROOF: Easy. □

Proposition 3.4. *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. □

3.2 Relations

Definition 3.5 (Domain)**.** The *domain* of a relation R is the set

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

Definition 3.6 (Range)**.** The *range* of a relation R is the set

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

Definition 3.7 (Reflexive)**.** Let R be a relation on X. Then R is *reflexive* iff, for all $x \in X$, we have xRx.

Definition 3.8 (Symmetric)**.** Let R be a relation on X. Then R is *symmetric* iff, whenever xRy, then yRx.

Definition 3.9 (Antisymmetric)**.** A relation R is *antisymmetric* iff, whenever xRy and yRx, then $x = y$.

Definition 3.10 (Transitive)**.** Let R be a relation on X. Then R is *transitive* iff, whenever xRy and yRz, then xRz.

Definition 3.11 (Identity Relation)**.** For any set X, the *identity relation* I_X on X is

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

3.3 Composition

Definition 3.12 (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 3.13. *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. □

Example 3.14. 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 3.15. *A relation R is transitive if and only if $RR \subseteq R$.*

PROOF: Easy. □

3.4 Inverses

Definition 3.16 (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 3.17. *For any relation R, we have*

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

PROOF: Easy. □

Proposition 3.18. *For any relation R, we have*

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

PROOF: Easy. □

Proposition 3.19. *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. □

Proposition 3.20. *A relation R is symmetric if and only if $R \subseteq R^{-1}$.*

PROOF: Easy. □

Proposition 3.21. *Let R be a relation between X and Y. Then*

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

PROOF: Easy. □

Proposition 3.22. *A relation R on a set X is reflexive if and only if $I_X \subseteq R$.*

PROOF: Easy. □

Proposition 3.23. *Let R be a relation on a set X. Then R is antisymmetric iff $R \cap R^{-1} \subseteq I_X$.*

PROOF: Easy. □

3.5 Equivalence Relations

Definition 3.24 (Equivalence Relation)**.** Let R be a relation on X. Then R is an *equivalence relation* iff it is reflexive, symmetric and transitive.

Definition 3.25 (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 3.26 (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 3.27 (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 3.28. *Let R be an equivalence relation on X. Then X/R is a partition of X that induces the relation R.*

Proof: Easy. □

Theorem 3.29. *Let P be a partition of X. Then X/P is an equivalence relation on X, and $P = X/(X/P)$.*

Proof: Easy. □

3.6 Functions

Definition 3.30 (Onto)**.** Let $f : X \to Y$. We say f maps X *onto* Y iff $\operatorname{ran} f = Y$.

Definition 3.31 (Image)**.** Let $f : X \to Y$ and $A \subseteq X$. The *image* of A under f is

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

Definition 3.32 (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 3.33. *For any set X, the identity relation I_X is a function $X \to X$.*

Proof: Easy. □

Definition 3.34 (Restriction)**.** Let $f : Y \to Z$ and $X \subseteq Y$. The *restriction* of f to X is the function $f \upharpoonright X : X \to Z$ defined by

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

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

Definition 3.35 (Projection)**.** Given sets X and Y, the *projection* maps $\pi_1 : X \times Y \to X$ and $\pi_2 : X \times Y \to Y$ are defined by

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

Definition 3.36 (Canonical Map)**.** Let X be a set and R an equivalence relation on X. The *canonical map* $\pi : X \to X/R$ is the map defined by $\pi(x) = x/R$.

Definition 3.37 (One-to-One)**.** A function $f : X \to Y$ 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 3.38. *Let $f : X \to Y$. 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. □

Proposition 3.39. *Let $f : X \to Y$. 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. □

3.7 Families

Proposition 3.40 (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. □

Proposition 3.41 (Generalized Commutative Law for Unions)**.** *Let $\{I_j\}_{j \in J}$ be a family of sets. Let $f : J \to J$ 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. □

Proposition 3.42 (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. □

Proposition 3.43 (Generalized Commutative Law for Intersections)**.** *Let $\{I_j\}_{j \in J}$ be a nonempty family of sets. Let $f : J \to J$ 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. □

Proposition 3.44. *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. □

Proposition 3.45. *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. □

Definition 3.46 (Projection)**.** Let $\{A_i\}_{i\in I}$ be a family of sets and $i \in I$. The *projection* function $\pi_i : \bigtimes_{i\in I} A_i \to A_i$ is defined by $\pi_i(a) = a_i$.

Proposition 3.47. *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. □

Proposition 3.48. *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. □

Proposition 3.49. *Let $f : X \to Y$. 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. □

Example 3.50. It is not true in general that, if $f : X \to Y$ and $\{A_i\}_{i\in I}$ is a nonempty family of subsets of X, then $f\left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} f(A_i)$.

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 $X \to Y$. Then $f\left(\bigcap_{i\in I} A_i\right) = f(\varnothing) = \varnothing$ but $\bigcap_{i\in I} f(A_i) = \{c\}$.

3.8 Inverses and Composites of Functions

Definition 3.51 (Inverse)**.** Given a function $f : X \to Y$, the *inverse* of f is the function $f^{-1} : \mathcal{P}Y \to \mathcal{P}X$ 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 3.52. *Let $f : X \to Y$. Then f maps X onto Y if and only if the inverse image of any nonempty subset of Y is nonempty.*

PROOF: Easy. □

Proposition 3.53. *Let $f : X \to Y$. Then f is one-to-one if and only if the inverse image of any singleton subset of Y is a singleton.*

PROOF: Easy. □

Proposition 3.54. *Let $f : X \to Y$. Let $B \subseteq Y$. Then*

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

PROOF: Easy. □

Proposition 3.55. *Let $f : X \to Y$. Let $A \subseteq X$. Then*

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

Equality holds if f is one-to-one.

PROOF: Easy. □

Proposition 3.56. *Let $f : X \to Y$. 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. □

Proposition 3.57. *Let $f : X \to Y$. 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. □

Proposition 3.58. *Let $f : X \to Y$ and $B \subseteq Y$. Then $f^{-1}(Y - B) = X - f^{-1}(B)$.*

PROOF: Easy. □

Proposition 3.59. *Let $f : X \to Y$ be one-to-one. Then the inverse of f as a relation, f^{-1}, is a function $f^{-1} : \operatorname{ran} f \to X$, and for all $y \in \operatorname{ran} f$, we have $f^{-1}(y)$ is the unique x such that $f(x) = y$.*

PROOF: Easy. $\square$

Proposition 3.60. *Let $f : X \to Y$ and $g : Y \to Z$. Then $gf : X \to Z$ and, for all $x \in X$, we have*

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

PROOF: Easy. $\square$

Example 3.61. Example 3.14 shows that function composition is not commutative in general.

Proposition 3.62. *Let $f : X \to Y$ and $g : Y \to Z$. Then*

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

PROOF: Easy. $\square$

Proposition 3.63. *Let $f : X \to Y$ and $g : Y \to X$. If $gf = I_X$ then f is one-to-one and g maps Y onto X.*

PROOF: Easy. $\square$

3.9 Choice Functions

Definition 3.64 (Choice Function)**.** A *choice function* for a set X is a function $f : \mathcal{P}X - \{\varnothing\} \to X$ such that $f(S) \in S$ for all S.

Proposition 3.65. *Every set has a choice function.*

PROOF: Given a nonempty set X, apply the Axiom of Choice to the family $\{S\}_{S \in \mathcal{P}X - \{\varnothing\}}$. $\square$

Proposition 3.66. *For any relation R, there exists a function $f \subseteq R$ such that* $\operatorname{dom} f = \operatorname{dom} R$*.*

PROOF:
⟨1⟩1. LET: R be a relation.
⟨1⟩2. PICK a choice function g for $\operatorname{ran} R$.
⟨1⟩3. LET: $f : \operatorname{dom} R \to \operatorname{ran} R$ be the function $f(x) = g(\{y \in \operatorname{ran} R : xRy\})$
⟨1⟩4. $f \subseteq R$ and $\operatorname{dom} f = \operatorname{dom} R$.
$\square$

Proposition 3.67. *If $\mathcal{C}$ is a set of pairwise disjoint nonempty sets , then there exists a set A such that, for all $C \in \mathcal{C}$, we have $A \cap C$ is a singleton.*

PROOF:
⟨1⟩1. LET: f be a choice function for $\bigcup \mathcal{C}$
⟨1⟩2. LET: $A = \{f(C) : C \in \mathcal{C}\}$
⟨1⟩3. For all $C \in \mathcal{C}$ we have $A \cap C = \{f(C)\}$
$\square$

Chapter 4

Equivalence

Definition 4.1 (Equivalent)**.** Sets E and F are *equivalent*, $E \sim F$, iff there exists a one-to-one correspondence between them.

Proposition 4.2. *For any set X, equivalence is an equivalence relation on $\mathcal{P}X$.*

PROOF: Easy.

Chapter 5

Order

Definition 5.1 (Partial Order)**.** A *partial order* on a set X is a relation on X that is reflexive, antisymmetric and transitive.

A *partially ordered set* or *poset* is a pair $(X, \leqslant)$ such that $\leqslant$ is a partial order on X. We write X for the poset $(X, \leqslant)$.

Given a partial order $\leqslant$, we write $\geqslant$ for the inverse of $\leqslant$.

We write $x < y$ or $y > x$ for $x \leqslant y \wedge x \neq y$. When this holds, we say x is *less than* y, *smaller* than y, or a *predecessor* of y; and y is *greater than* x, *larger* than x, or a *successor* of x.

Proposition 5.2. *For any set X, the relation $\subseteq$ is a partial order on $\mathcal{P}X$.*

PROOF: Easy. □

Proposition 5.3. *In a poset, we never have $x < y$ and $y < x$.*

PROOF: We would then have $x \leqslant y$ and $y \leqslant x$ hence $x = y$ by antisymmetry. But if $x < y$ or $y < x$ then $x \neq y$. □

Proposition 5.4. *The relation $<$ is transitive.*

PROOF:
⟨1⟩1. ASSUME: $x < y$ and $y < z$
⟨1⟩2. $x \leqslant y$ and $y \leqslant z$
⟨1⟩3. $x \leqslant z$
PROOF: Since $\leqslant$ is transitive.
⟨1⟩4. $x \neq z$
PROOF: By Proposition 5.3.
□

Proposition 5.5. *Let $<$ be a transitive relation on X such that we never have $x < y$ and $y < x$. Define $\leqslant$ by: $x \leqslant y$ iff $x < y$ or $x = y$. Then $\leqslant$ is a partial order on X.*

PROOF:

⟨1⟩1. $\leqslant$ is reflexive.
PROOF: By definition.
⟨1⟩2. $\leqslant$ is asymmetric.
PROOF: If $x \leqslant y$ and $y \leqslant x$, we must have $x = y$, because otherwise we would have $x < y$ and $y < x$.
⟨1⟩3. $\leqslant$ is transitive.
⟨2⟩1. LET: $x \leqslant y$ and $y \leqslant z$
⟨2⟩2. CASE: $x = y$
PROOF: We have $y \leqslant z$ so $x \leqslant z$.
⟨2⟩3. CASE: $y = z$
PROOF: We have $x \leqslant y$ so $x \leqslant z$.
⟨2⟩4. CASE: $x < y$ and $y < z$
PROOF: We have $x < z$ by transitivity, so $x \leqslant z$.
□

Definition 5.6 ((Strict) Initial Segment)**.** Let X be a poset and $a \in X$. The *(strict) initial segment* determined by a is

$$s(a) := \{x \in X : x < a\} \ .$$

Definition 5.7 (Weak Initial Segment)**.** Let X be a poset and $a \in X$. The *weak initial segment* determined by a is

$$\bar{s}(a) := \{x \in X : x \leqslant a\} \ .$$

Definition 5.8 (Immediate Successor)**.** Let X be a poset and $x, y \in X$. Then y is the *immediate successor* of x, and x is the *immediate predecessor* of y, iff $x < y$ and there is no z such that $x < z < y$.

Definition 5.9 (Least)**.** Let X be a partial order and $a \in X$. Then a is *least* in X iff $\forall x \in X. a \leqslant x$.

Proposition 5.10. *A poset has at most one least element.*

PROOF: If a and b are least then $a \leqslant b$ and $b \leqslant a$, hence $a = b$. □

Definition 5.11 (Greatest)**.** Let X be a partial order and $a \in X$. Then a is *greatest* in X iff $\forall x \in X. x \leqslant a$.

Proposition 5.12. *A poset has at most one greatest element.*

PROOF: If a and b are greatest then $a \leqslant b$ and $b \leqslant a$, hence $a = b$. □

Definition 5.13 (Minimal)**.** Let X be a poset and $a \in X$. Then a is *minimal* iff there is no $x \in X$ such that $x < a$.

Definition 5.14 (Maximal)**.** Let X be a poset and $a \in X$. Then a is *maximal* iff there is no $x \in X$ such that $a < x$.

Definition 5.15 (Lower Bound)**.** Let X be a poset. Let $E \subseteq X$ and $a \in X$. Then a is a *lower bound* for E iff $\forall x \in E. a \leqslant x$.

Definition 5.16 (Upper Bound)**.** Let X be a poset. Let $E \subseteq X$ and $a \in X$. Then a is an *upper bound* for E iff $\forall x \in E . x \leqslant a$.

Definition 5.17 (Greatest Lower Bound, Infimum)**.** Let X be a poset. Let $E \subseteq X$ and $a \in X$. Then a is the *greatest lower bound* or *infimum* for E iff a is the greatest element in the set of lower bounds for E.

Definition 5.18 (Least Upper Bound, Supremum)**.** Let X be a poset. Let $E \subseteq X$ and $a \in X$. Then a is the *least upper bound* or *supremum* for E iff a is the least element in the set of upper bounds for E.

Definition 5.19 (Total Order)**.** A partial order $\leqslant$ on a set X is a *total order*, *simple order* or *linear order* iff, for all $x, y \in X$, either $x \leqslant y$ or $y \leqslant x$. We then call the poset $(X, \leqslant)$ a *linearly ordered set* or a *chain*.

Proposition 5.20. *Let R be a partial order on X. Then R is total if and only if $X^2 \subseteq R \cup R^{-1}$.*

PROOF: Easy. $\square$

Proposition 5.21. *For any set X, the relation $\subseteq$ is a total order on X iff X is either $\emptyset$ or a singleton.*

PROOF: Easy. $\square$

Chapter 6

Natural Numbers

6.1 Natural Numbers

Definition 6.1 (Successor)**.** The *successor* of a set x, x^+, is defined by

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

Definition 6.2. We define

$$\begin{aligned} 0 &= \varnothing \\ 1 &= 0^+ \\ 2 &= 1^+ \end{aligned}$$

etc.

Definition 6.3 (Characteristic Function)**.** Let X be a set and $A \subseteq X$. The *characteristic function* of A is the function $\chi_A : X \to 2$ defined by

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

Theorem 6.4. *Let X be a set. The function $\chi : \mathcal{P}X \to 2^X$ that maps a subset A of X to χ_A is a one-to-one correspondence.*

PROOF: Easy. □

Definition 6.5. 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 $\omega = \bigcap\{X \in \mathcal{P}A : 0 \in X \wedge \forall n \in X.n^+ \in X\}$. □

Definition 6.6 (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 $\times$.

Proposition 6.7. *For any natural numbers m and n, if $m \in n$ then $m^+ \in n^+$.*

PROOF:
⟨1⟩1. LET: $P(n)$ be the property $\forall m \in n.m^+ \in n^+$
⟨1⟩2. $P(0)$
PROOF: Vacuous.
⟨1⟩3. For any natural number n, if $P(n)$ then $P(n^+)$.
⟨2⟩1. LET: n be a natural number.
⟨2⟩2. ASSUME: $P(n)$
⟨2⟩3. LET: $m \in n^+$
⟨2⟩4. $m \in n$ or $m = n$
⟨2⟩5. $m^+ \in n^+$ or $m^+ = n^+$
PROOF: ⟨2⟩2
⟨2⟩6. CASE: $m^+ \in n^{++}$
□

Theorem 6.8 (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. □

Proposition 6.9.

$$\forall n \in \omega.\forall x \in n.n \nsubseteq x$$

PROOF:
⟨1⟩1. $\forall x \in 0.0 \nsubseteq x$
PROOF: Vacuous.
⟨1⟩2. For any natural number n, if $\forall x \in n.n \nsubseteq x$ then $\forall x \in n^+.n^+ \nsubseteq x$.
⟨2⟩1. LET: n be a natural number.
⟨2⟩2. ASSUME: $\forall x \in n.n \nsubseteq x$
⟨2⟩3. LET: $x \in n^+$
⟨2⟩4. ASSUME: for a contradiction $n^+ \subseteq x$
⟨2⟩5. $x \in n$ or $x = n$
⟨2⟩6. CASE: $x \in n$
PROOF: Then we have $n \subseteq n^+ \subseteq x$ contradicting ⟨2⟩2.
⟨2⟩7. CASE: $x = n$
PROOF: Then we have $n \in n^+ \subseteq x = n$ and $n \subseteq n$ contradicting ⟨2⟩2.
□

Corollary 6.9.1. *For any natural number n we have $n \notin n$.*

Corollary 6.9.2. *For any natural number n we have $n \neq n^+$.*

Definition 6.10 (Transitive Set)**.** A set E is a *transitive* set iff, whenever $x \in y \in E$, then $x \in E$.

Proposition 6.11. *Every natural number is a transitive set.*

PROOF:
⟨1⟩1. 0 is a transitive set.
PROOF: Vacuously, if $x \in y \in 0$ then $x \in 0$.
⟨1⟩2. For any natural number n, if n is a transitive set, then n^+ is a transitive set.
⟨2⟩1. LET: n be a natural number.
⟨2⟩2. ASSUME: n is a transitive set.
⟨2⟩3. LET: $x \in y \in n^+$
⟨2⟩4. $y \in n$ or $y = n$
⟨2⟩5. CASE: $y \in n$
⟨3⟩1. $x \in n$
PROOF: ⟨2⟩2, ⟨2⟩3, ⟨2⟩5.
⟨3⟩2. $x \in n^+$
⟨2⟩6. CASE: $y = n$
⟨3⟩1. $x \in n$
PROOF: ⟨2⟩3, ⟨2⟩6
⟨3⟩2. $x \in n^+$
□

Proposition 6.12. *For any natural numbers m and n, if $m^+ = n^+$ then $m = n$.*

PROOF:
⟨1⟩1. LET: m and n be natural numbers.
⟨1⟩2. ASSUME: $m^+ = n^+$
⟨1⟩3. $m \in m^+ = n^+$
⟨1⟩4. $m \in n$ or $m = n$
⟨1⟩5. $n \in n^+ = m^+$
⟨1⟩6. $n \in m$ or $n = m$
⟨1⟩7. We cannot have $m \in n$ and $n \in m$
⟨2⟩1. ASSUME: for a contradiction $m \in n$ and $n \in m$
⟨2⟩2. $m \in m$
PROOF: Since m is a transitive set (Proposition 6.11).
⟨2⟩3. Q.E.D.
PROOF: This contradicts Proposition 6.9.
⟨1⟩8. $m = n$
□

Theorem 6.13 (Recursion Theorem)**.** *Let X be a set. Let $a \in X$. Let $f : X \to X$. There exists a function $u : \omega \to X$ 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: $\langle 3\rangle 2$
$\langle 3\rangle 7$. $x = y$
$\square$

Proposition 6.14. *For any natural number n, either $n = 0$ or there exists a natural number m such that $n = m^+$.*

PROOF: Easy induction on n. $\square$

Proposition 6.15. *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 6.16. *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:
⟨1⟩1. LET: $P(n)$ be the property: for any nonempty subset $E \subseteq n$, there exists $k \in E$ such that $\forall m \in E.k = m \vee k \in m$
⟨1⟩2. $P(0)$
PROOF: Vacuous as there is no nonempty subset of 0.
⟨1⟩3. For any natural number n, if $P(n)$ then $P(n^+)$.
⟨2⟩1. LET: n be a natural number.
⟨2⟩2. ASSUME: $P(n)$
⟨2⟩3. LET: E be a nonempty subset of n^+
⟨2⟩4. CASE: $E - \{n\} = \emptyset$
PROOF: Then $E = \{n\}$ so take $k = n$.
⟨2⟩5. CASE: $E - \{n\} \neq \emptyset$
⟨3⟩1. PICK $k \in E - \{n\}$ such that $\forall m \in E - \{n\}.k = m \vee k \in m$
PROOF: By ⟨2⟩2.
⟨3⟩2. $\forall m \in E.k = m \vee k \in m$
PROOF: Since $k \in n$.
□

6.2 Arithmetic

Definition 6.17 (Addition)**.** Define *addition* $+$ on ω by recursion thus:

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

Proposition 6.18. *For all $m, n, p \in \omega$ we have*

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

PROOF:
⟨1⟩1. LET: $P(p)$ be the property $\forall m, n \in \omega.m + (n + p) = (m + n) + p$
⟨1⟩2. $P(0)$
PROOF: $m + (n + 0) = m + n = (m + n) + 0$.
⟨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. $m + (n + p^+) = (m + n) + p^+$

PROOF:

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

□

Proposition 6.19. *For all $m, n \in \omega$, we have*

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

PROOF:
⟨1⟩1. LET: $P(m)$ be the property $\forall n \in \omega. m + n = n + m$
⟨1⟩2. $P(0)$
⟨2⟩1. LET: $Q(n)$ be the property $0 + n = n + 0$
⟨2⟩2. $Q(0)$
PROOF: Trivial.
⟨2⟩3. $\forall n \in \omega. Q(n) \Rightarrow Q(n^+)$
⟨3⟩1. LET: $n \in \omega$
⟨3⟩2. ASSUME: $Q(n)$
⟨3⟩3. $0 + n^+ = n^+ + 0$
PROOF:

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

⟨1⟩3. $\forall m \in \omega. P(m) \Rightarrow P(m^+)$
⟨2⟩1. LET: $m \in \omega$
⟨2⟩2. ASSUME: $P(m)$
⟨2⟩3. LET: $Q(n)$ be the property $m^+ + n = n + m^+$
⟨2⟩4. $Q(0)$
PROOF: ⟨1⟩2
⟨2⟩5. $\forall n \in \omega. Q(n) \Rightarrow Q(n^+)$
⟨3⟩1. LET: $n \in \omega$
⟨3⟩2. ASSUME: $Q(n)$
⟨3⟩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 6.20 (Multiplication)**.** Define *multiplication* $\cdot$ on ω by

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

Proposition 6.21. *For all $m, n, p \in \omega$, we have*

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

PROOF:
$\langle 1\rangle 1$. LET: $P(p)$ be the statement $\forall m, n \in \omega . m(n+p) = mn + mp$
$\langle 1\rangle 2$. $P(0)$
  PROOF:

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

$\langle 1\rangle 3$. $\forall p \in \omega . P(p) \Rightarrow P(p^+)$
  $\langle 2\rangle 1$. LET: $p \in \omega$
  $\langle 2\rangle 2$. ASSUME: $P(p)$
  $\langle 2\rangle 3$. LET: $m, n \in \omega$
  $\langle 2\rangle 4$. $m(n+p^+) = mn + mp^+$
    PROOF:

$$\begin{aligned} m(n+p^+) &= m(n+p)^+ \\ &= m(n+p) + m \\ &= (mn + mp) + m && (\langle 2\rangle 2) \\ &= mn + (mp + m) && (\text{Proposition 6.18}) \\ &= mn + mp^+ \end{aligned}$$

□

Proposition 6.22. *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:
$$\begin{aligned} m(np^+) &= m(np + n) \\ &= m(np) + mn && \text{(Proposition 6.21)} \\ &= (mn)p + mn && (\langle 2 \rangle 2) \\ &= (mn)p^+ \end{aligned}$$
□

Proposition 6.23. *For all $m, n \in \omega$, we have*
$$mn = nm \ .$$

Proof:
⟨1⟩1. Let: $P(m)$ be the statement $\forall n \in \omega . mn = nm$
⟨1⟩2. $P(0)$
⟨2⟩1. Let: $Q(n)$ be the statement $0n = n0$
⟨2⟩2. $Q(0)$
Proof: Trivial.
⟨2⟩3. $\forall n \in \omega . Q(n) \Rightarrow Q(n^+)$
⟨3⟩1. Let: $n \in \omega$
⟨3⟩2. Assume: $Q(n)$
⟨3⟩3. $Q(n^+)$
Proof:
$$\begin{aligned} 0n^+ &= 0n + 0 \\ &= 0n \\ &= n0 && (\langle 3 \rangle 2) \\ &= 0 \\ &= n^+0 \end{aligned}$$
⟨1⟩3. $\forall m \in \omega . P(m) \Rightarrow P(m^+)$
⟨2⟩1. Let: $m \in \omega$
⟨2⟩2. Assume: $P(m)$
⟨2⟩3. Let: $Q(n)$ be the statement $m^+n = nm^+$
⟨2⟩4. $Q(0)$
Proof: ⟨1⟩2

⟨2⟩5. $\forall n \in \omega . Q(n) \Rightarrow Q(n^+)$
⟨3⟩1. Let: $n \in \omega$
⟨3⟩2. Assume: $Q(n)$
⟨3⟩3. $Q(n^+)$
Proof:

$$\begin{aligned} m^+n^+ &= m^+n + m^+ \\ &= (m^+n+m)^+ \\ &= (nm^+ + m)^+ && (\langle 3\rangle 2) \\ &= (nm+n+m)^+ \\ &= (mn+m+n)^+ && (\langle 2\rangle 2\text{, Proposition 6.18, Proposition 6.19}) \\ &= (mn^+ + n)^+ \\ &= (n^+m+n)^+ && (\langle 2\rangle 2) \\ &= n^+m + n^+ \\ &= n^+m^+ \end{aligned}$$

∎

Definition 6.24 (Exponentiation)**.** Define *exponentiation* on ω by recursion:

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

Proposition 6.25. *For all $m, n, p \in \omega$ we have*

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

Proof:
⟨1⟩1. $m^{n+0} = m^n m^0$
Proof:

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

⟨1⟩2. If $m^{n+p} = m^n m^p$ 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 6.26. *For all $m, n, p \in \omega$ we have*

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

Proof:

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

PROOF: Both are equal to 1.

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

PROOF:

$$\begin{aligned} (m^n)^{p^+} &= (m^n)^p m^n \\ &= m^{np} m^n \\ &= m^{np+n} && \text{(Proposition 6.25)} \\ &= m^{np^+} \end{aligned}$$

□

6.3 Order on the Natural Numbers

Definition 6.27. Given natural numbers m and n, we write $m < n$ iff $m \in n$.

We write $m \leqslant n$ iff $m < n \vee m = n$.

Proposition 6.28. *The relation $\leqslant$ is a total order on ω.*

PROOF:

$\langle 1\rangle 1.$ $\leqslant$ is a partial order on ω.

$\langle 2\rangle 1.$ $<$ is transitive.

PROOF: Proposition 6.11.

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

PROOF: If $m < n$ and $n < m$ then $m < m$ by Proposition 6.11, contradicting Corollary 6.9.1.

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

$\langle 1\rangle 2.$ For all $m, n \in \omega$, either $m \leqslant n$ or $n \leqslant m$.

$\langle 2\rangle 1.$ LET: $P(n)$ be the statement: $\forall m \in \omega . m \leqslant n \vee n \leqslant m$

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

$\langle 3\rangle 1.$ LET: $Q(m)$ be the statement: $0 \leqslant m$

$\langle 3\rangle 2.$ $Q(0)$

PROOF: Since $0 \leqslant 0$.

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

PROOF: If $0 \leqslant m$ then $0 < m+1$ by transitivity.

$\langle 2\rangle 3.$ $\forall n \in \omega . P(n) \Rightarrow P(n+1)$

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

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

$\langle 3\rangle 3.$ $P(n+1)$

$\langle 4\rangle 1.$ LET: $Q(m)$ be the property $m \leqslant n+1 \vee n+1 \leqslant m$

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

PROOF: $\langle 2\rangle 2$

$\langle 4\rangle 3.$ $\forall m \in \omega . Q(m) \Rightarrow Q(m+1)$

$\langle 5\rangle 1.$ LET: $m \in \omega$

$\langle 5\rangle 2.$ ASSUME: $Q(m)$

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

PROOF: Then $m < n+1$

$\langle 5\rangle 4.$ CASE: $n < m$
PROOF: Then $n + 1 < m + 1$ by Proposition 6.7, so $n + 1 \leqslant m$.
$\langle 5\rangle 5.$ CASE: $n = m$
PROOF: Then $n + 1 = m + 1$.
□

Proposition 6.29. *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 6.9.1.
$\langle 1\rangle 3.$ 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 6.9.
$\langle 2\rangle 3.$ $m \neq n$
$\langle 2\rangle 4.$ $m \in n$
PROOF: Trichotomy.
□

Proposition 6.30. *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 6.7.
□

Proposition 6.31. *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:

$$\begin{aligned} m(k+1) &= mk + m \\ &< mk + n && \text{(Proposition 6.30)} \\ &< nk + n && \text{(Proposition 6.30)} \\ &= n(k+1) \end{aligned}$$

□

Proposition 6.32. *For any nonempty set of natural numbers E, there exists $k \in E$ such that $\forall m \in E.k \leqslant m$.*

PROOF:
$\langle 1 \rangle 1$. LET: $E \subseteq \omega$
$\langle 1 \rangle 2$. ASSUME: there is no $k \in E$ such that $\forall m \in E.k \leqslant m$.
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 $\langle 1 \rangle 2$.
$\langle 3 \rangle 4$. $\forall m < n+1.m \notin E$
□

Proposition 6.33. *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 6.34. *For every natural number n, we have n is not equivalent to a proper subset of n.*

PROOF:
$\langle 1 \rangle 1$. LET: $P(n)$ be the property: every one-to-one function $n \to n$ is onto.
$\langle 1 \rangle 2$. $P(0)$
PROOF: The only function $0 \to 0$ is $\emptyset$.
$\langle 1 \rangle 3$. $\forall n \in \omega.P(n) \Rightarrow P(n+1)$
$\langle 2 \rangle 1$. LET: $n \in \omega$

⟨2⟩2. ASSUME: $P(n)$
⟨2⟩3. ASSUME: $f : n + 1 \to n + 1$ is one-to-one.
⟨2⟩4. LET: $g : n \to n$ 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 $l \in \operatorname{ran} f$ as required.
⟨4⟩2. CASE: $f(n) < n$
⟨5⟩1. PICK $k < n$ such that $g(k) = f(n)$
⟨5⟩2. $f(k) = n$

□

Corollary 6.34.1. *Equivalent natural numbers are equal.*

Definition 6.35 (Lexicographical Order)**.** The *lexicographical* order on $\omega \times \omega$ is the relation S defined by $(a, b)S(x, y)$ iff $a < x$ or ($a = x$ and $b < y$).

Proposition 6.36. *The lexicographical order is a partial order on* $\omega \times \omega$.

PROOF: Easy. □

6.4 Finite Sets

Definition 6.37 (Finite)**.** A set is *finite* iff it is equivalent to a natural number; otherwise, it is *infinite*.

Proposition 6.38. *No finite set is equivalent to one of its proper subsets.*

PROOF: From Proposition 6.34. ∎

Proposition 6.39. *ω is infinite.*

PROOF: Since the function that maps n to $n+1$ is a one-to-one correspondence between ω and $\omega - \{0\}$. ∎

Proposition 6.40. *Every subset of a finite set is finite.*

PROOF: Proposition 6.33. ∎

Definition 6.41 (Number of Elements)**.** For any finite set E, the *number of elements* in E, $\sharp(E)$, is the unique natural number such that $E \sim \sharp(E)$.

Proposition 6.42. *Let E and F be finite sets. If $E \subseteq F$ then $\sharp(E) \leqslant \sharp(F)$.*

PROOF: Proposition 6.33. ∎

Proposition 6.43. *Let E and F be disjoint finite sets. Then $E \cup F$ is finite and $\sharp(E \cup F) = \sharp(E) \cup \sharp(F)$.*

PROOF:
⟨1⟩1. LET: $P(n)$ be the statement: $n \in \omega$ and for any $m \in \omega$, if $E \sim m$, $F \sim n$ and $E \cap F = \varnothing$, then $E \cup F \sim m + n$
⟨1⟩2. $P(0)$
  ⟨2⟩1. LET: $m \in \omega$
  ⟨2⟩2. LET: $E \sim m$ and $F \sim 0$
  ⟨2⟩3. $F = \varnothing$
  ⟨2⟩4. $E \cup F = E \sim m = m + 0$
⟨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. LET: $m \in \omega$
  ⟨2⟩4. LET: $E \sim m$ and $F \sim n + 1$
  ⟨2⟩5. ASSUME: $E \cap F = \varnothing$
  ⟨2⟩6. PICK $f \in F$
  ⟨2⟩7. $F - \{f\} \sim n$
  ⟨2⟩8. $E \cap (F - \{f\}) = \varnothing$
  ⟨2⟩9. $E \cup (F - \{f\}) \sim m + n$
    PROOF: ⟨2⟩2
  ⟨2⟩10. $E \cup F \sim m + n + 1$
∎

Corollary 6.43.1. *The union of two finite sets is finite.*

PROOF: Since, if E and F are finite, then $E \cup F = (E - F) \cup (E \cap F) \cup (F - E)$ and these are finite and disjoint. ∎

Proposition 6.44. *If E and F are finite sets then $E \times F$ is finite and $\sharp(E \times F) = \sharp(E)\sharp(F)$.*

PROOF:
⟨1⟩1. LET: $P(n)$ be the statement: $n \in \omega$ and for all $m \in \omega$, if $E \sim m$ and $F \sim n$ then $E \times F \sim mn$
⟨1⟩2. $P(0)$
PROOF: If $F \sim 0$ then $F = \emptyset$ so $E \times F = \emptyset \sim 0$.
⟨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. LET: $m \in \omega$
⟨2⟩4. ASSUME: $E \sim m$ and $F \sim n+1$
⟨2⟩5. PICK $f \in F$
⟨2⟩6. $F - \{f\} \sim n$
⟨2⟩7. $E \times (F - \{f\}) \sim mn$
⟨2⟩8. $E \times F = (E \times (F - \{f\})) \cup (E \times \{f\})$
⟨2⟩9. $E \times \{f\} \sim m$
⟨2⟩10. $E \times F \sim mn + m$
PROOF: Proposition 6.43.
□

Proposition 6.45. *For any finite sets E and F, we have E^F is finite and $\sharp(E^F) = \sharp(E)^{\sharp(F)}$.*

PROOF:
⟨1⟩1. LET: $P(n)$ be the property: $n \in \omega$ and for all $m \in \omega$, if $E \sim m$ and $F \sim n$ then $E^F \sim m^n$
⟨1⟩2. $P(0)$
PROOF: Since $E^{\emptyset} = \{\emptyset\} \sim 1$
⟨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. LET: $m \in \omega$
⟨2⟩4. LET: $E \sim m$ and $F \sim n+1$
⟨2⟩5. PICK $f \in F$
⟨2⟩6. $F - \{f\} \sim n$
⟨2⟩7. LET: $\phi : E^F \to E^{F - \{f\}} \times E$ be the function $\phi(g) = (g \restriction (F - \{f\}), g(f))$
⟨2⟩8. ϕ is a one-to-one correspondence
⟨2⟩9. $\sharp(E^F) = m^{n+1}$
PROOF:
$$\begin{aligned} \sharp(E^F) &= \sharp(E^{F-\{f\}} \times E) \\ &= \sharp(E^{F-\{f\}})\sharp(E) && \text{(Proposition 6.44)} \\ &= m^n m && (\langle 2\rangle 2, \langle 2\rangle 4) \\ &= m^{n+1} \end{aligned}$$
□

Corollary 6.45.1. *If E is finite then $\mathcal{P}E$ is finite and $\sharp(\mathcal{P}E) = 2^{\sharp(E)}$.*

Proposition 6.46. *The union of a finite set of finite sets is finite.*

PROOF:
⟨1⟩1. LET: $P(n)$ be the property: for any set E, if $E \sim n$ and every element of E is finite, then $\bigcup E$ is finite.
⟨1⟩2. $P(0)$
PROOF: Since $\bigcup \emptyset = \emptyset$ is finite.
⟨1⟩3. $\forall n \in \omega . P(n) \Rightarrow P(n+1)$
⟨2⟩1. LET: n be a natural number.
⟨2⟩2. ASSUME: $P(n)$
⟨2⟩3. LET: $E \sim n+1$
⟨2⟩4. PICK $X \in E$
⟨2⟩5. $E - \{X\} \sim n$
⟨2⟩6. $\bigcup (E - \{X\})$ is finite.
PROOF: ⟨2⟩2
⟨2⟩7. $\bigcup E = \bigcup (E - \{X\}) \cup X$
⟨2⟩8. $\bigcup E$ is finite.
PROOF: Corollary 6.43.1.
□

Proposition 6.47. *Every nonempty finite set of natural numbers has a greatest element.*

PROOF:
⟨1⟩1. LET: $P(n)$ be the property: for every $E \subseteq \mathbb{N}$, if $E \sim n$ then E has a greatest element.
⟨1⟩2. $P(1)$
PROOF: Since k is the greatest element of $\{k\}$.
⟨1⟩3. $\forall n \geqslant 1 . P(n) \Rightarrow P(n+1)$
⟨2⟩1. LET: $n \geqslant 1$
⟨2⟩2. ASSUME: $P(n)$
⟨2⟩3. ASSUME: $E \subseteq \omega$ and $E \sim n+1$
⟨2⟩4. PICK $k \in E$
⟨2⟩5. LET: l be the greatest element of $E - \{k\}$
⟨2⟩6. Either k or l is greatest in E.
□

Proposition 6.48. *Every infinite set has a subset equivalent to ω.*

PROOF:
⟨1⟩1. LET: X be an infinite set.
⟨1⟩2. PICK a choice function f for X.
⟨1⟩3. LET: $\mathcal{C}$ be the set of all finite subsets of X.
⟨1⟩4. For all $A \in \mathcal{C}$ we have $X - A \in \operatorname{dom} f$.
PROOF: For all $A \in \mathcal{C}$ we have $X - A \neq \emptyset$.
⟨1⟩5. LET: $U : \omega \to \mathcal{C}$ be the function defined recursively by $U(0) = \emptyset$ and $U(n+1) = U(n) \cup \{f(X - U(n))\}$ for all $n \in \omega$.
⟨1⟩6. LET: $v : \omega \to X$ be the function $v(n) = f(X - U(n))$
PROVE: v is one-to-one.

$\langle 1 \rangle 7.$ $\forall n \in \omega . v(n) \notin U(n)$

PROOF: Since $v(n) = f(X - U(n)) \in X - U(n)$.

$\langle 1 \rangle 8.$ $\forall n \in \omega . v(n) \in U(n+1)$

$\langle 1 \rangle 9.$ $\forall m, n \in \omega . n \leqslant m \Rightarrow U(n) \subseteq U(m)$

PROOF: Since $U(n) \subseteq U(n+1)$ for all n.

$\langle 1 \rangle 10.$ $\forall m, n \in \omega . n < m \Rightarrow v(n) \neq v(m)$

PROOF: Since $v(n) \in U(m)$ and $v(m) \notin U(m)$.

$\square$