

Summary of Halmos' Naive Set Theory

Robin Adams

August 25, 2023

Contents

| | | |
|----------|--|-----------|
| 1 | Primitive Terms and Axioms | 3 |
| 2 | Basic Properties and Operations on Sets | 5 |
| 2.1 | The Subset Relation | 5 |
| 2.2 | Comprehension Notation | 5 |
| 2.3 | The Empty Set | 6 |
| 2.4 | Unordered Pairs | 6 |
| 2.5 | Unions | 6 |
| 2.6 | Intersections | 7 |
| 2.7 | Unordered Triples | 7 |
| 2.8 | Relative Complements | 8 |
| 2.9 | Symmetric Difference | 10 |
| 2.10 | Power Sets | 11 |
| 3 | Relations and Functions | 13 |
| 3.1 | Ordered Pairs | 13 |
| 3.2 | Relations | 14 |
| 3.3 | Composition | 14 |
| 3.4 | Inverses | 15 |
| 3.5 | Equivalence Relations | 15 |
| 3.6 | Functions | 16 |
| 3.7 | Families | 17 |
| 3.8 | Inverses and Composites of Functions | 19 |
| 3.9 | Choice Functions | 20 |
| 4 | Equivalence | 21 |
| 5 | Order | 22 |
| 5.1 | Well Orderings | 26 |
| 6 | Natural Numbers | 31 |
| 6.1 | Natural Numbers | 31 |
| 6.2 | Arithmetic | 35 |
| 6.3 | Order on the Natural Numbers | 40 |

| | | |
|----------|------------------------|-----------|
| 6.4 | Finite Sets | 43 |
| 7 | Ordinal Numbers | 47 |

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. \square

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. \square

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. \square

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 , $f : X \rightarrow Y$, 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 1.16 (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 .

Definition 1.17 (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 $\times_{i \in I} A$.

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

Axiom 1.19 (Axiom of substitution). *If $S(a, b)$ is a sentence such that for each a in A the set $\{b : S(a, b)\}$ can be formed, then there exists a function F with domain A such that $F(a) = \{b : S(a, b)\}$ for each a in A .*

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 . \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 $A \neq B$.

2.2 Comprehension Notation

Theorem 2.5. *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

2.3 The Empty Set

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

PROOF: Immediate from the Axiom of Infinity. \square

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. \square

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. \square

Proposition 2.11.

$$\bigcup \emptyset = \emptyset$$

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

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 . \square

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 $x \in A$. \square

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 $x \in A$. \square

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 $x \in B$ ". \square

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

PROOF: Immediate from definitions. \square

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 $x \in \emptyset$. \square

Proposition 2.20. For any set A , we have

$$A \cap A = A \text{ .}$$

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

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 $x \in A$ ". \square

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 " $((x \in A \wedge x \in B) \vee x \in C) \Leftrightarrow (x \in A \wedge (x \in B \vee x \in C))$ ". \square

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:

$\langle 1 \rangle 1$. 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.

\square

2.7 Unordered Triples

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

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

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 $E - (E - A) \subseteq E$.

□

Proposition 2.29. For any set E we have

$$E - \emptyset = E$$

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

Proposition 2.30. For any set E we have

$$E - E = \emptyset .$$

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

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 $x \in E - A$. □

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 $x \in E$.

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

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

□

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:

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

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

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

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

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

□

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 $A \not\subseteq B$.

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

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

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

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

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:

$\langle 1 \rangle 1$. 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 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 $x \in A \vee x \in B$. \square

Proposition 2.43 (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 2.44 (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

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. \square

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 . \square

Proposition 2.48. *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 2.49. *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

2.10 Power Sets

Proposition 2.50.

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

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

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

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

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

Proposition 2.52. *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 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:

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

□

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. \square

3.2 Relations

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

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

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

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

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. \square

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. \square

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*

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

PROOF: Easy. \square

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

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

PROOF: Easy. \square

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. \square

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

PROOF: Easy. \square

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

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

PROOF: Easy. \square

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

PROOF: Easy. \square

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. \square

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. \square

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. \square

3.6 Functions

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

Definition 3.31 (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 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 $X \rightarrow X$.*

PROOF: Easy. \square

Definition 3.34 (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 3.35 (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 3.36 (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 3.37 (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 3.38. 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 3.39. 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

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. \square

Proposition 3.41 (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 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. \square

Proposition 3.43 (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 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. \square

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. \square

Definition 3.46 (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 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. \square

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. \square

Proposition 3.49. *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 3.50. 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 $\bigcap_{i \in I} f(A_i) = \{c\}$.

3.8 Inverses and Composites of Functions

Definition 3.51 (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 3.52. *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 3.53. *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 3.54. *Let $f : X \rightarrow Y$. Let $B \subseteq Y$. Then*

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

PROOF: Easy. \square

Proposition 3.55. *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 3.56. *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 3.57. *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 3.58. *Let $f : X \rightarrow Y$ and $B \subseteq Y$. Then $f^{-1}(Y - B) = X - f^{-1}(B)$.*

PROOF: Easy. \square

Proposition 3.59. *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 3.60. *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 3.61. Example 3.14 shows that function composition is not commutative in general.

Proposition 3.62. *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 3.63. *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

3.9 Choice Functions

Definition 3.64 (Choice Function). A *choice function* for a set X is a function $f : \mathcal{P}X - \{\emptyset\} \rightarrow X$ 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 $\{S\}_{S \in \mathcal{P}X - \{\emptyset\}}$. \square

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

PROOF:

$\langle 1 \rangle 1$. LET: R be a relation.

$\langle 1 \rangle 2$. PICK a choice function g for $\text{ran } R$.

$\langle 1 \rangle 3$. LET: $f : \text{dom } R \rightarrow \text{ran } R$ be the function $f(x) = g(\{y \in \text{ran } R : xRy\})$

$\langle 1 \rangle 4$. $f \subseteq R$ and $\text{dom } f = \text{dom } R$.

\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:

$\langle 1 \rangle 1$. LET: f be a choice function for $\bigcup \mathcal{C}$

$\langle 1 \rangle 2$. LET: $A = \{f(C) : C \in \mathcal{C}\}$

$\langle 1 \rangle 3$. 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, \leq) such that \leq is a partial order on X . We write X for the poset (X, \leq) .

Given a partial order \leq , we write \geq for the inverse of \leq .

We write $x < y$ or $y > x$ for $x \leq y \wedge x \neq y$. 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. \square

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

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

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

PROOF:

$\langle 1 \rangle 1$. ASSUME: $x < y$ and $y < z$

$\langle 1 \rangle 2$. $x \leq y$ and $y \leq z$

$\langle 1 \rangle 3$. $x \leq z$

PROOF: Since \leq is transitive.

$\langle 1 \rangle 4$. $x \neq z$

PROOF: By Proposition 5.3.

\square

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

PROOF:

⟨1⟩1. \leq is reflexive.

PROOF: By definition.

⟨1⟩2. \leq is asymmetric.

PROOF: If $x \leq y$ and $y \leq x$, we must have $x = y$, because otherwise we would have $x < y$ and $y < x$.

⟨1⟩3. \leq is transitive.

⟨2⟩1. LET: $x \leq y$ and $y \leq z$

⟨2⟩2. CASE: $x = y$

PROOF: We have $y \leq z$ so $x \leq z$.

⟨2⟩3. CASE: $y = z$

PROOF: We have $x \leq y$ so $x \leq z$.

⟨2⟩4. CASE: $x < y$ and $y < z$

PROOF: We have $x < z$ by transitivity, so $x \leq z$.

□

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

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

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 $\forall x \in X. a \leq x$.

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

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

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

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

PROOF: If a and b are greatest then $a \leq b$ and $b \leq a$, 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 $\forall x \in E. a \leq x$.

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 $\forall x \in E. x \leq a$.

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 \leq on a set X is a *total order*, *simple order* or *linear order* iff, for all $x, y \in X$, either $x \leq y$ or $y \leq x$. We then call the poset (X, \leq) 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

Theorem 5.22 (Zorn's Lemma). Let X be a poset such that every chain in X has an upper bound. Then X has a maximal element.

PROOF:

$\langle 1 \rangle 1$. PICK a choice function f for X .

$\langle 1 \rangle 2$. LET: \mathcal{X} be the set of chains in X .

$\langle 1 \rangle 3$. For all $A \in \mathcal{X}$,

LET: $\hat{A} = \{x \in X : A \cup \{x\} \in \mathcal{X}\}$

$\langle 1 \rangle 4$. LET: $g : \mathcal{X} \rightarrow \mathcal{X}$ be the function

$$g(A) = \begin{cases} A \cup \{f(\hat{A} - A)\} & \text{if } \hat{A} - A \neq \emptyset \\ A & \text{if } \hat{A} - A = \emptyset \end{cases}$$

$\langle 1 \rangle 5$. For $\mathcal{T} \subseteq \mathcal{X}$, let us say \mathcal{T} is a *tower* iff:

- $\emptyset \in \mathcal{T}$
- $\forall A \in \mathcal{T}. g(A) \in \mathcal{T}$
- For every chain \mathcal{C} in \mathcal{T} , we have $\bigcup \mathcal{C} \in \mathcal{T}$

$\langle 1 \rangle 6$. LET: \mathcal{T}_0 be the intersection of the set of all towers.

PROOF: The set of all towers is nonempty since \mathcal{X} is a tower.

$\langle 1 \rangle 7$. LET: $A = \bigcup \mathcal{T}_0$

$\langle 1 \rangle 8$. A is a chain in X .

$\langle 2 \rangle 1$. \mathcal{T}_0 is a chain under \subseteq

$\langle 3 \rangle 1$. Given $C \in \mathcal{T}_0$, let us say that C is *comparable* iff, for all $A \in \mathcal{T}_0$, either $A \subseteq C$ or $C \subseteq A$.

$\langle 3 \rangle 2$. For all $A, C \in \mathcal{T}_0$, if C is comparable and $A \subsetneq C$ then $g(A) \subseteq C$.
 PROOF: Since $g(A) - A$ has at most one element, so if $A \subsetneq C \subseteq g(A)$ then $C = g(A)$.
 $\langle 3 \rangle 3$. For $C \in \mathcal{T}_0$ comparable,
 LET: $\mathcal{U}_C = \{A \in \mathcal{T}_0 : A \subseteq C \vee g(C) \subseteq A\}$
 $\langle 3 \rangle 4$. For $C \in \mathcal{T}_0$ comparable, \mathcal{U}_C is a tower.
 $\langle 4 \rangle 1$. LET: $C \in \mathcal{T}_0$ be comparable
 $\langle 4 \rangle 2$. $\emptyset \in \mathcal{U}_C$
 PROOF: Since $\emptyset \subseteq C$.
 $\langle 4 \rangle 3$. $\forall A \in \mathcal{U}_C. g(A) \in \mathcal{U}_C$
 PROOF: By $\langle 1 \rangle 8$.
 $\langle 4 \rangle 4$. For every chain $\mathcal{C} \subseteq \mathcal{U}_C$ we have $\bigcup \mathcal{C} \in \mathcal{U}_C$
 $\langle 5 \rangle 1$. LET: $\mathcal{C} \subseteq \mathcal{U}_C$ be a chain.
 $\langle 5 \rangle 2$. CASE: $\exists A \in \mathcal{C}. g(C) \subseteq A$
 PROOF: Then $g(C) \subseteq \bigcup \mathcal{C}$
 $\langle 5 \rangle 3$. CASE: $\forall A \in \mathcal{C}. A \subseteq C$
 PROOF: Then $\bigcup \mathcal{C} \subseteq C$.
 $\langle 3 \rangle 5$. For $C \in \mathcal{T}_0$ comparable, $\mathcal{U}_C = \mathcal{T}_0$.
 $\langle 3 \rangle 6$. For $C \in \mathcal{T}_0$ comparable we have $g(C)$ is comparable.
 PROOF: Since for all $A \in \mathcal{T}_0$ either $A \subseteq C \subseteq g(C)$ or $g(C) \subseteq A$.
 $\langle 3 \rangle 7$. The set of comparable sets in \mathcal{T}_0 is a tower.
 $\langle 4 \rangle 1$. \emptyset is comparable.
 PROOF: $\forall A \in \mathcal{T}_0. \emptyset \subseteq A$
 $\langle 4 \rangle 2$. For all $C \in \mathcal{T}_0$, if A is comparable then $g(C)$ is comparable.
 PROOF: $\langle 3 \rangle 6$
 $\langle 4 \rangle 3$. For every chain $\mathcal{C} \subseteq \mathcal{T}_0$ of comparable sets, we have $\bigcup \mathcal{C}$ is comparable.
 $\langle 5 \rangle 1$. LET: $\mathcal{C} \subseteq \mathcal{T}_0$ be a chain of comparable sets.
 $\langle 5 \rangle 2$. LET: $A \in \mathcal{T}_0$
 $\langle 5 \rangle 3$. CASE: there exists $C \in \mathcal{C}$ such that $A \subseteq C$
 PROOF: Then $A \subseteq \bigcup \mathcal{C}$.
 $\langle 5 \rangle 4$. CASE: for all $C \in \mathcal{C}$ we have $C \subseteq A$
 PROOF: Then $\bigcup \mathcal{C} \subseteq A$.
 $\langle 3 \rangle 8$. Every set in \mathcal{T}_0 is comparable.
 $\langle 2 \rangle 2$. LET: $x, y \in A$
 $\langle 2 \rangle 3$. PICK $A, C \in \mathcal{T}_0$ such that $x \in A$ and $y \in C$
 $\langle 2 \rangle 4$. ASSUME: w.l.o.g. $A \subseteq C$
 $\langle 2 \rangle 5$. $x, y \in C$
 $\langle 2 \rangle 6$. $x \leq y$ or $y \leq x$
 PROOF: Since $C \in \mathcal{X}$ so C is a chain.
 $\langle 1 \rangle 9$. PICK an upper bound u for A .
 $\langle 1 \rangle 10$. $A \in \mathcal{T}_0$
 PROOF: Since \mathcal{T}_0 is a chain in \mathcal{T}_0 so $\bigcup \mathcal{T}_0 \in \mathcal{T}_0$.
 $\langle 1 \rangle 11$. $g(A) \in \mathcal{T}_0$
 $\langle 1 \rangle 12$. $g(A) \subseteq A$
 $\langle 1 \rangle 13$. $g(A) = A$

⟨1⟩14. $\hat{A} - A = \emptyset$

⟨1⟩15. $u \in A$

PROOF: Since $A \cup \{u\}$ is a chain so $u \in \hat{A}$ and therefore $u \in A$.

⟨1⟩16. u is maximal in X .

⟨2⟩1. LET: $x \in X$

⟨2⟩2. ASSUME: $u \leq x$

⟨2⟩3. $A \cup \{x\}$ is a chain.

⟨2⟩4. $x \in A$

⟨2⟩5. $x \leq u$

⟨2⟩6. $x = u$

□

Definition 5.23 (Cofinal). Let X be a poset and $A \subseteq X$. Then A is *cofinal* iff, for all $x \in X$, there exists $a \in A$ such that $x \leq a$.

Definition 5.24 (Similar). Two posets X and Y are *similar*, $X \cong Y$ iff there exists an order preserving one-to-one correspondence f between them. We write $f : X \cong Y$ and call f a *similarity*.

Proposition 5.25. Let X and Y be posets. Let f be a one-to-one correspondence between X and Y . Then f is a similarity if and only if, for all $x, y \in X$, we have $x < y$ iff $f(x) < f(y)$.

PROOF: Easy. □

Proposition 5.26. For any poset X we have $I_X : X \cong X$.

PROOF: Easy. □

Proposition 5.27. If $f : X \cong Y$ then $f^{-1} : Y \cong X$.

PROOF: Easy. □

Proposition 5.28. If $f : X \cong Y$ and $g : Y \cong Z$ then $g \circ f : X \cong Z$.

PROOF: Easy. □

Corollary 5.28.1. For any set E , similarity is an equivalence relation on the set of all posets that are subsets of E .

5.1 Well Orderings

Definition 5.29 (Well Ordered Set). A poset X is *well ordered*, and its ordering is a *well ordering*, iff every nonempty subset of X has a least element.

Proposition 5.30. Every well ordered set is totally ordered.

PROOF: For all x and y we have $\{x, y\}$ has a least element, so $x \leq y$ or $y \leq x$. □

Theorem 5.31 (Transfinite Induction). *Let X be a well ordered set. Let $S \subseteq X$ satisfy:*

$$\forall x \in X (\forall y < x. y \in S) \Rightarrow x \in S .$$

Then $S = X$.

PROOF: We have $X - S$ has no least element, so $X - S = \emptyset$. \square

Definition 5.32 (Continuation). Let A and B be well ordered sets. Then B is a *continuation* of A iff there exists $b \in B$ such that $A = s(b)$ and the order on A is the restriction of the order on B to A .

Proposition 5.33. *Let \mathcal{C} be a set of well ordered sets that is totally ordered under continuation. Then there exists a unique well ordering on $\bigcup \mathcal{C}$ such that $\bigcup \mathcal{C}$ is a continuation of every element of \mathcal{C} .*

PROOF: Define \leq on $\bigcup \mathcal{C}$ by: $x \leq y$ iff there exists $C \in \mathcal{C}$ such that $x, y \in C$ and $x \leq y$ in C . \square

Proposition 5.34. *Every totally ordered set has a cofinal well ordered subset.*

PROOF:

$\langle 1 \rangle 1$. LET: X be a totally ordered set.

$\langle 1 \rangle 2$. LET: \mathcal{C} be the poset of all well ordered subsets of X under continuation.

$\langle 1 \rangle 3$. Every chain in \mathcal{C} has an upper bound.

PROOF: Proposition 5.33.

$\langle 1 \rangle 4$. PICK a maximal element C of \mathcal{C}

PROVE: C is cofinal

PROOF: Zorn's Lemma

$\langle 1 \rangle 5$. LET: $x \in X$

$\langle 1 \rangle 6$. We cannot have $\forall c \in C. c < x$

PROOF: Then $C \cup \{x\}$ would be a larger chain.

$\langle 1 \rangle 7$. $\exists c \in C. x \leq c$

\square

Theorem 5.35 (Well Ordering Theorem). *Every set can be well ordered.*

PROOF:

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

$\langle 1 \rangle 2$. LET: \mathcal{W} be the poset of all well ordered subsets of X under continuation.

$\langle 1 \rangle 3$. Every chain in \mathcal{W} has an upper bound.

PROOF: Proposition 5.33.

$\langle 1 \rangle 4$. PICK a maximal $M \in \mathcal{W}$

PROOF: Zorn's Lemma

$\langle 1 \rangle 5$. $M = X$

PROOF: If $x \in X - M$ then $M \cup \{x\}$ with x as the greatest element is a continuation of M .

\square

Theorem 5.36 (Transfinite Recursion). *Let W be a well ordered set and X a set. Let S be the set of all functions f such that $\text{ran } f \subseteq X$, and there exists $a \in W$ such that $\text{dom } f = s(a)$. Then there exists a unique function $U : W \rightarrow X$ such that*

$$\forall a \in W. U(a) = f(U \upharpoonright s(a)) .$$

PROOF:

$\langle 1 \rangle 1$. Let us say that a subset $A \subseteq W \times X$ is *f-closed* iff, whenever $a \in W$ and $t : s(a) \rightarrow X$ satisfies $\forall c < a. (c, t(c)) \in A$, then $(a, f(t)) \in A$.

$\langle 1 \rangle 2$. LET: U be the intersection of the set of *f-closed* subsets of $W \times X$

PROOF: This set is nonempty since $W \times X$ is *f-closed*.

$\langle 1 \rangle 3$. U is *f-closed*.

$\langle 1 \rangle 4$. U is a function.

$\langle 2 \rangle 1$. LET: $P(a)$ be the property: there is at most one $x \in X$ such that $(a, x) \in U$

$\langle 2 \rangle 2$. LET: $a \in W$

$\langle 2 \rangle 3$. ASSUME: as transfinite induction hypothesis $\forall c < a. P(c)$

$\langle 2 \rangle 4$. LET: $(a, x), (a, y) \in U$

$\langle 2 \rangle 5$. $x = f(U \upharpoonright c)$

PROOF: If not then $U - \{(a, x)\}$ would be *f-closed*.

$\langle 2 \rangle 6$. $y = f(U \upharpoonright c)$

$\langle 2 \rangle 7$. $x = y$

$\langle 1 \rangle 5$. $\text{dom } U = W$

$\langle 2 \rangle 1$. LET: $a \in W$

$\langle 2 \rangle 2$. ASSUME: as transfinite induction hypothesis $\forall c < a. c \in \text{dom } U$

$\langle 2 \rangle 3$. $(a, f(U \upharpoonright s(a))) \in U$

$\langle 1 \rangle 6$. If $U' : W \rightarrow X$ and $\forall a \in W. U'(a) = f(U' \upharpoonright s(a))$, then $U' = U$.

PROOF: Prove $U'(a) = U(a)$ by transfinite induction on a .

□

Proposition 5.37. *Let X be a well ordered set and f a similarity between X and a subset of X . Then, for all $a \in X$, we have $a \leq f(a)$.*

PROOF:

$\langle 1 \rangle 1$. LET: $a \in X$

$\langle 1 \rangle 2$. ASSUME: as transfinite induction hypothesis $\forall c < a. c \leq f(c)$

$\langle 1 \rangle 3$. ASSUME: for a contradiction $f(a) < a$

$\langle 1 \rangle 4$. $f(a) \leq f(f(a))$

PROOF: $\langle 1 \rangle 2$

$\langle 1 \rangle 5$. $f(f(a)) < f(a)$

PROOF: From $\langle 1 \rangle 3$ since f is a similarity.

$\langle 1 \rangle 6$. Q.E.D.

PROOF: This is a contradiction.

□

Proposition 5.38. *Let X and Y be well ordered sets. Then there is at most one similarity between them.*

PROOF:

- ⟨1⟩1. LET: $f, g : X \cong Y$
 PROVE: $\forall a \in X. f(a) = g(a)$
- ⟨1⟩2. LET: $a \in X$
- ⟨1⟩3. ASSUME: as transfinite induction hypothesis $\forall c < a. f(c) = g(c)$
- ⟨1⟩4. $f(a)$ is the least element of $Y - \{f(c) : c < a\}$
- ⟨1⟩5. $g(a)$ is the least element of $Y - \{g(c) : c < a\}$
- ⟨1⟩6. $f(a) = g(a)$

□

Proposition 5.39. *A well ordered set is not similar to any of its initial segments.*

PROOF:

- ⟨1⟩1. LET: X be a well ordered set.
- ⟨1⟩2. ASSUME: for a contradiction $f : X \cong s(a)$ for some $a \in X$
- ⟨1⟩3. $f(a) < a$
- ⟨1⟩4. Q.E.D.

PROOF: This contradicts Proposition 5.37.

□

Theorem 5.40 (Comparability Theorem). *Given well ordered sets X and Y , either $X \cong Y$, or X is similar to an initial segment of Y , or Y is similar to an initial segment of X .*

PROOF:

- ⟨1⟩1. LET: $X_0 = \{a \in X : \exists b \in Y. s(a) \cong s(b)\}$
- ⟨1⟩2. LET: $U : X_0 \rightarrow Y$ be the function: for $a \in X_0$, we have $U(a)$ is the unique element in Y such that $s(a) \cong s(U(a))$
- ⟨1⟩3. LET: $Y_0 = \text{ran } U$
- ⟨1⟩4. Either $X_0 = X$ or there exists $a \in X$ such that $X_0 = s(a)$
 - ⟨2⟩1. ASSUME: $X_0 \neq X$
 - ⟨2⟩2. LET: a be the least element of $X - X_0$
 - ⟨2⟩3. LET: $x \in X_0$
 PROVE: $x < a$
 - ⟨2⟩4. PICK $f : s(x) \cong s(U(x))$
 - ⟨2⟩5. ASSUME: for a contradiction $a < x$
 - ⟨2⟩6. $f \upharpoonright s(a) : s(a) \cong s(f(a))$
 - ⟨2⟩7. $a \in X_0$
 - ⟨2⟩8. Q.E.D.

PROOF: This is a contradiction.

- ⟨1⟩5. Either $Y_0 = Y$ or there exists $b \in Y$ such that $Y_0 = s(b)$

PROOF: Similar.

- ⟨1⟩6. CASE: $X_0 = X$ and $Y_0 = Y$

PROOF: Then $U : X \cong Y$.

- ⟨1⟩7. CASE: $X_0 = X$ and $Y_0 \neq Y$

PROOF: Then $U : X \cong s(b)$ where $Y_0 = s(b)$.

⟨1⟩8. CASE: $X_0 \neq X$ and $Y_0 = Y$

PROOF: Then $U : s(a) \cong Y$ where $X_0 = s(a)$.

⟨1⟩9. CASE: $X_0 \neq X$ and $Y_0 \neq Y$

⟨2⟩1. LET: $X_0 = s(a)$ and $Y_0 = s(b)$

⟨2⟩2. $U : s(a) \cong s(b)$

⟨2⟩3. $a \in X_0$

⟨2⟩4. Q.E.D.

PROOF: This is a contradiction.

□

Corollary 5.40.1. *Let X be a well ordered set. Then any subset A of X is either similar to X or to an initial segment of X .*

PROOF: We cannot have X is similar to an initial segment of A , say $f : X \cong \{x \in A : x < a\}$, because then we would have $f(a) < a$ contradicting Proposition 5.37. □

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

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

etc.

Definition 6.3 (Characteristic Function). Let X be a set and $A \subseteq X$. The *characteristic function* of A is the function $\chi_A : X \rightarrow 2$ 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 $\chi : \mathcal{P}X \rightarrow 2^X$ that maps a subset A of X to χ_A is a one-to-one correspondence.

PROOF: Easy. \square

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

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:

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

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

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: $m \in n^+$

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

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

PROOF: $\langle 2 \rangle 2$

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

\square

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 . \square

Proposition 6.9.

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

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 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:

$\langle 1 \rangle 1$. 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 6.12. *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 6.11).

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

PROOF: This contradicts Proposition 6.9.

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

□

Theorem 6.13 (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 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 . □

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:

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

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:

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

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

PROOF:

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

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

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

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

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

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

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:

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

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

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

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

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

PROOF:

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

□

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

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

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

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

PROOF:

⟨1⟩1. $(m^n)^0 = m^{n0}$

PROOF: Both are equal to 1.

⟨1⟩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 $m \leq n$ iff $m < n \vee m = n$.

Proposition 6.28. *The relation \leq is a well ordering on ω .*

PROOF:

⟨1⟩1. \leq is a partial order on ω .

⟨2⟩1. $<$ is transitive.

PROOF: Proposition 6.11.

⟨2⟩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.

⟨2⟩3. Q.E.D.

⟨1⟩2. Any nonempty set E of natural numbers has a least element.

⟨2⟩1. LET: $E \subseteq \omega$

⟨2⟩2. ASSUME: E has no least element.

PROVE: $E = \emptyset$

⟨2⟩3. LET: $P(n)$ be the property $\forall m < n. m \notin E$

⟨2⟩4. $P(0)$

PROOF: Vacuous.

⟨2⟩5. For any natural number n , if $P(n)$ then $P(n+1)$

PROOF: If $P(n)$ then $n \notin E$ (otherwise n would be the least element of E) and so $P(n+1)$.

⟨2⟩6. $\forall n \in \omega. P(n)$

⟨2⟩7. $\forall n \in \omega. n \notin E$

□

Proposition 6.29. *For any natural numbers m and n , we have $m \in n$ if and only if $m \subsetneq n$.*

PROOF:

⟨1⟩1. LET: m and n be natural numbers.

⟨1⟩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. *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: $P(n)$

- ⟨2⟩3. LET: X be a proper subset of $n + 1$
- ⟨2⟩4. CASE: $X - \{n\} = n$
PROOF: Then $X = n$ so $X \sim n < n + 1$.
- ⟨2⟩5. CASE: $X - \{n\} \subsetneq n$
 - ⟨3⟩1. PICK $m < n$ such that $X - \{n\} \sim m$
 - ⟨3⟩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 6.33. *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. $f(k) = n$

□

Corollary 6.33.1. *Equivalent natural numbers are equal.*

Definition 6.34 (Lexicographical Order). The *lexicographical* order on $\omega \times \omega$ is the relation S defined by $(a, b)S(x, y)$ iff $a < x$ or $(a = x \text{ and } b < y)$.

Proposition 6.35. *The lexicographical order is a well ordering on $\omega \times \omega$.*

PROOF: Easy. □

6.4 Finite Sets

Definition 6.36 (Finite). A set is *finite* iff it is equivalent to a natural number; otherwise, it is *infinite*.

Proposition 6.37. *No finite set is equivalent to one of its proper subsets.*

PROOF: From Proposition 6.33. □

Proposition 6.38. *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 6.39. *Every subset of a finite set is finite.*

PROOF: Proposition 6.32. □

Definition 6.40 (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 6.41. *Let E and F be finite sets. If $E \subseteq F$ then $\sharp(E) \leq \sharp(F)$.*

PROOF: Proposition 6.32. □

Proposition 6.42. *Let E and F be disjoint finite sets. Then $E \cup F$ is finite and $\sharp(E \cup F) = \sharp(E) + \sharp(F)$.*

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 $E \cap F = \emptyset$, 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. $F = \emptyset$

⟨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: $E \cap F = \emptyset$
- ⟨2⟩6. PICK $f \in F$
- ⟨2⟩7. $F - \{f\} \sim n$
- ⟨2⟩8. $E \cap (F - \{f\}) = \emptyset$
- ⟨2⟩9. $E \cup (F - \{f\}) \sim m + n$
- PROOF: ⟨2⟩2
- ⟨2⟩10. $E \cup F \sim m + n + 1$

□

Corollary 6.42.1. *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 6.43. *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 6.42.

□

Proposition 6.44. *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: $\phi : E^F \rightarrow E^{F-\{f\}} \times E$ be the function $\phi(g) = (g \upharpoonright (F - \{f\}), g(f))$
- ⟨2⟩8. ϕ is a one-to-one correspondence
- ⟨2⟩9. $\sharp(E^F) = m^{n+1}$

PROOF:

$$\begin{aligned}
 \sharp(E^F) &= \sharp(E^{F-\{f\}} \times E) \\
 &= \sharp(E^{F-\{f\}}) \sharp(E) && \text{(Proposition 6.43)} \\
 &= m^n m && (\langle 2 \rangle 2, \langle 2 \rangle 4) \\
 &= m^{n+1}
 \end{aligned}$$

□

Corollary 6.44.1. *If E is finite then $\mathcal{P}E$ is finite and $\sharp(\mathcal{P}E) = 2^{\sharp(E)}$.*

Proposition 6.45. *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 6.42.1.

□

Proposition 6.46. *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 $\{k\}$.
 $\langle 1 \rangle 3$. $\forall n \geq 1. P(n) \Rightarrow P(n+1)$
 $\langle 2 \rangle 1$. LET: $n \geq 1$
 $\langle 2 \rangle 2$. ASSUME: $P(n)$
 $\langle 2 \rangle 3$. ASSUME: $E \subseteq \omega$ and $E \sim n+1$
 $\langle 2 \rangle 4$. PICK $k \in E$
 $\langle 2 \rangle 5$. LET: l be the greatest element of $E - \{k\}$
 $\langle 2 \rangle 6$. Either k or l is greatest in E .
 \square

Proposition 6.47. *Every infinite set has a subset equivalent to ω .*

PROOF:
 $\langle 1 \rangle 1$. LET: X be an infinite set.
 $\langle 1 \rangle 2$. PICK a choice function f for X .
 $\langle 1 \rangle 3$. LET: \mathcal{C} be the set of all finite subsets of X .
 $\langle 1 \rangle 4$. For all $A \in \mathcal{C}$ we have $X - A \in \text{dom } f$.
PROOF: For all $A \in \mathcal{C}$ we have $X - A \neq \emptyset$.
 $\langle 1 \rangle 5$. LET: $U : \omega \rightarrow \mathcal{C}$ be the function defined recursively by $U(0) = \emptyset$ and
 $U(n+1) = U(n) \cup \{f(X - U(n))\}$ for all $n \in \omega$.
 $\langle 1 \rangle 6$. LET: $v : \omega \rightarrow X$ 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 $v(n) = f(X - U(n)) \in X - U(n)$.
 $\langle 1 \rangle 8$. $\forall n \in \omega. v(n) \in U(n+1)$
 $\langle 1 \rangle 9$. $\forall m, n \in \omega. n \leq m \Rightarrow U(n) \subseteq U(m)$
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

Corollary 6.47.1. *A set is infinite if and only if it is equivalent to a proper subset.*

Chapter 7

Ordinal Numbers

Definition 7.1 (Ordinal (Number)). An *ordinal (number)* is a well ordered set α such that $\forall \xi \in \alpha. s(\xi) = \xi$.

Given ordinals α, β , we write $\alpha < \beta$ iff $\alpha \in \beta$.

Proposition 7.2. *Every natural number is an ordinal.*

PROOF: Easy. \square

Proposition 7.3. ω is an ordinal.

PROOF: Easy. \square

Proposition 7.4. If α is an ordinal number then so is α^+ .

PROOF: Easy. \square

Proposition 7.5. Let α be an ordinal and $\eta, \xi \in \alpha$. Then $\eta < \xi$ if and only if $\eta \in \xi$.

PROOF: Easy. \square

Proposition 7.6. Every ordinal is a transitive set.

PROOF: Easy. \square

Proposition 7.7. Every element of an ordinal is an ordinal.

PROOF: Easy. \square

Proposition 7.8. Similar ordinals are equal.

PROOF:

$\langle 1 \rangle 1$. LET: α, β be ordinals.

$\langle 1 \rangle 2$. LET: $f : \alpha \cong \beta$ be a similarity.

PROVE: $\forall \xi \in \alpha. f(\xi) = \xi$

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

$\langle 1 \rangle 4$. ASSUME: as transfinite induction hypothesis $\forall \eta < \xi. f(\eta) = \eta$
 $\langle 1 \rangle 5$. $f(\xi) \subseteq \xi$
 $\langle 2 \rangle 1$. LET: $\eta \in f(\xi)$
 $\langle 2 \rangle 2$. PICK $\zeta \in \alpha$ such that $f(\zeta) = \eta$
 $\langle 2 \rangle 3$. $\zeta \in \xi$
PROOF: Since $f(\zeta) \in f(\xi)$ and f is a similarity.
 $\langle 2 \rangle 4$. $f(\zeta) = \zeta$
PROOF: $\langle 1 \rangle 4$
 $\langle 2 \rangle 5$. $\eta = \zeta$
PROOF: $\langle 2 \rangle 2, \langle 2 \rangle 4$
 $\langle 2 \rangle 6$. $\eta \in \xi$
PROOF: $\langle 2 \rangle 3, \langle 2 \rangle 5$
 $\langle 1 \rangle 6$. $\xi \subseteq f(\xi)$
 $\langle 2 \rangle 1$. LET: $\eta \in \xi$
 $\langle 2 \rangle 2$. $\eta = f(\eta) \in f(\xi)$
 $\langle 1 \rangle 7$. $f(\xi) = \xi$
 \square

Proposition 7.9. *Let α and β be ordinals. Then the following are equivalent.*

1. $\alpha \in \beta$
2. $\alpha \subsetneq \beta$
3. β is a continuation of α .

PROOF:

$\langle 1 \rangle 1$. $1 \Rightarrow 3$
PROOF: If $\alpha \in \beta$ then $\alpha = s(\alpha)$.
 $\langle 1 \rangle 2$. $3 \Rightarrow 2$
PROOF: Immediate from definitions.
 $\langle 1 \rangle 3$. $2 \Rightarrow 1$
 $\langle 2 \rangle 1$. LET: γ be the least element of β such that $\gamma \notin \alpha$
 $\langle 2 \rangle 2$. $\alpha \subseteq \gamma$
 $\langle 3 \rangle 1$. LET: $\eta \in \alpha$
 $\langle 3 \rangle 2$. $\eta \subseteq \alpha$
 $\langle 3 \rangle 3$. $\gamma \notin \eta$
 $\langle 3 \rangle 4$. $\eta \in \gamma$ or $\eta = \gamma$
 $\langle 3 \rangle 5$. $\eta \neq \gamma$
PROOF: Since $\eta \in \alpha$ and $\gamma \notin \alpha$.
 $\langle 3 \rangle 6$. $\eta \in \gamma$
 $\langle 2 \rangle 3$. $\gamma \subseteq \alpha$
PROOF: For all $\eta \in \gamma$ we have $\eta \in \alpha$ by leastness of γ .
 $\langle 2 \rangle 4$. $\gamma = \alpha$
 $\langle 2 \rangle 5$. $\alpha \in \beta$
 \square

Proposition 7.10. *For any ordinal numbers α and β , either $\alpha = \beta$, or $\alpha < \beta$, or $\beta < \alpha$.*

PROOF:

- ⟨1⟩1. Either $\alpha = \beta$, or α is similar to an initial segment of β , or β is similar to an initial segment of α .
- ⟨1⟩2. CASE: α is similar to an initial segment of β .
 - ⟨2⟩1. PICK $\eta \in \beta$ such that $\alpha \sim s(\eta)$
 - ⟨2⟩2. $\alpha \sim \eta$
 - ⟨2⟩3. $\alpha = \eta$
 - PROOF: Proposition 7.8.
 - ⟨2⟩4. $\alpha \in \beta$
- ⟨1⟩3. CASE: β is similar to an initial segment of α .
 PROOF: Then $\beta \in \alpha$ similarly.

□

Proposition 7.11. *Every set of ordinals is well ordered by $<$.*

PROOF:

- ⟨1⟩1. LET: E be a set of ordinals.
- ⟨1⟩2. LET: A be a nonempty subset of E .
- ⟨1⟩3. PICK $\alpha \in A$
- ⟨1⟩4. CASE: $\alpha \cap A = \emptyset$
 PROOF: Then α is least in A .
- ⟨1⟩5. CASE: $\alpha \cap A \neq \emptyset$
 PROOF: Then $\alpha \cap A$ has a least element, which is least in A .

□

Definition 7.12 (Limit Ordinal). A *limit ordinal* is an ordinal number that is not 0 and not α^+ for any ordinal α .

Proposition 7.13. *For any set E of ordinal numbers, $\bigcup E$ is an ordinal and is the supremum of E .*

PROOF: Proposition 5.33. □

Theorem 7.14 (Burali-Forti Paradox). *There is no set whose members are exactly the ordinal numbers.*

PROOF: For any set of ordinals E , we have $(\bigcup E)^+$ is an ordinal that is not in E . □

Theorem 7.15 (Counting Theorem). *Every well ordered set is similar to a unique ordinal.*

PROOF:

- ⟨1⟩1. LET: X be a well ordered set.
- ⟨1⟩2. There exists an ordinal α such that $X \cong \alpha$.
 - ⟨2⟩1. For all $a \in X$, there exists a unique ordinal α such that $s(a) \cong \alpha$
 - ⟨3⟩1. LET: $a \in X$
 - ⟨3⟩2. ASSUME: as transfinite induction hypothesis that, for all $b < a$, there exists a unique ordinal β such that $s(b) \cong \beta$

