Summary of Halmos' Naive Set Theory

Robin Adams

August 28, 2023

Contents

1 Primitive Terms and Axioms **3**

2 Basic Properties and Operations on Sets **5**
2.1 The Subset Relation 6
2.2 Comprehension Notation 7
2.3 The Empty Set 7
2.4 Unordered Pairs 7
2.5 Unions 7
2.6 Intersections 8
2.7 Unordered Triples 9
2.8 Relative Complements 9
2.9 Symmetric Difference 12
2.10 Power Sets 13

3 Relations and Functions **15**
3.1 Ordered Pairs 15
3.2 Relations 16
3.3 Composition 16
3.4 Inverses 17
3.5 Equivalence Relations 17
3.6 Functions 18
3.7 Families 21
3.8 Inverses and Composites of Functions 23
3.8.1 Inverse Image 23
3.8.2 Inverse of a Function 25
3.9 Choice Functions 28

4 Equivalence **29**

5 Order **31**
5.1 Partial Orders 31
5.2 Linear Orders 34
5.3 Linear Continua 40
5.4 Well Orderings 40

6 Natural Numbers **45**
6.1 Natural Numbers 45

7 Ordinal Numbers **50**
7.1 Order on the Natural Numbers 53
7.2 Finite Sets 55
7.3 Ordinal Arithmetic 59
7.4 Arithmetic on the Natural Numbers 60

8 Countable Sets **63**

9 Cardinal Numbers **65**
9.1 Cardinal Arithmetic 65
9.2 Alephs 69

10 Field Theory **70**

11 Real Numbers **71**
11.1 Axioms for Real Numbers 71
11.2 Consequences of the Axioms 72
11.2.1 Negation 72
11.2.2 Subtraction 73

12 Integers **78**

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 $x \notin A$.

Definition 1.1 (Empty). A set is *empty* iff it has no elements; otherwise it is *nonempty.*

Definition 1.2 (Disjoint). Two sets A and B are *disjoint* iff there is no x such that $x \in A$ and $x \in B$.

Definition 1.3 (Pairwise Disjoint). We say the elements of a set x are *pairwise disjoint* iff, for all $y, z \in x$, either y and z are disjoint or $y = z$.

Definition 1.4 (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 1.5 (Axiom of Extensionality). *If two sets have the same elements then they are equal.*

Axiom 1.6 (Axiom of Regularity). *For any nonempty set A, there exists $m \in A$ such that m and A are disjoint.*

Axiom 1.7 (Axiom of Union). *For every set A, there exists a set that contains all the elements that belong to at least one element of A.*

Axiom 1.8 (Axiom of Pairing). *For any two sets, there exists a set that they both belong to.*

Axiom Schema 1.9 (Axiom Schema of Replacement). *For any property $P(x, y)$, the following is an axiom:*

Let A be a set such that, for all $x \in A$, there exists at most one y such that $P(x, y)$. Then there exists a set B whose elements are exactly those sets y such that $\exists x \in A.P(x, y)$.

Axiom 1.10 (Axiom of Infinity)**.** *There exists a set I that has an empty element and such that, for all $x \in I$, there exists $y \in I$ such that the elements of y are exactly x and the elements of x.*

Axiom 1.11 (Power Set Axiom)**.** *For any set A, there exists a set B such that every subset of A belongs to B.*

Axiom 1.12 (Axiom of Choice)**.** *Let A be a set of nonempty, pairwise disjoint sets. Then there exists a set C such that, for all $x \in A$, there is exactly one y such that $y \in C$ and $y \in x$.*

Chapter 2

Basic Properties and Operations on Sets

Axiom 2.1 (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 2.2. 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. □

Definition 2.3 ((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 2.4 (Power Set Axiom)**.** *For any set A, there exists a set that contains all the subsets of A.*

Definition 2.5 (Empty)**.** A set is *empty* iff it has no elements; otherwise it is *non-empty.*

Axiom 2.6 (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 2.7 (Ordered Pair)**.** For any sets a and b, the *ordered pair* (a, b) is defined by

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

Definition 2.8 (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 2.9 (Cartesian Product)**.** For any sets A and B, the *Cartesian product* $A \times B$ is

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

Definition 2.10 (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 2.11 (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 2.12 (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 2.13 (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 2.14 (Axiom of Choice)**.** *The Cartesian product of a non-empty family of non-empty sets is non-empty.*

Axiom 2.15 (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.*

2.1 The Subset Relation

Theorem 2.16. *For any set A, we have $A \subseteq A$.*

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

Theorem 2.17. *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 2.18. *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 2.19 (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 2.20. *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 2.21. *There exists a set with no elements.*

PROOF: Immediate from the Axiom of Infinity. □

Definition 2.22 (Empty Set)**.** The *empty set* $\emptyset$ is the set with no elements.

Theorem 2.23. *For any set A we have $\emptyset \subset A$.*

PROOF: Vacuous. □

2.4 Unordered Pairs

Definition 2.24 (Singleton)**.** For any set a, the *singleton* $\{a\}$ is defined to be $\{a, a\}$.

2.5 Unions

Definition 2.25 (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 2.26.

$$\bigcup \emptyset = \emptyset$$

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

Proposition 2.27. *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 2.28. We write $A \cup B$ for $\bigcup\{A, B\}$.

Proposition 2.29. *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 2.30 (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 2.31. *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 2.32. *For any sets a and b, we have $\{a\} \cup \{b\} = \{a, b\}$.*

Proof: Immediate from definitions. ∎

2.6 Intersections

Definition 2.33 (Intersection)**.** For any sets A and B, the *intersection* $A \cap B$ is defined to be $\{x \in A : x \in B\}$.

Proposition 2.34. *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 2.35. *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 2.36. *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 2.37. *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 2.38 (Disjoint)**.** Two sets A and B are *disjoint* if and only if $A \cap B = \emptyset$.

Definition 2.39 (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 2.40 (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.
$\square$

2.7 Unordered Triples

Definition 2.41 ((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 2.42 (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 2.43. *For any sets A and E, we have $A \subseteq E$ if and only if*

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

PROOF:
⟨1⟩1. LET: A and E be sets.
⟨1⟩2. If $A \subseteq E$ then $E - (E - A) = A$
  ⟨2⟩1. ASSUME: $A \subseteq E$
  ⟨2⟩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 2.44. *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 2.45. *For any set E we have*

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

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

Proposition 2.46. *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 2.47. *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 2.48. *Let A, B and E be sets. Then:*

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

PROOF:
$\langle 1 \rangle 1$. LET: A, B and E be sets.
$\langle 1 \rangle 2$. If $A \subseteq B$ then $E - B \subseteq E - A$.
PROOF: If $A \subseteq B$, $x \in E$ and $x \notin B$, then we have $x \in E$ and $x \notin A$.

$\langle 1 \rangle 3$. If $A \subseteq E$ and $E - B \subseteq E - A$ then $A \subseteq B$.
$\langle 2 \rangle 1$. Assume: $A \subseteq E$
$\langle 2 \rangle 2$. Assume: $E - B \subseteq E - A$
$\langle 2 \rangle 3$. Let: $x \in A$
$\langle 2 \rangle 4$. $x \in E$
$\langle 2 \rangle 5$. $x \notin E - A$
$\langle 2 \rangle 6$. $x \notin E - B$
$\langle 2 \rangle 7$. $x \in B$
$\square$

Example 2.49. 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 2.50 (De Morgan's Law)**.** *For any sets A, B and E, we have* $E - (A \cup B) = (E - A) \cap (E - B)$.

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

Proposition 2.51 (De Morgan's Law)**.** *For any sets A, B and E, we have* $E - (A \cap B) = (E - A) \cup (E - B)$.

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

Proposition 2.52. *For any sets A, B and E, if $A \subseteq E$ then*

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

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

Proposition 2.53. *For any sets A and B, we have $A \subseteq B$ if and only if $A - B = \emptyset$.*

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

Proposition 2.54. *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 2.55. *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 2.56. *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 $x \in B \cap (E - C)$.
∎

Proposition 2.57. *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 2.58 (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 2.59 (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 2.60 (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 2.61. *For any sets A and B, we have*

$$A + B = B + A$$

PROOF: From the commutativity of union. ∎

Proposition 2.62. *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 2.63. *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 2.64. *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 2.65.

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

Proof: The only subset of $\emptyset$ is $\emptyset$. $\square$

Proposition 2.66. *For any set a, we have*

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

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

Proposition 2.67. *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 2.68. *For any nonempty set $\mathcal{C}$ we have*

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

Proof:

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

$\square$

Proposition 2.69. *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 2.70. *For any set E, we have*

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

Proof: Since $\varnothing \in \mathcal{P}E$. □

Proposition 2.71. *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:
⟨1⟩1. Let: a, b, x and y be sets.
⟨1⟩2. Assume: $(a,b) = (x,y)$
⟨1⟩3. $a = x$
  Proof: $\{a\} = \bigcap(a,b) = \bigcap(x,y) = \{x\}$.
⟨1⟩4. $\{a,b\} = \{x,y\}$
⟨1⟩5. Case: $a = b$
  ⟨2⟩1. $x = y$
    Proof: Since $\{x,y\} = \{a,b\}$ is a singleton.
  ⟨2⟩2. $b = y$
    Proof: $b = a = x = y$
⟨1⟩6. Case: $a \neq b$
  ⟨2⟩1. $x \neq y$
    Proof: Since $\{x,y\} = \{a,b\}$ is not a singleton.
  ⟨2⟩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 (Injective)**.** A function $f : X \to Y$ is *one-to-one* or *injective* or an *injection* iff, for all $x, y \in X$, if $f(x) = f(y)$ then $x = y$. In this case, we write $f : X \rightarrowtail Y$.

Definition 3.31 (Surjective)**.** Let $f : X \to Y$. We say f is *surjective*, or a *surjection*, or f maps X *onto* Y iff $\operatorname{ran} f = Y$. In this case, we write $f : X \twoheadrightarrow Y$.

Definition 3.32 (Bijective)**.** Let $f : X \to Y$. Then f is *bijective*, or a *bijection*, iff it is injective and surjective.

Definition 3.33 (Image)**.** Let $f : X \to Y$ and $A \subseteq X$. The *image* of A under f is

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

Proposition 3.34. *Let $f : X \to Y$ and $A \subseteq B \subseteq X$. Then $f(A) \subseteq f(B)$.*

Proof:
⟨1⟩1. Let: X and Y be sets.
⟨1⟩2. Let: $f : X \to Y$
⟨1⟩3. Let: $A, B \in \mathcal{P}X$ with $A \subseteq B$.
⟨1⟩4. Let: $y \in f(A)$
⟨1⟩5. Pick $x \in A$ such that $f(x) = y$
  Proof: ⟨1⟩4
⟨1⟩6. $x \in B$
  Proof: ⟨1⟩3, ⟨1⟩5
⟨1⟩7. $y \in f(B)$
  Proof: ⟨1⟩5, ⟨1⟩6

$\square$

Proposition 3.35. *Let $f : X \to Y$. Let $\mathcal{A} \subseteq \mathcal{P}X$. Then $f\left(\bigcup \mathcal{A}\right) = \bigcup_{A \in \mathcal{A}} f(A)$.*

PROOF:

$$\begin{aligned} y \in f\left(\bigcup \mathcal{A}\right) &\Leftrightarrow \exists x \in \bigcup \mathcal{A}. y = f(x) \\ &\Leftrightarrow \exists x. \exists A \in \mathcal{A}(x \in A \wedge y = f(x)) \\ &\Leftrightarrow \exists A \in \mathcal{A}. \exists x \in A. y = f(x) \\ &\Leftrightarrow \exists A \in \mathcal{A}. y \in f(A) \\ &\Leftrightarrow y \in \bigcup_{A \in \mathcal{A}} f(A) \end{aligned}$$

$\square$

Proposition 3.36. *Let $f : X \to Y$. Let $\mathcal{A}$ be a nonempty subset of $\mathcal{P}X$. Then $f\left(\bigcap \mathcal{A}\right) \subseteq \bigcap_{A \in \mathcal{A}} f(A)$. Equality holds if f is injective.*

PROOF:
⟨1⟩1. LET: X and Y be sets.
⟨1⟩2. LET: $f : X \to Y$
⟨1⟩3. LET: $\mathcal{A}$ be a nonempty subset of $\mathcal{P}X$.
⟨1⟩4. $f\left(\bigcap \mathcal{A}\right) \subseteq \bigcap_{A \in \mathcal{A}} f(A)$
  ⟨2⟩1. LET: $y \in f\left(\bigcap \mathcal{A}\right)$
  ⟨2⟩2. PICK $x \in \bigcap \mathcal{A}$ such that $y = f(x)$
    PROOF: ⟨2⟩1
  ⟨2⟩3. LET: $A \in \mathcal{A}$
  ⟨2⟩4. $x \in A$
    PROOF: ⟨2⟩2, ⟨2⟩3
  ⟨2⟩5. $y \in f(A)$
    PROOF: ⟨2⟩2, ⟨2⟩4
⟨1⟩5. If f is injective then $f\left(\bigcap \mathcal{A}\right) = \bigcap_{A \in \mathcal{A}} f(A)$
  ⟨2⟩1. ASSUME: f is injective.
  ⟨2⟩2. LET: $y \in \bigcap_{A \in \mathcal{A}} f(A)$
  ⟨2⟩3. PICK $A \in \mathcal{A}$
    PROOF: $\mathcal{A}$ is nonempty by ⟨1⟩3.
  ⟨2⟩4. $y \in f(A)$
    PROOF: ⟨2⟩2, ⟨2⟩3
  ⟨2⟩5. PICK $x \in A$ such that $y = f(x)$
    PROOF: ⟨2⟩4
  ⟨2⟩6. $x \in \bigcap \mathcal{A}$
    ⟨3⟩1. LET: $A' \in \mathcal{A}$
    ⟨3⟩2. $y \in f(A')$
      PROOF: ⟨2⟩2, ⟨3⟩1
    ⟨3⟩3. PICK $x' \in A'$ such that $y = f(x')$
      PROOF: ⟨3⟩2
    ⟨3⟩4. $x = x'$
      PROOF: ⟨2⟩1, ⟨2⟩5, ⟨3⟩3
    ⟨3⟩5. $x \in A'$

PROOF: $\langle 3\rangle 3$, $\langle 3\rangle 4$

$\langle 2\rangle 7$. $y \in f\left(\bigcap \mathcal{A}\right)$

PROOF: $\langle 2\rangle 5$, $\langle 2\rangle 6$

□

Proposition 3.37. *Let X and Y be sets. Let $f : X \to Y$. Let $A, B \in \mathcal{P}X$. Then $f(A) - f(B) \subseteq f(A - B)$. Equality holds if f is injective.*

PROOF:

$\langle 1\rangle 1$. LET: X and Y be sets.

$\langle 1\rangle 2$. LET: $f : X \to Y$

$\langle 1\rangle 3$. LET: $A, B \in \mathcal{P}X$

$\langle 1\rangle 4$. $f(A) - f(B) \subseteq f(A - B)$

$\langle 2\rangle 1$. LET: $y \in f(A) - f(B)$

$\langle 2\rangle 2$. $y \in f(A)$

PROOF: $\langle 2\rangle 1$

$\langle 2\rangle 3$. PICK $x \in A$ such that $y = f(x)$.

PROOF: $\langle 2\rangle 2$

$\langle 2\rangle 4$. $x \notin B$

$\langle 3\rangle 1$. ASSUME: for a contradiction $x \in B$

$\langle 3\rangle 2$. $y \in f(B)$

PROOF: $\langle 2\rangle 3$, $\langle 3\rangle 1$

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

PROOF: $\langle 2\rangle 1$ and $\langle 3\rangle 2$ form a contradiction.

$\langle 2\rangle 5$. $x \in A - B$

PROOF: $\langle 2\rangle 3$, $\langle 2\rangle 4$

$\langle 2\rangle 6$. $y \in f(A - B)$

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

$\langle 1\rangle 5$. If f is injective then $f(A - B) = f(A) - f(B)$.

$\langle 2\rangle 1$. ASSUME: f is injective.

$\langle 2\rangle 2$. LET: $y \in f(A - B)$

$\langle 2\rangle 3$. PICK $x \in A - B$ such that $y = f(x)$

PROOF: $\langle 2\rangle 2$

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

PROOF: $\langle 2\rangle 3$

$\langle 2\rangle 5$. $y \in f(A)$

PROOF: $\langle 2\rangle 3$, $\langle 2\rangle 4$

$\langle 2\rangle 6$. $y \notin f(B)$

$\langle 3\rangle 1$. ASSUME: $y \in f(B)$

$\langle 3\rangle 2$. PICK $x' \in B$ such that $y = f(x')$

PROOF: $\langle 3\rangle 1$

$\langle 3\rangle 3$. $x = x'$

PROOF: $\langle 2\rangle 1$, $\langle 2\rangle 3$, $\langle 3\rangle 2$

$\langle 3\rangle 4$. $x \in B$

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

$\langle 3\rangle 5$. Q.E.D.

PROOF: $\langle 2\rangle 3$ and $\langle 3\rangle 4$ form a contradiction.

$\langle 2 \rangle 7$. $y \in f(A) - f(B)$
PROOF: $\langle 2 \rangle 5$, $\langle 2 \rangle 6$
$\square$

Definition 3.38 (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 3.39. *For any set X, the identity relation I_X is a function $X \to X$.*

PROOF: Easy. $\square$

Definition 3.40 (Restriction)**.** Let $f : Y \to Z$ and $X \subseteq Y$. The *restriction* of f to X is the function $f \restriction X : X \to Z$ defined by

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

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 $f = g \restriction X$.

Definition 3.41 (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 3.42 (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 $\pi(x) = x/R$.

Proposition 3.43. *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. $\square$

Proposition 3.44. *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. $\square$

3.7 Families

Proposition 3.45 (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 3.46 (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*

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

PROOF: Easy. □

Proposition 3.47 (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*

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

PROOF: Easy. □

Proposition 3.48 (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*

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

PROOF: Easy. □

Proposition 3.49. *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 3.50. *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 3.51 (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 3.52. *Let $\{A_i\}_{i\in I}$ and $\{B_j\}_{j\in J}$ be families of sets. Then*

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

PROOF: Easy. □

Proposition 3.53. *Let $\{A_i\}_{i \in I}$ and $\{B_j\}_{j \in J}$ be nonempty families of sets. Then*

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

PROOF: Easy. ☐

Proposition 3.54. *Let $f : X \to Y$. Let $\{A_i\}_{i \in I}$ be a family of subsets of X. Then*

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

PROOF: Easy. ☐

Example 3.55. 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 $f\left(\bigcap_{i \in I} A_i\right) = f(\emptyset) = \emptyset$ but $\bigcap_{i \in I} f(A_i) = \{c\}$.

3.8 Inverses and Composites of Functions

3.8.1 Inverse Image

Definition 3.56 (Inverse Image)**.** Let $f : X \to Y$. Let B be a subset of Y. Then the *inverse image* of B under f is

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

Proposition 3.57. *Let $f : X \to Y$. Let $B \subseteq Y$. Then*

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

Equality holds if f is surjective.

PROOF:
⟨1⟩1. LET: X and Y be sets.
⟨1⟩2. LET: $f : X \to Y$
⟨1⟩3. LET: $B \subseteq Y$
⟨1⟩4. $f(f^{-1}(B)) \subseteq B$
  ⟨2⟩1. LET: $y \in f(f^{-1}(B))$
  ⟨2⟩2. PICK $x \in f^{-1}(B)$ such that $f(x) = y$
  ⟨2⟩3. $f(x) \in B$
  ⟨2⟩4. $y \in B$
⟨1⟩5. If f is surjective then $f(f^{-1}(B)) = B$
  ⟨2⟩1. ASSUME: f is surjective.
  ⟨2⟩2. LET: $y \in B$

⟨2⟩3. PICK $x \in X$ such that $f(x) = y$
PROOF: ⟨2⟩1, ⟨2⟩2
⟨2⟩4. $x \in f^{-1}(B)$
PROOF: ⟨2⟩2, ⟨2⟩3
⟨2⟩5. $y \in f(f^{-1}(B))$
PROOF: ⟨2⟩3, ⟨2⟩4
□

Proposition 3.58. *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:
⟨1⟩1. LET: X and Y be sets.
⟨1⟩2. LET: $f : X \to Y$
⟨1⟩3. LET: $A \subseteq X$
⟨1⟩4. $A \subseteq f^{-1}(f(A))$
⟨2⟩1. LET: $x \in A$
⟨2⟩2. $f(x) \in f(A)$
⟨2⟩3. $x \in f^{-1}(f(x))$
⟨1⟩5. If f is injective then $f^{-1}(f(A)) = A$
⟨2⟩1. ASSUME: f is injective.
⟨2⟩2. LET: $x \in f^{-1}(f(A))$
⟨2⟩3. $f(x) \in f(A)$
PROOF: ⟨2⟩2
⟨2⟩4. PICK $x' \in A$ such that $f(x') = f(x)$
PROOF: ⟨2⟩3
⟨2⟩5. $x' = x$
PROOF: ⟨2⟩1, ⟨2⟩4
⟨2⟩6. $x \in A$
PROOF: ⟨2⟩4, ⟨2⟩5
□

Proposition 3.59. *Let $f : X \to Y$. Let $A \subseteq B \subseteq Y$. Then $f^{-1}(A) \subseteq f^{-1}(B)$.*

PROOF:
⟨1⟩1. LET: X and Y be sets.
⟨1⟩2. LET: $f : X \to Y$
⟨1⟩3. LET: $A \subseteq B \subseteq Y$
⟨1⟩4. LET: $x \in f^{-1}(A)$
⟨1⟩5. $f(x) \in A$
⟨1⟩6. $f(x) \in B$
⟨1⟩7. $x \in f^{-1}(B)$
□

Proposition 3.60. *Let $f : X \to Y$. Let $\mathcal{B} \subseteq Y$. Then*

$$f^{-1}\left(\bigcup \mathcal{B}\right) = \bigcup_{B \in \mathcal{B}} f^{-1}(B) \ .$$

PROOF:

$$\begin{aligned} x \in f^{-1}\left(\bigcup \mathcal{B}\right) &\Leftrightarrow f(x) \in \bigcup \mathcal{B} \\ &\Leftrightarrow \exists B \in \mathcal{B}. f(x) \in B \\ &\Leftrightarrow \exists B \in \mathcal{B}. x \in f^{-1}(B) \\ &\Leftrightarrow x \in \bigcup_{B \in \mathcal{B}} f^{-1}(B) \end{aligned}$$

□

Proposition 3.61. *Let $f : X \to Y$. Let $\{B_i\}_{i \in I}$ be a nonempty family of subsets of Y. Then*

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

PROOF: Easy. □

Proposition 3.62. *Let $f : X \to Y$ and $B \subseteq Y$. Then $f^{-1}(Y - B) = X - f^{-1}(B)$.*

PROOF: Easy. □

3.8.2 Inverse of a Function

Proposition 3.63. *Let $f : X \approx Y$. Then f^{-1} is a function, and is a bijection $f^{-1} : Y \approx X$.*

PROOF:
⟨1⟩1. LET: X and Y be sets.
⟨1⟩2. LET: $f : X \approx Y$
⟨1⟩3. f^{-1} is a function.
  ⟨2⟩1. LET: $(x, y), (x, z) \in f^{-1}$
  ⟨2⟩2. $(y, x), (z, x) \in f$
  ⟨2⟩3. $y = z$
    PROOF: f is injective.
⟨1⟩4. $\mathrm{dom}\, f^{-1} = Y$
  PROOF: Proposition 3.17, ⟨1⟩2
⟨1⟩5. $\mathrm{ran}\, f^{-1} = X$
  PROOF:

$$\begin{aligned} x \in \mathrm{ran}\, f^{-1} &\Leftrightarrow \exists y.(y, x) \in f^{-1} \\ &\Leftrightarrow \exists y.(x, y) \in f \\ &\Leftrightarrow x \in \mathrm{dom}\, f \\ &\Leftrightarrow x \in X \end{aligned}$$

⟨1⟩6. f^{-1} is injective.
  ⟨2⟩1. LET: $y, y' \in Y$
  ⟨2⟩2. ASSUME: $f^{-1}(y) = f^{-1}(y')$
  ⟨2⟩3. $y = y'$
    PROOF: $y = f(f^{-1}(y)) = f(f^{-1}(y')) = y'$.

□

Proposition 3.64. *Let $f : X \to Y$ and $g : Y \to Z$. Then $gf : X \to Z$ and, for all $x \in X$, we have*

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

PROOF: Easy. □

Example 3.65. Example 3.14 shows that function composition is not commutative in general.

Proposition 3.66. *The composite of two injective functions is injective.*

PROOF:
⟨1⟩1. LET: $f : X \rightarrowtail Y$ and $g : Y \rightarrowtail Z$
⟨1⟩2. LET: $x, y \in X$
⟨1⟩3. ASSUME: $(g \circ f)(x) = (g \circ f)(y)$
⟨1⟩4. $g(f(x)) = g(f(y))$
⟨1⟩5. $f(x) = f(y)$
PROOF: g is injective.
⟨1⟩6. $x = y$
PROOF: f is injective.
□

Proposition 3.67. *Let $f : X \to Y$ and $g : Y \to Z$. If $g \circ f$ is injective then f is injective.*

PROOF: If $f(x) = f(y)$ then $g(f(x)) = g(f(y))$ and so $x = y$. □

Proposition 3.68. *The composite of two surjective functions is surjective.*

PROOF:
⟨1⟩1. LET: $f : X \twoheadrightarrow Y$ and $g : Y \twoheadrightarrow Z$
⟨1⟩2. LET: $z \in Z$
⟨1⟩3. PICK $y \in Y$ such that $g(y) = z$
PROOF: Since g is surjective.
⟨1⟩4. PICK $x \in X$ such that $f(x) = y$
PROOF: Since f is surjective.
⟨1⟩5. $(g \circ f)(x) = z$
□

Proposition 3.69. *Let $f : X \to Y$ and $g : Y \to Z$. If $g \circ f$ is surjective then g is surjective.*

PROOF: Let $z \in Z$. Pick $x \in X$ such that $g(f(x)) = z$. Then there exists y such that $g(y) = z$, namely $y = f(x)$. □

Proposition 3.70. *The composite of two bijective functions is bijective.*

PROOF: Propositions 3.66 and 3.68. □

Proposition 3.71. *Let X, Y and Z be sets. Let $f : X \to Y$ and $g : Y \to Z$. Let $A \subseteq Z$. Then*
$$(g \circ f)^{-1}(A) = f^{-1}(g^{-1}(A)) \enspace .$$

PROOF:
$\langle 1 \rangle 1$. LET: X, Y and Z be sets.
$\langle 1 \rangle 2$. LET: $f : X \to Y$ and $g : Y \to Z$
$\langle 1 \rangle 3$. LET: $A \subseteq Z$
$\langle 1 \rangle 4$. $(g \circ f)^{-1}(A) = f^{-1}(g^{-1}(A))$
PROOF:
$\langle 2 \rangle 1$. LET: $x \in X$
$\langle 2 \rangle 2$. $x \in (g \circ f)^{-1}(A) \Leftrightarrow x \in f^{-1}(g^{-1}(A))$
PROOF:
$$\begin{aligned} x \in (g \circ f)^{-1}(A) &\Leftrightarrow (g \circ f)(x) \in A \\ &\Leftrightarrow g(f(x)) \in A && \text{(Proposition 3.64, } \langle 1 \rangle 2, \langle 2 \rangle 1) \\ &\Leftrightarrow f(x) \in g^{-1}(A) \\ &\Leftrightarrow x \in f^{-1}(g^{-1}(A)) \end{aligned}$$
□

Proposition 3.72. *Let $f : X \approx Y$ and $g : Y \approx Z$. Then*
$$(gf)^{-1} = f^{-1}g^{-1} : Z \to X \enspace .$$

PROOF: Easy. □

Definition 3.73 (Left Inverse, Right Inverse)**.** Let $f : X \to Y$ and $g : Y \to X$. Then g is a *left inverse* of f, and f is a *right inverse* of g, iff $g \circ f = I_X$.

Proposition 3.74. *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. □

Lemma 3.75. *Let $f : A \to B$. If there are functions $g : B \to A$ and $h : B \to A$ such that $\forall a \in A. g(f(a)) = a$ and $\forall b \in B. f(h(b)) = b$, then f is bijective and $g = h = f^{-1}$.*

PROOF:
$\langle 1 \rangle 1$. LET: A and B be sets.
$\langle 1 \rangle 2$. LET: $f : A \to B$ and $g, h : B \to A$
$\langle 1 \rangle 3$. ASSUME: $\forall a \in A. g(f(a)) = a$
$\langle 1 \rangle 4$. ASSUME: $\forall b \in B. f(h(b)) = b$
$\langle 1 \rangle 5$. f is injective.
PROOF: Proposition 3.74, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$.
$\langle 1 \rangle 6$. f is surjective.
PROOF: Proposition 3.74, $\langle 1 \rangle 2$, $\langle 1 \rangle 4$.
$\langle 1 \rangle 7$. $g = h$

⟨2⟩1. LET: $b \in B$
⟨2⟩2. $g(b) = h(b)$
PROOF:

$$g(b) = g(f(h(b))) \qquad (\langle 1\rangle 4, \langle 2\rangle 1)$$
$$= h(b) \qquad (\langle 1\rangle 3, \langle 1\rangle 2, \langle 2\rangle 1)$$

⟨1⟩8. $h = f^{-1}$
⟨2⟩1. LET: $b \in B$
⟨2⟩2. $f(h(b)) = b$
PROOF: ⟨1⟩4, ⟨2⟩1
⟨2⟩3. $h(b) = f^{-1}(b)$
□

3.9 Choice Functions

Definition 3.76 (Choice Function)**.** A *choice function* for a set X is a function $f : \mathcal{P}X - \{\emptyset\} \to X$ such that $f(S) \in S$ for all S.

Proposition 3.77. *Every set has a choice function.*

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

Proposition 3.78. *For any relation R, there exists a function $f \subseteq R$ such that* $\mathrm{dom}\, f = \mathrm{dom}\, R$*.*

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

Proposition 3.79. *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 $A \cap C = \{f(C)\}$
□

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.

Theorem 4.3 (Schröder-Bernstein)**.** *Let X and Y be sets. If there exist injective functions $X \to Y$ and $Y \to X$, then $X \sim Y$.*

PROOF:
⟨1⟩1. LET: $f : X \to Y$ and $g : Y \to X$ be one-to-one.
⟨1⟩2. ASSUME: w.l.o.g. $X \cap Y = \emptyset$
⟨1⟩3. For $x \in X$, let us say that x is the *parent* of $f(x)$; and for $y \in Y$, let us say that y is the *parent* of $g(y)$.
⟨1⟩4. For $z \in X \cup Y$, let the set of *descendants* of z be the intersection of all the subsets S of $X \cup Y$ such that $z \in S$ and, if $t \in S$ and t is the parent of u then $u \in S$.
⟨1⟩5. LET: X_X be the set of all elements of X that are descendants of the elements of X that have no parent.
⟨1⟩6. LET: X_Y be the set of all elements of X that are descendants of the elements of Y that have no parent.
⟨1⟩7. LET: $X_\infty = X - X_X - X_Y$
⟨1⟩8. LET: Y_X be the set of all elements of Y that are descendants of the elements of X that have no parent.
⟨1⟩9. LET: Y_Y be the set of all elements of Y that are descendants of the elements of Y that have no parent.
⟨1⟩10. LET: $Y_\infty = Y - Y_X - Y_Y$
⟨1⟩11. $f \upharpoonright X_X : X_X \sim Y_X$
⟨1⟩12. $g \upharpoonright Y_Y : Y_Y \sim X_Y$
⟨1⟩13. $f \upharpoonright X_\infty : X_\infty \sim Y_\infty$
⟨1⟩14. Define $h : X \to Y$ by $h(x) = g^{-1}(x)$ if $x \in X_Y$, and $f(x)$ if not.

$\langle 1 \rangle 15.$ $h : X \sim Y$
□

Theorem 4.4 (Cantor)**.** *For any set X we have $X \nsim \mathcal{P}X$.*

Proof: If $f : X \to \mathcal{P}X$ then $\{x \in X : x \notin f(x)\}$ is a subset of X not in $\operatorname{ran} f$. □

Chapter 5

Order

5.1 Partial Orders

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 or *smaller* than y; and y is *greater than* x, *larger* than x.

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

PROOF: From Theorems 2.16, 2.17 and 2.18. □

Proposition 5.3. *Let X be a set. Let $<$ be a relation on X. Then there exists a partial order $\leqslant$ on X such that*

$$\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$$

if and only if $<$ is irreflexive and transitive. In this case, $\leqslant$ is unique and is defined by

$$\forall x, y \in X(x \leqslant y \Leftrightarrow x < y \vee x = y) \ .$$

PROOF:
⟨1⟩1. LET: X be a set.
⟨1⟩2. LET: $<$ be a relation on X.
⟨1⟩3. If there exists a partial order $\leqslant$ on X such that $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$, then $<$ is irreflexive.
  PROOF: Trivial.
⟨1⟩4. If there exists a partial order $\leqslant$ on X such that $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$, then $<$ is transitive.
  ⟨2⟩1. LET: $\leqslant$ be a partial order on X.
  ⟨2⟩2. ASSUME: $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$

⟨2⟩3. Let: $x < y$ and $y < z$
⟨2⟩4. $x \leqslant y$
Proof: ⟨2⟩3
⟨2⟩5. $x \neq y$
Proof: ⟨2⟩3
⟨2⟩6. $y \leqslant z$
Proof: ⟨2⟩3
⟨2⟩7. $y \neq z$
Proof: ⟨2⟩3
⟨2⟩8. $x \leqslant z$
Proof: From ⟨2⟩4 and ⟨2⟩6 since $\leqslant$ is transitive by ⟨2⟩1.
⟨2⟩9. $x \neq z$
⟨3⟩1. Assume: for a contradiction $x = z$
⟨3⟩2. $y \leqslant x$
Proof: ⟨2⟩6, ⟨3⟩1
⟨3⟩3. $x = y$
Proof: From ⟨2⟩4 and ⟨3⟩2 since $\leqslant$ is antisymmetric by ⟨2⟩1.
⟨3⟩4. Q.E.D.
Proof: ⟨2⟩5 and ⟨3⟩3 form a contradiction.
⟨2⟩10. $x < z$
Proof: ⟨2⟩8, ⟨2⟩9
⟨1⟩5. If there exists a partial order $\leqslant$ on X such that $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$, then $\forall x, y \in X(x \leqslant y \Leftrightarrow x < y \vee x = y)$.
Proof: Trivial.
⟨1⟩6. If $<$ is irreflexive and transitive, then the relation $\leqslant$ defined by $\forall x, y \in X(x \leqslant y \Leftrightarrow x < y \vee x = y)$ is a partial order on X.
⟨2⟩1. Assume: $<$ is irreflexive.
⟨2⟩2. Assume: $<$ is transitive.
⟨2⟩3. Let: $\leqslant$ be the relation defined by $\forall x, y \in X(x \leqslant y \Leftrightarrow x < y \vee x = y)$
⟨2⟩4. $\leqslant$ is reflexive.
Proof: Immediate from ⟨2⟩3.
⟨2⟩5. $\leqslant$ is transitive.
⟨3⟩1. Let: $x, y, z \in X$
⟨3⟩2. Assume: $x \leqslant y$ and $y \leqslant z$
⟨3⟩3. $x < y$ or $x = y$
Proof: ⟨2⟩4, ⟨3⟩2
⟨3⟩4. $y < z$ or $y = z$
Proof: ⟨2⟩4, ⟨3⟩2
⟨3⟩5. Case: $x < y$ and $y < z$
⟨4⟩1. $x < z$
Proof: ⟨2⟩2
⟨4⟩2. $x \leqslant z$
Proof: ⟨2⟩4, ⟨4⟩1
⟨3⟩6. Case: $x = y$
Proof: Then $x \leqslant z$ from ⟨3⟩2
⟨3⟩7. Case: $y = z$

PROOF: Then $x \leqslant z$ from $\langle 3\rangle 2$

$\langle 2\rangle 6$. $\leqslant$ is antisymmetric.

$\langle 3\rangle 1$. LET: $x, y \in X$

$\langle 3\rangle 2$. ASSUME: $x \leqslant y$

$\langle 3\rangle 3$. ASSUME: $y \leqslant x$

$\langle 3\rangle 4$. $x < y$ or $x = y$

PROOF: $\langle 2\rangle 4$, $\langle 3\rangle 2$

$\langle 3\rangle 5$. $y < x$ or $y = x$

PROOF: $\langle 2\rangle 4$, $\langle 3\rangle 2$

$\langle 3\rangle 6$. $\neg(x < y \wedge y < x)$

$\langle 4\rangle 1$. ASSUME: for a contradiction $x < y$ and $y < x$

$\langle 4\rangle 2$. $x < x$

PROOF: $\langle 2\rangle 2$, $\langle 4\rangle 1$

$\langle 4\rangle 3$. Q.E.D.

PROOF: $\langle 2\rangle 1$ and $\langle 4\rangle 2$ form a contradiction.

$\langle 3\rangle 7$. $x = y$

PROOF: $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$

$\langle 1\rangle 7$. If $<$ is irreflexive, then the relation $\leqslant$ defined by $\forall x, y \in X(x \leqslant y \Leftrightarrow x < y \vee x = y)$ satisfies $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$.

PROOF: Trivial.

□

Proposition 5.4. *In a poset, we never have $x < y$ and $y < x$.*

PROOF: We would then have $x < x$ by transitivity, contradicting the irreflexivity of $<$. □

Definition 5.5 ((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 5.6 (Weak Initial Segment)**.** Let X be a poset and $a \in X$. The *weak initial segment* determined by a is

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

Definition 5.7 (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 5.8 (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 5.9. *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 5.10 (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 5.11. *A poset has at most one greatest element.*

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

Definition 5.12 (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 5.13 (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 5.14 (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 5.15 (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 5.16 (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 5.17 (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.

5.2 Linear Orders

Definition 5.18 (Linear Order)**.** A partial order $\leqslant$ on a set X is a *linear order*, *total order* or *simple 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 5.19. *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 5.20. *Let X be a set and $<$ a relation on X. Then there exists a linear order $\leqslant$ on X such that*

$$\forall x, y \in X.(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$$

if and only if $<$ is irreflexive, transitive, and:

$$\forall x, y \in X.(x < y \vee x = y \vee y < x) \ .$$

In this case, $\leqslant$ is unique and is defined by

$$\forall x, y \in X.(x \leqslant y \Leftrightarrow x < y \vee x = y)$$

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

⟨1⟩2. LET: $<$ be a relation on X

⟨1⟩3. If there exists a linear order $\leqslant$ on X such that $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$, then $<$ is irreflexive.

PROOF: Trivial.

⟨1⟩4. If there exists a linear order $\leqslant$ on X such that $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$, then $<$ is transitive.

⟨2⟩1. LET: $\leqslant$ be a linear order on X.

⟨2⟩2. ASSUME: $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$

⟨2⟩3. LET: $x < y$ and $y < z$

⟨2⟩4. $x \leqslant y$

PROOF: ⟨2⟩3

⟨2⟩5. $x \neq y$

PROOF: ⟨2⟩3

⟨2⟩6. $y \leqslant z$

PROOF: ⟨2⟩3

⟨2⟩7. $y \neq z$

PROOF: ⟨2⟩3

⟨2⟩8. $x \leqslant z$

PROOF: From ⟨2⟩4 and ⟨2⟩6 since $\leqslant$ is transitive.

⟨2⟩9. $x \neq z$

⟨3⟩1. ASSUME: for a contradiction $x = z$

⟨3⟩2. $y \leqslant x$

PROOF: ⟨2⟩6, ⟨3⟩1

⟨3⟩3. $x = y$

PROOF: From ⟨2⟩4 and ⟨3⟩2 since $\leqslant$ is antisymmetric.

⟨3⟩4. Q.E.D.

PROOF: ⟨2⟩5 and ⟨3⟩3 form a contradiction.

⟨2⟩10. $x < z$

PROOF: ⟨2⟩8, ⟨2⟩9

⟨1⟩5. If there exists a linear order $\leqslant$ on X such that $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$, then $\forall x, y \in X(x < y \vee x = y \vee y < x)$.

⟨2⟩1. LET: $\leqslant$ be a linear order on X.

⟨2⟩2. ASSUME: $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$

⟨2⟩3. LET: $x, y \in X$

⟨2⟩4. $x \leqslant y$ or $y \leqslant x$

⟨2⟩5. CASE: $x \leqslant y$

PROOF: Then $x < y$ or $x = y$ using ⟨2⟩2.

⟨2⟩6. CASE: $y \leqslant x$

PROOF: Then $y < x$ or $x = y$ using ⟨2⟩2.

⟨1⟩6. If there exists a linear order $\leqslant$ on X such that $\forall x, y \in X(x < y \Leftrightarrow x \leqslant y \wedge x \neq y)$, then $\forall x, y \in X(x \leqslant y \Leftrightarrow x < y \vee x = y)$.

PROOF: Trivial.

⟨1⟩7. If $<$ is irreflexive, transitive and satisfies $\forall x, y \in X.(x < y \vee x = y \vee y < x)$, then the relation $\leqslant$ defined by $\forall x, y(x \leqslant y \Leftrightarrow x < y \vee x = y)$ is a linear order on X.

⟨2⟩1. ASSUME: $<$ is irreflexive.

⟨2⟩2. ASSUME: $<$ is transitive.
⟨2⟩3. ASSUME: $\forall x, y \in X(x < y \lor x = y \lor y < x)$
⟨2⟩4. LET: $\leqslant$ be the relation defined by $\forall x, y(x \leqslant y \Leftrightarrow x < y \lor x = y)$
⟨2⟩5. $\leqslant$ is reflexive.
PROOF: Immediate from ⟨2⟩4.
⟨2⟩6. $\leqslant$ is transitive.
⟨3⟩1. LET: $x, y, z \in X$
⟨3⟩2. ASSUME: $x \leqslant y$ and $y \leqslant z$
⟨3⟩3. $x < y$ or $x = y$
PROOF: ⟨2⟩4, ⟨3⟩2
⟨3⟩4. $y < z$ or $y = z$
PROOF: ⟨2⟩4, ⟨3⟩2
⟨3⟩5. CASE: $x < y$ and $y < z$
⟨4⟩1. $x < z$
PROOF: ⟨2⟩2
⟨4⟩2. $x \leqslant z$
PROOF: ⟨2⟩4, ⟨4⟩1
⟨3⟩6. CASE: $x = y$
PROOF: Then $x \leqslant z$ from ⟨3⟩2
⟨3⟩7. CASE: $y = z$
PROOF: Then $x \leqslant z$ from ⟨3⟩2
⟨2⟩7. $\leqslant$ is antisymmetric.
⟨3⟩1. LET: $x, y \in X$
⟨3⟩2. ASSUME: $x \leqslant y$
⟨3⟩3. ASSUME: $y \leqslant x$
⟨3⟩4. $x < y$ or $x = y$
PROOF: ⟨2⟩4, ⟨3⟩2
⟨3⟩5. $y < x$ or $y = x$
PROOF: ⟨2⟩4, ⟨3⟩2
⟨3⟩6. $\neg(x < y \land y < x)$
⟨4⟩1. ASSUME: for a contradiction $x < y$ and $y < x$
⟨4⟩2. $x < x$
PROOF: ⟨2⟩2, ⟨4⟩1
⟨4⟩3. Q.E.D.
PROOF: ⟨2⟩1 and ⟨4⟩2 form a contradiction.
⟨3⟩7. $x = y$
PROOF: ⟨3⟩4, ⟨3⟩5, ⟨3⟩6
⟨2⟩8. $\forall x, y \in X(x \leqslant y \lor y \leqslant x)$
⟨3⟩1. LET: $x, y \in X$
⟨3⟩2. $x < y$ or $x = y$ or $y < x$
PROOF: ⟨2⟩3, ⟨3⟩1
⟨3⟩3. $x \leqslant y$ or $y \leqslant x$
PROOF: ⟨2⟩4, ⟨3⟩2

□

Theorem 5.21 (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: $g : \mathcal{X} \to \mathcal{X}$ 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. $A \subseteq C$
$\langle 2\rangle 5$. $x, y \in C$
$\langle 2\rangle 6$. $x \leqslant y$ or $y \leqslant x$
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 $\bigcup \mathcal{T}_0 \in \mathcal{T}_0$.
$\langle 1\rangle 11$. $g(A) \in \mathcal{T}_0$
$\langle 1\rangle 12$. $g(A) \subseteq A$
$\langle 1\rangle 13$. $g(A) = A$
$\langle 1\rangle 14$. $\hat{A} - A = \emptyset$
$\langle 1\rangle 15$. $u \in A$
PROOF: Since $A \cup \{u\}$ is a chain so $u \in \hat{A}$ and therefore $u \in A$.
$\langle 1\rangle 16$. u is maximal in X.
$\langle 2\rangle 1$. LET: $x \in X$
$\langle 2\rangle 2$. ASSUME: $u \leqslant x$
$\langle 2\rangle 3$. $A \cup \{x\}$ is a chain.
$\langle 2\rangle 4$. $x \in A$
$\langle 2\rangle 5$. $x \leqslant u$
$\langle 2\rangle 6$. $x = u$
$\square$

Definition 5.22 (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 $x \leqslant a$.

Definition 5.23 (Order Isomorphism)**.** Two posets X and Y are *(order) isomorphic*, $X \cong Y$ iff there exists an order preserving one-to-one correspondence f between them. We write $f : X \cong Y$ and call f a *(order) isomorphism.*

Proposition 5.24. *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. $\square$

Proposition 5.25. *For any poset X we have $I_X : X \cong X$.*

PROOF: Easy. □

Proposition 5.26. *If $f : X \cong Y$ then $f^{-1} : Y \cong X$.*

PROOF: Easy. □

Proposition 5.27. *If $f : X \cong Y$ and $g : Y \cong Z$ then $g \circ f : X \cong Z$.*

PROOF: Easy. □

Corollary 5.27.1. *For any set E, similarity is an equivalence relation on the set of all posets that are subsets of E.*

Definition 5.28 (Open Interval)**.** Let X be a linearly ordered set. Let $a, b \in X$ with $a < b$. The *open interval* (a, b) is

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

Definition 5.29 (Lexicographical Order)**.** Let A and B be linearly ordered sets. The *lexicographical* order on $A \times B$ is the relation $\leqslant$ defined by $(a, b) \leqslant (x, y)$ iff $a < x$ or ($a = x$ and $b \leqslant y$).

Definition 5.30 (Least Upper Bound Property)**.** A linearly ordered set A has the *least upper bound property* iff every nonempty subset of A bounded above has a least upper bound.

Proposition 5.31. *Let A be a linearly ordered set. Then A has the least upper bound property if and only if every nonempty subset of A bounded below has a greatest lower bound.*

PROOF:

⟨1⟩1. For any linearly ordered set A, if A has the least upper bound property then every nonempty subset of A bounded below has a greatest lower bound.

  ⟨2⟩1. LET: A be a linearly ordered set.

  ⟨2⟩2. ASSUME: A has the least upper bound property.

  ⟨2⟩3. LET: S be a nonempty subset of A bounded below.

  ⟨2⟩4. LET: $S\downarrow$ be the set of all lower bounds for S.

  ⟨2⟩5. $S\downarrow \neq \emptyset$

   PROOF: Since S is bounded below by ⟨2⟩3.

  ⟨2⟩6. $S\downarrow$ is bounded above.

   ⟨3⟩1. PICK $s \in S$

    PROOF: S is nonempty by ⟨2⟩3.

   ⟨3⟩2. s is an upper bound for $S\downarrow$.

  ⟨2⟩7. LET: l be the supremum of $S\downarrow$.

   PROOF: ⟨2⟩2, ⟨2⟩5, ⟨2⟩6

  ⟨2⟩8. l is a lower bound for S.

   ⟨3⟩1. LET: $s \in S$

⟨3⟩2. s is an upper bound for $S\downarrow$

⟨3⟩3. $l \leqslant s$

PROOF: ⟨2⟩7, ⟨3⟩2

⟨2⟩9. For any lower bound l' for S we have $l' \leqslant l$.

PROOF: Since l is an upper bound for $S\downarrow$ by ⟨2⟩7.

⟨1⟩2. For any linearly ordered set A, if every nonempty subset of A bounded below has a greatest lower bound then A has the least upper bound property.

⟨2⟩1. LET: $(A, \leqslant)$ be a linearly ordered set.

⟨2⟩2. ASSUME: Every nonempty subset of A bounded below has a greatest lower bound.

⟨2⟩3. $(A, \geqslant)$ has the least upper bound property.

⟨2⟩4. Every nonempty subset of A bounded below with respect to $\geqslant$ has ¡a greatest lower bound with respect to $\geqslant$.

⟨2⟩5. Every nonempty subset of A bounded above with respect to $\leqslant$ has a least upper bound with respect to $\leqslant$.

□

5.3 Linear Continua

Definition 5.32 (Linear Continuum)**.** A *linear continuum* is a linearly ordered set X with the least upper bound property such that, for all $x, y \in X$, if $x < y$ then there exists $z \in X$ such that $x < z < y$.

5.4 Well Orderings

Definition 5.33 (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 5.34. *Every well ordered set is totally ordered.*

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

Theorem 5.35 (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 $X - S = \emptyset$. □

Definition 5.36 (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 5.37. *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 $\leqslant$ on $\bigcup \mathcal{C}$ by: $x \leqslant y$ iff there exists $C \in \mathcal{C}$ such that $x, y \in C$ and $x \leqslant y$ in C. ∎

Proposition 5.38. *Every totally ordered set has a cofinal well ordered subset.*

PROOF:
⟨1⟩1. LET: X be a totally ordered set.
⟨1⟩2. LET: $\mathcal{C}$ be the poset of all well ordered subsets of X under continuation.
⟨1⟩3. Every chain in $\mathcal{C}$ has an upper bound.
PROOF: Proposition 5.37.
⟨1⟩4. PICK a maximal element C of $\mathcal{C}$
PROVE: C is cofinal
PROOF: Zorn's Lemma
⟨1⟩5. LET: $x \in X$
⟨1⟩6. We cannot have $\forall c \in C.c < x$
PROOF: Then $C \cup \{x\}$ would be a larger chain.
⟨1⟩7. $\exists c \in C.x \leqslant c$
∎

Theorem 5.39 (Well Ordering Theorem)**.** *Every set can be well ordered.*

PROOF:
⟨1⟩1. LET: X be a set.
⟨1⟩2. LET: $\mathcal{W}$ be the poset of all well ordered subsets of X under continuation.
⟨1⟩3. Every chain in $\mathcal{W}$ has an upper bound.
PROOF: Proposition 5.37.
⟨1⟩4. PICK a maximal $M \in \mathcal{W}$
PROOF: Zorn's Lemma
⟨1⟩5. $M = X$
PROOF: If $x \in X - M$ then $M \cup \{x\}$ with x as the greatest element is a continuation of M.
∎

Theorem 5.40 (Transfinite Recursion)**.** *Let W be a well ordered set and X a set. Let S be the set of all functions f such that* $\operatorname{ran} f \subseteq X$*, and there exists $a \in W$ such that* $\operatorname{dom} f = s(a)$*. Then there exists a unique function $U : W \to X$ such that*

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

PROOF:
⟨1⟩1. Let us say that a subset $A \subseteq W \times X$ is *f-closed* iff, whenever $a \in W$ and $t : s(a) \to X$ satisfies $\forall c < a.(c, t(c)) \in A$, then $(a, f(t)) \in A$.
⟨1⟩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.
⟨1⟩3. U is f-closed.
⟨1⟩4. U is a function.
⟨2⟩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: $(a, x), (a, y) \in U$
$\langle 2 \rangle 5$. $x = f(U \restriction c)$
Proof: If not then $U - \{(a, x)\}$ would be f-closed.
$\langle 2 \rangle 6$. $y = f(U \restriction c)$
$\langle 2 \rangle 7$. $x = y$
$\langle 1 \rangle 5$. $\operatorname{dom} U = W$
$\langle 2 \rangle 1$. Let: $a \in W$
$\langle 2 \rangle 2$. Assume: as transfinite induction hypothesis $\forall c < a.c \in \operatorname{dom} U$
$\langle 2 \rangle 3$. $(a, f(U \restriction s(a))) \in U$
$\langle 1 \rangle 6$. If $U' : W \to X$ and $\forall a \in W.U'(a) = f(U' \restriction s(a))$, then $U' = U$.
Proof: Prove $U'(a) = U(a)$ by transfinite induction on a.
□

Proposition 5.41. *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 $a \leqslant f(a)$.*

Proof:
$\langle 1 \rangle 1$. Let: $a \in X$
$\langle 1 \rangle 2$. Assume: as transfinite induction hypothesis $\forall c < a.c \leqslant f(c)$
$\langle 1 \rangle 3$. Assume: for a contradiction $f(a) < a$
$\langle 1 \rangle 4$. $f(a) \leqslant f(f(a))$
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 5.42. *Let X and Y be well ordered sets. Then there is at most one similarity between them.*

Proof:
$\langle 1 \rangle 1$. Let: $f, g : X \cong Y$
Prove: $\forall a \in X.f(a) = g(a)$
$\langle 1 \rangle 2$. Let: $a \in X$
$\langle 1 \rangle 3$. Assume: as transfinite induction hypothesis $\forall c < a.f(c) = g(c)$
$\langle 1 \rangle 4$. $f(a)$ is the least element of $Y - \{f(c) : c < a\}$
$\langle 1 \rangle 5$. $g(a)$ is the least element of $Y - \{g(c) : c < a\}$
$\langle 1 \rangle 6$. $f(a) = g(a)$
□

Proposition 5.43. *A well ordered set is not similar to any of its initial segments.*

Proof:
$\langle 1 \rangle 1$. Let: X be a well ordered set.

$\langle 1 \rangle 2$. ASSUME: for a contradiction $f : X \cong s(a)$ for some $a \in X$
$\langle 1 \rangle 3$. $f(a) < a$
$\langle 1 \rangle 4$. Q.E.D.
PROOF: This contradicts Proposition 5.41.
□

Theorem 5.44 (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:
$\langle 1 \rangle 1$. LET: $X_0 = \{a \in X : \exists b \in Y . s(a) \cong s(b)\}$
$\langle 1 \rangle 2$. LET: $U : X_0 \to Y$ be the function: for $a \in X_0$, we have $U(a)$ is the unique element in Y such that $s(a) \cong s(U(a))$
$\langle 1 \rangle 3$. LET: $Y_0 = \operatorname{ran} U$
$\langle 1 \rangle 4$. Either $X_0 = X$ or there exists $a \in X$ such that $X_0 = s(a)$
$\langle 2 \rangle 1$. ASSUME: $X_0 \neq X$
$\langle 2 \rangle 2$. LET: a be the least element of $X - X_0$
$\langle 2 \rangle 3$. LET: $x \in X_0$
PROVE: $x < a$
$\langle 2 \rangle 4$. PICK $f : s(x) \cong s(U(x))$
$\langle 2 \rangle 5$. ASSUME: for a contradiction $a < x$
$\langle 2 \rangle 6$. $f \restriction s(a) : s(a) \cong s(f(a))$
$\langle 2 \rangle 7$. $a \in X_0$
$\langle 2 \rangle 8$. Q.E.D.
PROOF: This is a contradiction.
$\langle 1 \rangle 5$. Either $Y_0 = Y$ or there exists $b \in Y$ such that $Y_0 = s(b)$
PROOF: Similar.
$\langle 1 \rangle 6$. CASE: $X_0 = X$ and $Y_0 = Y$
PROOF: Then $U : X \cong Y$.
$\langle 1 \rangle 7$. CASE: $X_0 = X$ and $Y_0 \neq Y$
PROOF: Then $U : X \cong s(b)$ where $Y_0 = s(b)$.
$\langle 1 \rangle 8$. CASE: $X_0 \neq X$ and $Y_0 = Y$
PROOF: Then $U : s(a) \cong Y$ where $X_0 = s(a)$.
$\langle 1 \rangle 9$. CASE: $X_0 \neq X$ and $Y_0 \neq Y$
$\langle 2 \rangle 1$. LET: $X_0 = s(a)$ and $Y_0 = s(b)$
$\langle 2 \rangle 2$. $U : s(a) \cong s(b)$
$\langle 2 \rangle 3$. $a \in X_0$
$\langle 2 \rangle 4$. Q.E.D.
PROOF: This is a contradiction.
□

Corollary 5.44.1. *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 5.41. □

Corollary 5.44.2. *For any sets X and Y, either there exists an injective function $X \to Y$, or there exists an injective function $Y \to X$.*

PROOF: Using the Well Ordering Theorem. □

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: $\langle 3\rangle 2$

$\langle 3\rangle 7.$ $x = y$

□

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

□

Chapter 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. □

Proposition 7.3. *ω is an ordinal.*

Proof: Easy. □

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

Proof: Easy. □

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. □

Proposition 7.6. *Every ordinal is a transitive set.*

Proof: Easy. □

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

Proof: Easy. □

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: $\eta \in \xi$
  $\langle 2\rangle 2$. $\eta = f(\eta) \in f(\xi)$
$\langle 1\rangle 7$. $f(\xi) = \xi$
□

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.
  $\langle 2\rangle 4$. $\gamma = \alpha$
  $\langle 2\rangle 5$. $\alpha \in \beta$
□

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 5.37. □

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 $s(b) \cong \beta$

⟨3⟩3. LET: $\alpha = \{\beta : \beta \text{ is an ordinal } \wedge \exists b < a.s(b) \cong \beta\}$
PROOF: This is a set by the Axiom of Substitution.
⟨3⟩4. α is an ordinal
⟨4⟩1. LET: $\gamma \in \beta \in \alpha$
⟨4⟩2. PICK $b < a$ and $f : s(b) \cong \beta$
⟨4⟩3. PICK $c < b$ such that $f(c) = \gamma$
⟨4⟩4. $f \upharpoonright s(c) : s(c) \cong \gamma$
⟨3⟩5. $s(a) \cong \alpha$
PROOF: The function $f : s(a) \to \alpha$ defined by $f(b)$ is the ordinal such that $s(b) \cong f(b)$ is a similarity.
⟨3⟩6. α is unique.
PROOF: Proposition 7.8.
⟨2⟩2. LET: $\alpha = \{\beta : \beta \text{ is an ordinal } \wedge \exists a \in X.s(a) \cong \beta\}$
PROOF: This is a set by the Axiom of Substitution.
⟨2⟩3. α is an ordinal.
PROOF: Similar.
⟨2⟩4. $X \cong \alpha$
PROOF: Similar.
⟨1⟩3. For any ordinals α and β, if $X \cong \alpha$ and $X \cong \beta$ then $\alpha = \beta$.
PROOF: Proposition 7.8.
□

7.1 Order on the Natural Numbers

Proposition 7.16. *For natural numbers m, n and k, if $m < n$ then $m + k < n + k$.*

PROOF:
⟨1⟩1. LET: $m, n \in \omega$
⟨1⟩2. ASSUME: $m < n$
⟨1⟩3. $m + 0 < n + 0$
⟨1⟩4. $\forall k \in \omega.m + k < n + k \Rightarrow m + k^+ < n + k^+$
PROOF: By Proposition 6.7.
□

Proposition 7.17. *For natural numbers m, n and k, if $m < n$ and $k \neq 0$ then $mk < nk$.*

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

PROOF:

$$\begin{aligned} m(k+1) &= mk + m \\ &< mk + n && \text{(Proposition 7.16)} \\ &< nk + n && \text{(Proposition 7.16)} \\ &= n(k+1) \end{aligned}$$

□

Proposition 7.18. *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:
⟨1⟩1. LET: $P(n)$ be the property: for every proper subset $X \subsetneq n$, there exists $m < n$ such that $X \sim m$.
⟨1⟩2. $P(0)$
PROOF: Vacuous.
⟨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: 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 7.19. *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 $n \to n$ is onto.
⟨1⟩2. $P(0)$
PROOF: The only function $0 \to 0$ 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: $f : n+1 \to n+1$ 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.

$\langle 3 \rangle 4$. 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.

$\langle 3 \rangle 5$. Case: $f(k) = n$ and $f(l) < n$

Proof: Similar.

$\langle 3 \rangle 6$. Case: $f(k) = n$ and $f(l) = n$

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

$\langle 2 \rangle 6$. g maps n onto n.

Proof: $\langle 2 \rangle 2$

$\langle 2 \rangle 7$. f maps $n + 1$ onto $n + 1$.

$\langle 3 \rangle 1$. Let: $l < n + 1$

$\langle 3 \rangle 2$. Case: $l < n$

$\langle 4 \rangle 1$. Pick $k < n$ such that $g(k) = l$

$\langle 4 \rangle 2$. $f(k) = l$ or $f(n) = l$

$\langle 3 \rangle 3$. Case: $l = n$

$\langle 4 \rangle 1$. Case: $f(n) = n$

Proof: Then $l \in \operatorname{ran} f$ as required.

$\langle 4 \rangle 2$. Case: $f(n) < n$

$\langle 5 \rangle 1$. Pick $k < n$ such that $g(k) = f(n)$

$\langle 5 \rangle 2$. $f(k) = n$

□

Corollary 7.19.1. *Equivalent natural numbers are equal.*

Proposition 7.20. *The lexicographical order is a well ordering on $\omega \times \omega$.*

Proof: Easy. □

7.2 Finite Sets

Definition 7.21 (Finite)**.** A set is *finite* iff it is equivalent to a natural number; otherwise, it is *infinite*.

Proposition 7.22. *No finite set is equivalent to one of its proper subsets.*

Proof: From Proposition 7.19. □

Proposition 7.23. *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 7.24. *Every subset of a finite set is finite.*

Proof: Proposition 7.18. □

Definition 7.25 (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 7.26. *Let E and F be finite sets. If $E \subseteq F$ then $\sharp(E) \leqslant \sharp(F)$.*

PROOF: Proposition 7.18. ∎

Proposition 7.27. *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 $E \cap F = \emptyset$, 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 7.27.1. *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 7.28. *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 $f \in F$

$\langle 2\rangle 6.$ $F - \{f\} \sim n$
$\langle 2\rangle 7.$ $E \times (F - \{f\}) \sim mn$
$\langle 2\rangle 8.$ $E \times F = (E \times (F - \{f\})) \cup (E \times \{f\})$
$\langle 2\rangle 9.$ $E \times \{f\} \sim m$
$\langle 2\rangle 10.$ $E \times F \sim mn + m$
PROOF: Proposition 7.27.
□

Proposition 7.29. *For any finite sets E and F, we have E^F is finite and $\sharp(E^F) = \sharp(E)^{\sharp(F)}$.*

PROOF:
$\langle 1\rangle 1.$ LET: $P(n)$ be the property: $n \in \omega$ and for all $m \in \omega$, if $E \sim m$ and $F \sim n$ then $E^F \sim m^n$
$\langle 1\rangle 2.$ $P(0)$
PROOF: Since $E^\emptyset = \{\emptyset\} \sim 1$
$\langle 1\rangle 3.$ $\forall n \in \omega . P(n) \Rightarrow P(n+1)$
$\langle 2\rangle 1.$ LET: $n \in \omega$
$\langle 2\rangle 2.$ ASSUME: $P(n)$
$\langle 2\rangle 3.$ LET: $m \in \omega$
$\langle 2\rangle 4.$ LET: $E \sim m$ and $F \sim n + 1$
$\langle 2\rangle 5.$ PICK $f \in F$
$\langle 2\rangle 6.$ $F - \{f\} \sim n$
$\langle 2\rangle 7.$ LET: $\phi : E^F \to E^{F - \{f\}} \times E$ be the function $\phi(g) = (g \restriction (F - \{f\}), g(f))$
$\langle 2\rangle 8.$ ϕ is a one-to-one correspondence
$\langle 2\rangle 9.$ $\sharp(E^F) = m^{n+1}$
PROOF:

$$\begin{aligned} \sharp(E^F) &= \sharp(E^{F-\{f\}} \times E) \\ &= \sharp(E^{F-\{f\}})\sharp(E) && \text{(Proposition 7.28)} \\ &= m^n m && (\langle 2\rangle 2, \langle 2\rangle 4) \\ &= m^{n+1} \end{aligned}$$

□

Corollary 7.29.1. *If E is finite then $\mathcal{P}E$ is finite and $\sharp(\mathcal{P}E) = 2^{\sharp(E)}$.*

Proposition 7.30. *The union of a finite set of finite sets is finite.*

PROOF:
$\langle 1\rangle 1.$ 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.
$\langle 1\rangle 2.$ $P(0)$
PROOF: Since $\bigcup \emptyset = \emptyset$ is finite.
$\langle 1\rangle 3.$ $\forall n \in \omega . P(n) \Rightarrow P(n+1)$
$\langle 2\rangle 1.$ LET: n be a natural number.
$\langle 2\rangle 2.$ ASSUME: $P(n)$
$\langle 2\rangle 3.$ LET: $E \sim n + 1$

$\langle 2\rangle 4.$ PICK $X \in E$
$\langle 2\rangle 5.$ $E - \{X\} \sim n$
$\langle 2\rangle 6.$ $\bigcup(E - \{X\})$ is finite.
PROOF: $\langle 2\rangle 2$
$\langle 2\rangle 7.$ $\bigcup E = \bigcup(E - \{X\}) \cup X$
$\langle 2\rangle 8.$ $\bigcup E$ is finite.
PROOF: Corollary 7.27.1.
$\square$

Proposition 7.31. *Every nonempty finite set of natural numbers has a greatest element.*

PROOF:
$\langle 1\rangle 1.$ LET: $P(n)$ be the property: for every $E \subseteq \mathbb{N}$, if $E \sim n$ then E has a greatest element.
$\langle 1\rangle 2.$ $P(1)$
PROOF: Since k is the greatest element of $\{k\}$.
$\langle 1\rangle 3.$ $\forall n \geqslant 1. P(n) \Rightarrow P(n+1)$
$\langle 2\rangle 1.$ LET: $n \geqslant 1$
$\langle 2\rangle 2.$ 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 7.32. *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 $X - A \in \operatorname{dom} f$.
PROOF: For all $A \in \mathcal{C}$ we have $X - A \neq \emptyset$.
$\langle 1\rangle 5.$ 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 $n \in \omega$.
$\langle 1\rangle 6.$ 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 $v(m) \notin U(m)$.
$\square$

Corollary 7.32.1. *A set is infinite if and only if it is equivalent to a proper subset.*

7.3 Ordinal Arithmetic

Definition 7.33 (Addition)**.** Let I be a well ordered set and $(\alpha_i)_{i \in I}$ be a sequence of ordinals. Choose a well ordered set A_i such that $A_i \cong \alpha_i$ for each $i \in I$, and assume the sets A_i are pairwise disjoint. The *sum* $\sum_{i \in I} \alpha_i$ is the ordinal of the well ordered set $\bigcup_{i \in I} A_i$, where:

- for $x, y \in A_i$, we have $x <_{\bigcup_{i \in I} A_i} y$ if and only if $x <_{A_i} y$
- for $x \in A_i$ and $y \in A_j$ with $i \neq j$, we have $x <_{\bigcup_{i \in I} A_i} y$ iff $i <_I j$

We write $\alpha + \beta$ for $\sum_{i \in 2} \gamma_i$ where $\gamma_0 = \alpha$ and $\gamma_1 = \beta$.

Proposition 7.34.

$$\begin{aligned} \alpha + 0 &= \alpha \\ 0 + \alpha &= \alpha \\ \alpha + 1 &= \alpha^+ \\ \alpha + (\beta + \gamma) &= (\alpha + \beta) + \gamma \end{aligned}$$

Proof: Easy. □

Proposition 7.35. *For any ordinals α and β, we have $\alpha < \beta$ if and only if there exists $\gamma \neq 0$ such that $\beta = \alpha + \gamma$.*

Proof: Easy. □

Proposition 7.36.

$$1 + \omega = \omega$$

Proof: Easy. □

Definition 7.37 (Multiplication)**.** Given ordinals α and β, the *product* $\alpha\beta$ is the ordinal of $\alpha \times \beta$ under the *reverse lexicographic order*: $(a, b) < (c, d)$ iff $b < d$ or ($b = d$ and $a < c$).

Proposition 7.38.

$$\begin{aligned} \alpha 0 &= 0 \\ 0 \alpha &= 0 \\ \alpha 1 &= \alpha \\ 1 \alpha &= \alpha \\ \alpha(\beta\gamma) &= (\alpha\beta)\gamma \\ \alpha(\beta + \gamma) &= \alpha\beta + \alpha\gamma \end{aligned}$$

Proof: Easy. □

Proposition 7.39. *For ordinals α and β, if $\alpha\beta = 0$ then $\alpha = 0$ or $\beta = 0$.*

PROOF: Easy. □

Example 7.40. The commutative law fails:

$$2\omega = \omega \neq \omega 2$$

PROOF: Easy. □

Example 7.41. The right distributive law fails:

$$(1+1)\omega = \omega \neq 1\omega + 1\omega = \omega 2$$

Definition 7.42 (Exponentiation)**.** Given ordinals α and β, define the ordinal α^β by

$$\begin{aligned} \alpha^0 &= 1 \\ \alpha^{\beta+1} &= \alpha^\beta \alpha \\ \alpha^\lambda &= \bigcup_{\beta<\lambda} \alpha^\beta & \qquad (\lambda \text{ a limit ordinal}) \end{aligned}$$

Proposition 7.43.

$$\begin{aligned} 0^\alpha &= 0 & \qquad (\alpha \geqslant 1) \\ 1^\gamma &= 1 \\ \alpha^{\beta+\gamma} &= \alpha^\beta \alpha^\gamma \\ \alpha^{\beta\gamma} &= (\alpha^\beta)^\gamma \end{aligned}$$

PROOF: Easy. □

Example 7.44. $(\alpha\beta)^\gamma$ is different from $\alpha^\gamma\beta^\gamma$ in general:

$$(2 \cdot 2)^\omega = \omega \neq 2^\omega 2^\omega = \omega^2 \ .$$

7.4 Arithmetic on the Natural Numbers

Proposition 7.45. *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:

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

□

Proposition 7.46. *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:

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

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

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

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

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

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

Proof: $\langle 1\rangle 2$

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

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

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

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

Proof:

$$\begin{aligned} m^+n^+ &= m^+n + m^+ \\ &= (m^+n + m)^+ \\ &= (nm^+ + m)^+ && (\langle 3\rangle 2) \\ &= (nm + n + m)^+ \\ &= (mn + m + n)^+ && (\langle 2\rangle 2, \text{Proposition 7.45}) \\ &= (mn^+ + n)^+ \\ &= (n^+m + n)^+ && (\langle 2\rangle 2) \\ &= n^+m + n^+ \\ &= n^+m^+ \end{aligned}$$

∎

Chapter 8

Countable Sets

Definition 8.1 (Countable)**.** A set A is *countable* or *denumerable* iff there exists an injective function $A \to \omega$.

Definition 8.2 (Countably Infinite)**.** A set is *countably infinite* iff it is similar to ω.

Proposition 8.3. *Every subset of a countable set is countable.*

Proof: Easy. ∎

Proposition 8.4. *Let X be a set. If there exists a function from ω onto X, then X is countable.*

Proof:
$\langle 1 \rangle 1$. Let: f be a function from ω onto X.
$\langle 1 \rangle 2$. Choose a function $g : X \to \omega$ such that, for all $x \in X$, we have $f(g(x)) = x$.
$\langle 1 \rangle 3$. g is one-to-one.
∎

Proposition 8.5. *$\omega \times \omega$ is countable.*

Proof: The sequence
$$(0,0), (0,1), (1,0), (0,2), (1,1), (2,0), \dots$$
is an enumeration of $\omega \times \omega$. ∎

Corollary 8.5.1. *A countable union of countable sets is countable.*

Proof:
$\langle 1 \rangle 1$. Let: A be a countable set of countable sets.
$\langle 1 \rangle 2$. Pick a surjection $f : \omega \to A$
$\langle 1 \rangle 3$. For $n \in \omega$, Pick a surjection $g_n : \omega \to f(n)$
$\langle 1 \rangle 4$. Pick a surjection $h : \omega \to \omega \times \omega$
$\langle 1 \rangle 5$. $\lambda n \in \omega . g_{\pi_1(h(n))}(\pi_2(h(n)))$ is a surjection $\omega \to \bigcup A$
∎

Corollary 8.5.2. *The Cartesian product of two countable sets is countable.*

Corollary 8.5.3. *For any countable set A, the set of all finite subsets of A is countable.*

Proof: Prove by induction on n that the set of all subsets of size n is countable. The set of all finite subsets is then the union of these. $\square$

Proposition 8.6. *$\mathcal{P}\omega$ is uncountable.*

Proof: Cantor's Theorem. $\square$

Chapter 9

Cardinal Numbers

Definition 9.1 (Cardinal Number)**.** A *cardinal number* or *initial ordinal* is an ordinal α such that, for all $\beta < \alpha$, we have $\beta \not\sim \alpha$.

Definition 9.2 (Cardinality)**.** For any set X, the *cardinality* of X, $\operatorname{card} X$, is the least ordinal that is equivalent to X.

Proposition 9.3. *Given sets X and Y, we have $X \sim Y$ if and only if* $\operatorname{card} X = \operatorname{card} Y$.

Proof: Easy. □

Proposition 9.4. *For sets X and Y, we have* $\operatorname{card} X \leqslant \operatorname{card} Y$ *if and only if there exists an injective function $X \to Y$.*

Proof: Easy. □

Proposition 9.5. *Every natural number is a cardinal. ω is a cardinal.*

Proof: Easy. □

Proposition 9.6. *Every inifinite cardinal is a limit ordinal.*

Proof: For α infinite we have $f : \alpha^+ \sim \alpha$ where $f(\alpha) = 0$ and $f(\beta) = \beta^+$ for all other β. □

9.1 Cardinal Arithmetic

Definition 9.7 (Addition)**.** Given a family of cardinal numbers $\{\kappa_i\}_{i \in I}$, let $\sum_{i \in I} \kappa_i$ be $\operatorname{card} \bigcup_{i \in I} A_i$, where $\{A_i\}_{i \in I}$ is a pairwise disjoint family of sets with $\operatorname{card} A_i = \kappa_i$ for all i.

We write $\kappa + \lambda$ for $\sum_{i \in 2} \kappa_i$ where $\kappa_0 = \kappa$ and $\kappa_1 = \lambda$.

Proposition 9.8.

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

Proof: Easy. ∎

Proposition 9.9. *Cardinal addition agrees with ordinal addition on the natural numbers.*

Proof: Easy induction. ∎

Proposition 9.10. *If $\kappa \leqslant \kappa'$ then $\kappa + \lambda \leqslant \kappa' + \lambda$.*

Proof: Easy. ∎

Proposition 9.11. *If κ is an infinite cardinal number then $\kappa + \kappa = \kappa$.*

Proof:
⟨1⟩1. Let: A be an infinite set.
Prove: $A \times 2 \sim A$
⟨1⟩2. Let: $\mathcal{F}$ be the set of all functions f such that there exists $X \subseteq A$ such that $f : X \times 2 \sim X$.
⟨1⟩3. $\mathcal{F}$ is non-empty.
Proof: Pick a subset $X \subseteq A$ such that $X \sim \omega$, and a bijection $X \times 2 \sim X$.
⟨1⟩4. $\mathcal{F}$ is partially ordered by extension.
⟨1⟩5. Every chain in $\mathcal{F}$ has an upper bound.
Proof: If $\mathcal{C} \subseteq \mathcal{F}$ is a chain then $\bigcup \mathcal{C} \in \mathcal{F}$.
⟨1⟩6. Pick $f \in \mathcal{F}$ maximal.
⟨1⟩7. Pick $X \subseteq A$ such that $f : X \times 2 \sim X$
⟨1⟩8. $X - A$ is finite.
⟨2⟩1. Assume: for a contradiction $X - A$ is infinite.
⟨2⟩2. Pick $Y \subseteq X - A$ such that $Y \sim \omega$.
⟨2⟩3. Pick $g : Y \times 2 \sim Y$
⟨2⟩4. $f \cup g : (X \cup Y) \times 2 \sim X \cup Y$
⟨2⟩5. Q.E.D.
Proof: This contradicts the maximality of f.
⟨1⟩9. $\operatorname{card} A + \operatorname{card} A = \operatorname{card} A$
Proof:

$$\begin{aligned}
2 \operatorname{card} A &= 2(\operatorname{card} X + \operatorname{card}(A - X)) \\
&= 2 \operatorname{card} X + 2 \operatorname{card}(A - X) \\
&= \operatorname{card} X + 2 \operatorname{card}(A - X) && (\langle 1 \rangle 7) \\
&= \operatorname{card} X && (\langle 1 \rangle 8) \\
&= \operatorname{card} X + \operatorname{card}(A - X) && (\langle 1 \rangle 8) \\
&= \operatorname{card} A
\end{aligned}$$

∎

Corollary 9.11.1. *For any cardinals κ and λ that are not both finite, we have*

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

Definition 9.12 (Multiplication)**.** Given a family of cardinal numbers $\{\kappa_i\}_{i \in I}$, let $\prod_{i \in I} \kappa_i = \operatorname{card} \bigtimes_{i \in I} \kappa_i$.

We write $\kappa\lambda$ for $\prod_{i \in 2} \kappa_i$ where $\kappa_0 = \kappa$ and $\kappa_1 = \lambda$.

Proposition 9.13.

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

Proposition 9.14. *Cardinal multiplication agrees with ordinal multiplication on the natural numbers.*

PROOF: Easy induction. □

Proposition 9.15. *If $\kappa \leqslant \kappa'$ then $\kappa\lambda \leqslant \kappa'\lambda$.*

PROOF: Easy. □

Proposition 9.16. *Let $\{\kappa_i\}_{i \in I}$ and $\{\lambda_i\}_{i \in I}$ be families of cardinal numbers with the same index set. If $\kappa_i < \lambda_i$ for all i, then $\sum_{i \in I} \kappa_i < \prod_{i \in I} \lambda_i$.*

PROOF:
⟨1⟩1. Choose a one-to-one function $f_i : \kappa_i \to \lambda_i$ for each $i \in I$
⟨1⟩2. $\sum_{i \in I} \kappa_i \leqslant \prod_{i \in I} \lambda_i$
  PROOF: Define $g : \sum_{i \in I} \kappa_i \to \prod_{i \in I} \lambda_i$ by

$$g(i, \eta)(j) = \begin{cases} f_i(\eta) & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

⟨1⟩3. There is no surjective function $\sum_{i \in I} \kappa_i < \prod_{i \in I} \lambda_i$
  ⟨2⟩1. LET: $h : \sum_i \kappa_i \to \prod_i \lambda_i$
  ⟨2⟩2. Choose $t(i) < \lambda_i$ for each $i \in I$ such that, for all $\eta < \kappa_i$, we have $t(i) \neq h(i, \eta)(i)$.
    PROOF: Since the function that maps η to $h(i, \eta)(i)$ cannot be surjective $\kappa_i \to \lambda_i$.
  ⟨2⟩3. For all $i \in I$ and $\eta < \kappa_i$ we have $h \neq t(i, \eta)$.
□

Proposition 9.17. *If κ is an infinite cardinal then $\kappa\kappa = \kappa$.*

PROOF:
⟨1⟩1. LET: A be an infinite set.
⟨1⟩2. LET: $\mathcal{F}$ be the set of all functions f such that there exists $X \subseteq A$ such that $f : X \times X \sim X$
⟨1⟩3. $\mathcal{F}$ is nonempty.
  PROOF: Pick a countably infinite $X \subseteq A$. Then $X \times X \sim X$.
⟨1⟩4. $\mathcal{F}$ is partially ordered by extension.
⟨1⟩5. Every chain in $\mathcal{F}$ has an upper bound.
⟨1⟩6. PICK $f \in \mathcal{F}$ maximal.
⟨1⟩7. PICK $X \subseteq A$ such that $f : X \times X \sim X$.
⟨1⟩8. $\operatorname{card} X = \operatorname{card} A$
  ⟨2⟩1. ASSUME: for a contradiction $\operatorname{card} X < \operatorname{card} A$
  ⟨2⟩2. $\operatorname{card} A = \operatorname{card}(A - X)$

PROOF: Corollary 9.11.1.

⟨2⟩3. $\operatorname{card} X < \operatorname{card}(A - X)$

⟨2⟩4. PICK $Y \subseteq A - X$ such that $Y \sim X$

⟨2⟩5. PICK $g : (X \times Y) \cup (Y \times X) \cup (Y \times Y) \sim Y$

PROOF:

$$\begin{aligned}
(X \times Y) \cup (Y \times X) \cup (Y \times Y) &\sim 3 \times X \times X && (\langle 2\rangle 4)\\
&\sim 3 \times X && (\langle 1\rangle 7)\\
&\sim X && (\text{Corollary 9.11.1})\\
&\sim Y && (\langle 2\rangle 4)
\end{aligned}$$

⟨2⟩6. $f \cup g : (X \cup Y) \times (X \cup Y) \sim X \cup Y$

⟨2⟩7. Q.E.D.

PROOF: This contradicts the maximality of f.

□

Corollary 9.17.1. *If κ and λ are non-zero cardinals that are not both finite, then*

$$\kappa\lambda = \max(\kappa, \lambda) \enspace .$$

Definition 9.18 (Exponentiation)**.** Given cardinal numbers κ and λ, let κ^λ be the cardinality of the set of all functions $\lambda \to \kappa$.

Proposition 9.19.

$$\begin{aligned}
\kappa^{\lambda+\mu} &= \kappa^\lambda \kappa^\mu \\
(\kappa\lambda)^\mu &= \kappa^\mu \lambda^\mu \\
\kappa^{\lambda\mu} &= (\kappa^\lambda)^\mu
\end{aligned}$$

PROOF: Easy. □

Proposition 9.20. *Cardinal exponentiation and ordinal exponentiation agree on the natural numbers.*

PROOF: Easy. □

Proposition 9.21.

$$\operatorname{card} \mathcal{P}X = 2^{\operatorname{card} X}$$

PROOF: Define $\chi : \mathcal{P}X \sim 2^X$ to be the function that maps S to the function $\chi_S : X \to 2$ where $\chi_S(x) = 1$ if $x \in S$ and $\chi_S(x) = 0$ if $x \notin S$. □

Proposition 9.22. *For any infinite cardinal κ we have $\kappa < 2^\kappa$.*

PROOF: Proposition 9.16. □

Proposition 9.23. *If $\kappa \leqslant \lambda$ then $\kappa^\mu \leqslant \lambda^\mu$.*

PROOF: Easy. □

9.2 Alephs

Definition 9.24 (Aleph)**.** Define the cardinal $\aleph_\alpha$ for every ordinal α as follows: $\aleph_\alpha$ is the least infinite cardinal greater than $\aleph_\beta$ for all $\beta < \alpha$.

Proposition 9.25.

$$\aleph_0 = \omega$$

PROOF: Easy. □

Definition 9.26 (Continuum Hypothesis)**.** The *continuum hypothesis* is the statement $\aleph_1 = 2^{\aleph_0}$.

Definition 9.27 (Generalized Continuum Hypothesis)**.** The *generalized continuum hypothesis* is the statement: for every ordinal α we have $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$.

Chapter 10

Field Theory

Definition 10.1 (Field)**.** A *field* is a triple $(K, +, \cdot)$ such that K is a set, $+$ and $\cdot$ are functions $K^2 \to K$, and:

1. $\forall x, y, z \in K. x + (y + z) = (x + y) + z$
2. $\forall x, y, z \in K. x(yz) = (xy)z$
3. $\forall x, y \in K. x + y = y + x$
4. $\forall x, y \in K. xy = yx$
5. There exists a unique $0 \in K$ such that $\forall x \in K. x + 0 = x$
6. There exists a unique $1 \in K$ such that $\forall x \in K. x1 = x$
7. $0 \neq 1$
8. $\forall x \in K. \exists!(-x) \in K. x + (-x) = 0$
9. For all $x \in K$, if $x \neq 0$ then $\exists!(1/x) \in K. x \cdot 1/x = 1$
10. $\forall x, y, z \in K. x(y + z) = xy + xz$

Definition 10.2 (Subtraction)**.** In any field K, define *subtraction* $- : K^2 \to K$ by $x - y = x + (-y)$.

Definition 10.3 (Ordered Field)**.** An *ordered field* is a quadruple $(K, +, \cdot, \leqslant)$ such that $(K, +, \cdot)$ is a field and $\leqslant$ is a linear order on K, and:

1. For all $x, y, z \in K$, if $x < y$ then $x + z < y + z$
2. For all $x, y, z \in K$, if $x < y$ and $0 < z$ then $xz < yz$

Chapter 11

Real Numbers

11.1 Axioms for Real Numbers

Let there be a set $\mathbb{R}$, whose elements are called *real numbers*.

Let there be two functions $+, \cdot : \mathbb{R}^2 \to \mathbb{R}$.

Let there be a relation $< \subseteq \mathbb{R}^2$.

Axiom 11.1 (Associativity of Addition).

$$\forall x, y, z \in \mathbb{R}. x + (y + z) = (x + y) + z$$

Axiom 11.2 (Associativity of Multiplication).

$$\forall x, y, z \in \mathbb{R}. x(yz) = (xy)z$$

Axiom 11.3 (Commutativity of Addition).

$$\forall x, y \in \mathbb{R}. x + y = y + x$$

Axiom 11.4 (Commutativity of Multiplication).

$$\forall x, y \in \mathbb{R}. xy = yx$$

Axiom 11.5 (Identity for Addition). *There exists a unique $z \in \mathbb{R}$ such that $\forall x \in \mathbb{R}. x + z = x$.*

Definition 11.6 (Zero). The real number *zero*, 0, is the unique real number such that $\forall x \in \mathbb{R}. x + 0 = x$.

Axiom 11.7 (Identity for Multiplication). *There exists a unique $i \in \mathbb{R}$ such that $\forall x \in \mathbb{R}. xi = x$. Further, we have $i \neq 0$.*

Definition 11.8 (One). The real number *one*, 1, is the unique real number such that $\forall x \in \mathbb{R}. x1 = x$.

Axiom 11.9 (Additive Inverses)**.** *For all $x \in \mathbb{R}$, there exists a unique $y \in \mathbb{R}$ such that $x + y = 0$.*

Axiom 11.10 (Multiplicative Inverses)**.** *For all $x \in \mathbb{R}$, if $x \neq 0$ then there exists a unique $y \in \mathbb{R}$ such that $xy = 1$.*

Axiom 11.11 (Distributive Law)**.**

$$\forall x, y, z \in \mathbb{R}. x(y + z) = xy + xz$$

Axiom 11.12 (Monotonicity of Addition)**.** *For all $x, y, z \in \mathbb{R}$, if $x < y$ then $x + z < y + z$.*

Axiom 11.13 (Monotonicity of Multiplication)**.** *For all $x, y, z \in \mathbb{R}$, if $x < y$ and $0 < z$ then $xz < yz$.*

Axiom 11.14 (Least Upper Bound Property)**.** *The relation $<$ is a strict linear order on $\mathbb{R}$ with the least upper bound property.*

11.2 Consequences of the Axioms

11.2.1 Negation

Definition 11.15 (Negation)**.** For any real number x, the *negation* of x, $-x$, is the unique real number such that $x + (-x) = 0$.

Theorem 11.16. *For any real numbers x and y, if $x + y = x$ then $y = 0$.*

PROOF:
⟨1⟩1. LET: $x, y \in \mathbb{R}$
⟨1⟩2. ASSUME: $x + y = x$
⟨1⟩3. $y = 0$
PROOF:

$$\begin{aligned}
y &= y + 0 && \text{(Definition of zero)} \\
&= y + (x + (-x)) && \text{(Definition of } -x\text{)} \\
&= (y + x) + (-x) && \text{(Associativity of Addition)} \\
&= (x + y) + (-x) && \text{(Commutativity of Addition)} \\
&= x + (-x) && (\langle 1\rangle 2) \\
&= 0 && \text{(Definition of } -x\text{)}
\end{aligned}$$

□

Theorem 11.17.

$$\forall x \in \mathbb{R}. 0x = 0$$

PROOF:
⟨1⟩1. LET: $x \in \mathbb{R}$
⟨1⟩2. $xx + 0x = xx$

PROOF:

$$\begin{aligned} xx + 0x &= (x+0)x && \text{(Distributive Law)} \\ &= xx && \text{(Definition of 0)} \end{aligned}$$

⟨1⟩3. $0x = 0$

PROOF: Theorem 11.16, ⟨1⟩2.

□

Theorem 11.18.

$$-0 = 0$$

PROOF: Since $0 + 0 = 0$. □

Theorem 11.19.

$$\forall x \in \mathbb{R}. -(-x) = x$$

PROOF: Since $-x + x = 0$. □

Theorem 11.20.

$$\forall x, y \in \mathbb{R}. x(-y) = -(xy)$$

PROOF:

$$\begin{aligned} x(-y) + xy &= x((-y) + y) && \text{(Distributive Law)} \\ &= x0 && \text{(Definition of } -y\text{)} \\ &= 0 && \text{(Theorem 11.17)} \end{aligned}$$ □

Theorem 11.21.

$$\forall x \in \mathbb{R}. (-1)x = -x$$

PROOF:

$$\begin{aligned} (-1)x &= -(1 \cdot x) && \text{(Theorem 11.20)} \\ &= -x && \text{(Definition of 1)} \end{aligned}$$ □

11.2.2 Subtraction

Theorem 11.22.

$$\forall x, y, z \in \mathbb{R}. x(y - z) = xy - xz$$

PROOF:

$$\begin{aligned} x(y - z) &= x(y + (-z)) && \text{(Definition of subtraction)} \\ &= xy + x(-z) && \text{(Distributive Law)} \\ &= xy + (-(xz)) && \text{(Theorem 11.20)} \\ &= xy - xz && \text{(Definition of subtraction)} \end{aligned}$$ □

Theorem 11.23.

$$\forall x, y \in \mathbb{R}. -(x + y) = -x - y$$

PROOF:

$$\begin{aligned}
-(x+y) &= (-1)(x+y) && \text{(Theorem 11.21)} \\
&= (-1)x + (-1)y && \text{(Distributive Law)} \\
&= -x + (-y) && \text{(Theorem 11.21)} \\
&= -x - y && \text{(Definition of subtraction)} \quad \square
\end{aligned}$$

Theorem 11.24.

$$\forall x, y \in \mathbb{R}. -(x-y) = -x + y$$

PROOF:

$$\begin{aligned}
-(x-y) &= -(x+(-y)) && \text{(Definition of subtraction)} \\
&= -x - (-y) && \text{(Theorem 11.23)} \\
&= -x + (-(-y)) && \text{(Definition of subtraction)} \\
&= -x + y && \text{(Theorem 11.19)} \quad \square
\end{aligned}$$

Definition 11.25 (Reciprocal)**.** Given $x \in \mathbb{R}$ with $x \neq 0$, the *reciprocal* of x, $1/x$, is the unique real number such that $x \cdot 1/x = 1$.

Theorem 11.26. *For any real numbers x and y, if $x \neq 0$ and $xy = x$ then $y = 1$.*

PROOF:
⟨1⟩1. LET: $x, y \in \mathbb{R}$
⟨1⟩2. ASSUME: $x \neq 0$
⟨1⟩3. ASSUME: $xy = x$
⟨1⟩4. $y = 1$
PROOF:

$$\begin{aligned}
y &= y1 && \text{(Definition of 1)} \\
&= y(x \cdot 1/x) && \text{(Definition of } 1/x, \langle 1\rangle 2) \\
&= (yx)1/x && \text{(Associativity of Multiplication)} \\
&= (xy)1/x && \text{(Commutativity of Multiplication)} \\
&= x \cdot 1/x && (\langle 1\rangle 3) \\
&= 1 && \text{(Definition of } 1/x, \langle 1\rangle 2)
\end{aligned}$$

□

Definition 11.27 (Quotient)**.** Given real numbers x and y with $y \neq 0$, the *quotient* x/y is defined by

$$x/y = x \cdot 1/y \ .$$

Theorem 11.28. *For any real number x, if $x \neq 0$ then $x/x = 1$.*

PROOF: Immediate from definitions. □

Theorem 11.29.

$$\forall x \in \mathbb{R}. x/1 = x$$

PROOF:

⟨1⟩1. LET: $x \in \mathbb{R}$
⟨1⟩2. $1/1 = 1$
PROOF: Since $1 \cdot 1 = 1$.
⟨1⟩3. $x/1 = x$
PROOF: Since $x/1 = x \cdot 1/1 = x \cdot 1 = x$.
□

Theorem 11.30. *For any real numbers x and y, if $x \neq 0$ and $y \neq 0$ then $xy \neq 0$.*

PROOF:
⟨1⟩1. LET: $x, y \in \mathbb{R}$
⟨1⟩2. ASSUME: $xy = 0$ and $x \neq 0$
PROVE: $y = 0$
⟨1⟩3. $y = 0$
PROOF:

$$\begin{aligned} y &= 1y && \text{(Definition of 1)} \\ &= (1/x)xy && \text{(Definition of } 1/x, \langle 1\rangle 2\text{)} \\ &= (1/x)0 && (\langle 1\rangle 2) \\ &= 0 && \text{(Theorem 11.17)} \end{aligned}$$

□

Theorem 11.31. *For any real numbers y and z, if $y \neq 0$ and $z \neq 0$ then $(1/y)(1/z) = 1/(yz)$.*

PROOF: Since $yz(1/y)(1/z) = 1 \cdot 1 = 1$. □

Corollary 11.31.1. *For any real numbers x, y, z, w with $y \neq 0 \neq w$, we have $(x/y)(z/w) = (xz)/(yw)$.*

Theorem 11.32. *For any real numbers x, y, z, w with $y \neq 0 \neq w$, we have*

$$\frac{x}{y} + \frac{z}{w} = \frac{xw + yz}{yw}$$

PROOF:

$$\begin{aligned} yw\left(\frac{x}{y} + \frac{z}{w}\right) &= yw\frac{x}{y} + yw\frac{z}{w} \\ &= wx + yz \end{aligned}$$

□

Theorem 11.33. *For any real number x, if $x \neq 0$ then $1/x \neq 0$.*

PROOF: Since $x \cdot 1/x = 1 \neq 0$. □

Theorem 11.34. *For any real numbers w, z, if $w \neq 0 \neq z$ then $1/(w/z) = z/w$.*

PROOF: Since $(z/w)(w/z) = (wz)/(wz) = 1$. □

Theorem 11.35. *For any real numbers a, x and y, if $y \neq 0$ then $(ax)/y = a(x/y)$*

PROOF: Since $ya(x/y) = ax$. ∎

Theorem 11.36. *For any real numbers x and y, if $y \neq 0$ then $(-x)/y = x/(-y) = -(x/y)$.*

PROOF:
⟨1⟩1. $(-x)/y = -(x/y)$
  PROOF: Take $a = -1$ in Theorem 11.35.
⟨1⟩2. $x/(-y) = -(x/y)$
  PROOF: Since $(-y)(-(x/y)) = y(x/y) = x$.
∎

Theorem 11.37. *For any real numbers x, y, z and w, if $x > y$ and $w > z$ then $x + w > y + z$.*

PROOF: We have $y + z < x + z < x + w$ by Monotonicity of Addition twice. ∎

Corollary 11.37.1. *For any real numbers x and y, if $x > 0$ and $y > 0$ then $x + y > 0$.*

Theorem 11.38. *For any real numbers x and y, if $x > 0$ and $y > 0$ then $xy > 0$.*

PROOF:

$$\begin{aligned} xy &> 0y && \text{(Monotonicity of Multiplication)} \\ &= 0 && \text{(Theorem 11.17)} \end{aligned}$$ ∎

Theorem 11.39. *For any real number x, we have $x > 0$ iff $-x < 0$.*

PROOF:
⟨1⟩1. If $0 < x$ then $-x < 0$
  PROOF: By Monotonicity of Addition adding $-x$ to both sides.
⟨1⟩2. If $-x < 0$ then $0 < x$
  PROOF: By Monotonicity of Addition adding x to both sides.
∎

Theorem 11.40. *For any real numbers x and y, we have $x > y$ iff $-x < -y$.*

PROOF:
⟨1⟩1. If $y < x$ then $-x < -y$.
  PROOF: By Monotonicity of Addition adding $-x - y$ to both sides.
⟨1⟩2. If $-x < -y$ then $y < x$.
  PROOF: By Monotonicity of Addition adding $x + y$ to both sides.
∎

Theorem 11.41. *For any real numbers x, y and z, if $x > y$ and $z < 0$ then $xz < yz$.*

PROOF:
⟨1⟩1. LET: x, y and z be real numbers.

$\langle 1 \rangle 2$. ASSUME: $x > y$
$\langle 1 \rangle 3$. ASSUME: $z < 0$
$\langle 1 \rangle 4$. $-z > 0$
PROOF: Theorem 11.39, $\langle 1 \rangle 3$.
$\langle 1 \rangle 5$. $x(-z) > y(-z)$
PROOF: $\langle 1 \rangle 2$, $\langle 1 \rangle 4$, Monotonicity of Multiplication.
$\langle 1 \rangle 6$. $-(xz) > -(yz)$
PROOF: Theorem 11.20, $\langle 1 \rangle 5$.
$\langle 1 \rangle 7$. $xz < yz$
PROOF: Theorem 11.39, $\langle 1 \rangle 6$.
□

Theorem 11.42. *For any real number x, if $x \neq 0$ then $xx > 0$.*

PROOF:
$\langle 1 \rangle 1$. If $x > 0$ then $xx > 0$
PROOF: By Monotonicity of Multiplication.
$\langle 1 \rangle 2$. If $x < 0$ then $xx > 0$
PROOF: Theorem 11.41.
□

Theorem 11.43.

$$0 < 1$$

PROOF: By Theorem 11.42 since $1 = 1 \cdot 1$. □

Definition 11.44 (Positive)**.** A real number x is *positive* iff $x > 0$.
We write $\mathbb{R}_+$ for the set of positive reals.

Theorem 11.45. *For any real numbers x and y, we have xy is positive if and only if x and y are both positive or both negative.*

PROOF: By the Monotonicity of Multiplication and Theorem 11.41. □

Corollary 11.45.1. *For any real number x, if $x > 0$ then $1/x > 0$.*

PROOF: Since $x \cdot 1/x = 1$ is positive. □

Theorem 11.46. *For any real numbers x and y, if $x > y > 0$ then $1/x < 1/y$.*

PROOF: If $1/y \leqslant 1/x$ then $1 < 1$ by Monotonicity of Multiplication. □

Theorem 11.47. *For any real numbers x and y, if $x < y$ then $x < (x+y)/2 < y$.*

PROOF: We have $2x < x + y$ and $x + y < 2y$ by Monotonicity of Addition, hence $x < (x + y)/2 < y$ by Monotonicity of Multiplication since $1/2 > 0$. □

Corollary 11.47.1. *$\mathbb{R}$ is a linear continuum.*

Definition 11.48 (Negative)**.** A real number x is *negative* iff $x < 0$.
We write $\overline{\mathbb{R}_+}$ for the set of nonnegative reals.

Chapter 12

Integers

Definition 12.1 (Inductive)**.** A set of real numbers A is *inductive* iff $1 \in A$ and $\forall x \in A . x + 1 \in A$.

Definition 12.2 (Positive Integer)**.** The set $\mathbb{Z}_+$ of *positive integers* is the intersection of the set of inductive sets.

Proposition 12.3. *Every positive integer is positive.*

PROOF: The set of positive reals is inductive. $\square$

Proposition 12.4. *1 is the least element of* $\mathbb{Z}_+$.

PROOF: Since $\{x \in \mathbb{R} : x \geqslant 1\}$ is inductive. $\square$