Axiomatic Set theory

Gudfit

Contents

1 Set Theory

Definition 1.1 (Set)**.** A *set* is any object in our universe of discourse. Sets are fundamental entities in mathematics that can contain elements, which themselves can be sets.

1.1 Properties

Definition 1.2 (Property)**.** A *property* is a mathematical statement or condition that can be evaluated as either *true* or *false* depending on the values of its variables. Properties are essential in defining sets, formulating mathematical expressions, and constructing logical arguments.

If $X, Y, \ldots, Z$ are free variables in a property $\mathbf{Q}$, we write $\mathbf{Q}(X, Y, \ldots, Z)$ to indicate that $\mathbf{Q}$ is a property concerning $X, Y, \ldots, Z$.

Definition 1.3 (Components of a Property)**.**

- Variables: Symbols like $X, Y, \ldots, Z$ representing elements from the universe of discourse. These can be individual variables or tuples of variables.
- Predicate Structure: The property $\mathbf{Q}$ typically involves logical connectives (such as $\wedge$, $\vee$, $\neg$), relational operators (such as $=, <, >$), and may include quantifiers when forming more complex statements.
- Truth Value: For any assignment of values to the variables $X, Y, \ldots, Z$, the property $\mathbf{Q}(X, Y, \ldots, Z)$ evaluates to either *true* or *false*.

Example. Examples of properties:

- Single Variable Property: $\mathbf{P}(x) : x$ is an even integer.
- Multiple Variables Property: $\mathbf{R}(x, y) : x$ is divisible by y.
- Geometric Property: $\mathbf{S}(A, B, C)$: Triangle ABC is equilateral.

1.2 Axioms

Definition 1.4 (Axiom of Existence)**.** There exists a set that contains no elements:

$$\exists A \, \forall x \, \neg (x \in A)$$

Remark. Definition 1.4 ensures that there is at least one set in our universe, preventing it from being empty.

Definition 1.5 (Axiom of Extensionality)**.** If every element of set X is also an element of set Y and every element of Y is an element of X, then $X = Y$:

$$\forall X \, \forall Y \, \left([\forall x (x \in X \leftrightarrow x \in Y)] \implies X = Y \right)$$

Remark. Definition 1.5 defines equality between sets based on their elements.

Definition 1.6 (Empty Set)**.** The unique set that contains no elements is called the *empty set* and is denoted by $\emptyset$.

Definition 1.7 (Axiom Schema of Comprehension)**.** For any property $\mathbf{P}(x)$ and any set A, there exists a set B such that an element x is in B if and only if x is in A and x satisfies the property $\mathbf{P}(x)$:

$$\forall A\, \exists B\, (\forall x\, (x \in B \leftrightarrow (x \in A \wedge \mathbf{P}(x))))$$

Remark. The Axiom Schema of Comprehension allows the formation of subsets from a set A using a property $\mathbf{P}(x)$.

Definition 1.8 (Set Builder Notation)**.** Given a property $\mathbf{P}(x)$ and a set A, the set B from Definition 1.7 is denoted by:

$$B = \{x \in A \mid \mathbf{P}(x)\}$$

Definition 1.9 (Axiom of Pairing)**.** For any sets A and B, there exists a set C such that an element x is in C if and only if $x = A$ or $x = B$:

$$\forall A\, \forall B\, \exists C\, (\forall x\, (x \in C \leftrightarrow (x = A \vee x = B)))$$

Definition 1.10 (Notation for Pairs)**.** The set C from Definition 1.9 is denoted by $\{A, B\}$. If $A = B$, we write $\{A\}$.

Definition 1.11 (Axiom of Union)**.** For any set S, there exists a set U such that an element x is in U if and only if $x \in A$ for some $A \in S$:

$$\forall S\, \exists U\, (\forall x\, (x \in U \leftrightarrow (\exists A\, (A \in S \wedge x \in A))))$$

Definition 1.12 (Union of a System of Sets)**.** Given a set S, the set U from Definition 1.11 is denoted by:

$$U = \bigcup S$$

Definition 1.13 (Union of Two Sets)**.** For sets A and B, the union $A \cup B$ is defined as:

$$A \cup B = \bigcup \{A, B\}$$

Definition 1.14 (Subset)**.** A set B is a *subset* of a set A if every element of B is also an element of A:

$$B \subseteq A \iff \forall x (x \in B \implies x \in A)$$

Definition 1.15 (Axiom of Power Set)**.** For any set S, there exists a set P such that an element X is in P if and only if $X \subseteq S$:

$$\forall S\, \exists P\, (\forall X\, (X \in P \leftrightarrow X \subseteq S))$$

Definition 1.16 (Power Set)**.** Given a set S, the set P from Definition 1.15 is called the *power set* of S, denoted by $\mathscr{P}(S)$.

Theorem 1.1. A set of all sets ($\{x|T\}$) does not exist and $\forall A \times x(x \notin A)$.

Proof. Suppose $V = \{x|T\}$ exists, then by Definition 1.7, $R = \{x \in V | x \notin x\}$ exists. However, we have $R \in \mathbb{R} \iff R \notin R$ by definition of R. Hence V doesn't exist.

Suppose $\exists A \forall x(x \in A)$ for the sake of contradiction. Then, A is the set of all sets which is impossible. ■

1.3 Elementary Operations on Sets

Definition 1.17 (Proper Subset)**.** A set B is a *proper subset* of a set A if $B \subseteq A$ and $B \neq A$. This is denoted by $B \subsetneq A$.

Definition 1.18 (Elementary Operations on Sets)**.** For sets A and B:

(i) Intersection:$A \cap B = \{x \mid x \in A \wedge x \in B\}$

(ii) Union: $A \cup B = \{x \mid x \in A \vee x \in B\}$

(iii) Difference: $A - B = \{x \mid x \in A \wedge x \notin B\}$

(iv) Symmetric Difference:$A \triangle B = (A - B) \cup (B - A)$

1.4 Basic Properties of Set Operations

Definition 1.19 (Intersection of a Collection of Sets)**.** For a non-empty set S, the *intersection* is defined as:

$$\bigcap S = \{x \mid \forall A \in S,\ x \in A\}$$

Definition 1.20 (System of Mutually Disjoint Sets)**.** A collection of sets S is called *mutually disjoint* if for any distinct sets $A, B \in S$, their intersection is empty:

$$\forall A, B \in S,\ (A \neq B \implies A \cap B = \emptyset)$$

1.4.1 Properties of Elementary Operations

- Commutative Laws:
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
  - $A \triangle B = B \triangle A$
- Associative Laws:
  - $(A \cup B) \cup C = A \cup (B \cup C)$
  - $(A \cap B) \cap C = A \cap (B \cap C)$
  - $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
- Distributive Laws:
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- De Morgan's Laws:
  - $U - (A \cup B) = (U - A) \cap (U - B)$

- $U - (A \cap B) = (U - A) \cup (U - B)$

- Other Properties:
  - $A - (B \cap C) = (A - B) \cup (A - C)$
  - $A - B = \emptyset \iff A \subseteq B$
  - $A \triangle B = \emptyset \iff A = B$

1.4.2 Proofs of Basic Set Properties

- Commutative Laws:

  (a) Union is Commutative: $A \cup B = B \cup A$

  Proof. Let x be an arbitrary element.

  $$\begin{aligned} x \in A \cup B &\iff x \in A \vee x \in B \\ &\iff x \in B \vee x \in A \\ &\iff x \in B \cup A. \end{aligned}$$

  Since $x \in A \cup B$ if and only if $x \in B \cup A$, we have $A \cup B = B \cup A$. ■

  (b) Intersection is Commutative: $A \cap B = B \cap A$

  Proof. Let x be an arbitrary element.

  $$\begin{aligned} x \in A \cap B &\iff x \in A \wedge x \in B \\ &\iff x \in B \wedge x \in A \\ &\iff x \in B \cap A. \end{aligned}$$

  Therefore, $A \cap B = B \cap A$. ■

  (c) Symmetric Difference is Commutative: $A \triangle B = B \triangle A$

  Proof. Recall that $A \triangle B = (A - B) \cup (B - A)$.

  $$\begin{aligned} A \triangle B &= (A - B) \cup (B - A) \\ &= (B - A) \cup (A - B) \\ &= B \triangle A. \end{aligned}$$

  Thus, $A \triangle B = B \triangle A$. ■

- Associative Laws:

  (a) Union is Associative: $(A \cup B) \cup C = A \cup (B \cup C)$

Proof. Let x be an arbitrary element.

$$\begin{aligned} x \in (A \cup B) \cup C &\iff x \in (A \cup B) \vee x \in C \\ &\iff (x \in A \vee x \in B) \vee x \in C \\ &\iff x \in A \vee x \in B \vee x \in C \\ &\iff x \in A \vee (x \in B \vee x \in C) \\ &\iff x \in A \cup (B \cup C). \end{aligned}$$

Therefore, $(A \cup B) \cup C = A \cup (B \cup C)$. ■

(b) Intersection is Associative: $(A \cap B) \cap C = A \cap (B \cap C)$

Proof. Let x be an arbitrary element.

$$\begin{aligned} x \in (A \cap B) \cap C &\iff x \in (A \cap B) \wedge x \in C \\ &\iff (x \in A \wedge x \in B) \wedge x \in C \\ &\iff x \in A \wedge x \in B \wedge x \in C \\ &\iff x \in A \wedge (x \in B \wedge x \in C) \\ &\iff x \in A \cap (B \cap C). \end{aligned}$$

Thus, $(A \cap B) \cap C = A \cap (B \cap C)$. ■

(c) Symmetric Difference is Associative: $(A \triangle B) \triangle C = A \triangle (B \triangle C)$

Proof. We will show that both sides are equal by showing that an element x belongs to one side if and only if it belongs to the other.
Recall that $A \triangle B = (A - B) \cup (B - A)$.
Let x be an arbitrary element.
Left Side:

$$x \in (A \triangle B) \triangle C \iff x \in (A \triangle B) \triangle C$$

Right Side:

$$x \in A \triangle (B \triangle C) \iff x \in A \triangle (B \triangle C)$$

The symmetric difference is associative, so $(A \triangle B) \triangle C = A \triangle (B \triangle C)$. ■

- Distributive Laws:

(a) Intersection Distributes over Union: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof. Let x be an arbitrary element.

$$\begin{aligned} x \in A \cap (B \cup C) &\iff x \in A \wedge (x \in B \vee x \in C) \\ &\iff (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\ &\iff x \in (A \cap B) \vee x \in (A \cap C) \\ &\iff x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Therefore, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. ■

(b) Union Distributes over Intersection: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof. Let x be an arbitrary element.

$$\begin{aligned} x \in A \cup (B \cap C) &\iff x \in A \vee (x \in B \wedge x \in C) \\ &\iff (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\ &\iff x \in (A \cup B) \wedge x \in (A \cup C) \\ &\iff x \in (A \cup B) \cap (A \cup C). \end{aligned}$$

Thus, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. ■

- De Morgan's Laws:

(a) Complement of Union: $U - (A \cup B) = (U - A) \cap (U - B)$

Proof. Let x be an arbitrary element in the universal set U.

$$\begin{aligned} x \in U - (A \cup B) &\iff x \in U \wedge x \notin A \cup B \\ &\iff x \in U \wedge \neg(x \in A \vee x \in B) \\ &\iff x \in U \wedge (x \notin A \wedge x \notin B) \\ &\iff (x \in U - A) \wedge (x \in U - B) \\ &\iff x \in (U - A) \cap (U - B). \end{aligned}$$

Therefore, $U - (A \cup B) = (U - A) \cap (U - B)$. ■

(b) Complement of Intersection: $U - (A \cap B) = (U - A) \cup (U - B)$

Proof. Let x be an arbitrary element in U.

$$\begin{aligned} x \in U - (A \cap B) &\iff x \in U \wedge x \notin A \cap B \\ &\iff x \in U \wedge \neg(x \in A \wedge x \in B) \\ &\iff x \in U \wedge (x \notin A \vee x \notin B) \\ &\iff (x \in U - A) \vee (x \in U - B) \\ &\iff x \in (U - A) \cup (U - B). \end{aligned}$$

Thus, $U - (A \cap B) = (U - A) \cup (U - B)$. ■

- Other Properties:

(a) Difference and Intersection: $A - (B \cap C) = (A - B) \cup (A - C)$

Proof. Let x be an arbitrary element.

$$\begin{aligned} x \in A - (B \cap C) &\iff x \in A \wedge x \notin B \cap C \\ &\iff x \in A \wedge \neg(x \in B \wedge x \in C) \\ &\iff x \in A \wedge (x \notin B \vee x \notin C) \\ &\iff (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \\ &\iff x \in (A - B) \vee x \in (A - C) \\ &\iff x \in (A - B) \cup (A - C). \end{aligned}$$

Therefore, $A - (B \cap C) = (A - B) \cup (A - C)$. ■

(b) Empty Difference and Subset: $A - B = \emptyset \iff A \subseteq B$

Proof. ($\implies$) Assume $A - B = \emptyset$.
Let $x \in A$. Since $x \notin A - B$, it must be that $x \notin A - B \implies x \notin A \wedge x \in B$ is false. However, $x \in A$, so the only possibility is $x \in B$. Therefore, $x \in B$, and thus $A \subseteq B$.
($\impliedby$) Assume $A \subseteq B$.
Then, for any $x \in A$, $x \in B$. Therefore, $x \notin A - B$. Hence, $A - B$ contains no elements, so $A - B = \emptyset$. ■

(c) Symmetric Difference and Equality: $A \triangle B = \emptyset \iff A = B$

Proof. ($\implies$) Assume $A \triangle B = \emptyset$.
Then, $(A - B) \cup (B - A) = \emptyset$. This implies $A - B = \emptyset$ and $B - A = \emptyset$. Therefore, $A \subseteq B$ and $B \subseteq A$, so $A = B$.
($\impliedby$) Assume $A = B$.
Then, $A - B = A - A = \emptyset$ and $B - A = B - B = \emptyset$. Thus, $A \triangle B = \emptyset$. ■

2 Functions

2.1 Ordered Pairs

Definition 2.1 (Ordered Pair)**.** An ordered pair (a,b) is defined as:

$$(a,b) \triangleq \{\{a\},\{a,b\}\}$$

Theorem 2.1. For any elements a,b,a',b':

$$(a,b) = (a',b') \iff a = a' \text{ and } b = b'$$

Proof. ($\impliedby$) If $a = a'$ and $b = b'$, then clearly $(a,b) = (a',b')$ by the definition of ordered pairs.

($\implies$) Assume $(a,b) = (a',b')$.

Case 1: If $a = b$, then

$$(a,b) = \{\{a\}\} = \{\{a'\},\{a',b'\}\}$$

This implies that $\{\{a\}\}$ is equal to a set containing one or two elements. The only possibility is that $\{a\} = \{a'\} = \{a',b'\}$, which can only occur if $a = a' = b'$.

Case 2: If $a \neq b$, then $a' \neq b'$ (since if $a' = b'$, we would be back to Case 1). We have:

$$\{\{a\},\{a,b\}\} = \{\{a'\},\{a',b'\}\}$$

This equality implies that the sets of elements are the same, so:

$$\{a\} = \{a'\} \implies a = a'$$

and

$$\{a,b\} = \{a',b'\} \implies \{a,b\} = \{a',b'\}$$

Since $a = a'$, it follows that $b = b'$.
Thus, in both cases, we conclude that $a = a'$ and $b = b'$. ■

Definition 2.2 (Ordered Triples and Quadruples)**.** Ordered tuples are defined recursively:

- The ordered triple (a,b,c) is defined as $((a,b),c)$.
- The ordered quadruple (a,b,c,d) is defined as $((a,b,c),d)$.

2.2 Relations

Definition 2.3 (Binary Relation)**.** A set R is called a binary relation if all its elements are ordered pairs:

$$R \text{ is a binary relation} \iff \forall a \in R,\ \exists x, \exists y,\ a = (x,y)$$

Notation 2.1. If $(x,y) \in R$, we write xRy and say that x is related to y by R.

Definition 2.4 (Domain, Range, and Field of a Binary Relation)**.** Let R be a binary relation.

- The domain of R is defined as:

$$dom(R) = \{x \mid \exists y,\ xRy\}$$

- The range of R is defined as:

$$ran(R) = \{y \mid \exists x,\ xRy\}$$

- The field of R is defined as:

$$field(R) = dom(R) \cup ran(R)$$

- If $field(R) \subseteq X$, we say that R is a relation in X, or a relation between elements of X.

Proposition 2.1. Let R be a binary relation. And let $A = \bigcup(\bigcup R)$. Then $(x,y) \in R$ implies $x \in A$ and $y \in A$.

Proof. If $(x,y) = \{\{x\},\{x,y\}\} \in \mathbb{R}$, then $\{x,y\} \in \bigcup R$, and thus $x,y \in A$. ■

Lemma 2.1. Let R be a binary relation. Then $dom(R)$ and $ran(R)$ exist.

Proof. Since every element $a \in R$ is an ordered pair (x,y), both x and y are elements of $\bigcup(\bigcup R)$. Therefore, $dom(R)$ and $ran(R)$ are subsets of $\bigcup(\bigcup R)$, which exists by the axioms of set theory. ■

Definition 2.5 (Image and Inverse Image)**.** Let R be a binary relation and A be a set.

- The image of A under R is defined as:

$$R[A] = \{y \in ran(R) \mid \exists x \in A,\ xRy\}$$

- The inverse image of A under R is defined as:

$$R^{-1}[A] = \{x \in dom(R) \mid \exists y \in A,\ xRy\}$$

Notation 2.2. We write $\{(x,y) \mid P(x,y)\}$ instead of $\{w \mid \exists x, \exists y,\ w = (x,y) \wedge P(x,y)\}$.

Definition 2.6 (Inverse Relation)**.** Let R be a binary relation. The inverse of R, denoted R^{-1}, is defined as:

$$R^{-1} = \{(x,y) \mid yRx\}$$

Definition 2.7 (Composition of Relations)**.** Let R and S be binary relations. The composition of R and S, denoted $S \circ R$, is defined as:

$$S \circ R = \{(x,z) \mid \exists y,\ xRy \text{ and } ySz\}$$

Definition 2.8 (Membership Relation and Identity Relation)**.** Let A be a set.

- The membership relation on A is defined as:

$$\in_A = \{(a,b) \mid a,b \in A \text{ and } a \in b\}$$

- The identity relation on A is defined as:

$$\mathrm{Id}_A = \{(a,a) \mid a \in A\}$$

Definition 2.9 (Cartesian Product)**.** Let A and B be sets. The Cartesian product of A and B, denoted $A \times B$, is defined as:

$$A \times B = \{(a,b) \mid a \in A \text{ and } b \in B\}$$

Lemma 2.2. Let A and B be sets. Then $A \times B$ exists.

Proof. For any $a \in A$ and $b \in B$, the ordered pair (a,b) is defined as $\{\{a\},\{a,b\}\}$. Since a and b are elements of $A \cup B$, both $\{a\}$ and $\{a,b\}$ are subsets of $A \cup B$. Therefore, (a,b) is an element of $\mathscr{P}(\mathscr{P}(A \cup B))$, which exists by the axiom of power set. Thus, $A \times B \subseteq \mathscr{P}(\mathscr{P}(A \cup B))$, and hence $A \times B$ exists. ■

Corollary. Let R and S be binary relations, and let A be a set. Then R^{-1}, $S \circ R$, $\in_A$, and Id_A exist.

Proof.

- Since yRx, we have $(x,y) \in ran(R) \times dom(R)$, so $R^{-1} \subseteq ran(R) \times dom(R)$, which exists.
- For $(x,z) \in S \circ R$, there exists y such that xRy and ySz. Therefore, $x \in dom(R)$ and $z \in ran(S)$, so $(x,z) \in dom(R) \times ran(S)$, which exists.
- For $a,b \in A$, $(a,b) \in A \times A$, so $\in_A \subseteq A \times A$, which exists.
- For $a \in A$, $(a,a) \in A \times A$, so $\mathrm{Id}_A \subseteq A \times A$, which exists.

■

Lemma 2.3. Let R be a binary relation and A be a set. Then the inverse image of A under R is equal to the image of A under R^{-1}:

$$R^{-1}[A] = R^{-1}[A]$$

In other words, the inverse image of A under R is the same as the image of A under R^{-1}.

Proof. By definition:

$$R^{-1}[A] = \{x \in dom(R) \mid \exists y \in A,\ xRy\}$$

Similarly, the image of A under R^{-1} is:

$$R^{-1}[A] = \{x \in ran(R^{-1}) \mid \exists y \in A,\ yR^{-1}x\}$$

Since $yR^{-1}x$ is equivalent to xRy, and $ran(R^{-1}) = dom(R)$, it follows that:

$$R^{-1}[A] = \{x \in dom(R) \mid \exists y \in A,\ xRy\} = R^{-1}[A]$$

Thus, the inverse image of A under R is equal to the image of A under R^{-1}. ■

Remark. This result clarifies any possible ambiguity in the expression $R^{-1}[A]$, confirming that the inverse image under R is the same as the image under R^{-1}.

Notation 2.3. We write A^2 instead of $A \times A$ to denote the Cartesian product of A with itself.

2.3 Functions

Definition 2.10 (Function)**.** A binary relation F is called a *function* (or *mapping*) if for all a, b_1, and b_2,

$$aFb_1 \wedge aFb_2 \implies b_1 = b_2.$$

For each $a \in dom(F)$, there exists a unique b such that aFb. This b is called the *value of F at a* and is denoted by $F(a)$ or F_a.

Notation 2.4. If F is a function with $dom(F) = A$ and $ran(F) \subseteq B$, we write $F{:}A \to B$. Other notations for the function F include:

$$\langle F(a) \mid a \in A\rangle, \quad \langle F_a \mid a \in A\rangle, \quad \langle F_a\rangle_{a\in A}.$$

The range of F can be denoted by $\{F(a) \mid a \in A\}$ or $\{F_a\}_{a\in A}$.

Lemma 2.4 (Function equality)**.** Let F and G be functions. Then,

$$F = G \iff dom(F) = dom(G) \text{ and } \forall x \in dom(F),\ F(x) = G(x).$$

Proof. ($\Rightarrow$) If $F = G$, then obviously $dom(F) = dom(G)$ and $F(x) = G(x)$ for all $x \in dom(F)$.

($\Leftarrow$) Assume $dom(F) = dom(G)$ and $F(x) = G(x)$ for all $x \in dom(F)$. For any $(x, F(x)) \in F$, we have $(x, F(x)) = (x, G(x)) \in G$. Therefore, $F \subseteq G$. Similarly, $G \subseteq F$, hence $F = G$. ■

Definition 2.11 (On, into, onto and restriction)**.** Let F be a function, and let A and B be sets.

- F is a function *on* A if $dom(F) = A$.
- F is a function *into* B if $ran(F) \subseteq B$.
- F is a function *onto* B if $ran(F) = B$.
- The *restriction* of F to A is the function $F \restriction_A$ defined by:

  $$F \restriction_A = \{(a,b) \in F \mid a \in A\}.$$

  If G is a restriction of F, then F is called an *extension* of G.

Theorem 2.2 (Function composition)**.** Let f and g be functions.

(i) The composition $g \circ f$ is a function.

(ii) The domain of $g \circ f$ is $dom(g \circ f) = dom(f) \cap f^{-1}[dom(g)$.

(iii) For all $x \in dom(g \circ f)$, we have $(g \circ f)(x) = g(f(x))$.

Proof. (i) Suppose $x(g \circ f)z_1$ and $x(g \circ f)z_2$. Then there exist y_1 and y_2 such that xfy_1, y_1gz_1, xfy_2, and y_2gz_2. Since f and g are functions, $y_1 = y_2$ and $z_1 = z_2$. Thus, $g \circ f$ is a function.

(ii) We have:

$$\begin{aligned} x \in dom(g \circ f) &\iff \exists z,\ x(g \circ f)z \\ &\iff \exists y,\ xfy \text{ and } y \in dom(g) \\ &\iff x \in dom(f) \text{ and } f(x) \in dom(g) \\ &\iff x \in dom(f) \cap f^{-1}[dom(g). \end{aligned}$$

(iii) For $x \in dom(g \circ f)$, there exists $y = f(x)$ such that $y \in dom(g)$ and $(g \circ f)(x) = g(y) = g(f(x))$.

■

Definition 2.12 (Invertible Function)**.** A function f is called *invertible* if f^{-1} is also a function.

Definition 2.13 (Injective Function)**.** A function f is said to be *injective* (or *one-to-one*) if for all $a_1, a_2 \in dom(f)$,

$$f(a_1) = f(a_2) \implies a_1 = a_2.$$

Notation 2.5. Let f be a function.

- If f is a function *on* A *onto* B, we may write $f : A \twoheadrightarrow B$.
- If f is an *injective* function *on* A *into* B, we may write $f : A \hookrightarrow B$.
- If f is an *injective* function *on* A *onto* B, we may write $f : A \hookrightarrow\!\!\!\!\twoheadrightarrow B$.

- If f is a function *on a subset* of A *into* B, we may write $f : A \rightharpoonup B$.

Theorem 2.3. Let f be a function.

(i) f is invertible if and only if f is injective.

(ii) If f is invertible, then f^{-1} is also invertible and $(f^{-1})^{-1} = f$.

Proof.

(i) ($\Rightarrow$) Suppose f^{-1} is a function. For any $a_1, a_2 \in dom(f)$, if $f(a_1) = f(a_2)$, then

$$a_1 = f^{-1}(f(a_1)) = f^{-1}(f(a_2)) = a_2.$$

Thus, f is injective.

($\Leftarrow$) Suppose f is injective. For any $y \in ran(f)$, there exists a unique $x \in dom(f)$ such that $f(x) = y$. Therefore, f^{-1} is a function.

(ii) Since f^{-1} is a function, we can consider its inverse. Using the property that $(f^{-1})^{-1} = f$, f^{-1} is invertible.

■

Definition 2.14 (Compatible Functions)**.** Let f and g be functions:

- Functions f and g are called *compatible* if

$$\forall x \in dom(f) \cap dom(g)\ f(x) = g(x).$$

- A set of functions F is called a *compatible system of functions* if any two functions $f, g \in F$ are compatible.

Lemma 2.5. Let f and g be functions.

(i) f and g are compatible if and only if $f \cup g$ is a function.

(ii) f and g are compatible if and only if

$$f|_{dom(f)\cap dom(g)} = g|_{dom(f)\cap dom(g)}$$

Proof. (i) ($\Rightarrow$) Suppose f and g are compatible. If $x(f \cup g)y_1$ and $x(f \cup g)y_2$, then either both $(x, y_1), (x, y_2) \in f$ or one in f and one in g. In both cases, $y_1 = y_2$ due to f and g being functions and compatible. Therefore, $f \cup g$ is a function.

($\Leftarrow$) Suppose $f \cup g$ is a function. For any $x \in dom(f) \cap dom(g)$, we have $(x, f(x)) \in f \cup g$ and $(x, g(x)) \in f \cup g$. Since $f \cup g$ is a function, $f(x) = g(x)$.

(ii) ($\Rightarrow$) For $x \in dom(f) \cap dom(g)$, $f \restriction_{dom(f)\cap dom(g)} (x) = f(x) = g(x) = g \restriction_{dom(f)\cap dom(g)} (x)$.

($\Leftarrow$) If $f \restriction_{dom(f)\cap dom(g)} = g \restriction_{dom(f)\cap dom(g)}$, then for all $x \in dom(f) \cap dom(g)$, $f(x) = g(x)$. Thus, f and g are compatible.

■

Theorem 2.4. If F is a compatible system of functions, then $\bigcup F$ is a function with domain $dom(\bigcup F) = \bigcup_{f \in F} dom(f)$. Moreover, $\bigcup F$ extends each function $f \in F$.

Proof. First, note that $\bigcup F$ is a relation. Suppose $(a,b_1),(a,b_2) \in \bigcup F$. Then there exist $f_1, f_2 \in F$ such that $(a,b_1) \in f_1$ and $(a,b_2) \in f_2$. Since f_1 and f_2 are compatible and $a \in dom(f)1 \cap dom(f)2$, we have $b_1 = b_2$. Therefore, $\bigcup F$ is a function.

The domain of $\bigcup F$ is:

$$dom(\bigcup F) = \{a \mid \exists b,\ (a,b) \in \bigcup F\} = \bigcup_{f \in F} dom(f)$$

For each $f \in F$, $f \subseteq \bigcup F$, so $\bigcup F$ extends f. ■

Definition 2.15. Let A and B be sets. We define:

$$B^A = \{f \mid f \text{ is a function on } A \text{ into } B\}.$$

Definition 2.16 (Indexed System of Sets)**.**

- Let $S = \langle S_i \mid i \in I \rangle$ be a function with domain I. We call S an *indexed system of sets* when each S_i is a set.
- A system of sets A is said to be *indexed* by S if $A = \{S_i \mid i \in I\} = ran(S)$.

Notation 2.6. If A is indexed by $S = \langle S_i \mid i \in I \rangle$, we may write:

$$\bigcup_{i \in I} S_i \quad \text{and} \quad \bigcap_{i \in I} S_i$$

instead of $\bigcup A$ and $\bigcap A$, respectively.

Definition 2.17 (Product of an Indexed System of Sets)**.** Let $S = \langle S_i \mid i \in I \rangle$ be an indexed system of sets. The *product* of S is defined as:

$$\prod_{i \in I} S_i = \{f \mid f \text{ is a function on } I \text{ such that } \forall i \in I,\ f(i) \in S_i\}.$$

Notation 2.7. Alternative notations for the product $\prod_{i \in I} S_i$ include:

$$\prod \langle S_i \mid i \in I \rangle, \quad \prod_{i \in I} S(i).$$

Proposition 2.2. If A and B be sets then B^A exists.

Proof. If f is a function from A into B then $f \subseteq A \times B$ or $f \in \mathscr{P}(A \times B)$. ■

Remark. If $S_i = A$ for all $i \in I$, then $\prod_{i \in I} S_i = A^I$.

Proposition 2.3. If $\langle S_i \mid i \in I \rangle$ is an indexed system of sets then $\prod_{i \in I} S(i)$ exists.

Proof. If f is a function on I and $f_i \in S_i$ for all $i \in I$, then f is a function onto $\bigcup_{i \in I} S_i$, hence $f \in (\bigcup_{i \in I} S_i)^I$ ■

2.4 Equivalences and Partitions

Definition 2.18 (Equivalence)**.** Let R be a binary relation in A.

- R is called *reflexive in* A if $\forall a \in A,\ aRa$.
- R is called *symmetric in* A if $\forall a,b \in A,\ (aRb \implies bRa)$.
- R is called *transitive in* A if $\forall a,b,c \in A,\ (aRb \wedge bRc \implies aRc)$.
- R is called an *equivalence on* A if it is reflexive, symmetric, and transitive in A.

Definition 2.19 (Equivalence Class)**.** Let E be an equivalence on A and let $a \in A$. The *equivalence class of* a *modulo* E is the set

$$[a]_E \triangleq \{x \in A \mid xEa\}.$$

Lemma 2.6. Let E be an equivalence on A and let $a,b \in A$.

(i) $aEb \iff [a]_E = [b]_E$

(ii) $\neg(aEb) \iff [a]_E \cap [b]_E = \emptyset$

Proof.

(i) ($\Rightarrow$) Suppose aEb. For any $c \in [a]_E$, cEa and aEb, so by transitivity, cEb. Therefore, $c \in [b]_E$, hence $[a]_E \subseteq [b]_E$. Similarly, since E is symmetric and bEa, we have $[b]_E \subseteq [a]_E$. Therefore, $[a]_E = [b]_E$.
($\Leftarrow$) Suppose $[a]_E = [b]_E$. Since aEa by reflexivity, $a \in [a]_E = [b]_E$, so aEb.

(ii) ($\Rightarrow$) Suppose $[a]_E \cap [b]_E \neq \emptyset$. Then there exists $c \in A$ such that $c \in [a]_E$ and $c \in [b]_E$. Thus, cEa and cEb. Since E is symmetric, aEc, and by transitivity, aEb.
($\Leftarrow$) Suppose aEb. Then $a \in [a]_E$ and $a \in [b]_E$, so $[a]_E \cap [b]_E \neq \emptyset$.

■

Definition 2.20 (Partition)**.** A system S of nonempty sets is called a *partition* of A if:

(i) S is a system of mutually disjoint sets.

(ii) $\bigcup S = A$.

Definition 2.21 (System of All Equivalence Classes)**.** Let E be an equivalence on A. The *system of all equivalence classes* modulo E is the set

$$A/E \triangleq \{[a]_E \mid a \in A\}.$$

Theorem 2.5. Let E be an equivalence on A. Then A/E is a partition of A.

Proof. First, each equivalence class $[a]_E$ is nonempty since $a \in [a]_E$ (by reflexivity).

If $[a]_E \neq [b]_E$, then by the lemma above, $[a]_E \cap [b]_E = \emptyset$. Therefore, A/E is a system of mutually disjoint nonempty sets.

For any $a \in A$, $a \in [a]_E \subseteq \bigcup A/E$. Thus, $A \subseteq \bigcup A/E$. Conversely, since $[a]_E \subseteq A$ for each $a \in A$, we have $\bigcup A/E \subseteq A$. Therefore, $\bigcup A/E = A$. ■

Definition 2.22 (Equivalence Induced by Partition)**.** Let S be a partition of A. The relation E_S in A is defined by

$$E_S \triangleq \{(a,b) \in A \times A \mid \exists C \in S,\ a \in C \wedge b \in C\}.$$

Theorem 2.6. Let S be a partition of A. Then E_S is an equivalence on A.

Proof.

- Reflexivity: For any $a \in A$, since $A = \bigcup S$, there exists $C \in S$ such that $a \in C$. Therefore, aE_Sa.
- Symmetry: If aE_Sb, then $a,b \in C$ for some $C \in S$. Hence, bE_Sa.
- Transitivity: If aE_Sb and bE_Sc, then $a,b \in C$ and $b,c \in D$ for some $C,D \in S$. Since $b \in C \cap D$ and S consists of disjoint sets, we have $C = D$. Therefore, $a,c \in C$, so aE_Sc.

■

Theorem 2.7.

(i) If E is an equivalence on A and $S = A/E$, then $E_S = E$.

(ii) If S is a partition of A, then $A/E_S = S$.

Proof. (i) For any $a,b \in A$:

$$\begin{aligned} aE_Sb &\iff \exists C \in S,\ a \in C \wedge b \in C \\ &\iff \exists c \in A,\ a \in [c]_E \wedge b \in [c]_E \\ &\iff [a]_E = [b]_E \\ &\iff aEb \quad \text{(by the lemma)} \end{aligned}$$

Thus, $E_S = E$.

(ii) For any $a \in A$, let C be the unique element of S containing a. Then, $[a]_{E_S} = \{b \in A \mid aE_Sb\} = C$. Therefore, $A/E_S = S$. ■

■

Notation 2.8. Theorem above shows that equivalences and partitions are essentially the same concepts from different perspectives.

Definition 2.23 (Set of Representatives)**.** A set $X \subseteq A$ is called a *set of representatives* for the equivalence E_S (or for the partition S of A) if

$$\forall C \in S,\ \exists a \in C,\ X \cap C = \{a\}.$$

2.5 Ordering

Definition 2.24 (Partial Ordering and Strict Ordering)**.** Let R be a binary relation on A.

- R is called *antisymmetric* in A if $\forall a,b \in A$, $(aRb \wedge bRa \implies a = b)$.
- R is called *asymmetric* in A if $\forall a,b \in A$, $\neg(aRb \wedge bRa)$.
- R is called a *(partial) ordering* of A if it is reflexive, antisymmetric, and transitive in A.
- R is called a *strict ordering* of A if it is asymmetric and transitive in A.
- If R is a partial ordering of A, then the pair (A,R) is called an *ordered set*.

Example. Define the relation $\subseteq_A$ on A as follows:

- $x \subseteq_A y \iff x,y \in A \wedge x \subseteq y$: Then, $(A,\subseteq_A)$ is an ordered set.
- The relation Id_A is a partial ordering of A.

Theorem 2.8 (Partial and Strict Orderings Correspondence)**.** Let R be a partial ordering of A.

(i) Then the relation S in A defined by

$$S \triangleq R - \mathrm{Id}_A$$

is a strict ordering.

(ii) Let S be a strict ordering of A. Then the relation R in A defined by

$$R \triangleq S \cup \mathrm{Id}_A$$

is a partial ordering.

Proof. Suppose aSb and bSa:

(i) Since $S \subseteq R$, we have aRb and bRa. As R is antisymmetric, we have $a = b$. However, S and Id_A are disjoint, so aSb and bSa imply $a \neq b$, which is a contradiction. Hence, S is asymmetric in A.
Now, assume aSb and bSc. Then aRc since R is transitive. Moreover, $a \neq c$ because S is asymmetric. Therefore, aSc; S is transitive in A.

(ii) Assume aRb and bRa. If $a \neq b$, then aSb and bSa, which is impossible. Therefore, $a = b$; R is antisymmetric.
Assume aRb and bRc. If $a = b$ or $b = c$, then aRc follows directly. If $a \neq b$ and $b \neq c$, then aSb and bSc, and thus aSc since S is transitive in A. Therefore, aRc; R is transitive in A.
R is reflexive in A since $\mathrm{Id}_A \subseteq R$.

■

Notation 2.9.

- If R is a partial ordering, we say $S = R - \mathrm{Id}_A$ *corresponds to the partial ordering* R.
- If S is a strict ordering, we say $R = S \cup \mathrm{Id}_A$ *corresponds to the strict ordering* S.

Definition 2.25 (Comparability)**.** Let $a,b \in A$ and let $\leq$ be a partial ordering on A.

- We say that a and b are *comparable* in the ordering $\leq$ if $a \leq b$ or $b \leq a$.
- We say that a and b are *incomparable* in the ordering $\leq$ if neither $a \leq b$ nor $b \leq a$.

These can be stated equivalently in terms of the corresponding strict ordering $<$.

- We say that a and b are *comparable* in the ordering $<$ if $a = b$ or $a < b$ or $b < a$.

- We say that a and b are *incomparable* in the ordering $<$ if none of $a = b$, $a < b$, and $b < a$ holds.

Definition 2.26 (Total Ordering)**.** An ordering $\leq$ (or $<$) is called *linear* or *total* if any two elements of A are comparable. The pair $(A, \leq)$ is then called a *totally ordered set*.

Definition 2.27 (Chain)**.** Let $(A, \leq)$ be an ordered set and $B \subseteq A$. B is a *chain* in A if any two elements of B are comparable.

Definition 2.28 (Least/Minimal/Greatest/Maximal Element)**.** Let $(A, \leq)$ be an ordered set and $B \subseteq A$.

- $b \in B$ is the *least element* of B in the ordering $\leq$ if $\forall x \in B$, $b \leq x$.
- $b \in B$ is a *minimal element* of B in the ordering $\leq$ if $\forall x \in B$, $(x \leq b \implies x = b)$.
- $b \in B$ is the *greatest element* of B in the ordering $\leq$ if $\forall x \in B$, $x \leq b$.
- $b \in B$ is a *maximal element* of B in the ordering $\leq$ if $\forall x \in B$, $(b \leq x \implies x = b)$.

Notation 2.10. Let $(A, \leq)$ be an ordered set and $B \subseteq A$.

- The least element of B is denoted $\min B$.
- The greatest element of B is denoted $\max B$.

Theorem 2.9 (Basic Properties of Least and Minimal Elements)**.** Let $(A, \leq)$ be an ordered set and $B \subseteq A$.

(i) B has at most one least element.
(ii) The least element of B—if it exists—is also minimal.
(iii) If B is a chain, then every minimal element of B is also least.

Proof. Let $(B, \leq)$ be a totally ordered set.

(i) If b and b' are least elements of B, then $b \leq b'$ and $b' \leq b$ by the definition. As $\leq$ is antisymmetric, we have $b = b'$.
(ii) Let b be the least element of B (assuming its existence). Take any $x \in B$ and assume $x \leq b$. Then, as b is the least, we have $b \leq x$. As $\leq$ is antisymmetric, $x = b$; b is minimal.
(iii) Let b be a minimal element of B. Take any $x \in B$. Since b and x are comparable, it is $x \leq b$ or $b \leq x$. If $x \leq b$, then $x = b$ as b is minimal. Therefore, b is the least.

■

Notation 2.11. 2.9 still holds when 'least' and 'minimal' are replaced by 'greatest' and 'maximal', respectively.

Definition 2.29 (Lower/Upper Bound and Infimum/Supremum)**.** Let $(A, \leq)$ be an ordered set and $B \subseteq A$.

- $a \in A$ is a *lower bound* of B in the ordered set $(A, \leq)$ if $\forall x \in B$, $a \leq x$.
- $a \in A$ is called an *infimum* (or *greatest lower bound*) of B in the ordered set $(A, \leq)$ if $a = \max\{\, x \in A \mid x \text{ is a lower bound of } B \,\}$.
- $a \in A$ is an *upper bound* of B in the ordered set $(A, \leq)$ if $\forall x \in B$, $x \leq a$.
- $a \in A$ is called a *supremum* (or *least upper bound*) of B in the ordered set $(A, \leq)$ if $a = \min\{\, x \in A \mid x \text{ is an upper bound of } B \,\}$.

Notation 2.12. Let $(A, \leq)$ be an ordered set and $B \subseteq A$.

- The infimum of B is denoted $\inf B$.
- The supremum of B is denoted $\sup B$.

Theorem 2.10 (Basic Properties of Infimum and Supremum)**.** Let $(A, \leq)$ be an ordered set and $B \subseteq A$.

(i) B has at most one infimum.
(ii) If b is the least element of B, then b is the infimum of B.
(iii) If $b \in B$ is the infimum of B, then b is the least element of B.

Proof. (i) The result follows from the definition and 2.9 (i).
(ii) b is a lower bound of B. If x is a lower bound of B, since $b \in B$, we must have $x \leq b$. Therefore, b is the greatest lower bound.
(iii) $b \in B$ is a lower bound of B, and thus b is the least element.

■

Notation 2.13. 2.10 still holds when 'least' and 'infimum' are replaced by 'greatest' and 'supremum', respectively.

Definition 2.30 (Isomorphism Between Ordered Sets)**.** An *isomorphism* between two ordered sets $(P, \leq)$ and $(Q, \preceq)$ is a function $f: P \iff Q$ such that

$$\forall p_1, p_2 \in P, (p_1 \leq p_2 \iff f(p_1) \preceq f(p_2)).$$

If an isomorphism exists between $(P, \leq)$ and $(Q, \preceq)$, then we say $(P, \leq)$ and $(Q, \preceq)$ are *isomorphic*.

Lemma 2.7 (One Implication Is Enough)**.** Let $(P, \leq)$ be a totally ordered set and let $(Q, \preceq)$ be an ordered set. Let $h: P \iff Q$ be a function such that

$$\forall p_1, p_2 \in P, (p_1 \leq p_2 \implies h(p_1) \preceq h(p_2)).$$

Then, h is an isomorphism between $(P, \leq)$ and $(Q, \preceq)$, and $(Q, \preceq)$ is totally ordered.

Proof. Take any $p_1, p_2 \in P$ and assume $h(p_1) \preceq h(p_2)$. Suppose $p_2 < p_1$ for the sake of contradiction. Since h is injective, $h(p_1) \neq h(p_2)$, and thus $h(p_1) \prec h(p_2)$. Then, we have $\neg(p_2 \leq p_1)$, which is a contradiction. Hence, $\neg(p_2 < p_1)$. Therefore, $p_1 \leq p_2$ since $(P, \leq)$ is totally ordered.

Now, take any $q_1, q_2 \in Q$. Since h is onto Q, there exist $p_1, p_2 \in P$ such that $q_1 = h(p_1)$ and $q_2 = h(p_2)$. Since P is totally ordered, it is $p_1 \leq p_2$ or $p_2 \leq p_1$. In either case, we have $q_1 \preceq q_2$ or $q_2 \preceq q_1$. Therefore, $(Q, \preceq)$ is totally ordered. ■

Proposition 2.4.

(i) Let R be a partial ordering of A and let S be the strict ordering of A corresponding to R. Let R^* be the partial ordering of A corresponding to S. Show that $R^* = R$.
(ii) Let S be a strict ordering of A and let R be the partial ordering of A corresponding to S. Let S^* be the partial ordering of A corresponding to R. Show that $S^* = S$.

Proof.

(i) $R^* = S \cup \mathrm{Id}_A = (R - \mathrm{Id}_A) \cup \mathrm{Id}_A = R$ since $\mathrm{Id}_A \subseteq R$.
(ii) $S^* = R - \mathrm{Id}_A = (S \cup \mathrm{Id}_A) - \mathrm{Id}_A = S$ since $\mathrm{Id}_A \cap S = \emptyset$.

■

Theorem 2.11. Let $(A_1, <_1)$ and $(A_2, <_2)$ be strictly ordered sets and let $A_1 \cap A_2 = \emptyset$. Define a relation $\prec$ on $B \triangleq A_1 \cup A_2$ as follows:

$$x \prec y \iff (x <_1 y) \vee (x <_2 y) \vee (x \in A_1 \wedge y \in A_2).$$

Show that $\prec$ is a strict ordering of B and $\prec \cap A_1^2 = <_1$, $\prec \cap A_2^2 = <_2$.

Proof. Note that $\prec = <_1 \cup <_2 \cup A_1 \times A_2$.

Suppose $x \prec y$ and $y \prec x$. By definition, $x, y \in A_1$ or $x, y \in A_2$. In both cases, we have ($x <_1 y$ and $y <_1 x$) or ($x <_2 y$ and $y <_2 x$), which are impossible as $<_1$ and $<_2$ are asymmetric. Hence, $\prec$ is asymmetric. Transitivity of $\prec$ can be shown easily.

Since $<_1 \cap A_2^2 = <_2 \cap A_1^2 = (A_1 \times A_2) \cap A_1^2 = (A_1 \times A_2) \cap A_2^2 = \emptyset$, we get $\prec \cap A_1^2 = <_1$ and $\prec \cap A_2^2 = <_2$. ■

Proposition 2.5. Let R be a reflexive and transitive relation in A (R is called a *preordering* of A). Define a relation E in A by

$$aEb \iff aRb \wedge bRa.$$

Show that E is an equivalence on A. Define the relation R/E in A/E by

$$[a]_E R/E [b]_E \iff aRb.$$

Show that R/E is well-defined and that R/E is a partial ordering of A/E.

Proof. Since $aEa \equiv aRa$ and R is reflexive, E is reflexive as well. Since $aEb \equiv bEa$, E is symmetric. Since $aEb \wedge bEc \iff (aRb \wedge bRc) \wedge (cRb \wedge bRa) \implies aRc \wedge cRa \iff aEc$, E is transitive. ✓

Assume $[a]_E = [a']_E$ and $[b]_E = [b']_E$. Then, we have aEa' and bEb' by Lemma 2.6, i.e., aRa', $a'Ra$, bRb', and $b'Rb$. By transitivity of R, it follows that $aRb \iff a'Rb'$. Therefore, R/E is well-defined. ✓

It can be shown readily that R/E is reflexive and transitive. To prove R/E is antisymmetric, assume $[a]_E R/E [b]_E$ and $[b]_E R/E [a]_E$. Then, aRb and bRa, which means aEb. Therefore, $[a]_E = [b]_E$ by Lemma 2.6. ✓ ■

3 Introduction to Natural Numbers

Notation 3.1. We cannot prove the existence of an "infinite" set in the classical sense or discuss infinity solely from the axioms introduced earlier. Therefore, we introduce additional concepts to construct the set of natural numbers.

Definition 3.1 (Successor)**.** The *successor* of a set x is defined as:

$$S(x) = x \cup \{x\}.$$

Notation 3.2. We denote the successor $S(n)$ of a natural number n as $n+1$. This notation does not imply the classical addition operation.

Notation 3.3 (Natural Numbers)**.** Natural numbers can be defined as:

- $0 = \emptyset$
- $1 = \{\emptyset\} = S(0) = 0 + 1$
- $2 = \{\emptyset, \{\emptyset\}\} = S(1) = 1 + 1$
- $\cdots$

Definition 3.2 (Inductive Set)**.** A set I is called *inductive* if:

$$0 \in I \quad \text{and} \quad \forall n \in I,\ n+1 \in I.$$

Definition 3.3 (Axiom of Infinity)**.** An inductive set exists.

Definition 3.4 (Set of All Natural Numbers)**.** The *set of all natural numbers* is defined as:

$$\mathbb{N} = \{x \mid x \in I \text{ for all inductive sets } I\}.$$

Notation 3.4. The existence of $\mathbb{N}$ is guaranteed by the Axiom of Infinity. If A is any inductive set, then:

$$\mathbb{N} = \{x \in A \mid x \in I \text{ for all inductive sets } I\}.$$

Lemma 3.1. The set $\mathbb{N}$ is inductive. Moreover, if I is an inductive set, then $\mathbb{N} \subseteq I$.

Proof. Since $0 \in I$ for all inductive sets I, it follows that $0 \in \mathbb{N}$. If $n \in \mathbb{N}$, then $n \in I$ for all inductive sets I, so $n+1 \in I$ for all I. Therefore, $n+1 \in \mathbb{N}$, showing that $\mathbb{N}$ is inductive. The inclusion $\mathbb{N} \subseteq I$ follows directly from the definition of $\mathbb{N}$. ■

Definition 3.5. Define the relation $<$ on $\mathbb{N}$ by:

$$m < n \quad \text{if and only if} \quad m \in n.$$

Notation 3.5. Although we have not yet proven that $<$ is a strict ordering on $\mathbb{N}$, we use $\leq$ to denote the relation:

$$\leq = < \cup \mathrm{Id}_{\mathbb{N}},$$

where $\mathrm{Id}_{\mathbb{N}}$ is the identity relation on $\mathbb{N}$.

3.1 Properties of Natural Numbers

Theorem 3.1 (Principle of Mathematical Induction)**.** Let $\mathbf{P}(n)$ be a property defined on $\mathbb{N}$. If:

$$\mathbf{P}(0) \quad \text{and} \quad \forall n \in \mathbb{N},\ \mathbf{P}(n) \implies \mathbf{P}(n+1),$$

then:

$$\forall n \in \mathbb{N},\ \mathbf{P}(n).$$

Proof. Let $A = \{n \in \mathbb{N} \mid \mathbf{P}(n)\}$. The premise states that A is inductive. Therefore, $\mathbb{N} \subseteq A$, which implies $\mathbf{P}(n)$ holds for all $n \in \mathbb{N}$. ■

Lemma 3.2.

(i) For all $n \in \mathbb{N}$, $0 \leq n$.

(ii) For all $k, n \in \mathbb{N}$, $k < n+1$ if and only if $k < n$ or $k = n$.

Proof. (i) We prove that $0 \leq n$ for all $n \in \mathbb{N}$ by induction. For $n = 0$, $0 = 0$, so $0 \leq 0$. Assume $0 \leq n$, then by the definition of successor, $n \leq n+1$. Therefore, $0 \leq n+1$.

(ii) From the definition of $n+1 = n \cup \{n\}$, we have $k \in n+1$ if and only if $k \in n$ or $k = n$. Thus, $k < n+1$ if and only if $k < n$ or $k = n$.

■

Theorem 3.2. The set $\mathbb{N}$ with the relation $\leq$ is totally ordered.

Proof. We need to show that $\leq$ is a total order on $\mathbb{N}$. First, we establish that $<$ is transitive and asymmetric.

Transitivity of $<$: Assume $k < m$ and $m < n$. By definition, $k \in m$ and $m \in n$. Since sets are transitive, $k \in n$, so $k < n$.

Asymmetry of $<$: For any $n \in \mathbb{N}$, $n \notin n$ because a set is not an element of itself. Therefore, $n < n$ is false.

Totality of $\leq$: For any $m, n \in \mathbb{N}$, either $m = n$, $m < n$, or $n < m$. This can be shown using induction on n.

Thus, $(\mathbb{N}, \leq)$ is a totally ordered set. ■

Theorem 3.3 (Strong Induction Principle)**.** Let $\mathbf{P}(n)$ be a property defined on $\mathbb{N}$. If for all $n \in \mathbb{N}$:

$$(\forall k < n,\ \mathbf{P}(k)) \implies \mathbf{P}(n),$$

then:

$$\forall n \in \mathbb{N},\ \mathbf{P}(n).$$

Proof. Assume the premise holds. Let $A = \{n \in \mathbb{N} \mid \forall k < n,\ \mathbf{P}(k)\}$. By induction, $A = \mathbb{N}$. Therefore, $\mathbf{P}(n)$ holds for all $n \in \mathbb{N}$. ■

Definition 3.6 (Well-Ordering)**.** A total order $\preceq$ on a set A is a *well-ordering* if every nonempty subset of A has a least element. The set A with the order $\preceq$ is called a *well-ordered set*.

Theorem 3.4. The set $\mathbb{N}$ with the relation $\leq$ is well-ordered.

Proof. Let $X \subseteq \mathbb{N}$ be a nonempty subset. We need to show that X has a least element. Suppose X has no least element. Then, for every $n \in \mathbb{N}$, there exists $m < n$ such that $m \in X$. By induction, this leads to a contradiction. Therefore, X must have a least element. ■

Theorem 3.5 (Strictly Increasing Functions)**.** For all $m, n \in \mathbb{N}$, if $m < n$, then $m+1 < n+1$.

Hence, the function $S: \mathbb{N} \to \mathbb{N}$ defined by $S(n) = n+1$ is one-to-one.

Proof. By Lemma 3.2, we have $m+1 \leq n$. Together with $n < n+1$, it follows that $m+1 < n+1$.

Now, take any $m,n \in \mathbb{N}$ with $m \neq n$. Then, by , we have $m < n$ or $n < m$. In both cases, $S(m) < S(n)$ or $S(n) < S(m)$, which implies $S(m) \neq S(n)$.

Therefore, S is one-to-one. ■

Theorem 3.6 (Injection into Proper Subsets)**.** There exists a proper subset $X \subsetneq \mathbb{N}$ and an injective function $f: \mathbb{N} \to X$.

Proof. Let $S: \mathbb{N} \to \mathbb{N}$ be defined by $S(n) = n+1$. By Theorem 3.5, S is injective.

Since there exists no $n \in \mathbb{N}$ such that $n \cup \{n\} = \emptyset$, we have $0 \notin ran(S)$, implying $ran(S) \subsetneq \mathbb{N}$.

Therefore, $S: \mathbb{N} \to \text{ran}(S)$ is the injective function we are looking for. ■

Theorem 3.7 (Unique Successor for Natural Numbers)**.** For all $n \in \mathbb{N} - \{0\}$, there exists a unique $k \in \mathbb{N}$ such that $n = k+1$.

Proof. Let $\mathbf{P}(x)$ be the property "$x = 0 \vee \exists! k \in \mathbb{N},\ x = k+1$."

Base Case: $\mathbf{P}(0)$ holds by definition.

Inductive Step: Assume $\mathbf{P}(n)$ holds for some $n \in \mathbb{N}$. We need to show that $\mathbf{P}(n+1)$ holds.

Suppose $n+1 = k+1$. By Theorem 3.5 and , we must have $k = n$. Thus, the predecessor k is unique.

Therefore, $\mathbf{P}(n+1)$ holds.

By the principle of mathematical induction (Principle of Mathematical Induction), $\forall n \in \mathbb{N},\ \mathbf{P}(n)$ holds. ■

Theorem 3.8 (Has Upper Bound Then Maximum Exists)**.** Let $\emptyset \subsetneq X \subseteq \mathbb{N}$. If X has an upper bound in the ordering $\leq$, then X has a greatest element.

Proof. Let

$$Y \triangleq \{\, k \in \mathbb{N} \mid k \text{ is an upper bound of } X \,\}.$$

The assumption states that $Y \neq \emptyset$.

By Theorem 3.4, which asserts that every non-empty subset of $\mathbb{N}$ has a least element, we have

$$n \triangleq \min Y = \sup X$$

exists.

Suppose, for the sake of contradiction, that $n \notin X$. Then, for all $m \in X$, $m < n$. This implies that $n \neq 0$ since $X \neq \emptyset$.

Therefore, n can be expressed as $n = k+1$ for some $k \in \mathbb{N}$ by Theorem 3.7, which states that every non-zero natural number has a unique predecessor.

Consequently, for all $m \in X$,

$$m \leq k$$

by 4.2, which typically refers to a previously established property about the ordering of natural numbers.

This implies that k is also an upper bound of X. However, $k < n$, contradicting the fact that $n = \sup X$ is the least upper bound.

Therefore, our assumption that $n \notin X$ is false. Hence, $n \in X$.

Since n is the least upper bound and $n \in X$, it follows that n is the greatest element of X by Theorem 2.10, which likely states that the least upper bound belongs to the set if it exists.

Thus, X has a greatest element. ■

Theorem 3.9 (Representation of Natural Numbers as Sets)**.** For all $n \in \mathbb{N}$, $n = \{ m \in \mathbb{N} \mid m < n \}$.

Proof. Let $\mathbf{P}(x)$ be the property "$x = \{ m \in \mathbb{N} \mid m < x \}$."

Base Case: $\mathbf{P}(0)$ holds since there exists no $m \in \mathbb{N}$ with $m < 0$, so $\{ m \in \mathbb{N} \mid m < 0 \} = \emptyset$, and $0 = \emptyset$.

Inductive Step: Assume $\mathbf{P}(n)$ holds for some $n \in \mathbb{N}$. We need to show that $\mathbf{P}(n+1)$ holds.

Then,

$$n+1 = \{ m \in \mathbb{N} \mid m < n \} \cup \{n\} = \{ m \in \mathbb{N} \mid m < n+1 \}.$$

By Theorem 3.5 and , $m < n+1$ if and only if $m < n$ or $m = n$.

Therefore, $n+1 = \{ m \in \mathbb{N} \mid m < n+1 \}$, and $\mathbf{P}(n+1)$ holds.

By the principle of mathematical induction (Principle of Mathematical Induction), $\forall n \in \mathbb{N},\ \mathbf{P}(n)$ holds. ■

Theorem 3.10 (No Strictly Decreasing Function on Natural Numbers)**.** There is no function $f : \mathbb{N} \to \mathbb{N}$ such that

$$\forall n \in \mathbb{N},\ f(n+1) < f(n).$$

Proof. Let $\mathbf{P}(x)$ be the property "There is no function $f : \mathbb{N} \to \mathbb{N}$ such that $f(0) = x$ and $\forall n \in \mathbb{N},\ f(n+1) < f(n)$."

We will prove $\forall x \in \mathbb{N},\ \mathbf{P}(x)$ by induction.

Base Case: Consider $x = 0$. Suppose, for contradiction, that there exists a function $f : \mathbb{N} \to \mathbb{N}$ such that $f(0) = 0$ and $\forall n \in \mathbb{N},\ f(n+1) < f(n)$.

Then, $f(1) < f(0) = 0$. However, since $f(1) \in \mathbb{N}$, this implies $f(1)$ is a negative integer, which contradicts $f : \mathbb{N} \to \mathbb{N}$.

Inductive Step: Assume $\mathbf{P}(k)$ holds for all $k < n$, where $n \in \mathbb{N}$. Suppose, for contradiction, that there exists a function $f : \mathbb{N} \to \mathbb{N}$ such that $f(n) = k$ for some k and $f(n+1) < f(n)$.

Define $g : \mathbb{N} \to \mathbb{N}$ by $g(m) = f(m+1)$. Then, $g : \mathbb{N} \to \mathbb{N}$ satisfies $g(m) < g(m-1)$ for all $m > 0$.

However, by the inductive hypothesis, such a function g cannot exist, leading to a contradiction.

Therefore, $\mathbf{P}(n)$ holds.

By the principle of strong induction (Strong Induction Principle), $\forall x \in \mathbb{N},\ \mathbf{P}(x)$ holds. ■

Theorem 3.11 (Finite Induction Principle)**.** Let $\mathbf{P}(x)$ be a property and let $k \in \mathbb{N}$. If

$$\mathbf{P}(k) \wedge \forall n \geq k,\ [\mathbf{P}(n) \implies \mathbf{P}(n+1)]$$

then

$$\forall n \geq k,\ \mathbf{P}(n).$$

Proof. Let $\mathbf{Q}(x)$ be the property "$x < k \vee \mathbf{P}(x)$."

Base Case: $\mathbf{Q}(0)$ holds since $\mathbf{P}(0)$ is assumed to hold if $0 \geq k$ or trivially holds otherwise.

Inductive Step: Assume $\mathbf{Q}(n)$ holds for some $n \in \mathbb{N}$. We need to show that $\mathbf{Q}(n+1)$ holds.

By the Well-Ordering Principle (theorem 3.2), we have three cases:

(i) $n+1 < k$: Then, $\mathbf{Q}(n+1)$ holds because $n+1 < k$.

(ii) $n+1 = k$: If $k \geq k$, then $\mathbf{P}(k)$ holds by assumption, so $\mathbf{Q}(n+1)$ holds.

(iii) $n+1 > k$: Then, since $n \geq k$, $\mathbf{P}(n)$ holds by assumption. Hence, $\mathbf{P}(n+1)$ holds by the inductive hypothesis.

Therefore, $\mathbf{Q}(n+1)$ holds.

By the principle of mathematical induction, $\forall n \in \mathbb{N},\ \mathbf{Q}(n)$ holds. Thus, $\forall n \geq k,\ \mathbf{P}(n)$ holds. ■

Theorem 3.12 (Finite Induction Principle Extended)**.** Let $\mathbf{P}(x)$ be a property and let $k \in \mathbb{N}$. If

$$\mathbf{P}(0) \wedge \forall n < k,\ [\mathbf{P}(n) \implies \mathbf{P}(n+1)]$$

then

$$\forall n \leq k,\ \mathbf{P}(n).$$

Proof. Let $\mathbf{Q}(x)$ be the property "$x > k \vee \mathbf{P}(x)$."

Base Case: $\mathbf{Q}(0)$ holds since $\mathbf{P}(0)$ is given.

Inductive Step: Assume $\mathbf{Q}(n)$ holds for some $n \in \mathbb{N}$. We need to show that $\mathbf{Q}(n+1)$ holds.

By the Well-Ordering Principle theorem 3.2, we have two cases:

(i) $n+1 > k$: Then, $\mathbf{Q}(n+1)$ holds because $n+1 > k$.

(ii) $n+1 \leq k$: Since $n < k$, by the hypothesis $\mathbf{P}(n)$ holds. Therefore, $\mathbf{P}(n+1)$ holds, and hence $\mathbf{Q}(n+1)$ holds.

Therefore, $\mathbf{Q}(n+1)$ holds.

By the principle of mathematical induction, $\forall n \in \mathbb{N},\ \mathbf{Q}(n)$ holds. Thus, $\forall n \leq k,\ \mathbf{P}(n)$ holds. ■

Theorem 3.13 (Double Induction Principle)**.** Let $\mathbf{P}(x,y)$ be a property. If

$$\forall m,n \in \mathbb{N},\ [\forall k,\ell \in \mathbb{N},\ (k < m \vee (k = m \wedge \ell < n)) \implies \mathbf{P}(k,\ell)] \implies \mathbf{P}(m,n),$$

then

$$\forall m,n \in \mathbb{N},\ \mathbf{P}(m,n).$$

Proof. Let $\mathbf{Q}(x)$ be the property "$\forall n \in \mathbb{N},\ \mathbf{P}(x,n)$."

Base Case: Consider $x = 0$. For any $n \in \mathbb{N}$, the condition $k < 0$ is false, so the implication reduces to $\mathbf{P}(0,n)$. Therefore, $\mathbf{Q}(0)$ holds if $\mathbf{P}(0,n)$ holds for all n.

Inductive Step: Assume $\mathbf{Q}(m)$ holds for all $m < x$ for some $x \in \mathbb{N}$. We need to show that $\mathbf{Q}(x)$ holds.

Take any $n \in \mathbb{N}$. To show $\mathbf{P}(x,n)$, consider all $k, \ell \in \mathbb{N}$ such that $k < x$ or $(k = x \wedge \ell < n)$. By the inductive hypothesis, $\mathbf{P}(k,\ell)$ holds for all such k, ℓ.

Therefore, by the hypothesis of the theorem, $\mathbf{P}(x,n)$ holds.

Since n was arbitrary, $\mathbf{Q}(x)$ holds.

By the principle of mathematical induction, $\forall x \in \mathbb{N},\ \mathbf{Q}(x)$ holds. Thus, $\forall m,n \in \mathbb{N},\ \mathbf{P}(m,n)$ holds. ■

3.2 Sequences and the Recursion Theorem

Definition 3.7 (Sequence)**.**

- A *sequence* is a function whose domain is either a natural number $n \in \mathbb{N}$ or $\mathbb{N}$ itself.
- A sequence with domain n is called a *finite sequence of length n* and is denoted:

  $$\langle a_0, a_1, \ldots, a_{n-1} \rangle.$$

  The set of all finite sequences of elements from a set A is:

  $$\mathrm{Seq}(A) = \bigcup_{n \in \mathbb{N}} A^n.$$

- A sequence with domain $\mathbb{N}$ is called an *infinite sequence* and is denoted:

  $$\langle a_n \mid n \in \mathbb{N} \rangle.$$

  The set of all infinite sequences of elements from A is $A^{\mathbb{N}}$.

Theorem 3.14 (Recursion Theorem)**.** Let A be a set, $a \in A$, and $g{:}A \times \mathbb{N} \to A$ be a function. Then there exists a unique function $f{:}\mathbb{N} \to A$ such that:

(i) $f(0) = a$,

(ii) $f(n+1) = g(f(n),n)$ for all $n \in \mathbb{N}$.

Proof. We construct f using induction. Define $f(0) = a$. Assume $f(n)$ is defined. Then set $f(n+1) = g(f(n),n)$. By induction, f is defined on all of $\mathbb{N}$. Uniqueness follows because any function satisfying the conditions must agree with this construction. ■

Theorem 3.15. Let $(A, \preceq)$ be a nonempty linearly ordered set satisfying:

(i) For every $p \in A$, there exists $q \in A$ such that $p \prec q$.

(ii) Every nonempty subset of A has a least element.

(iii) Every nonempty subset of A that has an upper bound has a greatest element.

Then $(A, \preceq)$ is order-isomorphic to $(\mathbb{N}, \leq)$.

Proof. Using the recursion theorem, construct a function $f: \mathbb{N} \to A$ such that:

- $f(0) = \min A$,
- $f(n+1) = \min\{a \in A \mid f(n) \prec a\}$.

This function f is injective and order-preserving. By properties (i)–(iii), f is surjective. Therefore, f is an order isomorphism between $\mathbb{N}$ and A. ■

Theorem 3.16 (General Recursion Theorem)**.** Let S be a set and $g: \text{Seq}(S) \to S$ be a function. Then there exists a unique function $f: \mathbb{N} \to S$ such that:

$$f(n) = g(\langle f(0), f(1), \ldots, f(n-1)\rangle) \quad \text{for all } n \in \mathbb{N}.$$

Proof. We construct f recursively. Define $f(0) = g(\langle\rangle)$, where $\langle\rangle$ is the empty sequence. Assume $f(k)$ is defined for $k < n$. Then set:

$$f(n) = g(\langle f(0), f(1), \ldots, f(n-1)\rangle).$$

By induction, f is defined on all of $\mathbb{N}$. Uniqueness follows from the construction. ■

Theorem 3.17 (Parametric Recursion Theorem)**.** Let P and A be sets, $a: P \to A$, and $g: P \times A \times \mathbb{N} \to A$ be functions. Then there exists a unique function $f: P \times \mathbb{N} \to A$ such that:

(i) $f(p,0) = a(p)$ for all $p \in P$,

(ii) $f(p,n+1) = g(p, f(p,n), n)$ for all $p \in P$ and $n \in \mathbb{N}$.

Proof. For each $p \in P$, define $f_p: \mathbb{N} \to A$ recursively by $f_p(0) = a(p)$ and $f_p(n+1) = g(p, f_p(n), n)$. Then define $f(p,n) = f_p(n)$. Uniqueness follows from the uniqueness in the recursion for each p. ■

Notation 3.6. In discussions involving natural numbers, we may write expressions like $\forall k < n,\ \mathbf{P}(k)$ to mean $\forall k \in \mathbb{N},\ k < n \implies \mathbf{P}(k)$. Similar shorthand applies for other relations such as $\leq, >, \geq$.

Theorem 3.18 (Monotonicity of Sequences in Ordered Sets)**.** Let $f: \mathbb{N} \to A$ be an infinite sequence where $(A, \preceq)$ is an ordered set. Then,

$$\forall n \in \mathbb{N},\ f_n \prec f_{n+1} \implies \forall m, n \in \mathbb{N},\ (n < m \implies f_n \prec f_m).$$

Proof. Fix any $n \in \mathbb{N}$ and let $\mathbf{P}(x)$ be the property "$f_n \prec f_x$."

Base Case: $\mathbf{P}(n+1)$ holds by assumption, since $f_n \prec f_{n+1}$.

Inductive Step: Suppose $\mathbf{P}(k)$ holds for some $k \in \mathbb{N}$. That is, $f_n \prec f_k$. Given that $f_k \prec f_{k+1}$, by the transitivity of $\preceq$, it follows that $f_n \prec f_{k+1}$, which means $\mathbf{P}(k+1)$ holds.

By the principle of mathematical induction (Theorem 3.11), we conclude that $\forall m \geq n+1,\ f_n \prec f_m$. Therefore, $\forall m, n \in \mathbb{N},\ (n < m \implies f_n \prec f_m)$. ■

Theorem 3.19 (Isomorphism to Natural Numbers)**.** Let $(A, \preceq)$ be a nonempty linearly ordered set. We define $q \in A$ to be a *successor* of $p \in A$ if there is no $r \in A$ such that $p \prec r \prec q$. Assume that $(A, \preceq)$ satisfies the following properties:

(i) Every $p \in A$ has a successor.

(ii) Every nonempty subset of A has a $\preceq$-least element.

(iii) If $p \in A$ is not the $\preceq$-least element of A, then p is a successor of some $q \in A$.

Then, $(A, \preceq)$ is isomorphic to $(\mathbb{N}, \leq)$.

Proof. By property (i), for each $p \in A$, the set $\{q \in A \mid p \prec q\}$ is nonempty and has a $\preceq$-least element by property (ii). Therefore, by the Recursion Theorem (Theorem 3.20), there exists a sequence $f : \mathbb{N} \to A$ such that:

$$f_0 = \min A \quad \text{and} \quad \forall n \in \mathbb{N},\ f_{n+1} = \min\{q \in A \mid f_n \prec q\}.$$

Claim 3.1. $ran(f) = A$.

Proof of Claim 3.1. Suppose, for contradiction, that $X = A - ran(f) \neq \emptyset$. By property (ii), X has a $\preceq$-least element, say $p = \min X$. Since p is not the least element of A (because $f_0 = \min A$ is in $ran(f)$), by property (iii), p must be a successor of some $q \in A$. However, $q \prec p$ implies $q \in ran(f)$, say $q = f_m$ for some $m \in \mathbb{N}$. Then, by the construction of f, $p = f_{m+1}$, which contradicts $p \notin ran(f)$. Therefore, $X = \emptyset$, and $ran(f) = A$. ■

Since $f_n \prec f_{n+1}$ for all $n \in \mathbb{N}$, by Theorem 3.18, it follows that $\forall m, n \in \mathbb{N},\ (m < n \implies f_m \prec f_n)$. This implies that f is injective.

Therefore, together with Claim 3.1, f is a bijection between $(\mathbb{N}, \leq)$ and $(A, \preceq)$. Moreover, f preserves the order, making it an isomorphism between the two ordered sets by Lemma 2.7. ■

Theorem 3.20 (The Recursion Theorem: Partial Version)**.** Let g be a function such that $dom(g) \subseteq A \times \mathbb{N}$ and $ran(g) \subseteq A$. Let $a \in A$. Then, there uniquely exists a sequence f of elements of A such that

(i) $f_0 = a$.

(ii) $\forall n \in \mathbb{N},\ [n+1 \in dom(f) \implies f_{n+1} = g(f_n, n)]$.

(iii) f is either an infinite sequence or a finite sequence of length $k+1$ where $(f_k, k) \notin dom(g)$.

Proof. Let $\overline{A} = A \cup \{\overline{a}\}$ where $\overline{a} \notin A$. (Such an $\overline{a}$ exists by Theorem 1.1 (ii).)

Define $\overline{g} : \overline{A} \times \mathbb{N} \to \overline{A}$ by

$$\overline{g}(x, n) = \begin{cases} g(x, n) & \text{if } (x, n) \in dom(g), \\ \overline{a} & \text{otherwise.} \end{cases}$$

By the Recursion Theorem (Theorem 3.14), there exists a sequence $\overline{f} : \mathbb{N} \to \overline{A}$ such that $\overline{f}_0 = a$ and $\forall n \in \mathbb{N},\ \overline{f}_{n+1} = \overline{g}(\overline{f}_n, n)$.

We consider two cases:

(a) Case 1: $\forall n \in \mathbb{N},\ \overline{f}_n \neq \overline{a}$.

Claim 3.2 (Infinite Sequence)**.** If $\forall n \in \mathbb{N},\ \overline{f}_n \neq \overline{a}$, then $\overline{f}$ is an infinite sequence of elements of A that satisfies conditions (i) and (ii).

Proof of Claim 3.2. The assumption implies that $(\overline{f}_n, n) \in dom(g)$ and $\overline{f}_{n+1} = g(\overline{f}_n, n) \in A$ for all $n \in \mathbb{N}$. Therefore, $\overline{f}$ satisfies conditions (i) and (ii). Since $\overline{f}_0 = a \in A$, $\overline{f}$ is an infinite sequence of elements of A. ■

(a) Case 2: $\exists n \in \mathbb{N},\ \overline{f}_n = \overline{a}$.

Claim 3.3 (Finite Sequence)**.** If $\exists n \in \mathbb{N},\ \overline{f}_n = \overline{a}$, then there exists $k \in \mathbb{N}$ such that $\overline{f}$ restricted to $k+1$ satisfies conditions (i), (ii), and (iii).

Proof of Claim 3.3. By the Well-Ordering Principle (theorem 3.4), let $\ell = \min\{n \in \mathbb{N} \mid \overline{f}_n = \overline{a}\}$. Since $\overline{f}_0 = a \neq \overline{a}$, $\ell \geq 1$, and thus $\ell = k+1$ for some $k \in \mathbb{N}$ by Theorem 3.7.

It follows that $\forall n \leq k,\ \overline{f}_n \in A$. Hence, $f = \overline{f} \restriction (k+1)$ is a finite sequence of length $k+1$ of elements of A.

We verify the conditions:

(i) $f_0 = \overline{f}_0 = a$.

(ii) For $n < k$, $f_{n+1} = \overline{f}_{n+1} = \overline{g}(\overline{f}_n, n) = g(f_n, n)$.

(iii) If $(f_k, k) \in dom(g)$, then $\overline{f}_{k+1} = g(f_k, k) \neq \overline{a}$, which contradicts $\overline{f}_{k+1} = \overline{a}$. Therefore, $(f_k, k) \notin dom(g)$.

■

Now, we establish uniqueness. Let f and h be two sequences of elements of A that satisfy conditions (i), (ii), and (iii). Without loss of generality, assume $dom(h) \subseteq dom(f)$.

Let $\mathbf{P}(x)$ be the property "$x \in dom(h) \wedge f_x = h_x$."

Clearly, $\mathbf{P}(0)$ holds since $f_0 = h_0 = a$.

Claim 3.4 (Inductive Property)**.** $\forall n \in \mathbb{N},\ (n+1 \in dom(f) \wedge \mathbf{P}(n) \implies \mathbf{P}(n+1))$.

Proof of Claim 3.4. Assume $n+1 \in dom(f)$ and $\mathbf{P}(n)$ holds. Then, since $(h_n, n) = (f_n, n) \in dom(g)$, we have $n+1 \in dom(h)$ and $h_{n+1} = g(h_n, n) = g(f_n, n) = f_{n+1}$. Hence, $\mathbf{P}(n+1)$ holds. ■

By Claims 3.4, if f is a finite sequence, then $h = f$ by Theorem 3.12. If f is an infinite sequence, then $h = f$ by Theorem 3.1. Therefore, the sequence f is unique. ■

Theorem 3.21 (Enumeration of Subsets of Natural Numbers)**.** Let $X \subseteq \mathbb{N}$. Then, there exists a one-to-one (finite or infinite) sequence f such that $ran(f) = X$.

Proof. If $X = \emptyset$, then the empty sequence $\langle\rangle$ satisfies $ran(f) = X$. Assume $X \neq \emptyset$.

Define the function $g: X \times \mathbb{N} \to X$ by:

$$g(x,n) = \min\{k \in X \mid x < k\},$$

whenever such a k exists. Specifically, set

$$g(x,n) = \begin{cases} \min\{k \in X \mid x < k\} & \text{if } x \text{ has an upper bound in } X, \\ \overline{a} & \text{otherwise,} \end{cases}$$

where $\overline{a} \notin X$ is an element added to X to handle undefined cases.

By the Recursion Theorem: Partial Version (Theorem 3.20), there exists a sequence f of elements of X such that:

(i) $f_0 = \min X$.

Note that $dom(g) = \{(x,n) \in X \times \mathbb{N} \mid \exists y \in X,\ x < y\}$.

Moreover, for each $n \in \mathbb{N}$ such that $n+1 \in dom(f)$, we have $f_n < f_{n+1}$. By Theorem 3.18, it follows that $\forall m,n \in \mathbb{N},\ (m < n \implies f_m < f_n)$, which means f is injective.

Suppose $Y = X - ran(f) \neq \emptyset$ for the sake of contradiction. By the Well-Ordering Principle (theorem 3.4), we may take $y = \min Y$. Then, by Theorem 3.8, we may let $z = \max\{x \in X \mid x < y\}$. Since $z \in ran(f)$, say $z = f_m$ for some $m \in \mathbb{N}$. Hence, $y = f_{m+1}$, which contradicts $y \notin ran(f)$. Therefore, $Y = \emptyset$, and $ran(f) = X$. ■

3.3 Arithmetic of Natural Numbers

Theorem 3.22. There uniquely exists a function $+: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that:

(i) For all $m \in \mathbb{N}$, $+(m,0) = m$.

(ii) For all $m,n \in \mathbb{N}$, $+(m,n+1) = S(+(m,n))$.

Proof. The result follows directly from the Parametric Recursion Theorem with $A = P = \mathbb{N}$, $a(p) = p$ for all $p \in \mathbb{N}$, and $g(p,x,n) = S(x)$ for all $p,x,n \in \mathbb{N}$. ■

Definition 3.8 (Addition)**.** The function $+$ defined in Theorem 3.22 is called *addition*.

Notation 3.7. For all $m \in \mathbb{N}$, we have $+(m,1) = +(m,0+1) = +(m,0)+1 = m+1$. Hence, we may write $m+n$ instead of $+(m,n)$ without causing any confusion regarding the notation $n+1$. We restate the defining properties of addition for future reference:

$$\forall m \in \mathbb{N}, \quad m+0 = m \tag{1}$$

$$\forall m,n \in \mathbb{N}, \quad m+(n+1) = (m+n)+1 \tag{2}$$

Theorem 3.23 (Addition is Commutative)**.** Addition is commutative; that is,

$$\forall m,n \in \mathbb{N}, \quad m+n = n+m.$$

Proof. We will prove by induction on n that $m+n=n+m$ for all $m,n\in\mathbb{N}$.

Base Case: For $n=0$, we have $m+0=m$ by (1). We need to show that $0+m=m$ for all $m\in\mathbb{N}$.

We prove $0+m=m$ by induction on m.

Base Case: $0+0=0$ by (1).

Inductive Step: Assume $0+m=m$ holds for some $m\in\mathbb{N}$. Then:

$$0+(m+1)=(0+m)+1=m+1,$$

using (2) and the induction hypothesis. Therefore, $0+m=m$ for all $m\in\mathbb{N}$.

Thus, $m+0=m=0+m$ for all $m\in\mathbb{N}$.

Inductive Step: Assume that $m+n=n+m$ holds for some $n\in\mathbb{N}$ and all $m\in\mathbb{N}$. We need to show that $m+(n+1)=(n+1)+m$ for all $m\in\mathbb{N}$.

Using (2) and the induction hypothesis:

$$\begin{aligned} m+(n+1) &= (m+n)+1 \\ &= (n+m)+1 \\ &= (n+1)+m, \end{aligned}$$

where the last equality follows from (2). Thus, $m+(n+1)=(n+1)+m$.

By induction, addition is commutative. ■

Theorem 3.24 (Addition is Associative)**.** Addition is associative; that is,

$$\forall k,m,n\in\mathbb{N},\quad (k+m)+n=k+(m+n).$$

Proof. We will prove by induction on n that $(k+m)+n=k+(m+n)$ for all $k,m,n\in\mathbb{N}$.

Base Case: For $n=0$, we have:

$$(k+m)+0=k+m=k+(m+0),$$

using (1).

Inductive Step: Assume $(k+m)+n=k+(m+n)$ holds for some $n\in\mathbb{N}$ and all $k,m\in\mathbb{N}$. We need to show that $(k+m)+(n+1)=k+(m+(n+1))$.

Using (2) and the induction hypothesis:

$$\begin{aligned} (k+m)+(n+1) &= ((k+m)+n)+1 \\ &= (k+(m+n))+1 \\ &= k+((m+n)+1) \\ &= k+(m+(n+1)). \end{aligned}$$

Therefore, the associativity of addition holds. ■

Theorem 3.25. There uniquely exists a function $\cdot:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ such that:

(i) For all $m \in \mathbb{N}$, $m \cdot 0 = 0$.

(ii) For all $m, n \in \mathbb{N}$, $m \cdot (n+1) = m \cdot n + m$.

Proof. The result follows directly from the Parametric Recursion Theorem with $A = P = \mathbb{N}$, $a(p) = 0$ for all $p \in \mathbb{N}$, and $g(p,x,n) = x + p$ for all $p, x, n \in \mathbb{N}$. ■

Definition 3.9 (Multiplication)**.** The function $\cdot$ defined in Theorem 3.25 is called *multiplication*. We restate the defining properties of multiplication:

$$\forall m \in \mathbb{N}, \quad m \cdot 0 = 0 \tag{3}$$

$$\forall m, n \in \mathbb{N}, \quad m \cdot (n+1) = m \cdot n + m \tag{4}$$

Theorem 3.26 (Multiplication is Commutative)**.** Multiplication is commutative; that is,

$$\forall m, n \in \mathbb{N}, \quad m \cdot n = n \cdot m.$$

Proof. We will prove by induction on n that $m \cdot n = n \cdot m$ for all $m, n \in \mathbb{N}$.

Base Case: For $n = 0$, we have $m \cdot 0 = 0$ by (3), and we need to show $0 \cdot m = 0$ for all $m \in \mathbb{N}$.

We prove $0 \cdot m = 0$ by induction on m.

Base Case: $0 \cdot 0 = 0$ by (3).

Inductive Step: Assume $0 \cdot m = 0$ holds for some $m \in \mathbb{N}$. Then:

$$0 \cdot (m+1) = (0 \cdot m) + 0 = 0 + 0 = 0,$$

using (4) and the induction hypothesis. Thus, $0 \cdot m = 0$ for all $m \in \mathbb{N}$.

Inductive Step: Assume $m \cdot n = n \cdot m$ holds for some $n \in \mathbb{N}$ and all $m \in \mathbb{N}$. We need to show that $m \cdot (n+1) = (n+1) \cdot m$ for all $m \in \mathbb{N}$.

Using (4) and the induction hypothesis:

$$\begin{aligned} m \cdot (n+1) &= m \cdot n + m \\ &= n \cdot m + m \\ &= (n \cdot m) + m \\ &= (n \cdot m + m \cdot 1) \\ &= m \cdot (n+1) \quad \text{(since addition is commutative).} \end{aligned}$$

Similarly:

$$\begin{aligned} (n+1) \cdot m &= n \cdot m + m \\ &= m \cdot n + m \\ &= m \cdot (n+1). \end{aligned}$$

Therefore, $m \cdot (n+1) = (n+1) \cdot m$.

By induction, multiplication is commutative. ■

Theorem 3.27 (Distributive Law)**.** Multiplication distributes over addition; that is,

$$\forall k,m,n \in \mathbb{N}, \quad k \cdot (m+n) = k \cdot m + k \cdot n,$$
$$\forall k,m,n \in \mathbb{N}, \quad (m+n) \cdot k = m \cdot k + n \cdot k.$$

Proof. We will prove the first statement by induction on n.

Base Case: For $n = 0$, we have:

$$k \cdot (m+0) = k \cdot m = k \cdot m + 0 = k \cdot m + k \cdot 0,$$

using (1) and (3).

Inductive Step: Assume $k \cdot (m+n) = k \cdot m + k \cdot n$ holds for some $n \in \mathbb{N}$ and all $k,m \in \mathbb{N}$. We need to show that $k \cdot (m+(n+1)) = k \cdot m + k \cdot (n+1)$.

Using (2) and (4):

$$\begin{aligned} k \cdot (m+(n+1)) &= k \cdot ((m+n)+1) \\ &= k \cdot (m+n) + k \\ &= (k \cdot m + k \cdot n) + k \\ &= k \cdot m + (k \cdot n + k) \\ &= k \cdot m + k \cdot (n+1). \end{aligned}$$

The second statement follows from the commutativity of multiplication:

$$(m+n) \cdot k = k \cdot (m+n) = k \cdot m + k \cdot n = m \cdot k + n \cdot k.$$

■

Theorem 3.28 (Multiplication is Associative)**.** Multiplication is associative; that is,

$$\forall k,m,n \in \mathbb{N}, \quad (k \cdot m) \cdot n = k \cdot (m \cdot n).$$

Proof. We will prove by induction on n that $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ for all $k,m,n \in \mathbb{N}$.

Base Case: For $n = 0$, we have:

$$(k \cdot m) \cdot 0 = 0 = k \cdot 0 = k \cdot (m \cdot 0),$$

using (3).

Inductive Step: Assume $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ holds for some $n \in \mathbb{N}$ and all $k,m \in \mathbb{N}$. We need to show that $(k \cdot m) \cdot (n+1) = k \cdot (m \cdot (n+1))$.

Using (4) and the induction hypothesis:

$$\begin{aligned} (k \cdot m) \cdot (n+1) &= (k \cdot m) \cdot n + k \cdot m \\ &= k \cdot (m \cdot n) + k \cdot m \\ &= k \cdot (m \cdot n + m) \\ &= k \cdot (m \cdot (n+1)). \end{aligned}$$

Therefore, multiplication is associative. ■

Lemma 3.3. For all $m \in \mathbb{N}$, $m \cdot 1 = m$.

Proof. Using (1) and (4):

$$\begin{aligned} m \cdot 1 &= m \cdot (0+1) \\ &= m \cdot 0 + m \\ &= 0 + m \\ &= m. \end{aligned}$$

■

Theorem 3.29. There uniquely exists a function $\uparrow : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that:

(i) For all $m \in \mathbb{N}$, $m \uparrow 0 = 1$.

(ii) For all $m, n \in \mathbb{N}$, $m \uparrow (n+1) = (m \uparrow n) \cdot m$.

Proof. The result follows directly from the Parametric Recursion Theorem with $A = P = \mathbb{N}$, $a(p) = 1$ for all $p \in \mathbb{N}$, and $g(p,x,n) = x \cdot p$ for all $p, x, n \in \mathbb{N}$. ■

Definition 3.10 (Exponentiation)**.** The function $\uparrow$ defined in Theorem 3.29 is called *exponentiation*. We write m^n instead of $m \uparrow n$. The defining properties are:

$$\forall m \in \mathbb{N}, \quad m^0 = 1 \tag{5}$$

$$\forall m, n \in \mathbb{N}, \quad m^{n+1} = m^n \cdot m \tag{6}$$

Theorem 3.30 (Laws of Exponents)**.** (i) For all $m \in \mathbb{N}$, $m^1 = m$.

(ii) For all $k, m, n \in \mathbb{N}$, $k^{m+n} = k^m \cdot k^n$.

(iii) For all $k, m, n \in \mathbb{N}$, $(m \cdot n)^k = m^k \cdot n^k$.

(iv) For all $k, m, n \in \mathbb{N}$, $(k^m)^n = k^{m \cdot n}$.

Proof. (i) Using (1) and (6):

$$m^1 = m^{0+1} = m^0 \cdot m = 1 \cdot m = m,$$

where we used (5) and Lemma 3.3.

(ii) We prove by induction on n that $k^{m+n} = k^m \cdot k^n$.

Base Case: For $n = 0$:

$$k^{m+0} = k^m = k^m \cdot 1 = k^m \cdot k^0,$$

using (5).

Inductive Step: Assume $k^{m+n} = k^m \cdot k^n$ holds for some $n \in \mathbb{N}$. Then:

$$\begin{aligned} k^{m+(n+1)} &= k^{(m+n)+1} \\ &= k^{m+n} \cdot k \\ &= (k^m \cdot k^n) \cdot k \\ &= k^m \cdot (k^n \cdot k) \\ &= k^m \cdot k^{n+1}. \end{aligned}$$

Thus, $k^{m+n} = k^m \cdot k^n$ for all $m, n \in \mathbb{N}$.

(iii) We prove by induction on k that $(m \cdot n)^k = m^k \cdot n^k$.

Base Case: For $k = 0$:

$$(m \cdot n)^0 = 1 = 1 \cdot 1 = m^0 \cdot n^0,$$

using (5).

Inductive Step: Assume $(m \cdot n)^k = m^k \cdot n^k$ holds for some $k \in \mathbb{N}$. Then:

$$\begin{aligned} (m \cdot n)^{k+1} &= (m \cdot n)^k \cdot (m \cdot n) \\ &= (m^k \cdot n^k) \cdot (m \cdot n) \\ &= (m^k \cdot m) \cdot (n^k \cdot n) \\ &= m^{k+1} \cdot n^{k+1}. \end{aligned}$$

(iv) We prove by induction on n that $(k^m)^n = k^{m \cdot n}$.

Base Case: For $n = 0$:

$$(k^m)^0 = 1 = k^0 = k^{m \cdot 0},$$

using (5) and (3).

Inductive Step: Assume $(k^m)^n = k^{m \cdot n}$ holds for some $n \in \mathbb{N}$. Then:

$$\begin{aligned} (k^m)^{n+1} &= (k^m)^n \cdot k^m \\ &= k^{m \cdot n} \cdot k^m \\ &= k^{m \cdot n + m} \\ &= k^{m \cdot (n+1)}. \end{aligned}$$

■

Theorem 3.31. There uniquely exists a function $\Sigma \colon \mathrm{Seq}(\mathbb{N}) \to \mathbb{N}$ such that:

(i) $\Sigma(\langle\rangle) = 0$.

(ii) For all sequences k of length $n+1$, $\Sigma(k) = \Sigma(k|_n) + k_n$.

Proof. Define $g: \text{Seq}(\mathbb{N}) \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by:

$$g(k,s,n) = \begin{cases} s + k_n & \text{if } n \in dom(k), \\ s & \text{otherwise.} \end{cases}$$

By the Parametric Recursion Theorem, there exists a function $f: \text{Seq}(\mathbb{N}) \times \mathbb{N} \to \mathbb{N}$ such that:

(i) $f(k,0) = 0$ for all $k \in \text{Seq}(\mathbb{N})$.

(ii) $f(k,n+1) = g(k, f(k,n), n)$ for all $k \in \text{Seq}(\mathbb{N})$ and $n \in \mathbb{N}$.

Define $\Sigma(k) = f(k, dom(k))$.

We can show by induction on n that $f(k,n) = \Sigma(k|_n)$, where $k|_n$ is the restriction of k to n.

Therefore, $\Sigma(k) = \Sigma(k|_n) + k_n$ for sequences k of length $n+1$.

Uniqueness follows from the construction. ■

Notation 3.8. For the function Σ defined in Theorem 3.31, we write:

$$\sum_{i=0}^{n-1} k_i$$

instead of $\Sigma(\langle k_0, k_1, \ldots, k_{n-1} \rangle)$.

3.4 Operations and Structures

Definition 3.11 (Operation)**.**

- A *unary operation* on a set S is a function from S (or a subset of S) to S, denoted $f: S \rightharpoonup S$.
- A *binary operation* on S is a function from $S \times S$ (or a subset of $S \times S$) to S, denoted $f: S^2 \rightharpoonup S$.

Notation 3.9 (Binary Operation)**.** Symbols such as $+, \times, *, \triangle$, etc., are often used to denote operations. The value of the operation $*$ at the pair (x,y) is then denoted $x * y$ instead of $*(x,y)$.

Definition 3.12 (Closedness Under Operation)**.** Let f be a binary operation on a set S and $A \subseteq S$. The set A is said to be *closed under the operation* f if:

$$\forall x, y \in A, \quad (x,y) \in \text{dom}\, f \implies f(x,y) \in A.$$

Definition 3.13 (n-Tuple)**.** Let $n \in \mathbb{N}$. An *n-tuple* is a finite sequence of length n.

Notation 3.10. Let $\langle a_0, a_1, \ldots, a_{n-1} \rangle$ and $\langle b_0, b_1, \ldots, b_{n-1} \rangle$ be two n-tuples. By the property of functions:

$$\langle a_0, a_1, \ldots, a_{n-1} \rangle = \langle b_0, b_1, \ldots, b_{n-1} \rangle \quad \iff \quad \forall i < n,\ a_i = b_i.$$

This satisfies the usual defining property of n-tuples.

Remark.

- If $\langle A_i \mid 0 \leq i < n \rangle$ is a finite sequence of sets, then the product of the indexed system $\prod_{0 \leq i < n} A_i$ is the set of all n-tuples $a = \langle a_0, a_1, \ldots, a_{n-1} \rangle$ such that $a_i \in A_i$ for all $i < n$.
- If $A_i = A$ for all $i < n$, then $\prod_{0 \leq i < n} A_i = A^n$.
- $A^0 = \{\langle\rangle\}$, the set containing only the empty sequence.

Notation 3.11. The *ordered pair* (a_0, a_1) is often defined as $\{\{a_0\}, \{a_0, a_1\}\}$. The 2-tuple $\langle a_0, a_1 \rangle$ is defined differently as the function $\{(0, a_0), (1, a_1)\}$. Consequently, $A_0 \times A_1$ does not generally equal $\prod_{0 \leq i < 2} A_i$.

However, there is a natural one-to-one correspondence:

$$\begin{aligned} \delta : A_0 \times A_1 &\longrightarrow \prod_{0 \leq i < 2} A_i \\ (a_0, a_1) &\longmapsto \langle a_0, a_1 \rangle. \end{aligned}$$

Therefore, for most practical purposes, we can use the notations $\langle a_0, a_1, \ldots, a_{n-1} \rangle$ and $(a_0, a_1, \ldots, a_{n-1})$ interchangeably.

Definition 3.14 (n-ary Relation)**.** An *n-ary relation* R in a set A is a subset of A^n. We write $R(a_0, a_1, \ldots, a_{n-1})$ instead of $\langle a_0, a_1, \ldots, a_{n-1} \rangle \in R$.

Definition 3.15 (n-ary Operation)**.** An *n-ary operation* F on a set A is a function $F : A^n \rightharpoonup A$. We write $F(a_0, a_1, \ldots, a_{n-1})$ instead of $F(\langle a_0, a_1, \ldots, a_{n-1} \rangle)$.

Remark.

- 1-ary relations in A can be considered as subsets of A.
- 1-ary operations on A are functions from A to A.
- Nonempty 0-ary operations on A can be identified with elements of A (constants). A nonempty 0-ary operation is of the form $\{(\langle\rangle, a)\}$ where $a \in A$.

Definition 3.16 (Structure)**.**

- A *type* τ is an ordered pair consisting of two finite sequences of natural numbers:

  $$\tau = (\langle r_0, r_1, \ldots, r_{m-1} \rangle, \langle f_0, f_1, \ldots, f_{n-1} \rangle).$$

- A *structure of type* τ is a tuple:

  $$\mathfrak{A} = (A, \langle R_0, R_1, \ldots, R_{m-1} \rangle, \langle F_0, F_1, \ldots, F_{n-1} \rangle),$$

  where:

  - A is a nonempty set called the *universe* of the structure.
  - For each $i < m$, R_i is an r_i-ary relation on A.
  - For each $j < n$, F_j is an f_j-ary operation on A. If $f_j = 0$, then F_j is required to be a nonempty function (a constant).

Example. The structure $\mathfrak{N} = (\mathbb{N}, \langle \leq \rangle, \langle 0, +, \cdot \rangle)$ is a structure of type $(\langle 2 \rangle, \langle 0, 2, 2 \rangle)$.

Notation 3.12. We often write the structure of type $\tau = (\langle r_0, \ldots, r_{m-1} \rangle, \langle f_0, \ldots, f_{n-1} \rangle)$ as a $(1+m+n)$-tuple, for example, $(\mathbb{N}, \leq, 0, +, \cdot)$, when it is understood which symbols represent relations and which represent operations.

Definition 3.17 (Isomorphism Between Structures)**.** Let $\mathfrak{A}$ and $\mathfrak{A}'$ be structures of the same type $\tau = (\langle r_0, \ldots, r_{m-1} \rangle, \langle f_0, \ldots, f_{n-1} \rangle)$, where:

$$\mathfrak{A} = (A, \langle R_0, \ldots, R_{m-1} \rangle, \langle F_0, \ldots, F_{n-1} \rangle),$$
$$\mathfrak{A}' = \left(A', \langle R'_0, \ldots, R'_{m-1} \rangle, \langle F'_0, \ldots, F'_{n-1} \rangle\right).$$

An *isomorphism* between $\mathfrak{A}$ and $\mathfrak{A}'$ is a bijection $h: A \to A'$ such that:

(i) For all $i < m$ and all $a \in A^{r_i}$:

$$R_i(a_0, \ldots, a_{r_i - 1}) \iff R'_i(h(a_0), \ldots, h(a_{r_i - 1})).$$

(ii) For all $j < n$ and all $a \in A^{f_j}$:

$$(a_0, \ldots, a_{f_j - 1}) \in \operatorname{dom} F_j \iff (h(a_0), \ldots, h(a_{f_j - 1})) \in \operatorname{dom} F'_j.$$

(iii) For all $j < n$ and all $a \in A^{f_j}$ with $(a_0, \ldots, a_{f_j - 1}) \in \operatorname{dom} F_j$:

$$h\left(F_j(a_0, \ldots, a_{f_j - 1})\right) = F'_j\left(h(a_0), \ldots, h(a_{f_j - 1})\right).$$

If such a mapping h exists, we say that $\mathfrak{A}$ and $\mathfrak{A}'$ are *isomorphic*, denoted $\mathfrak{A} \cong \mathfrak{A}'$.

Definition 3.18 (Automorphism)**.** An *automorphism* of a structure $\mathfrak{A}$ is an isomorphism from $\mathfrak{A}$ to itself.

Definition 3.19 (Closed Set)**.** Let $\mathfrak{A} = (A, \langle R_0, \ldots, R_{m-1} \rangle, \langle F_0, \ldots, F_{n-1} \rangle)$ be a structure. A subset $B \subseteq A$ is called *closed* if for all $j < n$ and all $a \in B^{f_j}$:

$$(a_0, \ldots, a_{f_j - 1}) \in \operatorname{dom} F_j \implies F_j(a_0, \ldots, a_{f_j - 1}) \in B.$$

Definition 3.20 (Closure)**.** Given a structure $\mathfrak{A} = (A, \langle R_0, \ldots, R_{m-1} \rangle, \langle F_0, \ldots, F_{n-1} \rangle)$ and a subset $C \subseteq A$, the *closure* of C, denoted $\operatorname{cl}(C)$, is defined as:

$$\operatorname{cl}(C) = \bigcap \{B \subseteq A \mid C \subseteq B \text{ and } B \text{ is closed}\}.$$

It is the smallest closed set containing C.

Theorem 3.32. Let $\mathfrak{A} = (A, \langle R_0, \ldots, R_{m-1} \rangle, \langle F_0, \ldots, F_{n-1} \rangle)$ be a structure and $C \subseteq A$. Define the sequence $\langle C_i \mid i \in \mathbb{N} \rangle$ recursively by:

$$C_0 = C,$$
$$C_{i+1} = C_i \cup \bigcup_{j=0}^{n-1} F_j[C_i^{f_j}], \quad \text{for all } i \in \mathbb{N}.$$

Then:

$$\operatorname{cl}(C) = \bigcup_{i=0}^{\infty} C_i.$$

Proof. Let $\tilde{C} = \bigcup_{i=0}^{\infty} C_i$.

Claim 1: $\tilde{C}$ is closed and $\mathrm{cl}(C) \subseteq \tilde{C}$.

Proof of Claim 1: Since $C_0 = C \subseteq \tilde{C}$, it suffices to show that $\tilde{C}$ is closed. Let $j < n$ and $a \in \tilde{C}^{f_j}$. For each $r < f_j$, there exists $i_r \in \mathbb{N}$ such that $a_r \in C_{i_r}$. Let $\bar{\imath} = \max\{i_r \mid r < f_j\}$. Then $a_r \in C_{\bar{\imath}}$ for all $r < f_j$. If $(a_0, \ldots, a_{f_j-1}) \in \mathrm{dom}\, F_j$, then:

$$F_j(a_0, \ldots, a_{f_j-1}) \in F_j[C_{\bar{\imath}}^{f_j}] \subseteq C_{\bar{\imath}+1} \subseteq \tilde{C}.$$

Thus, $\tilde{C}$ is closed.

Claim 2: $\tilde{C} \subseteq \mathrm{cl}(C)$.

Proof of Claim 2: Since $C_0 = C \subseteq \mathrm{cl}(C)$ and $\mathrm{cl}(C)$ is closed, it follows by induction that $C_i \subseteq \mathrm{cl}(C)$ for all $i \in \mathbb{N}$. Therefore, $\tilde{C} \subseteq \mathrm{cl}(C)$.

Combining both claims, we conclude $\mathrm{cl}(C) = \tilde{C}$. ■

Theorem 3.33 (General Induction Principle)**.** Let $\mathfrak{A} = (A, \langle R_0, \ldots, R_{m-1}\rangle, \langle F_0, \ldots, F_{n-1}\rangle)$ be a structure and $C \subseteq A$. Let $\mathbf{P}(x)$ be a property of elements in A. If:

(i) $\mathbf{P}(a)$ holds for all $a \in C$.

(ii) For all $j < n$ and all $a \in A^{f_j}$:

$$\big((a_0, \ldots, a_{f_j-1}) \in \mathrm{dom}\, F_j \text{ and } \forall i < f_j, \mathbf{P}(a_i)\big) \implies \mathbf{P}\left(F_j(a_0, \ldots, a_{f_j-1})\right).$$

Then $\mathbf{P}(x)$ holds for all $x \in \mathrm{cl}(C)$.

Proof. Let $B = \{x \in A \mid \mathbf{P}(x) \text{ holds}\}$. By assumption, $C \subseteq B$ and B is closed under the operations F_j. Therefore, $\mathrm{cl}(C) \subseteq B$. ■

Remark. The standard *Principle of Mathematical Induction* is a special case of the General Induction Principle applied to the structure $(\mathbb{N}, S)$, where $S(n) = n+1$ is the successor function.

4 Cardinality of Sets

Definition 4.1 (Equipotent Sets)**.** Let A and B be sets. A is *equipotent to* B if there exists a bijective function $f : A \twoheadrightarrow B$. We denote this by $|A| = |B|$.

Lemma 4.1 (Basic Properties of Equipotency)**.** Let A, B, and C be sets. The following properties hold:

(i) $|A| = |A|$.

(ii) If $|A| = |B|$, then $|B| = |A|$.

(iii) If $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$.

Proof.

(i) The identity function $\mathrm{Id}_A : A \hookrightarrow\!\!\!\!\rightarrow A$ is bijective.

(ii) If $|A| = |B|$, there exists a bijection $f : A \hookrightarrow\!\!\!\!\rightarrow B$. The inverse function $f^{-1} : B \hookrightarrow\!\!\!\!\rightarrow A$ is also bijective, hence $|B| = |A|$.

(iii) If $|A| = |B|$ via a bijection $f : A \hookrightarrow\!\!\!\!\rightarrow B$ and $|B| = |C|$ via a bijection $g : B \hookrightarrow\!\!\!\!\rightarrow C$, then the composition $g \circ f : A \hookrightarrow\!\!\!\!\rightarrow C$ is bijective, implying $|A| = |C|$.

■

Remark. Lemma 4.1 establishes that equipotency is an equivalence relation on the class of all sets.

Definition 4.2 (Cardinality Relations)**.**

- We say *the cardinality of A is less than or equal to the cardinality of B*, denoted $|A| \leq |B|$, if there exists an injective function $f : A \hookrightarrow B$.
- We say *the cardinality of A is less than the cardinality of B*, denoted $|A| < |B|$, if $|A| \leq |B|$ and $|A| \neq |B|$.

Lemma 4.2 (Basic Properties of Cardinal Inequality)**.** Let A, B, and C be sets. Then:

(i) If $|A| = |B|$, then $|A| \leq |B|$.

(ii) $|A| \leq |A|$.

(iii) If $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$.

Proof. (i) If $|A| = |B|$, there exists a bijection $f : A \hookrightarrow B$. Since bijections are injective, $|A| \leq |B|$.

(ii) The identity function $\mathrm{Id}_A : A \hookrightarrow A$ is injective, hence $|A| \leq |A|$.

(iii) If $|A| \leq |B|$ via an injective function $f : A \hookrightarrow B$ and $|B| \leq |C|$ via an injective function $g : B \hookrightarrow C$, then the composition $g \circ f : A \hookrightarrow C$ is injective, implying $|A| \leq |C|$.

■

Lemma 4.3 (Cantor-Bernstein Lemma)**.** If $A_1 \subseteq B \subseteq A$ and $|A_1| = |A|$, then $|B| = |A|$.

Remark. We provide two proofs for Lemma 4.3. The second proof is more fundamental as it does not rely on the Axiom of Infinity.

Proof 1. Let $f : A \hookrightarrow\!\!\!\!\rightarrow A_1$ be a bijection.

Define sequences $\langle A_i \rangle_{i \in \mathbb{N}}$ and $\langle B_i \rangle_{i \in \mathbb{N}}$ recursively by:

$$\begin{aligned} A_0 &= A, & B_0 &= B, \\ A_{n+1} &= f[A_n], & B_{n+1} &= f[B_n], \quad \forall n \in \mathbb{N}. \end{aligned}$$

By induction, it can be shown that $A_{n+1} \subseteq B_n \subseteq A_n$ for all $n \in \mathbb{N}$.

Let $C_n = A_n - B_n$ for each $n \in \mathbb{N}$. Then, $C_{n+1} = f[C_n]$.

Define:

$$C = \bigcup_{n=0}^{\infty} C_n \quad \text{and} \quad D = A - C.$$

Thus, $f[C] \subseteq C$, and we can define a function $g: A \to A$ by:

$$g(x) = \begin{cases} f(x) & \text{if } x \in C, \\ x & \text{if } x \in D. \end{cases}$$

This function g is injective because f is injective on C and acts as the identity on D, with $f[C]$ and D being disjoint.

Since $C_n \subseteq B_0 = B$ for all n, we have $f[C] \subseteq B$. Also, $D = A - C = A - ((A - B) \cup f[C]) \subseteq B$.

To show that g maps onto B, take any $y \in B$:

- If $y \in D$, then $g(y) = y$.
- If $y \in C$, since $y \notin A - B$, $y \in f[C]$, hence $y = f(x)$ for some $x \in C$, and $g(x) = y$.

Therefore, $g: A \hookrightarrow\!\!\!\!\rightarrow B$ is a bijection, establishing $|A| = |B|$. ■

Proof 2. Assume $f: A \hookrightarrow\!\!\!\!\rightarrow A_1$ is a bijection where $A_1 \subseteq B \subseteq A$.

Define a function $F: \mathscr{P}(A) \to \mathscr{P}(A)$ by:

$$F(X) = (A - B) \cup f[X].$$

This function is order-preserving: if $X \subseteq Y$, then $F(X) \subseteq F(Y)$.

By the Recursion (Fixed Point) Theorem, there exists a set $C \subseteq A$ such that:

$$C = (A - B) \cup f[C].$$

Let $D = A - C$. Then:

$$C = (A - B) \cup f[C] \quad \Rightarrow \quad D = B - f[C].$$

Define a function $g: A \to A$ by:

$$g(x) = \begin{cases} f(x) & \text{if } x \in C, \\ x & \text{if } x \in D. \end{cases}$$

Since $f[C] \subseteq C$ and $D = B - f[C] \subseteq B$, the function g is injective.

To show that g is bijective onto B, take any $y \in B$:

- If $y \in D$, then $g(y) = y$.
- If $y \in C$, since $y \in B$, and $C = (A - B) \cup f[C]$, $y \in f[C]$. Hence, $y = f(x)$ for some $x \in C$, and $g(x) = y$.

Thus, $g: A \hookrightarrow\!\!\!\!\rightarrow B$ is a bijection, implying $|A| = |B|$. ■

Theorem 4.1 (Cantor–Bernstein Theorem)**.** If $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$.

Proof. Assume $|X| \leq |Y|$ via an injective function $f: X \hookrightarrow Y$ and $|Y| \leq |X|$ via an injective function $g: Y \hookrightarrow X$.

By the Cantor-Bernstein Lemma (Lemma 4.3), since $g \circ f: X \hookrightarrow g[Y] \subseteq X$, and $|g[Y]| = |Y| \leq |X|$, it follows that $|X| = |Y|$. ■

Claim 4.1 (Existence of Cardinal Numbers)**.** There exist sets called *cardinal numbers* (or *cardinals*) with the property that for every set X, there is a unique cardinal $|X|$ (the *cardinal number of* X, the *cardinality of* X) such that sets X and Y are equipotent if and only if $|X| = |Y|$.

Remark. Claim 4.1 essentially asserts the existence of a unique "representative" for each equivalence class of mutually equipotent sets. This assumption is generally harmless as it serves for convenience. Although we could formulate the theorems without it, proving Claim 4.1 typically requires the Axiom of Choice, which is discussed in Axiom of Choice. However, for certain classes of sets, cardinal numbers can be defined without the Axiom of Choice.

Theorem 4.2 (Transitivity of Cardinal Inequalities)**.** Let A, B, and C be sets.

(i) If $|A| < |B|$ and $|B| \leq |C|$, then $|A| < |C|$.

(ii) If $|A| \leq |B|$ and $|B| < |C|$, then $|A| < |C|$.

Proof.

(i) We already have $|A| \leq |C|$ by Lemma 4.2. Let $g: B \hookrightarrow C$. Suppose $f: A \hookrightarrow\!\!\!\!\rightarrow C$ for the sake of contradiction. Then, $f^{-1} \circ g: B \hookrightarrow A$, i.e., $|B| \leq |A|$. By Cantor–Bernstein Theorem, we get $|A| = |B|$, which is a contradiction.

(ii) We already have $|A| \leq |C|$ by Lemma 4.2. Let $g: A \hookrightarrow B$. Suppose $f: A \hookrightarrow\!\!\!\!\rightarrow C$ for the sake of contradiction. Then, $g \circ f^{-1}: C \hookrightarrow B$, i.e., $|C| \leq |B|$. By Cantor–Bernstein Theorem, we get $|B| = |C|$, which is a contradiction.

■

Theorem 4.3 (Cardinality of Subsets)**.** If $A \subseteq B$, then $|A| \leq |B|$.

Proof. The identity function Id_A is an injective function from A into B. ■

Theorem 4.4 (Cardinality of Function Spaces)**.** If $S \subseteq T$, then $|A^S| \leq |A^T|$. In particular, $|A^m| \leq |A^n|$ if $m \leq n$.

Proof. If $T = \emptyset$, then $A^S = A^T = \{\emptyset\}$, and the inequality $|A^S| \leq |A^T|$ holds trivially.

Assume $T \neq \emptyset$. Fix some $t \in T$. Define the injection $f: A^S \hookrightarrow A^T$ by

$$f(g) = g \cup \{\, (x,t) \mid x \in T - S \,\}.$$

This function f is injective because for any distinct functions $g_1, g_2 \in A^S$, their extensions $f(g_1)$ and $f(g_2)$ differ on S, ensuring $f(g_1) \neq f(g_2)$. ■

Theorem 4.5 (Existence of Least Fixed Point for Monotone Functions)**.** Let $F\colon \mathscr{P}(A) \to \mathscr{P}(A)$ be *monotone*, i.e., if $X \subseteq Y \subseteq A$, then $F(X) \subseteq F(Y)$. Then, F has a least *fixed point* $\overline{X}$, that is, $F(\overline{X}) = \overline{X}$ and $\forall X \subseteq A,\ (F(X) = X \implies \overline{X} \subseteq X)$.

Proof. Let

$$T \triangleq \{\, X \subseteq A \mid F(X) \subseteq X \,\}.$$

Since $A \in T$, $T \neq \emptyset$. Define

$$\overline{X} \triangleq \bigcap T.$$

Then, for all $X \in T$, $\overline{X} \subseteq X$. Since F is monotone, applying F to both sides yields

$$F(\overline{X}) \subseteq F(X) \subseteq X.$$

Taking the intersection over all $X \in T$, we obtain

$$F(\overline{X}) \subseteq \bigcap T = \overline{X}.$$

Hence, $F(\overline{X}) \subseteq \overline{X}$, which means $\overline{X} \in T$.
On the other hand, since $\overline{X}$ is the intersection of all $X \in T$, and F is monotone,

$$F(\overline{X}) = \overline{X}.$$

Moreover, if $X \subseteq A$ is any fixed point of F, i.e., $F(X) = X$, then $X \in T$, and thus

$$\overline{X} = \bigcap T \subseteq X.$$

Therefore, $\overline{X}$ is the least fixed point of F. ■

Theorem 4.6 (Least Fixed Point via Iterative Construction)**.** A function $F\colon \mathscr{P}(A) \to \mathscr{P}(A)$ is *continuous* if, for each sequence $\langle X_i \mid i \in \mathbb{N} \rangle$ of subsets of A such that $\forall i, j \in \mathbb{N},\ (i \leq j \implies X_i \subseteq X_j)$, the following holds:

$$F\left(\bigcup_{i \in \mathbb{N}} X_i\right) = \bigcup_{i \in \mathbb{N}} F(X_i).$$

If $\overline{X}$ is the least fixed point of a monotone continuous function $F\colon \mathscr{P}(A) \to \mathscr{P}(A)$, then

$$\overline{X} = \bigcup_{i \in \mathbb{N}} X_i,$$

where the sequence is defined recursively by $X_0 = \emptyset$ and $\forall i \in \mathbb{N},\ X_{i+1} = F(X_i)$.

Proof. Let

$$\tilde{X} \triangleq \bigcup_{i \in \mathbb{N}} X_i.$$

We have $X_0 = \emptyset \subseteq X_1$.

If $X_n \subseteq X_{n+1}$, then $X_{n+1} \subseteq X_{n+2}$ since F is monotone. Hence, $\forall n \in \mathbb{N},\ X_n \subseteq X_{n+1}$.

Therefore, similarly to Theorem 4.2, we have $X_m \subseteq X_n$ whenever $m \leq n$.

Applying the continuity of F,

$$F(\tilde{X}) = F\left(\bigcup_{i\in\mathbb{N}} X_i\right) = \bigcup_{i\in\mathbb{N}} F(X_i) = \bigcup_{i=1}^{\infty} X_i = \tilde{X}.$$

Thus, $\tilde{X}$ is a fixed point of F, and by the minimality of $\overline{X}$, we have $\overline{X} \subseteq \tilde{X}$.

Next, we show that $\tilde{X} \subseteq \overline{X}$. Since $X_0 \subseteq \overline{X}$ and $X_{n+1} = F(X_n) \subseteq \overline{X}$ for all $n \in \mathbb{N}$ (because $\overline{X}$ is the least fixed point), it follows that

$$\tilde{X} = \bigcup_{i\in\mathbb{N}} X_i \subseteq \overline{X}.$$

Therefore, $\tilde{X} = \overline{X}$. ■

4.1 Finite Sets

Definition 4.3 (Finite and Infinite Sets)**.** A set S is *finite* if it is equipotent to some natural number $n \in \mathbb{N}$. We then define $|S| = n$ and say S *has n elements*. A set is *infinite* if it is not finite.

Remark. According to Definition 4.3, the cardinal numbers of finite sets correspond to natural numbers. Specifically, $\forall n \in \mathbb{N},\ |n| = n$.

Lemma 4.4 (Proper Subset of Finite Set)**.** If $n \in \mathbb{N}$ and $X \subsetneq n$, then there does not exist a bijective function $f : n \hookrightarrow\!\!\!\!\rightarrow X$.

Proof. We proceed by induction on n.

Base Case: If $n = 0$, then $X \subsetneq 0$ implies $X = \emptyset$, and $f : 0 \hookrightarrow\!\!\!\!\rightarrow \emptyset$ is the empty function, which is trivially bijective. However, $X \subsetneq n$ in this case is impossible since both X and n are empty. Thus, the statement holds vacuously.

Inductive Step: Assume that for some $n \in \mathbb{N}$, there is no bijection $f : n \hookrightarrow\!\!\!\!\rightarrow X$ for any $X \subsetneq n$.

Now, consider $n+1$ and let $X \subsetneq n+1$. There are two cases:

(a) $n \notin X$: Then $X \subseteq n$, and by the induction hypothesis, there is no bijection $f : n \hookrightarrow\!\!\!\!\rightarrow X - \{f(n)\}$, leading to a contradiction.

(b) $n \in X$: Since f is bijective, $f(k) = n$ for some $k < n$. Define a function $g : n \to X - \{n\}$ by:

$$g(i) = \begin{cases} f(n) & \text{if } i = k, \\ f(i) & \text{otherwise.} \end{cases}$$

This function g would be injective and map n to $X - \{n\}$, contradicting the induction hypothesis.

Thus, by induction, no bijection exists for $n+1$ when $X \subsetneq n+1$. ■

Corollary (Basic Properties of Finite Sets)**.** (i) If $m \neq n$ where $m, n \in \mathbb{N}$, then there is no bijective function $f : m \hookrightarrow\!\!\!\!\rightarrow n$.

(ii) If $|S| = m$ and $|S| = n$, then $m = n$.

(iii) $\mathbb{N}$ is infinite.

Proof. (i) If $m \neq n$, without loss of generality assume $m < n$. Then $m \subsetneq n$, and by Lemma 4.4, no bijection $f : m \hookrightarrow\!\!\!\!\rightarrow n$ exists.

(ii) If $|S| = m$ and $|S| = n$, then by Lemma 4.1, $m = n$.

(iii) Assume for contradiction that $\mathbb{N}$ is finite. Then there exists $n \in \mathbb{N}$ such that $|\mathbb{N}| = n$. However, by Theorem 4.8, $f : \mathbb{N} \hookrightarrow\!\!\!\!\rightarrow n$ would imply $|\mathbb{N}| \leq n$. But since $\mathbb{N}$ is infinite, this is impossible. Hence, $\mathbb{N}$ is infinite.

■

Theorem 4.7 (Subset of a Finite Set is Finite)**.** If X is a finite set and $Y \subseteq X$, then Y is finite.

Proof. Assume $X = \{x_0, x_1, \ldots, x_{n-1}\}$ with $\langle x_0, x_1, \ldots, x_{n-1} \rangle$ being an injective sequence, and $Y \neq \emptyset$.
Define a function $g : n \times \mathbb{N} \rightharpoonup n$ by:

$$g(a, -) = \begin{cases} \min\{ j \in n \mid a < j \wedge x_j \in Y \} & \text{if such } j \text{ exists,} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

By Theorem 3.20, there exists a sequence k of elements in n such that:

(i) $k_0 = \min\{ j \in n \mid x_j \in Y \}$ (since $Y \neq \emptyset$).

(ii) $\forall i \in \mathbb{N},\ k_{i+1} = g(k_i, i)$ whenever $i+1$ is in the domain of k.

(iii) k is either an infinite sequence or a finite sequence of length $\ell + 1$ where $(k_\ell, \ell) \notin dom(g)$.

By (ii) and the definition of g, k is strictly increasing, hence injective. If k were infinite, $\mathbb{N}$ would embed into n, implying $|\mathbb{N}| \leq n$, which contradicts the infiniteness of $\mathbb{N}$ (see Section 4.1).
Therefore, k is a finite sequence of length ℓ. Let $y_i = x_{k_i}$ for each $i < \ell$. The sequence $y = \langle y_0, y_1, \ldots, y_{\ell-1} \rangle$ is injective and covers Y, hence Y is finite with $|Y| \leq |X|$. ■

Theorem 4.8 (Image of a Finite Set is Finite)**.** If X is finite and f is a function, then $f[X]$ is finite. Moreover, $|f[X]| \leq |X|$.

Proof. If $f[X] = \emptyset$, it is trivially finite. Assume $f[X] \neq \emptyset$. Without loss of generality, assume $X = \{x_0, x_1, \ldots, x_{n-1}\}$ with $\langle x_0, x_1, \ldots, x_{n-1} \rangle$ being injective.

Define a function $g\colon \mathrm{Seq}(n) \rightharpoonup n$ by:

$$g(\langle k_0, k_1, \ldots, k_{\ell'-1}\rangle) = \begin{cases} 0 & \text{if } \ell' = 0, \\ \min\{k \in n \mid k_{\ell'-1} < k \wedge \forall i < \ell',\ f(x_k) \neq f(x_{k_i})\} & \text{if } \ell' > 0 \text{ and such } k \text{ exists}, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

By a recursive construction (similar to Theorem 3.20), there exists a sequence k of elements in n such that:

(i) $k_i = g(k \restriction_i)$ for all $i \in \mathbb{N}$.

(ii) k is either an infinite sequence or a finite sequence of length $\ell + 1$ where k is undefined at $\ell + 1$.

By the definition of g, k is injective. If k were infinite, $\mathbb{N}$ would embed into n, implying $|\mathbb{N}| \leq n$, which is impossible. Thus, k is finite with length ℓ.

Let $y = \langle f(x_{k_0}), f(x_{k_1}), \ldots, f(x_{k_{\ell-1}})\rangle$. This sequence is injective and covers $f[X]$, hence $f[X]$ is finite with $|f[X]| \leq |X|$. ■

Lemma 4.5 (Finite Union)**.** Let X and Y be finite sets. Then:

(i) $X \cup Y$ is finite; moreover, $|X \cup Y| \leq |X| + |Y|$.

(ii) If X and Y are disjoint, then $|X \cup Y| = |X| + |Y|$.

Proof. (i) Let $|X| = m$ and $|Y| = n$. Enumerate $X = \{x_0, x_1, \ldots, x_{m-1}\}$ and $Y = \{y_0, y_1, \ldots, y_{n-1}\}$ with injective sequences. Define a function $z\colon m + n \hookrightarrow\!\!\!\!\rightarrow X \cup Y$ by:

$$z_i = \begin{cases} x_i & \text{for } 0 \leq i < m, \\ y_{i-m} & \text{for } m \leq i < m + n. \end{cases}$$

This function is surjective, hence $|X \cup Y| \leq m + n$.

(ii) If X and Y are disjoint, then $z\colon m + n \hookrightarrow\!\!\!\!\rightarrow X \cup Y$ defined as above is bijective. Thus, $|X \cup Y| = m + n$.

■

Theorem 4.9 (Finite Union)**.** If S is finite and every $X \in S$ is finite, then $\bigcup S$ is finite.

Proof. Proceed by induction on $|S|$.

Base Case: If $|S| = 0$, then $\bigcup S = \emptyset$, which is finite.

Inductive Step: Assume that for all finite sets S with $|S| = n$, if every $X \in S$ is finite, then $\bigcup S$ is finite. Let $S = \{X_0, X_1, \ldots, X_n\}$ with $|S| = n + 1$ and each X_i finite.

By the induction hypothesis, $\bigcup_{i=0}^{n} X_i = \left(\bigcup_{i=0}^{n-1} X_i\right) \cup X_n$ is finite, as $\bigcup_{i=0}^{n-1} X_i$ is finite and finite unions preserve finiteness by Lemma 4.5. ■

Theorem 4.10 (Power Set of a Finite Set is Finite)**.** If X is finite, then $\mathscr{P}(X)$ is finite.

Proof. We prove by induction on $|X|$.

Base Case: If $|X|=0$, then $\mathscr{P}(X)=\{\emptyset\}$, which is finite.

Inductive Step: Assume that for all sets X with $|X|=n$, $\mathscr{P}(X)$ is finite. Let $|Y|=n+1$. Enumerate $Y=\{y_0,y_1,\ldots,y_n\}$ and let $X=\{y_0,y_1,\ldots,y_{n-1}\}$. Then:

$$\mathscr{P}(Y)=\mathscr{P}(X)\cup\{u\cup\{y_n\}\mid u\in\mathscr{P}(X)\}.$$

Define $f:\mathscr{P}(X)\to\mathscr{P}(Y)$ by $f(u)=u\cup\{y_n\}$. This function is injective, and hence $|\mathscr{P}(Y)|=2^n$, which is finite.

By the induction hypothesis, $\mathscr{P}(Y)$ is finite. ■

Theorem 4.11 (Infinite Sets Have Large Cardinality)**.** If X is infinite, then $|X|>n$ for all $n\in\mathbb{N}$.

Proof. We prove by induction on n that $|X|>n$.

Base Case: $n=0$. Since X is infinite, $|X|\geq 1>0$.

Inductive Step: Assume $|X|>n$ for some $n\in\mathbb{N}$. We need to show that $|X|>n+1$.

Since $|X|>n$, there exists an injective function $f:n+1\hookrightarrow X$. Suppose for contradiction that $|X|\leq n$. Then, by Section 4.1, X would be finite, contradicting the assumption that X is infinite. Therefore, $|X|>n+1$.

By induction, $|X|>n$ for all $n\in\mathbb{N}$. ■

Theorem 4.12. If $S=\{X_0,\cdots,X_{n-1}\}$ is a finite set of mutually disjoint sets. Then, $|\bigcup S|=\sum_{i=0}^{n-1}|X_i|$.

Proof. If $S=\emptyset$, then $|\bigcup S|=0=\sum_{i=0}^{n-1}|X_i|$.

Fix $n\in\mathbb{N}$ and assume the assertion holds for all S with $|S|=n$. Then, take any set T of mutually disjoint sets with $|T|=n+1$. Write $T=\{X_0,\cdots,X_n\}$ and let $S\triangleq=\{X_0,\cdots,X_{n-1}\}$. Then, since $\bigcup T=(\bigcup S)\cup X_n$, and since $\bigcup S$ and X_n are disjoint, $|\bigcup T|=|\bigcup S|+|X_n|=\sum_{i=0}^{n-1}|X_i|+|X_n|=\sum_{i=0}^{n}|X_i|$. Hence, the result follows from Principle of Mathematical Induction. ■

Theorem 4.13. If X and Y are finite, then $|X\times Y|=|X|\cdot|Y|$.

Proof. We shall use induction on $|Y|$.

Base Case: Suppose $|Y|=0$. Then,$|X\times Y|=0$ (since the Cartesian product with the empty set is empty), and $|X|\cdot|Y|=|X|\cdot 0=0$. Therefore, $|X\times Y|=|X|\cdot|Y|$ holds when $|Y|=0$.

Inductive Hypothesis: Assume that for all finite sets X and Y with $|Y|=n$, the equality $|X\times Y|=|X|\cdot|Y|$ holds.

Inductive Step: Let $Z=\{z_0,z_1,\ldots,z_n\}$ be a set with $|Z|=n+1$. Define $Y=\{z_0,z_1,\ldots,z_{n-1}\}$, so that $|Y|=n$.

Then, for any finite set X, $X\times Z=(X\times Y)\cup(X\times\{z_n\})$. Note that $X\times Y$ and $X\times\{z_n\}$ are disjoint because $z_n\notin Y$.

Observe that $X\times\{z_n\}$ can be naturally identified with X via the bijection $f:X\hookrightarrow X\times\{z_n\}$, defined by $f(x)=(x,z_n)$. Therefore,$|X\times\{z_n\}|=|X|$. By the induction hypothesis, $|X\times Y|=|X|\cdot|Y|=|X|\cdot n$. Hence,

$$|X\times Z|=|X\times Y|+|X\times\{z_n\}|=|X|\cdot n+|X|=|X|\cdot(n+1).$$

Therefore, $|X\times Z|=|X|\cdot|Z|$. Hence, the result follows from Principle of Mathematical Induction. ■

Theorem 4.14. If X is finite, $|\mathscr{P}(X)| = 2^{|X|}$.

Proof. Let $\mathbf{P}(x)$ be the property $\forall X,\ \big(|X| = x \implies |\mathscr{P}(X)| = 2^{|X|}\big)$.

Base Case: $\mathbf{P}(0)$ holds since $|\mathscr{P}(\emptyset)| = |\{\emptyset\}| = 1 = 2^0$.

Inductive Step: Assume $\mathbf{P}(n)$ holds for some $n \in \mathbb{N}$. That is, for any set X with $|X| = n$, $|\mathscr{P}(X)| = 2^n$.

Let $Y = \{y_0, y_1, \ldots, y_n\}$ be a set with $|Y| = n+1$. Define $X \triangleq \{y_0, y_1, \ldots, y_{n-1}\}$, so $|X| = n$.

As in the proof of Theorem 4.10, the power set $\mathscr{P}(Y)$ can be expressed as the union $\mathscr{P}(Y) = \mathscr{P}(X) \cup U$, where $U = \{u \subseteq Y \mid y_n \in u\}$.

Observe that $\mathscr{P}(X) \cap U = \emptyset$, as no subset of Y can both contain and not contain y_n. Furthermore, define the function

$$f : \mathscr{P}(X) \hookrightarrow U \quad \text{by} \quad f(x) = x \cup \{y_n\}.$$

This function f is a bijection because:

(i) Injectivity: If $x_1, x_2 \in \mathscr{P}(X)$ and $f(x_1) = f(x_2)$, then $x_1 \cup \{y_n\} = x_2 \cup \{y_n\}$. Since y_n is common to both, it follows that $x_1 = x_2$.

(ii) Surjectivity: For any $u \in U$, u contains y_n. Thus, $u = x \cup \{y_n\}$ for some $x \subseteq X$, meaning u is in the image of f.

Therefore, $|\mathscr{P}(X)| = |U|$.

Consequently,

$$\begin{aligned}
|\mathscr{P}(Y)| &= |\mathscr{P}(X)| + |U| && \text{(since } \mathscr{P}(X) \text{ and } U \text{ are disjoint)} \\
&= 2^n + 2^n && (\mathbf{P}(n) \text{ and } |\mathscr{P}(X)| = |U|) \\
&= 2^n \cdot 1 + 2^n \cdot 1 && \text{(rewriting } 2^n \text{ for clarity)} \\
&= 2^n \cdot 2 && (1 + 1 = 2) \\
&= 2^{n+1}. && (2^n \cdot 2 = 2^{n+1})
\end{aligned}$$

Therefore, $|\mathscr{P}(Y)| = 2^{n+1}$, which establishes $\mathbf{P}(n+1)$.

Hence, the result follows from Principle of Mathematical Induction.

$|\mathscr{P}(X)| = 2^{|X|}$.

■

Theorem 4.15. If X and Y are finite, then X^Y is finite and $|X^Y| = |X|^{|Y|}$.

Proof. Let $\mathbf{P}(x)$ be the property

"If X is finite and $|Y| = x$, then $|X^Y| = |X|^x$."

Base Case: $\mathbf{P}(0)$ holds since $|X^\emptyset| = |\{\emptyset\}| = 1 = |X|^0$ for all finite sets X.

Inductive Step: Fix $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$ holds. That is, for any finite set X and any set Y with $|Y| = n$, $|X^Y| = |X|^n$.

Let $Y = \{y_0, y_1, \ldots, y_n\}$ be a set with $|Y| = n+1$. Define $Z \triangleq \{y_0, y_1, \ldots, y_{n-1}\}$, so that $|Z| = n$.

Take any finite set X. We have: $|X^Y| = |X^Z \times X|$. This is because we can define a bijection $f: X^Y \hookrightarrow X^Z \times X$ by $f(g) = (g \restriction_Z,\ g(y_n))$, where $g \restriction_Z$ denotes the restriction of the function g to the subset Z.

Therefore, the cardinality satisfies:

$$\begin{aligned} |X^Y| &= |X^Z \times X| && \text{(by definition of Cartesian product)} \\ &= |X^Z| \cdot |X| && \text{(by Theorem 4.12)} \\ &= |X|^n \cdot |X| && (\mathbf{P}(n) \text{ holds}) \\ &= |X|^{n+1}. && \text{(by properties of exponentiation)} \end{aligned}$$

Hence, the result follows from Principle of Mathematical Induction.

$$|X^Y| = |X|^x.$$

■

Theorem 4.16. X is finite if and only if every $\emptyset \subsetneq U \subseteq \mathscr{P}(X)$ has a $\subseteq$-maximal element.

Proof.

($\Rightarrow$) Let $|X| = n$ and $\emptyset \subsetneq U \subseteq \mathscr{P}(X)$. Since $|Y| \leq n$ for all $Y \in U$, by Theorem 3.8, we may let $m \triangleq \max\{\, |Y| \mid Y \in U \,\}$.
There exists $Y \in U$ with $|Y| = m$. Then, for each $Y' \in U$ such that $Y \subseteq Y'$, we have $m \leq |Y'|$ by Theorem 4.3 and $|Y'| \leq m$ by the definition of m; thus $|Y'| = |Y| = m$ by Cantor–Bernstein Theorem, which implies we may not have $Y \subsetneq Y'$ by Lemma 4.4. Hence, Y is a maximal element of U.

($\Leftarrow$) Assume X is infinite. Let $U = \{\, Y \subseteq X \mid Y \text{ is finite} \,\}$. (Note $\emptyset \in U$, hence $U \neq \emptyset$.) Take any $Y \in U$. Since $Y \subsetneq X$, we may take $x \in X - Y$. Then, $Y \subsetneq Y \cup \{x\}$ and $Y \cup \{x\} \in U$ by Lemma 4.5. Hence, there is no maximal element of U.

■

4.2 Countably Infinite Sets

Definition 4.4 (Countably Infinite Set)**.** A set S is *countably infinite* if $|S| = |\mathbb{N}|$.

Definition 4.5 (Countable Set)**.** A set S is *countable* if $|S| \leq |\mathbb{N}|$.

Definition 4.6 (Cardinality of Countably Infinite Sets)**.** $|\mathbb{N}| = \aleph_0$, i.e., the cardinality of countably infinite sets is $\aleph_0$.

Remark. In the book, the author uses the terms 'countable' and 'at most countable' for $|S| = |\mathbb{N}|$ and $|S| \leq |\mathbb{N}|$, respectively.

Notation 4.1 (Cardinality of Countably Infinite Sets)**.** We use the symbol $\aleph_0$ (read *aleph-naught*) to denote the cardinality of countably infinite sets, i.e., $\aleph_0 = |\mathbb{N}|$.

Theorem 4.17 (Subset of a Countably Infinite Set is Countable)**.** A subset of a countably infinite set is countable.

Proof. Assume A is countably infinite and $B \subseteq A$ is infinite. Let $\langle a_i \rangle_{i \in \mathbb{N}}$ be an injective sequence whose range is A.

Let $g: \mathrm{Seq}(\mathbb{N}) \to \mathbb{N}$ be defined by

$$g(k) \triangleq \min \left\{ i \in \mathbb{N} \,\middle|\, a_i \in B - \{ a_{k_j} \mid j \in \mathrm{dom}(k) \} \right\}.$$

Note that g is well-defined since B is infinite. Then, by Theorem 3.16, there exists a sequence $\langle k_i \rangle_{i \in \mathbb{N}}$ of natural numbers such that $\forall n \in \mathbb{N}, k_n = g(k \restriction_n)$. By construction, $\langle k_i \rangle_{i \in \mathbb{N}}$ is injective, and thus $\langle a_{k_i} \rangle_{i \in \mathbb{N}}$ is an injective sequence whose range is B by the same argument of Claim 3.1. ■

Corollary. A set is countable if and only if it is either finite or countably infinite.

Proof.

($\Rightarrow$) Let S be countable. Let $f: S \hookrightarrow \mathbb{N}$. Then, $|S| = |ran(f)|$ and $ran(f)$ is a subset of $\mathbb{N}$. Hence, by Theorem 4.17, S is countably infinite if it is not finite.

($\Leftarrow$) If S is finite, then clearly $|S| \leq |\mathbb{N}|$, so S is countable. If S is countably infinite, then by definition, $|S| = |\mathbb{N}|$, which means S is countable.

■

Theorem 4.18 (Image of a Countably Infinite Set is Countable)**.** If X is countably infinite and f is a function, then $f[X]$ is countable.

Proof. If $f[X] = \emptyset$, then it is trivially countable. Assume $f[X] \neq \emptyset$. Without loss of generality, assume $X \subseteq \mathrm{dom}(f)$. Let $\langle x_i \rangle_{i \in \mathbb{N}}$ be an injective sequence whose range is X. Define $g: f[X] \to \mathbb{N}$ by

$$g(y) \triangleq \min\{ i \in \mathbb{N} \mid y = f(x_i) \}.$$

g is injective since if $g(y_1) = g(y_2)$, then $y_1 = f(x_{g(y_1)}) = f(x_{g(y_2)}) = y_2$. Therefore, $|f[X]| \leq \aleph_0$, meaning $f[X]$ is countable. ■

Theorem 4.19 (Product of Countable Sets is Countable)**.**

(i) If A and B are countably infinite, then $A \times B$ is countably infinite.
(ii) If A is countably infinite and $B \neq \emptyset$ is finite, then $A \times B$ is countably infinite.
(iii) If A and B are countable, then $A \times B$ is countable.

Proof.

(i) The function $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$f(x,y) = 2^x \cdot 3^y$$

is injective by elementary number theory (unique prime factorization). Also, we have an injection $g: \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ defined by $g(x) = (x, 0)$. Hence, by Cantor–Bernstein Theorem, we have $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

(ii) Let $|B| = n$. Then,

$$\begin{aligned} |A \times B| &= |\mathbb{N} \times n| && \text{(since } A \text{ is countably infinite)} \\ &\leq |\mathbb{N} \times \mathbb{N}| && \text{(Theorem 4.3)} \\ &= \aleph_0. && \text{(Theorem 4.19)} \end{aligned}$$

Let $b \in B$. Then,

$$\begin{aligned} \aleph_0 &= |A| && \text{(since } A \text{ is countably infinite)} \\ &= |A \times \{b\}| && (a \mapsto (a,b)) \\ &\leq |A \times B|. && \text{(Theorem 4.3)} \end{aligned}$$

Hence, by Cantor–Bernstein Theorem, $|A \times B| = \aleph_0$.

(iii) If one of A or B is empty, then $A \times B = \emptyset$, which is countable. If both A and B are finite, then $A \times B$ is finite by Theorem 4.13. If either A or B is countably infinite, and both are nonempty, then $A \times B$ is countably infinite by parts (i) and (ii).

■

Corollary (Product of Finite Countably Infinite Sets)**.** Let $\langle A_i \mid i \in n \rangle$ be a system of countably infinite sets where $n > 0$. Then, $\prod_{i=0}^{n-1} A_i$ is countably infinite.

Proof. Let $\mathbf{P}(x)$ be the property "$\prod_{i=0}^{x-1} A_i$ is countably infinite for each system $\langle A_i \mid i \in x \rangle$ of countably infinite sets." Clearly, $\mathbf{P}(1)$ holds since the product of a single countably infinite set is itself countably infinite.

Fix $n > 0$ and assume $\mathbf{P}(n)$ holds. Now, take any system $\langle A_i \mid i \in n+1 \rangle$ of countably infinite sets. Then, since we have a natural mapping $f : \prod_{i=0}^{n} A_i \hookrightarrow \left(\prod_{i=0}^{n-1} A_i\right) \times A_n$ defined by

$$f(\langle a_0, \cdots, a_n \rangle) \mapsto (\langle a_0, \cdots, a_{n-1} \rangle, a_n),$$

we get

$$\begin{aligned} \left| \prod_{i=0}^{n} A_i \right| &= \left| \left(\prod_{i=0}^{n-1} A_i \right) \times A_n \right| && \text{(by definition of product)} \\ &= \aleph_0. && \text{(Theorem 4.19)} \end{aligned}$$

Hence, we have $\mathbf{P}(n+1)$.

Therefore, by Theorem 3.1, the result follows. ■

Theorem 4.20 (Union of Countably Infinite Sets is Countable)**.** Let $\langle a_n \mid n \in \mathbb{N} \rangle$ be a countably infinite system of infinite sequences. Then,

$$\bigcup_{n \in \mathbb{N}} ran(a_n)$$

is countable.

Proof. Define $f : \mathbb{N} \times \mathbb{N} \twoheadrightarrow \bigcup_{n \in \mathbb{N}} \text{ran}(a_n)$ by $f(n,k) = a_n(k)$. The result follows by Theorem 4.18 and Theorem 4.19. ■

Remark. Note that we cannot yet prove the proposition "the union of a countably infinite system of countable sets is countable" since, if $\langle A_n \mid n \in \mathbb{N}\rangle$ is the system, we do not have enough tools to show the existence of $\langle a_n \mid n \in \mathbb{N}\rangle$ such that $\mathrm{ran}(a_n) = A_n$ for each $n \in \mathbb{N}$.

Theorem 4.21 (Sequences of Countably Infinite Sets are Countably Infinite)**.** If A is countably infinite, then $\mathrm{Seq}(A)$ is countably infinite.

Proof. It is enough to show $\mathrm{Seq}(\mathbb{N}) = \bigcup_{n\in\mathbb{N}} \mathbb{N}^n$ is countably infinite. Fix any $g\colon \mathbb{N} \twoheadrightarrow \mathbb{N}\times\mathbb{N}$. Define $\langle a_n \mid n \in \mathbb{N}\rangle$ recursively by

$$\begin{aligned} \forall i \in \mathbb{N}, \quad & a_0(i) \triangleq \langle\rangle \\ \forall n, i \in \mathbb{N}, & a_{n+1}(i) \triangleq \langle b_0, \cdots, b_{n-1}, i_2\rangle \\ & \qquad \text{where } g(i) = \langle i_1, i_2\rangle \text{ and } a_n(i_1) = \langle b_0, \cdots, b_{n-1}\rangle. \end{aligned}$$

The existence is justified by Recursion Theorem. Then, with Principle of Mathematical Induction, it is easy to prove that $\mathrm{ran}(a_n) = \mathbb{N}^n$ for each $n \in \mathbb{N}$. Hence, by Union of Countably Infinite Sets is Countable, $\bigcup_{n\in\mathbb{N}} \mathbb{N}^n$ is countably infinite. ■

Corollary (Finite Subsets of a Countably Infinite Set are Countably Infinite)**.** The set of all finite subsets of a countably infinite set is countably infinite.

Proof. Let A be countably infinite. Define $f\colon \mathrm{Seq}(A) \to \mathscr{P}(A)$ by

$$f(\langle a_0, \cdots, a_{n-1}\rangle) = \{\, a_0, \cdots, a_{n-1} \,\}.$$

Then, $ran(f)$ is countable by Theorem 4.18 and Theorem 4.21. Moreover, $ran(f)$ is countably infinite since we have an injection $a \mapsto \{a\}$. ■

Theorem 4.22 (Equivalence Classes of Countably Infinite Sets are Countable)**.** An equivalence relation on a countably infinite set has at most countably many equivalence classes.

Proof. Let E be an equivalence relation on a countably infinite set A. Let $f\colon A \twoheadrightarrow A/E$ be defined by $a \mapsto [a]_E$. Hence, by Theorem 4.18, A/E is countable. ■

Theorem 4.23 (Countable Closure of Countable Sets)**.** Let $\mathfrak{A} = (A, \langle R_0, \cdots, R_{m-1}\rangle, \langle F_0, \cdots, F_{n-1}\rangle)$ be a structure. If $C \subseteq A$ is countable, then $\overline{C}$ is also countable.

Proof. By Theorem 3.32, $\overline{C} = \bigcup_{i\in\mathbb{N}} C_i$ where $C_0 = C$ and $\forall i \in \mathbb{N}$, $C_{i+1} = C_i \cup \bigcup_{j=0}^{n-1} F_j[C_i^{f_j}]$.

Let $c\colon \mathbb{N} \twoheadrightarrow C$. Let $g\colon \mathbb{N} \twoheadrightarrow (n+1)\times\mathbb{N}\times\mathbb{N}^{f_0}\times\cdots\times\mathbb{N}^{f_{n-1}}$. Now, define $\langle a_i \mid i \in \mathbb{N}\rangle$ recursively by

$$\begin{aligned} \forall k \in \mathbb{N}, \quad & a_0(k) \triangleq c(k) \\ \forall i, k \in \mathbb{N}, \quad & a_{i+1}(k) \triangleq \begin{cases} F_p(a_i(r_p^0), \ldots, a_i(r_p^{f_p-1})) & \text{if } 0 \le p < n \\ a_i(q) & \text{if } p = n \end{cases} \\ & \qquad \text{where } g(k) = \langle p, q, \langle r_0^0, \ldots, r_0^{f_0-1}\rangle, \ldots, \langle r_{n-1}^0, \ldots, r_{n-1}^{f_{n-1}-1}\rangle\rangle. \end{aligned}$$

The existence is justified by Theorem 3.1. Then, by Theorem 3.1, it is easy to prove that $\mathrm{ran}(a_i) = C_i$ for each $i \in \mathbb{N}$. Hence, by Theorem 4.20, $\overline{C}$ is countable. ■

Theorem 4.24. Let $|A_1| = |A_2|$ and $|B_1| = |B_2|$.

(i) If $A_1 \cap B_1 = \emptyset$ and $A_2 \cap B_2 = \emptyset$, then $|A_1 \cup B_1| = |A_2 \cup B_2|$.
(ii) $|A_1 \times B_1| = |A_2 \times B_2|$.
(iii) $|\mathrm{Seq}(A_1)| = |\mathrm{Seq}(A_2)|$.

Proof. (i) Let $f_A : A_1 \rightarrowtail A_2$ and $f_B : B_1 \rightarrowtail B_2$ be bijections (since $|A_1| = |A_2|$ and $|B_1| = |B_2|$). Since $A_1 \cap B_1 = \emptyset$ and $A_2 \cap B_2 = \emptyset$, we can define a function

$$f : A_1 \cup B_1 \to A_2 \cup B_2$$

by

$$f(x) = \begin{cases} f_A(x) & \text{if } x \in A_1, \\ f_B(x) & \text{if } x \in B_1. \end{cases}$$

This function f is a bijection because f_A and f_B are bijections on disjoint domains and codomains. Therefore, $|A_1 \cup B_1| = |A_2 \cup B_2|$.

(ii) Let $f_A : A_1 \rightarrowtail A_2$ and $f_B : B_1 \rightarrowtail B_2$ be bijections. Define

$$g : A_1 \times B_1 \to A_2 \times B_2 \quad \text{by} \quad g(a,b) = (f_A(a),\ f_B(b)).$$

Since f_A and f_B are bijections, g is a bijection. Thus, $|A_1 \times B_1| = |A_2 \times B_2|$.

(iii) Let $f : A_1 \rightarrowtail A_2$ be a bijection. Define

$$g : \mathrm{Seq}(A_1) \to \mathrm{Seq}(A_2) \quad \text{by} \quad g(\langle a_0, a_1, \ldots, a_{n-1} \rangle) = \langle f(a_0), f(a_1), \ldots, f(a_{n-1}) \rangle.$$

Since f is a bijection, g is a bijection. Therefore, $|\mathrm{Seq}(A_1)| = |\mathrm{Seq}(A_2)|$. ■

Theorem 4.25. If A is finite and B is countably infinite, then $A \cup B$ is countably infinite.

Proof. Let $f_A : A \rightarrowtail \mathbb{N}$ and $f_B : B \rightarrowtail \mathbb{N}$ be injections (possible since $\mathbb{N}$ is infinite). Define

$$g : A \cup B \to \mathbb{N} \times \mathbb{N} \quad \text{by} \quad g(x) = \begin{cases} (f_A(x),\ 0) & \text{if } x \in A, \\ (f_B(x),\ 1) & \text{if } x \in B - A. \end{cases}$$

Since A is finite and B is countably infinite, $A \cup B$ is infinite. The function g is injective, so $|A \cup B| \leq |\mathbb{N} \times \mathbb{N}| = \aleph_0$ (by Theorem 4.19). Moreover, since $|B| = \aleph_0$ and $B \subseteq A \cup B$, we have $\aleph_0 \leq |A \cup B|$. Therefore, by the Cantor-Bernstein Theorem (Cantor–Bernstein Theorem), $A \cup B$ is countably infinite. ■

Theorem 4.26. If A is finite and nonempty, then $\mathrm{Seq}(A)$ is countably infinite.

Proof. Let $B \triangleq A \cup \mathbb{N}$. By Theorem 4.25, B is countably infinite. By Theorem 4.21, $\mathrm{Seq}(B)$ is countably infinite. Since $\mathrm{Seq}(A) \subseteq \mathrm{Seq}(B)$, we have $|\mathrm{Seq}(A)| \leq \aleph_0$.

To show that $|\mathrm{Seq}(A)| \geq \aleph_0$, fix any $a \in A$. Define s to be the infinite sequence where $s_i = a$ for all $i \in \mathbb{N}$. Then, define $f : \mathbb{N} \to \mathrm{Seq}(A)$ by $f(n) = s|_n$ (the restriction of s to its first n terms). This function is injective, so $\aleph_0 \leq |\mathrm{Seq}(A)|$.

Therefore, by the Cantor-Bernstein Theorem (Cantor–Bernstein Theorem), $|\mathrm{Seq}(A)| = \aleph_0$, and thus $\mathrm{Seq}(A)$ is countably infinite. ■

Theorem 4.27. Let A be a countably infinite set. The set

$$[A]^n = \{\, S \subseteq A \mid |S| = n \,\}$$

is countably infinite for all $n > 0$.

Proof. It suffices to show that $[\mathbb{N}]^n$ is countably infinite for all $n > 0$.

For $n = 1$, the function $i \mapsto \{i\}$ is an injective mapping from $\mathbb{N}$ onto $[\mathbb{N}]^1$, so $|[\mathbb{N}]^1| = \aleph_0$.

Assume, inductively, that $|[\mathbb{N}]^n| = \aleph_0$ for some $n \geq 1$. Define

$$f\colon [\mathbb{N}]^n \to [\mathbb{N}]^{n+1} \quad \text{by} \quad f(x) = x \cup \{\max(x) + 1\}.$$

Since f is injective, we have $\aleph_0 \leq |[\mathbb{N}]^{n+1}|$.

Conversely, since $|[\mathbb{N}]^n| = |\mathbb{N}^n| = \aleph_0$ by Section 4.2, there exists an injection $g\colon [\mathbb{N}]^n \hookrightarrow \mathbb{N}^n$. Define

$$h\colon [\mathbb{N}]^{n+1} \to \mathbb{N}^{n+1} \quad \text{by} \quad h(x) = (g(x - \{i\}),\ i)\,,$$

where $i = \max(x)$. Then h is injective, so $|[\mathbb{N}]^{n+1}| \leq |\mathbb{N}^{n+1}| = \aleph_0$.

Therefore, $|[\mathbb{N}]^{n+1}| = \aleph_0$, and by induction, $|[\mathbb{N}]^n| = \aleph_0$ for all $n > 0$. ■

Theorem 4.28. The set of eventually constant sequences of natural numbers is countable.

Proof. Let P be the set of eventually constant sequences of natural numbers.

Define a function $f\colon P \to \mathbb{N} \times \mathbb{N}^*$ by mapping each sequence to the pair consisting of its eventual constant value and the finite initial segment before it becomes constant. Since both $\mathbb{N}$ and the set of finite sequences $\mathbb{N}^*$ are countable, P is countable.

Alternatively, we can construct an injection from $\mathbb{N}$ into P by mapping each $n \in \mathbb{N}$ to the sequence that is constantly n after the first term. This shows $\aleph_0 \leq |P|$, and since P is a subset of $\mathrm{Seq}(\mathbb{N})$, which is countably infinite, we have $|P| = \aleph_0$. ■

Theorem 4.29. The set of eventually periodic sequences of natural numbers is countably infinite.

Proof. Let Q be the set of eventually periodic sequences of natural numbers.

Define a function $f\colon Q \to \mathbb{N} \times \mathbb{N}^* \times \mathbb{N}^*$ by mapping each sequence to the tuple (p^*, σ, τ), where p^* is the minimal period, σ is the finite initial segment before the periodicity starts, and τ is the repeating segment of length p^*. Since $\mathbb{N}$ and $\mathbb{N}^*$ (the set of finite sequences) are countable, Q is countable.

Furthermore, since the set of eventually constant sequences (from Theorem 4.28) is a subset of Q and is countably infinite, it follows that $|Q| = \aleph_0$. ■

Theorem 4.30. Let $(S, \preceq)$ be a linearly ordered set and let $\langle A_n \mid n \in \mathbb{N} \rangle$ be an infinite sequence of finite subsets of S. Then,

$$\bigcup_{n=0}^{\infty} A_n$$

is countable.

Proof. Without loss of generality, assume $A_n \neq \emptyset$ for each $n \in \mathbb{N}$.

Claim 4.2. For each finite $A \subseteq S$, there exists a unique isomorphism between $(|A|, \leq)$ and $(A, \preceq)$, where $|A| = \{0, 1, \ldots, |A|-1\}$.

Proof of Claim 4.2. We proceed by induction on $|A|$.

Base Case: If $|A| = 1$, the isomorphism is trivial.

Inductive Step: Assume uniqueness holds for all finite sets of size n. Let $|A| = n+1$. Since $(S, \preceq)$ is linearly ordered, A has a greatest element $a_{\max}$. Similarly, $|A|$ has a greatest element n. Any isomorphism f must map n to $a_{\max}$. The restriction of f to $\{0, 1, \ldots, n-1\}$ must be the unique isomorphism to $A - \{a_{\max}\}$ by the inductive hypothesis. Therefore, the isomorphism f is unique. ■

Using Claim 4.2, for each $n \in \mathbb{N}$, there exists a unique sequence a_n that lists the elements of A_n in order. Extend a_n to an infinite sequence by repeating its last element indefinitely.

Thus, each a_n is an element of $\mathrm{Seq}(S)$, and $ran(a_n) = A_n$. Therefore,

$$\bigcup_{n=0}^{\infty} A_n = \bigcup_{n=0}^{\infty} ran(a_n),$$

which is countable by Theorem 4.20. ■

Theorem 4.31. Any partition of a countable set has a set of representatives.

Proof. Let A be a countable set and let S be a partition of A. Since A is countable, there exists an injection $f : A \hookrightarrow \mathbb{N}$.

For each $C \in S$, define a_C to be the element in C such that $f(a_C) = \min\{f(x) \mid x \in C\}$. Then, the set $X = \{a_C \mid C \in S\}$ is a set of representatives, and since S is a partition, X contains exactly one element from each equivalence class.

Therefore, every partition of a countable set has a set of representatives. ■

4.3 Linear Orderings

Definition 4.7 (Similar Ordered Sets)**.** Totally ordered sets $(A, \leq)$ and $(B, \preceq)$ are *similar* (have the *same order type*) if they are isomorphic (see Definition 2.30).

Lemma 4.6. Every total ordering on a finite set is a well-ordering.

Proof. Let $(A, \leq)$ be a finite totally ordered set.

We proceed by induction on $|B|$, where $B \subseteq A$.

Base Case: If $|B| = 1$, then the only element of B is $\min B$.

Inductive Step: Assume that every subset $B \subseteq A$ with $|B| = n$ has a least element. Let $B \subseteq A$ with $|B| = n+1$ and write $B = \{b_0, b_1, \ldots, b_n\}$. Let $C = \{b_0, b_1, \ldots, b_{n-1}\}$. By the inductive hypothesis, C has a least element $\min C$.

If $b_n \leq \min C$, then b_n is the least element of B. Otherwise, $\min C$ is the least element of B.

Hence, by induction, every nonempty finite subset of A has a least element, i.e., $(A, \leq)$ is well-ordered. ■

Theorem 4.32 (Unique Finite Total Order)**.** If $(A_1, \leq_1)$ and $(A_2, \leq_2)$ are finite totally ordered sets with the same cardinality, then $(A_1, \leq_1)$ and $(A_2, \leq_2)$ are similar.

Proof. We proceed by induction on $n = |A_1| = |A_2|$.

Base Case: If $n = 0$, then $A_1 = A_2 = \emptyset$, and they are trivially similar via the isomorphism $\emptyset$.

Inductive Step: Assume the proposition holds whenever $|A_1| = |A_2| = n$. Now, consider $(A_1, \leq_1)$ and $(A_2, \leq_2)$ with $|A_1| = |A_2| = n+1$.

By Lemma 4.6, there exist $a_1 = \min A_1$ and $a_2 = \min A_2$.

Let $A_1' = A_1 - \{a_1\}$ and $A_2' = A_2 - \{a_2\}$. Then, $|A_1'| = |A_2'| = n$, and $(A_1', \leq_1)$ and $(A_2', \leq_2)$ are finite totally ordered sets.

By the inductive hypothesis, there exists an isomorphism $g : A_1' \hookrightarrow A_2'$.

Define $f = g \cup \{(a_1, a_2)\}$. Then, $f : A_1 \hookrightarrow A_2$ is an isomorphism between $(A_1, \leq_1)$ and $(A_2, \leq_2)$.

Therefore, by induction, the result follows. ■

Lemma 4.7. If $(A, \leq)$ is a totally ordered set, then $(A, \leq^{-1})$ is also a totally ordered set.

Proof. Take any $a, b \in A$. Since $\leq$ is total, either $a \leq b$ or $b \leq a$.

If $a \leq b$, then $b \leq^{-1} a$.

If $b \leq a$, then $a \leq^{-1} b$.

Therefore, $\leq^{-1}$ is a total ordering on A. ■

Lemma 4.8. Let $(A_1, \leq_1)$ and $(A_2, \leq_2)$ be totally ordered sets such that $A_1 \cap A_2 = \emptyset$. Define the relation $\leq$ on $A = A_1 \cup A_2$ by

$$a \leq b \iff (a, b \in A_1 \text{ and } a \leq_1 b) \vee (a, b \in A_2 \text{ and } a \leq_2 b) \vee (a \in A_1 \text{ and } b \in A_2).$$

Then, $\leq$ is a total ordering on A. The totally ordered set $(A, \leq)$ is called the *sum* of the totally ordered sets $(A_1, \leq_1)$ and $(A_2, \leq_2)$.

Proof. By Theorem 2.11 (assuming this exercise shows that such a relation is an ordering), $\leq$ is an ordering on A. Totality follows directly from the definition since any two elements $a, b \in A$ satisfy one of the conditions in the definition of $\leq$. ■

Lemma 4.9. Let $(A_1, \leq_1)$ and $(A_2, \leq_2)$ be totally ordered sets. Define the relation $\leq$ on $A = A_1 \times A_2$ by

$$(a_1, a_2) \leq (b_1, b_2) \iff (a_1 <_1 b_1) \vee (a_1 = b_1 \text{ and } a_2 \leq_2 b_2).$$

Then, $\leq$ is a total ordering on A. We call $\leq$ the *lexicographic ordering* (or *lexicographic product*) of $A_1 \times A_2$.

Proof. We will verify the properties of a total order.

- Transitivity: Assume $(a_1, a_2) \leq (b_1, b_2)$ and $(b_1, b_2) \leq (c_1, c_2)$.
  If $a_1 <_1 b_1$ or $b_1 <_1 c_1$, then by transitivity of $\leq_1$, $a_1 <_1 c_1$, so $(a_1, a_2) \leq (c_1, c_2)$.
  If $a_1 = b_1 = c_1$, then $a_2 \leq_2 b_2 \leq_2 c_2$, so $a_2 \leq_2 c_2$, and thus $(a_1, a_2) \leq (c_1, c_2)$.

- Antisymmetry: If $(a_1,a_2) \leq (b_1,b_2)$ and $(b_1,b_2) \leq (a_1,a_2)$, then $a_1 = b_1$ and $a_2 = b_2$, so $(a_1,a_2) = (b_1,b_2)$.
- Totality: For any $(a_1,a_2),(b_1,b_2) \in A$, either $a_1 <_1 b_1$, $a_1 = b_1$ and $a_2 \leq_2 b_2$, or $a_1 >_1 b_1$ (which would imply $(b_1,b_2) < (a_1,a_2)$). Therefore, $\leq$ is total.

■

Theorem 4.33 (Lexical Order)**.** Let $\langle (A_i, \leq_i) \mid i \in I \rangle$ be an indexed system of totally ordered sets where $I \subseteq \mathbb{N}$. Define the relation $\prec$ on $\prod_{i \in I} A_i$ by

$$f \prec g \iff \text{diff}(f,g) \neq \emptyset \text{ and } f_{i_0} <_{i_0} g_{i_0},$$

where

$$\text{diff}(f,g) = \{i \in I \mid f_i \neq g_i\} \quad \text{and} \quad i_0 = \min \text{diff}(f,g).$$

Then, $\prec$ is a total strict ordering on $\prod_{i \in I} A_i$. We call $\prec$ the *lexicographic ordering* of $\prod_{i \in I} A_i$.

Proof. We verify the properties of a total strict order.

- Transitivity: Assume $f \prec g$ and $g \prec h$. Let $i_0 = \min \text{diff}(f,g)$ and $j_0 = \min \text{diff}(g,h)$.
  If $i_0 < j_0$, then $f_{i_0} <_{i_0} g_{i_0} = h_{i_0}$, so $f \prec h$.
  If $i_0 = j_0$, then $f_{i_0} <_{i_0} g_{i_0} <_{i_0} h_{i_0}$, so $f_{i_0} <_{i_0} h_{i_0}$, and thus $f \prec h$.
  If $i_0 > j_0$, then $f_{j_0} = g_{j_0} <_{j_0} h_{j_0}$, so $f_{j_0} <_{j_0} h_{j_0}$, and since $j_0 = \min \text{diff}(f,h)$, we have $f \prec h$.
- Antisymmetry: Since $\prec$ is strict, it is irreflexive and antisymmetric by definition.
- Totality: For any $f \neq g$ in $\prod_{i \in I} A_i$, let $i_0 = \min \text{diff}(f,g)$. Then, either $f_{i_0} <_{i_0} g_{i_0}$ and $f \prec g$, or $g_{i_0} <_{i_0} f_{i_0}$ and $g \prec f$. Therefore, $\prec$ is total.

■

Definition 4.8 (Dense Ordered Set)**.** An ordered set $(X, \leq)$ is *dense* if

$$|X| \geq 2 \quad \text{and} \quad \forall a,b \in X,\ (a < b \implies \exists x \in X,\ a < x < b).$$

Definition 4.9 (Endpoints)**.** The least and greatest elements of a totally ordered set are called the *endpoints* of the set.

Theorem 4.34. Let $(P, \preceq)$ and $(Q, \leq)$ be countably infinite dense totally ordered sets without endpoints. Then, $(P, \preceq)$ and $(Q, \leq)$ are similar.

Proof. Let $\langle p_n \mid n \in \mathbb{N} \rangle$ be an injective sequence onto P, and let $\langle q_n \mid n \in \mathbb{N} \rangle$ be an injective sequence onto Q.

We define a *partial isomorphism* $h: P \to Q$ if h is a bijection between finite subsets of P and Q such that for all $p, p' \in dom(h)$,

$$p \preceq p' \iff h(p) \leq h(p').$$

Claim 4.3. Given a finite partial isomorphism h and elements $p \in P$ and $q \in Q$, there exists an extension h' of h such that $p \in dom(h')$ and $q \in ran(h')$.

Proof. Proof of Claim: Since P and Q are dense and have no endpoints, we can insert p and q into $dom(h)$ and $ran(h)$ respectively while preserving the order. The details involve considering where p and q fit relative to the elements in $dom(h)$ and $ran(h)$ and using the density to find suitable elements. ■

Using this claim, we can construct an increasing sequence of finite partial isomorphisms $\{h_n\}_{n\in\mathbb{N}}$ such that each h_n includes p_n and q_n. Define $h = \bigcup_{n\in\mathbb{N}} h_n$. Then h is an isomorphism between P and Q, showing that they are similar. ■

Theorem 4.35. Let $(P,\preceq)$ be a countably infinite totally ordered set, and let $(Q,\leq)$ be a countably infinite dense totally ordered set without endpoints. Then, there exists $h: P \hookrightarrow Q$ such that

$$\forall p, p' \in P,\ (p \prec p' \implies h(p) < h(p')).$$

Proof. Let $\langle\, p_n \mid n \in \mathbb{N} \,\rangle$ be an injective sequence onto P. If f is a partial isomorphism from P to Q with finite $dom(f)$, and if $p \in P$, there exists another partial isomorphism f_p from P to Q that extends f such that $p \in dom(f_p)$.

Then, one is able to make a sequence of compatible partial isomorphisms from P to Q recursively by

$$\begin{aligned} h_0 &= \emptyset \\ \forall n \in \mathbb{N}, \quad h_{n+1} &= (h_n)_{p_n} \end{aligned}$$

where $(h_n)_{p_n}$ is the extension of h_n such that $p_n \in dom([(h_n)_{p_n}])$. The rest is the same as the proof of Theorem 4.34. ■

4.4 Complete Linear Ordering

Definition 4.10 (Cut, Dedekind Cut, and Gap)**.** Let $(P,\leq)$ be a totally ordered set.

- A *cut* is a pair (A,B) of sets such that
  (i) $\{A,B\}$ is a partition of P.
  (ii) $\forall a \in A, \forall b \in B, a < b$
- A *Dedekind cut* is a cut (A,B) such that max$A$ does not exist.
- A *gap* is a cut (A,B) such that max$A$ and min$B$ do not exist.

Definition 4.11. Let $(P,\leq)$ be a totally ordered set with $\emptyset \subsetneq A \subseteq P$. We define the following:

- Bounded: The set A is *bounded* if it has both a lower bound and an upper bound.
- Bounded from Below: The set A is *bounded from below* if there exists a lower bound for A.
- Bounded from Above: The set A is *bounded from above* if there exists an upper bound for A.

Lemma 4.10 (Completeness $\Leftrightarrow$ No Gaps)**.** Let $(P,\leq)$ be a totally ordered set. Every nonempty subset $S \subseteq P$ that is bounded from above has a supremum if and only if $(P,\leq)$ contains no gaps.

Proof. We will prove the lemma by showing both implications.

($\Rightarrow$) Suppose, for contradiction, that $(P,\leq)$ has a gap (A,B). By definition of a gap:

- Every element $a \in A$ is less than every element $b \in B$.
- A is nonempty and B is nonempty.

Consider the set A. Since every $b \in B$ is an upper bound of A, A is bounded above. By assumption, A must have a supremum $\mu = \sup A$.

We analyze two cases:

(a) If $\mu \in A$, then $\mu = \max A$. However, this contradicts the existence of the gap (A,B), as there should be no maximum element in A.

(b) If $\mu \in B$, then μ would be the least element of B, i.e., $\mu = \min B$. This also leads to a contradiction because the gap (A,B) requires that there is no immediate successor or predecessor between A and B.

Both cases lead to contradictions, hence $(P,\leq)$ cannot have a gap.

($\Leftarrow$) Assume that $(P,\leq)$ contains a gap. We will show that there exists a nonempty subset $S \subseteq P$ that is bounded above but does not have a supremum.

Let S be a nonempty subset of P that is bounded above, but suppose S does not have a supremum. Define the following sets:

$$A \triangleq \{x \in P \mid \exists s \in S, x \leq s\}, \quad B \triangleq \{x \in P \mid \forall s \in S, x > s\}.$$

Claim 4.4. $\{A,B\}$ forms a partition of P.

Proof of Claim. Clearly, $A \cap B = \emptyset$ and $A \cup B = P$. If $A = P$, then S would have a maximum element, contradicting the assumption that S does not have a supremum. Similarly, $B \neq P$ because S is nonempty. Therefore, $\{A,B\}$ is a valid partition of P. ■

Claim 4.5. For all $a \in A$ and $b \in B$, $a < b$.

Proof of Claim. Take any $a \in A$ and $b \in B$. Since $a \in A$, there exists $s \in S$ such that $a \leq s$. Because $b \in B$, we have $s < b$. Therefore, $a < b$. ■

Claim 4.6. Neither $\max A$ nor $\min B$ exists.

Proof of Claim. Suppose $\min B$ exists. Let m' be an upper bound of S. If $m' \in S$, then $m' = \sup S$, which is a contradiction. Otherwise, m' must belong to B, implying $m \leq m'$, which would make $m = \sup S$, another contradiction. Thus, $\min B$ does not exist.

Similarly, assume $\max A$ exists. Since $S \subseteq A$, $\max A$ would be an upper bound of S. Any other upper bound M' of S must satisfy $M = M'$, leading to $\sup S = M$, a contradiction. Hence, $\max A$ does not exist. ■

Combining the above claims, (A,B) forms a gap in P, which contradicts the assumption that $(P,\leq)$ has no gaps. Therefore, if $(P,\leq)$ has no gaps, every nonempty subset $S \subseteq P$ that is bounded above must have a supremum.

■

Definition 4.12 (Complete Dense Totally Ordered Set)**.** Let $(P,\leq)$ be a dense totally ordered set. $(P,\leq)$ is said to be *complete* provided that every nonempty subset $S \subseteq P$ that is bounded from above has a supremum. Equivalently, $(P,\leq)$ has no gaps. (See Lemma 4.10.)

Theorem 4.36 (Completion)**.** Let $(P, \leq)$ be a dense totally ordered set without endpoints. Then, there exists a complete totally ordered set $(C, \preceq)$ such that:

(i) $P \subseteq C$.
(ii) For all $p, q \in P$, $p < q$ if and only if $p \prec q$.
(iii) For all $c, d \in C$, if $c \prec d$, then there exists $p \in P$ such that $c \prec p \prec d$. This means that P is dense in C.
(iv) C has no endpoints.

Moreover, such a complete totally ordered set $(C, \preceq)$ is unique up to isomorphism h that satisfies $\mathrm{Id}_P \subseteq h$. [1]

The complete totally ordered set $(C, \preceq)$ is referred to as the *completion* of $(P, \leq)$.

Proof. To construct the completion C, we utilize Dedekind cuts. First, observe that for any subset $B \subseteq P$, min$B$ exists if and only if there exists an element $p \in P$ such that $B = \{ x \in P \mid x \geq p \}$. Therefore, Dedekind cuts in $(P, \leq)$ fall into two categories:

(i) There exists a unique $p \in P$ such that $B = \{ x \in P \mid x \geq p \}$. In this case, we denote the cut as $[p]$.
(ii) (A, B) forms a gap, meaning there is no least element in B and no greatest element in A.

Note that for every $p \in P$, $[p]$ is a valid Dedekind cut of $(P, \leq)$.

We define the completion C and the order $\preceq$ on C as follows:

$$C \triangleq \{ (A, B) \mid (A, B) \text{ is a Dedekind cut of } (P, \leq) \}$$

$$(A, B) \preceq (A', B') \iff A \subseteq A'.$$

Claim 4.7. $(C, \preceq)$ is a totally ordered set.

Proof of Claim. It is clear that $(C, \preceq)$ is an ordered set. To establish totality, take any two Dedekind cuts (A, B) and (A', B') in C. Suppose, for contradiction, that they are incomparable; that is, $A - A' \neq \emptyset$ and $A' - A \neq \emptyset$. Let $a \in A - A'$ and $a' \in A' - A$. Then, $a < a'$ and $a' < a$, which is impossible due to the antisymmetry of the order. Therefore, (A, B) and (A', B') must be comparable. ■

Next, observe that for any $p, q \in P$ with $p < q$, the corresponding cuts satisfy $[p] \prec [q]$. This ensures that the embedding $P' = \{[p] \mid p \in P\}$ into C preserves the original order of P. Thus, $(P', \preceq |_{P' \times P'}) \cong (P, \leq)$.

We now demonstrate that $(C, \preceq)$ satisfies the properties required for the completion.

Claim 4.8. $(C, \preceq)$ is a densely ordered set.

Proof of Claim. Take any two elements $c = (A, B)$ and $d = (A', B')$ in C with $c \prec d$. Since $A \subsetneq A'$, there exists an element $p \in A' - A$. Because $(P, \leq)$ has no greatest element, p is not the least element of B', implying there exists $b \in B$ such that $b < p$.

Define the cut $[p] = (A'', B'')$. Since $b < p$, we have $A \subsetneq A''$ and $A'' \subsetneq A'$, thus $c \prec [p] \prec d$. This demonstrates that between any two distinct elements in C, there exists another element, confirming density. ■

Claim 4.9. $(C, \preceq)$ has no endpoints.

[1] In other words, if $(C, \preceq)$ and $(C^*, \preceq^*)$ both satisfy the above conditions, then there exists an isomorphism h between $(C, \preceq)$ and $(C^*, \preceq^*)$ such that for every $p \in P$, $h(p) = p$.

Proof of Claim. No Greatest Element: Take any $c = (A,B) \in C$. Since A has no greatest element, there exists $p \in A$ such that $p < a$ for some $a \in A$. Therefore, $[p] \prec c$, showing that c cannot be the greatest element.

No Least Element: Similarly, for any $c = (A,B) \in C$, there exists $p \in B$ such that p is not the least element of B. Thus, $c \prec [p]$, indicating that c cannot be the least element. ■

Claim 4.10. $(C, \preceq)$ is a complete totally ordered set.

Proof of Claim. Let $S \subseteq C$ be a nonempty set that is bounded above in C. Let (A_0, B_0) be an upper bound for S. Define:

$$A_S \triangleq \bigcup \{ A \mid (A,B) \in S \}, \quad B_S \triangleq \bigcap \{ B \mid (A,B) \in S \}.$$

The pair (A_S, B_S) forms a Dedekind cut since $B_S = P - A_S$. Moreover, A_S has no greatest element because if it did, that element would be a greatest element in some A for $(A,B) \in S$, contradicting the absence of a supremum for S.

Therefore, $(A_S, B_S) \in C$ and serves as the least upper bound (supremum) of S in C. Hence, $(C, \preceq)$ is complete. ■

Combining Claims 4.7, 4.8, 4.9, and 4.10, we conclude that $(C, \preceq)$ satisfies all the requirements stated in Theorem 4.36. Thus, the existence of such a completion is established.

Uniqueness: Suppose $(C, \preceq)$ and $(C^*, \preceq^*)$ are two complete completions of $(P, \leq)$. We will show that there exists an isomorphism $h : C \to C^*$ such that $h(p) = p$ for all $p \in P$.

Define for each $c \in C$, the set:

$$S_c \triangleq \{ p \in P \mid p \prec c \}, \quad S_{c^*} \triangleq \{ p \in P \mid p \prec^* c^* \}.$$

Since both C and C^* are complete, we can define $h(c) = \sup_{\preceq^*} S_c$. Similarly, define $h^{-1}(c^*) = \sup_{\preceq} S_{c^*}$.

- Well-Defined and Bijective: The mappings are well-defined due to completeness. For each $c \in C$, $h(c)$ is the unique supremum in C^*, and vice versa.
- Order-Preserving: If $c \preceq d$ in C, then $h(c) \preceq^* h(d)$ in C^*. This follows because $S_c \subseteq S_d$ implies $\sup S_c \preceq^* \sup S_d$.
- Inverse Property: Applying h and h^{-1} consecutively retrieves the original elements, ensuring that h is indeed an isomorphism.
- Identity on P: For each $p \in P$, $h(p) = p$ since $S_p = \{ x \in P \mid x \prec p \}$ and p is the supremum of S_p in both C and C^*.

Therefore, h is an isomorphism between $(C, \preceq)$ and $(C^*, \preceq^*)$ that fixes every element of P, proving the uniqueness of the completion up to isomorphism.

This completes the proof of Theorem 4.36. ■

Proposition 4.1. A dense totally ordered set $(P, \preceq)$ is complete if and only if every nonempty $S \subseteq P$ bounded from below has an infimum.

Proof. To establish the equivalence, we will leverage the concept of gaps and the previously established Lemma 4.10.

- Understanding Gaps in Inverse Order: Consider the inverse order $(P, \preceq^{\text{inv}})$, where $x \preceq^{\text{inv}} y$ if and only if $y \preceq x$ in $(P, \preceq)$. In this inverse ordering:
  – A pair (A, B) forms a *gap* in $(P, \preceq)$ if and only if (B, A) forms a gap in $(P, \preceq^{\text{inv}})$.
- Applying Lemma 4.10: By Lemma 4.10, a totally ordered set is complete if and only if it contains no gaps. Applying this to the inverse order, we deduce that:

$(P, \preceq)$ is complete $\iff$ Every nonempty set $S \subseteq P$ bounded above in $(P, \preceq^{\text{inv}})$ has a supremum in $(P, \preceq^{\text{inv}})$.

- Relating Boundedness in Original and Inverse Orders: Notice that a subset $S \subseteq P$ being *bounded above* in $(P, \preceq^{\text{inv}})$ is equivalent to S being *bounded from below* in $(P, \preceq)$. Moreover, the supremum of S in the inverse order corresponds to the infimum of S in the original order:

$$\sup_{\preceq^{\text{inv}}} S = \inf_{\preceq} S.$$

- Concluding the Equivalence: Combining the observations above, we conclude that:

$(P, \preceq)$ is complete $\iff$ Every nonempty subset $S \subseteq P$ that is bounded from below has an infimum in $(P, \preceq)$.

■

4.5 Cardinal Arithmetic

Definition 4.13 (Sum and Product of Two Cardinals)**.** Let $|A| = \kappa$ and $|B| = \lambda$.

- We write $|A \cup B| = \kappa + \lambda$ if $A \cap B$.
- We write $|A \times B| = \kappa \cdot \lambda$.

Justified by Theorem 4.24

Lemma 4.11. If $|A_1| = |A_2|$ and $|B_1| = |B_2|$, then $|A_1^{B_1}| = |A_2^{B_2}|$.

Proof. Let $f : A_1 \hookrightarrow\!\!\!\rightarrow A_2$ and $g : B_1 \hookrightarrow\!\!\!\rightarrow B_2$. Define the function $F : A_1^{B_1} \to A_2^{B_2}$ by

$$F(k) = f \circ k \circ g^{-1}.$$

Then, F is both injective and surjective. The commutative diagram below illustrates the mapping:

$$\begin{array}{ccc} B_1 & \xrightarrow{g} & B_2 \\ \downarrow{\scriptstyle k} & & \downarrow{\scriptstyle F(k)=f\circ k\circ g^{-1}} \\ A_1 & \xrightarrow{f} & A_2 \end{array}$$

Therefore, $|A_1^{B_1}| = |A_2^{B_2}|$. ■

Definition 4.14 (Exponentiation of Two Cardinals)**.** Let $|A| = \kappa$ and $|B| = \lambda$. The exponentiation of κ and λ, denoted by κ^λ, is defined as

$$\kappa^\lambda = |A^B|.$$

This definition is justified by Lemma 4.11.

Remark. Here are some fundamental properties regarding the sum, product, and exponentiation of cardinal numbers:

(i) $\kappa+\lambda=\lambda+\kappa$.
(ii) $\kappa+(\lambda+\mu)=(\kappa+\lambda)+\mu$.
(iii) $\kappa\leq\kappa+\lambda$.
(iv) If $\kappa_1\leq\kappa_2$ and $\lambda_1\leq\lambda_2$, then $\kappa_1+\lambda_1\leq\kappa_2+\lambda_2$.
(v) $\kappa\cdot\lambda=\lambda\cdot\kappa$.
(vi) $\kappa\cdot(\lambda\cdot\mu)=(\kappa\cdot\lambda)\cdot\mu$.
(vii) $\kappa\cdot(\lambda+\mu)=\kappa\cdot\lambda+\kappa\cdot\mu$.
(viii) $\kappa\leq\kappa\cdot\lambda$ if $\lambda>0$.
(ix) If $\kappa_1\leq\kappa_2$ and $\lambda_1\leq\lambda_2$, then $\kappa_1\cdot\lambda_1\leq\kappa_2\cdot\lambda_2$.
(x) $\kappa+\kappa=2\cdot\kappa$.
(xi) $\kappa\leq\kappa^\lambda$ if $\lambda>0$.
(xii) $\lambda\leq\kappa^\lambda$ if $\kappa>1$.
(xiii) If $\kappa_1\leq\kappa_2$ and $\lambda_1\leq\lambda_2$, then $\kappa_1^{\lambda_1}\leq\kappa_2^{\lambda_2}$.
(xiv) $\kappa\cdot\kappa=\kappa^2$.

Theorem 4.37 (Cardinal Exponentials)**.** Let κ,λ,μ be cardinal numbers.

(i) $\kappa^{\lambda+\mu}=\kappa^\lambda\cdot\kappa^\mu$
(ii) $(\kappa^\lambda)^\mu=\kappa^{\lambda\cdot\mu}$
(iii) $(\kappa\cdot\lambda)^\mu=\kappa^\mu\cdot\lambda^\mu$

Proof. Let $\kappa=|K|$, $\lambda=|L|$, and $\mu=|M|$.

(i) Assume $L\cap N=\emptyset$. Then, we may define $F:K^L\times K^M\hookrightarrow K^{L\cup M}$ by $(f,g)\mapsto f\cup g$.
(ii) Define $F:(K^L)^M\hookrightarrow K^{L\times M}$ by $f\mapsto\{\,((\ell,m),f_m(\ell))\,|\,m\in M,\,\ell\in L\,\}$.
(iii) Define $F:K^M\times L^M\hookrightarrow(K\times L)^M$ by $(f_1,f_2)\mapsto\{\,(m,(f_1(m),f_2(m)))\,|\,m\in M\,\}$.

■

Theorem 4.38 (Cantor's Theorem)**.** For every set X, $|X|<|\mathscr{P}(X)|$.

Proof. Consider the function $f:X\to\mathscr{P}(X)$ defined by $f(x)=\{x\}$. This function is injective because if $f(x)=f(y)$, then $\{x\}=\{y\}$, implying $x=y$. Therefore, $|X|\leq|\mathscr{P}(X)|$.

To show that $|X|<|\mathscr{P}(X)|$, assume for contradiction that there exists a surjective function $f:X\to\mathscr{P}(X)$. Define the set

$$S\triangleq\{\,x\in X\,|\,x\notin f(x)\,\}.$$

Since f is surjective, there exists some $z\in X$ such that $f(z)=S$. Now, consider whether $z\in S$:

- If $z\in S$, then by definition of S, $z\notin f(z)=S$, which is a contradiction.
- If $z\notin S$, then by definition of S, $z\in f(z)=S$, which is also a contradiction.

Thus, no such surjective function f can exist, and $|X|<|\mathscr{P}(X)|$. ■

Theorem 4.39. For every set X, $|\mathscr{P}(X)|=2^{|X|}$.

Proof. For each subset $S \subseteq X$, define its *characteristic function* $\chi_S : X \to \{0,1\}$ by

$$\chi_S(x) = \begin{cases} 1 & \text{if } x \in S, \\ 0 & \text{if } x \notin S. \end{cases}$$

Then, define the function $F : \mathscr{P}(X) \hookrightarrow 2^X$ by

$$F(S) = \chi_S.$$

This function is bijective because each subset S corresponds uniquely to its characteristic function χ_S, and every function $f : X \to \{0,1\}$ corresponds to the subset $S = \{\, x \in X \mid f(x) = 1 \,\}$. Therefore, $|\mathscr{P}(X)| = |2^X| = 2^{|X|}$. ■

Corollary. For any class of sets S, there exists a set Y such that for all $X \in S$, $|X| < |Y|$.

Proof. Let $Y \triangleq \mathscr{P}(\bigcup S)$. By Theorem 4.38 and Theorem 4.3, we have $|Y| = 2^{|\bigcup S|} > |\bigcup S| \geq |X|$ for all $X \in S$. Thus, such a set Y exists. ■

Proposition 4.2. For every cardinal number κ, $\kappa^\kappa \leq 2^{\kappa \cdot \kappa}$.

Proof. Since $\kappa \leq 2^\kappa$, we have

$$\kappa^\kappa \leq (2^\kappa)^\kappa = 2^{\kappa \cdot \kappa}$$

by Theorem 4.37. ■

Proposition 4.3. If $|A| \leq |B|$ and $A \neq \emptyset$, then there exists $f : B \twoheadrightarrow A$.

Proof. Fix some $a \in A$. Let $g : A \hookrightarrow B$. Then, define $f : B \twoheadrightarrow A$ by

$$f(b) \triangleq \begin{cases} g^{-1}(b) & \text{if } b \in \operatorname{ran} g, \\ a & \text{otherwise.} \end{cases}$$

■

Proposition 4.4. If there exists $g : B \twoheadrightarrow A$, then $2^{|A|} \leq 2^{|B|}$.

Proof. Let $g : B \twoheadrightarrow A$. Define $f : \mathscr{P}(A) \to \mathscr{P}(B)$ by

$$f(X) = g^{-1}[X].$$

Then, f is injective. ■

Definition 4.15 (Dedekind Infinite Set)**.** A set X is called *Dedekind infinite* if there exists an injection from X onto its proper subset. Conversely, a set X is called *Dedekind finite* if X is not Dedekind infinite.

Proposition 4.5. A Dedekind infinite set is infinite.

Proof. Let X be a set and suppose there exists $f : X \hookrightarrow X$ with $f[X] \subsetneq X$. Assume, for the sake of contradiction, that $|X| = n$ for some $n \in \mathbb{N}$. Since f is injective, $|f[X]| = |X| = n$, which contradicts Lemma 4.4. ■

Proposition 4.6. Every countably infinite set is Dedekind infinite.

Proof. It suffices to show that $\mathbb{N}$ is Dedekind infinite. Consider the function $f:\mathbb{N}\to\mathbb{N}$ defined by $f(n)=n+1$. By Theorem 3.5, f is injective and $0\notin\operatorname{ran} f$. Hence, $\mathbb{N}$ is Dedekind infinite. ■

Proposition 4.7. If X has a countably infinite subset, then X is Dedekind infinite.

Proof. Let $Y\subseteq X$ with $|Y|=\aleph_0$. By Proposition 4.6, there exists $f:Y\hookrightarrow Y$ such that $\operatorname{ran} f\subsetneq Y$. Define $g\triangleq f\cup\mathrm{Id}_{X-Y}$. Then, $g:X\hookrightarrow X$ and $Y-\operatorname{ran} f\subseteq X-\operatorname{ran} g$. Therefore, X is Dedekind infinite. ■

Proposition 4.8. If X is Dedekind infinite, then X has a countably infinite subset.

Proof. Let $f:X\hookrightarrow X$ with $\operatorname{ran} f\subsetneq X$. Choose $x\in X-\operatorname{ran} f$. Define the sequence $\langle x_n\rangle_{n\in\mathbb{N}}$ by

$$\begin{aligned} x_0 &\triangleq x,\\ x_{n+1} &\triangleq f(x_n),\quad \forall n\in\mathbb{N}. \end{aligned}$$

Let $\mathbf{P}(n)$ be the property "$\forall m<n,\ x_m\neq x_n$." $\mathbf{P}(0)$ is vacuously true, and $\mathbf{P}(1)$ follows from $x_0\notin\operatorname{ran} f$.

Assume $\mathbf{P}(n)$ holds for some $n\geq 1$. Then, for each $0\leq m<n$,

$$x_n=f(x_{n-1})\neq f(x_{m-1})=x_m,$$

since f is injective. Additionally, $x_0\neq x_n$ because $x_0\notin\operatorname{ran} f$. Hence, $\mathbf{P}(n+1)$ holds. By induction, $\langle x_n\rangle_{n\in\mathbb{N}}$ is injective, and thus $\{x_n\mid n\in\mathbb{N}\}$ is a countably infinite subset of X. ■

Remark. Proposition 4.7 and Proposition 4.8 establish that a set X is Dedekind infinite if and only if X has a countably infinite subset. In Axiom of Choice, we will show that a set is Dedekind infinite if and only if it is infinite using Axiom of Choice. (See Theorem 7.4.)

Proposition 4.9. If A and B are Dedekind finite, then $A\cup B$ is Dedekind finite.

Proof. Suppose, for the sake of contradiction, that $A\cup B$ is Dedekind infinite. Then, by Proposition 4.8, there exists $C\subseteq A\cup B$ such that C is countably infinite. Since at least one of $A\cap C$ and $B\cap C$ must be countably infinite, by Proposition 4.7, either A or B is Dedekind infinite, which contradicts the assumption that both A and B are Dedekind finite. Therefore, $A\cup B$ must be Dedekind finite. ■

Proposition 4.10. If A and B are Dedekind finite, then $A\times B$ is Dedekind finite.

Proof. Suppose, for the sake of contradiction, that $A\times B$ is Dedekind infinite. Then, by Proposition 4.8, there exists $C\subseteq A\times B$ such that C is countably infinite. Let $A'\triangleq\operatorname{dom} C$ and $B'\triangleq\operatorname{ran} C$. If both A' and B' were finite, then $C\subseteq A'\times B'$ would be finite by Theorem 4.13 and Theorem 4.7.

Without loss of generality, assume A' is infinite. Let $f:\mathbb{N}\twoheadrightarrow C$. Define $g:\mathbb{N}\twoheadrightarrow A'$ by

$$g(n)=a'\quad\text{where } (a',b')=f(n).$$

By Theorem 4.18, $\operatorname{ran} g=A'$ is countably infinite. Therefore, by Proposition 4.7, A is Dedekind infinite, which contradicts the assumption that A is Dedekind finite. Hence, $A\times B$ must be Dedekind finite. ■

5 Well-Ordered Sets

Notation 5.1 (Least Transfinite Number)**.** Let $\omega \triangleq \mathbb{N}$ be the least transfinite ordinal. We define:

- $\omega + 0 = \omega$
- $\omega + (n+1) = S(\omega + n)$ for each $n \in \mathbb{N}$

Using this recursion, we construct ordinals such as:

$$\omega \cdot 2 = \omega + \omega = \{0, 1, 2, \ldots, \omega, \omega+1, \omega+2, \ldots\},$$

$$\omega \cdot \omega = \{0, 1, \ldots, \omega, \omega+1, \ldots, \omega \cdot 2, \ldots, \omega \cdot 3, \ldots\}.$$

These sets are totally ordered by $\in$, and the ordering is a well-ordering.

Definition 5.1 (Initial Segment)**.**

- Let $(L, \leq)$ be a totally ordered set. A set $S \subsetneq L$ is called an *initial segment* of L if

$$\forall a \in S, \forall x \in L,\ (x < a \implies x \in S).$$

- Let $(W, \leq)$ be a well-ordered set. For any $a \in W$, the set

$$W[a] \triangleq \{x \in W \mid x < a\}$$

is called the *initial segment of W given by a*.

Definition 5.2 (Increasing Function)**.** A function f on a totally ordered set $(L, \leq)$ into itself is *strictly increasing* if

$$\forall x_1, x_2 \in L,\ (x_1 < x_2 \implies f(x_1) < f(x_2)).$$

Definition 5.3 (Smaller Order Type)**.** Let $(W_1, \leq_1)$ and $(W_2, \leq_2)$ be well-ordered sets. We say that W_1 has a *smaller order type* than W_2 if W_1 is isomorphic to an initial segment of W_2.

Lemma 5.1. Let $(W, \leq)$ be a well-ordered set, and let S be an initial segment of $(W, \leq)$. Then, there exists an element $a \in W$ such that $S = W[a]$.

Proof. Let $X \triangleq W - S$. Since $S \subsetneq W$, $X \neq \emptyset$. By the well-ordering property, X has a least element, say $a = \min X$. For any $x \in W$:

$$x \in S \iff x < a.$$

Therefore, $S = W[a]$. ■

Lemma 5.2. Let $(W, \leq)$ be a well-ordered set, and let $f : W \to W$ be a strictly increasing function. Then, for all $x \in W$, $x \leq f(x)$.

Proof. Assume, for contradiction, that the set

$$X \triangleq \{x \in W \mid f(x) > x\}$$

is nonempty. Since W is well-ordered, X has a least element, say $a = \min X$. By definition, $f(a) > a$. Since f is strictly increasing, applying f to both sides yields:

$$f(f(a)) > f(a).$$

This implies that $f(a) \in X$, contradicting the minimality of a because $f(a) > a$ would require $f(a)$ to be greater than itself in X, which is impossible. Hence, X must be empty, and $x \leq f(x)$ for all $x \in W$. ■

Corollary. Let $(W, \leq)$ be a well-ordered set. Then:

(i) No Well-Ordered Set is Isomorphic to an Initial Segment of Itself: No well-ordered set W is isomorphic to any of its proper initial segments.
(ii) Unique Automorphism: The identity map Id_W is the only automorphism of W.
(iii) Uniqueness of Isomorphism Between Well-Ordered Sets: If W_1 and W_2 are isomorphic well-ordered sets, then the isomorphism between them is unique.

Proof.

(i) No Well-Ordered Set is Isomorphic to an Initial Segment of Itself:
Suppose, for contradiction, that there exists an isomorphism $f : W \to W[a]$ for some $a \in W$. Then, $f(a) \in W[a]$, which implies $f(a) < a$. However, by Lemma 5.2, since f is strictly increasing, $a \leq f(a)$, leading to a contradiction. Therefore, no such isomorphism can exist.
(ii) Unique Automorphism:
Let f be an automorphism of W. Since both f and f^{-1} are strictly increasing, by Lemma 5.2, for all $x \in W$, $x \leq f(x)$ and $x \leq f^{-1}(x)$. This implies $f(x) \leq x$. Combining these, we have $x \leq f(x) \leq x$, hence $f(x) = x$ for all $x \in W$. Therefore, the only automorphism of W is the identity map Id_W.
(iii) Uniqueness of Isomorphism Between Well-Ordered Sets:
Suppose f and g are isomorphisms between W_1 and W_2. Then, $f \circ g^{-1}$ is an automorphism of W_2. By part (ii), $f \circ g^{-1} = \mathrm{Id}_{W_2}$, which implies $f = g$. Hence, the isomorphism between W_1 and W_2 is unique.

■

Theorem 5.1 (Comparability of Well-Ordered Sets)**.** Let $(W_1, \leq_1)$ and $(W_2, \leq_2)$ be well-ordered sets. Then, exactly one of the following holds:

(i) $(W_1, \leq_1)$ and $(W_2, \leq_2)$ are isomorphic.
(ii) $(W_1, \leq_1)$ is isomorphic to an initial segment of $(W_2, \leq_2)$.
(iii) $(W_2, \leq_2)$ is isomorphic to an initial segment of $(W_1, \leq_1)$.

Moreover, in each case, the isomorphism is unique.

Proof. The cases (i), (ii), and (iii) are mutually exclusive by Section 5 (i). Additionally, the uniqueness of the isomorphism follows from Section 5 (iii). Therefore, it suffices to show that one of the cases must hold.

Define the relation

$$f \triangleq \{\, (x, y) \in W_1 \times W_2 \mid W_1[x] \text{ is isomorphic to } W_2[y] \,\}.$$

We need to show that f is an isomorphism between W_1 and W_2, or that one of the well-ordered sets is isomorphic to an initial segment of the other.

Claim 5.1. f is an injective function.

Proof of Claim. Suppose there exist $x, x' \in W_1$ such that $f(x) = f(x') = y \in W_2$. Then, $W_1[x]$ and $W_1[x']$ are both isomorphic to $W_2[y]$. Since isomorphism between well-ordered sets preserves order type uniquely, $x = x'$. Therefore, f is injective. ■

Claim 5.2. f is a strictly increasing function.

Proof of Claim. Take any $x, x' \in W_1$ with $x <_1 x'$. Let h be the isomorphism between $W_1[x']$ and $W_2[f(x')]$. The restriction of h to $W_1[x]$ is an isomorphism between $W_1[x]$ and $W_2[h(x)]$. By Claim 5.1, this implies $f(x) = h(x) <_2 f(x')$. Hence, f is strictly increasing. ■

By Claim 5.2 and Lemma 2.7 (assuming it states that a strictly increasing injective function between well-ordered sets is an isomorphism onto its image), f is an isomorphism between $\operatorname{dom} f$ and $\operatorname{ran} f$. We now show that either $\operatorname{dom} f = W_1$ or $\operatorname{ran} f = W_2$.

Claim 5.3. If $\operatorname{dom} f \neq W_1$, then $\operatorname{ran} f = W_2$.

Proof of Claim. Let $S \triangleq \operatorname{dom} f$. If $S \neq W_1$, then S is an initial segment of W_1 by Lemma 5.1. Suppose $\operatorname{ran} f \neq W_2$. Then, $\operatorname{ran} f$ is an initial segment of W_2. Let $a \in W_1$ and $b \in W_2$ be such that $S = W_1[a]$ and $\operatorname{ran} f = W_2[b]$. Since f is an isomorphism between $W_1[a]$ and $W_2[b]$, it must map the least element of $W_1[a]$ to the least element of $W_2[b]$, and so on. However, this leads to a contradiction because a would have to be in $S = W_1[a]$, implying $a \in \operatorname{ran} f = W_2[b]$, which is impossible as f maps elements of W_1 to W_2. Therefore, $\operatorname{ran} f = W_2$. ■

By Claim 5.2 and Claim 5.3, one of the cases (i), (ii), or (iii) must hold. Thus, exactly one of the conditions in the theorem statement holds, completing the proof. ■

Proposition 5.1. Give an example of a totally ordered set $(L, \leq)$ and an initial segment S of L which is not of the form $\{ x \in L \mid x < a \}$ for all $a \in L$.

Proof. Consider a dense totally ordered set $(L, \leq)$ such as $(\mathbb{Q}, \leq)$. Let $S = \{ x \in \mathbb{Q} \mid x \leq 0 \}$. This set S is an initial segment of $\mathbb{Q}$, but it is not of the form $\{ x \in \mathbb{Q} \mid x < a \}$ for any $a \in \mathbb{Q}$.

Reasoning: If S were equal to $\{ x \in \mathbb{Q} \mid x < a \}$ for some $a \in \mathbb{Q}$, then there would exist $x \in \mathbb{Q}$ such that $x < a < y$ for some $y \in \mathbb{Q}$. However, since $\mathbb{Q}$ is dense, there exists a rational number x' with $a < x' < y$, which implies $x' \notin S$, contradicting the assumption that S includes all elements less than a. Therefore, such an a cannot exist, and S is not of the form $\{ x \in L \mid x < a \}$ for any $a \in L$. ■

Proposition 5.2. $\omega + 1$ is not isomorphic to ω (in the well-ordering by $\in$).

Proof. The well-ordered set ω is an initial segment of $\omega + 1$, but they are not isomorphic by Section 5 (i). Specifically, $\omega + 1$ contains an additional element beyond all elements of ω, preventing any isomorphism from ω to $\omega + 1$. ■

Proposition 5.3 (6.1.3)**.** There exist $2^{\aleph_0}$ well-orderings of $\mathbb{N}$.

Proof. Let S be the set of all well-orderings of $\mathbb{N}$. The cardinality of the set of all relations on $\mathbb{N}^2$ is $|\mathscr{P}(\mathbb{N}^2)| = |\mathscr{P}(\mathbb{N})| = 2^{\aleph_0}$ by Theorem 4.19 and Theorem 4.39. Hence, $|S| \leq 2^{\aleph_0}$.

Let $T \triangleq \{ f \in \mathbb{N}^{\mathbb{N}} \mid f : \mathbb{N} \hookrightarrow \mathbb{N} \}$. Define $F : T \to \mathscr{P}(\mathbb{N}^2)$ by

$$F(f) = \{ (f(m), f(n)) \mid m, n \in \mathbb{N} \wedge m \leq n \}.$$

For each $f \in T$, $(\mathbb{N}, \leq)$ and $(\mathbb{N}, F(f))$ are isomorphic, thus F is injective into S. For each $R \in S$, there exists a unique $f \in T$ defined by

$$f(n) = \min_R (\mathbb{N} - \{f(0), f(1), \ldots, f(n-1)\})$$

for all $n \in \mathbb{N}$. Hence, $|T| = |S|$.

Now, define $\sigma : \mathscr{P}(\mathbb{N}) \to T$ by

$$\sigma_X(2n) = \begin{cases} 2n & \text{if } n \notin X, \\ 2n+1 & \text{if } n \in X, \end{cases} \quad \text{and} \quad \sigma_X(2n+1) = \begin{cases} 2n+1 & \text{if } n \notin X, \\ 2n & \text{if } n \in X. \end{cases}$$

for each $n \in \mathbb{N}$. It is evident that σ is injective; hence

$$|T| \geq |\mathscr{P}(\mathbb{N})| = 2^{\aleph_0}.$$

By the (Cantor–Bernstein Theorem), $|S| = |T| = 2^{\aleph_0}$. ■

Proposition 5.4. For every infinite subset A of $\mathbb{N}$, $(A, \leq \cap A^2) \cong (\mathbb{N}, \leq)$.

Proof. Clearly, $(A, \leq \cap A^2)$ is well-ordered as a subset of $\mathbb{N}$ with the inherited order. Noting that every initial segment of A and $\mathbb{N}$ is finite, by Theorem 5.1, the only possibility is that A and $\mathbb{N}$ are isomorphic. Therefore, $(A, \leq \cap A^2) \cong (\mathbb{N}, \leq)$. ■

5.1 Ordinal Numbers

Definition 5.4 (Transitive Set)**.** A set T is *transitive* if every element of T is a subset of T, i.e.,

$$\forall u \forall v (u \in v \wedge v \in T \implies u \in T).$$

Definition 5.5 (Ordinal Number)**.** A set α is an *ordinal number* (or *ordinal*) if

(i) α is transitive,
(ii) α is well-ordered by $\in_\alpha = \{ (x, y) \in \alpha^2 \mid x \in y \}$.

Notation 5.2. We denote that α is an ordinal by writing $\alpha \in \mathrm{Ord}$. This notation is purely symbolic and does not imply that Ord is a set containing all ordinals, as such a set does not exist due to foundational set-theoretic reasons (see Theorem 5.2).

Notation 5.3. We define $\omega \triangleq \mathbb{N}$. (See Notation 5.1)

Lemma 5.3 (Successor of an Ordinal is an Ordinal)**.** If α is an ordinal number, then its successor $S(\alpha)$ is also an ordinal number.

Proof. Since α is transitive, the successor $S(\alpha) = \alpha \cup \{\alpha\}$ inherits transitivity. Additionally, $S(\alpha)$ is well-ordered by the membership relation $\in_{S(\alpha)}$, as it extends the well-ordering of α with the new element α. ■

Notation 5.4. The successor of an ordinal α is denoted by $\alpha + 1$.

Definition 5.6 (Successor and Limit Ordinals)**.** For an ordinal $\alpha \in \text{Ord}$:

- α is a *successor ordinal* if there exists an ordinal β such that $\alpha = \beta + 1$.
- If α is not a successor ordinal, it is called a *limit ordinal*.

Notation 5.5. For any ordinals α and β, we define $\alpha < \beta$ precisely when $\alpha \in \beta$.

Lemma 5.4. For every ordinal $\alpha \in \text{Ord}$, it holds that $\alpha \notin \alpha$.

Proof. Suppose, for contradiction, that $\alpha \in \alpha$. This would violate the asymmetry property of the well-ordering $\in_\alpha$, as it would imply $\alpha < \alpha$, which is impossible. ■

Lemma 5.5. If $\alpha \in \text{Ord}$ and $x \in \alpha$, then $x \in \text{Ord}$.

Proof. Let $x \in \alpha$. To show that x is transitive, consider any $u \in v \in x$. Since α is transitive and $v \in \alpha$, it follows that $u \in \alpha$. Therefore, $u \in x$, establishing the transitivity of x.

Additionally, the relation $\in_x = \in_\alpha \cap x^2$ inherits the well-ordering from α, ensuring that x is well-ordered by $\in_x$. Thus, x satisfies the definition of an ordinal. ■

Corollary (Ordinals as Sets of Smaller Ordinals)**.** For any ordinal α, it holds that

$$\alpha = \{\, \beta \mid \beta \text{ is an ordinal number with } \beta < \alpha \,\}.$$

Lemma 5.6. Let α and β be ordinal numbers. Then,

$$\alpha \subsetneq \beta \iff \alpha \in \beta.$$

Proof. ($\Rightarrow$) Assume $\alpha \subsetneq \beta$. Since β is well-ordered, the set $\beta - \alpha$ is non-empty and has a least element under $\in_\beta$, say γ. By the minimality of γ, it must hold that $\gamma = \alpha$, implying $\alpha \in \beta$.

($\Leftarrow$) Conversely, if $\alpha \in \beta$, then by the definition of ordinals, α is a subset of β. Moreover, since $\alpha \notin \alpha$ (from Lemma 5.4), it follows that α is a proper subset of β, i.e., $\alpha \subsetneq \beta$.

■

Theorem 5.2 (Basic Properties of Ordinals)**.** Let α, β, and γ be ordinal numbers. Then:

(i) If $\alpha < \beta$ and $\beta < \gamma$, then $\alpha < \gamma$.
(ii) It is not possible for both $\alpha < \beta$ and $\beta < \alpha$ to hold simultaneously.
(iii) For any two ordinals α and β, exactly one of the following is true:
  (a) $\alpha < \beta$,
  (a) $\alpha = \beta$, or
  (a) $\beta < \alpha$.
(iv) Every nonempty set of ordinal numbers has a least element under the well-ordering $\leq$.
(v) For any set X of ordinal numbers, there exists an ordinal α' such that $\alpha' \notin X$.

Proof. (i) Transitivity of Order: If $\alpha < \beta$ and $\beta < \gamma$, then by definition, $\alpha \in \beta$ and $\beta \in \gamma$. Since $\in$ is transitive, it follows that $\alpha \in \gamma$, hence $\alpha < \gamma$.

(ii) Irreflexivity of Order: Suppose for contradiction that both $\alpha < \beta$ and $\beta < \alpha$ hold. Then, $\alpha \in \beta$ and $\beta \in \alpha$. Given that α is transitive and $\beta \in \alpha$, it would imply $\alpha \in \alpha$, which contradicts Lemma 5.4.

(iii) Trichotomy Property: For any two ordinals α and β, consider $\gamma = \alpha \cap \beta$. If $\gamma = \alpha$, then $\alpha \subseteq \beta$, leading to either $\alpha = \beta$ or $\alpha \in \beta$ (i.e., $\alpha < \beta$). Similarly, if $\gamma = \beta$, then $\beta \subseteq \alpha$, resulting in either $\beta = \alpha$ or $\beta \in \alpha$ (i.e., $\beta < \alpha$). The case where γ is a proper subset of both α and β leads to a contradiction, as it would imply an element is less than itself.

(iv) Well-Ordering of Ordinals: Let A be a nonempty set of ordinals. By the well-ordering property, A contains a least element under $\leq$, ensuring that every nonempty collection of ordinals is well-ordered.

(v) Existence of Larger Ordinals: Given any set X of ordinals, consider the union $\bigcup X$. By Lemma 5.5 and Definition 5.4, $\bigcup X$ is an ordinal. Define $\alpha' = S(\bigcup X)$, the successor of $\bigcup X$. Since α' contains all elements of $\bigcup X$ and an additional element, it follows that $\alpha' \notin X$, satisfying the required condition.

■

Notation 5.6. The corollary Section 5.1 ensures that each ordinal is precisely the collection of all smaller ordinals, providing a clear structural understanding of ordinals as cumulative hierarchies.

Definition 5.7 (Supremum of a Set of Ordinals)**.** For any set X of ordinal numbers, the *supremum* (or least upper bound) of X is defined as

$$\sup X \triangleq \bigcup X.$$

Notation 5.7. The definition Definition 5.7 is justified by the following observations:

(i) If $\alpha \in X$, then $\alpha \in \sup X$, and since α is transitive, $\alpha \subseteq \sup X$. This implies $\alpha \leq \sup X$.

(ii) For any ordinal γ such that $\alpha \leq \gamma$ for all $\alpha \in X$, it follows that $\sup X \subseteq \gamma$, hence $\sup X \leq \gamma$.

Notation 5.8. For any ordinal $\alpha \in \mathrm{Ord}$, if $x \in \bigcup \alpha$, then $x \in y \in \alpha$ for some y, and since α is transitive, it follows that $x \in \alpha$. Therefore, $\bigcup \alpha \subseteq \alpha$.

Proposition 5.5 (Finite Ordinals are Natural Numbers)**.** An ordinal α is finite if and only if $\alpha \in \mathbb{N}$.

Proof.

($\Rightarrow$) Assume α is a finite ordinal. Suppose, for contradiction, that $\alpha \notin \mathbb{N}$. By the trichotomy property (Theorem 5.2), $\omega \subseteq \alpha$, which would imply that α is infinite, contradicting the assumption that α is finite. Therefore, $\alpha \in \mathbb{N}$.

($\Leftarrow$) Conversely, every natural number $n \in \mathbb{N}$ can be identified with the ordinal representing the set $\{0, 1, 2, \ldots, n-1\}$. Since these sets are finite and satisfy the transitivity and well-ordering conditions, it follows that every $n \in \mathbb{N}$ is a finite ordinal.

■

Proposition 5.6. A set X is transitive if and only if $X \subseteq \mathscr{P}(X)$.

Proof. By definition, a set X is transitive if every element of X is also a subset of X. That is,

$$\forall x \in X, \quad x \subseteq X.$$

The power set $\mathscr{P}(X)$ consists of all subsets of X. Therefore, if every element $x \in X$ is a subset of X, then $x \in \mathscr{P}(X)$. This means $X \subseteq \mathscr{P}(X)$.

Conversely, if $X \subseteq \mathscr{P}(X)$, then every element $x \in X$ satisfies $x \in \mathscr{P}(X)$, which implies $x \subseteq X$. Thus, X is transitive.

Therefore, X is transitive if and only if $X \subseteq \mathscr{P}(X)$. ■

Proposition 5.7. A set X is transitive if and only if $\bigcup X \subseteq X$.

Proof. (Necessity) Suppose X is transitive. Let $u \in \bigcup X$. Then there exists some $x \in X$ such that $u \in x$. Since $x \in X$ and X is transitive, $x \subseteq X$, so $u \in X$. Therefore, $\bigcup X \subseteq X$.

(Sufficiency) Conversely, suppose $\bigcup X \subseteq X$. Let $u \in v \in X$. Then $u \in \bigcup X$, and by assumption, $u \in X$. This shows that every element of an element of X is also in X, so X is transitive.

Thus, X is transitive if and only if $\bigcup X \subseteq X$. ■

Proposition 5.8.

(i) If X and Y are transitive, then $X \cup Y$ is transitive.

(ii) If X and Y are transitive, then $X \cap Y$ is transitive.

(iii) If Y is transitive and $S \subseteq \mathscr{P}(Y)$, then $Y \cup S$ is transitive.

(iv) There exist sets X and Y such that $X \in Y$, Y is transitive, but X is not transitive.

(v) There exist sets X and Y such that $X \subseteq Y$, Y is transitive, but X is not transitive.

Proof.

(i) Since X and Y are transitive, we have $\bigcup X \subseteq X$ and $\bigcup Y \subseteq Y$. Then,

$$\bigcup (X \cup Y) = \bigcup X \cup \bigcup Y \subseteq X \cup Y.$$

Therefore, $X \cup Y$ is transitive.

(ii) The intersection $X \cap Y$ consists of all elements common to both X and Y. Since both X and Y are transitive, any element $x \in X \cap Y$ satisfies $x \subseteq X$ and $x \subseteq Y$. Thus, $x \subseteq X \cap Y$, so $\bigcup (X \cap Y) \subseteq X \cap Y$, and $X \cap Y$ is transitive.

(iii) Let $u \in v \in Y \cup S$. We consider two cases:

- If $v \in Y$, since Y is transitive, $u \in Y \subseteq Y \cup S$.
- If $v \in S$, then $v \subseteq Y$ because $S \subseteq \mathscr{P}(Y)$. Therefore, $u \in Y \subseteq Y \cup S$.

In both cases, $u \in Y \cup S$, so $Y \cup S$ is transitive.

(iv) Let $X = \{\{\emptyset\}\}$ and $Y = \{\emptyset, \{\emptyset\}, X\}$. Then:

$$\bigcup Y = \emptyset \cup \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} \subseteq Y.$$

Thus, Y is transitive. However,

$$\bigcup X = \{\emptyset\} \not\subseteq X,$$

so X is not transitive.

(v) Let $X = \{\{\emptyset\}\}$ and $Y = \{\emptyset, \{\emptyset\}\}$. Clearly, $X \subseteq Y$. We have:

$$\bigcup Y = \emptyset \cup \{\emptyset\} = \{\emptyset\} \subseteq Y,$$

so Y is transitive. As before, X is not transitive because $\bigcup X = \{\emptyset\} \not\subseteq X$.

Thus, $X \subseteq Y$, Y is transitive, but X is not transitive.

■

Proposition 5.9. If every set $X \in S$ is transitive, then $\bigcup S$ is transitive.

Proof. Let $u \in v \in \bigcup S$. Then there exists some $X \in S$ such that $v \in X$. Since X is transitive, $u \in X$. Therefore, $u \in \bigcup S$. Hence, $\bigcup S$ is transitive. ■

Proposition 5.10. An ordinal α is a natural number if and only if every nonempty subset of α has a greatest element.

Proof. (Necessity) Suppose $\alpha \in \mathbb{N}$. Then α is a finite ordinal. Any nonempty subset $X \subseteq \alpha$ is finite and well-ordered by $\in$. By properties of finite well-ordered sets, X has a greatest element.

(Sufficiency) Conversely, assume every nonempty subset of α has a greatest element. Suppose α is not a natural number. By the characterization of finite ordinals, $\alpha \geq \omega$. However, ω does not have a greatest element because for any $n \in \omega$, there exists $n+1 > n$. This contradicts the assumption that every nonempty subset of α has a greatest element. Therefore, $\alpha \in \mathbb{N}$. ■

Proposition 5.11. If a set of ordinals X does not have a greatest element, then $\sup X$ is a limit ordinal.

Proof. Since X lacks a greatest element, $\sup X \notin X$. Suppose, for contradiction, that $\sup X$ is a successor ordinal, meaning $\sup X = \beta + 1$ for some ordinal β. Then, for all $\alpha \in X$, we have $\alpha < \sup X$, so $\alpha \leq \beta$.

This implies that β is an upper bound for X, and since $\beta < \beta + 1 = \sup X$, β is a smaller upper bound than $\sup X$. This contradicts the definition of $\sup X$ as the least upper bound of X. Therefore, $\sup X$ must be a limit ordinal. ■

Proposition 5.12. If X is a nonempty set of ordinals, then $\bigcap X$ is an ordinal, and $\bigcap X$ is the least element of X.

Proof. Let $m = \bigcap X$. We first show that m is an ordinal.

Transitivity: For any $u \in v \in m$, since $v \in m$, $v \in \alpha$ for all $\alpha \in X$. Similarly, $u \in v$ implies $u \in \alpha$ for all $\alpha \in X$ because each α is transitive. Therefore, $u \in m$, so m is transitive.

Well-Ordering: The relation $\in$ on m is well-founded and total because it is inherited from the ordinals in X.

Thus, m is an ordinal.

Now, we show that m is the least element of X.

Suppose, for contradiction, that there is some $\alpha \in X$ such that $\alpha < m$. Since $m \subseteq \alpha$ (as m is the intersection), this is impossible unless $\alpha = m$. Therefore, m is less than or equal to every element of X.

Since m is an element of X (as it is the intersection of all elements of X), it follows that m is the minimal element of X. ■

5.2 The Axiom Schema of Replacement

In the realm of set theory, certain seemingly straightforward constructions require assurance of their existence, which isn't always guaranteed by the existing axioms. For example, consider the desire to build a sequence such as

$$\langle \emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \dots \rangle$$

using Recursion Theorem principles. This task necessitates the existence of a set that encompasses all elements of this sequence. However, without sufficient axioms, proving the existence of such a set becomes problematic. This is where the Axiom Schema of Replacement becomes indispensable.

Definition 5.8 (Axiom Schema of Replacement)**.** Suppose $\mathscr{P}(x,y)$ is a property where for every x, there exists exactly one y that satisfies $\mathscr{P}(x,y)$. Then, for any set A, there exists a set B such that for every $x \in A$, there exists a $y \in B$ with $\mathscr{P}(x,y)$ holding true. Formally,

$$\forall x \exists! y \, \mathscr{P}(x,y) \implies \forall A \exists B \forall x (x \in A \implies \exists y (y \in B \wedge \mathscr{P}(x,y))).$$

Definition 5.9 (Operation Defined by a Property)**.** Let $\mathscr{P}(x,y)$ be a property such that for every x, there exists a unique y satisfying $\mathscr{P}(x,y)$. The function $\mathscr{F}$ defined by $\mathscr{P}$ is called the *operation defined by* $\mathscr{P}$, where $\mathscr{F}(x)$ denotes the unique y corresponding to each x.

Notation 5.9 (Image)**.** Given a property $\mathscr{P}(x,y)$ with the uniqueness condition and its corresponding operation $\mathscr{F}$, the image of a set A under $\mathscr{F}$ is denoted by

$$\mathscr{F}[A] \triangleq \{ \mathscr{F}(x) \mid x \in A \} = \{ y \mid \exists x \in A, \; y = \mathscr{F}(x) \}.$$

Theorem 5.3 (Counting Theorem)**.** Every well-ordered set $(W, \preceq)$ is order-isomorphic to exactly one ordinal number α. In other words, there exists a unique $\alpha \in \mathrm{Ord}$ such that $W \cong \alpha$.

Proof. Uniqueness: Suppose there are two distinct ordinals α and β such that $W \cong \alpha$ and $W \cong \beta$. Without loss of generality, assume $\alpha < \beta$. Since ordinals are well-ordered by the membership relation $\in$, α becomes an initial segment of β. However, a well-ordered set cannot be isomorphic to a proper initial segment of another well-ordered set. This contradiction implies that $\alpha = \beta$, ensuring uniqueness.

Existence: Define

$$A = \{\, a \in W \mid W[a] \text{ is order-isomorphic to some ordinal} \,\}.$$

For each $a \in A$, let α_a be the unique ordinal such that $W[a] \cong \alpha_a$. By the Axiom Schema of Replacement (Definition 5.8), the set

$$S = \{\, \alpha_a \mid a \in A \,\}$$

exists.

Claim 5.4. The set S is an ordinal.

Proof of Claim 5.4. The set S inherits a well-ordering from the membership relation $\in$, as each α_a is an ordinal. Additionally, for any $\gamma \in \alpha_a \in S$, the corresponding element $c = \varphi_a(\gamma)$ (where φ_a is the isomorphism between α_a and $W[a]$) satisfies $\gamma \in S$ because $W[c] \cong \gamma$. Hence, S is transitive and well-ordered, making it an ordinal. ■

Claim 5.5. Let $a \in A$, $b \in W$, and $b \prec a$. Then, $b \in A$ and $\alpha_b < \alpha_a$.

Proof of Claim 5.5. Consider the isomorphism $\varphi_a : W[a] \hookrightarrow \alpha_a$. The restriction $\varphi_a|_{W[b]}$ serves as an isomorphism between $W[b]$ and $\varphi_a[W[b]]$. Since $W[b]$ is an initial segment of $W[a]$, $\varphi_a[W[b]]$ is an initial segment of α_a, making it an ordinal β with $\beta < \alpha_a$. Therefore, $b \in A$ and $\alpha_b = \beta < \alpha_a$. ■

Now, define the function $f : A \to S$ by $f(a) = \alpha_a$. By Claims 5.4 and 5.5, f is an order-isomorphism between A and S. Since A encompasses all elements of W (as every initial segment $W[a]$ corresponds to some ordinal α_a), it follows that $W \cong S$. Thus, every well-ordered set is order-isomorphic to a unique ordinal. ■

Definition 5.10 (Order Type)**.** The *order type* of a well-ordered set W is the unique ordinal α such that $W \cong \alpha$, as established by the Counting Theorem (Theorem 5.3).

Theorem 5.4 (Recursion Theorem)**.** Let $\mathscr{G}$ be an operation. For any element a, there exists a unique infinite sequence $\langle a_n \mid n \in \mathbb{N} \rangle$ such that

(i) $a_0 = a$, and

(ii) $\forall n \in \mathbb{N},\ a_{n+1} = \mathscr{G}(a_n, n)$.

Proposition 5.13. Let $\mathscr{P}(x,y)$ be a property such that for every x, there is at most one y for which $\mathscr{P}(x,y)$ holds. Then, for every A, there exists a set B such that

$$\forall x \in A,\ [\exists y,\ \mathscr{P}(x,y) \implies \exists y \in B,\ \mathscr{P}(x,y)]\,.$$

Proof. Let $\mathscr{Q}(x,y)$ be the property

$$\mathscr{Q}(x,y) \iff (\mathscr{P}(x,y)) \vee (y = \emptyset \wedge \neg \exists z\, \mathscr{P}(x,z))\,.$$

Then, for each x, there exists a unique y satisfying $\mathscr{Q}(x,y)$:

- If $\mathscr{P}(x,y)$ holds, then y is unique by assumption.

- If $\mathscr{P}(x,y)$ does not hold for any y, then $y = \emptyset$ is the unique element satisfying $\mathscr{Q}(x,y)$.

By the Axiom Schema of Replacement, there exists a set $B = \{\, y \mid \exists x \in A,\ \mathscr{Q}(x,y)\,\}$. For every $x \in A$ such that $\exists y\, \mathscr{P}(x,y)$, the corresponding y is in B. ■

Proposition 5.14.

(i) The set $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots\}$ exists.

(ii) The set $\{\mathbb{N}, \mathscr{P}(\mathbb{N}), \mathscr{P}(\mathscr{P}(\mathbb{N})), \dots\}$ exists.

(iii) The set $\omega + \omega = \omega \cup \{\, \omega, \omega+1, (\omega+1)+1, \dots\}$ exists.

Proof. We utilize the Recursion Theorem (Theorem 5.4) for each part.

(i) Define $\mathscr{G}(x,n) = \{x\}$. Starting with $a_0 = \emptyset$, the sequence becomes:

$$a_0 = \emptyset, \quad a_1 = \{\emptyset\}, \quad a_2 = \{\{\emptyset\}\}, \quad a_3 = \{\{\{\emptyset\}\}\}, \ \dots$$

By the Axiom Schema of Replacement, the set $\{a_n \mid n \in \mathbb{N}\}$ exists.

(ii) Define $\mathscr{G}(x,n) = \mathscr{P}(x)$. Starting with $a_0 = \mathbb{N}$, the sequence is:

$$a_0 = \mathbb{N}, \quad a_1 = \mathscr{P}(\mathbb{N}), \quad a_2 = \mathscr{P}(\mathscr{P}(\mathbb{N})), \ \dots$$

Again, by the Axiom Schema of Replacement, the set $\{a_n \mid n \in \mathbb{N}\}$ exists.

(iii) Let $\mathscr{G}(x,n) = x+1$, where $x+1$ denotes the successor of x in ordinal arithmetic. Starting with $a_0 = \omega$, the sequence becomes:

$$a_0 = \omega, \quad a_1 = \omega+1, \quad a_2 = (\omega+1)+1, \quad \dots$$

The set $\{a_n \mid n \in \mathbb{N}\}$ exists, and so does $\omega \cup \{a_n \mid n \in \mathbb{N}\}$, which is $\omega + \omega$.

■

Proposition 5.15. Use the Recursion Theorem to define

$$\begin{aligned} & V_0 = \emptyset, \\ \forall n \in \mathbb{N}, \quad & V_{n+1} = \mathscr{P}(V_n), \\ & V_\omega = \bigcup_{n \in \mathbb{N}} V_n. \end{aligned}$$

Proof. Set $\mathscr{G}(x,n) = \mathscr{P}(x)$ and $a_0 = \emptyset$. By the Recursion Theorem, we obtain the sequence $\langle V_n \mid n \in \mathbb{N}\rangle$, where each $V_{n+1} = \mathscr{P}(V_n)$. Hence, $V_\omega = \bigcup_{n\in\mathbb{N}} V_n$ exists as well. ■

Proposition 5.16.

(i) Every $x \in V_\omega$ is finite.

(ii) V_ω is transitive.

(iii) V_ω is an inductive set.

The elements of V_ω are called *hereditarily finite sets*.

Proof. We first prove that each V_n is transitive.

Claim 5.6. $\forall n \in \mathbb{N},\ V_n \subseteq \mathscr{P}(V_n)$.

Proof of Claim 5.7. We have $V_0 = \emptyset \subseteq \mathscr{P}(V_0)$. Assume $V_n \subseteq \mathscr{P}(V_n)$. Then for any $x \in V_{n+1} = \mathscr{P}(V_n)$, $x \subseteq V_n \subseteq \mathscr{P}(V_n) = V_{n+1}$. Therefore, $x \in \mathscr{P}(V_{n+1})$. By induction, $V_n \subseteq \mathscr{P}(V_n)$ for all $n \in \mathbb{N}$. ■

From Claim 5.7 and (Principle of Mathematical Induction), it follows that for all $m,n \in \mathbb{N}$, if $m \leq n$, then $V_m \subseteq V_n$.

(i) Take any $x,y \in V_\omega$. Then, there exist $m,n \in \mathbb{N}$ such that $x \in V_m$ and $y \in V_n$. Without loss of generality, assume $m \leq n$. Then, $V_m \subseteq V_n$, so $x,y \in V_n$. Therefore, $\{x,y\} \subseteq V_n$, implying $\{x,y\} \in V_{n+1} \subseteq V_\omega$.

(ii) Let $X \in V_\omega$. Then, $X \in V_{n+1} = \mathscr{P}(V_n)$ for some $n \in \mathbb{N}$. By Claim 5.7, $V_n \subseteq \mathscr{P}(V_n)$, and since $X \subseteq V_n$, it follows that $X \subseteq V_n \subseteq V_{n+1}$. Therefore, $\bigcup X \subseteq V_n \subseteq V_\omega$, so $\bigcup X \in V_\omega$. Moreover, $\mathscr{P}(X) \subseteq \mathscr{P}(V_n) = V_{n+1} \subseteq V_\omega$, hence $\mathscr{P}(X) \in V_\omega$.

(iii) Suppose $X \in V_\omega$ and $f:X \to V_\omega$. By part (i), X is finite. Therefore, $f[X]$ is a finite subset of V_ω. By part (iv), $f[X] \in V_\omega$.

(iv) If X is a finite subset of V_ω, then there exists $n \in \mathbb{N}$ such that $X \subseteq V_n$. Therefore, $X \in V_{n+1} \subseteq V_\omega$.

■

Proposition 5.17.

(i) If $x,y \in V_\omega$, then $\{x,y\} \in V_\omega$.

(ii) If $X \in V_\omega$, then $\bigcup X \in V_\omega$ and $\mathscr{P}(X) \in V_\omega$.

(iii) If $X \in V_\omega$ and $f:X \to V_\omega$, then $f[X] \in V_\omega$.

(iv) If X is a finite subset of V_ω, then $X \in V_\omega$.

Proof. We first prove that each V_n is transitive.

Claim 5.7. $\forall n \in \mathbb{N},\ V_n \subseteq \mathscr{P}(V_n)$.

Proof of Claim 5.7. We have $V_0 = \emptyset \subseteq \mathscr{P}(V_0)$. Assume $V_n \subseteq \mathscr{P}(V_n)$. Then for any $x \in V_{n+1} = \mathscr{P}(V_n)$, $x \subseteq V_n \subseteq \mathscr{P}(V_n) = V_{n+1}$. Therefore, $x \in \mathscr{P}(V_{n+1})$. By induction, $V_n \subseteq \mathscr{P}(V_n)$ for all $n \in \mathbb{N}$. ■

From Claim 5.7 and the (Principle of Mathematical Induction), it follows that for all $m,n \in \mathbb{N}$, if $m \leq n$, then $V_m \subseteq V_n$.

(i) Take any $x, y \in V_\omega$. Then, there exist $m, n \in \mathbb{N}$ such that $x \in V_m$ and $y \in V_n$. Without loss of generality, assume $m \leq n$. Then, $V_m \subseteq V_n$, so $x, y \in V_n$. Therefore, $\{x, y\} \subseteq V_n$, implying $\{x, y\} \in V_{n+1} \subseteq V_\omega$.

(ii) Let $X \in V_\omega$. Then, $X \in V_{n+1} = \mathscr{P}(V_n)$ for some $n \in \mathbb{N}$. By Claim 5.7, $V_n \subseteq \mathscr{P}(V_n)$, and since $X \subseteq V_n$, it follows that $X \subseteq V_n \subseteq V_{n+1}$. Therefore, $\bigcup X \subseteq V_n \subseteq V_\omega$, so $\bigcup X \in V_\omega$. Moreover, $\mathscr{P}(X) \subseteq \mathscr{P}(V_n) = V_{n+1} \subseteq V_\omega$, hence $\mathscr{P}(X) \in V_\omega$.

(iii) Suppose $X \in V_\omega$ and $f : X \to V_\omega$. By part (i), X is finite. Therefore, $f[X]$ is a finite subset of V_ω. By part (iv), $f[X] \in V_\omega$.

(iv) If X is a finite subset of V_ω, then there exists $n \in \mathbb{N}$ such that $X \subseteq V_n$. Therefore, $X \in V_{n+1} \subseteq V_\omega$.

■

5.3 Transfinite Induction and Recursion

Theorem 5.5 (Transfinite Induction Principle: First Version)**.** Let $\mathscr{P}(x)$ be a property. Suppose that for every ordinal number α, the following holds:

$$\text{If } \mathscr{P}(\beta) \text{ is true for all ordinals } \beta < \alpha, \text{ then } \mathscr{P}(\alpha) \text{ is true.} \tag{1}$$

Then, $\mathscr{P}(\alpha)$ is true for every ordinal α.

Proof. Assume, for contradiction, that there exists an ordinal γ for which $\mathscr{P}(\gamma)$ does not hold. Define the set

$$S = \{\, \beta \mid \beta \text{ is an ordinal and } \beta \leq \gamma \text{ and } \neg\mathscr{P}(\beta) \,\}.$$

Since S is non-empty, by the well-ordering of ordinals, S contains a least element, say α.

By the minimality of α, for all $\beta < \alpha$, $\mathscr{P}(\beta)$ holds. Applying the induction hypothesis (1), it follows that $\mathscr{P}(\alpha)$ must hold, which contradicts the assumption that $\alpha \in S$.

Therefore, no such γ exists, and $\mathscr{P}(\alpha)$ holds for all ordinals α. ■

Theorem 5.6 (Transfinite Induction Principle: Second Version)**.** Let $\mathscr{P}(x)$ be a property. Suppose that:

(i) For every ordinal α, if $\mathscr{P}(\alpha)$ holds, then $\mathscr{P}(\alpha + 1)$ holds.

(ii) For every limit ordinal α, if $\mathscr{P}(\beta)$ holds for all $\beta < \alpha$, then $\mathscr{P}(\alpha)$ holds.

Then, $\mathscr{P}(\alpha)$ is true for every ordinal α.

Proof. To establish the result, consider any ordinal α and assume that $\mathscr{P}(\beta)$ is true for all $\beta < \alpha$.

- If α is a limit ordinal, then by condition (ii), $\mathscr{P}(\alpha)$ holds.
- If α is a successor ordinal, say $\alpha = \beta + 1$, then by condition (i) and the assumption that $\mathscr{P}(\beta)$ holds, it follows that $\mathscr{P}(\alpha)$ holds.

Hence, by Theorem 5.5, $\mathscr{P}(\alpha)$ holds for all ordinals α. ■

Definition 5.11 (Transfinite Sequence)**.** A *transfinite sequence of length* α is a function whose domain is the ordinal α.

Theorem 5.7 (Transfinite Recursion Theorem)**.** Let $\mathscr{G}$ be an operation. Then, the property $\mathscr{P}(x,y)$ defined as

$$\mathscr{P}(x,y) \iff \begin{cases} x \in \text{Ord and } y = t(x) \text{ for some computation } t \text{ of length } x \text{ based on } \mathscr{G}, \\ \text{or } x \notin \text{Ord and } y = \emptyset. \end{cases} \tag{2}$$

where t is called a *computation of length* α *based on* $\mathscr{G}$ if t is a function with domain $\alpha+1$ and for all $\beta \leq \alpha$, $t(\beta) = \mathscr{G}\left(t \restriction_\beta\right)$, defines an operation $\mathscr{F}$ such that for every ordinal α, $\mathscr{F}(\alpha) = \mathscr{G}\left(\mathscr{F} \restriction_\alpha\right)$.

Proof. First, we need to verify that $\mathscr{P}(x,y)$ defines a unique operation.

Claim 5.8. For every ordinal α, there exists a unique computation of length α based on $\mathscr{G}$.

Proof of Claim 5.8. Fix an ordinal α. Assume that for every $\beta < \alpha$, there exists a unique computation of length β. By the Axiom Schema of Replacement (Definition 5.8), the set

$$T = \{\, t \mid t \text{ is a computation of length } \beta \text{ for some } \beta < \alpha \,\}$$

exists.

Define $\hat{t} = \bigcup T$ and $\tau = \hat{t} \cup \{\, (\alpha, \mathscr{G}(\hat{t} \restriction_\alpha)) \,\}$.

Claim 5.9. τ is a well-defined function with domain $\alpha+1$.

Proof of Claim 5.9. We must show that T is a compatible family of functions. Take any $t_1, t_2 \in T$ with $\text{dom} t_1 = \beta_1 + 1$ and $\text{dom} t_2 = \beta_2 + 1$. Without loss of generality, assume $\beta_1 \leq \beta_2$. Then, $t_1 \subseteq t_2$ or $t_2 \subseteq t_1$ depending on whether $\beta_1 < \beta_2$ or $\beta_1 = \beta_2$. By the uniqueness of computations, t_1 and t_2 agree on their common domain.

Therefore, $\hat{t}$ is a well-defined function with domain α, and τ extends $\hat{t}$ by defining $\tau(\alpha) = \mathscr{G}(\hat{t} \restriction_\alpha)$. Hence, τ is a function with domain $\alpha+1$. ■

Claim 5.10. τ is a computation of length α based on $\mathscr{G}$.

Proof of Claim 5.10. By construction, for each $\beta \leq \alpha$, $\tau(\beta) = \mathscr{G}(\tau \restriction_\beta)$. Therefore, τ satisfies the definition of a computation of length α based on $\mathscr{G}$. ■

By Claims 5.9 and 5.10, τ is a computation of length α.

Uniqueness: Suppose there exists another computation σ of length α based on $\mathscr{G}$. By transfinite induction (Theorem 5.5), τ and σ must agree on all $\beta \leq \alpha$. Therefore, $\tau = \sigma$, ensuring uniqueness. ■

By Claim 5.8, $\mathscr{P}(x,y)$ defines a unique operation $\mathscr{F}$. Specifically, $\mathscr{F}(\alpha) = t(\alpha)$ where t is the unique computation of length α based on $\mathscr{G}$.

For any ordinal α, $\mathscr{F}(\alpha) = \mathscr{G}(\mathscr{F} \restriction_\alpha)$, as required. ■

Notation 5.10 (Function Application)**.** If $\mathscr{F}(z,x)$ is an operation in two variables, meaning $\mathscr{P}(z,x,y)$ is a property where for all z and x, there exists a unique y satisfying $\mathscr{P}(z,x,y)$, then we denote $\mathscr{F}_z(x)$ as $\mathscr{F}(z,x)$. This allows us to treat $\mathscr{F}_z$ as an operation in x.

Theorem 5.8 (Parametric Transfinite Recursion Theorem)**.** Let $\mathscr{G}_1$ and $\mathscr{G}_2$ be operations. Define $\mathscr{G}$ as follows:

$$\mathscr{G}(z,x) = \begin{cases} \mathscr{G}_1(z,\mathscr{F}(z,x)) & \text{if } x \text{ is a successor ordinal,} \\ \mathscr{G}_2(z,\mathscr{F}_z \restriction_x) & \text{if } x \text{ is a limit ordinal,} \\ \emptyset & \text{otherwise.} \end{cases}$$

Then, the property $\mathscr{Q}(z,x,y)$ defined by

$$\mathscr{Q}(z,x,y) \iff \begin{cases} x \in \text{Ord and } y = t(x) \text{ for some computation } t \text{ of length } x \text{ based on } \mathscr{G}, \\ \text{or } x \notin \text{Ord and } y = \emptyset, \end{cases} \tag{3}$$

where t is a computation of length α based on $\mathscr{G}$ and z, defines an operation $\mathscr{F}$ such that for all sets z and ordinals α, $\mathscr{F}(z,\alpha) = \mathscr{G}(z,\mathscr{F}_z \restriction \alpha)$.

Proof. To prove this theorem, modify the proof of Theorem 5.7 by incorporating the parameter z into the operation $\mathscr{G}$. Essentially, replace every instance of $\mathscr{G}$ with $\mathscr{G}(z,\cdot)$ in the proof of Theorem 5.7, ensuring that the computations now depend on z as well. ■

Theorem 5.9 (Advanced Transfinite Recursion)**.** Let $\mathscr{G}_1$ and $\mathscr{G}_2$ be operations. Define the operation $\mathscr{G}$ by

$$\mathscr{G}(x) = \begin{cases} \mathscr{G}_1(\mathscr{F}(x)) & \text{if } x \text{ is a successor ordinal,} \\ \mathscr{G}_2(\mathscr{F} \restriction_x) & \text{if } x \text{ is a limit ordinal,} \\ \emptyset & \text{otherwise.} \end{cases}$$

Then, the property $\mathscr{P}(x,y)$ defined by

$$\mathscr{P}(x,y) \iff \begin{cases} x \in \text{Ord and } y = t(x) \text{ for some computation } t \text{ of length } x \text{ based on } \mathscr{G}, \\ \text{or } x \notin \text{Ord and } y = \emptyset, \end{cases} \tag{4}$$

defines an operation $\mathscr{F}$ such that:

(i) For each ordinal α, $\mathscr{F}(\alpha+1) = \mathscr{G}_1(\mathscr{F}(\alpha))$.

(ii) For each limit ordinal α, $\mathscr{F}(\alpha) = \mathscr{G}_2(\mathscr{F} \restriction \alpha)$.

Proof. For any ordinal α, by the Transfinite Recursion Theorem (Theorem 5.7), there exists a unique computation t of length α based on $\mathscr{G}$. Depending on whether α is a successor or a limit ordinal, the computation $t(\alpha)$ is defined accordingly:

- If α is a successor ordinal, say $\alpha = \beta + 1$, then $\mathscr{F}(\alpha) = \mathscr{G}_1(\mathscr{F}(\beta))$.
- If α is a limit ordinal, then $\mathscr{F}(\alpha) = \mathscr{G}_2(\mathscr{F} \restriction \alpha)$.

This ensures that $\mathscr{F}$ satisfies the desired properties for both successor and limit ordinals. ■

Theorem 5.10 (Parametric Advanced Transfinite Recursion)**.** Let $\mathscr{G}_1$ and $\mathscr{G}_2$ be operations. Define the operation $\mathscr{G}$ by

$$\mathscr{G}(z,x) = \begin{cases} \mathscr{G}_1(z, \mathscr{F}(z,x)) & \text{if } x \text{ is a successor ordinal,} \\ \mathscr{G}_2(z, \mathscr{F}_z \restriction_x) & \text{if } x \text{ is a limit ordinal,} \\ \emptyset & \text{otherwise.} \end{cases}$$

Then, the property $\mathscr{Q}(z,x,y)$ defined by

$$\mathscr{Q}(z,x,y) \iff \begin{cases} x \in \text{Ord and } y = t(x) \text{ for some computation } t \text{ of length } x \text{ based on } \mathscr{G} \text{ and } z, \\ \text{or } x \notin \text{Ord and } y = \emptyset, \end{cases} \tag{5}$$

where t is a computation of length α based on $\mathscr{G}$ and z, defines an operation $\mathscr{F}$ such that for all sets z and ordinals α, $\mathscr{F}(z,\alpha) = \mathscr{G}(z, \mathscr{F}_z \restriction \alpha)$.

Proof. The proof follows by adapting the proof of Theorem 5.9, incorporating the parameter z. Specifically, replace every occurrence of $\mathscr{G}$ with $\mathscr{G}(z,\cdot)$, ensuring that computations are now dependent on z as well. ■

Corollary. Let Ω be an ordinal, A be a set, and define

$$S = \bigcup_{\alpha<\Omega} A^\alpha,$$

where A^α denotes the set of all transfinite sequences of elements of A of length α. Let $g: S \to A$ be a function. Then, there exists a unique function $f: \Omega \to A$ such that

$$f(\alpha) = g(f \restriction \alpha) \text{ for all ordinals } \alpha < \Omega.$$

Proof. Define an operation $\mathscr{G}$ by

$$\mathscr{G}(t) = \begin{cases} g(t) & \text{if } t \in S, \\ \emptyset & \text{otherwise.} \end{cases}$$

By the (Theorem 5.7), there exists an operation $\mathscr{F}$ such that for every ordinal α,

$$\mathscr{F}(\alpha) = \mathscr{G}(\mathscr{F} \restriction \alpha).$$

Define $f = \mathscr{F} \restriction_\Omega$. Then, f satisfies the required condition. ■

Proof of Transfinite Recursion Theorem. Define an auxiliary operation $\mathscr{G}'$ by

$$\mathscr{G}'(x) = \begin{cases} \mathscr{G}(x_n, n) & \text{if } x \text{ is a finite sequence of length } n+1 \text{ where } n \in \omega, \\ a & \text{otherwise.} \end{cases}$$

By the (Theorem 5.7), there exists an operation $\mathscr{F}$ such that

$$\mathscr{F}(\alpha) = \mathscr{G}'(\mathscr{F} \restriction \alpha)$$

for every ordinal α.

Now, let $\langle a_n \mid n \in \mathbb{N} \rangle = \mathscr{F} \restriction_\omega$. Then:

(i) $a_0 = \mathscr{F}(0) = \mathscr{G}'(\emptyset) = a$.

(ii) For each $n \in \mathbb{N}$,

$$a_{n+1} = \mathscr{F}(n+1) = \mathscr{G}'(\mathscr{F} \restriction_{n+1}) = \mathscr{G}(a_n, n).$$

Thus, the sequence $\langle a_n \rangle$ satisfies the required conditions, proving the theorem. ■

5.4 Ordinal Arithmetic

Definition 5.12 (Addition of Ordinal Numbers)**.** For each ordinal β, the addition of ordinals is defined recursively as follows:

$$\beta + 0 = \beta, \tag{1}$$
$$\beta + (\alpha + 1) = (\beta + \alpha) + 1 \quad \text{for all ordinals } \alpha, \tag{2}$$
$$\beta + \alpha = \sup\{\, \beta + \gamma \mid \gamma < \alpha \,\} \quad \text{for all limit ordinals } \alpha \neq 0. \tag{3}$$

Remark. Let $\mathscr{G}_1$ and $\mathscr{G}_2$ be operations defined by

$$\mathscr{G}_1(z,x) = x + 1,$$
$$\mathscr{G}_2(z,x) = \begin{cases} \bigcup ran(x) & \text{if } x \text{ is a non-empty function,} \\ z & \text{otherwise.} \end{cases}$$

Using the (Parametric Advanced Transfinite Recursion), we obtain an operation $\mathscr{F}$ such that for each ordinal β:

(i) $\mathscr{F}(\beta, 0) = \mathscr{G}_2(\beta, \emptyset) = \beta$.

(ii) $\mathscr{F}(\beta, \alpha+1) = \mathscr{G}_1(\beta, \mathscr{F}(\beta,\alpha)) = \mathscr{F}(\beta,\alpha) + 1$ for all ordinals α.

(iii) $\mathscr{F}(\beta,\alpha) = \mathscr{G}_2\left(\beta, \mathscr{F}_\beta \restriction_\alpha\right) = \bigcup ran\left(\mathscr{F}_\beta \restriction_\alpha\right)$ for all limit ordinals α.

Let $\mathscr{P}(\alpha)$ be the property that $\mathscr{F}(\beta,\alpha)$ is an ordinal for each ordinal α. Using transfinite induction (Theorem 5.5), we can show that $\mathscr{F}(\beta,\alpha)$ is indeed an ordinal for all α and β. Thus, Definition 5.12 is justified, and we denote $\beta + \alpha$ as $\mathscr{F}(\beta,\alpha)$.

Notation 5.11. Ordinal addition is not commutative or right-cancellative:

- For any $n \in \omega - \{0\}$, $n + \omega = \omega \neq \omega + n$.
- $1 + \omega = \omega = 2 + \omega$, but $1 \neq 2$.

Theorem 5.11 (Sum of well ordered set and ordinal)**.** Let $(W_1, \leq_1)$ and $(W_2, \leq_2)$ be well-ordered sets isomorphic to ordinals α_1 and α_2, respectively. Let $(W, \leq)$ be the sum of $(W_1, \leq_1)$ and $(W_2, \leq_2)$ (see Lemma 4.8). Then, $(W, \leq)$ is order-isomorphic to $\alpha_1 + \alpha_2$.

Proof. Assume that W_1 and W_2 are disjoint and that $W = W_1 \cup W_2$. We proceed by transfinite induction on α_2.

Base Case: If $\alpha_2 = 0$, the result is trivial since $\alpha_1 + 0 = \alpha_1$.

Successor Case: Suppose $\alpha_2 = \beta + 1$ for some ordinal β, and assume the theorem holds for β. Then, W_2 has a greatest element, say a, and $W_2[a]$ is isomorphic to β. The sum $W[a]$ is then the sum of W_1 and $W_2[a]$, which by the induction hypothesis is isomorphic to $\alpha_1 + \beta$. Adding a corresponds to adding 1, so W is isomorphic to $(\alpha_1 + \beta) + 1 = \alpha_1 + \alpha_2$.

Limit Case: Suppose α_2 is a limit ordinal, and assume the theorem holds for all $\beta < \alpha_2$. For each $\beta < \alpha_2$, there exists an element $a_\beta \in W_2$ such that $W_2[a_\beta]$ is order-isomorphic to β. By the induction hypothesis, $W[a_\beta]$ is isomorphic to $\alpha_1 + \beta$. The union of these isomorphisms gives an isomorphism between W and $\alpha_1 + \alpha_2$.

Therefore, by transfinite induction, W is isomorphic to $\alpha_1 + \alpha_2$. ■

Lemma 5.7. Let α, β, and γ be ordinals. Then:

(i) $\alpha < \beta \iff \gamma + \alpha < \gamma + \beta$.

(ii) $\alpha = \beta \iff \gamma + \alpha = \gamma + \beta$.

(iii) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

Proof. **(i)** ($\Rightarrow$) Assume $\alpha < \beta$. We proceed by transfinite induction on γ. The base case $\gamma = 0$ is trivial. Suppose the result holds for γ. Then:

$$\gamma + \alpha < \gamma + \beta.$$

If γ is a successor ordinal, the result follows from the recursive definition of addition. For limit ordinals, the supremum property ensures the inequality holds.

($\Leftarrow$) Conversely, assume $\gamma + \alpha < \gamma + \beta$. If $\alpha = \beta$, this would imply $\gamma + \alpha = \gamma + \beta$, contradicting the assumption. If $\beta < \alpha$, then $\gamma + \beta < \gamma + \alpha$, which also contradicts the assumption. Therefore, $\alpha < \beta$.

(ii) Follows directly from (i).

(iii) We prove by transfinite induction on γ. The base case $\gamma = 0$ is straightforward. For successor ordinals, we have:

$$\begin{aligned}(\alpha + \beta) + (\gamma + 1) &= [(\alpha + \beta) + \gamma] + 1 \\ &= [\alpha + (\beta + \gamma)] + 1 \quad \text{(by induction hypothesis)} \\ &= \alpha + [(\beta + \gamma) + 1] \\ &= \alpha + (\beta + (\gamma + 1)).\end{aligned}$$

For limit ordinals, both sides equal the supremum of the previous values, thus the equality holds. ■

Lemma 5.8. Let $\alpha \leq \beta$ be ordinals. Then, there exists a unique ordinal ξ such that $\alpha + \xi = \beta$.

Proof. Consider the set $\beta - \alpha = \{ \nu \mid \alpha \leq \nu < \beta \}$, which is well-ordered. There exists an ordinal ξ order-isomorphic to $\beta - \alpha$. By Theorem 5.11, $\alpha + \xi = \beta$. Uniqueness follows from Lemma 5.7. ■

Definition 5.13 (Multiplication of Ordinal Numbers)**.** For each ordinal β, the multiplication of ordinals is defined recursively as follows:

$$\beta \cdot 0 = 0, \tag{4}$$

$$\beta \cdot (\alpha + 1) = (\beta \cdot \alpha) + \beta \quad \text{for all ordinals } \alpha, \tag{5}$$

$$\beta \cdot \alpha = \sup\{\, \beta \cdot \gamma \mid \gamma < \alpha \,\} \quad \text{for all limit ordinals } \alpha \neq 0. \tag{6}$$

Remark. Define operations $\mathscr{G}_1$ and $\mathscr{G}_2$ by

$$\mathscr{G}_1(z,x) = \begin{cases} x+z & \text{if } x \text{ and } z \text{ are ordinals,} \\ \emptyset & \text{otherwise,} \end{cases}$$

$$\mathscr{G}_2(z,x) = \begin{cases} \bigcup ran(x) & \text{if } x \text{ is a non-empty function,} \\ 0 & \text{otherwise.} \end{cases}$$

Using the Parametric Transfinite Recursion Theorem (Theorem 5.10), we obtain an operation $\mathscr{F}(\beta,\alpha)$ that justifies Definition 5.13.

Theorem 5.12. Let α and β be ordinals. Then, the order type of the lexicographic ordering of $\beta \times \alpha$ is $\alpha \cdot \beta$.

Proof. We prove by transfinite induction on β.

Base Case: For $\beta = 0$, the product $\beta \times \alpha$ is empty, and $0 \cdot \alpha = 0$, so the order types match.

Successor Case: Assume the theorem holds for β, and consider $\beta + 1$. The set $(\beta + 1) \times \alpha$ can be partitioned into $\beta \times \alpha$ and $\{\beta\} \times \alpha$. By the induction hypothesis, $\beta \times \alpha$ has order type $\alpha \cdot \beta$. The set $\{\beta\} \times \alpha$ has order type α. Combining these, the order type of $(\beta + 1) \times \alpha$ is $\alpha \cdot \beta + \alpha = \alpha(\beta + 1)$.

Limit Case: Suppose β is a limit ordinal, and the theorem holds for all $\beta' < \beta$. Then, $\beta \times \alpha = \bigcup_{\beta' < \beta} \beta' \times \alpha$. By the induction hypothesis, each $\beta' \times \alpha$ has order type $\alpha \cdot \beta'$. Taking the union, the order type of $\beta \times \alpha$ is $\alpha \cdot \beta$.

Therefore, the order type of $\beta \times \alpha$ is $\alpha \cdot \beta$. ■

Definition 5.14 (Exponentiation of Ordinal Numbers)**.** For each ordinal β, the exponentiation of ordinals is defined recursively as follows:

$$\beta^0 = 1, \tag{7}$$

$$\beta^{\alpha+1} = \beta^\alpha \cdot \beta \quad \text{for all ordinals } \alpha, \tag{8}$$

$$\beta^\alpha = \sup\{\, \beta^\gamma \mid 0 < \gamma < \alpha \,\} \quad \text{for all limit ordinals } \alpha \neq 0. \tag{9}$$

Notation 5.12. Define operations $\mathscr{G}_1$ and $\mathscr{G}_2$ by

$$\mathscr{G}_1(z,x) = \begin{cases} x \cdot z & \text{if } x \text{ and } z \text{ are ordinals,} \\ \emptyset & \text{otherwise,} \end{cases}$$

$$\mathscr{G}_2(z,x) = \begin{cases} \bigcup ran(x) & \text{if } x \text{ is a non-empty function,} \\ 1 & \text{otherwise.} \end{cases}$$

Using the Parametric Transfinite Recursion Theorem (Theorem 5.10), we obtain an operation $\mathscr{F}(\beta,\alpha)$ that justifies Definition 5.14.

Remark. Ordinal arithmetic differs from cardinal arithmetic in several ways:

- $2^{\aleph_0} > \aleph_0$, but $2^{\omega} = \omega$.
- $\aleph_0^n = \aleph_0$ for any finite n, but $\omega^n > \omega$.
- ω^{ω} is countable; it corresponds to the order type of the lexicographic ordering of $\mathbb{N}^{\mathbb{N}}$.

Remark. We can generate larger ordinals using arithmetic operations:

$$0, 1, \ldots, \omega, \omega+1, \ldots, \omega \cdot 2, \ldots, \omega^2, \ldots, \omega^3, \ldots, \omega^{\omega}, \ldots$$

Defining

$$\varepsilon_0 = \sup\{\, \omega, \omega^{\omega}, \omega^{\omega^{\omega}}, \omega^{\omega^{\omega^{\omega}}}, \ldots \},$$

we can then consider ordinals like $\varepsilon_0 + 1$, $\varepsilon_0 + \omega$, ε_0^{ω}, $\varepsilon_0^{\varepsilon_0}$, and so on.

Proposition 5.18. For all ordinals α, β, and γ,

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma).$$

Proof. The case when $\gamma = 0$ is evident by (4). Moreover, if $\alpha = 0$ or $\beta = 0$, the equality follows from Claims 5.11 of Proposition 5.19.

We proceed by transfinite induction on γ.

Case 1: Successor Ordinal $\gamma = \delta + 1$

Assume the induction hypothesis holds for all $\gamma' < \gamma$. Then,

$$\begin{aligned}
(\alpha \cdot \beta) \cdot (\delta + 1) &= (\alpha \cdot \beta) \cdot \delta + \alpha \cdot \beta && \text{by (5)} \\
&= \alpha \cdot (\beta \cdot \delta) + \alpha \cdot \beta && \text{by Induction Hypothesis} \\
&= \alpha \cdot (\beta \cdot \delta + \beta) && \text{by Prop 5.19} \\
&= \alpha \cdot (\beta \cdot (\delta + 1)) && \text{by (5).}
\end{aligned}$$

Case 2: Limit Ordinal γ

Assume γ is a nonzero limit ordinal and the induction hypothesis holds for all $\gamma' < \gamma$. Let $\alpha \neq 0$ and $\beta \neq 0$.

Take any $\xi < (\alpha \cdot \beta) \cdot \gamma$. Then, there exists $\xi' < \gamma$ such that $\xi < (\alpha \cdot \beta) \cdot \xi'$. By the induction hypothesis,

$$\xi < \alpha \cdot (\beta \cdot \xi') < \alpha \cdot (\beta \cdot \gamma).$$

Thus, $(\alpha \cdot \beta) \cdot \gamma \leq \alpha \cdot (\beta \cdot \gamma)$.

Conversely, take any $\xi < \alpha \cdot (\beta \cdot \gamma)$. Since $\beta \cdot \gamma$ is a nonzero limit ordinal by Claim 5.12 of Prop 5.19, there exists $\xi' < \gamma$ such that $\xi < \alpha \cdot (\beta \cdot \xi')$. By the induction hypothesis,

$$\xi < (\alpha \cdot \beta) \cdot \xi' < (\alpha \cdot \beta) \cdot \gamma.$$

Hence, $\alpha \cdot (\beta \cdot \gamma) \leq (\alpha \cdot \beta) \cdot \gamma$.

Therefore, by transfinite induction, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ for all ordinals α, β, and γ. ■

Proposition 5.19. For all ordinals α, β, and γ,

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma.$$

Proof. We begin with the following claims.

Claim 5.11. Let α and β be ordinals. Then, $\alpha \cdot \beta = 0$ if and only if $\alpha = 0$ or $\beta = 0$.

Proof.

($\Rightarrow$) Assume $\alpha \cdot \beta = 0$. If $\alpha \neq 0$ and $\beta \neq 0$, then by the definition of ordinal multiplication, $\alpha \cdot \beta$ would be a nonzero ordinal, which is a contradiction. Hence, $\alpha = 0$ or $\beta = 0$.

($\Leftarrow$) If $\alpha = 0$ or $\beta = 0$, then by the definitions (4) and (5), $\alpha \cdot \beta = 0$.

■

Claim 5.12. If α and β are nonzero ordinals and β is a limit ordinal, then $\alpha \cdot \beta$ is a nonzero limit ordinal.

Proof. Take any $\xi < \alpha \cdot \beta$. Then, there exists $\delta < \beta$ such that $\xi < \alpha \cdot \delta$ by (6). Therefore,

$$\xi + 1 \leq \alpha \cdot \delta < \alpha \cdot (\delta + 1) \leq \alpha \cdot \beta,$$

which shows that $\alpha \cdot \beta$ is a limit ordinal. Additionally, since α and β are nonzero, $\alpha \cdot \beta \neq 0$ by Claim 5.11.
■

Now, we prove the main statement using transfinite induction on γ.

Case 1: Successor Ordinal $\gamma = \delta + 1$

Assume the induction hypothesis holds for all $\gamma' < \gamma$. Then,

$$\begin{aligned}
\alpha \cdot (\beta + (\delta + 1)) &= \alpha \cdot ((\beta + \delta) + 1) && \text{by (2)} \\
&= \alpha \cdot (\beta + \delta) + \alpha && \text{by (5)} \\
&= (\alpha \cdot \beta + \alpha \cdot \delta) + \alpha && \text{by Induction Hypothesis} \\
&= \alpha \cdot \beta + (\alpha \cdot \delta + \alpha) && \text{by ((iii))} \\
&= \alpha \cdot \beta + \alpha \cdot (\delta + 1) && \text{by (5).}
\end{aligned}$$

Case 2: Limit Ordinal γ

Assume γ is a nonzero limit ordinal and the induction hypothesis holds for all $\gamma' < \gamma$. Let $\alpha \neq 0$.

Take any $\xi < \alpha \cdot (\beta + \gamma)$. Then, there exists $\delta < \beta + \gamma$ such that $\xi < \alpha \cdot \delta$. Since γ is a limit ordinal, there exists $\delta' < \gamma$ such that $\delta < \beta + \delta'$. By the induction hypothesis,

$$\xi < \alpha \cdot (\beta + \delta') \leq \alpha \cdot (\beta + \gamma).$$

Hence, $\alpha \cdot (\beta + \gamma) \leq \alpha \cdot \beta + \alpha \cdot \gamma$.

Conversely, take any $\xi < \alpha \cdot \beta + \alpha \cdot \gamma$. Since $\alpha \cdot \gamma$ is a nonzero limit ordinal by Claim 5.12, there exists $\xi' < \alpha \cdot \gamma$ such that $\xi < \alpha \cdot \beta + \xi'$. Furthermore, there exists $\xi'' < \gamma$ such that $\xi' < \alpha \cdot \xi''$. Therefore,

$$\xi < \alpha \cdot \beta + \alpha \cdot \xi'' = \alpha \cdot (\beta + \xi'') < \alpha \cdot (\beta + \gamma),$$

which implies $\alpha \cdot \beta + \alpha \cdot \gamma \leq \alpha \cdot (\beta + \gamma)$.

Therefore, by transfinite induction, $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ for all ordinals α, β, and γ. ■

Proposition 5.20. Simplify:

(i) $(\omega + 1) + \omega$

(ii) $\omega + \omega^2$

(iii) $(\omega + 1) \cdot \omega^2$

Proof.

(i)

$$\begin{aligned} (\omega + 1) + \omega &= \omega + (1 + \omega) && \text{by ((iii))} \\ &= \omega + \omega && \text{since } 1 + \omega = \omega \\ &= \omega \cdot 2. \end{aligned}$$

(ii)

$$\begin{aligned} \omega + \omega^2 &= \omega \cdot 1 + \omega \cdot \omega \\ &= \omega \cdot (1 + \omega) && \text{by Prop 5.19} \\ &= \omega \cdot \omega && \text{since } 1 + \omega = \omega \\ &= \omega^2. \end{aligned}$$

(iii) Observe that $\omega^2 = \omega \cdot \omega \leq (\omega + 1) \cdot \omega$ by ((ii)).

Take any $\xi < (\omega + 1) \cdot \omega$. Then, there exists $n < \omega$ such that $\xi < (\omega + 1) \cdot n$. Hence,

$$\begin{aligned} \xi &< (\omega + 1) \cdot n \\ &\leq (\omega + \omega) \cdot n && \text{by ((i)) and ((ii))} \\ &= \omega \cdot (2 \cdot n) && \text{by Prop 5.18} \\ &\leq \omega \cdot \omega && \text{by (6).} \end{aligned}$$

Therefore, $(\omega + 1) \cdot \omega \leq \omega^2$.

Conversely, take any $\xi < \omega^2$. Since ω^2 is a limit ordinal, there exists $n < \omega$ such that $\xi < \omega \cdot n$. Hence, $\xi < (\omega + 1) \cdot \omega$, which implies $(\omega + 1) \cdot \omega = \omega^2$. Therefore,

$$(\omega + 1) \cdot \omega^2 = \omega^3 \quad \text{by Prop 5.18.}$$

■

Proposition 5.21. For every ordinal α, there uniquely exist an ordinal β and a natural number n such that $\alpha = \beta + n$.

Proof. Let $\beta = \sup\{\, \gamma \mid \gamma \leq \alpha \text{ and } \gamma \text{ is a limit ordinal} \,\}$. Then, $\beta \leq \alpha$ by definition. Hence, by Lemma 5.8, there exists an ordinal ξ such that $\alpha = \beta + \xi$.

Claim 5.13. β is a limit ordinal.

Proof of Claim 5.13. Suppose, for contradiction, that $\beta = \delta + 1$ for some ordinal δ. Then, since $\delta < \beta$, there exists a limit ordinal γ such that $\delta < \gamma < \alpha$, which contradicts the definition of β as the supremum of such ordinals. Therefore, β must be a limit ordinal. ■

Claim 5.14. ξ is a natural number.

Proof of Claim 5.14. Suppose $\xi \geq \omega$. Then, by Lemma 5.8, there exists an ordinal δ such that $\xi = \omega + \delta$. Substituting back, we get $\alpha = \beta + \omega + \delta$, which implies $\alpha \geq \beta + \omega$. However, $\beta + \omega$ is a limit ordinal, contradicting the maximality of β. Therefore, ξ must be a natural number. ■

Uniqueness: Assume $\alpha = \beta + n = \beta' + n'$ where β and β' are limit ordinals and n, n' are natural numbers. Suppose $\beta < \beta'$. Then, $\beta + n \leq \beta' + n' = \alpha$ implies $n \geq \omega + n'$, which is impossible since n, n' are natural numbers. Hence, $\beta = \beta'$ and $n = n'$ by Proposition (ii). ■

Proposition 5.22. Let α and β be ordinals such that $\alpha \leq \beta$. Then, there can be 0, 1, or infinitely many ξ such that $\xi + \alpha = \beta$.

Proof. Assume ξ_1 and ξ_2 are two distinct ordinals such that $\xi_1 + \alpha = \xi_2 + \alpha = \beta$. Without loss of generality, assume $\xi_1 < \xi_2$. Then,

$$\xi_1 + \alpha \leq (\xi_1 + 1) + \alpha \leq \xi_2 + \alpha = \beta,$$

which implies $\xi_1 + 1 \leq \xi_2$. Continuing this process, we obtain an infinite ascending chain of ordinals $\xi_1 < \xi_1 + 1 < \xi_1 + 2 < \cdots$, each satisfying $\xi_n + \alpha = \beta$. Therefore, there are infinitely many such ξ.

If $\alpha = 0$ or $\beta = 0$, the number of solutions can be 0 or 1 accordingly. ■

Proposition 5.23. Find the least ordinal $\alpha > \omega$ such that $\xi + \alpha = \alpha$ for all $\xi < \alpha$.

Proof. We assert that $\alpha = \omega^2$ satisfies the condition.

Claim 5.15. If ξ is an ordinal less than ω^2, then $\xi + \omega^2 = \omega^2$.

Proof of Claim 5.15. By definition, there exists $n < \omega$ such that $\xi < \omega \cdot n$. Hence,

$$\xi + \omega^2 \leq \omega \cdot n + \omega^2 = \omega \cdot (n + \omega) = \omega \cdot \omega = \omega^2.$$

Since $\omega^2 \leq \xi + \omega^2$, it follows that $\xi + \omega^2 = \omega^2$. ■

Now, suppose $\omega < \alpha < \omega^2$. Then, there exists $m \in \omega$ such that $\alpha < \omega \cdot m$. Let $n = \max\{ m \in \omega \mid \alpha > \omega \cdot m \}$. Then,

$$\omega + \alpha > \omega + \omega \cdot n = \omega \cdot (n+1) \geq \alpha,$$

which contradicts $\alpha + \omega^2 = \omega^2$. Hence, ω^2 is the least ordinal satisfying the condition. ■

Proposition 5.24. Let α, β, and γ be ordinals with $\gamma \neq 0$.

(i) $\alpha < \beta \iff \gamma \cdot \alpha < \gamma \cdot \beta$

(ii) $\alpha = \beta \iff \gamma \cdot \alpha = \gamma \cdot \beta$

Proof.

(i) We prove this by transfinite induction on β.

Case 1: Successor Ordinal $\beta = \delta + 1$ Assume the statement holds for all $\beta' < \beta$. Then, for any $\alpha < \beta$,

$$\begin{aligned} \gamma \cdot \alpha &\leq \gamma \cdot \delta && \text{by Induction Hypothesis} \\ &< \gamma \cdot (\delta + 1) && \text{by (5)} \\ &= \gamma \cdot \beta. \end{aligned}$$

Hence, $\gamma \cdot \alpha < \gamma \cdot \beta$.

Case 2: Limit Ordinal β Assume β is a nonzero limit ordinal. For any $\alpha < \beta$,

$$\gamma \cdot \alpha < \gamma \cdot \beta$$

by the induction hypothesis and the properties of ordinal multiplication. Therefore, $\alpha < \beta \implies \gamma \cdot \alpha < \gamma \cdot \beta$.

Conversely, assume $\gamma \cdot \alpha < \gamma \cdot \beta$. If $\alpha = \beta$, the statement holds trivially. If $\beta < \alpha$, then by the induction hypothesis, $\gamma \cdot \beta < \gamma \cdot \alpha$, which contradicts the assumption. Hence, $\alpha < \beta$.

(ii) This follows directly from part (i). If $\alpha = \beta$, then trivially $\gamma \cdot \alpha = \gamma \cdot \beta$. Conversely, if $\gamma \cdot \alpha = \gamma \cdot \beta$, then by part (i), $\alpha = \beta$.

■

Proposition 5.25. Let α, β, and γ be ordinals with $\alpha < \beta$.

(i) $\alpha + \gamma \leq \beta + \gamma$

(ii) $\alpha \cdot \gamma \leq \beta \cdot \gamma$

Proof.

(i) We prove $\alpha+\gamma \leq \beta+\gamma$ by transfinite induction on γ.

Case 1: Successor Ordinal $\gamma = \delta+1$ Assume the statement holds for γ. Then,

$$\begin{aligned}\alpha+(\delta+1) &= (\alpha+\delta)+1 \quad \text{by (2)}\\ &\leq (\beta+\delta)+1 \quad \text{by Induction Hypothesis}\\ &= \beta+(\delta+1) \quad \text{by (2).}\end{aligned}$$

Case 2: Limit Ordinal γ Assume γ is a nonzero limit ordinal. For any $\xi < \alpha+\gamma$, there exists $\delta < \gamma$ such that $\xi < \alpha+\delta$. By the induction hypothesis,

$$\xi < \beta+\delta < \beta+\gamma.$$

Hence, $\alpha+\gamma \leq \beta+\gamma$.

(ii) We prove $\alpha\cdot\gamma \leq \beta\cdot\gamma$ by transfinite induction on γ.

Case 1: Successor Ordinal $\gamma = \delta+1$ Assume the statement holds for γ. Then,

$$\begin{aligned}\alpha\cdot(\delta+1) &= \alpha\cdot\delta+\alpha \quad \text{by (5)}\\ &< \beta\cdot\delta+\beta \quad \text{by Induction Hypothesis and ((i))}\\ &= \beta\cdot(\delta+1) \quad \text{by Prop 5.19.}\end{aligned}$$

Case 2: Limit Ordinal γ Assume γ is a nonzero limit ordinal. For any $\xi < \alpha\cdot\gamma$, there exists $\delta < \gamma$ such that $\xi < \alpha\cdot\delta$. By the induction hypothesis,

$$\xi < \beta\cdot\delta < \beta\cdot\gamma.$$

Hence, $\alpha\cdot\gamma \leq \beta\cdot\gamma$.

■

Proposition 5.26. (i) Ordinal addition is not right-cancellative; that is, there exist α, β, and γ such that $\alpha+\gamma = \beta+\gamma$ but $\alpha \neq \beta$.

(ii) Ordinal multiplication is not right-cancellative; that is, there exist α, β, and $\gamma \neq 0$ such that $\alpha\cdot\gamma = \beta\cdot\gamma$ but $\alpha \neq \beta$.

(iii) Ordinal addition and multiplication are not right-distributive; that is, there exist α, β, and γ such that $(\alpha+\beta)\cdot\gamma \neq \alpha\cdot\gamma+\beta\cdot\gamma$.

Proof. (i) Take $\alpha = 0$, $\beta = 1$, and $\gamma = \omega$. Then,

$$0+\omega = \omega = 1+\omega,$$

but $0 \neq 1$.

(ii) Take $\alpha = 1$, $\beta = 2$, and $\gamma = \omega$. Then,

$$1\cdot\omega = \omega = 2\cdot\omega,$$

but $1 \neq 2$.

(iii) Take $\alpha = \beta = 1$ and $\gamma = \omega$. Then,

$$(1+1)\cdot\omega = 2\cdot\omega = \omega \quad \text{but} \quad 1\cdot\omega + 1\cdot\omega = \omega+\omega = \omega\cdot 2 \neq \omega.$$

Therefore, $(\alpha+\beta)\cdot\gamma \neq \alpha\cdot\gamma+\beta\cdot\gamma$.

■

Proposition 5.27. An ordinal α is a limit ordinal if and only if $\alpha = \omega\cdot\beta$ for some ordinal β.

Proof.

($\Rightarrow$) Let α be a limit ordinal. We prove by transfinite induction on α.

(i) Assume that for every limit ordinal $\gamma < \alpha$, there exists an ordinal β such that $\gamma = \omega\cdot\beta$.

(ii) Case 1: Suppose there exists a limit ordinal $\gamma < \alpha$ with no limit ordinal δ such that $\gamma < \delta < \alpha$. By the induction hypothesis, $\gamma = \omega\cdot\beta$ for some β. Then,

$$\alpha = \gamma+\omega = \omega\cdot\beta+\omega = \omega\cdot(\beta+1).$$

(iii) Case 2: Suppose that for every limit ordinal $\gamma < \alpha$, there exists a limit ordinal δ with $\gamma < \delta < \alpha$. Define

$$\beta = \sup\{\,\xi \mid \omega\cdot\xi < \alpha\,\}.$$

By Claim 5.12, $\omega\cdot\beta$ is a limit ordinal and $\omega\cdot\beta \leq \alpha$. For any $\xi < \alpha$, $\xi < \omega\cdot\beta$. Hence, $\alpha \leq \omega\cdot\beta$. Therefore, $\alpha = \omega\cdot\beta$.

($\Leftarrow$) Suppose $\alpha = \omega\cdot\beta$ for some ordinal β. We prove that α is a limit ordinal by transfinite induction on β.

(i) If $\beta = 0$, then $\alpha = 0$, which is not a limit ordinal. However, since $\alpha > \omega$, this case does not arise.

(ii) Assume $\beta = \delta+1$. Then,

$$\alpha = \omega\cdot(\delta+1) = \omega\cdot\delta+\omega,$$

which is a limit ordinal by Claim 5.12.

(iii) If β is a limit ordinal, then $\alpha = \omega\cdot\beta$ is also a limit ordinal by Claim 5.12.

Therefore, every limit ordinal α can be expressed as $\alpha = \omega\cdot\beta$ for some ordinal β. Conversely, if $\alpha = \omega\cdot\beta$ for some ordinal β, then α is a limit ordinal. ■

Proposition 5.28. Let α, β, and γ be ordinals.

(i) $\alpha^{\beta+\gamma} = \alpha^{\beta}\cdot\alpha^{\gamma}$

(ii) $(\alpha^{\beta})^{\gamma} = \alpha^{\beta\cdot\gamma}$

Proof. We first establish the following lemmas.

Lemma 5.9. Let α and β be ordinals. If $\alpha > 1$ and β is a nonzero limit ordinal, then α^β is a nonzero limit ordinal.

Proof of Lemma 5.9. Take any $\xi < \alpha^\beta$. Then, there exists $\gamma < \beta$ such that $\xi < \alpha^\gamma$ by (9). Therefore,

$$\xi + 1 \leq \alpha^\gamma < \alpha^{\gamma+1} \leq \alpha^\beta,$$

which shows that α^β is a limit ordinal. Additionally, since $\alpha > 1$ and β is nonzero, $\alpha^\beta \neq 0$. ■

Lemma 5.10. Let α be a nonzero ordinal. Then, $0^\alpha = 0$.

Proof of Lemma 5.10. We proceed by transfinite induction on α.

Base Case: $\alpha = 0$

$0^0 = 1$ by definition, but since α is nonzero, this case does not apply.

Successor Case: $\alpha = \delta + 1$

$0^{\delta+1} = 0^\delta \cdot 0 = 0$ by (4).

Limit Case: α is a limit ordinal

$$0^\alpha = \sup\{\, 0^\gamma \mid 0 < \gamma < \alpha \,\} = \sup\{\, 0 \,\} = 0.$$

■

Lemma 5.11. Let α be an ordinal. Then, $1^\alpha = 1$.

Proof of Lemma 5.11. We proceed by transfinite induction on α.

Base Case: $\alpha = 0$

$1^0 = 1$ by definition.

Successor Case: $\alpha = \delta + 1$

$1^{\delta+1} = 1^\delta \cdot 1 = 1$ by Induction Hypothesis and (5).

Limit Case: α is a limit ordinal

$$1^\alpha = \sup\{\, 1^\gamma \mid 0 < \gamma < \alpha \,\} = \sup\{\, 1 \,\} = 1.$$

■

(i) $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$ We prove this by transfinite induction on γ.

Base Case: $\gamma = 0$

$$\alpha^{\beta+0} = \alpha^\beta = \alpha^\beta \cdot 1 = \alpha^\beta \cdot \alpha^0.$$

Successor Case: $\gamma = \delta + 1$ Assume the statement holds for γ. Then,

$$\begin{aligned}
\alpha^{\beta+(\delta+1)} &= \alpha^{(\beta+\delta)+1} \quad \text{by ((i))} \\
&= \alpha^{\beta+\delta} \cdot \alpha \quad \text{by (8)} \\
&= (\alpha^{\beta} \cdot \alpha^{\delta}) \cdot \alpha \quad \text{by Induction Hypothesis} \\
&= \alpha^{\beta} \cdot (\alpha^{\delta} \cdot \alpha) \quad \text{by ((iii))} \\
&= \alpha^{\beta} \cdot \alpha^{\delta+1} \quad \text{by (8).}
\end{aligned}$$

Limit Case: γ is a limit ordinal Assume γ is a nonzero limit ordinal. For any $\xi < \alpha^{\beta+\gamma}$, there exists $\delta < \gamma$ such that $\xi < \alpha^{\beta+\delta}$. By the induction hypothesis,

$$\xi < \alpha^{\beta} \cdot \alpha^{\delta} \leq \alpha^{\beta} \cdot \alpha^{\gamma}.$$

Conversely, for any $\xi < \alpha^{\beta} \cdot \alpha^{\gamma}$, there exists $\delta < \gamma$ such that $\xi < \alpha^{\beta} \cdot \alpha^{\delta} = \alpha^{\beta+\delta}$. Hence, $\alpha^{\beta+\gamma} = \alpha^{\beta} \cdot \alpha^{\gamma}$.

(ii) $(\alpha^{\beta})^{\gamma} = \alpha^{\beta \cdot \gamma}$ We prove this by transfinite induction on γ.

Base Case: $\gamma = 0$

$$(\alpha^{\beta})^{0} = 1 = \alpha^{0} = \alpha^{\beta \cdot 0}.$$

Successor Case: $\gamma = \delta + 1$ Assume the statement holds for γ. Then,

$$\begin{aligned}
(\alpha^{\beta})^{\delta+1} &= (\alpha^{\beta})^{\delta} \cdot \alpha^{\beta} \quad \text{by (8)} \\
&= \alpha^{\beta \cdot \delta} \cdot \alpha^{\beta} \quad \text{by Induction Hypothesis} \\
&= \alpha^{\beta \cdot \delta + \beta} \quad \text{by Prop 5.18} \\
&= \alpha^{\beta \cdot (\delta+1)} \quad \text{by (5).}
\end{aligned}$$

Limit Case: γ is a limit ordinal Assume γ is a nonzero limit ordinal. For any $\xi < (\alpha^{\beta})^{\gamma}$, there exists $\delta < \gamma$ such that $\xi < (\alpha^{\beta})^{\delta}$. By the induction hypothesis,

$$\xi < \alpha^{\beta \cdot \delta} < \alpha^{\beta \cdot \gamma}.$$

Conversely, for any $\xi < \alpha^{\beta \cdot \gamma}$, there exists $\delta < \gamma$ such that $\xi < \alpha^{\beta \cdot \delta} = (\alpha^{\beta})^{\delta}$. Hence, $(\alpha^{\beta})^{\gamma} = \alpha^{\beta \cdot \gamma}$.

Therefore, both statements hold by transfinite induction. ■

Proposition 5.29. Let α, β, and γ be ordinals.

(i) $\alpha \leq \beta \implies \alpha^{\gamma} \leq \beta^{\gamma}$

(ii) $\alpha > 1 \wedge \beta < \gamma \implies \alpha^{\beta} < \alpha^{\gamma}$

Proof.

(i) We prove $\alpha^\gamma \leq \beta^\gamma$ by transfinite induction on γ.

Base Case: $\gamma = 0$

$$\alpha^0 = 1 \leq 1 = \beta^0.$$

Successor Case: $\gamma = \delta + 1$ Assume $\alpha^\delta \leq \beta^\delta$. Then,

$$\alpha^{\delta+1} = \alpha^\delta \cdot \alpha \leq \beta^\delta \cdot \beta = \beta^{\delta+1},$$

where the inequality follows from $\alpha \leq \beta$ and $\alpha, \beta > 0$.

Limit Case: γ is a limit ordinal Assume $\alpha^\gamma = \sup\{\alpha^\delta \mid \delta < \gamma\} \leq \sup\{\beta^\delta \mid \delta < \gamma\} = \beta^\gamma$.

Therefore, by transfinite induction, $\alpha^\gamma \leq \beta^\gamma$.

(ii) We prove $\alpha^\beta < \alpha^\gamma$ by transfinite induction on γ.

Base Case: $\gamma = 0$ Since $\gamma \neq 0$, this case does not apply.

Successor Case: $\gamma = \delta + 1$ Assume $\alpha^\beta < \alpha^\delta$. Then,

$$\alpha^{\delta+1} = \alpha^\delta \cdot \alpha > \alpha^\beta \cdot \alpha = \alpha^{\beta+1} > \alpha^\beta,$$

where the inequalities follow from $\alpha > 1$ and ordinal multiplication properties.

Limit Case: γ is a limit ordinal Assume $\alpha^\beta < \alpha^\delta$ for all $\delta < \gamma$. Then,

$$\alpha^\gamma = \sup\{\alpha^\delta \mid \delta < \gamma\} > \alpha^\beta.$$

Therefore, by transfinite induction, $\alpha^\beta < \alpha^\gamma$ whenever $\alpha > 1$ and $\beta < \gamma$.

■

Proposition 5.30. Find the least ordinal ξ such that:

(i) $\omega + \xi = \xi$.

(ii) $\omega \cdot \xi = \xi$ and $\xi \neq 0$.

(iii) $\omega^\xi = \xi$.

Proof.

(i) We have

$$\omega + \omega \cdot \omega = \omega \cdot (1 + \omega) = \omega \cdot \omega = \omega^2,$$

which satisfies $\omega + \omega^2 = \omega^2$. Therefore, the least such ordinal is ω^2.

(ii) We observe that

$$\omega \cdot \omega^\omega = \omega^{1+\omega} = \omega^\omega.$$

Hence, ω^ω satisfies $\omega \cdot \omega^\omega = \omega^\omega$ and $\omega^\omega \neq 0$. Therefore, the least such ordinal is ω^ω.

(iii) Define ε as the least ordinal satisfying $\omega^\varepsilon = \varepsilon$. This ordinal is known as ε_0 and is defined as:

$$\varepsilon_0 = \sup\{\, \omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \dots \}.$$

Therefore, the least ordinal ξ such that $\omega^\xi = \xi$ is ε_0.

■

Proposition 5.31. Let α and β be ordinals. Define $s\colon (\beta \to \alpha) \to \mathscr{P}(\beta)$ by

$$s(f) = \{\, \xi < \beta \mid f(\xi) \neq 0 \,\}.$$

Let

$$S(\beta, \alpha) = \{\, f\colon \beta \to \alpha \mid s(f) \text{ is finite} \,\}.$$

Define $\prec$ on $S(\beta, \alpha)$ as follows:

$$f \prec g \iff \exists \xi_0 < \beta \, [f(\xi_0) < g(\xi_0) \wedge (\forall \xi > \xi_0, f(\xi) = g(\xi))].$$

Then, $(S(\beta, \alpha), \prec)$ is isomorphic to α^β.

Proof. We first verify that $\prec$ is a strict total ordering on $S(\beta, \alpha)$.

Claim 5.16. $\prec$ is a strict total ordering on $S(\beta, \alpha)$.

Proof of Claim 5.16. Irreflexivity and Asymmetry: Suppose $f \prec g$ and $g \prec f$. Then, there exist $\xi_0, \xi_1 < \beta$ such that

$$f(\xi_0) < g(\xi_0) \quad \text{and} \quad g(\xi_1) < f(\xi_1),$$

with $f(\xi) = g(\xi)$ for all $\xi > \xi_0$ and $f(\xi) = g(\xi)$ for all $\xi > \xi_1$. Without loss of generality, assume $\xi_0 \leq \xi_1$. Then, $f(\xi_1) = g(\xi_1)$ since $\xi_1 > \xi_0$, which contradicts $g(\xi_1) < f(\xi_1)$. Hence, $\prec$ is asymmetric.

Transitivity: Suppose $f \prec g$ and $g \prec h$. Let $\xi_0 = \max\{\xi_f, \xi_g\}$, where ξ_f and ξ_g are the respective ordinals witnessing $f \prec g$ and $g \prec h$. Then,

$$f(\xi_0) \leq g(\xi_0) < h(\xi_0),$$

and $f(\xi) = h(\xi)$ for all $\xi > \xi_0$. Therefore, $f \prec h$.

Totality: For any distinct $f, g \in S(\beta, \alpha)$, let $\xi = \min\{\, \xi < \beta \mid f(\xi) \neq g(\xi) \,\}$. Then, either $f(\xi) < g(\xi)$ or $g(\xi) < f(\xi)$, and $f(\xi') = g(\xi')$ for all $\xi' > \xi$. Hence, $f \prec g$ or $g \prec f$. ■

Next, we construct an isomorphism between $(S(\beta, \alpha), \prec)$ and α^β.

We proceed by transfinite induction on β.

(i) Base Case: $\beta = 0$

$$S(0, \alpha) = \{\, f\colon 0 \to \alpha \,\} = \{\, f \,\},$$

where f is the empty function. Since $\alpha^0 = 1$, which corresponds to the single function in $S(0, \alpha)$, the base case holds.

(ii) Successor Case: $\beta = \delta + 1$ Assume there exists an isomorphism $h: S(\delta, \alpha) \to \alpha^\delta$. Define $h': S(\delta + 1, \alpha) \to \alpha^{\delta+1}$ by

$$h'(f) = (\alpha^\delta \cdot f(\delta), h(f \restriction \delta)).$$

Then, h' is an isomorphism between $(S(\delta+1,\alpha), \prec)$ and $\alpha^{\delta+1}$ by Prop 5.18.

(iii) Limit Case: β is a limit ordinal Assume β is a nonzero limit ordinal and that for all $\beta' < \beta$, there exists an isomorphism $h_{\beta'}: S(\beta', \alpha) \to \alpha^{\beta'}$.

Define $h: S(\beta, \alpha) \to \alpha^\beta$ by

$$h(f) = \sup\{ h_{\beta'}(f \restriction \beta') \mid \beta' < \beta \}.$$

Since f has finite support, this supremum exists and corresponds to the ordinal α^β. Therefore, h is an isomorphism.

Therefore, by transfinite induction, $(S(\beta,\alpha), \prec)$ is isomorphic to α^β. ■

5.5 The Normal Form

Lemma 5.12. Let α and β be ordinals.

(i) If $0 < \alpha \leq \beta$, then $\{ \xi \in \text{Ord} \mid \alpha \cdot \xi \leq \beta \}$ has a greatest element.
(ii) If $1 < \alpha \leq \beta$, then $\{ \xi \in \text{Ord} \mid \alpha^\xi \leq \beta \}$ has a greatest element.

Proof.

(i) Since $\beta < \beta + 1 \leq \alpha \cdot (\beta + 1)$ by 5.25, there exists δ such that $\alpha \cdot \delta > \beta$. Hence, $\delta_0 \triangleq \min\{ \xi \leq \delta \mid \alpha \cdot \xi > \beta \}$ exists by the Axiom of Comprehension and part (iv) of Theorem 5.2.

Suppose δ_0 is a limit ordinal for the sake of contradiction. We have $\delta_0 \neq 0$ by definition. There exists $\delta_1 < \delta_0$ such that $\beta < \alpha \cdot \delta_1$ by (6), which is immediately a contradiction. Hence, δ_0 must be a successor ordinal, i.e., $\delta_0 = \gamma + 1$ for some ordinal γ. Therefore, $\gamma = \max\{ \xi \in \text{Ord} \mid \alpha \cdot \xi \leq \beta \}$.

(ii) Replace every multiplication in the proof of (i) with exponentiation. The proof structure remains analogous.

■

Lemma 5.13. Let α and β be ordinals with $\alpha \neq 0$. Then, there uniquely exist ordinals γ and ρ such that $\beta = \alpha \cdot \gamma + \rho$ and $\rho < \alpha$.

Proof. Let $\gamma = \max\{ \xi \in \text{Ord} \mid \alpha \cdot \xi \leq \beta \}$ exist by part (i) of Lemma 5.12. By the Ordinal Division Algorithm (similar to Euclid's Division in natural numbers), there exists a unique ρ such that $\beta = \alpha \cdot \gamma + \rho$ and $\rho < \alpha$.

Uniqueness: Suppose $\beta = \alpha \cdot \gamma_1 + \rho_1 = \alpha \cdot \gamma_2 + \rho_2$ where $\rho_1, \rho_2 < \alpha$. If $\gamma_1 < \gamma_2$, then $\alpha \cdot \gamma_1 + \rho_1 < \alpha \cdot \gamma_2$ by part (i) of Proposition 5.25, contradicting $\alpha \cdot \gamma_1 + \rho_1 = \alpha \cdot \gamma_2 + \rho_2$. Hence, $\gamma_1 = \gamma_2$ and consequently, $\rho_1 = \rho_2$. ■

Theorem 5.13. Every ordinal $\alpha > 0$ can be uniquely expressed as

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n$$

where $k_1, k_2, \ldots, k_n$ are nonzero finite ordinals, and $\beta_1 > \beta_2 > \cdots > \beta_n$. The expression is called the *normal form* of α.

Proof. We prove the existence and uniqueness of the normal form by transfinite induction on α.

Base Case: $\alpha = 1$

$$1 = \omega^0 \cdot 1$$

is the normal form.

Induction Hypothesis: Assume every ordinal $\alpha' < \alpha$ has a unique normal form.

Successor Case: Suppose $\alpha = \omega^{\beta_1} \cdot k_1 + \cdots + \omega^{\beta_n} \cdot k_n$ is in normal form and we consider $\alpha + 1$. The normal form of $\alpha + 1$ is simply $\alpha + 1$ since adding 1 does not disrupt the decreasing exponents.

Limit Case: Let α be a limit ordinal. By part (ii) of Lemma 5.12, there exists γ such that $\omega^\gamma \leq \alpha < \omega^{\gamma+1}$. Using Lemma 5.13, we can express α as

$$\alpha = \omega^\gamma \cdot k + \rho$$

where $\rho < \omega^\gamma$. By the induction hypothesis, ρ has a unique normal form with exponents less than γ. Thus, the normal form of α is

$$\omega^\gamma \cdot k + (\text{normal form of } \rho)$$

ensuring that the exponents are in strictly decreasing order.

Uniqueness: Suppose α has two normal forms:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \cdots + \omega^{\beta_n} \cdot k_n = \omega^{\gamma_1} \cdot \ell_1 + \cdots + \omega^{\gamma_m} \cdot \ell_m.$$

By comparing the highest exponents, $\beta_1 = \gamma_1$ and $k_1 = \ell_1$. Removing these terms and applying the induction hypothesis to the remaining parts ensures that all exponents and coefficients match uniquely. ■

Definition 5.15 (Weak Goodstein Sequence)**.** Let $g: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a function defined by:

$$g(n,b) = \sum_{i=0}^{m} c_i \cdot (b+1)^i - 1$$

where $n = \sum_{i=0}^{m} c_i \cdot b^i$ is the base-b representation of n. If $n = 0$ or $b \leq 1$, define $g(n,b) = 0$.

The *weak Goodstein sequence starting at* $m > 0$ is the infinite sequence $\langle m_i \rangle_{i \in \mathbb{N}}$ such that:

(i) $m_0 = m$, and

(ii) for all $k \in \mathbb{N}$, $m_{k+1} = g(m_k, k+2)$.

The existence and uniqueness of such a sequence are guaranteed by the Recursion Theorem.

Remark. First few terms of the weak Goodstein sequence starting at $m = 21$ are:

$$m_0 = 21 = 2^4 + 2^2 + 1$$
$$m_1 = 3^4 + 3^2 = 90$$
$$m_2 = 4^4 + 3 \cdot 4^1 + 3 = 271$$
$$m_3 = 5^4 + 3 \cdot 5^1 + 2 = 642$$
$$m_4 = 6^4 + 3 \cdot 6^1 + 1 = 1315$$
$$m_5 = 7^4 + 3 \cdot 7^1 = 2422$$
$$m_6 = 8^4 + 2 \cdot 8^1 + 7 = 4119$$
$$m_7 = 9^4 + 2 \cdot 9^1 + 6 = 6585$$
$$m_8 = 10^4 + 2 \cdot 10^1 + 5 = 10025$$

Lemma 5.14. There is no strictly decreasing infinite sequence of ordinal numbers. An infinite sequence f of ordinal numbers is *strictly decreasing* if $\forall n \in \mathbb{N},\ f(n+1) < f(n)$.

Proof of Lemma 5.14. Suppose f is a strictly decreasing infinite sequence of ordinal numbers. Since ordinals are well-ordered by $\leq$, the set $\operatorname{ran} f$ must have a least element. However, because f is strictly decreasing, no such least element can exist within an infinite sequence, leading to a contradiction. Hence, no such infinite strictly decreasing sequence exists. ■

Theorem 5.14. For each $m \in \mathbb{N}_{>0}$, the weak Goodstein sequence starting at m eventually terminates with $m_n = 0$ for some n.

Proof of Theorem 5.14. Let $m > 0$ and consider the weak Goodstein sequence $\langle m_i \rangle_{i \in \mathbb{N}}$ starting at m.

Suppose $m_i > 0$ for all $i \in \mathbb{N}$ for the sake of contradiction. For each $a \in \mathbb{N}$, write m_a in base-$(a+2)$ as:

$$m_a = \sum_{i=0}^{m} c_i \cdot (a+2)^i$$

where $c_i < a+2$. Define:

$$\alpha_a = \sum_{i=0}^{m} \omega^{d_i} \cdot k_i$$

where d_i corresponds to the exponents in the hereditary base-$(a+2)$ notation and $k_i = c_i$.

The sequence $\langle \alpha_0, \alpha_1, \alpha_2, \ldots \rangle$ is strictly decreasing because at each step, the base increases and the representation changes such that $\alpha_{a+1} < \alpha_a$.

However, by Lemma 5.14, no such infinite strictly decreasing sequence of ordinals can exist. This contradiction implies that the weak Goodstein sequence must terminate, i.e., there exists some n such that $m_n = 0$. ■

Remark. The *hereditary base-n notation* is a base-n notation where every exponent is itself written in a hereditary base-n notation. For instance,

$$100 = \omega^{\omega^1} + \omega^2 + 1$$

is the hereditary base-3 notation of 100.

Definition 5.16 (Goodstein Sequence)**.** The Goodstein sequence starting at $m > 0$ is the sequence $\langle m_i \rangle_{i \in \mathbb{N}}$ where:

(i) $m_0 = m$, and

(ii) for each $k \in \mathbb{N}$, m_{k+1} is obtained by writing m_k in hereditary base-$(k+2)$ notation, replacing every occurrence of $k+2$ with $k+3$, and then subtracting one.

The existence and uniqueness of such a sequence are guaranteed by the Recursion Theorem.

Remark. First few terms of the Goodstein sequence starting at $m = 21$ are:

$$
\begin{aligned}
m_0 &= 21 = 2^{2^{2^1}} + 2^{2^1} + 1 \\
m_1 &= 3^{3^{3^1}} + 3^{3^1} = 7625597485014 \\
m_2 &= 4^{4^{4^1}} + 3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4^1 + 3 = 4^{4^{4^1}} + 3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4^1 + 3 \\
&\approx 1.340781 \times 10^{155} \\
m_3 &= 5^{5^{5^1}} + 3 \cdot 5^3 + 3 \cdot 5^2 + 3 \cdot 5^1 + 2 \\
&\approx 1.911013 \times 10^{2184} \\
m_4 &= 6^{6^{6^1}} + 3 \cdot 6^3 + 3 \cdot 6^2 + 3 \cdot 6^1 + 1 \\
&\approx 2.659120 \times 10^{36305} \\
m_5 &= 7^{7^{7^1}} + 3 \cdot 7^3 + 3 \cdot 7^2 + 3 \cdot 7^1 \\
&\approx 3.759824 \times 10^{695974} \\
m_6 &= 8^{8^{8^1}} + 3 \cdot 8^3 + 3 \cdot 8^2 + 2 \cdot 8^1 + 7 \\
&\approx 6.014521 \times 10^{15151335}
\end{aligned}
$$

Theorem 5.15. Goodstein's Theorem: For each $m > 0$, the Goodstein sequence starting at m eventually terminates with $m_n = 0$ for some $n \in \mathbb{N}$.

Proof. Let $m > 0$ and consider the Goodstein sequence $\langle m_i \rangle_{i \in \mathbb{N}}$ starting at m.

Suppose, for contradiction, that $m_i > 0$ for all $i \in \mathbb{N}$. For each $a \in \mathbb{N}$, write m_a in hereditary base-$(a+2)$ notation as:

$$m_a = \sum_{i=0}^{m} c_i \cdot (a+2)^i$$

where $c_i < a+2$. Define:

$$\alpha_a = \sum_{i=0}^{m} \omega^{d_i} \cdot k_i$$

where d_i corresponds to the exponents in the hereditary base-$(a+2)$ notation and $k_i = c_i$.

The sequence $\langle \alpha_0, \alpha_1, \alpha_2, \ldots \rangle$ is strictly decreasing because at each step, the base increases and the representation changes such that $\alpha_{a+1} < \alpha_a$.

However, by Lemma 5.14, no such infinite strictly decreasing sequence of ordinals can exist. This contradiction implies that the Goodstein sequence must terminate, i.e., there exists some n such that $m_n = 0$. ■

6 Aleph

6.1 Initial Ordinals

Definition 6.1 (Initial Ordinal)**.** An ordinal number α is called an *initial ordinal* if it is not equipotent to any $\beta < \alpha$.

Example.

- Every natural number is an initial ordinal.
- ω is an initial ordinal. (See part (iii)).
- None of $\omega+1, \omega+2, \ldots, \omega\cdot\omega, \ldots, \omega^\omega, \ldots$ is initial.

Theorem 6.1. Each well-orderable set X is equipotent to a unique initial ordinal number.

Proof. By Theorem 5.3, there exists an ordinal number α such that $|X| = |\alpha|$. Hence, $\alpha_0 \triangleq \min\{\, \xi \in \mathrm{Ord} \mid |X| = |\xi| \,\}$ exists by the Axiom of Comprehension and part (iv) of Theorem 5.2.

Claim 6.1. α_0 is a limit ordinal.

Proof of Claim 6.1. Suppose, for contradiction, that α_0 is not a limit ordinal. Then, $\alpha_0 = \delta + 1$ for some ordinal δ. Since $\delta < \alpha_0$, by the definition of α_0, there exists a limit ordinal $\gamma < \alpha_0$ such that $|\gamma| = |X|$, which contradicts the minimality of α_0. Therefore, α_0 must be a limit ordinal. ■

By the uniqueness part, α_0 is the unique initial ordinal equipotent to X. ■

Definition 6.2 (Cardinality of Well-Orderable Sets)**.** If X is a well-orderable set, we define $|X|$ to be the unique initial ordinal which is equipotent to X. This is justified by Theorem 6.1.

Lemma 6.1. Let A be any set. Then, there exists the least ordinal number α such that $|\alpha| \not\leq |A|$.

Proof. By Theorem 5.3, for each well-ordered set (W,R) where $W \subseteq A$, there exists a unique ordinal α such that $(W,R) \cong \alpha$. Hence, by the Axiom of Replacement, the set

$$H \triangleq \{\, \alpha \in \mathrm{Ord} \mid \exists R \subseteq A \times A,\ (\mathrm{field}R, R) \cong \alpha \,\}$$

exists.

Claim 6.2. $\forall \alpha \in \mathrm{Ord},\ (|\alpha| \leq |A| \iff \alpha \in H)$.

Proof of Claim 6.2.

($\Rightarrow$) If $|\alpha| \leq |A|$, then there exists an injective function $f\colon \alpha \hookrightarrow A$. Let $W = \mathrm{ran}f$, and define $R = \{\, (f(\beta), f(\gamma)) \mid \beta < \gamma < \alpha \,\}$. Then, (W,R) is a well-ordered set isomorphic to α, so $\alpha \in H$.

($\Leftarrow$) If $\alpha \in H$, then there exists a well-ordering $R \subseteq A \times A$ such that $(\text{field}R, R) \cong \alpha$. Hence, $|\alpha| \leq |A|$.

■

As H is a set of ordinal numbers, it is well-ordered by $\in$. Moreover, if $\alpha \in \beta \in H$, then $\alpha \subsetneq \beta$ by Lemma 5.6; thus $|\alpha| \leq |\beta| \leq |A|$ by Theorem 4.3, which implies $\alpha \in H$ by Claim 6.2. Hence, $H \in \text{Ord}$.

We have $H \notin H$ by Lemma 5.4; hence $|H| \not\leq |A|$ by Claim 6.2. Moreover, every $\alpha < H$ satisfies $|\alpha| \leq |A|$ by Claim 6.2; therefore, H is the least ordinal we are looking for. ■

Definition 6.3 (Hartogs Number)**.** For any set A, let $h(A)$ denote the least ordinal α such that $|\alpha| \not\leq |A|$. $h(A)$ is called the *Hartogs number* of A. This is justified by Lemma 6.1.

Lemma 6.2. $\forall \alpha \in \text{Ord}$, $|\alpha| < |h(\alpha)|$.

Proof. Suppose $\alpha \in \text{Ord}$.

- If $\alpha = h(\alpha)$, then $|h(\alpha)| \not\leq |\alpha|$, which is impossible since $|\alpha| = |h(\alpha)|$. Hence, $\alpha \neq h(\alpha)$.
- If $\alpha > h(\alpha)$, then $|h(\alpha)| \leq |\alpha|$ by Theorem 4.3 and lemma 5.6, which contradicts the definition of $h(\alpha)$.

Therefore, $\alpha < h(\alpha)$. Then, by Theorem 4.3 and lemma 5.6, $|\alpha| \leq |h(\alpha)|$. But $|\alpha| \neq |h(\alpha)|$ since $|h(\alpha)| \not\leq |\alpha|$. Hence, $|\alpha| < |h(\alpha)|$. ■

Lemma 6.3. For any set A, $h(A)$ is an initial ordinal.

Proof of Lemma 6.3. Suppose that there exists $\beta < h(A)$ such that $|\beta| = |h(A)|$. Then, $|\beta| \leq |A|$ by the definition of $h(A)$, while $|\beta| = |h(A)|$, which contradicts $|h(A)| \not\leq |A|$. Therefore, no such β exists, and $h(A)$ is an initial ordinal. ■

Definition 6.4 (Ordinal Omega)**.**

$$\begin{aligned} \omega_0 &= \omega \\ \omega_{\alpha+1} &= h(\omega_\alpha) && \text{for all ordinals } \alpha \\ \omega_\alpha &= \sup\{\, \omega_\beta \mid \beta < \alpha \,\} && \text{for all nonzero limit ordinals } \alpha \end{aligned}$$

Remark. Since $|\omega_{\alpha+1}| \not\leq |\omega_\alpha|$, we have $|\omega_\alpha| < |\omega_{\alpha+1}|$ as one of the two ordinals must have the other as its subset. Therefore, with Theorem 5.6, one can prove that $\alpha < \beta \implies |\omega_\alpha| < |\omega_\beta|$.

Theorem 6.2. (i) For each $\alpha \in \text{Ord}$, ω_α is an infinite initial ordinal number.
(ii) If Ω is an infinite initial ordinal number, then there exists $\alpha \in \text{Ord}$ such that $\Omega = \omega_\alpha$.

Proof.

(i) ω_α is infinite for all $\alpha \in \text{Ord}$ by construction. If $\alpha = 0$ or α is a successor ordinal, then ω_α is an initial ordinal by Lemma 6.3.

Suppose α is a nonzero limit ordinal. Assume, for contradiction, that there exists $\gamma < \omega_\alpha$ such that $|\gamma| = |\omega_\alpha|$. By Lemma 6.2, $|\gamma| < |\omega_\alpha|$, which is a contradiction. Therefore, ω_α is an initial ordinal.

(ii) We first prove the following claim.

Claim 6.3. For each ordinal α and infinite initial ordinal $\Omega < \omega_\alpha$, there exists $\gamma < \alpha$ such that $\Omega = \omega_\gamma$.

Proof of Claim 6.3. We will use transfinite induction on α.

Base Case: $\alpha = 0$

$$\omega_0 = \omega$$

is the least infinite initial ordinal.

Successor Case: Assume the claim holds for α. Let $\Omega < \omega_{\alpha+1} = h(\omega_\alpha)$. Then, by the definition of the Hartogs number, $|\Omega| \leq |\omega_\alpha|$. Since Ω is an initial ordinal, $|\Omega| \neq |\omega_\alpha|$, thus $\Omega < \omega_\alpha$. By the induction hypothesis, there exists $\gamma < \alpha$ such that $\Omega = \omega_\gamma$.

Limit Case: Assume α is a nonzero limit ordinal and the claim holds for all $\beta < \alpha$. Let $\Omega < \omega_\alpha$. Then, there exists $\beta < \alpha$ such that $\Omega < \omega_\beta$. By the induction hypothesis, there exists $\gamma < \beta < \alpha$ such that $\Omega = \omega_\gamma$. ■

Now, take any infinite initial ordinal Ω. Then, $\Omega \leq \omega_\Omega$ by the definition of ω_α. If $\Omega = \omega_\Omega$, then it satisfies the condition. If $\Omega < \omega_\Omega$, then by Claim 6.3, there exists $\gamma < \Omega$ such that $\Omega = \omega_\gamma$. Hence, every infinite initial ordinal is of the form ω_γ for some $\gamma \in \text{Ord}$.

■

Definition 6.5 (Alephs)**.** For each $\alpha \in \text{Ord}$, define $\aleph_\alpha = \omega_\alpha$. The Alephs represent the cardinalities of well-orderable infinite sets.

Proposition 6.1. If X is an infinite well-orderable set, then X has nonisomorphic well-orderings.

Proof. Let $R \subseteq X \times X$ be a well-ordering of X. Then, by Theorem 6.1, there exists a unique ordinal α such that $(X, R) \cong \alpha$. Let $f : X \hookrightarrow \alpha$.

By Proposition 5.5, $\omega \subseteq \alpha$. By Theorem 4.25, there exists a bijection $g : \omega \hookrightarrow (\omega \cup \{\alpha\})$. Define $f' : X \hookrightarrow (\alpha + 1)$ by

$$f'(x) \triangleq \begin{cases} g(f(x)) & \text{if } f(x) \in \omega, \\ f(x) & \text{otherwise.} \end{cases}$$

Then, $R' \triangleq \{\, (x,y) \in X^2 \mid f'(x) < f'(y) \,\}$ is a well-ordering of X isomorphic to $\alpha + 1$. Since $\alpha + 1 \neq \alpha$, the well-orderings R and R' are nonisomorphic. ■

Proposition 6.2. Let $\alpha, \beta \in \text{Ord}$ where α and β are countable. Then, $\alpha + \beta$, $\alpha \cdot \beta$, and α^β are countable.

Proof. This is a special case of Proposition 6.8. ■

Proposition 6.3.

$$\forall A,\ \exists f : \mathscr{P}(A \times A) \twoheadrightarrow h(A)$$

Proof. For each well-ordering R of $W \subseteq A$, let α_R be the unique ordinal isomorphic to (W,R) thanks to Theorem 6.1. Note that $|\alpha_R| = |W| \leq |A|$ since $W \subseteq A$, and thus $\alpha_R < h(A)$ by Lemma 6.2. Define a function $f : \mathscr{P}(A \times A) \to h(A)$ by

$$f(R) \triangleq \begin{cases} \alpha_R & \text{if } R \text{ is a well-ordering of field}R, \\ 0 & \text{otherwise.} \end{cases}$$

Then, $\operatorname{ran} f$ exactly equals H defined in the proof of Lemma 6.1, which in turn equals $h(A)$. Therefore, f is a surjection from $\mathscr{P}(A \times A)$ to $h(A)$. ■

Proposition 6.4.

$$\forall A,\ |A| < |A| + |h(A)|$$

Proof. Without loss of generality, assume $A \cap h(A) = \emptyset$. Since we already have $|A| \leq |A| + |h(A)|$, we only need to prove $|A| \neq |A| + |h(A)|$.

Suppose $|A| = |A| + |h(A)|$ for the sake of contradiction. Then, we have $|h(A)| \leq |A| + |h(A)| = |A|$, which contradicts $|h(A)| \not\leq |A|$. ■

Proposition 6.5.

$$\forall A,\ |h(A)| < |\mathscr{P}(\mathscr{P}(A \times A))|$$

Proof. As in the proof of Lemma 6.1, $\alpha \in h(A)$ if and only if there exists some $R \subseteq A \times A$ such that $(\text{field}R, R) \cong \alpha$. Define $f : \mathscr{P}(h(A)) \to \mathscr{P}(\mathscr{P}(A \times A))$ by

$$f(X) \triangleq \{\, R \subseteq A \times A \mid \exists \alpha \in X,\ (\text{field}R, R) \cong \alpha \,\}.$$

Then, f is injective; thus

$$|h(A)| < |\mathscr{P}(h(A))| \leq |\mathscr{P}(\mathscr{P}(A \times A))|$$

by Theorem 4.38. ■

Proposition 6.6. Let $h^*(A)$ be the least ordinal α such that there does not exist $f : A \twoheadrightarrow \alpha$.

(i) $h^*(A)$ exists for all A.
(ii) $\forall \alpha \in \text{Ord},\ (\alpha \geq h^*(A) \implies \nexists f : A \twoheadrightarrow \alpha)$.
(iii) $h^*(A)$ is an initial ordinal.
(iv) $h(A) \leq h^*(A)$.
(v) If A is well-orderable, then $h(A) = h^*(A)$.

Proof.

(i) Let $\text{Pt}(A)$ be the set of all partitions of A. Define

$$H^* \triangleq \{\, \alpha \in \text{Ord} \mid \exists S \in \text{Pt}(A),\ \exists R \subseteq S \times S,\ (S,R) \cong \alpha \,\}.$$

H^* exists by Theorem 5.3 and the Axiom of Scheme Replacement.

Claim 6.4. $\forall \alpha \in \mathrm{Ord}, (\exists f{:}A \twoheadrightarrow \alpha \iff \alpha \in H^*)$.

Proof.

($\Rightarrow$) Let $f{:}A \twoheadrightarrow \alpha$. Then, $S \triangleq \{ f^{-1}[\{\beta\}] \mid \beta < \alpha \}$ is a partition of A, and the relation $R = \{ (f^{-1}[\{\beta\}], f^{-1}[\{\gamma\}]) \mid \beta < \gamma < \alpha \}$ is isomorphic to α. Hence, $\alpha \in H^*$.

($\Leftarrow$) If $\alpha \in H^*$, then there exists $S \in \mathrm{Pt}(A)$ and $R \subseteq S \times S$ such that $(S,R) \cong \alpha$. Let $g{:}S \hookrightarrow \alpha$ be the isomorphism. Define $f{:}A \to \alpha$ by

$$f(a) \triangleq g(C) \quad \text{where } C \in S \text{ is the unique element such that } a \in C.$$

Then, f is surjective since $\mathrm{rang} = \alpha$.

■

By Claim 6.4, H^* consists exactly of those ordinals α for which there exists a surjection $f{:}A \twoheadrightarrow \alpha$. Since H^* is a set of ordinals, it is well-ordered by $\in$. Moreover, if $\alpha \in \beta \in H^*$, then $\alpha \subsetneq \beta$ by Lemma 5.6; thus $|\alpha| \leq |\beta| \leq |A|$ by Theorem 4.3, which implies $\alpha \in H^*$ by Claim 6.4. Hence, $H^* \in \mathrm{Ord}$. We have $H^* \notin H^*$ by Lemma 5.4; hence $\nexists f{:}A \twoheadrightarrow H^*$ by Claim 6.4. If $\alpha \in H^*$, then $\exists f{:}A \twoheadrightarrow \alpha$ by Claim 6.4. Therefore, $h^*(A) = H^*$.

(ii) Take any $\alpha \in \mathrm{Ord}$. Assume $\exists f{:}A \twoheadrightarrow \alpha$. Then, by Claim 6.4, $\alpha < h^*(A)$.

(iii) Suppose $|h(A)| \leq |A|$. Then, by the definition of $h(A)$, $|h(A)| \not\leq |A|$, which is a contradiction. Hence, $h(A) \leq h^*(A)$.

(iv) If A is well-orderable, then $h(A) = h^*(A)$.

Proof. Assume A is well-orderable. By Theorem 6.1, each ordinal $\alpha < h(A)$ can be mapped onto by a well-ordering of A. Conversely, by the definition of $h^*(A)$, no ordinal $\alpha \geq h^*(A)$ can be mapped onto by A. Hence, $h(A)$ is the least ordinal not surjectively mapped onto by A, which implies $h(A) = h^*(A)$. ■

■

Remark.

- Every infinite well-orderable set is equipotent to a unique infinite initial ordinal number. (See Theorem 6.1)
- α is an infinite initial ordinal if and only if $\alpha = \omega_\gamma$ for some $\gamma \in \mathrm{Ord}$. (See Theorem 6.2)

6.2 Addition and Multiplication

Theorem 6.3 (Square of Alephs)**.** $\forall \alpha \in \mathrm{Ord}, \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$

Proof. Take any ordinal α and define $\preceq$ on $\omega_\alpha \times \omega_\alpha$ by

$$(\alpha_1, \alpha_2) \preceq (\beta_1, \beta_2) \iff (\max\{\alpha_1, \alpha_2\}, \alpha_1, \alpha_2) \leq_\alpha (\max\{\beta_1, \beta_2\}, \beta_1, \beta_2)$$

where $\leq_\alpha$ is the lexicographical ordering of $\omega_\alpha \times \omega_\alpha \times \omega_\alpha$. Then, $\preceq$ is naturally a well-ordering of $\omega_\alpha \times \omega_\alpha$ since R_α is a well-ordering.

Now, we will prove by transfinite induction on α. We already have $\aleph_0 \cdot \aleph_0 = \aleph_0$ by Theorem 4.19.

Assume for induction that for all $\beta < \alpha$, $\aleph_\beta \cdot \aleph_\beta \leq \aleph_\beta$.

Claim 6.5. For any $(\alpha_1, \alpha_2) \in \omega_\alpha \times \omega_\alpha$, we have $|X| < \aleph_\alpha$ where

$$X \triangleq \{\, (\xi_1, \xi_2) \in \omega_\alpha \times \omega_\alpha \mid (\xi_1, \xi_2) \prec (\alpha_1, \alpha_2) \,\}.$$

Proof of Claim 6.5. Let $\beta \triangleq \max\{\alpha_1, \alpha_2\} + 1$. We have $\beta < \omega_\alpha$. Then, for every $(\xi_1, \xi_2) \in X$,

$$\max\{\xi_1, \xi_2\} \leq \max\{\alpha_1, \alpha_2\} < \beta$$

by definition. Hence, $\xi_1 < \beta$ and $\xi_2 < \beta$. In other words, $X \subseteq \beta \times \beta$.

As ω_α is an initial ordinal, $|\beta| < \aleph_\alpha$. Moreover, by Theorem 6.1, there exists $\gamma < \alpha$ such that $|\beta| \leq \aleph_\gamma$. Therefore,

$$\begin{aligned} |X| &\leq |\beta \times \beta| && \text{(by Theorem 4.3)} \\ &\leq \aleph_\gamma \cdot \aleph_\gamma \\ &\leq \aleph_\gamma && \text{(Induction Hypothesis)} \\ &< \aleph_\alpha. \end{aligned}$$

■

If the order type of $(\omega_\alpha \times \omega_\alpha, \preceq)$ were greater than ω_α, then there exists an initial segment X of $(\omega_\alpha \times \omega_\alpha, \preceq)$ such that $|X| = \aleph_\alpha$, which is impossible by Claim 6.5. Hence, $\aleph_\alpha \cdot \aleph_\alpha \leq \aleph_\alpha$. The result follows from Theorem 5.5. ■

Corollary.

(i) $\forall \alpha, \beta \in \text{Ord}, (\alpha \leq \beta \implies \aleph_\alpha \cdot \aleph_\beta = \aleph_\beta)$
(ii) $\forall \alpha \in \text{Ord}, \forall n \in \mathbb{N}, n \cdot \aleph_\alpha = \aleph_\alpha$

Proof.

(i) It is direct that $\aleph_\beta = 1 \cdot \aleph_\beta \leq \aleph_\alpha \cdot \aleph_\beta$. On the other hand, by Theorem 6.3, $\aleph_\alpha \cdot \aleph_\beta \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta$. Hence, by the (Theorem 4.1), $\aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$.
(ii) It is direct that $\aleph_\alpha = 1 \cdot \aleph_\alpha \leq n \cdot \aleph_\alpha$. On the other hand, by Theorem 6.3, $n \cdot \aleph_\alpha \leq \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$. Hence, by the (Theorem 4.1), $n \cdot \aleph_\alpha = \aleph_\alpha$.

■

Corollary.

(i) $\forall \alpha, \beta \in \text{Ord}, (\alpha \leq \beta \implies \aleph_\alpha + \aleph_\beta = \aleph_\beta)$
(ii) $\forall \alpha \in \text{Ord}, \forall n \in \mathbb{N}, n + \aleph_\alpha = \aleph_\alpha$

Proof.

(i) $\aleph_\beta \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\beta + \aleph_\beta = 2 \cdot \aleph_\beta = \aleph_\beta$. Hence, by the (Theorem 4.1), $\aleph_\alpha + \aleph_\beta = \aleph_\beta$.

(ii) $\aleph_\alpha \leq n + \aleph_\alpha \leq \aleph_\alpha + \aleph_\alpha = 2 \cdot \aleph_\alpha = \aleph_\alpha$. Hence, by the (Theorem 4.1), $n + \aleph_\alpha = \aleph_\alpha$.

■

Proposition 6.7. Let $0 < n < \omega$ and $\alpha \in \mathrm{Ord}$.

(i) $\aleph_\alpha^n = \aleph_\alpha$.

(ii) $|[\aleph_\alpha]^n| = \aleph_\alpha$. (See Theorem 4.27 for notation.)

(iii) $|[\aleph_\alpha]^{<\omega}| = \aleph_\alpha$ where $[\aleph_\alpha]^{<\omega} = \bigcup_{n\in\omega}[\aleph_\alpha]^n$.

Proof. This is a special case of Proposition 6.8. ■

Proposition 6.8. Let $\alpha, \beta \in \mathrm{Ord}$, and assume $|\alpha| \leq \aleph_\gamma$ and $|\beta| \leq \aleph_\gamma$. Then, $|\alpha + \beta| \leq \aleph_\gamma$, $|\alpha \cdot \beta| \leq \aleph_\gamma$, and $|\alpha^\beta| \leq \aleph_\gamma$.

Proof. We directly have $|\alpha + \beta| \leq \aleph_\gamma$ and $|\alpha \cdot \beta| \leq \aleph_\gamma$ from Theorem 6.3 and Corollary 6.2.

It is evident that, if β is finite, $|\alpha^\beta| \leq \aleph_\gamma$. One may prove this by transfinite induction (Theorem 5.5).

By Prop 5.31, $|\alpha^\beta| = |X|$ where

$$X \triangleq \{ f : \beta \to \alpha \mid s(f) \text{ is finite} \}$$

and $s(f) \triangleq \{ \xi < \beta \mid f(\xi) \neq 0 \}$.

For each $n \in \omega$, let $A_n \triangleq \{ f : \beta \to \alpha \mid |s(f)| = n \} \subseteq X$. Let $P_n \triangleq \{ \text{injections on } n \text{ into } \beta \}$, whose cardinality is at most $\aleph_\gamma^n = \aleph_\gamma$ by Corollary 6.2.(i). Hence, for all $0 < n < \omega$,

$$\begin{aligned} |A_n| &= |P_n \times \prod_{i<n} \alpha| && \text{(by Prop 4.3)} \\ &\leq \aleph_\gamma \cdot \aleph_\gamma^n \\ &= \aleph_\gamma. && \text{(by Corollary 6.2.(i))} \end{aligned}$$

Moreover, A_n is well-ordered by $\preceq$ (in Prop 5.31); hence there exists a unique ordinal η_n isomorphic to A_n by Theorem 6.1. Let h_n be the unique isomorphism between η_n and A_n. As $\eta_n \leq \omega_\gamma$, extend h_n by

$$h_n' \triangleq h_n \cup \{ (\xi, \min_{\preceq} A_n) \mid \eta_n \leq \xi < \omega_\gamma \}$$

so that $h_n' : \aleph_\gamma \twoheadrightarrow A_n$. Define $g : \omega \times \aleph_\gamma \twoheadrightarrow X$ by $g(n, \beta) = h_n'(\beta)$. Therefore, $|X| \leq |\omega \times \aleph_\gamma| = \aleph_\gamma$ in a similar manner as the proof of Prop 6.7.(iii). ■

Proposition 6.9. Let $\alpha \in \mathrm{Ord}$ and let f be a function on α. Then, $|\mathrm{ran} f| \leq |\alpha|$.

Proof. Define $g : f[\alpha] \hookrightarrow \alpha$ by

$$g(x) = \min f^{-1}[\{x\}].$$

Then, g is injective, as each $x \in \mathrm{ran} f$ is mapped to the smallest ordinal β such that $f(\beta) = x$. Therefore, $|\mathrm{ran} f| \leq |\alpha|$. ■

Proposition 6.10. Let $X \subseteq \omega_\alpha$ with $|X| < \aleph_\alpha$. Then, $|\omega_\alpha - X| = \aleph_\alpha$.

Proof. The statement is true when $\alpha = 0$, as $\omega_0 = \omega$ and removing a finite or countable subset from ω leaves ω, which is still countable.

Hence, assume $\alpha > 0$. We already have $|\omega_\alpha - X| \leq \aleph_\alpha$ by Prop 4.3. Suppose $|\omega_\alpha - X| < \aleph_\alpha$ for the sake of contradiction.

By Theorem 6.1, there exist $\beta_1, \beta_2 \in \omega_\alpha$ such that $|\beta_1| = |X|$ and $|\beta_2| = |\omega_\alpha - X|$. Let $\gamma_0 \triangleq \max\{\gamma_1, \gamma_2\}$. Then,

$$\begin{aligned} |\omega_\alpha| &= |X| + |\omega_\alpha - X| \\ &\leq \aleph_{\gamma_1} + \aleph_{\gamma_2} \\ &\leq \aleph_{\gamma_0} + \aleph_{\gamma_0} \\ &= \aleph_{\gamma_0} && \text{(by Corollary 6.2)} \\ &< \aleph_\alpha, \end{aligned}$$

which is a contradiction. ■

7 Axiom of Choice

Definition 7.1 (Choice Function)**.** A function $g: S \to \bigcup S$ is called a *choice function for S* if

$$\forall X \in S,\ (X \neq \varnothing \implies g(X) \in X).$$

Theorem 7.1 (Well-Ordering Theorem)**.** A set A can be well-ordered if and only if the set $\mathscr{P}(A)$ has a choice function.

Proof.

($\Rightarrow$) Assume $\preceq$ well-orders A. Define $g: \mathscr{P}(A) \to A$ by

$$g(X) \triangleq \begin{cases} \min_{\preceq} X & \text{if } X \neq \varnothing, \\ \varnothing & \text{otherwise.} \end{cases}$$

Then, g is a choice function for $\mathscr{P}(A)$.

($\Leftarrow$) Fix any choice function $g: \mathscr{P}(A) \to A$ for $\mathscr{P}(A)$ and any element $a \notin A$. Let $\mathbf{G}(x)$ be the operation defined by

$$\mathbf{G}(x) \triangleq \begin{cases} g(A - \operatorname{ran}(x)) & \text{if } x \text{ is a function and } A - \operatorname{ran}(x) \neq \varnothing, \\ a & \text{otherwise.} \end{cases}$$

Then, by the Transfinite Recursion Theorem (Theorem 5.7), there exists an operation $\mathbf{F}(x)$ such that

$$\forall \alpha \in \mathrm{Ord},\ \mathbf{F}(\alpha) = \mathbf{G}\left(\mathbf{F} \restriction_\alpha\right).$$

Claim 7.1. There exists $\lambda < h(A)$ such that $\mathbf{F}(\lambda) = a$.

Proof of Claim 7.1. Assume $\alpha < \beta$ and $\mathbf{F}(\beta) \neq a$. Then, $\mathbf{F}(\beta) \in A - \operatorname{ran}(\mathbf{F} \restriction_\beta)$ and $\mathbf{F}(\alpha) \in \operatorname{ran}(\mathbf{F} \restriction_\beta)$; thus, $\mathbf{F}(\alpha) \neq \mathbf{F}(\beta)$. Hence, $\mathbf{F} \restriction_{\beta+1}$ is injective if $\mathbf{F}(\beta) \neq a$.
Suppose $\forall \alpha < h(A), \mathbf{F}(\alpha) \neq a$ for the sake of contradiction. Then, $\mathbf{F} \restriction_{h(A)}$ is an injection on $h(A)$ into A by the preceding discussion, which contradicts the definition of $h(A)$. ■

Hence, by Claim 7.1, we may let $\lambda \triangleq \min\{\, \alpha < h(A) \mid \mathbf{F}(\alpha) = a \,\}$. The discussion in the proof of Claim 7.1 says that $\mathbf{F} \restriction_\lambda$ is injective. Clearly, we have $\mathbf{F}[\lambda] \subseteq A$ by definition of λ. If it were $\mathbf{F}[\lambda] \subsetneq A$, then $\mathbf{F}(\lambda) \in A - \mathbf{F}[\lambda]$; thus $\mathbf{F}(\lambda) \neq a$, which is a contradiction. Hence, $\mathbf{F} \restriction_\lambda : \lambda \hookrightarrow\!\!\!\!\rightarrow A$. $R \triangleq \{\, (\mathbf{F}(\alpha), \mathbf{F}(\beta)) \in A^2 \mid \alpha < \beta < \lambda \,\}$ is a well-ordering of A.

■

Theorem 7.2 (Finite Sets Have Choice)**.** Every finite system of sets has a choice function.

Proof. Let $\mathbf{P}(n)$ be the property "for every set S with $|S| = n$, there exists a choice function for S." $\mathbf{P}(0)$ and $\mathbf{P}(1)$ are evidently true.

Fix any $0 < n < \omega$ and assume $\mathbf{P}(n)$. Take any set S with $|S| = n+1$ and fix $X \in S$. Without loss of generality, $X \neq \varnothing$. Then, $|S - \{X\}| = n$, and thus there exists a choice function g for $S - \{X\}$. Fix any $x \in X$. Then, $g' \triangleq g \cup \{(X, x)\}$ is a choice function for S. The result follows by induction. ■

Definition 7.2 (Axiom of Choice)**.** There exists a choice function for every set.

$$\forall S, \exists g \in \left(\bigcup S\right)^S, \forall X \in S, (X \neq \varnothing \implies g(X) \in X)$$

Theorem 7.3 (Equivalence of Axiom of Choice and Others)**.** The following are equivalent:.

(i) Axiom of Choice
(ii) Every partition has a set of representatives.
(iii) If $\{\, X_i \mid i \in I \,\}$ is an indexed system of nonempty sets, then there exists a function f on I such that $\forall i \in I, f(i) \in X_i$.

Proof.

(i) $\Rightarrow$ (ii) Let g be a choice function for a partition S. Then, $X = \operatorname{ran}(g)$ is a set of representatives for S.
(ii) $\Rightarrow$ (iii) Let $C_i \triangleq \{i\} \times X_i$ for each $i \in I$. Then, since $\forall i, i' \in I$, $(i \neq i' \implies C_i \cap C_{i'} = \varnothing)$, $S \triangleq \{\, C_i \mid i \in I \,\}$ is a partition. Let g be a set of representatives for S. Then, for each $i \in I$, there uniquely exists $x \in X_i$ such that $(i, x) \in g \cap C_i$. Hence, g is a function on I and $\forall i \in I$, $g(i) \in X_i$.
(iii) $\Rightarrow$ (i) Take any set S and let $I \triangleq S - \{\varnothing\}$. Let $X_C \triangleq C$ for all $C \in I$. Hence, the indexed system of sets $\{\, X_C \mid C \in I \,\}$ has a function f on I such that $f(C) \in X_C = C$ for each $C \in I$.
If $\varnothing \notin S$, then f is a choice function for S. If $\varnothing \in S$, then $f \cup \{(\varnothing, \varnothing)\}$ is a choice function for S.

■

Theorem 7.4 (Infinite Sets Have Countably Infinite Subsets)**.** Every infinite set has a countably infinite subset.

Proof. Let A be an infinite set. By the Well-Ordering Theorem (Theorem 7.1), there exists $f : \Omega \hookrightarrow\!\!\!\!\rightarrow A$ where $\Omega \in \mathrm{Ord}$ with $\omega \leq \Omega$. Then, $f[\omega]$ is a countably infinite subset of A. ■

Theorem 7.5 (Infinite Sets Have Aleph Cardinality)**.** For every infinite set S, there uniquely exists $\alpha \in \mathrm{Ord}$ such that $|S| = \aleph_\alpha$.

Proof. By the Well-Ordering Theorem (Theorem 7.1), $|S| = |\Omega|$ for some infinite ordinal Ω. Then, by Theorem 6.1 and Theorem 6.2, there exists $\alpha \in \mathrm{Ord}$ such that $|\Omega| = \aleph_\alpha$. The uniqueness is evident. ■

Definition 7.3 (Cardinals)**.** For every set X, $|X|$ is the unique initial ordinal equipotent to X.

Remark. Claim 4.1 is justified by Definition 7.3, which is supported by the following facts:

- There exists $f : X \twoheadrightarrow Y$ if and only if $|X| = |Y|$.
- There exists $f : X \hookrightarrow Y$ if and only if $|X| \leq |Y|$.

Theorem 7.6 (Cardinals are Totally Ordered)**.** For any sets A and B, we have $|A| \leq |B|$ or $|B| \leq |A|$.[2]

Proof of Theorem 7.6. Since $|A|$ and $|B|$ are cardinal numbers (initial ordinals), by the Well-Ordering Theorem and the properties of cardinals, $|A| \leq |B|$ or $|B| \leq |A|$. ■

Theorem 7.7 (Union of Countable Collections of Countable Sets is Countable)**.** The union of a countably infinite collection of countable sets is countable.

Proof. Let $|S| = \aleph_0$ and $\forall X \in S$, $|X| \leq \aleph_0$. Fix any injective sequence $\langle A_n \mid n \in \mathbb{N} \rangle$ onto S. For each $n \in \mathbb{N}$, as $|A_n| \leq \aleph_0$, there exists $f_n : \mathbb{N} \to A_n$ that is surjective. Let $P_n \triangleq \{ f \in A_n^{\mathbb{N}} \mid \mathrm{ran}(f) = A_n \}$, which is nonempty.

By part (iii) of Theorem 7.3, there exists a function g on $\mathbb{N}$ such that $\forall n \in \mathbb{N}$, $g(n) \in P_n$. Then, we can define $\eta : \mathbb{N} \times \mathbb{N} \to \bigcup S$ by $\eta(n,k) = g(n)(k)$; hence, $\bigcup S$ is countable by Theorem 4.18. ■

Theorem 7.8 (Aleph One is Less Than or Equal to the Power Set of Aleph Zero)**.** $\aleph_1 \leq 2^{\aleph_0}$.

Proof. This is a consequence of Theorem 7.5 and Cantor's Theorem (Theorem 4.38). ■

Theorem 7.9 (Image Size is Bounded by Domain Size)**.** If f is a function on A, then $|\mathrm{ran}(f)| \leq |A|$.

Proof. Since $|A| = |\alpha|$ for some ordinal α by Theorem 7.5, the result follows from Exercise 6.9. ■

Theorem 7.10 (Union of Aleph-α Sized Sets)**.** Let $\alpha \in \mathrm{Ord}$. If $|S| \leq \aleph_\alpha$ and $\forall X \in S$, $|X| \leq \aleph_\alpha$, then $\left|\bigcup S\right| \leq \aleph_\alpha$.[3]

Proof. Without loss of generality, assume $S \neq \varnothing$ and $\forall X \in S$, $X \neq \varnothing$. Write $S = \{ X_\nu \mid \nu < \omega_\alpha \}$ and, for each $\nu < \omega_\alpha$, choose a transfinite sequence $\langle x_\nu(k) \mid k < \omega_\alpha \rangle$ such that $X_\nu = \{ a_\nu(k) \mid k < \omega_\alpha \}$. We may define $f : \omega_\alpha \times \omega_\alpha \to \bigcup S$ by $f(\nu, \kappa) = x_\nu(\kappa)$. Hence,

$$\left|\bigcup S\right| \leq \aleph_\alpha \cdot \aleph_\alpha \quad \text{(by Exercise 6.9)} = \aleph_\alpha \quad \text{(by Theorem 6.3)}.$$

Thus, the result follows. ■

Theorem 7.11 (Zorn's Lemma)**.** The following are equivalent:.

[2] This theorem requires the Axiom of Choice.
[3] This theorem requires the Axiom of Choice.

- Axiom of Choice
- Let $(A, \preceq)$ be a partially ordered set. If every chain in $(A, \preceq)$ has an upper bound, then there exists a maximal element of A.

Proof.

(i) $\Rightarrow$ (ii) Let $(A, \preceq)$ be a partially ordered set such that every chain in $(A, \preceq)$ has an upper bound. Fix any $b \in A$ and a choice function g for $\mathscr{P}(A)$. Let $\mathbf{G}(x)$ be an operation defined by

$$\mathbf{G}(x) \triangleq \begin{cases} g(A_x) & \text{if } x \text{ is a transfinite sequence of length } \alpha, \\ & \quad A_x \triangleq \{\, a \in A \mid \forall \xi < \alpha, x(\xi) \prec a \,\} \text{ is nonempty} \\ b & \text{otherwise.} \end{cases},$$

Then, by the Transfinite Recursion Theorem (Theorem 5.7), there exists an operation $\mathbf{F}(x)$ such that

$$\forall \alpha \in \mathrm{Ord},\ \mathbf{F}(\alpha) = \mathbf{G}\left(\mathbf{F} \restriction_\alpha\right).$$

Similarly to the discussion in Claim 7.1 of Theorem 7.1, $\mathbf{F}(\alpha) = b$ for some $\alpha < h(A)$. Let $\lambda \triangleq \min\{\alpha < h(A) \mid \mathbf{F}(\alpha) = b\}$. The discussion in the proof of Claim 7.1 says that $\mathbf{F} \restriction_\lambda$ is injective.
For any $a \in A$, there exists $\xi < \lambda$ such that $a \preceq \mathbf{F}(\xi)$. (Otherwise, $\mathbf{F}(\lambda) \neq b$ by definition.) Hence, $A = \bigcup_{\xi<\lambda} \{\, y \in A \mid y \preceq \mathbf{F}(\xi) \,\}$. Moreover, $\lambda \leq \omega_\gamma$ since, otherwise, $\mathbf{F} \restriction_{\omega_\gamma}$ is an injection on ω_γ into $\{\, y \in A \mid y \preceq \mathbf{F}(\omega_\gamma) \,\}$, which is a contradiction. Hence, $|A| \leq \aleph_\gamma$ by Theorem 7.10.

(ii) $\Rightarrow$ (i) It suffices to show that every system of nonempty sets S has a choice function. Let $F \triangleq \{\, f : S \rightharpoonup \bigcup S \mid \forall X \in dom(f),\ f(X) \in X \,\}$. Then, $(F, \subseteq)$ is a partially ordered set. Moreover, if $C \subseteq F$ is a chain in $(F, \subseteq)$, then $\bigcup C$ is an upper bound of C.
Therefore, by the assumption, there exists a maximal element $\overline{f}$ of F. Suppose $dom(\overline{f}) \subsetneq S$ for the sake of contradiction. Take any $X \in S - dom(\overline{f})$ and $x \in X$. Then, $\overline{f} \cup \{(X, x)\} \in F$ is clearly greater than $\overline{f}$, which is a contradiction. Hence, $dom(\overline{f}) = S$, i.e., $\overline{f}$ is a choice function for S.

■

Theorem 7.12 (Initial Ordinal Less Than Aleph-γ Implies Cardinality Bound)**.** Let $\gamma \in \mathrm{Ord}$ and let $(A, \preceq)$ be a totally ordered set. If $\forall x \in A, |\{\, y \in A \mid y \preceq x \,\}| < \aleph_\gamma$, then $|A| \leq \aleph_\gamma$.

Proof. In the same way as in the proof of Zorn's Lemma (Theorem 7.11), we construct an operation $\mathbf{F}(x)$ and let $\lambda = \min\{\, \alpha < h(A) \mid \mathbf{F}(\alpha) = b \,\}$. For any $a \in A$, there exists $\xi < \lambda$ such that $a \preceq \mathbf{F}(\xi)$. (Otherwise, $\mathbf{F}(\lambda) \neq b$ by definition.) Hence, $A = \bigcup_{\xi<\lambda} \{\, y \in A \mid y \preceq \mathbf{F}(\xi) \,\}$. Moreover, $\lambda \leq \omega_\gamma$ since, otherwise, $\mathbf{F} \restriction_{\omega_\gamma}$ is an injection on ω_γ into $\{\, y \in A \mid y \preceq \mathbf{F}(\omega_\gamma) \,\}$, which is a contradiction. Hence, $|A| \leq \aleph_\gamma$ by Theorem 7.10. ■

Proposition 7.1. If a set A can be totally ordered, then every system of finite subsets of A has a choice function.

Proof. Let $\preceq$ be a total ordering of A. Take any system S of finite subsets of A. Define $f : S \to A \cup \{\varnothing\}$ by

$$f(X) \triangleq \begin{cases} \min_\preceq X & \text{if } X \neq \varnothing, \\ \varnothing & \text{otherwise.} \end{cases}$$

(The definition is justified by Lemma 4.6.) Then, f is a choice function for S. ■

Proposition 7.2. If A can be well-ordered, then $\mathscr{P}(A)$ can be totally ordered.

Proof. Assume $(A, \leq)$ is a well-ordered set. Define $\prec$ on $\mathscr{P}(A)$ by

$$X \prec Y \iff X \neq Y \wedge \min_{\leq}(X \triangle Y) \in X,$$

where $X \triangle Y$ denotes the symmetric difference of X and Y.

- Asymmetry: Since $(X \triangle Y) \cap (X \cap Y) = \varnothing$, $\prec$ is asymmetric on $\mathscr{P}(A)$.
- Transitivity: Assume $X \prec Y$ and $Y \prec Z$. Then, let $a \triangleq \min_{\leq}(X \triangle Y) \in X$ and $b \triangleq \min_{\leq}(Y \triangle Z) \in Y$. Since $a \notin Y$, $a \neq b$.
  - If $a < b$, then $a \notin Z$ by minimality of b. Therefore, $a \in X \triangle Z$. For all $x < a$, $x \in X \iff x \in Y$ and $x \in Y \iff x \in Z$, so $x \notin X \triangle Z$. Thus, $a = \min_{\leq}(X \triangle Z) \in X$, so $X \prec Z$.
  - If $b < a$, then $b \in X$ by minimality of a. Therefore, $b \in X \triangle Z$. Similarly, $b = \min_{\leq}(X \triangle Z) \in X$, so $X \prec Z$.

  Thus, $\prec$ is transitive.
- Totality: For any $X, Y \in \mathscr{P}(A)$ with $X \neq Y$, $\min_{\leq}(X \triangle Y) \in X \triangle Y$. Therefore, either $X \prec Y$ or $Y \prec X$. Hence, $\prec$ is a total ordering of $\mathscr{P}(A)$.

■

Proposition 7.3. Let $(A, \preceq)$ be a partially ordered set in which every chain has an upper bound. Then, for every $a \in A$, there exists a $\preceq$-maximal element $x \in A$ such that $a \preceq x$.[4]

Proof. Replace $\mathbf{G}(x)$ in the proof of Zorn's Lemma (Theorem 7.11) with

$$\mathbf{G}(x) \triangleq \begin{cases} g(A_x) & \text{if } x \text{ is a transfinite sequence of length } \alpha > 0 \\ & \quad \text{and } A_x \triangleq \{\, a \in A \mid \forall \xi < \alpha,\, x(\xi) \prec a \,\} \text{ is nonempty} \\ a & \text{if } x = \varnothing, \\ b & \text{otherwise,} \end{cases},$$

where g is a choice function for $\mathscr{P}(A)$ and b is a fixed element in A.

Then, if c is an upper bound of $\mathbf{F}[\lambda]$, then $a \preceq c$ and c is a maximal element. ■

Proposition 7.4. The following are equivalent:.

(i) Zorn's Lemma (Theorem 7.11).
(ii) For every partially ordered set $(A, \preceq)$, the set of all chains of $(A, \preceq)$ has an $\subseteq$-maximal element.

Proof.

($\Rightarrow$) Let $\mathscr{C} \subseteq \mathscr{P}(A)$ be the set of all chains of $(A, \preceq)$. Then, $(\mathscr{C}, \subseteq)$ is a partially ordered set such that every chain $\mathscr{D}$ in $(\mathscr{C}, \subseteq)$ has an upper bound $\bigcup \mathscr{D}$. Hence, by Zorn's Lemma, $\mathscr{C}$ has a $\subseteq$-maximal element.

($\Leftarrow$) Let $(A, \preceq)$ be a partially ordered set in which every chain has an upper bound. By assumption, the set of all chains of $(A, \preceq)$ has a $\subseteq$-maximal element C. The union C is itself a chain.
Let c be an upper bound of C. If c is not maximal, there exists $c' \succ c$. Then $C \cup \{c'\}$ is a chain, contradicting the maximality of C. Thus, c is a maximal element of A.

[4] This theorem requires the Axiom of Choice.

■

Proposition 7.5. The following are equivalent:.

(i) Zorn's Lemma (Theorem 7.11).
(ii) Let A be a set. Assume that, for each $B \subseteq A$ such that $(B, \subseteq)$ is a totally ordered set, $\bigcup B \in A$. Then, A has an $\subseteq$-maximal element.

Proof.

($\Rightarrow$) Given the conditions, every chain in $(A, \subseteq)$ has an upper bound (namely, its union). By Zorn's Lemma, A has a $\subseteq$-maximal element.

($\Leftarrow$) Let $(A, \preceq)$ be a partially ordered set where every chain has an upper bound. Let $\mathscr{C}$ be the set of all chains in $(A, \preceq)$. For any chain $\mathscr{D} \subseteq \mathscr{C}$, $\bigcup \mathscr{D}$ is also a chain in $(A, \preceq)$ because all elements are comparable. By assumption, $\mathscr{C}$ has a $\subseteq$-maximal element. Then, similar to the previous part, there exists a maximal element in A.

■

Proposition 7.6 (Tukey's Lemma)**.** A set $\mathscr{F}$ has *finite character* if

$$\forall X, \left(X \in \mathscr{F} \iff [X]^{<\omega} \subseteq \mathscr{F}\right).$$

The following are equivalent:.

(i) Zorn's Lemma (Theorem 7.11).
(ii) Every set of finite character has an $\subseteq$-maximal element.

Proof.

($\Rightarrow$) Let $\mathscr{F}$ be a set of finite character.

Claim 7.2. For any chain $\mathscr{G} \subseteq \mathscr{F}$, $\bigcup \mathscr{G} \in \mathscr{F}$.

Proof of Claim 7.2. Take any finite subset $A \subseteq \bigcup \mathscr{G}$. Then $A \subseteq G$ for some $G \in \mathscr{G}$ because $\mathscr{G}$ is a chain. Since $G \in \mathscr{F}$ and $\mathscr{F}$ is of finite character, $A \in \mathscr{F}$. Thus, $[\bigcup \mathscr{G}]^{<\omega} \subseteq \mathscr{F}$. Therefore, $\bigcup \mathscr{G} \in \mathscr{F}$. ■

By the assumption and Claim 7.2, every chain in $(\mathscr{F}, \subseteq)$ has an upper bound in $\mathscr{F}$. By Zorn's Lemma, $\mathscr{F}$ has a $\subseteq$-maximal element.

($\Leftarrow$) Let $(A, \preceq)$ be a partially ordered set. Define $\mathscr{F} \triangleq \{\, C \subseteq A \mid C \text{ is a chain in } (A, \preceq) \,\}$. $\mathscr{F}$ has finite character:
– If $C \in \mathscr{F}$, then every finite subset of C is also a chain, so $[C]^{<\omega} \subseteq \mathscr{F}$.
– If $[X]^{<\omega} \subseteq \mathscr{F}$, then every pair of elements in X is comparable, so X is a chain, i.e., $X \in \mathscr{F}$.
By assumption, $\mathscr{F}$ has a $\subseteq$-maximal element, which is a maximal chain in A. By Zorn's Lemma equivalent, there exists a maximal element in A.

■

Proposition 7.7. Let E be a binary relation on A. Then, there exists a function $f: A \to A$ such that $\forall x \in A, ((x, f(x)) \in E \iff \exists y \in A, (x, y) \in E)$.[5]

[5]This exercise requires the Axiom of Choice.

Proof. If $A = \varnothing$, then the function f is trivially defined. Assume $A \neq \varnothing$. Fix any $a \in A$. Let g be a choice function for $\mathscr{P}(A)$. Define $f{:}A \to A$ by

$$f(x) \triangleq \begin{cases} g(E[\{x\}]) & \text{if } \exists y \in A,\ (x,y) \in E, \\ g(A \setminus E[\{x\}]) & \text{otherwise.} \end{cases}$$

Then, f satisfies the required condition. ■

Proposition 7.8. For each set X, if $|X| > \aleph_0$, then X has a subset of cardinality $\aleph_1$.[6]

Proof. By Theorem 7.5, there exists $\alpha \in \mathrm{Ord}$ such that $|X| = \aleph_\alpha$. Then, $\alpha \geq 1$. Since $\aleph_1 \leq \aleph_\alpha = |X|$, there exists an injection $f{:}\ \aleph_1 \hookrightarrow X$. Thus, $\mathrm{ran}(f)$ is a subset of X with cardinality $\aleph_1$. ■

Proposition 7.9. Let $(A, \preceq)$ be a totally ordered set. A sequence $\langle a_n \mid n \in \mathbb{N} \rangle$ of elements of A is *strictly decreasing* if $\forall n \in \mathbb{N},\ a_{n+1} \prec a_n$. Then, $(A, \preceq)$ is a well-ordered set if and only if there is no strictly decreasing infinite sequence in A.

Proof.

($\Rightarrow$) Suppose there exists a strictly decreasing sequence $\langle a_n \mid n \in \mathbb{N} \rangle$ in A. Let α be the order type of $(A, \preceq)$. If $h{:}A \to \alpha$ is an isomorphism, then $h(a_n)$ forms a strictly decreasing sequence in α, contradicting the well-ordering property.

($\Leftarrow$) Assume $(A, \preceq)$ is not well-ordered. Then, there exists a nonempty subset $X \subseteq A$ without a minimal element. Using the Axiom of Choice, define a sequence by repeatedly selecting elements from X, each less than the previous, forming a strictly decreasing sequence.

■

Proposition 7.10. Let $\langle F_{a,b} \rangle_{a \in A,\, b \in B}$ be a nonempty indexed system of sets.

(i) If $A \neq \varnothing$, then

$$\bigcap_{a \in A} \left[\bigcup_{b \in B} F_{a,b} \right] = \bigcup_{f \in B^A} \left[\bigcap_{a \in A} F_{a,f(a)} \right].$$

(ii) If $B \neq \varnothing$, then

$$\bigcup_{a \in A} \left[\bigcap_{b \in B} F_{a,b} \right] = \bigcap_{f \in B^A} \left[\bigcup_{a \in A} F_{a,f(a)} \right].$$

[7]

Proof.

(i) Let $L \triangleq \bigcap_{a \in A} \left[\bigcup_{b \in B} F_{a,b} \right]$ and $R \triangleq \bigcup_{f \in B^A} \left[\bigcap_{a \in A} F_{a,f(a)} \right]$.

- ($\subseteq$) Take any $x \in L$. For each $a \in A$, there exists $b_a \in B$ such that $x \in F_{a,b_a}$. Define $f{:}A \to B$ by $f(a) = b_a$. Then $x \in \bigcap_{a \in A} F_{a,f(a)} \subseteq R$.

[6] This exercise requires the Axiom of Choice.

[7] Part (ii) requires the Axiom of Choice.

- ($\supseteq$) Take any $x \in R$. Then, there exists $f \in B^A$ such that $x \in \bigcap_{a \in A} F_{a,f(a)}$. Hence, for each $a \in A$, $x \in F_{a,f(a)} \subseteq \bigcup_{b \in B} F_{a,b}$. Therefore, $x \in L$.

(ii) The proof of (ii) is analogous, using De Morgan's laws and the Axiom of Choice where necessary. The key step involves showing that the complement of the left-hand side equals the complement of the right-hand side, and then applying De Morgan's laws to conclude equality.

■

Proposition 7.11. Let A be a set. For each partial ordering $\preceq$ of A, there exists a total ordering $\leq$ of A such that $\forall a, b \in A$, $(a \preceq b \implies a \leq b)$.[8]

Proof. Let $\mathfrak{P} \subseteq \mathscr{P}(A \times A)$ be the set of all partial orderings of A that extend $\preceq$. Order $\mathfrak{P}$ by inclusion. By Zorn's Lemma, there exists a maximal element P in $\mathfrak{P}$ containing $\preceq$.

Suppose P is not a total order; then there exist $x, y \in A$ incomparable under P. Define a new relation P' by adding (x, y) to P, along with all necessary pairs to maintain a partial order. This contradicts the maximality of P. Therefore, P is a total ordering extending $\preceq$. ■

[8] This exercise requires the Axiom of Choice.