Summary for
Introduction to Set Theory

SEUNGWOO HAN

Hrbacek, Karel, and Thomas J. Jech. *Introduction to Set Theory, Revised and Expanded*. 3rd ed., CRC Press, 1999.

Contents

Chapter 1

Sets

1.1 Introduction to Sets

Definition 1.1.1: Set

Every object in the universe of discourse is called a *set*.

1.2 Properties

Definition 1.2.1: Property

Any mathematical sentence* is called a *property*. If $X, Y, \cdots, Z$ are free variables of a property $\mathbf{Q}$, we write $\mathbf{Q}(X, Y, \cdots, Z)$ and say $\mathbf{Q}(X, Y, \cdots, Z)$ is a property of $X, Y, \cdots, Z$.

*Refer to mathematical logic textbook for detailed discussion.

1.3 Axioms

Axiom I The Axiom of Existence

There exists a set which has no elements.

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

Note:-

The Axiom of Existence guarantees that the universe of discourse is not void.

Axiom II The Axiom of Extensionality

If every element of X is an element of Y and every element of Y is an element of X, then $X = Y$.

$$\forall X\, \forall Y\, [\forall x\, (x \in X \iff x \in Y) \implies X = Y]$$

Note:-

The Axiom of Extensionality defines the equality relation with the containment relation($\in$).

Lemma 1.3.1

There exists only one set with no elements.

Proof. Let A and B are sets such that $\forall x\, \neg(x \in A)$ and $\forall x\, \neg(x \in B)$. Then, we have $\forall x\, (x \in A \iff x \in B)$. Therefore, by The Axiom of Extensionality, $A = B$ is guaranteed. □

Definition 1.3.2: Empty Set

The unique set with no elements is called the *empty set* and is denoted $\varnothing$.

Note:-

Definition 1.3.2 is justified by Lemma 1.3.1.

Axiom III The Axiom Schema of Comprehension

Let $\mathbf{P}(x)$ be a property of x. For any set A, there exists a set B such that $x \in B$ if and only if $x \in A$ and $\mathbf{P}(x)$.

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

Note:-

Axiom III is a axiom *schema* since it provides unlimited amount of axioms for varying $\mathbf{P}$.

Lemma 1.3.3

Let $\mathbf{P}(x)$ be a property of x. For any set A, there uniquely exists a set B such that $x \in B$ if and only if $x \in A$ and $\mathbf{P}(x)$.

Proof. Let B' be another set such that $x \in B'$ if and only if $x \in A$ and $\mathbf{P}(x)$. Then, for any x, we have $x \in B' \iff x \in A \wedge \mathbf{P}(x) \iff x \in B$. Hence, by The Axiom of Extensionality, we have $B = B'$. □

Notation 1.3.4: Set-Builder Notation

Let $\mathbf{P}(x)$ be a property of x. Let A be a set. The unique set B such that $x \in B$ if and only if $x \in A$ and $\mathbf{P}(x)$ is denoted $\{x \in A \mid \mathbf{P}(x)\}$.

Note:-

Notation 1.3.4 is justified by Lemma 1.3.3.

Axiom IV The Axiom of Pair

For any A and B, there exists C such that $x \in C$ if and only if $x = A$ or $x = B$.

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

Note:-

Similarly, the set C such that $x \in C \iff x = A \vee x = B$ is unique by The Axiom of Extensionality.

Notation 1.3.5

Let A and B be sets. The unique set C such that $x \in C$ if and only if $x = A$ or $x = B$ is denoted $\{A, B\}$. In particular, if $A = B$, we write $\{A\}$ instead of $\{A, A\}$.

Axiom V The Axiom of Union

For any S, there exists U such that $x \in U$ if and only if $x \in A$ for some $A \in S$.

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

Definition 1.3.6: The Union of System of Sets

Let S be a set. The unique set U such that $x \in U$ if and only if $x \in A$ for some $A \in S$ is denoted $\bigcup S$.

Definition 1.3.7: The Union of Two Sets

Let A and B be sets. Then, $A \cup B$ denotes the unique set $\bigcup\{A, B\}$.

Definition 1.3.8: Subset

Let A and B sets. B is said to be a *subset* of A if $\forall x\, (x \in B \implies x \in A)$. If B is a subset of A, then we write $B \subseteq A$.

Axiom VI The Axiom of Power Set

For any S, there exists P such that $X \in P$ if and only if $X \subseteq S$.

Note:-

Similarly, the set P is unique by The Axiom of Extensionality.

Definition 1.3.9: Power Set

Let S be a set. The unique set P such that $X \in P$ if and only if $X \subseteq S$ is called the *power set* of S and is denoted $\mathcal{P}(S)$.

Lemma 1.3.10

Let $\mathbf{P}(x)$ be a property of x. Let A and A' be sets such that $\mathbf{P}(x) \implies x \in A \wedge x \in A'$. Then, $\{\, x \in A \mid \mathbf{P}(x)\,\} = \{\, x \in A' \mid \mathbf{P}(x)\,\}$.

Proof. For all x, we have $x \in A \wedge \mathbf{P}(x) \iff \mathbf{P}(x) \iff x \in A' \wedge \mathbf{P}(x)$. Therefore, by The Axiom of Extensionality, the result follows. $\square$

Notation 1.3.11

Let $\mathbf{P}(x)$ be a property of x. If there exists a set A such that $\mathbf{P}(x)$ implies $x \in A$, we write $\{\, x \mid \mathbf{P}(x)\,\} \triangleq \{\, x \in A \mid \mathbf{P}(x)\,\}$, and it is called *the set of all x with the property* $\mathbf{P}(x)$.

Note:-

Notation 1.3.11 is justified by Lemma 1.3.10.

Selected Problems

Exercise 1.3.1

The set of all x such that $x \in A$ and $x \notin B$ exists.

Proof. We have $x \in A \wedge x \notin B \implies x \in A$. Hence, the set exists and is equal to $\{x \in A \mid x \in A \wedge x \notin B\}$. $\square$

Exercise 1.3.2

Prove The Axiom of Existence only from The Axiom Schema of Comprehension and The Weak Axiom of Existence.

Weak Axiom of Existence Some set exists.

Proof. Let A be a set known to exist. Then, there exists $B = \{x \in A \mid x \neq x\}$ by The Axiom Schema of Comprehension. Since $\forall x\,(x = x)$, $\forall x\,(x \notin B)$. $\square$

Exercise 1.3.3

(a) Prove that a set of all sets($\{x \mid \top\}$) does not exist.
(b) Prove that $\forall A \,\exists x\,(x \notin A)$.

Proof.

(a) Suppose $V = \{x \mid \top\}$ exists. Then, by The Axiom Schema of Comprehension, $R = \{x \in V \mid x \notin x\}$ exists. However, we have $R \in R \iff R \notin R$ by definition of R. Hence, V does not exist.
(b) Suppose $\exists A \,\forall x\,(x \in A)$ for the sake of contradiction. Then, A is the set of all sets, which is impossible by (a). $\square$

Exercise 1.3.6

Prove $\forall X\, \neg(\mathcal{P}(X) \subseteq X)$.

Proof. Let $Y = \{u \in X \mid u \notin u\}$. Then, by definition, $Y \subseteq X$, and thus $Y \in \mathcal{P}(X)$. Now, suppose $Y \in X$ for the sake of contradiction. Then, $Y \in Y \iff Y \in X \wedge Y \notin Y \iff Y \notin Y$, which is a contradiction. Hence, $Y \notin X$. $\square$

1.4 Elementary Operations on Sets

Definition 1.4.1: Proper Subset

Let A and B sets. B is said to be a *proper subset* of A if $B \subseteq A$ and $B \neq A$. If B is a proper subset of A, we write $B \subsetneq A$.

Definition 1.4.2: Elementary Operations on Sets

(i) Intersection
- The *intersection* of A and B, $A \cap B$, is the set $\{x \mid x \in A \land x \in B\}$.

(ii) Union
- The *union* of A and B, $A \cup B$, is the set $\{x \mid x \in A \lor x \in B\}$.

(iii) Difference
- The *difference* of A and B, $A \setminus B$, is the set $\{x \mid x \in A \land x \notin B\}$.

(iv) Symmetric Difference
- The *symmetric difference* of A and B, $A \triangle B$, is the set $(A \setminus B) \cup (B \setminus A)$.

Lemma 1.4.3 Simple Properties of Elementary Operations

(i) Commutativity
- $A \cap B = B \cap A$
- $A \cup B = B \cup A$
- $A \triangle B = B \triangle A$

(ii) Associativity
- $(A \cap B) \cap C = A \cap (B \cap C)$
- $(A \cup B) \cup C = A \cup (B \cup C)$
- $(A \triangle B) \triangle C = A \triangle (B \triangle C)$

(iii) Distributivity
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(iv) De Morgan's Laws
- $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$
- $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$

(v) Miscellaneous
- $A \cap (B \setminus C) = (A \cap B) \setminus C$
- $A \setminus B = \varnothing \iff A \subseteq B$
- $A \triangle B = \varnothing \iff A = B$

Definition 1.4.4: Intersection of System of Sets

Let S be a nonempty set. Then, the *intersection* $\bigcap S$ is the set $\{x \mid \forall A \in S\,(x \in A)\}$.

Note:-

Note that $\bigcap S$ exists for all nonempty S since $\forall A \in S\,(x \in A) \implies x \in A_1$ where A_1 is any set such that $A_1 \in S$.

Definition 1.4.5: System of Mutually Disjoint Sets

We say the sets A and B are *disjoint* if $A \cap B = \varnothing$. A set S is a *system of mutually disjoint sets* if $\forall A, B \in S$, $(A \neq B \implies A \cap B = \varnothing)$.

Selected Problems

Exercise 1.4.2

(i) $A \setminus B = (A \cup B) \setminus B = A \setminus (A \cap B)$

(ii) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$

(iii) $A \cap B = A \setminus (A \setminus B)$

Proof.

(i)
$$
\begin{aligned}
x \in A \wedge x \notin B &\iff x \in A \wedge x \notin B \vee x \in B \wedge x \notin B && \triangleright\ \vee\text{-intro / }\vee\text{-syllogism} \\
&\iff (x \in A \vee x \in B) \wedge x \notin B && \triangleright\ \text{Distribution}
\end{aligned}
$$

$$
\begin{aligned}
x \in A \wedge x \notin B &\iff x \in A \wedge x \notin A \vee x \in A \wedge x \notin B && \triangleright\ \vee\text{-intro / }\vee\text{-syllogism} \\
&\iff x \in A \wedge (x \notin A \vee x \notin B) && \triangleright\ \text{Distribution} \\
&\iff x \in A \wedge \neg(x \in A \wedge x \in B) && \triangleright\ \text{De Morgan's Law}
\end{aligned}
$$

(ii)
$$
\begin{aligned}
x \in A \wedge \neg(x \in B \wedge x \notin C) &\iff x \in A \wedge (x \notin B \vee x \in C) && \triangleright\ \text{De Morgan's Law} \\
&\iff (x \in A \wedge x \notin B) \vee (x \in A \wedge x \in C) && \triangleright\ \text{Distribution}
\end{aligned}
$$

(iii) By (ii), $A \setminus (A \setminus B) = (A \setminus A) \cup (A \cap B) = A \cap B$. □

Exercise 1.4.4

For any set A, prove that a “complement” of A ($\{x \mid x \notin A\}$) does not exist.

Proof. Let B be the complement of A for the sake of contradiction. Then, $A \cup B$ is the set of all sets, which is impossible by Exercise 1.3.3. □

Chapter 2

Relations, Function, and Ordering

2.1 Ordered Pairs

Definition 2.1.1: Ordered Pair

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

Theorem 2.1.2

$(a, b) = (a', b') \iff a = a' \wedge b = b'$

Proof. $(\Leftarrow)$ is direct.

$(\Rightarrow)$ If $a = b$, we have $\{\{a\}\} = \{\{a'\}, \{a', b'\}\}$, and thus $\{a\} = \{a'\} = \{a', b'\}$, leaving the only option $a = a' = b'$.

If $a \neq b$, we must have $a' \neq b'$ by the argument above. Hence, we have $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$, which implies $\{a\} = \{a'\}$ and $\{a, b\} = \{a', b'\}$. □

Definition 2.1.3: Ordered Triples and Quadruples

- $(a, b, c) = ((a, b), c)$
- $(a, b, c, d) = ((a, b, c), d)$

Selected Problems

Exercise 2.1.1

If $a, b \in A$, then $(a, b) \in \mathcal{P}(\mathcal{P}(A))$.

Proof. If $a, b \in A$, then $\{a\}, \{a, b\} \in \mathcal{P}(A)$, and thus $(a, b) = \{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A)$. □

2.2 Relations

Definition 2.2.1: Binary Relation

A set R is a *binary relation* if all elements of R are ordered pairs.

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

Notation 2.2.2

If $(x,y)\in R$, we write xRy and say *x is in relation R with y*.

Definition 2.2.3: Domain, Range, and Field of Binary Relation

Let R be a binary relation.
- $\operatorname{dom} R \triangleq \{\, x \mid \exists y\ xRy \,\}$ is called the *domain* of R.
- $\operatorname{ran} R \triangleq \{\, y \mid \exists x\ xRy \,\}$ is called the *range* of R.
- $\operatorname{field} R \triangleq \operatorname{dom} R \cup \operatorname{ran} R$ is called the *field* of R.
- If $\operatorname{field} R \subseteq X$, we say that R is a *relation in X* or that R is a relation *between* elements of X.

Lemma 2.2.4

Let R be a binary relation. Then, $\operatorname{dom} R$ and $\operatorname{ran} R$ exist.

Proof. By Exercise 2.2.1, if xRy, then $x, y \in A \triangleq \bigcup\left(\bigcup R\right)$. Hence, $\operatorname{dom} R$ and $\operatorname{ran} R$ exist. □

Definition 2.2.5: Image and Inverse Image

Let R be a binary relation and A be a set.
- $R[A] \triangleq \{\, y \in \operatorname{ran} R \mid \exists x \in A,\ xRy \,\}$ is called the *image* of A under R.
- $R^{-1}[A] \triangleq \{\, x \in \operatorname{dom} R \mid \exists y \in A,\ xRy \,\}$ is called the *inverse image* of A under R.

Notation 2.2.6

We write $\{\,(x,y) \mid \mathbf{P}(x,y)\,\}$ instead of $\{\, w \mid \exists x,\ \exists y,\ w = (x,y) \land \mathbf{P}(x,y)\,\}$.

Definition 2.2.7: Inverse Relation

Let R be a binary relation. The *inverse* of R is the set

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

Definition 2.2.8: Composition

Let R and S be binary relations. The relation

$$S \circ R \triangleq \{(x,z) \mid \exists y,\ xRy \land ySz\}$$

is called the *composition* of R and S.

Definition 2.2.9: Membership Relation and Identity Relation

Let A be a set.

- The *membership relation on A* is defined by

$$\in_A \triangleq \{(a,b) \mid a,b \in A \wedge a \in b\}.$$

- The *identity relation on A* is defined by

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

Definition 2.2.10: Cartesian Product

Let A and B be sets. The set $A \times B \triangleq \{(a,b) \mid a \in A \wedge b \in B\}$ is called the *Cartesian product* product of A and B.

Lemma 2.2.11

Let A and B be sets. $A \times B$ exists.

Proof. If $a \in A$ and $b \in B$, by Exercise 2.1.1, we have $(a,b) \in \mathcal{P}(\mathcal{P}(A \cup B))$. □

Corollary 2.2.12

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

Proof.

- If yRx, then $(x,y) \in (\operatorname{ran} R) \times (\operatorname{dom} R)$.
- If $(x,z) \in S \circ R$, then $(x,z) \in (\operatorname{dom} R) \times (\operatorname{ran} S)$.
- If $a,b \in A$, then $(a,b) \in A \times A$.
- If $a \in A$, then $(a,a) \in A \times A$. □

Lemma 2.2.13

Let R be a binary relation. The inverse image of A under R is equal to the image of A under R^{-1}.

Proof. Note that $\operatorname{dom} R = \{x \mid \exists y\, xRy\} = \{x \mid \exists y\, yR^{-1}x\} = \operatorname{ran} R^{-1}$. Therefore,

$$\begin{aligned}
& x \in (\text{the inverse image of } A \text{ under } R) \\
\iff & x \in \operatorname{dom} R \wedge \exists y \in A,\ xRy \\
\iff & x \in \operatorname{ran} R^{-1} \wedge \exists y \in A,\ yR^{-1}x \\
\iff & x \in (\text{the image of } A \text{ under } R^{-1}).
\end{aligned}$$

□

Note:-

Lemma 2.2.13 resolves the possible ambiguity on the expression $R^{-1}[A]$.

Notation 2.2.14

We write A^2 instead of $A \times A$.

Selected Problems

Exercise 2.2.1

Let R be a binary relation. Let $A = \bigcup\left(\bigcup R\right)$. Prove that $(x, y) \in R$ implies $x \in A$ and $y \in A$.

Proof. If $(x, y) = \{\{x\}, \{x, y\}\} \in R$, Then $\{x, y\} \in \bigcup R$, and thus $x, y \in A$. $\square$

Exercise 2.2.3

Let R be a binary relation and A and B be sets. Prove:

(i) $R[A \cup B] = R[A] \cup R[B]$.
(ii) $R[A \cap B] \subseteq R[A] \cap R[B]$.
(iii) $R[A \setminus B] \supseteq R[A] \setminus R[B]$.
(iv) Show by an example that $\subseteq$ and $\supseteq$ in parts (ii) and (iii) cannot be replaced by $=$.
(v) $R^{-1}[R[A]] \supseteq A \cap \operatorname{dom} R$ and $R[R^{-1}[B]] \supseteq B \cap \operatorname{ran} R$. Give examples where equality does not hold.

Proof.

(i) $$\begin{aligned} y \in R[A \cup B] &\iff \exists x,\ x \in A \cup B \wedge xRy \\ &\iff \exists x,\ (x \in A \wedge xRy) \vee (x \in B \wedge xRy) \\ &\iff y \in R[A] \vee y \in R[B] \iff y \in R[A] \cup R[B] \end{aligned}$$
(ii) Take any $y \in R[A \cap B]$. Then, there exists $x \in A \cap B$ such that xRy. Hence, $y \in R[A]$ and $y \in R[B]$.
(iii) Take any $y \in R[A] \setminus R[B]$. Then, there exists $x \in A$ such that xRy. If $x \in B$, it implies that $y \in R[B]$, which is a contradiction. Hence, $x \in A \setminus B$. Therefore, $y \in R[A \setminus B]$.
(iv) Let a, b, and c be mutually different sets. Let $R = \{(a, a), (b, a), (c, c)\}$. Let $A = \{a, c\}$ and $B = \{b, c\}$. Then, $R[A \cap B] = \{c\} \subsetneq R[A] \cap R[B] = \{a, c\}$, and $R[A] \setminus R[B] = \varnothing \subsetneq R[A \setminus B] = \{a\}$.
(v) Take any $a \in A \cap \operatorname{dom} R$. Then, there exists b such that aRb. Moreover, $b \in R[A]$. Since $bR^{-1}a$, we conclude that $a \in R^{-1}[R[A]]$.
Take any $b \in B \cap \operatorname{ran} R$. Then, there exists a such that aRb. Moreover, $a \in R^{-1}[B]$. Hence, $b \in R[R^{-1}[B]]$.

Exercise 2.2.4

Let $R \subseteq X \times Y$. Prove:

(i) $R[X] = \operatorname{ran} R$ and $R^{-1}[Y] = \operatorname{dom} R$.
(ii) $\operatorname{dom} R = \operatorname{ran} R^{-1}$ and $\operatorname{ran} R = \operatorname{dom} R^{-1}$.
(iii) $(R^{-1})^{-1} = R$.
(iv) $R^{-1} \circ R \supseteq \mathrm{Id}_{\operatorname{dom} R}$ and $R \circ R^{-1} \supseteq \mathrm{Id}_{\operatorname{ran} R}$

Proof.

(i) We already have $R[X] \subseteq \operatorname{ran} R$ by definition. Take any $y \in \operatorname{ran} R$. There exists x such that $(x, y) \in R$. Since $R \subseteq X \times Y$, $x \in X$. Therefore, $y \in R[X]$; $\operatorname{ran} R \subseteq R[X]$. A similar argument goes for $R^{-1}[Y]$.
(ii) See the proof of Lemma 2.2.13.
(iii) For any relation R and for all x and y, we have $xRy \iff yR^{-1}x$. Since R^{-1} is also a relation, we have $xRy \iff yR^{-1}x \iff x(R^{-1})^{-1}y$.
(iv) Take any $x \in \operatorname{dom} R$. Then, there exists y such that xRy. Then, $yR^{-1}x$, and thus $x(R^{-1} \circ R)x$. A similar argument goes for $R \circ R^{-1}$. $\square$

Exercise 2.2.8

$A \times B = \varnothing$ if and only if $A = \varnothing$ or $B = \varnothing$.

Proof. ($\Rightarrow$) If $A \neq \varnothing$ and $B \neq \varnothing$, we have $(a, b) \in A \times B$ where $a \in A$ and $b \in B$, and thus $A \times B \neq \varnothing$.

($\Leftarrow$) If $A \times B \neq \varnothing$, then $a \in A$ and $b \in B$ where $(a, b) \in A \times B$. □

2.3 Functions

Definition 2.3.1: Function

A binary relation F is called a *function* (or *mapping*) if

$$\forall a \, \forall b_1 \, \forall b_2 \, (aFb_1 \wedge aFb_2 \implies b_1 = b_2).$$

For each $a \in \operatorname{dom} F$, the unique b such that aFb is called the *value of F at a* and is denoted $F(a)$ of F_a.

Notation 2.3.2

If F is a function with $\operatorname{dom} F = A$ and $\operatorname{ran} F \subseteq B$, we write $F : A \to B$, $\langle F(a) \mid a \in A \rangle$, $\langle F_a \mid a \in A \rangle$, $\langle F_a \rangle_{a \in A}$ for the function F. The range of the function F can then be denoted $\{F(a) \mid a \in A\}$ or $\{F_a\}_{a \in A}$.

Lemma 2.3.3

Let F and G be functions. $F = G \iff \operatorname{dom} F = \operatorname{dom} G \wedge \forall x \in \operatorname{dom} F,\ F(x) = G(x)$.

Proof. ($\Rightarrow$) is direct.

($\Leftarrow$) Take any $(x, F(x)) \in F$. Then, we have $(x, F(x)) = (x, G(x)) \in G$. Therefore, $F \subseteq G$. Similarly, $G \subseteq F$, and thus $F = G$. □

Definition 2.3.4

Let F be a function and A and B be sets.

- F is a function *on* A if $\operatorname{dom} F = A$.
- F is a function *into* B if $\operatorname{ran} F \subseteq B$.
- F is a function *onto* B if $\operatorname{ran} F = B$.
- The *restriction* of the function F *to* A is the function $F\big|_A \triangleq \{(a, b) \in F \mid a \in A\}$. If G is a restriction of F to some A, we say that F is an *extension* of G.

Theorem 2.3.5

Let f and g be functions.

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

(ii) $\operatorname{dom}(g \circ f) = (\operatorname{dom} f) \cap f^{-1}[\operatorname{dom} g]$.

(iii) $\forall x \in \operatorname{dom}(g \circ f)$, $(g \circ f)(x) = g(f(x))$.

Proof.

(i) Suppose $x(g \circ f)z_1$ and $x(g \circ f)z_2$. There exists y_1 and y_2 such that xfy_1, y_1gz_1, xfy_2, and y_2gz_2. Since f and g are functions, we have $y_1 = y_2$ and $z_1 = z_2$. Therefore, $g \circ f$ is a function.

(ii) $$\begin{aligned} x \in \operatorname{dom}(g \circ f) &\iff \exists z\, x(g \circ f)z \\ &\iff \exists z\, \exists y\, xfy \wedge ygz \\ &\iff x \in \operatorname{dom} f \wedge f(x) \in \operatorname{dom} g \iff x \in \operatorname{dom} f \wedge x \in f^{-1}[\operatorname{dom} g] \end{aligned}$$ □

Definition 2.3.6: Invertible Function

A function f is said to be *invertible* if f^{-1} is a function.

Definition 2.3.7: Injective Function

A function f is said to be *injective* (or *one-to-one*) if

$$\forall a_1, a_2 \in \operatorname{dom} f,\ (f(a_1) = f(a_2) \implies a_1 = a_2).$$

Notation 2.3.8

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

Theorem 2.3.9

Let f be a function.

(i) f is invertible if and only if f is one-to-one.
(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. Then, $f^{-1}(f(a)) = a$ for all $a \in \operatorname{dom} f$. Hence, for all $a_1, a_2 \in \operatorname{dom} f$ such that $f(a_1) = f(a_2)$, it follows that $a_1 = f^{-1}(f(a_1)) = f^{-1}(f(a_2)) = a_2$; f is one-to-one.
($\Leftarrow$) Suppose f is one-to-one. If $yf^{-1}x_1$ and $yf^{-1}x_2$, then x_1fy and x_2fy, i.e., $y = f(x_1) = f(x_2)$. Therefore, $x_1 = x_2$; f^{-1} is a function.

(ii) As f is a relation, by Exercise 2.2.4 (iii), $(f^{-1})^{-1} = f$, and thus f^{-1} is invertible. □

Definition 2.3.10: Compatible Functions

- Functions f and g are called *compatible* if $\forall x \in (\operatorname{dom} f) \cap (\operatorname{dom} g)$, $f(x) = g(x)$.
- A set of functions F is called a *compatible system of functions* if any two functions f and g from F are compatible.

Lemma 2.3.11

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

Proof.

(i) ($\Rightarrow$) Suppose $x(f\cup g)y_1$ and $x(f\cup g)y_2$. WLOG, $(x,y_1)\in f$. If $(x,y_2)\in f$, since f is a function, $y_1=y_2$. If $(x,y_2)\in g$, since f and g are compatible, $y_1=f(x)=g(x)=y_2$. Therefore, $f\cup g$ is a function.
($\Leftarrow$) Take any $x\in(\operatorname{dom} f)\cap(\operatorname{dom} g)$. $(x,f(x))\in f\cup g$ and $(x,g(x))\in f\cup g$. Since $f\cup g$ is a function, we have $f(x)=g(x)$.

(ii) Let $A=(\operatorname{dom} f)\cap(\operatorname{dom} g)$.
($\Rightarrow$) By definition, $\operatorname{dom} f\big|_A=\operatorname{dom} g\big|_A=(\operatorname{dom} f)\cap(\operatorname{dom} g)$. Moreover, for all $x\in(\operatorname{dom} f)\cap(\operatorname{dom} g)$, $f\big|_A(x)=f(x)=g(x)=g\big|_A(x)$. Hence, the result follows by Lemma 2.3.3.
($\Leftarrow$) Take any $x\in A$. Then, $f(x)=f\big|_A(x)=g\big|_A(x)=g(x)$. □

Theorem 2.3.12

If F is a compatible system of functions, then $\bigcup F$ is a function with $\operatorname{dom}\bigcup F=\bigcup\{\operatorname{dom} f\mid f\in F\}$. The function $\bigcup F$ extends all $f\in F$.

Proof. Note that $\bigcup F$ is already a relation. If $(a,b_1),(a,b_2)\in\bigcup F$, 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 $a\in(\operatorname{dom} f_1)\cap(\operatorname{dom} f_2)$, we have $b_1=f_1(a)=f_2(a)=b_2$. Hence, $\bigcup F$ is a function.

$\operatorname{dom}\bigcup F=\bigcup\{\operatorname{dom} f\mid f\in F\}$ since

$$\begin{aligned} x\in\operatorname{dom}\bigcup F &\iff \exists y,\ (x,y)\in\bigcup F\\ &\iff \exists y,\ \exists f\in F,\ (x,y)\in f\\ &\iff \exists f\in F,\ x\in\operatorname{dom} f \iff x\in\bigcup\{\operatorname{dom} f\mid f\in F\}.\end{aligned}$$

Take any $f\in F$. As $f\cup\bigcup F=\bigcup F$, f and $\bigcup F$ are compatible by Lemma 2.3.11 (i). Moreover, $\operatorname{dom} f\cap\operatorname{dom}\bigcup F=\operatorname{dom} f$. Hence, by Lemma 2.3.11 (ii), $f=f\big|_{\operatorname{dom} f}=\left(\bigcup F\right)\big|_{\operatorname{dom} f}$; $\bigcup F$ extends each $f\in F$. □

Definition 2.3.13

Let A and B be sets. Then, we define

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

Definition 2.3.14: Indexed System of Sets

- Let $S=\langle S_i\mid i\in I\rangle$ be a function with domain I. We call the function S an *indexed system of sets* whenever we stress that the values of S are sets.
- We say that a system of sets A is *indexed* by S if $A=\{S_i\mid i\in I\}=\operatorname{ran} S$.

Notation 2.3.15

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

$$\bigcup\{S_i\mid i\in I\}\quad\text{or}\quad\bigcup_{i\in I}S_i$$

instead of $\bigcup A$. Similarly, we may write $\bigcap\{S_i\mid i\in I\}$ or $\bigcap_{i\in I}S_i$ instead of $\bigcap A$.

Definition 2.3.16: Product of Indexed System of Sets

Let $S = \langle S_i \mid i \in I \rangle$ be an indexed system of sets. We call the set

$$\prod S \triangleq \{ f \mid f \text{ is a function on } I \text{ and } \forall i \in I,\ f_i \in S_i \}$$

the *product* of the indexed system S.

Notation 2.3.17

Other notations for the product of the indexed system $S = \langle S_i \mid i \in I \rangle$ are:

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

Note:-

The existence of B^A and $\prod_{i \in I} S_i$ is proved in Exercise 2.3.9.

Note:-

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

Selected Problems

Exercise 2.3.4

Let f be a function. If there exists a function g such that $g \circ f = \mathrm{Id}_{\operatorname{dom} f}$, then f is invertible and $f^{-1} = g\big|_{\operatorname{ran} f}$.

Proof. For $x_1, x_2 \in \operatorname{dom} f$, suppose $f(x_1) = f(x_2)$. Then, $x_1 = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = x_2$. Hence, f is one-to-one and is inverible by Theorem 2.3.9.

Take any $(y, x) \in f^{-1}$. Then, as $x \in \operatorname{dom} f$, we must have $(y, x) \in \mathrm{Id}_{\operatorname{dom} f}$. Hence, $f^{-1} \subseteq g\big|_{\operatorname{ran} f}$. Now, take any $(y, x) \in g\big|_{\operatorname{ran} f}$. Since $y \in \operatorname{ran} f$, there exists $x' \in \operatorname{dom} f$ such that $(x', y) \in f$. Since $g \circ f = \mathrm{Id}_{\operatorname{dom} f}$, we have $x = x'$. Therefore, $(y, x) \in f^{-1}$; $g\big|_{\operatorname{ran} f} \subseteq f^{-1}$. □

Exercise 2.3.6

Let f be a function.

(i) $f^{-1}[A \cap B] = f^{-1}[A] \cap f^{-1}[B]$

(ii) $f^{-1}[A \setminus B] = f^{-1}[A] \setminus f^{-1}[B]$

Proof. Thanks to Exercise 2.2.3 (ii) and (iii), we only need to prove the other inclusions.

(i) Take any $x \in f^{-1}[A] \cap f^{-1}[B]$. Then, there exists $a \in A$ and $b \in B$ such that $x f a$ and $x f b$. Since f is a function, $a = b$, and thus $x \in f^{-1}[A \cap B]$.

(ii) Take any $x \in f^{-1}[A \setminus B]$. Then, $f(x) \in A \setminus B$. If $x \in f^{-1}[B]$, we would have $f(x) \in B$; thus $x \notin f^{-1}[B]$. Therefore, $x \in f^{-1}[A] \setminus f^{-1}[B]$. □

Exercise 2.3.8

Every system of sets A can be indexed by a function.

Proof. Let S be the function Id_A so $S_i = i$ for all $i \in A$. Then, $A = \{S_i \mid i \in A\}$; A is indexed by S. $\square$

Exercise 2.3.9

(i) Let A and B be sets. Prove that B^A exists.

(ii) Let $\langle S_i \mid i \in I\rangle$ be an indexed system of sets. Prove that $\prod_{i\in I} S_i$ exists.

Proof.

(i) If f is a function from A into B, then $f \subseteq A \times B$, i.e., $f \in \mathcal{P}(A \times B)$.

(ii) 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, $f \in \left(\bigcup_{i\in I} S_i\right)^I$. $\square$

Exercise 2.3.10

Let $\langle F_a \mid a \in \bigcup S\rangle$ be an indexed system of sets.

(i) $\bigcup_{a\in\bigcup S} F_a = \bigcup_{C\in S}\left[\bigcup_{a\in C} F_a\right]$

(ii) $\bigcap_{a\in\bigcup S} F_a = \bigcap_{C\in S}\left[\bigcap_{a\in C} F_a\right]$ if $S \neq \varnothing$ and $\forall C \in S,\ C \neq \varnothing$.

Proof.

(i)
$$\begin{aligned} x \in \bigcup_{a\in\bigcup S} F_a &\iff \exists a \in \bigcup S,\ x \in F_a \\ &\iff \exists C \in S,\ \exists a \in C,\ x \in F_a \\ &\iff \exists C \in S,\ x \in \bigcup_{a\in C} F_a \iff x \in \bigcup_{C\in S}\left[\bigcup_{a\in C} F_a\right] \end{aligned}$$

(ii)
$$\begin{aligned} x \in \bigcap_{a\in\bigcup S} F_a &\iff \forall a \in \bigcup S,\ x \in F_a \\ &\iff \forall C \in S,\ \forall a \in C,\ x \in F_a \\ &\iff \forall C \in S,\ x \in \bigcap_{a\in C} F_a \iff x \in \bigcap_{C\in S}\left[\bigcap_{a\in C} F_a\right] \end{aligned}$$ $\square$

Exercise 2.3.11

Let $\langle F_a \mid a \in A\rangle$ be an nonempty indexed system of sets.

(i) $B \setminus \bigcup_{a\in A} F_a = \bigcap_{a\in A}(B \setminus F_a)$

(ii) $B \setminus \bigcap_{a\in A} F_a = \bigcup_{a\in A}(B \setminus F_a)$

Proof.

(i)
$$\begin{aligned} x \in B \setminus \bigcup_{a\in A} F_a &\iff x \in B \wedge \neg(\exists a \in A,\ x \in F_a) \\ &\iff x \in B \wedge \forall a \in A,\ x \notin F_a \\ &\iff \forall a \in A,\ (x \in B \wedge x \notin F_a) \iff x \in \bigcap_{a\in A}(B \setminus F_a) \end{aligned}$$

(ii)
$$\begin{aligned} x \in B \setminus \bigcap_{a\in A} F_a &\iff x \in B \wedge \neg(\forall a \in A,\ x \in F_a) \\ &\iff x \in B \wedge \exists a \in A,\ x \notin F_a \\ &\iff \exists a \in A,\ (x \in B \wedge x \notin F_a) \iff x \in \bigcup_{a\in A}(B \setminus F_a) \end{aligned}$$ $\square$

Exercise 2.3.12

Let R be a relation and let $\langle F_a \mid a \in A\rangle$ be an indexed system of sets.

(i) $R\left[\bigcup_{a\in A} F_a\right] = \bigcup_{a\in A} R[F_a]$

(ii) $R\left[\bigcap_{a\in A} F_a\right] \subseteq \bigcap_{a\in A} R[F_a]$ if $A \neq \varnothing$.

(iii) $R\left[\bigcap_{a\in A} F_a\right] = \bigcap_{a\in A} R[F_a]$ if $A \neq \varnothing$ and R is an injective function.

(iv) $R^{-1}\left[\bigcap_{a\in A} F_a\right] = \bigcap_{a\in A} R^{-1}[F_a]$ if $A \neq \varnothing$ and R is a function.

Proof.

(i) $y \in R\left[\bigcup_{a\in A} F_a\right] \iff \exists x \in \bigcup_{a\in A} F_a,\ xRy$
$\iff \exists a \in A,\ \exists x \in F_a,\ xRy$
$\iff \exists a \in A,\ y \in R[F_a] \iff x \in \bigcup_{a\in A} R[F_a]$

(ii) Take any $y \in R\left[\bigcap_{a\in A} F_a\right]$. Then, there exists $x \in \bigcap_{a\in A} F_a$ such that xRy. Hence, for all $a \in A$, $y \in R[F_a]$, i.e., $y \in \bigcap_{a\in A} R[F_a]$.

(iii) If R is an injective function, then R^{-1} is also a function. Hence, the result follows from (iv) and the fact that $R = (R^{-1})^{-1}$.

(iv) Thanks to (ii), since R^{-1} is a relation, we only need to prove the other inclusion. Take any $x \in \bigcap_{a\in A} R^{-1}[F_a]$. Fix any $a^* \in A$. Then, there exists $y^* \in F_{a^*}$ such that xRy^*.
Now, take any $a \in A$. Then, $\exists y \in F_a$ such that xRy. Since R is a function, $y = y^*$; $y^* \in F_a$, i.e., $y^* \in \bigcap_{a\in A} F_a$. Therefore, $x \in R^{-1}\left[\bigcap_{a\in A} F_a\right]$. □

Exercise 2.3.13

Let $\langle F_{a,b} \rangle_{a\in A,\, b\in B}$ be a nonempty indexed system of sets. Assuming that $\forall a \in A, \forall b_1, b_2 \in B$, $(b_1 \neq b_2 \implies F_{a,b_1} \cap F_{a,b_2} = \varnothing)$, the following equation holds.

$$\bigcap_{a\in A}\left[\bigcup_{b\in B} F_{a,b}\right] = \bigcup_{f\in B^A}\left[\bigcap_{a\in A} F_{a,f(a)}\right]$$

Proof. 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 $x \in L$. Let $f \triangleq \{(a,b) \in A \times B \mid x \in F_{a,b}\}$. Then, by assumption, f is a function. Moreover, as $x \in L$, f is a function on A into B. Therefore, $x \in \bigcap_{a\in A} F_{a,f(a)} \subseteq R$; thus $L \subseteq R$. ✓

($\supseteq$) Note that, for each $a \in A$, and $f : A \to B$, $\bigcap_{a\in A} F_{a,f(a)} \subseteq \bigcap_{a\in A}\left[\bigcup_{b\in B} F_{a,b}\right] = L$. Therefore, $R \subseteq L$. □

2.4 Equivalences and Partitions

Definition 2.4.1: 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 2.4.2: 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 2.4.3

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

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

Proof.

(i) ($\Rightarrow$) Suppose aEb. Take any $c \in [a]_E$. Then, cEa and aEb, and thus cEb by transitivity. Hence, $c \in [b]_E$; $[a]_E \subseteq [b]_E$. $[b]_E \subseteq [a]_E$ can be shown similarly since bEa holds as E is symmetric.
($\Leftarrow$) Suppose $[a]_E = [b]_E$. Since aEa by reflexivity, we have $a \in [a]_E = [b]_E$. Therefore, aEb.

(ii) ($\Rightarrow$) Suppose $[a]_E \cap [b]_E \neq \varnothing$. Then, there exists $c \in [a]_E \cap [b]_E$, i.e., cEa and cEb. Then, as E is symmetric, we have aEc, and therefore aEb by transitivity.
($\Leftarrow$) Suppose aEb. Then, since aEa by reflexivity, we have $a \in [a]_E$. We can see $a \in [b]_E$ from (i). Hence, $[a]_E \cap [b]_E \neq \varnothing$. □

Definition 2.4.4: Partition

A system S of nonempty sets is called a *partition* of A if
(i) S is a system of mutually disjoint sets (Definition 1.4.5) and
(ii) $\bigcup S = A$.

Definition 2.4.5: 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 2.4.6

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

Proof. If $[a]_E \neq [b]_E$, then by Lemma 2.4.3, we have $[a]_E \cap [b]_E = \varnothing$. Since E is reflexive, $a \in [a]_E$; each $[a]_E$ is nonempty. Therefore, A/E is a system of mutually disjoint nonempty sets.

Take any $a \in A$. Since E is reflexive, $a \in [a]_E \subseteq \bigcup A/E$. Therefore, $A \subseteq \bigcup A/E$. Conversely, since $[a]_E \subseteq A$, we have $\bigcup A/E \subseteq A$. □

Definition 2.4.7

Let S be a partition of A. The relation E_S in A is defined by

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

Theorem 2.4.8

Let S be a partition of A. Then, E_S is a equivalence on A.

Proof.

- Take any $a \in A$. As $A = \bigcup S$, there exists $C \in S$ such that $a \in C$. Therefore, aE_Sa. E_S is reflexive.
- Assume aE_Sb. Then, there exists $C \in S$ such that $a, b \in C$. Hence, bE_Sa. E_S is symmetric.

- Assume aE_Sb and bE_Sc. Then, there exist $C,D \in S$ such that $a,b \in C$ and $b,c \in D$. Then, $C \cap D \neq \varnothing$ as b belongs to both sets. Hence, $C = D$, which implies aE_Sc. E_S is transitive. $\square$

Theorem 2.4.9

(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) $aE_Sb \underbrace{\iff}_{\text{Definition 2.4.7}} \exists C \in S,\ a \in C \wedge b \in C \iff \exists c \in A,\ a \in [c]_E \wedge b \in [c]_E \underbrace{\iff}_{\text{Lemma 2.4.3}} aEb.$

(ii) Take any $[a]_{E_S} \in A/E_S$. Since S is a partition, there (uniquely) exists C such that $a \in C$. Then, for all b, we have $b \in C \iff aE_Sb \underbrace{\iff}_{\text{Lemma 2.4.3}} b \in [a]_{E_S}$; $C = [a]_{E_S}$. Therefore, $A/E_S \subseteq S$.
For the converse, take any $C \in S$. As C is nonempty, we may take some $a \in C$. Similarly, we have $C = [a]_{E_S}$. Therefore, $C \subseteq A/E_S$. $\square$

Note:-

Theorem 2.4.9 essentially states that equivalence and partition describe the same "mathematical reality."

Definition 2.4.10: 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

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

Selected Problems

Exercise 2.4.2

Let f be a function on A onto B. Define a relation E in A by: aEb if and only if $f(a) = f(b)$.

(i) Show that E is an equivalence on A.
(ii) Show that $[a]_E = [a']_E$ implies that $f(a) = f(a')$ so that the function φ on A/E into B defined by $\varphi([a]_E) = f(a)$ is well-defined. Show also that φ is *onto* B.
(iii) Let j be the function on A onto A/E given by $j(a) = [a]_E$. Show that $\varphi \circ j = f$.

Proof.

(i) E can readily be shown to be reflexive, symmetric, and transitive.
(ii) Assume $[a]_E = [a']_E$. Then, $f(a) = f(a')$ by definition of E. Hence, φ is well-defined. Take any $b \in B$. Since f is onto, there exists $a \in A$ such that $f(a) = b$. Hence, $\varphi([a]_E) = f(a) = b$; φ is onto B.
(iii) $\operatorname{dom}(\varphi \circ j) = (\operatorname{dom} j) \cap j^{-1}[\operatorname{dom} \varphi] = A = \operatorname{dom} f$ since j is onto. For all $a \in A$, $(\varphi \circ j)(a) = \varphi([a]_E) = f(a)$. Hence, by Lemma 2.3.3, $\varphi \circ j = f$. $\square$

2.5 Orderings

Definition 2.5.1: Partial Ordering and Strict Ordering

Let R be a binary relation in 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 2.5.2

- Define the relation $\subseteq_A$ in A as follows: $x \subseteq_A y$ if and only if $x, y \in A \wedge x \subseteq y$. Then, $(A, \subseteq_A)$ is an ordered set.
- The relation Id_A is a partial ordering of A.

Theorem 2.5.3

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

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

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.

(i) Suppose aSb and bSa. Since $S \subseteq R$, we have aRb and bRa. As R is antisymmetric, we have aRa, which is impossible since $S \cap \mathrm{Id}_S = \varnothing$. Hence, S is asymmetric in A.
Now, assuming aSb and bSc, we also have aRc since R is transitive. Moreover, a cannot be equal to c since S is shown to be asymmetric. Therefore, aSc; S is transitive in A.

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

Notation 2.5.4

- If R is a partial ordering, we say $S = R \setminus \mathrm{Id}_A$ *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 2.5.5: Comparability

Let $a, b \in A$ and let $\leq$ be a partial ordering of 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 $b \leq a$.

They 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 2.5.6: 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 2.5.7: 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 2.5.8: 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 2.5.9

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 2.5.10

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—it it exists—is also minimal.
(iii) If B is a chain, then every minimal element of B is also least.

Proof.

(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. □

Note:-

Theorem 2.5.10 still holds when 'least' and 'minimal' are replaced by 'greatest' and 'maximal', respectively.

Definition 2.5.11: 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 an *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 2.5.12

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 2.5.13

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 Theorem 2.5.10 (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. □

Note:-

Theorem 2.5.13 still holds when 'least' and 'infimum' are replaced by 'greatest' and 'supremum', respectively.

Definition 2.5.14: Isomorphism Between Ordered Sets

An *isomorphism* between two ordered sets $(P, \leq)$ and $(Q, \preceq)$ is a function $f : P \hookrightarrow\!\!\!\!\rightarrow Q$ 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*. This is justified by Exercise 2.5.13.

Lemma 2.5.15

Let $(P, \leq)$ be a totally ordered set and let $(Q, \preceq)$ be an ordered set. Let $h : P \hookrightarrow\!\!\!\!\rightarrow Q$ 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 $(Q, \leq)$ 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. Then, 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.

Take any $q_1, q_2 \in Q$. Then, since h is onto Q, there exist $p_1, p_2 \in P$ such that $q_1 = h(p_1)$ and $p_2 = h(p_2)$. 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 $p_2 \preceq q_1$. Therefore, $(Q, \preceq)$ is totally ordered. □

Selected Problems

Exercise 2.5.1

(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) $R^* = S \cup \mathrm{Id}_A = (R \setminus \mathrm{Id}_A) \cup \mathrm{Id}_A = R$ since $\mathrm{Id}_A \subseteq R$.

(ii) $S^* = R \setminus \mathrm{Id}_A = (S \cup \mathrm{Id}_A) \setminus \mathrm{Id}_A = S$ since $\mathrm{Id}_A \cap S = \varnothing$.

□

Exercise 2.5.6

Let $(A_1, <_1)$ and $(A_2, <_2)$ be strictly ordered sets and let $A_1 \cap A_2 = \varnothing$. 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 $<_1 \cap A_2^2 = <_2 \cap A_1^2 = (A_1 \times A_2) \cap A_1^2 = (A_1 \times A_2) \cap A_2^2 = \varnothing$, we get $\prec \cap A_1^2 = <_1$ and $\prec \cap A_2^2 = <_2$. □

Exercise 2.5.7

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 2.4.3, 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 2.4.3. ✓ □

Exercise 2.5.8

Let $A = \mathcal{P}(X)$ where X is a set.

(i) Any $S \subseteq A$ has a supremum in the ordering $\subseteq_A$; $\sup S = \bigcup S$.

(ii) Any $S \subseteq A$ has an infimum in the ordering $\subseteq_A$; $\inf S = \begin{cases} \bigcap S & \text{if } S \neq \varnothing \\ X & \text{if } S = \varnothing \end{cases}$.

Proof.

(i) As $C \subseteq_A \bigcup S$ for all $C \in S$, $\bigcup S$ is an upper bound of S. Let U be any upper bound of S. Take any $x \in \bigcup S$. Then, there exists $C \in S$ such that $x \in C$. Since $C \subseteq_A U$, we have $x \in U$. Therefore, $\bigcup S \subseteq U$; $\bigcup S$ is the least upper bound of S.

(ii) If $S = \varnothing$, then any $C \in A$ is an lower bound of S. Since $\bigcup A = X$—by (i), the supremum of the set of lower bounds of S—is a lower bound of S, X is the infimum of $S = \varnothing$. ✓
If $S \neq \varnothing$, as $\bigcap S \subseteq C$ for all $C \in S$, $\bigcap S$ is a lower bound of S. Let L be any lower bound of S. Take any $x \in L$. Then, $\forall C \in L$, $x \in C$, i.e., $x \in \bigcap S$. Therefore, $L \subseteq_A \bigcap S$; $\bigcap S$ is the infimum of S. ✓ □

Exercise 2.5.9

Let $\mathrm{Fn}(X,Y)$ be the set of all functions mapping a subset of X into Y, i.e., $\mathrm{Fn}(X,Y) = \bigcup_{Z \in \mathcal{P}(X)} Y^Z$. Define a relation $\leq$ in $\mathrm{Fn}(X,Y)$ by

$$f \leq g \iff f \subseteq g.$$

(i) $\leq$ is a partial ordering of $\mathrm{Fn}(X,Y)$.

(ii) Let $F \subseteq \mathrm{Fn}(X,Y)$. $\sup F$ exists if and only if F is a compatible system of functions. Moreover, $\sup F = \bigcup F$ if it exists.

Proof.

(i) $\leq \,=\, \subseteq_{\mathrm{Fn}(X,Y)}$ by definition; $\subseteq_{\mathrm{Fn}(X,Y)}$ is already a partial ordering of $\mathrm{Fn}(X,Y)$.

(ii) ($\Rightarrow$) Assume $h \in \mathrm{Fn}(X,Y)$ is a supremum of F. Then, $\forall f \in F$, $f \subseteq s$. Take any $f, g \in F$. Then, $f \cup g \subseteq h$, and thus $f \cup g$ is a function as h is a function. Therefore, by Lemma 2.3.11, f and g are compatible. Hence, F is a compatible system of functions.
($\Leftarrow$) Assume F is a compatible system of functions. Then, $\bigcup F \in \mathrm{Fn}(X,Y)$ by Theorem 2.3.12, and $f \leq \bigcup F$ for all $f \in F$ by definition; $\bigcup F$ is an upper bound of F. Let U be any upper bound of S. Take any $(x,y) \in \bigcup F$. Then, there exists $f \in S$ such that $(x,y) \in f$. Since $f \subseteq_A U$, we have $x \in U$. Therefore, $\bigcup F \subseteq U$; $\bigcup F$ is the least upper bound of S. □

Exercise 2.5.10

Let $\mathrm{Pt}(A)$ be the set of all partitions of A. Define a relation $\preccurlyeq$ in $\mathrm{Pt}(A)$ by

$$S_1 \preccurlyeq S_2 \iff \forall C \in S_1,\ \exists D \in S_2,\ C \subseteq D.$$

(We say that the partition S_1 is a *refinement* of the partition S_2 if $S_1 \preccurlyeq S_2$.)

(i) $\preccurlyeq$ is a partial ordering of $\mathrm{Pt}(A)$.
(ii) $\inf T$ exists for all $T \subseteq \mathrm{Pt}(A)$.
(iii) $\sup T$ exists for all $T \subseteq \mathrm{Pt}(A)$.

Proof.

(i) $\preccurlyeq$ is reflexive since, for all $S \in \mathrm{Pt}(A)$ and $C \in S$, $C \subseteq C$, i.e., $S \preccurlyeq S$. ✓

Assume $S_1 \preccurlyeq S_2$ and $S_2 \preccurlyeq S_1$. Take any $C \in S_1$. Then, there exists $D \in S_2$ such that $C \subseteq D$. In addition, there exists $E \in S_1$ such that $D \subseteq E$. We have $C \subseteq E$ but C is nonempty as S_1 is a partition, which implies $C \cap E \neq \varnothing$. Therefore, as S_1 is a partition, we must have $C = E$ and thus $C = D$. Hence, $S_1 \subseteq S_2$. This shows that $\preccurlyeq$ is antisymmetric. ✓

Assume $S_1 \preccurlyeq S_2$ and $S_2 \preccurlyeq S_3$. Take any $C \in S_1$. There exists $D \in S_2$ such that $C \subseteq D$. There exists $E \in S_3$ such that $D \subseteq E$. Hence, $C \subseteq E$; $S_1 \preceq S_3$. This shows that $\preccurlyeq$ is transitive. ✓

(ii) Define a relation E in A by $E \triangleq \{(a,b) \in A^2 \mid \forall S \in T, \exists C \in S,\ a \in C \wedge b \in C\}$. It can be easily shown that E is an equivalence mimicking the proof of Theorem 2.4.8. Then, $A/E \in \mathrm{Pt}(A)$ by Theorem 2.4.6.

> ***Claim 1.*** A/E is a lower bound of T.
>
> ***Proof.*** If $T = \varnothing$, there is nothing to prove; so assume $T \neq \varnothing$. Take any $S \in T$ and $a \in A$. Then, there exists $C \in S$ such that $a \in S$ since S is a partition of A. Let $b \in [a]_E$. Then, there exists $D \in S$ such that $a, b \in D$, which implies $C = D$. Therefore, $[a]_E \subseteq C$. Hence, $A/E \preccurlyeq S$. □

> ***Claim 2.*** For each lower bound L of T, $L \preccurlyeq A/E$.
>
> ***Proof.*** If $T = \varnothing$, then $A/E = \{A^2\}$ and every partition of A is a lower bound. Since $S \preccurlyeq \{A^2\}$ for all $S \in \mathrm{Pt}(A)$, the result follows.
>
> Now, assume $T \neq \varnothing$. Let L be a lower bound of T. Take any $D \in L$. Fix some $a \in D$. Then, each $d \in D$ has the property that $\forall S \in T, \exists C \in S, \{a, d\} \subseteq D \subseteq C$ as L is a lower bound of T. Therefore, $d \in [a]_E$; $D \subseteq [a]_E$. Hence, $L \preccurlyeq A/E$. □

Claims 1 and 2 say that $\inf T = A/E$. Hence, $\inf T$ exists.

(iii) Let $T' \triangleq \{S' \in \mathrm{Pt}(A) \mid \forall S \in T, S \preccurlyeq S'\}$. By (ii), $S^* \triangleq \inf T'$ exists.

> ***Claim 3.*** S^* is an upper bound of T.
>
> ***Proof.*** In (ii), we showed that $S^* = A/E$ where $E = \{(a,b) \in A^2 \mid \forall S' \in T', \exists C' \in S', a \in C' \wedge b \in C'\}$. Take any $S \in T$ and let $C \in S$. Fix some $c_0 \in C$.
>
> Now, take arbitrary $c \in C$. Then, for all $S' \in T'$, since $S \preccurlyeq S'$, there exists $D' \in S'$ such that $c \in C \subseteq D'$. Hence, we have cEc_0; $C \subseteq [c_0]_E$. Therefore, $S \preccurlyeq S^*$. □

Claim 3 essentially says that $S^* \in T'$. By Theorem 2.5.13 (iii), $S^* = \min T'$, i.e., $S^* = \sup T$. □

Exercise 2.5.13

If h is isomorphism between $(P, \leq)$ and $(Q, \preceq)$, then h^{-1} is an isomorphism between $(Q, \preceq)$ and $(P, \leq)$.

Proof. Take any $q_1, q_2 \in Q$. Then, we have $q_1 \preceq q_2 \iff h(h^{-1}(q_1)) \preceq h(h^{-1}(q_2)) \iff h^{-1}(q_1) \leq h^{-1}(q_2)$. □

Exercise 2.5.14

If f is an isomorphism between $(P_1, \leq_1)$ and $(P_2, \leq_2)$, and if g is an isomorphism between $(P_2, \leq_2)$ and $P_3, \leq_3$, then $g \circ f$ is an isomorphism between $(P_1, \leq_1)$ and $(P_3, \leq_3)$.

Proof. $\operatorname{ran}(g \circ f) = g[\operatorname{ran} f] = P_3$. Moreover, $g \circ f$ is one-to-one. Hence, $g \circ f : P_1 \hookrightarrow\!\!\!\rightarrow P_3$. For all $p, q \in P_1$, we have $p \leq_1 q \iff f(p) \leq_2 f(q) \iff g(f(p)) \leq_3 \iff g(f(q))$. Hence, $g \circ f$ is an isomorphism between $(P_1, \leq_1)$ and $(P_3, \leq_3)$. □

Chapter 3

Natural Numbers

3.1 Introduction to Natural Numbers

Note:-

We cannot prove an existence of an 'infinite' set (in the classical sense) or discuss infinity only from Axioms I to VI.

Definition 3.1.1: Successor

The *successor* of a set x is the set $S(x) = x \cup \{x\}$.

Notation 3.1.2: $n+1$

We write $n+1$ to denote $S(n)$. There is no implication regarding the classic "addition" in this notation.

Notation 3.1.3: Natural Numbers

- $0 = \varnothing$
- $1 = \{\varnothing\} = S(0) = 0 + 1$
- $2 = \{\varnothing, \{\varnothing\}\} = S(1) = 1 + 1$
- $\ldots$

Definition 3.1.4: Inductive Set

A set I is called *inductive* if

$$0 \in I \wedge \forall n \in I,\ (n+1) \in I.$$

Axiom VII Axiom of Infinity

An inductive set exists.

Definition 3.1.5: Set of All Natural Numbers

The *set of all natural numbers* is the set

$$\mathbb{N} \triangleq \{\, x \mid x \in I \text{ for all inductive set } I \,\}.$$

Note:-

Axiom of Infinity guarantees the existence of $\mathbb{N}$. For, if A is any inductive set, then $\mathbb{N} = \{ x \in A \mid x \in I \text{ for all inductive set } I \}$.

Lemma 3.1.6

$\mathbb{N}$ is inductive. In addition, if I is an inductive set, then $\mathbb{N} \subseteq I$.

Proof. Since $0 \in I$ for all inductive set, $0 \in \mathbb{N}$. If $n \in \mathbb{N}$, then $n \in I$ for all inductive set, and thus $(n+1) \in I$ for all inductive set. Therefore, $(n+1) \in \mathbb{N}$. Hence, $\mathbb{N}$ is inductive.

$\mathbb{N} \subseteq I$ directly follows from the definition of $\mathbb{N}$. □

Definition 3.1.7

The relation $<$ on $\mathbb{N}$ is defined by: $m < n$ if and only if $m \in n$.

Notation 3.1.8

Although we did not prove $<$ is a strict ordering of $\mathbb{N}$, we shall use $\leq$ to denote the relation on $\mathbb{N}$:

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

Selected Problems

Exercise 3.1.1

(i) $\forall x,\ x \subseteq S(x)$
(ii) $\forall x,\ \neg(\exists z,\ x \subsetneq z \subsetneq S(x))$

Proof.

(i) $x \subseteq x \subseteq x \cup \{x\} = S(x)$
(ii) Take any z such that such that $x \subseteq z \subseteq S(x) = x \cup \{x\}$. If $z \subseteq x$, then we have $z = x$. If $z \nsubseteq x$, then there exists y such that $y \in z$ and $y \notin x$. However, $y \in x \cup \{x\}$, and thus $y = x$. Therefore, $S(x) \subseteq z$; $z = S(x)$. In conclusion, any z such that $x \subseteq z \subseteq S(x)$ must satisfy $z = x$ or $z = S(x)$. □

3.2 Properties of Natural Numbers

Theorem 3.2.1 The Induction Principle

Let $\mathbf{P}(x)$ be a property (possibly with parameters).

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

Proof. The premise simply says that $A = \{n \in \mathbb{N} \mid \mathbf{P}(n)\}$ is inductive. Therefore, $\mathbb{N} \subseteq A$ follows. □

Lemma 3.2.2

(i) $\forall n \in \mathbb{N},\ 0 \leq n$
(ii) $\forall k, n \in \mathbb{N},\ (k < n+1 \iff k < n \vee k = n)$

Proof.

(i) Let $\mathbf{P}(x)$ be the property "$0 \leq x$." $\mathbf{P}(0)$, i.e., $0 \leq 0$, holds since $0 = 0$.

Now, assume $n \in \mathbb{N}$ and $\mathbf{P}(n)$. If $n = 0$, then we have $0 \in S(0) = n+1$ by definition (Definition 3.1.1). If $0 < n$, then $0 \in n$, and thus $0 \in n \cup \{n\} = S(n)$. Therefore, by The Induction Principle, the result follows.

(ii) Note that $k \in n \cup \{n\}$ if and only if $k \in n$ or $k = n$. $\square$

Theorem 3.2.3 $(\mathbb{N}, \leq)$ is Totally Ordered

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

Proof. We first need to prove that $(\mathbb{N}, \leq)$ is an ordered set.

Claim 1. $<$ is transitive in $\mathbb{N}$.

Proof. Let $\mathbf{P}(x)$ be the property "$\forall k, m \in \mathbb{N}, (k < m \land m < x \implies k < x)$." $\mathbf{P}(0)$ is true because there is no $m \in \mathbb{N}$ such that $m \in 0 = \varnothing$.

Now assume $n \in \mathbb{N}$ and $\mathbf{P}(n)$. Now, let $k, m \in \mathbb{N}$ and $k < m$ and $m < n+1$. By Lemma 3.2.2 (ii), $m < n$ or $m = n$.

- If $m < n$, then we have $k < n$ as $\mathbf{P}(n)$ holds,
- If $m = n$, then we immediately have $k < n$.

In both cases, we have $k < n$; thus $k < n+1$ by Lemma 3.2.2 (ii). Therefore, the result follows from The Induction Principle. $\square$

Claim 2. $<$ is asymmetric in $\mathbb{N}$.

Proof. Let $\mathbf{P}(x)$ be the property "$\neg(x < x)$." $\mathbf{P}(0)$ evidently holds since $\varnothing \notin \varnothing$.

Now, assume $n \in \mathbb{N}$ and $\mathbf{P}(n)$. Suppose $(n+1) < (n+1)$ for the sake of contradiction. By Lemma 3.2.2 (ii), we have $(n+1) = n$ or $(n+1) < n$. In both cases, we have $n < n$ by $n < (n+1)$ (from Lemma 3.2.2 (ii)) and Claim 1, which contradicts $\mathbf{P}(n)$. Therefore, $\mathbf{P}(n+1)$ holds. The result follows from The Induction Principle. $\square$

Hence, $(\mathbb{N}, \leq)$ is an ordered set by Claims 1 and 2 and Theorem 2.5.3. We are left to prove that $\leq$ is a total ordering of $\mathbb{N}$.

Claim 3. $\forall n, m \in \mathbb{N}, n < m \implies (n+1) \leq m$

Proof. Let $\mathbf{P}(x)$ be the property "$\forall n \in \mathbb{N}, (n < x \implies n+1 \leq x)$." $\mathbf{P}(0)$ holds since there is no $n \in \mathbb{N}$ such that $n < 0$.

Now, assume $m \in \mathbb{N}$ and $\mathbf{P}(m)$. Take any $n \in \mathbb{N}$ such that $n < (m+1)$. Then, by Lemma 3.2.2, we have $n = m$ or $n < m$. If $n = m$, then we have $(n+1) = (m+1)$, which implies $(n+1) \leq (m+1)$. If $n < m$, then $(n+1) \leq m < (m+1)$. Therefore, the result follows from The Induction Principle. $\square$

Claim 4. $<$ is a total ordering of $\mathbb{N}$.

Proof. Let $\mathbf{P}(x)$ be the property "$\forall m \in \mathbb{N}, m = x \lor m < x \lor x < m$." $\mathbf{P}(0)$ is essentially Lemma 3.2.2 (i).

Assume $n \in \mathbb{N}$ and $\mathbf{P}(n)$. Take any $m \in \mathbb{N}$. If $m < n$ or $m = n$, we have $m < (n+1)$ by Lemma 3.2.2 (ii). If $n < m$, by Claim 3, we have $(n+1) \leq m$. Hence, $\mathbf{P}(n+1)$ holds. Therefore, the result follows from The Induction Principle. $\square$

$\square$

Notation 3.2.4

We may write "$\forall k < n, \mathbf{P}(k)$" instead of "$\forall k \in \mathbb{N}, (k < n \implies \mathbf{P}(k))$" or "$\exists k < n, \mathbf{P}(k)$" instead of "$\exists k \in \mathbb{N}, k < n \wedge \mathbf{P}(k)$" when no confusion may arise. We may similarly write $(\forall/\exists)k(\leq/>/\geq)n, \mathbf{P}(k)$.

Theorem 3.2.5 The Strong Induction Principle

Let $\mathbf{P}(x)$ be a property (possibly with parameters). If, for all $n \in \mathbb{N}$, $\mathbf{P}(k)$ holds for all $k < n$, then $\mathbf{P}(n)$ holds for all $n \in \mathbb{N}$.

$$\forall n \in \mathbb{N}, [\forall k < n, \mathbf{P}(k) \implies \mathbf{P}(n)] \implies \forall n \in \mathbb{N}, \mathbf{P}(n)$$

Proof. Assume the premise $(\forall n \in \mathbb{N}, [\forall k < n, \mathbf{P}(k) \implies \mathbf{P}(n)])$. Let $\mathbf{Q}(n)$ be the property "$\forall k < n, \mathbf{P}(k)$." $\mathbf{Q}(0)$ holds since there is no $k < 0$.

Now, assume $n \in \mathbb{N}$ and $\mathbf{Q}(n)$. Then, by the premise, we have $\mathbf{P}(n)$. Lemma 3.2.2 (ii) enables us to say that $\forall k \in \mathbb{N}, (k < n+1 \implies P(k))$. Therefore, $\forall n \in \mathbb{N}$, $\mathbf{Q}(n)$ holds by The Induction Principle.

Take any $k \in \mathbb{N}$. Then, we have $k < k+1$ and thus $\mathbf{P}(k)$ holds by $\mathbf{Q}(k+1)$. □

Definition 3.2.6: Well-Ordering

A total ordering $\preceq$ of a set A is a *well-ordering* if every nonempty subset of A has a least element. Then, the ordered set $(A, \preceq)$ is called a *well-ordered set*.

Theorem 3.2.7 $(\mathbb{N}, \leq)$ is Well-Ordered

$(\mathbb{N}, \leq)$ is a well-ordered set.

Proof. Let $X \subseteq \mathbb{N}$ has no least element. For each $n \in \mathbb{N}$, if $\forall k < n$, $k \in \mathbb{N} \setminus X$, we must have $n \in \mathbb{N} \setminus X$ since otherwise $n = \min X$. Then, by The Strong Induction Principle, $\forall n \in \mathbb{N}, n \in \mathbb{N} \setminus X$, i.e., $X = \varnothing$. □

Theorem 3.2.8

Let $\varnothing \subsetneq X \subseteq \mathbb{N}$. 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 says that $Y \neq \varnothing$. By $(\mathbb{N}, \leq)$ is Well-Ordered, $n \triangleq \min Y = \sup X$ exists.

Suppose $n \notin X$ for the sake of contradiction. Then, $\forall m \in X$, $m < n$, which implies $n \neq 0$ as $X \neq \varnothing$. Therefore, $n = k+1$ for some $k \in \mathbb{N}$ by Exercise 3.2.4; and thus $\forall m \in X$, $m \leq k$ by Lemma 3.2.2 (ii). Then, k is an upper bound of A and $k < n$, which is a contradiction to $n = \sup X$. Therefore, $n \in X$, and hence $n = \max X$ by Theorem 2.5.13. □

Selected Problems

Exercise 3.2.2

$\forall m, n \in \mathbb{N}, (m < n \implies m+1 < n+1)$. Hence, $S : \mathbb{N} \to \mathbb{N}$ where $n \mapsto n+1$ defines a one-to-one function on $\mathbb{N}$.

Proof. By Claim 3 in the proof of $(\mathbb{N}, \leq)$ is Totally Ordered, we have $m+1 \leq n$. Together with $n < n+1$, we have $m+1 < n+1$.

Now, take any $m, n \in \mathbb{N}$ with $m \neq n$. Then, by $(\mathbb{N}, \leq)$ is Totally Ordered, we have $m < n$ or $n < m$, i.e., $S(m) < S(n)$ or $S(n) < S(m)$. In both cases, $S(m) \neq S(n)$. Therefore, S is one-to-one. □

Exercise 3.2.3

There exists $X \subsetneq \mathbb{N}$ and $f : \mathbb{N} \to X$ such that f is injective.

Proof. Let $S : \mathbb{N} \to \mathbb{N}$ where $n \mapsto n+1$. Then, S is injective by Exercise 3.2.2. Since there exists no $n \in \mathbb{N}$ such that $n \cup \{n\} = \varnothing$, $0 \notin \operatorname{ran} S$; $\operatorname{ran} S \subsetneq \mathbb{N}$. Therefore, $S : \mathbb{N} \to \operatorname{ran} S$ is the function we are looking for. □

Exercise 3.2.4

$\forall n \in \mathbb{N} \setminus \{0\}, \exists! k \in \mathbb{N}, n = k+1$

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

Now, assume $\mathbf{P}(n)$ where $n \in \mathbb{N}$. There exists $k \in \mathbb{N}$ such that $n+1 = k+1$, namely, $k = n$. If k' is another natural number such that $n+1 = k'+1$, then by Exercise 3.2.2, we have $k = k'$. Hence, $\mathbf{P}(n+1)$ holds. The result follows from The Induction Principle. □

Exercise 3.2.6

$\forall n \in \mathbb{N}, n = \{m \in \mathbb{N} \mid m < n\}$

Proof. Let $\mathbf{P}(x)$ be the property "$x = \{m \in \mathbb{N} \mid m < x\}$." We have $\mathbf{P}(0)$ since there exists no $m \in \mathbb{N}$ with $m < 0$.

Now, assume $\mathbf{P}(n)$ where $n \in \mathbb{N}$. Then, $n+1 = \{m \in \mathbb{N} \mid m < n\} \cup \{n\}$. By Lemma 3.2.2 (ii), $m < n+1$ if and only if $m < n$ or $m = n$. Therefore, $\{m \in \mathbb{N} \mid m < n\} \cup \{n\} = \{m \in \mathbb{N} \mid m < n \vee m = n\} = \{m \in \mathbb{N} \mid m < n+1\}$; $\mathbf{P}(n+1)$ holds. The result follows from The Induction Principle. □

Exercise 3.2.8

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

For the sake of induction, assume $\forall k < n, P(k)$ where $n \in \mathbb{N}$. Suppose there exists $f : \mathbb{N} \to \mathbb{N}$ such that $f(0) = n$ and $\forall k \in \mathbb{N}, f(k+1) < f(k)$. Now, define $g : \mathbb{N} \to \mathbb{N}$ by $g(k) = f(k+1)$. Then, $g(0) = f(1) < n$ and $\forall k \in \mathbb{N}, g(k+1) = f((k+1)+1) < f(k+1) = g(k)$. However, by $\mathbf{P}(g(0))$, such g cannot exist; by contradiction, $\mathbf{P}(n)$ holds. Hence, $\forall m \in \mathbb{N}, \mathbf{P}(m)$ by The Strong Induction Principle.

Finally, suppose there exists $f : \mathbb{N} \to \mathbb{N}$ such that $\forall n \in \mathbb{N}, f(n+1) < f(n)$. Then, by $\mathbf{P}(f(0))$, such f may not exist. □

Exercise 3.2.11

Let $\mathbf{P}(x)$ be a property and let $k \in \mathbb{N}$.

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

Proof. Let $\mathbf{Q}(x)$ be the property "$x < k \vee \mathbf{P}(x)$." If $k = 0$, then $\mathbf{P}(0)$ holds. If $k > 0$, then $0 < k$ holds. Hence, in both cases, $\mathbf{Q}(0)$ holds.

Now assume $\mathbf{Q}(n)$ holds where $n \in \mathbb{N}$. Then, by $(\mathbb{N}, \leq)$ is Totally Ordered, we have $n+1 < k$, $n+1 = k$, or $n+1 > k$. If $n+1 < k$ or $n+1 = k$, we immediately have $\mathbf{Q}(n+1)$. If $n+1 > k$, we have $n \geq k$ by Lemma 3.2.2 (ii). Therefore, $\mathbf{P}(n)$ holds, and thus $\mathbf{P}(n+1)$ holds by assumption. Hence, $\mathbf{Q}(n+1)$. By The Induction Principle, $\forall n \in \mathbb{N}$, $n < k \vee \mathbf{P}(n)$. In other words, $\forall n \geq k$, $\mathbf{P}(n)$. □

Exercise 3.2.12 The Finite Induction Principle

Let $\mathbf{P}(x)$ be a property and let $k \in \mathbb{N}$.

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

Proof. Let $\mathbf{Q}(x)$ be the property "$x > k \vee \mathbf{P}(x)$." $\mathbf{Q}(0)$ holds as $\mathbf{P}(0)$.

Now, assume $\mathbf{Q}(n)$ holds where $n \in \mathbb{N}$. Then, by $(\mathbb{N}, \leq)$ is Totally Ordered, we have $n+1 \leq k$ or $n+1 > k$. If $n+1 > k$, then we immediately have $\mathbf{Q}(n+1)$. If $n+1 \leq k$, by Lemma 3.2.2, $n+1 < k+1$. By Exercise 3.2.2 and $(\mathbb{N}, \leq)$ is Totally Ordered, we must have $n < k$. Hence, $\mathbf{P}(n)$ holds, and therefore $\mathbf{P}(n+1)$ holds by the assumption. By The Induction Principle, $\forall n \in \mathbb{N}$, $n > k \vee \mathbf{P}(n)$. In other words, $\forall n \leq k$, $\mathbf{P}(n)$. □

Exercise 3.2.13 The Double Induction Principle

Let $\mathbf{P}(x, y)$ be a property.

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

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

Now, assume $\forall k < m$, $\mathbf{Q}(k)$ where $m \in \mathbb{N}$. For the sake of induction, assume again that $\forall \ell < n$, $\mathbf{P}(m, \ell)$ where $n \in \mathbb{N}$. Now, we have $\mathbf{P}(k, \ell)$ for all $k, \ell \in \mathbb{N}$ such that $k < m$ or $k = m$ and $\ell < n$. Hence, by [$*$], $\mathbf{P}(m, n)$. By The Strong Induction Principle, we have $\forall n \in \mathbb{N}$, $\mathbf{P}(m, n)$. In other words, $\mathbf{Q}(m)$. Again by The Strong Induction Principle, we have $\forall m \in \mathbb{N}$, $\mathbf{Q}(m)$, that is to say $\forall m, n \in \mathbb{N}$, $\mathbf{P}(m, n)$. □

3.3 The Recursion Theorem

Definition 3.3.1: Sequence

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

$$\langle a_i \mid i < n \rangle \quad \text{or} \quad \langle a_i \mid i = 0, 1, \cdots, n-1 \rangle \quad \text{or} \quad \langle a_0, a_1, \cdots, a_{n-1} \rangle.$$

In particular, $\langle\rangle = \varnothing$—the *empty sequence*—is the unique sequence of length 0.

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

denote the set of all finite sequence of elements of A.
- A sequence whose domain is $\mathbb{N}$ is called a *infinite sequence* and is denoted

$$\langle a_i \mid i \in \mathbb{N} \rangle \quad \text{or} \quad \langle a_i \mid i = 0, 1, 2, \cdots \rangle \quad \text{or} \quad \langle a_i \rangle_{i=0}^{\infty}.$$

Infinite sequences of elements of A are members of $A^{\mathbb{N}}$. We also use the notation $\{ a_i \mid i \in \mathbb{N} \}$ or $\{a_i\}_{i=0}^{\infty}$, etc., for the range of the sequence $\langle a_i \mid i \in \mathbb{N} \rangle$.

Note:-

- A natural number $n \in \mathbb{N}$ is the set of all natural numbers less than n. See Exercise 3.2.6.
- Since $A^n \in \mathcal{P}(\mathbb{N} \times A)$ for each $n \in \mathbb{N}$, $\mathcal{A} = \{ w \mid \exists n \in \mathbb{N},\ w = A^n \}$ exists, and thus $\mathrm{Seq}(A) = \bigcup \mathcal{A}$ exists.

Theorem 3.3.2 The Recursion Theorem

Let A be a set, $a \in A$, and $g : A \times \mathbb{N} \to A$. Then, there uniquely exists an infinite sequence $f : \mathbb{N} \to A$ such that

(i) $f_0 = a$ and

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

Proof. We say $t : (m+1) \to A$ is an *m-step computation based on a and g* if $t_0 = a$ and $\forall k < m$, $t_{k+1} = g(t_k, k)$. Let $F \triangleq \{ t \in \mathrm{Seq}(A) \mid t \text{ is an } m \text{ step computation for some } m \in \mathbb{N} \}$. Let $f \triangleq \bigcup F$.

Claim 1. f is a function.

Proof. We shall show that F is a compatible system of functions so we may conclude f is a function thanks to Theorem 2.3.12. Take any $t, u \in F$. Let $n = \operatorname{dom} t \in \mathbb{N}$ and $m = \operatorname{dom} u \in \mathbb{N}$. WLOG, $n \le m$ (thanks to $(\mathbb{N}, \le)$ is Totally Ordered), i.e., $n \subseteq m$. Hence, $(\operatorname{dom} t) \cap (\operatorname{dom} u) = n$. If $n = 0$, then it is done; assume $n > 0$. Then, there exists $n' \in \mathbb{N}$ such that $n' + 1 = n$ by Exercise 3.2.4.

Surely, $t_0 = a = u_0$. Moreover, if $t_k = u_k$ where $k < n'$, then $k + 1 < n' + 1 = n$ (Exercise 3.2.2) and $t_{k+1} = g(t_k, k) = g(u_k, k) = u_{k+1}$. Therefore, by The Finite Induction Principle, we have $\forall k \le n'$, $t_k = u_k$; t and u are compatible. □

Claim 2. $\operatorname{dom} f = \mathbb{N}$ and $\operatorname{ran} f \subseteq A$.

Proof. We already have $\operatorname{dom} f \subseteq \mathbb{N}$ and $\operatorname{ran} f \subseteq A$ by Theorem 2.3.12. To show $\operatorname{dom} f = \mathbb{N}$, it suffices to show that, for any $n \in \mathbb{N}$, there is an n-step computation based on a and g. Clearly, $t = \{(0,a)\}$ is a 0-step computation.

Assume there exists an n-step computation $t\colon (n+1) \to A$ where $n \in \mathbb{N}$. Then, define $u\colon ((n+1)+1) \to A$ by $u \triangleq t \cup \{(n+1, g(t_n, n))\}$. Then, one may easily verify that u is an $(n+1)$-step computation. Therefore, by The Induction Principle, the result follows. $\square$

We now check if f satisfies the conditions (i) and (ii).

(i) Clearly, $f_0 = a$.

(ii) Take any $n \in \mathbb{N}$. Let t be an $(n+1)$-step computation. Then, $\forall k \le n$, $f_k = t_k$, and $f_{n+1} = t_{n+1} = g(t_n, n) = g(f_n, n)$.

Now, we are left to show the uniqueness of such f.

Let $h\colon \mathbb{N} \to A$ be a sequence that satisfies the conditions (i) and (ii). Clearly, $f_0 = a = h_0$. And, if $f_n = h_n$, then $f_{n+1} = g(f_n, n) = g(h_n, n) = h_{n+1}$. Therefore, by The Induction Principle, $\forall k \in \mathbb{N}$, $f_k = h_k$, i.e., $f = k$ by Lemma 2.3.3. $\square$

Theorem 3.3.3

Let $(A, \preceq)$ be a nonempty linearly ordered set with the properties:

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

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

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

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

Proof. By (i), $\{a \in A \mid x \prec a\} \ne \varnothing$ for each $x \in A$ and it has a $\preceq$-least element. Hence, we may define $g\colon A \times \mathbb{N} \to A$ by $g(x,n) \triangleq \min\{a \in A \mid x \prec a\}$. Then, The Recursion Theorem guarantees the existence of a function $f\colon \mathbb{N} \to A$ such that:

- $f_0 = \min A$ $\qquad \triangleright$ (i) and $A \ne \varnothing$
- $\forall n \in \mathbb{N}$, $f_{n+1} = g(f_n, n) = \min\{a \in A \mid f_n \prec a\}$.

By Exercise 3.3.1, we have $f_m \prec f_n$ whenever $m < n$. This also implies that f is injective.

Claim 1. $\operatorname{ran} f = A$

Proof. Suppose $\operatorname{ran} f \subsetneq A$ for the sake of contradiction. Then, $A \setminus \operatorname{ran} f \ne \varnothing$, and thus we may take $p = \min(A \setminus \operatorname{ran} f)$, which gives $p \ne f_0$ immediately. Hence, $B = \{a \in A \mid a \prec p\} \ne \varnothing$ and p is an upper bound of B. By (iii), $q = \max B$ exists. Since $q \prec p$, we have $q \in \operatorname{ran} f$, i.e., $q = f_m$ for some $m \in \mathbb{N}$.

Suppose there is some $r \in A$ such that $q \prec r \prec p$. Then, $r \in B$, which contradicts the maximality of q. Hence, $p = \min\{a \in A \mid f_m \prec a\} = f_{m+1}$, which contradicts $p \notin \operatorname{ran} f$. $\square$

We have $f\colon \mathbb{N} \hookrightarrow\!\!\!\!\rightarrow A$ by Claim 1. Hence, by $(\mathbb{N}, \le)$ is Totally Ordered and Lemma 2.5.15, f is an isomorphism between $(\mathbb{N}, \le)$ and $(A, \preceq)$. $\square$

Theorem 3.3.4 The Recursion Theorem: General Version

Let S be a set and let $g\colon \operatorname{Seq}(S) \to S$. Then, there exists a unique sequence $f\colon \mathbb{N} \to S$ such that

$$\forall n \in \mathbb{N},\ f_n = g\left(f\big|_n\right) = g(\langle f_0, f_1, \cdots, f_{n-1}\rangle).$$

Proof. Define $G\colon \operatorname{Seq}(S)\times\mathbb{N}\to\operatorname{Seq}(S)$ by

$$G(t,n)=\begin{cases} t\cup\{(n,g(t))\} & \text{if } t \text{ is a sequence of length } n\\ \langle\rangle & \text{otherwise.}\end{cases}$$

Then, by The Recursion Theorem, there exists a sequence $F:\mathbb{N}\to\operatorname{Seq}(S)$ such that:

- $F_0=\langle\rangle$
- $\forall n\in\mathbb{N},\ F_{n+1}=G(F_n,n)$.

If $F_k\in S^k$, then $F_{k+1}=F_k\cup\{k,g(F_k)\}\in S^{k+1}$. Hence, by The Induction Principle, $\forall n\in\mathbb{N}, F_n\in S^n$. Moreover, since $F_k\subsetneq_{\operatorname{Seq}(S)}F_{k+1}$, by Exercise 3.3.1, $\forall m,n\in\mathbb{N},(m<n\implies F_m\subsetneq F_n)$; hence $\{F_n\mid n\in\mathbb{N}\}$ is a compatible system of functions.

Let $f\triangleq\bigcup_{n\in\mathbb{N}}F_n$. Then, we have $f\big|_n=F_n$ for all $n\in\mathbb{N}$. Therefore, for each $n\in\mathbb{N}$, $f_n=F_{n+1}(n)=g(F_n)=g\left(f\big|_n\right)$.

Let $h\colon\mathbb{N}\to S$ be another sequence such that $\forall n\in\mathbb{N},\ h_n=g\left(h\big|_n\right)$. Suppose $\forall k<n, f_k=h_k$. Then, we have $f_n=g\left(f\big|_n\right)=g\left(h\big|_n\right)=h_n$. Therefore, by The Strong Induction Principle, $f=h$. □

Theorem 3.3.5 The Recursion Theorem: Parametric Version

Let $a:P\to A$ and $g:P\times A\times\mathbb{N}\to A$ be functions. Then, there uniquely exists a function $f:P\times\mathbb{N}\to A$ such that

(i) $\forall p\in P,\ f(p,0)=a(p)$
(ii) $\forall n\in\mathbb{N},\ \forall p\in P,\ f(p,n+1)=g(p,f(p,n),n)$.

Proof. Let $G\colon A^P\times\mathbb{N}\to A^P$ be defined by

$$G(x,n)(p)=g(p,x(p),n)$$

for each $x\in A^P$, $p\in P$, and $n\in\mathbb{N}$. Then, by The Recursion Theorem, there exists $F:\mathbb{N}\to A^P$ such that

$$F_0=a\quad\text{and}\quad\forall n\in\mathbb{N},\ F_{n+1}=G(F_n,n).$$

Now, let $f:P\times\mathbb{N}\to A$ be defined by $f(p,n)=F_n(p)$. We now check if f satisfies the conditions:

(i) For all $p\in P$, we have $f(p,0)=F_0(p)=a(p)$.
(ii) For each $n\in\mathbb{N}$ and $p\in P$, $f(p,n+1)=F_{n+1}(p)=G(F_n,n)(p)=g(p,F_n(p),n)=g(p,f(p,n),n)$.

Let $h\colon P\times\mathbb{N}\to A$ be another function that satisfies (i) and (ii). Clear, we have $\forall p\in P, f(p,0)=a(p)=h(p,0)$. Assuming $\forall p\in P, f(p,n)=h(p,n)$ gives, for all $p\in P$, $f(p,n+1)=g(p,f(p,n),n)=g(p,h(p,n),n)=h(p,n+1)$. Hence, by The Induction Principle, we get $f=h$. □

Selected Problems

Exercise 3.3.1

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 "$f_n\prec f_x$." $\mathbf{P}(n+1)$ evidently holds. Now, suppose $\mathbf{P}(k)$ holds where $k\in\mathbb{N}$. Then, chaining $f_n\prec f_k$ and $f_k\prec f_{k+1}$ gives $\mathbf{P}(k+1)$. Therefore, by Exercise 3.2.11, we get $\forall m\geq n+1,\ f_n\prec f_m$. □

Exercise 3.3.2

Let $(A, \preceq)$ be a nonempty linearly ordered set. We say that $q \in A$ is a *successor* of $p \in A$ if there is no $r \in A$ such that $p \prec r \prec q$. Assume $(A, \preceq)$ has 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 (i), for each $p \in P$, $\{q \in A \mid p \prec q\} \neq \varnothing$, and thus it has a $\preceq$-least element by (ii). Therefore, by The Recursion Theorem, there exists a sequence $f : \mathbb{N} \to A$ such that $f_0 = \min A$ and $\forall n \in \mathbb{N}$, $f_{n+1} = \min\{q \in A \mid f_n \prec q\}$.

Claim 1. $\operatorname{ran} f = A$

Proof. Suppose $X \triangleq A \setminus \operatorname{ran} f \neq \varnothing$ for the sake of contradiction. Then, by (ii), we may take $p = \min X$. Since $\min A = f_0 \in \operatorname{ran} f$, p is not the $\preceq$-least element of A. Hence, by (iii), p is a successor of some $q \in A$. As $q \prec p$, we have $q \in \operatorname{ran} f$ by minimality of q, i.e., $q = f_m$ for some $m \in \mathbb{N}$. Since there is no $r \in A$ such that $q \prec r \prec p$, we have $p = f_{m+1}$ by definition, which contradicts $p \notin \operatorname{ran} f$. □

Since $f_n \prec f_{n+1}$ for all $n \in \mathbb{N}$, by Exercise 3.3.1, $\forall m, n \in \mathbb{N}$, $(m < n \implies f_m \prec f_n)$, which means f is injective.

Therefore, together with Claim 1, f is an isomorphism between $(\mathbb{N}, \leq)$ and $(A, \preceq)$ by Lemma 2.5.15. □

Exercise 3.3.5 The Recursion Theorem: Partial Version

Let g be a function such that $\operatorname{dom} g \subseteq A \times \mathbb{N}$ and $\operatorname{ran} g \subseteq A$. Let $a \in A$. Then, there uniquely exists a sequence f of elements of A such that

(i) $f_0 = a$
(ii) $\forall n \in \mathbb{N}$, $[n+1 \in \operatorname{dom} f \implies f_{n+1} = g(f_n, n)]$
(iii) f is either an infinite sequence or a finite sequence of length $k+1$ and $(f_k, k) \notin \operatorname{dom} g$.

Proof. Let $\overline{A} = A \cup \{\overline{a}\}$ where $\overline{a} \notin A$. (Such $\overline{a}$ exists by Exercise 1.3.3 (ii).) Define $\overline{g} : \overline{A} \times \mathbb{N} \to \overline{A}$ by

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

Then, The Recursion Theorem guarantees the existence of $\overline{f} : \mathbb{N} \to \overline{A}$ such that $\overline{f}_0 = a$ and $\forall n \in \mathbb{N}$, $\overline{f}_{n+1} = \overline{g}(\overline{f}_n, n)$. We have two cases: "$\forall n \in \mathbb{N}$, $\overline{f}_n \neq \overline{a}$" and "$\exists n \in \mathbb{N}$, $\overline{f}_n = \overline{a}$." They are resolved by Claims 1 and 2, respectively.

Claim 1. 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 (i) and (ii).

Proof. The assumption essentially says that $(\overline{f}_n, n) \in \operatorname{dom} g$ and $\overline{f}_{n+1} = g(\overline{f}_n, n) \in A$ for all $n \in \mathbb{N}$, i.e., $\overline{f}$ satisfies (i) and (ii). As $\overline{f}_0 = a \in A$, $\overline{f}$ is an infinite sequence of elements of A. □

Claim 2. If "$\exists n \in \mathbb{N}, \overline{f}_n = \overline{a}$," then there exists $k \in \mathbb{N}$ such that $\overline{f}\big|_{k+1}$ satisfies the conditions (i), (ii), and (iii).

Proof. By $(\mathbb{N}, \leq)$ is Well-Ordered, we have $\ell \triangleq \min\{n \in \mathbb{N} \mid \overline{f}_n = \overline{a}\}$. Since $\overline{f}_0 \in A$, we have $\ell \neq 0$, and thus $\ell = k+1$ for some $k \in \mathbb{N}$ by Exercise 3.2.4. It immediately follows that $\forall n \leq k, \overline{f}_n \in A$. Hence, $f \triangleq \overline{f}\big|_{k+1}$ is a finite sequence of length $k+1$ of elements of A.

We check if f satisfies the conditions (i), (ii), and (iii):

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

(ii) If $n < k$, i.e., $n+1 \in \operatorname{dom} f = k+1$, then $f_{n+1} = \overline{f}_{n+1} = \overline{g}(\overline{f}_n, n) = g(f_n, n)$.

(iii) If $(f_k, k) \in \operatorname{dom} g$, then we would have $\overline{f}_\ell = \overline{g}(\overline{f}_k, k) = \overline{g}(f_k, k) = g(f_k, k) \neq \overline{a}$. Hence, we must have $(f_k, k) \notin \operatorname{dom} g$. □

Now, we prove the uniqueness. Let f and h be two sequences of elements of A that satisfies the conditions (i), (ii), and (iii). WLOG, $\operatorname{dom} h \subseteq \operatorname{dom} f$.

Let $\mathbf{P}(x)$ be the property "$x \in \operatorname{dom} h \wedge f_x = h_x$." $\mathbf{P}(0)$ evidently holds.

Claim 3. $\forall n \in \mathbb{N}, (n+1 \in \operatorname{dom} f \wedge \mathbf{P}(n) \implies \mathbf{P}(n+1))$

Proof. Assume $n+1 \in \operatorname{dom} f$ and $\mathbf{P}(n)$. Then, since $(h_n, n) = (f_n, n) \in \operatorname{dom} g$, $n+1 \in \operatorname{dom} h$ and $h_{n+1} = g(h_n, n) = g(f_n, n) = f_{n+1}$. Hence, $\mathbf{P}(n+1)$ holds. □

If f is a finite sequence, Claim 3 and The Finite Induction Principle imply $h = f$. If f is an infinite sequence, Claim 3 and The Induction Principle imply $h = f$. □

Exercise 3.3.6

If $X \subseteq \mathbb{N}$, then there is a one-to-one (finite or infinite) sequence f such that $\operatorname{ran} f = X$.

Proof. If $X = \varnothing$, $\langle\rangle$ is the one we are looking for. Assume $X \neq \varnothing$.

Let $g = \left\{((x,n), y) \in (X \times \mathbb{N}) \times X \;\middle|\; y = \min\{k \in X \mid x < k\}\right\}$. Then, g is a function with $\operatorname{dom} g \subseteq \mathbb{N} \times \mathbb{N}$ and $\operatorname{ran} g \subseteq \mathbb{N}$. By The Recursion Theorem: Partial Version, there exists a sequence f of elements of X such that

(i) $f_0 = \min X$ ▹ $\min X$ exists by $(\mathbb{N}, \leq)$ is Well-Ordered

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

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

Note that $\operatorname{dom} g = \{(x,n) \in X \times \mathbb{N} \mid \exists y \in X, x < y\}$. Moreover, for each $n \in \mathbb{N}$ such that $n+1 \in \operatorname{dom} f$, we have $f_n < f_{n+1}$; hence $\forall m, n \in \operatorname{dom} f, (m < n \implies f_m < f_n)$ (in the similar manner of Exercise 3.3.1), and thus f is injective.

Suppose $Y = X \setminus \operatorname{ran} f \neq \varnothing$ for the sake of contradiction. By $(\mathbb{N}, \leq)$ is Well-Ordered, we may take $y = \min Y$. Then, by Theorem 3.2.8, we may let $z = \max\{x \in X \mid x < y\}$. $z = f_m$ for some $m \in \operatorname{dom} f$. Hence, $y = f_{m+1}$. □

3.4 Arithmetic of Natural Numbers

Theorem 3.4.1

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

(i)) $\forall m \in \mathbb{N}, +(m, 0) = m$

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

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

Definition 3.4.2: Addition

The function $+$ defined in Theorem 3.4.1 is called the *addition*.

Notation 3.4.3

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 Notation 3.1.2. We restate the defining properties of the addition for future reference:

$$\forall m \in \mathbb{N},\ m+0 = m \qquad [1]$$

$$\forall m,n \in \mathbb{N},\ m+(n+1) = (m+n)+1 \qquad [2]$$

Theorem 3.4.4 $+$ is Commutative

Addition is commutative; that is to say

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

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

Claim 1. $\mathbf{P}(0)$ holds.

Proof. Since $m+0 = m$ already, we only need to prove $0+m = m$ for all $m \in \mathbb{N}$. We shall make use of induction. First of all $0+0 = 0$ holds by [1].

Suppose $0+m = m$ where $m \in \mathbb{N}$. Then,

$$\begin{aligned} 0+(m+1) &= (0+m)+1 && \triangleright\ [2] \\ &= m+1. && \triangleright\ 0+m = m \end{aligned}$$

Hence, by The Induction Principle, $0+m = m$ for all $m \in \mathbb{N}$. $\square$

Claim 2. $\forall n \in \mathbb{N},\ [\mathbf{P}(n) \implies \mathbf{P}(n+1)]$

Proof. Assume $\mathbf{P}(n)$. We shall show $\mathbf{P}(n+1)$ holds by induction. $0+(n+1) = (n+1)+0$ is already shown by Claim 1. Hence, assume $m+(n+1) = (n+1)+m$ for fixed $m \in \mathbb{N}$. Then,

$$\begin{aligned} (m+1)+(n+1) &= ((m+1)+n)+1 && \triangleright\ [2] \\ &= (n+(m+1))+1 && \triangleright\ \mathbf{P}(n) \\ &= ((n+m)+1)+1 && \triangleright\ [2] \\ &= ((m+n)+1)+1 && \triangleright\ \mathbf{P}(n) \\ &= (m+(n+1))+1 && \triangleright\ [2] \\ &= ((n+1)+m)+1 && \triangleright\ m+(n+1) = (n+1)+m \\ &= (n+1)+(m+1). && \triangleright\ [2] \end{aligned}$$

Hence, by The Induction Principle, $\mathbf{P}(n+1)$ holds. $\square$

From Claim 1, Claim 2, and The Induction Principle, we get $\forall m,n \in \mathbb{N},\ m+n=n+m$. □

Theorem 3.4.5 + is Associative

Addition is associative; that is to say

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

Proof. Let $\mathbf{P}(x)$ be the property "$\forall k,m \in \mathbb{N},\ (k+m)+x = k+(m+x)$." $\mathbf{P}(0)$ is direct by [1].
Now, fix any $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$. Then, for all $k,m \in \mathbb{N}$,

$$\begin{aligned}(k+m)+(n+1) &= ((k+m)+n)+1 && \triangleright\ [2]\\ &= (k+(m+n))+1 && \triangleright\ \mathbf{P}(n)\\ &= k+((m+n)+1) && \triangleright\ [2]\\ &= k+(m+(n+1)). && \triangleright\ [2]\end{aligned}$$

Hence, by The Induction Principle, the result follows. □

Theorem 3.4.6

There uniquely exists a function $\cdot : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ such that
(i) $\forall m \in \mathbb{N},\ m\cdot 0 = 0$
(ii) $\forall m,n \in \mathbb{N},\ m\cdot(n+1) = m\cdot n + m$.

Proof. The result directly follows from exploiting The Recursion Theorem: Parametric Version 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 3.4.7: Multiplication

The function $\cdot$ defined in Theorem 3.4.6 is called the *multiplication*.

$$\forall m \in \mathbb{N},\ m\cdot 0 = 0 \qquad [3]$$

$$\forall m,n \in \mathbb{N},\ m\cdot(n+1) = m\cdot n + m \qquad [4]$$

Theorem 3.4.8 · is Commutative

Multiplication is commutative, i.e.,

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

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

Claim 1. $\mathbf{P}(0)$ holds.

Proof. Since $m\cdot 0 = 0$ already by [3], we only need to prove $0\cdot m = 0$ for all $m \in \mathbb{N}$. We shall make use of induction. First of all $0\cdot 0 = 0$ holds by [3].
Suppose $0\cdot m = 0$ where $m \in \mathbb{N}$. Then,

$$\begin{aligned}0\cdot(m+1) &= 0\cdot m + 0 && \triangleright\ [4]\\ &= 0+0 && \triangleright\ 0\cdot m = 0\\ &= 0.\end{aligned}$$

Hence, by The Induction Principle, $0\cdot m = 0$ for all $m \in \mathbb{N}$. □

Claim 2. $\forall n \in \mathbb{N}, [\mathbf{P}(n) \implies \mathbf{P}(n+1)]$

Proof. Fix any $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$. We shall prove $\mathbf{P}(n+1)$ by induction. We already have $0 \cdot (n+1) = (n+1) \cdot 0$ by Claim 1.

Fix any $m \in \mathbb{N}$ and assume $m \cdot (n+1) = (n+1) \cdot m$. Then,

$$\begin{aligned}
(m+1)\cdot(n+1) &= (m+1)\cdot n + (m+1) && \triangleright [4] \\
&= n\cdot(m+1) + (m+1) && \triangleright \mathbf{P}(n) \\
&= (n\cdot m + n) + (m+1) && \triangleright [4] \\
&= (m\cdot n + n) + (m+1) && \triangleright \mathbf{P}(n) \\
&= (m\cdot n + m) + (n+1) && \triangleright + \text{ is Commutative}, + \text{ is Associative} \\
&= m\cdot(n+1) + (n+1) && \triangleright [4] \\
&= (n+1)\cdot m + (n+1) && \triangleright m\cdot(n+1) = (n+1)\cdot m \\
&= (n+1)\cdot(m+1). && \triangleright [4]
\end{aligned}$$

Hence, by The Induction Principle, $\mathbf{P}(n+1)$ holds.

From Claim 1, Claim 2, and The Induction Principle, we get $\forall m, n \in \mathbb{N},\ m \cdot n = n \cdot m$. □

Theorem 3.4.9 · Distributes Over +

Multiplication is distributive over addition, i.e.,

$$\begin{aligned}
&\forall k, m, n \in \mathbb{N},\ k\cdot(m+n) = k\cdot m + k\cdot n \quad \text{and} \\
&\forall k, m, n \in \mathbb{N},\ (m+n)\cdot k = m\cdot k + n\cdot k.
\end{aligned}$$

Proof. Let $\mathbf{P}(x)$ be the property "$\forall k, m \in \mathbb{N},\ k\cdot(m+x) = k\cdot m + k\cdot x$." $\mathbf{P}(0)$ holds by [1] and [3].

Fix any $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$. Then, for each $k, m \in \mathbb{N}$,

$$\begin{aligned}
k\cdot(m+(n+1)) &= k\cdot((m+n)+1) && \triangleright + \text{ is Associative} \\
&= k\cdot(m+n) + k && \triangleright [4] \\
&= (k\cdot m + k\cdot n) + k && \triangleright \mathbf{P}(n) \\
&= k\cdot m + (k\cdot n + k) && \triangleright + \text{ is Associative} \\
&= k\cdot m + k\cdot(n+1). && \triangleright [4]
\end{aligned}$$

Hence, by The Induction Principle, we have $\forall k, m, n \in \mathbb{N},\ k\cdot(m+n) = k\cdot m + k\cdot n$.

Now, we have, for each $k, m, n \in \mathbb{N}$,

$$\begin{aligned}
(m+n)\cdot k &= k\cdot(m+n) && \triangleright \cdot \text{ is Commutative} \\
&= k\cdot m + k\cdot n \\
&= m\cdot k + n\cdot k. && \triangleright \cdot \text{ is Commutative}
\end{aligned}$$

□

Theorem 3.4.10 · is Associative

Multiplication is associative, i.e.,

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

Proof. Let $\mathbf{P}(x)$ be the property "$\forall k, m \in \mathbb{N}, (k \cdot m) \cdot x = k \cdot (m \cdot x)$." $\mathbf{P}(0)$ is direct from [3]. Fix any $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$. Then, for each $k, m \in \mathbb{N}$,

$$\begin{aligned}
(k \cdot m) \cdot (n+1) &= (k \cdot m) \cdot n + k \cdot m && \triangleright \text{ [4]} \\
&= k \cdot (m \cdot n) + k \cdot m && \triangleright \ \mathbf{P}(n) \\
&= k \cdot (m \cdot n + m) && \triangleright \ \cdot \text{ Distributes Over } + \\
&= k \cdot (m \cdot (n+1)). && \triangleright \text{ [4]}
\end{aligned}$$

Hence, the result follows by The Induction Principle. ☐

Lemma 3.4.11

$\forall m \in \mathbb{N},\ m \cdot 1 = m$

Proof.

$$\begin{aligned}
m \cdot 1 &= m \cdot (0+1) && \triangleright \text{ [1], } + \text{ is Commutative} \\
&= m \cdot 0 + m && \triangleright \text{ [4]} \\
&= 0 + m && \triangleright \text{ [3]} \\
&= m && \triangleright \text{ [1], } + \text{ is Commutative}
\end{aligned}$$

☐

Theorem 3.4.12

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

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

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

Proof. The result directly follows from exploiting The Recursion Theorem: Parametric Version 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 3.4.13: Exponentiation

The function $\uparrow$ defined in Theorem 3.4.12 is called the *exponentiation*. We write m^n instead of $m \uparrow n$.

$$\forall m \in \mathbb{N},\ m^0 = 1 \qquad [5]$$

$$\forall m, n \in \mathbb{N},\ m^{n+1} = m^n \cdot m \qquad [6]$$

Theorem 3.4.14 Laws of Exponents

(i) $\forall m \in \mathbb{N},\ m^1 = m$

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

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

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

Proof.

(i) Take any $m \in \mathbb{N}$. Then,

$$\begin{aligned}
m^1 &= m^{0+1} && \triangleright \text{ [1], } + \text{ is Commutative} \\
&= m^0 \cdot m && \triangleright \text{ [6]} \\
&= 1 \cdot m && \triangleright \text{ [5]} \\
&= m. && \triangleright \ \cdot \text{ is Commutative, Lemma 3.4.11}
\end{aligned}$$

(ii) Let $\mathbf{P}(x)$ be the property "$\forall k, m \in \mathbb{N}, k^{m+x} = k^m \cdot k^x$." $\mathbf{P}(0)$ holds since, for each $k, m \in \mathbb{N}$,

$$\begin{aligned} k^{m+0} &= k^m && \triangleright [1] \\ &= k^m \cdot 1 && \triangleright \text{Lemma 3.4.11} \\ &= k^m \cdot k^0. && \triangleright [5] \end{aligned}$$

Now, fix $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$. Then,

$$\begin{aligned} k^{m+(n+1)} &= k^{(m+n)+1} && \triangleright + \text{ is Associative} \\ &= k^{m+n} \cdot k && \triangleright [6] \\ &= (k^m \cdot k^n) \cdot k && \triangleright \mathbf{P}(x) \\ &= k^m \cdot (k^n \cdot k) && \triangleright \cdot \text{ is Associative} \\ &= k^m \cdot k^{n+1}. && \triangleright [6] \end{aligned}$$

Therefore, by The Induction Principle, the result follows.

(iii) Let $\mathbf{P}(x)$ be the property "$\forall m, n \in \mathbb{N}$, $(m \cdot n)^x = m^x \cdot n^x$." $\mathbf{P}(0)$ holds since, for each $m, n \in \mathbb{N}$,

$$\begin{aligned} (m \cdot n)^0 &= 1 && \triangleright [5] \\ &= 1 \cdot 1 && \triangleright \text{Lemma 3.4.11} \\ &= m^0 \cdot n^0. && \triangleright [5] \end{aligned}$$

Now, fix $k \in \mathbb{N}$ and assume $\mathbf{P}(k)$. Then,

$$\begin{aligned} (m \cdot n)^{k+1} &= (m \cdot n)^k \cdot (m \cdot n) && \triangleright [6] \\ &= (m^k \cdot n^k) \cdot (m \cdot n) && \triangleright \mathbf{P}(k) \\ &= (m^k \cdot m) \cdot (n^k \cdot n) && \triangleright \cdot \text{ is Commutative}, \cdot \text{ is Associative} \\ &= m^{k+1} \cdot n^{k+1}. && \triangleright [6] \end{aligned}$$

Therefore, by The Induction Principle, the result follows.

(iv) Let $\mathbf{P}(x)$ be the property "$\forall k, m \in \mathbb{N}, (k^m)^x = k^{m \cdot x}$." $\mathbf{P}(0)$ holds since, for each $k, m \in \mathbb{N}$,

$$\begin{aligned} (k^m)^0 &= 1 && \triangleright [5] \\ &= k^0 && \triangleright [5] \\ &= k^{m \cdot 0}. && \triangleright [3] \end{aligned}$$

Now, fix $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$. Then,

$$\begin{aligned} (k^m)^{n+1} &= (k^m)^n \cdot k^m && \triangleright [6] \\ &= k^{m \cdot n} \cdot k^m && \triangleright \mathbf{P}(n) \\ &= k^{m \cdot n + m} && \triangleright \text{Laws of Exponents (ii)} \\ &= k^{m \cdot (n+1)}. && \triangleright [4] \end{aligned}$$

Therefore, by The Induction Principle, the result follows. □

Theorem 3.4.15

There uniquely exists $\Sigma\colon \operatorname{Seq}(\mathbb{N}) \to \mathbb{N}$ such that

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

(ii) $\Sigma(k) = \Sigma\left(k|_n\right) + k_n$for all $k \in \mathrm{Seq}(\mathbb{N})$ with length $n+1$.

Proof. Let $g\colon \mathrm{Seq}(\mathbb{N}) \times \mathbb{N} \times \mathbb{N}$ be defined by

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

Then, by The Recursion Theorem: Parametric Version, there exists a function $f\colon \mathrm{Seq}(\mathbb{N}) \times \mathbb{N} \to \mathbb{N}$ such that

(i) $\forall k \in \mathrm{Seq}(\mathbb{N}), f(k,0) = 0$

(ii) $\forall n \in \mathbb{N},\ \forall k \in \mathrm{Seq}(\mathbb{N}), f(k,n+1) = g(k,f(k,n),n) = \begin{cases} f(k,n) + k_n & \text{if } n \in \operatorname{dom} k \\ f(k,n) & \text{otherwise.} \end{cases}$ [∗]

Now, define $\Sigma\colon \mathrm{Seq}(\mathbb{N}) \to \mathbb{N}$ by $\Sigma(k) = f(k, \operatorname{dom} k)$. (i) evidently holds.

Claim 1. Let $k, \ell \in \mathrm{Seq}(\mathbb{N})$. If $k \subseteq \ell$, then $f(k, \operatorname{dom} k) = f(\ell, \operatorname{dom} k)$.

Proof. Let $\mathbf{P}(x)$ be the property

$$\forall k, \ell \in \mathrm{Seq}(\mathbb{N}),\ [\operatorname{dom} k = x \wedge k \subseteq \ell \implies f(k,x) = f(\ell,x)].$$

$\mathbf{P}(0)$ is evident. Now, fix $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$.

Fix any $k \in \mathrm{Seq}(\mathbb{N})$ with $\operatorname{dom} k = n+1$. Then, for any $\ell \in \mathrm{Seq}(\mathbb{N})$ with $k \subseteq \ell$,

$$\begin{aligned} f(\ell, n+1) &= f(\ell,n) + \ell_n && \triangleright\ [*] \\ &= f\left(\ell|_n, n\right) + \ell_n && \triangleright\ \mathbf{P}(n) \\ &= f\left(k|_n, n\right) + k_n && \triangleright\ k \subseteq \ell \\ &= f(k,n) + k_n && \triangleright\ \mathbf{P}(n) \\ &= f(k, n+1). && \triangleright\ [*] \end{aligned}$$

Hence, by The Induction Principle, the result follows. □

Let $k \in \mathrm{Seq}(\mathbb{N})$ with length $n+1$. Then, $\Sigma(k) = f(k,n+1) = f(k,n) + k_n$.

$$\begin{aligned} \Sigma(k) &= f(k, n+1) \\ &= f(k,n) + k_n && \triangleright\ [*] \\ &= f\left(k|_n, n\right) + k_n && \triangleright\ \text{Claim 1} \\ &= \Sigma\left(k|_n\right) + k_n. \end{aligned}$$

The uniqueness easily follows. □

Notation 3.4.16: Summation

For the function Σ defined in Theorem 3.4.15, we write

$$\sum_{0 \le i < n} k_i \quad \text{or} \quad \sum_{i=0}^{n-1} k_i$$

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

Selected Problems

> **Exercise 3.4.2**
> $\forall k, m, n \in \mathbb{N}, (m < n \iff m + k < n + k)$

Proof. Let $\mathbf{P}(x)$ be the property "$\forall m, n \in \mathbb{N}, (m < n \iff m + x < n + x)$." $\mathbf{P}(0)$ is evident from [1].

Now, fix any $k \in \mathbb{N}$ and assume $\mathbf{P}(k)$. Then, for all $m, n \in \mathbb{N}$,

$$\begin{aligned} m < n &\iff m + k < n + k && \triangleright\ \mathbf{P}(k) \\ &\iff (m + k) + 1 < (n + k) + 1 && \triangleright\ \text{Exercise 3.2.2} \\ &\iff m + (k + 1) < n + (k + 1). && \triangleright\ + \text{ is Associative} \end{aligned}$$

By The Induction Principle, the result follows. □

> **Exercise 3.4.3**
> $\forall m, n \in \mathbb{N}, (m \leq n \iff \exists! k \in \mathbb{N}, n = m + k)$

Proof. $(\Rightarrow)$ Fix any $m \in \mathbb{N}$ and let $\mathbf{P}(x)$ be the property "$\exists k \in \mathbb{N}, x = m + k$." $\mathbf{P}(m)$ holds since $k = 0$ would satisfy by [1].

Fix any $n \in \mathbb{N}$ such that $m \leq n$ and assume $\mathbf{P}(n)$. Then, there exists k such that $n = m + k$, which leads to $n + 1 = m + (k + 1)$ by + is Associative. Hence, $\mathbf{P}(n + 1)$ holds. Therefore, $\forall n \geq m, \exists k \in \mathbb{N}, n = m + k$ by Exercise 3.2.11.

To prove the uniqueness, assume $m + k = m + \ell$ where $k, \ell, m \in \mathbb{N}$. WLOG, $k \leq \ell$. If it were $k < \ell$, by Exercise 3.4.2 and + is Commutative, we must have $m + k = k + m < \ell + m = \ell + m$. Hence, $k = \ell$.

$(\Leftarrow)$ Let $\mathbf{P}(x)$ be the property "$\forall m, n \in \mathbb{N}, (n = m + x \implies m \leq n)$." We have evidently $\mathbf{P}(0)$ by [1].

Fix any $k \in \mathbb{N}$ and assume $\mathbf{P}(k)$. Then, for each $m, n \in \mathbb{N}$ such that $n = m + (k + 1)$, we have $n = (m + 1) + k$ thanks to + is Commutative and + is Associative, and thus $m < m + 1 \leq n$ by $\mathbf{P}(k)$. Hence, by The Induction Principle, the result follows. □

> **Exercise 3.4.6**
> $\forall k, m, n \in \mathbb{N}, [k \neq 0 \implies (m < n \iff m \cdot k < n \cdot k)]$

Proof. Let $\mathbf{P}(x)$ be the property "$\forall m, n \in \mathbb{N}, (m < n \iff m \cdot k < n \cdot k)$." $\mathbf{P}(1)$ holds since, for all $n \in \mathbb{N}$,

$$\begin{aligned} n \cdot 1 &= n \cdot (0 + 1) && \triangleright\ [1], + \text{ is Commutative} \\ &= n \cdot 0 + n && \triangleright\ [4] \\ &= 0 + n && \triangleright\ [3] \\ &= n. && \triangleright\ [1], + \text{ is Commutative} \end{aligned}$$

Now, fix any $k \in \mathbb{N}$ and assume $\mathbf{P}(k)$. Then, for each $m, n \in \mathbb{N}$ with $m < n$,

$$\begin{aligned} m \cdot (k + 1) &= m \cdot k + m && \triangleright\ [4] \\ &< m \cdot k + n && \triangleright\ \text{Exercise 3.4.2} \\ &< n \cdot k + n && \triangleright\ \mathbf{P}(k), + \text{ is Commutative, Exercise 3.4.2} \\ &= n \cdot (k + 1). && \triangleright\ [4] \end{aligned}$$

Therefore, by Exercise 3.2.11, the result follows. □

3.5 Operations and Structures

Definition 3.5.1: Operation

- A *unary operation* on S is a function $S \rightharpoonup S$.
- A *binary operation* on S is a function $S^2 \rightharpoonup S$.

Notation 3.5.2: Binary Operation

Non-letter symbols such as $+$, $\times$, $*$, $\triangle$, etc., are often used to denote operations. The value of the operation $*$ at (x, y) is then denoted $x * y$ rather than $*(x, y)$.

Definition 3.5.3: Closedness Under Operation

Let f be a binary operation on S and $A \subseteq S$. A is said to be *closed under the operation* f if $\forall x, y \in A$, $[(x, y) \in \operatorname{dom} f \implies f(x, y) \in A]$.

Definition 3.5.4: n-Tuple

Let $n \in \mathbb{N}$. An n-tuple is a finite sequence of length n.

Note:-

Let $\langle a_0, \cdots, a_{n-1} \rangle$ and $\langle b_0, \cdots, b_{n-1} \rangle$ be two n-tuples. We have, by Lemma 2.3.3,

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

This satisfies the usual defining property of n-tuple.

Note:-

- If $\langle A_i \mid 0 \leq i < n \rangle$ is a finite sequence (of sets), then the product of the indexed system of sets $\prod_{0 \leq i < n} A_i$ (Definition 2.3.16) is just the set of all n-tuples $a = \langle a_0, \cdots, a_{n-1} \rangle$ such that $\forall i < n,\ a_i \in A_i$.
- If $\forall i < n, A_i = A$, then $\prod_{0 \leq i < n} A_i = A^n$.
- $A^0 = \{\langle\rangle\}$.

Notation 3.5.5

The 'ordered pair' (Definition 2.1.1), $(a_0, a_1) = \{\{a_0\}, \{a_0, a_1\}\}$, is different set from the '2-tuple' (Definition 3.5.4), $\langle a_0, a_1 \rangle = \{(0, a_0), (1, a_1)\}$. Consequently, $A_0 \times A_1$ (Definition 2.2.10) does not generally equal to $\prod_{0 \le i < 2} A_i$ (Definition 2.3.16).

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

$$\begin{aligned} \delta : A_0 \times A_1 &\hookrightarrow\!\!\!\!\rightarrow \prod\nolimits_{0 \le i < 2} A_i \\ (a_0, a_1) &\longmapsto \langle a_0, a_1 \rangle, \end{aligned}$$

for almost all practical purposes—when only the defining property of n-tuple is needed)—it makes so difference which definition one uses.

Therefore, we do not distinguish between ordered pairs and 2-tuples now on. That is to say we use notations

$$\langle a_0, \cdots, a_{n-1} \rangle \quad \text{and} \quad (a_0, \cdots, a_{n-1})$$

interchangeably from now on.

Definition 3.5.6: n-ary Relation

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

Definition 3.5.7: n-ary Operation

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

Note:-

- 1-ary relations in A need not be distinguished from subsets of A.
- 1-ary operations on A need not be distinguished from functions $A \rightharpoonup A$.
- Nonempty 0-ary operations on A need not be distinguished from A. (A nonempty 0-ary operation is of the form $\{(\langle\rangle, a)\}$ where $a \in A$; a nonempty 0-ary operation is called a *constant*.)

Definition 3.5.8: Structure

- A *type* τ is an ordered pair $(\langle r_0, \cdots, r_{m-1} \rangle, \langle f_0, \cdots, f_{n-1} \rangle)$ of finite sequences of natural numbers.
- A *structure of type* τ is a triple

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

where R_i is an r_i-ary relation on A for each $i < m$ and F_j is an f_j-ary operation on A for each $j < n$. In addition, we require $F_j \neq \varnothing$ if $f_j = 0$, i.e., F_j should be constant. A is called the *universe* of the structure $\mathfrak{A}$.

Example 3.5.9

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

Notation 3.5.10

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

Definition 3.5.11: Isomorphism Between Structures

Let $\mathfrak{A}$ and $\mathfrak{A}'$ be structures of the same type $\tau=(\langle r_0,\cdots,r_{m-1}\rangle,\langle f_0,\cdots,f_{n-1}\rangle)$. Write $\mathfrak{A}=(A,\langle R_0,\cdots,R_{m-1}\rangle,\langle F_0,\cdots,F_{n-1}\rangle)$ and $\mathfrak{A}'=(A',\langle R'_0,\cdots,R'_{m-1}\rangle,\langle F'_0,\cdots,F'_{n-1}\rangle)$. An *isomorphism* between structures $\mathfrak{A}$ and $\mathfrak{A}'$ is a mapping $h\colon A\hookrightarrow\!\!\!\rightarrow A'$ such that

(i) $\forall i<m,\ \forall a\in A^{r_i},\ [R_i(a_0,\cdots,a_{r_i-1})\iff R'_i(h(a_0),\cdots,h(a_{r_i}-1))]$

(ii) $\forall j<n,\ \forall a\in A^{f_j},\big[(a_0,\cdots,a_{f_j-1})\in\operatorname{dom}F_j\iff(h(a_0),\cdots,h(a_{f_j-1}))\in\operatorname{dom}F'_j\big]$

(iii) $\forall j<n,\ \forall a\in A^{f_j},\big[(a_0,\cdots,a_{f_j-1})\in\operatorname{dom}F_j$
$$\implies h(F_j(a_0,\cdots,a_{f_j-1}))=F'_j(h(a_0),\cdots,h(a_{f_j-1}))\big].$$

If $\mathfrak{A}$ and $\mathfrak{A}'$ are isomorphic, then we write $\mathfrak{A}\cong\mathfrak{A}'$.

Definition 3.5.12: Automorphism

An isomorphism between a structure $\mathfrak{A}$ and itself is called an *automorphism*.

Definition 3.5.13: Closed Set

Fix a structure $\mathfrak{A}=(A,\langle R_0,\cdots,R_{m-1}\rangle,\langle F_0,\cdots,F_{n-1}\rangle)$. A set $B\subseteq A$ is called *closed* if

$$\forall j<n,\ \forall a\in B^{f_j},\ [(a_0,\cdots,a_{f_j-1})\in\operatorname{dom}F_j\implies F_j(a_0,\cdots,a_{f_j-1})\in B].$$

Definition 3.5.14: Closure

Fix a structure $\mathfrak{A}=(A,\langle R_0,\cdots,R_{m-1}\rangle,\langle F_0,\cdots,F_{n-1}\rangle)$. Let $C\subseteq A$. The *closure* of C,

$$\overline{C}\triangleq\bigcap\{B\subseteq A\mid C\subseteq B\text{ and }B\text{ is closed}\},$$

is the least closed set containing all elements of C.

Theorem 3.5.15

Let $\mathfrak{A}=(A,\langle R_0,\cdots,R_{m-1}\rangle,\langle F_0,\cdots,F_{n-1}\rangle)$ be a structure and let $C\subseteq A$. If the sequence $\langle C_i\mid i\in\mathbb{N}\rangle$ is defined recursively by

$$C_0=C;$$
$$\forall i\in\mathbb{N},\ C_{i+1}=C_i\cup\bigcup_{j=0}^{n-1}F_j[C_i^{f_j}],$$

then $\overline{C}=\bigcup_{i=0}^{\infty}C_i$.

Proof. Note the recursive definition is justified by The Recursion Theorem. Let $\tilde{C}\triangleq\bigcup_{i=0}^{\infty}C_i$.

Claim 1. $\overline{C} \subseteq \tilde{C}$

Proof. Since we have $C_0 \subseteq \tilde{C}$, it is enough to show that $\tilde{C}$ is closed.

Take any $j < n$ and $a \in \tilde{C}^{f_j}$. By the definition of $\tilde{C}$, $\forall r < f_j$, $\exists i_r \in \mathbb{N}$, $a_r \in C_{i_r}$. We may take $\bar{\imath} = \max\{i_r \mid r < f_j\}$ by Exercise 3.5.13. Since $C_i \subseteq C_{i+1}$ for all $i \in \mathbb{N}$, we have $a_r \in C_{i_r} \subseteq C_{\bar{\imath}}$ for all $r < f_j$. Hence, if $(a_0, \cdots, a_{f_j-1}) \in \operatorname{dom} F_j$, we have $F_j(a_0, \cdots, a_{f_j-1}) \in F_j[C_{\bar{\imath}}^{f_j}] \subseteq C_{\bar{\imath}+1} \subseteq \tilde{C}$. Hence, $\tilde{C}$ is closed. □

Claim 2. $\tilde{C} \subseteq \overline{C}$

Proof. Clearly $C_0 = C \subseteq \overline{C}$. If $C_i \subseteq \overline{C}$, then, for each $j < n$, $F_j[C_i^{f_j}] \subseteq \overline{C}$ since $\overline{C}$ is closed. Hence, $C_{i+1} \subseteq \overline{C}$. Therefore, by The Induction Principle, $\forall i \in \mathbb{N}$, $C_i \subseteq \overline{C}$; hence $\tilde{C} \subseteq \overline{C}$. □

Combining Claims 1 and 2 completes the proof. □

Theorem 3.5.16 The General Induction Principle

Let $\mathfrak{A} = (A, \langle R_0, \cdots, R_{m-1} \rangle, \langle F_0, \cdots, F_{n-1} \rangle)$ be a structure and let $C \subseteq A$. Let $\mathbf{P}(x)$ be a property. If

(i) $\forall a \in C$, $\mathbf{P}(a)$

(ii) $\forall j < n, \forall a \in A^{f_j}, \left[(a_0, \cdots, a_{f_j-1}) \in \operatorname{dom} F_j \wedge \forall i < f_j, \mathbf{P}(a_i) \implies \mathbf{P}(F_j(a_0, \cdots, a_{f_j-1}))\right]$

hold, then $\forall x \in \overline{C}$, $\mathbf{P}(x)$.

Proof. Let $B = \{x \in A \mid \mathbf{P}(x)\}$. (i) says $C \subseteq B$ and (ii) says B is closed. Therefore, $\overline{C} \subseteq B$. □

Note:-

The Induction Principle is a special case of The General Induction Principle for the structure $(\mathbb{N}, S)$ where S is the successor function.

Selected Problems

Exercise 3.5.4

Let $B = \mathcal{P}(A)$. Show that $(B, \cup_B, \cap_B)$ and $(B, \cap_B, \cup_B)$ are isomorphic structures.

Proof. Let $h \colon B \to B$ be defined by $h(X) = A \setminus X$. If $A \setminus X = A \setminus Y$, then $X = A \setminus (A \setminus X) = A \setminus (A \setminus Y) = Y$ by **??**. Moreover, $h(h(X)) = X$ for all $X \in B$. Hence, $h \colon B \hookrightarrow\!\!\!\!\rightarrow B$. □

Exercise 3.5.7

Let R be a set whose elements are n-tuples. Then, R is an n-ary relation in A for some A.

Proof. Let $a \in R$. Then, $a = \{(0, a_0), \cdots, (n-1, a_{n-1})\}$. For each $i < n$, $a_i \in \{i, a_i\} \in (i, a_i) \in a \in R$. Hence, $a_i \in \bigcup[\bigcup(\bigcup R)]$, i.e., R is an n-ary relation in $A = \bigcup[\bigcup(\bigcup R)]$. □

Exercise 3.5.10

Let A be a sequence of length n. Then, $\prod_{0 \le i < n} A_i \neq \varnothing \iff \forall i < n, A_i \neq \varnothing$

Proof. Let $\mathbf{P}(x)$ be the property "if A is a sequence of length x, then $\prod_{0\le i<n} A_i \neq \varnothing \iff \forall i<n,\ A_i \neq \varnothing$." $\mathbf{P}(0)$ holds since, if A is a function with $\operatorname{dom} A = \varnothing$, then $\prod A = \{\varnothing\}$.

Fix $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$ holds. Take any sequence A of length $n+1$.

- Assume $\prod A \neq \varnothing$ and take $a \in \prod A$. Then, for each $i < n+1$, $a_i \in A_i$; and thus $A_i \neq \varnothing$.
- Assume $\forall i < n+1$, $A_i \neq \varnothing$. Then, by $\mathbf{P}(n)$, we may take $a' \in \prod_{0\le i<n} A_i$. We also may take $b \in A_n$. Then, $a' \cup \{(n,b)\} \in \prod A$.

Hence, $\mathbf{P}(n)$ holds. Thus, the result follows by The Induction Principle. □

Exercise 3.5.13

Let $\langle k_0,\cdots,k_{n-1}\rangle$ be a finite sequence of natural numbers of length $n \geq 1$. Then, its range $\{k_0,\cdots,k_{n-1}\}$ has a greatest element.

Proof. Let $\mathbf{P}(x)$ be the property "the range of a finite sequence of natural numbers of length x has a greatest element."

Let $\langle k_0\rangle$ be a sequence of natural numbers of length 1. Then, $k_0 = \max \operatorname{ran}\langle k_0\rangle$. Hence, $\mathbf{P}(1)$.

Fix any $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$. Take any $k \in \operatorname{Seq}(\mathbb{N})$ with length $n+1$. Let $k' = \langle k_0,\cdots,k_{n-1}\rangle$ be another sequence. Then, by $\mathbf{P}(n)$, there exists $m' = \max\{k_0,\cdots,k_{n-1}\}$. Now, let $m = \max\{m', k_n\}$. Then, for all $i<n$, $k_i \le m' \le m$, and $k_n \le m$. Hence, m is an upper bound of $\operatorname{ran} k$; the result follows by Theorem 3.2.8 and Exercise 3.2.11. □

Exercise 3.5.15

Let $R \subseteq A^2$ be a binary relation. Define a binary operation F_R on A^2 by

$$F_R((a_1,a_2),(b_1,b_2)) = \begin{cases} (a_1,b_2) & \text{if } a_2 = b_1 \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Then,

(i) The closure of R in (A^2, F_R) is a transitive relation.

(ii) If R is reflexive and symmetric, $\overline{R}$ is also an equivalence.

Proof.

(i) Take any $a,b,c \in A$ and assume $a\overline{R}b$ and $b\overline{R}c$. Then, since $\overline{R}$ is closed, $F((a,b),(b,c)) = (a,c) \in \overline{R}$. Hence, $\overline{R}$ is transitive.

(ii) $\mathrm{Id}_A \subseteq R \subseteq \overline{R}$; $\overline{R}$ is reflexive.

Let $\mathbf{P}(x,y)$ be the property "$y\overline{R}x$." As $R \subseteq \overline{R}$, we have $\forall (a,b) \in R$, $\mathbf{P}(a,b)$. Now, take any $(a,b),(b,c) \in A^2$ such that $\mathbf{P}(a,b)$ and $\mathbf{P}(b,c)$. Then, by (i), we have $c\overline{R}a$; $\mathbf{P}(F_R((a,b),(b,c)))$ hold. Therefore, by The General Induction Principle, $b\overline{R}a$ holds for all $(a,b) \in \overline{R}$. □

Chapter 4

Finite, Countable, and Uncountable Sets

4.1 Cardinality of Sets

Definition 4.1.1: Equipotent Sets

Let A and B be sets. A is *equipotent to* B if there is a function $f : A \hookrightarrow\!\!\!\rightarrow B$. We write $|A| = |B|$.

Lemma 4.1.2

Let A, B, and C be sets.

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

Proof.

(i) Id_A is an injective function on A onto A.
(ii) If $f : A \hookrightarrow\!\!\!\rightarrow B$, then $f^{-1} : B \hookrightarrow\!\!\!\rightarrow A$.
(iii) If $f : A \hookrightarrow\!\!\!\rightarrow B$, and if $g : B \hookrightarrow\!\!\!\rightarrow C$, then $f \circ g : A \hookrightarrow\!\!\!\rightarrow C$. $\square$

Note:-
Lemma 4.1.2 essentially says that $|A| = |B|$ behaves like an equivalence relation.

Definition 4.1.3

- We say *the cardinality of A is less than or equal to the cardinality of B* if there is a function $f : A \hookrightarrow B$. We write $|A| \le |B|$.
- We say *the cardinality of A is less than the cardinality of B* if $|A| \le |B|$ and $\neg(|A| = |B|)$. We write $|A| < |B|$.

Lemma 4.1.4

Let A, B, and C be sets.

(i) If $|A| = |B|$, then $|A| \le |B|$.
(ii) $|A| \le |A|$
(iii) If $|A| \le |B|$ and $|B| \le |C|$, then $|A| \le |C|$.

Proof.

(i) If $f : A \hookrightarrow\!\!\!\rightarrow B$, then f is injective as well.

(ii) Id_A is an injective function on A into A.

(iii) If $f : A \hookrightarrow B$, and if $g : B \hookrightarrow C$, then $f \circ g : A \hookrightarrow C$. □

Lemma 4.1.5

If $A_1 \subseteq B \subseteq A$ and $|A_1| = |A|$, then $|B| = |A|$.

Note:-

We present two proofs for Lemma 4.1.5. The second proof can be viewed as a more fundamental proof in the sense that it does not depend on Axiom of Infinity.

Proof 1. Let $f : A \hookrightarrow\!\!\!\!\to A_1$. Define a sequence $\langle A_i \mid i \in \mathbb{N} \rangle$ and $\langle B_i \mid i \in \mathbb{N} \rangle$ recursively by

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

thanks to The Recursion Theorem.

We clearly have $A_1 \subseteq B_0 \subseteq A_0$. If $A_{n+1} \subseteq B_n \subseteq A_n$, then $A_{n+2} = f[A_{n+1}] \subseteq B_{n+1} = f[B_n] \subseteq A_{n+1} = f[A_n]$ by [$*$]. Hence, by [$*$] and The Induction Principle, we have $A_{n+1} \subseteq B_n \subseteq A_n$ for all $n \in \mathbb{N}$.

Let, for each $n \in \mathbb{N}$, $C_n \triangleq A_n \setminus B_n$. Then, by Exercise 2.3.6 (ii), $C_{n+1} = f[A_n] \setminus f[B_n] = f[A_n \setminus B_n] = f[C_n]$. Let

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

Hence, $f[C] = \bigcup_{n=1}^{\infty} C_n \subseteq C$. Now, define a function $g : A \to A$ by

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

We immediately notice that $g\big|_C = f\big|_C$ and $g\big|_D$ are injective and their ranges—$f[C]$ and D—are disjoint; g is injective.

As, $\forall n \geq 1$, $C_n \subseteq A_n \subseteq B_0 = B$, we have $f[C] \subseteq B$. If $x \in D$, then $x \in A \setminus C_0 = A \setminus (A \setminus B) = B$ by **??**.

Now, we shall show $B \subseteq f[C] \cup D$ and thus $B = \operatorname{ran} g$. Take any $y \in B$. Then, $y \in C$ or $y \in D$. If $y \in D$, then it is done; so assume $y \in C$. Then, as $y \notin A \setminus B = C_0$, $y \in f[C]$. Hence, $g : A \hookrightarrow\!\!\!\!\to B$. □

Proof 2. Let $f : A \hookrightarrow\!\!\!\!\to A_1$. Let $F : \mathcal{P}(A) \to \mathcal{P}(A)$ be defined by $F(X) = (A \setminus B) \cup f[X]$. If $X \subseteq Y \subseteq A$, then $F(X) = (A \setminus B) \cup f[X] \subseteq (A \setminus B) \cup f[Y] = F(Y)$. Hence, by Exercise 4.1.10, there exists $C \subseteq A$ such that

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

Let $D \triangleq A \setminus C$.

Now, define a function $g : A \to A$ by

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

Then, since $f[C] \subseteq C$, g is injective.

Moreover, $f[C] \subseteq \operatorname{ran} f = A_1 \subseteq B$ and $D = A \setminus C = A \setminus ((A \setminus B) \cup f[C]) \subseteq A \setminus (A \setminus B) = B$, and thus $\operatorname{ran} g \subseteq B$.

Now, take any $y \in B$. If $y \in C$, then, as $y \notin A \setminus B$, $y \in f[C]$. Hence, $B \subseteq f[C] \cup D$. Therefore, $g : A \hookrightarrow\!\!\!\!\to B$. □

Theorem 4.1.6 Cantor–Bernstein Theorem

If $|X| \le |Y|$ and $|Y| \le |X|$, then $|X| = |Y|$.

Proof. Let $f : X \hookrightarrow Y$ and $g : Y \hookrightarrow X$. Then, $g : Y \hookrightarrow\!\!\!\!\rightarrow g[Y]$, i.e., $|Y| = |g[Y]|$; and $g \circ f : X \hookrightarrow\!\!\!\!\rightarrow (g \circ f)[X]$, i.e., $|X| = |(g \circ f)[X]|$. Moreover, $(g \circ f)[X] \subseteq g[Y] \subseteq X$. Hence, by Lemma 4.1.5, $|g[Y]| = |X|$. We conclude $|X| = |Y|$ from Lemma 4.1.2. $\square$

Assumption 4.1.7

There are 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) and sets X and Y are equipotent if and only if $|X|$ is equal to Y.

Note:-

Assumption 4.1.7 essentially asserts the existence of a unique "representative" for each class of mutually equipotent sets. Assumption 4.1.7 is *harmless* in the sense that we only use it for convenience and we could formulate the theorems without it. We prove Assumption 4.1.7 in Chapter 8: Axiom of Choice. However, for certain classes of sets, cardinal numbers can be defined without the Axiom of Choice.

Selected Problems

Exercise 4.1.2

Let A, B, and C be sets.

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

Proof.

(i) We already have $|A| \le |C|$ by Lemma 4.1.4 (iii). 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., $|B| \le |A|$. By Cantor–Bernstein Theorem, we get $|A| = |B|$, which is a contradiction.
(ii) We already have $|A| \le |C|$ by Lemma 4.1.4 (iii). 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., $|C| \le |B|$. By Cantor–Bernstein Theorem, we get $|B| = |C|$, which is a contradiction.

$\square$

Exercise 4.1.3

If $A \subseteq B$, then $|A| \le |B|$.

Proof. Id_A is an injective function on A into B. $\square$

Exercise 4.1.7

If $S \subseteq T$, then $|A^S| \le |A^T|$. In particular, $|A^m| \le |A^n|$ if $m \le n$.

Proof. If $T = \varnothing$, then $A^S = A^T = \{\varnothing\}$ and it is done.

Assume $T \neq \varnothing$. Fix some $t \in T$. Now, define $f : A^S \hookrightarrow A^T$ by $g \mapsto g \cup \{(x,t) \mid x \in T \setminus S\}$. $\square$

Exercise 4.1.10

Let $F : \mathcal{P}(A) \to \mathcal{P}(A)$ 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 to say $F(\overline{X}) = \overline{X}$ and $\forall X \subseteq A$, $(F(X) = X \implies \overline{X} \subseteq X)$.

Proof. Let $T \triangleq \{X \subseteq A \mid F(X) \subseteq X\}$. Then, as $A \in T$, $T \neq \varnothing$; we may let $\overline{X} \triangleq \bigcap T$.

Then, for all $X \in T$, $\overline{X} \subseteq X$; and thus $F(\overline{X}) \subseteq F(X) \subseteq X$. We have $F(\overline{X}) \subseteq \bigcap T = \overline{X}$, i.e., $\overline{X} \in T$.

On the other hand, we have $F(F(\overline{X})) \subseteq F(\overline{X})$, or $F(\overline{X}) \in T$, and thus $\overline{X} = \bigcap T \subseteq F(\overline{X})$. Therefore, $F(\overline{X}) = \overline{X}$. Moreover, if X is a fixed point, then $X \in T$, and thus $\overline{X} = \bigcap T \subseteq X$. □

Exercise 4.1.14

A function $F : \mathcal{P}(A) \to \mathcal{P}(A)$ is *continuous* if, for each sequence $\langle X_i \mid i \in \mathbb{N} \rangle$ of subsets of A such that $\forall i, j \in \mathbb{N}$, $(i \leq j \implies X_i \subseteq X_j)$, $F\left(\bigcup_{i \in \mathbb{N}} X_i\right) = \bigcup_{i \in \mathbb{N}} F(X_i)$ holds.

If $\overline{X}$ is the least fixed point of a monotone continuous function, $F : \mathcal{P}(A) \to \mathcal{P}(A)$, then $\overline{X} = \bigcup_{i \in \mathbb{N}} X_i$ where we define recursively $X_0 = \varnothing$, $\forall i \in \mathbb{N}$, $X_{i+1} = F(X_i)$.

Proof. Let $\tilde{X} \triangleq \bigcup_{i \in \mathbb{N}} X_i$. We have $X_0 = \varnothing \subseteq X_1$.

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 Exercise 3.3.1, we have $X_m \subseteq X_n$ whenever $m \leq n$. Hence, $F(\tilde{X}) = \bigcup_{i \in \mathbb{N}} F(X_i) = \bigcup_{i=1}^{\infty} X_i = \tilde{X}$; $\tilde{X}$ is a fixed point of F; hence $\overline{X} \subseteq \tilde{X}$.

We have $X_0 \subseteq \overline{X}$. If $X_n \subseteq \overline{X}$ for $n \in \mathbb{N}$, then $X_{n+1} \subseteq F(\overline{X})) = \overline{X}$. Hence, by The Induction Principle, $\tilde{X} \subseteq \overline{X}$. □

4.2 Finite Sets

Definition 4.2.1: Finite Set and Infinite Set

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.

Note:-

According to Definition 4.2.1, cardinal numbers of finite sets are the natural numbers. We evidently have $\forall n \in \mathbb{N}$, $|n| = n$.

Lemma 4.2.2

If $n \in \mathbb{N}$ and $X \subsetneq n$, then there is no $f : n \hookrightarrow\!\!\!\!\rightarrow X$.

Proof. If $n = 0$, there is no $X \subsetneq n$; the assertion is true.

Assume the assertion holds for n. Suppose there is some $f : (n+1) \hookrightarrow\!\!\!\!\rightarrow X$ where $X \subsetneq n+1$. There are two cases: $n \in X$ and $n \notin X$.

If $n \notin X$, then $X \subseteq n$, and thus $f\big|_n : n \hookrightarrow\!\!\!\!\rightarrow X \setminus \{f(n)\}$; however $X \setminus \{f(n)\} \subsetneq X \subseteq n$, which is a contradiction.

If $n \in X$, then $n = f(k)$ for some $k \leq n$. Define a function g on n by following:

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

Then, $g : n \hookrightarrow\!\!\!\!\rightarrow X \setminus \{n\}$ and $X \setminus \{n\} \subsetneq n$, which is also a contradiction. □

Corollary 4.2.3

(i) If $m \neq n$ where $m, n \in \mathbb{N}$, then there is no $f : m \hookrightarrow\!\!\!\!\rightarrow n$.
(ii) If $|S| = m$ and $|S| = n$, then $m = n$.
(iii) $\mathbb{N}$ is infinite.

Proof.
(i) If $n \neq m$, by $(\mathbb{N}, \leq)$ is Totally Ordered, we have $n \subsetneq m$ or $m \subsetneq n$. In either case, we do not have such function by Lemma 4.2.2.
(ii) By Lemma 4.1.2, we have $|m| = |n|$. (i) asserts that $m = n$; otherwise we cannot have $|m| = |n|$.
(iii) By Exercise 3.2.3, there exists $f : \mathbb{N} \hookrightarrow\!\!\!\!\rightarrow X$ where $X \subsetneq \mathbb{N}$. If there exists $n \in \mathbb{N}$ and $g : n \hookrightarrow\!\!\!\!\rightarrow \mathbb{N}$, $g^{-1} \circ f^{-1} \circ f \circ g$ is a function on n onto a proper subset of n. This contradicts Lemma 4.2.2. □

Theorem 4.2.4

If X is a finite set and $Y \subseteq X$, then Y is finite.

Proof. We may assume $X = \{x_0, \cdots, x_{n-1}\}$, where $\langle x_0, \cdots, x_{n-1} \rangle$ is an injective sequence, and $Y \neq \varnothing$.

Let $g : n \times \mathbb{N} \rightharpoonup n$ be defined by

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

By The Recursion Theorem: Partial Version, there exists a sequence k of elements in n such that

(i) $k_0 = \min\{ j \in n \mid x_j \in Y \}$. $\qquad \triangleright\, Y \neq \varnothing$
(ii) $\forall i \in \mathbb{N}$, $[i + 1 \in \operatorname{dom} k \implies k_{i+1} = g(k_i, i) = \min\{ j \in n \mid k_i < j \wedge x_j \in Y \}]$.
(iii) k is either an infinite sequence or a finite sequence of length $\ell + 1$ and $(k_\ell, \ell) \notin \operatorname{dom} g$.

By (ii) and [$*$], $\forall i \in \mathbb{N}$, $(i + 1 \in \operatorname{dom} k \implies k_i < k_{i+1})$. Hence, k is injective. If k were an infinite sequence, i.e., $k : \mathbb{N} \hookrightarrow n$, then $|\mathbb{N}| \leq |n|$. Together with Exercise 4.1.3 and Cantor–Bernstein Theorem, we get $|\mathbb{N}| = |n|$, which contradicts Corollary 4.2.3 (iii). Hence, k is a finite sequence of length ℓ.

Let $y_i \triangleq x_{k_i}$ for each $i < \ell$. By (i) and (ii), the sequence y is injective and its range is a subset of Y. By the same argument of Claim 1 of Theorem 3.3.3, we have $\operatorname{ran} y = Y$. Therefore, $y : \ell \hookrightarrow\!\!\!\!\rightarrow Y$; Y is finite. □

Theorem 4.2.5

If X is finite and f is a function, then $f[X]$ is finite. Moreover, $|f[X]| \leq |X|$.

Proof. If $f[X] = \varnothing$, then it is done; assume $f[X] \neq \varnothing$. WLOG, $X \subseteq \operatorname{dom} f$.

We may assume $X = \{x_0, \cdots, x_{n-1}\}$, where $\langle x_0, \cdots, x_{n-1} \rangle$ is an injective sequence. Let $g :$ Seq$(n) \rightharpoonup n$ be defined by

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

Then, one may modify The Recursion Theorem: General Version to its partial version like The Recursion Theorem: Partial Version to get a sequence k of elements of n such that:

(i) $\forall i \in \operatorname{dom} k$, $k_i = g\left(k\big|_i\right)$. In particular, $k_0 = 0$.

(ii) k is either an infinite sequence or a finite sequence of length $\ell + 1$ and $k \notin \operatorname{dom} g$.

By (i) and [$*$], $\forall i, j \in \operatorname{dom} k$, $(i \neq j \implies f(x_{k_i}) \neq f(x_{k_j}))$, i.e., the sequence $y = \langle f(x_{k_i}) \mid i \in \operatorname{dom} k \rangle$ is injective and its range is a subset of $f[X]$.

By the similar reason as in the proof of Theorem 4.2.4, k is finite and $\operatorname{ran} y = f[X]$. Finally, we get $|f[X]| \le |X|$ from $x \circ y^{-1} : f[X] \hookrightarrow X$. $\square$

Lemma 4.2.6

Let X and Y be finite sets.

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

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

Proof.

(i) Write $X = \{x_0, \cdots, x_{m-1}\}$ and $Y = \{y_0, \cdots, y_{n-1}\}$ where $\langle x_0, \cdots, x_{m-1} \rangle$ and $\langle y_0, \cdots, y_{n-1} \rangle$ are injective sequences.

Now, define $z : (n+m) \twoheadrightarrow X \cup Y$ by

$$z_i = x_i \quad \text{for } 0 \le i < n \quad \text{and} \quad z_i = y_{i-n} \quad \text{for } n \le i < n+m.$$

(Here, $i - n$ is the unique $k \in \mathbb{N}$ such that $i = n + k$. See Exercise 3.4.3.) Hence, by Theorem 4.2.5, $X \cup Y$ is finite and $|X \cup Y| \le n + m$.

(ii) If X and Y are disjoint, then $z : (n+m) \hookrightarrow\!\!\!\!\rightarrow X \cup Y$. Hence, $|X \cup Y| = n + m$. $\square$

Theorem 4.2.7

If S is finite and if every $X \in S$ is finite, then $\bigcup S$ is finite.

Proof. If $|S| = 0$, then it is done.

Assume that the statement is true for all S with $|S| = n$. Let $S = \{X_0, \cdots, X_n\}$ be a set with $n+1$ elements such that each $X_i \in S$ is finite. Then, we have

$$\bigcup S = \left(\bigcup_{i=0}^{n-1} X_i\right) \cup X_n$$

but $\bigcup_{i=0}^{n-1} X_i$ is finite by induction hypothesis and thus $\bigcup S$ is finite by Lemma 4.2.6. Hence, by The Induction Principle, the result follows. $\square$

Theorem 4.2.8

If X is finite, then $\mathcal{P}(X)$ is finite.

Proof. If $|X| = 0$, then $\mathcal{P}(X) = \{\varnothing\}$, which is indeed finite.

Fix any $n \in \mathbb{N}$ and assume that $\mathcal{P}(X)$ is finite for all X with $|X| = n$. Take any Y with $|Y| = n+1$. Let $Y = \{y_0, \cdots, y_n\}$ and $X \triangleq \{y_0, \cdots, y_{n-1}\}$. Note that $\mathcal{P}(Y) = \mathcal{P}(X) \cup U$ where $U = \{u \subseteq Y \mid y_n \in u\}$. Moreover, $f : \mathcal{P}(X) \to U$ defined by $f(x) = x \cup \{y_n\}$ is injective and onto U. Hence, U is finite. By Lemma 4.2.6, $\mathcal{P}(Y)$ is finite. The result follows by The Induction Principle. $\square$

Theorem 4.2.9

If X is infinite, then $|X| > n$ for all $n \in \mathbb{N}$.

Proof. We clearly have $0 \leq |X|$.

For induction, fix any $n \in \mathbb{N}$ and assume $n \leq |X|$, i.e., there exists $f : n \hookrightarrow X$. By Theorem 4.2.5, $\operatorname{ran} f \subsetneq X$; we may take $x \in X \setminus \operatorname{ran} f$. Then, $g \triangleq f \cup \{(n, x)\}$ is an injective function on $n+1$ into X; hence $n+1 \leq |X|$. Therefore, by The Induction Principle, we have $n \geq |X|$ for all $n \in \mathbb{N}$, which is suffices to induce the result. □

Selected Problems

Exercise 4.2.1

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

Proof. If $S = \varnothing$, then $\left|\bigcup S\right| = 0 = \sum_{i=0}^{n-1} |X_i|$.

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 $\bigcup T = \left(\bigcup S\right) \cup X_n$, and since $\bigcup S$ and X_n are disjoint, $\left|\bigcup T\right| = \left|\bigcup S\right| + |X_n| = \sum_{i=0}^{n-1} |X_i| + |X_n| = \sum_{i=0}^{n} |X_i|$. Hence, the result follows from The Induction Principle. □

Exercise 4.2.2

If X and Y are finite, then $|X \times Y| = |X| \cdot |Y|$.

Proof. We shall exploit the induction on $|Y|$. If $|Y| = 0$, then

$$\begin{aligned} |X \times Y| &= 0 && \triangleright \text{ Exercise 2.2.8} \\ &= |X| \cdot |Y|. && \triangleright \text{ [3]} \end{aligned}$$

Assume the statement holds for all X and Y with $|Y| = n$. Let $Z = \{z_0, \cdots, z_n\}$ be a set with $|Z| = n+1$. Let $Y \triangleq \{z_0, \cdots, z_{n-1}\}$. Then, for all X, $X \times Z = (X \times Y) \cup (X \times \{z_n\})$. Note that $X \times \{z_n\}$ can be identified with X via $f : X \hookrightarrow\!\!\!\!\rightarrow X \times \{z_n\}$ defined by $x \mapsto (x, z_n)$. Hence, if X is finite,

$$\begin{aligned} |X \times Z| &= |X \times Y| + |X \times \{z_n\}| && \triangleright \text{ Lemma 4.2.6} \\ &= |X \times Y| + |X| && \triangleright\ |X \times \{z_n\}| = |X| \\ &= |X| \cdot |Y| + |X| && \triangleright\ \mathbf{P}(n) \\ &= |X| \cdot (|Y| + 1) && \triangleright \text{ [4]} \\ &= |X| \cdot |Z|. \end{aligned}$$

Therefore, by The Induction Principle, the result follows. □

Exercise 4.2.3

If X is finite, $|\mathcal{P}(X)| = 2^{|X|}$.

Proof. Let $\mathbf{P}(x)$ be the property "$\forall X, (|X| = x \implies |\mathcal{P}(X)| = 2^{|X|})$." $\mathbf{P}(0)$ holds since $|\mathcal{P}(\varnothing)| = |\{\varnothing\}| = 1 = 2^0$.

Fix $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$. Let $Y = \{y_0, \cdots, y_n\}$ be a set with $|Y| = n+1$. Let $X \triangleq \{y_0, \cdots, y_{n-1}\}$. As in the proof of Theorem 4.2.8, $\mathcal{P}(Y) = \mathcal{P}(X) \cup U$ where $U = \{u \subseteq$

$Y \mid y_n \in u\}$. Note that $\mathcal{P}(X) \cap U = \varnothing$ and $f : \mathcal{P}(X) \hookrightarrow\!\!\!\twoheadrightarrow U$ defined by $x \mapsto x \cup \{y_n\}$ asserts $|\mathcal{P}(X)| = |U|$. Therefore,

$$\begin{aligned}
|\mathcal{P}(Y)| &= |\mathcal{P}(X)| + |U| && \triangleright \text{ Lemma 4.2.6} \\
&= 2^n + 2^n && \triangleright\ |\mathcal{P}(X)| = |U|,\ \mathbf{P}(n) \\
&= 2^n \cdot 1 + 2^n \cdot 1 && \triangleright \text{ Lemma 3.4.11} \\
&= 2^n \cdot 2 && \triangleright\ \cdot \text{ Distributes Over } + \\
&= 2^{n+1}. && \triangleright\ [6]
\end{aligned}$$

Therefore, by The Induction Principle, the result follows. □

Exercise 4.2.4

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 $|X^Y| = |X|^x$." $\mathbf{P}(0)$ holds since $|X^\varnothing| = |\{\varnothing\}| = 1 = |X|^0$ for all X.

Fix $n \in \mathbb{N}$ and assume $\mathbf{P}(n)$. Let $Y = \{y_0, \cdots, y_n\}$ be a set with $|Y| = n + 1$. Let $Z \triangleq \{y_0, \cdots, y_{n-1}\}$. Take any finite set X.

We have $|X^Y| = |X^Z \times X|$ since we may define $f : X^Y \hookrightarrow\!\!\!\twoheadrightarrow X^Z \times X$ by $g \mapsto \big(g\big|_Z, g(y_n)\big)$. Hence,

$$\begin{aligned}
|X^Y| &= |X^Z \times X| \\
&= |X^Z| \cdot |X| && \triangleright \text{ Exercise 4.2.1} \\
&= |X|^n \cdot |X| && \triangleright\ \mathbf{P}(n) \\
&= |X|^{n+1}. && \triangleright\ [6]
\end{aligned}$$

The result follows by The Induction Principle. □

Exercise 4.2.6

X is finite if and only if every $\varnothing \subsetneq U \subseteq \mathcal{P}(X)$ has a $\subseteq$-maximal element.

Proof.

($\Rightarrow$) Let $|X| = n$ and $\varnothing \subsetneq U \subseteq \mathcal{P}(X)$. Since $|Y| \leq n$ for all $Y \in U$, by Theorem 3.2.8, 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 Exercise 4.1.3 and $|Y'| \leq m$ by definition of m; thus $|Y'| = |Y| = m$ by Cantor–Bernstein Theorem, which implies we may not have $Y \subsetneq Y'$ by Lemma 4.2.2. Hence, Y is a maximal element of U.

($\Leftarrow$) Assume X is infinite. Let $U = \{Y \subseteq X \mid Y \text{ is finite}\}$. (Note $\varnothing \in U$, hence $U \neq \varnothing$.) Take any $Y \in U$. Since $Y \subsetneq X$, we may take $x \in X \setminus Y$. Then, $Y \subsetneq Y \cup \{x\}$ and $Y \cup \{x\} \in U$ by Lemma 4.2.6. Hence, there is no maximal element of U. □

4.3 Countably Infinite sets

Definition 4.3.1: Countably Infinite Set

- A set S is *countably infinite* if $|S| = |\mathbb{N}|$.
- A set S is *countable* if $|S| \leq |\mathbb{N}|$.
- $|\mathbb{N}| = \mathbb{N}$, i.e., the cardinality of countably infinite sets is $\mathbb{N}$.

Note:-

In the book, the author uses the term 'countable' and 'at most countable' for $|S| = |\mathbb{N}|$ and $|S| \leq |\mathbb{N}|$, respectively.

Notation 4.3.2: 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 4.3.3

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 $g\colon \operatorname{Seq}(\mathbb{N}) \to \mathbb{N}$ be defined by

$$g(k) \triangleq \min\left\{ i \in \mathbb{N} \,\middle|\, a_i \in B \setminus \{ a_{k_j} \mid j \in \operatorname{dom} k \} \right\}.$$

Note that g is well-defined since B is infinite. Then, by The Recursion Theorem: General Version, there exists a sequence $\langle k_i \rangle_{i\in\mathbb{N}}$ of natural numbers such that $\forall n \in \mathbb{N}$, $k_n = g\left(k\big|_n\right)$. 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 1 of Theorem 3.3.3. □

Corollary 4.3.4

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, $|S| = |\operatorname{ran} f|$ and $\operatorname{ran} f$ is a subset of $\mathbb{N}$. Hence, by Theorem 4.3.3, S is countably infinite if it is not finite.

($\Leftarrow$) Theorem 4.2.9 □

Theorem 4.3.5

If X is countably infinite and f is a function, then $f[X]$ is countable.

Proof. If $f[X] = \varnothing$, then it is done; assume $f[X] \neq \varnothing$. WLOG, $X \subseteq \operatorname{dom} f$. Let $\langle x_i \rangle_{i\in\mathbb{N}}$ be an injective sequence whose range is X. Let $g\colon f[X] \to \mathbb{N}$ be defined by

$$g(y) \triangleq \min\{ i \in \mathbb{N} \mid y = f(x_i) \}.$$

g is injective, and thus $|f[X]| \leq \aleph_0$. □

Theorem 4.3.6

(i) If A and B are countably infinite, then $A \times B$ is countably infinite.
(ii) If A is countably infinite and $B \neq \varnothing$ 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. Also, we have an injection $g\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ 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, we have

$$\begin{aligned} |A \times B| &= |\mathbb{N} \times n| \\ &\leq |\mathbb{N} \times \mathbb{N}| && \triangleright \text{ Exercise 4.1.3} \\ &= \aleph_0. && \triangleright \text{ Theorem 4.3.6} \end{aligned}$$

Let $b \in B$. Then, we have

$$\begin{aligned} \aleph_0 &= |A| \\ &= |A \times \{b\}| && \triangleright\ a \mapsto (a, b) \\ &\leq |A \times B|. && \triangleright \text{ Exercise 4.1.3} \end{aligned}$$

Hence, by Cantor–Bernstein Theorem, $|A \times B| = \aleph_0$.

(iii) If one of them is empty, then $A \times B = \varnothing$. If A and B are finite, then $A \times B$ is finite by Exercise 4.2.2. If any of them is countably infinite, and if both are nonempty, then $A \times B$ is countably infinite by (i) and (ii). □

Corollary 4.3.7

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. $\mathbf{P}(1)$ evidently holds.

Fix $n > 0$ and assume $\mathbf{P}(n)$. Now, take any system $\langle A_i \mid i \in n+1 \rangle$ of countably infinite sets. Then, since we have a natural mapping $f : \prod_{i=0}^{n} A_i \hookrightarrow\!\!\!\!\rightarrow \left(\prod_{i=0}^{n-1} A_i\right) \times A_n$ defined by $\langle a_0, \cdots, a_n \rangle \mapsto (\langle a_0, \cdots, a_{n-1} \rangle, a_n)$, we get

$$\begin{aligned} \left|\prod_{i=0}^{n} A_i\right| &= \left|\left(\prod_{i=0}^{n-1} A_i\right) \times A_n\right| \\ &= |\mathbb{N} \times \mathbb{N}| && \triangleright\ \mathbf{P}(n) \\ &= \aleph_0. && \triangleright \text{ Theorem 4.3.6} \end{aligned}$$

Hence, we have $\mathbf{P}(n+1)$.

Therefore, by Exercise 3.2.11, the result follows. □

Theorem 4.3.8

Let $\langle a_n \mid n \in \mathbb{N} \rangle$ countably infinite system of infinite sequences. Then, $\bigcup_{n\in\mathbb{N}} \operatorname{ran} a_n$ is countable.

Proof. Define $f : \mathbb{N} \times \mathbb{N} \twoheadrightarrow \bigcup_{n\in\mathbb{N}} \operatorname{ran} a_n$ by $f(n, k) = a_n(k)$. The result follows by Theorem 4.3.5 and Theorem 4.3.6. □

Note:-

Note that we cannot yet prove the proposition "the union of 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 $\operatorname{ran} a_n = A_n$ for each $n \in \mathbb{N}$.

Theorem 4.3.9

If A is countably infinite, then $\operatorname{Seq}(A)$ 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 $g : \mathbb{N} \twoheadrightarrow \mathbb{N}\times\mathbb{N}$. Define $\langle a_n \mid n \in \mathbb{N}\rangle$ recursively by

$$\begin{aligned} \forall i \in \mathbb{N},\quad & a_0(i) = \langle\rangle \\ \forall n, i \in \mathbb{N},\, & a_{n+1}(i) = \langle b_0, \cdots, b_{n-1}, i_2\rangle \\ & \qquad\qquad \text{where } g(i) = (i_1, i_2) \text{ and } a_n(i_1) = \langle b_0, \cdots, b_{n-1}\rangle. \end{aligned}$$

The existence is justified by The Recursion Theorem. Then, with The Induction Principle, it is easy to prove that $\operatorname{ran} a_n = \mathbb{N}^n$ for each $n \in \mathbb{N}$. Hence, by Theorem 4.3.8, $\bigcup_{n\in\mathbb{N}} \mathbb{N}^n$ is countably infinite. □

Corollary 4.3.10

The set of all finite subsets of a countably infinite set is countably infinite.

Proof. Let A be countably infinite. Let $f : \mathrm{Seq}(A) \to \mathcal{P}(A)$ by $f(\langle a_0, \cdots, a_{n-1}\rangle) = \{a_0, \cdots, a_{n-1}\}$. Then, $\operatorname{ran} f$ is countable by Theorem 4.3.5 and Theorem 4.3.9. $\operatorname{ran} f$ is countably infinite since we have an injection $a \mapsto \{a\}$. □

Theorem 4.3.11

An equivalence on a countably infinite set has at most countably many equivalence classes.

Proof. Let E be an equivalence on a countably infinite set A. Let $f : A \twoheadrightarrow A/E$ be defined by $a \mapsto [a]_E$. Hence, by Theorem 4.3.5, A/E is countable. □

Theorem 4.3.12

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. Theorem 3.5.15 says that $\overline{C} = \bigcup_{i\in\mathbb{N}} C_i$ where $C_0 = C$ and $C_{i+1} = C_i \cup \bigcup_{j=0}^{n-1} F_j[C_i^{f_j}]$.

Let $c : \mathbb{N} \twoheadrightarrow C$. Let $g : \mathbb{N} \twoheadrightarrow (n+1)\times\mathbb{N}\times\mathbb{N}^{f_0}\times\cdots\times\mathbb{N}^{f_{n-1}}$. Now, define $\langle a_i \mid i \in \mathbb{N}\rangle$ recursively by

$$\begin{aligned} \forall k \in \mathbb{N} \qquad & a_0(k) \triangleq c(k) \\ \forall i, k \in \mathbb{N},\quad & a_{i+1}(k) \triangleq \begin{cases} F_p(a_i(r_p^0), \cdots, a_i(r_p^{f_p-1})) & \text{if } 0 \le p < n \\ a_i(q) & \text{if } p = n \end{cases} \\ & \qquad \text{where } g(k) = \langle p, q, \langle r_0^0, \cdots, r_0^{f_0-1}\rangle, \cdots, \langle r_{n-1}^0, \cdots, r_{n-1}^{f^{n-1}-1}\rangle\rangle. \end{aligned}$$

It is apparent by The Induction Principle that $\operatorname{ran} a_i = C_i$ for each $i \in \mathbb{N}$. Hence, by Theorem 4.3.8, $\overline{C}$ is countable. □

Selected Problems

Exercise 4.3.1

Let $|A_1| = |A_2|$ and $|B_1| = |B_2|$.

(i) If $A_1 \cap B_1 = \varnothing$ and $A_2 \cap B_2 = \varnothing$, 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 $f_A : A_1 \hookrightarrow\!\!\!\rightarrow A_2$ and $f_B : B_1 \hookrightarrow\!\!\!\rightarrow B_2$. Then, $f_A \cup f_B : A_1 \cup B_1 \hookrightarrow\!\!\!\rightarrow A_2 \cup B_2$.

(ii) Let $f_A : A_1 \hookrightarrow\!\!\!\rightarrow A_2$ and $f_B : B_1 \hookrightarrow\!\!\!\rightarrow B_2$. We may define $g : A_1 \times B_1 \hookrightarrow\!\!\!\rightarrow A_2 \times B_2$ by $(a, b) \mapsto (f_A(a), f_B(b))$.

(iii) Let $f : A_1 \hookrightarrow\!\!\!\rightarrow A_2$. We may define $g : \operatorname{Seq}(A_1) \hookrightarrow\!\!\!\rightarrow \operatorname{Seq}(A_2)$ by

$$\langle a_0, \cdots, a_{n-1} \rangle \mapsto \langle f(a_0), \cdots, f(a_{n-1}) \rangle.$$

□

Exercise 4.3.2

If A is finite and B is countably infinite, then $A \cup B$ is countably infinite.

Proof. Let $f_A : A \hookrightarrow \mathbb{N}$ and $f_B : B \hookrightarrow \mathbb{N}$. Then, we may define $g : A \cup B \hookrightarrow \mathbb{N} \times \mathbb{N}$ by

$$g(x) = \begin{cases} (f_A(x), 0) & \text{if } x \in A \\ (f_B(x), 1) & \text{if } x \in B \setminus A \end{cases}$$

Hence, $|A \cup B| \le \aleph_0$ by Theorem 4.3.6. Moreover, $\aleph_0 = |B| \le |A \cup B|$ by Exercise 4.1.3. The result follows from Cantor–Bernstein Theorem. □

Exercise 4.3.4

If A is finite and nonempty, then $\operatorname{Seq}(A)$ is countably infinite.

Proof. Let $B \triangleq A \cup \mathbb{N}$. Then, by Exercise 4.3.2, B is countably infinite and $\operatorname{Seq}(B)$ is countably infinite by Theorem 4.3.9. Hence, as $\operatorname{Seq}(A) \subseteq \operatorname{Seq}(B)$, $|\operatorname{Seq}(A)| \le \aleph_0$.

Fix any $a \in A$. Let s be the infinite sequence with $\forall i \in \mathbb{N}$, $s_i = a$. Then, we have $f : \mathbb{N} \hookrightarrow \operatorname{Seq}(A)$ defined by $f(n) = s\big|_n$; thus $\aleph_0 \le |\operatorname{Seq}(A)|$. The result follows from Cantor–Bernstein Theorem. □

Exercise 4.3.5

Let A be countably infinite. The set $[A]^n = \{ S \subseteq A \mid |S| = n \}$ is countably infinite for all $n > 0$.

Proof. It is enough to show that $[\mathbb{N}]^n$ is countably infinite for all $n > 0$. Evidently, $i \mapsto \{i\}$ is an injective mapping on $\mathbb{N}$ onto $[\mathbb{N}]^1$. Hence, $|[\mathbb{N}]^1| = \aleph_0$.

For the sake of induction, fix $n > 0$ and assume $|[\mathbb{N}]^n| = \aleph_0$. We may define $f : [\mathbb{N}]^n \hookrightarrow [\mathbb{N}]^{n+1}$ by

$$f(x) \triangleq x \cup \big\{ \max\{ i \in \mathbb{N} \mid i \in x \} + 1 \big\}.$$

Hence, $\aleph_0 \le |[\mathbb{N}]^{n+1}|$.

Now, since $|[\mathbb{N}]^n| = |\mathbb{N}^n| = \aleph_0$ by Corollary 4.3.7, there exists an injection $g : [\mathbb{N}]^n \hookrightarrow \mathbb{N}^n$. We define $h : [\mathbb{N}]^{n+1} \hookrightarrow \mathbb{N}^{n+1}$ by

$$h(x) \triangleq g(x \setminus \{i\}) \cup \{(n, i)\}$$
$$\text{where } i = \max x.$$

Hence, $|[\mathbb{N}]^{n+1}| \le |\mathbb{N}^{n+1}| \le \aleph_0$. Exercise 3.2.11 assures that $\forall n > 0$, $|[\mathbb{N}]^n| = \aleph_0$. □

Exercise 4.3.6

A sequence $\langle s_n \rangle_{n=0}^{\infty}$ of natural numbers is *eventually constant* if

$$\exists n_0, s \in \mathbb{N},\ \forall n \geq n_0,\ s_n = s.$$

The set of eventually constant sequences of natural numbers is countable.

Proof. Let P be the set of eventually constant sequences of natural numbers. As $P \subseteq Q$ where Q is the set of eventually periodic sequences of natural numbers (see Exercise 4.3.7), we have $|P| \leq \aleph_0$ by Exercises 4.1.3 and 4.3.7.

Moreover, we may define an injective infinite sequence into P recursively by

$$\begin{aligned} g_0 &= \langle 0, 0, \cdots \rangle \\ \forall n \in \mathbb{N}, \quad g_{n+1} &= \langle n+1, a_0, a_1, \cdots \rangle \\ &\qquad \text{where } g_n = \langle a_0, a_1, \cdots \rangle. \end{aligned}$$

Hence, $\aleph_0 \leq |P|$. The result follows by Cantor–Bernstein Theorem. $\square$

Exercise 4.3.7

A sequence $\langle s_n \rangle_{n=0}^{\infty}$ of natural numbers is *eventually periodic* if

$$\exists n_0 \in \mathbb{N},\ \exists p > 0,\ \forall n \geq n_0,\ s_{n+p} = s_n.$$

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. We may define $f : Q \to \mathrm{Seq}(\mathbb{N}) \times \mathbb{N}$ by

$$\begin{aligned} f(x) &\triangleq \left(x\big|_{n^*+p^*}, p^* \right) \\ &\qquad \text{where } n^* = \min\{ n_0 \in \mathbb{N} \mid \exists p > 0,\ \forall n \geq n_0,\ s_{n+p} = s_n \} \\ &\qquad\quad \text{and } p^* = \min\{ p > 0 \mid \forall n \geq n^*,\ s_{n+p} = s_n \}. \end{aligned}$$

Then, it can be easily shown that f is injective. Hence, $|Q| \leq |\mathrm{Seq}(\mathbb{N}) \times \mathbb{N}| = \aleph_0$ by Theorems 4.3.6 and 4.3.9.

Moreover, as $P \subseteq Q$ where P is the set of eventually constant sequences of natural numbers and $\aleph_0 \leq |P|$ by Exercise 4.3.6, we have $|Q| = \aleph_0$ by Exercise 4.1.3 and Cantor–Bernstein Theorem. $\square$

Exercise 4.3.10

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. WLOG, $A_n \neq \varnothing$ for each $n \in \mathbb{N}$.

> ***Claim 1.*** For each finite $A \subseteq S$, there uniquely exists a unique isomorphism between $\left(|A|, \leq \cap |A|^2\right)$ and $(A, \preceq \cap A^2)$.
>
> ***Proof.*** We have existence for each A by Theorem 4.5.3. Hence, we only prove the uniqueness by induction. If $|A| = 0$, we have only one isomorphism $\varnothing$.
>
> Fix some $n \in \mathbb{N}$ and assume the proposition holds for all A with cardinality n. Take

any $A \subseteq S$ with $|A| = n+1$. Let f and g be two isomorphisms between $(n+1, \leq \cap (n+1)^2)$ and $(A, \leq \cap A^2)$. Then, $f(n) = g(n)$ since the greatest element is unique. Let $B = A \setminus \{f(n)\}$. Then, $f\big|_n$ and $g\big|_n$ are isomorphisms between $(n, \leq \cap n^2)$ and $(B, \leq \cap B^2)$. Hence, $f\big|_n = g\big|_n$, and thus $f = g$. The result follows from The Induction Principle.

Claim 1 enables us to guarantee the existence of infinite sequence $\langle a_n \mid n \in \mathbb{N} \rangle$ such that, for each $n \in \mathbb{N}$:

(i) $a_n\big|_{|A_n|}$ is the isomorphism between $\left(|A_n|, \leq\big|_{|A_n|^2}\right)$ and $\left(A_n, \preceq\big|_{A_n^2}\right)$.

(ii) $\forall k \geq |A_n|$, $a_n(k) = a_n(0)$.

Hence, $\operatorname{ran} a_n = A_n$ for each $n \in \mathbb{N}$, and thus $\bigcup_{n=0}^{\infty} A_n$ is countable by Theorem 4.3.8. □

Exercise 4.3.11

Any partition of a countable set has a set of representatives.

Proof. Let A be countable and S be a partition of A. There exists $f : A \hookrightarrow \mathbb{N}$. Then,

$$X \triangleq \{ f^{-1}(\min f[C]) \mid C \in S \}$$

is a set of representatives. □

4.4 Complete Linear Ordering

Definition 4.4.1: 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 4.4.2

Let $(P, \leq)$ be a totally ordered set and let $\varnothing \subsetneq A \subseteq P$.

- A is *bounded* if A has both lower and upper bounds.
- A is *bounded from below* if it has a lower bound.
- A is *bounded from above* if it has an upper bound.

Lemma 4.4.3

Let $(P, \leq)$ be a totally ordered set. Every nonempty $S \subseteq P$ bounded from above has a supremum if and only if $(P, \leq)$ has no gap.

Proof.

($\Rightarrow$) Suppose (A, B) is a gap of $(P, \leq)$. Then, as any $b \in B$ is a supremum of A, A is bounded from above. Hence, by assumption, there exists $\mu = \sup A$. There are two cases: $\mu \in A$ and $\mu \in B$.

If $\mu \in A$, then by Theorem 2.5.13 (iii), $\mu = \max A$, which contradicts the fact that (A, B) is a gap. If $\mu \in B$, as any $b \in B$ is an upper bound of A, $\forall b \in B$, $\mu \leq b$, i.e., $\mu = \min B$, which is a contradiction as well.

($\Leftarrow$) Suppose there is nonempty $S \subseteq P$ such that S is bounded above and S has no supremum. Let

$$A \triangleq \{x \in P \mid \exists s \in S,\ x \leq s\},$$
$$B \triangleq \{x \in P \mid \forall s \in S,\ x > s\}.$$

Claim 1. $\{A, B\}$ is a partition of P.

Proof. We have $A \cap B = \varnothing$ and $A \cup B = P$. As $A = P$ implies the existence of $\max S$, which contradicts the nonexistence of $\sup S$ by Item Theorem 2.5.13 (ii), we have $B \neq \varnothing$; moreover, as $B = P$ is impossible by $S \cap P = \varnothing$, we have $A \neq \varnothing$. Hence, $\{A, B\}$ is a partition of P. □

Claim 2. $\forall a \in A,\ \forall b \in B,\ a < b$.

Proof. Take any $a \in A$ and $b \in B$. Then, there exists $s \in S$ such that $a \leq s$. As $b \in B$, we have $a \leq s < b$. Hence, $a < b$. □

Claim 3. $\max A$ and $\min B$ do not exist.

Proof. Suppose $m = \min B$ exists for the sake of contradiction. Let m' be an upper bound of S. If $m' \in S$, then $m' = \sup S$, which is a contradiction. Hence, we have $\forall s \in S,\ m' > s$, i.e., $m' \in B$. This implies $m \leq m'$, that is to say $m = \sup S$. Hence, $\min B$ does not exist.

Suppose $M = \max A$ exists for the sake of contradiction. Then, as $S \subseteq A$, M is an upper bound of S. Let M' be another upper bound of S. Then, as $\forall s \in S$, $M \leq s \leq M'$, $M = \sup S$, which is a contradiction. Hence, $\max A$ does not exist. □

Combining Claims 1 to 3 gives the result. □

Definition 4.4.4: Complete Dense Totally Ordered Set

Let $(P, \leq)$ be a dense totally ordered set. $(P, \leq)$ is said to be *complete* if every nonempty $S \subseteq P$ bounded from above has a supremum, i.e., if $(P, \leq)$ has no gap. (See Lemma 4.4.3.)

Theorem 4.4.5 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) $\forall p, q \in P,\ (p < q \iff p \prec q)$.
(iii) $\forall c, d \in C,\ (c \prec d \implies \exists p \in P,\ c \prec p \prec d)$, i.e., P is dense in C.
(iv) C does not have endpoints.

Moreover, such $(C, \preceq)$ is unique up to isomorphism h with $\mathrm{Id}_P \subseteq h$.[†] The complete totally ordered set $(C, \preceq)$ is called the *completion* of $(P, \leq)$.

[†]In other words, if $(C, \preceq)$ and $(C^*, \preceq^*)$ satisfy all the requirements, then there exists an isomorphism h between $(C, \preceq)$ and $(C^*, \preceq^*)$ such that $\forall p \in P,\ h(p) = p$.

Proof. For each $B \subseteq P$, one may easily verify that $\min B$ exists if and only if there exists $p \in P$ such that $B = \{x \in P \mid x \geq p\}$. Hence, there are two types of Dedekind cuts—a Dedekind cut (A, B) such that:

(i) There (uniquely) exists $p \in P$ such that $B = \{x \in P \mid x \geq p\}$; in this case we write $(A, B) = [p]$.

(ii) (A, B) is a gap.

Note that $[p]$ is a Dedekind cut of $(P, \leq)$ for all $p \in P$.

Now, define C and a relation $\preceq$ on C by:

$$C \triangleq \{(A, B) \mid (A, B) \text{ is a Dedekind cut of } (P, \leq)\}$$

and

$$(A, B) \preceq (A', B') \iff A \subseteq A'.$$

Claim 1. $(C, \preceq)$ is a totally ordered set.

Proof. It is evident that $(C, \preceq)$ is an ordered set. Take any $(A, B), (A', B') \in C$. Suppose they are incomparable for the sake of contradiction, i.e., $A \setminus A' = A \cap B' \neq \varnothing$ and $A' \setminus A = A' \cap B \neq \varnothing$. Let $a \in A \cap B'$ and $a' \in A' \cap B$. Then, $a < a'$ and $a' < a$, which is impossible by asymmetry of $<$. □

If $p < q$ where $p, q \in P$, then we have $[p] \prec [q]$. Hence, $(P', \preceq \cap P'^2) \cong (P, \leq)$ where $P' \triangleq \{[x] \mid x \in P\}$. Thus, we simply prove that $(C, \preceq)$ is a completion of $(P', \preceq \cap P'^2)$.

Claim 2. $\forall c, d \in C, (c \prec d \implies \exists p \in P, c \prec [p] \prec d)$.

Proof. Take any $c, d \in C$ with $c \prec d$. In other words, $c = (A, B)$ and $d = (A', B')$ with $A \subsetneq A'$. Take $p \in A' \setminus A$. As $(P, \leq)$ has no greatest element, WLOG, we may assume p is not a least element of B. Let $[p] = (A'', B'')$.

- As $(P, \leq)$ is totally ordered, the fact that p is not a least element of B asserts the existence of $b \in B$ such that $b < p$. Hence, $\forall x \in B''$, $\forall a \in A$, $a < b < p \leq x$. Thus, $B'' \subsetneq B$; $(A, B) \prec [p]$. ✓
- As A' has no greatest element and $(P, \leq)$ is totally ordered, there exists $a' \in A'$ such that $p < a'$. Then, we have $\forall x \in A''$, $\forall b' \in B'$, $x < p < a' < b'$, i.e., $A'' \subsetneq A'$. Hence, $[p] \prec (A', B')$. ✓ □

Claim 2 also shows that $(C, \preceq)$ is a densely ordered set.

Claim 3. $(C, \preceq)$ has no endpoints.

Proof. Take any $(A, B) \in C$.

- In the same way as in the proof of Claim 2, any $p \in B$ which is not a least element of B (which exists) satisfies $(A, B) \prec [p]$. Hence, C has no greatest element. ✓
- Take any $p \in A$. As A has no greatest element, there exists $a \in A$ such that $p < a$. Hence, $[p] \prec (A, B)$. ✓ □

Claim 4. $(C, \preceq)$ is complete.

Proof. Let $\varnothing \subsetneq S \subseteq C$ be bounded from above. Let (A_0, B_0) be an upper bound of S. Define

$$A_S \triangleq \bigcup \{A \mid (A, B) \in S\} \quad \text{and} \quad B_S \triangleq P \setminus A_S = \bigcap \{B \mid (A, B) \in S\}.$$

As $B_0 \subseteq B_S$, (A_S, B_S) is a cut. Moreover, if x is a greatest element of A_S, then x is a greatest element of some A where $(A, B) \in S$. Hence, A_S has no greatest element; $(A_S, B_S) \in C$.

As $A \subseteq A_S$ for all $(A, B) \in S$, (A_S, B_S) is an upper bound of S. If (A', B') is another upper bound of S, then $\forall (A, B) \in S$, $A \subseteq A'$, i.e., $A_S \subseteq A'$. Hence, $(A_S, B_S) \preceq (A', B')$. Thus, $(A_S, B_S) = \sup_{\preceq} S$. □

Claims 1 to 4 shows that $(C,\preceq)$ satisfies the requirements of the theorem; hence the existence part is done. We now prove the uniqueness.

Claim 5. Let $(C,\preceq)$ and $(C^*,\preceq^*)$ be two complete totally ordered sets that satisfies (i)–(iv). Then, there exists an isomorphism h between $(C,\preceq)$ and $(C^*,\preceq^*)$ such that $\forall p \in P$, $h(p)=p$.

Proof. For each $c \in C$ and $c^* \in C^*$ define

$$S_c \triangleq \{\, p \in P \mid p \prec c \,\} \quad \text{and} \quad S_{c^*} \triangleq \{\, p \in P \mid p \prec^* c^* \,\}.$$

Note that:
- (I) $\sup_{\preceq} S_c = c$ and $\sup_{\preceq^*} S_{c^*} = c^*$ by (iii).
- (II) Take any $c \in C$. By (iii) and (iv), there exists $q \in P$ such that $c \prec q$. Hence, $\forall p \in S_c$, $p \prec c \prec q$, and thus, $\forall p \in S_c$, $p \prec^* q$ by (ii). Therefore, every S_c is bounded from above in $(C^*,\preceq^*)$. By symmetry, every S_{c^*} is bounded from above in $(C,\preceq)$.
- (III) For $p \in P$ and $\varnothing \subsetneq X \subseteq P$ such that both $\sup_{\preceq} X$ and $\sup_{\preceq^*} X$ exist, we have

$$p \prec \sup_{\preceq} X \iff \exists x \in X,\, p \prec x \iff \exists x \in X,\, p \prec^* x \iff p \prec^* \sup_{\preceq^*} X.$$

Now, define $h\colon C \to C^*$ by $c \mapsto \sup_{\preceq^*} S_c$. h is well-defined by (II) and $(C^*,\preceq^*)$ being complete. We now show that h is a desired isomorphism.

- Take any $c^* \in C^*$. Let $c \triangleq \sup_{\preceq} S_{c^*}$. Then,

$$\begin{aligned} h(c) &= \sup_{\preceq^*} S_c \\ &= \sup_{\preceq^*}\{\, p \in P \mid p \prec \sup_{\preceq} S_{c^*} \,\} \\ &= \sup_{\preceq^*}\{\, p \in P \mid p \prec^* \sup_{\preceq^*} S_{c^*} \,\} && \triangleright \text{(III)} \\ &= \sup_{\preceq^*}\{\, p \in P \mid p \prec^* c^* \,\} && \triangleright \text{(I)} \\ &= \sup_{\preceq^*} S_{c^*} = c^*. && \triangleright \text{(I)} \end{aligned}$$

  Hence, h is onto C^*. ✓
- Take any $c,d \in C$ with $c \prec d$. Then, by (iii), there exist $p_1,p_2 \in P$ such that $c \prec p_1 \prec p_2 \prec d$. We then have $\sup_{\preceq^*} S_c \preceq^* p_1 \prec^* p_2 \preceq^* \sup_{\preceq^*} S_d \prec$. Hence, $h(c) \prec^* h(d)$; h is an isomorphism. ✓
- For each $p \in P \subseteq C \cap C^*$, by (I), $h(p) = \sup_{\preceq^*} S_p = p$. ✓

Thus the theorem is now proven. □

Selected Problems

Exercise 4.4.4

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. We notice that (A,B) is a gap of $(P,\preceq)$ if and only if (B,A) is a gap of $(P,\preceq^{-1})$. Hence, by Lemma 4.4.3, $(P,\preceq)$ is complete if and only if every nonempty set $S \subseteq P$ bounded from above in $(P,\preceq^{-1})$ has an supremum in $(P,\preceq^{-1})$.

Note that $S \subseteq P$ is bounded from above in $(P,\preceq^{-1})$ if and only if S is bounded from below in $(P,\preceq)$, and $\sup_{\preceq^{-1}} S = \inf_{\preceq} S$. □

4.5 Linear Orderings

Definition 4.5.1: Similar Ordered Sets

Totally ordered sets $(A, \leq)$ and $(B, \preceq)$ are *similar* (have *the same order type*) if they are isomorphic. (Definition 2.5.14)

Lemma 4.5.2

Every total ordering on a finite set is a well-ordering.

Proof. Let $(A, \leq)$ be a finite totally ordered set. If $B \subseteq A$ has $|B| = 1$, then the only element of B is $\min B$.

Now, fix $n > 0$ and assume that every $B \subseteq A$ with $|B| = n$ has a least element. Take any $B \subseteq A$ with $|B| = n+1$ and write $B = \{b_0, \cdots, b_n\}$. Let $C \triangleq \{b_0, \cdots, b_{n-1}\}$. Then, if $b_n \leq \min C$, then b_n is a least element of B; otherwise, $\min C$ is a least element of B. Hence, by Exercise 3.2.11, every nonempty finite subset of A has a least element, i.e., $(A, \leq)$ is well-ordered. □

Theorem 4.5.3

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 shall conduct the induction on the size of the sets. If $A_1 = A_2 = \varnothing$, then they are evidently similar by the isomorphism $\varnothing$.

Fix $n \in \mathbb{N}$ and assume the proposition holds whenever $|A_1| = |A_2| = n$. Take any totally ordered sets $(A_1, \leq_1)$ and $(A_2, \leq_2)$ such that $|A_1| = |A_2| = n+1$. By Lemma 4.5.2, there exist $a_1 = \min A_1$ and $a_2 = \min A_2$. Let $A_1' \triangleq A_1 \setminus \{a_1\}$ and $A_2' \triangleq A_2 \setminus \{a_2\}$. Since $(A_1', \leq_1 \cap A_1'^2)$ and $(A_2', \leq_2 \cap A_2'^2)$ are finite totally ordered sets with $|A_1'| = |A_2'| = n$, there exists an isomorphism $g : A_1' \hookrightarrow\!\!\!\!\rightarrow A_2'$ by the induction hypothesis. Then, $f \triangleq g \cup \{(a_1, a_2)\}$ is an isomorphism between $(A_1, \leq_1)$ and $(A_2, \leq_2)$. Therefore, the result follows from The Induction Principle. □

Lemma 4.5.4

If $(A, \leq)$ is a totally ordered set, then $(A, \leq^{-1})$ is also a totally ordered set.

Proof. Take any $a, b \in A$. Then, it is $a \leq b$ or $b \leq a$. If $a \leq b$, then $b \leq^{-1} b$. If $b \leq a$, then $a \leq^{-1} b$. Hence, $(A, \leq^{-1})$ is totally ordered. □

Lemma 4.5.5

Let $(A_1, \leq_1)$ and $(A_2, \leq_2)$ be totally ordered sets such that $A_1 \cap A_2 = \varnothing$. The relation $\leq$ on $A = A_1 \cup A_2$ defined by

$$a \leq b \iff (a \leq_1 b) \vee (a \leq_2 b) \vee (a \in A_1 \wedge b \in A_2)$$

is a total ordering. 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. Exercise 2.5.6 already shows that $\leq$ is an ordering of A. Totality follows directly by the definition. □

Lemma 4.5.6

Let $(A_1, \leq_1)$ and $(A_2, \leq_2)$ be totally ordered sets. The relation $\leq$ on $A = A_1 \times A_2$ defined by

$$(a_1, a_2) \leq (b_1, b_2) \iff a_1 <_1 b_1 \lor (a_1 = b_1 \land a_2 \leq_2 b_2)$$

is a total ordering. We call $\leq$ the *lexicographic ordering* (*lexicographic product*) of $A_1 \times A_2$.

Proof.

- Assume $(a_1, a_2) < (b_1, b_2)$ and $(b_1, b_2) < (c_1, c_2)$. If $a_1 <_1 b_1$, then, we have $a_1 <_1 c_1$ by $b_1 <_1 c_1$. If $b_1 <_1 c_1$, then, we have $a_1 <_1 c_1$ by $a_1\, {}_1 b_1$. In the only left case, we have $a_1 = b_1 = c_1$ and $a_2 \leq_2 b_2 \leq_2 c_2$. Hence, $(a_1, a_2) < (c_1, c_2)$. Thus $<$ is transitive in A. ✓
- Assume $(a_1, a_2) < (b_1, b_2)$ and $(b_1, b_2) < (a_1, a_2)$. Since $a_1 \leq_1 b_1$ and $b_1 \leq_1 a_1$, by antisymmetry of $\leq_1$, $a_1 = b_1$. The only option now is $a_2 \leq_2 b_2$ and $b_2 \leq_2 a_2$, which implies $a_2 = b_2$ by the antisymmetry of $\leq_2$. Hence, $(a_1, a_2) = (b_1, b_2)$, which is a contradiction. Thus, $<$ is asymmetric in A. ✓
- Let $(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$. As $\leq_1$ is total, WLOG, $a_1 \leq_1 b_1$. If $a_1 < b_1$, then we immediately have $(a_1, a_2) < (b_1, b_2)$. Now, assume $a_1 = b_1$. Then, as $\leq_2$ is total, WLOG, $a_2 \leq_2 b_2$, and thus $(a_1, a_2) \leq (b_1, b_2)$. Hence, $\leq$ is a total ordering. ✓ □

Theorem 4.5.7

Let $\langle (A_i, \leq_i) \mid i \in I \rangle$ be an indexed system of totally ordered sets where $I \subseteq \mathbb{N}$. The relation $\prec$ on $\prod_{i \in I} A_i$ defined by

$$f \prec g \iff \operatorname{diff}(f, g) \triangleq \{ i \in I \mid f_i \neq g_i \} \neq \varnothing \land f_{i_0} <_{i_0} g_{i_0}$$
$$\text{where } i_0 = \min\nolimits_{\leq} \operatorname{diff}(f, g)$$

is a total strict ordering of $\prod_{i \in I} A_i$. We call $\leq$ the *lexicographic ordering* (*lexicographic product*) of $\prod_{i \in I} A_i$.

Proof.

- Assume $f \prec g$ and $g \prec h$ and let $i_0 = \min \operatorname{diff}(f, g)$ and $j_0 = \min \operatorname{diff}(g, h)$.
  - If $i_0 \leq j_0$, then $f_{i_0} < g_{i_0} \leq h_{i_0}$ and $\operatorname{diff}(f, h) = i_0$.
  - If $j_0 < i_0$, then $f_{j_0} = g_{j_0} < h_{j_0}$ and $\operatorname{diff}(f, h) = j_0$.

  Hence, $f \prec h$; $\prec$ is transitive in $\prod_{i \in I} A_i$. ✓
- For $f, g \in \prod_{i \in I} A_i$ with $f \neq g$, since $i_0 = \operatorname{diff}(f, g) = \operatorname{diff}(g, f)$, we cannot have $f \prec g$ and $g \prec f$ because of the asymmetry of $<_{i_0}$. ✓
- If $\operatorname{diff}(f, g) = \varnothing$, we have $f = g$. If $i_0 = \min \operatorname{diff}(f, g)$, then we have $f \prec g$ when $f_{i_0} <_{i_0} g_{i_0}$ and $g \prec f$ when $g_{i_0} <_{i_0} f_{i_0}$. Hence, $\prec$ is a total ordering. ✓

Definition 4.5.8: Dense Ordered Set

An ordered set $(X, \leq)$ is *dense* if

$$2 \leq |X| \land \forall a, b \in X, (a < b \implies \exists x \in X, a < x < b).$$

Definition 4.5.9: Endpoints

We now will call the least and greatest elements of a totally ordered set *endpoints* of the set.

Theorem 4.5.10

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. Let $\langle q_n \mid n \in \mathbb{N} \rangle$ be an injective sequence onto Q. Let us call $h\colon P \rightharpoonup Q$ a *partial isomorphism* from P to Q if

$$\forall p, p' \in \operatorname{dom} h,\ (p \prec p' \iff h(p) < h(p')).$$

Claim 1. If h is a partial isomorphism from P to Q with finite $\operatorname{dom} h$, and if $p \in P$ and $q \in Q$, then there exists a partial isomorphism $h_{p,q}$ from P to Q that extends h such that $p \in \operatorname{dom} h_{p,q}$ and $q \in \operatorname{ran} h_{p,q}$.

Proof. Write $h = \{(p_{i_0}, q_{i_0}), \cdots, (p_{i_k}, q_{i_k})\}$ where $p_{i_0} \prec p_{i_1} \prec \cdots \prec p_{i_k}$ and thus $q_{i_0} < q_{i_1} < \cdots < q_{i_k}$. (This is justified by Theorem 4.5.3.) We have four cases:

- Assume $p \in \operatorname{dom} h$. Then, let $h' \triangleq h$.
- Assume $p \prec p_{i_0}$. Then, as Q has no least element, $n = \min\{i \in \mathbb{N} \mid q_i < q_{i_0}\}$ exists. Let $h' \triangleq h \cup \{(p, q_n)\}$.
- Assume there exists $e < k$ such that $p_{i_e} \prec p \prec p_{i_{e+1}}$. Then, as Q is dense, $n = \min\{i \in \mathbb{N} \mid q_{i_e} < q_i < q_{i_{e+1}}\}$ exists. Let $h' \triangleq h \cup \{(p, q_n)\}$.
- Assume $p_{i_k} \prec p$. Then, as Q has no greatest element, $n = \min\{i \in \mathbb{N} \mid q_{i_k} < q_i\}$ exists. Let $h' \triangleq h \cup \{(p, q_n)\}$.

Then, h' is a partial isomorphism from P to Q and $p \in \operatorname{dom} h'$. Similarly, one may extend h' in the same way so it has q in its range. $\square$

Now, we may create a sequence of compatible partial isomorphisms from P to Q recursively by

$$\begin{gathered} h_0 = \varnothing \\ \forall n \in \mathbb{N}, \quad h_{n+1} = (h_n)_{p_n, q_n} \end{gathered}$$

where $(h_n)_{p_n,q_n}$ is the extension of h_n (provided by the steps in the proof of Claim 1) such that $p_n \in \operatorname{dom}[(h_n)_{p_n,q_n}]$ and $q_n \in \operatorname{ran}[(h_n)_{p_n,q_n}]$. Then, $h \triangleq \bigcup_{n \in \mathbb{N}} h_n$ is a function by Theorem 2.3.12. It is easy to check if $h\colon P \hookrightarrow\!\!\!\rightarrow Q$ is a desired isomorphism. $\square$

Theorem 4.5.11

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 $h\colon P \hookrightarrow Q$ such that

$$\forall p, p' \in P,\ (p \prec p' \implies h(p) < h(p')).$$

Proof. This is essentially the one-sided version of Theorem 4.5.10. Let $\langle p_n \mid n \in \mathbb{N} \rangle$ be an injective sequence onto P. In a similar way as Claim 1 in the proof of Theorem 4.5.10, if f is a partial isomorphism from P to Q with finite $\operatorname{dom} f$, and if $p \in P$, there exists another partial isomorphism f_p from P to Q that extends f such that $p \in \operatorname{dom} f_p$.

Then, one is able to make a sequence of compatible partial isomorphisms from P to Q recursively by

$$\begin{gathered} h_0 = \varnothing \\ \forall n \in \mathbb{N}, \quad h_{n+1} = (h_n)_{p_n} \end{gathered}$$

where $(h_n)_{p_n}$ is the extension of h_n such that $p_n \in \operatorname{dom}[(h_n)_{p_n}]$. The rest is the same as the proof of Theorem 4.5.10. $\square$

Selected Problems

Exercise 4.5.1

Assume that $(A_1, \leq_1)$ is similar to $(B_1, \preceq_1)$ and $(A_2, \leq_2)$ is similar to $(B_2, \preceq_2)$.

(i) Assuming $A_1 \cap A_2 = B_1 \cap B_2 = \varnothing$, the sum of $(A_1, \leq_1)$ and $(A_2, \leq_2)$ is similar to the sum of $(B_1, \preceq_1)$ and $(B_2, \preceq_2)$. (See Lemma 4.5.5.)

(ii) The lexicographic product of $(A_1, \leq_1)$ and $(A_2, \leq_2)$ is similar to the lexicographic product of $(B_1, \preceq_1)$ and $(B_2, \preceq_2)$.

Proof. Let f_1 be an isomorphism between $(A_1, \leq_1)$ and $(B_1, \preceq_1)$, and let f_2 be an isomorphism between $(A_2, \leq_2)$ and $(B_2, \preceq_2)$.

(i) $g \triangleq f_1 \cup f_2$ is an isomorphism between 'the sum of $(A_1, \leq_1)$ and $(A_2, \leq_2)$' and 'the sum of $(B_1, \preceq_1)$ and $(B_2, \preceq_2)$'.

(ii) $g : A_1 \times A_2 \hookrightarrow\!\!\!\!\rightarrow B_1 \times B_2$ defined by $(a_1, a_2) \mapsto (f_1(a_1), f_2(a_2))$ is an isomorphism between 'the lexicographic product of $(A_1, \leq_1)$ and $(A_2, \leq_2)$' and 'the lexicographic product of $(B_1, \preceq_1)$ and $(B_2, \preceq_2)$'. □

Exercise 4.5.2

Give an example of linear orderings $(A_1, \leq_1)$ and $(A_2, \leq_2)$ such that the sum of $(A_1, \leq_1)$ and $(A_2, \leq_2)$ does not have the same order type as the sum of $(A_2, \leq_2)$ and $(A_1, \leq_1)$. Do the same for lexicographic product.

Proof. Let $A = \{a, b\}$ where $a \neq b$ and $a, b \notin \mathbb{N}$ with $\preceq = \{(a,a), (a,b), (b,b)\}$.

- The sum of $(\mathbb{N}, \leq)$ and $(A, \preceq)$ has a greatest element b but the sum of $(A, \preceq)$ and $(\mathbb{N}, \leq)$ does not have a greatest element. Hence, they are not similar.
- The lexicographic product of $(\mathbb{N}, \leq)$ and $(A, \preceq)$ is isomorphic to $(\mathbb{N}, \leq)$ via the isomorphism $(n, x) \mapsto \begin{cases} 2 \cdot n & \text{if } x = a \\ 2 \cdot n + 1 & \text{if } x = b. \end{cases}$ However, $\{a\} \times \mathbb{N}$, a subset of $A \times \mathbb{N}$, is bounded above by $(b, 0)$ but it does not have a greatest element in the lexicographic product of $(A, \preceq)$ and $(\mathbb{N}, \leq)$. Hence, they are not similar. □

Exercise 4.5.3

The sum and the lexicographic product of two well-orderings are well-orderings.

Proof. Let $(A_1, \leq_1)$ and $(A_2, \leq_2)$ be well-orderings.

- Assume $A \cap B = \varnothing$. Let $(B, \leq)$ be the sum of $(A_1, \leq_1)$ and $(A_2, \leq_2)$. Take any $C \subseteq B$ with $C \neq \varnothing$. If $C \cap A_1 = \varnothing$, then $\min_{\leq} C = \min_{\leq_2} C$. Otherwise, $\min_{\leq} C = \min_{\leq_1}(C \cap A_1)$.
- Let $(A_1 \times A_2, \leq)$ be the lexicographic product of $(A_1, \leq_1)$ and $(A_2, \leq_2)$. Take any $R \subseteq A_1 \times A_2$ with $R \neq \varnothing$. Let $a_1 \triangleq \min_{\leq_1} \operatorname{dom} R$ and $a_2 \triangleq \min_{\leq_2} R[\{a_1\}]$. Then, $(a_1, a_2) = \min_{\leq} R$. □

Exercise 4.5.4

If $\langle A_i \mid i \in \mathbb{N} \rangle$ is an infinite sequence of totally ordered sets of natural numbers and $|A_i| \geq 2$ for all $i \in \mathbb{N}$, then the lexicographic ordering of $\prod_{i \in \mathbb{N}} A_i$ is *not* a well-ordering.

Proof. For each $i \in \mathbb{N}$, justified by $|A_i| \geq 2$, let $a_i \triangleq \min A_i$ and $b_i \triangleq \min(A_i \setminus \{a_i\})$. Define $X \subseteq \prod_{i \in \mathbb{N}} A_i$ by

$$X \triangleq \left\{ f \in \prod_{i \in \mathbb{N}} A_i \,\middle|\, \exists i \in \mathbb{N}, [f(i) = b_i \wedge \forall j \in \mathbb{N}, (i \neq j \implies f(j) = a_j)] \right\}.$$

Then, X, being similar to $(\mathbb{N}, \leq^{-1})$, does not have a least element. $\square$

> **Exercise 4.5.5**
>
> Let $\langle (A_i, \leq_i) \mid i \in I \rangle$ be an indexed system of mutually disjoint totally ordered sets where $I \subseteq \mathbb{N}$. The relation $\prec$ on $\bigcup_{i \in I} A_i$ defined by
>
> $$a \prec b \iff (\exists i \in I,\ a <_i b) \vee (\exists i, j \in I,\ i < j \wedge a \in A_i \wedge b \in A_j)$$
>
> is a strict total ordering. Moreover, if all $\leq_i$ are well-orderings, so is $\preceq$.

Proof.

- Assume $a \prec b$ and $b \prec c$. There exist $i, j, k \in I$ such that $a \in A_i$, $b \in A_j$ and $c \in A_k$. Then, we have $i \leq j \leq k$. If $i < j$ or $j < k$, we immediately have $a \prec c$ by definition. If $i = j = k$, by transitivity of $<_i$, we have $a \prec c$. Hence, $\prec$ is transitive in $\bigcup_{i \in I} A_i$. ✓
- Suppose $a \prec b$ and $b \prec a$ for the sake of contradiction. There exists $i, j \in I$ such that $a \in A_i$ and $b \in A_j$. We cannot have $i < j$ or $j < i$ as it contradicts one of $a \prec b$ and $b \prec a$. Hence, $i = j$ by totality of $(\mathbb{N}, \leq)$. Then, we have $a <_i b$ and $b <_i a$, which is impossible by asymmetry of $<_i$. Hence, $\prec$ is asymmetric in $\bigcup_{i \in I} A_i$. ✓
- Take any $a, b \in \bigcup_{i \in I} A_i$. There exists $i, j \in I$ such that $a \in A_i$ and $b \in A_j$. If $i \neq j$, we immediately have $a \prec b$ or $b \prec a$. If $i = j$, as $\leq_i$ is total, we have $a \leq_i b$ or $b \leq_i a$. Thus, $a \preceq b$ or $b \preceq a$. Hence, $\preceq$ is total. ✓
- Assume $\leq_i$ is a well-ordering for each $i \in \mathbb{N}$. Take any $X \subseteq \bigcup_{i \in I} A_i$ with $X \neq \varnothing$. Let $i_0 \triangleq \min\{i \in I \mid A_i \cap X \neq \varnothing\}$, thanks to $(\mathbb{N}, \leq)$ is Well-Ordered and X being nonempty. Then, let $a \triangleq \min_{\leq_{i_0}}(A_{i_0} \cap X)$, which exists as $\leq_{i_0}$ is a well-ordering. Then, $a = \min_{\preceq} X$. ✓ $\square$

> **Exercise 4.5.7**
>
> Let $\preceq$ be the lexicographical ordering of $\mathbb{N}^{\mathbb{N}}$ (where $\mathbb{N}$ is ordered in the usual way) and let $P \subseteq \mathbb{N}^{\mathbb{N}}$ be the set of all eventually periodic, but not eventually constant, sequences of natural numbers. (See Exercises 4.3.6 and 4.3.7 for the definitions.) Then, $(P, \preceq \cap P^2)$ is a countably infinite dense totally ordered set without endpoints.

Proof. We already have $\preceq \cap P^2$ is a total ordering.

> ***Claim 1.*** P is countably infinite.
>
> ***Proof.*** As P is a subset of the set of all eventually periodic sequences, by Exercises 4.1.3 and 4.3.7, $|P| \leq \aleph_0$. We may define an injective infinite sequence into P recursively by
>
> $$\begin{aligned} g_0 &= \langle 0, 1, 0, 1, \cdots \rangle \\ \forall n \in \mathbb{N}, \quad g_{n+1} &= \langle n+1, a_0, a_1, \cdots \rangle \\ &\quad \text{where } g_n = \langle a_0, a_1, \cdots \rangle. \end{aligned}$$
>
> Hence, $\aleph_0 \leq |P|$; thus $|P| = \aleph_0$ by Cantor–Bernstein Theorem. $\square$

> ***Claim 2.*** $(P, \preceq \cap P^2)$ is dense.
>
> ***Proof.*** Take any $f, g \in P$ with $f \prec g$. Then, $f_{i_0} < g_{i_0}$ where $i_0 = \min\{i \in \mathbb{N} \mid f_i \neq g_i\}$.

Define $h \in \mathbb{N}^{\mathbb{N}}$ by

$$h_i \triangleq \begin{cases} f_i & \text{if } i \leq i_0 \\ f_i + 1 & \text{otherwise.} \end{cases}$$

Then, it is evidently $f \prec h \prec g$.

There exist $n_0 \in \mathbb{N}$ and $p > 0$ such that $\forall n \geq n_0, f_{n+p} = f_n$. Let $n_0' \triangleq \max\{n_0, i_0 + 1\}$. Then, for each $n \geq n_0'$, we have $h_{n+p} = f_{n+p} + 1 = f_n + 1 = h_n$; thus $h \in P$. Hence, $(P, \preceq \cap P^2)$ is dense. □

Claim 3. $(P, \preceq \cap P^2)$ has no endpoints.

Proof. Fix any $f \in P$. Then, we may define $g \in \mathbb{N}^{\mathbb{N}}$ by $\forall n \in \mathbb{N}, g_n = f_n + 1$. It is easy to show that $f \prec g$ and $g \in P$. Hence, $(P, \preceq \cap P^2)$ has no greatest element.

We may also define $h \in \mathbb{N}^{\mathbb{N}}$ by

$$\forall n \in \mathbb{N},\ h_n = \begin{cases} 0 & \text{if } n = 0 \\ f_{n-1} & \text{otherwise.} \end{cases}$$

As f is not eventually constant, $f \neq h$ and we may let $i_0 \triangleq \min\{i \in \mathbb{N} \mid f_i \neq 0\}$. As $\forall i < i_0, f_i = 0$, $\min \operatorname{diff}(f, h) = i_0$. Since $0 = h_{i_0} < f_{i_0}$, $h \prec f$. Thus, $(P, \preceq \cap P^2)$ has no least element. □

Combining Claims 1 to 3 gives the desired result. □

Exercise 4.5.11

Let $(A, \preceq)$ be a dense totally ordered set. Show that for all $a, b \in A$ such that $a \prec b$, the *closed interval* $[a, b] \triangleq \{x \in A \mid a \preceq x \preceq b\}$ is infinite.

Proof. Assume there are some $a, b \in A$ such that $a \prec b$ and $I = [a, b]$ is finite. Let $|I| = n$. (Since $a, b \in I$, $n \geq 2$.) Then, by Theorem 4.5.3, there exists an isomorphism $h \colon n \hookrightarrow\!\!\!\!\rightarrow I$ between $(n, \leq \cap n^2)$ and $(I, \preceq \cap I^2)$. Then, $\exists i < n$, $h(0) \prec h(i) \prec h(1)$ as $(A, \preceq)$ is dense. However, there does not exist $i \in \mathbb{N}$ with $0 < i < 1$ by Exercise 3.1.1, which is a contradiction. □

Exercise 4.5.12

Let $(P, \preceq)$ and $(Q, \leq)$ be countably infinite dense totally ordered sets with both endpoints. Then, $(P, \preceq)$ and $(Q, \leq)$ are similar.

Proof. Define the following:

$$\begin{array}{ll} p \triangleq \min_{\preceq} P & p' \triangleq \max_{\preceq} P \\ q \triangleq \min_{\leq} Q & q' \triangleq \max_{\leq} Q \\ P_0 \triangleq P \setminus \{p, p'\} & Q_0 \triangleq Q \setminus \{q, q'\}. \end{array}$$

Then, $(P_0, \preceq \cap P_0^2)$ and $(Q_0, \preceq \cap Q_0^2)$ are countably infinite dense totally ordered sets without endpoints. Hence, by Theorem 4.5.10, we have an isomorphism $h \colon P_0 \hookrightarrow\!\!\!\!\rightarrow Q_0$ between them. Then, $h' \cup \{(p, q), (p', q')\}$ is an isomorphism between $(P, \preceq)$ and $(Q, \leq)$. □

Chapter 5

Cardinal Numbers

5.1 Cardinal Arithmetic

Definition 5.1.1: 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 $|A \times B| = \kappa \cdot \lambda$.

These are justified by Exercise 4.3.1 (i) and (ii).

Lemma 5.1.2

If $|A_1| = |A_2|$ and $|B_1| = |B_2|$, then $\left|A_1^{B_1}\right| = \left|A_2^{B_2}\right|$.

Proof. Let $f : A_1 \hookrightarrow\!\!\!\!\!\rightarrow A_2$ and $g : B_1 \hookrightarrow\!\!\!\!\!\rightarrow B_2$. Define $F : A_1^{B_1} \to A_2^{B_2}$ by $k \mapsto f \circ k \circ g^{-1}$. Then, F is one-to-one and onto.

$$\begin{tikzcd} B_1 \arrow[r, "g"] \arrow[d, "k"] & B_2 \arrow[d, "F(k)=f\circ k\circ g^{-1}"] \\ A_1 \arrow[r, "f"] & A_2 \end{tikzcd}$$

□

Definition 5.1.3: Exponentiation of Two Cardinals

Let $|A| = \kappa$ and $|B| = \lambda$. We write $\kappa^\lambda = \left|A^B\right|$. This is justified by Lemma 5.1.2.

Note:-

Here are some direct facts regarding sum, product, and exponentiation of cardinal numbers.

(i) $\kappa + \lambda = \lambda + \kappa$.
(ii) $\kappa + (\lambda + \mu) = (\lambda + \kappa) + \mu$.
(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) $\kappa \cdot (\lambda \cdot \mu) = (\lambda \cdot \kappa) \cdot \mu$.
(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 5.1.4

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 $L \cap N = \varnothing$. Then, we may define $F : K^L \times K^M \hookrightarrow\!\!\!\!\!\rightarrow K^{L \cup M}$ by $(f, g) \mapsto f \cup g$.
(ii) Define $F : (K^L)^M \hookrightarrow\!\!\!\!\!\rightarrow K^{L \times M}$ by $f \mapsto \left\{ \left((\ell, m), f_m(\ell)\right) \,\middle|\, m \in M,\ \ell \in L \right\}$.
(iii) Define $F : K^M \times L^M \hookrightarrow\!\!\!\!\!\rightarrow (K \times L)^M$ by $(f_1, f_2) \mapsto \left\{ \left(m, (f_1(m), f_2(m))\right) \,\middle|\, m \in M \right\}$. □

Theorem 5.1.5 Cantor's Theorem

$\forall X,\ |X| < |\mathcal{P}(X)|$

Proof. The function $f : X \to \mathcal{P}(X)$ defined by $f(x) = \{x\}$ is injective, and we have $|X| \leq |\mathcal{P}(X)|$.

We now show that there exists no function on X onto $\mathcal{P}(X)$. Let $f : X \to \mathcal{P}(X)$ be arbitrary. Define $S \triangleq \{x \in X \mid x \notin f(x)\}$ and suppose there exists $z \in X$ such that $f(z) = S$ for the sake of contradiction. Then, we have $z \in S$ if and only if $z \notin f(z) = S$. Therefore, f is not onto $\mathcal{P}(X)$. □

Theorem 5.1.6

$\forall X,\ |\mathcal{P}(X)| = 2^{|X|}$

Proof. For each $S \subseteq \mathbb{N}$, define the *characteristic function* of S, $\chi_S : X \to \{0, 1\}$ by

$$\chi_S(n) \triangleq \begin{cases} 0 & \text{if } n \in S \\ 1 & \text{if } n \notin S. \end{cases}$$

Then, we define $F : \mathcal{P}(X) \hookrightarrow\!\!\!\!\!\rightarrow 2^X$ by $S \mapsto \chi_S$. □

Corollary 5.1.7

$\forall S,\ \exists Y,\ \forall X \in S,\ |X| < |Y|$

Proof. Take any S. Then, let $Y \triangleq \mathcal{P}\left(\bigcup S\right)$. By Theorem 5.1.5 and Exercise 4.1.3, $|Y| > \left|\bigcup S\right| \geq |X|$ for all $X \in S$. □

Selected Problems

Exercise 5.1.4

For every cardinal number κ, $\kappa^\kappa \le 2^{\kappa \cdot \kappa}$.

Proof. As $\kappa \le 2^\kappa$, we have $\kappa^\kappa \le (2^\kappa)^\kappa = 2^{\kappa \cdot \kappa}$ by Theorem 5.1.4 (ii). ☐

Exercise 5.1.5

If $|A| \le |B|$ and $A \ne \varnothing$, 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

$$f(b) \triangleq \begin{cases} g^{-1}(b) & \text{if } b \in \operatorname{ran} g \\ a & \text{otherwise.} \end{cases}$$

☐

Exercise 5.1.6

If there exists $g : B \twoheadrightarrow A$, then $2^{|A|} \le 2^{|B|}$.

Proof. Let $g : B \twoheadrightarrow A$. Define $f : \mathcal{P}(A) \to \mathcal{P}(B)$ by $X \mapsto g^{-1}[X]$. Then, f is injective. ☐

Definition 5.1.8: Dedekind Infinite Set

- A set X is called *Dedekind infinite* if there exists an injection on X onto its proper subset.
- A set X is called *Dedekind finite* if X is not Dedekind infinite.

Exercise 5.1.8

A Dedekind infinite set is infinite.

Proof. Let X be a set and let $f : X \hookrightarrow X$ with $f[X] \subsetneq X$. Suppose $|X| = n$ for some $n \in \mathbb{N}$ for the sake of contradiction. Then, $|f[X]| = |X| = n$ as f is injective, but this is impossible by Lemma 4.2.2. ☐

Exercise 5.1.9

Every countably infinite set is Dedekind infinite.

Proof. It is enough to show that $\mathbb{N}$ is Dedekind infinite. By Exercise 3.2.2, $f : \mathbb{N} \to \mathbb{N}$ defined by $n \mapsto n+1$ is injective but $0 \notin \operatorname{ran} f$. Hence, $\mathbb{N}$ is Dedekind infinite. ☐

Exercise 5.1.10

If X has a countably infinite subset, then X is Dedekind infinite.

Proof. Let $Y \subseteq X$ and $|Y| = \aleph_0$. By Exercise 5.1.9, there exists $f : Y \hookrightarrow Y$ such that $\operatorname{ran} f \subsetneq Y$. Let $g \triangleq f \cup \operatorname{Id}_{X \setminus Y}$. Then, $g : X \hookrightarrow X$ and $Y \setminus \operatorname{ran} f \subseteq X \setminus \operatorname{ran} g$. Therefore, X is Dedekind infinite. ☐

Exercise 5.1.11

If X is Dedekind infinite, then X has a countably infinite subset.

Proof. Let $f : X \hookrightarrow X$ with $\operatorname{ran} f \subsetneq X$. Fix any $x \in X \setminus \operatorname{ran} f$. Define $\langle x_n \rangle_{n\in\mathbb{N}}$ by

$$\begin{aligned} x_0 &\triangleq x \\ \forall n \in \mathbb{N}, \quad x_{n+1} &\triangleq f(x_n). \end{aligned}$$

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 $x_0 \notin \operatorname{ran} f$.

Fix $n \geq 1$ and assume $\mathbf{P}(n)$ for the sake of induction. Then, for each $0 < m < n$, $x_n = f(x_{n-1}) \neq f(x_{m-1}) = x_m$ as f is injective. $x_0 \neq x_n$ since $x_0 \notin \operatorname{ran} f$. Hence, $\mathbf{P}(n+1)$ holds. By The Induction Principle, $\langle x_n \rangle_{n\in\mathbb{N}}$ is injective, and thus $\{x_n \mid n \in \mathbb{N}\}$ is a countably infinite subset of X. $\square$

Note:-

Exercise 5.1.10 and Exercise 5.1.11 say that X is Dedekind infinite if and only if X has a countably infinite subset. In Chapter 8, we will show that a set is Dedekind infinite if and only if it is infinite using The Axiom of Choice. (See Theorem 8.1.5.)

Exercise 5.1.12

If A and B are Dedekind finite, then $A \cup B$ is Dedekind finite.

Proof. Suppose $A \cup B$ is Dedekind infinite for the sake of contradiction. Then, by Exercise 5.1.11, there exists $C \subseteq A \cup B$ such that C is countably infinite. Noting that at least one of $A \cap C$ and $B \cap C$ is countably infinite, by Exercise 5.1.10, we conclude A or B is Dedekind infinite, which is a contradiction. $\square$

Exercise 5.1.13

If A and B are Dedekind finite, then $A \times B$ is Dedekind finite.

Proof. Suppose $A \times B$ is Dedekind infinite for the sake of contradiction. Then, by Exercise 5.1.11, 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 A' and B' were both finite, then $C \subseteq A' \times B'$ would be finite by Exercise 4.2.2 and Theorem 4.2.4.

WLOG, A' is infinite. Let $f : \mathbb{N} \twoheadrightarrow C$. Then, define $g : \mathbb{N} \twoheadrightarrow A'$ by $n \mapsto a'$ where $(a', b') = f(n)$. Hence, by Theorem 4.3.5, $\operatorname{ran} g = A'$ is countably infinite. Therefore, by Exercise 5.1.10, A is Dedekind infinte, which is a contradiction. $\square$

Chapter 6

Ordinal Numbers

6.1 Well-Ordered Sets

Notation 6.1.1

Let $\omega \triangleq \mathbb{N}$ be the least transfinite number. We let $\omega+0=\omega$ and $\omega+(n+1)=S(\omega+n)$ for each $n \in \mathbb{N}$. In this fashion, one may let

$$\omega \cdot 2=\omega+\omega=\{0,1,2,\cdots,\omega,\omega+1,\omega+2,\cdots\},$$

$$\omega \cdot \omega=\{0,1,\cdots,\omega,\omega+1,\cdots,\omega \cdot 2,\cdots,\omega \cdot 3,\cdots\}.$$

These sets are totally ordered by $\in$, and the ordering is a well-ordering.

Definition 6.1.2: 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. If $a \in W$, we call the set

$$W[a] \triangleq \{x \in W \mid x<a\}$$

the *initial segment of W given by a*.

Lemma 6.1.3

If $(W,\leq)$ is a well-ordered set, and if S is an initial segment of $(W,\leq)$, then there exists $a \in W$ such that $S=W[a]$.

Proof. Let $X \triangleq W \setminus S$. As $X \neq \varnothing$, there exists $a \triangleq \min X$. If $x<a$, then $x \notin X$, and thus $x \in S$. Conversely, if $x \geq a$, then $x \in S$ would imply $a \in S$, and thus $x \in X$. Hence, $x \in S \iff x<a$. □

Definition 6.1.4: Increasing Function

A function f on a totally ordered set $(L,\leq)$ into L is *strictly increasing* if

$$\forall x_1,x_2 \in L,\ (x_1<x_2 \implies f(x_1)<f(x_2)).$$

Note:-

Every automorphism of a totally ordered set is strictly increasing.

Lemma 6.1.5

If $(W, \leq)$ is a well-ordered set and if $f : W \to W$ is a strictly increasing function, then $\forall x \in W$, $x \leq f(x)$.

Proof. Suppose $X \triangleq \{x \in W \mid f(x) > x\}$ is nonempty for the sake of contradiction. Let $a = \min X$. Then, $f(a) < a$, and $f(f(a)) < f(a)$ as f is strictly increasing. Hence, $f(a) \in X$ even though $f(a) < a$, which is a contradiction. □

Corollary 6.1.6

(i) No well-ordered set is isomorphic to an initial segment of itself.
(ii) Id_W is the unique automorphism of a well-ordered set $(W, \leq)$.
(iii) If W_1 and W_2 are isomorphic well-ordered sets, then the isomorphism between W_1 and W_2 is unique.

Proof.

(i) Suppose $f : W \to W[a]$ is an isomorphism for some $a \in W$ for the sake of contradiction. Then, $f(a) \in W[a]$ and therefore $f(a) < a$, which contradicts Lemma 6.1.5.
(ii) Let f be an automorphism of W. Then, both f and f^{-1} are strictly increasing functions, and thus by Lemma 6.1.5, for all $x \in W$, $f(x) \geq w$ and $f^{-1}(x) \geq x$. Hence, $x \geq f(x)$. Therefore, $f(x) = x$ for all $x \in W$ due to antisymmetry.
(iii) If f and g are isomorphisms between W_1 and W_2, then $f \circ g^{-1}$ is an automorphism of W_2. Then, by (ii), $f \circ g^{-1} = \mathrm{Id}_{W_2}$; thus $f = g$. □

Theorem 6.1.7

If $(W_1, \leq_1)$ and $(W_2, \leq_2)$ are 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. (i), (ii), and (iii) are mutually exclusive by Corollary 6.1.6 (i). Also, the uniqueness follows from Corollary 6.1.6 (iii). Hence, we only need to show at least one of them holds. Define $f \triangleq \{(x, y) \in W_1 \times W_2 \mid W_1[x] \text{ is isomorphic to } W_2[y]\}$.

Claim 1. f is an injective function.

Proof. First of all, f is a function since, if $W_1[x]$ is isomorphic to $W_2[y]$ and $W_2[y']$, then $y = y'$ (otherwise, one would be an initial segment of the other). By symmetry, f is injective. □

Claim 2. f is strictly increasing.

Proof. Take $x, x' \in W_1$ with $x <_1 x'$. If h is the isomorphism between $W_1[x']$ and $W_2[f(x')]$, then $h|_{W_1[x]}$ is an isomorphism between $W_1[x]$ and $W_2[h(x)]$. Hence, by Claim 1, $f(x) = h(x) <_2 f(x')$. □

By Claim 2 and Lemma 2.5.15, f is an isomorphism between $\operatorname{dom} f$ and $\operatorname{ran} f$. Claim 3 completes the proof.

> ***Claim 3.*** If $\operatorname{dom} f \neq W_1$, then $\operatorname{ran} f = W_2$.
>
> ***Proof.*** Let $S \triangleq \operatorname{dom} f$. If $z < x$ and $x \in S$, then by the same argument in the proof of Claim 2, $z \in S$. Hence, S is an initial segment of W_1.
>
> Suppose $T \triangleq \operatorname{ran} f \neq W_2$ for the sake of contradiction. Then, by the same argument, T is an initial segment of W_2. $S = W_1[a]$ and $T = W_2[b]$ for some $a \in W_1$ and $b \in W_2$ by Lemma 6.1.3; in other words, $(a, b) \in f$, or $a \in \operatorname{dom} f = W_1[a]$, which is impossible.

By symmetry, if $\operatorname{ran} f \neq W_2$, we must have $\operatorname{dom} f = W_1$. □

Definition 6.1.8

Let $(W_1, \leq_1)$ and $(W_2, \leq_2)$ be well-ordered sets. We say W_1 has *smaller order type* than W_2 if W_1 is isomorphic to an initial segment of W_2.

Note:-

By Theorem 6.1.7, for two well-ordered sets, if they are not isomorphic, then one of them has smaller order type than the other.

Selected Problems

Exercise 6.1.1

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. If $(L, \leq)$ is dense and $\ell \in L$, then $S \triangleq \{x \in L \mid x \leq \ell\}$ is never equal to $\{x \in L \mid x < a\}$ where $a \in L$. For if they are equal, there exists $x \in L$ such that $\ell < x < a$ and such x is not in S. One example would be $(\mathbb{Q}, \leq)$ and $S = \{x \in \mathbb{Q} \mid x \leq 0\}$. □

Exercise 6.1.2

$\omega + 1$ is not isomorphic to ω (in the well-ordering by $\in$).

Proof. ω is an initial segment of $\omega + 1$, and thus they are not isomorphic by Corollary 6.1.6 (i). □

Exercise 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 $|\mathcal{P}(\mathbb{N}^2)| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$ by Theorems 4.3.6 and 5.1.6. Hence, $|S| \leq 2^{\aleph_0}$.

Let $T \triangleq \{f \in \mathbb{N}^{\mathbb{N}} \mid f : \mathbb{N} \hookrightarrow\!\!\!\rightarrow \mathbb{N}\}$. Define $F : T \to \mathcal{P}(\mathbb{N}^2)$ by $f \mapsto \{(f(m), f(n)) \mid m, n \in \mathbb{N} \wedge m \leq n\}$. Then, for each $f \in T$, $(\mathbb{N}, \leq)$ and $(\mathbb{N}, F(f))$ is an isomorphism, thus F is into S. For each $R \in S$, there exists one and only $f \in T$ defined by $f_n = \min_R \left(\mathbb{N} \setminus f\big|_n\right)$ for all $n \in \mathbb{N}$. Hence, $|T| = |S|$.

Now, define $\sigma : \mathcal{P}(\mathbb{N}) \to T$ by

$$\sigma_X(2\cdot n) = \begin{cases} 2\cdot n & \text{if } n \notin X \\ 2\cdot n+1 & \text{if } n \in X \end{cases} \quad \text{and} \quad \sigma_X(2\cdot n+1) = \begin{cases} 2\cdot n+1 & \text{if } n \notin X \\ 2\cdot n & \text{if } n \in X \end{cases}$$

for each $n \in \mathbb{N}$. It is evident that σ is injective; hence $|T| \geq |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$. By Cantor–Bernstein Theorem, $|S| = |T| = 2^{\aleph_0}$. □

Exercise 6.1.4

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. Noting that every initial segment of A and $\mathbb{N}$ is finite, Theorem 6.1.7 leaves only one option—A and $\mathbb{N}$ are isomorphic. □

6.2 Ordinal Numbers

Definition 6.2.1: 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 6.2.2: 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 6.2.3

We write $\alpha \in \mathrm{Ord}$ instead of "α is an ordinal number." This is just a syntactic sugar, not implying Ord is the set of all ordinals, which does not exist by Theorem 6.2.13 (v).

Note:-

Every natural number is an ordinal. ($(\mathbb{N}, \leq)$ is Well-Ordered)

Definition 6.2.4

$\omega \triangleq \mathbb{N}$. (Notation 6.1.1)

Lemma 6.2.5

If α is an ordinal number, then $S(\alpha)$ is also an ordinal number.

Proof. As α is transitive, $S(\alpha) = \alpha \cup \{\alpha\}$ is transitive. Moreover, $S(\alpha)$ is well-ordered by $\in_{S(\alpha)}$ as $(\alpha, \in_\alpha)$ is well-ordered. □

Notation 6.2.6

We denote the successor of α by $\alpha + 1$.

Definition 6.2.7: Successor Ordinal and Limit Ordinal

Let $\alpha \in \mathrm{Ord}$.
- α is called a *successor ordinal* if $\alpha = \beta + 1$ for some $\beta \in \mathrm{Ord}$.
- Otherwise, α is called a *limit ordinal*.

Definition 6.2.8

For all ordinals α and β, we define $\alpha < \beta$ if and only if $\alpha \in \beta$.

Lemma 6.2.9

$\forall \alpha \in \mathrm{Ord},\ \alpha \notin \alpha$

Proof. If $\alpha \in \alpha$, then it will contradict the asymmetry of $<_\alpha$. □

Lemma 6.2.10

$\forall \alpha \in \mathrm{Ord},\ \forall x \in \alpha,\ x \in \mathrm{Ord}$

Proof. Take any $x \in \alpha$.
- To show x is transitive, let $u \in v \in x$. As α is transitive, we have $v \in \alpha$, and therefore $u \in \alpha$ by the same reason. Then, as $\in_\alpha$ is transitive in α, $u \in x$. ✓
- As α is transitive, $x \subseteq \alpha$. Therefore, $\in_x = \in_\alpha \cap x^2$. As $\in_\alpha$ is a well-ordering, so is $\in_x$. ✓ □

Corollary 6.2.11

Let α be an ordinal number. Then, $\alpha = \{\beta \mid \beta \text{ is an ordinal number with } \beta < \alpha\}$.

Lemma 6.2.12

Let α and β be ordinal numbers. Then $\alpha \subsetneq \beta \iff \alpha \in \beta$.

Proof.

($\Rightarrow$) $\beta \setminus \alpha$ is nonempty, and thus there exists $\gamma \triangleq \min_{\in_\beta}(\beta \setminus \alpha)$. Note that, any $\delta \in \gamma \setminus \alpha$ would be an element of $\beta \setminus \alpha$ less than γ, which contradicts the minimality of γ. Hence, $\gamma \setminus \alpha = \varnothing$, i.e., $\gamma \subseteq \alpha$.

Now we claim that $\alpha \subseteq \gamma$ and thus $\alpha = \gamma \in \beta$. Take any $\delta \in \alpha$ and suppose $\delta \notin \gamma$ for the sake of contradiction. As $\in_\beta$ is a total ordering, it is either $\gamma \in \delta$ or $\gamma = \delta$. In both cases, as $\in_\beta$ is transitive, $\gamma \in \alpha$, which contradicts $\gamma \in \beta \setminus \alpha$.

($\Leftarrow$) Take any $\gamma \in \alpha$. Then, as β is transitive, we have $\gamma \in \beta$ as well. Hence, $\alpha \subseteq \beta$. Since $\alpha \neq \beta$ by Lemma 6.2.9, we conclude $\alpha \subsetneq \beta$. □

Theorem 6.2.13

Let α, β, and γ be ordinal numbers.

(i) $\alpha < \beta \wedge \beta < \gamma \implies \alpha < \gamma$
(ii) $\neg(\alpha < \beta \wedge \beta < \alpha)$
(iii) $(\alpha < \beta) \vee (\alpha = \beta) \vee (\beta < \alpha)$
(iv) Every nonempty set of ordinal numbers has a $\leq$-least element.
(v) For every set X of ordinal numbers, $\exists \alpha' \in \mathrm{Ord},\ \alpha' \notin X$.

Proof.

(i) The result follows as γ is transitive.

(ii) If $\alpha \in \beta \in \alpha$, as α is transitive, we have $\alpha \in \alpha$, which contradicts Lemma 6.2.9.

(iii) Let $\gamma \triangleq \alpha \cap \beta$. If $\alpha = \beta$, then $\gamma = \alpha$ is an ordinal. If $\alpha \neq \beta$, then we have either $\gamma \subsetneq \alpha$ or $\gamma \subseteq \beta$; hence γ is an ordinal by Lemmas 6.2.10 and 6.2.12.

We have three cases: $\gamma = \alpha$, $\gamma = \beta$, or $\gamma \subsetneq \alpha \wedge \gamma \subsetneq \beta$. The last case is not possible since we have $\gamma \in \alpha$ and $\gamma \in \beta$ by Lemma 6.2.12, which implies $\gamma \in \alpha \cap \beta = \gamma$ that contradicts Lemma 6.2.9. The first two cases lead to one of $\alpha = \beta$, $\alpha \in \beta$, and $\beta \in \alpha$ by Lemma 6.2.12.

(iv) Let A be a nonempty set of ordinals. Fix any $\alpha \in A$. If $\alpha \cap A = \varnothing$, then by (iii), $\alpha = \min_{\leq} A$. If $\alpha \cap A \neq \varnothing$, then $\alpha \cap A \subseteq \alpha$ has $\beta \triangleq \min_{\in_\alpha} A$, which is a $\leq$-minimal element of A.

(v) Let X be a set of ordinal numbers. Then, $\bigcup X$ is transitive by Exercise 6.2.5. Moreover, (iv) implies that $\in$ well-orders $\bigcup X$. Hence, $\bigcup X$ is an ordinal.

Let $\alpha \triangleq S\left(\bigcup X\right)$. α is an ordinal by Lemma 6.2.5. Suppose $\alpha \in X$ for the sake of contradiction. Then, $\alpha \subseteq \bigcup X$; which implies $\alpha = \bigcup X$ or $\alpha \in \bigcup X$ by Lemma 6.2.12. In both cases, $\alpha \in S\left(\bigcup X\right) = \alpha$, which contradicts Lemma 6.2.9. □

Note:-

Theorem 6.2.13 (v) insists that:
- There is no set of all ordinals.
- For each set of ordinals X, $\bigcup X$ is an ordinal. (See the proof.)

Definition 6.2.14: Supremum of a Set of Ordinals

If X is a set of ordinal numbers, $\bigcup X$ is the *supremum* of X and is denoted $\sup X$.

Note:-

Definition 6.2.14 is justified the fact that:

(i) If $\alpha \in X$, then $\alpha \in \bigcup X$, and thus $\alpha \subseteq \bigcup X$, i.e., $\alpha \leq \bigcup X$, as $\bigcup X$ is an ordinal.

(ii) If $\forall \alpha \in X$, $\alpha \leq \gamma$, i.e., $\forall \alpha \in X$, $\alpha \subseteq \gamma$, then $\bigcup X \subseteq \gamma$, i.e, $\bigcup X \leq \gamma$.

Note:-

Let $\alpha \in \mathrm{Ord}$. If $x \in \bigcup \alpha$, then $x \in y \in \alpha$ for some y, and thus $x \in \alpha$ as α is transitive. Hence, $\bigcup \alpha \subseteq \alpha$.

Theorem 6.2.15

An ordinal α is finite if and only if $\alpha \in \mathbb{N}$.

Proof.

($\Rightarrow$) Let α be an ordinal such that $\alpha \notin \mathbb{N}$. Then, by Theorem 6.2.13 (iii), $\omega \subseteq \alpha$; thus α is not finite. □

Selected Problems

Exercise 6.2.1

A set X is transitive if and only if $X \subseteq \mathcal{P}(X)$.

Proof. X is transitive iff every $x \in X$ is a subset of X iff every $x \in X$ is an element of $\mathcal{P}(X)$ iff $X \subseteq \mathcal{P}(X)$. □

Exercise 6.2.2

A set X is transitive if and only if $\bigcup X \subseteq X$.

Proof.
($\Rightarrow$) Take any $u \in \bigcup X$. There exists some $x \in X$ such that $u \in x$. As X is transitive, $u \in X$. Hence, $\bigcup X \subseteq X$.
($\Leftarrow$) Let $u \in v \in X$. Then, $u \in \bigcup X \subseteq X$. Hence, X is transitive. $\square$

Exercise 6.2.4

(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 $S \subseteq \mathcal{P}(Y)$, then $Y \cup S$ is transitive.
(iv) There exist X and Y such that $X \in Y$, Y is transitive, but X is not transitive.
(v) There exist X and Y such that $X \subseteq Y$, Y is transitive, but X is not transitive.

Proof.
(i) $\bigcup(X \cup Y) = \left(\bigcup X\right) \cup \left(\bigcup Y\right) \subseteq X \cup Y$ by Exercise 6.2.2. Hence, $X \cup Y$ is transitive.
(ii) $\bigcup(X \cap Y) \subseteq \left(\bigcup X\right) \cap \left(\bigcup Y\right) \subseteq X \cup Y$ by Exercise 6.2.2. Hence, $X \cap Y$ is transitive.
(iii) Let $u \in v \in Y \cup S$. If $v \in Y$, then $u \in Y \subseteq Y \cup S$ as Y is transitive. If $v \in S$, then $u \in v \subseteq Y$. Hence, $Y \cup S$ is transitive.
(iv) Let $Y \triangleq \{\varnothing, \{\varnothing\}, X\}$ where $X \triangleq \{\{\varnothing\}\}$. Then, $\bigcup Y = \{\varnothing, \{\varnothing\}\} \subseteq Y$; Y is transitive by Exercise 6.2.2. However, $\bigcup X = \{\varnothing\} \nsubseteq X$; X is not transitive.
(v) Let $X \triangleq \{\{\varnothing\}\}$ and $Y \triangleq \{\varnothing, \{\varnothing\}\}$. Then, $\bigcup Y = \{\varnothing\} \subseteq Y$; Y is transitive by Exercise 6.2.2. X is not transitive as in (iii). $\square$

Exercise 6.2.5

If every $X \in S$ is transitive, then $\bigcup S$ is transitive.

Proof. Let $u \in v \in \bigcup S$. Then, $v \in X$ for some $X \in S$. As X is transitive, then $u \in X \subseteq \bigcup S$; hence $\bigcup S$ is transitive. $\square$

Exercise 6.2.6

An ordinal α is a natural number if and only if every nonempty subset of α has a greatest element.

Proof.
($\Rightarrow$) If $\alpha \in \mathbb{N}$, then α is a finite set of natural numbers. Hence, if $\varnothing \subsetneq X \subseteq \alpha$, by Theorem 4.2.4, X is also finite. Then, by Exercise 3.5.13, X has a greatest element.
($\Leftarrow$) Suppose $\alpha \notin \mathbb{N}$ for the sake of contradiction. By Theorem 6.2.15, $\omega \leq \alpha$. However, ω does not have a greatest element. $\square$

Exercise 6.2.7

If a set of ordinals X does not have a greatest element, then $\sup X$ is a limit ordinal.

Proof. $\sup X \notin X$; otherwise $\sup X$ would be a greatest element of X. Suppose $\sup X$ is a successor ordinal for the sake of contradiction, i.e., $\bigcup X = \beta + 1$ for some ordinal β.

Take any $\alpha \in X$. Then, $\alpha \leq \beta + 1$ but α cannot equal $\beta + 1 = \sup X$. As $\neg(\beta < \alpha < \beta + 1)$ and $<$ totally orders X, we get $\alpha \leq \beta$, which contradicts the minimality of $\sup X$. $\square$

Exercise 6.2.8

If X is a nonempty set of ordinals, then $\bigcap X \in \mathrm{Ord}$, and $\bigcap X$ is a least element of X.

Proof. Let $m \triangleq \bigcap X$. Let $u \in v \in m$. Then, $\forall \alpha \in X$, $u \in v \in \alpha$. As each $\alpha \in X$ is ordinal, $\forall \alpha \in X$, $u \in \alpha$, i.e., $u \in m$. Hence, m is transitive. Moreover, by Theorem 6.2.13 (iv), m is well-ordered by $\in$. Hence, m is an ordinal.

Let $m' \triangleq m+1$. Suppose $\forall \alpha \in X$, $m' \leq \alpha$ for the sake of contradiction. Then, $m' \leq m$, which is a contradiction. Hence, there exists $\alpha \in X$ such that $m \leq \alpha < m'$. Then, by Exercise 3.1.1, $\alpha = m$; thus $m \in X$. Therefore, $m = \min X$. □

6.3 The Axiom Schema of Replacement

We lack some tools to guarantee the existence of some sets that look harmless. For example, you might want to construct a sequence

$$\langle \varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \cdots \rangle$$

with the help of The Recursion Theorem, but it requires an existence of set such to which every element of the sequence belongs. However, we do not have enough axioms to prove the existence. To get through this difficulty, The Axiom Schema of Replacement comes to rescue.

Axiom VIII The Axiom Schema of Replacement

Let $\mathbf{P}(x,y)$ be a property such that $\forall x\, \exists! y\, \mathbf{P}(x,y)$. For every set A, there exists a set B such that, for every $x \in A$, there exists $y \in B$ for which $\mathbf{P}(x,y)$ holds.

$$\forall x \exists! y \mathbf{P}(x,y) \implies \forall A \exists B \forall x \big[x \in A \implies \exists y [y \in B \land \mathbf{P}(x,y)] \big]$$

Definition 6.3.1: Operation

Let $\mathbf{P}(x,y)$ be a property such that $\forall x\, \exists! y\, \mathbf{P}(x,y)$. $\mathbf{F}$ is the *operation defined by* $\mathbf{P}$ when $\mathbf{F}(x)$ denotes the unique y for which $\mathbf{P}(x,y)$.

Note:-

Let $\mathbf{P}(x,y)$ be a property such that $\forall x\, \exists! y\, \mathbf{P}(x,y)$ and let $\mathbf{F}$ be the operation defined by $\mathbf{P}$. Let A be a set. The Axiom Schema of Replacement guarantees the existence of the set

$$\{\, y \mid \exists x \in A,\ \mathbf{P}(x,y) \,\} = \{\, y \mid \exists x \in A,\ y = \mathbf{F}(x) \,\}.$$

Notation 6.3.2: Image

Let $\mathbf{P}(x,y)$ be a property such that $\forall x\, \exists! y\, \mathbf{P}(x,y)$ and let $\mathbf{F}$ be the operation defined by $\mathbf{P}$. Then, we write $\mathbf{F}[A] \triangleq \{\, \mathbf{F}(x) \mid x \in A \,\}$ instead of $\mathbf{F}[A] = \{\, y \mid \exists x \in A,\ y = \mathbf{F}(x) \,\}$.

Theorem 6.3.3 The Counting Theorem

For every well-ordered set $(W, \preceq)$, $\exists! \alpha \in \mathrm{Ord}$, $(W, \preceq) \cong \alpha$.

Proof. Let α and β be two distinct ordinal numbers with $\alpha < \beta$. Then, $\alpha = \{\gamma \in \beta \mid \gamma < \alpha\} = \beta[\alpha]$ (Corollary 6.2.11 and Lemma 6.2.10) is an initial segment of β; thus α and β are not isomorphic by Corollary 6.1.6 (i). Hence, the uniqueness follows.

Let $A \triangleq \{a \in W \mid W[a]$ is isomorphic to some ordinal number$\}$. By the same reason as above, for each $a \in A$, there uniquely exists an ordinal number α_a which is isomorphic to $W[a]$. Let $\mathbf{P}(x, y)$ be the property

$$(x \in A \text{ and } y \text{ is an ordinal isomorphic to } W[x]) \text{ or } (x \notin A \text{ and } y = \varnothing).$$

Hence, by The Axiom Schema of Replacement, there exists the set $S \triangleq \{\alpha_a \mid a \in A\}$.

Claim 1. S is an ordinal number.

Proof. S is well-ordered by $\in$ by Theorem 6.2.13 (iv). Let $\gamma \in \alpha_a \in S$. Let $\varphi : \alpha_a \hookrightarrow\!\!\!\!\rightarrow W[a]$ be the isomorphism between α_a and $W[a]$ and let $c \triangleq \varphi(\gamma)$. Then, $\varphi\big|_\gamma$ is an isomorphism between γ and $W[c]$; thus $\gamma \in S$. Hence, S is an ordinal.

Claim 2. Let $a \in A$, $b \in W$, and $b \prec a$. Then, $b \in A$. Moreover, $\alpha_b < \alpha_a$.

Proof. Let $\varphi : W[a] \hookrightarrow\!\!\!\!\rightarrow \alpha_a$ be the isomorphism between $W[a]$ and α_a. Then, $\varphi\big|_{W[b]}$ is an isomorphism between $W[b]$ and $\varphi[W[b]]$. As $W[b]$ is an initial segment of $W[a]$, $\varphi[W[b]]$ is an initial segment of α_a. Hence, $\varphi[W[b]]$ is an ordinal. By Lemma 6.2.12, $\varphi[W[b]] = \beta$ for some $\beta < \alpha_a$. Hence, $b \in A$ and $\alpha_b = \beta$. □

Now, define $f : A \to S$ by $a \mapsto \alpha_a$. By Claims 1 and 2, f is an isomorphism between A and S. If $\exists c \in W$, $A = W[c]$, then $c \in A$ by definition. Hence, A is not an initial segment of W in spite of Claim 2; $A = W$. (See Definition 6.1.2.) Hence, f is an isomorphism between A and an ordinal S. □

Definition 6.3.4: Order Type

If W is a well-ordered set, then the *order type* of W is the unique ordinal number isomorphic to W. This is justified by The Counting Theorem.

Theorem 6.3.5 The Recursion Theorem

Let $\mathbf{G}$ be an operation. For any a, there exists a unique infinite sequence $\langle a_n \mid n \in \mathbb{N}\rangle$ such that

(i) $a_0 = a$ and
(ii) $\forall n \in \mathbb{N}$, $a_{n+1} = \mathbf{G}(a_n, n)$.

The proof of The Recursion Theorem is given in the next section.

Selected Problems

Exercise 6.3.1

Let $\mathbf{P}(x, y)$ be a property such that for every x there is at most one y for which $\mathbf{P}(x, y)$ holds. Then, for every A, there exists a set B such that

$$\forall x \in A, [\exists y, \mathbf{P}(x, y) \implies \exists y \in B, \mathbf{P}(x, y)].$$

Proof. Let $\mathbf{Q}(x, y)$ be the property

$$\mathbf{P}(x, y) \vee [y = \varnothing \wedge \neg \exists z\, \mathbf{P}(x, z)].$$

Then, for each x, there uniquely exists y such that $\mathbf{Q}(x, y)$ holds. If $\neg \exists z \mathbf{P}(x, z)$, then $y = \varnothing$ is the only one which satisfies $\mathbf{Q}(x, y)$; otherwise, y that satisfies $\mathbf{P}(x, y)$ is unique.

Let A be any set. By The Axiom Schema of Replacement, the set $B \triangleq \{ y \mid \exists x \in A, \mathbf{Q}(x, y) \}$ exists. Then, for each $x \in A$ such that $\exists y \mathbf{P}(x, y)$, the y also satisfies $\mathbf{Q}(x, y)$; hence $y \in B$. □

Exercise 6.3.2

(i) $\{ \varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\{\{\varnothing\}\}\}, \cdots \}$ exists.

(ii) $\{ \mathbb{N}, \mathcal{P}(\mathbb{N}), \mathcal{P}(\mathcal{P}(\mathbb{N})), \cdots \}$ exists.

(iii) $\omega + \omega = \omega \cup \{ \omega, \omega + 1, (\omega + 1) + 1, \cdots \}$ exists.

Proof.

(i) Let $\mathbf{P}(x, y)$ be the property

$$[\exists a\, \exists b\; x = (a, b) \wedge y = \{a\}] \vee [\neg(\exists a\, \exists b\; x = (a, b)) \wedge y = \varnothing].$$

The result follows from The Recursion Theorem with $a = \varnothing$.

(ii) Let $\mathbf{P}(x, y)$ be the property

$$[\exists a\, \exists b\; x = (a, b) \wedge y = \mathcal{P}(a)] \vee [\neg(\exists a\, \exists b\; x = (a, b)) \wedge y = \varnothing].$$

The result follows from The Recursion Theorem with $a = \mathbb{N}$.

(iii) Let $\mathbf{P}(x, y)$ be the property

$$[\exists a\, \exists b\; x = (a, b) \wedge y = S(a)] \vee [\neg(\exists a\, \exists b\; x = (a, b)) \wedge y = \varnothing].$$

Then, the set $B = \{ \omega, \omega + 1, (\omega + 1) + 1, \cdots \}$ exists by The Recursion Theorem with $a = \omega$. Hence, the union of B and ω exists. □

Exercise 6.3.3

Use The Recursion Theorem to define

$$\begin{aligned} V_0 &= \varnothing \\ \forall n \in \omega, V_{n+1} &= \mathcal{P}(V_n) \\ V_\omega &= \textstyle\bigcup_{n \in \omega} V_n. \end{aligned}$$

Proof. Let $\mathbf{P}(x, y)$ be the property

$$[\exists a\, \exists b\; x = (a, b) \wedge y = \mathcal{P}(a)] \vee [\neg(\exists a\, \exists b\; x = (a, b)) \wedge y = \varnothing].$$

Then, by The Recursion Theorem, $\langle V_n \mid n \in \mathbb{N} \rangle$ exists. Hence, V_ω exists as well. □

Exercise 6.3.4

(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.
(i) By The Induction Principle and Theorem 4.2.8, V_n is finite for all $n \in \omega$. Take any $x \in V_\omega$. $x \in V_{n+1} = \mathcal{P}(V_n)$ for some $n \in \omega$ as $V_0 = \varnothing$. Hence, $x \subseteq V_n$ is finite by Theorem 4.2.4.
(ii) Let $x \in y \in V_\omega$. Then, $y \in V_{n+1} = \mathcal{P}(V_n)$ for some $n \in \omega$. Then, $x \in y \subseteq V_n$; hence $x \in V_\omega$. Therefore, V_ω is transitive.
(iii) $\varnothing \in V_1 \subseteq V_\omega$. Assume $x \in V_\omega$. Then, $x \in V_n$ for some $n \in \omega$. Then, $\{x\} \in V_{n+1}$; thus $S(x) = x \cup \{x\} \subseteq V_n \cup V_{n+1} \subseteq V_\omega$. Hence, V_ω is inductive. $\square$

Exercise 6.3.5

(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 $\mathcal{P}(X) \in V_\omega$.
(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 1. $\forall n \in \mathbb{N}$, $V_n \subseteq \mathcal{P}(V_n)$.

Proof. We have $\varnothing = V_0 \subseteq \mathcal{P}(V_0)$. Fix any $n \in \mathbb{N}$ and assume $V_n \subseteq \mathcal{P}(V_n)$. Take any $x \in V_{n+1}$. Then, $x \subseteq V_n \subseteq \mathcal{P}(V_n) = V_{n+1}$, i.e., $x \in \mathcal{P}(V_{n+1})$. By The Induction Principle, $\forall n \in \mathbb{N}$, $V_n \subseteq \mathcal{P}(V_n)$.

From Claim 1 and The Induction Principle, one may conclude $\forall m, n \in \omega, (m \le n \implies V_m \subseteq V_n)$.
(i) Take any $x, y \in V_\omega$. Then, there exist $m, n \in \omega$ such that $x \in V_m$ and $y \in V_n$. WLOG, $m \le n$, and thus $V_m \subseteq V_n$. Therefore, $\{x, y\} \subseteq V_n$; $\{x, y\} \in V_\omega$.
(ii) $X \in V_{n+1}$ for some $n \in \omega$. By Claim 1, V_{n+1} is transitive, and thus $x \subseteq V_n$ for each $x \in X$. Hence, $\bigcup X \subseteq V_n$; so $\bigcup X \in V_\omega$. Moreover, if $A \subseteq X$, then $A \subseteq V_n$, i.e., $A \in V_{n+1}$. Hence, $\mathcal{P}(X) \subseteq V_{n+1}$; $\mathcal{P}(X) \in V_\omega$.
(iii) By Exercise 6.3.4 (i), X is finite. Hence, $f[X]$ is a finite subset of V_ω by Theorem 4.2.5. Hence, by (iv), $f[X] \in V_\omega$.
(iv) Let $f : X \to \mathbb{N}$ be defined by $f(x) \triangleq \min\{m \in \mathbb{N} \mid x \in X_m\}$. Let $n \triangleq \max \operatorname{ran} f$. Then, $\forall x \in X$, $x \in V_n$. Hence, $X \subseteq V_n$; $X \in V_\omega$. $\square$

6.4 Transfinite Induction and Recursion

Theorem 6.4.1 The Transfinite Induction Principle: First Version

Let $\mathbf{P}(x)$ be a property. Assume that, for each ordinal number α, [1] holds. Then, $\mathbf{P}(\alpha)$ holds for all ordinals α.

$$\text{If } \mathbf{P}(\beta) \text{ holds for each ordinal } \beta \text{ such that } \beta < \alpha, \text{ then } \mathbf{P}(\alpha) \text{ holds.} \qquad [1]$$

Proof. Suppose there exists an ordinal γ such that $\neg\mathbf{P}(\gamma)$ for the sake of contradiction. Let $S \triangleq \{\beta \mid \beta \text{ is an ordinal such that } \beta \le \alpha \text{ and } \neg\mathbf{P}(\beta)\}$. As $S \ne \varnothing$, by Theorem 6.2.13 (iv), S has a least element α. As every ordinal $\beta < \alpha$ satisfies $\mathbf{P}(\beta)$, by assumption, we must have $\mathbf{P}(\alpha)$ by [1], which contradicts $\alpha \in S$. $\square$

Theorem 6.4.2 The Transfinite Induction Principle: Second Version

Let $\mathbf{P}(x)$ be a property. Assume that:
(i) For each ordinal α, $\mathbf{P}(\alpha) \implies \mathbf{P}(\alpha + 1)$.

(ii) For each limit ordinal α, if $\mathbf{P}(\beta)$ holds for each ordinal β such that $\beta < \alpha$, then $\mathbf{P}(\alpha)$ holds.

Then, $\mathbf{P}(\alpha)$ holds for all ordinals α.

Proof. Take any ordinal α and assume that $\mathbf{P}(\beta)$ holds for all ordinals less than α. If α is a limit ordinal, then $\mathbf{P}(\alpha)$ holds by (ii). Otherwise, i.e., if $\alpha = \beta + 1$ for some ordinal β, then, by (i), $\mathbf{P}(\alpha)$ holds as $\mathbf{P}(\beta)$ holds. Therefore, [1] holds. The result follows from The Transfinite Induction Principle: First Version. □

Definition 6.4.3: Transfinite Sequence

A function whose domain is an ordinal α is called *transfinite sequence of length α*.

Theorem 6.4.4 The Transfinite Recursion Theorem

Let $\mathbf{G}$ be an operation. Then, the property $\mathbf{P}(x, y)$ stated in [2] defines an operation $\mathbf{F}$ such that $\forall \alpha \in \mathrm{Ord}$, $\mathbf{F}(\alpha) = \mathbf{G}\left(\mathbf{F}\big|_{\alpha}\right)$ where $\mathbf{F}\big|_{\alpha}$ is the transfinite sequence of length α defined by $x \mapsto \mathbf{F}(x)$.

$$\mathbf{P}(x, y) \text{ is the property defined by:}$$
$$\begin{cases} x \in \mathrm{Ord} \text{ and } y = t(x) \text{ for some computation } t \\ \qquad \text{of length } x \text{ based on } \mathbf{G}, \\ \text{or } x \notin \mathrm{Ord} \wedge y = \varnothing \end{cases} \qquad [2]$$

where t is called a *computation of length α based on* $\mathbf{G}$ if t is a function whose domain is $\alpha + 1$ and for all $\beta \leq \alpha$, $t(\beta) = \mathbf{G}\left(t\big|_{\beta}\right)$.

Proof. We first have to show that $\mathbf{P}(x, y)$ defined in [2] defines an operation.

Claim 1. For any ordinal α, there uniquely exists a computation of length α based on $\mathbf{G}$.

Proof. Fix any ordinal α and assume for the sake of induction that:

$$\text{For each ordinal } \beta \text{ with } \beta < \alpha, \\ \text{there uniquely exists a computation of length } \beta. \qquad [*]$$

Then, by The Axiom Schema of Replacement, a set

$$T \triangleq \{\, t \mid t \text{ is a computation of length } \beta \text{ for some } \beta < \alpha \,\}$$

exists. Note that, for each $\beta < \alpha$, there uniquely exists $t \in T$ whose length is β by [*]. Let $\hat{t} \triangleq \bigcup T$ and $\tau \triangleq \hat{t} \cup \{(\alpha, \mathbf{G}(\hat{t}))\}$.

Claim 2. τ is a function and $\operatorname{dom}\tau = \alpha + 1$.

Proof. We have to show that T is a compatible system of functions. First, take any $t_1, t_2 \in T$ and let $\beta_1 \triangleq \operatorname{dom} t_1$ and $\beta_2 \triangleq \operatorname{dom} t_2$. WLOG, by Theorem 6.2.13 (iii), $\beta_1 \leq \beta_2$.

For the sake of transfinite induction, fix any ordinal γ with $\gamma < \beta_1$ and assume that $t_1(\delta) = t_2(\delta)$ for all ordinals $\delta < \gamma$. Then, $t_1\big|_\gamma = t_2\big|_\gamma$; thus $t_1(\gamma) = \mathbf{G}\left(t_1\big|_\gamma\right) = \mathbf{G}\left(t_2\big|_\gamma\right) = t_2(\gamma)$. Hence, by The Transfinite Induction Principle: First Version, $t_1(\gamma) = t_2(\gamma)$ for all ordinals $\gamma < \beta_1$.

Hence, $\hat{t}$ is a function by Theorem 2.3.12 and

$$\begin{aligned} \operatorname{dom}\hat{t} &= \textstyle\bigcup_{t\in T} \operatorname{dom} t && \triangleright \text{ Theorem 2.3.12} \\ &= \textstyle\bigcup_{\beta<\alpha}(\beta+1) && \triangleright\ [*] \\ &= \alpha. \end{aligned}$$

Therefore, by Theorem 2.3.12, τ is a function and $\operatorname{dom}\tau = \alpha \cup \{\alpha\} = \alpha + 1$. □

Claim 3. For each ordinal β with $\beta \leq \alpha$, $\tau(\beta) = \mathbf{G}\left(\tau\big|_\beta\right)$.

Proof. If $\beta = \alpha$, we immediately have $\tau(\alpha) = \mathbf{G}(\hat{t}) = \mathbf{G}\left(\tau\big|_\alpha\right)$. If $\beta < \alpha$, then take $t \in T$ with $\operatorname{dom} t = \beta + 1$. Then, we have $\tau(\beta) = t(\beta) = \mathbf{G}\left(t\big|_\beta\right) = \mathbf{G}\left(\tau\big|_\beta\right)$ as $t \subseteq \tau$. □

Claims 2 and 3 asserts that τ is a computation of length α based on $\mathbf{G}$.

To prove the uniqueness, let σ be another computation of length α. Note that, if $\tau(\delta) = \sigma(\delta)$ for all $\delta < \gamma$, then $\tau(\gamma) = \mathbf{G}\left(\tau\big|_\gamma\right) = \mathbf{G}\left(\sigma\big|_\gamma\right) = \sigma(\gamma)$. Hence, by The Transfinite Induction Principle: First Version, $\tau(\gamma) = \sigma(\gamma)$ for all $\gamma \leq \alpha$; thus $\tau = \sigma$.

Hence, we showed that [$*$] implies, there uniquely exists a computation of length α. Hence, by The Transfinite Induction Principle: First Version, for all ordinals α, there uniquely exists y that satisfies $\mathbf{P}(\alpha, y)$. □

By Claim 1, $\forall x\, \exists! y\ \mathbf{P}(x, y)$; $\mathbf{P}$ defines an operation $\mathbf{F}$. (In other words, $\mathbf{F}(\alpha) = t(\alpha)$ where t is the unique computation of length α based on $\mathbf{G}$.)

Fix any ordinal α. Let t be the unique computation of length α. Then, for each $\gamma < \alpha$, $t\big|_{\gamma+1}$ is a computation of length γ, and thus $\mathbf{F}(\gamma) = t\big|_{\gamma+1}(\gamma) = t(\gamma)$; in other words, $\mathbf{F}\big|_\alpha = t\big|_\alpha$. Then,

$$\begin{aligned} \mathbf{F}(\alpha) &= t(\alpha) && \triangleright \text{ Definition of } \mathbf{F} \\ &= \mathbf{G}\left(t\big|_\alpha\right) && \triangleright\ t \text{ is a computation} \\ &= \mathbf{G}\left(\mathbf{F}\big|_\alpha\right). && \triangleright\ \mathbf{F}\big|_\alpha = t\big|_\alpha \end{aligned}$$

The theorem is now proven. □

Notation 6.4.5

If $\mathbf{F}(z, x)$ is an operation in two variables, i.e., $\mathbf{P}(z, x, y)$ is an property such that $\forall z\, \forall x\, \exists! y\ \mathbf{P}(z, x, y)$ and $\mathbf{F}(z, x)$ denotes the unique y such that $\mathbf{P}(z, x, y)$. We write $\mathbf{F}_z(x)$ in place of $\mathbf{F}(z, x)$ so that we may treat $\mathbf{F}_z$ as an operation.

Theorem 6.4.6 The Transfinite Recursion Theorem: Parametric Version

Let $\mathbf{G}$ be an operation. Then, the property $\mathbf{Q}(z,x,y)$ stated in [3] defines an operation $\mathbf{F}$ such that $\forall z$, $\forall \alpha \in \mathrm{Ord}$, $\mathbf{F}(z,\alpha) = \mathbf{G}\left(z, \mathbf{F}_z\big|_\alpha\right)$.

$\mathbf{Q}(z,x,y)$ is the property defined by:

$$\begin{cases} \quad x \in \mathrm{Ord} \text{ and } y = t(x) \text{ for some computation } t \\ \qquad\quad \text{of length } x \text{ based on } \mathbf{G} \text{ and } z, \\ \text{or } x \notin \mathrm{Ord} \wedge y = \varnothing \end{cases} \tag{3}$$

where t is called a *computation of length α based on* $\mathbf{G}$ *and* z if t is a function whose domain is $\alpha+1$ and for all $\beta \leq \alpha$, $t(\beta) = \mathbf{G}\left(z, t\big|_\beta\right)$.

Proof. Replace every $\mathbf{G}(-)$ into $\mathbf{G}(z,-)$ in the proof of The Transfinite Recursion Theorem. □

Note:-

We now present some variations of The Transfinite Recursion Theorem and The Transfinite Recursion Theorem: Parametric Version.

Theorem 6.4.7

Let $\mathbf{G}_1$ and $\mathbf{G}_2$ be operations. Let $\mathbf{G}$ be the operation defined in [4]. Then, the property $\mathbf{P}(x,y)$ stated in [2] defines an operation $\mathbf{F}$ such that:

(i) For each ordinal α, $\mathbf{F}(\alpha+1) = \mathbf{G}_1(\mathbf{F}(\alpha))$.

(ii) For each limit ordinal α, $\mathbf{F}(\alpha) = \mathbf{G}_2\left(\mathbf{F}\big|_\alpha\right)$.

$y = \mathbf{G}(x)$ if and only if

$$\begin{cases} \quad x \text{ is a transfinite sequence of length } \alpha+1 \text{ and } y = \mathbf{G}_1(x(\alpha)), \\ \text{or } x \text{ is a transfinite sequence of length } \alpha \text{ such that } \alpha \text{ is a limit ordinal} \\ \qquad\quad \text{and } y = \mathbf{G}_2(x), \\ \text{or } x \text{ is not a transfinite sequence and } y = \varnothing. \end{cases} \tag{4}$$

Proof. For each ordinal α, $\mathbf{F}(\alpha) = \mathbf{G}\left(\mathbf{F}\big|_\alpha\right)$ by The Transfinite Recursion Theorem.

- If α is an ordinal, then $\mathbf{F}(\alpha+1) = \mathbf{G}\left(\mathbf{F}\big|_{\alpha+1}\right) = \mathbf{G}_1\left(\mathbf{F}\big|_{\alpha+1}(\alpha)\right) = \mathbf{G}_1\left(\mathbf{F}(\alpha)\right)$.
- If α is a limit ordinal, then $\mathbf{F}(\alpha) = \mathbf{G}\left(\mathbf{F}\big|_\alpha\right) = \mathbf{G}_2\left(\mathbf{F}\big|_\alpha\right)$. □

Theorem 6.4.8

Let $\mathbf{G}_1$ and $\mathbf{G}_2$ be operations. Let $\mathbf{G}$ be the operation defined in [5]. Then, the property $\mathbf{Q}(z,x,y)$ stated in [3] defines an operation $\mathbf{F}$ such that:

(i) For each ordinal α and each set z, $\mathbf{F}(z,\alpha+1) = \mathbf{G}_1(z, \mathbf{F}(z,\alpha))$.

(ii) For each limit ordinal α and each set z, $\mathbf{F}(z,\alpha) = \mathbf{G}_2\left(z, \mathbf{F}_z\big|_\alpha\right)$.

$y = \mathbf{G}(z,x)$ if and only if

$$\begin{cases} \quad x \text{ is a transfinite sequence of length } \alpha+1 \text{ and } y = \mathbf{G}_1(z, x(\alpha)), \\ \text{or } x \text{ is a transfinite sequence of length } \alpha \text{ such that } \alpha \text{ is a limit ordinal} \\ \qquad\quad \text{and } y = \mathbf{G}_2(z,x), \\ \text{or } x \text{ is not a transfinite sequence and } y = \varnothing. \end{cases} \tag{5}$$

Proof. For each ordinal α and each set z, $\mathbf{F}(z,\alpha) = \mathbf{G}\left(z, \mathbf{F}_z\big|_\alpha\right)$ by The Transfinite Recursion Theorem: Parametric Version. Then, for each set z:

- If α is an ordinal, then $\mathbf{F}(z,\alpha+1) = \mathbf{G}\left(z, \mathbf{F}_z\big|_{\alpha+1}\right) = \mathbf{G}_1\left(z, \mathbf{F}_z\big|_{\alpha+1}(\alpha)\right) = \mathbf{G}_1(z, \mathbf{F}(z,\alpha))$.
- If α is a limit ordinal, then $\mathbf{F}(z,\alpha) = \mathbf{G}\left(z, \mathbf{F}_z\big|_\alpha\right) = \mathbf{G}_2\left(z, \mathbf{F}_z\big|_\alpha\right)$. □

Corollary 6.4.9

Let Ω be an ordinal number, A be a set, and $S = \bigcup_{\alpha<\Omega} A^\alpha$ be the set of all transfinite sequences of elements of A of length less than Ω. Let $g : S \to A$. Then, there exists a unique function $f : \Omega \to A$ such that

$$f(\alpha) = g\left(f\big|_\alpha\right) \text{ for all ordinals } \alpha < \Omega.$$

Proof. Define an operation $\mathbf{G}$ by

$$\mathbf{G}(t) \triangleq \begin{cases} g(t) & \text{if } t \in S \\ \varnothing & \text{otherwise.} \end{cases}$$

Then, by The Transfinite Recursion Theorem, there exists an operation $\mathbf{F}$ such that $\mathbf{F}(\alpha) = \mathbf{G}\left(\mathbf{F}\big|_\alpha\right)$ holds for all ordinals α. Then, $f \triangleq \mathbf{F}\big|_\Omega$ satisfies the condition. □

***Proof of* The Recursion Theorem.** Define an operation $\mathbf{G}'$ by

$$\mathbf{G}'(x) \triangleq \begin{cases} \mathbf{G}(x_n, n) & \text{if } x \text{ is a sequence of length } n+1 \text{ where } n \in \omega \\ a & \text{otherwise.} \end{cases}$$

By The Transfinite Recursion Theorem, there exists an operation $\mathbf{F}$ such that $\mathbf{F}(\alpha) = \mathbf{G}'\left(\mathbf{F}\big|_\alpha\right)$ for all ordinals α. Now, let $\langle a_n \rangle_{n\in\mathbb{N}} \triangleq \mathbf{F}\big|_\omega$. Then,

- $a_0 = \mathbf{F}(0) = \mathbf{G}'(\varnothing) = a$
- For each $n \in \mathbb{N}$, $a_{n+1} = \mathbf{F}(n+1) = \mathbf{G}'\left(\mathbf{F}\big|_{n+1}\right) = \mathbf{G}\left(\mathbf{F}\big|_{n+1}(n), n\right) = \mathbf{G}(\mathbf{F}(n), n) = \mathbf{G}(a_n, n)$. □

6.5 Ordinal Arithmetic

Definition 6.5.1: Addition of Ordinal Numbers

For each ordinal β:

$$\beta + 0 = \beta. \quad [1]$$
$$\beta + (\alpha+1) = (\beta+\alpha)+1 \text{ for all ordinals } \alpha. \quad [2]$$
$$\beta + \alpha = \sup\{\beta+\gamma \mid \gamma < \alpha\} \text{ for all limit ordinals } \alpha \neq 0. \quad [3]$$

Note:-

Let $\mathbf{G}_1$ and $\mathbf{G}_2$ be operations defined by

$$\mathbf{G}_1(z,x) = x+1$$
$$\mathbf{G}_2(z,x) = \begin{cases} \bigcup \operatorname{ran} x & \text{if } x \text{ is a nonempty function} \\ z & \text{otherwise.} \end{cases}$$

Then, Theorem 6.4.8 gives an operation $\mathbf{F}$ such that: for each ordinal β,

(i) $\mathbf{F}(\beta,0) = \mathbf{G}_2(\beta,\varnothing) = \beta$.

(ii) $\mathbf{F}(\beta, \alpha+1) = \mathbf{G}_1(\beta, \mathbf{F}(\beta,\alpha)) = \mathbf{F}(\beta,\alpha)+1$ for each ordinal α.
(iii) $\mathbf{F}(\beta,\alpha) = \mathbf{G}_2\left(\beta, \mathbf{F}_\beta\big|_\alpha\right) = \bigcup \operatorname{ran}\left(\mathbf{F}_\beta\big|_\alpha\right)$ for each limit ordinal α.

Let $\mathbf{P}(\alpha)$ be the property "$\mathbf{F}(\beta,\alpha)$ is an ordinal for each ordinal α."

- For each ordinal α, if $\mathbf{P}(\alpha)$ holds, then $\mathbf{F}(\beta,\alpha+1) = \mathbf{F}(\beta,\alpha)+1$ is an ordinal for all ordinals β by Lemma 6.2.5.
- For each limit ordinal α, if $\mathbf{P}(\beta)$ holds for all ordinals $\beta < \alpha$, then $\operatorname{ran}\left(\mathbf{F}_\beta\big|_\alpha\right)$ is a set of ordinals, and thus $\mathbf{F}(\beta,\alpha) = \bigcup \operatorname{ran}\left(\mathbf{F}_\beta\big|_\alpha\right)$ is an ordinal. (See the proof of Theorem 6.2.13 (v)).

Therefore, by The Transfinite Induction Principle: Second Version, $\mathbf{F}(\beta,\alpha)$ is an ordinal for each ordinal α and β. Hence, Definition 6.5.1 is justified; $\beta+\alpha$ is just a shortcut for $\mathbf{F}(\beta,\alpha)$.

Note:-

- Addition of ordinals is not commutative:

$$n+\omega = \sup\{\, n+m \mid n<\omega \,\} = \omega \neq \omega+n \text{ for all } n \in \omega \setminus \{0\}.$$

- Addition of ordinals is not right-cancellative:

$$1+\omega = \omega = 2+\omega \text{ but } 1 \neq 2.$$

Theorem 6.5.2

Let $(W_1, \leq_1)$ and $(W_2, \leq_2)$ be well-ordered sets, isomorphic to α_1 and α_2, respectively, and let $(W, \leq)$ be the sum of $(W_1, \leq_1)$ and $(W_2, \leq_2)$. (See Lemma 4.5.5.) Then, $(W, \leq) \cong \alpha_1+\alpha_2$.

Proof. We may assume that W_1 and W_2 are disjoint, that $W = W_1 \cup W_2$. We shall conduct The Transfinite Induction Principle: Second Version on α_2.

- Let $\alpha_2 = \beta+1$ for some ordinal β and assume the theorem holds whenever $W_2 \cong \beta$. W_2 has a greatest element a, which is also a greatest element of W. Moreover, $W_2[a] \cong \beta$, and thus $W[a]$ is isomorphic to the sum of W_1 and $W_2[a]$.

  By the induction hypothesis, we have an isomorphism $h \colon W[a] \hookrightarrow\!\!\!\!\rightarrow \alpha_1+\beta$. Then, $h \cup \{(a, \alpha_1+\beta)\}$ is an isomorphism between W and $(\alpha_1+\beta)+1 = \alpha_1+(\beta+1) = \alpha_1+\alpha_2$.
- Let α_2 is a limit ordinal and assume the theorem holds whenever W_2 is isomorphic to an ordinal less than α_2. For each $\beta < \alpha_2$, justified by Theorem 6.1.7, let a_β be the unique element of W_2 such that $\beta \cong W_2[a_\beta]$.

  Then, by the induction hypothesis, for each $\beta < \alpha_2$, noting that the sum of W_1 and $W_2[a_\beta] \cong W[a_\beta]$, we may let f_β to be the unique isomorphism between $\alpha_1+\beta$ and $W[a_\beta]$. (Once again, uniqueness follows from Theorem 6.1.7.) Now, define $f \triangleq \bigcup_{\beta<\alpha_2} f_\beta$. If $\beta < \gamma < \alpha_2$, then $f_\gamma\big|_{\alpha_1+\beta}$ is an isomorphism between $\alpha_1+\beta$ and $W[a_\beta]$, and thus $f_\beta \subsetneq f_\gamma$. Therefore, by Theorem 2.3.12, f is a function, and f is an isomorphism between $\bigcup\{\, \alpha_1+\beta \mid \beta<\alpha_2 \,\} = \alpha_1+\alpha_2$ and W. □

Lemma 6.5.3

Let α, β, and γ be ordinals.

(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) (⇒) Fix any ordinal β and assume $\alpha < \beta' \implies \gamma + \alpha < \gamma + \beta'$ for all ordinals α, β, and γ with $\beta' < \beta$ for the sake of induction. We shall assume $\beta \neq 0$. Take any ordinals α and γ such that $\alpha < \beta$ If $\beta = \delta + 1$, then $\delta \geq \alpha$. (Otherwise, we have $\delta < \alpha < \delta + 1$, which is impossible.) Then, we have

$$\begin{aligned}
\gamma + \alpha &\leq \gamma + \delta && \triangleright \text{ Induction Hypothesis} \\
&< (\gamma + \delta) + 1 \\
&= \gamma + (\delta + 1) && \triangleright \text{ [2]} \\
&= \gamma + \beta.
\end{aligned}$$

In the case of β being an limit ordinal, then $\alpha + 1 < \beta$, and thus

$$\begin{aligned}
\gamma + \alpha &< (\gamma + \alpha) + 1 \\
&= \gamma + (\alpha + 1) && \triangleright \text{ [2]} \\
&\leq \sup\{\gamma + \delta \mid \delta < \beta\} && \triangleright\ \alpha + 1 < \beta \\
&= \gamma + \beta. && \triangleright \text{ [3]}
\end{aligned}$$

The result follows from The Transfinite Induction Principle: First Version.

(⇐) Assume $\gamma + \alpha < \gamma + \beta$ where α, β, and γ are ordinals. We clearly cannot have $\alpha = \beta$. If $\beta < \alpha$, then (⇒) implies $\gamma + \beta < \gamma + \alpha$, which is impossible. Hence, the only remaining option is $\alpha < \beta$.

(ii) By (i), $\alpha < \beta$ or $\alpha > \beta$ immediately implies $\gamma + \alpha \neq \gamma + \beta$. Hence, the result follows.

(iii) We shall conduct the transfinite induction on γ. Fix any ordinal γ and assume $(\alpha + \beta) + \gamma' = \alpha + (\beta + \gamma')$ for all ordinals α, β, and γ' such that $\gamma' < \gamma$. Note the case $\gamma = 0$ is evident by [1].

If $\gamma = \delta + 1$ for some ordinal δ, then

$$\begin{aligned}
(\alpha + \beta) + (\delta + 1) &= [(\alpha + \beta) + \delta] + 1 && \triangleright \text{ [2]} \\
&= [\alpha + (\beta + \delta)] + 1 && \triangleright \text{ Induction Hypothesis} \\
&= \alpha + [(\beta + \delta) + 1] && \triangleright \text{ [2]} \\
&= \alpha + [\beta + (\delta + 1)]. && \triangleright \text{ [2]}
\end{aligned}$$

Now, assume γ is a limit ordinal other than 0.

Claim 1. $\beta + \gamma$ is a limit ordinal.

Proof. If $\xi < \beta + \gamma = \sup\{\beta + \delta \mid \delta < \gamma\}$, there exists $\delta < \gamma$ such that $\xi < \beta + \delta$. Then,

$$\begin{aligned}
\xi + 1 &< (\beta + \delta) + 1 \\
&= \beta + (\delta + 1) && \triangleright \text{ [2]} \\
&= \beta + \gamma. && \triangleright\ \delta + 1 < \gamma, \text{ (i)}
\end{aligned}$$

□

Claim 2. $(\alpha + \beta) + \gamma \leq \alpha + (\beta + \gamma)$

Proof. Take any $\delta < \gamma$. Then, as $\beta + \delta < \beta + \gamma$ by (i), $\xi \triangleq (\beta + \delta) + 1$ satisfies $\beta + \delta < \xi < \beta + \gamma$ thanks to Claim 1.

Then,

$$\begin{aligned}(\alpha+\beta)+\delta &= \alpha+(\beta+\delta) && \triangleright \text{ Induction Hypothesis}\\ &< \alpha+\xi. && \triangleright \text{ (i)}\end{aligned}$$

Hence, $\sup\{(\alpha+\beta)+\delta \mid \delta<\gamma\} \leq \sup\{\alpha+\xi \mid \xi<\beta+\gamma\}$. □

Claim 3. $\alpha+(\beta+\gamma) \leq (\alpha+\beta)+\gamma$

Proof. If $\xi<\beta+\gamma$, then there exists $\delta<\gamma$ such that $\xi<\beta+\delta$ by Claim 1; thus

$$\begin{aligned}\alpha+\xi &< \alpha+(\beta+\delta) && \triangleright \text{ (i)}\\ &= (\alpha+\beta)+\delta. && \triangleright \text{ Induction Hypothesis}\end{aligned}$$

In other words, $\sup\{\alpha+\xi \mid \xi<\beta+\gamma\} \leq \sup\{(\alpha+\beta)+\delta \mid \delta<\gamma\}$. □

Claims 2 and 3 finishes the proof with the help of The Transfinite Induction Principle: First Version. □

Lemma 6.5.4

Let α and β be ordinals. If $\alpha \leq \beta$, then there uniquely exists an ordinal ξ such that $\alpha+\xi=\beta$.

Proof. $\beta \setminus \alpha = \{\nu \mid \alpha \leq \nu < \beta\}$ is a well-ordered set by Theorem 6.2.13 (iv). There exists an ordinal ξ which is isomorphic to $\beta\setminus\alpha$. Moreover, the sum of α and $\beta\setminus\alpha$ is β; hence $\alpha+\xi=\beta$ by Theorem 6.5.2. The uniqueness follows from Lemma 6.5.3 (ii). □

Definition 6.5.5: Multiplication Of Ordinal Numbers

For each ordinal β:

$$\beta\cdot 0=\beta. \tag{4}$$
$$\beta\cdot(\alpha+1)=\beta\cdot\alpha+\beta \text{ for all ordinals } \alpha. \tag{5}$$
$$\beta\cdot\alpha=\sup\{\beta\cdot\gamma \mid \gamma<\alpha\} \text{ for all limit ordinals } \alpha\neq 0. \tag{6}$$

Note:-

Let $\mathbf{G}_1$ and $\mathbf{G}_2$ be operations defined by

$$\mathbf{G}_1(z,x)=\begin{cases} x+z & \text{if } x \text{ and } z \text{ are ordinals}\\ \varnothing & \text{otherwise}\end{cases}$$

$$\mathbf{G}_2(z,x)=\begin{cases} \bigcup \operatorname{ran} x & \text{if } x \text{ is a nonempty function}\\ 0 & \text{otherwise.}\end{cases}$$

Then, Theorem 6.4.8 gives an operation $\mathbf{F}(\beta,\alpha)$ that justifies Definition 6.5.5.

Theorem 6.5.6

Let α and β be ordinal numbers. Then, the order type of the lexicographic ordering of $\beta\times\alpha$ is $\alpha\cdot\beta$.

Proof. We shall conduct The Transfinite Induction Principle: Second Version on β. Let $\mathbf{P}(\beta)$ be the property that

"for all ordinals α, the function h on $\beta \times \alpha$ defined by $(\eta, \xi) \mapsto \alpha \cdot \eta + \xi$ is an isomorphism between $\beta \times \alpha$ and $\alpha \cdot \beta$."

$\mathbf{P}(0)$ evidently holds.

Take any ordinals α and β and assume that $\mathbf{P}(\beta)$ holds. Let h' be the function on $(\beta+1) \times \alpha$ defined by $(\eta, \xi) \mapsto \alpha \cdot \eta + \xi$. Then, $h'|_{\beta \times \alpha}$ is the isomorphism between $\beta \times \alpha$ and $\alpha \cdot \beta$ by $\mathbf{P}(\beta)$. For all ordinals $\eta < \beta$ and $\xi_1, \xi_2 < \alpha$,

$$\begin{aligned} \alpha \cdot \eta + \xi_1 &< \alpha \cdot \eta + \alpha && \triangleright \text{ Lemma 6.5.3 (i)} \\ &= \alpha \cdot (\eta + 1) && \triangleright \text{ [5]} \\ &\leq \alpha \cdot \beta && \triangleright \text{ Exercise 6.5.8 (i)} \\ &\leq \alpha \cdot \beta + \xi_2; && \triangleright \text{ Lemma 6.5.3 (i)} \end{aligned}$$

moreover,

$$\alpha \cdot \beta + \xi_1 < \alpha \cdot \beta + \xi_2 \quad \triangleright \text{ Lemma 6.5.3 (i)}$$
$$\text{if } \xi_1 < \xi_2.$$

Hence, h is an isomorphism between $(\beta+1) \times \alpha$ and $\operatorname{ran} h$. It is evident that $\alpha \cdot \beta \subseteq \operatorname{ran} h \subseteq \alpha \cdot (\beta+1)$.

Now, take any γ such that $\alpha \cdot \beta \leq \gamma < \alpha \cdot (\beta+1)$. Then, by Lemma 6.5.4, there exists an ordinal ξ such that $\gamma = \alpha \cdot \beta + \xi$. Then, by Corollary 6.1.6 (i), $\xi < \beta$; hence $\gamma = h'(\beta, \xi)$; thus $\operatorname{ran} h = \alpha \cdot (\beta+1)$.

Now, take any ordinal β and assume that $\mathbf{P}(\beta')$ holds for all $\beta' < \beta$. Take any ordinal α. By the inductive assumption, The Axiom Schema of Replacement, and The Counting Theorem, there exists a set

$$H \triangleq \{ h_{\beta'} \mid h_{\beta'} \text{ is an isomorphism between } \beta' \times \alpha \text{ and } \alpha \cdot \beta' \text{ where } \beta' < \beta \}.$$

Let $h' \triangleq \bigcup H$. Then, by the inductive assumption, H is a compatible system of functions, hence h' is a function with $\operatorname{dom} h' = \bigcup_{\beta' < \beta} \beta' \times \alpha = \beta \times \alpha$ by Theorem 2.3.12. Moreover, $\operatorname{ran} h' = \bigcup_{\beta' < \beta} \alpha \cdot \beta' = \alpha \cdot \beta$. It is evident that h' is a isomorphism. The result follows from The Transfinite Induction Principle: Second Version. $\square$

Definition 6.5.7: Exponentiation of Ordinal Numbers

For each ordinal β:

$$\beta^0 = 1. \tag{7}$$
$$\beta^{\alpha+1} = \beta^\alpha \cdot \beta \text{ for all ordinals } \alpha. \tag{8}$$
$$\beta^\alpha = \sup\{ \beta^\gamma \mid 0 < \gamma < \alpha \} \text{ for all limit ordinals } \alpha \neq 0. \tag{9}$$

In the textbook, it defines $\beta^\alpha = \sup\{ \beta^\gamma \mid \gamma < \alpha \}$ for limit ordinals, which results in $0^\omega = \sup\{ 0^0, 0^1, 0^2, \cdots \} = \sup\{0, 1\} = 1$. I considered this as a mistake or a typo, so we just define in this way.

Note:-

Let $\mathbf{G}_1$ and $\mathbf{G}_2$ be operations defined by

$$\mathbf{G}_1(z,x) = \begin{cases} x \cdot z & \text{if } x \text{ and } z \text{ are ordinals} \\ \varnothing & \text{otherwise} \end{cases}$$

$$\mathbf{G}_2(z,x) = \begin{cases} \bigcup \operatorname{ran} x & \text{if } x \text{ is a nonempty function} \\ 1 & \text{otherwise.} \end{cases}$$

Then, Theorem 6.4.8 gives an operation $\mathbf{F}(\beta,\alpha)$ that justifies Definition 6.5.7.

Note:-

Ordinal arithmetic differs from arithmetic of cardinals.

- $2^{\aleph_0} > \aleph_0$ but $2^\omega = \omega$.
- $\aleph_0^n = \aleph_0$ but $\omega^n > \omega$.
- ω^ω is countable. (It is an order type of lexicographic ordering of $\mathrm{Seq}(\mathbb{N})$.)

Note:-

One can use arithmetic operations to generate larger and larger ordinals:

$$0, 1, \cdots, \omega, \omega+1, \cdots, \omega \cdot 2, \cdots \omega \cdot 3, \cdots,$$
$$\omega \cdot \omega = \omega^2, \cdots, \omega^3, \cdots, \omega^\omega, \cdots, \omega^{\omega}, \cdots, \omega^{\omega^2}, \cdots, \omega^{\omega^3}, \cdots, \omega^{\omega^\omega}, \cdots$$

We define

$$\varepsilon \triangleq \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \cdots\}$$

and then form $\varepsilon+1$, $\varepsilon+\omega$, ε^ω, ε^ε, $\varepsilon^{\varepsilon^\varepsilon}$, etc.

Selected Problems

Note:-

The proof of Exercise 6.5.1 depends on Exercise 6.5.2 and Exercise 6.5.7; and the proof of Exercise 6.5.2 depends on Exercise 6.5.7.

Exercise 6.5.1

For all ordinals α, β, and γ, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

Proof. Note that it is evident when $\gamma = 0$ by [4]. Moreover, the cases when $\alpha = 0$ or $\beta = 0$ follows from Claim 1 of Exercise 6.5.2. We shall exploit The Transfinite Induction Principle: Second Version on γ.

Fix any ordinal γ and assume that, for all ordinals α, β, and γ' with $\gamma' < \gamma$, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$. Then,

$$\begin{aligned} (\alpha \cdot \beta) \cdot (\gamma+1) &= (\alpha \cdot \beta) \cdot \gamma + \alpha \cdot \beta && \triangleright\ [5] \\ &= \alpha \cdot (\beta \cdot \gamma) + \alpha \cdot \beta && \triangleright\ \text{Induction Hypothesis} \\ &= \alpha \cdot (\beta \cdot \gamma + \beta) && \triangleright\ \text{Exercise 6.5.2} \\ &= \alpha \cdot [\beta \cdot (\gamma+1)]. && \triangleright\ [5] \end{aligned}$$

Now, fix an nonzero limit ordinal γ and assume, for all ordinals α, β, and γ' with $\gamma' < \gamma$, $(\alpha \cdot \beta) \cdot \gamma' = \alpha \cdot (\beta \cdot \gamma')$. Now, take any ordinals $\alpha \neq 0$ and $\beta \neq 0$.

Take any $\xi < (\alpha \cdot \beta) \cdot \gamma$. Then, there exists $\xi' < \gamma$ such that $\xi < (\alpha \cdot \beta) \cdot \xi'$. Hence,

$$\begin{aligned} \xi &< (\alpha \cdot \beta) \cdot \xi' \\ &= \alpha \cdot (\beta \cdot \xi') && \triangleright \text{ Induction Hypothesis} \\ &< \alpha \cdot (\beta \cdot \gamma); && \triangleright \text{ Exercise 6.5.7 (i)} \end{aligned}$$

we have $(\alpha \cdot \beta) \cdot \gamma \leq \alpha \cdot (\beta \cdot \gamma)$.

Take any $\xi < \alpha \cdot (\beta \cdot \gamma)$. As $\beta \cdot \gamma$ is a nonzero ordinal by Claim 2 of Exercise 6.5.2. Hence, there exists $\xi' < \beta \cdot \gamma$ such that $\xi < \alpha \cdot \xi'$. Moreover, there exists $\xi'' < \gamma$ such that $\xi' < \beta \cdot \xi''$ as γ is a limit ordinal. Hence,

$$\begin{aligned} \xi &< \alpha \cdot \xi' \\ &< \alpha \cdot (\beta \cdot \xi'') && \triangleright \text{ Exercise 6.5.7 (i)} \\ &= (\alpha \cdot \beta) \cdot \xi'' && \triangleright \text{ Induction Hypothesis} \\ &< (\alpha \cdot \beta) \cdot \gamma; && \triangleright \text{ Exercise 6.5.7 (i)} \end{aligned}$$

we have $\alpha \cdot (\beta \cdot \gamma) \leq (\alpha \cdot \beta) \cdot \gamma$. The result follows from The Transfinite Induction Principle: Second Version. □

Exercise 6.5.2

For all ordinals α, β, and γ, $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Proof. We first begin with the following claims.

Claim 1. Let α and β be ordinals. Then, $\alpha \cdot \beta = 0 \iff \alpha = 0 \vee \beta = 0$.

Proof.

($\Rightarrow$) Note that $0 + \alpha$, which is isomorphic to the sum of $\varnothing$ and α, has the order type α; hence, $0 + \alpha = \alpha$.

Assume $\alpha \neq 0$ and $\beta \neq 0$. Then,

$$\begin{aligned} 0 < \alpha &= 0 + \alpha \\ &= \alpha \cdot 0 + \alpha && \triangleright [4] \\ &= \alpha \cdot 1 && \triangleright [5] \\ &\leq \alpha \cdot \beta; && \triangleright \text{ Exercise 6.5.7 (i)} \end{aligned}$$

$\alpha \cdot \beta \neq 0$.

($\Leftarrow$) If is evident when $\beta = 0$ by [4]. Hence, we shall conduct The Transfinite Induction Principle: Second Version on β. (In other words, we shall prove $0 \cdot \beta = 0$.)

Fix any ordinal β and assume $0 \cdot \beta = 0$. Then,

$$\begin{aligned} 0 \cdot (\beta + 1) &= 0 \cdot \beta + 0 && \triangleright [5] \\ &= 0 \cdot \beta && \triangleright [1] \\ &= 0. && \triangleright \text{ Induction Hypothesis} \end{aligned}$$

Now, fix any limit ordinal $\beta \neq 0$ and assume $0 \cdot \delta = 0$ for all ordinals $\delta < \beta$. Then, $0 \cdot \beta = \sup\{\, 0 \cdot \delta \mid \delta < \beta \,\} = \sup\{0\} = 0$. The result follows from The Transfinite Induction Principle: Second Version. □

Claim 2. If α and β are nonzero ordinals and β a limit ordinal, then $\alpha \cdot \beta$ is a nonzero limit ordinal.

Proof. Let $\xi < \alpha \cdot \beta$. Then, there exists $\delta < \beta$ such that $\xi < \alpha \cdot \delta$ by [6]. Then, as $\delta + 1 < \beta$, we have

$$\begin{aligned} \xi + 1 &\leq \alpha \cdot \delta \\ &< \alpha \cdot (\delta + 1) && \triangleright \text{ Exercise 6.5.7 (i)} \\ &\leq \alpha \cdot \beta. && \triangleright \text{ [6]} \end{aligned}$$

Hence, $\alpha \cdot \beta$ is a limit ordinal. We have $\alpha \cdot \beta \neq 0$ from Claim 1.

When, $\alpha = 0$, then the both sides are equal to 0 by Claim 1 and [1]. Hence, we may assume $\alpha \neq 0$. The case $\gamma = 0$ is evident from [1] and [4]. We shall exploit The Transfinite Induction Principle: Second Version on γ.

Fix any ordinal γ and assume that, for all ordinals α and β, the property "$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$" holds. Then, for all ordinals α and β

$$\begin{aligned} \alpha \cdot [\beta + (\gamma + 1)] &= \alpha \cdot [(\beta + \gamma) + 1] && \triangleright \text{ [2]} \\ &= \alpha \cdot (\beta + \gamma) + \alpha && \triangleright \text{ [5]} \\ &= (\alpha \cdot \beta + \alpha \cdot \gamma) + \alpha && \triangleright \text{ Induction Hypothesis} \\ &= \alpha \cdot \beta + (\alpha \cdot \gamma + \alpha) && \triangleright \text{ Lemma 6.5.3 (iii)} \\ &= \alpha \cdot \beta + \alpha \cdot (\gamma + 1). && \triangleright \text{ [5]} \end{aligned}$$

Now, fix any limit ordinal $\gamma \neq 0$ and assume $\alpha \cdot (\beta + \gamma') = \alpha \cdot \beta + \alpha \cdot \gamma'$ for all ordinals α, β, and γ' with $\gamma' < \gamma$. Take any ordinals α and β. When, $\alpha = 0$, then the both sides are equal to 0 by Claim 1 and [1]. Hence, we may assume $\alpha \neq 0$.

Note that $\beta + \gamma$ is a limit ordinal by Claim 1 of Lemma 6.5.3. Hence, $\alpha \cdot (\beta + \gamma) = \sup\{\, \alpha \cdot \xi \mid \xi < \beta + \gamma \,\}$ by [6].

Take any $\xi < \beta + \gamma$. Then, there exists $\delta < \gamma$ such that $\xi < \beta + \delta$ as γ is a limit ordinal. Hence,

$$\begin{aligned} \alpha \cdot \xi &< \alpha \cdot (\beta + \delta) && \triangleright \text{ Lemma 6.5.3 (i)} \\ &= \alpha \cdot \beta + \alpha \cdot \delta && \triangleright \text{ Induction Hypothesis} \\ &< \alpha \cdot \beta + \alpha \cdot \gamma; && \triangleright \text{ Lemma 6.5.3 (i), Exercise 6.5.7 (i)} \end{aligned}$$

we have $\alpha \cdot (\beta + \gamma) \leq \alpha \cdot \beta + \alpha \cdot \gamma$.

Now, take any $\xi < \alpha \cdot \beta + \alpha \cdot \gamma$. Then, by Claim 2, $\alpha \cdot \gamma$ is a limit ordinal; thus there exists $\xi' < \alpha \cdot \gamma$ such that $\xi < \alpha \cdot \beta + \xi'$. There exists $\xi'' < \gamma$ such that $\xi' < \alpha \cdot \xi''$ as γ is a limit ordinal. Hence,

$$\begin{aligned} \xi &< \alpha \cdot \beta + \xi' \\ &< \alpha \cdot \beta + \alpha \cdot \xi'' && \triangleright \text{ Lemma 6.5.3 (i)} \\ &= \alpha \cdot (\beta + \xi'') && \triangleright \text{ Induction Hypothesis} \\ &< \alpha \cdot (\beta + \gamma); && \triangleright \text{ Lemma 6.5.3 (i), Exercise 6.5.7 (i)} \end{aligned}$$

we have $\alpha \cdot \beta + \alpha \cdot \gamma \leq \alpha \cdot (\beta + \gamma)$. The result follows from The Transfinite Induction Principle: Second Version. $\square$

Exercise 6.5.3

Simplify:

(i) $(\omega+1)+\omega$

(ii) $\omega+\omega^2$

(iii) $(\omega+1)\cdot\omega^2$.

Proof.

(i)

$$\begin{aligned}(\omega+1)+\omega &= \omega+(1+\omega) && \triangleright \text{ Lemma 6.5.3 (iii)}\\ &= \omega+\omega && \triangleright\ 1+\omega=\omega\\ &= \omega\cdot 2\end{aligned}$$

(ii)

$$\begin{aligned}\omega+\omega^2 &= \omega\cdot 1+\omega\cdot\omega\\ &= \omega\cdot(1+\omega) && \triangleright \text{ Exercise 6.5.2}\\ &= \omega\cdot\omega && \triangleright\ 1+\omega=\omega\\ &= \omega^2\end{aligned}$$

(iii) We have $\omega^2=\omega\cdot\omega\le(\omega+1)\cdot\omega$ by Exercise 6.5.8 (ii).

Take any $\xi<(\omega+1)\cdot\omega$. Then, there exists $n<\omega$ such that $\xi<(\omega+1)\cdot n$. Then,

$$\begin{aligned}\xi &< (\omega+1)\cdot n\\ &\le (\omega+\omega)\cdot n && \triangleright \text{ Lemma 6.5.3 (i), Exercise 6.5.8 (ii)}\\ &= \omega\cdot(2\cdot n) && \triangleright \text{ Exercise 6.5.1}\\ &\le \omega\cdot\omega; && \triangleright\ [6]\end{aligned}$$

hence, $(\omega+1)\cdot\omega\le\omega^2$. Therefore, $(\omega+1)\cdot\omega=\omega^2$, which implies $(\omega+1)\cdot\omega^2=\omega^3$ by Exercise 6.5.1. □

Exercise 6.5.4

For every ordinal α, there uniquely exist an ordinal β and a natural number n such that $\alpha=\beta+n$.

Proof. Let $\beta\triangleq\sup\{\gamma\mid\gamma\le\alpha \text{ and } \gamma \text{ is a limit ordinal}\}$. Then, $\beta\le\alpha$ by definition. Hence, there exists an ordinal ξ such that $\alpha=\beta+\xi$ by Lemma 6.5.4.

Claim 1. β is a limit ordinal.

Proof. Suppose $\beta=\delta+1$ is for some ordinal δ for the sake of contradiction. Then, as $\delta<\beta$, there exists $\gamma\le\alpha$ such that γ is a limit ordinal and $\delta<\gamma$. Then, $\beta=\delta+1<\gamma$ as γ is a limit ordinal, which is a contradiction. □

Claim 2. ξ is a natural number.

Proof. Suppose $\xi\ge\omega$ for the sake of induction. Then, there exists an ordinal δ such that $\xi=\omega+\delta$ by Lemma 6.5.4. Then, we have $\alpha=(\beta+\omega)+\delta$ by Lemma 6.5.3 (iii) while $\beta+\omega$ is a limit ordinal (Claim 1 of Lemma 6.5.3) such that $\beta<\beta+\omega\le\alpha$, which contradicts the definition of β. □

Hence, we have the existence; now we prove the uniqueness. Assume $\alpha = \beta + n = \beta' + n'$ where β and β' are limit ordinals and n and n' are natural numbers. For the sake of contradiction, suppose $\beta < \beta'$. Then, as β' is a limit ordinal, $\beta + m < \beta'$ for all ordinals $m < \omega$. Hence, $\beta' \geq \sup\{\beta + m \mid m < \omega\} = \beta + \omega$. We have

$$\begin{aligned} \beta + n &= \beta' + n' \\ &\geq (\beta + \omega) + n' && \triangleright \text{ Exercise 6.5.8 (i)} \\ &= \beta + (\omega + n'), && \triangleright \text{ Lemma 6.5.3 (iii)} \end{aligned}$$

which implies $n \geq \omega + n'$ by Lemma 6.5.3 (i). This is a contradiction; hence $\beta = \beta'$. As $\beta + n = \beta + n'$, we get $n = n'$ by Lemma 6.5.3 (ii). □

Exercise 6.5.5

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 different ordinals such that $\xi_1 + \alpha = \xi_2 + \alpha = \beta$. WLOG, $\xi_1 < \xi_2$, i.e., $\xi_1 + 1 \leq \xi_2$. Then,

$$\begin{aligned} \xi_1 + \alpha &\leq (\xi_1 + 1) + \alpha && \triangleright \text{ Exercise 6.5.8 (i)} \\ &\leq \xi_2 + \alpha && \triangleright \text{ Exercise 6.5.8 (i)} \\ &= \xi_1 + \alpha; \end{aligned}$$

Hence, $\xi_1 + \alpha = \xi_1 + (1 + \alpha)$ by Lemma 6.5.3 (iii), which implies $\alpha + 1 = \alpha$ by Lemma 6.5.3 (ii). By induction, we have $\alpha + n = \alpha$ for all $n \in \omega$; which says $(\xi_1 + n) + \alpha = \beta$ for all $n \in \omega$. $(\xi_1 + n)$'s are all different by Lemma 6.5.3 (ii). □

Exercise 6.5.6

Find the least $\alpha > \omega$ such that $\xi + \alpha = \alpha$ for all $\xi < \alpha$.

Proof. We first assert that $\alpha = \omega^2$ satisfies the condition.

> ***Claim 1.*** If ξ is an ordinal less than ω^2, then $\xi + \omega^2 = \omega^2$.
>
> ***Proof.*** By definition, there exists $n < \omega$ such that $\xi < \omega \cdot n$. Then,
>
> $$\begin{aligned} \xi + \omega^2 &\leq \omega \cdot n + \omega^2 && \triangleright \text{ Exercise 6.5.8 (i)} \\ &= \omega \cdot (n + \omega) && \triangleright \text{ Exercise 6.5.2} \\ &= \omega \cdot \omega. && \triangleright\ n + \omega = \omega \end{aligned}$$
>
> Hence, $\omega^2 \leq \xi + \omega^2 \leq \omega^2$; thus $\xi + \omega^2 = \omega^2$. □

Now, let $\omega < \alpha < \omega^2$. Then, as there exists $m \in \omega$ such that $\alpha < \omega \cdot m$, we may let $n \triangleq \max\{m \in \omega \mid \alpha > \omega \cdot m\}$ by Theorem 3.2.8. Then,

$$\begin{aligned} \omega + \alpha &> \omega + \omega \cdot n \\ &= \omega \cdot 1 + \omega \cdot n \\ &= \omega \cdot (n + 1) && \triangleright \text{ Exercise 6.5.2, } \cdot \text{ is Commutative} \\ &\geq \alpha; \end{aligned}$$

$\omega + \alpha \neq \alpha$. Hence, ω^2 is the least ordinal that satisfies the condition. □

Exercise 6.5.7

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) ($\Rightarrow$) We will conduct The Transfinite Induction Principle: Second Version on β.

Fix any ordinal β and assume $\alpha < \beta \implies \gamma \cdot \alpha < \gamma \cdot \beta$ for all ordinals α and $\gamma \neq 0$. Then, if $\alpha < \beta + 1$ and $\gamma \neq 0$, we have

$$\begin{aligned} \gamma \cdot \alpha &\leq \gamma \cdot \beta && \triangleright\ \alpha \leq \beta, \text{Induction Hypothesis} \\ &= \gamma \cdot \beta + 0 && \triangleright\ [1] \\ &< \gamma \cdot \beta + \gamma && \triangleright\ \text{Lemma 6.5.3 (i)} \\ &= \gamma \cdot (\beta + 1). && \triangleright\ [5]. \end{aligned}$$

Now, fix any limit ordinal β and assume that $\alpha < \beta' \implies \gamma \cdot \alpha < \gamma \cdot \beta'$ holds for all $\beta' < \beta$ and $\gamma \neq 0$. Now, let $\alpha < \beta$ and $\gamma \neq 0$. Then, we have $\alpha + 1 < \beta$ as β is a limit ordinal. Hence,

$$\begin{aligned} \gamma \cdot \alpha &< \gamma \cdot (\alpha + 1) && \triangleright\ \text{Induction Hypothesis} \\ &\leq \gamma \cdot \beta. && \triangleright\ [6] \end{aligned}$$

Therefore, the result follows from The Transfinite Induction Principle: Second Version.

($\Leftarrow$) Assume $\gamma \cdot \alpha < \gamma \cdot \beta$ where α, β, and γ are ordinals with $\gamma \neq 0$ We clearly cannot have $\alpha = \beta$. If $\beta < \alpha$, then ($\Rightarrow$) implies $\gamma \cdot \beta < \gamma \cdot \alpha$, which is impossible. Hence, the only remaining option is $\alpha < \beta$.

(ii) By (i), $\alpha < \beta$ or $\alpha > \beta$ immediately implies $\gamma \cdot \alpha \neq \gamma \cdot \beta$. Hence, the result follows. □

Exercise 6.5.8

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 shall conduct The Transfinite Induction Principle: Second Version on γ. If $\gamma = 0$, then it is obvious by [1].

Fix any ordinal γ and assume $\alpha + \gamma \leq \beta + \gamma$ for all ordinals α and β with $\alpha < \beta$. Take any ordinals α and β such that $\alpha < \beta$. Then,

$$\begin{aligned} \alpha + (\gamma + 1) &= (\alpha + \gamma) + 1 && \triangleright\ \text{Lemma 6.5.3 (iii)} \\ &\leq (\beta + \gamma) + 1 && \triangleright\ \text{Induction Hypothesis} \\ &= \beta + (\gamma + 1). && \triangleright\ \text{Lemma 6.5.3 (iii)} \end{aligned}$$

Now, fix any limit ordinal $\gamma \neq 0$ and assume, for each ordinal $\gamma' < \gamma$, $\alpha + \gamma' \leq \beta + \gamma'$ for all ordinals α and β with $\alpha < \beta$. Let $\xi < \alpha + \gamma$; then there exists $\delta < \gamma$ such that $\xi < \alpha + \delta$. Then,

$$\begin{aligned} \xi &< \alpha + \delta \\ &\leq \beta + \delta && \triangleright\ \text{Induction Hypothesis} \\ &< \beta + \gamma. && \triangleright\ \text{Lemma 6.5.3 (i)} \end{aligned}$$

Hence, $\alpha+\delta \leq \beta+\gamma$. The result follows from The Transfinite Induction Principle: Second Version.

(ii) We shall conduct The Transfinite Induction Principle: Second Version on γ. If $\gamma = 0$, then it is obvious by [4].

Fix any ordinal γ and assume $\alpha+\gamma \leq \beta+\gamma$ for all ordinals α and β with $\alpha < \beta$. Take any ordinals α and β such that $\alpha < \beta$. Then,

$$\begin{aligned} \alpha \cdot (\gamma+1) &= \alpha \cdot \gamma + \alpha && \triangleright \text{[5]} \\ &< \alpha \cdot \gamma + \beta && \triangleright \text{Lemma 6.5.3 (i)} \\ &\leq \beta \cdot \gamma + \beta && \triangleright \text{Induction Hypothesis, (i)} \\ &= \beta \cdot (\gamma+1). && \triangleright \text{[5]} \end{aligned}$$

Now, fix any limit ordinal $\gamma \neq 0$ and assume, for each ordinal $\gamma' < \gamma$, $\alpha \cdot \gamma' \leq \beta \cdot \gamma'$ for all ordinals α and β with $\alpha < \beta$. Let $\xi < \alpha \cdot \gamma$. Then, there exists $\delta < \gamma$ such that $\xi < \alpha \cdot \delta$. Then,

$$\begin{aligned} \xi &< \alpha \cdot \delta \\ &\leq \beta \cdot \delta && \triangleright \text{Induction Hypothesis} \\ &< \beta \cdot \gamma. && \triangleright \text{Lemma 6.5.3 (i)} \end{aligned}$$

Hence, $\alpha \cdot \gamma \leq \beta \cdot \gamma$. The result follows from The Transfinite Induction Principle: Second Version. ☐

Exercise 6.5.9

(i) Ordinal addition is not right-cancellative; that is to say 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 to say 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 is not right-distributive; that is to say there exist α, β, and γ such that $(\alpha+\beta)\cdot\gamma \neq \alpha\cdot\gamma+\beta\cdot\gamma$.

Proof.

(i) $\alpha = 0$, $\beta = 1$, and $\gamma = \omega$ is a counterexample; $0+\omega = 1+\omega = \omega$.

(ii) $\alpha = 1$, $\beta = 2$, and $\gamma = \omega$ is a counterexample; $1\cdot\omega = 2\cdot\omega = \omega$.

(iii) $\alpha = \beta = 1$ and $\gamma = \omega$ is a counterexample; $(1+1)\cdot\omega = \omega \neq \omega\cdot 2 = \omega\cdot 1+\omega\cdot 1$. ☐

Exercise 6.5.10

An ordinal α is a limit ordinal if and only if $\alpha = \omega \cdot \beta$ for some ordinal β.

Proof.

($\Rightarrow$) Take any limit ordinal α and assume that, for every limit ordinal γ less than α, there exists β such that $\gamma = \omega \cdot \beta$ for the sake of induction. We have two cases:

- Assume there exists some limit ordinal $\gamma < \alpha$ such that there is no limit ordinal δ such that $\gamma < \delta < \alpha$. By the induction hypothesis, $\gamma = \omega \cdot \beta$ for some ordinal β. Then, $\gamma+\omega$ is a limit ordinal by Claim 1 of Lemma 6.5.3, and there is no limit ordinal between γ and $\gamma+\omega$. Hence, $\alpha = \gamma+\omega = \omega\cdot\beta+\omega = \omega\cdot(\beta+1)$.
- Assume that, for every limit ordinal $\gamma < \alpha$, there exists a limit ordinal δ such that $\gamma < \delta < \alpha$. Let $\beta \triangleq \sup\{\xi \mid \omega\cdot\xi < \alpha\}$. ($\beta$ is well-defined since $\omega\cdot\xi < \alpha$ implies $\xi < \alpha$.)

Claim 1. There is no ordinal ξ such that $\xi + \omega = \alpha$.

Proof. Suppose ξ is an ordinal such that $\xi + \omega = \alpha$ for the sake of contradiction. Then, there uniquely exists η and n such that $\xi = \eta + n$ where η is a limit ordinal and $n \in \omega$ by Exercise 6.5.4. Then, $\alpha = (\eta + n) + \omega = \eta + \omega$, but there is no limit integral between η and α, which is a contradiction. □

Claim 2. β is a limit ordinal.

Proof. It is easy to check that $\omega \cdot \xi < \alpha \implies \omega \cdot (\xi + 1) < \alpha$ by the assumption. Suppose $\beta = \delta + 1$ for some ordinal δ for the sake of contradiction. Then, as $\delta < \beta$, there exists ξ such that $\delta < \xi$ and $\omega \cdot \xi < \alpha$. Then, $\delta + 1 < \xi + 1$ and $\omega \cdot (\xi + 1) < \alpha$ by Lemma 6.5.3 (i). Hence, $\delta + 1 < \xi + 1 \leq \beta$. Therefore, β is a limit ordinal. □

Take any $\xi < \omega \cdot \beta$. Then, there exists $\delta < \beta$ such that $\xi < \omega \cdot \delta$ by Claim 2. Moreover, there exists ξ' such that $\delta < \xi'$ and $\omega \cdot \xi' < \alpha$. Hence, $\xi < \omega \cdot \delta < \omega \cdot \xi' < \alpha$; thus $\omega \cdot \beta \leq \alpha$.

Take any $\xi < \alpha$. Then, as α is a limit ordinal, $\xi + \omega \leq \alpha$. Claim 1 further asserts that $\xi + \omega < \alpha$. By the induction hypothesis and Claim 1 of Lemma 6.5.3, $\xi + \omega = \omega \cdot \delta$ for some δ. Then, $\delta \leq \beta$ by definition of β. Therefore, $\xi < \omega \cdot \delta \leq \omega \cdot \beta$; we have $\alpha \leq \omega \cdot \beta$.

In both cases, we have $\alpha = \omega \cdot \beta$ for some β. Therefore, by The Transfinite Induction Principle: Second Version, every limit ordinal α can be expressed as $\alpha = \omega \cdot \beta$.

($\Leftarrow$) We shall conduct The Transfinite Induction Principle: Second Version on β. Note that $\omega \cdot 0 = 0$ is a limit ordinal.

Take any ordinal β. Then, $\omega \cdot (\beta + 1) = \omega \cdot \beta + \omega$ is a limit ordinal by Claim 1 of Lemma 6.5.3.

Now, take any limit ordinal $\beta \neq 0$. Then, by Claim 2 of Exercise 6.5.2, $\omega \cdot \beta$ is a limit ordinal. The result follows from The Transfinite Induction Principle: Second Version. □

Exercise 6.5.13

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 need the following lemmas:

Claim 1. 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. Take any $\xi < \alpha^\beta$. Then, there exists $\gamma < \beta$ such that $\xi < \alpha^\gamma$ by [9]. Then,

$$\begin{aligned} \xi + 1 &\leq \alpha^\gamma \\ &< \alpha^{\gamma+1} && \triangleright \text{ Exercise 6.5.14 (ii)} \\ &\leq \alpha^\beta. && \triangleright \text{ [9]} \end{aligned}$$

Hence, α^β is a limit ordinal. Since $1 = \alpha^0 < \alpha^\beta$ by [7] and Exercise 6.5.14 (ii), α^β is nonzero. □

Claim 2. Let α be a nonzero ordinal. Then, $0^\alpha = 0$.

Proof. Let $\mathbf{P}(\alpha)$ be the property "if α is a nonzero ordinal, then $0^\alpha = 0$." $\mathbf{P}(0)$ holds by vacuous truth. Take any ordinal α. Then,

$$\begin{aligned} 0^{\alpha+1} &= 0^\alpha \cdot 0 && \triangleright \text{[8]} \\ &= 0. && \triangleright \text{[4]} \end{aligned}$$

Take any limit ordinal $\alpha \neq 0$ and assume $\mathbf{P}(\alpha')$ holds for all $\alpha' < \alpha$. Then,

$$0^\alpha = \sup\{\, 0^\gamma \mid 0 < \gamma < \alpha \,\} = \sup\{0\} = 0.$$

The result follows from The Transfinite Induction Principle: Second Version. □

Claim 3. Let α be an ordinal. Then, $1^\alpha = 1$.

Proof. We already have $1^0 = 1$ by [7]. Take any ordinal α and assume $1^\alpha = 1$. Then,

$$\begin{aligned} 1^{\alpha+1} &= 1^\alpha \cdot 1 && \triangleright \text{[8]} \\ &= 1 \cdot 1 && \triangleright \text{Induction Hypothesis} \\ &= 1. \end{aligned}$$

. Then,

$$\begin{aligned} 1^{\alpha+1} &= 1^\alpha \cdot 1 && \triangleright \text{[8]} \\ &= 1 \cdot 1 && \triangleright \text{Induction Hypothesis} \\ &= 1. \end{aligned}$$

Take any limit ordinal $\alpha \neq 0$ and assume $1^\gamma = 1$ for all $\gamma < \alpha$. Then,

$$\begin{aligned} 1^\alpha &= \sup\{\, 1^\gamma \mid 0 < \gamma < \alpha \,\} && \triangleright \text{[9]} \\ &= \sup\{1\} && \triangleright \text{Induction Hypothesis, } 1^1 = 1 \\ &= 1. \end{aligned}$$

The result follows from The Transfinite Induction Principle: Second Version. □

(i) We shall conduct The Transfinite Induction Principle: Second Version on γ. Let $\mathbf{P}(\gamma)$ be the property "for all ordinals α and β, $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$." $\mathbf{P}(0)$ evidently holds.

Take any ordinal γ and assume $\mathbf{P}(\gamma)$. Then, for all ordinals α and β,

$$\begin{aligned} \alpha^{\beta+(\gamma+1)} &= \alpha^{(\beta+\gamma)+1} && \triangleright \text{Lemma 6.5.3 (i)} \\ &= \alpha^{\beta+\gamma} \cdot \alpha && \triangleright \text{[8]} \\ &= (\alpha^\beta \cdot \alpha^\gamma) \cdot \alpha && \triangleright \text{Induction Hypothesis} \\ &= \alpha^\beta \cdot (\alpha^\gamma \cdot \alpha) && \triangleright \text{Exercise 6.5.1} \\ &= \alpha^\beta \cdot \alpha^{\gamma+1}. && \triangleright \text{[8]} \end{aligned}$$

Now, take any limit ordinal $\gamma \neq 0$ and assume $\mathbf{P}(\gamma')$ for all ordinals $\gamma' < \gamma$. The result is clear when $\beta = 0$; hence further assume $\beta \neq 0$. Then, by Claim 1 of Lemma 6.5.3 and, $\beta + \gamma$ is a nonzero limit ordinal.

Take any $\xi < \alpha^{\beta+\gamma}$. Then, there exists $\delta < \beta + \gamma$ such that $\xi < \alpha^\delta$ by [9].

Moreover, there exists $\delta' < \gamma$ such that $\delta < \beta + \delta'$ by [3]. Then,

$$\begin{aligned}
\xi &< \alpha^{\delta} \\
&< \alpha^{\beta+\delta'} && \triangleright \text{ Exercise 6.5.14 (ii)} \\
&= \alpha^{\beta} \cdot \alpha^{\delta'} && \triangleright \text{ Induction Hypothesis} \\
&< \alpha^{\beta} \cdot \alpha^{\gamma}; && \triangleright \text{ Exercise 6.5.14 (ii), Exercise 6.5.7 (i)}
\end{aligned}$$

hence $\alpha^{\beta+\gamma} \le \alpha^{\beta} \cdot \alpha^{\gamma}$.

Take any $\xi < \alpha^{\beta} \cdot \alpha^{\gamma}$. By Claim 1 and [6], there exists $\delta < \alpha^{\gamma}$ such that $\xi < \alpha^{\beta} \cdot \delta$. By [9], there exists $\gamma' < \gamma$ such that $\delta < \alpha^{\gamma'}$. Then,

$$\begin{aligned}
\xi &< \alpha^{\beta} \cdot \delta \\
&< \alpha^{\beta} \cdot \alpha^{\gamma'} && \triangleright \text{ Exercise 6.5.7 (i)} \\
&= \alpha^{\beta+\gamma'} && \triangleright \text{ Induction Hypothesis} \\
&< \alpha^{\beta+\gamma}; && \triangleright \text{ Lemma 6.5.3 (i), Exercise 6.5.14 (ii)}
\end{aligned}$$

hence $\alpha^{\beta} \cdot \alpha^{\gamma} \le \alpha^{\beta+\gamma}$. The result follows form The Transfinite Induction Principle: Second Version.

(ii) We shall conduct The Transfinite Induction Principle: Second Version on γ. Let $\mathbf{P}(\gamma)$ be the property "for all ordinals α and β, $(\alpha^{\beta})^{\gamma} = \alpha^{\beta\cdot\gamma}$." $\mathbf{P}(0)$ holds by [4] and [7].

Take any ordinal γ and assume $\mathbf{P}(\gamma)$. Take any ordinals α and β. Then,

$$\begin{aligned}
(\alpha^{\beta})^{\gamma+1} &= (\alpha^{\beta})^{\gamma} \cdot \alpha^{\beta} && \triangleright \text{ [8]} \\
&= \alpha^{\beta\cdot\gamma} \cdot \alpha^{\beta} && \triangleright \text{ Induction Hypothesis} \\
&= \alpha^{\beta\cdot\gamma+\beta} && \triangleright \text{ (i)} \\
&= \alpha^{\beta\cdot(\gamma+1)}. && \triangleright \text{ [5]}
\end{aligned}$$

Hence, $\mathbf{P}(\gamma+1)$ holds.

Now, take any limit ordinal $\gamma \ne 0$ and assume $\mathbf{P}(\gamma')$ holds for all $\gamma' < \gamma$. Fix any ordinals α and β. If $\alpha = 0$, it is evident from Claim 2, [7], and Claim 1 of Exercise 6.5.2. Also, Claim 3 covers the case $\alpha = 1$; hence we may assume $\alpha > 1$. Moreover, if $\beta = 0$, then it is all clear from Claim 1 of Exercise 6.5.2 and [7].

Take any $\xi < (\alpha^{\beta})^{\gamma}$. There exists $\gamma' < \gamma$ such that $\xi < (\alpha^{\beta})^{\gamma'}$ by [9]. Then,

$$\begin{aligned}
\xi &< (\alpha^{\beta})^{\gamma'} \\
&= \alpha^{\beta\cdot\gamma'} && \triangleright \text{ Induction Hypothesis} \\
&< \alpha^{\beta\cdot\gamma}; && \triangleright \text{ Exercise 6.5.7 (i), Exercise 6.5.14 (ii)}
\end{aligned}$$

hence $(\alpha^{\beta})^{\gamma} \le \alpha^{\beta\cdot\gamma}$.

Take any $\xi < \alpha^{\beta\cdot\gamma}$. By Claim 2 of Exercise 6.5.2, $\beta\cdot\gamma$ is a nonzero limit ordinal; and thus there exists $\delta < \beta\cdot\gamma$ such that $\xi < \alpha^{\delta}$ by [9]. Moreover, there exists $\gamma' < \gamma$ such that $\delta < \beta\cdot\gamma'$ by [6]. Then,

$$\begin{aligned}
\xi &< \alpha^{\delta} \\
&< \alpha^{\beta\cdot\gamma'} && \triangleright \text{ Exercise 6.5.14 (ii)} \\
&= (\alpha^{\beta})^{\gamma'} && \triangleright \text{ Induction Hypothesis} \\
&< (\alpha^{\beta})^{\gamma}; && \triangleright\ \alpha^{\beta} > 1, \text{ Exercise 6.5.14 (ii)}
\end{aligned}$$

hence $\alpha^{\beta\cdot\gamma} = (\alpha^{\beta})^{\gamma}$. The result follows from The Transfinite Induction Principle: Second Version. □

Exercise 6.5.14

Let α, β, and γ be ordinals.

(i) $\alpha \leq \beta \implies \alpha^\gamma \leq \beta^\gamma$

(ii) $\alpha > 1 \land \beta < \gamma \implies \alpha^\beta < \alpha^\gamma$

Proof.

(i) We will make use of The Transfinite Induction Principle: Second Version on γ. Let $\mathbf{P}(\gamma)$ be the property "for all ordinals α and β, $\alpha \leq \beta \implies \alpha^\gamma \leq \beta^\gamma$." $\mathbf{P}(0)$ evidently holds by [7].

Take any ordinal γ and assume $\mathbf{P}(\gamma)$. Then, for all ordinals α and β with $\alpha \leq \beta$,

$$\begin{aligned} \alpha^{\gamma+1} &= \alpha^\gamma \cdot \alpha && \triangleright\ [8] \\ &\leq \beta^\gamma \cdot \alpha && \triangleright\ \text{Induction Hypothesis, Exercise 6.5.8 (ii)} \\ &\leq \beta^\gamma \cdot \beta && \triangleright\ \text{Exercise 6.5.7 (i)} \\ &= \beta^{\gamma+1}. && \triangleright\ [8] \end{aligned}$$

Now, take any limit ordinal $\gamma \neq 0$ and assume that $\mathbf{P}(\gamma')$ holds for all ordinals $\gamma' < \gamma$. Take any ordinals α and β with $\alpha \leq \beta$. Take any $\xi < \alpha^\gamma$. Then, there exists $\delta < \gamma$ such that $\xi < \alpha^\delta$ by [8]. We then have

$$\begin{aligned} \xi &< \alpha^\delta \\ &\leq \beta^\delta && \triangleright\ \text{Induction Hypothesis} \\ &\leq \beta^\gamma. && \triangleright\ [9] \end{aligned}$$

Hence, $\alpha^\gamma \leq \beta^\gamma$. The result follows from The Transfinite Induction Principle: Second Version.

(ii) We will make use of The Transfinite Induction Principle: Second Version on γ. Let $\mathbf{P}(\gamma)$ be the property "for all ordinals α and β, $\alpha > 1 \land \beta < \gamma \implies \alpha^\beta < \alpha^\gamma$." $\mathbf{P}(0)$ evidently holds by vacuous truth.

Take any ordinal γ and assume $\mathbf{P}(\gamma)$ holds. Take any ordinals α and β with $\alpha > 1$ and $\beta < \gamma + 1$. Then,

$$\begin{aligned} \alpha^\beta &\leq \alpha^\gamma && \triangleright\ \text{Induction Hypothesis} \\ &< \alpha^\gamma \cdot \alpha && \triangleright\ \text{Exercise 6.5.7 (i)} \\ &= \alpha^{\gamma+1}. && \triangleright\ [8] \end{aligned}$$

Now, take any limit ordinal $\gamma \neq 0$ and assume $\mathbf{P}(\gamma')$ holds for all $\gamma' < \gamma$. Take any ordinals α and β with $\alpha > 1$ and $\beta < \gamma$. Then, as $\beta + 1 < \gamma$,

$$\begin{aligned} \alpha^\beta &< \alpha^{\beta+1} && \triangleright\ \text{Induction Hypothesis} \\ &\leq \alpha^\gamma. && \triangleright\ [9] \end{aligned}$$

The result follows from The Transfinite Induction Principle: Second Version. □

Exercise 6.5.15

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

$$\begin{aligned}\omega + \omega\cdot\omega &= \omega\cdot 1 + \omega\cdot\omega \\ &= \omega\cdot(1+\omega) && \triangleright \text{ Exercise 6.5.2} \\ &= \omega\cdot\omega. && \triangleright\ 1+\omega=\omega\end{aligned}$$

Hence, $\omega^2 = \omega\cdot\omega$ satisfies the property.

Assume an ordinal ξ satisfies $\omega + \xi = \xi$. Let $\mathbf{P}(n)$ be the property "$n \in \omega$ and $\xi \geq \omega\cdot n$." $\mathbf{P}(0)$ holds since $\omega\cdot 0 = 0$.

Take any $n\in\omega$ and assume $\mathbf{P}(n)$. Then,

$$\begin{aligned}\omega\cdot(n+1) &= \omega\cdot(1+n) && \triangleright + \text{ is Commutative} \\ &= \omega+\omega\cdot n && \triangleright\ [5] \\ &\leq \omega+\xi && \triangleright \text{ Induction Hypothesis, Lemma 6.5.3 (i)} \\ &= \xi.\end{aligned}$$

Hence, by The Induction Principle, $\xi \geq \omega\cdot n$ for all $n\in\omega$. Thus, $\xi \geq \sup\{\,\omega\cdot 0, \omega\cdot 1, \omega\cdot 1, \cdots\} = \omega^2$. Hence, the least such ordinal is ω^2.

(ii) We have

$$\begin{aligned}\omega\cdot\omega^{\omega} &= \omega^1\cdot\omega^{\omega} \\ &= \omega^{1+\omega} && \triangleright \text{ (i)} \\ &= \omega^{\omega}. && \triangleright\ 1+\omega=\omega\end{aligned}$$

Hence, ω^{ω} satisfies the property.

Assume an ordinal $\xi \neq 0$ satisfies $\omega\cdot\xi = \xi$. Let $\mathbf{P}(n)$ be the property "$n\in\omega$ and $\xi \geq \omega^n$." $\mathbf{P}(0)$ holds since $\xi\neq 0$.

Take any $n\in\omega$ and assume $\mathbf{P}(n)$. Then,

$$\begin{aligned}\omega^{n+1} &= \omega^{1+n} && \triangleright + \text{ is Commutative} \\ &= \omega\cdot\omega^n && \triangleright \text{ (i)} \\ &\leq \omega\cdot\xi && \triangleright \text{ Induction Hypothesis, Exercise 6.5.7 (i)} \\ &= \xi.\end{aligned}$$

Hence, by The Induction Principle, $\xi \geq \omega^n$ for all $n\in\omega$. Therefore, $\xi \geq \sup\{\,\omega^0, \omega^1, \omega^2, \cdots\} = \omega^{\omega}$. Hence, the least such ordinal is ω^{ω}.

(iii) Let $\mathbf{G}(\alpha)$ be an operation defined by

$$\mathbf{G}(\alpha) \triangleq \begin{cases} \omega^{\alpha} & \text{if } \alpha \text{ is an ordinal} \\ \varnothing & \text{otherwise.}\end{cases}$$

Then, by Theorem 6.3.5, there exists a sequence $\langle\, a_n \mid n\in\omega \,\rangle$ such that $a_0 = \omega$ and $a_{n+1} = \mathbf{G}(a_n) = \omega^{a_n}$ for all $n\in\omega$ so that $\varepsilon = \sup\{\, a_n \mid n\in\omega\,\}$.

> ***Claim 1.*** $\forall n\in\omega$, $a_n < a_{n+1}$.
>
> *Proof.* Let $\mathbf{P}(n)$ be the property "$a_n < a_{n+1}$." $\mathbf{P}(0)$ holds evidently.

Take any $n \in \omega$ and assume $\mathbf{P}(n)$. Then,

$$\begin{aligned} a_{n+1} &= \omega^{a_n} \\ &< \omega^{a_{n+1}} && \triangleright \text{ Induction Hypothesis, Exercise 6.5.14 (ii)} \\ &= a_{n+2}. \end{aligned}$$

The result follows from The Induction Principle. □

Note that Claim 1 asserts that ε is a limit ordinal.

Take any $\xi < \omega^\varepsilon$. Then, there exists $\delta < \varepsilon$ such that $\xi < \omega^\delta$ by Claim 1. There exists $n \in \omega$ such that $\delta < a_n$. Then,

$$\begin{aligned} \xi &< \omega^\delta \\ &< \omega^{a_n} && \triangleright \text{ Exercise 6.5.14 (ii)} \\ &= a_{n+1} \\ &\leq \varepsilon. \end{aligned}$$

Hence, $\omega^\varepsilon \leq \varepsilon$.

Take any $\xi < \varepsilon$. Then, there exists $n \in \omega$ such that $\xi < a_n$. Then,

$$\begin{aligned} \xi &< a_n \\ &< a_{n+1} && \triangleright \text{ Claim 1} \\ &= \omega^{a_n} \\ &\leq \omega^\varepsilon; && \triangleright \text{ Exercise 6.5.14 (ii)} \end{aligned}$$

hence $\varepsilon \leq \omega^\varepsilon$. Therefore, $\omega^\varepsilon = \varepsilon$.

Suppose $\xi < \varepsilon$ is an ordinal such that $\omega^\xi = \xi$ for the sake of contradiction. Then, by the same argument, $\omega^\xi = \xi < \omega^\varepsilon$, which is a contradiction. □

Exercise 6.5.16

Let α and β be ordinals. Define $s\colon (\beta \to \alpha) \to \mathcal{P}(\beta)$ be defined by

$$s(f) \triangleq \{\, \xi < \beta \mid f(\xi) \neq 0 \,\}.$$

(The domain of s is the set of functions on β into α.) Let

$$S(\beta, \alpha) \triangleq \{\, f : \beta \to \alpha \mid s(f) \text{ is finite} \,\}.$$

Define $\prec$ on $S(\beta, \alpha)$ as follows:

$$f \prec g \iff \exists \xi_0 < \beta,\ f(\xi_0) < g(\xi_0) \land [\forall \xi < \beta,\ (\xi_0 < \xi \implies f(\xi) = g(\xi))].$$

Then, $(S(\beta, \alpha), \preceq)$ is isomorphic to α^β.

Proof. We first have to justify that $\prec$ is a strict total ordering of $S(\beta, \alpha)$.

Claim 1. $\prec$ is a strict total ordering of $S(\beta, \alpha)$.

Proof.

- Suppose there exist $f, g \in S(\beta, \alpha)$ such that $f \prec g$ and $g \prec f$ for the sake of contradiction. There exist $\xi_0, \xi_1 \in \beta$ such that

(a) $f(\xi_0) < g(\xi_0) \wedge [\forall \xi < \beta, (\xi_0 < \xi \implies f(\xi) = g(\xi))]$ and
(b) $f(\xi_1) > g(\xi_1) \wedge [\forall \xi < \beta, (\xi_1 < \xi \implies f(\xi) = g(\xi))]$.

WLOG, $\xi_0 \le \xi_1$. However, we cannot have $\xi_0 = \xi_1$ as $\in_\beta$ is a strict ordering. Hence, $\xi_0 < \xi_1$; thus $f(\xi_1) = g(\xi_1)$ by (a), which is impossible by (b). Hence, $\prec$ is asymmetric on $S(\beta,\alpha)$. ✓

- Assume $f \prec g$ and $g \prec h$ where $f, g, h \in S(\beta,\alpha)$. There exist $\xi_0, \xi_1 \in \beta$ such that
  (a) $f(\xi_0) < g(\xi_0) \wedge [\forall \xi < \beta, (\xi_0 < \xi \implies f(\xi) = g(\xi))]$ and
  (b) $g(\xi_1) < h(\xi_1) \wedge [\forall \xi < \beta, (\xi_1 < \xi \implies g(\xi) = h(\xi))]$.

  Let $\xi_2 \triangleq \max\{\xi_0, \xi_1\}$. Then, we have $f(\xi_2) < h(\xi_2)$ and, for all $\xi_2 < \xi < \beta$, then $f(\xi) = g(\xi) = h(\xi)$. Hence, $f \prec h$; $\prec$ is transitive on $S(\beta,\alpha)$. ✓
- Take any $f, g \in S(\beta,\alpha)$ with $f \ne g$. Let $A \triangleq \{\xi < \beta \mid f(\xi) \ne g(\xi)\}$. As $A \subseteq s(f) \cup s(g)$, A is nonempty and finite by Lemma 4.2.6 and Theorem 4.2.4. Hence, we may let $\gamma \triangleq \max A$. If $f(\gamma) < g(\gamma)$, then $f \prec g$; if $g(\gamma) < f(\gamma)$, then $g \prec f$. Hence, $\preceq$ is a total ordering of $S(\beta,\alpha)$. ✓ □

We shall conduct The Transfinite Induction Principle: Second Version on β. Let $\mathbf{P}(\beta)$ be the property "For all ordinals α, $(S(\beta,\alpha),\preceq)$ is isomorphic to α^β." We have $\mathbf{P}(0)$ since $|S(\beta,\alpha)| = |\{\varnothing\}| = 1$.

Take any ordinal β and assume $\mathbf{P}(\beta)$. Let $h\colon S(\beta,\alpha) \hookrightarrow\!\!\!\!\rightarrow \alpha^\beta$ be an isomorphism between $S(\beta,\alpha)$ and α^β. First, note that:

- $f \in S(\beta+1,\alpha)$ if and only if $f\big|_\beta \in S(\beta,\alpha)$.
- For $f, g \in S(\beta+1,\alpha)$ such that $f(\beta) = g(\beta)$, $f \prec g \iff f\big|_\beta \prec g\big|_\beta$.
- For $f, g \in S(\beta+1,\alpha)$, if $f(\beta) < g(\beta) \implies f \prec g$.

Define a function $h'\colon S(\beta+1,\alpha) \hookrightarrow\!\!\!\!\rightarrow \alpha \times \alpha^\beta$ by $f \mapsto \Big(f(\beta), h\Big(f\big|_\beta\Big)\Big)$. Then, h' is an isomorphism between $(S(\beta+1,\alpha),\preceq)$ and $\alpha \times \alpha^\beta$, which has the order type $\alpha^\beta \cdot \alpha = \alpha^{\beta+1}$ by Theorem 6.5.6.

Take any limit ordinal $\beta \ne 0$ and assume $\mathbf{P}(\beta')$ holds for all $\beta' < \beta$. Fix any ordinal α. If $\alpha = 0$ or $\alpha = 1$, it is immediate; hence assume $\alpha > 1$. For each $\beta' < \beta$, let $h_{\beta'}$ denote the isomorphism between $S(\beta',\alpha)$ and $\alpha^{\beta'}$. Note that:

- For each $\beta' < \beta$ and $f \in S(\beta,\alpha)$, $f\big|_{\beta'} \in S(\beta',\alpha)$.

Define $h\colon S(\beta,\alpha) \twoheadrightarrow \alpha^\beta$ by $f \mapsto h_{\gamma+1}\Big(f\big|_{\gamma+1}\Big)$ where $\gamma = \max s(f)$. (It is easy to prove that $\operatorname{ran} h = \alpha^\beta$.) Take any $f, g \in S(\beta,\alpha)$ with $f \prec g$. Let $\gamma_1 = \max s(f)$ and $\gamma_2 = \max s(g)$. We must have $\gamma_1 \le \gamma_2$ since $f \prec g$; and $f\big|_{\gamma_2+1} \prec g\big|_{\gamma_2+1}$ as $f(\xi) = g(\xi)$ for all $\gamma_2 < \xi < \beta$. If $\gamma_1 = \gamma_2$, then $h(f) \prec h(g)$ by definition.

If $\gamma_1 < \gamma_2$, as $A \triangleq \Big\{f \cup \{(\xi,0) \mid \gamma_1 < \xi \le \gamma_2\} \,\Big|\, f \in S(\gamma_1+1,\alpha)\Big\}$, which is isomorphic to $S(\gamma_1+1,\alpha)$ (under $\prec$), is an initial segment of $S(\gamma_2+1,\alpha)$, we have $h(f) < h(g)$ since $f\big|_{\gamma_1+1} \in S(\gamma_1+1,\alpha)$ while $g\big|_{\gamma_2+1} \notin A$. Hence, h is an isomorphism. The result follows from The Transfinite Induction Principle: Second Version. □

6.6 The Normal Form

Lemma 6.6.1

Let α and β be ordinals.
(i) If $0 < \alpha \le \beta$, then $\{\xi \in \mathrm{Ord} \mid \alpha \cdot \xi \le \beta\}$ has a greatest element.
(ii) If $1 < \alpha \le \beta$, then $\{\xi \in \mathrm{Ord} \mid \alpha^\xi \le \beta\}$ has a greatest element.

Proof.

(i) Since $\beta < \beta + 1 \leq \alpha \cdot (\beta + 1)$ by Exercise 6.5.7 (i), 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 Schema of Comprehension and Theorem 6.2.13 (iv).

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, there exists γ such that $\delta_0 = \gamma + 1$, and $\gamma = \max\{\, \xi \in \mathrm{Ord} \mid \alpha \cdot \xi \leq \beta \,\}$.

(ii) Replace every multiplication in the proof of (i) into exponentiation. □

Lemma 6.6.2

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. $\gamma \triangleq \max\{\, \xi \in \mathrm{Ord} \mid \alpha \cdot \xi \leq \beta \,\}$ exists by Lemma 6.6.1 (i). By Lemma 6.5.4, there exists ρ such that $\beta = \alpha \cdot \gamma + \rho$. Then, we have $\rho < \alpha$; otherwise $\gamma + 1$ would satisfy $\alpha \cdot (\gamma + 1) \leq \beta$ by [5]. Hence, the existence is shown.

Let $\beta = \alpha \cdot \gamma_1 + \rho_1 = \alpha \cdot \gamma_2 + \rho_2$ where $\rho_1, \rho_2 < \alpha$. Suppose $\gamma_1 < \gamma_2$ for the sake of contradiction. Then, as $\gamma_1 + 1 \leq \gamma_2$,

$$\begin{aligned}
\alpha \cdot \beta_1 + (\alpha + \rho_2) &= (\alpha \cdot \beta_1 + \alpha) + \rho_2 && \triangleright \text{ Lemma 6.5.3 (iii)} \\
&= \alpha \cdot (\beta_1 + 1) + \rho_2 && \triangleright \text{ [5]} \\
&\leq \alpha \cdot \beta_2 + \rho_2 && \triangleright \text{ Exercise 6.5.7 (i), Exercise 6.5.8 (i)} \\
&= \alpha \cdot \beta_1 + \rho_1;
\end{aligned}$$

thus $\alpha \leq \alpha + \rho_2 \leq \rho_1$ by Lemma 6.5.3 (i), which contradicts $\rho_1 < \alpha$. Hence, $\gamma_1 = \gamma_2$. $\rho_1 = \rho_2$ follows from Lemma 6.5.3 (ii). □

Theorem 6.6.3

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 $k_1, k_2, \cdots, k_n$ are nonzero finite ordinals, and $\beta_1 > \beta_2 > \cdots > \beta_n$. The expression is called the *normal form* of α.

Proof. Let $\mathbf{P}(\alpha)$ be the property stated in the theorem. $\mathbf{P}(1)$ is clearly true since $1 = \omega^0 \cdot 1$ is unique.

Fix any ordinal $\alpha > 1$ and assume $\mathbf{P}(\alpha')$ holds for all $0 < \alpha' < \alpha$. By Lemma 6.6.1 (ii), there exists $\beta_1 \triangleq \max\{\, \xi \in \mathrm{Ord} \mid \omega^\xi \leq \alpha \,\}$. Then, there exists k_1 and ρ such that $\alpha = \omega^{\beta_1} \cdot k_1 + \rho$ and $\rho < \omega_1^\beta$. If $k_1 \geq \omega$, then we have

$$\begin{aligned}
\omega^{\beta_1 + 1} &= \omega^{\beta_1} \cdot \omega && \triangleright \text{ [5]} \\
&\leq \omega^{\beta_1} \cdot k_1 && \triangleright \text{ Exercise 6.5.7 (i)} \\
&\leq \alpha, && \triangleright \text{ Lemma 6.5.3 (i)}
\end{aligned}$$

contradicting the maximality of β_1. Hence, k_1 is finite.

By the induction hypothesis,

$$\rho = \omega^{\beta_2} \cdot k_2 + \omega^{\beta_3} \cdot k_3 + \cdots + \omega^{\beta_n} \cdot k_n$$

where $k_2, k_3, \cdots, k_n$ are nonzero finite ordinals, and $\beta_2 > \beta_3 > \cdots > \beta_n$. Hence, the existence is shown.

Claim 1. If $\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n$ is in its normal form and $\beta_1 < \gamma$, then $\alpha > \omega^{\gamma}$.

Proof. For any $k < \omega$ and ordinals $\xi < \zeta$, we have

$$\begin{aligned} \omega^{\xi} \cdot k &< \omega^{\xi} \cdot \omega && \triangleright \text{ Exercise 6.5.7 (i)} \\ &= \omega^{\xi+1} && \triangleright \text{ [8]} \qquad [*] \\ &\leq \omega^{\zeta}. && \triangleright \text{ Exercise 6.5.14 (ii)} \end{aligned}$$

Hence, one may repeatedly apply [$*$] to acquire $\alpha \geq \omega^{\beta_1} \cdot \sum_{i=1}^{n} k_i$ (rigorously with The Induction Principle on n), hence $\alpha > \omega^{\gamma}$ once again by [$*$]. □

Let

$$\begin{aligned} \alpha &= \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n \\ &= \omega^{\gamma_1} \cdot \ell_1 + \omega^{\gamma_2} \cdot \ell_2 + \cdots + \omega^{\gamma_m} \cdot \ell_m \end{aligned}$$

be two normal forms of α. By Claim 1, we must have $\beta_1 = \gamma_1$. Let

$$\begin{aligned} \delta &= \omega^{\beta_1} = \omega^{\gamma_1} \\ \rho &= \omega^{\beta_2} \cdot k_2 + \omega^{\beta_3} \cdot k_3 + \cdots + \omega^{\beta_n} \cdot k_n \\ \sigma &= \omega^{\gamma_2} \cdot \ell_2 + \omega^{\gamma_3} \cdot \ell_3 + \cdots + \omega^{\gamma_m} \cdot \ell_m \end{aligned}$$

so that $\alpha = \delta \cdot k_1 + \rho = \delta \cdot \ell_1 + \sigma$. Once again by Claim 1, ρ and σ are less than δ. Then, by Lemma 6.6.2, $k_1 = \ell_1$ and $\rho = \sigma$. By the induction hypothesis, $n = m$, and $k_i = \ell_i$ and $\beta_i = \gamma_i$ for all $1 < i \leq n$. The result follows from The Transfinite Induction Principle: First Version. □

Definition 6.6.4: Weak Goodstein Sequence

Let $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a function which is defined by:

$$f(n, b) = \sum_{i=0}^{m} c_i \cdot (b+1)^i - 1 \qquad \text{where } n = \sum_{i=0}^{m} c_i \cdot b^i \text{ is the base-}b\text{ representation of } n$$

for each $n > 0$ and $b > 1$, and $f(n, b) = 0$ otherwise.

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 $k \in \mathbb{N}$, $m_{k+1} = f(m_k, k+2)$,

whose existence and uniqueness is guaranteed by The Recursion Theorem. In other words, the next entry of m_k is obtained by writing m_k in base-$(k+2)$, replacing the bases with $k+3$, and then subtracting one.

Note:-

First few terms of the weak Goodstein sequence starting at $m = 21$ are:

$$\begin{aligned}
m_0 &= 21 = 2^4 + 2^2 + 1 \\
m_1 &= 3^4 + 3^2 = 90 \\
m_2 &= 4^4 + 4^2 - 1 = 4^4 + 3 \cdot 4^1 + 3 = 271 \\
m_3 &= 5^4 + 3 \cdot 5^1 + 2 = 642 \\
m_4 &= 6^4 + 3 \cdot 6^1 + 1 = 1315 \\
m_5 &= 7^4 + 3 \cdot 7^1 = 2422 \\
m_6 &= 8^4 + 3 \cdot 8^1 - 1 = 8^4 + 2 \cdot 8^1 + 7 = 4119 \\
m_7 &= 9^4 + 2 \cdot 9^1 + 6 = 6585 \\
m_8 &= 10^4 + 2 \cdot 10^1 + 5 = 10025
\end{aligned}$$

Lemma 6.6.5

There is no strictly decreasing infinite sequence of ordinal numbers. An infinite sequence f of ordinal numbers is *strictly decreasing* if $\forall i \in \mathbb{N}$, $f(n+1) < f(n)$.

Proof. Suppose f is a strictly decreasing infinite sequence of ordinal numbers for the sake of contradiction. Then, as $\operatorname{ran} f$ is a set of ordinal numbers, by Theorem 6.2.13 (iv), there exists $n \in \mathbb{N}$ such that, $f(n) \leq f(m)$ for all $m \in \mathbb{N}$. However, we must have $f(n) > f(n+1)$, which is a contradiction. □

Theorem 6.6.6

For each $m \in \mathbb{N}_{>0}$, the weak Goodstein sequence starting at m eventually terminates with $m_n = 0$ for some n.

Proof. Take any $m > 0$ and let $\langle m_i \rangle_{i \in \mathbb{N}}$ be the weak Goodstein sequence starting at m.

Suppose $m_i > 0$ for all $i \in \mathbb{N}$ for the sake of contradiction. For each $a \in \mathbb{N}$, we may write m_a in base-$(a+2)$ as:

$$m_a = (a+2)^{d_1} \cdot k_1 + (a+2)^{d_2} \cdot k_2 + \cdots + (a+2)^{d_n} \cdot k_n$$

where $\omega > d_1 > d_2 > \cdots > d_n$ and $k_i < a+2$, and let

$$\alpha_a \triangleq \omega^{d_1} \cdot k_1 + \omega^{d_2} \cdot k_2 + \cdots + \omega^{d_n} \cdot k_n.$$

Then, the sequence $\langle \alpha_0, \alpha_1, \cdots \rangle$ is clearly strictly decreasing, contradicting Lemma 6.6.5. □

Note:-

The *hereditary base-n notation* is a base-n notation but every exponent should itself be a number less than n or written in a hereditary base-n notation. For instance,

$$100 = 3^{3^1} + 2 \cdot 3^2 + 1$$

is the hereditary base-3 notation of 100.

Definition 6.6.7: Goodstein Sequence

The Goodstein sequence starting at $m > 0$ is the sequence where $m_0 = m$ and the next entry of m_k is obtained by writing m_k in the hereditary base-$(k+2)$ notation, replacing every occurrence of $k+2$ with $k+3$, and subtracting one.

Note:-

First few terms of Goodstein sequence starting at $m = 21$ are:

$$
\begin{aligned}
m_0 &= 2^{2^{2^1}} + 2^{2^1} + 1 && = 21 \\
m_1 &= 3^{3^{3^1}} + 3^{3^1} && = 7625597485014 \\
m_2 &= 4^{4^{4^1}} + 4^{4^1} - 1 = 4^{4^{4^1}} + 3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4^1 + 3 && \approx 1.340781 \times 10^{155} \\
m_3 &= 5^{5^{5^1}} + 3 \cdot 5^3 + 3 \cdot 5^2 + 3 \cdot 5^1 + 2 && \approx 1.911013 \times 10^{2184} \\
m_4 &= 6^{6^{6^1}} + 3 \cdot 6^3 + 3 \cdot 6^2 + 3 \cdot 6^1 + 1 && \approx 2.659120 \times 10^{36305} \\
m_5 &= 7^{7^{7^1}} + 3 \cdot 7^3 + 3 \cdot 7^2 + 3 \cdot 7^1 && \approx 3.759824 \times 10^{695974} \\
m_6 &= 8^{8^{8^1}} + 3 \cdot 8^3 + 3 \cdot 8^2 + 2 \cdot 8^1 + 7 && \approx 6.014521 \times 10^{15151335}
\end{aligned}
$$

Theorem 6.6.8 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. Take any $m > 0$ and let $\langle m_i \rangle_{i \in \mathbb{N}}$ be the Goodstein sequence starting at m.

Suppose $m_i > 0$ for all $i \in \mathbb{N}$ for the sake of contradiction. For each $a \in \mathbb{N}$, we get ω_a by writing m_a in the hereditary base-$(a+2)$ notation and replacing every $a+2$ with ω. Then, the sequence $\langle \alpha_0, \alpha_1, \cdots \rangle$ is clearly strictly decreasing, contradicting Lemma 6.6.5. $\square$

Chapter 7

Alephs

7.1 Initial Ordinals

Definition 7.1.1: Initial Ordinal

An ordinal number α is called an *initial ordinal* if it is not equipotent to any $\beta < \alpha$.

Example 7.1.2

- Every natural number is an initial ordinal.
- ω is an initial ordinal. (Corollary 4.2.3 (iii))
- None of $\omega+1, \omega+2, \cdots, \omega\cdot\omega, \cdots, \omega^{\omega}, \cdots$ is initial.

Theorem 7.1.3

Each well-orderable set X is equipotent to a unique initial ordinal number.

Proof. By The Counting Theorem, there exists an ordinal number α such that $|X| = |\alpha|$. Hence, $\alpha_0 \triangleq \min\{\, \alpha \in \mathrm{Ord} \mid |X| = |\alpha| \,\}$ exists by The Axiom Schema of Comprehension and Theorem 6.2.13 (iv). Then, α_0 is a limit ordinal because $\exists \beta < \alpha_0$, $|\alpha_0| = |\beta|$ would imply $|\beta| = |X|$, which contradicts the minimality of α_0.

If α_1 and α_2 are different initial ordinals, then we cannot have $|\alpha_1| = |\alpha_2|$ since one of them is less than the other. Hence, the uniqueness is shown. □

Definition 7.1.4: 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 α. This is justified by Theorem 7.1.3.

Lemma 7.1.5

Let A be any set. Then, there exists the least ordinal number α such that $|\alpha| \not\preceq |A|$.

Proof. By The Counting Theorem, for each well-ordered set (W, R) where $W \subseteq A$, there exists a unique ordinal α such that α is isomorphic to (W, R). Hence, by The Axiom Schema of Replacement, the set

$$H \triangleq \{\, \alpha \in \mathrm{Ord} \mid \exists R \subseteq A \times A,\ (\operatorname{field} R, R) \cong \alpha \,\}$$

exists.

Claim 1. $\forall \alpha \in \mathrm{Ord}, (|\alpha| \leq |A| \iff \alpha \in H)$

Proof.
($\Rightarrow$) It is direct from the definition.
($\Leftarrow$) Let $f : \alpha \hookrightarrow A$ and $W \triangleq \operatorname{ran} f$. Define $R \triangleq \{ (f(\beta), f(\gamma)) \mid \beta < \gamma < \alpha \}$. Then, (W, R) is a well-ordered set and f is an isomorphism between α and (W, R). ☐

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 6.2.12; thus $|\alpha| \leq |\beta| \leq |A|$ by Exercise 4.1.3, which implies $\alpha \in H$ by Claim 1. Hence, $H \in \mathrm{Ord}$.

We have $H \notin H$ by Lemma 6.2.9; hence $|H| \not\leq |A|$ by Claim 1. Moreover, every $\alpha < H$ satisfies $|\alpha| \leq |A|$ by Claim 1; H is the least ordinal we are looking for. ☐

Definition 7.1.6: Hartogs Number

For any 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 7.1.5.

Lemma 7.1.7

$\forall \alpha \in \mathrm{Ord}, |\alpha| < |h(\alpha)|$

Proof.

- If $\alpha = h(\alpha)$, it contradicts $|h(\alpha)| \not\leq |\alpha|$.
- If $\alpha > h(\alpha)$, then we have $|h(\alpha)| \leq |\alpha|$ by Exercise 4.1.3 and Lemma 6.2.12, which is a contradiction.

Hence, we must have $\alpha < h(\alpha)$. Then, by Exercise 4.1.3 and Lemma 6.2.12, $|\alpha| \leq |h(\alpha)|$; but $|\alpha| \neq |h(\alpha)|$. Therefore, the result follows. ☐

Lemma 7.1.8

For any A, $h(A)$ is an initial ordinal.

Proof. Suppose that $\exists \beta < h(A), |\beta| = |h(A)|$. Then, $|\beta| \leq |A|$ by definition of $h(A)$ while we also have $|\beta| = |h(A)|$, which contradicts $|h(A)| \not\leq |A|$. ☐

Definition 7.1.9

$$
\begin{aligned}
\omega_0 &= \omega \\
\omega_{\alpha+1} &= h(\omega_\alpha) && \text{for all ordinals } \alpha \\
\omega_\alpha &= \sup\{ \omega_\beta \mid \beta < \alpha \} && \text{for all nonzero limit ordinals } \alpha
\end{aligned}
$$

Note:-

Since $|\omega_{\alpha+1}| \not\leq |\omega_\alpha|$, we have $|\omega_\alpha| < |\omega_{\alpha+1}|$ as one of two ordinals must have the other as its subset. Therefore, with The Transfinite Induction Principle: Second Version, one might be able to prove $\alpha < \beta \implies |\omega_\alpha| < |\omega_\beta|$.

Theorem 7.1.10

(i) For each $\alpha \in \mathrm{Ord}$, ω_α is an infinite initial ordinal number.
(ii) If Ω is an infinite initial ordinal number, then $\exists \alpha \in \mathrm{Ord}, \Omega = \omega_\alpha$.

Proof.

(i) ω_α is infinite for all $\alpha \in \mathrm{Ord}$ by the discussion above. If $\alpha = 0$ or α is a successor ordinal, then ω_α is initial ordinal by Lemma 7.1.8.

Take any nonzero limit ordinal α and suppose $\exists\gamma < \omega_\alpha, |\gamma| = |\omega_\alpha|$ for the sake of contradiction. Then, there exists $\beta < \alpha$ such that $\gamma < \omega_\beta$, which implies $|\omega_\alpha| = |\gamma| \le |\omega_\beta| < |\omega_\alpha|$.

(ii) We first prove the following claim.

> ***Claim 1.*** For each ordinal α and infinite initial ordinal $\Omega < \omega_\alpha$, $\exists\gamma < \alpha$, $\Omega = \omega_\gamma$.
>
> ***Proof.*** We will conduct the transfinite induction on α. Let $\mathbf{P}(\alpha)$ be the property "If $\Omega < \omega_\alpha$ is an infinite initial ordinal, then $\exists\gamma < \alpha$, $\Omega = \omega_\gamma$." $\mathbf{P}(0)$ holds since ω_0 is the least infinite initial ordinal.
>
> Take any ordinal α and assume $\mathbf{P}(\alpha)$. Take any infinite initial ordinal $\Omega < \omega_{\alpha+1} = h(\omega_\alpha)$. Then, by Definition 7.1.6, $|\Omega| \le |\omega_\alpha|$. $\omega_\alpha < \Omega$ is not an option since we have $|\omega_\alpha| = |\Omega|$ by Exercise 4.1.3, Lemma 6.2.12, and Theorem 5.1.5, which contradicts the fact that Ω is an initial ordinal. If $\Omega = \omega_\alpha$, then it is done. If $\Omega < \omega_\alpha$, then by $\mathbf{P}(\alpha)$, there exists $\gamma < \alpha < \alpha + 1$ such that $\Omega = \omega_\gamma$.
>
> Now, take any nonzero limit ordinal α and assume $\mathbf{P}(\alpha')$ holds for all $\alpha' < \alpha$. Take any infinite initial ordinal $\Omega < \omega_\alpha$. Then, by Definition 7.1.9, there exists $\beta < \alpha$ such that $\Omega < \omega_\beta$. Hence, by the induction hypothesis, $\Omega = \omega_\gamma$ for some $\gamma < \beta < \alpha$. $\square$

One may readily show that $\alpha \le \omega_\alpha$ for all $\alpha \in \mathrm{Ord}$ with The Transfinite Induction Principle: Second Version. Take any infinite limit ordinal Ω. Then, $\Omega \le \omega_\Omega < \omega_{\Omega+1}$. By Claim 1, there exists an ordinal $\gamma \le \Omega$ such that $\Omega = \omega_\gamma$. $\square$

Note:-

- Every infinite well-orderable set is equipotent to a unique infinite initial ordinal number. (Theorem 7.1.3)
- α is an infinite initial ordinal if and only if $\alpha = \omega_\gamma$ for some $\gamma \in \mathrm{Ord}$. (Theorem 7.1.10)

Definition 7.1.11: Alephs

$\aleph_\alpha = \omega_\alpha$ for each $\alpha \in \mathrm{Ord}$. They represent cardinalities of well-orderable infinite sets.

Selected Problems

Exercise 7.1.1

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 The Counting Theorem, there exists $\alpha \in \mathrm{Ord}$ such that $(X, R) \cong \alpha$. Let $f : X \hookrightarrow\!\!\!\!\rightarrow \alpha$.

By Theorem 6.2.15, $\omega \subseteq \alpha$. By Exercise 4.3.2, there exists $g : \omega \hookrightarrow\!\!\!\!\rightarrow (\omega \cup \{\alpha\})$. Define $f' : X \hookrightarrow\!\!\!\!\rightarrow (\alpha + 1)$ 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 $\alpha + 1$. $\square$

Exercise 7.1.2

Let $\alpha, \beta \in \mathrm{Ord}$ where α and β are countable. Then, $\alpha + \beta$, $\alpha \cdot \beta$, and α^β are countable.

Proof. This is a special case of Exercise 7.2.4. □

Exercise 7.1.3

$\forall A, \exists f : \mathcal{P}(A \times A) \twoheadrightarrow h(A)$

Proof. For each well-ordering R of $W \subseteq A$, let α_R be the unique ordinal isomorphic to (W, R) thanks to The Counting Theorem. Note that $|\alpha_R| = |A| < |h(A)|$ by Lemma 7.1.7, and thus $\alpha_R < h(A)$. Define a function $f : \mathcal{P}(A \times A) \to h(A)$ 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 7.1.5, which in turn equals $h(A)$. □

Exercise 7.1.4

$\forall A, |A| < |A| + |h(A)|$

Proof. WLOG, $A \cap h(A) = \varnothing$. 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 $|h(A)| \not\leq |A|$. □

Exercise 7.1.5

$\forall A, |h(A)| < |\mathcal{P}(\mathcal{P}(A \times A))|$

Proof. As in the proof of Lemma 7.1.5, $\alpha \in h(A)$ if and only if there exists some $R \subseteq A \times A$ such that $(\operatorname{field} R, R)$ is isomorphic to α. Define $f : \mathcal{P}(h(A)) \to \mathcal{P}(\mathcal{P}(A \times A))$ by

$$X \mapsto \{ R \subseteq A \times A \mid \exists \alpha \in X, (\operatorname{field} R, R) \cong \alpha \}.$$

Then, f is injective; thus $|h(A)| < |\mathcal{P}(h(A))| \leq |\mathcal{P}(\mathcal{P}(A \times A))|$ by Cantor's Theorem. □

Exercise 7.1.6

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) $\forall \alpha \in \mathrm{Ord}, (\alpha \geq h^*(A) \implies \nexists f : A \twoheadrightarrow \alpha)$.

(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 $\mathrm{Pt}(A)$ be the set of all partitions of A. Let

$$H^* \triangleq \{ \alpha \in \mathrm{Ord} \mid \exists S \in \mathrm{Pt}(A), \exists R \subseteq S \times S, (S, R) \cong \alpha \}.$$

H^* exists by The Counting Theorem and The Axiom Schema of Replacement.

Claim 1. $\forall \alpha \in \mathrm{Ord}, (\exists f : A \twoheadrightarrow \alpha \iff \alpha \in H^*)$

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 on S defined by $R = \{ (f^{-1}[\{\beta\}], f^{-1}[\{\gamma\}]) \mid \beta < \gamma < \alpha \}$ is isomorphic to α since $\operatorname{ran} f = \alpha$. Hence, $\alpha \in H^*$.

($\Leftarrow$) There exist $S \in \mathrm{Pt}(A)$ and $R \subseteq S \times S$ such that $(S,R) \cong \alpha$. Let $g : S \hookrightarrow\!\!\!\!\rightarrow \alpha$ be the isomorphism between (S,R) and α. Define $f : A \to \alpha$ by $a \mapsto g(C)$ where $C \in S$ is the unique element of S such that $a \in C$. Then, $\operatorname{ran} f = \alpha$ as each $C \in S$ is nonempty. $\square$

Claim 1 says that H^* is transitive. Moreover, by Theorem 6.2.13 (iv), H^* is well-ordered by $\in$. Hence, $H^* \in \mathrm{Ord}$.

By Lemma 6.2.9, $H^* \notin H^*$; thus $\nexists f : A \twoheadrightarrow H^*$ by Claim 1. If $\alpha \in H^*$, then $\exists f : A \twoheadrightarrow H^*$ by Claim 1. Therefore, $h^*(A) = H^*$.

(ii) Take any $\alpha \in \mathrm{Ord}$. Assume $\exists f : A \twoheadrightarrow \alpha$. Then, by Claim 1, $\alpha < h^*(A)$.

(iii) Suppose $\exists \beta < h^*(A)$, $|\beta| = |h^*(A)|$ for the sake of contradiction. Then, there exists $f : A \twoheadrightarrow \beta$. Let $g : \beta \hookrightarrow\!\!\!\!\rightarrow h^*(A)$. Then, $g \circ f : A \twoheadrightarrow h^*(A)$, which is a contradiction.

(iv) Take any $\alpha < h(A)$. Then, $\exists g : \alpha \hookrightarrow A$. Now, define $f : A \to \alpha$ by

$$f(a) \triangleq \begin{cases} g^{-1}(a) & \text{if } a \in \operatorname{ran} g \\ 0 & \text{otherwise.} \end{cases}$$

Then, f is onto α; thus $\alpha < h^*(A)$ by Claim 1. Therefore, $h(A) \le h^*(A)$.

(v) Assume $(A, \preceq)$ is a well-ordered set. Take any $\alpha < h^*(A)$. Then, there exists $f : A \twoheadrightarrow \alpha$. Define $g : \alpha \to A$ by $g(\beta) \triangleq \min_{\preceq} f^{-1}[\{\beta\}]$. It is well defined since f is onto α. Then, g is injective; thus $|\alpha| \le |A|$, which implies $\alpha < h(A)$. $\square$

7.2 Addition and Multiplication of Alephs

Note:-

Refer to Section 5.1: Cardinal Arithmetic for definitions of addition and multiplication between two cardinals.

Theorem 7.2.1

$\forall \alpha \in \mathrm{Ord}, \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$

Proof. Take any ordinal α and define $\preceq$ on $\omega_\alpha \times \omega_\alpha$ by

$$(\alpha_1, \alpha_2) \preceq (\beta_1, \beta_2) \iff (\max\{\alpha_1, \alpha_2\}, \alpha_1, \alpha_2) \le_\alpha (\max\{\beta_1, \beta_2\}, \beta_1, \beta_2)$$

where $\le_\alpha$ 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 4.3.6.

Take any ordinal α and assume that $\forall \beta < \alpha$, $\aleph_\beta \cdot \aleph_\beta \le \aleph_\beta$.

Claim 1. 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. Let $\beta \triangleq \max\{\alpha_1, \alpha_2\} + 1$. We have $\beta < \omega_\alpha$. Then, for every $(\xi_1, \xi_2) \in X$, we have $\max\{\xi_1, \xi_2\} \leq \max\{\alpha_1, \alpha_2\} < \beta$ 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 7.1.3, there exists $\gamma < \alpha$ such that $|\beta| \leq \aleph_\gamma$. Therefore,

$$\begin{aligned} |X| &\leq |\beta \times \beta| && \triangleright \text{ Exercise 4.1.3} \\ &\leq \aleph_\gamma \cdot \aleph_\gamma \\ &\leq \aleph_\gamma && \triangleright \text{ Induction Hypothesis} \\ &< \aleph_\alpha. \end{aligned}$$

□

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 1. Hence, $\aleph_\alpha \cdot \aleph_\alpha \leq \aleph_\alpha$. The result follows from The Transfinite Induction Principle: First Version. □

Corollary 7.2.2

(i) $\forall \alpha, \beta \in \mathrm{Ord}, (\alpha \leq \beta \implies \aleph_\alpha \cdot \aleph_\beta = \aleph_\beta)$

(ii) $\forall \alpha \in \mathrm{Ord}, \forall n \in \mathbb{N}, n \cdot \aleph_\alpha = \aleph_\alpha$

Proof.

(i) It is direct that $\aleph_\beta = 1 \cdot \aleph_\beta \leq \aleph_\alpha \cdot \aleph_\beta$. On the other hand, by Theorem 7.2.1, $\aleph_\alpha \cdot \aleph_\beta \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta$. Hence, by Cantor–Bernstein Theorem, $\aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$.

(ii) It is direct that $\aleph_\alpha = 1 \cdot \aleph_\alpha \leq n \cdot \aleph_\alpha$. On the other hand, by Theorem 7.2.1, $n \cdot \aleph_\alpha \leq \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$. Hence, by Cantor–Bernstein Theorem, $\aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$. □

Corollary 7.2.3

(i) $\forall \alpha, \beta \in \mathrm{Ord}, (\alpha \leq \beta \implies \aleph_\alpha + \aleph_\beta = \aleph_\beta)$

(ii) $\forall \alpha \in \mathrm{Ord}, \forall n \in \mathbb{N}, n + \aleph_\alpha = \aleph_\alpha$

Proof.

(i) $\aleph_\beta \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\beta + \aleph_\beta = 2 \cdot \aleph_\beta = \aleph_\beta$.

(ii) $\aleph_\alpha \leq n + \aleph_\alpha \leq \aleph_\alpha + \aleph_\alpha = 2 \cdot \aleph_\alpha = \aleph_\alpha$. □

Selected Problems

Exercise 7.2.3

Let $0 < n < \omega$ and $\alpha \in \mathrm{Ord}$.

(i) $\aleph_\alpha^n = \aleph_\alpha$.

(ii) $|[\aleph_\alpha]^n| = \aleph_\alpha$. (See Exercise 4.3.5 for notation.)

(iii) $|[\aleph_\alpha]^{<\omega}| = \aleph_\alpha$ where $[\aleph_\alpha]^{<\omega} = \bigcup_{n \in \omega} [\aleph_\alpha]^n$.

Proof.

(i) If $\aleph_\alpha^n = \aleph_\alpha$ for some $n \in \omega$, then

$$\begin{aligned} \aleph_\alpha^{n+1} &= \aleph_\alpha^n \cdot \aleph_\alpha \\ &= \aleph_\alpha \cdot \aleph_\alpha && \triangleright \text{ Induction Hypothesis} \\ &= \aleph_\alpha. && \triangleright \text{ Theorem 7.2.1} \end{aligned}$$

Hence, the result follows by The Induction Principle.

(ii) The proof is analogous to that of Exercise 4.3.5.

(iii) By Theorem 7.2.1, there exists $g : \aleph_\alpha \twoheadrightarrow \aleph_\alpha \times \aleph_\alpha$. Define an infinite sequence of functions $\langle a_n \mid n \in \omega \rangle$ recursively by

$$\begin{aligned} &\forall \beta \in \aleph_\alpha, \quad a_0(\beta) = \varnothing \\ &\forall n \in \omega, \forall \beta \in \aleph_\alpha, a_{n+1}(\beta) = a_n(\beta_1) \cup \{\beta_2\} \\ &\qquad\qquad\qquad\qquad \text{where } g(\beta) = (\beta_1, \beta_2). \end{aligned}$$

The existence is justified by The Recursion Theorem. Then, for each $n \in \omega$, $\operatorname{ran} a_n = \bigcup_{i=0}^{n} [\aleph_\alpha]^i$. Hence, one may define $f : \omega \times \aleph_\alpha \twoheadrightarrow [\aleph_\alpha]^{<\omega}$ by $f(n, \beta) = a_n(\beta)$. Since $|\omega \times \aleph_\alpha| = \aleph_0 \cdot \aleph_\alpha = \aleph_\alpha$ by Corollary 7.2.2 (i), there exists $f' : \aleph_\alpha \twoheadrightarrow [\aleph_\alpha]^{<\omega}$. Hence, by Exercise 7.2.5, $|[\aleph_\alpha]^{<\omega}| \leq \aleph_\alpha$. The result follows from Cantor–Bernstein Theorem. □

> **Exercise 7.2.4**
>
> Let $\alpha, \beta, \gamma \in \mathrm{Ord}$, 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 7.2.1 and Corollary 7.2.3.

It is evident that, if β is finite, $|\alpha^\beta| \leq \aleph_\gamma$. One may prove this by The Induction Principle.

By Exercise 6.5.16, $|\alpha^\beta| = |X|$ 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 $A_n \triangleq \left\{ f : \beta \to \alpha \middle| |s(f)| = n \right\} \subseteq X$. Let P_n be the set of all injections on n into β, whose cardinality is at most $\aleph_\gamma^n = \aleph_\gamma$ by Exercise 7.2.3 (i). Hence, for all $0 < n < \omega$,

$$\begin{aligned} |A_n| &= \left| P_n \times \textstyle\prod_{i<n} \alpha \right| \\ &\leq \aleph_\gamma \cdot \aleph_\gamma^n \\ &= \aleph_\gamma. && \triangleright \text{ Exercise 7.2.3 (i)} \end{aligned}$$

Moreover, A_n is well-ordered by $\preceq$ (in Exercise 6.5.16); hence there exists a unique ordinal η_n isomorphic to A_n by The Counting Theorem. 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 $g(n, \xi) = h'_n(\xi)$ Therefore, $|X| \leq |\omega \times \aleph_\gamma| = \aleph_\gamma$ in the similar manner as the proof of Exercise 7.2.3 (iii). □

> **Exercise 7.2.5**
>
> Let $\alpha \in \mathrm{Ord}$ and let f be a function on α. Then, $|\operatorname{ran} f| \leq |\alpha|$.

Proof. Define $g : f[\alpha] \hookrightarrow \alpha$ by $g(x) \triangleq \min f^{-1}[\{x\}]$. Then, g is injective. □

> **Exercise 7.2.6**
>
> Let $X \subseteq \omega_\alpha$ with $|X| < \aleph_\alpha$. Then, $|\omega_\alpha \setminus X| = \aleph_\alpha$.

Proof. The statement is true when $\alpha = 0$. Hence, assume $\alpha > 0$. We already have $|\omega_\alpha \setminus X| \leq \aleph_\alpha$ by Exercise 4.1.3. Suppose $|\omega_\alpha \setminus X| < \aleph_\alpha$ for the sake of contradiction.

By The Counting Theorem, there exist $\beta_1, \beta_2 \in \omega_\alpha$ such that $|\beta_1| = |X|$ and $|\beta_2| = |\omega_\alpha \setminus X|$. Then, there exist $\gamma_1, \gamma_2 \in \alpha$ such that $|\beta_1| \leq \aleph_{\gamma_1}$ and $|\beta_2| \leq \aleph_{\gamma_2}$. Let $\gamma_0 \triangleq \max\{\gamma_1, \gamma_2\}$. Then,

$$\begin{aligned} |\omega_\alpha| &= |X| + |\omega_\alpha \setminus X| \\ &\leq \aleph_{\gamma_1} + \aleph_{\gamma_2} \\ &\leq \aleph_{\gamma_0} + \aleph_{\gamma_0} \\ &= \aleph_{\gamma_0} && \triangleright \text{ Corollary 7.2.3} \\ &< \aleph_\alpha, \end{aligned}$$

which is a contradiction. □

Chapter 8

Axiom of Choice

8.1 The Axiom of Choice and its Equivalents

Definition 8.1.1: 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 8.1.2 Well-Ordering Theorem

A set A can be well-ordered if and only if the set $\mathcal{P}(A)$ has a choice function.

Proof.

$(\Rightarrow)$ Assume $\preceq$ well-orders A. Define $g : \mathcal{P}(A) \to A$ 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 of $\mathcal{P}(A)$.

$(\Leftarrow)$ Fix any choice function $g : \mathcal{P}(A) \to A$ of $\mathcal{P}(A)$ and any $a \notin A$. Let $\mathbf{G}(x)$ be the operation defined by

$$\mathbf{G}(x) \triangleq \begin{cases} g(A \setminus \operatorname{ran} x) & \text{if } x \text{ is a function and } A \setminus \operatorname{ran} x \neq \varnothing \\ a & \text{otherwise.} \end{cases}$$

Then, by The Transfinite Recursion Theorem, there exists an operation $\mathbf{F}(x)$ such that $\forall \alpha \in \mathrm{Ord},\ \mathbf{F}(\alpha) = \mathbf{G}\left(\mathbf{F}\big|_{\alpha}\right)$.

> ***Claim 1.*** There exists $\lambda < h(A)$ such that $\mathbf{F}(\lambda) = a$.
>
> ***Proof.*** Assume $\alpha < \beta$ and $\mathbf{F}(\beta) \neq a$. Then, $\mathbf{F}(\beta) \in A \setminus \operatorname{ran}\left(\mathbf{F}\big|_{\beta}\right)$ and $\mathbf{F}(\alpha) \in \left(\mathbf{F}\big|_{\beta}\right)$; thus $\mathbf{F}(\alpha) \neq \mathbf{F}(\beta)$. Hence, $\mathbf{F}\big|_{\beta+1}$ is injective if $\mathbf{F}(\beta) \neq a$.
>
> Suppose $\forall \alpha < h(A),\ \mathbf{F}(\alpha) \neq a$ for the sake of contradiction. Then, $\mathbf{F}\big|_{h(A)}$ is an injection on $h(A)$ into A by the preceding discussion, which contradicts Definition 7.1.6. □

Hence, by Claim 1, we may let $\lambda \triangleq \min\{\, \xi < h(A) \mid \mathbf{F}(\xi) = a \,\}$. The discussion in the proof of Claim 1 says that $\mathbf{F}\big|_{\lambda}$ is injective. Clearly, we have $\mathbf{F}[\lambda] \subseteq A$ by definition of λ. If it were $\mathbf{F}[\lambda] \subsetneq A$, then $\mathbf{F}(\lambda) \in A \setminus \mathbf{F}[\lambda]$; thus $\mathbf{F}(\lambda) \neq a$, which is a contradiction. Hence, $\mathbf{F}\big|_{\lambda} : \lambda \hookrightarrow\!\!\!\rightarrow A$. $R \triangleq \{\, (\mathbf{F}(\alpha), \mathbf{F}(\beta)) \in A^2 \mid \alpha < \beta < \lambda \,\}$ is a well-ordering of A. □

Theorem 8.1.3

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 $X \in S$. WLOG, $X \neq \varnothing$. Then, $|S \setminus \{X\}| = n$, and thus there exists a choice function g for $S \setminus \{X\}$. Fix any $x \in X$. Then, $g' \triangleq g \cup \{(X, x)\}$ is a choice function for S. The result follows from The Induction Principle. □

Axiom IX The 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 8.1.4

TFAE.

(i) The Axiom of Choice

(ii) Every partition has a set of representatives.

(iii) If $\langle X_i \mid i \in I \rangle$ 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) ⇒ (ii) Let f be a choice function for a partition S. Then, $X = \operatorname{ran} f$ is a set of representatives for S.

(ii) ⇒ (iii) Let $C_i \triangleq \{i\} \times X_i$ for each $i \in I$. Then, as $\forall i, i' \in I,\ (i \neq i' \implies C_i \cap C_{i'} = \varnothing)$, $S \triangleq \{\, C_i \mid i \in I \,\}$ is a partition. Let f be a set of representatives for S. Then, for each $i \in I$, there uniquely exists $x \in X_i$ such that $(i, x) \in f \cap C_i$. Hence, f is a function on I and $\forall i \in I,\ f(i) \in X_i$.

(iii) ⇒ (i) Take any S and let $I \triangleq S \setminus \{\varnothing\}$. 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. □

Note:-

From now, the results that depend on The Axiom of Choice is marked with [AoC].

Theorem 8.1.5

Every infinite set has a countably infinite subset. [AoC]

Proof. Let A be an infinite set. By Well-Ordering Theorem, 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 8.1.6

For every infinite set S, there uniquely exists $\alpha \in \mathrm{Ord}$ such that $|S| = \aleph_\alpha$. [AoC]

Proof. By Well-Ordering Theorem, $|S| = |\Omega|$ for some infinite ordinal Ω. Then, by Theorems 7.1.3 and 7.1.10, there exists $\alpha \in \mathrm{Ord}$ such that $|\Omega| = \aleph_\alpha$. The uniqueness is evident. □

Definition 8.1.7: Cardinals

For every set X, $|X|$ is the unique initial ordinal equipotent to X.

Note:-

Assumption 4.1.7 is justified by Definition 8.1.7, which is justified by these facts:

- There exists $f : X \hookrightarrow\!\!\!\!\rightarrow Y$ if and only if $|X|$ is equal to $|Y|$.
- There exists $f : X \hookrightarrow Y$ if and only if $|X|$ is less than or equal to $|Y|$.

Theorem 8.1.8

For any sets A and B, we have $|A| \le |B|$ or $|B| \le |A|$. [AoC]

Proof. $|A|$ and $|B|$ are ordinal numbers, □

Theorem 8.1.9

The union of countably infinite collection of countable sets is countable. [AoC]

Proof. Let $|S| = \aleph_0$ and $\forall X \in S$, $|S| \le \aleph_0$. Fix any injective sequence $\langle A_n \mid n \in \mathbb{N} \rangle$ onto S. For each $n \in \mathbb{N}$, as $|A_n| \le \aleph_0$, there exists $f : \mathbb{N} \twoheadrightarrow A_n$. Let $P_n \triangleq \{ f \in A_n^{\mathbb{N}} \mid \operatorname{ran} f = A_n \}$, which is nonempty.

By Theorem 8.1.4 (iii), there exists a function g on $\mathbb{N}$ such that $\forall n \in \mathbb{N}$, $g_n \in P_n$. Then, we can define $\eta : \mathbb{N} \times \mathbb{N} \twoheadrightarrow \bigcup S$ by $\eta(n,k) = g_n(k)$; hence $\bigcup S$ is countable by Theorem 4.3.5. □

Theorem 8.1.10

$\aleph_1 \le 2^{\aleph_0}$ [AoC]

Proof. This is a consequence of Theorem 8.1.6 and Cantor's Theorem. □

Theorem 8.1.11

If f is a function on A, then $|\operatorname{ran} f| \le |A|$. [AoC]

Proof. Since $|A| = |\alpha|$ for some ordinal α by Theorem 8.1.6, the result follows from Exercise 7.2.5. □

Theorem 8.1.12

Let $\alpha \in \mathrm{Ord}$. If $|S| \le \aleph_\alpha$ and $\forall X \in S$, $|X| \le \aleph_\alpha$, then $\left|\bigcup S\right| \le \aleph_\alpha$. [AoC]

Proof. WLOG, $S \neq \varnothing$ 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 $f : \omega_\alpha \times \omega_\alpha \twoheadrightarrow \bigcup S$ by $f(\nu, \kappa) = x_\nu(\kappa)$. Hence,

$$\begin{aligned} \left|\bigcup S\right| &\leq \aleph_\alpha \cdot \aleph_\alpha && \triangleright \text{ Theorem 8.1.11} \\ &= \aleph_\alpha. && \triangleright \text{ Theorem 7.2.1} \end{aligned}$$

Thus, the result follows. □

Theorem 8.1.13 Zorn's Lemma

TFAE.

- The 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.

($\Rightarrow$) 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 $\mathcal{P}(A)$. Let $\mathbf{G}(x)$ be an operation defined by

$$\mathbf{G}(x) \triangleq \begin{cases} g(A_x) & \text{if } x \text{ is a transfinite sequence of length } \alpha \\ & \quad \text{and } A_x \triangleq \{a \in A \mid \forall \xi < \alpha,\ x(\xi) \prec a\} \text{ is nonempty} \\ b & \text{otherwise.} \end{cases}$$

Then, by The Transfinite Recursion Theorem, there exists an operation $\mathbf{F}(x)$ such that $\forall \alpha \in \mathrm{Ord}$, $\mathbf{F}(\alpha) = \mathbf{G}\left(\mathbf{F}\big|_\alpha\right)$. Similarly to the discussion in Claim 1 of Well-Ordering Theorem, $\mathbf{F}(\alpha) = b$ for some $\alpha < h(A)$. Let $\lambda \triangleq \min\{\alpha \in h(A) \mid \mathbf{F}(\alpha) = b\}$. Then, the set $C \triangleq \mathbf{F}[\lambda]$ is a chain in $(A, \preceq)$; so it has an upper bound $c \in A$.

If $c \prec a$ for some $a \in A$, then $a \in A_{\mathbf{F}|_\lambda}$; thus $\mathbf{F}(\lambda) = g\left(A_{\mathbf{F}|_\lambda}\right) \neq b$, which is a contradiction. Hence, c is a maximal element of A.

($\Leftarrow$) It suffices to show that every system of nonempty sets S has some choice function. Let $F \triangleq \{f : S \rightharpoonup \bigcup S \mid \forall X \in \operatorname{dom} f,\ f(X) \in X\}$. Then, $(F, \subseteq_F)$ is a partially ordered set. Moreover, if $C \subseteq F$ is a chain in $(F, \subseteq_F)$, then $\bigcup C$ is an upper bound of C.

Therefore, by the assumption, there exists a maximal element $\overline{f}$ of F. Suppose $\operatorname{dom} \overline{f} \subsetneq S$ for the sake of contradiction. Take any $X \in S \setminus \operatorname{dom} \overline{f}$ and $x \in X$. Then, $\overline{f} \cup \{(X, x)\} \in F$ is clearly greater than $\overline{f}$, which is a contradiction. Hence, $\operatorname{dom} \overline{f} = S$, i.e., $\overline{f}$ is a choice function for S. □

Theorem 8.1.14

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 $|A| \leq \aleph_\gamma$. [AoC]

Proof. In the same way as in the proof of Zorn's Lemma, we construct an operation $\mathbf{F}(x)$ and $\lambda = \min\{\alpha < h(A) \mid \mathbf{F}(\alpha) = b\}$.

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, $\mathbf{F}\big|_{\omega_\gamma}$ 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 8.1.12. □

Selected Problems

Exercise 8.1.1

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 of finite subsets S 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 4.5.2.) Then, f is a choice function for S. ☐

Exercise 8.1.2

If A can be well-ordered, then $\mathcal{P}(A)$ can be totally ordered.

Proof. Assume $(A, \leq)$ is a well-ordered set. Then, define $\prec$ on $\mathcal{P}(A)$ by

$$X \prec Y \iff X \neq Y \wedge \min_{\leq}(X \mathbin{\triangle} Y) \in X.$$

- Since $(X \mathbin{\triangle} Y) \cap (X \cap Y) = \varnothing$, $\prec$ is asymmetric on $\mathcal{P}(A)$. ✓
- Assume $X \prec Y$ and $Y \prec Z$. Then, $a \triangleq \min_{\leq}(X \mathbin{\triangle} Y) \in X$ and $b \triangleq \min_{\leq}(Y \mathbin{\triangle} Z) \in Y$. Then, since $a \notin Y$, $a \neq b$.
  - If $a < b$, then $a \notin Z$ by minimality of b. Therefore, $a \in X \mathbin{\triangle} Z$. If $x \in A$ and $x < a < b$, then $x \in X \iff x \in Y$ by minimality of a and $x \in Y \iff x \in Z$ by minimality of b. Therefore, $x \notin X \mathbin{\triangle} Z$; thus $a = \min_{\leq}(X \mathbin{\triangle} Z) \in X$.
  - If $b < a$, then $b \in X$ by minimality of a. Therefore, $b \in X \mathbin{\triangle} Z$. Similarly, if $x \in A$ and $x < b < a$, then $x \in X \iff x \in Y \iff x \in Z$ by minimality of a and b; thus $b = \min_{\leq}(X \mathbin{\triangle} Z) \in X$.

  Hence, in both cases, we have $X \prec Z$; $\prec$ is transitive in $\mathcal{P}(A)$. ✓
- Take any $X, Y \in \mathcal{P}(A)$ with $X \neq Y$. Then, $\min_{\leq}(X \mathbin{\triangle} Y) \in X \mathbin{\triangle} Y \subseteq X \cup Y$; thus we have $X \prec Y$ or $Y \prec X$. Hence, $\preceq$ is a total ordering of $\mathcal{P}(A)$. ✓ ☐

Exercise 8.1.3

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 $a \preceq x$. [AoC]

Proof. Replace $\mathbf{G}(x)$ in the proof of Zorn's Lemma with

$$\mathbf{G}(x) \triangleq \begin{cases} g(A_x) & \text{if } x \text{ is a transfinite sequence of length } \alpha > 0 \\ & \quad \text{and } A_x \triangleq \{\, a \in A \mid \forall \xi < \alpha,\ x(\xi) \prec a \,\} \text{ is nonempty} \\ a & \text{if } x = \varnothing \\ b & \text{otherwise.} \end{cases}$$

Then, if c is an upper bound of $\mathbf{F}[\lambda]$, then $a \preceq c$ and c is a maximal element. ☐

Exercise 8.1.4

TFAE.

- Zorn's Lemma

- For every partially ordered set $(A, \preceq)$, the set of all chains of $(A, \preceq)$ has an $\subseteq$-maximal element.

Proof.

($\Rightarrow$) Let $\mathcal{C} \subseteq \mathcal{P}(A)$ be the set of all chains of $(A, \preceq)$. Then, $(\mathcal{C}, \subseteq_{\mathcal{C}})$ is a partially ordered set such that every chain in $\mathcal{D}$ of $(\mathcal{C}, \subseteq_{\mathcal{C}})$ has an upper bound $\bigcup \mathcal{D}$. (If $a_1, a_2 \in \bigcup \mathcal{D}$, then there exists $C_1, C_2 \in \mathcal{D}$ such that $a_1 \in C_1$ and $a_2 \in C_2$. WLOG, $C_1 \subseteq C_2$; thus $a_1, a_2 \in C_2$, which implies a_1 and a_2 is comparable.) Hence, by assumption, P has a $\subseteq$-maximal element.

($\Leftarrow$) Let $(A, \preceq)$ be a partially ordered set in which every chain of $(A, \preceq)$ has an upper bound. Let $\mathcal{C} \subseteq \mathcal{P}(A)$ be the set of all chains of $(A, \preceq)$. Hence, there exists a chain $C \in \mathcal{C}$, such that, if $C \subsetneq X \subseteq A$, then $X \notin \mathcal{C}$. By assumption, there exists an upper bound $c \in A$ of C.

Suppose c is not a $\preceq$-maximal element of A for the sake of contradiction. There exists $c' \in A$ such that $c \prec c'$. Then, $C \cup \{c'\}$ would be a chain in $(A, \preceq)$, contradicting the maximality of C. Hence, c is a $\preceq$-maximal element. □

Exercise 8.1.5

TFAE.

- Zorn's Lemma
- Let A be a set. Assume that, for each $B \subseteq A$ such that $(B, \subseteq_B)$ is a totally ordered set, $\bigcup B \in A$. Then, A has an $\subseteq$-maximal element.

Proof.

($\Rightarrow$) Let A be a set and assume that, for each $B \subseteq A$ such that $(B, \subseteq_B)$ is a totally ordered set, $\bigcup B \in A$. This essentially says that, every chain in $(A, \subseteq_A)$ has an upper bound. Hence, by Zorn's Lemma, A has a $\subseteq$-maximal element.

($\Leftarrow$) Let $(A, \preceq)$ be a partially ordered set in which every chain of $(A, \preceq)$ has an upper bound. Let $\mathcal{C} \subseteq \mathcal{P}(A)$ be the set of all chains in $(A, \preceq)$. If $C \subseteq \mathcal{C}$ is a chain in the partially ordered set $(\mathcal{C}, \subseteq_{\mathcal{C}})$, then $\bigcup C$ is also a chain in $(A, \preceq)$, i.e., $\bigcup C \in \mathcal{C}$. Therefore, by assumption, there an $\subseteq$-maximal element $C_0 \in \mathcal{C}$ of $(\mathcal{C}, \subseteq_{\mathcal{C}})$.

By assumption, there exists an upper bound $c \in A$ of C_0. If $\exists c' \in A$, $c \prec c'$, then $C_0 \cup \{c'\} \in \mathcal{C}$, which contradicts the maximality of C_0. Hence, c is a $\preceq$-maximal element of $(A, \preceq)$. □

Exercise 8.1.6 Tukey's Lemma

A set $\mathcal{F}$ has *finite character* if

$$\forall X, (X \in \mathcal{F} \iff [X]^{<\omega} \subseteq \mathcal{F}).$$

TFAE.

- Zorn's Lemma
- Every set of finite character has an $\subseteq$-maximal element.

Proof.

($\Rightarrow$) Let $\mathcal{F}$ be a set of finite character.

Claim 1. For any $\mathcal{G} \subseteq \mathcal{F}$, if $(\mathcal{G}, \subseteq_{\mathcal{G}})$ is a totally ordered set, then $\bigcup \mathcal{G} \in \mathcal{F}$.

> ***Proof.*** Take any $\mathcal{G} \subseteq \mathcal{F}$ such that $(\mathcal{G}, \subseteq_{\mathcal{G}})$ is a totally ordered set. Take any $A \in \left[\bigcup \mathcal{G}\right]^{<\omega}$ and write $A = \{a_0, a_1, \cdots, a_{n-1}\}$. Then, by Theorem 8.1.3, we may let, for each $i < n$, A_i be an element of $\mathcal{G}$ such that $a_i \in A_i$. As $(\mathcal{G}, \subseteq_{\mathcal{G}})$ is a totally ordered set, there exists $i_0 \in n$ such that $\forall i < n, A_i \subseteq A_{i_0}$, so we have $A \in A_0 \subseteq \bigcup \mathcal{G}$. Therefore, $\bigcup \mathcal{G} \in \mathcal{F}$ because $\mathcal{F}$ is of finite character. □

By Claim 1 and Exercise 8.1.5, $\mathcal{F}$ has a $\subseteq$-maximal element.

(⇐) Let $(A, \preceq)$ be a partially ordered set. Let $\mathcal{C} = \mathcal{P}(A)$ be the set of all chains in $(A, \preceq)$.

> ***Claim 2.*** $\mathcal{C}$ has finite character.
>
> ***Proof.***
>
> (⇒) Take any $C \in \mathcal{C}$. Since every subset of C is also a chain, hence $[C]^{<\omega} \subseteq \mathcal{C}$.
>
> (⇐) Take any X such that $[X]^{<\omega} \subseteq \mathcal{C}$. Take any $a_1, a_2 \in X$. Then, the assumption says $\{x_1, x_2\}$ is a chain; thus x_1 and x_2 are comparable in $\preceq$. Hence, X is a chain in $(A, \preceq)$. □

Therefore, by assumption and Claim 2, $\mathcal{C}$ has a $\subseteq$-maximal element. Hence, by Exercise 8.1.4, Zorn's Lemma is implied. □

> **Exercise 8.1.7**
>
> Let E be a binary relation on A. Then, there exists a function $f : A \to A$ such that $\forall x \in A, ((x, f(x)) \in E \iff \exists y \in A, (x, y) \in E)$. [AoC]

Proof. If $A = \varnothing$, then it is done; so assume $A \neq \varnothing$. Fix any $a \in A$. Let g be a choice function for $\mathcal{P}(A)$. Then, 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 condition. □

> **Exercise 8.1.8**
>
> For each X, if $|X| > \aleph_0$, then X has a subset of cardinality $\aleph_1$. [AoC]

Proof. By Theorem 8.1.6, there exists $\alpha \in \mathrm{Ord}$ such that $|X| = \aleph_\alpha$. Then, we have $\alpha \geq 1$. As $\aleph_1 \leq \aleph_\alpha = |X|$, there exists $f : \omega_1 \hookrightarrow X$; thus $\operatorname{ran} f$ is a subset of X with cardinality $\aleph_1$. □

> **Exercise 8.1.10**
>
> 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.

(⇒) Suppose there exists a strictly decreasing sequence $\langle a_n \mid n \in \mathbb{N} \rangle$ of elements of A for the sake of contradiction. Let $\alpha \in \mathrm{Ord}$ be the order type of $(A, \preceq)$. If $h : A \hookrightarrow\!\!\!\!\rightarrow \alpha$ is an isomorphism between them, then $f : \mathbb{N} \to \alpha$ defined by $f(n) \triangleq h(a_n)$ is a strictly decreasing infinite sequence in α, which contradicts Lemma 6.6.5.

(⇐) Assume $(A, \preceq)$ is not a well-ordered set. Then, there exists nonempty $X \subseteq A$ such that there is no least element of X. Let f be a choice function for $\mathcal{P}(X)$. Fix some $a_0 \in X$. Define a sequence $\langle a_n \mid n \in \mathbb{N} \rangle$ recursively by $a_{n+1} = f(\{x \in X \mid x \prec a_n\})$. Then, $\langle a_n \mid n \in \mathbb{N} \rangle$ is a strictly decreasing infinite sequence in A. □

Exercise 8.1.11

Let $\langle F_{a,b} \rangle_{a\in A,\, b\in B}$ be a nonempty indexed system of sets.

(i) $\bigcap_{a\in A}\left[\bigcup_{b\in B} F_{a,b}\right] = \bigcup_{f\in B^A}\left[\bigcap_{a\in A} F_{a,f(a)}\right]$ if $A \neq \varnothing$.

(ii) $\bigcup_{a\in A}\left[\bigcap_{b\in B} F_{a,b}\right] = \bigcap_{f\in B^A}\left[\bigcup_{a\in A} F_{a,f(a)}\right]$ if $B \neq \varnothing$. [AoC]

Proof.

(i) Let $L \triangleq \bigcap_{a\in A}\left[\bigcup_{b\in B} F_{a,b}\right]$ and $R \triangleq \bigcup_{f\in B^A}\left[\bigcap_{a\in A} F_{a,f(a)}\right]$.

(⊆) Take any $x \in L$. Let $E \triangleq \{(a,b) \in A \times B \mid x \in F_{a,b}\}$. By Exercise 8.1.7, there exists $f : A \to B$ such that, for each $a \in A$, $(a, f(a)) \in E$ if and only if $a \in \operatorname{dom} R$. $(\operatorname{dom} E = A$ as $x \in L$.) Therefore, $x \in \bigcap_{a\in A} F_{a,f(a)} \subseteq R$; thus $L \subseteq R$.

(⊇) Same as in the proof of Exercise 2.3.13.

(ii) Let $L \triangleq \bigcup_{a\in A}\left[\bigcap_{b\in B} F_{a,b}\right]$ and $R \triangleq \bigcap_{f\in B^A}\left[\bigcup_{a\in A} F_{a,f(a)}\right]$. If $A = \varnothing$, then it is done; so assume $A \neq \varnothing$. Let $\mathcal{U} \triangleq \bigcup_{(a,b)\in A\times B} F_{a,b}$. Then,

$$
\begin{aligned}
\mathcal{U} \setminus L &= \textstyle\bigcap_{a\in A}\left[\mathcal{U} \setminus \bigcap_{b\in B} F_{a,b}\right] && \triangleright \text{ Exercise 2.3.11} \\
&= \textstyle\bigcap_{a\in A}\left[\bigcup_{b\in B}(\mathcal{U} \setminus F_{a,b})\right] && \triangleright \text{ Exercise 2.3.11} \\
&= \textstyle\bigcup_{f\in B^A}\left[\bigcap_{a\in A}(\mathcal{U} \setminus F_{a,f(a)})\right] && \triangleright \text{ (i)} \\
&= \textstyle\bigcup_{f\in B^A}\left[\mathcal{U} \setminus \bigcup_{a\in A} F_{a,f(a)}\right] && \triangleright \text{ Exercise 2.3.11} \\
&= \mathcal{U} \setminus R. && \triangleright \text{ Exercise 2.3.11}
\end{aligned}
$$

Since $L, R \subseteq \mathcal{U}$, by Exercise 1.4.2 (iii), $L = \mathcal{U} \cap L = \mathcal{U} \setminus (\mathcal{U} \setminus L) = \mathcal{U} \setminus (\mathcal{U} \setminus R) = \mathcal{U} \cap R = R$. □

Exercise 8.1.12

Let A be a set. For each partial ordering $\preceq$ of A, there exists a total ordering $\leq$ of A such that $\forall a, b \in A$, $(a \preceq b \implies a \leq b)$. [AoC]

Proof. Let $\mathfrak{P} \subseteq \mathcal{P}(A \times A)$ be the set of all partial orderings of A. It is easy to see that, if $\mathcal{C}$ is a chain in the partially ordered set $(\mathfrak{P}, \subseteq_{\mathfrak{P}})$, then $\bigcup \mathcal{C}$ is also a partial ordering of A. Then, by Exercise 8.1.3, the partially ordered set $(\mathfrak{P}, \subseteq_{\mathfrak{P}})$ has a $\subseteq$-maximal element $P \in \mathfrak{P}$ such that $\preceq \subseteq P$.

Suppose x_0 and y_0 are incomparable in P for the sake of contradiction. Let

$$P' \triangleq P \cup \{(a, y_0) \in A^2 \mid aPx_0\} \cup \{(x_0, a) \in A^2 \mid y_0 Pa\}.$$

In particular, $x_0 P' y_0$. It is evident that P' is reflexive.

- Take any $a, b \in A$ and assume $aP'b$ and $bP'a$.
  - If aPb and bPa, then by antisymmetry of P.
  - In the case of $\neg(aPb) \wedge bPa$, we have either $b = y_0 \wedge aPx_0$ or $a = x_0 \wedge y_0 Pb$. If $b = y_0$ and aPx_0, then we have $y_0 P x_0$ by transitivity of P, which is a contradiction. The other case leads to a contradiction in a similar manner.
  - If $(a,b), (b,a) \in \{(a, y_0) \in A^2 \mid aPx_0\}$, then we have $a = b = y_0$. The case $(a,b), (b,a) \in \{(x_0, a) \in A^2 \mid y_0 Pa\}$ can be treated similarly.

  - If $(a, b) \in \{(a, y_0) \in A^2 \mid aPx_0\}$ and $(b, a) \in \{(x_0, a) \in A^2 \mid y_0Pa\}$, then it $x_0 = b = y_0$, which is a contradiction.

  Therefore, we conclude $a = b$; P' is antisymmetric in A.
- Take any $a, b, c \in A$ and assume $aP'b$ and $bP'c$.

$\square$

End.