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[a] 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 $X, Y, \cdots, Z$.

[a]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. $\square$

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 $\mathbf{P}(x)$.

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

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 $x \in B' \iff x \in A \land \mathbf{P}(x) \iff x \in B$. Hence, by The Axiom of Extensionality, we have $B = B'$. $\square$

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 $x = B$.

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

Note:-

Similarly, the set C such that $x \in C \iff x = A \lor x = B$ 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 $A \in S$.

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

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 $\mathbf{P}(x) \implies x \in A \land x \in A'$. Then, $\{\, x \in A \mid \mathbf{P}(x) \,\} = \{\, x \in A' \mid \mathbf{P}(x) \,\}$.

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

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 $\{ x \in A \mid x \in A \wedge x \notin B \}$. □

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 $\forall x\,(x = x)$, $\forall x\,(x \notin B)$. □

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). □

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, $Y \notin X$. □

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 $\{x \mid x \in A \wedge x \in B\}$.

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

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

(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 $\{\, w \mid \exists x,\ \exists y,\ w = (x,y) \wedge \mathbf{P}(x,y)\,\}$.

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

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

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 $A = \bigcup(\bigcup R)$. 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 $x, y \in A$. □

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 $R \circ R^{-1}$. □

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 $x f y_1$, $y_1 g z_1$, $x f y_2$, and $y_2 g z_2$. 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) $$x \in \operatorname{dom}(g \circ f) \iff \exists z\, x(g \circ f)z \iff \exists z\, \exists y\; x f y \wedge y g z \iff x \in \operatorname{dom} f \wedge f(x) \in \operatorname{dom} g \iff x \in \operatorname{dom} f \wedge x \in f^{-1}[\operatorname{dom} g] \qquad \square$$

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 $f : A \to B$ be a function.

- If f is a function *onto* B, we may write $f : A \twoheadrightarrow B$.
- If f is one-to-one, we may write $f : A \hookrightarrow B$.
- If f is one-to-one and onto B, we may write $f : A \hookrightarrow\!\!\!\!\rightarrow B$.

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 $y f^{-1} x_1$ and $y f^{-1} x_2$, then $x_1 f y$ and $x_2 f y$, 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. $\square$

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, $(y, x) \in f^{-1}$; $g\big|_{\operatorname{ran} f} \subseteq f^{-1}$. $\square$

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 xfa and xfb. 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, $x \in f^{-1}[A] \setminus f^{-1}[B]$. $\square$

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

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, $[a]_E \cap [b]_E \neq \varnothing$. $\square$

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

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

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, $aE_S a$. E_S is reflexive.
- Assume $aE_S b$. Then, there exists $C \in S$ such that $a, b \in C$. Hence, $bE_S a$. E_S is symmetric.
- Assume $aE_S b$ and $bE_S c$. 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 $aE_S c$. E_S is transitive. □

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

(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 $b \in C \iff aE_S b \underbrace{\iff}_{\text{Lemma 2.4.3}} b \in [a]_{E_S}$; $C = [a]_{E_S}$. 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, $C \subseteq A/E_S$. □

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, $\varphi \circ j = f$. □

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 *linearly 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. $\square$

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 linearly 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 linearly 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 linearly 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 linearly 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 linearly 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 $\mathrm{Id}_A \cap S = \varnothing$.

$\square$

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 $\prec \cap A_2^2 = <_2$. $\square$

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 anti-symmetric, 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. ✓ $\square$

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. $\mathrm{ran}(g \circ f) = g[\mathrm{ran}\, f] = P_3$. 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 "$0 \le x$." $\mathbf{P}(0)$, i.e., $0 \le 0$, 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 $k = n$. □

Theorem 3.2.3 $(N, \le)$ is Linearly Ordered

$(N, \le)$ is a linearly ordered set.

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

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

Proof. Let $\mathbf{P}(x)$ be the property "$\forall k, m \in \mathbb{N}, (k < m \wedge m < x \implies k < x)$." $\mathbf{P}(0)$ 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. □

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. □

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

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

Proof. Let $\mathbf{P}(x)$ be the property "$\forall n \in \mathbb{N}, (n < x \implies n+1 \le x)$." $\mathbf{P}(0)$ 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 $(n+1) \le (m+1)$. If $n < m$, then $(n+1) \le m < (m+1)$. Therefore, the result follows from The Induction Principle. □

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

Proof. Let $\mathbf{P}(x)$ be the property "$\forall m \in \mathbb{N},\ m = x \vee m < x \vee x < m$." $\mathbf{P}(0)$ 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 $(n+1) \le m$. Hence, $\mathbf{P}(n+1)$ holds. Therefore, the result follows from The Induction Principle. □

□

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 $n \in \mathbb{N}$.

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

Proof. Assume the premise $(\forall n \in \mathbb{N}, [\forall k < n, \implies \mathbf{P}(k) \implies \mathbf{P}(n)])$. 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 linear 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 $\mathbb{N}$ 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 $\mathbb{N}$ 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 $(N, \le)$ is Linearly Ordered, we have $m+1 \le n$. Together with $n < n+1$, we have $m+1 < n+1$.

Now, take any $m, n \in \mathbb{N}$ with $m \ne n$. Then, by $(N, \le)$ is Linearly Ordered, we have $m < n$ or $n < m$, i.e., $S(m) < S(n)$ or $S(n) < S(m)$. In both cases, $S(m) \ne S(n)$. 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 $k \in \mathbb{N}$.

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

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 $(N, \leq)$ is Linearly 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 $(N, \leq)$ is Linearly 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 $(N, \leq)$ is Linearly 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.

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

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.

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

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 $\operatorname{Seq}(A) = \bigcup \mathcal{A}$ 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 $F \triangleq \{ t \in \operatorname{Seq}(A) \mid t \text{ is an } m \text{ step computation for some } m \in \mathbb{N} \}$. 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 $(N, \le)$ is Linearly 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. □

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, $\forall k \leq n$, $f_k = t_k$, 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. □

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 $(\mathbb{N}, \leq)$.

Proof. By (i), $\{a \in A \mid x \prec a\} \neq \varnothing$ 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:

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

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, $A \setminus \operatorname{ran} f \neq \varnothing$, and thus we may take $p = \min(A \setminus \operatorname{ran} f)$, which gives $p \neq f_0$ immediately. Hence, $B = \{a \in A \mid a \prec p\} \neq \varnothing$ 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 $p \notin \operatorname{ran} f$. □

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

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 $G\colon \mathrm{Seq}(S)\times\mathbb{N}\to\mathrm{Seq}(S)$ 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 $F:\mathbb{N}\to\mathrm{Seq}(S)$ 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 $F_k\subsetneq_{\mathrm{Seq}(S)} F_{k+1}$, 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 $p \notin \operatorname{ran} f$. $\square$

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. $\square$

Exercise 3.3.5 The Recursion Theorem: Finite 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. $\square$

> ***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 $\mathbb{N}$ 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 $(f_k, k) \notin \operatorname{dom} g$. $\square$

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. $\square$

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 $h = f$. $\square$

> **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 $g = \Big\{((x,n),y) \in (X \times \mathbb{N}) \times X \,\Big|\, y = \min\{k \in X \mid x < k\}\Big\}$. 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: Finite Version, there exists a sequence f of elements of X such that

(i) $f_0 = \min X$ ▷ $\min X$ exists by $\mathbb{N}$ 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 $\mathbb{N}$ 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, $y = f_{m+1}$. $\square$

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 $p, x, n \in \mathbb{N}$. □

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 $m \in \mathbb{N}$. □

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. □

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 $\cdot$ 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. □

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 on a subset of S into S.
- A *binary operation* on S is a function on a subset of S^2 into 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 $\langle A_i \mid 0 \le i < n \rangle$ is a finite sequence (of sets), then the product of the indexed system of sets $\prod_{0 \le i < n} A_i$ (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 $\prod_{0 \le i < n} A_i = A^n$.

- $A^0 = \{\langle\rangle\}$.

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

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

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 on a subset of A^n into 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 on a subset of A into 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 $F_j \ne \varnothing$ 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

$\mathfrak{N} = (\mathbb{N}, \langle \leq \rangle, \langle 0, +, \cdot \rangle)$ 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) $\forall j < n,\ \forall a \in A^{f_j}, \big[(a_0, \cdots, a_{f_j-1}) \in \operatorname{dom} F_j$

$$\implies h(F_j(a_0, \cdots, a_{f_j-1})) = F'_j(h(a_0), \cdots, h(a_{f_j-1}))\big].$$

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 Exercise 1.4.2 (iii). 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 3.5.13

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 $i < n$, $k_i \leq m' \leq m$, and $k_n \leq m$. 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 $(a,b) \in \overline{R}$. □

End.