

Chapter 2

Language of Mathematics 2 (Set Theory)

This chapter contains a brief introduction to set theory which is essential for doing mathematics. There are two main axiomatic systems to introduce sets, viz. Zermelo–Fraenkel axiomatic system and the Gödel–Bernays axiomatic system. Here, in this text, we shall give an account of Zermelo–Fraenkel axiomatic set theory together with the axiom of choice (an axiom which is independent of the Zermelo–Fraenkel axiomatic system). We also discuss some of the important and useful equivalents of the axiom of choice. The ordinal and the cardinal numbers are introduced and discussed in a rigorous way. For the further formal development of the theory, the reader is referred to the ‘*Set Theory and Continuum hypothesis*’ by P.J. Cohen or the ‘*Axiomatic set theory*’ by P. Suppes.

2.1 Set, Zermelo–Fraenkel Axiomatic System

‘Set’, ‘belongs to,’ and ‘equal to’ are primitive terms of which the reader has intuitive understanding. Their use is governed by some postulates in axiomatic set theory.

To take the help of intuition in ascertaining the use of the primitive terms, we regard a set as a collection of objects. ‘A class of students,’ ‘a flock of sheep,’ ‘a bunch of flowers,’ and ‘a packet of biscuits’ are all examples of sets of things. The notation ‘ $a \in A$ ’ stands for the statement ‘ a belongs to A ’ (‘ a is an element of A ,’ or also for ‘ a is a member of A ’). The negation of ‘ $a \in A$ ’ is denoted by ‘ $a \notin A$.’ The notation ‘ $A = B$ ’ stands for the statement ‘ A is equal to B .’ The negation of ‘ $A = B$ ’ is denoted by ‘ $A \neq B$.’ The following axiom relates ‘ \in ’ and ‘ $=$.’

Axiom 1 (*Axiom of extension*) Let A and B be sets. Then,

$$'A = B' \text{ if and only if 'for all } x (x \in A \text{ if and only if } x \in B) \text{'}$$

Thus, two sets A and B are equal if they have same members. Two equal sets are treated as same. If $A = B$, then we may substitute A for B and B for A in any course of discussion.

Remark 2.1.1 To be logically sound in the use of primitive terms, axiom of extension is a necessity.

Let A and B be sets. We say that A is a **subset** of B (A is contained in B or B contains A) if every member of A is a member of B . The statement ' A is a subset of B ' is the same as the statement ' $\text{For all } x(\text{if } x \in A, \text{ then } x \in B)$.' The notation ' $A \subseteq B$ ' (or also ' $B \supseteq A$ ') stands for the statement ' A is a subset of B .' Thus, ' $A = B$ ' (axiom of extension) if and only if ' $A \subseteq B$ and $B \subseteq A$.' The negation of ' $A \subseteq B$ ' is denoted by ' $A \not\subseteq B$.' Since the negation of the statement ' $\text{For all } x(\text{if } x \in A, \text{ then } x \in B)$ ' is logically same as the statement ' $\text{There exists } x(x \in A \text{ and } x \notin B)$,' the notation ' $A \not\subseteq B$ ' stands for the statement ' $\text{There exists } x(x \in A \text{ and } x \notin B)$.' Thus, to say that A is not a subset of B is to say that there is an element of A which is not in B .

Every set is a subset of itself, because ' $\text{For all } x(\text{if } x \in A, \text{ then } x \in A)$ ' is a tautology (always a true statement). If $A \subseteq B$ and $A \neq B$, then we say that A is a **proper subset** of B . The notation ' $A \subset B$ ' stands for the statement ' A is a proper subset of B .' Thus, A is a proper subset of B if every member of A is a member of B , and there is a member of B which is not a member of A . More precisely, ' $A \subset B$ ' represents the statement ' $(\text{For all } x(\text{if } x \in A, \text{ then } x \in B))$ and $(\text{there exists } x(x \in B \text{ and } x \notin A))$.'

Proposition 2.1.2 *If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Proof Suppose that $A \subseteq B$ and $B \subseteq C$. Let $x \in A$. Since $A \subseteq B$, $x \in B$. Further, since $B \subseteq C$, $x \in C$. Thus, ' $\text{for all } x(\text{if } x \in A, \text{ then } x \in C)$.' This shows that $A \subseteq C$.
#

Some of the axioms of set theory are designed to produce different sets out of given sets. The first one is to generate subsets of a set.

Consider the set A of all men and the statement ' x is a teacher.' Some members of A are teachers, and some of them are not. The condition that ' x is a teacher' defines a subset of A , namely the set of all male teachers. To make it more formal, we have:

Axiom 2 (*Axiom of specification*) Let A be a set, and $P(x)$ be a valid statement involving the free symbol x . Then, there is a set B such that

$$\text{'for all } x(x \in B \text{ if and only if } (x \in A \text{ and } P(x))).'$$

Thus, to every set A , and to every statement $P(x)$, there is a unique set B whose members are exactly those members of A for which $P(x)$ is true.

The set B described above is denoted by $\{x \in A \mid P(x)\}$. Clearly, B is a subset of A .

Proposition 2.1.3 *Let A be a set. Then there is a set B such that $B \notin A$.*

Proof Consider the statement ‘ x is a set and $x \notin x$.’ By the axiom of specification, there is a unique set $B = \{x \in A \text{ such that } x \text{ is a set and } x \notin x\}$. We show that $B \notin A$. Suppose that $B \in A$. If $B \in B$, then $B \notin B$. Next, if $B \notin B$, then since $B \in A$ (supposition), and B is a set, $B \in B$. Thus, ‘ $B \notin B$ if and only if $B \in B$.’ This is a contradiction (P if and only if $\neg P$ is a contradiction) to the supposition that $B \in A$. Hence, $B \notin A$. $\#$

Corollary 2.1.4 *There is no set containing all sets.*¹ $\#$

Let A and B be sets. Consider the statement ‘ $x \in B$.’ The set $\{x \in A \mid x \in B\}$ is denoted by ‘ $A \cap B$,’ and it is called the **intersection** of A and B . Thus,

$$x \in A \cap B \text{ if and only if } (x \in A \text{ and } x \in B).$$

Since ‘ $[x \in A \text{ and } x \in B] \text{ if and only if } [x \in B \text{ and } x \in A]$ ’ is a tautology, we have the following proposition.

Proposition 2.1.5 $A \cap B = B \cap A$. $\#$

Proposition 2.1.6 $A \cap B \subseteq A$ and $A \cap B \subseteq B$.

Proof By the definition, $x \in A \cap B$ if and only if $[x \in A \text{ and } x \in B]$. Further, ‘if $[x \in A \text{ and } x \in B]$, then $x \in A$ ’ is a tautology. Thus, if $x \in A \cap B$, then $x \in A$. This shows that $A \cap B \subseteq A$. Similarly, $A \cap B \subseteq B$. $\#$

Proposition 2.1.7 If $[C \subseteq A \text{ and } C \subseteq B]$, then $[C \subseteq A \cap B]$.

Proof Suppose that $C \subseteq A$ and $C \subseteq B$. Let $x \in C$. Since $C \subseteq A$ and $C \subseteq B$, $x \in A$ and $x \in B$. Thus, $x \in A \cap B$. Hence, if $x \in C$, then $x \in A \cap B$. This shows that $C \subseteq A \cap B$. $\#$

Proposition 2.1.8 $[A \cap B = A] \text{ if and only if } [A \subseteq B]$.

Proof Suppose that $A \cap B = A$. Since $A \cap B \subseteq B$ (Proposition 2.1.6), $A \subseteq B$. Suppose that $A \subseteq B$. Since $A \subseteq A$, $A \subseteq A \cap B$ (Proposition 2.1.7). Also, $A \cap B \subseteq A$ (Proposition 2.1.6). By the axiom of extension, $A \cap B = A$. $\#$

Proposition 2.1.9 $(A \cap B) \cap C = A \cap (B \cap C)$.

Proof Let $x \in (A \cap B) \cap C$. By the definition, $(x \in A \text{ and } x \in B)$ and $x \in C$. This implies (tautologically) that $x \in A$ and $(x \in B \text{ and } x \in C)$. It follows that $x \in A \cap (B \cap C)$. Thus, $(A \cap B) \cap C \subseteq A \cap (B \cap C)$. Similarly, $A \cap (B \cap C) \subseteq (A \cap B) \cap C$. By the axiom of extension, the result follows. $\#$

¹In pre-axiomatic intuitive development of set theory, people took for granted that there is a set containing all sets. The argument used in the proof of the Proposition 2.1.3 led to a paradox known as ‘Russel’s paradox.’ In fact, the need for axiomatization of set theory was consequence of such paradoxes.

Let A and B be sets. Consider the statement $x \notin B$. By the axiom of specification, there is a unique set defined by $\{x \in A \mid x \notin B\}$. This set is denoted by $A - B$, and it is called the *complement* of B in A (or A *difference* B). Clearly, $A - B$ is a subset of A .

Proposition 2.1.10 $A - B = A - (A \cap B)$.

Proof Let $x \in A - B$. By the definition, $x \in A$ and $x \notin B$. This implies (tautologically) that $x \in A$ and $(x \in A \text{ and } x \notin B)$. Thus, $x \in A - (A \cap B)$. This shows that $A - B \subseteq A - (A \cap B)$. Similarly, $A - (A \cap B) \subseteq A - B$. By the axiom of extension, the result follows. \sharp

To have something in our hand, we formally assume the existence of a set as an axiom.

Axiom 3 (*Axiom of existence*) There exists a set.

Let A be a set. Consider $A - A$. If B is any set, then

$$(x \in A \text{ and } x \notin A) \text{ if and only if } (x \in B \text{ and } x \notin B)$$

is a tautology (note that ' $(P \text{ and } \neg P)$ if and only if $(Q \text{ and } \neg Q)$ ' is a tautology). Thus, $x \in (A - A)$ if and only if $x \in (B - B)$, and so $A - A = B - B$. Therefore, the set $A - A$ is independent of A . This set is called the **empty set**, or the **void set**, or the **null set**, and it is denoted by \emptyset . Thus, $\emptyset = \{x \in A \mid x \notin A\}$. Clearly, ' $x \in \emptyset$ ' is a contradiction. Further, the statement '*if $x \in \emptyset$, then Q* ' is a tautology whatever the statement Q may be.

Let $P(x)$ be any contradiction involving the symbol x . Clearly, then $\emptyset = \{x \in A \mid P(x)\}$. Intuitively, one may think of \emptyset as a set containing no elements.

Proposition 2.1.11 The empty set \emptyset is a subset of every set.

Proof Let B be a set. We have to show that '*if $x \in \emptyset$, then $x \in B$* .' Since $x \in \emptyset$ is a contradiction, '*if $x \in \emptyset$, then $x \in B$* ' is a tautology. Hence, $\emptyset \subseteq B$. \sharp

Proposition 2.1.12 $A - B = \emptyset$ if and only if $A \subseteq B$.

Proof Suppose that $A - B = \emptyset$. Let $x \in A$. Since $A - B = \emptyset$, $x \notin A - B$ (for $x \notin \emptyset$ is a tautology). Further, since $x \in A$ and $x \notin A - B$, $x \in B$. Hence, $A \subseteq B$. Conversely, suppose that $A \subseteq B$. We have to show that $A - B = \emptyset$. Already (Proposition 2.1.11), we have $\emptyset \subseteq A - B$. Let $x \in A - B$. Then, $x \in A$ and $x \notin B$. Since $A \subseteq B$, it follows that $x \in B$ and $x \notin B$. This, in turn, implies that $x \in \emptyset$. Hence, $A - B \subseteq \emptyset$. \sharp

Axiom 4 (*Axiom of replacement*) Let A be a set, and $P(x, y)$ be a statement formula involving x and y such that $\forall x \in A ((P(x, y) \text{ and } P(x, z)) \implies y = z)$. Then, there is a set $B = \{y \mid P(x, y) \text{ holds for some } x \in A\}$.

The axiom tells that if A is a set, and there is a correspondence from the members of A to another collection of objects associating each member of A a unique member of the collection, then the image is set. This axiom will be used in our discussions on ordinals.

The following axiom helps us to generate more sets.

Axiom 5 (*Pairing axiom*) Let A and B be sets. Then, there is a set C such that $A \in C$ and $B \in C$.

Consider the statement ' $x = A$ or $x = B$.' By the axiom of specification, we have a unique set $\{x \in C \mid x = A \text{ or } x = B\}$. This set is also independent of the set C . It contains A and B as elements and nothing else. We denote this set by $\{A, B\}$. The set $\{A, A\}$ is denoted by $\{A\}$, and it is called a singleton.

We have the empty set \emptyset . Consider $\{\emptyset\}$. Since $\emptyset \in \{\emptyset\}$ and $\emptyset \notin \emptyset$, $\emptyset \neq \{\emptyset\}$. If $\{\emptyset\} = \{\{\emptyset\}\}$, then $\emptyset = \{\emptyset\}$. This is a contradiction. Hence, $\{\emptyset\} \neq \{\{\emptyset\}\}$. Similarly, $\{\{\{\emptyset\}\}\} \neq \{\{\emptyset\}\}$. Axiom of pairing gives us other new sets such as $\{\emptyset, \{\emptyset\}\}$, $\{\{\emptyset, \{\emptyset\}\}\}$ and $\{\{\emptyset\}\}$. This way we produce several sets.

Axiom 6 (*Union Axiom*) Let A be a set of sets. Then, there is a set U such that ' $(X \in A \text{ and } x \in X)$ implies that $x \in U$.'

By the axiom of specification, we have the unique set given by

$$\{x \in U \mid x \in X \text{ for some } X \in A\}.$$

This set is denoted by $\bigcup_{X \in A} X$, and it is called the **union** of the family A of sets. Thus,

$$x \in \bigcup_{X \in A} X \text{ if and only if } x \in X \text{ for some } X \in A.$$

What is $\bigcup_{X \in \emptyset} X$? If $x \in \bigcup_{X \in \emptyset} X$, then there exists $X \in \emptyset$ such that $x \in X$. But $X \in \emptyset$ is a contradiction. Hence, $\bigcup_{X \in \emptyset} X = \emptyset$. Clearly, $\bigcup_{X \in \{A\}} X = A$.

The set $\bigcup_{X \in \{A, B\}} X$ is denoted by $A \cup B$. Thus,

$$x \in A \cup B \text{ if and only if } x \in A \text{ or } x \in B.$$

The set $A \cup B$ is called the **union** of A and B .

Proposition 2.1.13 $A \subseteq A \cup B$.

Proof Suppose that $x \in A$. Then, the statement ' $x \in A$ or $x \in B$ ' is true (if P , then $(P \text{ or } Q)$ is a tautology). Hence, if $x \in A$, then $x \in A \cup B$. Thus, $A \subseteq A \cup B$. \sharp

Proposition 2.1.14 $A \cup \emptyset = A$.

Proof Since $x \in \emptyset$ is always false, $x \in A$ if and only if $(x \in A \text{ or } x \in \emptyset)$. Hence, $A \cup \emptyset = A$. \sharp

Proposition 2.1.15 $A \cup B = B \cup A$.

Proof Clearly, ‘ $(x \in A \text{ or } x \in B) \text{ if and only if } (x \in B \text{ or } x \in A)$ ’ is a tautology. Hence, $A \cup B = B \cup A$. \sharp

Proposition 2.1.16 $A \cup A = A$.

Proof Since the statement ‘ $(x \in A \text{ or } x \in A) \text{ if and only if } x \in A$ ’ is a tautology, the result follows. \sharp

Proposition 2.1.17 $A \cup B = A \text{ if and only if } B \subseteq A$.

Proof Suppose that $A \cup B = A$. By the Proposition 2.1.13, $B \subseteq A \cup B = A$. Next, suppose that $B \subseteq A$. Then, $A \subseteq A \cup B \subseteq A \cup A = A$. Hence, $A \cup B = A$. \sharp

Proposition 2.1.18 $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof Let $x \in (A \cup B) \cup C$. By the definition, ‘ $(x \in A \text{ or } x \in B) \text{ or } x \in C$.’ This implies (tautologically) that ‘ $x \in A \text{ or } (x \in B \text{ or } x \in C)$.’ It follows that ‘ $x \in A \cup (B \cup C)$.’ Thus, ‘ $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.’ Similarly, ‘ $A \cup (B \cup C) \subseteq (A \cup B) \cup C$.’ By the axiom of extension, the result follows. \sharp

Proposition 2.1.19 *The union distributes over intersection, and the intersection distributes over union in the following sense:*

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, and
2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof 1. Let $x \in A \cup (B \cap C)$. By the definition, ‘ $x \in A \text{ or } (x \in B \text{ and } x \in C)$.’ This implies (tautologically) that ‘ $(x \in A \text{ or } x \in B) \text{ and } (x \in A \text{ or } x \in C)$.’ In turn, ‘ $x \in (A \cup B) \cap (A \cup C)$.’ This shows that ‘ $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.’ Similarly, ‘ $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.’ By the axiom of extension, ‘ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.’

Similarly, we can prove 2. \sharp

Theorem 2.1.20 (De Morgan’s Law) *Let A , B , and C be sets. Then,*

1. $A - (B \cup C) = (A - B) \cap (A - C)$.
2. $A - (B \cap C) = (A - B) \cup (A - C)$.

Proof 1. First observe that the statement ‘ $x \notin (B \cup C)$ ’ is logically equivalent to the statement ‘ $x \notin B \text{ and } x \notin C$.’ Let $x \in A - (B \cup C)$. Then, by the definition, ‘ $x \in A \text{ and } x \notin (B \cup C)$.’ This implies that ‘ $x \in A \text{ and } (x \notin B \text{ and } x \notin C)$.’ In turn, it follows that ‘ $(x \in A \text{ and } x \notin B) \text{ and } (x \in A \text{ and } x \notin C)$.’ Thus, ‘ $x \in (A - B) \cap (A - C)$.’ This shows that ‘ $A - (B \cup C) \subseteq (A - B) \cap (A - C)$.’ Similarly, ‘ $(A - B) \cap (A - C) \subseteq A - (B \cup C)$.’ The result follows by the axiom of extension. The proof of 2 is similar. \sharp

Axiom 7 (Power Set Axiom) Given a set A , there is a set Ω such that $B \subseteq A$ implies that $B \in \Omega$.

Consider the statement ‘ x is a subset of A .’ By the axiom of specification, we have a unique set given by

$$\{x \in \Omega \mid x \text{ is a subset of } A\}.$$

This set is independent of the choice of Ω in the power set axiom. We denote this set by $\wp(A)$ and call it the **power set** of A .

Since the empty set \emptyset is a subset of every set, $\wp(A)$ can never be an empty set. What is $\wp(\emptyset)$? Since $\emptyset \subseteq \emptyset$, $\emptyset \in \wp(\emptyset)$. Suppose that $A \in \wp(\emptyset)$. Then, $A \subseteq \emptyset$. But, then if $x \in A$, then $x \in \emptyset$. Since $x \in \emptyset$ is a contradiction, $x \in A$ is also a contradiction. Hence, $A = \emptyset$. Thus, $\wp(\emptyset) = \{\emptyset\}$. Further, $A \in \wp(\{\emptyset\})$ if and only if $A \subseteq \{\emptyset\}$. This shows that $A = \emptyset$ or $A = \{\emptyset\}$. Thus, $\wp(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. Further, $\wp(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$, and so on.

The next axiom is the axiom of regularity (also called the axiom of foundation). It is used specially in discussions involving ordinal arithmetic. In axiomatic set theory, the members of sets are also sets. Indeed, any mathematical discussion can be modeled so that all the objects considered are sets of sets. For example, 1 can be represented by $\{\emptyset\}$, 2 can be represented by $\{\emptyset, \{\emptyset\}\}$, and so on. The axiom is designed to restrict uncomfortable situations such as $A \in A$, ($A \in B$ and $B \in A$), and ($A \in B$ and $B \in C$ and $C \in A$) in any course of discussion.

Axiom 8 (Axiom of regularity) If A is a nonempty set of sets, then ‘there exists X ($X \in A$ and $X \cap A = \emptyset$).’

Thus, given a nonempty set A of sets, there is a set X in A such that no member of X is in A .

Theorem 2.1.21 Let A be a set of sets. Then, $A \notin A$.

Proof Let A be a set. $\{A\} \neq \emptyset$. By the axiom of regularity, there exists $X \in \{A\}$ such that if $x \in X$, then $x \notin \{A\}$. Now, $X \in \{A\}$ if and only if $X = A$. Thus, if $x \in A$, then $x \notin \{A\}$. Since $A \in \{A\}$, $A \notin A$. \sharp

Theorem 2.1.22 Given sets A and B , $A \notin B$ or $B \notin A$.

Proof Suppose that $A \in B$ and $B \in A$. Then, $B \in A$, $B \in \{A, B\}$, $A \in B$, and also $A \in \{A, B\}$. Thus, there is no $X \in \{A, B\}$ such that $x \in X$ implies that $x \notin \{A, B\}$. This contradicts the axiom of regularity. \sharp

Let X be a set. The set $X^+ = X \cup \{X\}$ is called the **successor** of X .

Proposition 2.1.23 Let X and Y be sets. Then, $X^+ = Y^+$ if and only if $X = Y$.

Proof If $X = Y$, then $X^+ = Y^+$. Suppose that $X \neq Y$ and $X^+ = Y^+$. Then, $X \cup \{X\} = Y \cup \{Y\}$. Since $X \in X \cup \{X\}$, $X \in Y \cup \{Y\}$, and since $X \neq Y$, $X \in Y$. Similarly, $Y \in X$. This is a contradiction (Theorem 2.1.22). \sharp

A set S is called a **successor set** if

- (i) $\{\emptyset\} \in S$, and
- (ii) $X \in S$ implies $X^+ \in S$.

The following axiom asserts that there is an infinite set.

Axiom 9 (*Axiom of infinity*) There exists a successor set.

Proposition 2.1.24 *Let X be a set of successor sets. Then, $\bigcap_{S \in X} S$ is also a successor set.*

Proof Since each S is a successor set, $\{\emptyset\} \in S$, for all $S \in X$. Hence, $\{\emptyset\} \in \bigcap_{S \in X} S$. Let $x \in \bigcap_{S \in X} S$. Then, $x \in S$, for all $S \in X$. Since each $S \in X$ is a successor set, $x^+ \in S$, for all $S \in X$. Hence, $x^+ \in \bigcap_{S \in X} S$. \sharp

Corollary 2.1.25 *Let X be a successor set. Then X contains the smallest successor set contained in X .*

Proof The intersection of all successor sets contained in X is the smallest successor set contained in X . \sharp

Corollary 2.1.26 *Let X and Y be successor sets. Let A be the smallest successor set contained in X , and B the smallest successor set contained in Y . Then $A = B$.*

Proof $X \cap Y$ is also a successor set. Thus, A and B are both smallest successor sets contained in $X \cap Y$. \sharp

Let X be a successor set. The smallest successor set contained in X , which is the smallest successor set contained in any other successor set, is called the set of *natural numbers*. The set of natural numbers is denoted by \mathbb{N} . $\{\emptyset\}$ is denoted by 1, and it is called *one*. $\{\emptyset\}^+ = \{\emptyset, \{\emptyset\}\}$ is denoted by 2, and it is called *two*, and so on. The properties of the set \mathbb{N} of natural numbers can be faithfully described in the form of Peano's axioms as given below:

Peano's Axiom

P_1 . $1 \in \mathbb{N}$.

P_2 . For all $x \in \mathbb{N}$, $x^+ \in \mathbb{N}$.

P_3 . $x^+ = y^+$ if and only if $x = y$.

P_4 . For all $x \in \mathbb{N}$, $1 \neq x^+$.

P_5 . If M is a set such that $1 \in M$ and $x^+ \in M$ for all $x \in M \cap \mathbb{N}$, then $\mathbb{N} \subseteq M$. Further properties of the natural number system \mathbb{N} will be discussed in detail in the next chapter.

Exercises

2.1.1 Show that

- (i) $A \cap \emptyset = \emptyset$
- (ii) $A \cup \emptyset = A$

(iii) $A - \emptyset = A$

(iv) $\emptyset - A = \emptyset$.

2.1.2 Show that $A - (A - B) = A \cap B$.

2.1.3 Show that $A - (A \cap B) = A - B$.

2.1.4 Show that $A \cup B = A$ if and only if $B \subseteq A$.

2.1.5 Show that $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

2.1.6 Show that $(A \cap B) \cup C = A \cap (B \cup C)$ if and only if $C \subseteq A$.

2.1.7 Show that $A \subseteq B$ implies $C \cup A \subseteq C \cup B$.

2.1.8 Show that $(A - B) - C = (A - C) - B$.

2.1.9 Show that

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

(ii) $A = A \cup (B \cap A)$.

2.1.10 Put $A \oplus B = (A - B) \cup (B - A)$. Show that

(i) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.

(ii) $A \oplus \emptyset = A = \emptyset \oplus A$.

(iii) $A \oplus B = B \oplus A$.

(iv) $A \oplus B = \emptyset$ if and only if $A = B$.

(v) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$.

(vi) $A \oplus C = B \oplus C$ if and only if $A = B$.

2.1.11 $A \subset B$ if and only if $\wp(A) \subseteq \wp(B)$.

2.1.12 Show that $\wp(A \cap B) = \wp(A) \cap \wp(B)$.

2.1.13 Show that $\wp(A) \cup \wp(B) \subseteq \wp(A \cup B)$. Show by means of an example that equality need not hold.

2.1.14 Suppose that A contains n elements. Show that $\wp(A)$ contains 2^n elements.

2.1.15 Can $\wp(A)$ be \emptyset ? Support.

2.1.16 Show that a union of successor sets is a successor set.

2.1.17 Let A be a successor set. Can $\wp(A)$ be a successor set? support.

2.1.18 Let A and B be successor sets. Can $A - B$ be a successor set? Support.

2.1.19 Show that $X^+ \neq X$ for every set X .

2.1.20 $(X^+)^+ \neq X$ for every set X .

2.1.21 Show that the empty set is not successor of any set.

2.2 Cartesian Product and Relations

Let X be a set. Let $a, b \in X$. Then, the set $\{\{a\}, \{a, b\}\}$ is a subset of $\wp(X)$. We denote the set $\{\{a\}, \{a, b\}\}$ by (a, b) and call it an **ordered pair**. Thus, $(a, b) \in \wp(\wp(X))$.

Proposition 2.2.1 $(a, b) = (b, a)$ if and only if $a = b$.

Proof Suppose that $(a, b) = (b, a)$. Then, $\{\{a\}, \{a, b\}\} = \{\{b\}, \{b, a\}\}$. Since $\{a, b\} = \{b, a\}$, $\{a\} = \{b\}$. Hence, $a = b$. Clearly, $a = b$ implies $(a, b) = (a, a) = (b, a)$. $\#$

Observe that $(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$.

Let X and Y be sets. Then, the set

$$X \times Y = \{(a, b) \mid a \in X \text{ and } b \in Y\}$$

is called the **cartesian product** of X and Y . Clearly, $X \times Y \subseteq \wp(\wp(X \cup Y))$.

Proposition 2.2.2 Let A, B , and C be sets. Then,

- (i) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
- (ii) $(A \cap B) \times C = (A \times C) \cap (B \times C)$.
- (iii) $(A - B) \times C = (A \times C) - (B \times C)$.

Proof (i). Let $(x, y) \in (A \cup B) \times C$. By the definition, ' $x \in A \cup B$ and $y \in C$.' This implies that ' $(x \in A \text{ and } y \in C) \text{ or } (x \in B \text{ and } y \in C)$.' Thus, ' $(x, y) \in (A \times C) \text{ or } (x, y) \in (B \times C)$.' By the definition, $(x, y) \in (A \times C) \cup (B \times C)$. It follows that ' $(A \cup B) \times C \subseteq (A \times C) \cup (B \times C)$.' Similarly, it follows that ' $(A \times C) \cup (B \times C) \subseteq (A \cup B) \times C$.' By the axiom of extension, $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

Similarly, we can prove (ii) and (iii). $\#$

Proposition 2.2.3 $A \times B = \emptyset$ if and only if $(A = \emptyset \text{ or } B = \emptyset)$.

Proof Suppose that $A = \emptyset$, and $(x, y) \in A \times B$. Then, $x \in \emptyset$ and $y \in B$. Since $x \in \emptyset$ is a contradiction, $(x, y) \in \emptyset \times B$ is also a contradiction. Hence, $\emptyset \times B = \emptyset$. Similarly, $A \times \emptyset = \emptyset$. Now, suppose that $A \neq \emptyset$ and $B \neq \emptyset$. Then, there is an element $x \in A$ and an element $y \in B$. In turn, $(x, y) \in A \times B$. Hence, $A \times B \neq \emptyset$. $\#$

Relations

Consider the relation 'is father of.' Nehru is father of Indira, and Feroze Gandhi is the father of Rajeev Gandhi. This gives us pairs (Nehru, Indira) and (Feroze Gandhi, Rajeev Gandhi). If we look at the set R of all pairs (a, b) , where a is father of b , then the set R faithfully describes the relation of 'is father of.' One is genuinely tempted to define a relation as a set of ordered pairs.

Definition 2.2.4 A subset R of $X \times X$ is called a **relation** on X . If $(x, y) \in R$, then we say that x is related to y under the relation R . We also express it by writing xRy .

Example 2.2.5 \emptyset is a relation on X in which no pair of elements in X are related. $X \times X$ is the largest (universal) relation on X in which each pair of elements in X is related.

Example 2.2.6 $\Delta = \{(x, x) \mid x \in X\}$ is a relation on X called the **diagonal** relation on X . This is the most selfish relation on X .

Example 2.2.7 Let $X = \{a, b, c\}$. $R = \{(a, b), (b, a), (a, c)\}$ is a relation on X .

Example 2.2.8 Let X be a set. Then, $R = \{(a, b) \mid a, b \in X \text{ and } a \in b\}$ is a relation on X .

Example 2.2.9 Let X be a set. Then, $R = \{(A, B) \mid A, B \in \wp(X) \text{ and } A \subseteq B\}$ is a relation on $\wp(X)$.

Let R and S be relations on X . Then, $R \cup S$, $R \cap S$, and $R - S$ are all subsets of $X \times X$, and hence, they are also relations on X .

Definition 2.2.10 Let R and S be relations on X . The relation

$$RoS = \{(x, z) \in X \times X \mid (x, y) \in S \text{ and } (y, z) \in R \text{ for some } y \in X\}$$

is called the **composition** of R and S .

Proposition 2.2.11 Let R , S , and T be relations on X . Then,

$$(RoS)oT = Ro(SoT).$$

Proof Let $(x, y) \in (RoS)oT$. By the definition,

there exists $z \in X$ such that $(x, z) \in T$, and $(z, y) \in RoS$.

Again, by the definition,

there exist z and $u \in X$ such that $(x, z) \in T$, $(z, u) \in S$, and $(u, y) \in R$.

Thus,

there exists $u \in X$ such that $(x, u) \in SoT$, and $(u, y) \in R$.

Hence, $(x, y) \in Ro(SoT)$. This shows that $(RoS)oT \subseteq Ro(SoT)$. Similarly, $Ro(SoT) \subseteq (RoS)oT$. By the axiom of extension, the result follows. \sharp

Proposition 2.2.12 $Ro\Delta = R = \Delta oR$.

Proof Since $(x, x) \in \Delta$ for all $x \in X$, $(x, y) \in Ro\Delta$ if and only if $(x, y) \in R$. This proves that $Ro\Delta = R$. Similarly, $R = \Delta oR$. \sharp

Proposition 2.2.13 *Let R , S and T be relations on X . Then*

- (i) $Ro(S \cup T) = (RoS) \cup (RoT)$
- (ii) $Ro(S \cap T) \subseteq (RoS) \cap (RoT)$
- (iii) $(R \cup S)oT = (RoT) \cup (SoT)$
- (iv) $(R \cap S)oT \subseteq (RoT) \cap (SoT)$

Proof (i) Let $(x, y) \in Ro(S \cup T)$. By the definition,

there exists $z \in X$ such that $(x, z) \in S \cup T$, and $(z, y) \in R$.

Thus,

there exists $z \in X$ such that $((x, z) \in S, \text{ and } (z, y) \in R)$ or $((x, z) \in T, \text{ and } (z, y) \in R)$.

In turn, it follows that ' $(x, y) \in (RoS)$ or $(x, y) \in (RoT)$.' Hence, $(x, y) \in (RoS) \cup (RoT)$. This shows that $Ro(S \cup T) \subseteq (RoS) \cup (RoT)$. Similarly, $(RoS) \cup (RoT) \subseteq Ro(S \cup T)$. By the axiom of extension, $Ro(S \cup T) = (RoS) \cup (RoT)$.

Similarly, we can prove the rest. ‡

Example 2.2.14 Let $X = \{a, b, c\}$. Let $R = \{(a, b), (a, c)\}$ and $S = \{(b, c), (b, b)\}$. Then $RoS = \emptyset$, and $SoR = \{(a, c), (a, b)\} = R$ (verify). Thus, RoS need not be SoR . Observe that $R = SoR = \Delta oR$, and $S \neq \Delta$. If we take $T = \{(a, a), (b, c), (b, b)\}$, then $RoT = \{(a, c), (a, b)\} = R$ and $ToR = R$. But $T \neq \Delta$. Thus, $RoT = R = ToR$ need not imply that $T = \Delta$.

Definition 2.2.15 Let R be a relation on X . Then, the relation

$$R^{-1} = \{(x, y) \in X \times X \mid (y, x) \in R\}$$

is called the **inverse** of R .

Example 2.2.16 Let $R = \{(a, b), (a, c)\}$ be a relation on the set $X = \{a, b, c\}$. Then, $R^{-1} = \{(b, a), (c, a)\}$. Now, $RoR^{-1} = \{(b, b), (c, c)\}$, and $R^{-1}oR = \{(a, a)\}$. Thus, here again, $RoR^{-1} \neq R^{-1}oR$.

Proposition 2.2.17 *Let R and S be relations on X . Then,*

- (i) $(R^{-1})^{-1} = R$
- (ii) $(RoS)^{-1} = S^{-1}oR^{-1}$.

Proof Clearly, $(x, y) \in R$ if and only if $(y, x) \in R^{-1}$. Also, $(y, x) \in R^{-1}$ if and only if $(x, y) \in (R^{-1})^{-1}$. Thus, $R = (R^{-1})^{-1}$. To prove (ii), let $(x, y) \in (RoS)^{-1}$. Then, $(y, x) \in RoS$. Hence, there exists $z \in X$ such that $(y, z) \in S$ and $(z, x) \in R$. Thus, $(x, z) \in R^{-1}$, and $(z, y) \in S^{-1}$ for some $z \in X$. But, then $(x, y) \in S^{-1}oR^{-1}$. This shows that $(RoS)^{-1} \subseteq S^{-1}oR^{-1}$. Similarly, $S^{-1}oR^{-1} \subseteq (RoS)^{-1}$. ‡

Types of Relations

Definition 2.2.18 A relation R on X is said to be

- (i) a **reflexive relation** if $(x, x) \in R$ for all $x \in X$, or equivalently if $\Delta \subseteq R$.
- (ii) a **symmetric relation** if $(x, y) \in R$ implies that $(y, x) \in R$, or equivalently if $R^{-1} = R$.
- (iii) an **antisymmetric relation** if $(x, y) \in R$ and $(y, x) \in R$ implies that $x = y$, or equivalently if $R \cap R^{-1} \subseteq \Delta$.
- (iv) a **transitive relation** if when ever $(x, y) \in R$ and $(y, z) \in R$, $(x, z) \in R$, or equivalently if $R \circ R \subseteq R$.

Example 2.2.19 Let $X = \{a, b, c\}$ and

$$R = \{(a, a), (b, b), (c, c), (a, b), (b, c), (c, b)\}.$$

Then, R is reflexive but none of the rest of the three.

Example 2.2.20 Let $X = \{a, b, c\}$ and $R = \{(a, b), (b, a)\}$. Then, R is symmetric but none of the rest of the three.

Example 2.2.21 Let $X = \{a, b, c\}$ and $R = \{(c, b), (a, c)\}$. Then, R is antisymmetric but none of the rest of the three.

Example 2.2.22 Let $X = \{a, b, c\}$ and

$$R = \{(a, b), (b, a), (a, a), (b, b), (a, c), (b, c)\}.$$

Then, R is transitive but none of the rest of the three.

Example 2.2.23 Let $X = \{a, b, c\}$ and

$$R = \{(a, a), (b, b), (c, c), (a, b), (b, a), (b, c), (c, b)\}.$$

Then, R is reflexive and symmetric but neither antisymmetric nor transitive.

Example 2.2.24 Let $X = \{a, b, c\}$ and

$$R = \{(b, c), (c, b), (b, b), (c, c)\}.$$

Then, R is symmetric and transitive but neither reflexive nor antisymmetric.

Proposition 2.2.25 Let R be a relation on X which is symmetric and transitive. Suppose that for all $x \in X$, there exists $y \in X$ such that $(x, y) \in R$. Then, R is reflexive.

Proof Let $x \in X$. Then, $(x, y) \in R$ for some $y \in X$. Since R is symmetric, $(y, x) \in R$. Since R is transitive, $(x, x) \in R$. Thus, R is reflexive. \sharp

Example 2.2.26 The relation which is reflexive, symmetric, and antisymmetric is the diagonal relation. Thus, a reflexive, symmetric, and antisymmetric relations are also transitive.

Exercises

2.2.1 Suppose that $A \times C \subseteq B \times C$, $C \neq \emptyset$. Show that $A \subseteq B$.

2.2.2 Show that $(A \times B = B \times A)$ if and only if $(A = \emptyset \text{ or } B = \emptyset \text{ or } A = B)$.

2.2.3 Suppose that A , B , and C are nonempty sets. Is $(A \times B) \times C = A \times (B \times C)$? Support.

2.2.4 Show that $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

2.2.5* Suppose that $A \subseteq A \times A$. Show that $A = \emptyset$.

Hint. Use the axiom of regularity.

2.2.6* Suppose that $A = A \times B$. Show that $A = \emptyset$.

2.2.7 Suppose that A contains n elements and B contains m elements. Show that $A \times B$ contains $n \cdot m$ elements.

2.2.8 Show that the number of relations on a set containing n elements is 2^{n^2} .

2.2.9 Let $X = \{a, b, c\}$, $R = \{(a, b), (b, c), (c, a)\}$ and $S = \{(a, a), (a, c), (b, b)\}$. Find out (i) $R \cup S$, (ii) $R \cap S$, (iii) RoS , and (iv) R^{-1} .

2.2.10 Show by means of an example that equality in Proposition 2.2.13 (ii) and (iv) need not hold.

2.2.11 Find out the number of reflexive relations on a set containing n elements.

Hint. A reflexive relation on $X \times X$ can be written as $\Delta \cup S$, where $S \subseteq X \times X - \Delta$.

2.2.12 Find out the number of symmetric relations on a set containing n elements.

2.2.13 Find out the number of antisymmetric relations on a set containing n elements.

2.3 Equivalence Relation

The concept of equality in mathematics is best described in terms of equivalence relations.

Definition 2.3.1 A relation R on X which is reflexive, symmetric, and transitive is called an **equivalence relation** on X .

Example 2.3.2 The diagonal relation Δ is the smallest equivalence relation on X . The universal relation $X \times X$ is the largest equivalence relation on X . The relation $R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$ is an equivalence relation on $X = \{a, b, c\}$.

Definition 2.3.3 Let R be an equivalence relation on X . Let $x \in X$. The subset

$$R_x = \{y \in X \mid (x, y) \in R\}$$

is called the **equivalence class** of X modulo R determined by the element x .

Thus, for example, the equivalence class Δ_x of X modulo Δ determined by x is the singleton $\{x\}$. For the equivalence relation $R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$ on $X = \{a, b, c\}$, the equivalence classes are $R_a = \{a, b\} = R_b$ and $R_c = \{c\}$.

Since R is reflexive, $(x, x) \in R$ for all $x \in X$, and hence, $x \in R_x$ for all $x \in X$.

Proposition 2.3.4 Let R be an equivalence relation on X . Then, the following hold.

- (i) $x \in R_x$ for all $x \in X$.
- (ii) $R_x = R_y$ if and only if $(x, y) \in R$.
- (iii) $R_x \neq R_y$ if and only if $R_x \cap R_y = \emptyset$.

Proof (i) Since R is reflexive, $(x, x) \in R$ for all $x \in X$, and hence $x \in R_x$ for all $x \in X$.

(ii) Suppose that $R_x = R_y$. Since R is an equivalence relation, $y \in R_y = R_x$. Hence $(x, y) \in R$. Conversely, suppose that $(x, y) \in R$. Since R is symmetric, $(y, x) \in R$. Let $z \in R_x$. Then, $(x, z) \in R$. Since R is transitive, $(y, z) \in R$. Thus, $z \in R_y$. Hence, $R_x \subseteq R_y$. Similarly, $R_y \subseteq R_x$. This shows that $R_x = R_y$.

(iii) Suppose that $R_x \cap R_y \neq \emptyset$. Let $z \in R_x \cap R_y$. Then, $(x, z) \in R$ and $(y, z) \in R$. Since R is symmetric and transitive, $(x, y) \in R$. It follows from (ii) that $R_x = R_y$. Clearly, if $R_x \cap R_y = \emptyset$, then $R_x \neq R_y$, for $x \in R_x$. \sharp

Let X be a non emptyset. A set \wp of nonempty subsets of X is called a **partition** of X if the following hold.

- (i) Union of members of \wp is X , i.e., $\bigcup_{A \in \wp} A = X$.
- (ii) If A and B are distinct members of \wp , then $A \cap B = \emptyset$.

Corollary 2.3.5 Let R be an equivalence relation on X . Then, $\wp_R = \{R_x \mid x \in X\}$ is a partition of X .

Proof Follows from the above proposition. \sharp

The partition \wp_R is the partition determined by the equivalence relation R . The set \wp_R is also denoted by X/R , and it is also called the **quotient set** of X modulo R .

Proposition 2.3.6 Let \wp be a partition of X . Define a relation R^\wp on X by $R^\wp = \bigcup_{A \in \wp} A \times A$. Then R^\wp is an equivalence relation such that $\wp_{R^\wp} = \wp$.

Proof Since union of members of \wp is X , given $x \in X$, $x \in A$ for some $A \in \wp$. Hence $(x, x) \in R^\wp$ for all $x \in X$. Thus, R^\wp is reflexive. Suppose that $(x, y) \in R^\wp$. Then, there is an element $A \in \wp$ such that $x, y \in A$, and so $y, x \in A$. Hence, $(y, x) \in R^\wp$. Thus, R^\wp is symmetric. Suppose that $(x, y) \in R^\wp$ and $(y, z) \in R^\wp$. Then, there is an element $A \in \wp$ and an element $B \in \wp$ such that $x, y \in A$ and $y, z \in B$. Since $y \in A \cap B$, $A \cap B \neq \emptyset$. Further, since \wp is a partition, $A = B$. Hence, $x, z \in A \in \wp$. Thus, $(x, z) \in R^\wp$. This shows that R^\wp is transitive.

Next, R_x^\wp is the member A of \wp such that $x \in A$. Hence, $\wp_{R^\wp} = \wp$. \sharp

Proposition 2.3.7 $R^{\wp_R} = R$ for every equivalence relation R .

Proof Suppose that $(x, y) \in R$. Then $x, y \in R_x \in \wp_R$. Hence $(x, y) \in R^{\wp_R}$. Suppose that $(x, y) \in R^{\wp_R}$. Then there exists $R_z \in \wp_R$ such that $x, y \in R_z$. Hence, there is an element $z \in X$ such that $(x, z) \in R$ and $(y, z) \in R$. Since R is symmetric and transitive, $(x, y) \in R$. This shows that $R = R^{\wp_R}$. \sharp

Remark 2.3.8 It is apparent from the above discussions that every partition can be realized faithfully as an equivalence relation, and every equivalence relation can be realized faithfully as a partition.

Example 2.3.9 Let R be a relation (not necessarily equivalence) on X . Define $R_x = \{y \in X \mid (x, y) \in R\}$. Suppose that $\wp = \{R_x \mid x \in X\}$ is a partition of X . Can we infer that R is an equivalence relation? No. For example, take $X = \{a, b, c\}$, $R = \{(a, b), (b, c), (c, a)\}$. Then, $R_a = \{b\}$, $R_b = \{c\}$, $R_c = \{a\}$. Thus, $\{R_a, R_b, R_c\}$ is a partition of X , whereas R is not an equivalence relation (it is neither reflexive nor symmetric nor transitive).

Example 2.3.10 Let $\wp \subseteq \wp(X)$ (not necessarily a partition). Consider the relation R^\wp on X given by $R^\wp = \{(x, y) \mid \text{such that } x, y \in A \text{ for some } A \in \wp\}$. Suppose that R^\wp is an equivalence relation. Can we infer that \wp is a partition? Again, no. For example, take $\wp = \{\{a, b\}, \{b, c\}, \{c, a\}\} \subseteq \wp(X)$, where $X = \{a, b, c\}$. Then, $R^\wp = X \times X$ is an equivalence relation.

Exercises

2.3.1 Let R and S be equivalence relations on X . Show that RoS is an equivalence relation if and only if $RoS = SoR$.

2.3.2 Let p_n denote the number of equivalence relations on a set containing n elements. Show that

$$p_{n+1} = \sum_{r=0}^n ({}^nC_r) p_r$$

Hint. p_n is the number of partitions of a set containing n elements.

2.3.3 Let $X = \{a, b, c, d\}$ and

$$R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (a, c), (b, a), (c, b), (c, a)\}.$$

Show that R is an equivalence relation. Find \wp_R . Can we find an other relation S such that $\wp_R = \wp_S$? Support.

2.3.4 Show that the intersection of symmetric relations is symmetric. Deduce that for every relation R on X , there is smallest symmetric relation containing R . This relation is called the symmetric closure of R . Find the symmetric closures of all the relations given above.

2.3.5 Show that the intersection of transitive relations is transitive. Deduce that for every relation R on X , there is smallest transitive relation containing R . This relation is called the transitive closure of R . Find the transitive closures of all the relations given above.

2.3.6 Show that the intersection of equivalence relations is equivalence relation. Deduce that for every relation R on X , there is smallest equivalence relation containing R . This relation is called the equivalence closure of R . Find the equivalence closures of all the relations given above.

2.3.7 Is composite of two symmetric relations always symmetric? If not under what conditions it is symmetric.

2.3.8 Is composite of two transitive relations always transitive? If not under what conditions it is transitive.

2.4 Functions

Let X and Y be sets. A subset f of $X \times Y$ (the Cartesian product) is called a **function** or a **mapping** (or a **map**) from X to Y if the following two conditions hold.

- (i) For all $x \in X$, *there exists* $y \in Y$ such that $(x, y) \in f$.
- (ii) If $(x, y_1) \in f$ and $(x, y_2) \in f$, *then* $y_1 = y_2$.

X is called the **domain**, and Y is called the **co-domain** of f . If $(x, y) \in f$, we write $y = f(x)$ and call it the **image** of the element $x \in X$ under the map f . Thus, under this notation, $f = \{(x, f(x)) \mid x \in X\}$.

Intuitively, a function f from X to Y is an association or a correspondence which associates to each $x \in X$, a unique $y \in Y$ which we denote by $f(x)$. Thus, to define a map f from X to Y , it is sufficient to give a unique $f(x)$ in Y for all $x \in X$. Any two functions f and g from X to Y are equal if and only if $f(x) = g(x)$ for all $x \in X$.

We also adopt the notation $f : X \longrightarrow Y$ to say that f is a map from X to Y .

Let f be a map from X to Y and g be a map from Y to Z . Then, gof defined by

$$gof = \{(x, z) \mid (x, y) \in f \text{ and } (y, z) \in g \text{ for some } y \in Y\}$$

is also a map from X to Z , and it is called the **composite** of f and g . Thus, the map gof from X to Z is given by $(gof)(x) = g(f(x))$ for all $x \in X$.

The subset Δ of $X \times X$ is also a map from X to X . This map is called the **identity map** on X , and it is denoted by I_X . Thus, $I_X(x) = x$ for all $x \in X$. Clearly, $f \circ I_X = f = I_Y \circ f$ for every map f from X to Y .

Let Y be a subset of X . Then, $i_Y = \{(y, y) \mid y \in Y\}$ is a map from Y to X called the **inclusion** map from Y to X . This map is sometimes denoted by the symbol $Y \hookrightarrow X$.

Let f be a map from X to A , and Y a subset of X . The composition foi_Y is a map from Y to A , and it is called the **restriction** of f to Y . The map foi_Y is also denoted by $f|_Y$.

Let X and Y be sets and $y \in Y$. Then, $X \times \{y\}$ is a map f from X to Y such that $f(x) = y$ for all $x \in X$. This map is called a **constant** map.

Let X and Y be sets. Consider the Cartesian product $X \times Y$. The map p_1 from $X \times Y$ to X defined by $p_1((x, y)) = x$ is called the first **projection** and the map p_2 from $X \times Y$ to Y defined by $p_2((x, y)) = y$ is called the second projection map.

Proposition 2.4.1 *Let f be a map from X to Y , g a map from Y to Z , and h a map from Z to U . Then $(hog)of = ho(gof)$.*

Proof Clearly, $((hog)of)(x) = (hog)(f(x)) = h(g(f(x))) = h((gof)(x)) = (ho(gof))(x)$ for all $x \in X$. Hence $ho(gof) = (hog)of$. \sharp

Let f be a map from X to Y . Then $f \subseteq X \times Y$. Consider $f^{-1} = \{(y, x) \mid (x, y) \in f\}$. Then $f^{-1} \subseteq Y \times X$ need not be a map from Y to X for two reasons: (i) for $y \in Y$, there may not be any $x \in X$ such that $(x, y) \in f$, and so there may not be any $x \in X$ such that $(y, x) \in f^{-1}$, (ii) $(y, x_1) \in f^{-1}$ and $(y, x_2) \in f^{-1}$ need not imply that $x_1 = x_2$. Thus, f^{-1} will be a map if and only if the following two conditions hold.

- (i) For all $y \in Y$, there is an element $x \in X$ such that $(x, y) \in f$.
- (ii) If $(x_1, y) \in f$ and $(x_2, y) \in f$, then $x_1 = x_2$.

A map f from X to Y is called a **surjective** map (also called an **onto** map) if for all $y \in Y$, there is an element $x \in X$ such that $(x, y) \in f$. Thus, f is a surjective map if for all $y \in Y$, there is an element $x \in X$ such that $f(x) = y$.

A map f from X to Y is called an **injective** map (also called a **one – one** map) if $(x_1, y) \in f$, $(x_2, y) \in f$ implies that $x_1 = x_2$. Thus, f is injective map if whenever $f(x_1) = f(x_2)$, $x_1 = x_2$. In other words, f is injective if whenever $x_1 \neq x_2$, $f(x_1) \neq f(x_2)$.

A map f which is injective as well as surjective is called a **bijective** map (also called a **one-one-onto** map).

Thus, f^{-1} is a map if and only if f is *bijective*, and then, the map f^{-1} is called the **inverse** of f . The inverse of a bijective map is also bijective.

Example 2.4.2 An injective map need not be surjective. For example, take $X = \{a, b\}$, $Y = \{x, y, z\}$. Define a map f from X to Y by $f(a) = x$ and $f(b) = y$. Then, f is *injective* but it is not *surjective*, for there is no element in X whose image is z .

Example 2.4.3 A surjective map need not be injective. Take $X = \{a, b, c\}$ and $Y = \{x, y\}$. Define a map f from X to Y by $f(a) = x = f(b)$, $f(c) = y$. Then, f is *surjective*, but it is not *injective*.

Proposition 2.4.4 *Let f be a bijective map from X to Y . Then, f^{-1} is also a bijective map from Y to X . Also (i) $(f^{-1})^{-1} = f$, (ii) $f^{-1}of = I_X$, and $fof^{-1} = I_Y$.*

Proof Let f be a bijective map. Then, we have already observed that f^{-1} is a map from Y to X . Suppose that $(y_1, x) \in f^{-1}$ and $(y_2, x) \in f^{-1}$. Then, $(x, y_1) \in f$ and $(x, y_2) \in f$. Since f is a map, $y_1 = y_2$. Thus, f^{-1} is injective. Let $x \in X$, then $(x, f(x)) \in f$, and hence, $(f(x), x) \in f^{-1}$. This shows that f^{-1} is surjective. We also observe that $(f^{-1}of)(x) = f^{-1}(f(x)) = x$ for all $x \in X$, and $(fof^{-1})(y) = f(f^{-1}(y)) = y$ for all $y \in Y$. Thus, $f^{-1}of = I_X$, and $fof^{-1} = I_Y$. The fact that $(f^{-1})^{-1} = f$ follows from the definition of f^{-1} .

Proposition 2.4.5 *(i) The composite of any two injective maps is an injective map, (ii) the composite of any two surjective maps is a surjective, and (iii) the composite of any two bijective maps is a bijective map.*

Proof (i) Let f be an injective map from X to Y and g be an injective map from Y to Z . Suppose $(gof)(x_1) = (gof)(x_2)$. Then, $g(f(x_1)) = g(f(x_2))$. Since g is injective, $f(x_1) = f(x_2)$. Further, since f is injective, $x_1 = x_2$. Hence, gof is injective.

(ii) Suppose that f and g are surjective maps. Let $z \in Z$. Since g is surjective, there exists an element $y \in Y$ such that $g(y) = z$. Again, since f is surjective, there exists an element $x \in X$ such that $f(x) = y$. But, then $(gof)(x) = g(f(x)) = g(y) = z$. Hence, gof is surjective.

(iii) Follows from (i) and (ii). \sharp

Proposition 2.4.6 *Let f be a map from X to Y and g be a map from Y to Z . Then, the following hold. (i) If gof is surjective, then g is surjective. (ii) If gof is injective, then f is injective.*

Proof (i) Suppose that gof is surjective. Let $z \in Z$. Since gof is surjective, there exists $x \in X$ such that $(gof)(x) = z$, i.e., $g(f(x)) = z$. Hence, g is surjective.

(ii) Suppose that gof is injective and $f(x_1) = f(x_2)$. Then, $g(f(x_1)) = g(f(x_2))$, i.e., $(gof)(x_1) = (gof)(x_2)$. Since gof is injective, $x_1 = x_2$. Hence, f is injective. \sharp

Corollary 2.4.7 *If gof is bijective, then g is surjective and f is injective.* \sharp

Proposition 2.4.8 *A map f from X to Y is injective if and only if it can be left canceled in the sense that if $fog = foh$, then $g = h$. A map f is surjective if and only if it can be right canceled in the sense that if $gof = hof$, then $g = h$.*

Proof Suppose that f is injective and $fog = foh$. Then, $f(g(z)) = (fog)(z) = (foh)(z) = f(h(z))$ for all $z \in Z$. Since f is injective, $g(z) = h(z)$ for all $z \in Z$. This shows that $g = h$. Now, suppose that f is not injective. Then, there exist elements $x_1, x_2 \in X$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$. Take $Z = \{x_1, x_2\}$. Define a map g from Z to X by $g(x_1) = x_1 = g(x_2)$ and a map h from Z to X by $h(x_1) = x_2 = h(x_2)$. Then, $g \neq h$ but $fog = foh$.

Next, suppose that f is surjective and g, h are maps from Y to Z such that $gof = hof$. Then, $g(f(x)) = h(f(x))$ for all $x \in X$. Since f is surjective, $g(y) = h(y)$ for all $y \in Y$. This shows that $g = h$. Now, suppose that f is not surjective. Then, there exists an element $y_0 \in Y$ such that $y_0 \neq f(x)$ for all $x \in X$. Take $Z = \{a, b\}$. Define a map g from Y to Z by $g(y_0) = a$, $g(y) = b$ for all $y \neq y_0$, and a map h from Y to Z by $h(y) = b$ for all $y \in Y$. Clearly, then, $g \neq h$ and $gof = hof$. \sharp

Corollary 2.4.9 *A map f from X to Y is bijective if and only if it can be canceled from left as well as from right.* \sharp

Proposition 2.4.10 *Let f be a map from X to Y . Then f is bijective if and only if there exists a map g from Y to X such that $gof = I_X$ and $fog = I_Y$. Further, then $g = f^{-1}$.*

Proof If f is bijective, then $f^{-1}of = I_X$ and $fog^{-1} = I_Y$ (Proposition 2.4.4). Let g be a map from Y to X such that $gof = I_X$ and $fog = I_Y$. Since $gof = I_X$ is injective, f is injective. Since $fog = I_Y$ is surjective, f is surjective. Further, then $f^{-1}of = I_X = gof$, and $fog^{-1} = I_Y = fog$. The result follows from the above corollary. \sharp

Corollary 2.4.11 *Let f be a bijective map from X to Y , and g be a bijective map from Y to Z . Then $(gof)^{-1} = f^{-1}og^{-1}$.*

Proof Clearly,

$$(f^{-1}og^{-1})o(gof) = (f^{-1}o(g^{-1}og))of = f^{-1}of = I_X.$$

Similarly,

$$(gof)o(f^{-1}og^{-1}) = I_Y.$$

The result follows. \sharp

Proposition 2.4.12 *There is no surjective map from any set X to its power set $\wp(X)$.*

Proof Let f be a map from X to $\wp(X)$. Consider the set $A = \{x \in X \mid x \notin f(x)\}$. Then, $A \in \wp(X)$. Suppose that $f(y) = A$ for some $y \in X$. If $y \notin A = f(y)$, then $y \in A$. If $y \in A = f(y)$, then $y \notin f(y) = A$. Hence, the supposition that $f(y) = A$ for some $y \in X$ is false. This shows that f can not be surjective. \sharp

Let X and Y be sets. The set of all maps from X to Y is denoted by Y^X . What are X^\emptyset and \emptyset^X ?

Example 2.4.13 Let X be a set, and 2 denotes the set $\{0, 1\}$. Define a map ϕ from $\wp(X)$ to 2^X by $\phi(A)(x) = 0$ if $x \notin A$ and $\phi(A)(x) = 1$ if $x \in A$. Check that the map ϕ is bijective.

Let f be a map from X to Y . Let $A \subseteq X$ and $B \subseteq Y$. The subset $f(A) = \{f(a) \mid a \in A\}$ of Y is called the **image** of A under the map f . The subset $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$ of X is called the **inverse image** of B under f .

What are $f^{-1}(Y)$ and $f^{-1}(\emptyset)$? To say that f is surjective is to say that $f(X) = Y$.

Proposition 2.4.14 *Let f be a map from X to Y and $A \subseteq X$. Then $A \subseteq f^{-1}(f(A))$. Also $A = f^{-1}(f(A))$ for all $A \subseteq X$ if and only if f is injective.*

Proof Let $a \in A$. Then, $f(a) \in f(A)$, and hence, by the definition, $a \in f^{-1}(f(A))$. Thus, $A \subseteq f^{-1}(f(A))$. Suppose that f is injective. Let $x \in f^{-1}(f(A))$. Then, $f(x) \in f(A)$ (by def). Hence, there exists an element $a \in A$ such that $f(x) = f(a)$. Since f is injective, $x = a \in A$. Thus, $f^{-1}(f(A)) \subseteq A$, and therefore, $A = f^{-1}(f(A))$. Suppose that f is not injective. Then, there exist elements $x_1, x_2 \in X$, $x_1 \neq x_2$ such that $f(x_1) = f(x_2) = y$ (say). Take $A = \{x_1\}$. Then, $f(A) = \{y\}$ and $\{x_1, x_2\} \subseteq f^{-1}(f(A))$. Hence, $A \neq f^{-1}(f(A))$. $\#$

Proposition 2.4.15 *Let f be a map from X to Y and $B \subseteq Y$. Then $f(f^{-1}(B)) \subseteq B$. Also $B = f(f^{-1}(B))$ for all $B \subseteq Y$ if and only if f is surjective.*

Proof Let $y \in f(f^{-1}(B))$. Then, $y = f(x)$ for some $x \in f^{-1}(B)$. But then $y = f(x) \in B$. Hence, $f(f^{-1}(B)) \subseteq B$. Suppose that f is surjective and $y \in B$. Then, there exists an element $x \in X$ such that $f(x) = y$. Clearly, $x \in f^{-1}(B)$, and hence, $y = f(x) \in f(f^{-1}(B))$. Therefore, $B = f(f^{-1}(B))$. Suppose now that f is not surjective. Then, there exists an element $b \in Y$ such that $b \notin f(X)$. But, then $f^{-1}(\{b\}) = \emptyset$, and hence, $f(f^{-1}(\{b\})) = \emptyset \neq \{b\}$. $\#$

Proposition 2.4.16 *Let f be a map from X to Y . Let A_1 and A_2 be subsets of X . Then, the following hold.*

- (i) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
- (ii) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.

Further, in (ii), equality holds for every pair of subsets A_1 and A_2 of X if and only if f is injective.

Proof The proof of (i) and (ii) is left as exercises. We prove the last assertion. Suppose now that f is injective. Let $y \in f(A_1) \cap f(A_2)$. Then, there is an element $a \in A_1$ and an element $b \in A_2$ such that $y = f(a) = f(b)$. Since f is injective, $a = b \in A_1 \cap A_2$, and so $y = f(a) \in f(A_1 \cap A_2)$. Thus, $f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$. But already (from (ii)) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. Thus, equality holds in (ii) if f is injective. Conversely, suppose that f is not injective. Then, we have two distinct elements x_1, x_2 in X such that $f(x_1) = f(x_2) = b$ (say). Take $A_1 = \{x_1\}$, $A_2 = \{x_2\}$. Then, $f(A_1 \cap A_2) = f(\emptyset) = \emptyset$, whereas $f(A_1) \cap f(A_2) = \{b\} \neq \emptyset$. $\#$

Proposition 2.4.17 *Let f be a map from X to Y . Let B_1 and B_2 be subsets of Y . Then, the following hold.*

- (i) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.
- (ii) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
- (iii) $f^{-1}(B_1 - B_2) = f^{-1}(B_1) - f^{-1}(B_2)$.

Proof (i) Let $x \in f^{-1}(B_1 \cap B_2)$. By the definition, $f(x) \in B_1 \cap B_2$. Thus, $f(x) \in B_1$ and $f(x) \in B_2$. This implies that $x \in f^{-1}(B_1)$ and $x \in f^{-1}(B_2)$. In turn, $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$. This shows that $f^{-1}(B_1 \cap B_2) \subseteq f^{-1}(B_1) \cap f^{-1}(B_2)$. Similarly,

$f^{-1}(B_1) \cap f^{-1}(B_2) \subseteq f^{-1}(B_1 \cap B_2)$. This proves (i). Similarly, we can prove the rest of the two. \sharp

Family of sets.

Let I be a set and X be a set of sets. A surjective map A from I to X is called a **family of sets**. We denote the image $A(\alpha)$ of α by A_α . This family of sets is denoted by $\{A_\alpha \mid \alpha \in I\}$. The set I is called the **indexing set** of the family.

Let $\{A_\alpha \mid \alpha \in I\}$ be a family of sets. Then, the set

$$\bigcup_{\alpha \in I} A_\alpha = \{x \mid x \in A_\alpha \text{ for some } \alpha \in I\}$$

is called the **union** of the family, and

$$\bigcap_{\alpha \in I} A_\alpha = \{x \mid x \in A_\alpha \text{ for all } \alpha \in I\}$$

is called the **intersection** of the family.

Proposition 2.4.18 (De Morgan's Law) *Let X be a set and $\{A_\alpha \mid \alpha \in I\}$ be a family of sets. Then, $\{X - A_\alpha \mid \alpha \in I\}$ is another family of sets and*

- (i) $X - (\bigcup_{\alpha \in I} A_\alpha) = \bigcap_{\alpha \in I} (X - A_\alpha)$.
- (ii) $X - (\bigcap_{\alpha \in I} A_\alpha) = \bigcup_{\alpha \in I} (X - A_\alpha)$.

The proof of the above proposition is left as an exercise.

Let $\{X_i, i \in \{1, 2\}\} = \{X_1, X_2\}$ be a family of sets containing only two sets X_1 and X_2 . An element (x_1, x_2) of the Cartesian product $X_1 \times X_2$ can be faithfully realized as a map x from $\{1, 2\}$ to $X_1 \cup X_2$ with $x(1) = x_1$ and $x(2) = x_2$. This prompts us to define the Cartesian product of an arbitrary family as follows:

Definition 2.4.19 Let $\{X_\alpha \mid \alpha \in I\}$ be a family of sets. Let $\prod_{\alpha \in I} X_\alpha$ denote the set of all maps x from I to $\bigcup_{\alpha \in I} X_\alpha$ with the property that $x(\alpha) \in X_\alpha$ for all $\alpha \in I$. The set $\prod_{\alpha \in I} X_\alpha$ is called the **Cartesian product** of the family. Further, for each $\alpha_0 \in I$, the map p_{α_0} from $\prod_{\alpha \in I} X_\alpha$ to X_{α_0} defined by $p_{\alpha_0}(x) = x(\alpha_0)$ is called the α_0^{th} *projection map*.

The Axioms 1–9 constitute the Zermelo–Fraenkel (ZF) axiomatic system for set theory.

Consider the set X of countries in the world. How to select a unique city in each country? More explicitly, how to get a map c from the set X to the set of all cities in the world so that $c(A) \in A$ for all countries A in X . Here, we can give a rule to define the map c by saying that $c(A)$ is the capital of the country A . In general, if $\{X_\alpha \mid \alpha \in I\}$ is a nonempty family of nonempty sets, how to choose a unique member from each class. The following is an other fundamental and important axiom of set theory which ensures the existence of such a map.

Axiom 10 (*Axiom of Choice*) Let $\{X_\alpha \mid \alpha \in I\}$ be a nonempty family of nonempty sets (i.e., I is nonempty, and $X_\alpha \neq \emptyset$ for all $\alpha \in I$). Then, $\prod_{\alpha \in I} X_\alpha$ is nonempty set. More explicitly, there exists a map c from I to $\bigcup_{\alpha \in I} X_\alpha$ (called a choice function) such that $c(\alpha) \in X_\alpha$ for all $\alpha \in I$.

Remark 2.4.20 K. Godel in 1932 proved that the axiom of choice is consistent with the ZF axiomatic system. More explicitly, the negation of the axiom of choice is not a theorem in the ZF axiomatic system. Later, P. Cohn established that the axiom of choice is not a theorem in ZF axiomatic system. In turn, the axiom of choice is independent of the ZF axiomatic system. It also follows that the ZF axiomatic system is incomplete. The Axioms 1–10 constitute ZFC axiomatic system. The axiomatic system ZFC is also incomplete. Consider the following hypothesis: ‘If there is an injective map from \mathbb{N} to X , and there is an injective map from X to $2^{\mathbb{N}}$, then there is a bijective from \mathbb{N} to X , or else there is a bijective map from X to $2^{\mathbb{N}}$.’ This hypothesis is called the continuum hypothesis (CH). Godel and Cohen proved that the continuum hypothesis is independent of the ZFC axiomatic system. The Whitehead problem in group theory asks: ‘Is every abelian group A with $EXT^1(A, \mathbb{Z}) = \{0\}$ a free abelian group?’ The Whitehead problem is also an undecidable proposition in ZFC .

Let f be a map from X to Y and g a map from Z to U . Then, the map $f \times g$ from $X \times Z$ to $Y \times U$ defined by $(f \times g)((x, z)) = (f(x), g(z))$ is called the **Cartesian product** of the map f with the map g . Clearly, products of injective maps are injective maps, and those of surjective maps are surjective.

Let f be a map from X to Y and S an equivalence relation on Y . Then, $(f \times f)^{-1}(S)$ is an equivalence relation on X (verify). Let R be an equivalence relation on X . Then, $(f \times f)(R)$ need not be an equivalence relation on Y even if f is surjective (give an example to support this).

The equivalence relation $(f \times f)^{-1}(\Delta)$ on X is called the **kernel** of f , and it is denoted by **ker** f . It follows from the definitions that f is injective if and only if $\text{ker } f = \Delta$ (the diagonal relation on X).

Proposition 2.4.21 *Let f be a surjective map from X to Y . Let R be an equivalence relation on X containing the kernel of f . Then $(f \times f)(R)$ is an equivalence relation on Y such that $(f \times f)^{-1}((f \times f)(R)) = R$.*

Proof Clearly, $(f \times f)(R)$ is symmetric. Since f is surjective, $(f \times f)(R)$ is also reflexive. We prove that it is transitive also. Let $(u, v), (v, w) \in (f \times f)(R)$. Then, there exist $(x, y), (z, t) \in R$ such that $(f(x), f(y)) = (u, v)$ and $(f(z), f(t)) = (v, w)$. This shows that $f(y) = f(z) = v$. Hence, $(y, z) \in (f \times f)^{-1}(\Delta) = \text{ker } f \subseteq R$. Since R is transitive, $(x, t) \in R$. But, then $(u, w) = (f(x), f(t)) \in (f \times f)(R)$. Thus, $(f \times f)(R)$ is an equivalence relation. Finally, we show that $(f \times f)^{-1}((f \times f)(R)) = R$. Clearly, $R \subseteq (f \times f)^{-1}((f \times f)(R))$. Let $(x, y) \in (f \times f)^{-1}((f \times f)(R))$. Then, $(f(x), f(y)) \in (f \times f)(R)$. Hence, there exists $(z, t) \in R$ such that $(f(x), f(y)) = (f(z), f(t))$. But then $f(x) = f(z)$ and $f(y) = f(t)$. This shows that (x, z) and (y, t) belong to $(f \times f)^{-1}(\Delta)$. Since $(f \times f)^{-1}(\Delta)$ is supposed to be contained in R , $(x, z), (y, t)$ and (z, t) are all in R . Since R is an equivalence relation, $(x, y) \in R$. This completes the proof. \sharp

Corollary 2.4.22 (Correspondence Theorem) *Let f be a surjective map from X to Y . Let $R(X)$ denote the set of all equivalence relations on X containing $\ker f$ and $R(Y)$ the set of all equivalence relations on Y . Then, f induces a bijective map \bar{f} from $R(X)$ to $R(Y)$ defined by $\bar{f}(R) = (f \times f)(R)$.*

Proof From the above proposition, it follows that $(f \times f)(R) \in R(Y)$ for all $R \in R(X)$. Thus, \bar{f} is a map from $R(X)$ to $R(Y)$. Since f is surjective, $f \times f$ is also surjective. Hence, $(f \times f)((f \times f)^{-1}(S)) = S$ for all $S \in R(Y)$. This shows that \bar{f} is surjective (note that $(f \times f)^{-1}(S) \in R(X)$). Further, suppose that $\bar{f}(R_1) = \bar{f}(R_2)$. Then, $(f \times f)(R_1) = (f \times f)(R_2)$. Since R_1 and R_2 are equivalence relations containing $\ker f$, it follows from the above proposition that $R_1 = (f \times f)^{-1}((f \times f)(R_1)) = (f \times f)^{-1}((f \times f)(R_2)) = R_2$. This proves that \bar{f} is injective. \sharp

Let X be a set and R be an equivalence relation on X . Consider the quotient set $X/R = \{R_x \mid x \in X\}$. The map ν from X to X/R defined by $\nu(x) = R_x$ is called the **quotient map**. Clearly, ν is surjective and $(\nu \times \nu)^{-1}(\Delta) = \{(x, y) \mid R_x = \nu(x) = \nu(y) = R_y\} = R$. Thus, every equivalence relation is kernel of a map. We shall show that if f is a surjective map from X to Y , then Y can be realized as a quotient set through a bijective map.

Theorem 2.4.23 *Let f be a surjective map from X to Y . Let R be an equivalence relation on X containing $\ker f$. Let $S = (f \times f)(R)$. Then, there is a bijective map \bar{f} from X/R to Y/S such that the diagram*

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 \nu \downarrow & & \downarrow \nu \\
 X/R & \xrightarrow{\bar{f}} & Y/S
 \end{array}$$

is commutative.

Proof Suppose that $R_{x_1} = R_{x_2}$. Then, $(x_1, x_2) \in R$, and so $(f(x_1), f(x_2)) \in (f \times f)(R) = S$. Hence, $S_{f(x_1)} = S_{f(x_2)}$. This shows that we have a map \bar{f} from X/R to Y/S defined by $\bar{f}(R_x) = S_{f(x)}$. Further, since f is surjective, every member of Y/S is of the form $S_{f(x)} = \bar{f}(R_x)$. This shows that \bar{f} is surjective. Suppose that $\bar{f}(R_{x_1}) = \bar{f}(R_{x_2})$. Then, $S_{f(x_1)} = S_{f(x_2)}$. This means that $(f(x_1), f(x_2)) \in S = (f \times f)(R)$. In turn, $(x_1, x_2) \in (f \times f)^{-1}((f \times f)(R))$. From the Proposition 2.4.21, it follows that $(x_1, x_2) \in R$. This means that $R_{x_1} = R_{x_2}$, and so \bar{f} is also injective. The commutativity of the diagram is evident. \sharp

Corollary 2.4.24 (Fundamental Theorem of Maps) *Let f be a surjective map from X to Y , and $R = (f \times f)^{-1}(\Delta) = \ker f$. Then there is a bijective map ϕ from X/R to Y such that $\phi \circ \nu = f$.*

Proof Clearly, $(f \times f)((f \times f)^{-1}(\Delta)) = \Delta$. Take $S = \Delta$ in the above theorem. One also observes that the quotient map ν from Y to Y/Δ is bijective map given by $\nu(y) = \{y\}$. Take $\phi = \nu^{-1} \circ f$. The result follows from the above theorem. \sharp

Exercises

2.4.1 Let X be a finite set containing n elements and Y be a set containing m elements. Suppose that $n \leq m$. Find the number of injective maps from X to Y . What happens if $m < n$?

2.4.2 Find the number of surjective maps from a set containing n elements to a set containing m elements.

2.4.3 Let X be a set. Show that there is no injective map from $P(X)$ to X .

2.4.4 Let X^Y denote the set of all maps Y to X . Suppose that $X \neq \emptyset$. Show that there is a surjective map from Y to X^Y if and only if X is a singleton set.

2.4.5 Let X , Y , and Z be sets. Show that there is a bijective map from $X^{Y \times Z}$ to $(X^Y)^Z$.

2.4.6 Let R and S be two equivalence relations on a set X such that $R \subseteq S$. Show that there is a bijective map $\phi : X/S \rightarrow (X/R)/(\nu \times \nu)(S)$ such that the diagram formed by quotient maps is commutative.

2.4.7 Let $\{X_\alpha \mid \alpha \in I\}$ be a family of nonempty sets. Show that each projection map is a surjective map.

Hint. Use the axiom of choice.

2.4.8 Let $f : X \rightarrow Y$ be a surjective map. Show that there is an injective map t from Y to X such that $f \circ t = I_Y$.

Hint. Use the axiom of choice.

2.4.9 Let $f : X \rightarrow Y$ be an injective map. Show that there is a surjective map $s : Y \rightarrow X$ such that $s \circ f = I_X$.

2.4.10 Let X be a nonempty set. Show that the following conditions on X are equivalent:

- (i) Every injective map from X to X is surjective.
- (ii) Every surjective map from X to X is injective.
- (iii) Every injective map from X to X is bijective.

Hint. Use the Exercises 2.4.8 and 2.4.9.

A set satisfying the condition in Exercise 2.4.10 is called a **finite set**. A set which is not finite is called an **infinite set**.

2.4.11 Show that every subset of a finite set is finite, and every set containing an infinite set is infinite.

2.4.12 Show that the union of two finite sets is finite.

2.4.13 Show that every successor set is infinite (This justifies the name ‘Axiom of Infinity’ for the existence of successor set).

Hint. If X is a successor set, then the map $x \longleftarrow x^+$ is an injective map from $X \cup \{\emptyset\}$ to itself which is not surjective.

2.4.14 Show that $f(A) - f(B) \subseteq f(A - B)$. Show further that the equality holds provided that f is injective.

2.5 Partial Order

Let X be a set. A relation R on X is called a **partial order** if it is reflexive, anti-symmetric, and transitive. Usually, a partial order is denoted by ‘ \leq .’ A pair (X, \leq) , where \leq is a partial order on X , is called a **partially ordered set**.

Example 2.5.1 Let Y be a set and $X = \wp(Y)$. Then, the relation $\{(A, B) \mid A \subseteq B\}$ is a partial order, and it is called the inclusion relation on X . We denote this relation also by \subseteq . Thus, (X, \subseteq) is a partial ordered set. Note that the inverse of a partial order is also a partial order. Thus, \supseteq is also a partial order on X .

Example 2.5.2 Let $X = \{a, b, c, d\}$. Then,

$$R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (c, d)\}$$

is a partial order on X .

Let (X, \leq) be a partially ordered set and Y be a subset of X . Then, the induced relation on Y is also a partial order on Y which is denoted by \leq_Y .

A partial order \leq on X is called a **total order** if given x, y in X , $x \leq y$ or $y \leq x$. Example 2.5.2 is not a total order. Example 2.5.1 is a total order if and only if Y is singleton (prove it).

Example 2.5.3 Let $X = \{a, b, c, d\}$ and

$$R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (a, c), (c, d), (a, d), (b, d)\}.$$

Then, R is a total order on X

Let (X, \leq) be a partially ordered set. A subset Y of X is called a **chain** in X if the induced partial order on Y is a total order on Y .

Example 2.5.4 Let $Y = \{a, b, c\}$ and $X = \wp(Y)$. Then, the inclusion relation is a partial order on X . The subset $Z = \{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}\}$ is a chain in X .

Let (X, \leq) be a partially ordered set and $A \subseteq X$. An element $x \in X$ is called an **upper bound (lower bound)** of A if $a \leq x (x \leq a)$ for all a in A .

Remark 2.5.5 A subset of a partially ordered set need not have any upper bound (lower bound). It may have several upper bounds (lower bounds). Give examples to support it.

Let (X, \leq) be a partially ordered set. An element $a \in X$ is called a **maximal (minimal) element** if $a \leq x (x \leq a)$ implies that $x = a$.

In Example 2.5.2, b and d are maximal elements, whereas a and c are minimal elements of X . Thus, there may be so many maximal or minimal elements of a partially ordered set. There may not be any maximal or minimal elements (give examples to support it).

Example 2.5.6 Let $X = \wp(Y) - \{Y, \emptyset\}$, where $Y = \{a, b, c\}$. Then, X is a partially ordered set with respect to inclusion. Clearly, $\{a, b\}$, $\{b, c\}$, $\{a, c\}$ are maximal elements and $\{a\}$, $\{b\}$, $\{c\}$ are minimal elements.

Example 2.5.7 Let $X = \{a, b, c\}$ and $\Delta = \{(a, a), (b, b), (c, c)\}$. Then, Δ is a partial order on X such that each element is maximal and also each element is minimal.

Example 2.5.8 Let Y be an infinite set and X be the set of all finite subsets of Y . Then, X is a partially ordered set with respect to inclusion relation which has no maximal element. If we take the set Z of infinite subsets of Y , then it has no minimal elements.

Let (X, \leq) be a partially ordered set. An element $a \in X$ is called the **largest (least)** element of X if $x \leq a (a \leq x)$ for all $x \in X$. If x_1 and x_2 are largest (least) elements of X , $x_1 \leq x_2$ and $x_2 \leq x_1$. By the antisymmetry of \leq , $x_1 = x_2$. Thus, there is a unique largest (least) element in a partially ordered set provided it exists.

It may be observed that a largest (least) element is also a maximal (minimal) but a maximal (minimal) element need not be the largest (least). In Example 2.5.2, b and d (a and c) are maximal (minimal) but none of them are largest (least). It may also be noticed that largest (least) need not exist (see Example 2.5.6).

Let (X, \leq) be a partially ordered set and $A \subseteq X$. Let $U(A)(L(A))$ denote the set of all upper (lower) bounds of A (note that $U(A)(L(A))$ may be empty sets also). Then, \leq induces a partial order on $U(A)(L(A))$. Note that all elements of A are lower (upper) bounds of $U(A)(L(A))$. Thus, $A \subseteq L(U(A))(A \subseteq U(L(A)))$. The least (largest) element of $U(A)(L(A))$ (if exists) is called the **least upper bound (greatest lower bound)** of A . The least upper bound (greatest lower bound) of A is denoted by **l.u.b(A) (g.l.b(A))** or **sup A (inf A)**. If A has the largest (least) element, then that is the l.u.b (g.l.b) of A .

Remark 2.5.9 Least upper bound (greatest lower bound) need not exist even if A has upper (lower) bounds: Let $Y = \{a, b, c, d\}$ and $X = \wp(Y) - \{\{a, b\}\}$. Then, \subseteq defines a partial order on X . Take $A = \{\{a\}, \{b\}\}$. Then, $U(A) = \{\{a, b, c\}, \{a, b, d\}, Y\}$. Clearly, $U(A)$ has no least element. Thus, A has no l.u.b.

Theorem 2.5.10 *Let (X, \leq) be a partially ordered set. Then, the following conditions are equivalent.*

- (1) *Every nonempty subset of X which has an upper bound has least upper bound in X .*
- (2) *Every nonempty subset of X which has a lower bound has greatest lower bound.*

Proof Assume 1. Let A be a nonempty subset of X which has a lower bound. Then, $L(A) \neq \emptyset$. Clearly, $\emptyset \neq A \subseteq U(L(A))$. Hence, $L(A)$ has an upper bound. By 1, $L(A)$ has the least upper bound a (say). Since a is the least element of $U(L(A))$ (by the definition of l.u.b) and $A \subseteq U(L(A))$, $a \leq x$ for all $x \in A$. Thus, $a \in L(A)$. Further, if $y \in L(A)$, then $y \leq x$ for all $x \in U(L(A))$. In particular, $y \leq a$. Thus, a is the largest element of $L(A)$. This shows that a is the g.l.b.A.

The proof of $2 \implies 1$ is similar. $\#$

A partial order \leq on X is called a **complete order** if it satisfies any one (and hence both) of the equivalent conditions of the above theorem.

Let (X, \leq) be a partially ordered set. A subset Y of X is called an **initial segment** of X if $y \in Y$ and $x \leq y$ implies that $x \in Y$. Thus, X itself is an initial segment of (X, \leq) . For each $x \in X$, the subset $\sigma_x = \{y \in Y \mid y \leq x\}$ is an initial segment of X associated with the element $x \in X$. The map σ from X to $\wp(X)$ defined by $\sigma(x) = \sigma_x$ is an injective map from X to $\wp(X)$ which is order preserving in the sense that ' $x \leq y \iff \sigma_x \subseteq \sigma_y$.' Again, for each $x \in X$, the subset $\eta_x = \{y \in X \mid y < x\}$ is also an initial segment. This initial segment is called the **strict initial segment** associated with x .

A partial order \leq on X is called a **well-order** if every nonempty subset of X has the least element. A pair (X, \leq) , where \leq is a well-order, is called a **well-ordered set**. Every well-order is a total order: Let \leq be a well-order on X . Let $x, y \in X$. Then, $\{x, y\}$ is a nonempty subset of X . Since \leq is a well-order, $\{x, y\}$ has a least element. If x is the least element, then $x \leq y$; if y is the least element, then $y \leq x$. This proves that every well-order is a total order. Indeed, a well-order is a complete order. For, suppose that \leq is a well-order on X . Let A be a nonempty subset of X which has an upper bound. Then, the set $U(A)$ of upper bounds of A is a nonempty subset of X . Since \leq is a well-order on X , $U(A)$ has the least element a (say). Evidently, a is the least upper bound of A . A complete order need not be a well-order. For example, the inclusion relation on the power set $\wp(X)$ of $X = \{a, b, c\}$ is a complete order, but it is not a well-order.

Proposition 2.5.11 *Let (X, \leq) be a well-ordered set. Then, a proper subset Y of X is an initial segment if and only if it is strict initial segment η_x for some $x \in X$. It need not be σ_x for any $x \in X$.*

Proof Let Y be a proper subset of X . Then, $X - Y \neq \emptyset$. Since (X, \leq_X) is a well-ordered set, $X - Y$ has least element x (say). Clearly, $\eta_x \subseteq Y$. Since Y is an initial segment, $x \not\leq_X y$ for any $y \in Y$. This shows that $Y \subseteq \eta_x$. Thus, $Y = \eta_x$. Note that the successor \mathbb{N}^+ of \mathbb{N} is a well-ordered set with usual inclusion ordering, and \mathbb{N} is a proper subset of \mathbb{N}^+ which is an initial segment, but it is not σ_x for any $x \in \mathbb{N}^+$. $\#$

Finally, we state and prove the two important equivalents of axiom of choice which are commonly used in mathematics.

Zorn's Lemma: Let (X, \leq) be a nonempty partially ordered set in which every chain has an upper bound. Then, (X, \leq) has a maximal element.

Well-ordering principle: On every set, there is a well-order.

Theorem 2.5.12 *The following are equivalent:*

- (1) *Axiom of choice.*
- (2) *Zorn's lemma.*
- (3) *Well-ordering principle.*

Proof The following is the scheme of the proof. We shall prove that $2 \implies 3$, $3 \implies 1$, and then $1 \implies 2$.

($2 \implies 3$). Assume 2. Let X be a set. We have to show the existence of a well-order on X . If $X = \emptyset$, then there is nothing to do. Assume that X is a nonempty set. Consider the set Σ given by

$$\Sigma = \{(Y, \leq_Y) \mid \leq_Y \text{ is a well-order on } Y, \text{ where } Y \subseteq X\}.$$

If $x \in X$, then there is the unique partial order $\leq_{\{x\}}$ on $\{x\}$ which is a well-order. Thus, $(\{x\}, \leq_x) \in \Sigma$. Hence, Σ is nonempty set. We say that $(Y, \leq_Y) \leq (Z, \leq_Z)$ if $(Y, \leq_Y) = (Z, \leq_Z)$ or else $Y \subset Z$, $\leq_Z \restriction Y = \leq_Y$, and $Y = \eta_z$ for some $z \in Z$. Clearly, (Σ, \leq) is a nonempty partially ordered set. Let $\Omega = \{(Y_\alpha, \leq_{Y_\alpha}) \mid \alpha \in \Lambda\}$ be a chain in (Σ, \leq) . Take $Y_0 = \bigcup_{\alpha \in \Lambda} Y_\alpha$. Then, there is a unique order \leq_{Y_0} on Y_0 whose restriction to each Y_α is \leq_{Y_α} . If A is a nonempty subset of Y_0 , then $A \cap Y_{\alpha_0} \neq \emptyset$ for some $\alpha_0 \in \Lambda$. If $(Y_\alpha, \leq_{Y_\alpha}) \leq (Y_{\alpha_0}, \leq_{Y_{\alpha_0}})$ for all $\alpha \in \Lambda$, then $Y_0 = Y_{\alpha_0}$, and so A has the least element. If not, then there is an element $\alpha \in \Lambda$ such that $(Y_{\alpha_0}, \leq_{Y_{\alpha_0}}) < (Y_\alpha, \leq_{Y_\alpha})$. Hence, there is an element $x \in Y_0$ such that $Y_{\alpha_0} = \eta_x$.

Let a be the least element of $A \cap Y_{\alpha_0}$. Let b be any element of A . Then, b is not strictly less than a , for then b will be a member of $A \cap Y_{\alpha_0}$. Hence, $a \leq_{Y_0} b$. Thus, a is the least element of A . It follows that (Y_0, \leq_{Y_0}) is a well-ordered set, and it is an upper bound of Ω . This shows that every chain in (Σ, \leq) has an upper bound. By the Zorn's lemma, there is a maximal element (M, \leq_M) of (Σ, \leq) . We show that $M = X$. Suppose not. Then, there is an element $x_0 \in X - M$. Consider the set $L = M \cup \{x_0\}$. Extend the well-order \leq_M on M to the well-order \leq_L on L by defining $x \leq_L x_0$ for all $x \in M$. Clearly, $(L, \leq_L) \in \Sigma$, and it is larger than (M, \leq_M) . This is a contradiction to the maximality of (M, \leq_M) . Thus, $M = X$, and \leq_X is a well-order on X . This completes the proof of $2 \implies 3$.

($3 \implies 1$). Assume 3. Let $\{X_\alpha \mid \alpha \in \Lambda\}$ be a nonempty family of nonempty sets. By the well-ordering principle, there is a well-order \leq_α on X_α for each α . For each $\alpha \in \Lambda$, let $c(\alpha)$ denote the least element of X_α . This gives us a map c from Λ to $\bigcup_{\alpha \in \Lambda} X_\alpha$ such that $c(\alpha) \in X_\alpha$. This completes the proof of $3 \implies 1$.

($1 \implies 2$). Assume 1. Let (X, \leq) be a nonempty partially ordered set in which every chain has an upper bound. We need to show the existence of a maximal element.

Recall the map σ from X to $\wp(X)$ given by $\sigma(x) = \sigma_x$, where $\sigma_x = \{y \in X \mid y \leq x\}$ is the initial segment associated with x . Clearly, σ is an injective map which is order preserving in the sense that ' $x \leq y$ if and only if $\sigma(x) \subseteq \sigma(y)$.' Consider $Y = \sigma(X)$. Then, (X, \leq) is order isomorphic to (Y, \subseteq) . It is sufficient, therefore, to show that (Y, \subseteq) has a maximal element. Let $C(X)$ denote the set of all chains in X . Then, $(C(X), \subseteq)$ is also a partially ordered set. Further, since every chain in (X, \leq) has an upper bound, every member of $C(X)$ is contained in a member of Y . Thus, Y is co-final in $(C(X), \subseteq)$. It follows that the maximal members of (Y, \subseteq) are same as those of $(C(X), \subseteq)$. It is sufficient, therefore, to show that $(C(X), \subseteq)$ has a maximal element.

Now, $C(X)$ satisfies the following two properties:

- (i) If $A \in C(X)$, then all subsets of A also belong to $C(X)$. In particular, $\emptyset \in C(X)$.
- (ii) If Γ is a chain in $(C(X), \subseteq)$, then $\bigcup_{A \in \Gamma} A \in C(X)$.

By the axiom of choice, we have a map c from $\wp(X) - \{\emptyset\}$ to X such that $c(A) \in A$ for all $A \in \wp(X) - \{\emptyset\}$. For each $A \in C(X)$, consider the set $\tilde{A} = \{x \in X \mid A \cup \{x\} \in C(X)\}$. To say that A is maximal in $(C(X), \subseteq)$ is to say that $\tilde{A} = A$. Define a map χ from $C(X)$ to X by $\chi(A) = A$ if $\tilde{A} - A = \emptyset$, and $\chi(A) = A \cup \{c(\tilde{A} - A)\}$ if $\tilde{A} - A \neq \emptyset$. We need to show that there is an element $A \in C(X)$ such that $\chi(A) = A$.

Let us call a subset Σ of $C(X)$ to be a tower in $C(X)$ if the following 3 conditions hold.

- (i) $\emptyset \in \Sigma$.
- (ii) $\chi(A) \in \Sigma$ for all $A \in \Sigma$.
- (iii) If Γ is a chain in (Σ, \subseteq) , then $\bigcup_{A \in \Gamma} A \in \Sigma$.

Clearly, $C(X)$ is a tower, and the intersection of a family of towers is a tower. Let Σ_0 denote the smallest tower in $C(X)$. Indeed, it is the intersection of all towers in $C(X)$. It is sufficient to show that Σ_0 is a chain in $(C(X), \subseteq)$. For, then $B = \bigcup_{A \in \Sigma_0} A \in \Sigma_0$, and so $\chi(B) \in \Sigma_0$. Since $\chi(B) \subseteq B$, it follows that $\chi(B) = B$.

Now, we show that Σ_0 is a chain in $C(X)$. More explicitly, we need to show that for any pair $A, B \in \Sigma_0$, $A \subseteq B$, or $B \subseteq A$. Let

$$\Gamma = \{A \in \Sigma_0 \mid \text{for all } B \in \Sigma_0, A \subseteq B \text{ or } B \subseteq A\}.$$

Clearly, $\emptyset \in \Gamma$. Let $A \in \Gamma$. Consider

$$\Gamma_A = \{B \in \Sigma_0 \mid B \subseteq A \text{ or } \chi(A) \subseteq B\}.$$

We show that Γ_A is tower. Clearly, $\emptyset \in \Gamma_A$. Let $B \in \Gamma_A$. Then, $B \subseteq A$ or $\chi(A) \subseteq B$. Suppose that $B \subseteq A$. If $B = A$, then $\chi(A) = \chi(B)$, and so in this case, $\chi(B) \in \Gamma_A$. Suppose that $B \subset A$. Then, $\chi(B) \subseteq A$. For, if not, then, since $A \in \Gamma$, $A \subset \chi(B)$. This is not true, for $\chi(B)$ contains at the most one more element than B . Thus, in this case also, $\chi(B) \in \Gamma_A$. Finally, if $\chi(A) \subseteq B$, then $\chi(A) \subseteq \chi(B)$. In this case also, $\chi(B) \in \Gamma_A$.

Let $\{B_\alpha \mid \alpha \in \Lambda\}$ be a chain in Γ_A . Then, from the definition of Γ_A , either each B_α is contained in A or $\chi(A)$ is contained in some B_α . This shows that $\bigcup_{\alpha \in \Lambda} B_\alpha \subseteq A$ or $\chi(A) \subseteq \bigcup_{\alpha \in \Lambda} B_\alpha$. Hence, $\bigcup_{\alpha \in \Lambda} B_\alpha \in \Gamma_A$.

This completes the proof of the fact that Γ_A is a tower contained in Σ_0 . Since Σ_0 is the smallest tower, it follows that $\Gamma_A = \Sigma_0$.

Finally, we prove that $\Gamma = \Sigma_0$. Indeed, again, we prove that Γ is a tower. Clearly, $\emptyset \in \Gamma$. Let $A \in \Gamma$. Consider $\chi(A)$. Let $B \in \Sigma_0$. Then, from what we have proved above, $\Gamma_A = \Sigma_0$, and so $B \in \Gamma_A$. Hence, $B \subseteq A \subseteq \chi(A)$, or $\chi(A) \subseteq B$. This shows that $\chi(A) \in \Gamma$. Let $\{A_\alpha \mid \alpha \in \Lambda\}$ be a chain in Γ . Let $B \in \Sigma_0$. Then, either each A_α is contained in B , or $B \subseteq A_\alpha$ for some α . This means that $\bigcup_{\alpha \in \Lambda} A_\alpha \subseteq B$, or $B \subseteq \bigcup_{\alpha \in \Lambda} A_\alpha$. This means that $\bigcup_{\alpha \in \Lambda} A_\alpha \in \Gamma$. Hence, Γ is a tower. In turn, $\Gamma = \Sigma_0$. Hence, Σ_0 is a chain. \sharp

Exercises

2.5.1 Let (X, \leq) be a partially ordered set. Let $A \subseteq B$. Show that $U(A) \supseteq U(B)$ and $L(A) \supseteq L(B)$.

2.5.2 Show that $U(A) = U(L(U(A)))$ and $L(A) = L(U(L(A)))$.

2.5.3 Show that g.l.b need not exist.

2.5.4 Let $A \subseteq B$. Show that

- (i) $\text{g.l.b}B \leq \text{g.l.b}A$
- (ii) $\text{l.u.b}A \leq \text{l.u.b}B$.

2.5.5 Show by means of an example that l.u.bA need not belong to A .

2.5.6 Show that $(P(X), \subseteq)$ is order complete.

2.5.7 Give an example of a partially ordered set which is not complete.

2.5.8 A partially ordered set (L, \leq) is called a **lattice** if any pair of points a, b has the least upper bound denoted by $a \vee b$ as well as the greatest lower bound $a \wedge b$. Show that $(P(X), \subseteq)$ is a lattice.

2.5.9 Let (X, \leq_X) and (Y, \leq_Y) be well-ordered sets. Show that $X \times Y$ with dictionary order is a well-ordered set.

2.5.10 Let f be a surjective map from X to Y . Use axiom of choice to show the existence of an injective map g from Y to X such that fog is the identity map on Y .

2.6 Ordinal Numbers

Definition 2.6.1 A well-ordered set (α, \leq) is called an **ordinal number** if for each $x \in \alpha$, the strict initial segment $\eta_x = \{a \in \alpha \mid a < x\}$ is same as x .

There is a unique well-order $\phi = \phi \times \phi$ on the set ϕ . Clearly, the statement ' $\forall x \in \phi, \eta_x = \{a \in \alpha \mid a < x\} = x$ ' is vacuously satisfied. Thus, the \emptyset together with this ordering is an ordinal. This ordinal number is denoted by 0. However, if (α, \leq) is an ordinal number, where $\alpha \neq \emptyset$, then $\emptyset \in \alpha$, and indeed, ϕ is the least element of α . For, by the definition of an ordinal number, if x is the least element of α , then $\emptyset = \{a \in \alpha \mid a < x\} = \eta_x = x$.

Example 2.6.2 Consider the set $1 = \{\emptyset\}$. There is only one well-order \leq on 1. The strict initial segment $\eta_\emptyset = \{x \mid x < \emptyset\} = \emptyset$. It follows that $(1, \leq)$ is an ordinal number. The set $2 = \{\phi, \{\phi\}\}$ with the inclusion ordering is clearly an ordinal number. Indeed, all natural numbers are ordinals.

Example 2.6.3 Consider the set \mathbb{N} of natural numbers together with inclusion ordering. Let A be a nonempty subset of \mathbb{N} . If $\emptyset \in A$, then ϕ is the least element of A . Let $x \in A$. Then, since $x \in \mathbb{N}$ is an ordinal, $\eta_x = x$ is a well-ordered set. Clearly, the least element of $A \cap \eta_x$ is the least element of A . It follows that \mathbb{N} together with the usual inclusion ordering is a well-ordered set. By the definition, $\eta_x = x$. Thus, \mathbb{N} with usual ordering is an ordinal. This ordinal will be denoted by ω .

Example 2.6.4 Consider the set the successor \mathbb{N}^+ of the set \mathbb{N} of natural numbers. We extend the well-ordering of \mathbb{N} to the ordering $\leq_{\mathbb{N}^+}$ on \mathbb{N}^+ by defining $n \leq_{\mathbb{N}^+} \mathbb{N}$ for all $n \in \mathbb{N}$. Clearly, $(\mathbb{N}^+, \leq_{\mathbb{N}^+})$ is a well-order. Further, it is also an ordinal number, for the strict initial segment $\eta_{\mathbb{N}} = \{n \in \mathbb{N}^+ \mid n <_{\mathbb{N}^+} \mathbb{N}\} = \mathbb{N}$. This ordinal is the continuation of ω , and it is denoted by $\omega + 1$. Similarly, we have the ordinal number $\omega + 2$, and so on. The axiom of replacement ensures the existence of the set $\{\omega + n \mid n \in \omega\}$ of ordinal numbers such that $\omega + n^+ = (\omega + n)^+$. This is a well-ordered set of ordinal numbers with ω the least ordinal number. Indeed, $\omega + n^+$ is the continuation of $\omega + n$. There is a unique well-order $\leq_{\omega(2)}$ on the union $\omega 2 = \bigcup_{n \in \omega} (\omega + n)$ subject to the condition that their restriction to each $\omega + n$ is the order $\leq_{\omega+n}$ of the ordinal number $\omega + n$. This process continues to generate different ordinal numbers.

Definition 2.6.5 Two partially ordered sets (X, \leq_X) , and (Y, \leq_Y) are said to be **order isomorphic** (also called similar) if there is a bijective map f from X to Y such that $a \leq_X b$ implies that $f(a) \leq_Y f(b)$.

Proposition 2.6.6 Let f be an order isomorphism from a partially ordered set (X, \leq_X) to a partially ordered set (Y, \leq_Y) . Then

- (i) $a <_X b$ implies that $f(a) <_Y f(b)$,
- (ii) f^{-1} is an order isomorphism from (Y, \leq_Y) to (X, \leq_X) , and
- (iii) the relation of being 'order isomorphic to' is an equivalence relation on any set of partially ordered sets.

Proof (i) Suppose that $a <_X b$. Then, by the definition, $f(a) \leq_Y f(b)$. Suppose that $f(a) = f(b)$. Since f is bijective, $a = b$. This is a contradiction to the supposition that $a <_X b$.

(ii) Suppose that f is an order isomorphism. Suppose that $c \leq_Y d$, where $c, d \in Y$. Suppose that $a = f^{-1}(c)$, and $b = f^{-1}(d)$. Then, $f(a) = c$ and $f(b) = d$. If $b <_X a$, then from (i), $d = f(b) <_Y f(a) = c$. This is a contradiction. Hence, $f^{-1}(c) \leq_X f^{-1}(d)$.

(iii) Since I_X is an order isomorphism from (X, \leq_X) to itself, the relation is reflexive. If f is an order isomorphism from (X, \leq_X) to (Y, \leq_Y) , then, from (ii), it follows that f^{-1} is an order isomorphism from (Y, \leq_Y) to (X, \leq_X) . This shows that the relation is symmetric. Since the composition of two order isomorphisms is an order isomorphism, it follows that the relation is transitive.

Proposition 2.6.7 *A well-ordered set (X, \leq_X) may be order isomorphic to a proper subset Y with induced well-ordering. If f is an injective order preserving map from a well-ordered subset (X, \leq_X) to itself, then $a \leq f(a)$ for all $a \in X$.*

Proof \mathbb{N} is a well-ordered set with usual ordering, and the successor map s from \mathbb{N} to its proper subset $\mathbb{N} - \{0\}$ is an order isomorphism. Let f be an injective order preserving map from a well-ordered subset (X, \leq_X) to itself. Let $A = \{x \in X \mid f(x) <_X x\}$. Suppose that $A \neq \emptyset$. Since (X, \leq_X) is a well-ordered set, A has the least element b (say). Then, $f(b) <_X b$. From the above proposition, $f(f(b)) <_X f(b)$. This means that $f(b) \in A$. This is a contradiction. Hence, $A = \emptyset$, and so $a \leq_X f(a)$ for all $a \in X$. \sharp

Corollary 2.6.8 *Let (X, \leq_X) and (Y, \leq_Y) be two well-ordered sets which are order isomorphic. Then, there is a unique order isomorphism from X to Y .*

Proof Let f and g be two order isomorphisms from X to Y . Then, $g^{-1} \circ f$ is an order isomorphism from X to itself. From the previous proposition, $a \leq_X g^{-1}(f(a))$ for all $a \in X$. This means that $g(a) \leq_Y f(a)$ for all $a \in X$. Similarly, considering the order isomorphism $f^{-1} \circ g$, we conclude that $f(a) \leq_X g(a)$ for all $a \in X$. This shows that $f = g$. \sharp

Corollary 2.6.9 *A well-ordered set can not be order isomorphic to any of its strict initial segment.*

Proof Let (X, \leq_X) be a well-ordered set. Let $x \in X$. Consider the strict initial segment η_x . Let f be a map from X to η_x . Then, $f(x) <_X x$. From the Proposition 2.6.7, it follows that f can not be an order isomorphism. \sharp

Corollary 2.6.10 *The only order isomorphism from a well-ordered set (X, \leq_X) to itself is the identity map.* \sharp

Corollary 2.6.11 *Let (X, \leq_X) and (Y, \leq_Y) be well-ordered sets. Then, one and only one of the following hold:*

- (i) (X, \leq_X) is order isomorphic to a strict initial segment of (Y, \leq_Y) .
- (ii) (Y, \leq_Y) is order isomorphic to a strict initial segment of (X, \leq_X) .
- (iii) (X, \leq_X) is order isomorphic to (Y, \leq_Y) .

Proof From the Corollary 2.6.9, it follows that at the most one of the above condition can hold. We need to prove that at least one of the three conditions hold. Let (X, \leq_X) and (Y, \leq_Y) be well-ordered sets. Further, from the Corollary 2.6.9, it again follows that in any well-ordered set the strict initial segment associated with a is order isomorphic to an strict initial segment associated with b if and only if $a = b$. Let

$$\Sigma = \{x \in X \mid \eta_x \text{ is order isomorphic to } \eta_y \text{ for some, } y \in Y\}.$$

Let $a \in \Sigma$, and $x <_X a$, $x \in X$. Then, there is a unique element $b \in Y$ such that η_a is order isomorphic to η_b . Let f be the unique order isomorphism from η_a to η_b . Then, $f(x) \in \eta_b$, and the restriction of f to η_x is an order isomorphism from η_x to $\eta_{f(x)}$. Hence, $x \in \Sigma$. This ensures that Σ is an initial (not necessarily proper) segment of X . We have the map χ from Σ to Y given by the condition that η_x is order isomorphic to $\eta_{\chi(x)}$. Clearly, χ is an injective order preserving map. Observe that the image $\chi(\Sigma)$ is also an initial segment of Y . If $\Sigma = X$, then X will either be order isomorphic to Y or it is order isomorphic to a proper initial segment of Y . Suppose that $\Sigma \neq X$. Then, Σ is a proper segment, and hence, there is an element $x \in X - \Sigma$ such that $\eta_x = \Sigma$. Suppose that $\chi(\Sigma) \neq Y$. Then $\chi(\Sigma)$ is a proper segment of Y . Hence, there exists an element $y \in Y$ such that $\chi(\Sigma) = \eta_y$. But then η_x is order isomorphic to η_y , where $x \notin \Sigma$. This is a contradiction to the choice of Σ . Hence, $\chi(\Sigma) = Y$. This means that Y is order isomorphic to the initial segment Σ of X . \sharp

Proposition 2.6.12 *Let (α, \leq_α) and (β, \leq_β) be ordinal which are order isomorphic as well-ordered set. Then $(\alpha, \leq_\alpha) = (\beta, \leq_\beta)$.*

Proof Let f be an order isomorphism from α to β . We need to show that $f(x) = x$ for all $x \in \alpha$. Consider $\gamma = \{x \in \alpha \mid f(x) = x\}$. Suppose that $\gamma \neq \alpha$. Then, $\alpha - \gamma \neq \emptyset$. Since (α, \leq_α) is a well-ordered set, $\alpha - \gamma \neq \emptyset$ has the least element a (say). Then, $f(x) = x$ for all $x \in \eta_a$. Since f is an order isomorphism, and α and β are ordinals, $a = \eta_a = f(\eta_a) = \eta_{f(a)} = f(a)$. This is a contradiction. Hence, $\gamma = \alpha$. This shows that $(\alpha, \leq_\alpha) = (\beta, \leq_\beta)$. \sharp

Corollary 2.6.13 *Every set of ordinal numbers is a total order.*

Proof Follows from Corollary 2.6.11 and the above proposition. \sharp

Corollary 2.6.14 *Every set of ordinal numbers is well-ordered.*

Proof Let Ω be a set of ordinal numbers. Let Σ be a nonempty subset of Ω . Let $\alpha \in \Sigma$. If $\alpha \leq \beta$ for all $\beta \in \Sigma$, then α is the least element of Σ , and there is nothing to do. Suppose that there is a $\beta \in \Sigma$ such that $\beta < \alpha$. From the definition of ordinal number, $\beta \in \alpha$. This means that $\alpha \cap \Sigma$ is non empty subset of α . Since α is a well-ordered set, it has the least element γ (say). We show that γ is the least element of Σ . Let $\delta \in \Sigma$. If $\alpha \leq \delta$, then $\gamma \leq \delta$. If not, then $\delta < \alpha$, and so $\delta \in \alpha \cap \Sigma$. Since γ is the least element of $\alpha \cap \Sigma$, $\gamma \leq \delta$. This shows that γ is the least element of Σ . \sharp

The ordinals are of two types: Consider the ordinal ω . For all $n < \omega$, there is an ordinal number m such that $n < m < \omega$. In other words, there is no immediate predecessor of ω . Such ordinals are called the **limit ordinals**. All the natural numbers have immediate predecessors. These are not limit ordinals. The ordinal $\omega 2$ is also a limit ordinal.

Corollary 2.6.15 *Let Ω be a set of ordinal numbers. Then, Ω is a order complete with respect to the ordering of ordinal numbers.*

Proof The result follows from the fact that every well-ordered set is order complete. \sharp

Corollary 2.6.16 *Let Ω be a set of ordinal numbers. Then, there is an ordinal number $\alpha \notin \Omega$. In other words, there is no set containing all ordinal numbers.*

Proof Let Ω be a set of ordinal numbers. Let $\beta = \bigcup_{\alpha \in \Omega} \alpha$. Then, there is a unique order \leq_β on β whose restriction to each $\alpha \in \Omega$ is the order \leq_α on α . Consider (β, \leq_β) . Let $a \in \beta$. Then, $a \in \alpha$ for some $\alpha \in \Omega$. Hence, the strict initial segment η_a is a itself. This shows that (β, \leq_β) is an ordinal number which is an upper bound (indeed, l.u.b of Ω) of Ω . β may be a member of Ω in case it is a limit ordinal. However, the successor β^+ of β is an ordinal number which does not belong to Ω . \sharp

Proposition 2.6.17 *Let (X, \leq_X) be a well-ordered set. Then, there is a unique ordinal (α, \leq_α) which is order isomorphic to (X, \leq_X) .*

Proof The uniqueness part is evident from the Proposition 2.6.12. We show the existence of an ordinal which is order isomorphic to (X, \leq_X) . Let a be an element of X such that for each $x \in \eta_a$, there is, of course, unique ordinal α_x which is order isomorphic to η_x . Clearly, the least element of X is such an element. It is also clear that η_a is order isomorphic to the ordinal β , where β is the l.u.b of the set $\{\alpha_x \mid x \in \eta_a\}$ of ordinals. This shows that if each strict initial segment of η_a is order isomorphic to an ordinal number, then η_a is also order isomorphic to an ordinal number.

Let

$$\Sigma = \{a \in X \mid \forall x \in \eta_a, \eta_x \text{ is order isomorphic to an ordinal number } \alpha_x\}.$$

Clearly, the least element of X belongs to Σ . We first show that $\Sigma = X$. Suppose not. Then, $X - \Sigma$ is a nonempty subset of X . Since (X, \leq_X) is a well-ordered set, it has the least element a (say). Then, for all $x <_X a$, $x \in \Sigma$. This means that for all $y \in \eta_x$, η_y is order isomorphic to an ordinal α_y . From what we have already proved, it follows that η_x is also order isomorphic to an ordinal number α_x . We arrive at a contradiction that $a \in \Sigma$. Thus, $\Sigma = X$. Repeating again the previous arguments, we see that X is order isomorphic to an ordinal. \sharp

Remark 2.6.18 The above proposition may prompt us to introduce an ordinal number as an equivalence class of well-ordered sets. But the equivalence classes are not sets. As such, one needs to select unique members from each equivalence classes. Indeed, this is what we have done in our approach.

Arithmetic of Ordinal Numbers

Let (A, \leq_A) and (B, \leq_B) be two well-ordered sets. We have an order \leq_{AB} on $A \times \{0\} \cup B \times \{1\}$ defined as follows: (i) $(a, 0) \leq_{AB} (a', 0)$ if and only if $a \leq_A a'$, (ii) $(b, 1) \leq_{AB} (b', 1)$ if and only if $b \leq_B b'$, and (iii) $(a, 0) \leq_{AB} (b, 1)$ for all $a \in A$ and $b \in B$. Clearly, \leq_{AB} is a well-order. If (A, \leq_A) is order isomorphic to (C, \leq_C) and (B, \leq_B) is order isomorphic to (D, \leq_D) , then it is clear that $(A \times \{0\} \cup B \times \{1\}, \leq_{AB})$ is order isomorphic to $(C \times \{0\} \cup D \times \{1\}, \leq_{CD})$. Thus, we can define, unambiguously, the sum $\alpha + \beta$ of two ordinal numbers as follows: Suppose that α is order isomorphic to (A, \leq_A) and β is order isomorphic to (B, \leq_B) . Define $\alpha + \beta$ to be the unique ordinal number which is order isomorphic to $(A \times \{0\} \cup B \times \{1\}, \leq_{AB})$. The following properties addition of ordinal numbers can be easily observed:

- (i) $\alpha + 0 = \alpha = 0 + \alpha$, and
- (ii) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
for all ordinals α, β , and γ .

The addition of ordinal number is not commutative. Indeed, $1 + \omega = \omega$ is limit ordinal, where as $\omega + 1 = \omega^+$ is not limit ordinal.

Next, suppose that (A, \leq_A) and (B, \leq_B) are two well-ordered sets. We have the lexicographic ordering $\leq_{A \times B}$ on $A \times B$ defined as follows: $(a, b) \leq_{A \times B} (c, d)$ if $b <_B d$ or $b = d$ and $a \leq_A c$. It can be checked that this order is a well-order. Further, if (A, \leq_A) is order isomorphic to (C, \leq_C) and (B, \leq_B) is order isomorphic to (D, \leq_D) , then $(A \times B, \leq_{A \times B})$ is order isomorphic to $(C \times D, \leq_{C \times D})$. This prompts us to define the multiplication \cdot on ordinals as follows: Suppose that the ordinal α is order isomorphic to the well-ordered set (A, \leq_A) and the ordinal β is order isomorphic to (B, \leq_B) . Define $\alpha \cdot \beta$ to be the unique ordinal which is order isomorphic to the well-ordered set $(A \times B, \leq_{A \times B})$. The following properties of \cdot can be easily observed.

- (i) $\alpha \cdot 0 = 0 = 0 \cdot \alpha$,
- (ii) $\alpha \cdot 1 = \alpha = 1 \cdot \alpha$,
- (iii) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$, and
- (iv) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$
for all ordinal numbers α, β , and γ . Note that the left distributivity of \cdot over $+$ need not hold.

For further arithmetical properties of ordinals, refer to Naive set theory by Halmos, or to the set theory by Vipul Kakkar.

2.7 Cardinal Numbers

The abstraction of the counting process of finite sets leads to the concept of the ordinal numbers. On a finite set X , any two well-order structure is order isomorphic. Indeed, two finite well-ordered sets (X, \leq_X) and (Y, \leq_Y) define the same ordinal

numbers if and only if their sizes are same in the sense that there is a bijective map from X to Y . However, this is not the situation in infinite case. Indeed, on the same infinite set X , we can have different well-order structures which define different ordinal numbers. For example, the usual well-order \leq on the set \mathbb{N} of natural numbers determines the ordinal number ω . We have another order \leq' on \mathbb{N} defined as follows: If $m \neq 1 \neq n$, then $m \leq' n$ if and only if $m \leq n$. Also, $m \leq' 1$ for all $m \in \mathbb{N}$. Clearly, (\mathbb{N}, \leq') is a well-ordered set, and the initial segment η_1 in (\mathbb{N}, \leq') is $\mathbb{N} - \{1\}$. Note that (\mathbb{N}, \leq) and (\mathbb{N}, \leq') are not order isomorphic. (\mathbb{N}, \leq') is order isomorphic to the ordinal $\omega + 1$. Similarly, we have another well-order on \mathbb{N} defined as follows: If $m, n \in \mathbb{N} - \{1, 2\}$, $m \leq'' n$ if and only if $m \leq n$. Also, $m \leq'' 1 \leq'' 2$ for all $m, n \in \mathbb{N} - \{1, 2\}$. Then, (\mathbb{N}, \leq'') is order isomorphic to $\omega + 2$, and so on. Thus, there are infinitely many nonorder isomorphic well-order structures on \mathbb{N} corresponding to different ordinals. Thus, ordinals are good for counting, but it does not distinguish the size of the infinite sets. This prompts us to look for an other concept, the concept of cardinals which measures the size of sets.

Definition 2.7.1 Let X and Y be sets. We say that X dominates Y if there is an injective map from Y to X . X and Y are said to be **equipotent** or **equinumerous** if there is a bijective map from X to Y . We use the notation $X \approx Y$ to say that X is equipotent to Y .

Theorem 2.7.2 (Schröder-Bernstein Theorem) *If X dominates Y and Y also dominates X , then X is equipotent to Y . More explicitly, if there is an injective map from X to Y , and also there is an injective map from Y to X , then there is a bijective map from X to Y .*

Proof Let f be an injective map from X to Y and g be an injective map from Y to X . We have to show that X and Y are equipotent. Put $X - g(Y) = Z$. Then, $X = g(Y) \cup Z$, where $g(Y)$ and Z are disjoint. Since Y and $g(Y)$ are equipotent, it is sufficient to show that $g(Y)$ and X are equipotent. Let $u \in (gof)^r(Z) \cap (gof)^s(Z)$, where $r < s$. Then, there exist $x, y \in Z$ such that $u = (gof)^r(x) = (gof)^s(y)$. Since gof is injective, $x = (gof)^{s-r}(y)$. This means that $x \in Z \cap g(Y)$. This is impossible. It follows that $(gof)^r(Z) \cap (gof)^s(Z) = \emptyset$ for all $r \neq s$. Put $U = \bigcup_{r \in \mathbb{N}} (gof)^r(Z)$, and $V = \bigcup_{r \in \mathbb{N} - \{1\}} (gof)^r(Z)$. Then, $U = (gof)(Z) \cup V$. From what we have observed, it follows that $(gof)(Z)$ and V are disjoint. Also, U and V are equipotent. Indeed, gof is a bijective map from U to V . Also Z and $(gof)(Z)$ are equipotent. Since $U = (gof)(Z) \cup V$, $Z \cup U$ is equipotent to U (note that Z and U are disjoint). Now, put $g(Y) - U = W$. Then, $g(Y) = U \cup W$. Hence, $X = U \cup W \cup Z$. Since $U \cup Z$ is equipotent to U , $U \cup W$ is equipotent to X . This shows that $g(Y)$ is equipotent to X . \sharp

Definition 2.7.3 An ordinal number α is said to be a **cardinal number** if whenever an ordinal number β is equipotent to α , $\alpha \leq \beta$.

Thus, all natural numbers are cardinal numbers. ω is a cardinal number, whereas $\omega + 1$ is not a cardinal number. The ordinal number ω considered as a cardinal number is

denoted by \aleph_0 . Indeed, an infinite cardinal number is a limit ordinal. It follows from the properties of ordinal numbers that a set of cardinal numbers is totally ordered.

Let X be a set. From the well-ordering principle, there is a well-order on X . The set of all ordinal numbers which are order isomorphic to the different well-order structures on X has the least element. This least element is clearly a cardinal number, and it is called the cardinal number of X . The cardinal number of X is denoted by $|X|$. Evidently, $|X| = |Y|$ if and only if X is equipotent to Y . Further, if $a = |X|$ and $b = |Y|$ are two cardinal numbers, then $a \leq b$ if and only if there is an injective map from X to Y .

Definition 2.7.4 A set X is said to be a **countable set** if $|X|$ is a natural number, or it is \aleph_0 . It is said to be an infinite countable set if $|X| = \aleph_0$. Thus, X is countably infinite if and only if there is a bijective map from X to \mathbb{N} . A set X is said to be **uncountable** if it is not countable.

Since there is no surjective map from \mathbb{N} to the power set $\wp(\mathbb{N})$, $\wp(\mathbb{N})$ is uncountable. Observe that $\wp(\mathbb{N})$ and $2^{\mathbb{N}}$ are equipotent, and so $|\wp(\mathbb{N})| = |2^{\mathbb{N}}|$. The cardinal number $|2^{\mathbb{N}}|$ is denoted by \aleph_1 . The cardinal number $|2^{\aleph_1}|$ is denoted by \aleph_2 , and so on. If \aleph is an cardinal number, then the cardinal number $|2^{\aleph}|$ is denoted by 2^{\aleph} . If A is equipotent to B , and C is equipotent to D , then A^C is equipotent to B^D . Thus, we can, unambiguously, define the power a^b as follows: Suppose that $a = |A|$ and $b = |B|$. Define $a^b = |A^B|$. In turn, for each cardinal number \aleph , we have the cardinal number 2^{\aleph} , and we have a chain of infinite cardinal numbers $\aleph_0, \aleph_1, \aleph_2, \dots, \aleph_\alpha, \aleph_{\alpha+1}, \dots$, where $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$ of infinite cardinal numbers, where α runs over a chain of ordinal numbers.

Continuum hypothesis. The continuum hypothesis (CH) asserts that there is no cardinal number in between $\aleph_0 = |\mathbb{N}|$ and $\aleph_1 = |2^{\mathbb{N}}|$. More precisely, it asserts that if there is a set A such that there is an injective map from \mathbb{N} to A , and there is an injective map from A to $2^{\mathbb{N}}$, then A is equipotent to \mathbb{N} or it is equipotent to $2^{\mathbb{N}}$.

K. Gödel in 1939 proved that if the *ZF* axiomatic system is consistent, then adjunction of *CH* in *ZF* does not lead to any contradiction. In other words, *CH* is consistent with the *ZF* axiomatic system. Further, in 1963, *P. Cohen* proved that *ZF* axiomatic system does not lead to a proof of *CH*. Consequently, *CH* is independent of the *ZF* axiomatic system.

Generalized continuum hypothesis. The generalized continuum hypothesis (GCH) asserts that for each ordinal α , there is no cardinal number between \aleph_α and $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$. The topologist *Sierpinski* proved that GCH implies axiom of choice. *K. Gödel* also showed that GCH is consistent with the *ZF* axiomatic system.

Arithmetic of Cardinal Numbers

Let (A, C) and (B, D) be pairs of equipotent sets. Suppose that $A \cap B = \emptyset = C \cap D$. It is evident that $A \cup C$ is equipotent to $B \cup D$. Thus, we have the addition $+$ on a suitable set Ω of cardinal numbers defined by $a + b = |(A \times \{0\}) \cup (B \times \{1\})|$, where $a = |A|$ and $b = |B|$. The following properties of $+$ can be verified easily.

- (i) $a + 0 = a = 0 + a$,
- (ii) $(a + b) + c = a + (b + c)$,
- (iii) $a + b = b + a$, and
- (iii) $a \leq b$ and $c \leq d$ implies that $a + c \leq b + d$
for all $a, b, c, d \in \Omega$.

We can also define sum of an arbitrary family of cardinal numbers as follows: Let $\{a_\alpha = |A_\alpha| \mid \alpha \in \Lambda\}$ be a family of cardinal numbers. We define

$$\Sigma_{\alpha \in \Lambda} a_\alpha = \left| \bigcup_{\alpha \in \Lambda} A_\alpha \times \{\alpha\} \right|.$$

Recall that a set X is said to be a finite set if every injective map from X to itself is a surjective map. It is easily observed that a set X is finite if and only if $|X|$ is a natural number.

Proposition 2.7.5 *A set X is infinite if and only if there is an injective map from the set \mathbb{N} of natural numbers to X .*

To prove this result, we need the following recursion theorem whose proof can be found in the next chapter.

Recursion Theorem. Let X be a set and $a \in X$. Let f be a map from X to X . Then, there is a unique map g from \mathbb{N} to X such that $g(1) = a$ and $g(n^+) = f(g(n))$ for all $n \in \mathbb{N}$.

Proof of the proposition 2.7.5: Let X be an infinite set. Let f be an injective map from X to X which is not surjective. Let $a \in X$ which is not in the image of f . By the recursion theorem, there is a unique map g from \mathbb{N} to X with $g(1) = a$ and is such that $g(n^+) = f(g(n))$. Let

$$M = \{m \in \mathbb{N} \mid g(m) = g(n) \text{ implies that } m = n\}.$$

Since a is not in the image of f , $1 \in M$. Suppose that $m \in M$. Then, $g(m) = g(n)$ implies that $m = n$. Suppose that $g(m^+) = g(n)$. Then, $n \neq 1$. Hence, there is an element $r \in \mathbb{N}$ such that $n = r^+$. By the definition of g , $f(g(m)) = f(g(r))$. Since f is injective, $g(m) = g(r)$. This means that $m = r$, and so $m^+ = n$. It follows that $m^+ \in M$. By P_5 , $M = \mathbb{N}$. This shows that g is injective. \sharp

Proposition 2.7.6 $\aleph_0 + \aleph_0 = \aleph_0$.

Proof It is sufficient to give a bijective map from $\mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\}$ to \mathbb{N} . Let X denote the set $\{2n \mid n \in \mathbb{N}\}$ of even natural numbers and Y denote the set $\{2n + 1 \mid n \in \mathbb{N}\}$ of odd natural numbers. Then, X and Y are disjoint. Further, $n \rightsquigarrow 2n$ is a bijective map from \mathbb{N} to X , and $n \rightsquigarrow 2n + 1$ is a bijective map from \mathbb{N} to Y . This shows that $\mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\}$ is equipotent to \mathbb{N} . The result follows. \sharp

Corollary 2.7.7 *For every natural number n , $\aleph_0 + n = \aleph_0$.*

Proof $(\mathbb{N} \times \{0\} \cup n \times \{1\}) \subset (\mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\})$. From the above proposition, it follows that $(\mathbb{N} \times \{0\} \cup n \times \{1\})$ is equipotent to a subset of \mathbb{N} . Also, the map $n \rightsquigarrow (n, 0)$ is an injective map from \mathbb{N} to $(\mathbb{N} \times \{0\} \cup n \times \{1\})$. By the Schröder–Bernstein theorem, \mathbb{N} is equipotent to $(\mathbb{N} \times \{0\} \cup n \times \{1\})$. The result follows. \sharp

Proposition 2.7.8 *If a is an infinite cardinal, then $a + a = a$.*

Proof Let us suppose that $a = |A|$, where A is an infinite set. We need to show that $A \times \{0\} \cup A \times \{1\}$ is equipotent to A . Let

$$\Sigma = \{(X, f) \mid X \subseteq A, f \text{ is a bijective map from } X \text{ to } X \times \{0\} \cup X \times \{1\}\}.$$

Since A is infinite, by the Proposition 2.7.5, there is a subset X of A which is equipotent to \mathbb{N} . From the Proposition 2.7.6, X and $X \times \{0\} \cup X \times \{1\}$ are equipotent. Hence, $\Sigma \neq \emptyset$. Define a partial order \leq on Σ by putting $(X, f) \leq (Y, g)$ if $X \subseteq Y$ and $g|_X = f$. Clearly, (Σ, \leq) is a nonempty partially ordered set. Let $\{(X_\alpha, f_\alpha) \mid \alpha \in \Lambda\}$ be a chain in (Σ, \leq) . Let $X = \bigcup_{\alpha \in \Lambda} X_\alpha$ and f be the map whose restriction to each X_α is f_α . It is an easy observation that f is a bijective map from X to $X \times \{0\} \cup X \times \{1\}$. This shows that (X, f) is an upper bound of the chain. By the Zorn's lemma, (Σ, \leq) has a maximal element (X_0, f_0) (say). Now, we show that $A - X_0$ is a finite set. Suppose not. Again, by the Proposition 2.7.5, there is a subset Z of $A - X_0$ which is equipotent to \mathbb{N} . But, then there is a bijective map h from Z to $Z \times \{0\} \cup Z \times \{1\}$. Take $U = X_0 \cup Z$, and the map ϕ from U to $U \times \{0\} \cup U \times \{1\}$ whose restriction to X_0 is f_0 , and whose restriction to Z is h . Clearly, $(U, \phi) \in \Sigma$. This is a contradiction to the maximality of (X_0, f_0) . Thus, $A - X_0$ is finite. From the Corollary 2.7.7,

$$a = |A| = |X_0| = |X_0 \times \{0\} \cup X_0 \times \{1\}| = |X_0| + |X_0| = a + a.$$

\sharp

Now, we define the product \cdot of two cardinal numbers as follows: First observe that $|A| = |C|$ and $|B| = |D|$ imply that $|A \times B| = |C \times D|$. Thus, we can, unambiguously, define the product $a \cdot b$ of two cardinal numbers $a = |A|$ and $b = |B|$ by $a \cdot b = |A \times B|$. The following properties of the multiplication \cdot can be easily observed:

- (i) $a \cdot 0 = 0 = 0 \cdot a$,
- (ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- (iii) $a \cdot b = b \cdot a$, and
- (iv) $a \cdot (b + c) = a \cdot b + a \cdot c$
for all ordinal numbers a, b , and c .

The proof of the following proposition uses Zorn's lemma, and it is similar to the proof of the Proposition 2.7.8.

Proposition 2.7.9 *If a is an infinite cardinal number, then $a \cdot a = a$.* ‡

As a corollary, we obtain the following:

Proposition 2.7.10 *If $a \leq b$, then $a \cdot b = b$.* ‡

Gödel–Bernays Axiomatic system

In 1920, John von Neumann attempted an other axiomatic system for set theory. His axiomatic system significantly differed from the ZF axiomatic system. Indeed, for him, the primitive term (concept) was that of a correspondence (a map) instead of a set. Later, Gödel and Bernays modified it to make it more appealing and near to ZF system. For them, the primitive term is class instead of set. A member of a class in this axiomatic system is a set. Most of the axioms of the Gödel–Bernays system is same as those of ZF axiomatic system with set replaced by class except the axiom of replacement. Further, in this axiomatic system, a set may be a class, but then it does contain all sets or all ordinal numbers. Sets are those classes which are adequate to develop mathematics. The Gödel–Bernays axiomatic system is most suitable for the categorical discussions.

Algebra 1

Groups, Rings, Fields and Arithmetic

Lal, R.

2017, XVII, 433 p., Hardcover

ISBN: 978-981-10-4252-2