Appendix-111
Resolution No. 38 {38-1 [38-1-13(6)]}

Department of Distance and Continuing Education
University of Delhi

B.A.(Prog) Mathematics
Semester-I
Course Credit - 4
Discipline Specific Course (DSC-1)

ELEMENTS OF DISCRETE MATHEMATICS

As per the UGCF - 2022 and National Education Policy 2020

Content Writers

Dr. Deepti Jain

Dr. Ankit Gupta

Mr. Sanyam Gupta

Academic Coordinator

Deekshant Awasthi

Ist edition: 2022

E-mail: ddceprinting@col.du.ac.in
maths@col.du.ac.in

Published by:

Department of Distance and Continuing Education under the aegis of Campus of Open Learning, University of Delhi

Printed by:
5, Cavalry Lane, School of Open Learning, University of Delhi, Delhi-110007

Contents

Lesson - 1

Discrete Mathematics

Structure

1.1 Introduction

We have studied some concept of sets in earlier classes or standard. In this section we will introduce the basis concept of set and some concepts related to the set like subset, power set and so on. We will deal with the Venn diagram also which describe the concepts of set in more attractive way. We will introduce the statement or proposition with some logical operations. This section also discussed about the conditional statements and after that we will describe mathematical technique to proof the result that is called Mathematical Induction.

The concept of set serves as a fundamental part of the present day mathematics. Today this concept is being used in almost every branch of mathematics. Sets are used to define the concepts of relations and functions. The study of geometry, sequences, probability, etc. requires the knowledge of sets. In everyday life, we often speak of collections of objects of a particular kind, such as, a pack of cards, a crowd of people, a cricket team, etc. In mathematics also, we come across collections, for example, of natural numbers, points, prime numbers, etc. A set is a well-defined collection of objects.

1.2 Learning Objectives

After reading this lesson, the reader should be able to :

- define sets and its basic type
- understand the concept of power set and Venn diagram
- understand propositions and logical operations.
- learn about conditional statements.
- learn about a Mathematical technique of proof of results.

1.3 Sets

Definition 1.1. A well-defined collection of distinct objects is said to be set. These objects is called elements or members of the set.

Remark 1. Usually we denote the set using capital letters like A,B,C,D and so on.

2. All the elements of a set are written within braces.

3. We use the symbol "$\in$" when an element belongs to the set and "$\notin$" when an element does not belong to the set.

4. The elements of a set are usually denoted by small letters a,b,c,x,y, etc.

Example 1.1. Let $A = \{1, 2, 3, 4\}$ is a set then $1 \in A, 2 \in A, 3 \in A, 4 \in A$ ("$\in$" reads as "belongs to") whereas $5 \notin A, 7 \notin A$ ("$\notin$" reads as "does not belongs to").

$1, 2, 3, 4$ are the only elements of set A.

There are two method for representing a set:

(i) Roster or tabular form

(ii) Set-builder form

Roster or tabular form - In this form, we write a set as a list of all the elements of the set within the curly braces $\{\}$ separated by commas.

Example 1.2. (a) A $= \{2, 4, 6\}$

(b) B $= \{1, 2, 3, 6, 7, 14, 21, 42\}$

In part (a), A is set of all positive even numbers less than 7 and in part (b), B is the set of all natural number which divides 42.

Set-builder form - In this form, we write a set as all the elements of the set satisfying a common property. All other elements outside the set does not satisfy that property.

In example 1.2 (a), A $= \{2, 4, 6\}$ which has the common property that all the elements of A are even number less than 7, therefore we can write the set A in set-builder form,
A $= \{x \mid x$ is even number less than 7$\}$

In example 1.2 (b), B $= \{1, 2, 3, 6, 7, 14, 21, 42\}$ has set-builder form,
B $= \{x \mid x$ is odd number which divides 42$\}$

Example 1.3. (a) A $= \{a, e, i, o, u\}$ has set-builder form,
A $= \{x \mid x$ is a vowel in English alphabet$\}$

(b) A $= \{x \mid x$ is an odd number$\}$ has roster form,
A $= \{1, 3, 5, 7, \ldots, \}$

(c) The set consist of all letters with the word "hello" can be denoted by {h,e,l,o} or in set-builder form $\{x \mid x$ is a letter in the word "hello"$\}$

Example 1.4. (a) $\mathbb{N}$: The set of all natural numbers
Roster form, $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$
Set-builder form, $\mathbb{N} = \{x \mid x$ is a natural number$\}$

(b) $\mathbb{Z}$: the set of all integers
Roster form, $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
Set-builder form, $\mathbb{Z} = \{x \mid x$ is an integer$\}$

(c) $\mathbb{Z}^+$: the set of all positive integers

Roster form, $\mathbb{Z} = \{1, 2, 3, \ldots\}$
Set-builder form, $\mathbb{Z} = \{x \mid x \text{ is positive integer}\}$

(d) $\mathbb{Q}$: set of rational numbers
Set-builder form, $\mathbb{Q} = \{x \mid x \text{ is rational number}\}$
or $\mathbb{Q} = \{x \mid x = \frac{p}{q} \quad p, q \in \mathbb{Z},\ q \neq 0\}$
There is no roster form of set of rational numbers.

Example 1.5. Write a set of the solution of equation $x^2 + x - 6 = 0$ in roster form.

Solution.

$$x^2 + x - 6 = 0$$
$$\Rightarrow (x-2)(x+3) = 0$$
$$\Rightarrow x = 2, -3$$

set is {2,-3}

Example 1.6. Write the set A $= \{4, 9, 16, \ldots\}$ in set builder form.

Solution. A $= \{2^2, 3^2, 4^2, \ldots\}$
$A = \{x \mid x$ is a square of natural number except 1
or A $= \{x \mid x = (n+1)^2, \text{where } n \in \mathbb{N}\}$

Example 1.7. Write the set A $= \{\frac{2}{1}, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}\}$ in set-builder form.

Solution. A $= \{x \mid x = \frac{n}{n-1}, \text{where } n \in \mathbb{N} \text{ and } 2 \leq n \leq 5\}$

Example 1.8. Write the set A $= \{x : x \text{ is positive integer and } x^2 \leq 20\}$ in roster form.

Solution. A $= \{1, 2, 3, 4\}$

1.3.1 The Empty Set

Definition 1.2. A set which does not have any element is said to be an empty set. We can call this set as null set or void set.

This set is denoted by ϕ or $\{\}$.

Example 1.9. (a) A $= \{x \mid x \text{ is real number and } x^2 - 1 = 0\}$
then $A = \{\}$ or $A = \phi$.

(b) A $= \{x \mid x \in \mathbb{N} \text{ and } 1 < x < 2\}$
then $A = \{\}$ or $A = \phi$.

(c) A $= \{x \mid x^2 = 4, x \text{ is odd}\}$
then $A = \{\}$ or $A = \phi$.

(d) A $= \{x \mid x \text{ is a student studying in both X and XI class}\}$
then $A = \{\}$ or $A = \phi$.

1.3.2 Equal set

Definition 1.3. Two sets A and B are said to be equal if they have exactly the same elements. we write it as $A = B$.

Remark. If two set A and B are not equal then we write it as A $\neq$ B.

Example 1.10. (a) A = $\{1, 2, 3, 4\}$ and B = $\{3, 4, 1, 2\}$ then A=B.

(b) A = $\{1, 2, 3, 4\}$ and B = $\{x \mid x$ is positive integer and $x^2 \leq 12\}$

then $A = B$ as $B = \{1, 2, 3, 4\}$.

(c) A =$\{0\}$ and B = $\{x \mid x - 5 = 0\} = \{5\}$
then $A \neq B$.

(d) A = $\{x \mid x > 15$ and $x < 5\}$ and B = $\{x \mid x^2 = 25\}$
A = $\{\}$ and B = $\{5, -5\}$ then $A \neq B$.

1.4 Subsets

Definition 1.4. Let A and B be two sets, The set A is called subset of a set B if every element of A is also an element of B. We denote it as A $\subseteq$ B.

Remark. 1. By using the symbol "$\Rightarrow$" which means "implies", we can write the definition of subset as A $\subseteq$ B if a $\in$ A $\Rightarrow$ a $\in$ B
We read this statement as A is subset of B if "a" belongs to A implies "a" belongs to B.
or A is subset of set B if "x" is an element of A implies "x" is an element of B.

2. If A is not subset of set B, we can denote it as A $\nsubseteq$ B.

3. A is a subset of itself i.e A $\subseteq$ A.

4. ϕ is subset of every set.

Example 1.11. (a) Let A = $\{1, 2, 3\}$ and B = $\{1, 2, 3, 5, 7\}$ then A $\subseteq$ B.

(b) Let A = $\{1, 2, 3\}$ and B = $\{3, 4, 5, 6\}$ then B $\nsubseteq$ A.

(c) $\mathbb{Z}^+$, the set of positive integer then $\mathbb{Z}^+ \subseteq \mathbb{Z}$

Example 1.12. Let A = $\{1, 2, 3, 4, 5, 6\}$, B = $\{2, 4, 5, 6\}$ and C = $\{1, 2, 3, 4, 5, 6\}$ then

$$\begin{gathered}\text{A} \nsubseteq \text{B and B} \subseteq \text{A}\\ \text{B} \subseteq \text{C and C} \nsubseteq \text{B}\\ \text{A} \subseteq \text{C and C} \subseteq \text{A}\end{gathered}$$

1.4.1 Power Set

Definition 1.5. For any set A, the collection of all subsets of a set A is called the power set of A. It is denoted by $P(A)$, i.e. $P(A) = \{S \mid S$ is subset of A$\}$.

Remark - In P(A) every element is a set.

Example 1.15 (a) Let A = {1,2} then P(A) = $\{\phi, \{1\}, \{2\}, \{1, 2\}\}$

(b) Let A = {1,2,3} then P(A) = $\{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\{1, 2, 3\}\}$

Remark 1. n(A) denote the number of elements in the set A.

2. If n(A) = m, then n(P(A)) = 2^m.

1.4.2 Finite and Infinite sets

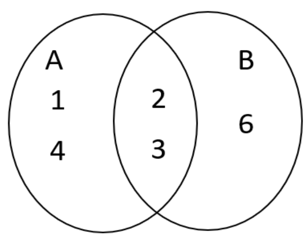
Definition 1.6. A set which is empty or which has exactly n distinct elements, where $n \in \mathbb{N}$, is called finite set. A set that is not finite is called infinite set.

In this case, n is called the cardinality of A and is denoted by $|A|$.
In example 1.15 (b), $|A| = 3$ and $|P(A)| = 8$
Note: The set of integers is infinite.

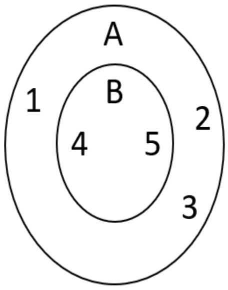
1.5 Venn Diagram

We have deal with the elements and subsets of a set. For example, when we study the system of numbers, we are interested in the set of natural numbers and its subsets such as the set of all prime numbers, the set of all even numbers, and so on. This basic set is called the "Universal Set". The universal set is usually denoted by U, and all its subsets by the letters A, B, C, X etc. Most of the relationships between sets can be represented by means of diagrams which are known as Venn diagrams. These diagrams consist of rectangles and closed curves usually circles. The universal set is represented usually by a rectangle and its subsets by circles. In Venn diagrams, the elements of the sets are written in their respective circles.

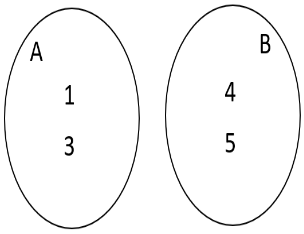
Example 1.13. Let $A = \{1, 2, 3, 4\}$ and $B = \{2, 3, 6\}$ then
Venn diagram



Example 1.14. Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{4, 5\}$ then
Venn diagram



Example 1.15. Let $A = \{1, 3\}$ and $B = \{4, 5\}$
then Venn diagram



In-text Exercise 1.1. In-text Exercise 1.1

1. Let $A = \{1, 2, 4, a, b, c\}$. Identify each of the following as true or false.
   (a) $2 \in A$
   (b) $3 \in A$
   (c) $c \notin A$
   (d) $\varnothing \in A$
   (e) $\{\} \notin A$
   (f) $A \in A$
2. In each part, give the set of letters in each word by listing the elements of the set.
   (a) AARDVARK
   (b) BOOK
   (c) MISSISSIPPI
3. Let $A = \{1, \{2, 3\}, 4\}$. Identify each of the following as true or false.
   (a) $3 \in A$
   (b) $\{1, 4\} \subseteq A$

(c) $\{2,3\} \subseteq A$
(d) $\{2,3\} \in A$
(e) $\{4\} \in A$
(f) $\{1,2,3\} \subseteq A$

In Exercise 4 and 5, write the set in the form $\{x \mid P(x)\}$, where $P(x)$ is a property that describes the elements of the set.

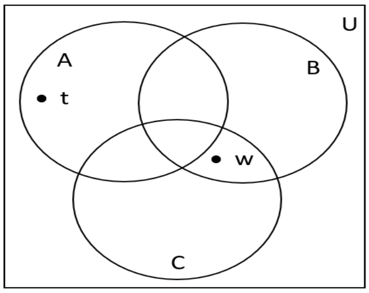
4. $\{a, e, i, o, u\}$
5. $\{-2, -1, 0, 1, 2\}$
6. Which of the following sets are the empty set?
   (a) $\{x \mid x$ is a real number and $x^2 - 1 = 0\}$
   (b) $\{x \mid x$ is a real number and $x^2 + 1 = 0\}$
   (c) $\{x \mid x$ is a real number and $x^2 = -9\}$
   (d) $\{x \mid x$ is a real number and $x = 2x + 1\}$
   (e) $\{x \mid x$ is a real number and $x = x + 1\}$
7. List all the subsets of {JAVA, PASCAL, C++}.
8. Let $A = \{1, 2, 5, 8, 11\}$. Identify each of the following as true or false.
   (a) $\{5,1\} \subseteq A$
   (b) $\{8,1\} \in A$
   (c) $\{1,8,2,11,5\} \nsubseteq A$
   (d) $\varnothing \subseteq A$
   (e) $\{1,6\} \nsubseteq A$
   (f) $\{2\} \subseteq A$
   (g) $\{3\} \notin A$
   (h) $A \subseteq \{11, 2, 5, 1, 8, 4\}$
9. Let $A = \{1\}, B = \{1, a, 2, b, c\}, C = \{b, c\}, D = \{a, b\}$, and $E = \{1, a, 2, b, c, d\}$. For each part, replace the symbol $\square$ with either $\subseteq$ or $\nsubseteq$ to give a true statement.
   (a) $A \square B$
   (b) $\varnothing \square A$
   (c) $B \square C$
   (d) $C \square E$
   (e) $D \square C$
   (f) $B \square E$

In Exercise 10, find the set of smallest cardinality that contains the given sets as subsets.

10. $\{1,2\},\{1,3\},\varnothing$

11. Is it possible to have two different (appropriate) universal sets for a collection of sets? Would having different universal sets create any problems? Explain.

12. Use the Venn diagram to identify each of the following as true or false.



    (a) $B \subseteq A$
    (b) $A \subseteq C$
    (c) $C \subseteq B$
    (d) $w \in A$
    (e) $t \in A$
    (f) $w \in B$

13. Complete the following statement. A generic Venn diagram for three sets has _____ regions. Describe them in words.

14. If $P(B) = \{\{\}, \{m\}, \{n\}, \{m,n\}\}$, then find B.

15. If $P(B) = \{\{a\}, \{\}, \{c\}, \{b,c\}, \{a,b\}, \ldots\}$ and $|P(B)| = 8$, then $B =$_____

In Exercise 16, draw a Venn diagram that represents these relationships.

16. $x \in A, x \in B, x \notin C, y \in B, y \in C$, and $y \notin A$

1.6 Propositions and Logical Operations

A declarative sentence or a meaningful sentence which is either true or false but not both is called statement or proposition.

Example 1.16. The earth moves around the sun.

Solution. The declarative sentence is a statement which has true value or which is true.

Example 1.17. $2 + 3 = 6$

Solution. The declarative sentence is a statement which has false value or which is false.

Example 1.18. Do you go to college?

Solution. It is a question, so this is not a statement.

Example 1.19. Is $5 + x = 10$ statement?

Solution. It is a declarative sentence but not a statement as the value of this statement depends on x.

1.6.1 Logical Connectives and Compound Statements

We generally use the letter $x, y, z, \dots$ as the prepositional variables and these variable may be replaced by any real number. Also the mathematical operations are used to combine two or more variables. In similar way, the letters $p, q, r, \dots$ denote propositional variable i.e these variable may be replaced by any statement or proposition. When we combine two or more statement by some logical connectives, then we get a compound statement.

Example 1.20.

$$
\begin{aligned}
p &: \text{The Sun is not shining today.} \\
q &: \text{Its raining.} \\
p \text{ and } q &: \text{The sun is not shining today and its raining.}
\end{aligned}
$$

Hence we combine the statement p, q by the connector "and" and get the compound statement p and q. The true or false value of any compound statement depends on the true or false value of statements and on the type of connectives to be used. Now we will discuss some important connectives.

Negation - If p is any statement, then negation of p is a statement "not p" and denoted by "$\sim p$".

Remark. 1. If p is true, then $\sim$ p is false.
2. If p is false, then $\sim p$ is true.

Truth Table - A table which shows the truth values of a compound statement in terms of its component parts, is said to be a truth table.
The truth table table of negation of statement p is given as follows:

p	$\sim p$
T	F
F	T

Example 1.21. $p : 2 + 3 > 1$, is an statement. Give the negation of this statement.

Solution. $\sim p : 2 + 3 \leq 1$
Since p is true and therefore $\sim p$ is false.

1.6.2 Conjunction

If p and q are two prepositions, then conjunction of p and q is a compound statement "p and q" denoted by $p \wedge q$. The connective "and" is denoted by symbol $\wedge$.
Truth table of conjunction is given as follows:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Example 1.22. Form the conjunction of p and q where $p : 3 < 4$ and $q : -5 > -9$

Solution. $p \wedge q : 3 < 4 \text{ and } -5 > -9$
since the statement p is true and q is also true. Therefore the value of $p \wedge q$ is also true.

Example 1.23. Form the conjunction of p and q where p : 5 is positive integer and $q : \sqrt{2}$ is rational number.

Solution. $p \wedge q$: 5 is positive integer and $\sqrt{2}$ is rational number.
since p is true and q is false. Therefore the value of $p \wedge q$ is false.

Example 1.24. Find the truth table of $(p \wedge q) \wedge \sim p$.

p	q	$p \wedge q$	$\sim p$	$(p \wedge q) \wedge \sim p$
T	T	T	F	F
F	T	F	T	F
T	F	F	F	F
F	F	F	T	F

1.6.3 Disjunction

If p and q are two prepositions, then disjunction of p and q is compound prepositions "p *or* q" denoted by $p \vee q$. The connective "or" is denoted by symbol $\vee$. Truth table of disjunction is given as follows:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Example 1.25. Form the disjunction of p and q where $p : 2 + 5 \neq 8$ and q : Delhi is Capital of India.

Solution. $p \vee q : 2 + 5 \neq 8$ or Delhi is Capital of India.
since p is true and q is true.
Therefore the disjunction $p \vee q$ is true.

Example 1.26. Find the truth table of $(p \vee q) \wedge \sim p$.

p	q	$p \vee q$	$\sim p$	$(p \vee q) \wedge \sim p$
T	T	T	F	F
T	F	T	F	F
F	T	T	T	T
F	F	F	T	F

1.6.4 Quantifiers

We have to learned how to write a set in set-builder form. In this form we specified the property of all elements of a set and write the property in a statement. If this statement is true then that element lies in that set. Here we will denote this statement by $P(x)$ and its called predicate. Each choice of x gives the proposition $p(x)$ that is either true or false. There are two common constructions first "if $P(x)$, then execute the particular step" and second is "while $Q(x)$, do specific action " These two predicates $P(x)$ and $Q(x)$ are called the guard for the block of programming code in computers.

Example 1.27. Let $A = \{x \mid x$ is an integer less than $5\}$. Here A is a set-builder form, $P(x)$ is the statement "x is an integer less than 5". $P(1)$ is "1 is an integer less than 1", which is true. Therefore $1 \in A$. Similarly we can check that $P(2), P(3), P(4)$ are only true statements. Hence $A = \{1, 2, 3, 4\}$

Now we will see that there is a universal quantification of a predicate $P(x)$ which is a statement "For all value of x,$P(x)$ is true". This universal quantification of P(x) is denoted by $\forall\ x\ P(x)$. The symbol "$\forall$" is called universal quantifiers.

Example 1.28. Let $Q(x) : x+10 < 15$. Then for all x $Q(x)$ is false statement as $Q(12)$ is not true.

In-text Exercise 1.2. 1. Which of the following are statement?

(a) Is 2 a positive number ?

(b) $x^2 + x + 1 = 0$

(c) Study logic.

(d) There will be snow in January.

(e) If stock prices fall, then I will lose money.

2. Give the negation of each of the following statements.

   (a) It will rain tomorrow or it will snow tomorrow.

   (b) If you drive, then I will walk.

3. In each of the following, form the conjunction and the disjunction of p and q.

   (a) p : I will drive my car.
   q : I will be late.

   (b) p : NUM > 10
   q : NUM ≤ 15

4. Determine the truth or falsity of each of the following statements.

   (a) $2 < 3$ or 3 is a positive integer.

   (b) $2 \geq 3$ or 3 is a positive integer.

   (c) $2 < 3$ or 3 is not a positive integer.

   (d) $2 \geq 3$ or 3 is not a positive integer.

5. find the truth value of each proposition if p and r are true and q is false.

   (a) $\sim p \ \wedge (q \vee r)$

   (b) $p \ \wedge (\sim (q \vee \sim r))$

   (c) $(r \wedge \sim q) \vee (p \vee r)$

   (d) $(q \ \wedge r) \wedge (p \vee \sim r)$

1.6.5 Conditional Statements / Implication

If we consider two prepositions p and q then the compound statement "if p then q", is called conditional statement or implication. We will denote this compound statement by "$p \Rightarrow q$". The first statement p is called the antecedent or hypothesis and the second statement q is called consequent or conclusion.

Example 1.29. Let

$$p : \text{Weather is bad.}$$
$$q : \text{Its raining}$$

Form the implication $p \Rightarrow q$

Solution. $p \Rightarrow q$
If weather is bad, then its raining.

The compound statement "if p then q " has either true or false value, depends upon the true or false value of p and q statement. Truth table of $p \Rightarrow q$ is as follows:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

If $p \Rightarrow q$ is an implication, then the converse of $p \Rightarrow q$ is $q \Rightarrow p$ and the contrapositive of $p \Rightarrow q$ is $\sim q \Rightarrow \sim p$.

Example 1.30. Find the contrapositive and converse of the compound statement "If it is raining, then I will not go market".

Solution. Let p : It is raining
q : I will not go market

statement p implies q
Converse - $q \Rightarrow p$
i.e If I will not go market, then it is raining.

Contrapositive - $\sim q \Rightarrow \sim p$
If I will go market, then it is not raining.

1.6.6 Biconditional / Biimplication

Let p and q are prepositions then the compound statement "p if and only if q" is called an equivalence or biconditional. It is denoted by $p \Leftrightarrow q$. This has true or false value, depends on the true or false value of p and q. Truth table of $p \Leftrightarrow q$ is as follows:

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Example 1.31. Let $5 > 3$ if and only if $0 < 5 - 3$. Then this equivalence is true or false ?

Solution. Let

$$p : 5 > 3$$
$$q : 0 < 5 - 3$$

Since p is true, q is also true,
therefore $p \Leftrightarrow q$ is true.

Example 1.32. Find the truth table of $(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$

p	q	$p \Rightarrow q$	$\sim q$	$\sim p$	$\sim q \Rightarrow \sim p$	$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$
T	T	T	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

A compound preposition that is always true is called tautology. A compound prepositions that is always false is said to be contradiction or an absurdity, and a statement that may be either true or false, depending on the true or false value of its propositional variables, is said to be contingency.

Example 1.33. In example 1.35 the equivalence $p \Rightarrow q \Leftrightarrow (\sim q \Rightarrow \sim p)$ has true value always. Therefore it is tautology.

Example 1.34. The statement $p \wedge \sim p$ has truth table.

p	$\sim p$	$p \wedge \sim p$
T	F	F
T	F	F
F	T	F
F	T	F

Since it has always false values, therefore $p \wedge \sim p$ is contradiction.

Example 1.35. The statement $(p \Rightarrow q) \wedge (p \vee q)$ has truth table.

p	q	$p \Rightarrow q$	$p \vee q$	$(p \Rightarrow q) \wedge (p \vee q)$
T	T	T	T	T
T	F	F	T	F
F	T	T	T	T
F	F	T	F	F

Since the value of given statement depends on the value of $p \Rightarrow q$ and $p \vee q$. Therefore this is contingency.

Theorem 1.1. The operations for propositions have the following basic logical equivalence properties.

Commutative Properties

1. $p \vee q \equiv q \vee p$
2. $p \wedge q \equiv q \wedge p$

Associative Properties

3. $p \vee (q \vee r) \equiv (p \vee q) \vee r$
4. $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

Distributive Properties

5. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

6. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

Idempotent Properties

7. $p \vee p \equiv p$
8. $p \wedge p \equiv p$

Properties of Negation

9. $\sim (\sim p) \equiv p$
10. $\sim (p \vee q) \equiv (\sim p) \wedge (\sim q)$
11. $\sim (p \wedge q) \equiv (\sim p) \vee (\sim q)$

Theorem 1.2. (a) $(p \Rightarrow q) \equiv ((\sim p) \vee q)$
(b) $(p \Rightarrow q) \equiv (\sim q \Rightarrow \sim p)$
(c) $(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge ((q \Rightarrow p))$
(d) $\sim (p \Rightarrow q) \equiv (p \wedge \sim q)$
(e) $\sim (p \Leftrightarrow q) \equiv ((p \wedge \sim q) \vee (p \wedge \sim q))$

Theorem 1.3. Each of the following is a tautology.
(a) $(p \wedge q) \Rightarrow p$
(b) $(p \wedge q) \Rightarrow q$
(c) $p \Rightarrow (p \vee q)$
(d) $q \Rightarrow (p \vee q)$
(e) $\sim p \Rightarrow (p \Rightarrow q)$
(f) $\sim (p \Rightarrow q) \Rightarrow p$
(g) $(p \wedge (p \Rightarrow q)) \Rightarrow q$
(h) $(\sim p \wedge (p \vee q)) \Rightarrow q$
(i) $(\sim q \wedge (p \Rightarrow q)) \Rightarrow \sim p$
(j) $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$

The results of theorem 2 and theorem 3 can be proved using truth table.

In-text Exercise 1.3. 1. Write each of the following statements in terms of p, q, r, and logical connectives where p : I am awake; q : I work hard; r : I dream of home.

(a) I am awake implies that I work hard.
(b) I dream of home only if I am awake.
(c) Working hard is sufficient for me to be awake.
(d) Being awake is necessary for me not to dream of home.

2. State the converse of each of the following implications.

(a) If $2 + 2 = 4$, then I am not the Queen of England.
(b) If I am not President of the united states, then I will walk to work.
(c) If I am late, then I did not take the train to work.
(d) If I have time and I am not too tired, then I will go to the store.
(e) If I have enough money, then I will buy a car and I will buy a house.

3. Determine the truth value for each of the following statements.

   (a) If 2 is even, then New York has a large population.

   (b) If 2 is even, then New York has a small population.

   (c) If 2 is odd, then New York has a large population.

   (d) If 2 is odd, then New York has a small population.

4. Let $p, q,$ and r be the following statements: p : I will study discrete structure; q : I will go to a movie; r : I am in a good mood. Write English sentences corresponding to the following statements.

   (a) $((\sim p) \wedge q) \Rightarrow r$

   (b) $r \Rightarrow (p \vee q)$

   (c) $(\sim r) \Rightarrow ((\sim q) \vee p)$

   (d) $(q \wedge (\sim p)) \Leftrightarrow r$

5. Let p, q, r and s be the following statements: $p : 4 > 1$; $q : 4 < 5$; $r : 3 \leq 3$; $s : 2 > 2$. Write English sentences corresponding to the following statements.

   (a) $(p \wedge s) \Rightarrow q$

   (b) $\sim$

   (c) $(\sim r) \Rightarrow p$

6. Construct truth tables to determine whether the given statement is a tautology, a contingency or absurdity.

   (a) $p \Rightarrow (q \Rightarrow p)$

   (b) $q \Rightarrow (q \Rightarrow p)$

7. If $p \Rightarrow q$ is false, can you determine the truth value of $(\sim (p \wedge q)) \Rightarrow q$? Explain your answer.

1.7 Mathematical Induction

We use generally some techniques to proof the results and statements in mathematics. Mathematical Induction also one of the technique to proof the results. If we want to proof some result or statement or any other formula working for all natural numbers then we can use this technique, In this technique, first we will prove that the given result is true for $n = 1$ and then assume that the result is true for any $k \in \mathbb{N}$. Now we will show that the given result is also true for $k + 1$. Therefore this technique says that the result is true for all $n \in \mathbb{N}$. These steps is called induction step. Hence this technique is called Mathematical Induction.

Example 1.36. Show that the following result is true for all $n \geq 1$, by mathematical induction
$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$

Solution. for $n = 1$, $\frac{n(n+1)}{2} = \frac{1(1+1)}{2} = \frac{2}{2} = 1$
which is clearly true.
Let result is true for $n = k$

$$\text{i.e} \quad 1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2} \tag{1.1}$$

Now we will show that result is true for $n = k + 1$

$$\begin{aligned} 1 + 2 + 3 + \ldots + k + k + 1 &= (1 + 2 + \ldots + k) + k + 1 \\ &= \frac{k(k+1)}{2} + k + 1 \quad \text{(using 1.1)} \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \\ &= \frac{(k+1)((k+1)+1)}{2} \end{aligned}$$

Thus we have proved that the result is true for $n = k + 1$
Hence by Principle of Mathematical Induction, the result is true for all $n \geq 1$.

Example 1.37. Let $A_1, A_2, A_3 \ldots A_n$ be any n-sets. Show the following result using mathematical induction.

$$\overline{(\bigcup_{i=1}^{n} A_i)} = \bigcap_{i=1}^{n} \overline{A_i}$$

(where $\overline{A}$ denote the complement of set A)

Solution. for $n = 1$, $\overline{A_1} = \overline{A_1}$ which is clearly true.
Let result is true for $n = k$

$$\overline{(\bigcup_{i=1}^{k} A_i)} = \bigcap_{i=1}^{k} \overline{A_i} \tag{1.2}$$

Now we will show that the result is true for $n = k + 1$

$$
\begin{aligned}
\overline{(\bigcup_{i=1}^{k+1} A_i)} &= \overline{A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_{k+1}} \\
&= \overline{A_1 \cup A_2 \cup \ldots \cup A_k \cup A_{k+1}} \\
&= \overline{(A_1 \cup A_2 \cup \ldots \cup A_k) \cup A_{k+1}} \\
&= \overline{(A_1 \cup A_2 \cup \ldots \cup A_k)} \cap \overline{A_{k+1}} \\
&= (\bigcap_{i=1}^{k} \overline{A_i}) \cap \overline{A_{k+1}} \quad \text{(using 1.2)} \\
&= (\bigcap_{i=1}^{k+1} \overline{A_i})
\end{aligned}
$$

Thus we have proved that the result is true for $n = k + 1$.
Hence by Principle of Mathematical Induction, the result is true for all $n \geq 1$.

In-text Exercise 1.4. In Exercise 1 through 4, prove the statement is true by using mathematical induction.

1. $2 + 4 + 6 + \ldots + 2n = n(n + 1)$
2. $1 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$
3. $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$
4. $a + ar + ar^2 + \ldots + ar^{n-1} = \frac{a(1-r^n)}{1-r}$ for $r \neq 1$

1.8 Summary

- A well defined collection of objects is said to be set. These objects is called elements or members of the set.
- Methods for representing set
  - (i) Roster or tabular form
  - (ii) Set-builder form
- A set which does not have any element is called empty set.
- Two sets are said to be equal if they have exactly same elements.
- A is subset of a set B if every element of A is also belongs to B.
- The collection of all subset of a set A is called power set of A.
- A set which has n distinct elements or empty set is called finite otherwise infinite.

- A declarative sentence or a meaningful sentence which is either true or false but not both, is called statement or proposition.
- The letter $p, q, r, \ldots$ denote proposition variables.
- When two or more statements or propositions combined by logical connectives, then it is called compound statements.
- p is a statement, then negation of p is the statement not p, denoted by $\sim p$.
- A table which shows the truth values of a compound statement in terms of its component parts, is said to be a truth table.
- If p and q are two statements, then conjunction of p and q is the compound statement "p and q" denoted by $p \wedge q$.
- If p and q are two statements, disjunction of p and q is the compound statement "p or q" denoted by $p \vee q$.
- $P(x)$ is called predicate of a set in set-builder form.
- If p and q are two statements then "if p then q " is called conditional statement.
- If $p \Rightarrow q$ then $q \Rightarrow p$ is converse $\sim q \Rightarrow \sim p$ is contrapositive.
- A statement that is always true is tautology.
- A statement that is always false is contradiction.
- A statement that may be either true or false is called contingency.
- Mathematical Induction - We will check the result for $n = 1$, assume it is true for $n = k$ and will show for $n = k + 1$.

1.9 Self-Assessment Exercise

1.10 Solutions to the In-text Exercises

Solutions to the In-text exercise 1.1

1. (a) True
   (b) False
   (c) False
   (d) False
   (e) True
   (f) False

2. (a) $\{\text{A}, \text{R}, \text{D}, \text{V}, \text{K}\}$
   (b) $\{\text{B}, \text{O}, \text{K}\}$
   (c) $\{\text{M}, \text{I}, \text{S}, \text{P}\}$
3. (a) False
   (b) True
   (c) False
   (d) True
   (e) False
   (f) False
4. $\{x \mid x \text{ is a vowel }\}$
5. $\{x \mid x \in Z \text{ and } x^2 < 5\}$
6. (b), (c), (e)
7. $\{\}, \{$JAVA$\}, \{$PASCAL$\}, \{C{+}{+}\}$, {JAVA, PASCAL}, {JAVA, C++}, {PASCAL, C++}, {JAVA, PASCAL, C++}.
8. (a) True
   (b) False
   (c) False
   (d) True
   (e) True
   (f) True
   (g) True
   (h) True
9. (a) $\subseteq$
   (b) $\subseteq$
   (c) $\not\subseteq$
   (d) $\subseteq$
   (e) $\not\subseteq$
   (f) $\subseteq$
10. $\{1, 2, 3\}$
11. Yes, Yes, the complement of a set would not be defined unambiguously.
12. (a) False
    (b) False

(c) Insufficient information

(d) False

(e) True

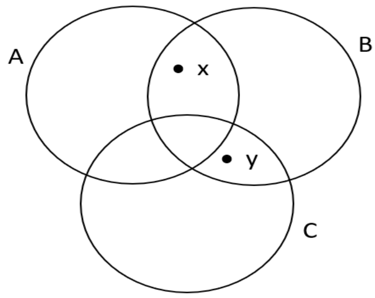
(f) True

13. Eight. There are three parts that represent what is left of each set when common parts are removed, three regions that each represent the part shared by one of the three pairs of sets, a region that represents what all three sets have in common, and a region outside all three sets.

14. $B = \{m, n\}$

15. $B = \{a, b, c\}$

16.



is one solution.

Solutions to the In-text exercise 1.2

1. (b), (d), and (e) are statements.

2. (a) It will not rain tomorrow and it will not snow tomorrow.

   (b) It is not the case that if you drive, I will walk.

3. (a) I will drive my car and I will be late.
   I will drive my car or I will be late.

   (b) $10 < \text{NUM} \leq 15$.
   $\text{NUM} > 10$ or $\text{NUM} \leq 15$.

4. (a) TRUE

   (b) TRUE

   (c) TRUE

   (d) FALSE

   (a) FALSE

   (b) TRUE

(c) TRUE

(d) FALSE

Solutions to the In-text exercise 1.3

1. (a) $p \Rightarrow q$
   (b) $r \Rightarrow p$
   (c) $q \Rightarrow p$
   (d) $\sim r \Rightarrow p$

2. (a) If I am not the Queen of England, then $2 + 2 = 4$
   (b) If I walk to work, then I am not the President of the United States.
   (c) If I did not take the train to work, then I am late.
   (d) If I go to the store, then I have time and I am not too tired.
   (e) If I buy a car and I buy a house, then I have enough money.

3. (a) True
   (b) False
   (c) True
   (d) True

4. (a) If I do not study discrete structures and I go to a movie, then I am in a good mood.
   (b) If I am in a good mood, then I will study discrete structures or I will go to a movie.
   (c) If I am not in a good mood, then I will not go to a movie or I will study discrete structures.
   (d) I will go to a movie and I will not study discrete structures.

5. (a) If $4 > 1$ and $2 > 2$, then $4 < 5$.
   (b) It is not true that $3 \leq 3$ and $4 < 5$..
   (c) If $3 > 3$, then $4 > 1$.

6. (a)

p	q	$p \quad \Rightarrow$	$(q \Rightarrow p)$
T	T	T	T
T	F	T	T
F	T	T	F
F	F	T	T
		↑	

tautology

(b)

p	q	$q \quad \Rightarrow$	$(q \Rightarrow p)$
T	T	T	T
T	F	T	T
F	T	F	F
F	F	T	T
		↑	

contingency

7. Yes. If $p \Rightarrow q$ is false then p is true and q is false. Hence $p \wedge q$ is false, $\sim (p \wedge q)$ is true, and $\sim (p \wedge q)) \Rightarrow q$ is false.

Solutions to the In-text exercise 1.4

Note: Only the outlines of the induction proofs are given. These are not complete proofs.

1. Basic step: $n = 1 \quad P(1) : 2(1) = 1(1 + 1)$ is true.
   Induction step: $P(k) : 2 + 4 + \ldots + 2k = k(k + 1)$.
   $P(k + 1) : 2 + 4 + \ldots + 2(k + 1) = (k + 1)(k + 2)$.
   LHS of $P(k+1) : 2+4+\ldots+2k+2(k+1) = k(k+1)+2(k+1) = (k+1)(k+2)$
   RHS of $P(k + 1)$.

2. Basic step: $n = 0 \quad P(0) : 2^0 = 2^{0+1} - 1$ is true.
   Induction step: LHS of $P(k+1) : 1+2^1+2^2+\ldots+2^k+2^{k+1} = (2^{k+1}-1)+2^{k+1} = 2.2^{k+1} - 1$.
   RHS of $P(k + 1)$.

3. Basic step: $n = 1 \quad P(1) : 1^2 = \frac{1(1+1)(2+1)}{6}$ is true.
   Induction step: LHS of $P(k + 1)$:
   $1^2 + 2^2 + \ldots + k^2 + (k + 1)^2$

$$
\begin{aligned}
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= (k+1)(\frac{k(2k+1)}{6} + (k+1)) \\
&= \frac{k+1}{6}(2k^2 + k + 6(k+1)) \\
&= \frac{k+1}{6}(2k^2 + 7k + 6) \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}
\end{aligned}
$$

RHS of $P(k + 1)$.

4. Basic step: $n = 1 \quad P(1) : a = \frac{a(1-r^1)}{1-r}$ is true.
   Induction step: LHS of $P(k+1) : a + ar + \ldots + ar^{k-1} + ar^k = \frac{a(1-r^k)}{1-r} + ar^k = \frac{a-ar^k+ar^k-ar^{k+1}}{1-r} = \frac{a(1-r^{k+1})}{1-r}$. RHS of $P(k+1)$.

Lesson - 2

Relations and POSETs

Structure

2.1 Learning Objectives

After going through this chapter, the reader should be able to:

- define various types of relations on a set;
- understand about the various properties of relations;
- define the equivalence relations and equivalence classes;
- define the partial order relation and partially ordered set.

2.2 Introduction

Mathematics is all about finding the patterns - a recognisable link between quantities. In day-to-day life, we come across several patterns that characterize relations such as father and son, brother and sister, teacher and student etc. In the arena of Mathematics, we come across many relations between objects/numbers such as number m is less than or equal to n, set A is a subset of B. In al these cases, one can notice that a relation always involves pairs of objects in a particular order. Relation maps elements of one set to the elements of another sets.

In this chapter, we will study about the importance of relations and their properties. We will also discuss about the equivalence class and partial order relation and their importance in the field of Algebra and Discrete Mathematics. Relations and partial order set are the building block of the discrete mathematics.

2.3 Relations and their properties

In this chapter, our main focus will be on relations only and their various types. Suppose A is the set of all subjects offered by the University of Delhi and B is the collection of all the students admitted in School of open learning, University of Delhi, then a relation R can be defined between A and B as follow. Let $x \in A$ and $y \in B$, then, we say x is related to y by the relation R if a particular subject x is chosen by the student y, and we denote this by xFy. Since, in a relation order matters, therefore, we say R as a relation from A to B. One can define more than one relation between the set A and B. Suppose, A is the set of all real numbers, then, in mathematics, unknowingly, we already studied many commonly used relations from A to A. The most common relation between A to A is "less than," which is usually denoted by $<$. We say x is related to y if $x < y$, on the other hand, $>$, $\geq$, and $\leq$ are examples of relations over A, the set of real numbers.

One of the easiest way to represent a relation between a set A to B is "to write their elements in ordered pair precisely." That is, suppose that $A = \{1, 2, 3, 4\}$ and R is a relation from A to A define as follow: Let xRy if and only if $x = y + 2$. Then, one can easily verify that the element 3 is related to 1. For, this relation, we can easily write all the pairs which are related to each others, which are $3R1$ and $4R2$. For a relation, most of the times, it would be enough to provide the foregoing list of related pairs. Therefore, we can say that the relation R is completely known if all R-related pairs are known. The above defined relation R can be written in the form of ordered pairs, $\{(3, 1), (4, 2)\}$. In each ordered pair, the first element is related to its corresponding second element. This method of specifying a relation does not require any special symbol or description and so is suitable for any relation between any two sets.

Note. From this ordered pair notation, one can easily say that a relation from the set A to B is a subset of $A \times B$.

On the other hand, any subset of $A \times B$ can be treated as a relation from A to B, even if we have no alternative description for the same. Now, we define the notion of a relation formally:

Definition 2.1. Let A and B be two nonempty sets. Then a relation R from A to B is a subset of directed set $A \times B$, that is, $R \subseteq A \times B$. Whenever the ordered pair $(a, b) \in R$, we say the element a is related to b by the relation R. Sometimes, we denote the same with aRb.

Suppose a is not related to b by R, then we write $a \not R b$. Now, we provide a number of examples to illustrate the concept of relation.

Example 2.1. Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b\}$. Then $R = \{(1, a), (2, b), (4, a)\}$ is a relation from A to B.

Example 2.2. Let $A = \{1, 2, 3, 4\}$. Then we define a relation R on A

$$aRb \quad \text{if and only if} \quad a > b$$

Then

$$R = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$$

Example 2.3. Let $A = \mathbb{R}$ be the set of all real numbers. Then, we define the relation R on A:

$$xRy \text{ if and only if } x \text{ and } y \text{ holds the equation } x^2 + y^2 = 1$$

In the above example, we have the collection of all the ordered pairs, which lie on the unit circle.

Example 2.4. Let A be the set of all the straight lines in a plane. Then, we can define the following relation R on A:

$$l_1 R l_2 \text{ if and only if } l_1 \text{ is perpendicular to } l_2$$

Next we define some notion which are used frequently in relation.

Definition 2.2. Let R be a relation from A to B. Then the domain of R, denoted by $\mathrm{Dom}(R)$, is the collection of all the elements in A, which are related to some element in B.

That is, $\mathrm{Dom}(R)$ is the collection of all the first elements in the ordered pairs in R.

Definition 2.3. Let R be a relation from A to B. Then the range of R, denoted by $\mathrm{Ran}(R)$ is the subset of B having all those elements which are paired with some element in A.

Note. All the elements of A and B, which are not in $\mathrm{Dom}(R)$ and $\mathrm{Ran}(R)$ in any way respectively, are not part of relation R.

Example 2.5. In the Example 2.2, the $\mathrm{Dom}(R) = \{2, 3, 4\}$ and $\mathrm{Ran}(R) =\{1, 2, 3\}$.

Example 2.6. In the Example 2.3, the $\text{Dom}(R) = \text{Ran}(R) = [-1, 1]$.

Definition 2.4. Let R be a relation from A to B and let $x \in A$. Then we define $R(x)$, the R-relative set of x as

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

that is, the collection of all the elements of B which are related to x.

Similarly, let $A_1 \subseteq A$, then the R-relative set of A_1, which is denoted by $R(A_1)$ is defined as

$$R(A_1) = \{y \in B | (x, y) \in R \text{ for some } x \in A_1\}.$$

From the definition, we can easily notice that $R(A_1)$ is the union of the sets $R(x)$ for $x \in A_1$.

Example 2.7. Let A be the collection of all the English alphabet and let

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

. Then, here $R(a) = \{a, b, c\}$ and $R(b) = \{s\}$. Let $A_1 = \{c, d\}$, then $R(A_1) = \{a, d, f\}$.

In the following result, we show some set theoretic relation between the R-relative sets.

Theorem 2.1. Let R be a relation from A to B and let A_1 and A_2 be two nonempty subsets of A. Then:

1. If $A_1 \subseteq A_2$, then $R(A_1) \subseteq R(A_2)$;
2. $R(A_1 \bigcup A_2) = R(A_1) \bigcup R(A_2)$;
3. $R(A_1 \bigcap A_2) \subseteq R(A_1) \bigcap R(A_2)$.

Proof. Let R be a relation from A to B and let A_1 and A_2 be two non-empty subsets of A.

1. If $y \in R(A_1)$, then there exists some $x \in A_1$ such that $(x, y) \in R$. By the given hypothesis, we have $A_1 \subseteq A_2$, thus we have $x \in A_2$. Hence, we have $y \in R(A_2)$. Therefore
$$R(A_1) \subseteq R(A_2).$$
2. Since, we have $A_1 \subseteq (A_1 \bigcup A_2)$ then by part (1), we have
$$R(A_1) \subseteq R(A_1 \bigcup A_2).$$
Similarly, $A_2 \subseteq (A_1 \bigcup A_2)$ implies that
$$R(A_2) \subseteq R(A_1 \bigcup A_2).$$

Thus, we have

$$R(A_1)\bigcup R(A_2) \subseteq R(A_1 \bigcup A_2).$$

Conversely, let $y \in R(A_1 \bigcup A_2)$, then there exists some $x \in A_1 \bigcup A_2$ such that $(x, y) \in R$. Since $x \in A_1 \bigcup A_2$, then either $a \in A_1$ or $x \in A_2$ or in both. If $x \in A_1$ and $(x, y) \in R$, therefore, we must have $y \in R(A_1)$. Similarly, if $x \in A_2$, then we have $y \in R(A_2)$. In both the case, we have $y \in R(A_1)\bigcup R(A_2)$. Hence, we have

$$R(A_1 \bigcup A_2) \subseteq R(A_1)\bigcup R(A_2).$$

Thus,

$$R\left(A_1 \bigcup A_2\right) = R(A_1)\bigcup R(A_2).$$

3. Since, we have $A_1 \bigcap A_2 \subseteq A_1$ and $A_1 \bigcap A_2 \subseteq A_2$, then by part (1), we have

$$R(A_1 \bigcap A_2) \subseteq R(A_1)$$

and

$$R(A_1 \bigcap A_2) \subseteq R(A2).$$

Thus, we have

$$R(A_1 \bigcap A_2) \subseteq R(A_1)\bigcap R(A_2)$$

.

□

In the above Theorem, equality in part (3) does not hold good in general. For this, we have the following example.

Example 2.8. Let R be a relation define on a set $A = \{a, b, c, d, e, f\}$ as

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

Then, we consider $A_1 = \{a\}$ and $A_2 = \{b\}$. Then, we have $R(A_1) = \{a, b, c\}$ and $R(A_2) = \{a, c\}$. Here, we have $A_1 \cap A_2 = \emptyset$, thus $R(A_1 \cap A_2) = \emptyset$ but $R(A_1) \cap R(A_2) = \{a, c\} \neq \emptyset$.

In the following result, we will show that a relation can be determine with the help of its R-relative sets.

Theorem 2.2. Let R and S be two relations from the set A to B and let $R(a) = S(a)$ for all $a \in A$, then $R = S$.

Proof. Let $(a, b) \in R$, then we have $b \in R(a)$. By the given hypothesis, we have $R(a) = S(a)$, that is, $b \in S(a)$. Therefore, we have $(a, b) \in S$. Hence, $R \subseteq S$. Similarly, we have $S \subseteq R$. Thus, $R = S$. □

In-text Exercise 2.1. 1. Find the domain and range of the following relation R:

(a) $A = \{a, b, c, d\}$ and $B = \{1, 2, 3\}$
$R = \{(a, 1), (a, 2), (b, 1), (c, 2), (d, 1)\}$;

(b) $A = \{1, 2, 3, 4\}$ and $B = \{1, 4, 6, 8, 9\}$. The relation R is define as follow:

$$aRb \text{ if and only if } b = a^2;$$

(c) $A = \{1, 2, 3, 4, 8\}$ and $B = \{1, 4, 6, 9\}$; aRb if and only if a divides b;

(d) $A = \{1, 2, 3, 4, 8\}$ and $B = \{1, 4, 6, 9\}$; aRb if and only if $a < b$.

2. Let $A = \mathbb{R}$ be the set of all real numbers. Then, consider a relation R on A such that aRb if and only if $2a + 3b = 6$. Find $Dom(R)$ and $Ran(R)$.

3. Let $A = \mathbb{N}$, the set of all natural numbers, and R be the relation defined as aRb if and only if there exists a $k \in \mathbb{N}$ such that $a = b^k$. Then find

   (a) $R(4)$;

   (b) $R(3)$.

2.4 Types of Relations

In this section, we will learn about the various types of relations. In many real life applications, we deal with relations on a set A to A rather than from A to B.

2.4.1 Reflexive and Irreflexive Relations

Definition 2.5. A relation R on a set A is said to be reflexive if $(a, a) \in R$ for all $a \in A$.

That is, a relation is reflexive if every element of A is related to A.

Example 2.9. Let A be the set of all real number. Then consider a relation R on A, define as $(a, b) \in R$ if and only if $a \leq b$.

Then, one can easily check that for all $a \in \mathbb{R}$, we have $a \leq a$. Thus, R is a reflexive relation.

Definition 2.6. A relation R on a set A is said to be irreflexive if $a \not R a$ for every $a \in A$.

That is, a relation is irreflexive, if no element of A is related to itself.

Example 2.10. Let us consider a relation

$$R = \{(a, b) \in A \times A \mid a \neq b\}$$

Then, R is the relation of inequality on A. Then R is irreflexive, because $(a, a) \notin R$ for all $a \in A$.

Remark. Irreflexive is not the negation of reflexive. The negation of reflexive would be:

not reflexive if there exists some $a \in A$ such that $a \not R a$.
Thus, there are relations, which are neither reflexive nor irreflexive.

Example 2.11. Let $A = \{1, 2, 3, 4\}$ and R be a relation on A define as

$$R = \{(1, 1), (1, 2), (2, 3), (3, 3), (4, 4\}$$

Here, $(2, 2) \notin R$, therefore R is not reflexive. Also, we have $(1, 1) \in R$, thus R is neither irreflexive as well.

From the last example, one can conclude that reflexive and irreflexive relations are not complement to each other. We have relations, which are neither reflexive nor irreflexive.

Remark. By the definition of reflexive relation, one can observe that R is reflexive on a set A, then

$$Dom(R) = Ran(R) = A.$$

2.4.2 Symmetric, Antisymmetric and Asymmetric Relations

Definition 2.7. A relation R on a set A is said to be symmetric if whenever $(a, b) \in R$, we have $(b, a) \in R$.

Remark. A relation R is not symmetric if there exists some a and $b \in A$ such that aRb, but $b \not R a$.

Example 2.12. Let A be a set of all person living in Delhi and let R be relation on A defined as

$$(x, y) \in R \text{ if and only if } x \text{ is friend of } y.$$

Then R is a symmetric relation. As, whenever $(x, y) \in R$, means x is friend of y, which means y is friend of x. Therefore $(y, x) \in R$.

Definition 2.8. A relation R on a set A is said to be asymmetric if whenever $(a, b) \in R$, then $(b, a) \notin R$.

We can observe the following:

Remark. A relation is not asymmetric if there exists have some $a, b \in A$ such that whenever $(a, b) \in R$ implies that $(b, a) \in R$ too.

Example 2.13. Let $A = \{1, 2, 3, 4\}$ and let

$$R = \{(1, 2), (2, 2), (3, 4), (4, 1)\}$$

Then R is not asymmetric, as $(2, 2) \in R$.

Definition 2.9. A relation R on a set A is said to be antisymmetric if whenever $(a, b) \in R$ and $(b, a) \in R$, then $a = b$.

That is, a relation is antisymmetric if whenever $a \neq b$, then either $a \not R b$ or $b \not R a$.

Example 2.14. Let A be the set of all natural numbers and let

$$R = \{(a, b) \in A \times A \,|\, a \text{ divides } b\}$$

Let us consider two elements $a, b \in A$. Suppose a divides b and b divides a, then we have $a = b$. Hence R is antisymmetric relation.

Is R defined in the last example, a symmetric or asymmetric relation?

Example 2.15. Let $\mathbb{Z}$ be the set of all integers and let

$$R = \{(x, y) \,|\, x < y\}.$$

Then, one can easily verify that if $x < y$, that is, xRy, then $y \not< x$. Thus, R is a asymmetric relation on $\mathbb{Z}$.

Similarly, if suppose x is related to y and y is also related to x, that is, we have $x < y$ and $y < x$, which is not possible, hence the hypothesis of antisymmetric relation can not hold, that is, R is vacuously antisymmetric relation.

Check, whether R is symmetric?

2.4.3 Transitive Relation

Definition 2.10. A relation R on a set A is said to be transitive if whenever $(a, b) \in R$ and $(b, c) \in R$, then we have $(a, c) \in R$.

Note. If such a, b, and c do not exist, then R is transitive vacuously.

Example 2.16. Consider the Example 2.15, that is, R is the relation less than. Then whenever $(a, b) \in R$ and $(b, c) \in R$, that is, $a < b$ and $b < c$ then by transitivity, we have $a < c$, that is, $(a, c) \in R$. Hence R is a transitive relation.

Example 2.17. Let us consider $A = \{1, 2, 3, 4\}$ and let

$$R = \{(1, 2), (1, 3), (4, 3)\}$$

Then, there does not exist no triplets $a, b, c \in A$ such that $(a, b) \in R$ and $(b, c) \in R$. Thus, R is transitive vacuously.

We can summarize the reflexive, symmetric and transitive relations as follows:

Result 2.1. Let R be a relation on a set A. Then R is

1. reflexive if $a \in R(a)$ for all $a \in A$;
2. symmetry if $a \in R(b)$ if and only if $b \in R(a)$;
3. transitive if whenever $b \in R(a)$ and $c \in R(b)$, then $c \in R(a)$.

In-text Exercise 2.2.

1. Let $A = \{1, 2, 3, 4\}$. Check whether the relation is reflexive, symmetric, anti-symmetric or transitive.

(a) $R = \{(1,1),(2,2),(3,3)\}$;

(b) $R = \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$;

(c) $R = \{(1,3),(4,2),(2,4),(3,1),(2,2)\}$

2. Check whether the given relation is reflexive, symmetric, anti-symmetric or transitive.

   (a) $A = \mathbb{Z}$; aRb if and only if $a+b$ is even;

   (b) $A = \mathbb{R}$; aRb if and only if $a^2+b^2=1$;

   (c) $A = \mathbb{R}^2$; $(a,b)R(c,d)$ if and only if $a=c$.

2.5 Equivalence Relation

In this section, we discuss about an important class of relations known as equivalence relation. We will learn that every equivalence relation forms a partition of the set.

Definition 2.11. A relation R defined on a non-empty set A is called an equivalence relation if it is a reflexive, symmetric and transitive.

Now, we will discuss some examples of equivalence relation.

Example 2.18. Let A be the set of all the lines on a plane and let R be a relation on A define as l_1 is related to l_2 if and only if l_1 is parallel to l_2.

Then,

1. Every line l is parallel to itself, therefore $(l,l) \in R$ for all $l \in A$. Thus, R is reflexive.

2. Let $(l_1,l_2) \in R$, that is, l_1 is parallel to l_2, which means l_2 is parallel to l_1. Hence $(l_2,l_1) \in R$ and thus R is a symmetric relation.

3. Let $(l_1,l_2) \in R$ and $(l_2,l_3) \in R$, that is, l_1 is parallel to l_2 and l_2 is parallel to l_3. Thus, l_1 is parallel to l_3, $(l_1,l_3) \in R$. Hence, R is transitive.

Therefore, R is an equivalence relation.

Example 2.19. Let $A = \{1,2,3,4\}$ and let

$$R = \{(1,1),(1,2),(2,2),(3,4),(3,3),(4,3),(4,4)\}$$

Here, one can easily observe that $(a,a) \in R$ for all $a \in A$. Therefore R is reflexive.

Even R is transitive as well (Check yourself!). But R is not symmetric as $(1,2) \in R$ but $(2,1) \notin R$. Thus, R is not an equivalence relation.

Example 2.20. Let $A = \mathbb{N}$, the set of all natural numbers, and let R be defined by

$$(a,b) \in R \text{ if and only if } a > b.$$

Is R an equivalence relation?

Solution. Since $a \nless a$. Thus, R is not reflexive. Also, if $a < b$, it does not follow that $b < a$. Thus, R is neither symmetric too.

But, if have $a < b$ and $b < c$ which imply that $a < c$. Thus, R is transitive relation. Hence, R is not an equivalence relation.

In the above example, if we replace the relation $<$ by $\leq$, then is R an equivalence relation?

Example 2.21. Let $A = \mathbb{Z}$, the set of all integers and let

$$R = \{(a, b) \in A \times A \,|\, a \equiv b(\text{mod}(n))\}$$

for some $n \in \mathbb{Z}^+$. Then show that R is an equivalence relation.

Solution. Here

1. We have, for all $a \in A$, $(a - a) = 0$ is divided by n. Thus, $(a, a) \in R$ for all $a \in A$. Hence, R is reflexive.

2. Let $(a, b) \in R$, that is $(a - b)$ is divided by n. Therefore, we have $(b - a) = -(b - a)$ is also divided by n, R is symmetric.

3. Let $(a, b) \in R$ and $(b, c) \in R$, that is, $(a - b)$ and $(b - c)$ both are divided by n. Hence, $(a - c) = (a - b) + (b - c)$ is divisible by n. Thus, R is transitive as well.

Therefore, R is an equivalence relation.

Now, we define an important aspect of set theory, known as partition of a set. Later, we will show that every equivalence relation generates partition of the set and vice-verse.

Definition 2.12. A collection of pairwise disjoint subsets of a given set is called partition of the set, where the union of the subsets must equal to the entire set.

Let A be a given set. Then a collection $\{B_i \,|\, i \in \Lambda\}$ forms partition of A, if

1. $$A = \bigcup_{i \in \Lambda} B_i$$

2. $B_i \bigcap B_j = \emptyset$ for all $i \neq j$.

Also, the sets in partition are either disjoint or identical.

Example 2.22. Let us consider $A = \{a, b, c, d, e, f\}$. Then one possible partition of A is

$$\{a, c, e\}, \{b, d\}, \{f\}$$

In the Example 2.22, the collection $\{a, e\}$ and $\{b, c, d, f\}$ also forms another partition of A. Thus, one can conclude that partition of a set is not unique.

In the next result, we will show that every partition of a set A generates an equivalence relation. Later, we will show that this result is other way around as well.

Here, we recall that the sets in partition of a set are either disjoint or identical. Also, they are known as blocks of $\mathcal{P}$.

Theorem 2.3. Let $\mathcal{P}$ be a partition of a given non-empty set A. We define a relation R on A as follows:

$(a, b) \in R$ if and only if a and b are members of the same block.

Then R is an equivalence relation on A.

Proof.

1. Let $a \in A$ and let a be in some block say B_a. Then obviously $a \in B_a$. Therefore, $(a, a) \in R$.

2. Let $(a, b) \in R$, that is a and b both are in the same block, then b and a also lie in the same block. Thus, R is symmetric.

3. The relation R is transitive as whenever a and b are in same block, say A_1, and b and c are in same block say A_2. Thus, we have $b \in A_1 \bigcap A_2$, that is, $A_1 \bigcap A_2 \neq \emptyset$. Since, blocks are either disjoint or identical. Therefore, we have $A_1 = A_2$. Hence, we have $a, b, c \in A_1 = A_2$. That is, a and c both are in same block. Thus, we have whenever $(a, b) \in R$ and $(b, c) \in R$. Hence $(a, c) \in R$.

Therefore, R is an equivalence relation. □

Now, we will demonstrate the above result, with the help of an example.

Example 2.23. Let $A = \{1, 2, 3, 4\}$ and consider a partition

$$\mathcal{P} = \{\{1, 2\}, \{3, 4\}\}$$

Find the equivalence relation R on A generated by $\mathcal{P}$.

Solution. Here, we have

$$\mathcal{P} = \{\{1, 2\}, \{3, 4\}\}$$

Then, by the Theorem 2.3, one can construct an equivalence relation as follow:

Two elements in A are related to each others, if they lie in the same block. Then, we have

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}$$

Then, one verify that R is an equivalence relation generated by partition $\mathcal{P}$.

In the following, we will demonstrate that every partition of a set generates an equivalence relation. We will do this, with the help of an example:

Example 2.24. Let $A = \{1, 2, 3, 4, 5, 6, 7\}$ be a non-empty set and let

$$\mathcal{P} = \{\{1, 2, 5\}, \{3, 4\}, \{6, 7\}\}$$

be a partition of A. Here, the blocks of $\mathcal{P}$ are $\{1,2,5\}, \{3,4\}$ and $\{6,7\}$.
Consider $A_1 = \{1,2,5\}$ and $1 \in A_1$. For the equivalence relation, each element of A_1 must be related to every other element in A_1. That is, we have

$$R_1 = \{(1,1),(1,2),(1,5),(2,1),(2,2),(2,5),(5,1),(5,2),(5,5)\}$$

Repeat the same for the blocks $\{3,4\}$ and $\{6,7\}$. Thus, we have

$$R_2 = \{(3,3),(3,4),(4,3),(4,4)\}$$

and

$$R_3 = \{(6,6),(6,7),(7,6),(7,7)\}$$

Hence, the equivalence relation R generated by the partition $\mathcal{P}$ is $R = R_1 \bigcup R_2 \bigcup R_3$.

Thus, we can say that the partition $\mathcal{P}$ consist of

$$\{R(a) \mid a \in A\}$$

In words,we can say that $\mathcal{P}$ consists of all distinct R-relative sets which are generated by the elements of A.

Note. For a given partition of A, one can simply construct an equivalence relation on A.

In then following results, we will show that all the equivalence relations on a given non-empty set A can be produced from partitions.

Theorem 2.4. Let R be an equivalence relation on a given non-empty set A and let $a, b \in A$. Then, we have

$$(a,b) \in R \text{ if and only if } R(a) = R(b)$$

That is, for an equivalence relation, two elements are related to each other if and only if their R-relative sets coincide.

Proof. Let R be an equivalence relation on A and let $a, b \in A$ such that $R(a) = R(b)$. Then, we have to show that $(a,b) \in R$, that is, a is related to b.

Since R is reflexive, therefore $(b,b) \in R$, that is, $b \in R(b)$. By the given hypothesis, we have $R(a) = R(b)$, that is, $b \in R(a)$. Thus, we have $(a,b) \in R$.

Conversely, Let $(a,b) \in R$. Then, we have to show that $R(a) = R(b)$, which is same as proving the following two results:

1. $R(a) \subseteq R(b)$;

2. $R(b) \subseteq R(a)$.

We have $(a,b) \in R$, that is, $b \in R(a)$ and as R is a symmetric relation thus, we have, $a \in R(b)$.

Now, let $x \in R(a)$ which implies $(a,x) \in R$. Since, R is an equivalence relation, thus transitive. Hence, we $(b,x) \in R$, that is, $x \in R(b)$. Therefore, we have $R(a) \subseteq R(b)$.

Similarly, let $y \in R(b)$, that is $(b,y) \in R$. Also, we have $(a,b) \in R$. So, by transitivity, we have $(a,y) \in R$. Hence, we have $R(b) \subseteq R(a)$. Therefore, we have $R(a) = R(b)$. □

Now, we will provide our main result which connect the partition of a set with its corresponding equivalence relation.

Theorem 2.5. Let R be an equivalence relation on a given non-empty set A and let $\mathcal{P}$ be the collection of all distinct relative sets $R(a)$ for $a \in A$. Then, $\mathcal{P}$ is a partition of A. Also, R is the equivalence relation generated by $\mathcal{P}$.

Before, providing the proof, we recall the definition of a partition of a set A. We say $\mathcal{P}$ is a partition of a set A, if

1. Every element of A belongs to some relative sets;

2. Every two pair of partition are either identical or disjoint

   that is, whenever $R(a)$ and $R(b)$ are not identical then

$$R(a) \bigcap R(b) = \emptyset$$

Proof. Since R is an equivalence relation on A, therefore R is reflexive. Thus, we have $a \in R(a)$ for all $a \in A$. Hence, every element of A is a part of some $R(a)$.

Let $R(a) \bigcap R(b) \neq \emptyset$. Now, we have to show that $R(a) = R(b)$.

Let there exist some $c \in R(a) \bigcap R(b)$, that is, $(a,c) \in R$ and $(b,c) \in R$. Since, R is symmetric, thus, we have $(c,b) \in R$. By the transitivity of R, one can say that $(a,b) \in R$. Hence, by the Theorem 2.4, we have $R(a) = R(b)$.

Now, we will show that R is the equivalence relation generated by this partition $\mathcal{P}$. Again, from the Theorem 2.4, we have $(a,b) \in R$ if and only if a and b belong to the same block of partition $\mathcal{P}$. Therefore, partition $\mathcal{P}$ generated the relation R, which is an equivalence relation. Hence the result. □

Remark. Let R be an equivalence relation on A, then the R-relative sets, $R(a)$ are called equivalence classes of R and they are denoted by $[a]$.

The partition $\mathcal{P}$ constructed in Theorem 2.5 are nothing but the collection of equivalence classes of R.

Definition 2.13. Partition of a set A, generated by an equivalence relation R is called quotient set of A and is denoted by A/R.

Example 2.25. Let $A = \{1, 2, 3, 4\}$ be a set and let

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 3), (3, 3), (4, 4)\}$$

Then, one can easily verify that R is an equivalence relation on A. Also, we have $R(1) = \{1, 2\} = R(2)$ and $R(3) = \{3, 4\} = R(4)$. Hence, the quotient set

$$A/R = \{\{1, 2\}, \{3, 4\}\}.$$

Example 2.26. Let $A = \mathbb{Z}$ be the set of all integers and let R be a relation on A, define as

$$(a, b) \in R \text{ if and only if } a - b \text{ is divisible by } 2$$

Then, one can easily verify that R is an equivalence relation on A and its equivalence classes are

$$R(0) = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$$
$$R(1) = \{\ldots, -7, -5, -3, -1, 1, 3, 5, 7, \ldots\}$$

Since $R(0) \cup R(1) = A$ and $R(0) \cap R(1) = \emptyset$. Thus, we have A/R consists of $R(0)$, that is set of all even integers and $R(1)$, set of all odd integers only.

Working Rule for Determining partitions A/R for a finite set A Let $\mathcal{P}$ be a partition of A and let R be the corresponding equivalence relation generated by the partition $\mathcal{P}$.

step 1 Let A_1 be a member of $\mathcal{P}$ and let $a \in A_1$. Then from the above example, one can observe that A_1 consists of all elements $x \in A$ which are related to a, that is, $(a, x) \in R$.

Therefore, we have $R(a) \subseteq A_1$. Also, we have $A_1 \subseteq R(a)$. Thus, we have $A_1 = R(a)$.

step 2 Let there exist some $b(\neq a) \in A$ and $b \in A_2$, then by the case (1), we have $A_2 = R(b)$.

step 3 Repeat the step (3), until all the elements of A are excluded.

2.6 Equivalence Classes

Let R be an equivalence relation defined on a non-empty set A. For any $a \in A$, we define the equivalence class of a to be the set

$$\{b \in A \mid aRb\}$$

We denote the equivalence class of a by $[a]$.

Clearly, for each $a \in A$, we have an equivalence class. In the following, we provide some properties of equivalence classes:

1. Every equivalence class is non-empty.
   This is because of the fact that aRa.

2. Two equivalence classes are either same or disjoint.
   For $a, b \in A$, if we are $[a] = [b]$, then we are done.
   Let if possible, for $a, b \in A$ and $[a] \bigcap [b] \neq \emptyset$.

   then there exists some $x \in [a]$ and $x \in [b]$. Therefore, we have

$$aRx \text{ and } aRb$$

   As R is symmetric, thus, we have aRx and xRb. Thus, by transitivity of R, we have aRb. Hence $b \in [a]$.
   Let $t \in [a]$, therefore aRt also, we have aRb as well. Hence, by symmetric and transitivity, we have bRa and aRt, thus bRt. That is, $t \in [b]$. Hence, we have $[a] \subseteq [b]$.

   Similarly, we have $[b] \subseteq [a]$. Thus, $[a] = [b]$.

3. Union of equivalence classes equals to the set itself.
   Since $a \in [a]$ for all $a \in A$. Therefore

$$A = \bigcup_{a \in A} [a]$$

In the next example, we demonstrate the following:

Example 2.27. Let R be a relation defined on the set of integers $\mathbb{Z}$ such that

$$aRb \text{ if and only if } a = b \text{ or } a = -b$$

Then, R is an equivalence relation (Try yourself!).

Then, for any $a \in \mathbb{Z}$, the equivalence class of a is given by

$$\begin{aligned}[a] &= \{b \in \mathbb{Z} \,|\, aRb\} \\ &= \{a, -a\}\end{aligned}$$

Example 2.28. Let R be a relation defined on the set of integers $\mathbb{Z}$ such that aRb, if

$$a \equiv b(mod 4)$$

Then, the equivalence class of

$$\begin{aligned}[0] =&\{a \,|\, a \equiv 0(mod 4)\} \\ =&\{a \,|\, a \text{ is divisible by } 4\}\end{aligned}$$

Similarly, we have

$$\begin{aligned}[1] =&\{a \,|\, a \equiv 1(mod 4)\} \\ =&\{a \,|\, a - 1 \text{ is divisible by } 4\}\end{aligned}$$

Hence, we have

$$[0] =\{\dots, -8, -4, 0, 4, 8, \dots\}$$
$$[1] =\{\dots, -7, -3, 1, 5, 9, \dots\}$$

In general, equivalence class of a is given by

$$\begin{aligned}[a] =&\{b \mid a \equiv b(mod4)\}\\ =&\{b \mid b - aa \text{ is divisible by } 4\}\\ =&\{\dots, a-8, a-4, a, a+4, a+8, \dots\}\end{aligned}$$

In-text Exercise 2.3. 1. Determine whether the given relation R on a set A is an equivalence relation.

(a) $A = \{1, 2, 3, 4\}$
$R = \{(1, 1), (2, 1), (2, 2), (3, 3), (4, 4), (4, 3)\}$;

(b) $A = \{1, 2, 3, 4\}$
$R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (3, 1), (2, 3), (3, 3), (4, 4), (3, 2)\}$

2. Let A be the set of all the students admitted in SOL, then aRb if and only if a and b have the same last name. Is, R an equivalence relation.

3. Let $\{\{1, 3, 5\}, \{2, 4\}\}$ be a partition of the set $A = \{1, 2, 3, 4, 5\}$. Find the corresponding equivalence relation on A.

4. Let $S = \{1, 2, 3, 4, 5\}$ and $A = S \times S$. let us define the following relation R on A:

$$(a, b)R(c, d) \text{ if and only if } ac = bd$$

Show that R is an equivalence relation.

2.7 Partially Ordered Relations

In the previous section, we studied about the equivalence relation. We also studied that every equivalence relation generates equivalence classes which forms a partition of the underlying set A. Even, every partition of A generate an equivalence relation on A as well. In this section, we will discuss another important relation, known as Partial ordered relation on P. We will study various application of the same.

Definition 2.14. A relation R on a given non-empty set P is called a partial order relation if R is reflexive, antisymmetric and transitive.

The set P together with the partial order R is called a partially ordered set and it is denoted by (P, R). Sometimes, it is also known as poset.

Example 2.29. Let $\mathcal{P}(A)$ be the power set of A. Then, we define a relation R on $\mathcal{P}(A)$ as

$$X \text{ is related to } Y \text{ if } X \subseteq Y$$

where $X, Y \in \mathcal{P}(A)$. Then, we have

1. As $X \subseteq X$ for all $X \in \mathcal{P}(A)$. Therefore, R is reflexive.
2. Let $(X, Y) \in R$ and $(Y, X) \in R$, that is, $X \subseteq Y$ and $Y \subseteq X$. Therefore, we have $X = Y$. Hence R is antisymmetric.
3. Let $(X, Y) \in R$, $(Y, Z) \in R$, that is, $X \subseteq Y$ and $Y \subseteq Z$. Then, we have $(X, Z) \in R$. Hence R is transitive.

Therefore R is a partial order relation.

Example 2.30. Let P be the set of all integers and the usual $\leq$ (less than or equal to) relation is a partial order relation on P. As, we have

1. for every $a \in P$, we have $a \leq a$, that is $(a, a) \in R$. Thus, R is reflexive.
2. Let $(a, b) \in R$ and $(b, a) \in R$. That is, we have $a \leq b$ and $b \leq a$. Then, we have $a = b$. Hence, R is antisymmetric.
3. Similarly, one can prove that R is transitive.

Thus R is a partial order relation.

Example 2.31. Let $\mathcal{M}$ be the collection of all the equivalence relation on a set P. Then, $\mathcal{M}$ with the relation $\subseteq$, known as "partial order of set containment" forms a partial order relation.
That is, let R and S be two equivalence relation on P, then we define the relation "$\subseteq$" on $\mathcal{M}$ as

$$R \subseteq S \text{ if and only if } (x, y) \in R \text{ implies } (x, y) \in S \text{ for all } x, y \in P$$

Example 2.32. Check whether the relation $<$ on the set of natural numbers, a partial order relation.

Solution. As $a \not< a$ for $a \in P$. Thus, the given relation is not reflexive. Hence the given relation is neither partial order nor equivalence.

Definition 2.15. Let R be a relation define on a set A. Then the inverse relation of R, denoted by R^{-1} is define as

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

Result 2.2. Let P be a non-empty set and R be a partial order relation on P. Then the inverse relation, R^{-1} is also a partial order relation on P.

Solution. Let R be a partial order relation on P. Then

1. R is reflexive, therefore, we have $(a, a) \in R$ for all $a \in P$. Hence, we have $(a, a) \in R^{-1}$ for all $a \in P$. Therefore, R^{-1} is reflexive.
2. Let $(a, b) \in R^{-1}$ and $(b, a) \in R^{-1}$. Thus, by definition of inverse relation, we have $(b, a) \in R$ and $(b, a) \in R$. Since, R is an antisymmetric relation. Hence, we have $a = b$. Therefore, R^{-1} is an antisymmetric relation.

3. Let $(x, y) \in R^{-1}$ and $(y, z) \in R^{-1}$. That is, we have $(y, x) \in R$ and $(z, y) \in R$. Hence, by transitivity of R, we have $(z, x) \in R$. Thus, $(x, z) \in R^{-1}$. Hence R^{-1} is transitive.

Therefore, R^{-1} is a partial order relation.

Note. The partially ordered set (P, R^{-1}) is called the dual of the poset (P, R).

Since, we have $(R^{-1})^{-1} = R$. Thus, the dual of the dual is nothing but the same relation R.

The most common partial order relations are $\leq$ and $\geq$ defined on $\mathbb{Z}$. Therefore, it a common practice to mention a partial order on a set A with the symbol $\leq$ or with $\geq$ for R. Thus the reader may see the symbol $\leq$ used for many different partial orders on different sets. To distinguish various partial orders from one another, we may also use different symbols such as $\leq_1$, $\leq'$, $\geq_1$, $\geq'$ and so on.

Remark. Let $(A, \leq)$ is a partially ordered set, then we will use $(A, \geq)$ for the dual poset of $(A, \leq)$.

Similarly, the dual of poset $(A, \leq_1)$ will be denoted by $(A, \geq_1)$

Definition 2.16. Let $(A, \leq)$ be a partially ordered set, then we say $a, b \in A$ are comparable if either

$$a \leq b \text{ or } b \leq a$$

Example 2.33. Let $A = \mathbb{N}$, be the set of all natural numbers and let R be a relation define on A such that

$$aRb \text{ if and only if } a \mid b$$

Then, one can easily verify that

1. for all $a \in A$, we have a is divisible by a which implies $(a, a) \in R$. Therefore, R is reflexive.

2. Let $(a, b) \in R$ and $(b, a) \in R$, that is, a is divisible by b and b is divisible by a. Hence, we have $a = b$, the relation R is antisymmetric.

3. Let $(a, b) \in R$ and $(b, c) \in R$, that is, a is divisible by b and b is divisible by c, then we have a is divisible by c. Thus, $(a, c) \in R$. Hence R is a transitive relation.

Therefore, R is a partial order relation.

Here, one can observe that $3 \nmid 4$ and $4 \nmid 3$, that neither 3 is divisible by 4 nor 4 is divisible by 3. Hence, 3 and 4 are not comparable. But elements $2, 4$ are comparable as $2 \mid 4$.

Remark. Thus the word “partial” in partially ordered set $(A, \leq)$ is used because of the fact that in A some elements are comparable and some may not be comparable.

What if, in a set, every elements are comparable to each other?

Definition 2.17. Let R be a partial order relation on a given set A, where every pair of elements is comparable, that is, for all $a, b \in A$, we have either $a \leq b$ or $b \leq a$, then the set A is called linearly ordered set.

A linearly ordered set A is also known as totally ordered set or chain.

Example 2.34. Consider the set $P = \mathbb{Z}$ be the set of integers then the usual less than or equal to relation $\leq$ is a partial order on P. Then, one can easily observe that for every pair $a, b \in P$, we have either $a \leq b$ or $b \leq a$. Thus, $(P, \leq)$ is a chain.

In the next result, we will show how to construct new partial order relations from the existing one.

Theorem 2.6. Let $(A, \leq)$ and $(B, \leq)$ be two partially order sets. Then $(A \times B, \leq)$ is a partial order set, with the partial order $\leq$ defined as

$$(a, b) \leq (a', b') \text{ if and only if } a \leq a' \text{ and } b \leq b'$$

Proof. Here, we have to show that the partial order $\leq$ on the product space $A \times B$ is a partial order relation, that is, reflexive, antisymmetric and transitive.

1. Let $(a, b) \in A \times B$, that is, $a \in A$ and $b \in B$. As, $(A, \leq)$ and $(B, \leq)$ both are reflexive, thus, we have $a \leq a$ and $b \leq b$. Hence, we have

   $$(a, b) \leq (a, b)$$

   for all $a \in A$ and $b \in B$. Thus, $\leq$ is reflexive in $A \times B$.

2. Now let $(a, b) \leq (a', b')$ and $(a', b') \leq (a, b)$ for some $a, a' \in A$ and $b, b' \in B$. Then,, we have

   $$a \leq a' \text{ and } a' \leq a \text{ also } b \leq b' \text{ and } b' \leq b$$

   Since $(A, \leq)$ and $(B, \leq)$ both are antisymmetric (being partial order), thus, we have $a = a'$ and $b = b'$. Hence, we have $(a, b) = (a', b')$. Therefore, $\leq$ is antisymmetric on $A \times B$.

3. Let

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

   for some $a, a', a'' \in A$ and $b, b', b'' \in B$. Then we have

   $$a \leq a' \text{ and } a' \leq a''$$

   Therefore, we have $a \leq a''$, by the transitivity of the poset $(A, \leq)$. Similarly, we have

   $$b \leq b' \text{ and } b' \leq b''$$

   Hence, we have $b \leq b''$

Thus, we have

$$(a, b) \leq (a'', b'')$$

Therefore, $\leq$ is a partial order on $A \times B$ and hence $A \times B$ is a partial order set. $\square$

Remark. The partial order $\leq$ defined on the Cartesian product $A \times B$ is also called the product partial order.

In-text Exercise 2.4. 1. Determine whether the relation R is a partial order on the set p;

   (a) $A = \mathbb{Z}$ and aRb if and only if $a = 2b$;
   (b) $A = \mathbb{Z}$ and aRb if and only if b^2 divides a;
   (c) $A = \mathbb{R}$ and aRb if and only if $a \leq b$;

2. Let A be the collection of all the lines and R be a relation define on A as

$$l_1 R l_2 \text{ if and only if } l_1 \text{ is parallel to } l_2$$

   Then, check whether R is a partial order relation.

3. Let A be the collection of all the candidates applying for the B. Sc (H) Mathematics and let R be a relation define on A such that

$$aRb \text{ if and only if } a \text{ is a friend of } b$$

2.8 Summary

In this chapter, we have covered the following:

1. A relation R from A to B is a subset of $A \times B$ and whenever $(a, b) \in R$, then we say a is related to b.

2. Let R be a relation from A to B and let $x \in A$. Then, we have

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

3. A relation R on a set A is

   (a) reflexive if aRa for all $a \in A$;
   (b) irreflexive if $a \not R a$ for every $a \in A$;
   (c) symmetric if whenever aRb, then we have bRa;
   (d) asymmetric if whenever aRb then $b \not R a$;
   (e) antisymmetric if whenever aRb and bRa, then $a = b$;
   (f) transitive if whenever aRb and bRc then aRc;

4. A relation R, which is reflexive, symmetric and transitive is called equivalence relation

5. Every equivalence relation generates equivalence classes and vice versa;

6. For an equivalence relation R on a set A, we have

$$R(a) = R(b) \text{ if and only if } (a, b) \in R$$

7. A relation R, which is reflexive, anti-symmetric and transitive is called partial ordered set.

2.9 Self-Assessment Exercise

1. Give an example of a relation which is
   (a) Reflexive, not symmetric and not transitive;
   (b) Not reflexive but transitive;
   (c) neither reflexive nor transitive.

2. Let R be a relation on the set of all integers $\mathbb{Z}$ define as

$$aRb \text{ if and only if } a - b \text{ is an even integers}$$

   Show that R is an equivalence relation.

3. Let R be a relation from A to B. Then for subsets $A_1, A_2 \subseteq A$, show that $R(A_1 \cap A_2) = R(A_1) \cap R(A_2)$ if and only if $R(a) \cap R(b) = \emptyset$ for any distinct $a, b \in A$

4. Check, whether "greater than" relation $>$ is a partial order relation on the set of real numbers.

5. Let $A = \mathbb{R}^2$. Then show that the relation R on A define as

$$(a, b)R(c, d) \text{ if and only if } a^2 + b^2 = c^2 + d^2$$

   is an equivalence relation.

2.10 Solutions to In-text Exercises

In-text Exercise 2. 1

1 (a) $Dom(R) = \{a, b, c, d\}$ and $Ran(R) = \{1, 2\}$
(b) $Dom(R) = \{1, 2, 3, 4\}$ and $Ran(R) = \{1, 4, 6, 8\}$
(c) $Dom(R) = \{1, 2, 3, 4\}$ and $Ran(R) = \{1, 4, 6, 9\}$
(d) $Dom(R) = \{1, 2, 3, 4, 8\}$ and $Ran(R) = \{4, 6, 9\}$

2 Here $Dom(R) = \mathbb{R}$, set of all real numbers and $Ran(R) = \{x \in \mathbb{R} \mid x = (6-2a)/3,\ \text{for } a\ in\mathbb{R}\}$

3 (a) $R(4) = \{2, 4\}$
(b) $R(3) = \{3\}$

In-text Exercise 2. 2

1 (a) R is symmetric, anti-symmetric as well as transitive relation, it is not reflexive, as $(4,4) \notin R$.
(b) R is neither reflexive as $(1,1) \notin R$, it is nor symmetric as well as $(1,2) \in R$ but $(2,1) \notin R$.
(c) R is neither reflexive, symmetric, anti-symmetric nor transitive.

2 (a) R is an equivalence relation but not anti-symmetric as we have $(1,3) \in R$ and $(3,1) \in R$ but $1 \neq 3$.
(b) Here, R is neither reflexive, anti-symmetric nor transitive. But R is a symmetric relation.
(c) R is an equivalence relation but not anti-symmetric as $(1,2)R(1,3)$ and $(1,3)R(1,2)$ but $(1,2) \neq (1,3)$

In-text Exercise 2. 3

1 (a) R is not an equivalence relation as R is not symmetric;
(b) R is an equivalence relation.

2 Here R is an equivalence relation but R is not anti-symmetric;

3 Here the relation R is

$$R = \{(1,1), (1,3), (1,5), (3,1), (3,3), (3,5), (5,1), (5,3),$$

$$(5,5), (2,2), (2,4), (4,2), (4,4)\}$$

4 Here R is reflexive as $(a,b)R(a,b)$ for all $(a,b) \in A$. Also, R is symmetric and transitive as well.

In-text Exercise 2. 4

1 (a) R is not reflexive as $1 \not{R} 1$, hence R is not a partial order relation.
(b) Here, R is not reflexive as $2 \not{R} 2$, hence R is not a partial order relation.
(c) Here R is a partial order relation.

2 R is not an anti-symmetric relation. Thus, R is not a partial order relation.

3 Here R is neither anti-symmetric nor transitive. Hence, R is not a partial order relation.

Lesson - 3

Functions and other properties

Structure

3.1 Learning Objectives

After going through this chapter, we should be able to :

- define functions from the set A to B;
- define and study the composition and algebra of two functions;
- understand different types of functions, like- one-one, onto, everywhere defined and bijective functions;
- study the inverse of function, whenever it exists and their respective properties;

- introduce and study the poset with the help of Hasse diagrams;
- study Lattices and its algebraic structure.

3.2 Introduction

In this chapter, our focus will be on a special type of relation known as function. Functions play very important role in mathematics, computer science other diverse field of education. Later, we will also revisit the partial order set and its various properties. Finally, we will discuss some basic notion for lattices, which will be used frequently in later chapters.

3.3 Functions

In this section, we will define the notion of a function, which is a special type of relation. Later on, we study some basic properties and types of functions. We will demonstrate all these properties with the help of various examples.

Definition 3.1. Let A and B be two non-empty sets. Then a function f from A to B is a relation from A to B satisfying the following properties

1. for all $a \in \mathrm{Dom}(f)$, $f(a)$, the f-relative set of a is non-empty.
   That is, $\mathrm{Dom}(f) = A$;
2. For every $a \in\mathrm{Dom}(f)$, f-relative set of a contains exactly one element of B.
   That is, whenever $a_1 = a_2$, we have $f(a_1) = f(a_2)$.

Remark. Whenever $a \notin Dom(f)$, then $f(a) = \emptyset$.

For the simplicity, we mention the relation f with the set of pairs

$$\{(a, f(a)) \,|\, a \in Dom(f)\}$$

Functions are also known as mappings or transformations because, here every element of A is mapped to a unique element of B. The element $b = f(a)$ is referred as image of a under f and the element a is called pre image of b under f.

Example 3.1. Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$ and let us define a relation f from A to B as

$$f = \{(1, a), (2, a), (3, b), (4, c)\}$$

Here, we have

$$\begin{aligned} f(1) =&f(2) = a \\ &f(3) = b \\ &f(4) = c \end{aligned}$$

Here, each $a \in A$ is assign to a single value of B, therefore f is a function.

Again, consider a relation define from $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$ defined as

$$f = \{(1, a), (2, a), (3, a), (4, a), (1, b)\}$$

Here, we have $f(1) = a$ as well as $f(1) = b$, therefore, $f(1) = \{a, b\}$, which is not a singleton set. Hence, f is not a function.
In the Example 3.1, the domain of f is $\{1, 2, 3, 4\}$ and Range of $f = \{a, b, c\}$. Here, one can notice that, for a function, $Ran(f)$ may not be equal to co-domain of f.

Example 3.2. Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$. Consider the relation

$$R = \{(1, a), (2, b), (3, c)\}$$

Then, again R is not a function as $R(4) = \emptyset$.

Example 3.3. Let $A = \mathbb{R}$ be the set of all real numbers, and let $p(x)$ be polynomial with real coefficients, that is

$$p(x) = a_0 + a_1 x + \ldots + a_n x_n.$$

Then p may be realized as a relation on $\mathbb{R}$, define as

for each $r \in \mathbb{R}$, we have $p(r)$, by putting $x = r$ in $p(x)$.

Since all relative sets $p(r)$ are well defined and for each $r \in \mathbb{R}$, $p(r)$ generates a unique value in $\mathbb{R}$. Thus, the relation p is a function from $\mathbb{R}$ to $\mathbb{R}$.

Example 3.4. Let $A = \mathbb{N}$, be the set of all natural numbers and let B, be the set of all even integers. Then, we can define a function $f\colon A \to B$ as

$$f(n) = 2n \text{ for all } n \in A$$

One can easily confirm that f is a function defined by giving a formula for the values $f(n)$.

Example 3.5. Let $A = \mathbb{Z}$, be the set of all integers and let $B = \{0, 1\}$. Let $f\colon A \to B$ define as

$$f(x) = \begin{cases} 0 & \text{if } x \text{ is even} \\ 1 & \text{if } x \text{ is odd} \end{cases}$$

Then f is a function because for each $x \in A$, $f(x)$ is either 0 or 1, singleton.

Now, we define a special type of function and composition of two function.

Definition 3.2. Let A be a non-empty set. Then the identity function I_A on A is defined as

$$I_A(a) = a \text{ for all } a \in A$$

Whenever $A_1 \subseteq A$, then we have $I_A(A_1) = A_1$.

Definition 3.3. Let $f\colon A \to B$ and $g\colon B \to C$ be two functions. Then, the composition of f and g, is a relation from A to C, define as

$$g \circ f\colon A \to C$$

as, $a \in Dom(g \circ f)$. Then

$$g \circ f(a) = g\left(f(a)\right)$$

Since, f and g both are functions, then for each $a \in A$, $f(a)$ is a singleton element, that is, there exists some $b \in B$ such that $f(a) = b$. Therefore, we have $g(f(a)) = g(b)$. Since, g is a function, thus, for $b \in B$, there exists some $c \in C$, such that

$$g(b) = c$$

Thus, we have, for each $a \in A$, there exists some $c \in C$ such that $g \circ f(a) = c$, that is, $g \circ f(a)$ contains just one element of C. Hence, $g \circ f$ is a well define function form A to C.

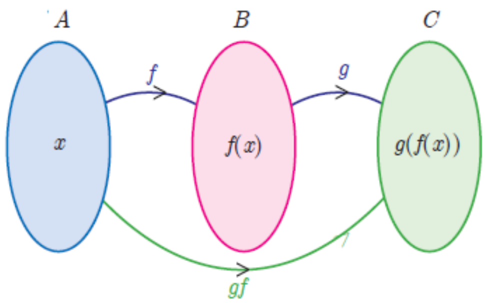


Figure 3.1: Composition of two functions

Example 3.6. Let $A = C = \mathbb{N}$ be the set of all natural numbers, $B = \mathbb{E}$, be the set of all even natural numbers. Let us define two functions $f\colon A \to B$ and $g\colon B \to C$ as

$$f(x) = 2x$$

$$g(x) = x/2$$

Then, find $g \circ f$

Solution. Consider

$$g \circ f(x) = g(f(x)) = g(2x) = (2x)/2 = x$$

Hence, we have $g \circ f(x) = x$.

3.4 Bijective Functions

In the following, we define some special class of functions, which are onto function and one-one function.

Definition 3.4. Let f be a function define from a set A to B. Then, we say

1. f is onto if $Ran(f) = B$;

2. f is one-one if for
$$f(a) = f(b) \text{ imples } a = b$$

3. f is everywhere defined, if $Dom(f) = A$.

Example 3.7. Let us consider $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$, and let us define a function f from A to B as

$$f = \{(1, a), (2, a), (3, c), (4, d)\}$$

Then the function f is not onto, as $Ran(f) = \{a, c, d\} \neq B$. Also, we have $f(1) = f(2) = a$, but $1 \neq 2$. Hence, f is neither one-one nor onto.

Example 3.8. Let us consider $A = B = \mathbb{Z}$, be the set of all integers and let $f\colon A \to B$ be a function defined as
$$f(a) = a + 1 \text{ for all } a \in A.$$

Then

1. f is one-one:
   Consider
$$f(a) = f(b) \quad \Rightarrow \quad a + 1 = b + 1$$
$$a = b$$

2. f is onto:

   For all $b \in B$, there always exists some $a = b - 1 \in A$, such that
$$f(a) = f(b - 1) = (b - 1) + 1 = b$$

   Hence, $Ran(f) = B$, thus, f is onto.

Is f everywhere defined?

3.4.1 Invertible Function

Definition 3.5. A function $f\colon A \to B$ is said to be invertible if its inverse relation f^{-1}, is also a function.

Example 3.9. Consider a function f defined from $A = \{1, 2, 3\}$ to $B = \{a, b, c\}$ as

$$f = \{(1, a), (2, a), (3, a)\}$$

Then, f is a function, which is everywhere defined. But

$$f^{-1} = \{(a, 1), (a, 2), (a, 3)\}$$

is not a function (Why?). Therefore, f is not invertible.

In the next result, we will provide a necessary and sufficient condition for a function to be invertible.

Theorem 3.1. Let $f\colon A \to B$ be a function. Then

1. Then f^{-1} is a function from B to A if and only if f is one-one. Also, If f^{-1} is a function, then
2. the function f^{-1} is one-one.
3. f^{-1} is everywhere defined if and only if f is onto. Also,
4. f^{-1} is onto if and only if f is everywhere defined.

Proof. 1. Here, we have to prove

 (a) If f^{-1} is a function then f is one-one, that is,

$$f(x) = f(y) \Rightarrow x = y$$

 (b) If f is one-one then f^{-1} is a function.

 Let if possible f^{-1} is not a function. Therefore, for some $y \in B$, $f^{-1}(y)$ is not singleton, that is, there exists $x_1, x_2 \in A$ such that

$$f(x_1) = y = f(x_2)$$

 But, we have $x_1 \neq x_2$. Therefore f is not one-one.

 Conversely, let f is not one-one, therefore, there exists $x_1 \neq x_2 \in A$ such that $f(x_1) = f(x_2)$. Let $f(x_1) = y$ for some $y \in B$. Hence, we have $x_1, x_2 \in f^{-1}(y)$, that is, $f^{-1}(y)$ is not singleton. Thus, f^{-1} is not a function. Hence the proof.

2. Here, we have given then f^{-1} is a function and we have to show that f^{-1} is also one-one.

 Since, f^{-1} is a function, thus $\left(f^{-1}\right)^{-1} = f$ is also a function. Thus, by case (1), we have f^{-1} is one-one.

3. Let f is a function from A to B, then a function f is onto if $Ran(f) = B$. Also, f is everywhere defined if $Dom(f) = A$. Also, we have

$$Dom(f^{-1}) = Ran(f)$$

Thus, f^{-1} is everywhere defined if and only if $Dom(f^{-1}) = B$. Thus, we have $B = Dom(f^{-1}) = Ran(f)$. Hence, we have $Ran(f) = B$. Therefore f is onto. Hence, we have f^{-1} is everywhere defined if and only if f is onto.

4. Likewise in case (3), We have $Ran(f^{-1}) = D0m(f)$ and since f is defined everywhere, thus, we have $Dom(f) = A$. Therefore $A = Ran(f^{-1})$. Hence, f is defined everywhere if and only if f^{-1} is onto.

□

Thus, from the above theorem, one can conclude that whenever f is one-one and onto then f^{-1} is also one-one and onto and vice-versa. That is, we have

$$f(a) = b \Leftrightarrow a = f^{-1}(b)$$

Example 3.10. Let $A = B = \mathbb{R}$ be the set of all real numbers and let $f \colon A \to B$ be a function defined as

$$f(x) = |x|$$

Is f invertible?

Solution. To check, f is invertible, we have to check f is one-one. Here $2 \neq -2 \in \mathbb{R}$. But $f(2) = f(-2) = 2$.

Hence, one can conclude that f is not one-one. Thus, f is not invertible.

In the following, we will notice some results concerning the composition of functions.

Theorem 3.2. Let $f \colon A \to B$ be a function. Then

1. $I_B \circ f = f$;
2. $f \circ I_A = f$

   Also, if f is one-one and onto then,

3. $f^{-1} \circ f = I_A$
4. $f \circ f^{-1} = I_B$.

Proof. 1. Consider

$$\begin{aligned}(I_B \circ f)(a) &= I_B(f(a)) \\ &= f(a)\end{aligned}$$

for all $a \in Dom(f) \subseteq A$. Therefore, we have $I_B \circ f = f$

2. Likewise case (1), we have

$$\begin{aligned}(f \circ I_A)(a) &= f(I_A(a)) \\ &= f(a)\end{aligned}$$

for all $a \in Dom(f) \subseteq A$. Therefore, we have $f \circ I_A = f$

Now, suppose that f is one-one and onto function from A to B. Then, from Theorem 3.1, we have the solution $f(a) = b$ is equivalent to the equation $a = f^{-1}(b)$. Since f and f^{-1} both are defined everywhere and onto, thus we have

$$f\left(f^{-1}(b)\right) = b \text{ and } f^{-1}(f(a)) = a$$

for $a \in A$ and $b \in B$.

3. For all $a \in A$, consider

$$\begin{aligned}I_A(a) &= a \\ &= f^{-1}(f(a)) \\ &= \left(f^{-1} \circ f\right)(a)\end{aligned}$$

Hence, we have $I_A = f^{-1} \circ f$.

4. For all $b \in B$, we have

$$\begin{aligned}I_B(b) &= b \\ &= f(f^{-1}(b)) \\ &= \left(f \circ f^{-1}\right)(b)\end{aligned}$$

Hence, we have $I_B = f \circ f^{-1}$.

□

Theorem 3.3.
1. Let $f\colon A \to B$ and $g\colon B \to A$ be two functions such that $g \circ f = I_A$ and $f \circ g = I_B$. Then f is one to one correspondence from A to B and g is one to one correspondence from B to A. Also, f is the inverse of g and g is the inverse of f.

2. Let $f\colon A \to B$ and $g\colon B \to C$ be invertible. Then $g \circ f$ is invertible. Also

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Proof.
1. We have

$$f \circ g = I_B \text{ and } g \circ f = I_A$$

that is, $f \circ g(b) = f(g(b))$ and $g \circ f(a) = g(f(a)) = a$ for all $a \in A$ and $b \in B$.

Hence, we have $Ran(f) = B$ and $Ran(g) = A$, thus f and g both are onto. Also, consider

$$f(x) = f(y)$$

Hence, we have $x = g(f(x)) = g(f(y)) = y$. Hence f is one-one. Similarly, we can show that g is one to one. Thus, f and g both are invertible.

Also, f^{-1} is defined everywhere, that is $Dom(f^{-1}) = Ran(f) = B$. Therefore, for $b \in B$, we have

$$\begin{aligned} f^{-1}(b) &= f^{-1}(f(g(b))) \\ &= (f^{-1} \circ f)g(b) \\ &= I_A(g(b)) \\ &= g(b) \end{aligned}$$

Hence, we have $f^{-1} = g$. Also, $f = (f^{-1})^{-1} = g^{-1}$. Since f and g are onto, f^{-1} and g^{-1} are onto. Thus, f and g are everywhere defined.

2. As f^{-1} and g^{-1} are functions. Thus, the composition $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ is also a function. Hence $g \circ f$ is invertible.

□

Example 3.11. Let $A = B = \mathbb{R}$, the set of all real numbers and let $f : A \to B$ be a function defined as

$$f(x) = x^3$$

and let $g : B \to A$ be defined as

$$g(x) = \sqrt[3]{x}.$$

Show that f is one-one and onto. Also, show that $g = f^{-1}$.

Solution. Let $x \in \mathbb{R}$ and $y = f(x) = x^3$. Hence, we have $x = \sqrt[3]{y} = g(y)$. Therefore, $g(y) = g(f(x)) = (g \circ f)(x)$.

Thus, $g \circ f = I_A$. Similarly, one can show that $f \circ g = I_B$. Thus, by the Theorem 3.3, both f and g are one-one and onto.

In the next result, we will show that over the finite sets, a function is one-one if and only if its onto.

Theorem 3.4. Let A and B be two finite sets such that the number of elements in A and B are same. Let $f : A \to B$ be defined everywhere. Then f is one-one if and only if f is onto.

Proof. Let $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ be two finite sets such that both have same cardinality (finite), that is, the number of elements in the set A and B are same. Let f be a function from A to B which is defined everywhere.
Then, suppose f is one-one, that is $f(a_1), f(a_2), \ldots, f(a_n)$ must map to n distinct elements, that is, $f(a_1) \neq f(a_n)$ of B. Since, the number of elements in B is also n, hence f must be onto.

Similarly, suppose f is onto, then $f(a_1), f(a_2), \ldots f(a_n)$ form the entire set B, thus all must be distinct. Hence f is one-one. □

Thus, one can say that if f is a function define from A to B, where A and B are finite sets having same number of elements. Then, to prove that a function is bijective it is sufficient to show that f is either one-one or onto.

In-text Exercise 3.1. 1. Let $A = \{a, b, c, d\}$ and $B = \{1, 2, 3\}$. Check whether the given relation R from A to B is a function.

- (a) $R = \{(a, 1), (b, 2), (c, 1), (d, 2)\}$;
- (b) $R = \{(a, 1), (b, 2), (a, 2), (c, 1), (d, 1)\}$
- (c) $R = \{(a, 1), (b, 1), (c, 1), (d, 1)\}$
- (d) $R = \{(a, 1), (a, 2), (b, 1)\}$

2. Check whether the relation R from A to B is a function.
$A = \{$ the set of all students in SOL $\}$
$B = \{x \mid x$ is a 10 character number$\}$
aRb if b is the PAN card number of person a.

3. Let $A = B = C = \mathbb{R}$, be the set of real numbers and let $f\colon A \to B$, $g\colon B \to C$ be two functions defined by $f(a) = a + 1$ and $g(b) = b^2 + 2$. Evaluate

- (a) $g \circ f(2)$;
- (b) $f \circ g(2)$;
- (c) $g \circ f(x)$;
- (d) $f \circ g(x)$;
- (e) $f \circ f(x)$;
- (f) $g \circ g(x)$.

4. Check the given function from A to B is one-one or onto or both or neither.

- (a) $A = \{a, b, c\}$ and $B = \{x, y, z, w\}$
  $f = \{(a, x), (b, y), (c, z)\}$
- (b) $A = \{a, b, c, d\}$ and $B = \{x, y, z\}$
  $f = \{(a, x), (b, y), (c, z), (d, x)\}$
- (c) $A = B = \mathbb{R}^2$
  $f((a, b)) = (a + b, a - b)$
- (d) $A = B = \mathbb{R}$
  $f(x) = x^2$.

5. Let f be a function from A to B. Find f^{-1}

- (a) $A = B = \mathbb{R}$; $f(x) = \frac{2x-1}{3}$;
- (b) $A = B = \{1, 2, 3, 4, 5\}$
  $f = \{(1, 3), (2, 4), (3, 1), (4, 2), (5, 5)\}$

6. Give a bijective function between the set of all natural numbers $\mathbb{N}$ and $A = \{x \mid x \text{ is a positive even integer}\}$

7. Let f be a function from $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$. Check, whether f^{-1} is a function.

   (a) $f = \{(1, a), (2, a), (3, c), (4, d)\}$

   (b) $f = \{(1, a), (2, c), (3, b), (4, d)\}$

3.5 Lexicographic Order

In the last chapter, we studied about the partially ordered set and relations on a set P. We also discussed about the product partial order, which was defined on the Cartesian product $A \times B$.

Here, we will define another useful partial order relation on $A \times B$, generated by the partial order relations on A and B, where $(A, \leq)$ and $(B, \leq)$ are posets.

Definition 3.6. Let $(A, \leq)$ and $(B, \leq)$ be two partial ordered sets. Then a partial order relation on $A \times B$ is defined as

$$(a, b) \preceq (a', b') \text{ if } a < a' \text{ or if } a = a' \text{ and } b \leq b'$$

This ordering is known as lexicographic or dictionary order.

In this type of ordering, the first coordinate of the tupple dominates except there will be a tie. Also, one can easily verify that whenever $(A, \leq)$ and $(B, \leq)$ both are linearly ordered sets, then the lexicographic order $\preceq$ on $A \times B$ is also a linear order.

Example 3.12. Let $A = \mathbb{Z}$, be the set of integers with usual ordering. Then, one can define the lexicographic order on $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ as vertical line in $\mathbb{Z}^2$.

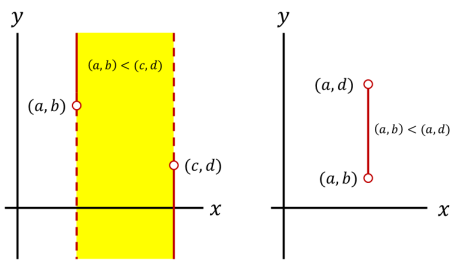


Figure 3.2: Dictionary Order

We can extend the lexicographic ordering to Cartesian product of finite family of sets, that is, let $A_1, A_2, \ldots A_n$ are non-empty sets. Then consider

$$G = A_1 \times A_2 \times \ldots A_n$$

We define a lexicographic ordering over G as follows:

$$(a_1, a_2, \ldots, a_n) \preceq (a'_1, a'_2, \ldots, a'_n) \text{ if and only if}$$

$a_1 < a_1'$ or
$a_1 = a_1'$, and $a_2 < a_2'$ or
$a_1 = a_1', a_2 = a_2'$ and $a_3 < a_3'$ or
$a_1 = a_1', a_2 = a_2', \ldots a_{n-1} = a_{n-1}'$ and $a_n < a_n'$

Example 3.13. Let $G = \{a, b, \ldots, z\}$ be the collection of all the alphabets in English, with usual linearly ordered, that is $(a \leq b, b \leq c, \ldots y \leq z)$. Let $G^n = G \times G \times \ldots G$ (n-factors) can be identified with the set of all words having length n. Then lexicographic order on G^n has the property that if $A_1 \preceq A_2$, where $A_1, A_2 \in G^n$. Then A_1 would precede A_2 in usual dictionary order listing.

Then, one can easily observe that Bat$\preceq$ Cat, park$\preceq$ part.

One can extend the above example in general as follow:

Let S be a poset, then we can lexicographic order to S^* (collection of all strings) in the following way:

Let $x, y \in S^*$, where $x = a_1 a_2 \ldots a_n$ and $y = b_1 b_2 \ldots b_m$ are in S^* with $n \leq m$, then we say that $x \preceq y$ if $(a_1, a_2, \ldots, a_n) \preceq (b_1, b_2, \ldots, b_n)$ in S^n under lexicographic ordering of S^n.

Note. The elements of S^n and S^* are of the same length n but with different notations, that is, $(a_1, a_2, \ldots, a_n) \in S^n$ and $a_1 a_2 \ldots a_n \in S^*$.

The notations differ for some historical reasons and they are interchangeable depending on context.

Example 3.14. Let $S = \{a, b, \ldots, z\}$ be the collection of all alphabets with usual order. Then S^* is the set of all possible "words" of any length. Then, we have

$$\text{help} \preceq \text{helping}$$

in S^*, while

$$\text{helper} \preceq \text{helpin}$$

in S^6.

Remark. Consider

$$\text{help} \preceq \text{helping}$$

this type of order is also known as prefix order. That is, any word is greater than all of its prefixes. The words occur in the dictionary also follow the prefix ordering.

Thus, the prefix order is a dictionary order but for the words of any finite length n.

3.6 Hasse Diagrams

In the following, we will introduce the concept of Hasse Diagrams of the partially order set.

Definition 3.7. A finite partially ordered set P can be represented by Hasse Diagram where elements of P are represented by points in a plane and whenever xRy $(x \neq y)$, we draw the point y higher than x and connect with x via a line segment.

Non-comparable elements are not joined. That is, there will be no horizontal line in the diagram.

Example 3.15. Let $A = \{1, 2, 3, 5, 7, 11, 13\}$ be a non-empty set. Consider the partial order of divisibility on A, that is $a \leq b$ if and only if a divides b. Then the following partially ordered set A can be represented by the Hasse diagram given by the Figure 3.5. Here, every element of A is divisible by 1 and all are co-prime, thus we have 1 is

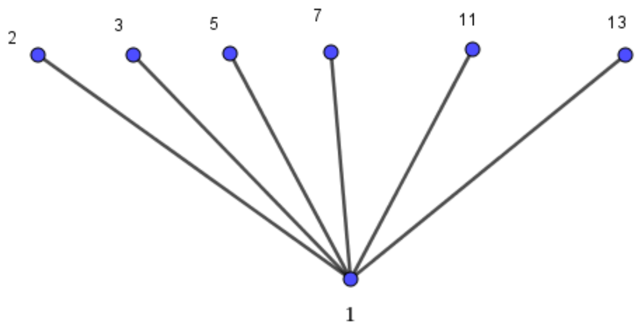


Figure 3.3: Hasse Diagram

at the lower level and all the other elements are in the upper level.

Remark. Let A be a partially ordered set and the element x is related to y and y is related to z, then because of transitivity the element x is related to z. Then, in the Hasse diagram, we do not have to connect x with z directly as they are connected via y.

Example 3.16. Let $A = \{1, 2, 3, 4, 6, 12\}$. Consider the partial order of divisibility on the set A. That is, xRy if and only if x divides y. Here, the elements in the partial order is given by

$$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 6), (1, 12), (2, 2), (2, 4), (2, 6), (2, 12),$$

$$(3, 3), (3, 6), (3, 12), (4, 4), (4, 12), (6, 6), (6, 12), (12, 12)\}$$

Hence, the Hasse diagram of the poset is represented by Figure 3.4.

Example 3.17. Let $A = \{a, b, c\}$ and $S = \mathcal{P}(A)$, be the power set of A. Then $\mathcal{P}(A)$ is a partially ordered set under the set inclusion relation " $\subseteq''$.

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

This poset is represented by the following Hasse diagram:

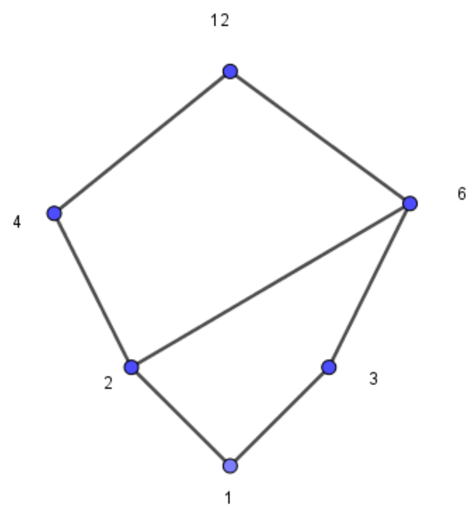


Figure 3.4: Hasse Diagram

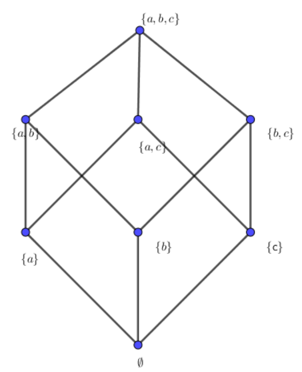


Figure 3.5: Hasse Diagram

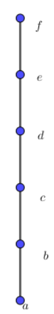
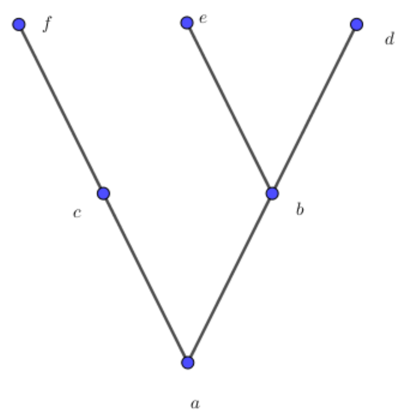


Figure 3.6: Linearly Ordered Set

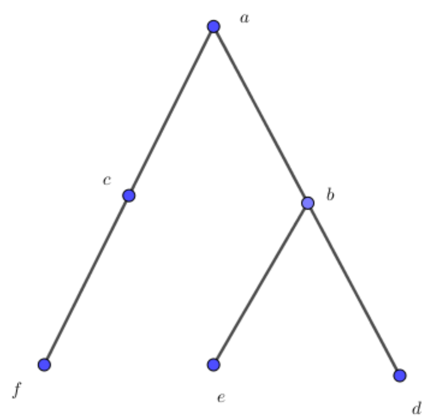
Remark. Hasse diagram of a finite linearly ordered set is always in the from of straight line as shown in the Figure 3.6.

That is, let $A = \{a, b, c, d, e, f\}$ be a finite linearly ordered set such that $a \leq b \leq c \ldots \leq f$. Then, its Hasse diagram is always in the from of straight line as shown in the Figure 3.6. In the next example, we will demonstrate the Hasse diagram of the poset $(A, \leq)$ and its dual $(A \geq)$.

Example 3.18. Let $(A, \leq)$ be a partially ordered set, where $A = \{a, b, c, d, e, f\}$ having some relation R, whose Hasse diagram is as follow:



Then, the dual poset $(A, \geq)$ is represented by the Hasse diagram:



In-text Exercise 3.2. 1. Consider the partial order of divisibility on the set A, that is, aRb if and only if a divides b. Draw the Hasse diagram of the given poset.

(a) $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$

(b) $A = \{2, 4, 8, 16, 32\}$

(c) $A = \{1, 2, 3, 5, 7, 11, 13\}$

2. Find the lexicographic ordering of the following:

   (a) $(1, 1, 2), (1, 2, 1)$

   (b) $(1, 2, 3, 4), (2, 3, 4, 5)$

   (c) Hi, Him.

3.7 Functions between Posets

In this section, we study the functions between two partially ordered sets. We will define the notion of isomorphism for the same.

Definition 3.8. Let $(A, \leq)$ and $(B, \leq')$ be two posets. Then a map $f\colon A \to B$ is called

1. an isotone or order preserving if whenever $x \leq y$, we have $f(x) \leq' f(y)$ for all $x, y \in A$
2. a poset homomorphism or order embedding if

$$x \leq y \text{ if and only if } f(x) \leq' f(y)$$

   for all $x, y \in A$;

3. a poset isomorphism if f is one-one, onto and poset homomorphism.

If $f\colon A \to B$ is an isomorphism, then we say that $(A, \leq)$ and $(B, \leq')$ are isomorphic posets.

For the cause of simplicity, we use the symbol $\leq$ for both the relations $\leq$ and $\leq'$.

In the next result, we will show that every poset homomorphism is always one-one.

Lemma 3.1. Every poset homomorphism is always one-one.

Proof. Let $f\colon A \to B$ be a poset homomorphism. Then, for $x, y \in A$, let

$$f(x) = f(y)$$

$\Rightarrow$ $f(x) \leq f(y)$ and $f(y) \leq f(x)$

$\Rightarrow$ $x \leq y$ and $y \leq x$.

$\Rightarrow$ $x = y$. Therefore, f is one-one. □

Remark. Every one-one function need not be poset homomorphism.

Example 3.19. Consider a set $A = \{0, 1\}$ with usual relation $\leq$. Then consider a map $f\colon A \to A$, defined as

$$f(0) = 1 \text{ and } f(1) = 0$$

Then, the map f is one-one (its actually bijective). But f is not a poset homomorphism as, we have $0 \leq 1$ but $f(0) = 1 \not\leq 0 = f(1)$.

Example 3.20. Let $A = \mathbb{Z}^+$ be the set of all positive integers and let $\leq$ be the usual less than or equal to partial order on A. Let B be the collection of all positive even numbers with $\leq$ usual partial order. Then consider the function $f\colon A \to B$ defined as

$$f(x) = 2x$$

Then, f is an isomorphism between A and B.

Solution. Here, we have to show the following:

1. f is one-one.

   Let $f(x) = f(y)$, that is, we have $2x = 2y$. Thus, we have $x = y$. Hence, we have f is one-one. Also, we have $Dom(f) = A$, therefore, f is everywhere defined.

2. f is onto.

   Let $c \in B$, that is, $c = 2m$ for some $m \in \mathbb{Z}^+$. Thus, we have $f(m) = 2m = c$. Hence f is onto.

3. f is poset homomorphism.

   Let $x, y \in A$ such that $x \leq y$. Therefore, we have $2x \leq 2y$. Hence we have $f(x) \leq f(y)$. Similarly, we have whenever $f(x) \leq f(y)$ implies that $x \leq y$. Hence, we have

   $$x \leq y \text{ if and only if } f(x) \leq f(y)$$

Therefore, f is a poset isomorphism.

Let $f\colon A \to B$ be a poset isomorphism from the poset $(A, \leq)$ to poset $(B, \leq')$. Let A' be a subset of A and let $f(A') = B'$ is the corresponding subset of B. Then, we have the following:

Theorem 3.5. Suppose the elements of A' have some property relating to other elements of A, and if this property is completely defined on $\leq$, then the elements of B' must possess exactly the same property with respect to $\leq'$.

Consider the Hasse diagram in the Figure 3.7, defined on a poset $(A, \leq)$, where $A = \{a, b, c, d\}$

Let $f\colon A \to B$ be a poset isomorphism. Then, from the Hasse diagram of A, we can notice that $a \leq x$ for all $x \in A$. Thus, the image of a, that is, $f(a)$ must be related to all the elements of $f(A)$, that is, $f(a) \leq' x$ for all $x \in f(A)$.

Also, we have $c \nleq d$ and $d \nleq c$ in A. Thus, we have $f(c) \nleq' f(d)$ and $f(d) \nleq' f(c)$. The pair of the kind c and d is called incomparable in A.

Note. Let $(A, \leq)$ and $(B, \leq')$ be two finite posets and let $f\colon A \to B$ be a bijective function. Let H be any Hasse diagram of $(A, \leq)$. Then, we have the following:

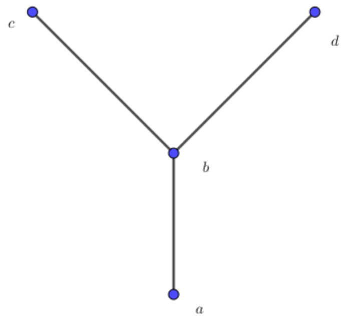


Figure 3.7: Hasse Diagram

1. If f is a poset isomorphism and if we replace each label a of H with $f(a)$, then the resultant Hasse diagram will be the Hasse diagram for $(B, \leq')$;
2. If H becomes a Hasse diagram for $(B, \leq')$, whenever each label a is replaced by $f(a)$. Then f is poset isomorphism.

Thus, for finite posets, isomorphism means the same shape.

Example 3.21. Let $A = \{1, 2, 3, 6\}$ with the partial order relation $\leq$ defined as $a \leq b$ if and only if a divides b. Let $B = \{a, b\}$ and $A' = \mathcal{P}(B)$ and let $\leq'$ be the set inclusion partial order relation on A'. Let us define a function $f\colon A \to A'$ as

$$f(1) = \emptyset, \quad f(2) = \{a\}, \quad f(3) = \{b\}, \quad f(6) = \{a, b\}$$

then,

1. f is one-one and onto;
2. f is everywhere defined.

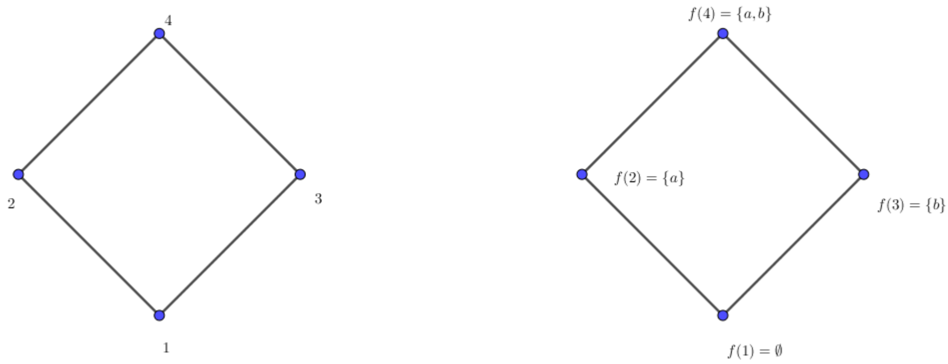


Figure 3.8: Poset Isomorphism

Also, if we replace each label $a \in A$ of the Hasse diagram of A is replaced by $f(a)$, we will get the Hasse diagram for A'. Hence, f is a poset isomorphism.

In-text Exercise 3.3. 1. Let $A = B = \mathbb{Z}$ with usual $\leq$. Check whether the given function f from A to B is poset isomorphism.

(a) $f(x) = -x$
(b) $f(x) = \frac{x}{2}$
(c) $f(x) = x^2$

3.8 Bounds of a POSETS

In this section, we will discuss about an algebraic structure which is connected with mathematical logic and partially ordered set. We will also discuss certain external properties of the elements of posets which lead us to define algebraic structure known as lattice.

3.8.1 Greatest and Least Element

If we consider the set of natural numbers and the elementary arithmetic operations, which are gcd and lcm of two numbers a and b, then one can notice that for every pair $a, b \in \mathbb{N}$, there always exists a number which divides both a and b, also called the greatest common divisor or $gcd(a, b)$ of a and b such that $gcd(a, b) \leq a$ as well as from b. Similarly, there is the least common multiple of a and b, such that $a \leq lcm(a, b)$ and $b \leq lcm(a, b)$. On the same line, we define the greatest and the least elements

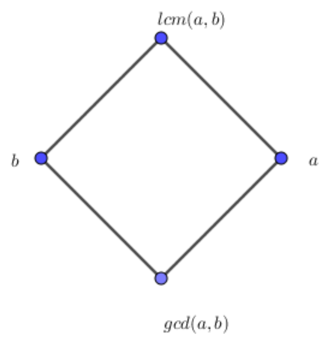


Figure 3.9: Greatest and the least element

for a partially ordered set.

Definition 3.9. Let $(A, \leq)$ be a partially ordered set. If

1. there exists an element $a \in A$ such that $x \leq a$ for all $x \in A$. Then $a \in A$ is called a greatest element or top element of A;

2. there exists an element $b \in A$ such that $b \leq x$ for all $x \in A$. Then $b \in A$ is called a least element or bottom element of A.

Greatest and least element of a poset $(A, \leq)$, if exist then, they will be unique and they will be comparable with all other elements of A. Therefore, now onwards we will use the least and the greatest element of A.
Consider the following examples:

Example 3.22. Let $A = \{a, b, c\}$. Then consider a poset $(\mathcal{P}(A), \subseteq)$, with the partial order, set inclusion. Let
$$L = \{\emptyset, \{1, 2\}, \{2\}, \{3\}\}$$
Then, $(L, \subseteq)$ is a poset and $\emptyset$ is the least element of L as $\emptyset \subseteq B$ for all $B \in L$. But L has no greatest element.

Example 3.23. Let us consider $M = \{\{2\}, \{3\}, \{1, 2\}, \{1, 2, 3\}\}$. Then $(M, \subseteq)$ is again a poset and $\{1, 2, 3\}$ is the greatest element of M, because $B \subseteq \{1, 2, 3\}$ for all $B \in M$. Here, M has no least element.

Example 3.24. Consider $N = \{\{2\}, \{3\}, \{1, 3\}\}$. Here, in the poset $(N, \subseteq)$ neither has the least element nor the greatest element.

Example 3.25. Consider $O = \{\emptyset, \{1\}, \{3\}, \{1, 3\}\}$. Then $(O, \subseteq)$ is a poset. Then O has both the greatest and the least elements, which are $\{1, 2, 3\}$ and $\emptyset$ respectively.

3.8.2 Maximal and Minimal Elements

Definition 3.10. Let $(A, \leq)$ be a poset. Then an element $a \in A$ is called a maximal element of A, if there does not exist any $x \in A$ such that $a < b$.

That is, a maximal element need not be comparable with all the elements of poset. Similarly, we have

Definition 3.11. Let $(A, \leq)$ be a poset. Then an element $b \in A$ is called a minimal element of A, if there does not exist any $x \in A$ such that $x < b$.

We already mentioned that the least and the greatest elements, if exist are always unique. That is, there is at the most one least and one greatest element.

Remark. But there may be none, one or more than one maximal and minimal element of a poset $(A, \leq)$.

Consider the Example 3.22, here the minimal element is $\emptyset$ but $\{3\}, \{1, 2\}$ both are maximal elements of $(L, \subseteq)$.

Note. Every greatest element is maximal and every least element is minimal.

Also, a minimal element need not be the least one and maximal element need not be the greatest element.

1. A poset $(A, \leq)$ may not have a maximal element. Consider the poset $(\mathbb{N}, \leq)$, with the usual less than or equal to relation. Then $(\mathbb{N}, \leq)$ has no maximal element.

2. Consider a set $A = \{2, 3, 4, 6, 7\}$ with the partial order "divisible", that is $a \leq b$ if and only if a divides b. Then $4, 6$ and 7 all are maximal elements. That is, $(A, \leq)$ has more than one maximal elements.
   We can also observe that $(A, \leq)$ has no greatest element. That is, a maximal element need not be the greatest element.

With the help of maximal element, we are in position to prove that the greatest element of a poset $(A, \leq)$ is unique, if it exists.

Result 3.1. The greatest element of a poset is always a maximal element and it is always unique, if exists.

Proof. Let $(A, \leq)$ be a poset. Let if possible, there exist two greatest element $a, b \in A$. Thus, from the definition, we have $x \leq a$ and $x \leq b$ for all $x \in A$. Since, $a, b \in A$. Thus, we have $a \leq b$ and $b \leq a$. Hence, by the anti-symmetric property, we have $a = b$. Thus, the greatest element is unique.

Now, we will show that every greatest element is a maximal element.
For, this, let $a \in A$ be the greatest element of A. Let if possible, a is not the maximal element of A. Then, there exists some $y \in A$ such that $a < y$, that is, we have $a \leq y$ but $a \neq y$. Since, a is the greatest element of A, thus, we have $y \leq a$. Hence, we have $a = y$. Hence, a is a maximal element of A. □

Similarly, we have the following result.

Result 3.2. The least element of a poset is always a minimal element and it is always unique, if exists.

Example 3.26. Let us consider $A = \{2, 3, 4, 6, 7\}$. Then consider a partial order relation $\leq$, define as $a \leq b$ if and only if a divides b. Here, minimal elements are $2, 3$ and 7. Because, there does not exist $a \in A$ such that $a \leq 2$, $a \leq 3$ and $a \leq 7$. Hence, there is no least element of this poset.

In the next result, we will provide a sufficient condition for the existence of maximal and minimal elements.

Theorem 3.6. Every non-empty finite subset of a poset $(A, \leq)$ has maximal and minimal elements.

Proof. Let $(A, \leq)$ be a poset and let $A = \{x_1, x_2, \ldots, x_n\}$ be a non-empty set. Let x_1 is a maximal element of A, then we are done.

If not, there must exist some $x_i \in A$ such that $x_1 < x_i$. If x_i is a maximal element of A, then we are done. If not, again, there exist some $x_j \in A$ such that $x_i < x_j$.

Continue like this, this process will end after a finite number of steps. Hence, we get some element $x \in A$, which is a maximal element.

On the similar lines, one can show that there exists minimal element of A as well. □

In the following, we define upper bound, lower bound, supremum and infimum of a poset, which is analogous to the respective concept in analysis.

Definition 3.12. Let $(A, \leq)$ be a partially ordered set and $B \subseteq A$. Then

1. $a \in A$ is called an upper bound of B if $x \leq a$ for all $x \in B$;
2. $a \in A$ is called a lower bound of B if $b \leq x$ for all $x \in B$;
3. The least upper bound of B, if it exists is called the supremum or the least upper bound of B and is denoted by $\sup B$;
4. The greatest lower bound of B, if it exists, is called the infimum or the greatest lower bound of B and it is denoted by $\inf B$.

Remark. The supremum and the infimum of a set B is always unique, if they exist. Also, the supremum and infimum of the set may or may not belong to the set.

Let $A = \mathbb{R}$ be the set of all real numbers with usual $\leq$. Then consider posets $(A, \leq)$ and $B = (0, 1) \subseteq A$. Then $\inf B = \{0\}$ and $\sup B = \{1\}$ which are not belong to B.

Again consider, $A = \mathbb{N}$, the set of natural numbers with usual $\leq$ relation. Then $(A, \leq)$ has the infimum element that is, $1 \in A$ but A has no supremum element in A.

Note.

1. There can be more than one upper bound (respectively, lower bound) of a set. But there will be at the most one supremum (respectively, infimum).
2. The greatest element of the set is always belongs to the set, whereas the supremum or upper bound of the set may lie outside of the set.
3. If the supremum of the set, lies in the set then it will be nothing but the greatest element of the set.

The following is an equivalent version of well ordering principle.

Theorem 3.7 (Zorn's Lemma). Let $(A, \leq)$ be a poset such that every chain of elements in A has an upper bound in A, then A has at least one maximal element.

From the above discussion, one can say that in general not every poset $(A, \leq)$ has sup or inf.

Example 3.27. Let us consider a poset $(A, \leq)$ with the Hasse diagram3.10.

1. Then $B = \{1, 2, 3\}$ is a subset of A and the upper bound of B are $5, 6, 10$ and 8 and the least upper bound of B is 5 as we have $5 \leq 6$, $5 \leq 8$ and $5 \leq 10$.

   Also, the lower bound of B is 1 only. Thus, it will be the infimum or the greatest lower bound of B.
2. Consider $C = \{8, 10\} \subseteq A$. Then, C has no upper bound in A. But has lower bounds, which are $1, 2, 3, 4, 5$ and 6. Here the infimum of C is 6.
3. Consider $D = \{1, 3, 4, 6\} \subseteq A$. Then the upper bounds of D are $6, 8$ and 10 and the supremum of D is 6. Also, the lower bound of D is only 1, which is the infimum of the set D.

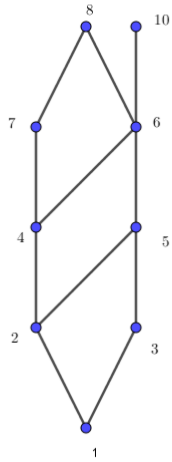


Figure 3.10: Poset $(A, \leq)$

In-text Exercise 3.4. 1. Let $A = \{2, 4, 6, 9, 12, 18, 27, 36, 48, 60, 72\}$ be a set and $\leq$ be a partial order relation defined as $a \leq b$ if and only if a divides b. Then find

- (a) maximal elements;
- (b) minimal elements;
- (c) the supremum of $B = \{2, 9\}$, if exists;
- (d) the infimum of $B = \{2, 9\}$, if exists;
- (e) the greatest and least element, if exist.

2. Give a poset that has

- (a) maximal element but no minimal element;
- (b) minimal element but no maximal element;
- (c) both maximal and minimal element;
- (d) neither a maximal, nor a minimal element.

3.9 Summary

In this chapter, we have covered the following:

1. A function f from A to B is a relation from A to B such that
   - (a) for all $a \in Dom(f)$, $f(a)$, the f-relative set of a is non-empty;
   - (b) for every $a \in Dom(f)$, f-relative set of a contains exactly one element of B.
2. Let A be a non-empty set. Then the identity function I_A on A is define as

$$I_A(a) = a \text{ for all } a \in A$$

3. A function f, define from A to B, is
   (a) onto if $Ran(f) = B$;
   (b) one-one if
   $$f(a) = f(b) \Rightarrow a = b$$
   (c) everywhere defined, if $Dom(f) = A$.
4. A function f is said to be invertible if its inverse relation f^{-1} is also a function;
5. If f and g be two invertible functions, such that $f \circ g$ exists. Then $f \circ g$ is also invertible and
   $$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$$
6. Let $(A, \leq)$ and $(B, \leq')$ be two posets. Then a map $f\colon A \to B$ is called
   (a) isotone if whenever $x \leq y$, we have $f(x) \leq' f(y)$, for all $x, y \in A$;
   (b) poset homomorphism if
   $$x \leq y \text{ if and only if } f(x) \leq' f(y)$$
   (c) poset isomorphism if f is one-one, onto and poset homomorphism.

3.10 Self-Assessment Exercise

1. Check, whether the given function f is one-one and onto
   (a) $f\colon \mathbb{N} \to \mathbb{Q}$ define as
   $$f(x) = \frac{x}{x+1}$$
   (b) $f\colon \mathbb{R}^+ \to \mathbb{R}$ define as
   $$f(x) = x^2$$
   (c) $f\colon A \to B$, where $A = \{1, 4, 9, 16\}$ and $B = \{1, 2, 3, 4\}$ and
   $$f(x) = \sqrt{x}, \text{ the positive square root of } x$$
2. Give an example of a function, which is
   (a) one-one but not onto;
   (b) onto but not one-one;
   (c) one-one and onto both;
   (d) neither one-one nor onto.
3. Show that if a function f is one-one then f^{-1} is also one-one, if exists.
4. Find the dual of the following posets

(a) $(\mathbb{Z}, \leq)$;

(b) $(\mathcal{P}(A), \supseteq)$;

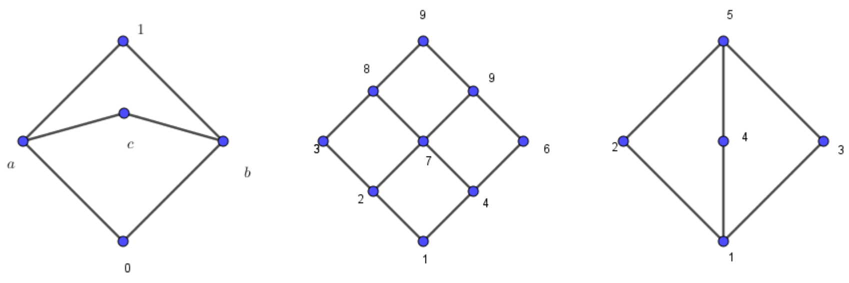
(c) $(\mathbb{Z}, \leq)$, where $a \leq b$ if and only if a divides b.

5. Let $A = B = \mathbb{Q}$, the set of rational numbers and $f\colon A \to B$ defined by

$$f(x) = x + 1.$$

Then, show that f is isotone. Also, check whether f is a poset homomorphism.

6. Check, whether the posets with the following Hasse diagrams are lattices.



(i) (ii) (iii)

3.11 Solutions to In-text Exercise

In-text Exercise 3. 1

1. (a) R is a function;
   (b) R is not a function as $R(a) = \{1, 2\}$, which is not singleton;
   (c) R is a function;
   (d) R is not a function as $R(a) = \{1, 2\}$.
2. Here R is a function as for each $a \in A$, $R(a)$ has at the most one element from B.
3. (a) 11;
   (b) 7;
   (c) $(x + 1)^2 + 2 = x^2 + 2x + 3$
   (d) $x^2 + 3$;
   (e) $x + 2$;
   (f) $(x + 2)^2 + 2 = x^2 + 2x + 6$
4. (a) f is not onto as $w \in B$, there does not exist any $x \in A$ such that $f(x) = w$.
   (b) f is not one-one as we have $f(a) = f(d) = x$ but $a \neq d$;
   (c) f is one-one and onto both;
   (d) f is not one-one as $f(1) = f(-1) = 1$ but $1 \neq -1$.

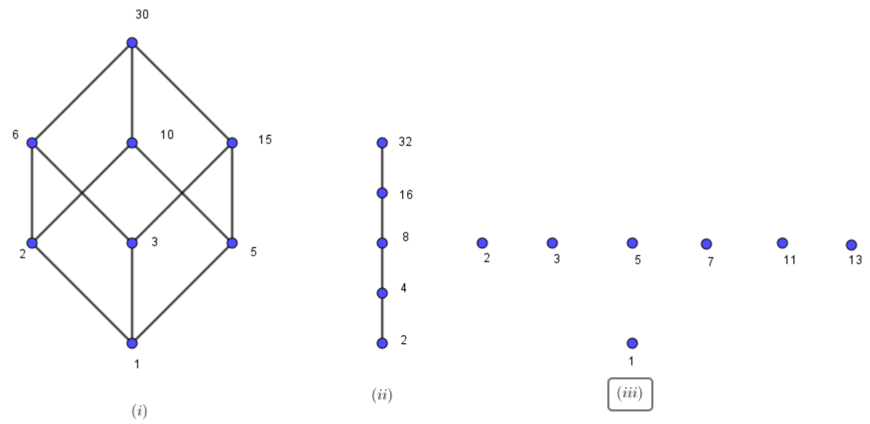


Figure 3.11: Hasse Diagram

5. (a) Here $f^{-1}(x) = \frac{3x+1}{2}$;
   (b) $f^{-1} = \{(3,1),(4,2),(1,3),(2,4),(5,5)\}$
6. Consider the function $f\colon \mathbb{N} \to A$ define as

$$f(x) = 2x$$

7. (a) f^{-1} is not a function;
   (b) f^{-1} is a function.

In-text Exercise 3. 2

1. See Figure 3.11
2. (a) $(1,1,2) \preceq (1,2,1)$
   (b) $(1,2,3,4) \preceq (2,3,4,5)$
   (c) Hi $\preceq$ Him

In-text Exercise 3. 3

1. (a) No, as $1 \leq 2$ but $f(1) = -1 \nleq -2 = f(2)$
   (b) Yes
   (c) No, as f is not one-one.

Unit Overview

This unit is devoted to basic introduction to lattices, its properties and its different types. We have kept the treatment of concepts as elementary as possible. We have carefully prepared the ground for students who will progress to study its computer science applications in future. Within lattice theory we have placed emphasis on sublattices, product of lattices and distributive lattices. The study of lattices combines algebraic, order-theoretic and graph-theoretic ideas to provide results which are linked to the partial ordered sets studied in the previous unit.

Chapter 1 provides a firm foundation for the concept of lattices as a special kind of partial ordered set as well as an algebraic structure. It further discusses sublattice of a lattice. In chapter 2, we studies product of lattices and isomorphism between lattices. Chapter 3 deals with two different types of lattices, namely distributive lattice and complemented lattice. Complemented distributive lattices will be studied extensively in the following unit.

Lattice theory has many applications in the field of computer science and concept analysis. The field of concept analysis has already made an impact on lattice theory and has a lot to offer to social scientists concerned with data analysis. Many of the topics covered are relevant to and have connections with computer science or information science. We will see many applications to the theory in the following unit.

Lesson - 4

Introduction to Lattices

Structure

4.1 Learning Objectives

After reading this lesson, the reader should be able:

- to understand the concept of lattices as a special kind of poset as well as an algebraic structure and equivalence between the two approaches.
- to identify lattices (both finite and infinite) among posets.
- to find join and meet of subsets of a lattice, when they exist.
- to recognise bounded lattices and find their bounds.
- to list sublattices of a lattice.

4.2 Introduction

The development of 'Lattice Theory' started in 1854, when George Boole (1815 - 1864) introduced an important class of algebraic structures in his publication 'Mathematical Analysis of Logic'. His goal was to find a mathematical model for human reasoning. In his honor these structures have been called Boolean algebras. They are special types of lattices. It was E. Schröder, who about 1890 considered the lattice concept in today's sense. Later in 1933-37, a series of articles were published by G. Birkhoff, Von Neumann, Ore etc. Their work showed that lattices have fundamental applications in modern algebra, projective geometry, point-set theory, functional analysis, and logic and probability. As a result of all this pioneer work, lattice theory was recognised as a substantial branch of modern algebra.

We have already seen partially ordered sets in the previous chapters. Many important properties of a partially ordered set P are expressed in terms of the existence of upper bounds and lower bounds of subsets of P. One of the most important classes of partially ordered sets defined in this way is lattices. Here we present some basic properties of such partially ordered sets, and also consider lattices as algebraic structures in a way that is reminiscent of the study of, for example, groups and rings.

4.3 Lattices as a POSET

Let us first recall definitions of least upper bound and greatest lower bound of a subset of a poset.

Definition 4.1. Let P be a poset and let $S \subseteq P$. An element $x \in P$ is an upper bound of S if $s \leq x$ for all $s \in S$. An element $y \in P$ is a lower bound of S if $y \leq s$ for all $s \in S$. The set of all upper bounds of S is denoted by S^u (read as 'S upper') and the set of all lower bounds of S is denoted by S^l (read as 'S lower'):

$$S^u := \{x \in P \mid s \leq x, \forall s \in S\} \qquad \text{and} \qquad S^l := \{y \in P \mid s \geq y, \forall s \in S\}.$$

Definition 4.2. Let P be a poset and let $S \subseteq P$. If S^u has a least element x, then x is called the least upper bound of S. Equivalently, x is the least upper bound of S if

(i) x is an upper bound of S

(ii) $x \leq y$ for all upper bounds y of S, i.e. if $s \leq y, \forall s \in S$, then $x \leq y$.

Definition 4.3. Let P be a poset and let $S \subseteq P$. If S^l has a greatest element x, then x is called the greatest lower bound of S. Equivalently, x is the greatest lower bound of S if

(i) x is a lower bound of S

(ii) $x \geq y$ for all lower bounds y of S, i.e. if $s \geq y, \forall s \in S$, then $x \geq y$.

Since least elements and greatest elements are unique, least upper bounds and greatest lower bounds are unique when they exist. The least upper bound of S is also called the supremum of S and is denoted by $\sup S$; the greatest lower bound of S is also called the infimum of S and is denoted by $\inf S$.

Remark. Recall from the previous chapter that the top and bottom elements of a poset P are denoted by $\top$ and $\bot$ respectively. If P has a top element, then $P^u = \{\top\}$ in which case $\sup P = \top$. When P has no top element, we have $P^u = \emptyset$ and hence $\sup P$ does not exist. Similarly, $\inf P = \bot$, if P has a bottom element.

Now we define the term 'Lattice'.

Definition 4.4. A lattice is a poset $(L, \leq)$ in which every subset $\{a, b\}$ consisting of two elements has a least upper bound and a greatest lower bound. We denote the least upper bound of $\{a, b\}$ by $a \vee b$ and call it the join of a and b. Similarly, we denote the greatest lower bound of $\{a, b\}$ by $a \wedge b$ and call it the meet of a and b.

4.3.1 Remarks on join($\vee$) and meet($\wedge$)

1. Let P be a poset. Let $x, y \in P$ such that $x \vee y$ and $x \wedge y$ exist in P, then $x \wedge y \leq x, y \leq x \vee y$. This holds because $x \wedge y$ is a lower bound of x and y while $x \vee y$ is an upper bound.

2. Let P be any poset. If x and y belongs to P and $x \leq y$, then y is the least upper bound of $\{x, y\}$ and x is the greatest lower bound of $\{x, y\}$. Thus whenever $x \leq y$, we have $x \vee y = y$ and $x \wedge y = x$. In particular, since $\leq$ is reflexive, we have $x \vee x = x$ and $x \wedge x = x$.

3. In a poset P, the least upper bound $x \vee y$ of $\{x, y\}$ may fail to exist for two different reasons:

   (a) x and y have no common upper bound, or

   (b) the set of upper bounds of $\{x, y\}$ has no least element.

   In Figure 4.1(i) the set $\{b, c\}$ has no upper bound because b and c has no common upper bound. Thus $\{b, c\}^u = \emptyset$ and hence $b \vee c$ does not exist. In (ii) we find that $\{c, d\}^u = \{a, b\}$ which has no least element as a and b are not comparable. Hence $c \vee d$ does not exist.

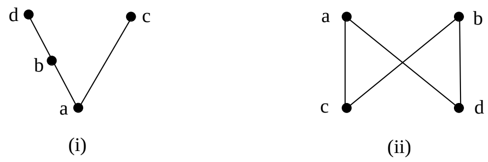


Figure 4.1:

4. Consider the poset shown in Figure 4.2. At first glance anybody would think that $a \vee b = e$, but on careful inspection we find that $\{a, b\}^u = \{d, e, f\}$. Since d and e are minimal elements of $\{d, e, f\}$ and $d \parallel e$, the set $\{d, e, f\}$ has no least element and hence $a \vee b$ does not exist.

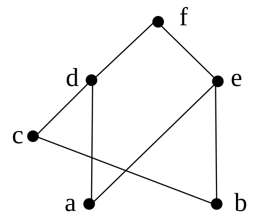


Figure 4.2:

5. Let P be a lattice. Then for all $a, b, c, d \in P$,

   (i) $a \leq b$ implies $a \vee c \leq b \vee c$ and $a \wedge c \leq b \wedge c$,

   (ii) $a \leq b$ and $c \leq d$ imply $a \vee c \leq b \vee d$ and $a \wedge c \leq b \wedge d$.

   Proof. (i) By the definition of join, we know that $b \leq b \vee c$ and $c \leq b \vee c$. By combining $a \leq b$ and $b \leq b \vee c$, using transitivity we get $a \leq b \vee c$. Thus, $b \vee c$ is an upper bound of $\{a, c\}$. Since $a \vee c$ is the least upper bound of $\{a, c\}$, therefore $a \vee c \leq b \vee c$.

   (ii) We know that $a \leq b \leq b \vee d$ and $c \leq d \leq b \vee d$. This implies that $b \vee d$ is an upper bound of $\{a, c\}$, since $a \vee c$ is the least upper bound of $\{a, c\}$ we get $a \vee c \leq b \vee d$.

   □

Example 4.1. Every chain is a lattice. Let P be a chain and let $x, y \in P$. Then either $x \leq y$ or $y \leq x$. If $x \leq y$, then $x \vee y = y$ and $x \wedge y = x$, and if $y \leq x$, then $x \vee y = x$ and $x \wedge y = y$. Hence P is a lattice.

Example 4.2. Let X be a set and let $L = \mathcal{P}(X)$, the power set of X. We have seen that inclusion relation, $\subseteq$, is a partial order relation on L. Let A and B belong to the poset $(L, \subseteq)$. Then $A \vee B$ is the set $A \cup B$ as $A \subseteq A \cup B$, $B \subseteq A \cup B$, and, if $A \subseteq C$ and $B \subseteq C$, then it follows that $A \cup B \subseteq C$. Similarly, we can show that the element $A \wedge B$ is the set $A \cap B$ in $(L, \subseteq)$. Thus, L is a lattice. Figure 4.3 shows Hasse diagram of $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$.

Example 4.3. Consider the poset $(Z^+, \leq)$, where for a and b in Z^+, $a \leq b$ if and only if $a \mid b$. Recall that k is the greatest common divisor of a and b if

- k divides both a and b (i.e., $k \leq a$ and $k \leq b$),
- if j divides both a and b, then j divides k (i.e., $j \leq k$ for all lower bounds j of $\{a, b\}$).

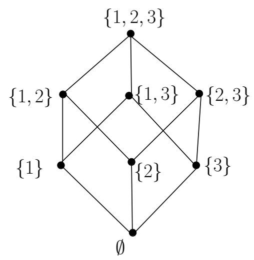


Figure 4.3:

Thus the greatest common divisor of a and b is precisely the meet of a and b in $(Z^+, \leq)$. Similarly, the join of a and b in $(Z^+, \leq)$ is given by their least common multiple. Thus $(Z^+, \leq)$ is a lattice in which

$$a \vee b = lcm(a, b) \qquad \text{and} \qquad a \wedge b = gcd(a, b).$$

Example 4.4. Let n be a positive integer and let D_n be the set of all positive divisors of n. Then D_n is a lattice under the divisibility relation as considered in Example 4.3. Thus, if $n = 18$, we have $D_{18} = \{1, 2, 3, 6, 9, 18\}$. The Hasse diagram of D_{18} is shown in Figure 4.4(i). If $n = 30$, we have $D_{30} = \{1, 2, 3, 5, 6, 10, 12, 18, 36\}$. The Hasse diagram of D_{30} is shown in Figure 4.4(ii).

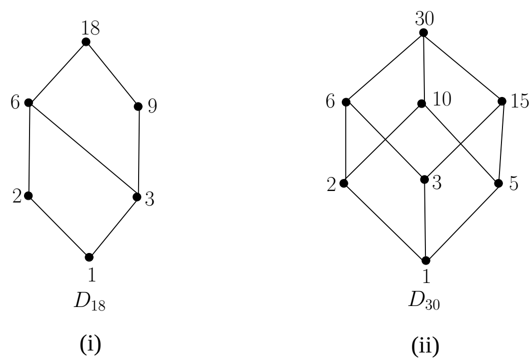


Figure 4.4:

Problem 4.1. Which of the following diagrams in Figure 4.5 represent lattices?

Solution. Hasse diagrams $(a), (b), (c)$ and (g) represent lattices. Diagram (d) does not represent a lattice because neither $b \vee c$ nor $d \wedge e$ exist. Diagram (e) does not represent a lattice because $e \vee f$ does not exist. Diagram (f) does not represent a lattice because $a \vee b$ does not exist.

In-text Exercise 4.1. 1. Draw the Hasse diagram of the poset $P = \{1, 2, 3, 4, 5, 6, 7\}$ under divisibility order. Find the join and meet, where they exist, of each of the following subsets of P. Either specify the join or meet or indicate why it fails to exist. Is P a lattice?

(i) $\{3\}$, (ii) $\{4, 6\}$, (iii) $\{2, 3\}$, (iv) $\{2, 3, 6\}$, (v) $\{1, 5\}$.

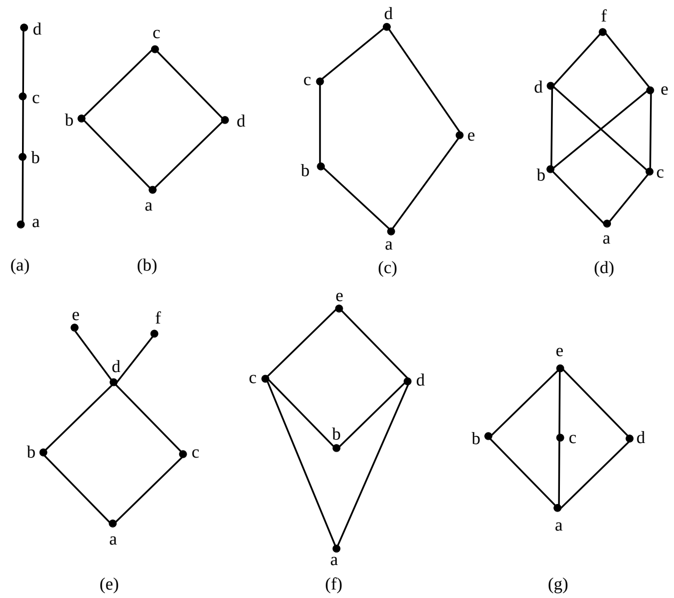


Figure 4.5:

4.4 Lattices as Algebraic Structures

In the last section we introduced lattices as posets of special type. In this section we view a lattice as an algebraic structure $(L, \wedge, \vee)$ and explore the properties of the binary operations $\vee$ and $\wedge$. We first amplify the connection between $\wedge, \vee$ and $\leq$. We prove this connection in the following lemma:

Lemma 4.1. (The Connecting Lemma): Let L be a lattice and let $a, b \in L$. Then the following are equivalent:

(i) $a \leq b$

(ii) $a \vee b = b$

(iii) $a \wedge b = a$.

Proof. It is shown in Section 4.3.1(2) that (i) implies both (ii) and (iii). Now we assume (ii) is true. Then b is an upper bound for $\{a, b\}$ and therefore $b \geq a$. Thus, (i) holds. Similarly, (iii) implies a is a lower bound of $\{a, b\}$ and therefore $a \leq b$ and hence (i) hold. $\square$

Definition 4.5. An (algebraic) lattice $(L, \wedge, \vee)$ is a set L with two binary operations $\wedge$ (meet) and $\vee$ (join) which satisfy the following laws for all $x, y, z \in L$:

$(L1)$ $x \wedge y = y \wedge x,$	$x \vee y = y \vee x,$
$(L2)$ $x \wedge (y \wedge z) = (x \wedge y) \wedge z,$	$x \vee (y \vee z) = (x \vee y) \vee z,$
$(L3)$ $x \wedge (x \vee y) = x,$	$x \vee (x \wedge y) = x,$
$(L4)$ $x \wedge x = x,$	$x \vee x = x.$

$(L1)$ is the commutative law, $(L2)$ is the associative law, $(L3)$ is the absorption law, and $(L4)$ is the idempotent law.

In the following theorem we will establish the equivalence of two definitions of lattices. We will do it in two steps.

Step 1: Consider a poset $(L, \leq)$. Define $\vee$ and $\wedge$ operations on L using supremum and infimum of elements as

$$a \vee b = \sup\{a, b\} \qquad \text{and} \qquad a \wedge b = \inf\{a, b\},$$

and show that these operations satisfy all four identities $(L_1) - (L_4)$ given in Definition 4.5, thus forming an algebraic lattice.

Step 2: Conversely, we begin with an algebraic lattice $(L, \vee, \wedge)$. We define a binary relation $\leq$ on L as

$$a \leq b \Leftrightarrow a \wedge b = a,$$

and show that it is a partial order relation on L, thus making $(L, \leq)$ a poset. We will further verify that supremum and infimum defined using this partial order relation agrees with the join and meet operations of the algebraic lattice $(L, \vee, \wedge)$, i.e.,

$$a \vee b = \sup\{a, b\} \qquad \text{and} \qquad a \wedge b = \inf\{a, b\}.$$

Theorem 4.1. (Equivalence of lattice as a poset and lattice as a algebraic structure)

(i) Let $(L, \leq)$ be a lattice ordered set. If we define

$$x \wedge y := \inf\ \{x, y\}, \qquad x \vee y := \sup\ \{x, y\},$$

then $(L, \wedge, \vee)$ is an algebraic lattice.

(ii) Let $(L, \wedge, \vee)$ be an algebraic lattice. If we define

$$x \leq y \Leftrightarrow x \wedge y = x,$$

then $(L, \leq)$ is a lattice ordered set.

Proof. .

(i) Let $(L, \leq)$ be a lattice ordered set. For all $x, y, z \in L$ we have:

$(L1)$ $x \wedge y = \inf\{x, y\} = \inf\{y, x\} = y \wedge x,$
$x \vee y = \sup\{x, y\} = \sup\{y, x\} = y \vee x.$

$(L2)$ $x \wedge (y \wedge z) = x \wedge \inf\{y, z\} = \inf\{x, \inf\{y, z\}\} = \inf\{x, y, z\}$
$= \inf\{\inf\{x, y\}, z\} = \inf\{x, y\} \wedge z = (x \wedge y) \wedge z,$
and similarly $x \vee (y \vee z) = (x \vee y) \vee z.$

$(L3)$ $x \wedge (x \vee y) = x \wedge \sup\{x, y\} = \inf\{x, \sup\{x, y\}\} = x,$
$x \vee (x \wedge y) = x \vee \inf\{x, y\} = \sup\{x, \inf\{x, y\}\} = x.$

$(L4)$ $x \wedge x = \inf\{x\} = x,$
$x \vee x = \sup\{x\} = x.$

(ii) Let $(L, \wedge, \vee)$ be an algebraic lattice. Clearly, for all x, y, z in L:

- $x \wedge x = x$ and $x \vee x = x$ by $(L4)$; so $x \leq x$, i.e., $\leq$ is reflexive.
- If $x \leq y$ and $y \leq x$, then $x \wedge y = x$ and $y \wedge x = y$, and by $(L1)$ $x \wedge y = y \wedge x$, so $x = y$, i.e., $\leq$ is antisymmetric.
- If $x \leq y$ and $y \leq z$, then $x \wedge y = x$ and $y \wedge z = y$. Therefore

$$x = x \wedge y = x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z,$$

so $x \leq z$ by $(L2)$, i.e., $\leq$ is transitive.

This proves $(L, \leq)$ is a poset.
Now, let $x, y \in L$. Then $x \wedge (x \vee y) = x$ implies $x \leq x \vee y$ and similarly $y \wedge (y \vee x) = y$ implies $y \leq x \vee y$. Thus, $x \vee y$ is an upper bound of $\{x, y\}$. Now let $z \in L$ be any upper bound of $\{x, y\}$. Then $x \leq z$ and $y \leq z$. This implies

$$\begin{aligned} (x \vee y) \vee z &= x \vee (y \vee z) \quad (by(L1)) \\ &= x \vee z \quad (\because y \leq z), \\ &= z \quad (\because x \leq z), \end{aligned}$$

Hence, $(x \vee y) \vee z = z$, and implies $x \vee y \leq z$. Thus $x \vee y$ is the least upper bound of $\{x, y\}$, i.e., $\sup\{x, y\} = x \vee y$. Similarly $\inf\{x, y\} = x \wedge y$. Hence $(L, \leq)$ is a lattice ordered set.

□

It follows from The Connecting Lemma that Theorem 4.1 yields a one-to-one relationship between lattice ordered sets and algebraic lattices. Therefore we shall use the term lattice for both concepts. We may henceforth say 'Let L be a lattice', replacing L by $(L, \leq)$ or by $(L, \wedge, \vee)$ if we want to emphasize that we are thinking of it as a special kind of poset or as an algebraic structure. The number of elements of L, denoted by $|L|$, is called the cardinality (or order) of the lattice L.

In a lattice L, associativity of $\wedge$ and $\vee$ allows us to write iterated joins and meets unambiguously without brackets. An easy induction shows that these correspond to sups and infs in the following way:

$$\bigvee\{a_1, a_2, ..., a_n\} = a_1 \vee a_2 \vee ... \vee a_n,$$

$$\bigwedge\{a_1, a_2, ..., a_n\} = a_1 \wedge a_2 \wedge ... \wedge a_n,$$

for $a_1, a_2, ..., a_n \in L (n \geq 1)$. Consequently, if F is a subset of a poset, then $\bigvee F$ and $\bigwedge F$ denote the supremum and infimum of F respectively, whenever they exist. We say that the supremum of F is the join of all elements and infimum is the meet of all elements of F.

4.5 Bounded Lattice

Definition 4.6. Let $(L, \wedge, \vee)$ be a lattice. We say that L has a one if there exists $1 \in L$ such that $a = a \wedge 1$ for all $a \in L$. Further, L is said to have zero if there exists $0 \in L$ such that $a = a \vee 0$ for all $a \in L$. A lattice $(L, \wedge, \vee)$ possessing 0 and 1 is called bounded.

Remark.

- The lattice $(L, \wedge, \vee)$ has a one if and only if $(L, \leq)$ has a top element $\top$ and, in that case, $1 = \top$. Similarly, the lattice $(L, \wedge, \vee)$ has a zero if and only if $(L, \leq)$ has a bottom element $\perp$ and, in that case, $0 = \perp$.
- In a lattice, zero and one elements, if exist, are unique.
- A finite lattice L is bounded, with $1 = \bigvee L$ and $0 = \bigwedge L$.

  Proof. Let $L = \{a_1, a_2, a_3, ..., a_n\}$. Let $b = \bigvee L = a_1 \vee a_2 \vee ... \vee a_n$. Then b is a unit element as $a_i \leq b$ for each i. Similarly, $\bigwedge L = a_1 \wedge a_2 \wedge ... \wedge a_n$ is a zero element of L. □

- If L is a bounded lattice, then for all $a \in L$, $0 \leq a \leq 1$ as

$$a \vee 0 = a, \quad a \wedge 0 = 0$$

$$a \vee 1 = 1, \quad a \wedge 1 = a.$$

Example 4.5. The lattice $\mathbb{N}$ under the partial order of divisibility is not a bounded lattice since it has a zero element, the number 1, but has no greatest element.

Example 4.6. The lattice $\mathbb{Z}$ under the usual partial order $\leq$ is not bounded since it has neither a zero element nor a one element.

Example 4.7. The lattice $\mathcal{P}(X)$ of all subsets of a set X, is bounded. Its one element is X and its zero element is $\emptyset$. In particular, the lattice $\mathcal{P}(\mathbb{N})$ is bounded with zero element as $\emptyset$ and one element as $\mathbb{N}$.

In-text Exercise 4.2.

1. Which of the following structures $(L, \leq)$ are lattices, lattices with a zero element, lattices with a unit element?
   (a) L is the set of all finite subsets of an infinite set A and $\leq$ is the inclusion relation $\subseteq$.
   (b) L_0 with inclusion relation $\subseteq$, where L_0 is a set of subsets of an infinite set A defined as follows:

$$L_0 := \{X \subseteq A \mid X \quad \text{finite}\} \cup A$$

(c) L is the set of all infinite subsets of an infinite set A and $\leq$ is inclusion relation.

(d) L is the set of all subsets of a set A containing a fixed subset, C, i.e., $L = \{X : C \subseteq X \subseteq A\}$ and $\leq$ is inclusion relation.

2. Which of the following is/are correct regarding lattices.

(a) $(\{1, 2, 3, 6, 9, 18\}, /)$ is a bounded lattice, where / is divisibility order.

(b) $(\mathbb{Z}, \leq)$ is a bounded lattice.

(c) $([0, 1], \leq)$ is a bounded lattice.

(d) $((0, 1), \leq)$ is a bounded lattice.

4.6 Sublattices

Definition 4.7. Let L be a lattice. A non-empty subset M of L is called a sublattice of L if it is closed with respect to $\vee$ and $\wedge$ of any two elements i.e., $a, b \in M \Rightarrow a \vee b \in M$ and $a \wedge b \in M$. The set of all sublattices of L is denoted by Sub L, and $\text{Sub}_0\ L = \text{Sub}\ L \cup \{\emptyset\}$.

Example 4.8. .

1. Any singleton subset of a lattice L is a sublattice of L.

2. Any non-empty chain in a lattice is a sublattice. Let M be a non-empty chain in a lattice L. Since M is a chain, for any $x, y \in M$, $x \vee y, x \wedge y \in M$, and hence a sublattice. Thus, when testing that a non-empty subset M is a sublattice, it is sufficient to consider non-comparable elements.

3. For any two elements x, y in a lattice L, the interval

$$[x, y] := \{a \in L \mid x \leq a \leq y\}$$

is a sublattice of L.

Proof. Let $a, b \in [x, y]$. Then $x \leq a \leq y$ and $x \leq b \leq y$. This implies that y is an upper bound of $\{a, b\}$. Since $a \vee b$ is the least upper bound of $\{a, b\}$, therefore $a \vee b \leq y$. Thus, $x \leq a \leq a \vee b \leq y$ implies that $a \vee b \in [x, y]$. Similarly, $a, b \in [x, y]$ implies that x is a lower bound of $\{a, b\}$ and since $a \wedge b$ is the greatest lower bound, therefore $x \leq a \wedge b$. Thus, $x \leq a \wedge b \leq a \leq y$ implies that $a \wedge b \in [x, y]$. Hence $[x, y]$ is a sublattice of L. □

4. The lattice D_n of all positive divisors of n is a sublattice of the lattice Z^+ under the partial relation of divisibility. It is straightforward as lcm and gcd of any two divisors of n is also a divisor of n and hence belong to D_n.

5. Consider the lattice $(\mathcal{P}(\mathbb{N}), \subseteq)$. Consider its subset M defined as $M := \{A \subseteq \mathbb{N} \mid A \quad \text{finite}\}$. Since union and intersection of finite subsets of $\mathbb{N}$ is a finite subset of $\mathbb{N}$, the set M is closed with respect to join and meet and hence is a sublattice of $(\mathcal{P}(\mathbb{N}), \subseteq)$.

6. Consider the lattice L and its subsets M, P and Q shown in Figure 4.6. The subset M is not a sublattice of L since $a \wedge b = 0 \notin M$. The subset P is also not a sublattice of L since $a \vee b = c \notin P$. The subset Q is a sublattice of L.

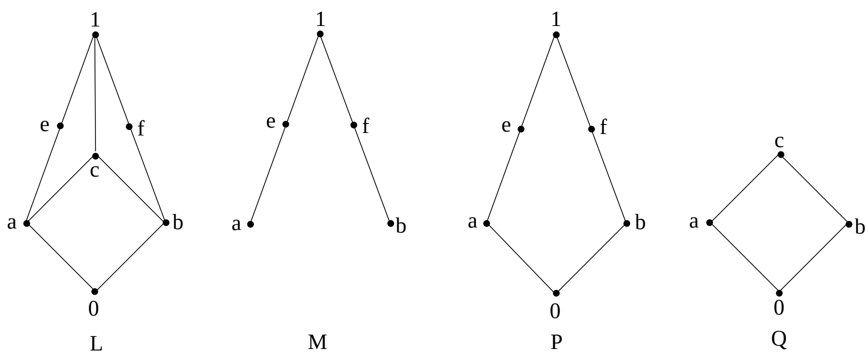


Figure 4.6:

7. A subset of a lattice $(L, \leq)$ may be a lattice in its own right without being a sublattice of $(L, \leq)$. For example consider the lattice $(L, \leq)$ and its subset P shown in Figure 4.6. Here $(P, \leq)$ is a lattice when considered as a poset itself, but it is not a sublattice of $(L, \leq)$, i.e., the operations $\vee_P$ and $\wedge_P$ are not the restrictions of the operations $\vee_L$ and $\wedge_L$.

8. The set of all sublattices of a lattice L forms a poset under inclusion relation and as discussed in Example 4.2, $(SubL, \subseteq)$ forms a lattice. Similarly, $(Sub_0\ L, \subseteq)$ also forms a lattice.

Problem 4.2. Let L be a lattice. Prove that the following are equivalent:

(i) L is a chain,

(ii) Every non-empty subset of L is a sublattice,

(iii) Every two-element subset of L is a sublattice.

Proof. (i) $\Rightarrow$ (ii) Let L be a chain and let M be a non-empty subset of L. We will show that M is closed with respect to join and meet. Let $x, y \in M$. Since L is a chain and $M \subseteq L$, therefore either $x \leq y$ or $x \geq y$. If $x \leq y$, then $x \vee y = y \in M$ and $x \wedge y = x \in M$, and if $x \geq y$, then $x \vee y = x \in M$ and $x \wedge y = y \in M$. Hence M is closed w.r.t join and meet and therefore is a sublattice of L.

(ii) $\Rightarrow$ (iii) This is automatically true as (iii) is a particular case of (ii).

(iii) ⇒ (i) Let $x, y \in L$ be any two elements. Let $M = \{x, y\}$. Then M is a two-element subset of L and therefore by (iii) is closed w.r.t. join and meet. This implies $x \vee y \in M$, i.e., $x \vee y$ is either x or y. If $x \vee y = x$, then $x \geq y$, and if $x \vee y = y$, then $x \leq y$. Thus any two elements in L are comparable and hence L is a chain. □

Problem 4.3. Consider the lattices L, M and N shown in Figure 4.7.

(i) Find L as a sublattice of M.

(ii) The shaded elements of N do not form a sublattices. Why?

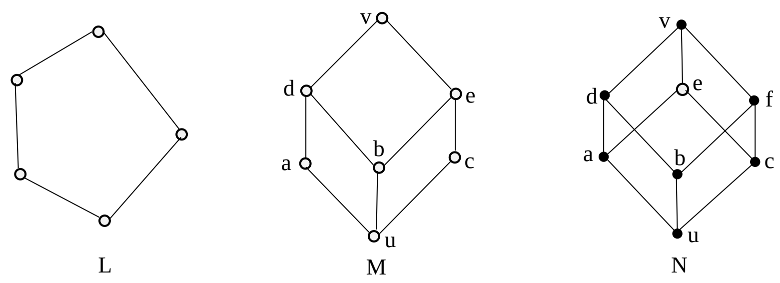


Figure 4.7:

Proof. (i) We need to find out a sublattice of M which is also isomorphic to L. The subset $\{u, a, d, v, c\}$ in M is a sublattice of M and is isomorphic to L. It is important to note here that subset $K = \{u, a, d, v, e\}$ in M is isomorphic to L but is not a sublattice of M as $d \wedge e = b \notin K$. Similarly, $\{u, b, d, v, c\}$ and $\{u, b, d, v, e\}$ are also not sublattices of M.

(ii) Let $M = \{u, a, b, c, d, f, v\}$ be the set of shaded elements of the lattice N. For $a, c \in M$, $a \vee c = e$ in N and $e \notin M$, therefore M is not closed w.r.t join and thus is not a sublattice of N.

□

Problem 4.4. Draw a labelled diagram of $(\text{Sub}_0 2^2, \subseteq)$.

Solution. The Figure 4.8 shows a labelled diagram of 2^2 and $(\text{Sub}_0 2^2, \subseteq)$. Here

$\text{Sub}_0 2^2 = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, c\}, \{c, d\}, \{a, b\}, \{b, d\}, \{a, b, d\}, \{a, c, d\}, \{a, b, c, d\}\}$.

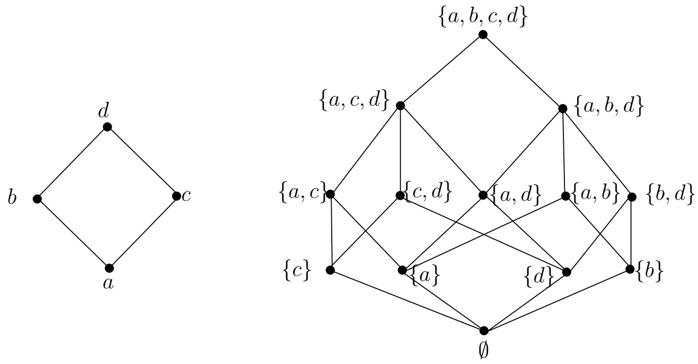
In-text Exercise 4.3. 1. Are the following statements true/false? Explain your answer.

(a) Every finite lattice is bounded.

(b) An infinite lattice can never be a bounded lattice.

(c) Sublattice of a bounded lattice is a bounded lattice.

(d) Every finite sublattice of a lattice is bounded.



2^2 $(\mathrm{Sub}_0 2^2, \subseteq)$

Figure 4.8:

(e) An unbounded lattice may have a bounded sublattice.

(f) If M is a bounded sublattice of a bounded lattice L, then the zero element of both L and M is the same.

(g) If M is a bounded sublattice of a bounded lattice L, then the one element of both L and M is the same.

2. List all the sublattices of the lattice shown in Figure 4.9.

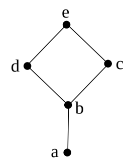


Figure 4.9:

4.7 Summary

In this chapter we have covered the following points:

1. A lattice is a poset $(L, \leq)$ in which every subset $\{a, b\}$ consisting of two elements has a least upper bound and a greatest lower bound.

2. The least upper bound of $\{a, b\}$ is denoted by $a \vee b$ and is called the join of a and b. The greatest lower bound of $\{a, b\}$ is denoted by $a \wedge b$ and is called the meet of a and b.

3. If L is a lattice. Then for all $a, b, c, d \in L$, the following hold:

   (a) $a \wedge b \leq a, b \leq a \vee b$.

   (b) $a \leq b$ implies $a \vee c \leq b \vee c$ and $a \wedge c \leq b \wedge c$.

(c) $a \leq b$ and $c \leq d$ imply $a \vee c \leq b \vee d$ and $a \wedge c \leq b \wedge d$.

4. Every chain is a lattice.

5. For any set X, $L = (\mathcal{P}(X); \subseteq)$ is a lattice. For $A, B \in L$, $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.

6. $L = (\mathbb{Z}^+; \leq)$ is a lattice where $a \leq b$ if and only if $a \mid b$. For $a, b \in (\mathbb{Z}^+; \leq)$, $a \wedge b = gcd(a, b)$ and $a \vee b = lcm(a, b)$.

7. Let L be a lattice. Then for all $a, b \in L$, $a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$. Therefore we may denote a lattice by $(L; \leq)$ OR by $(L; \wedge, \vee)$.

8. A lattice $(L, \wedge, \vee)$ is said to have one if there exists $1 \in L$ such that $a = a \wedge 1$ for all $a \in L$. Similarly, L is said to have zero if there exists $0 \in L$ such that $a = a \vee 0$ for all $a \in L$.

9. A lattice $(L, \wedge, \vee)$ possessing 0 and 1 is called bounded.

10. Every finite lattice has zero and one elements and therefore bounded.

11. An infinite lattice may be bounded or may not be bounded. $(\mathcal{P}(\mathbb{N}); \subseteq)$ and $(\mathbb{Z}; \leq)$ are examples of infinite bounded and not bounded lattices, respectively.

12. A non-empty subset M of a lattice L is called a sublattice of L if $a, b \in M \Rightarrow a \vee b \in M$ and $a \wedge b \in M$. The set of all sublattices of L is denoted by Sub L, and $\text{Sub}_0\ L = \text{Sub}\ L \cup \{\emptyset\}$.

13. Every single-element subset of a lattice is a sublattice. Every non-empty chain is a sublattice. Every interval in a lattice is a sublattice.

14. It is clear from the definition that every sublattice is a lattice. However, any subset of L which is a lattice need not be a sublattice. A subset of a lattice $(L, \leq)$ may be a lattice in its own right without being a sublattice of $(L, \leq)$. Such an example is given in Example 4.8(7).

4.8 Self Assessment Exercise

1.1 Give the Hasse diagram of all nonisomorphic lattices that have one, two, three, four, or five elements.

1.2 The poset $Q = \{1, 2, 4, 5, 6, 12, 20, 30, 60\}$ of $(\mathbb{N}_0; \preceq)$ is not a lattice. Draw a diagram of Q and find elements $a, b, c, d \in Q$ such that $a \vee b$ and $c \wedge d$ do not exist in Q.

1.3 Consider the poset of divisors of 30, D_{30}, under divisibility order. Is it a lattice? If the bottom element 1 and the top element 30 is deleted from D_{30}, is the result still a lattice? Explain.

1.4 Give an example of a poset P in which there are three elements a, b, c such that

(a) $\{x, y, z\}$ is an antichain,

(b) $x \vee y, y \vee z$ and $z \vee x$ fail to exist,

(c) $\bigvee\{x, y, z\}$ exists.

[Hint: P will have more than three elements.]

1.5 Consider the Hasse diagrams shown in Figure 4.10.

(a) Which of these posets are not lattices? Explain. [Hint: (i), (iii) and (iv) are not lattices. why?]

(b) Which of these posets are bounded lattices? Explain.

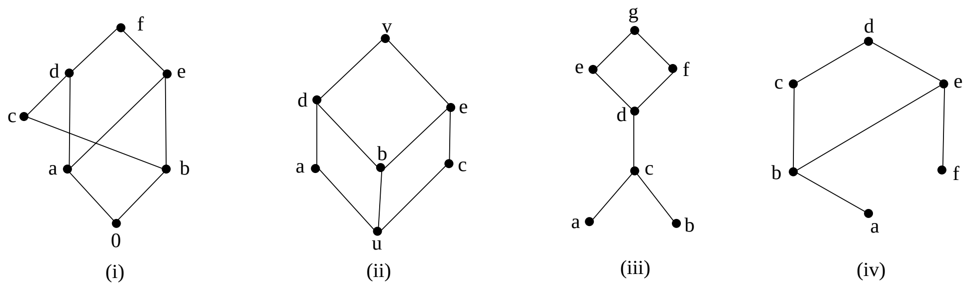


Figure 4.10:

1.6 Prove that any finite lattice is bounded. Give an example of a lattice without a zero and one element.

1.7 Prove that in a lattice $(L, \leq)$ every finite nonempty subset S has a least upper bound and a greatest lower bound.

1.8 Is $M := \{A \subseteq \mathbb{N} \mid A \quad \text{finite}\}$ a sublattice of $\mathcal{P}(\mathbb{N})$? Is M bounded? Is $\mathcal{P}(\mathbb{N})$ bounded?

1.9 Let $L = \mathcal{P}(S)$ be the lattice of all subsets of a set S under the inclusion relation. Let T be a non-empty subset of S. Show that $\mathcal{P}(T)$ is a sublattice of L.

1.10 Let L be a lattice and let $a, b \in L$. The interval $[a, b]$ is defined as the set of all $x \in L$ such that $a \leq x \leq b$. Prove that $[a, b]$ is a sublattice of L.

1.11 Show that a subset of a chain is a sublattice.

1.12 Find all sublattices of D_{24} that contain at least five elements.

1.13 Draw a labelled diagram of the lattice $(\text{Sub}_0 3, \subseteq)$.

4.9 Answers to In-Text Exercises

Excercise 1.1

1. The Hasse diagram of P is shown in Figure 4.11.

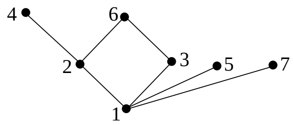


Figure 4.11:

   (i) $\wedge\{3\} = 3$, $\vee\{3\} = 3$
   (ii) $\{4,6\}^u = \emptyset$ and $\{4,6\}^l = \{1,2\}$, therefore $\vee\{4,6\}$ does not exist and $\wedge\{4,6\} = 1$.
   (iii) $\{2,3\}^u = \{6\}$ and $\{2,3\}^l = \{1\}$, therefore $\vee\{2,3\} = 6$ and $\wedge\{2,3\} = 1$.
   (iv) $\{2,3,6\}^u = \{6\}$ and $\{2,3,6\}^l = \{1\}$, therefore $\vee\{2,3,6\} = \{6\}$ and $\wedge\{2,3,6\} = \{1\}$.
   (v) $\{1,5\}^u = \{5\}$ and $\{1,5\}^l = \{1\}$, therefore $\vee\{1,5\} = \{5\}$ and $\wedge\{1,5\} = \{1\}$.

   Since $4 \vee 6$ does not exist, therefore P is not a lattice.

Excercise 1.2

1. (a) Lattice with zero element; empty set is the zero element.
   (b) Lattice with zero and one element; empty set is the zero element and A is one element.
   (c) May not be a lattice. Let $A = \mathbb{N}$, and $X = \{2n \mid n \in \mathbb{N}\}$ and $Y = \{2n+1 \mid n \in \mathbb{N}\}$. Then X and Y are two infinite subsets of A and $X \wedge Y = \emptyset \notin L$. Thus L is not a lattice.
   (d) Lattice with zero and one element; set C is the zero and A is the one element.

2. (a) True. Every finite lattice is bounded.
   (b) False. it has neither zero nor one element.
   (c) True. Integers 0 and 1 are zero and one elements.
   (d) False. It has neither zero nor one element.

Excercise 1.3

1. (a) True. If L is a finite lattice then $\bigvee L = 1$ and $\bigwedge L = 0$.
   (b) False. $(\mathcal{P}(\mathbb{N}), \subseteq)$ is an infinite lattice and $1 = \mathbb{N}$ and $0 = \emptyset$.

(c) False. $M = \{A \subseteq \mathbb{N} \mid A \quad \text{finite}\}$ is a sublattice of $L = (\mathcal{P}(\mathbb{N}), \subseteq)$. Lattice L is bounded while M has no one element.

(d) True. Since a sublattice is a lattice and every finite lattice is bounded.

(e) True. The lattice $L = (\mathbb{N}; \leq)$ is not bounded but $(\{1, 2\}; \leq)$ is a bounded sublattice of L.

(f) False. Let $L = \{0, 1, 2\}$ be a chain of length 3 and $M = \{1, 2\}$, then M is a sublattice of L. The zero element of M is 1 while zero element of L is 0.

(g) False. Let $L = \{0, 1, 2\}$ be a chain of length 3 and $M = \{0, 1\}$, then M is a sublattice of L. The one element of M is 1 while one element of L is 2.

2.

$$\begin{aligned}\text{Sub}L \;=\; & \{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \{a, b\}, \{b, d\}, \{b, c\}, \{d, e\}, \{c, e\}, \{a, d\}, \{a, c\}, \{b, e\}, \\ & \{a, e\}, \{a, b, d\}, \{a, b, c\}, \{a, b, e\}, \{b, d, e\}, \{b, c, e\}, \{a, b, d, e\}, \{a, b, c, e\}, \\ & \{b, d, c, e\}, \{a, b, c, d, e\}\}.\end{aligned}$$

4.10 References

[1]Davey, B. A., & Priestley, H. A. (2002). Introduction to lattices and order. Cambridge university press.

[2] Lidl, R., & Pilz, G. (2012). Applied abstract algebra. Springer Science & Business Media.

[3] Kolman, B., Busby, R. C., & Ross, S. (1995). Discrete mathematical structures. Prentice-Hall, Inc.

4.11 Suggested Readings

[1] Birkhoff, G. (1940). Lattice theory (Vol. 25). American Mathematical Soc.

[2] Grätzer, G. (2002). General lattice theory. Springer Science & Business Media.

Lesson - 5

Product and Isomorphism of Lattices

Structure

5.1 Learning Objectives

After reading this lesson, the reader should be able:

- to understand coordinate-wise product of lattices.
- to identify isomorphic copies of original lattices in the product of lattices.
- to understand isomorphism between lattices.
- to learn properties of lattices which retain under isomorphism and product of lattices.

5.2 Introduction

There are several different ways to join two lattices together and taking product is one of the ways. In this construction we require that the sets being joined are disjoint. There is no restriction on taking product of a lattice with itself as we can always take isomorphic copies of the original lattice which are disjoint. In this chapter we discuss the concept of product of lattices and the connection between the operations of the product with the operations of each coordinate of the product.

Further, we need to be able to recognize when two lattices are 'essentially the same' in the sense that either of the algebraic structure can be obtained from the other just by renaming of the elements. We define lattice isomorphism between two lattices. Two strictly weaker notions that relate to isomorphisms namely monomorphisms and endomorphisms are also being discussed. We also know that every lattice is a poset, therefore it is important to discuss relationships between order-isomorphisms and lattice-isomorphisms.

5.3 Product of Lattices

Theorem 5.1. Let $(L, \vee_1, \wedge_2)$ and $(K, \vee_2, \wedge_2)$ be lattices. Define $\vee$ and $\wedge$ coordinatewise on $L \times K$, as follows:

$$(l_1, k_1) \vee (l_2, k_2) = (l_1 \vee_1 l_2, k_1 \vee_2 k_2),$$

$$(l_1, k_1) \wedge (l_2, k_2) = (l_1 \wedge_1 l_2, k_1 \wedge_2 k_2).$$

Then $(L \times K, \vee, \wedge)$ is a lattice.

Proof. We will show that $\vee$ and $\wedge$ defined on $L \times K$ satisfy the identities $(L_1) - (L_4)$ given in Definition 4.5. We will prove it for join and urge the reader to prove similarly the identities for meet operation.

(L_1):

$$\begin{aligned} (l_1, k_1) \vee (l_2, k_2) &= (l_1 \vee_1 l_2, k_1 \vee_2 k_2) \text{ (by definition)} \\ &= (l_2 \vee_1 l_1, k_2 \vee_2 k_1) \text{ } (\because \vee_1 \text{ and } \vee_2 \text{ are commutative)} \\ &= (l_2, k_2) \vee (l_1, k_1) \text{ (by definition).} \end{aligned}$$

(L_2):

$$\begin{aligned} (l_1, k_1) \vee ((l_2, k_2) \vee (l_3, k_3)) &= (l_1, k_1) \vee (l_2 \vee_1 l_3, k_2 \vee_2 k_3) \text{ (by definition)} \\ &= (l_1 \vee_1 (l_2 \vee_1 l_3), k_1 \vee_2 (k_2 \vee_2 k_3)) \text{ (by definition)} \\ &= ((l_1 \vee_1 l_2) \vee_1 l_3, (k_1 \vee_2 k_2) \vee_2 k_3) \text{ } (\because \vee_1 \& \vee_2 \text{ are associative)} \\ &= (l_1 \vee_1 l_2, k_1 \vee_2 k_2) \vee (l_3, k_3) \text{ (by definition)} \\ &= ((l_1, k_1) \vee (l_2, k_2)) \vee (l_3, k_3) \text{ (by definition).} \end{aligned}$$

(L_3):

$$\begin{aligned}(l_1,k_1)\vee((l_1,k_1)\wedge(l_2,k_2)) &= (l_1,k_1)\vee(l_1\wedge_1 l_2, k_1\wedge_2 k_2) \ \ \text{(by definition)}\\ &= (l_1\vee_1(l_1\wedge_1 l_2), k_1\vee_2(k_1\wedge_2 k_2)) \ \ \text{(by definition)}\\ &= (l_1,k_1) \ \ (\because \text{ join and meet of } L \text{ and } K \text{ satisfy absorption law}).\end{aligned}$$

(L_4):

$$\begin{aligned}(l_1,k_1)\vee(l_1,k_1) &= (l_1\vee_1 l_1, k_1\vee_2 k_1)\\ &= (l_1,k_1) \ \ (\text{because } \vee_1 \text{ and } \vee_2 \text{ satisfy idempotent law}).\end{aligned}$$

Hence $(L\times K,\vee,\wedge)$ is a lattice. □

Definition 5.1. Let L and K be lattices. The set of ordered pairs

$$\{(x,y)\mid x\in L, y\in K\}$$

with operations $\vee$ and $\wedge$ defined by

$$(l_1,k_1)\vee(l_2,k_2)=(l_1\vee l_2, k_1\vee k_2),$$

$$(l_1,k_1)\wedge(l_2,k_2)=(l_1\wedge l_2, k_1\wedge k_2),$$

forms a lattice of product of L and K, denoted in symbols $L\times K$, and called the product lattice (or direct product of lattices L and K).

Remark. Let L and K be lattices. Then we know that L and K are also posets. In the previous chapters we have seen that product of posets is a poset with coordinate wise partial order relation. Now the lattice formed by the product poset, $L\times K$, of lattices L and K is the same as that obtained by defining $\vee$ and $\wedge$ coordinate-wise on $L\times K$.

Proof. Let L and K be lattices. Then by Theorem 5.1, $L\times K$ is a lattice. Now let $(l_1,k_1),(l_2,k_2)\in L\times K$.

$$\begin{aligned}(l_1,k_1)\vee(l_2,k_2)=(l_2,k_2) &\Leftrightarrow l_1\vee l_2=l_2 \ \text{ and } \ k_1\vee k_2=k_2\\ &\Leftrightarrow l_1\le l_2 \ \text{ and } \ k_1\le k_2\\ &\Leftrightarrow (l_1,k_1)\le(l_2,k_2).\end{aligned}$$

Therefore

$$\sup\{(l_1,k_1),(l_2,k_2)\}=(l_1,k_1)\vee(l_2,k_2), \ \text{ and}$$

$$\inf\{(l_1,k_1),(l_2,k_2)\}=(l_1,k_1)\wedge(l_2,k_2).$$

Therefore by the connecting lemma the two lattices are equivalent. Hence the proof. □

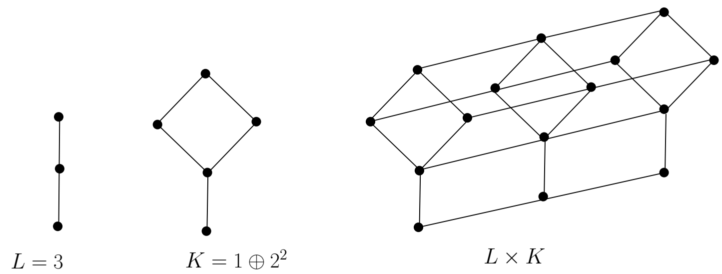


Figure 5.1:

The product of lattices can graphically be described in terms of the Hasse diagram. Figure 5.1 shows the product of the lattices $L = 3$ and $K = 1 \oplus 2^2$. One may notice that isomorphic copies of L and K sit inside $L \times K$ as the sublattices $L \times \{0\}$ and $\{0\} \times K$.

It is easy to verify that the product of lattices L and K always contains sublattices isomorphic to L and K, in fact $L \times K$ contains as many copies of sublattice isomorphic to K as many elements in L and as many copies of sublattice isomorphic to L as many elements in K. The product of more than two lattices or powers of a lattice are iteratively defined.

Problem 5.1. Let L and K be the finite chains $\{0, 1, 2\}$ and $\{0, 1\}$ respectively. Draw the Hasse diagram of the product lattice $L \times K \times K$.

Solution: The Hasse diagram of the product lattice $L \times K \times K$ is shown in Figure 5.2.

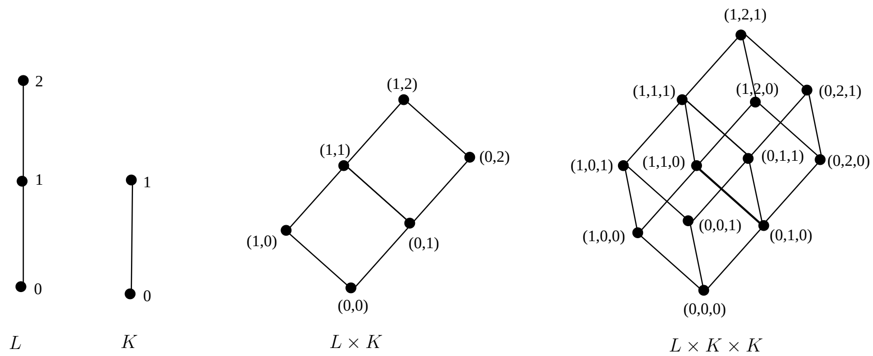


Figure 5.2:

In-text Exercise 5.1. 1. If L and K are chains of length 2, draw the Hasse diagram of $L \times K$ with the product partial order. Label all the elements of $L \times K$. Is $L \times K$ also a chain?

2. Which of the following statements are true or false? Explain your answer.

(a) Product of two lattices is a lattice.

(b) Product of two chains is a chain.

(c) If $\top_1$ and $\top_2$ are top elements for lattices L_1 and L_2, then $(\top_1, \top_2)$ is the top element for $L_1 \times L_2$.

(d) Product of bounded lattices need not be a bounded lattice.

5.4 Homomorphism of Lattices

From the viewpoint of lattices as algebraic structures it is natural to think of those maps between lattices which preserve the operations join and meet. Since lattices are also partially ordered sets, order-preserving maps are also available. We need to explore the relationship between these classes of maps. We begin with some definitions.

Definition 5.2. Let L and K be two lattices. A map $f : L \to K$ is said to be join-homomorphism if it is join-preserving, i.e.,

$$f(a \vee b) = f(a) \vee f(b), \qquad \forall a, b \in L.$$

Definition 5.3. Let L and K be two lattices. A map $f : L \to K$ is said to be meet-homomorphism if it is meet-preserving, i.e.,

$$f(a \wedge b) = f(a) \wedge f(b), \qquad \forall a, b \in L.$$

Definition 5.4. Let L and K be two lattices. A map $f : L \to K$ is said to be order-homomorphism if it is order-preserving, i.e.,

$$a \leq b \implies f(a) \leq f(b), \qquad \forall a, b \in L.$$

Definition 5.5. Let L and K be two lattices. A map $f : L \to K$ is said to be a lattice homomorphism if f is join-preserving and meet-preserving, i.e.,

$$f(a \vee b) = f(a) \vee f(b) \quad \text{and} \quad f(a \wedge b) = f(a) \wedge f(b), \qquad \forall a, b \in L.$$

In this case, $f(L)$ is called homomorphic image of L. An injective homomorphism is called monomorphism, and a surjective homomorphism is called epimorphism.

Theorem 5.2. Every join-homomorphism is an order-homomorphism.

Proof. Let L and K be two lattices. Let $f : L \to K$ be a join-homomorphism from L to K. Let $a, b \in L$ be such that $a \leq b$. We will show that $f(a) \leq f(b)$. Since $a \leq b$, Therefore by connecting lemma, $a \vee b = b$. Applying function f on it, we get $f(a \vee b) = f(b)$. Since f is a join-homomorphism, therefore $f(a \vee b) = f(a) \vee f(b)$. Thus, $f(a \vee b) = f(a) \vee f(b) = f(b)$ which again by connecting lemma implies that $f(a) \leq f(b)$. Hence f is an order-homomorphism. □

Theorem 5.3. Every meet-homomorphism is an order-homomorphism.

Proof. Let L and K be two lattices. Let $f : L \to K$ be a meet-homomorphism from L to K. Let $a, b \in L$ be such that $a \leq b$.

$$\begin{aligned} a \leq b \;&\Rightarrow\; a \wedge b = a \;\text{ (by connecting lemma)} \\ &\Rightarrow\; f(a \wedge b) = f(a) \;\; (\because f \text{ is well-defined}) \\ &\Rightarrow\; f(a) \wedge f(b) = f(a) \;\; (\because f \text{ is meet-preserving}) \\ &\Rightarrow\; f(a) \leq f(b) \;\text{ (by connecting lemma).} \end{aligned}$$

Hence, f is an order-preserving map. □

Remark. The converse of the Results 5.2, 5.3 are not true. Let L and K be the lattices with Hasse diagrams of Figure 5.3, respectively. We define

$$f : L \to K; \quad f(0_1) = 0_2, f(a_1) = f(b_1) = a_2, f(1_1) = 1_2.$$

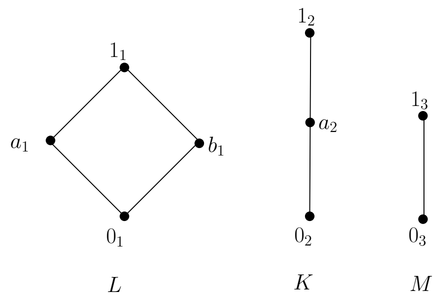


Figure 5.3:

The map f is an order-homomorphisms but f is neither a meet-homomorphism nor a join-homomorphism, since

$$f(a_1 \wedge b_1) = f(0_1) = 0_2 \quad \text{and} \quad f(a_1) \wedge f(b_1) = a_2 \wedge a_2 = a_2,$$

$$f(a_1 \vee b_1) = f(1_1) = 1_2 \quad \text{and} \quad f(a_1) \vee f(b_1) = a_2 \vee a_2 = a_2.$$

Remark. Every lattice-homomorphism is both a join-homomorphism and a meet-homomorphism by definition. A very natural question arises: Is every join-homomorphism is a lattice-homomorphism? Or we may re-phrase the same question as: Is every join-homomorphism a meet-homomorphism? Similarly we may ask is every meet-homomorphism a join-homomorphism? The answer to these questions are in negative. Consider the following examples. Let L and M be the lattices with Hasse diagrams of Figure 5.3, respectively. We define

$$g : L \to M; \quad g(0_1) = g(a_1) = g(b_1) = 0_3, g(1_1) = 1_3;$$
$$h : L \to M; \quad h(0_1) = 0_3, h(a_1) = h(b_1) = h(1_1) = 1_3.$$

The map g is a meet-homomorphism, since

$$g(a_1 \wedge b_1) = g(0_1) = 0_3 = g(a_1) \wedge g(b_1), \quad \text{etc.}$$

However, g is not a join-homomorphism, since

$$g(a_1 \vee b_1) = g(1_1) = 1_3 \quad \text{and} \quad g(a_1) \vee g(b_1) = 0_3 \vee 0_3 = 0_3.$$

Thus, g is not a lattice-homomorphism.

Similarly, h is a join-homomorphism but not a meet-homomorphism, since

$$h(a_1 \wedge b_1) = h(0_1) = 0_3 \quad \text{and} \quad h(a_1) \wedge h(b_1) = 1_3 \wedge 1_3 = 1_3.$$

Thus, h is not a lattice-homomorphism.

5.5 Isomorphism of Lattices

Definition 5.6. Let L and K be two lattices. A bijective lattice homomorphism $f : L \to K$ is called a lattice isomorphism. We say that L and K are isomorphic lattice and denote this by $L \cong K$.

Definition 5.7. Let L and K be two lattices. If $f : L \to K$ is a one-to-one homomorphism, then the sublattice $f(L)$ of K is isomorphic to L and we call f an embedding of L into K.

The relationship between the different homomorphisms is symbolized in Figure 5.4.

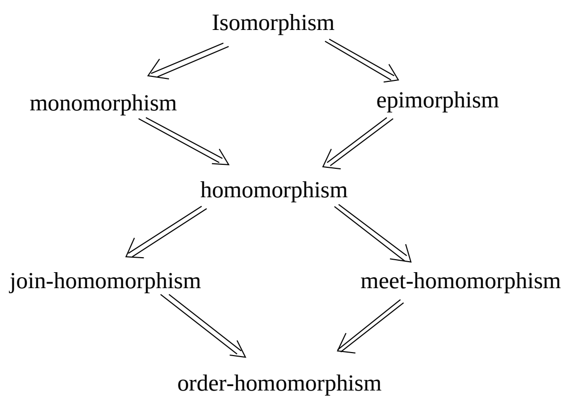


Figure 5.4:

In general, an order-homomorphism map may not be a lattice homomorphism. However such a demarcation dispute between order-isomorphism and lattice-isomorphism does not arise, as shown by the following theorem.

Theorem 5.4. Let L and K be lattices and let $f : L \to K$ be a map. f is a lattice isomorphism if and only if f is an order-isomorphism.

Proof. Assume that f is a lattice isomorphism. Then for $a, b \in L$, by connecting lemma,

$$a \leq b \Leftrightarrow a \vee b = b \Leftrightarrow f(a \vee b) = f(b) \Leftrightarrow f(a) \vee f(b) = f(b) \Leftrightarrow f(a) \leq f(b).$$

Thus, f is an order-embedding and hence is an order-isomorphism.
Conversely, assume that f is an order-isomorphism. Then f is a bijective map. To show that f is a lattice-isomorphism we will show that f is meet-preserving and join-preserving. Let $a, b \in L$. Since f is an order-isomorphism, therefore we have

$$a \leq a \vee b \quad \Rightarrow \quad f(a) \leq f(a \vee b) \tag{5.1}$$
$$b \leq a \vee b \quad \Rightarrow \quad f(b) \leq f(a \vee b) \tag{5.2}$$

(5.1) and (5.2) implies that $f(a \vee b)$ is an upper bound for $\{f(a), f(b)\}$ and therefore

$$f(a) \vee f(b) \leq f(a \vee b) \tag{5.3}$$

Now, since f is onto, therefore there exists $c \in L$ such that

$$f(a) \vee f(b) = f(c).$$

Then since $f(a) \leq f(c)$ and $f(b) \leq f(c)$, and f is an order isomorphism, we have $a \leq c$ and $b \leq c$. This implies $a \vee b \leq c$.

$$\Rightarrow f(a \vee b) \leq f(c) = f(a) \vee f(c). \tag{5.4}$$

Thus from Inequalities (5.3) and (5.4), we get

$$f(a \vee b) = f(a) \vee f(b).$$

This shows that f is a join-homomorphism.
Next, we will show that f is a meet-homomorphism. Since f is an order isomorphism, therefore for $a, b \in L$, we have

$$a \wedge b \leq a \quad \Rightarrow \quad f(a \wedge b) \leq f(a) \tag{5.5}$$
$$a \wedge b \leq b \quad \Rightarrow \quad f(a \wedge b) \leq f(b) \tag{5.6}$$

(5.5) and (5.6) implies that $f(a \wedge b)$ is a lower bound for $\{f(a), f(b)\}$ and therefore

$$f(a \vee b) \leq f(a) \wedge f(b). \tag{5.7}$$

Now, since f is onto, therefore there exists $d \in L$ such that

$$f(a) \wedge f(b) = f(d).$$

Then since $f(d) \leq f(a)$ and $f(d) \leq f(b)$, and f is an order isomorphism, we have $d \leq a$ and $d \leq b$. This implies $d \leq a \wedge b$.

$$\Rightarrow f(a) \wedge f(b) = f(d) \leq f(a \wedge b). \tag{5.8}$$

Thus from Inequalities (5.7) and (5.8), we get

$$f(a \wedge b) = f(a) \wedge f(b).$$

This shows that f is a meet-homomorphism and hence a lattice-isomorphism.

□

Result 5.1. Inverse of a lattice isomorphism is a lattice isomorphism.

Proof. Let L and K be lattices and let $f : L \to K$ be a lattice isomorphism. Since f is a bijective map, f^{-1} exists and is bijective. We will show that f^{-1} is meet and join preserving. Let $a, b \in K$. Then since f is surjective, there exist $c, d \in L$ such that $f(c) = a$ and $f(d) = b$. Then,

$$\begin{aligned} f^{-1}(a \vee b) &= f^{-1}(f(c) \vee f(d)) \\ &= f^{-1}(f(c \vee d)) \\ &= c \vee d \\ &= f^{-1}(a) \vee f^{-1}(b). \end{aligned}$$

Similarly,

$$\begin{aligned} f^{-1}(a \wedge b) &= f^{-1}(f(c) \wedge f(d)) \\ &= f^{-1}(f(c \wedge d)) \\ &= c \wedge d \\ &= f^{-1}(a) \wedge f^{-1}(b). \end{aligned}$$

Thus, f^{-1} is a lattice homomorphism from K to L. □

Remark.

1. We write $M \rightarrowtail L$ to indicate that the lattice L has a sublattice isomorphic to the lattice M. From the previous chapters it follows that, $M \rightarrowtail L$ implies $M \hookrightarrow L$.

2. For bounded lattices L and K it is often appropriate to consider homomorphisms $f : L \to K$ such that $f(0) = 0$ and $f(1) = 1$.

Problem 5.2. Let $f : L \to K$ be a lattice homomorphism.

(i) Show that if M is a sublattice of L, then $f(M)$ is a sublattice of K.

(ii) Show that if N is a sublattice of K, then $f^{-1}(N) \in Sub_0 L$.

Solution:.

(i) Let $f(a), f(b) \in f(M)$. Then since f is a lattice homomorphism and $M \in SubL$, we have
$$f(a) \vee f(b) = f(a \vee b) \in f(M).$$
Similarly,
$$f(a) \wedge f(b) = f(a \wedge b) \in f(M).$$
Thus, $f(M)$ is a sublattice of K.

(ii) Since f is not given to be surjective, $f^{-1}(N)$ may be empty and therefore belongs to Sub_0L. Now, let $f^{-1}(N)$ is non-empty and let $f^{-1}(a), f^{-1}(b)$ be any two elements in $f^{-1}(N)$. Then there exists $c, d \in L$ such that $f^{-1}(a) = c$ and $f^{-1}(b) = d$. Then,
$$\begin{aligned} f(c \vee d) &= f(c) \vee f(d) \\ &= f(f^{-1}(a)) \vee f(f^{-1}(b)) \\ &= a \vee b \\ \Rightarrow c \vee d &= f^{-1}(a \vee b). \end{aligned}$$
This implies $f^{-1}(a) \vee f^{-1}(b) = c \vee d = f^{-1}(a \vee b) \in f^{-1}(N)$.
Similarly, we can show that $f^{-1}(a) \wedge f^{-1}(b) = c \wedge d = f^{-1}(a \wedge b) \in f^{-1}(N)$. Thus, $f^{-1}(N)$ is a sublattice of L.

Problem 5.3. Let L and K be lattices and let $f : L \to K$ be a homomorphism. If M is a bounded sublattice of L, does it imply that $f(M)$ is a bounded sublattice of K.

Solution: By Problem 5.2(i), we know that if $M \in SubL$ then $f(M) \in SubK$. Now we will show that $f(M)$ is bounded. Let $f(M) = N$ and let 0_M and 1_M be zero and one element of M. We will show that $f(0_M) = 0_N$ and $f(1_M) = 1_N$.
Let $a \in N$. Then there exists $x \in M$ such that $f(x) = a$. Then,
$$\begin{aligned} f(0_M) \vee a &= f(0_M) \vee f(x) \\ &= f(0_M \vee x) \\ &= f(x) \\ &= a. \end{aligned}$$
Similarly, it can be shown that $f(1_M) \wedge a = a$ for all $a \in N$. Thus, $f(0_M) = 0_N$ and $f(1_M) = 1_N$, and hence $f(M)$ is a bounded sublattice of K.

In-text Exercise 5.2. 1. Show that D_6, the set of all divisors of 6, is isomorphic to 2×2.

2. Show that 2×2 and 4 are not isomorphic.

5.6 Summary

In this chapter we have covered the following points:

1. Let L and K be lattices. The set of ordered pairs

$$\{(x, y) \mid x \in L, y \in K\}$$

with operations $\vee$ and $\wedge$ defined by

$$(l_1, k_1) \vee (l_2, k_2) = (l_1 \vee l_2, k_1 \vee k_2),$$

$$(l_1, k_1) \wedge (l_2, k_2) = (l_1 \wedge l_2, k_1 \wedge k_2),$$

forms a lattice of product of L and K, denoted in symbols $L \times K$, and called the product lattice.

2. The product of lattices L and K always contains sublattices isomorphic to L and K, in fact $L \times K$ contains as many copies of sublattice isomorphic to K as many elements in L and as many copies of sublattice isomorphic to L as many elements in K.

3. Let L and K be two lattices. A map $f : L \to K$ is said to be a

   - join-homomorphism if it is join-preserving, i.e.,

   $$f(a \vee b) = f(a) \vee f(b), \qquad \forall a, b \in L.$$

   - meet-homomorphism if it is meet-preserving, i.e.,

   $$f(a \wedge b) = f(a) \wedge f(b), \qquad \forall a, b \in L.$$

   - order-homomorphism if it is order-preserving, i.e.,

   $$a \leq b \implies f(a) \leq f(b), \qquad \forall a, b \in L.$$

   - lattice homomorphism if f is join-preserving and meet-preserving, i.e.,

   $$f(a \vee b) = f(a) \vee f(b) \quad \text{and} \quad f(a \wedge b) = f(a) \wedge f(b), \qquad \forall a, b \in L.$$

   In this case, $f(L)$ is called homomorphic image of L.

4. An injective homomorphism is called monomorphism, and a surjective homomorphism is called epimorphism.

5. A bijective lattice homomorphism $f : L \to K$ is called a lattice isomorphism. We say that L and K are isomorphic lattice and denote this by $L \cong K$.

6. If $f : L \to K$ is a one-to-one lattice homomorphism, then the sublattice $f(L)$ of K is isomorphic to L and we call f an embedding of L into K.

7. Every join-homomorphism is an order-homomorphism. Every meet-homomorphism is anorder-homomorphism. The converse of these two statements are not true.

8. Every lattice-homomorphism is both join-homomorphism and meet-homomorphism. The converse of the statement is not true.

9. Let L and K be lattices and let $f : L \to K$ be a map. f is a lattice isomorphism if and only if f is an order-isomorphism.

10. Inverse and composition of lattice isomorphisms is lattice isomorphism.

11. Homomorphic image of a bounded lattice is bounded.

12. Lattice isomorphism preserves sublattices i.e., image of a sublattice under a lattice homomorphism is a sublattice.

5.7 Self Assessment Exercise

2.1 Draw the product of the lattices 3 and $2^2 \oplus 1$ and shade in elements which form a sublattice isomorphic to $1 \oplus (2 \times 3) \oplus 1$.

2.2 Show that composition of two lattice isomorphisms is a lattice isomorphism.

2.3 Draw the Hasse diagram of D_5 and D_6 and show that $D_5 \times D_6 \cong D_{30}$. Is it true for D_4 and D_6? Can we say that $D_4 \times D_6 \cong D_{24}$?

2.4 In which of the following cases is the map $\phi : L \to K$ (i) join-homomorphism, (ii) homomorphism?

(a) $L = K = (\mathbb{Z}; \leq)$, and $\phi(x) = x + 1$.

(b) $L = (\mathcal{P}(S); \subseteq)$ with $|S| > 1, K = 2$, and $\phi(U) = 1$ if $U \neq \emptyset$ and $\phi(\emptyset) = 0$.

(c) $L = (\mathcal{P}(S); \subseteq)$ with $|S| > 1, K = 2$, and $\phi(U) = 1$ if $U = S$ and $\phi(U) = 0$ if $U \neq S$.

(d) $L = (\mathcal{P}(S); \subseteq), K = 2$, and $\phi(U) = 1$ if $x \in U$ and $\phi(U) = 0$ otherwise (with $x \in S$ fixed).

(e) $L = K = (\mathbb{N}_0; \preceq)$ and $\phi(x) = nx$ (with $n \in \mathbb{N}_0$ fixed).

(f) $L = K = (\mathcal{P}(\mathbb{N}); \subseteq)$ and ϕ defined by

$$\phi(U) = \begin{cases} \{1\} & \text{if } \ 1 \in U, \\ \{2\} & \text{if } \quad 2 \in U \quad \text{and} \quad 1 \notin U, \\ \emptyset & \text{otherwise.} \end{cases}$$

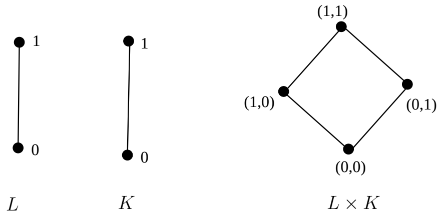


Figure 5.5:

5.8 Answers to In-Text Exercises

Excercise 2.1

1. The Hasse diagram of $L \times K$ is shown in Figure 5.5. No, it is not a chain as the element $(0, 1)$ is not comparable to $(1, 0)$ in $L \times K$.

2. (a) True.
   (b) False. An example is shown in the Exercise 6.
   (c) True. $(\top_1, \top_2) \geq (l_1, l_2)$ for each $(l_1, l_2) \in L_1 \times L_2$.
   (d) False. $(0_L, 0_K)$ is the zero element of $L \times K$ and $(1_L, 1_K)$ is the one element of $L \times K$.

Excercise 2.2

1. The Hasse diagram for D_6 and 2×2 are shown in Figure 5.6. We define a map

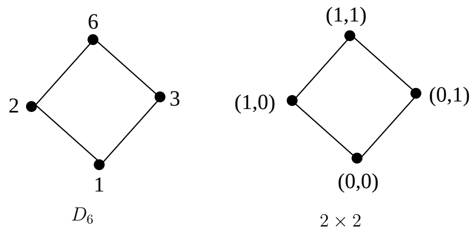


Figure 5.6:

   $f : D_6 \to 2 \times 2$ as

$$f(1) = (0, 0), f(2) = (1, 0), f(3) = (0, 1), f(6) = (1, 1).$$

   It is easy to verify that f is an isomorphism and hence $D_6 \cong 2 \times 2$.

2. 4 is a chain and every pair of elements in it is comparable while 2×2 is not a chain and has a pair of non-comparable elements. Thus, 4 is not isomorphic to 2×2.

5.9 References

[1]Davey, B. A., & Priestley, H. A. (2002). Introduction to lattices and order. Cambridge university press.

[2] Lidl, R., & Pilz, G. (2012). Applied abstract algebra. Springer Science & Business Media.

[3] Kolman, B., Busby, R. C., & Ross, S. (1995). Discrete mathematical structures. Prentice-Hall, Inc.

5.10 Suggested Readings

[1] Birkhoff, G. (1940). Lattice theory (Vol. 25). American Mathematical Soc.

[2] Grätzer, G. (2002). General lattice theory. Springer Science & Business Media.

Lesson - 6

Distributive and Complemented Lattices

Structure

6.1 Learning Objectives

After reading this lesson, the reader should be able:

- to define distributive lattices.
- to identify distributive and non-distributive lattices.
- to prove or disprove existence of a complement of an element in simple lattices.
- to check the uniqueness of complement of an element in a lattice.

6.2 Introduction

In previous chapters we began an exploration of the algebraic theory of lattices, along with many results on join ($\vee$) and meet ($\wedge$) to ensure that each lattice $(L; \vee, \wedge)$ arose from a lattice $(L; \leq)$ and vice-versa. Now we introduce identities linking join and meet which are not implied by the laws (L_1)-(L_4) defining lattices. These hold in many of our lattices, in particular in powersets. In the second part of the chapter we study a different feature of elements of lattices, namely the existence of complements. We study these special features with the aim of defining very 'rich' type of algebraic structure, Boolean algebras.

6.3 Distributive lattices

Definition 6.1. A lattice L is called distributive if for all $a, b, c \in L$ the following laws hold:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),$$
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

These equations are called distributive laws. A lattice which is not distributive is called nondistributive lattice.

Result 6.1. The two distributive laws given in Definition 6.1 are equivalent, i.e., If L is a lattice and $a, b, c \in L$, then the following are equivalent:

(i) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$;

(ii) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Proof. Firstly we assume (i) holds. Then, for $a, b, c \in L$,

$$\begin{aligned}
(a \wedge b) \vee (a \wedge c) &= ((a \wedge b) \vee a) \wedge ((a \wedge b) \vee c) && \text{(by (i))} \\
&= a \wedge (c \vee (a \wedge b)) && \text{(by absorption law and commutative law)} \\
&= a \wedge ((c \vee a) \wedge (c \vee b)) && \text{(by (i))} \\
&= (a \wedge (c \vee a)) \wedge (c \vee b) && \text{(by associativity)} \\
&= a \wedge (c \vee b) && \text{(by absorption law)} \\
&= a \wedge (b \vee c) && \text{(by commutativity)}
\end{aligned}$$

Thus, (i) implies (ii).

Next, we assume that (ii) holds. Then for $a, b, c \in L$, we have

$$\begin{aligned}
(a \vee b) \wedge (a \vee c) &= ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) && \text{(by (ii))} \\
&= a \vee (c \wedge (a \vee b)) && \text{(by absorption law and commutative law)} \\
&= a \vee ((c \wedge a) \vee (c \wedge b)) && \text{(by (ii))} \\
&= (a \vee (c \wedge a)) \vee (c \wedge b) && \text{(by associative law)} \\
&= a \vee (c \wedge b) && \text{(by absorption law)} \\
&= a \vee (b \wedge c) && \text{(by commutative law)}
\end{aligned}$$

Thus, (ii) implies (i). Hence the proof.

□

Remark. In view of the above result, if a lattice satisfy one of the distributive law then it will surely satisfy the other law too. Thus, to check for the distributivity of a lattice it is sufficient to check for one of the distributive laws. In other words, L is distributive if and only if one of the distributive laws holds.

Example 6.1. Any powerset lattice $(\mathcal{P}(X); \cup, \cap)$ is distributive as for any $A, B, C \in \mathcal{P}(X)$,

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

. In general, any lattice of sets is distributive. We know from the set theory that union and intersection satisfy distributive laws.

Example 6.2. The 'diamond lattice' M_3 and the 'pentagon lattice' N_5 shown in Figure 6.1 are not distributive.

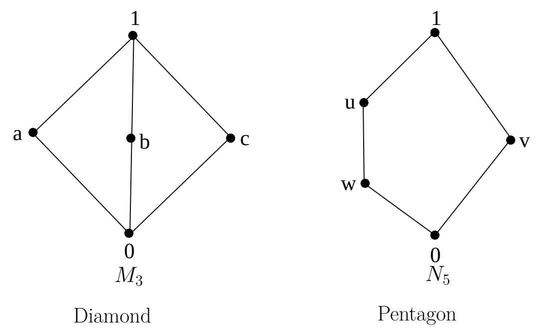


Figure 6.1:

To see this in M_5, note that

$$a \wedge (b \vee c) = a \wedge 1 = a \neq 0 = 0 \vee 0 = (a \wedge b) \vee (a \wedge c).$$

In N_5, we have

$$w \vee (u \wedge v) = w \vee 1 = 1 \neq u = u \wedge 1 = (w \vee u) \wedge (w \vee v).$$

Hence both M_3 and N_5 are not distributive.

These simple looking examples turn out to play a crucial role in the identification of nondistributive lattices as can be seen in the following theorem.

Theorem 6.1. A lattice is distributive if and only if it does not contain a sublattice isomorphic to the diamond or the pentagon.

A lattice which "contains" the diamond or the pentagon must clearly be nondistributive. The converse needs much more work and here we are omitting this proof. This is a powerful theorem and can be used quite efficiently by inspecting the Hasse diagram of a lattice. As an application of Theorem 6.1 we get the following corollary.

Corollary 6.1. Every chain is a distributive lattice.

Proof. Since a chain can never contain a diamond or a pentagon as a sublattice therefore by Theorem 6.1, a chain is a distributive lattice. □

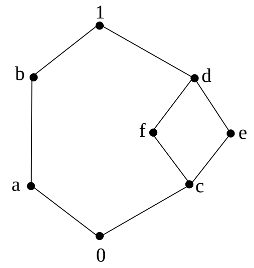


Figure 6.2:

Example 6.3. The lattice with Hasse diagram shown in Figure 6.2 cannot be distributive since it contains the pentagon $\{0, a, b, 1, e\}$ as a sublattice.

Example 6.4. The lattice with Hasse diagram shown in Figure 6.3 cannot be distributive since it contains the diamond $\{a, b, c, d, 1\}$ as a sublattice.

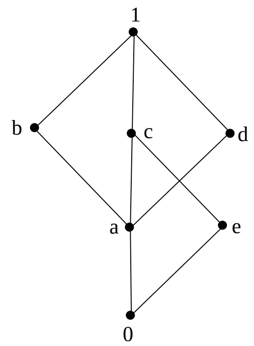


Figure 6.3:

Theorem 6.2. A lattice L is distributive if and only if the cancellation rule $x \wedge y = x \wedge z, x \vee y = x \vee z \Rightarrow y = z$ holds for all $x, y, z \in L$.

Proof. Let L be a distributive lattice and let $x, y, z \in L$ be such that $x \wedge y = x \wedge z, x \vee y = x \vee z$. We will show that $y = z$. Consider,

$$
\begin{aligned}
y &= y \wedge (x \vee y) && \text{(by absorption law)} \\
&= y \wedge (x \vee z) && (\because x \vee y = x \vee z) \\
&= (y \wedge x) \vee (y \wedge z) && \text{(by distributive law)} \\
&= (x \wedge y) \vee (y \wedge z) && \text{(by commutative law)} \\
&= (x \wedge z) \vee (y \wedge z) && (\because x \wedge y = x \wedge z) \\
&= (z \wedge x) \vee (z \wedge y) && \text{(by commutative law)} \\
&= z \wedge (x \vee y) && \text{(by distributive law)} \\
&= z \wedge (x \vee z) && (\because x \vee y = x \vee z) \\
&= z && \text{(by absorption law).}
\end{aligned}
$$

This proves the cancellation law.

Conversely, let lattice L satisfy cancellation law. We will show that L is distributive. On the contrary assume that L is not distributive. Then by Theorem 6.1, L has a sublattice isomorphic to either M_3 or N_5. We will discuss both cases one by one.

Case 1. L has a sublattice isomorphic to M_3.
Let $M_3 = \{0, a, b, c, 1\}$ as shown in the Hasse diagram in Figure 6.1. Then $a \vee b = a \vee c = 1$ and $a \wedge b = a \wedge c = 0$, but $b \neq c$. This shows that cancellation law fails in L, which is a contradiction to our assumption.

Case 2. L has a sublattice isomorphic to N_5.
Let $N_5 = \{0, u, v, w, 1\}$ as shown in the Hasse diagram in Figure 6.1. Then $v \vee u = v \vee w = 1$ and $v \wedge u = v \wedge w = 0$, but $u \neq w$. Thus, cancellation law fails in L, which is a contradiction.

By Case 1 and Case 2, we conclude that our assumption is wrong. Thus, L has no sublattice isomorphic to N_5 or M_3 and hence is distributive. □

The above theorem provides another useful tool to test distributivity of a lattice. We get the following corollary as a consequence of the above theorem.

Corollary 6.2. The lattice $L = (\mathbb{N}, gcd, lcm)$ is a distributive lattice.

Proof. Let $a, b, c \in \mathbb{N}$ be such that $lcm(a, b) = lcm(a, c)$ and $gcd(a, b) = gcd(a, c)$. Then $b = c$ and cancellation law holds. Thus, L is distributive. □

We know that new lattices can be manufactured by forming sublattices, products and homomorphic images. In the following results we will see that distributivity is preserved by these constructions.

Result 6.2. Every sublattice of a distributive lattice is distributive.

Proof. Let L be a distributive lattice and let M be a sublattice of L. Assume that M is not distributive. Then there exist $a, b, c \in M$ such that $a \wedge_M (b \vee_M c) \neq (a \wedge_M b) \vee_M (a \wedge_M c)$ in M. Since M is a sublattice of L, join $(\vee_M)$ and meet $(\wedge_M)$ in M is restriction of the join $(\vee_L)$ and meet $(\wedge_L)$ in L. Therefore, $a \wedge_L (b \vee_L c) \neq (a \wedge_L b) \vee_L (a \wedge_L c)$, which is a contradiction to the fact that L is distributive. Thus, our assumption is wrong. Hence M is distributive.

□

Result 6.3. If L and K are distributive, then $L \times K$ is distributive.

Proof. Let $(l_1, k_1), (l_2, k_2), (l_3, k_3) \in L \times K$. We will show that these elements satisfy distributive law.
Consider,

$$(l_1, k_1) \wedge ((l_2, k_2) \vee (l_3, k_3))$$

$$
\begin{aligned}
&= (l_1, k_1) \wedge (l_2 \vee l_3, k_2 \vee k_3) && \text{(by def of } \vee \text{ in product)}\\
&= (l_1 \wedge (l_2 \vee l_3), k_1 \wedge (k_2 \vee k_3)) && \text{(by def of } \wedge \text{ in product)}\\
&= ((l_1 \wedge l_2) \vee (l_1 \wedge l_3), (k_1 \wedge k_2) \vee (k_1 \wedge k_3)) && (\because L \text{ and } K \text{ are distributive})\\
&= (l_1 \wedge l_2, k_1 \wedge k_2) \vee (l_1 \wedge l_3, k_1 \wedge k_3) && \text{(by def of } \vee \text{ in product)}\\
&= ((l_1, k_1) \wedge (l_2, k_2)) \vee ((l_1, k_1) \wedge (l_1, k_3)) && \text{(by def of } \wedge \text{ in product)}
\end{aligned}
$$

Since $(l_1, k_1), (l_2, k_2), (l_3, k_3)$ are arbitrary elements in $L \times K$, this proves the distributive law in $L \times K$. Hence $L \times K$ is distributive.

□

Result 6.4. If L is a distributive lattice and K is the image of L under a homomorphism, then K is distributive. In other words, homomorphic image of a distributive lattice is distributive.

Proof. Let $f : L \to K$ be a lattice-homomorphism. Let $x, y, z \in K$. Since K is image of L under f, therefore there exist $a, b, c \in L$ such that $f(a) = x, f(b) = y$ and $f(c) = z$. Consider,

$$
\begin{aligned}
x \wedge (y \vee z) &= f(a) \wedge (f(b) \vee f(c)) &&\\
&= f(a) \wedge (f(b \vee c)) && (f \text{ is join-homomorphism})\\
&= f(a \wedge (b \vee c)) && (f \text{ is meet-homomorphism})\\
&= f((a \wedge b) \vee (a \wedge c)) && \text{(L is distributive)}\\
&= f(a \wedge b) \vee f(a \wedge c) && (f \text{ is join-homomorphism})\\
&= (f(a) \wedge f(b)) \vee (f(a) \wedge f(c)) && (f \text{ is meet-homomorphism})\\
&= (x \wedge y) \vee (x \wedge z)
\end{aligned}
$$

Hence K is distributive.

□

A particularly useful consequence of the above results may be presented as a single proposition as follows:

Proposition 6.1. If a lattice is isomorphic to a sublattice of a product of distributive lattices, then it is distributive.

Example 6.5. Consider Figure 6.4. The lattice L_1 is a sublattice of 3×3. Since 3×3 is distributive therefore L_1 is a distributive.

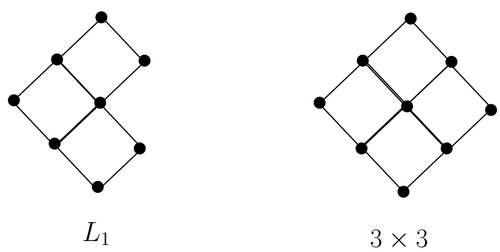


Figure 6.4:

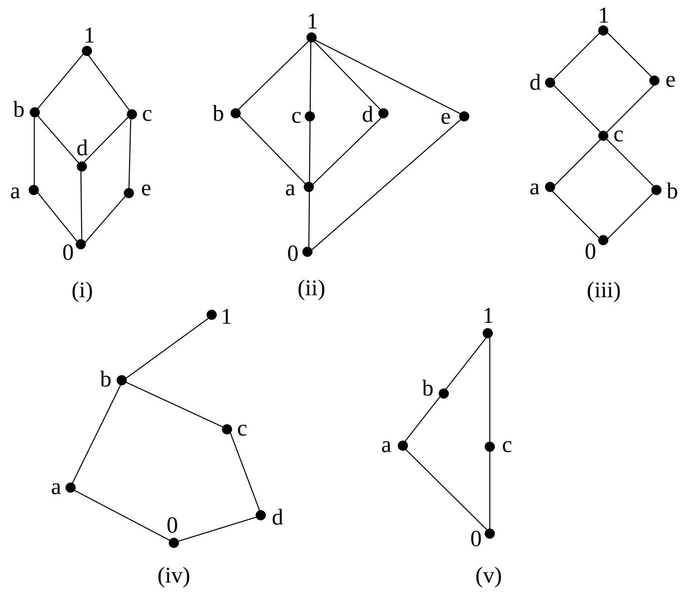


Figure 6.5:

Problem 6.1. Which of the lattices of Figure 6.5 are distributive. Use Theorem 6.1 and Proposition 6.1 to justify the answer.

Solution. (i) It has a sublattice $\{0, a, b, 1, e\}$ isomorphic to N_5 and therefore by Theorem 6.1 it is not distributive.

(ii) It has a sublattice $\{a, b, c, d, 1\}$ isomorphic to M_3, therefore by Theorem 6.1 it is not distributive.

(iii) It is a sublattice of 3×3. Since each chain is distributive and product of distributive is distributive, therefore, 3×3 is distributive. Thus, the given lattice being a sublattice of distributive is distributive.

(iv) It has a sublattice $\{0, a, b, c, d\}$ isomorphic to N_5 and therefore it is not distributive.

(v) The given lattice itself is isomorphic to N_5 and therefore not distributive.

In-text Exercise 6.1. 1. Is (D_{12}, gcd, lcm) a distributive lattice, where D_{12} is the set of all divisors of 12?

2. Which of the lattices of Figure 6.6 are distributive lattices?

6.4 Complemented Lattices

Definition 6.2. A lattice L with 0 and 1 is called complemented if for each $x \in L$ there is at least one element y such that $x \wedge y = 0$ and $x \vee y = 1$. Each such y is called a complement of x.

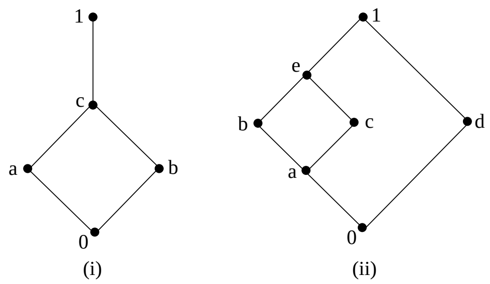


Figure 6.6:

Example 6.6. The lattice $L = \mathcal{P}(X)$ is such that every element has a complement, since if $A \in L$, then its set complement $\bar{A} = X - A$ has the properties $A \vee \bar{A} = X$ and $A \wedge \bar{A} = \emptyset$. That is, the set complement of A is also the complement of A in the lattice L. Also, it is important to notice that complement in L is uniquely determined by set-complement.

Example 6.7. In a bounded lattice, 1 is a complement of 0 and 0 is a complement of 1.

Example 6.8. Not every lattice with 0 and 1 is complemented. For instance, in a chain with three elements, $\{0, a, 1\}$, $0 < a < 1$, a does not have a complement. In fact, every chain with more than two elements is not complemented, as none of the elements in a chain other than 0 and 1 has complements.

Example 6.9. A complement need not be unique. Consider the diamond lattice M_3 shown in Figure 6.1. The element a in the diamond has two complements b and c, as $a \vee b = 1$ and $a \wedge b = 0$, and $a \vee c = 1$ and $a \wedge c = 0$. Similarly, the element b has two complements, a and c, and c has two complements, a and b.

Example 6.10. Consider the lattices D_{18} and D_{30} discussed in Example ?? and shown in Figure 4.4. Observe that every element in D_{30} has a unique complement. For example, 2 is a complement of 15, 10 is a complement of 3 and 5 is a complement of 6. However, the elements 3 and 6 in D_{18} have no complements.

Theorem 6.3. If L is a distributive lattice, then each $x \in L$ has at most one complement.

Proof. Suppose $x \in L$ has two complements y_1 and y_2. Then $x \vee y_1 = 0 = x \vee y_2$ and $x \wedge y_1 = 0 = x \wedge y_2$. Since L is distributive, therefore by cancellation law $y_1 = y_2$. Hence the proof. □

Remark. In a non-distributive lattice L, an element may have more than one complement. For example, in both M_3 and N_5 there are elements having more than one complement.

Definition 6.3. In a complemented distributive lattice L, each element $x \in L$ has a unique complement. We denote this complement of x by x'.

Complemented distributive lattices will be studied extensively in the following chapters.

Problem 6.2. Which of the lattices shown in Figure 6.5 are complemented?

Solution. (i) In this lattice, 1 and 0 are complements of each other, a and c are complements of each other, and b and e are complements of each other. The element d has no complement and therefore the lattice is not complemented.

(ii) In this lattice 1 and 0 are complements of each other, elements b, c, d and e are complements of each other. The element a has no complement and hence the lattice is not complemented.

(iii) In this lattice, no element other than 0 and 1 has a complement and therefore it is not complemented.

(iv) In this lattice, no element other than 0 and 1 has a complement and therefore it is not complemented.

(v) In this lattice, the element c is complement of a and b, and vice-versa. Hence it is complemented.

In-text Exercise 6.2. 1. Which of the following statements are true/false? Explain your answers.

(a) Every sublattice of a complemented lattice is complemented.

(b) Every homomorphic image of a complemented lattice is complemented.

(c) Product of two complemented lattices is complemented.

(d) If L and M are isomorphic lattices and L is complemented, then M is also complemented.

2. Which of the lattices of Figure 6.6 are complemented?

6.5 Summary

In this chapter we have covered the following points:

1. A lattice L is called distributive if for all $a, b, c \in L$ the following distributive laws hold:
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),$$
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

2. A lattice which is not distributive is called nondistributive lattice.

3. In a lattice, the two distributive laws are equivalent. Thus, if a lattice satisfy one of the distributive law then it will surely satisfy the other law too.

4. Every powerset lattice $(\mathcal{P}(X); \cap; \cup)$ is distributive.

5. Every chain is a distributive lattice.

6. The lattice $(\mathbb{N}; gcd, lcm)$ is distributive.

7. The diamond lattice M_3 and pentagon lattice N_5 are not distributive.

8. A lattice L is distributive if and only if L does not have any sublattice isomorphic to M_3 or N_5.

9. A lattice L is distributive if and only cancellation law, $a \vee b = a \vee c$ and $a \wedge b = a \wedge c \Rightarrow b = c$, holds for all $a, b, c \in L$.

10. Every sublattice of a distributive lattice is distributive.

11. Product of distributive lattices is distributive.

12. Homomorphic image of distributive lattices is distributive.

13. If a lattice is isomorphic to a sublattice of a product of distributive lattices, then it is distributive.

14. A bounded lattice L is called complemented if for each $x \in L$ there is at least one element y such that $x \wedge y = 0$ and $x \vee y = 1$. Each such y is called a complement of x.

15. An element in a lattice need not have a complement.

16. Complement of a element in a lattice, if exists, need not be unique.

17. If an element x in a bounded lattice has a unique complement, then we denote it by x'.

18. In a bounded lattice, 1 is a complement of 0 and 0 is a complement of 1.

19. Every element A in lattice $L = (\mathcal{P}(X); \cap, \cup)$ has a unique complement which is set-complement of A w.r.t. X.

20. No chain having more than two elements is complemented.

21. In a distributive lattice every element has at most one complement.

22. In a distributive complemented lattice, every element has a unique complement.

6.6 Self Assessment Exercise

3.1 Show that the following inequalities hold in any lattice;

(i) $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$,

(ii) $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$.

3.2 Let L be a bounded distributive lattice. Prove that if $a, b \in L$ and a has a complement a', then

$$a \vee (a' \wedge b) = a \vee b, \quad \text{and}$$

$$a \wedge (a' \vee b) = a \wedge b.$$

3.3 Show that if a bounded lattice has two or more elements, then $0 \neq 1$.

3.4 Let L be a bounded lattice with at least two elements. Show that no element of L is its own complement.

3.5 Show that the set $\mathbb{N}$, ordered by divisibility, is a distributive lattice. Is it complemented?

3.6 In the lattice defined by the Hasse diagram given in the Figure 6.7, how many complements does the element b have?

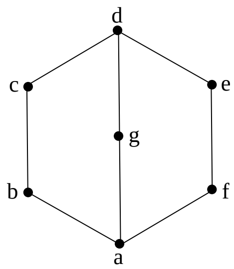


Figure 6.7:

3.7 Which of the following statements are true/false? Explain your answers.

(a) A lattice with 4 or fewer elements is distributive.

(b) Every chain is a distributive lattice.

(c) Every distributive lattice is a bounded lattice.

(d) Every sublattice of a distributive lattice is also distributive.

(e) Every sublattice of a complemented lattice is complemented.

3.8 Is the lattice $(\{1, 2, 3, 5, 30\}; |)$ with divisibility order distributive? Is it complemented?

3.9 Which of the lattices of Figure 6.8 are distribute and which are complemented? Explain your answers.

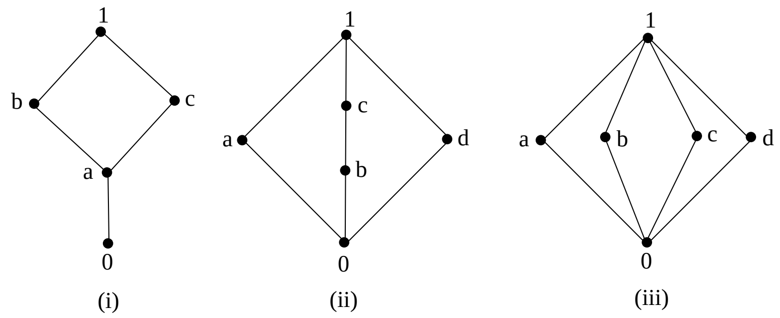


Figure 6.8:

6.7 Answers to In-Text Exercises

Excercise 3.1

1. We know that $D_{12} = \{1, 2, 3, 4, 6, 12\}$ and the Hasse diagram of D_{12} is shown in Figure 6.9. D_{12} contains a sublattice $\{1, 2, 4, 12, 3\}$ isomorphic to N_5 and hence

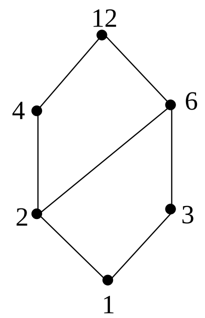


Figure 6.9: The lattice D_{12}.

is not distributive.

2. (i) This lattice does not have any sublattice isomorphic to M_3 as M_3 has three non-comparable elements while this lattice does not have three non-comparable elements. Also it does not have any sublattice isomorphic to N_5 as N_5 has two pairs of non-comparable elements while this has only one pair of non-comparable elements, namely a and b. Thus, It is distributive.

   (ii) It has a sublattice $\{0, a, e, 1, d\}$ isomorphic to N_5, therefore it is not distributive.

Excercise 3.2

1. (a) False. A sublattice of a complemented lattice need not be complemented. For example, take $L = (\mathcal{P}(\mathbb{N}), \cup, \cap)$. Then L is complemented and complement of an element is the set complement. Now let $M = \{A \subset \mathbb{N} \mid A \text{ is finite}\}$. Then M is a sublattice of L and it is not bounded and therefore is not complemented.

(b) True. We know that homomorphic image of a bounded lattice is bounded. Let $f : L \to K$ be a homomorphism and L be a complemented lattice. Then one can easily verify that $f(L)$ is also complemented as each $f(x) \in f(L)$ has a complement $f(y)$ in $f(L)$, where y is complement of x in L.

(c) True. Let L and K be complemented lattices. Let $(l, k) \in L \times K$. Since L and K are complemented, there exist a complement l_1 of l in L and complement k_1 of k in K. The it is easy to verify that (l_1, k_1) is a complement of (l, k) in $L \times K$.

(d) True. Let ϕ be an isomorphism from L to M. Let $a \in M$ be arbitrary. Then there exists $x \in L$ such that $\phi(x) = a$. Let y be a complement of x in L, then it can be easily verified that $\phi(y)$ is a complement of $\phi(x) = a$.

2. (i) It is not complemented as elements a, b and c have no complements.
(ii) It is complemented. 0 and 1 are complements of each other. The element d is a complement of each of a, b, c, e and vice-versa.

6.8 References

[1]Davey, B. A., & Priestley, H. A. (2002). Introduction to lattices and order. Cambridge university press.

[2] Lidl, R., & Pilz, G. (2012). Applied abstract algebra. Springer Science & Business Media.

[3] Kolman, B., Busby, R. C., & Ross, S. (1995). Discrete mathematical structures. Prentice-Hall, Inc.

6.9 Suggested Readings

[1] Birkhoff, G. (1940). Lattice theory (Vol. 25). American Mathematical Soc.

[2] Grätzer, G. (2002). General lattice theory. Springer Science & Business Media.

Unit Overview

Boolean algebras have many important applications in mathematics and they are the subject of the classical Stone Representation Theorem which identifies them all (up to isomorphism) with sub-algebras of powerset algebras. Boolean algebra was introduced by George Boole in 1847 as a tool for the mathematical analysis of logic. It was not used for practical purposes, however, until the late 1930s, when A. Nakashima and, independently, C. E. Shannon used it for analyzing relay contact networks. After World War II, the switching theory was extended to include sequential systems (i.e., systems whose outputs depend not only on the inputs but also on the previous states of the system). Based on these advances in theory, digital electronic computers and other digital systems were developed. Today, digital electronic systems are widely used, and the corresponding theories are studied in mathematics, computer science, and electrical engineering. The purpose of this unit is to introduce Boolean algebra, its properties and its applications to switching circuits.

Chapter 1 provides a basic introduction to Boolean algebra as a distributive complemented lattice. Within Boolean algebra we have emphasized on Boolean isomorphism and De Morgan's law. Then after, Boolean polynomials and Boolean polynomial functions on Boolean algebras are defined. Chapter 2 deals with normal and minimal forms of polynomials as a simplified form is always desirable. Chapter 3 discusses applications of Boolean algebra and Boolean polynomials in the field of switching circuits. In this chapter we learn to formulate a circuit in mathematical form and to design a desirable circuit with given properties using various logic gates.

We have kept the treatment of concepts as elementary as possible. We have carefully prepared the ground for students who will progress to study its computer science applications in future.

Lesson - 7

Boolean Algebra

Structure

7.1 Learning Objectives

After reading this lesson, the reader should be able:

- to understand the concept of Boolean algebras and their properties.
- to identify Boolean algebras.
- to learn about Boolean polynomials and Boolean polynomial functions.
- to construct the truth table for a given Boolean polynomial function.

7.2 Introduction

Boolean algebras are special lattices which are useful in the study of logic, both digital computer logic and that of human thinking, and of switching circuits. This latter application was initiated by C.E. Shannon, who showed that fundamental properties of electrical circuits of bistable elements can be represented by using Boolean algebras. We shall consider such applications in later chapters.

7.3 Boolean Algebras

Firstly, we recall definitions of distributive lattice and complemented lattice.

Definition 7.1. A lattice L is called distributive if for all $a, b, c \in L$ the following distributive laws hold:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Definition 7.2. A lattice L with 0 and 1 is called complemented if for each $x \in L$ there is at least one element y such that $x \wedge y = 0$ and $x \vee y = 1$. Each such y is called a complement of x.

Definition 7.3. A complemented distributive lattice is called a Boolean algebra (or a Boolean lattice).

Distributivity in a Boolean algebra guarantees the uniqueness of complements. Therefore, every element in a Boolean algebra has a unique complement.

Notation. From now on, B will denote a Boolean algebra with two binary operations $\vee$ and $\wedge$, with zero element 0 and a one element 1, and the operation of complementation $'$, in short B $= (B, \wedge, \vee, 0, 1,')$ or $B = (B, \wedge, \vee)$, or simply B.

Example 7.1. $(\mathcal{P}(X), \cap, \cup, \emptyset, X,')$ is the Boolean algebra of the power set of a set X. Here $\cap$ and $\cup$ are the set-theoretic operations intersection and union, and the complement is the set-theoretic complement, namely $X - A = A'$; $\emptyset$ and X are the zero and one elements. If X has n number of elements then $\mathcal{P}(X)$ has 2^n elements.

Example 7.2. Let $\mathbb{B} = \{0, 1\}$ be the chain of length two, 2, where the operations are defined by

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

	$'$
0	1
1	0

Then $(\mathbb{B}, \cap, \cup, 0, 1,')$ is a Boolean algebra.

Example 7.3. If $n \in \mathbb{N}$, we can make $\mathbb{B}^n$ a Boolean algebra by taking the following operations:

$$(i_1, i_2, ..., i_n) \wedge (j_1, j_2, ..., j_n) := (i_1 \wedge j_1, i_2 \wedge j_2, ..., i_n \wedge j_n),$$
$$(i_1, i_2, ..., i_n) \vee (j_1, j_2, ..., j_n) := (i_1 \vee j_1, i_2 \vee j_2, ..., i_n \vee j_n),$$
$$(i_1, i_2, ..., i_n)' := (i_1', i_2', ..., i_n'),$$

and $0 = (0, 0, ..., 0), 1 = (1, 1, ..., 1)$.
More generally, any direct product of Boolean algebra is a Boolean algebra.

Definition 7.4. Let B_1 and B_2 be Boolean algebras. Then the mapping $f : B_1 \to B_2$ is called a Boolean isomorphism from B_1 to B_2 if f is a lattice isomorphism and $f(x') = (f(x))'$ for all $x \in B_1$.

Next, we will focus on finite Boolean algebras and their structures. Firstly, we will restrict our attention to the Boolean algebra $(\mathcal{P}(S); \cap, \cup)$, where S is a finite set and we begin by finding all essentially different examples. In this direction, we are stating the following result without proof.

Theorem 7.1. If $S_1 = \{x_1, x_2, ..., x_n\}$ and $S_2 = \{y_1, y_2, ..., y_n\}$ are any two finite sets with n elements, then the Boolean algebras $(\mathcal{P}(S_1); \cap, \cup)$ and $(\mathcal{P}(S_2); \cap, \cup)$ are isomorphic. Consequently, the Hasse diagrams of these Boolean algebras may be drawn identically.

Since both S_1 and S_2 have same number of elements, we may define a one-one onto correspondence f between the elements of S_1 and S_2. For each subset A of S_1, the set of corresponding elements $f(A)$ forms a subset of S_2. One may easily verify that if A, B are any subsets of S_1 such that $A \subseteq B$, then $f(A) \subseteq f(B)$ in S_2. Also $f(A') = (f(A))'$ implies that the Boolean algebras $(\mathcal{P}(S_1); \cap, \cup)$ and $(\mathcal{P}(S_2); \cap, \cup)$ are isomorphic.

The essential point of this theorem is that the Boolean algebra $(\mathcal{P}(S); \cap, \cup)$ does not depend in any way on the nature of the elements in S, it is completely determined by the number of elements in it. Thus, for each $n \in \mathbb{N}_0$, there is only one type of lattice having the form $(\mathcal{P}(S); \cap, \cup)$. It has 2^n elements. Also we know that $\mathbb{B}^n = \{0, 1\}^n$ has 2^n elements. If $S = \{1, 2, 3, ..., n\}$, then we may define

$$f : \{0, 1\}^n \to \mathcal{P}(S), \quad \text{as follows}$$
$$f(i_1, i_2, ..., i_n) = \{k \mid i_k = 1\}.$$

Then one may verify that f is a Boolean isomorphism. Thus, each lattice $(\mathcal{P}(S); \cap, \cup)$ is isomorphic with $\mathbb{B}^n$, where $n = |S|$ and thus possess all the properties of $\mathbb{B}^n$. In fact, Each finite Boolean algebra is isomorphic to $\mathbb{B}^n$, for some $n \in \mathbb{N}$ and therefore, has 2^n number of elements.

Example 7.4. Consider the lattice D_6 consisting of all positive integer divisors of 6 under divisibility order. $D_6 = \{1, 2, 3, 6\}$ is isomorphic to $\mathbb{B}^2$. In fact, $f : D_6 \to \mathbb{B}^2$ is a Boolean isomorphism, where

$$f(1) = (0, 0), f(2) = (1, 0), f(3) = (0, 1), f(6) = (1, 1).$$

Thus, D_6 is a Boolean algebra.

Example 7.5. Consider the lattices D_{20} and D_{30} of all positive divisors of 20 and 30, respectively, under the divisibility order. Since D_{20} has 6 elements and $6 \neq 2^n$ for any $n \in \mathbb{N}$, we conclude that D_{20} is not a Boolean algebra. The lattice D_{30} has 8 elements and $8 = 2^3$. Also D_{30} is a distributive complemented lattice and hence a Boolean algebra. The map $f : D_{30} \to \mathbb{B}^3$ defined as

$$\begin{aligned} f(1) &= (0, 0, 0), & f(2) &= (1, 0, 0), & f(3) &= (0, 1, 0), \\ f(5) &= (0, 0, 1), & f(6) &= (1, 1, 0), & f(10) &= (1, 0, 1), \\ f(15) &= (0, 1, 1), & f(30) &= (1, 1, 1) \end{aligned}$$

is a Boolean isomorphism. Thus, $D_{30} \cong \mathbb{B}^3$.

7.4 De Morgan's Law

Theorem 7.2. (De Morgan's Law) For all x, y in a Boolean algebra, we have

$$(x \wedge y)' = x' \vee y' \quad \text{and} \quad (x \vee y)' = x' \wedge y'.$$

Proof. We want to show that complement of $(x \wedge y)$ is $x' \vee y'$, therefore we consider

$$\begin{aligned} (x \wedge y) \vee (x' \vee y') &= (x \vee (x' \vee y')) \wedge (y \vee (x' \vee y')) \\ &= ((x \vee x') \vee y') \wedge (y \vee (y' \vee x')) \\ &= (1 \vee y') \wedge (y \vee y') \vee x' \\ &= 1 \wedge (1 \vee y') \\ &= 1 \wedge 1 \\ &= 1. \end{aligned}$$

Next, we consider

$$\begin{aligned} (x \wedge y) \wedge (x' \vee y') &= (x \wedge (x' \vee y')) \wedge (y \wedge (x' \vee y')) \\ &= ((x \wedge x') \vee (x \wedge y')) \wedge ((y \wedge x') \vee (y \wedge y')) \\ &= (0 \vee (x \wedge y')) \wedge ((y \wedge x') \vee 0) \\ &= (x \wedge y') \wedge (y \wedge x') \\ &= x \wedge (y' \wedge y) \wedge x' \\ &= x \wedge 0 \wedge x' \\ &= 0. \end{aligned}$$

This implies that $(x \wedge y)' = x' \vee y'$.

Similarly, one can easily show that $(x \vee y)' = x' \wedge y'$.

□

Corollary 7.1. In a Boolean algebra B we have for all $x, y \in B$,

$$x \leq y \Leftrightarrow x' \geq y'.$$

Proof.

$$x \leq y \Leftrightarrow x \vee y = y \Leftrightarrow x' \wedge y' = (x \vee y)' = y' \Leftrightarrow x' \geq y'.$$

□

Theorem 7.3. In a Boolean algebra B, for all $x, y \in B$, the following are equivalent:

(i) $x \leq y$

(ii) $x \wedge y' = 0$

(iii) $x' \vee y = 1$

(iv) $x \wedge y = x$

(v) $x \vee y = y$.

Proof. By connecting lemma we know that $(i), (iv)$ and (v) are equivalent. Now we will prove that (i) is equivalent to both (ii) and (iii).
$(i) \Rightarrow (ii)$

$$\begin{aligned} 0 &= x \wedge 0 \\ &= x \wedge (y \wedge y') \\ &= (x \wedge y) \wedge (x \wedge y') \\ &= x \wedge (x \wedge y') \\ &= x \wedge y' \end{aligned}$$

$(ii) \Rightarrow (i)$
To show that $x \leq y$ we will show that $x \wedge y = x$.

$$\begin{aligned} x \wedge y &= (x \wedge y) \vee 0 \\ &= (x \wedge y) \vee (x \wedge y') \\ &= ((x \wedge y) \vee x) \wedge ((x \wedge y) \vee y') \\ &= x \wedge [(x \vee y') \wedge (y \vee y')] \\ &= x \wedge [(x \vee y') \wedge 1] \\ &= x \wedge (x \vee y') \\ &= x. \end{aligned}$$

This establishes the equivalence of (i) and (ii). Next,
$(i) \Rightarrow (iii)$

$$\begin{aligned} 1 &= 1 \vee y \\ &= (x \vee x') \vee y \\ &= (x' \vee x) \vee y \\ &= x' \vee (x \vee y) \\ &= x' \vee y. \end{aligned}$$

Next, to show that (iii) implies (i) we will show that $x \vee y = y$.
$(iii) \Rightarrow (i)$

$$\begin{aligned} x \vee y &= 1 \wedge (x \vee y) \\ &= (x' \vee y) \wedge (x \vee y) \\ &= [(x' \wedge (x \vee y))] \vee [y \wedge (x \vee y)] \\ &= [(x' \wedge x) \vee (x' \wedge y)] \vee y \\ &= 0 \vee (x' \wedge y) \vee y \\ &= (x' \wedge y) \vee y \\ &= y. \end{aligned}$$

This establishes the equivalence of (i) and (iii). Hence the proof. □

In-text Exercise 7.1. 1. Determine which of the lattices shown in Figure 7.1 are Boolean algebras. Explain your answer.

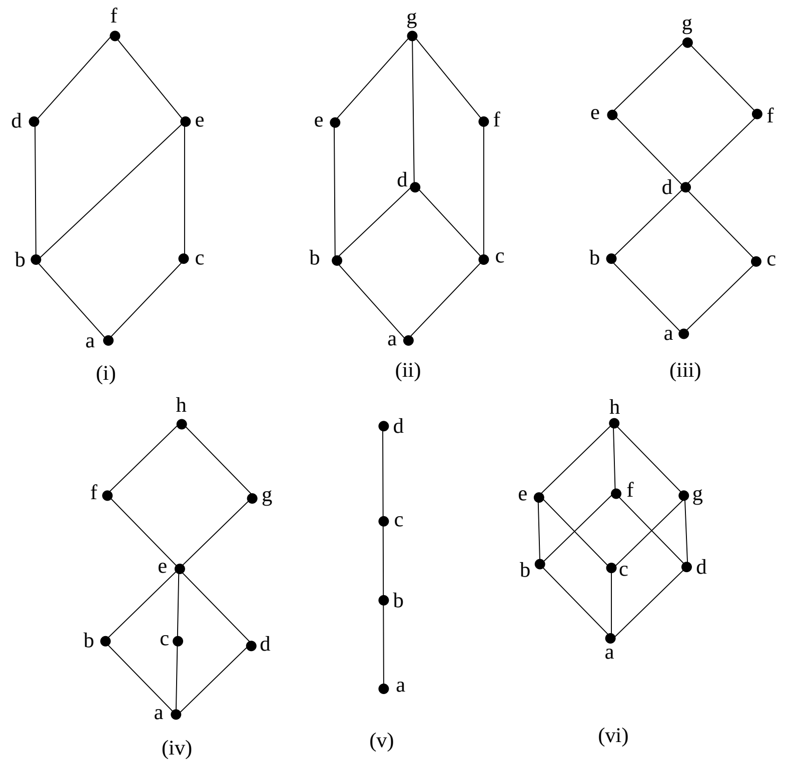


Figure 7.1:

2. Are there any Boolean algebras having 9 elements? Why or why not?

3. Is D_{42} a Boolean algebra? Why or why not?

7.5 Boolean Polynomials or Boolean Expressions

Let $X = \{x_1, x_2, ..., x_n\}$ be a set of n symbols or variables. A Boolean Polynomial $p(x_1, x_2, ..., x_n)$ in X, is defined recursively as follows:

1. $x_1, x_2, ..., x_n$ are all Boolean polynomials.
2. The symbols 0 and 1 are Boolean polynomials.
3. If $p(x_1, x_2, ..., x_n)$ and $q(x_1, x_2, ..., x_n)$ are two Boolean polynomials, then so are
$$p(x_1, x_2, ..., x_n) \vee q(x_1, x_2, ..., x_n)$$
and
$$p(x_1, x_2, ..., x_n) \wedge q(x_1, x_2, ..., x_n).$$
4. If $p(x_1, x_2, ..., x_n)$ is a Boolean polynomial, then so is
$$(p(x_1, x_2, ..., x_n))'.$$
5. There are no Boolean polynomials in X other than those that can be obtained by repeated use of rule 1, 2, 3 and 4.

Boolean polynomials are also called Boolean expressions.

Two Boolean polynomials are equal if their sequences of symbols are identical. We denote the set of all Boolean polynomials in $\{x_1, x_2, ..., x_n\}$ by P_n.

Example 7.6. The following are some examples of Boolean polynomials over $\{x_1, x_2, x_3\}$:

1. $p_1(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge x_3$
2. $p_2(x_1, x_2, x_3) = (x_1 \vee x_2') \vee (x_2 \wedge 1)$
3. $p_3(x_1, x_2, x_3) = (x_1 \vee (x_2' \wedge x_3)) \vee (x_1 \wedge (x_2 \wedge 0))$
4. $p_4(x_1, x_2, x_3) = (x_1 \wedge (x_2 \vee x_3')) \wedge ((x_1' \wedge x_3)' \vee (x_2' \wedge 0))$

Since every Boolean polynomial over $x_1, ..., x_n$ is a boolean polynomial over $x_1, ..., x_n, x_{n+1}$, we have
$$P_1 \subset P_2 \subset P_3 \cdots \subset P_n \subset P_{n+1} \subset \cdots .$$

Next, we introduce the concept of Boolean polynomial function as follows:

Definition 7.5. Let B be a Boolean algebra, let B^n be the product of n copies of B, and let p be a Boolean polynomial in P_n. Then
$$\bar{p}_B : B^n \to B; \quad (a_1, a_2, ..., a_n) \mapsto \bar{p}_B(a_1, a_2, ..., a_n),$$
is called the Boolean polynomial function of degree n induced by p on B. Here $\bar{p}_B(a_1, a_2, ..., a_n)$ is the element in B which is obtained from p by replacing each x_i by $a_i \in B, 1 \le i \le n$.

Definition 7.6. Two Boolean polynomials $p, q \in P_n$ are equivalent (in symbols $p \sim q$) if their Boolean polynomial functions on $\mathbb{B}$ are equal, i.e.,

$$p \sim q \Leftrightarrow \bar{p}_{\mathbb{B}} = \bar{q}_{\mathbb{B}}.$$

Equivalently, two Boolean polynomials are equivalent if one can be obtained from other by using laws of Boolean algebra. For example, $p = x \wedge y$ and $q = y \wedge x$ are equivalent Boolean polynomials in P_2.

Result 7.1. Let $p, q \in P_n$, $p \sim q$ and B is any Boolean algebra then

$$\bar{p}_B = \bar{q}_B.$$

7.6 Truth Table

The truth table of a Boolean polynomial function of degree n is the table of the value of the function on each element of $\mathbb{B}^n$. Clearly the value of the function on any element is either 0 or 1. Here we present some examples of the truth table of various Boolean polynomial functions.

Example 7.7. Consider the Boolean polynomial

$$p(x, y, z) = (x \wedge y) \vee (y \wedge z').$$

Construct the truth table for the Boolean polynomial function $\bar{p}_B : \mathbb{B}^3 \to \mathbb{B}$.

Solution. The truth table for the given Boolean polynomial function is as follows:

x	y	z	$\bar{p}_B(x, y, z) = (x \wedge y) \vee (y \wedge z')$
0	0	0	$(0 \wedge 0) \vee (0 \wedge 0') = 0$
0	0	1	$(0 \wedge 0) \vee (0 \wedge 1') = 0$
0	1	0	$(0 \wedge 1) \vee (1 \wedge 0') = 1$
0	1	1	$(0 \wedge 1) \vee (1 \wedge 1') = 0$
1	0	0	$(1 \wedge 0) \vee (0 \wedge 0') = 0$
1	0	1	$(1 \wedge 0) \vee (0 \wedge 1') = 0$
1	1	0	$(1 \wedge 1) \vee (1 \wedge 0') = 1$
1	1	1	$(1 \wedge 1) \vee (1 \wedge 1') = 1$

Example 7.8. Consider the Boolean polynomial

$$p(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \vee (x_2' \wedge x_3)).$$

Construct the truth table for the Boolean polynomial function $\bar{p}_B : \mathbb{B}^3 \to \mathbb{B}$.

Solution. The Boolean polynomial function $\bar{p}_B : \mathbb{B}^3 \to \mathbb{B}$ is described by substituting all 2^3 ordered triples of $\mathbb{B}^3$ for x_1, x_2, x_3. The truth table for this Boolean polynomial function is as follows:

x_1	x_2	x_3	$\bar{p}_B(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \vee (x_2' \wedge x_3))$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Example 7.9. Apply the rules of Boolean arithmetic to show that the Boolean polynomials $(x \wedge z) \vee (y' \vee (y' \wedge z)) \vee ((x \wedge y') \wedge z')$ and $(x \wedge z) \vee y'$ are equivalent.

Solution. Consider,

$$(x \wedge z) \vee (y' \vee (y' \wedge z)) \vee ((x \wedge y') \wedge z')$$

$$\begin{aligned}
&= (x \wedge z) \vee y' \vee ((x \wedge y') \wedge z') && \text{(by } (L_4)) \\
&= (x \wedge z) \vee (y' \vee ((x \wedge y') \wedge z')) && \text{(by } (L_1)) \\
&= (x \wedge z) \vee [(y' \vee (x \wedge y')) \wedge (y' \vee z')] && \text{(by distributive law)} \\
&= (x \wedge z) \vee [y' \wedge (y' \vee z')] && \text{(by } (L_4)) \\
&= (x \wedge z) \vee y' && \text{(by } (L_4))
\end{aligned}$$

Hence $(x \wedge z) \vee (y' \vee (y' \wedge z)) \vee ((x \wedge y') \wedge z')$ and $(x \wedge z) \vee y'$ are equivalent.

Example 7.10. Rewrite the polynomial $p(x, y, z) = (x \vee (y \vee z')) \wedge ((x' \wedge z)' \wedge (y' \vee 0))$ into the form of three variables and two operations format.

Solution. Consider,

$$(x \vee (y \vee z')) \wedge ((x' \wedge z)' \wedge (y' \vee 0))$$

$$\begin{aligned}
&= (x \vee (y \vee z')) \wedge ((x \vee z') \wedge y') && \text{(using De Morgan's law)} \\
&= ((x \vee z') \vee y) \wedge (x \vee z') \wedge y' && \text{(by } L_1) \\
&= [((x \vee z') \vee y) \wedge (x \vee z')] \wedge y' && \\
&= (x \vee z') \wedge y' && \text{(by } L_4)
\end{aligned}$$

Thus, $(x \vee (y \vee z')) \wedge ((x' \wedge z)' \wedge (y' \vee 0)) = (x \vee z') \wedge y'$.

7.7 Summary

1. A lattice L with 0 and 1 is called complemented if for each $x \in L$ there is at least one element y such that $x \wedge y = 0$ and $x \vee y = 1$. Each such y is called a complement of x.

2. A complemented distributive lattice is called a Boolean algebra (or a Boolean lattice).

3. $(\mathcal{P}(X), \cap, \cup, \emptyset, X, ')$ is the Boolean algebra of the power set of a set X.

4. $\mathbb{B}$, the chain of length two, 2, is a Boolean algebra.

5. Any product of Boolean algebras is a Boolean algebra.

6. Let B_1 and B_2 be Boolean algebras. Then the mapping $f : B_1 \to B_2$ is called a Boolean isomorphism from B_1 to B_2 if f is a lattice isomorphism and $f(x') = (f(x))'$ for all $x \in B_1$.

7. Any two finite Boolean algebras with same number of elements are isomorphic.

8. Any finite Boolean algebra has number of elements in 2^n form.

9. (De Morgan's Law:)For all x, y in a Boolean algebra, we have

$$(x \wedge y)' = x' \vee y' \quad \text{and} \quad (x \vee y)' = x' \wedge y'.$$

10. Let $X = \{x_1, x_2, ..., x_n\}$ be a set of n symbols. The boolean polynomials in X are the objects which can be obtained by finitely many successive applications of:

    (i) $x_1, x_2, ..., x_n$ and 0 , 1 are Boolean polynomials.

    (ii) if p and q are Boolean polynomials, then so are $p \wedge q$, $p \vee q, p'$.

11. Two Boolean polynomials $p, q \in P_n$ are equivalent (in symbols $p \sim q$) if their Boolean polynomial functions on $\mathbb{B}$ are equal, i.e.,

$$p \sim q \Leftrightarrow \bar{p}_{\mathbb{B}} = \bar{q}_{\mathbb{B}}.$$

Equivalently, two Boolean polynomials are equivalent if one can be obtained from other by using laws of Boolean algebra.

7.8 Self-Assessment Exercise

Exercise 1. Show that D_{110} is a Boolean algebra.

Exercise 2. Show that in a Boolean algebra, for any a and b,

$$(a \wedge b) \vee (a \wedge b') = a.$$

Exercise 3. Show that in a Boolean algebra, for any a and b,

$$b \wedge (a \vee (a' \wedge (b \vee b'))) = b.$$

Exercise 4. Show that in a Boolean algebra, for any a, b and c,

$$(a \wedge b \wedge c) \vee (b \wedge c) = b \wedge c.$$

Exercise 5. Show that in a Boolean algebra, for any a, b and c,

$$((a \vee c) \wedge (b' \vee c))' = (a' \vee b) \wedge c'.$$

Exercise 6. Show that in a Boolean algebra, for any a, b and c, if $a \leq b$, then

$$a \vee (b \wedge c) = b \wedge (a \vee c).$$

Exercise 7. Compute the truth table of the Boolean polynomial function $\bar{p}_B : \mathbb{B}^3 \to \mathbb{B}$ defined by p given as follows:

(i) $p(x, y, z) = x \wedge (y \vee z')$

(ii) $p(x, y, z) = (x \vee y) \wedge (z \vee x')$

(iii) $p(x, y, z) = (x \wedge y') \vee (y \wedge (x' \vee y))$

(iv) $p(x, y, z) = (x \wedge y) \vee (x' \wedge (y \wedge z'))$.

Exercise 8. Apply the rules of Boolean arithmetic to show that the following Boolean polynomials are equivalent:

(i) $(x \vee y) \wedge (x' \vee y)$ and y,

(ii) $x \wedge (y \vee (y' \wedge (y \vee y')))$ and x,

(iii) $(z' \vee x) \wedge ((x \wedge y) \vee z) \wedge (z' \vee y)$ and $x \wedge y$,

(iv) $[(x \wedge z) \vee (y' \vee z)'] \vee [(y \wedge z) \vee (x \wedge z')]$ and $x \vee y$

Exercise 9. Rewrite the given polynomial to get the required format.

(i) $(x \wedge y' \wedge z) \vee (x \wedge y \wedge z)$; two variables and one operation,

(ii) $(z \vee (y \wedge (x \vee x'))) \wedge (y \wedge z')'$; one variable,

(iii) $(y \wedge z) \vee x' \vee (w \wedge w') \vee (y \wedge z')$; two variables and two operations.

7.9 Solutions to In-text Exercises

Excercise 1.1

1. (i) The element b has no complement and therefore the given lattice is not a Boolean algebra.

   (ii) The element d has no complement and therefore the given lattice is not a Boolean algebra.

(iii) The element d has no complement and therefore the given lattice is not a Boolean algebra.

(iv) The given lattice has a sublattice isomorphic to M_3 and therefore not distributive and hence not a Boolean algebra. OR the element e has no complement and hence the lattice is not a Boolean algebra.

(v) The element b has no complement and therefore the given lattice is not a Boolean algebra.

(vi) The given lattice is isomorphic to 2^3. Since 2 is a Boolean lattice and product of Boolean lagebras is a Boolean algebra, therefore the given lattice is a Boolean algebra.

2. The number of elements in a finite Boolean algebra is always of the form 2^n, for some $n \in \mathbb{N}$ and since $9 \neq 2^n$ for any $n \in \mathbb{N}$, therefore there is no Boolean algebra with 9 elements.

3. The lattice $D_{42} = \{1, 2, 3, 6, 7, 14, 21, 42\}$. The Figure 7.2 shows the Hasse diagram of D_{42}. It has 8 elements and is isomorphic to 2^3 which being product of Boolean algebras is a Boolean algebra. Hence D_{42} is a Boolean algebra.

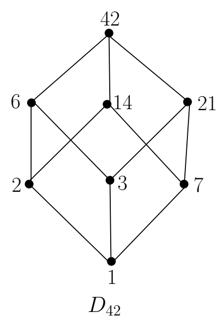


Figure 7.2:

7.10 Suggested Reading

[1]Davey, B. A., & Priestley, H. A. (2002). Introduction to lattices and order. Cambridge university press.

[2] Lidl, R., & Pilz, G. (2012). Applied abstract algebra. Springer Science & Business Media.

[3] Kolman, B., Busby, R. C., & Ross, S. (1995). Discrete mathematical structures. Prentice-Hall, Inc.

Lesson - 8

Normal and Minimal Forms of Boolean Polynomials

Structure

8.1 Learning Objectives

After reading this lesson, the reader should be able:

- to understand the concept of normal forms of Boolean polynomials.
- to be able to write a given polynomial in disjunctive normal form and conjunctive normal form.
- to understand the concept and importance of minimal form of Boolean polynomials.

- to be able to find prime implicants of a Boolean polynomial and reduce it into minimal form using Quine McClusky method.
- to be able to simplify a Boolean polynomial by Karnaugh diagram.

8.2 Introduction

We have seen in the previous chapter that it is possible and desirable to simplify a given Boolean polynomial by using the axioms of a Boolean algebra. For this process of simplification it is often difficult to decide which axioms should be used and in which order they should be used. There are several systematic methods to simplify Boolean polynomials. This problem area in the theory of Boolean algebras is called the optimization or minimization problem for Boolean polynomials; it is of importance in applications such as the simplification of switching circuits.

In this chapter we define normal forms of Boolean polynomials and learn ways to represent polynomial into disjunctive and conjunctive normal forms. Further, we define minimal form of Boolean polynomials and explain Quine McClusky method to reduce a Boolean polynomial into its minimal form. In the end, we describe Karnaugh diagrams, another way of representing/simplifying the Boolean polynomials.

8.3 Normal Forms of Boolean Polynomials

We frequently want to replace a given polynomial p by an equivalent polynomial which is of simpler or more systematic form. This is achieved by considering so-called normal forms. The collection of normal forms is a system of representatives for different classes of P_n.

Definition 8.1. $N \subseteq P_n$ is called a system of normal forms if:

(i) every $p \in P_n$ is equivalent to some $q \in N$;

(ii) for all $q_1, q_2 \in N, q_1 \neq q_2$ implies $q_1 \nsim q_2$.

Notation: To simplify notation, we shall from now on write $\mathbf{p}+\mathbf{q}$ for $\mathbf{p} \vee \mathbf{q}$ and $\mathbf{pq}$ for $\mathbf{p} \wedge \mathbf{q}$.

Boolean Identities

Let $(B, +, \cdot, ')$ be a Boolean algebra. Then for all $x, y, z \in B$ the following identities hold:

1.	$x + x = x$ $x \cdot x = x$	Idempotent Law
2.	$x + 0 = x$ $x \cdot 1 = x$	Identity Law
3.	$x + 1 = 1$ $x \cdot 0 = 0$	Domination Law
4.	$(x')' = x$	Double Complement Law
5.	$x + y = y + x$ $x \cdot y = y \cdot x$	Commutative Law
6.	$x + (y + z) = (x + y) + z$ $x(yz) = (xy)z$	Associative Law
7.	$x + xy = x$ $x(x + y) = x$	Absorption Law
8.	$x + yz = (x + y)(x + z)$ $x(y + z) = xy + xz$	Distributive Law
9.	$x + x' = 1$	Unit Property
10.	$x \cdot x' = 0$	Zero Property
11.	$(xy)' = x' + y'$ $(x + y)' = x'y'$	De Morgan's Law

8.3.1 Disjunctive Normal Form (as join of meets)

Definition 8.2. A product expression (briefly a product) is a Boolean polynomial in which '+' does not occur. A product expression in which every variable or its complement is presented once is called a minterm.

Definition 8.3. A representation of a Boolean polynomial $p \in P_n$ as a sum of product of x_1 (or x_1'), x_2 (or x_2'),..., x_n (or x_n') is called its disjunctive normal form (in short DN form).

Steps to write Disjunctive Normal Form of a given Boolean polynomial

1. If $p \in P_n$, we first write down the truth table of $\bar{p}$.
2. We look at each $(b_1, b_2, ..., b_n) \in \mathbb{B}^n$ for which $\bar{p}(b_1, b_2, ..., b_n) = 1$ and write down the term $x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$, where $x_i^1 = x_i$ and $x_i^0 = x_i'$.
3. The sum of all such terms is equivalent to p and is the required DN form of p.
4. We further reduce or simplify it using Boolean arithmetic to get a shorter form.

Example 8.1. Find the disjunctive normal form of $p = ((x_1+x_2)'x_1+x_2''')'+x_1x_2+x_1x_2'$.

Solution. We list the values of $\bar{p}$ in a truth table. First, $\bar{p}(0, 0) = ((0 + 0)'0 + 0''')' + 00 + 00' = 0$, and so on:

b_1	b_2	$\bar{p}(b_1, b_2)$	
0	0	0	
0	1	1	$\leftarrow$
1	0	1	$\leftarrow$
1	1	1	$\leftarrow$

Now, we look for the terms (b_1, b_2) for which $\bar{p}(b_1, b_2) = 1$. Such terms are marked with an arrow in the truth table. We write down the corresponding minterms as follows:

(1) $(b_1, b_2) = (0, 1)$
$x_1^{b_1} x_2^{b_2} = x_1^0 x_2^1 = x_1' x_2$

(2) $(b_1, b_2) = (1, 0)$
$x_1^{b_1} x_2^{b_2} = x_1^1 x_2^0 = x_1 x_2'$

(3) $(b_1, b_2) = (1, 1)$
$x_1^{b_1} x_2^{b_2} = x_1^1 x_2^1 = x_1 x_2$

So, $p \sim x_1' x_2 + x_1 x_2' + x_1 x_2$. This may be further reduced as follows

$$\begin{aligned} p \sim x_1' x_2 + x_1 x_2' + x_1 x_2 \quad &= x_1' x_2 + x_1 x_2 + x_1 x_2' \\ &\sim (x_1' + x_1) x_2 + x_1 x_2' \\ &\sim x_2 + x_1 x_2' \\ &\sim (x_2 + x_1)(x_2 + x_2') \\ &\sim (x_1 + x_2) 1 \\ &\sim x_1 + x_2. \end{aligned}$$

Thus, $p \sim x_1 + x_2$.

Example 8.2. Find the disjunctive normal form of $p = x_1(x_2 + x_3)' + (x_1 x_2 + x_3') x_1$.

Solution. The truth table for p is as follows:

b_1	b_2	b_3	$\bar{p}(b_1, b_2, b_3)$
0	0	0	0
1	0	0	1 $\leftarrow$
0	1	0	0
0	0	1	0
1	1	0	1 $\leftarrow$
1	0	1	0
0	1	1	0
1	1	1	1 $\leftarrow$

We look for the terms (b_1, b_2, b_3) for which $\bar{p}(b_1, b_2, b_3) = 1$ and write the corresponding minterms as follows:

(1) $(b_1, b_2, b_3) = (1, 0, 0)$
$x_1^{b_1} x_2^{b_2} x_3^{b_3} = x_1^1 x_2^0 x_3^0 = x_1 x_2' x_3'$

(2) $(b_1, b_2, b_3) = (1, 1, 0)$
$x_1^{b_1} x_2^{b_2} x_3^{b_3} = x_1^1 x_2^1 x_3^0 = x_1 x_2 x_3'$

(3) $(b_1, b_2, b_3) = (1, 1, 1)$
$x_1^{b_1} x_2^{b_2} x_3^{b_3} = x_1^1 x_2^1 x_3^1 = x_1 x_2 x_3$

So, $p \sim x_1 x_2' x_3' + x_1 x_2 x_3' + x_1 x_2 x_3$. This may be simplified as follows:

$$\begin{aligned} p \sim x_1x_2'x_3' + x_1x_2x_3' + x_1x_2x_3 &= x_1x_3'(x_2' + x_2) + x_1x_2x_3 \\ &\sim x_1x_3' + x_1x_2x_3 \\ &\sim x_1(x_3' + x_2x_3) \\ &\sim x_1(x_3' + x_2)(x_3' + x_3) \\ &\sim x_1(x_3' + x_2) \\ &\sim x_1x_3' + x_1x_2. \end{aligned}$$

Thus, $x_1x_3' + x_1x_2$ is the DN form of p.

Example 8.3. Find a Boolean polynomial p that induces the function f:

b_1	b_2	b_3	$f(b_1, b_2, b_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

Solution. We only look at the elements for which $f(b_1, b_2, b_3) = 1$ and get a polynomial p immediately:

$$p = x_1'x_2'x_3' + x_1'x_2x_3 + x_1x_2'x_3'.$$

The first and the third summand can be combined:

$$\begin{aligned} p &\sim x_1'x_2'x_3' + x_1x_2'x_3' + x_1'x_2x_3 \\ &\sim (x_1' + x_1)x_2'x_3' + x_1'x_2x_3 \\ &\sim x_2'x_3' + x_1'x_2x_3 \end{aligned}$$

Let $q := x_2'x_3' + x_1'x_2x_3$. Then q is also a solution to our problem, i.e., $\bar{p} = \bar{q} = f$.

Example 8.4. Reduce the following Boolean polynomial in the DN form

$$p = ((xy')' + z')(x' + z')'.$$

Solution. .

$$\begin{aligned} p &= ((xy')' + z')(x' + z')' \\ &= ((x' + y) + z')(xz) && \text{(De Morgan's Law)} \\ &= (xz)(x' + y + z') && \text{(Commutative Law)} \\ &= xzx' + xzy + xzz' && \text{(Distributive Law)} \\ &= xx'z + xyz + 0 && (zz' = 0 \text{ and } x \cdot 0 = 0) \\ &= 0 + xyz + 0 && (xx' = 0 \text{ and } 0 \cdot z = 0) \\ &= xyz. && (xyz + 0 = xyz) \end{aligned}$$

Example 8.5. Are $x_1(x_2 + x_3)' + x_1' + x_3'$ and $(x_1x_3)'$ equivalent?

Solution. Let $p = x_1(x_2 + x_3)' + x_1' + x_3'$ and $q = (x_1x_3)'$. We will show that the Boolean polynomial function $\bar{p}_B$ and $\bar{q}_B$ induced by p and q respectively are same on $\mathbb{B}^3$. The truth table of p and q are as follows:

b_1	b_2	b_3	$\bar{p}(b_1, b_2, b_3)$
0	0	0	1
1	0	0	1
0	1	0	1
0	0	1	1
1	1	0	1
1	0	1	0
0	1	1	1
1	1	1	0

b_1	b_2	b_3	$\bar{q}(b_1, b_2, b_3)$
0	0	0	1
1	0	0	1
0	1	0	1
0	0	1	1
1	1	0	1
1	0	1	0
0	1	1	1
1	1	1	0

Since $\bar{p}_B(b_1, b_2, b_3) = \bar{q}_B(b_1, b_2, b_3)$ for each $(b_1, b_2, b_3) \in \mathbb{B}^3$, therefore $p \sim q$.

In-text Exercise 8.1. Attempt the following questions:

1. Simplify the following Boolean polynomials:

   (i) $xy + xy' + x'y$

   (ii) $xy' + x(yz)' + z$.

2. Let $f : \mathbb{B}^3 \to \mathbb{B}$ have the value 1 precisely at the arguments $(0, 0, 0), (0, 1, 0), (0, 1, 1), (1, 0, 0)$. Find a Boolean polynomial p with $\bar{p} = f$ and try to simplify p.

3. Find the disjunctive normal form of the following:

   (i) $x_1(x_2 + x_3)' + (x_1x_2 + x_3')x_1$;

   (ii) $((x_2 + x_1x_3)(x_1 + x_3)x_2)'$.

8.3.2 Conjunctive Normal Form (as meet of joins)

Definition 8.4. A maxterm is a sum expression in which each variable or its complement appears once. For example, $x_1 + x_2' + x_3$ is a max term in P_3.

Definition 8.5. A representation of a Boolean polynomial p as the product of maxterms is called the conjunctive normal form (in short, CN form) of p.

Remark. In the disjunctive normal form of a given polynomial, if we interchange the roles of $0, 1$ and '+', '·', we get the conjunctive normal form.

Steps to write Conjunctive Normal Form of a given Boolean polynomial

1. If $p \in P_n$, we first write down the truth table of $\bar{p}$.
2. We look at each $(b_1, b_2, ..., b_n) \in \mathbb{B}^n$ for which $\bar{p}(b_1, b_2, ..., b_n) = 0$ and write down the term $x_1^{b_1} + x_2^{b_2} + \cdots + x_n^{b_n}$, where $x_i^1 = x_i'$ and $x_i^0 = x_i$.
3. The product of all such terms is equivalent to p and is the required CN form of p.

Example 8.6. Write the CN form of the Boolean polynomial $p = x_1'x_2 + x_1x_2'$

Solution. The truth table of the Boolean polynomial p is as follows:

b_1	b_2	$\bar{p}(b_1, b_2)$
0	0	0
1	0	1
0	1	1
1	1	0

Now we look at the elements (b_1, b_2) for which $\bar{p}(b_1, b_2) = 0$ and write the sum expression for each.

(1) $(b_1, b_2) = (0, 0)$
$x_1^{b_1} + x_2^{b_2} = x_1^0 + x_2^0 = x_1 + x_2$

(2) $(b_1, b_2) = (1, 1)$
$x_1^{b_1} + x_2^{b_2} = x_1^1 + x_2^1 = x_1' + x_2'$

Thus, $p \sim (x_1 + x_2)(x_1' + x_2')$ and this is the required CN form of p.

Example 8.7. Write the CN form of the Boolean polynomial $p = xy' + x(yz)' + z$.

Solution. The truth table of the Boolean polynomial p is as follows:

b_1	b_2	b_3	$\bar{p}(b_1, b_2, b_3)$
0	0	0	0
1	0	0	1
0	1	0	0
0	0	1	1
1	1	0	1
1	0	1	1
0	1	1	1
1	1	1	1

Now we look at the elements (b_1, b_2, b_3) for which $\bar{p}(b_1, b_2, b_3) = 0$ and write the sum expression for each.

(1) $(b_1, b_2, b_3) = (0, 0, 0)$
$x^{b_1} + y^{b_2} + z^{b_3} = x^0 + y^0 + z^0 = x + y + z$

(2) $(b_1, b_2, b_3) = (0, 1, 0)$
$x^{b_1} + y^{b_2} + z^{b_3} = x^0 + y^1 + z^0 = x + y' + z$

Thus, $p \sim (x + y + z)(x + y' + z)$ and this is the required CN form of p.

Remark. A way to come from the disjunctive normal form to conjunctive normal form of a Boolean polynomial p is to write p as $(p')'$, expand p' by using De Morgan's laws and negate this again.

Example 8.8. Convert the following DN form of p to CN form:

$$p = x_1'x_2 + x_1x_2'.$$

Solution. Consider,

$$\begin{aligned} p = (p')' &= ((x_1'x_2 + x_1x_2')')' \\ &= ((x_1'x_2)'(x_1x_2')')' \\ &= ((x_1 + x_2')(x_1' + x_2))' \\ &= (x_1x_1' + x_1x_2 + x_2'x_1' + x_2'x_2)' \\ &= (0 + x_1x_2 + x_2'x_1' + 0)' \\ &= (x_1x_2 + x_1'x_2')' \\ &= (x_1' + x_2')(x_1 + x_2). \end{aligned}$$

In-text Exercise 8.2. Solve the following questions:

1. Find the conjunctive normal norm of $p = (xy' + z')(x' + z)'$.

2. Put the polynomial $p = x(y + z)$ in the CN form.

3. Find the CN form of the polynomial $p = x(y' + z) + z'$.

8.4 Minimal Forms of Boolean Polynomials

In this section we will discuss the reduction of Boolean polynomial to a "minimal form" with respect to a suitably chosen minimality condition which we will apply on sum-of-product expressions i.e., disjunctive normal form.

Definition 8.6. A variable x_i, complemented or not, along with 0 and 1 is called a literal.

Notation. We adopt the following notations:
$d_f :=$ the total number of literals in a sum of product expressions of f.
$e_f :=$ the number of summands in f.

Definition 8.7. A sum of product Boolean expression f is said to be simpler than a sum of product expression g if

$$e_f < e_g, \text{ or } e_f = e_g \text{ and } d_f < d_g.$$

Definition 8.8. A Boolean expression f is said to be minimal if there is no simpler sum of product expression equivalent to f. In other words, the minimal form of a Boolean polynomial f is the shortest sum-of-product expression with the smallest possible number of literals which is equivalent to f.

Definition 8.9. An expression p implies an expression q if for all $b_1, b_2, ..., b_n \in \mathbb{B}$, $\bar{p}_{\mathbb{B}}(b_1, b_2, ..., b_n) = 1 \Rightarrow \bar{q}_{\mathbb{B}}(b_1, b_2, ..., b_n) = 1$. In this case, p is called an implicant of q.

Definition 8.10. A prime implicant for an expression p is a product expression α which implies p, but which does not imply p if one factor in α is deleted. A product β whose factors form a subset of the factors of another product, say α, is called subproduct of α. For example, $q = x_1x_3$ is a subproduct of $x_1x_2x_3$ and also of $x_1x_2'x_3$

Example 8.9. Show that $q = x_1x_3$ is a prime implicant of $p = x_1x_2x_3+x_1x_2'x_3+x_1'x_2'x_3'$.

Solution. Firstly, we will show that $q = x_1x_3$ implies $p = x_1x_2x_3 + x_1x_2'x_3 + x_1'x_2'x_3'$.

Now, $\bar{q}(0,0,0) = \bar{q}(1,0,0) = \bar{q}(0,1,0) = \bar{q}(0,0,1) = \bar{q}(1,1,0) = \bar{q}(0,1,1) = 0$,

and, $\bar{q}(1,0,1) = \bar{q}(1,1,1) = 1$.

Also, $\bar{p}(1,0,1) = \bar{p}(1,1,1) = 1$.

Thus, expression q implies expression p, i.e., q is an implicant of p. Next, we will show that q is a prime implicant.

Now, $q = x_1x_3$. Remove one factor x_3 from q and let $q_1 = x_1$. Then $\bar{q}_1(1,0,0) = 1$ while $\bar{p}(1,0,0) = 0$. Thus, q_1 does not imply p.

Similarly, remove x_1 from q and let $q_2 = x_3$. Then $\bar{q}_2(0,0,1) = 1$ while $\bar{p}(0,0,1) = 0$. Thus, q_2 does not imply p.
Hence, q is a prime factor of p.

Theorem 8.1. A Boolean polynomial $p \in P_n$ is equivalent to the sum of all prime implicants of p.

Definition 8.11. A sum of prime implicants of p is called irredundant if it is equivalent to p, but does not remain equivalent if any of its summands is removed.
A minimal sum-of-product expression must be irredundant.

Now, we describe a method a method to obtain a minimal form of a Boolean polynomial, namely Quine Mc-Clusky Method.

8.4.1 Quine Mc-Clusky Method

We begin with disjunctive normal form of a Boolean polynomial and obtain all prime implicants. We make the sum of prime implicants irredundant to obtain the minimal form of p. We will explain it with the help of an example.

Let p be a Boolean polynomial whose DN form d is given as

$$d = wxyz' + wxy'z' + wx'yz + wx'yz' + w'x'yz + w'x'yz' + w'x'y'z.$$

Step 1. Represent all product expressions in terms of zero-one-sequences, such that x_i and x_i' are denoted by 1 and 0, respectively. Missing variables are indicated by a '–'(dash), e.g., $w'x'y'z$ is 0001, $w'x'z$ is $00-1$.

Step 2. The product expressions, regarded as binary n-tuples, are partitioned into classes according to their numbers of ones. We sort the classes according to increasing numbers of ones. In our example,

					row number
$w'x'y'z$	0	0	0	1	(1)
$w'x'yz'$	0	0	1	0	(2)
$w'x'yz$	0	0	1	1	(3)
$wx'yz'$	1	0	1	0	(4)
$wxy'z'$	1	1	0	0	(5)
$wx'yz$	1	0	1	1	(6)
$wxyz'$	1	1	1	0	(7)

Step 3. Each expression with r ones is added to each expression containing $r+1$ ones. We only have to compare expressions in neighboring classes with dashes in the same position. If two expressions differ in exactly one position, then they are of the forms $p = i_1 i_2 \cdots i_r \cdots i_n$ and $q = i_1 i_2 \cdots i_r' \cdots i_n$, where all i_k are in $\{0, 1, -\}$, and $i_r \in \{0, 1\}$, respectively. Then p and q reduces to $i_1 i_2 \cdots i_{r-l} - i_{r+l} \cdots i_n$, and p and q are ticked. In our example this yields

					row number	
$w'x'y'z$	0	0	0	1	(1)	$\checkmark$
$w'x'yz'$	0	0	1	0	(2)	$\checkmark$
$w'x'yz$	0	0	1	1	(3)	$\checkmark$
$wx'yz'$	1	0	1	0	(4)	$\checkmark$
$wxy'z'$	1	1	0	0	(5)	$\checkmark$
$wx'yz$	1	0	1	1	(6)	$\checkmark$
$wxyz'$	1	1	1	0	(7)	$\checkmark$

$\Rightarrow$

row number					
(1)(3)	0	0	–	1	
(2)(3)	0	0	1	–	$\checkmark$
(2)(4)	–	0	1	0	$\checkmark$
(3)(6)	–	0	1	1	$\checkmark$
(4)(6)	1	0	1	–	$\checkmark$
(4)(7)	1	–	1	0	
(5)(7)	1	1	–	0	

The expressions with ticks are not prime implicants and will be subject to further reduction. They yield the single expression

row number				
(2)(3)(4)(6)	–	0	1	–

Step 4. Thus we have found all prime implicants, namely

row number					
(1)(3)	0	0	–	1	w'x'z
(4)(7)	1	–	1	0	wyz'
(5)(7)	1	1	–	0	wxz'
(2)(3)(4)(6)	–	0	1	–	x'y

As the sum of all prime implicants is not necessarily in minimal form (because some summands might be superfluous), we perform the last step in the procedure.

Step 5. Construct a table of prime implicants, heading elements for the columns are the product expressions in d, and at the begining of the rows are the prime implicants calculated in Step 3. A cross $\times$ is marked off at the intersection of the ith row and jth column if the prime implicant in the ith row is a subproduct of the product expression in the jth column.

A product expression is said to cover another product expression if it is a subproduct of the latter one. In order to find a minimal sum of prime implicants, which is equivalent to d, we choose a subset of the set of prime implicants in such a way that each product expression in d is covered by at least one prime implicant of the subset.

A prime implicant is called a main term if it covers a product expression which is not covered by any other prime implicant; the sum of the main terms is called the core.

Either the summands of the core together cover all product expressions in d; then the core is already the (unique) minimal form of d. Otherwise, we denote by $q_1, ..., q_k$ those product expressions which are not covered by prime implicants in the core. The prime implicants not in the core are denoted by $p_l, ..., p_m$ · We form a second table with index elements q_j for the columns and index elements p_i for the rows. The mark $\times$ is placed in the entry (i, j) indicating that p_i covers q_j. We then try to find a minimal subcollection of $p_1, ..., p_m$ which covers all of $q_1, ..., q_k$ and add them to the core.

In our example, we get the following table of prime implicants:

		(1)	(2)	(3)	(4)	(5)	(6)	(7)
(1)(3)	00–1	×		×				
(4)(7)	1–10				×			×
(5)(7)	11–0					×		×
(2)(3)(4)(6)	–01–		×	×	×		×	

The core is given by the sum of those prime implicants which are the only ones to cover a summand in d, namely by the sum of $00-1$, $-01-$, and $11-0$. This sum already covers all summands in d, so the minimal form of d is given by the core $w'x'z + y'z + wxz'$. The prime implicant wyz' was superfluous.

Example 8.10. Find all prime implicants of $f = w'x'y'z' + w'x'yz' + w'xy'z + w'xyz' + w'xyz + wx'y'z' + wx'yz + wxy'z + wxyz + wxyz'$ and find the minimal form of f using the Quine-McCluskey method.

Solution. Steps 1 and 2.

						row number	
0 ones	$w'x'y'z'$	0	0	0	0	(1)	$\surd$
1 ones	$w'x'yz'$	0	0	1	0	(2)	$\surd$
	$wx'y'z'$	1	0	0	0	(3)	$\surd$
2 ones	$w'xy'z$	0	1	0	1	(4)	$\surd$
	$w'xyz'$	0	1	1	0	(5)	$\surd$
3 ones	$w'xyz$	0	1	1	1	(6)	$\surd$
	$wx'yz$	1	0	1	1	(7)	$\surd$
	$wxy'z$	1	1	0	1	(8)	$\surd$
	$wxyz'$	1	1	1	0	(9)	$\surd$
4 ones	$wxyz$	1	1	1	1	(10)	$\surd$

Step 3. Combination of rows i and j yields the following simplifications:

(1)(2)	0	0	–	0	A
(1)(3)	–	0	0	0	B
(2)(5)	0	–	1	0	C
(4)(6)	0	1	–	1	$\surd$
(4)(8)	–	1	0	1	$\surd$
(5)(6)	0	1	1	–	$\surd$
(5)(9)	–	1	1	0	$\surd$
(6)(10)	–	1	1	1	$\surd$
(7)(10)	1	–	1	1	D
(8)(10)	1	1	–	1	$\surd$
(9)(10)	1	1	1	–	$\surd$

Repeating this step by combining the rows as indicated gives

(4)(6)(8)(10)	–	1	–	1	E
(5)(6)(9)(10)	–	1	1	–	F

The marking of the expressions by $\surd$ or letters $A, B, ...$ is done after the simplification. Having found the prime implicants we denote them by A, B, C, D, E, F. Here is the list of all prime implicants of f.

(1)(2)	0	0	–	0	$w'x'z'$	A
(1)(3)	–	0	0	0	$x'y'z'$	B
(2)(5)	0	–	1	0	$w'yz'$	C
(7)(10)	1	–	1	1	wyz	D
(4)(6)(8)(10)	–	1	–	1	xz	E
(5)(6)(9)(10)	–	1	1	–	xy	F

Step 4. We make the table of prime implicants, where the first "row" represents the product expressions of f and first "column" represent all the prime implicants of f.

		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
0 0 – 0	A	×	×								
– 0 0 0	B	×		×							
0 – 1 0	C		×			×					
1 – 1 1	D							×			×
– 1 – 1	E				×		×		×		×
– 1 1 –	F					×	×			×	×

The product expressions numbered $(3), (4), (7), (8)$ and (9) are implied by exactly one prime implicant and therefore, the core, i.e., the sum of the main terms, is $B + D + E + F$ (in our short notation). Column (2) is the only product expression that is not covered by the core. The prime implicants which are not in the core are A and C. The new table is as follows:

		(2)
0 0 – 0	A	×
0 – 1 0	C	×

This means that the minimal form of f is

$$A + B + D + E + F$$

if we use A; it is

$$C + B + D + E + F$$

if we choose C. In our usual notation the minimal form of f is

$$w'x'z' + x'y'z' + wyz + xz + xy$$

or

$$w'yz' + x'y'z' + wyz + xz + xy.$$

8.4.2 Karnaugh Map

In this section we describe a different way of representing Boolean polynomials, namely via Karnaugh Map (or Karnaugh diagrams).

Definition 8.12. Karnaugh diagram for n-variables is a rectangle divided into 2^n cells where each cell represents a minterm in the variables.

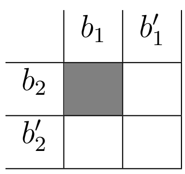
We explain it with the help of an example. Consider the polynomial $p = x_1x_2$ with two variables.

row	b_1	b_2	minterm	$\bar{p}(b_1, b_2) = b_1b_2$
(1)	0	0	$x_1'x_2'$	0
(2)	1	0	x_1x_2'	0
(3)	0	1	$x_1'x_2$	0
(4)	1	1	x_1x_2	1

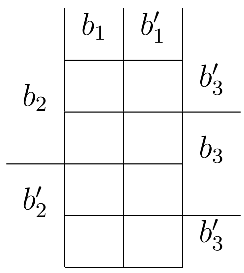
The minterms in forth column has value 1 for $(1, 1)$ and value 0 everywhere else. The Karnaugh diagram for two variables consists of $2^2 = 4$ cells. It consists of a b_1 and b_1' columns and a b_2 and b_2' row for two input variables b_1, b_2.

	b_1	b_1'
b_2	(4)	(3)
b_2'	(2)	(1)

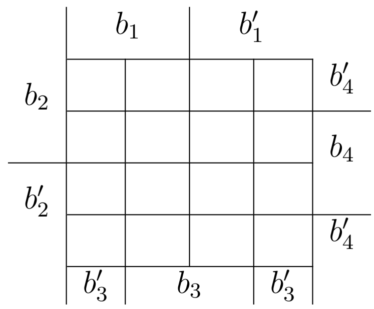
Each section in the intersection of a row and a column corresponds to a minterm. We shade the cell corresponding the minterm where the polynomial function has value 1. In the case of the function $\bar{p}$ above, we have shaded the section corresponding to x_1x_2 where $\bar{p}$ has value 1; the others have value 0.



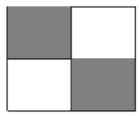
Karnaugh diagrams with three input variables b_1, b_2, b_3 can be presented as follows:



Karnaugh diagram for four input variables are of the following form:



We give examples of the Karnaugh diagrams of some polynomials in x_1 and x_2:

$x_1' + x_2'$:  $x_1x_2 + x_1'x_2'$:  $x_1'x_2 + x_1x_2'$: 

Steps to Simplify Boolean Polynomial using Karnaugh Diagram

Karnaugh diagrams can be used to simplify Boolean polynomials.

- We try to collect as many shaded portions of the diagram as possible to form a block, which represent a simple polynomial.
- We may use shaded parts of the diagram more than once, since the polynomials corresponding to blocks are connected by '+'.
- The idea is to identify the largest possible blocks and to cover all shaded cells (or 1's cell) with the fewest blocks, using the largest block first.

Example 8.11. Use a Karnaugh diagram to simplify the following:

(i) $xy + xy'$

(ii) $xy' + x'y + x'y'$

Solution. (i) For $p = xy + xy'$ the Karnaugh diagram is given in Figure 8.1. The two shaded cells can be grouped together in one block and represents the polynomial y. Thus, the minimal form of p is y, i.e., $p \sim y$ as $x + x' = 1$.

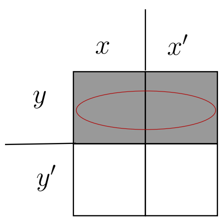


Figure 8.1:

(ii) For $q = xy' + x'y + x'y'$ the karnaugh diagram is given in Figure 8.2. The shaded cells are covered in two groups of blocks. One block represents x' and the other represents y'. Thus $q \sim x' + y'$.

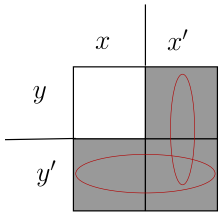


Figure 8.2:

Example 8.12. Simplify the polynomial $p = (x + y)(x + z) + xyz$ using Karnaugh diagram.

Solution. The Karnaugh diagram of p is shown in Figure 8.3. The diagram consists of two blocks. The vertical block represents x and the other block represents yz as it is in intersection of y and z. Thus, $p \sim x + yz$.

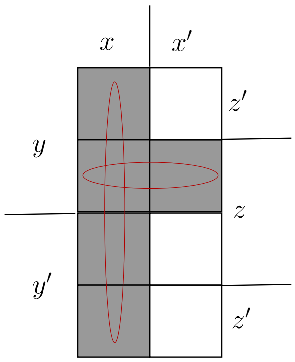


Figure 8.3:

Example 8.13. Find the minimal form for $p = x_1x_2x_3' + x_1'x_2x_4 + x_2x_3x_4' + x_1'x_2'x_4 + x_2x_3x_4 + x_1'x_2x_3'x_4'$ using Karnaugh diagram.

Solution. The Karnaugh diagram of p is shown in Figure 8.4. The diagram consists of two blocks. The horizontal block represents x_2 and the other block represents $x_1'x_4$. Thus, $p \sim x_2 + x_1'x_4$.

Example 8.14. Find simple function for the Karnaugh diagram shown in Figure 8.5.

Solution. The Boolean polynomial for the given Karnaugh diagram is $p = x_2x_4' + x_1'x_3 + x_1'x_2'x_4$.

In-text Exercise 8.3. Attempt the following questions:

1. Use Quine Mc-Clusky method to find the minimal form of P whose disjunctive normal form is $xy'z + x'yz' + xyz' + xyz$.

2. Use Karnaugh diagram to find the minimal form of $p = xyz + xyz' + x'yz + x'yz'$.

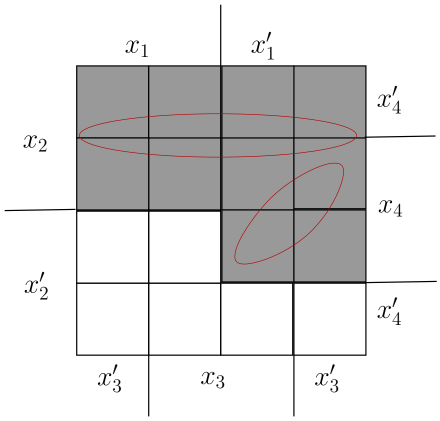


Figure 8.4:

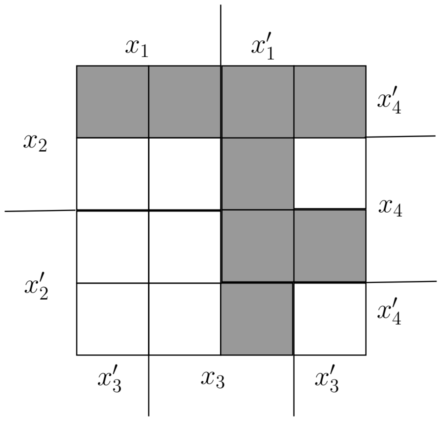


Figure 8.5:

8.5 Summary

1. To simplify notation, we write $\mathbf{p}+\mathbf{q}$ for $\mathbf{p} \vee \mathbf{q}$ and $\mathbf{pq}$ for $\mathbf{p} \wedge \mathbf{q}$.
2. A product expression (briefly a product) is a Boolean polynomial in which '+' does not occur. A product expression in which every variable or its complement is presented once is called a minterm.
3. A representation of a Boolean polynomial $p \in P_n$ as a sum of product of x_1 (or x_1'), x_2 (or x_2'),..., x_n (or x_n') is called its disjunctive normal form (in short DN form).
4. Steps to write Disjunctive Normal Form of a given Boolean polynomial
   (a) If $p \in P_n$, we first write down the truth table of $\bar{p}$.
   (b) We look at each $(b_1, b_2, ..., b_n) \in \mathbb{B}^n$ for which $\bar{p}(b_1, b_2, ..., b_n) = 1$ and write down the term $x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$, where $x_i^1 = x_i$ and $x_i^0 = x_i'$.
   (c) The sum of all such terms is equivalent to p and is the required DN form of p.

(d) We further reduce or simplify it using Boolean arithmetic to get a shorter form.

5. A maxterm is a sum expression in which each variable or its complement appears once. For example, $x_1 + x_2' + x_3$ is a max term in P_3.

6. A representation of a Boolean polynomial p as the product of maxterms is called the conjunctive normal form (in short, CN form) of p.

7. In the disjunctive normal form of a given polynomial, if we interchange the roles of $0, 1$ and '+', '·', we get the conjunctive normal form.

8. Steps to write Conjunctive Normal Form of a given Boolean polynomial

   (a) If $p \in P_n$, we first write down the truth table of $\bar{p}$.

   (b) We look at each $(b_1, b_2, ..., b_n) \in \mathbb{B}^n$ for which $\bar{p}(b_1, b_2, ..., b_n) = 0$ and write down the term $x_1^{b_1} + x_2^{b_2} + \cdots + x_n^{b_n}$, where $x_i^1 = x_i'$ and $x_i^0 = x_i$.

   (c) The product of all such terms is equivalent to p and is the required CN form of p.

9. The minimal form of a Boolean polynomial f is the shortest sum of product expression with the smallest possible number of literals which is equivalent to f.

10. An expression p implies an expression q if for all $b_1, b_2, ..., b_n \in \mathbb{B}$, $\bar{p}_{\mathbb{B}}(b_1, b_2, ..., b_n) = 1 \Rightarrow \bar{q}_{\mathbb{B}}(b_1, b_2, ..., b_n) = 1$. In this case, p is called an implicant of q.

11. A prime implicant for an expression p is a product expression α which implies p, but which does not imply p if one factor in α is deleted. A product β whose factors form a subset of the factors of another product, say α, is called subproduct of α.

12. A Boolean polynomial $p \in P_n$ is equivalent to the sum of all prime implicants of p.

13. A sum of prime implicants of p is called irredundant if it is equivalent to p, but does not remain equivalent if any of its summands is removed.

14. A minimal sum of product expression must be irredundant.

15. Quine Mc-Clusky Method and Karnaugh maps (or Karnaugh Diagrams) are two ways to obtain minimal form of Boolean polynomials.

8.6 Self Assessment Exercise

1. Find the disjunctive normal form of

$$((x_2 + x_1x_3)(x_1 + x_3)x_2)'.$$

2. Find the disjunctive normal form of

$$(x'y + xyz' + xy'z + x'y'z't + t')'.$$

3. Find the conjunctive normal form of

$$(x_1 + x_2 + x_3)(x_1x_2 + x_1'x_3)'.$$

4. Find the disjunctive normal form of

$$x_1'x_2 + x_3(x_1' + x_2).$$

5. Find hte disjunctive normal form of the polynomial whose conjunctive normal form is $(x + y + z)(x + y + z')(x + y' + z)(x + y' + z')(x' + y + z)$.

6. Use the Quine Mc-Clusky method to find a minimal form of $xyz' + xy'z + xy'z' + x'yz + x'y'z$.

7. Find all the prime implicants of $f = wx'y'z + w'xy'z' + wx'y'z' + w'xyz + w'x'y'z' + wxyz + wx'yz + w'xyz' + w'x'yz'$. by using Quine Mc-Clusky method and further minimize it.

8. Use a Karnaugh diagram to simplify the following:

    (i) $x_1x_2x_3' + x_1'x_2x_3' + (x_1 + x_2'x_3')(x_1 + x_2 + x_3)' + x_3(x_1' + x_2)$

    (ii) $xyz + xy'z + xy'z' + x'yz' + x'yz + x'y'z'$

    (iii) $(x_1 + x_2)(x_1 + x_3) + x_1x_2x_3$

    (iv) $x_1x_2'x_3 + x_1x_2'x_3' + x_1'x_2x_3 + x_1x_2x_3 + x_1'x_2'x_3'$

    (v) $x_1x_2x_3 + x_2x_3x_4 + x_1'x_2x_4' + x_1'x_2x_3x_4' + x_1'x_2'x_4'$

8.7 Solutions to In-text Exercises

Excercise 2.1

1. (i) $x + y$

    (ii) $x + z$

2. $x'z' + y'z' + x'y$

3. (i) $x_1x_3' + x_1x_2$

(ii) $x_2' + x_1' x_2 x_3'$

Excercise 2.2

1. $(x + y + z)(x' + y + z')(x + y + z')(x + y' + z)(x + y' + z')(x' + y' + z')$
2. $(x + y + z)(x + y + z')(x + y' + z)(x + y' + z')(x' + y + z)$
3. $(x + y + z')(x + y' + z')$

Exercise 2.3

1. $yz' + xz$
2. y

8.8 Suggested Reading

[1]Davey, B. A., & Priestley, H. A. (2002). Introduction to lattices and order. Cambridge university press.

[2] Lidl, R., & Pilz, G. (2012). Applied abstract algebra. Springer Science & Business Media.

[3] Kolman, B., Busby, R. C., & Ross, S. (1995). Discrete mathematical structures. Prentice-Hall, Inc.

Lesson - 9

Switching Circuits

Structure

9.1 Learning Objectives

After reading this lesson, the reader should be able:

- to learn the mathematical way of designing a diagram of a circuit.
- to learn to draw symbolic representation of a circuit.
- to learn applications of switching circuit.

9.2 Introduction

One of the most important applications of lattice theory and also one of the oldest applications of modern algebra is the use of Boolean algebras in modeling and simplifying switching or relay circuits. The aim of this chapter is to describe electrical or electronic switching circuits in a mathematical way or to design a diagram of a circuit with given properties. We will use logic gates to present diagrams of switching circuits.

9.3 Electrical Circuits

Definition 9.1. A switch is a device in an electric circuit which lets (or does not let) the current to flow through the circuit. The switch can assume two states: closed and open.
Closed (On) state allows the current to flow and Open (off) state that does not allow the current to flow. The closed and open switches are symbolized as shown in Figure 9.1

Figure 9.1:

Definition 9.2. Two switches S_1 and S_2 are inter connected in either series or in parallel.

(a) Two switches S_1 and S_2 are said to be connected in series if the current pass only when both are in closed state and current does not flow if any one of the switches or both switches are open. It is symbolized as shown in Figure 9.2.

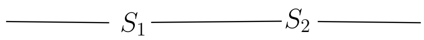


Figure 9.2:

(b) Two switches S_1 and S_2 are said to be connected in parallel if current flows when any one or both are closed and does not flow when both are open. It is symbolized as shown in Figure 9.3.

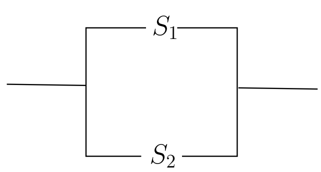


Figure 9.3:

Note. The symbol S_1' indicates a switch which is open if and only if S_1 is closed and is called complement of S_1.
If a switch S_1 appears in two separate places in a circuit, then they are either both open or both closed.

Definition 9.3. The following definitions give a connection between electrical switches and the elements of a Boolean algebra. Let $X_n = \{x_1, x_2, ..., x_n\}$.

(i) Each $x_1, x_2, ..., x_n \in X_n$ is called a switch.

(ii) Every $p \in P_n$ is called a switching circuit.

(iii) x_i' is called the complementation switch of x_i.

(iv) $x_i x_j$ is called the series connection of x_i and x_j.

(v) $x_i + x_j$ is called the parallel connection of x_i and x_j.

(vi) For $p \in P_n$ the corresponding polynomial function $\bar{p} \in P_n(\mathbb{B})$ is called the switching function of p.

(vii) $\bar{p}(a_1, a_2, ..., a_n)$ is called the value of the switching circuit p at $a_1, a_2, ..., a_n \in \mathbb{B}$. The $a_i's$ are called input variables.

The mathematical models of circuits can be graphically represented by using contact diagrams. Instead of S_i we use x_i according to Definition 9.3. For instance, the polynomial (i.e., the circuit) $x_1x_2 + x_1x_3$ can be represented as

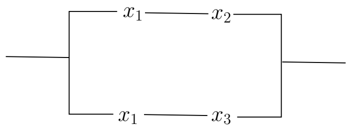


Figure 9.4:

The electrical realization of the same circuit would be

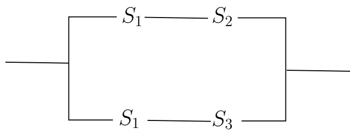


Figure 9.5:

Example 9.1. Draw the contact diagram of the polynomial $x((y+w')+z'(x+w+z'))y$.

Solution. The contact diagram of the polynomial is given by the diagram in Figure 9.6.

Example 9.2. Draw the contact diagram of the polynomial $x_1(x_2(x_3+x_4)+x_3(x_5+x_6))$.

Solution. The contact diagram of the polynomial is given by the diagram in Figure 9.7.

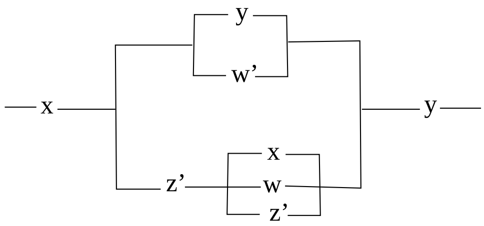


Figure 9.6:

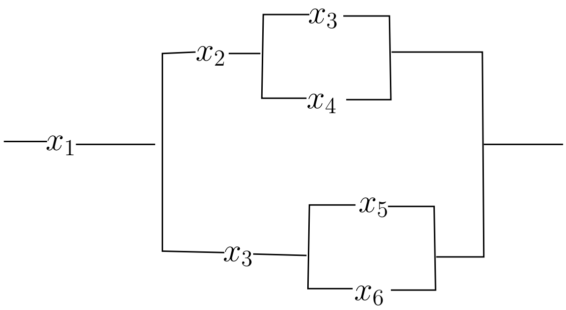


Figure 9.7:

Note. In order to find a possible simplification of an electrical circuit retaining its original switching properties we can look for a "simple" Boolean polynomial which is equivalent to the original polynomial. This can be done by transposing the given polynomial into disjunctive normal form and then applying the Quine-McCluskey algorithm.

Example 9.3. Simplify $p = (x_1 + x_2)(x_1 + x_3) + x_1x_2x_3$ and draw the contact diagram of the simplified form.

Solution.

$$\begin{aligned} p &= (x_1 + x_2)(x_1 + x_3) + x_1x_2x_3 \\ &\sim x_1 + x_1x_2 + x_2x_3 + x_1x_2x_3 \\ &\sim x_2x_3 + (x_1 + x_1x_2 + x_1x_2x_3) \\ &\sim x_2x_3 + x_1 \end{aligned}$$

Thus, $p \sim x_1 + x_2x_3$ and the contact diagram of it is as follow:

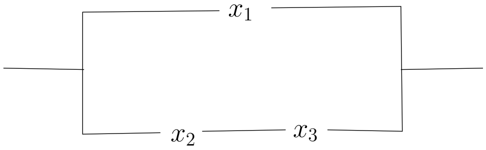


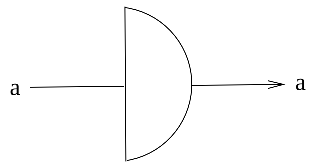
Figure 9.8:

9.4 Logic Gates

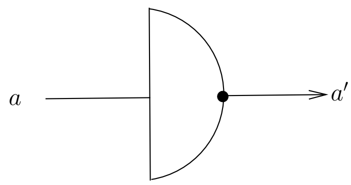
Nowadays, electrical switches are of less importance than semiconductor elements. These elements are types of electronic blocks which are predominant in the logical design of digital building components of electronic computers. In this context the switches are represented as so-called gates, or combinations of gates. We call this the symbolic representation. Thus a gate (or a combination of gates) is a polynomial p which has, as values in $\mathbb{B}$, the elements obtained by replacing x_i by $a_i \in \mathbb{B}$ for each i. We also say that the gate is a realization of a switching function. If $\bar{p}(a_1, ..., a_n) = 1$ (or 0), we have current (or no current) in the switching circuit p.

Definition 9.4. We define some special gates as follows:

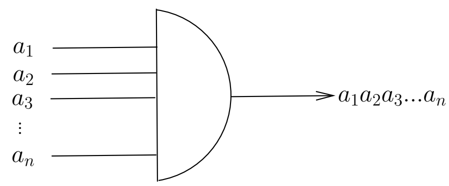
(i) Identity Gate
It symbolizes the polynomial x i.e., $p(x) = x$, and is shown as follows:



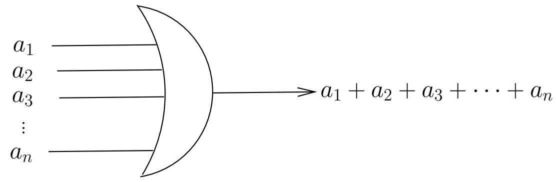
(ii) NOT-Gate (or Inverter Gate)
It symbolizes the polynomial x' i.e., $p(x) = x'$, and is shown as follows:



(iii) AND-Gate
It symbolizes the polynomial $p(x_1, x_2, ..., x_n) = x_1x_2...x_n$, and is shown as follows:



(iv) OR-Gate
It symbolizes the polynomial $p(x_1, x_2, ..., x_n) = x_1 + x_2 + \cdots + x_n$, and is shown as follows:



Note. A short notation for the NOT-gate is to draw a black disc immediately before or after one of the other gates to indicate complement. Some examples are shown in Figure 9.9.

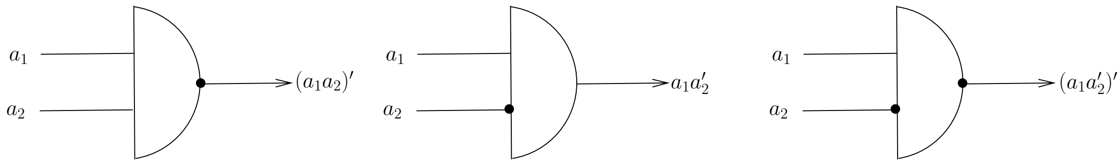
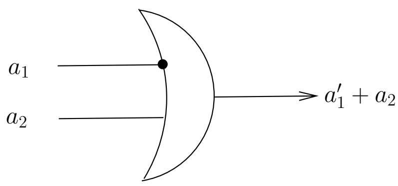


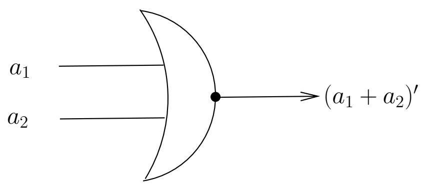
Figure 9.9: NOT-Gates

Definition 9.5. In propositional logic the three more polynomials $(x_1' + x_2), (x_1 + x_2)'$ and $(x_1x_2)'$ are also defined and the gates corresponding to these are as follows:

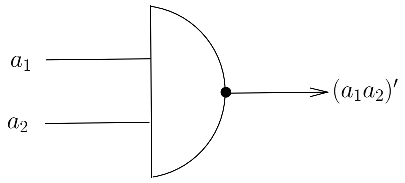
1. Subjunction Gate
   It symbolizes the polynomial $p(x_1, x_2) = x_1' + x_2$, and is shown as follows:



2. NOR-Gate (NOT + OR)
   It symbolizes the polynomial $p(x_1, x_2) = (x_1 + x_2)'$, and is shown as follows:

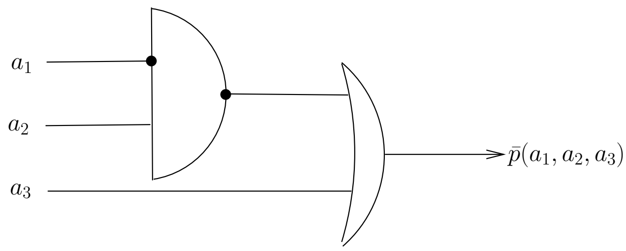


3. NAND-Gate (NOT + AND)
   It symbolizes the polynomial $p(x_1, x_2) = (x_1x_2)'$, and is shown as follows:



Exercise 10. Determine the symbolic representation of $p = (x_1'x_2)' + x_3$.

Solution. The symbolic representation is as follows:



Exercise 11. Determine the Boolean polynomial p of the circuit given in Figure 9.10

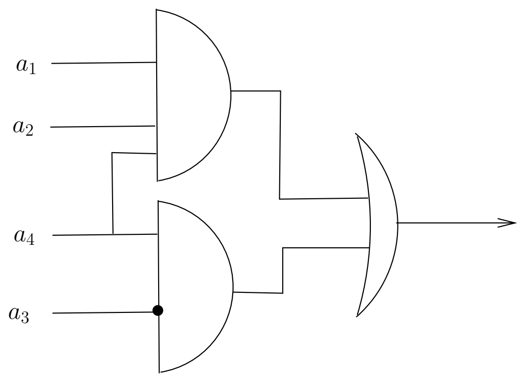


Figure 9.10:

Solution. The polynomial corresponding to the given circuit is $q = x_1x_2x_4 + x_3'x_4$.

In-text Exercise 9.1. Attempt the following exercise questions:

1. Determine the symbolic representation of the circuit given by $p = (x_1 + x_2 + x_3)(x_1' + x_2)(x_1x_3 + x_1'x_2)(x_2' + x_3)$.

2. Determine the Boolean polynomial p of the circuit given in Figure 9.11.

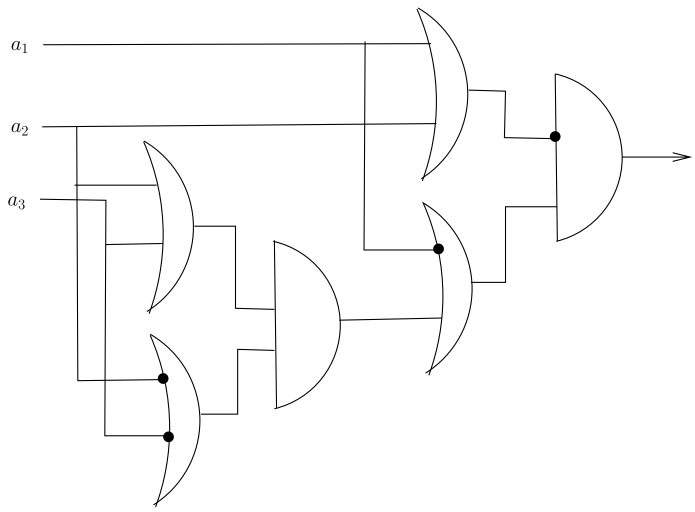


Figure 9.11:

9.5 Applications of Switching Circuits

In this section we describe some of the applications of switching circuits by examples.

Example 9.4. In a large room there are electrical switches next to the three doors to operate the central lighting. The three switches operate alternatively, i.e., each switch can switch on or switch off the lights. We wish to determine the switching circuit p, its symbolic representation, and contact diagram.

Each switch has two positions: either on or off. We denote the switches by x_1, x_2, x_3 and the two possible states of the switches x_i by $a_i \in \{0, 1\}$. The light situation in the room is given by the value $\bar{p}(a_1, a_2, a_3) = 0 (= 1)$ if the lights are off (are on, respectively). We arbitrarily choose $\bar{p}(1, 1, 1) = 1$.

(i) If we operate one or all three switches, then the lights go off, i.e., we have $\bar{p}(a_1, a_2, a_3) = 0$ for all (a_1, a_2, a_3) which differ in one or in three places from $(1, 1, 1)$.

(ii) If we operate two switches, the lights stay on, i.e., we have $\bar{p}(a_1, a_2, a_3) = 1$ for all those (a_1, a_2, a_3) which differ in two places from $(1, 1, 1)$.

This yields the following table of function values:

a_1	a_2	a_3	minterms	$\bar{p}(a_1, a_2, a_3)$
1	1	1	$x_1x_2x_3$	1
1	1	0	$x_1x_2x_3'$	0
1	0	1	$x_1x_2'x_3$	0
1	0	0	$x_1x_2'x_3'$	1
0	1	1	$x_1'x_2x_3$	0
0	1	0	$x_1'x_2x_3'$	1
0	0	1	$x_1'x_2'x_3$	1
0	0	0	$x_1'x_2'x_3'$	0

From this tabular we can derive the DN form for the switching circuit p which is as follows:

$$p = x_1x_2x_3 + x_1x_2'x_3' + x_1'x_2x_3' + x_1'x_2'x_3.$$

This p is in minimal form. The symbolic representation of the circuit p is given in Figure 9.12.

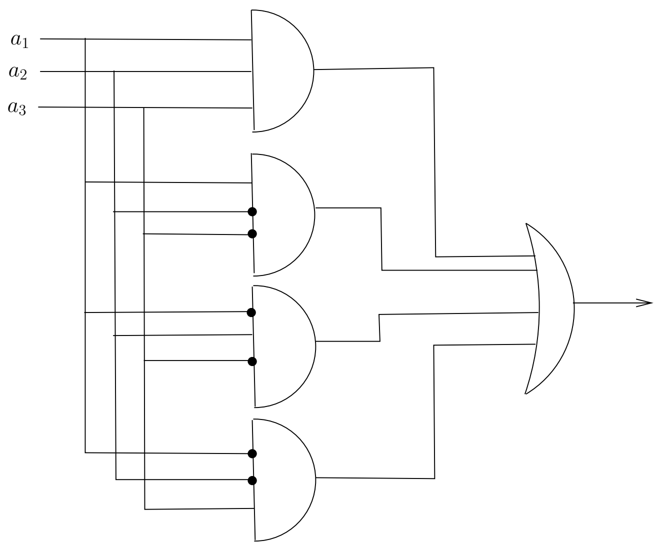


Figure 9.12:

This switching circuit can also be represented as

$$\begin{aligned} p &= x_1x_2x_3 + x_1x_2'x_3' + x_1'x_2x_3' + x_1'x_2'x_3 \\ &\sim (x_1(x_2x_3 + x_2'x_3')) + (x_1'(x_2x_3' + x_2'x_3)) \end{aligned}$$

The contact diagram of this circuit is as follows:

Example 9.5. A motor is supplied by three generators. The operation of each generator is monitored by a corresponding switching element which closes a circuit as soon as a generator fails. We demand the following conditions from the electrical monitoring system:

(i) A warning lamp lights up if one or two generators fail.

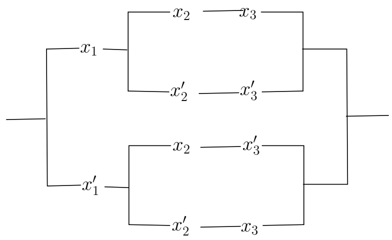


Figure 9.13:

(ii) An acoustic alarm is initiated if two or all three generators fail.

Determine the electric circuit and the corresponding symbolic representation of the circuit.

We determine a symbolic representation as a mathematical model of this problem. Let $a_i = 0$ denote that generator i is operating, $i \in \{1, 2, 3\}$; $a_i = 1$ denotes that generator i does not operate. The table of function values has two parts $p_1(a_1, a_2, a_3)$ and $p_2(a_1, a_2, a_3)$, defined by:

$$\begin{array}{lll} \bar{p_1}(a_1, a_2, a_3) & = 1: & \text{acoustic alarm sounds;} \\ \bar{p_1}(a_1, a_2, a_3) & = 0: & \text{acoustic alarm does not sound;} \\ \bar{p_2}(a_l, a_2, a_3) & = 1: & \text{warning lamp lights up;} \\ \bar{p_2}(a_1, a_2, a_3) & = 0: & \text{warning lamp is not lit up} \end{array}$$

Then we obtain the following table for the function values:

a_1	a_2	a_3	$\bar{p_1}(a_1, a_2, a_3)$	$\bar{p_2}(a_1, a_2, a_3)$
1	1	1	1	0
1	1	0	1	1
1	0	1	1	1
1	0	0	0	1
0	1	1	1	1
0	1	0	0	1
0	0	1	0	1
0	0	0	0	0

For p_1 we choose the disjunctive normal form, namely

$$\begin{aligned} p &= x_1x_2x_3 + x_1x_2x_3' + x_1x_2'x_3 + x_1'x_2x_3 \\ &\sim x_1x_2 + (x_1x_2' + x_1'x_2)x_3 \\ &\sim (x_1x_2 + (x_1x_2' + x_1'x_2))(x_1x_2 + x_3) \\ &\sim ((x_1x_2 + x_1x_2') + x_1'x_2)(x_1x_2 + x_3) \\ &\sim (x_1 + x_1'x_2)(x_1x_2 + x_3) \\ &\sim (x_1 + x_2)(x_1x_2 + x_3) \\ &\sim x_1x_2 + x_1x_2 + x_1x_3 + x_2x_3 \\ &\sim x_1x_2 + x_1x_3 + x_2x_3. \end{aligned}$$

For p_2 we choose conjunctive normal form, which is preferable when there are many 1's as function values:

$$p_2 = (x_1 + x_2 + x_3)(x_1' + x_2' + x_3').$$

The symbolic representation is given in Figure 9.14

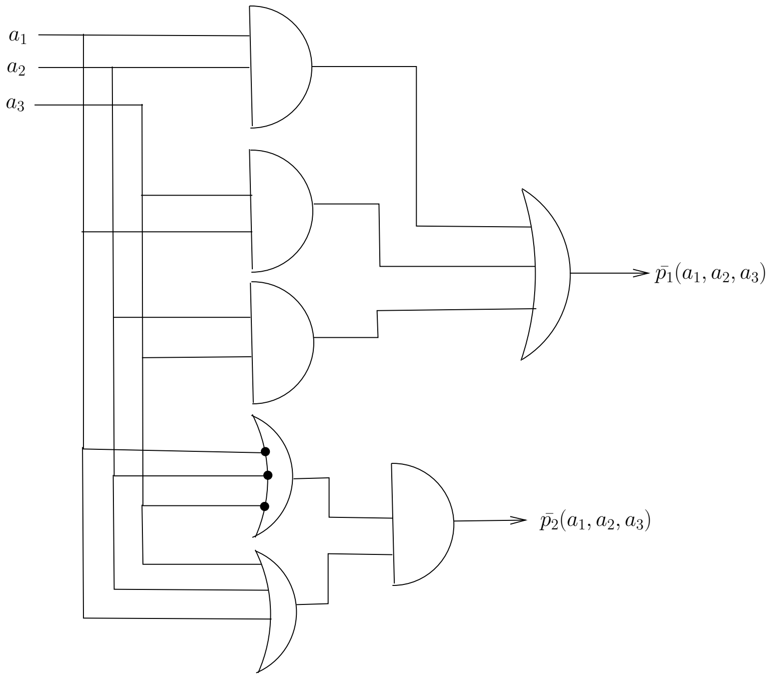


Figure 9.14:

Exercise 12. A voting-machine for three voters has three YES-NO switches. Current is in the circuit precisely when YES has a majority. Draw the contact diagram and the symbolic representation by gates and simplify it.

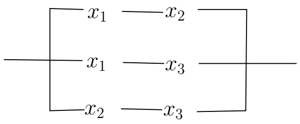
Solution. We determine a symbolic representation as a mathematical model of this problem. Let $a_i = 0$ denote that voter i has pressed NO switch, $i \in \{1, 2, 3\}$; $a_i = 1$ denotes that voter i has pressed YES switch. Let $\bar{p}(a_1, a_2, a_3) = 1$ means YES has majority. Then the table of function values of circuit p is as follows:

a_1	a_2	a_3	$\bar{p}(a_1, a_2, a_3)$
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

From this tabular we can derive the DN form for the switching circuit p which is as follows:

$$p = x_1x_2x_3 + x_1x_2x_3' + x_1x_2'x_3 + x_1'x_2x_3 \sim x_1x_2 + x_1x_3 + x_2x_3.$$

The contact diagram of this circuit is as follows:



The symbolic representation is shown in Figure 9.15:

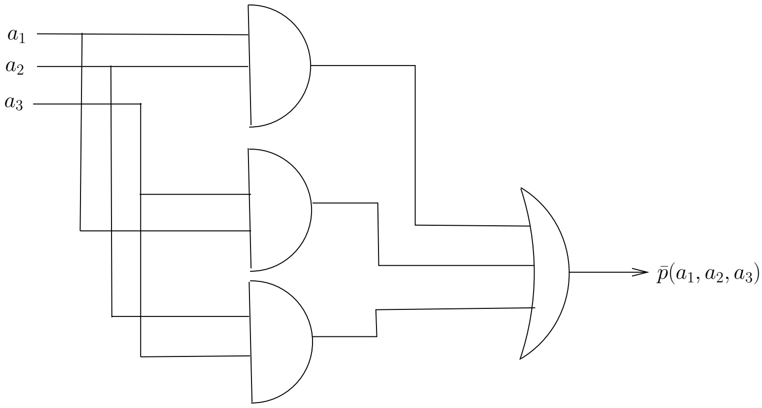


Figure 9.15:

In-text Exercise 9.2. 1. An oil pipeline has three pipelines b_1, b_2, b_3 which feed it. Design a plan for switching off the pipeline at three points S_1, S_2, S_3 such that oil flows in the following two situations: S_1 and S_3 are both open or both closed but S_2 is open; S_1 is open and S_2, S_3 are closed.

9.6 Summary

In this chapter we have covered the following points:

1. A switch is a device in an electric circuit which lets (or does not let) the current to flow through the circuit. The switch can assume two states: closed and open. Closed (On) state allows the current to flow and Open (off) state that does not allow the current to flow.

2. Two switches S_1 and S_2 are said to be connected in series if the current pass only when both are in closed state and current does not flow if any one of the switches or both switches are open.

3. Two switches S_1 and S_2 are said to be connected in parallel if current flows when any one or both are closed and does not flow when both are open.

4. The symbol S_1' indicates a switch which is open if and only if S_1 is open and is called complement of S_1.

5. A connection between electrical switches and the elements of a Boolean algebra is as follows: Let $X_n = \{x_1, x_2, ..., x_n\}$.

   (i) Each $x_1, x_2, ..., x_n \in X_n$ is called a switch.

   (ii) Every $p \in P_n$ is called a switching circuit.

   (iii) x_i' is called the complementation switch of x_i.

   (iv) $x_i x_j$ is called the series connection of x_i and x_j.

   (v) $x_i + x_j$ is called the parallel connection of x_i and x_j.

   (vi) For $p \in P_n$ the corresponding polynomial function $\bar{p} \in P_n(\mathbb{B})$ is called the switching function of p.

   (vii) $\bar{p}(a_1, a_2, ..., a_n)$ is called the value of the switching circuit p at $a_1, a_2, ..., a_n \in \mathbb{B}$. The a_i are called input variables.

6. A symbolic representation of a switching circuit is in terms of logic gates. A logic gate (or a combination of gates) is a polynomial p which has, as values in $\mathbb{B}$, the elements obtained by replacing x_i by $a_i \in \mathbb{B}$ for each i. We also say that the gate is a realization of a switching function. If $\bar{p}(a_1, ..., a_n) = 1$ (or 0), we have current (or no current) in the switching circuit p.

9.7 Self Assessment Exercise

1. Find the symbolic representation of a simple circuit for which the binary polynomial function f in three variables is defined as follows: f is 0 at $(0, 0, 1), (0, 1, 1), (0, 1, 0), (1, 1, 1), (1, 0, 0), (1, 1, 0)$, and has value 1 otherwise.

2. In a production process there are three motors operating, but only two are allowed to operate at the same time. Design a switching circuit which prevents that more than two motors can be switched on simultaneously.

3. Design a switching circuit that enables you to operate one lamp in a room from four different switches in that room.

4. A hall light is controlled by two switches, one upstairs and one downstairs. Design a circuit so that the light can be switched on or off from the upstairs or the downstairs.

9.8 Solutions to In-Text Exercises

Excercise 3.1

1. The symbolic representation of the circuit is given in Figure 9.16.

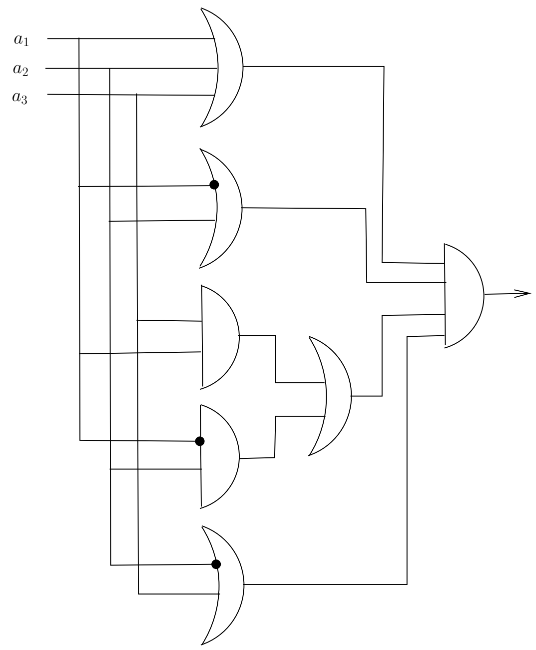


Figure 9.16:

2. The circuit is given by $p = ((x_2 + x_3)(x_2' + x_3') + x_1')(x_1 + x_2)'$.

Excercise 3.2

1. The circuit is given by

$$p = x_1x_2x_3 + (x_1'x_2 + x_1x_2')x_3'.$$

The symbolic representation of the circuit is given in Figure 9.17.

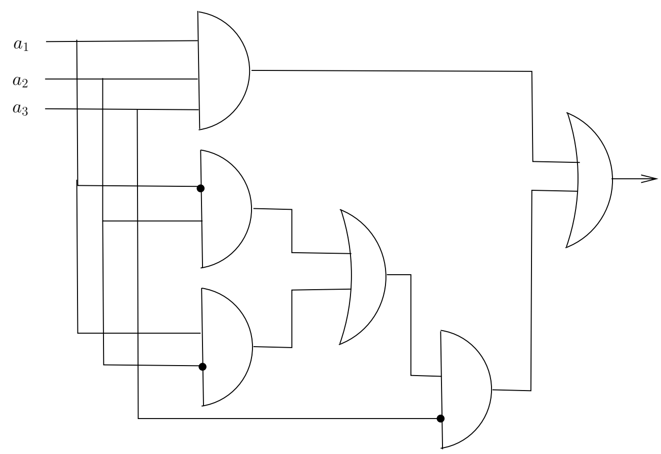


Figure 9.17:

9.9 References

[1]Davey, B. A., & Priestley, H. A. (2002). Introduction to lattices and order. Cambridge university press.

[2] Lidl, R., & Pilz, G. (2012). Applied abstract algebra. Springer Science & Business Media.

[3] Kolman, B., Busby, R. C., & Ross, S. (1995). Discrete mathematical structures. Prentice-Hall, Inc.

9.10 Suggested Readings

[1] Birkhoff, G. (1940). Lattice theory (Vol. 25). American Mathematical Soc.

[2] Grätzer, G. (2002). General lattice theory. Springer Science & Business Media.