BCA-05++-02

VARDHAMAN MAHAVEER OPEN UNIVERSITY, KOTA

Discrete Mathematics

Course Development Commitee

Chairman
Prof. (Dr.) Naresh Dadhich
Vice-Chancellor
Vardhaman Mahaveer Open University, Kota

Co-ordinator/Convener and Members

Convernor/Coordinator
Prof. (Dr.) D.S. Chauhan
Department of Mathematics
University of Rajasthan, Jaipur

Member Secretary/Coordinator
Sh. Rakesh Sharma
Assistant Professor (Computer Application)
V.M. Open University, Kota

Members

1. Prof. (Dr.) D.S. Chauhan
   Department of Mathematics
   University of Rajasthan, Jaipur
2. Prof. (Dr.) M.C. Govil
   Govt. Engineering College, Ajmer
3. Prof. (Dr.) A.K. Nagawat
   University of Rajasthan, Jaipur
4. Dr. (Mrs.) Madhavi Sinha
   BITS, Jaipur

Editing and Course Writing

Editor
Prof. (Dr.) D.S. Chauhan
Department of Mathematics
University of Rajasthan, Jaipur

Writers

1. Sh. Rajeev Srivastava
   HOD Computer Department
   L.B.S. College, Jaipur
2. Dr. Paresh Vyas
   Asstt. Prof. (Mathematics)
   University of Rajasthan, Jaipur
3. Dr. K. N. Singh
   Associate Prof. (Retd.)
   University of Rajasthan, Jaipur
4. Sh. Rakesh Pandey
   Lecturer Department of Mathematic
   S.S. Jain Subodh PG College Jaipu

Academic and Administrative Management

Prof. (Dr.) Naresh Dadhich
Vice-Chancellor
Vardhaman Mahaveer Open University,
Kota

Prof. (Dr.) M.K. Ghadoliya
Director (Academic)
Vardhaman Mahaveer Open University
Kota

Mr. Yogendra Goyal
Incharge
Material Production and Distribut
Department

Course Material Production

Mr. Yogendra Goyal
Incharge
Material Production Officer
Vardhaman Mahaveer Open University
Kota

Production : DEC. 2010 **ISBN 13/978-81-8496-249-9**

ted and published on behalf of Registrar V. M. Open University, Kota.
ted By THE POOJA,KOTA .500 Copies

Vardhaman Mahaveer Open University, Kota

Discrete Mathematics

UNIT 1 : Number System

Structure of the Unit

1.0 Objectives

After going through this unit student will be able to :

- To learn how data is represented in the computer.
- Understand various number system *i.e.* positional and non-positional.
- Learn to convert number from one number system to another.

1.1 Introduction

Ever since people discovered that it was necessary to count objects, they have been looking for easier ways to count them. The abacus, developed by the Chinese, is one of the earliest known calculators. It is still in use in some parts of the world. Man's earliest number or counting system was probably developed to help determine how many possessions a person had. As daily activities became more complex, numbers became more important in trade, time, distance, and all other phases of human life.

We are familiar with the decimal number system in which digits are 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9. Computer cannot understand all these characters because computer is an electronic device. It is a bistable device means with two states "On" and "Off". Therefore, computer deals with data converted into simplest form which can be processed electronically, that is in binary form, where it substitutes "On" with "1" and "Off" with 0.

The computer uses binary digits for its operation. In the binary system there are only two digits 0 and 1. The programmer feeds instruction and data in alphabets and decimal digits. But for the operation of the computer these are converted to binary bits.

To store and process data in a binary form, a coding scheme had been devised to represent characters as standardized methods. Data stored in a coded form is basically of three types-Numeric, Alphabetic and Alphanumeric. Every computer stores these data types in a coded form *i.e.* in binary number system.

This chapter deals with the conversion of binary numbers to decimal numbers and vice versa. It also deals with hexadecimal and octal system. Computer circuitry is usually designed to process hexadecimal or octal number. Before going into the details, it is essential to have a basic understanding of the number system.

1.2 Number system

Until now, you have probably used only one number system, the decimal system. You may also be familiar with the Roman numeral system, even though you seldom use it. Number systems are basically of two types :

- Non-Positional
- Positional

Non-positional number system :

In early days, human begins counted on fingers. When ten fingers were not adequate, stones, pebbles, or sticks were used to indicate values. This method of counting uses an additive approach or the non-positional number system. In this system, we have symbols such as I for 1, II for 2, III for 3,

IIII for 4, IIIII for 5, etc. is known as Roman Number System. Each symbol represents the same value regardless of its position in the number and the symbols are simply added to find out the value of a particular number. Since it is very difficult to perform arithmetic with such a number system, positional systems were developed.

Positional number system :

Positional notation is a system where the value of a number is defined not only by the symbol but by the symbol's position. In a positional number system, there are only a few symbols called digits, and these symbols represent different values depending on the position they occupy in the number.

Each position in the positional notation system represents a power of the base, or radix. A POWER is the number of times a base is multiplied by itself. The power is written above and to the right of the base and is called an EXPONENT. Examine the following base 10 line graph :

Radix point ↓ $10^3\ 10^2\ 10^1\ 10^0 \cdot 10^{-1}\ 10^{-2}\ 10^{-3}$
$10^3 = 10 \times 100$, or 1000
$10^2 = 10 \times 10$, or 100
$10^1 = 10 \times 1$, or 10
$10^0 = 1$(any number raised to the power of 0 equals 1)
$10^{-1} = 1 \div 10$, or .1
$10^{-2} = 1 \div 100$, or .01
$10^{-3} = 1 \div 1000$, or .001

The value of each digit in such a number is determined by three considerations:

1. The digit itself,
2. The position of the digit in the number, and
3. The base of the number system.

Base or Radix :

The base, or radix, of a number system tells you the number of symbols used in that system. The base of any system is always expressed in decimal numbers. The total number of digits available in the number system *i.e.* decimal number system contains 10 digits (*i.e.* 0 to 9) having base 10. Therefore number in this system is represented by $(\text{number})_{\text{base}}$ *i.e.* $275 = (275)_{10}$.

Computing the value of a positional number :

- A number = Digit x $\text{Base}^{(\text{position of the digit})}$

i.e. $(275)_{10} = 2 \times 10^2 + 7 \times 10^1 + 5 \times 10^0$.

Hence the value of a number can be viewed as the sum of the positional values of the symbols in the number. The rightmost symbol in the number has the lowest weight, whereas the leftmost symbol in

the number has the highest weight. Hence the rightmost and the leftmost symbols in a number are also called the **least significant digit (LSD)** and the **most significant digit (MSD)** respectively.

The following table shows the base and base set values of different number system :

Number system	Base	Base set	Largest 4 digit number
Decimal	10	0, 1, 2, 3, 4, 5, 6, 7, 8, 9	9999
Binary	2	0, 1	1111
Octal	8	0, 1, 2, 3, 4, 5, 6, 7	7777
Hexadecimal	16	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *A*, *B*, *C*, *D*, *E*, *F*	FFFF

1.2.1 Data representation in computers :

The computer system is made up of a number of electronic circuits. These circuits work on the basis of 2 states :

- Low charge
- High charge

The computer manipulates these different states so that it can do something useful. The binary system is ideal for this manipulation, since it is also based on the same concept of 2 states (numbers). The binary system is used to represent the 2 states in the computer – "0" for low charge and "1" for high charge. Other number systems can be used, but for them more than 2 states will have to be created, which is not practical.

1.2.2 Decimal Number System :

The terms *unit* and *number* when used with the decimal system are almost self-explanatory. By definition the unit is a single object. A number is a symbol representing a unit or a quantity.

The base of a number system is indicated by a subscript (decimal number) following the value of the number. The following are examples of numerical values in different bases with the subscript to indicate the base:

$$7592_{10} \quad 10_2 \quad 567_8$$

You should notice the highest value symbol used in a number system is always one less than the base of the system. In base 10 the largest value symbol possible is 9; in base 2 it is 1; in base 8 it is 7.

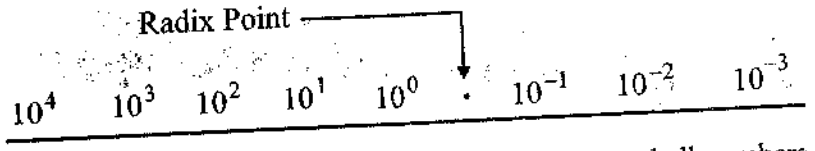
The base, or radix, of the decimal system is 10. There are 10 digits available in decimal number system as shown in the above table. It is known as Base 10 system. Therefore the number 847 in this system is represented by $(847)_{10}$.

$$847 = 8 \times 10^2 + 4 \times 10^1 + 7 \times 10^0$$

$$= 800 + 40 + 7 = 847.$$

The successive positions to the left of the decimal point represent units, tens, hundreds, thousands, lacs etc. Each position represents a specific power of the base 10. The principles that apply to the decimal system apply in any other positional number system.

The following graph illustrates the progression of powers of 10 :



All numbers to the left of the decimal point are whole numbers, and all numbers to the right of the decimal point are fractional numbers. When you use any base other than the decimal system, the division between whole numbers and fractional numbers is referred to as the RADIX POINT. The decimal point is actually the radix point of the decimal system, but the term radix point is normally not used with the base 10 number system.

1.2.3 Binary Number System :

The simplest possible number system is the BINARY, or base 2, system. You will be able to use the information just covered about the decimal system to easily relate the same terms to the binary system.

The base, or radix–you should remember from our decimal section–is the number of symbols used in the number system. Since this is the base 2 system, only two symbols, 0 and 1, are used. The base is indicated by a subscript, as shown in the following example :

1_2

When you are working with the decimal system, you normally don't use the subscript. Now that you will be working with number systems other than the decimal system, it is important that you use the subscript so that you are sure of the system being referred to.

Why Binary?

Almost all computers use binary numbers. Therefore, the question that arises is 'Why do we use binary numbers instead of decimal numbers?' The reasons are as under :

- Information is handled in a computer by electronic/electrical components, such as transistors, semiconductors etc., all of which can only indicate two states or conditions –on(1) or off(0). All information is represented within the computer by the presence or absence of these types of signals. The binary number system, which has only two digits (0 and 1), is most suitable for expressing the two possible states.
- Computer circuits only have to handle two binary digits; this greatly simplifies the internal circuit design of computers.
- Everything that can be done in decimal number system can also be done in binary number system.

The prefix '*bi*' means 2. Binary system thus refers to a number system which has only two unique digits. Binary numbers contains two unique digits 0 and 1. It is known as Base 2 system. The number thus formed is the combination of these two digits such as $(1001)_2$.

$$(1001)_2 = 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 8 + 0 + 0 + 1 = (9)_{10}.$$

$$(100101)_2 = 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

$$= 32 + 0 + 0 + 4 + 1 = (37)_{10}.$$

Decimal and Binary Comparison :

	Decimal	Binary	
10^0	0	0	2^0
	1	1	
	2	10	2^1
	3	11	
	4	100	2^2
	5	101	
	6	110	
	7	111	
	8	1000	2^3
	9	1001	
10^1	10	1010	
	11	1011	
	12	1100	
	13	1101	
	14	1110	
	15	1111	
	16	10000	2^4
	17	10001	
	18	10011	
	19	10011	
	20	10100	

1.2.4 Octal Number System :

The octal, or base 8, number system is a common system used with computers. Because of its relationship with the binary system, it is useful in programming some types of computers.

In octal number system, there are 8 unique digits available in octal number system. These are from 0 – 7. Thus, any number formed by these digits is combination of these digits. It is known as Base 8 system. The base, or radix, is indicated by the subscript 8. The value of a digit in a number depends upon its position in the number. Therefore, the number 502 of octal number system can be expressed as:

$$(502)_8 = 5 \times 8^2 + 0 \times 8^1 + 2 \times 8^0$$
$$= 5 \times 64 + 0 + 2$$
$$= 320 + 0 + 2$$
$$= (322)_{10}.$$

1.2.5 Hexadecimal Number System :

The hex number system is a more complex system in use with computers. The name is derived from the fact the system uses 16 symbols. It is beneficial in computer programming because of its relationship to the binary system. Since 16 in the decimal system is the fourth power of 2 (or 24); one hex digit has a value equal to four binary digits.

In Hexadecimal Number System, there are 16 digits available. These are from 0 – 9 and *A*, *B*, *C*, *D*, *E*, *F* where *A* denotes 10, *B* denotes 11 ... and *F* denotes 15. Thus, any number formed is combination of these digits. It is known as Base 16 system. The value of a digit in a number depends upon its position in the number. Therefore, the number *A*58 of hexadecimal number system can be expressed as :

$$(A\ 58)_{16} = A\ (10) \times 16^2 + 5 \times 16^1 + 8 \times 16^0$$
$$= 10 \times 256 + 80 + 8$$
$$= 2560 + 88$$
$$= (2648)_{10}.$$

The hexadecimal notations are used not only to represent numbers, but also used to represent binary numbers in compact form. This is so because in most of the computers data occupy multiple of 4 bits which is equivalent to single hexadecimal digit.

1.3 Conversion to decimal number system from another number system

Usually numbers expressed in decimal number system are much more meaningful to us, because we have been using decimal numbers in our daily routine life. Any number in one number system can be represented in any other number system. There are many methods, which can be used to convert numbers from one base to another. The following steps are required to convert a number from any base to base 10 :

For conversion of a number from any number system to decimal number system (base 10), multiply each of digit of the number by (Base Value)$^{\text{position of the digit}}$ and then add the result. *i.e.*

- Determine the column (positional) value of each digit. This depends on the position of the digit and the base of the number system.

- Multiply the obtained column values by the digits in the corresponding columns.
- Sum the products calculated in the above step. The total is the equivalent value in decimal.

Fractional Numbers :

In any number system, fractional numbers are formed in the same general way as in the decimal number system. For example, in the decimal number system :

$$0.475 = (4 \times 10^{-1}) + (7 \times 10^{-2}) + (5 \times 10^{-3})$$

$$= 0.4 + 0.07 + 0.005.$$

1.3.1 Binary to Decimal :

For conversion of a number from binary number system to decimal number system, follow the above procedure *i.e.* multiply each of binary digit by $2^{\text{position of the digit}}$ and then add the result.

Example :

$$(10001)_2 = (?)_{10}.$$

Step 1 : Determine the column values

Column number (From right)	Column value
1	$2^0 = 1$
2	$2^1 = 2$
3	$2^2 = 4$
4	$2^3 = 8$
5	$2^4 = 16$

Step 2 : Multiply column values by corresponding column digits

16	8	4	2	1
× 1	× 0	× 0	× 0	× 1
16	0	0	0	1

Step 3 : Sum the products

$16 + 0 + 0 + 0 + 1 = 17$

or $1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 16 + 0 + 0 + 0 + 1 = 17$

Hence $(10001)_2 = (17)_{10}$.

Example :

$$(100.101)_2 = (?)_{10}$$

$$(101.101)_2 = 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0 + 1 \times 2^{-1} + 0 \times 2^{-2} + 1 \times 2^{-3}$$

$$= 4 + 0 + 0 + 1/2 + 0/4 + 1/8$$

$$= 4 + 0.5 + 0 + 0.125$$

$$= (4.625)_{10}.$$

1.3.2 Octal to Decimal :

For conversion of a number from octal number system to decimal number system, multiply each of octal digit by $8^{\text{position of the digit}}$ and then add the result.

Example :

$$(3067.51)_8 = (?)_{10}$$

$$(3067.51)_8 = 3 \times 8^3 + 0 \times 8^2 + 6 \times 8^1 + 7 \times 8^0 + 5 \times 8^{-1} + 1 \times 8^{-2}$$

$$= 3 \times 512 + 0 + 48 + 7 + 5/8 + 1/64$$

$$= 1536 + 55 + 0.625 + 0.015625$$

$$(3067.51)_8 = (1591.640625)_{10}.$$

1.3.3 Hexadecimal to Decimal

Similarly, for conversion of a number from hexadecimal number system to decimal number system, multiply each of hexadecimal digit by $(16)^{\text{position of the digit}}$ and then add the result.

Example :

$$(C1B.2C)_{16} = (?)_{10}$$

$$= C \times 16^2 + 1 \times 16^1 + B \times 16^0 + 2 \times 16^{-1} + C \times 16^{-2}$$

$$= 12 \times 16^2 + 16 + 11 \times 1 + 2/16 + 12/256$$

$$= 3072 + 27 + 0.125 + 0.046875$$

$$(C1B.2C)_{16} = (3099.171875)_{10}.$$

1.4 Conversion to another number system from decimal number system

As decimal number may contain only integer or integer part along with fractional part, thus calculation shall be done in two parts. The following steps are used to convert a number from decimal to another base :

Integer Part :

1. Divide the decimal number by the value of the new base.
2. Record the remainder.
3. **Repeat the step :**
   (i) With the quotient and then step.
   (ii) Until the quotient becomes 0 or less than the value of the new base.

Fractional Part :

1. Multiply the fractional part by the value of the new base.
2. Record the integer part, if it exists, else record 0.
3. **Repeat the step :**
   (i) with the result of the previous multiplication and then step.
   (ii) until the fractional part becomes 0.

   In case of infinite calculations, generally 6 digits are taken.

1.4.1 Decimal to Binary :

Example :

$$(31)_{10} = (?)_2$$

Here the new base is 2.

31/2 = 15 Remainder 1
15/2 = 7 Remainder 1
7/2 = 3 Remainder 1
3/2 = 1 Remainder 1

or

2	31	
2	15	1
2	7	1
2	3	1
	1	1

Now start writing in the order from the last obtained till the first remainder. Thus the binary equivalent of

$$(31)_{10} = (11111)_2$$

Example :

$$(31.625)_{10} = (?)_2$$

Convert integer part *i.e.* 31 into binary as above = 11111

Convert fraction part 0.625 into binary as below :-

0.625 × 2 = 1.25 take away integer part and record = 1

0.25 × 2 = 0.50 take away integer part and record = 0

0.50 × 2 = 1.00 take away integer part and record = 1

Thus binary equivalent of fraction part is 101.

Hence $(31.625)_{10} = (11111.101)_2$

1.4.2 Decimal to Octal :

$$(953)_{10} = (?)_8$$

Here the new base is 8.

953/8 = 119 Remainder 1
119/8 = 14 Remainder 7
14/8 = 1 Remainder 6

or

8	953	
8	119	1
8	14	7
	1	6

Now start writing in the order from the last obtained till the first remainder. Thus the octal equivalent of

$$(953)_{10} = (1671)_8$$

1.4.3 Decimal to Hexadecimal :

$$(953)_{10} = (?)_{16}$$

Here the new base is 16.

953/16 = 59 Remainder 9
59/16 = 3 Remainder 11(*B*)

or

16	953	
16	59	9
	3	11(*B*)

Now start writing in the order from the last obtained till the first remainder. Thus the hexadecimal equivalent of

$$(953)_{10} = (3B9)_{16}$$

1.5 Conversion from a base other than 10 (binary, octal, hexadecimal) to a base other than 10 (binary, octal, hexadecimal)

The following steps are used to convert a number from a base other than 10, to a base other than 10 *i.e.* binary to octal, hexadecimal and vice-versa :

(i) Convert the original number to a decimal number (base 10),

(ii) Convert the decimal number obtained in step-I to the new base number.

1.5.1 Binary to Octal and vice-versa :

$$(100010)_2 = (?)_8$$

Step 1 : Convert 100010 to base 10

$$(100010)_2 = 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$$
$$= 32 + 0 + 0 + 0 + 2 + 0 = (34)_{10}$$

Step 2 : Convert $(34)_{10}$ to base 8

34/8 = 4 remainder 2

4/8 = 0 remainder 4

Hence $(34)_{10} = (42)_8$

Therefore $(100010)_2 = (34)_{10} = (42)_8$

Shortcut method for Binary to Octal Conversion :

A binary number is easily converted to a octal number by dividing the bits of the binary number into groups of 3-bits. This is because of the fact that the maximum value of one digit is equal to the maximum value of three digits in binary. Therefore, the value of one octal digit is equivalent to 3 bits of binary.

Binary Coded Octal Numbers

Octal number	Binary coded octal number	Decimal equivalent
0	000	0
1	001	1
2	010	2
3	011	3
4	100	4
5	101	5
6	110	6
7	111	7

$(100010)_2 = (?)_8$

Divide the bits into group of 3 from right as 100 – 010

As per the above table, 010 is equivalent to 2 in octal number and 100 is equivalent to 4 in octal number. Therefore octal equivalent of the given binary number is $(42)_8$

Hence $(100010)_2 = (42)_8$ Which is same as converted above.

Now for quick conversion of octal to binary, each digit of octal number is converted into its 3-bits of its binary equivalent.

1.5.2 Binary to Hexadecimal and vice-versa

$(100010)_2 = (?)_{16}$

Step 1 : Convert 100010 to base 10

$$(100010)_2 = 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$$

$$= 32 + 0 + 0 + 0 + 2 + 0 = (34)_{10}$$

Step 2 : Convert $(34)_{10}$ to base 16

34/16 = 2 remainder 2

2/16 = 0 remainder 2

Hence $(34)_{10} = (22)_{16}$

Therefore $(100010)_2 = (34)_{10} = (22)_{16}$

Shortcut method for Binary to Octal Conversion :

A binary number is easily converted to a hexadecimal number by dividing the bits of the binary number into groups of 4-bits. This is because of the fact that the maximum value of one digit is equal to the maximum value of four digits in binary. Therefore, the value of one hexadecimal digit is equivalent to 4 bits of binary.

Binary Coded Hexadecimal Numbers

Hexadecimal number	Binary coded octal number	Decimal equivalent
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
A	1010	10
B	1011	11
C	1100	12
D	1101	13
E	1110	14
F	1111	15

$(100010)_2 = (?)_{16}$

Divide the bits into group of 4 from right as 0010 – 0010.

As per the above table, 0010 is equivalent to 2 in hexadecimal number and 0010 is equivalent to 2 in hexadecimal number. Therefore hexadecimal equivalent of the given binary number is $(22)_{16}$

Hence $(100010)_2 = (22)_{16}$ which is same as converted above.

Now for quick conversion of hexadecimal to binary, each digit of octal number is converted into its 4-bits of its binary equivalent.

Self-learning exercise-1

1. The decimal equivalent of the binary number $(-10011)_2$ is :

(a) – 12 *(b)* – 15

(c) – 19 *(d)* – 21 [ ]

2. 16 is the base of, which of the following number system :

(a) Binary *(b)* Octal

(c) Hexadecimal *(d)* Decimal [ ]

3. When you use any base other than the decimal system, the division between whole numbers and fractional numbers is referred as :

(a) Binary point *(b)* Radix point

(c) Matrix point *(d)* Decimal point [ ]

4. Which of the following statement is flase ?

   (a) All the natural numbers are integers

   (b) All the rational numbers are integers

   (c) All the rational numbers are real numbers

   (d) All the integers all real numbers [ ]

5. The octal representation of the binary number 110011_2 is :

   (a) $(303)_8$ *(b)* $(63)_8$

   (c) $(33)_8$ *(d)* None of these [ ]

6. The hexadecimal representation of the binary number 10101010 is :

   (a) *AA* *(b)* 1010

   (c) *BB* *(d)* 99 [ ]

7. The conversion of $3CF_{16}$ to decimal notation is :

   (a) 759 *(b)* 597

   (c) 965 *(d)* 976 [ ]

8. What is the equivalent of decimal number 39.625 in binary form :

   (a) 100111.101 *(b)* 110110.100

   (c) 110011.101 *(d)* 1000010.100 [ ]

1.6 Summary

You should have a basic understanding of number systems. The number systems that were dealt with are used extensively in the microprocessor and computer fields.

A NUMBER is a symbol used to represent one or more units. The RADIX is the base of a positional number system. It is equal to the number of symbols used in that number system.

A POSITIONAL NOTATION is a system in which the value or magnitude of a number is defined not only by its digits or symbol value, but also by its position. Each position represents a power of the radix, or base, and is ranked in ascending or descending order.

Data stored in a coded form is basically of three types : Numeric, Alphabetic and Alphanumeric. Every computer stores these data types in a coded form *i.e.* in binary other number system. Number system is of two types : Non-Positional Number System and Positional Number System. Almost all computers use binary numbers. Information is handled in a computer by electronic/electrical components, such as transistors, semiconductors etc., all of which can only indicate two states or conditions : on (1) or off (0). All information is represented within the computer by the presence or absence of these types of signals. The binary number system, which has only two digits (0 and 1), is most suitable for expressing the two possible states.

The OCTAL NUMBER SYSTEM is a base 8 system and is quite useful as a tool in the conversion of binary numbers. This system works because 8 is an integral power of 2; that is, 23 = 8. The use of octal numbers reduces the number of digits required to represent the binary equivalent of a decimal number.

The HEX NUMBER SYSTEM is a base 16 system and is sometimes used in computer systems. A binary number can be converted directly to a base 16 number if the binary number is first broken into groups of four digits.

To CONVERT A WHOLE BASE 10 NUMBER to another system, divide the decimal number by the base of the number system to which you are converting. Continue dividing the quotient of the previous division until it can no longer be done.

Glossary :

Base : The total number of digits used in a positional number system. It is also known as radix.

Binary : A characteristic or property involving a selection, choice or condition in which there are two possibilities. In number system, it refers to the system in which the base used is two, each number expressed in powers of two by using only two digits *i.e.* 0 and 1.

Bit : Acronym for Binary Digit *i.e.* 0 and 1. It stands for one binary piece of information.

Byte : A fixed number of adjacent bits, which represent a particular character or symbol. Normally a byte consists of eight bits.

Character : A single alphabet numeric or special symbol that is used to represent data.

Decimal number : A number system with a base of 10. The ten allowable

System : Digits are 0,1,2,3,4,5,6,7,8,9.

Hexadecimal : A number system with a base of 16, Its digits range from 0

Number system : To f.

Octal Number : A number system with a base of 8. The octal digits range from 0 to 7.

Further Readings :

The following books are suggested for further reading :

1. Computer Fundamentals, P.K. Sinha, BPB publication.
2. Computer System Arcitecture, M.Morris Mano, PHI.
3. Digital Principles and applications, Malvino,Leach, TMH.

1.7 Answers to self-learning exercises

Self-learning exercise-1

1. *c*	**2.** *c*	**3.** *b*	**4.** *b*
5. *b*	**6.** *c*	**7.** *d*	**8.** *a*

1.8 Exercises

1. Why binary number system is important in representing data in computer ? Explain.
2. Explain the significance of base/radix of a number system.
3. What is the difference between positional and non-positional number systems? Give examples of both types of number systems.
4. Find the decimal equivalent of the following binary numbers :

   (a) 1010001.1011 *(b)* 11000101

   (c) 1001.1011 *(d)* 1001011
5. Convert the decimal numbers into binary :

   (a) 347.125 *(b)* 954.525

   (c) 545 *(d)* 1011
6. Convert the following numbers to decimal numbers :

   (a) $(C2BA)_{16}$ *(d)* $(100011)_2$

   (c) $(2416)_8$ *(d)* $(162F)_{16}$
7. Convert octal numbers to hexadecimal number system :

   (a) 7437 *(b)* 5416

   (c) 6472 *(d)* 5627
8. Convert the following whole hexadecimal numbers to their decimal equivalents :

   (a) C *(b)* 9F

   (c) D52, *(d)* 67E

   (e) ABCD
9. Convert the following binary numbers to their hexadecimal equivalents :

   (a) 1001.1111 *(b)* 110101.011001

   (c) 10100111 .111011 *(d)* 10000001.1101

   (e) 10000.1 *(f)* 1000000.0000111

□□□

UNIT 2 : Number Arithmetic and Computer Codes

Structure of the Unit

2.0 Objectives

After going through this unit student will be able to :

- To learn number arithmetic like addition, subtraction in binary number system
- Understanding of floating point numbers
- Learn different computer codes

2.1 Introduction

Unsigned and signed integers :

An integer is a number with no fractional part; it can be positive, negative or zero. In ordinary usage, one uses a minus sign to designate a negative integer. However, a computer can only store information in bits, which can only have the values zero or one. We might expect, therefore, that the storage of negative integers in a computer might require some special technique.

Consider a single digit decimal number: in a single decimal digit, you can write a number between 0 and 9. In two decimal digits, you can write a number between 0 and 99, and so on. Since nine is equivalent to $10^1 - 1$, 99 is equivalent to $10^2 - 1$, etc., in n decimal digits, you can write a number between 0 and $10^n - 1$. Analogously, in the binary number system,

An unsigned integer containing n bits can have a value between 0 and $2^n - 1$ (which is 2^n different values) :

When a computer performs an unsigned integer arithmetic operation, there are three possible problems which can occur :

1. If the result is too large to fit into the number of bits assigned to it, an "**overflow**" is said to have occurred. For example if the result of an operation using 16 bit integers is larger than 65,535, an overflow results.
2. In the division of two integers, if the result is not itself an integer, a "**truncation**" is said to have occurred: 10 divided by 3 is truncated to 3, and the extra 1/3 is lost. This is not a problem, of course, if the programmer's intention was to ignore the remainder!
3. Any division by zero is an error, since division by zero is not possible in the context of arithmetic.

Signed Integers :

Signed integers are stored in a computer using 2's complement. As you recall, when computing the 2's complement of a number it was necessary to know how many bits were to be used in the final result; leading zeroes were appended to the most significant digit in order to make the number the appropriate length. Since the process of computing the 2's complement involves first computing the 1's complement, these leading zeros become leading ones, and the left most bit of a negative number is therefore always 1. In computers, the left most bit of a signed integer is called the "**sign bit**".

Consider an 8 bit signed integer: let us begin with $0\,0\,0\,0\,0\,0\,0\,0_2$ and start counting by repeatedly adding 1 :

When you get to 127, the integer has a value of $0\,1\,1\,1\,1\,1\,1\,1_2$; this is easy to see because you know now that a 7 bit integer can contain a value between 0 and $2^7 - 1$, or 127. What happens when we add 1?

- If the integer were unsigned, the next value would be $1\,0\,0\,0\,0\,0\,0\,0_2$, or 128 (2^7). But since this is a signed integer, $1\,0\,0\,0\,0\,0\,0\,0_2$ is a negative value: the sign bit is 1!
- Since this is the case, we must ask the question: what is the decimal value corresponding to the signed integer $1\,0\,0\,0\,0\,0\,0\,0_2$? To answer this question, we must take the 2's complement of that value, by first taking the 1's complement and then adding one.
- The 1's complement is $0\,1\,1\,1\,1\,1\,1\,1_2$, or decimal 127. Since we must now add 1 to that, our conclusion is that the signed integer $1\,0\,0\,0\,0\,0\,0\,0_2$ must be equivalent to decimal -128!

Odd as this may seem, it is in fact the only consistent way to interpret 2's complement signed integers. Let us continue now to "count" by adding 1 to $1\,0\,0\,0\,0\,0\,0\,0_2$:

- $1\,0\,0\,0\,0\,0\,0\,0_2 + 0\,0\,0\,0\,0\,0\,0\,1_2$ is $1\,0\,0\,0\,0\,0\,0\,1_2$.

- To find the decimal equivalent of $1\ 0\ 0\ 0\ 0\ 0\ 0\ 1_2$, we again take the 2's complement: the 1's complement is $0\ 1\ 1\ 1\ 1\ 1\ 1\ 0_2$ and adding 1 we get $0\ 1\ 1\ 1\ 1\ 1\ 1\ 1_2$ (127) so $1\ 0\ 0\ 0\ 0\ 0\ 0\ 1_2$ is equivalent to -127.
- We see then that once we have accepted the fact that $1\ 0\ 0\ 0\ 0\ 0\ 0\ 0_2$ is decimal – 128, counting by adding one works as we would expect.
- Note that the most negative number which we can store in an 8 bit signed integer is –128, which is -2^{8-1}, and that the largest positive signed integer we can store in an 8 bit signed integer is 127, which is $2^{8-1} - 1$.
- The number of integers between – 128 and + 127 (inclusive) is 256, which is 2^8; this is the same number of values which an unsigned 8 bit integer can contain (from 0 to 255).
- Eventually we will count all the way up to $1\ 1\ 1\ 1\ 1\ 1\ 1\ 1_2$. The 1's complement of this number is obviously 0, so $1\ 1\ 1\ 1\ 1\ 1\ 1\ 1_2$ must be the decimal equivalent of – 1.

Using our deliberations on 8 bit signed integers as a guide, we come to the following observations about signed integer arithmetic in general :

- If a signed integer has n bits, it can contain a number between -2^{n-1} and $+(2^{n-1} - 1)$.
- Since both signed and unsigned integers of n bits in length can represent 2^n different values, there is no inherent way to distinguish signed integers from unsigned integers simply by looking at them; the software designer is responsible for using them correctly.
- No matter what the length, if a signed integer has a binary value of all 1's, it is equal to decimal – 1.

You should verify that a signed short integer can hold decimal values from –32,768 to + 32,767, a signed long integer can contain values from – 2,147,483,648 to + 2,147,483,647 and a signed double integer can represent decimal values from

– 9,223,372,036, 854,775,808 to + 9,223,372,036,854,775,807.

2.2 Binary arithmetic

As in decimal number system, binary arithmetic involves mainly four operations like Addition, Subtraction, Multiplication and Division. The operations of each are described below :

***(A)* Addition :**

To perform addition on binary numbers following rules may be applied :

$0 + 0 = 0$

$0 + 1 = 1$

$1 + 0 = 1$

$1 + 1 = 10$ or 0 with carry over 1.

Example :

Carries	10001	
	11101	29
	+ 10001	+ 17
	101110	46

Example :

	11001	25
	+ 110	+ 6
	11111	31

Example :

	111001	57
	+ 110111	+ 55
	1110000	112

***(B)* Subtraction :**

To perform subtraction on binary numbers following rules may be applied :

$0 - 0 = 0$

$1 - 0 = 1$

$1 - 1 = 0$

$0 - 1 = 1$ with one as borrow.

Simple subtraction :

Example :

	11011	27
	− 1001	− 9
	10010	18

Example :

	11001	25
	− 1010	− 10
	1111	15

Subtraction of Binary number by 2's compliment method :

1's compliment of a binary number is obtained by flipping the each digit *i.e.* making all 0's to 1's and all 1's to 0's.

2's compliment of a binary number is obtained by adding 1 to its 1's compliment.

While performing subtraction on binary numbers following steps may be followed :

- Both the numbers should be of the same size. If not, then make both the numbers of the same size by adding leading zeros.
- Compliment the number to be subtracted by flipping the each digit *i.e.* changing 1's to 0's and 0's to 1's. The compliment of 1001 is 0110.
- Perform binary addition as above *i.e.* Add the first number to the result obtained in the above step.
- If the result of the addition is increased by one digit means there is a carry of 1, then remove this (ignore the left most digit) and add to the final result.
- If the size of the result is not increased (equal to the original size), then re-compliment the answer and attach a negative (–) sign in front of the number.

Example :

11001 –1010	25 –10	
Step 1 : (Make the number of same size)		11001 – 01010
Step 2 : (Take 2's compliment of second number)		
1's compliment		10101
2's compliment		+1
		10110
Step 3 : (Add the first number to the result obtained in step-2)		11001 +10110
Step 4 : (Size is more the original size, hence ignore the left most digit)		101111

Example :

1101	13	
−10101	−21	
Step 1 : (Make the number of same size)		01101
		− 10101
Step 2 : (Take 2's compliment of second number)	1's compliment	01010
	2's compliment	+1
Step 3 : (Add the first number to the result obtained in step-2)		01011 01101
		+ 01011
Step 4 : (Size is equal to the original size, hence re-compliment the result and attach a-ve sign		11000 00111
		+ 1
		−1000

***(C)* Multiplication :**

The multiplication of binary numbers follows the same convention as of decimal number system. The result may be obtained by sequence of additions and shifts.

Example :

1101	13
× 101	× 5
1101	65
0000 ×	
1101××	
1000001	

***(D)* Division :**

The division in binary number system is also same as of in decimal number system. It may be performed as sequence of subtraction and shifts.

Example : 11100 divided by 100 (28 ÷ 4)

111	Quotient
100 √ 11100	
100	
0110	
100	
0100	
100	
000	Remainder
Therefore answer is **111**	

2.3 Signed binary integers

It was noted previously that we will not be using a minus sign (–) to represent negative numbers. We would like to represent our binary numbers with only two symbols, 0 and 1. There are a few ways to represent negative binary numbers. The simplest of these methods is called ones complement, where the sign of a binary number is changed by simply toggling each bit (0's become 1's and vice-versa). This has some difficulties, among them the fact that zero can be represented in two different ways (for an eight bit number these would be 0000 0000 and 1111 1111)., we will use a method called two's complement notation which avoids the pitfalls of one's complement, but which is a bit more complicated.

To represent an n bit signed binary number the leftmost bit, has a special significance. The difference between a signed and an unsigned number is given in the table below for an 8 bit number.

The value of bits in signed and unsigned binary numbers								
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Unsigned	$2^7 = 128$	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$
Signed	$-(2^7) = -128$	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$

Now see the changes of the value of some binary numbers :

Binary	Unsigned	Signed
0010 0011	35	35
1010 0011	163	–93
1111 1111	255	–1
1000 0000	128	–128

If Bit 7 is not set (as in the first example) the representation of signed and unsigned numbers is the same. However, when Bit 7 is set, the number is always negative. For this reason Bit 7 is sometimes called the sign bit. Signed numbers are added in the same way as unsigned numbers, the only difference is in the way they are interpreted. This is important for designers of arithmetic circuitry because it means that numbers can be added by the same circuitry regardless of whether or not they are signed.

To form a two's complement number that is negative you simply take the corresponding positive number, invert all the bits, and add 1. The example below illustrated this by forming the number negative 35 as a two's complement integer :

$$35_{10} = 0010\ 0011_2$$

$$\text{invert} -> 1101\ 1100_2$$

$$\text{add } 1 -> 1101\ 1101_2$$

So 1101 1101 is our two's complement representation of – 35. We can check this by adding up the contributions from the individual bits.

$$1101\ 1101_2 = -128 + 64 + 0 + 16 + 8 + 4 + 0 + 1 = -35.$$

The same procedure (invert and add 1) is used to convert the negative number to its positive equivalent. If we want to know what what number is represented by 1111 1101, we apply the procedure again

$$? = 1111\ 1101_2$$

$$\text{invert} -> 0000\ 0010_2$$

$$\text{add } 1 -> 0000\ 0011_2$$

Since 0000 0011 represents the number 3, we know that 1111 1101 represents the number – 3.

2.4 Computer codes

Numeric data is not the only form of data handled by a computer. We often require to process alphanumeric data also. An alphanumeric data is a string of symbols, where a symbol may be one of the letters *A, B, C,.... Z,* or one of the digits 0, 1, 2, 3,...9, or special character, such as +, –, *, / . () etc. Alphabetic data consists of only the letters and blank spaces and numeric data consists only the digits.

A computer accepts data and instructions in machine language (0's and 1's form). Data must be represented internally by the bits 0 and 1. The binary coding schemes are used to represent data internally in the computer memory. In binary coding, every symbol of text data is represented by a group of bits. The group of bits used to represent a symbol is called a byte. Modern computers use 8 bits to represents a symbol.

The most popular text code systems are :

- BCD and EBCDIC
- ASCII
- UNICODE
- Gray Code

2.4.1 BCD and EBCDIC :

BCD : The BCD stands for binary coded decimal. The BCD code system is one of the early code systems. It was defined by IBM for its early computer. It was one of the first code systems to represents data in binary form. This code system consisted of 6 – bit code to represent a single character and maximum 64 (26) characters can be represented inside the computer.

To encode a decimal number using the common BCD encoding, each decimal digit is stored in a 4-bit nibble :

Decimal :	0	1	2	3	4	5	6	7	8	9
BCD :	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001

Thus, the BCD encoding for the number 127 would be :

0001 0010 0111.

We have used a group of four bits to represent a digit (character) in *BCD*. 4-bits *BCD* coding system can be used to represent only decimal numbers because four bits are insufficient to represent the

various characters used by a computer. Hence, instead of using four bits with only 16 possible characters, computer designers commonly use six bits to represent characters in BCD. In 6-bit BCD code, the four BCD numeric place positionare retained but two additional zone positions are addedd. With six bits, it is possible to represent 64 different characters. This is sugfficient to code the decimal digits (10), alphabetic letters (26), and other special characters (28).

The following table illustrates the coding of alphabetic and numreic characters in BCD :

	BCD Code		Octal
Character	**Zone**	**Digit**	**Equivalent**
A	11	0001	61
B	11	0010	62
C	11	0011	63
D	11	0100	64
E	11	0101	65
F	11	0110	66
G	11	0111	67
H	11	1000	70
I	11	1001	71
J	10	0001	41
K	10	0010	42
L	10	0011	43
M	10	0100	44
N	10	0101	45
O	10	0110	46
P	10	0111	47
Q	10	1000	50
R	10	1001	51
S	01	0010	22
T	01	0011	23
U	01	0100	24
V	01	0101	25
W	01	0110	26
X	01	0111	27
Y	01	1000	30
Z	01	1001	31
0	00	0000	00
1	00	0001	01
2	00	0010	02
3	00	0011	03
4	00	0100	04
5	00	0101	04
6	00	0110	06
7	00	0111	07
8	00	1000	10
9	00	1001	11

Ex. Write the Binary digits used to record the word COMPUTER in BCD.

Sol. In BCD binary notation

C = 110011	U = 010100
O = 100110	T = 010101
M = 100100	E = 110101
P = 100111	R = 101001

Hence, the binary digits

110011	100110	100100	100111	010100	010101	110101	101001
C	O	M	P	U	T	E	R

Will record the word COMPUTER in BCD.

EBCDIC :

EBCDIC stands for Extended Binary Coded Decimal Interchange Code.

In BCD, 6-bit code only 64 characters can be represented. Hence, the BCD code was extended from a 6-bit code to 8-bit code and new code system is named as EBCDIC. In this code system, it is possible to represent 256 (2) different characters. EBCDIC code system isdeveloped by IBM, still used in IBM mainframe and midrange system, but it is rarely used in personal computers.

Since EBCDIC is an 8-bit code, it can be esily divided into two 4-bits groups. Each of these 4-bit groups can be represented by one hexadecimal digit. Hence hexadecimal number system is used as shotcut notation for memory dump by computers that use EBCDIC for internal representation of characters. This results in a one-to-four reduction in volume of memory dump.

The following table shows the alphabetic and numeric characters in EBCDIC along with their hexadecimal equivalent :

EBCDIC Code			Hexadecimal Equivalent
Character	**Zone**	**Digit**	
A	1100	0001	C1
B	1100	0010	C2
C	1100	0011	C3
D	1100	0100	C4
E	1100	0101	C5
F	1100	0110	C6
G	1100	0111	C7
H	1100	1000	C8
I	1100	1001	C9

EBCDIC Code			Hexadecimal Equivalent
Character	Zone	Digit	
J	1101	0001	D1
K	1101	0010	D2
L	1101	0011	D3
M	1101	0100	D4
N	1101	0101	D5
O	1101	0110	D6
P	1101	0111	D7
Q	1101	1000	D8
R	1101	1001	D9
S	1110	0010	E2
T	1110	0011	E3
U	1110	0100	E4
V	1110	0101	E5
W	1110	0110	E6
X	1110	0111	E7
Y	1110	1000	E8
Z	1110	1001	E9
0	1111	0000	F0
1	1111	0001	F1
2	1111	0010	F2
3	1111	0011	F3
4	1111	0100	F4
5	1111	0101	F4
6	1111	0110	F6
7	1111	0111	F7
8	1111	1000	F8
9	1111	1001	F9

Ex. Represent 'SHORT' in EBCDIC code.

Sol. By table we have :

1110 0010	1100 1000	1101 0110	1101 1001	1110 0011
S	H	O	R	T

2.4.2 ASCII :

The American Standard Code for Information Interchange is a standard seven-bit code that was proposed by ANSI in 1963, and finalized in 1968. Other sources also credit much of the work on ASCII to work done in 1965. ASCII was established to achieve compatibility between various types of data processing equipment.

ASCII, pronounced "ask-key", is the common code for microcomputer equipment. The standard ASCII character set consists of 128 decimal numbers ranging from zero through 127 assigned to letters, numbers, punctuation marks, and the most common special characters. The Extended ASCII Character Set also consists of 128 decimal numbers and ranges from 128 through 255 representing additional special, mathematical, graphic, and foreign characters.

ASCII is of two type : ASCII-7 and ASCII-8. ASCII-7 is a 7 bit code that can represent 128 (27) different characters. Computers using 8-bit byte (group of 8 bits for 1 byte) and the 7-bit ASCII either se the 8th bit (leftmost bit) of each byte as zero or use it as a parity bit.

ASCII-8 is an extended version of ASCII-7. It is an 8-bit code that can represent 256 (28) different characters. The additional bit is added to the left of the 7th bit (leftmost bit) of ASCII-7 codes.

ASCII (Decimal)	Character	ASCII-7	(Hexa Decimal)	ASCII-8
65	A	100 0001	41	0100 0001
66	B	100 0010	42	0100 0010
67	C	100 0011	43	0100 0011
68	D	100 0100	44	0100 0100
69	E	100 0101	45	0100 0101
70	F	100 0110	46	0100 0110
71	G	100 0111	47	0100 0111
72	H	100 1000	48	0100 1000
73	I	100 1001	49	0100 1001
74	J	100 1010	4A	0100 1010
75	K	100 1011	4B	0100 1011
76	L	100 1100	4C	0100 1100
77	M	100 1101	4D	0100 1101
78	N	100 1110	4E	0100 1110
79	O	100 1111	4F	0100 1111
80	P	101 0000	50	0101 0000
81	Q	101 0001	51	0101 0001
82	R	101 0010	52	0101 0010

ASCII (Decimal)	Character	ASCII-7	(Hexa Decimal)	ASCII-8
83	S	101 0011	53	0101 0011
84	T	101 0100	54	0101 0100
85	U	101 0101	55	0101 0101
86	V	101 0110	56	0101 0110
87	W	101 0111	57	0101 0111
88	X	101 1000	58	0101 1000
89	Y	101 1001	59	0101 1001
90	Z	101 1010	5A	0101 1010
97	a	110 0001	61	0110 0001
100	d	110 0100	64	0110 0100
101	e	110 0101	65	0110 0101
102	f	110 0110	66	0110 0110
103	g	110 0111	67	0110 0111
104	h	110 1000	68	0110 1000
105	i	110 1001	69	0110 1001
106	j	110 1010	6A	0110 1010
107	k	110 1011	6B	0110 1011
108	l	110 1100	6C	0110 1100
109	m	110 1101	6D	0110 1101
110	n	110 1110	6E	0110 1110
111	o	110 1111	6F	0110 1111
112	p	111 0000	70	0111 0000
113	q	111 0001	71	0111 0001
114	r	111 0010	72	0111 0010
115	s	111 0011	73	0111 0011
116	t	111 0100	74	0111 0100
117	u	111 0101	75	0111 0101
118	v	111 0110	76	0111 0110
119	w	111 0111	77	0111 0111
120	x	111 1000	78	0111 1000
121	y	111 1001	79	0111 1001
122	z	111 1010	7A	0111 1010

ASCII (Decimal)	Character	ASCII-7	(Hexa Decimal)	ASCII-8
48	0	011 0000	30	0011 0000
49	1	011 0001	31	0011 0001
50	2	011 0010	32	0011 0010
51	3	011 0011	33	0011 0011
52	4	011 0100	34	0011 0100
53	5	011 0101	35	0011 0101
54	6	011 0110	36	0011 0110
55	7	011 0111	37	0011 0111
56	8	011 1000	38	0011 1000
57	9	011 1001	39	0011 1001

Ex. *Write the ASCII-7 coding for the word "BOY" in both binary and hexadecimal notations. How many bytes are required to store this word using this coding?*

Sol. In ASCII-7

B = 100 0010 in binary and 42 in hexadecimal

O = 100 1111 in binary and 4F in hexadecimal

Y = 101 1001 in binary and 59 in hexadecimal

Hence, the ASCII-7 coding for the word "BOY" will be

	100 0010	100 1111	101 1001
in binary	B	O	Y
	42	4F	59
	B	O	Y

Since each character in ASCII-7 require one byte for its representation and there are four character in the word "BOY", three bytes will be required to store this word using this coding.

Ex. *Write the ASCII-8 coding for the word "John" in both binary and hexadecimal notations. How many bytes are required to store this word using this coding ?*

Sol. In ASCII-8

J = 0100 1010 in binary and 4A in hexadecimal

o = 0110 1110 in binary and 6F in hexadecimal

h = 0110 1000 in binary and 68 in hexadecimal

n = 0110 1110 in binary and 6E in hexadecimal

Hence, the ASCII-8 coding for the word "John" will be

	0100 1010	0110 1110	0110 1000	0110 1110
in binary	J	o	h	n
	4A	6F	68	6E
	J	o	h	n

Since each character in ASCII-8 require one byte for its representation and there are four character in the word "BOY", four bytes will be required to store this word using this coding.

2.4.3 UNICODE :

Unicode provides a unique number for every character,

no matter what the platform,

no matter what the program,

no matter what the language.

Fundamentally, computers just deal with numbers. They store letters and other characters by assigning a number for each one. Before Unicode was invented, there were hundreds of different encoding systems for assigning these numbers. No single encoding could contain enough characters: for example, the European Union alone requires several different encodings to cover all its languages. Even for a single language like English no single encoding was adequate for all the letters, punctuation, and technical symbols in common use.

These encoding systems also conflict with one another. That is, two encodings can use the same number for two *different* characters, or use different numbers for the same character. Any given computer (especially servers) needs to support many different encodings; yet whenever data is passed between different encodings or platforms, that data always runs the risk of corruption.

Unicode is changing all that!

Unicode provides a unique number for every character, no matter what the platform, no matter what the program, no matter what the language. The Unicode Standard has been adopted by such industry leaders as Apple, HP, IBM, JustSystems, Microsoft, Oracle, SAP, Sun, Sybase, Unisys and many others. Unicode is required by modern standards such as XML, Java, ECMAScript (JavaScript), LDAP, CORBA 3.0, WML, etc., and is the official way to implement ISO/IEC 10646. It is supported in many operating systems, all modern browsers, and many other products. The emergence of the Unicode Standard, and the availability of tools supporting it, are among the most significant recent global software technology trends.

Incorporating Unicode into client-server or multi-tiered applications and websites offers significant cost savings over the use of legacy character sets. Unicode enables a single software product or a single website to be targeted across multiple platforms, languages and countries without re-engineering. It allows data to be transported through many different systems without corruption.

Unicode Features :

Today, Unicode is internationally accepted as a universal character-encoding standard because:-

- It provides a consistent way of encoding multilingual plain text.This enables data transfer through different systems without the risk of corruption.
- It defines codes for character used in all major languages of the world used for written communication.
- It also defines codes for special characters (such as various types of punctuation marks), mathematical symblos, technical symblos, and diacritics are modifying character marks such as titdle.
- It has the capacity to encode as many as a million characters.
- It assign each character a unique numeric value and name keeping character coding simple and efficient.
- It reserves a part of the code space for private use to enable users to assign codes for their own characters and symbols.
- It specifies an algorithm for presentation of text with bi-directional behavior.
- It affords simplicity and consistency of ASCII. Unicode characters that correspond to the familiar ASCII character set have the same bypte values as that of ASCII.

2.5 Floating point representation

The floating-point representation of a number needs two parts. The first part represents a signed, fixed-point number called the ***mantissa***. The second part designates the position of the decimal (or binary) point is called the ***exponent***. The fixed point mantissa may be a fraction or an integer. For example, the decimal number + 6132.789 is represented in floating point as follows :

Sign		Sign	
0	.6132789	0	04
mantissa		**exponent**	

The mantissa has a 0 in the leftmost position to denote a plus. The mantissa here is considered to be a fixed-point fraction, so the decimal point is assumed to be at the left of the most significant digit. The decimal mantissa, when stored in a register, requires at least 29 flip-flops. This representation is equivalent to the number expressed as a fraction times 10 to an exponent, that is + .6132780 × 10^{+04}, because of this analogy; the mantissa is sometimes called the ***fraction part***.

Floating point is always interpreted to represent a number in the following form :

$$m \times r^e$$

Only the mantissa m and the exponent e are physically represented in the register (including their signs). The radix r and the radix-point position of the mantissa are always assumed. Arithmetic operations with floating-point numbers are more complicated than arithmetic operations with fixed-point numbers and their execution takes longer and requires more complex hardware. However, floating point representation is must for scientific computations.

Self-learning exercise-1

1. 1's compliment of the number 1011001 is :

(a) 0100110 *(b)* 1100110

(c) 0110010 *(d)* 0110011 [ ]

2. EBCDIC code expresses any character in how many binary digits :

(a) 2 *(b)* 4

(c) 8 *(d)* 16 [ ]

3. $(11011)_2 + (10011)_2$ is equal to :

(a) $(45)_{10}$ *(b)* $(46)_{10}$

(c) $(48)_{10}$ *(d)* $(49)_{10}$ [ ]

4. $(1000)_2 - (111)_2$ is equal to :

(a) 1101_2 *(b)* 10001_2

(c) 10111_2 *(d)* None of these [ ]

5. If a number written in floating point notation is $.6132784E + 4$, then its mantissa and exponent are respectively :

(a) + 4, .613284 *(b)* 6.1327884, + 5

(c) .6132784, + 4 *(d)* + 5, 6.132784 [ ]

6. In ASCII, the symbols II stands for :

(a) Information interchange *(b)* Interchange information

(c) International information *(d)* International interchange [ ]

7. The decimal number 12 in natural BCD code can be written as :

(a) 001010 *(b)* 1100

(c) 00010010 *(d)* None of these [ ]

8. The BCD code is also known as :

(a) 8420 code *(b)* 8421 code

(c) 8422 code *(d)* 8423 code [ ]

2.6 Summary

An integer is a number with no fractional part; it can be positive, negative or zero. In ordinary usage, one uses a minus sign to designate a negative integer. However, a computer can only store information in bits, which can only have the values zero or one. An unsigned integer containing n bits can have a value between 0 and $2n - 1$ (which is 2 n different values). Signed integers are stored in a computer using 2's complement. In computers, the left most bit of a signed integer is called the "**sign bit**".

The BCD code system is one of the early code systems. It was one of the first code systems to represents data in binary form. This code system consisted of 6- bit code to represent a single character and maximum 64 (26) characters can be represented inside the computer.

EBCDIC stands for Extended Binary Coded Decimal Interchange Code. In BCD, 6-bit code only 64 characters can be represented. Hence, the BCD code was extended from a 6-bit code to 8-bit code and new code system is named as EBCDIC. In this code system, it is possible to represent 256 (2) different characters. EBCDIC code system isdeveloped by IBM, still used in IBM mainframe and midrange system, but it is rarely used in personal computers.

The American Standard Code for Information Interchange is a standard seven-bit code that was proposed by ANSI in 1963, and finalized in 1968. ASCII, pronounced "ask-key", is the common code for microcomputer equipment. The standard ASCII character set consists of 128 decimal numbers ranging from zero through 127 assigned to letters, numbers, punctuation marks, and the most common special characters. The Extended ASCII Character Set also consists of 128 decimal numbers and ranges from 128 through 255 representing additional special, mathematical, graphic, and foreign characters. ASCII is of two type- ASCII -7 and ASCII-8.

Unicode provides a unique number for every character, no matter what the platform, no matter what the program, no matter what the language. The Unicode Standard has been adopted by such industry leaders as Apple, HP, IBM, JustSystems, Microsoft, Oracle, SAP, Sun, Sybase, Unisys and many others. Unicode is required by modern standards such as XML, Java, ECMAScript (JavaScript), LDAP, CORBA 3.0, WML, etc., and is the official way to implement ISO/IEC 10646. It is supported in many operating systems, all modern browsers, and many other products.

The floating-point representation of a number needs two parts. The first part represents a signed, fixed-point number called the ***mantissa***. The second part designates the position of the decimal (or binary) point is called the ***exponent***. The fixed point mantissa may be a fraction or an integer.

Further Readings :

1. Computer Fundamentals, P.K. Sinha, BPB publication.
2. Computer System Arcitecture, M. Morris Mano, PHI.
3. Digital Principles and applications, Malvino,Leach, TMH.

2.7 Answers to self-learning exercises

Self-learning exercise-1

1. *a*	**2.** *c*	**3.** *b*	**4.** *d*
5. *c*	**6.** *a*	**7.** *c*	**8.** *b*

2.8 Exercises

1. What does ASCII stand for ?
2. What are computer codes? Explain.
3. What is mantissa ?
4. Explain 2's compliment method in detail.
5. What are signed and unsigned integers ?

□□□

Unit 3 : Sets and Algebra of Sets

Structure of the Unit

3.0 Objectives

After reading this unit you will be able to

- Understand the notion of set.
- Learn various ways of sets representations
- Learn different set theoretic operations.
- Learn laws of algebra of sets.

3.1 Introduction

The concept of set is founding stone in the development of field of "Pure Mathematics". Pure Mathematics is a discipline of notions which give rise to systems amenable to mathematical treatment. In fact, set theory is the basis of algebra. The central aim of this unit is to present basic essentials of the set theory.

3.2 Sets, their representation and notations

A set is well defined collection of objects. Here "well defined objects" means that the objects are definite and distinguishable. The objects are called the elements or members of the set. Capital letters A, B, C.... and lower case letters a, b, c, ... are used respectively to denote sets and elements of sets. A set may be of numbers, alphabets, or anything else as defined. The elements of a set are written in brace { }, however the order of elements in a set does not matter. The elements in a set are listed with a comma (,) sign between them. For example

$$A = \{a, b, c, d\}$$
$$B = \{1, 3, 5\}$$
$$C = \{5, 3, 1\}$$
$$D = \{\text{Rajesh, Naresh, Haresh}\}$$

Here, B and C represent the same set. A set may have finite or infinite number of elements. A set with finite number of elements is called finite set. A set that contains infinite number of elements is called infinite set. Since all the elements of an infinite set can not be listed therefore some of the elements are listed followed by a dotted line that indicates that the rest of elements are of the same fashion *e.g.* $E = \{3, 5, 7, 9 .....\}$. There are two basic ways to write a set :

***(i)* Roster form :** The examples of sets given above are in roster form. In this form, a set is specified by listing all its elements.

***(ii)* Set builder form :** In this form, a set is specified by mentioning properties that define the elements of the set as follows :

$$A = \{x \mid P(x)\}$$

This means that A is set of those x which follow property $P(x)$. Here the symbol "|" denote "such that". Set builder form is useful when a set cannot be represented in roster form. For example, if we consider the set of those real numbers which are greater than -1 and less than 0, then it is conveniently represented as

$$A = \{x \mid x \text{ is a real number and } -1 < x < 0\}$$

Ex.1. *Specify the set* $A = \{1, 2, 3, 4\}$ *in set builder form.*

Sol. $A = \{x \mid x \text{ is positive integer and } 1 \le x \le 4\}$.

Sets can also be represented pictorially by Venn-diagrams. This will be illustrated after explaining some basic concepts.

We, now list some sets of numbers and their notations.

1. Set of integers

$$Z = \{x \mid x \text{ is an integer}\}$$
$$= \{\ldots\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4 \ldots\ldots\}$$

2. Set of real numbers

$$R = \{x \mid x \text{ is a real number}\}$$
$$= (-\infty, \infty)$$

3. Set of natural numbers

$$N = \{x \mid x \text{ is a natural number}\}$$
$$= \{1, 2, 3, \ldots\ldots\}$$

4. Set of whole numbers

$$W = \{x \mid x \text{ is a whole number}\}$$
$$= \{0, 1, 2, 3 \ldots\ldots\}$$

5. Set of rational numbers

$$Q = \{x \mid x = p/q, p \text{ and } q \text{ are integers and } q \neq 0\}.$$

6. Set of complex numbers.

$$C = \{x \mid x = a + ib, a \text{ and } b \text{ are real numbers and } i^2 = -1\}$$

Cardinality of a set : The number of elements present in a finite set A is called cardinality of the set A and is denoted as $n(A)$ or $|A|$.

The cardinality is a basis of principle of inclusion-exclusion.

Equivalent sets : Two sets A and B are said to be equivalent if there is one-one correspondence between them. It is represented as $A \sim B$. For example,

$A = \{a, b, c, d, e\}$ $B = \{x, y, z, t, s\}$ are equivalent.

Equal sets : Two sets A and B are said to be equal and denoted as $A = B$ if they have identical elements *e.g.* $A = \{3, 2, 1, 4\}$; $B = \{1, 2, 3, 4\}$ are equal sets. Here every element of A is in B and vice versa.

Null set : A set that contains no element is called null set or void set or empty set. It is denoted by ϕ.

Singleton set : A set that contains a single element is called a singleton set.

Sub sets : A set may have a set within itself. For example the set $B = \{2, 4, 8, 10\}$ is present in the set $A = \{1, 2, 4, 8, 10, 12, 14\}$. This leads to idea of subset. We define, if every element of a set A is also an element of the set B, then A is called subset of B and it is denoted as $A \subseteq B$. Here the symbol "$\subseteq$" stands for "is subset of". A set may have many subsets. From the definition of subset it is obvious to conclude that every set is subset of itself. Similarly, a null set is considered as subset of all sets. There are two types of subsets : **proper subsets** and **improper subsets.** If A is subset of B *i.e.* $A \subseteq B$ but $A \neq B$, then A is called proper subset of B and is denoted as $A \subset B$. If a subset is not proper then it is a improper subset.

Ex.2. *Is N a proper subset of Z ?*

Sol. $N = \{1, 2, 3 .....\}$

$$Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$$

Obviously $N \neq Z$ and $N \subseteq Z$

$\Rightarrow$ $N \subset Z$

Hence N is proper subset of Z.

Power set : Power set of A, denoted as $P(A)$ is the set of all possible subsets of the set A. Thus, power set of $A = P(A) = \{X \mid X \subseteq A\}$. For example, let $A = \{a, b\}$. Then power set of A is $P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$.

Note that if the cardinality of the set A is n then cardinality of its power set $P(A)$ is 2^n.

Universal set : In set theory, the universal set is largest fixed set such that all the sets under study are subsets of it. For example, in student population studies the set of all students of the world constitute a universal set. Similarly for any set of natural numbers the set of real numbers R will be a universal set. Universal set is denoted by U.

Complement of a set : Let A be a set and U be a universal set. Then complement of A, denoted by A' or A^C is the set that contains elements of U but no element of A. Symbolically

$$A' = \{x \mid x \in U, x \notin A\}.$$

Disjoint sets : Two set A and B are called disjoint sets if not a single element is common to both A and B, e.g. sets $A = \{1, 2, 3, 4\}$; $B = \{5, 6, 7, 8\}$ are disjoint sets.

Self-learning exercise-1

1. Which of the following is not a set :

   (a) $A = [1, 2]$ *(b)* $B = \{1, 2, 3\}$

   (c) $C = \{x \mid x = 1\}$ *(d)* None of these

2. Write the set $A = \{2, 4, 6 ....\}$ in the set builder form.

3. Write the following set in roster form :

   (i) Set of natural numbers multiple of 3 and less than 19

   (ii) Set of squares of integers less than 26.

4. Is $A = \{x \mid x + 1 = 2$ and $3x + 1 = 2\}$ a null set ?

5. If $U = \{1, 2, 3, 4, 5, 6\}$ and $A = \{1, 2\}$. Then write A'.

6. Let $A \{x \mid x \in N, 1 \leq x < 7\}$. List all the elements of the set A.

Illustrative examples

Ex.1. *List the elements of the following set*

(i) $A = \{x \mid x \in N, 0 < x < 5\}$

(ii) $B = \{x \mid x \in N, 7 + x = 14\}$

Sol. *(i)* We know that N stands for set of natural numbers *i.e.* $N = \{1, 2, 3 ....\}$. A is set of those natural numbers which satisfy the criterion $0 < x < 5$. The natural numbers following the rule $0 < x < 5$ are 1, 2, 3, 4.

Hence the set $A = \{1, 2, 3, 4\}$.

(ii) B is set of those natural numbers x such that

$$7 + x = 14 \Rightarrow x = 7.$$

Thus $B = \{7\}$ is a singleton set.

Ex.2. *Show that* $A = \{1, 2\}$ *is not a subset of* $B = \{1, 4, 5, 6\}$.

Sol. We know that A is subset of B if $A \subseteq B$. In order to show that A is not a subset of B it is sufficient to show that there is alleast one element of A that does not belong to B. We see that $2 \in A$ is not an element of B. Hence $A \nsubseteq B$.

Ex.3. *Insert the correct symbols* $\subseteq$ *or* $\nsubseteq$ *between A, B, C where*

$A = \{1, 2, 3\}, B = \{1, 2, 3, 4\}, C = \{1, 2, 3, 4, 5\}$.

Sol. $A \subseteq B \subseteq C$.

Ex.4. *Insert the correct symbol* $\subset$ *or* $\not\subset$ *between A, B, C, D where* $A = \{1\}, B = \{1, 2, 3\}$, $C = \{1, 2, 3, 4\}, D = \{3, 2, 1\}$.

Sol. $A \subset B \subset C$. Note that B and D are the same set as they have same elements. Therefore, $B = D$ hence $B \not\subset D$ or $D \not\subset B$.

Ex.5. *Show that* $A = \{1, 2, 3, 4\}$ *is not a subset of* $Z = \{x \mid x$ *is an even integer}.*

Sol. Given that $Z = \{0, \pm 2, \pm 4, \pm 6 ....\}$ A is not a subset of Z because 1 and 3 don't belong to Z.

3.3 Ordered pair and Cartesian product of sets

An ordered pair is a pair of objects wherein the objects follow certain relationship and accordingly constitute an ordered pair. An ordered pair is denoted as (a, b) where a is called the first component and b is called the second component. Obviously $(a, b) \neq (b, a)$ in general. Note that $(a, b) = (b, a)$ if and only if $a = b$. To illustrate, let us consider the following information about persons and the cities they come from is given as :

Ramesh	Jaipur
Suresh	Delhi

Then this information can be presented in ordered pairs like (Ramesh, Jaipur), (Suresh, Delhi).

The concept of an ordered pair paves the way for the notion of Cartesian product of sets.

Let A and B be two non-empty sets. Then Cartesian product of A and B, denoted by $A \times B$, is defined as

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

Note that $A \times B \neq B \times A$, in general.

Similarly, product of n sets $A_1, A_2 \ldots A_n$ is defined as

$$A_1 \times A_2 \times A_3 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots a_n \in A_n\}$$

Here $(a_1, a_2, \ldots, a_n)$ is called n-tuple of elements $a_1, a_2, a \ldots a_n$.

3.4 Sets operations

There are some operations defined in the theory of sets. When two or more sets undergo with these operations they yield new sets. These operations are of immense significance in combinatorics.

3.4.1 Union of sets :

The union of two sets A and B is the set of all elements which belong to A or to B. Then union of A and B is denoted as $A \cup B$ and is read as "A union B".

Thus, $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

For example, let $A = \{1, 2, 3\}$, $B = \{1, 4, 5\}$

Then $A \cup B = \{1, 2, 3, 4, 5\}$

3.4.2 Intersection of sets :

The intersection of two sets A and B is the set of all elements which belong to both A and B. The intersection of A and B is denoted by $A \cap B$ and is read as "A intersection B".

Thus, $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

Thus, we observe that $A \cap B$ is the set of those elements which are common in A and B.

If A and B don't have any element in common, then $A \cap B = \phi$.

3.4.3 Difference of sets :

Let A and B be two sets. The difference of A and B (or the relative complement of B with respect to A), denoted as $A - B$, is the set of those elements of A which don't belong to B.

Thus symbolically,

$$A - B = \{x \mid x \in A, x \notin B\}$$

Similarly, the difference of B and A is

$$B - A = \{x \mid x \in B, x \notin A\}$$

As an illustration let us consider

$$A = \{1, 2, 3, 4\}, B = \{4, 5, 6, 7, 8, 9\}$$

Then, $A - B = \{1, 2, 3\}$ and $B - A = \{5, 6, 7, 8, 9\}$

3.4.4 Symmetric difference of sets :

Let A and B be two sets. The symmetric difference of A and B. denoted as $A \oplus B$ or $A \Delta B$, is the set of those elements that belong to A or to B but not to both. That is $A \oplus B$ is the set of elements which belong to exactly one of A and B.

Thus, $$A \oplus B = (A - B) \cup (B - A)$$
$$= (A \cup B) - (A \cap B)$$

Note that the symmetric difference is also referred to as Boolean sum.

Example : Let $A = \{4, 5, 6, 7\}$, $B = \{7, 8, 9, 10\}$

Then $$A \oplus B = (A - B) \cup (B - A)$$
$$= \{4, 5, 6\} \cup \{8, 9, 10\}$$
$$= \{4, 5, 6, 8, 9, 10\}$$

3.5 Venn-diagram of sets

A Venn-diagram of a set is a pictorial depiction by sets of points in a plane. The set is represented by disk lying in the rectangle where interior to the rectangle represents the universal set.

If two sets A and B are disjoint then they are shown by disks with no common space between them [see figure 1].

If $A \subseteq B$. Then the disk representing A is shown entirely within the disk representing the set B [see figure 2]

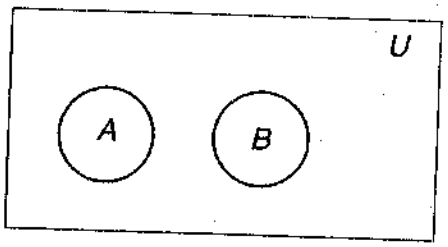


Fig. 1

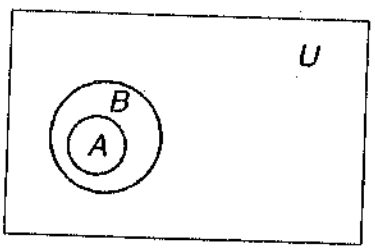


Fig. 2

3.5.1 Set operations in Venn-diagram :

The various operations used in set theory are shown below in the diagrams by shaded areas.

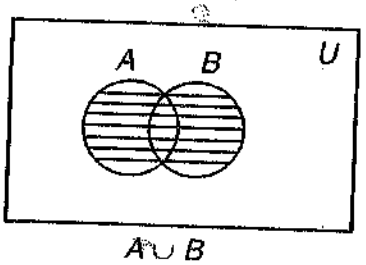


Fig. 3

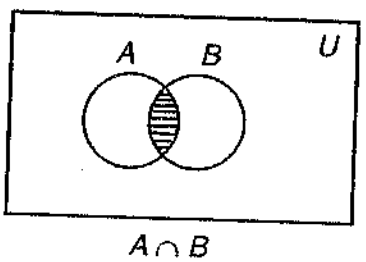
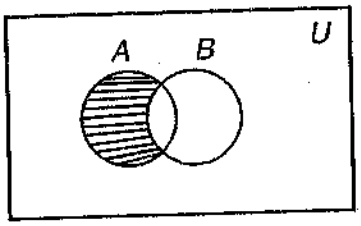
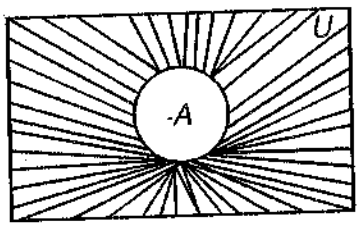


Fig. 4



$A - B$

Fig. 5



A'

Fig. 6

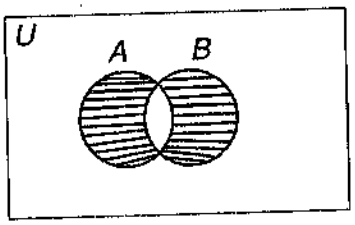


Fig. 7

$$A \oplus B = (A - B) \cup (B - A)$$

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

3.6 Laws of algebra of sets

We have seen that fundamental operations of union, intersection and complementation of sets yield a new set. It is interesting to note that these set operations follow some algebraic laws which help establish important relationship among the set operations. These laws are listed in the table given below and are followed by proofs of some of the laws :

S. No.	Name of the law	Law
1.	Idempotent	$A \cup A = A$ and $A \cap A = \phi$
2.	Associative	(i) $A \cup (B \cup C) = (A \cup B) \cap C$ (ii) $A \cap (B \cap C) = (A \cap B) \cap C$
3.	Distributive	(i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4.	Identity	(i) $A \cup \phi = A$; $A \cap U = A$ (ii) $A \cap \phi = \phi$; $A \cup U = U$
5.	Commutative	(i) $A \cup B = B \cup A$; (ii) $A \cap B = B \cap A$
6.	Complement	(i) $A \cup A' = U$; $A \cap A' = \phi$ (ii) $\phi' = U$; $U' = \phi$
7.	Involution	$(A')' = A$
8.	De-Morgan	(i) $(A \cap B)' = A' \cup B'$ (ii) $(A \cup B)' = A' \cap B'$

3.6.1 Idempotent laws : $A \cup A = A$.

Proof : In order to prove $A \cup A = A$, we shall show that $A \subseteq A \cup A$ and $A \cup A \subseteq A$

[Recall that $A \subseteq B, B \subseteq A \Leftrightarrow A = B$]

Let $x \in A \Rightarrow x \in A$ or $x \in A$ (note)

$\Rightarrow$ $x \in A \cup A$

$\because$ $x \in A$ and we find that $x \in A \cup A$

$\Rightarrow$ $A \subseteq A \cup A$ .....(1)

Again, let $x \in A \cup A$

$\Rightarrow$ $x \in A$ or $x \in A$

Thus $A \cup A \subseteq A$ .....(2)

From (1), (2), we find that $A = A \cup A$

3.6.2 Associative laws :

(i) $A \cup (B \cup C) = (A \cup B) \cup C$

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

Proof : *(i)* We shall show that

$A \cup (B \cup C) \subseteq (A \cup B) \cup C$ and $(A \cup B) \cup C \subseteq A \cup (B \cup C)$

Let $x \in A \cup (B \cup C)$

$\Rightarrow$ $x \in A$ or $x \in B \cup C$

$\Rightarrow$ $x \in A$ or $x \in B$ or $x \in C$

$\Rightarrow$ $x \in A \cup B$ or $x \in C$

$\Rightarrow$ $x \in (A \cup B) \cup C$

Since $x \in A \cup (B \cup C) \Rightarrow x \in (A \cup B) \cup C$

This means that $A \cup (B \cup C) \subseteq (A \cup B) \cup C$ .....(1)

Similarly, we can show that

$(A \cup B) \cup C \subseteq A \cup (B \cup C)$ .....(2)

From (1), (2) we find that

$(A \cup B) \cup C = A \cup (B \cup C)$

(ii) Left as an exereise for you.

3.6.3 Distributive laws :

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

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

Proof : *(i)* Let $x \in A \cup (B \cap C)$

$\Rightarrow$ $x \in A$ or $x \in B \cap C$

$\Rightarrow$ $x \in A$ or $x \in B$ and $x \in C$

$\Rightarrow \quad x \in A \cup B$ and $x \in A \cup C$

$\Rightarrow \quad x \in (A \cup B) \cap (A \cup C)$

Thus we have shown that

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) \quad \text{.....(1)}$$

Again, let $x \in (A \cup B) \cap (A \cup C)$

$\Rightarrow \quad x \in A \cup B$ and $x \in A \cup C$

$\Rightarrow \quad x \in A$ or $x \in B$ and $x \in A$ or $x \in C$

$\Rightarrow \quad x \in A$ or $x \in B \cap C$

$\Rightarrow \quad x \in A \cup (B \cap C)$

Thus, we see that

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C) \quad \text{.....(2)}$$

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

Proof of *(ii)* left as an exercise for the student.

3.6.5 De-Morgan laws :

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

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

Proof. ***(i)*** Let $x \in (A \cup B)'$

$\Rightarrow \quad x$ does not belong to $A \cup B$

$\Rightarrow \quad x$ does not belong to A and x does not belong to B

$\Rightarrow \quad x \in A'$ and $x \in B'$

$\Rightarrow \quad x \in A' \cap B'$

Thus,

$$(A \cup B)' \subseteq A' \cap B' \quad \text{.....(1)}$$

Again, let $x \in A' \cap B' \Rightarrow x \in A'$ and $x \in B'$

$\Rightarrow \quad x \notin A$ and $x \notin B$

$\Rightarrow \quad x \notin A \cup B$

$\Rightarrow \quad x \in (A \cup B)'$

Thus, we conclude that

$$A' \cap B' \subseteq (A \cup B)' \quad \text{.....(2)}$$

From (1) and (2), we find that

$$(A \cup B)' = A' \cap B'$$

Similarly, you can prove the *(ii)* result

Ex. *Using laws of algebra of sets or otherwise prove the following*

(i) $A - B = A \cap B'$

(ii) $A \cup B = (A - B) \cup B$

Sol. *(i)* We know that

$$A - B = \{x \mid x \in A, x \notin B\}$$

$\because \quad x \notin B \Rightarrow x \in B'$

Thus,

$$A - B = \{x \mid x \in A, x \in B'\}$$

Since $x \in A$ and $x \in B' \Rightarrow x \in A \cap B'$

Hence,

$$A - B = \{x \mid x \in A \cap B'\}$$

Consequently $A - B = A \cap B'$

(ii) Let us consider $(A - B) \cup B$

Now,

$$(A - B) \cup B = (A \cap B') \cup B \qquad [\because A - B = A \cap B']$$

$$= B \cup (A \cap B') \qquad \text{[Commutativity]}$$

$$= (B \cup A) \cap (B \cup B') \qquad \text{[Distributivity]}$$

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

$$= A \cup B$$

Self-learning exercise-2

1. Let $A = \{1, 2, 3, 4\}$ $B = \{4, 5\}$ Then the set $\{4\}$ stands for

(i) $A \cup B$ *(ii)* $A \cap B$

(iii) A' *(iv)* B'

2. Let $A = \{2, 4, 6, 8\}$, $B = \{2, 8\}$. Then find

(i) $A \cup B$ *(ii)* $A \cap B$

(iii) $A \oplus B$ *(iv)* $A - B$

3. Using the following Venn-diagram examine whether the given statements are true :

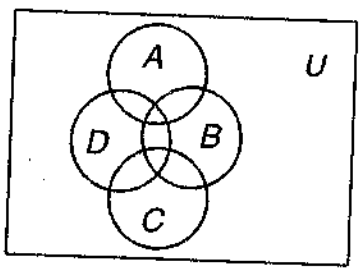


Fig. 8

(i) C and A are disjoint

(ii) $A \subset C'$ or $C \subset A'$

(iii) $B \cap D \subset D$

(iv) $B \subset D$ or $D \subset B$

(v) $A \cap B \cap D$ and $B \cap C \cap D$ are disjoint sets.

3.7 Summary

In this unit you have studied the theory of sets. A set is well defined collection of objects, which are amenable to many set theoretic operations such as union, intersection, complement and difference of sets. After having gone through these concepts, you come across with various laws of algebra of sets.

3.8 Answers to self-learning exercises

Self-learning exercise-1

1. *(a)* 2. $A = \{x \mid x \text{ is even positive integer}\}$

3. *(i)* $\{3, 6, 9, 12, 15, 18\}$

   (ii) $\{1, 4, 9, 16, 25\}$

4. Yes, A is null set because there doesn't exist a number x such that $x + 1 = 2$ and $3x + 1 = 2$ hold simultaneously

5. $A' = \{3, 4, 5, 6\}$

6. $A = \{1, 2, 3, 4, 5, 6\}$

Self-learning exercise-2

1. *(ii)* 2. *(i)*

3. *(i)* True *(ii)* True *(iii)* True *(iv)* True

3.9 Exercises

1. Consider the following sets

   $A = \{x \mid x \text{ is an integer} > 2\}$

   $B = \{a \mid a \text{ is a positive integer multiple of } 3\}$

   Is B a subset of A ?

2. Consider the following sets

   $A = \{1\}, B = \{1, 2\}, C = \{1, 2, 3\}, D = \{3\}, \phi$

   Which of the above are subsets of the set $\{1, 3, 2\}$? Is there any proper subset of the set $\{1, 3, 2\}$?

3. Let $A = \{1, 2, 3, 4, 5\}, B = \{1, a, b, c\}$

   Find $A \cup B, A \cap B, A - B, B - A$ and $A \oplus B$

4. Considering the problem 3, show $A \cup B$ and $A \cap B$ in Venn-diagrams.

5. Show that $A - B = A \cap B'$

6. Let $A = \{a, b, c, d\}$. Then find $P(A)$.

7. Let A and B be two sets then show that

   $A - B = B' - A' = A \cap B'$

8. For sets A, B, C show that

   (i) $A - (B \cup C) = (A - B) \cap (A - C)$

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

9. Using Venn-diagram for any sets A, B, C show that

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

   (ii) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$

□□□

UNIT 4 : Propositional Calculus

Structure of the Unit

4.0 Objectives

After reading this unit you will be able to understand

- The notion of proposition
- Various connectives that give rise to compound propositions
- Laws of algebra of propositions
- Arguments, their validity and logic

4.1 Introduction

The notion of proposition is one of the important ingredient of theory of logic, which together with other things serves as a basis for diverse areas of computer science. Infact, the notion of proposition has got a mathematical basis and is studied as "propositional calculus". The proposition calculus deals with the analysis of statements which are either true or false but not both simultaneously.

4.2 Proposition

A proposition is a declarative sentence that is either true or false but not both. A proposition has a truth value accordingly its being true or false. Sentences involving commands, exclamations, questioning are not propositions. A proposition may have truth value T or F, T stands for the case when the proposition is true and F stands for the case when the proposition is false. Propositions are represented by letters $p, q, r, \ldots$ which are known as proposition variables.

Ex.1. *Which of the following are propositions ?*

(a) *Jaipur is in Rajasthan.*

(b) $2 + 5 = 6$

(c) *How are you ?*

(d) *What a rainy day it was !*

Sol. The expressions *(a)* and *(b)* are declarative statements. *(a)* is true and *(b)* is false. Expressions *(c)* and *(d)* are not propositions since neither is true or false.

Now the question arises whether we can make out a single proposition while using two or more propositions. The answer is affirmative. It is done with the help of logical operators (connectives).

4.2.1 Compound proposition and connectives :

A proposition is called a simple proposition if it cannot be reduced (sub divided) into another simpler proposition. Connective are used to make compound proposition. A compound proposition is obtained from combinations of propositions with the help of connectives. The truth value of a compound statement can be completely determined. A compound proposition obtained from simpler propositions $p, q, r,\ldots$ is denoted as $P(p, q, r,\ldots)$, where $p, q, r,\ldots$ are called variables of the compound proposition $P(p, q, r,\ldots)$.

There are three basic connectives : conjunction ($\wedge$), disjunction ($\vee$) and negation ($\sim$).

Conjunction: Conjunction of propositions p and q is denoted by $p \wedge q$. Some authors write it as $p \cdot q$ or pq or p and q.

$p \wedge q$ is read as "p and q".

The proposition $p \wedge q$ is true whenever both p and q are true; otherwise $p \wedge q$ is false. This can easily be seen by the truth table. A truth table is a table that contains the truth values of a compound proposition for all possible cases. Thus, the truth table of $p \wedge q$ is as given below :

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

From the first line of the table, we find that $p \wedge q$ is true when both p and q are true. Similarly from the other lines we get the respective meanings.

Disjunction : Disjunction of propositions p and q is denoted by $p \vee q$. Some authors write it as $p + q$.

$p \vee q$ is read as "p or q"

The statement $p \vee q$ is true whenever either p or q is true or both p and q are true; otherwise $p \vee q$ is false. This can be shown as follows in the truth table

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

Negation : Negation of a proposition p is denoted by $\sim p$. Some authors write it as p', $\bar{p}$ or $\neg p$.

Negation of p, that is $\sim p$ is read as "not p" or "it is false that p" or "It is not true that p".

The truth table of negation is as follows :

p	$\sim p$
T	F
F	T

Ex.1. *Write the following compound propositions in symbolic from.*

(i) *It is not hot* ***(ii)*** *It is hot or it is not raining*

(iii) *He is dark but tall* ***(iv)*** *It is false that it is raining or it is cold*

(v) *John is neither tall nor intelligent.*

Sol. We know that the symbols $\wedge$, $\vee$ and $\sim$ stands for "and", "or" and "not" or "it is false that" respectively. Hence, we will use these accordingly.

(i) Let p be "It is hot today"

Then $\sim p$ reads "It is not hot today"

(ii) Let p be "It is hot" and q be "It is raining"

Then required symbolic form is $p \vee \sim q$

(iii) Let p be "He is dark" and q be "He is tall"

Then the required symbolic form is $p \wedge \sim q$

(iv) Let p be "It is raining" and q be "It is cold"

Then the required symbolic form is $\sim p \vee q$

(v) Let p be "John is tall" and q be "John is intelligent".

Then required form is $\sim p \wedge \sim q$

Ex.2. *Let p : "It is hot today" and q : "It is raining". Then write simple verbal expression which describes the following propositions :*

(i) $\sim q$ *(ii)* $p \vee \sim q$

(ii) $p \wedge q$ *(iv)* $p \vee q$

(v) $\sim p \wedge \sim q$ *(vi)* $\sim (\sim p)$

(vii) $\sim p \vee \sim q$

Sol. *(i)* $\sim q \equiv$ It is not raining or it is false that it is raining

(ii) $p \vee \sim q \equiv$ It is hot today or it is not raining

(iii) $p \wedge q \equiv$ It is hot today and raining

(iv) $p \vee q \equiv$ It is hot today or it is raining

(v) $\sim p \wedge \sim q \equiv$ It is neither hot today nor raining or It is not hot today and it is not raining

(vi) $\sim (\sim p) \equiv$ It is false that it is not hot today

(vii) $\sim p \vee \sim q \equiv$ It is false that it is hot today or it is not raining

Ex.3. *Let p : "He is rich", q : "He plays golf". Assuming that "He is poor" is equivalent of $\sim p$ i.e.*

He is not rich, write the following compound propositions in symbolic form.

(i) He is either rich or plays golf.

(ii) It is false that he is poor or plays golf.

(iii) He is not poor but plays golf.

(iv) He is rich or he is poor and plays golf.

(v) It is not true that he is not rich or he does not play golf.

Sol. *(i)* $p \vee q$ *(ii)* $\sim (\sim p \vee q)$

(iii) $\sim (\sim p) \wedge q$ *(iv)* $p \vee (\sim p \wedge q)$

(v) $\sim (\sim p \vee \sim q)$

Ex.4. *Let p be "Ramesh plays cricket"; let q be "Ramesh plays hockey", and let r be "Ramesh plays chess". Then express the following propositions in symbolic form.*

(i) It is false that Ramesh plays chess or cricket but hockey

(ii) Ramesh plays cricket and chess but not hockey

Sol. *(i)* $\sim [(r \vee p) \wedge q)$ *(ii)* $(p \vee r) \wedge \sim q$

Self-learning exercise-1

1. Which is not true about a proposition ?

(a) Proposition has definite truth value.

(b) Proposition is a declarative sentence.

(c) A proposition may be of the form $p \vee q$.

(d) A proposition can never be of the form $\sim p$.

2. The symbol $\vee$ stands for

(a) or *(b)* and

(c) not *(d)* implication.

3. Let p : Jaipur is in Delhi $q : 2 + 2 = 4$

(i) Then the truth value of $p \vee q$ is

(a) T *(b)* F

(ii) The truth value of $p \wedge q$ is :

(a) T *(b)* F

4. Let $p : 2 + 2 = 4$; $q : 5 + 5 = 10$; $r : 8 + 3 = 20$.

Then truth value of $(p \vee q) \vee r$ and $(p \wedge q) \wedge r$ respectively are :

(a) T, F *(b)* T, T

(c) F, T *(d)* F, F

5. If truth value of $\sim (p \wedge q)$ is T. Then the truth value of $\sim p \vee \sim q$:

(a) is F. *(b)* is T

(c) depends on the values of p and q. *(d)* can't be determined.

4.2.2 Tautologies and contradictions :

A compound proposition $P(p, q, ...)$ is called tautology if P is true for any truth value of its variables *i.e.* P is tautology if it contains only T in the last column of its truth table. Similarly, a proposition $P(p, q,...)$ is a contradiction if P is false for any truth values of its variables *i.e.* P is contradiction if it contains only F in the last column of its truth table. Note that if $P(p, q, ...)$ is a tautology then $\sim P(p, q, ...)$ is a contradiction, and vice versa.

Ex.1. *Prove that* $(\sim p \wedge \sim q) \wedge (p \wedge q)$ *is not a tautology.*

Sol. Let us construct the truth table $(\sim p \wedge \sim q) \wedge (p \wedge q)$ as given below :

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

Since the truth value of $(\sim p \wedge \sim q) \wedge (p \wedge q)$ is F for all possible values of p and q. Hence the given proposition is not a tautology but a contradiction.

Ex.2. *Prove that the proposition* $\sim [p \vee (\sim p \vee \sim q)]$ *is a contradiction.*

Sol. Let us construct the truth table of $\sim [p \vee (\sim p \vee \sim q)]$ as given below :

p	q	$\sim p$	$\sim q$	$\sim p \vee \sim q$	$p \vee (\sim p \vee \sim q)$	$\sim [p \vee (\sim p \vee \sim q)]$
T	T	F	F	F	T	F
T	F	F	T	T	T	F
F	T	T	F	T	T	F
F	F	T	T	T	T	F

Since the truth values of $\sim [p \vee (\sim p \vee \sim q)]$ are F for all possible values of p and q, hence the proposition is a contradiction.

Ex.3. *Verify whether the proposition "He works hard or he does not work hard" is tautology.*

Sol. Let p be "He works hard"

Then $\sim p$ is "He does not work hard"

The given proposition is a tautology if $p \vee \sim p$ is true for are possible values of p and $\sim p$. We construct the following truth table for $p \vee \sim p$

p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

Since $p \vee \sim p$ is true for all values of p and $\sim p$, hence it is a tautology.

4.2.3 Logically equivalent propositions :

Let P $(p, q, ...)$ and Q $(p, q,...)$ be two propositions. Then P and Q are said to be logically equivalent, denoted by $P \equiv Q$, if they have some truth tables.

For example, $\sim (\sim p \vee \sim q) \equiv p \wedge q$ as can be seen in the following tables

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

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

Since both the propositions are true in first case and false in other three cases, the propositions are logically equivalent *i.e.* $p \wedge q \equiv \sim (\sim p \vee \sim q)$

Ex. *Prove that the proposition "He neither studies nor dances" is logically equivalent to the proposition "It is false that he studies or dances".*

Sol. Let p be "He studies" and q be "He dances"

Then the proposition "He neither studies nor dances" can be written in symbolic form as $\sim p \wedge \sim q$. The proposition "It is false that the studies or dances" can be represented as $\sim [p \vee q]$.

To see the logical equivalence of these propositions we construct the following truth tables :

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

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

We see that $\sim p \wedge \sim q \equiv \sim(p \vee q)$.

Self-learning exercise-2

1. Prove that $\sim p \vee \sim q \equiv \sim(p \wedge q)$.
2. Show that $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$.
3. Prove that $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.
4. Show that $q \wedge \sim q$ is not a tautology.

4.3 Laws of algebra of propositions

The theory of propositions has a beauty in the sense that the propositions follow certain algebraic laws which are not only quite useful in simplifying the expressions but also give an edge to the notion. The laws have some parallels to their counterpart laws in standard algebra you are familiar with. Infact, in some cases the connectives $\vee$ and $\wedge$ act like + and · However all laws don't follow same analogy.

The laws are listed in the following table :

Indempotent laws	$p \vee p = p$ and $p \wedge p = p$
Associative laws	*(i)* $p \vee (q \vee r) = (p \vee q) \vee r$ *(ii)* $p \wedge (q \wedge r) = (p \wedge q) \wedge r$
Distributive laws	*(i)* $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$ *(ii)* $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$
Commutative laws	*(i)* $p \vee q = q \vee p$ *(ii)* $p \wedge q = q \wedge p$
Involution law	$\sim(\sim p) = p$
Identity laws	*(i)* $p \vee F = p$, $p \wedge T = p$ *(ii)* $p \vee T = T$, $p \wedge F = F$
Complement laws	*(i)* $p \vee \sim p = T$, $p \wedge \sim p = F$ *(ii)* $\sim T = F$, $\sim F = T$
De'Morgan's laws	*(i)* $\sim(p \vee q) = \sim p \wedge \sim q$ *(i)* $\sim(p \wedge q) = \sim p \vee \sim q$

The validity of the above laws can be established by the relevant truth table. Many other laws can be given with the help of the laws listed above.

For example, $p \vee (p \wedge q) = p$ and $p \wedge (p \vee q) = p$ hold good and are called absorption laws. These can be derived in the following manner.

Let us consider

$$p \vee (p \wedge q) = (p \wedge T) \vee (p \wedge q) \qquad [\because p \wedge T = p]$$
$$= p \wedge (T \vee q) \qquad \text{[Distributive law]}$$
$$= p \wedge T \qquad [\because T \vee q = T]$$
$$= p$$

Now, we prove some of the laws given in the table.

De'Morgan's laws :

(i) $\sim (p \wedge q) = \sim p \vee \sim q$

(ii) $\sim (p \vee q) = \sim p \wedge \sim q$

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

From the table we see that

$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$

Similarly, you can verify that

$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$

Ex.1. *Show that* $p \vee (q \vee r) \equiv (p \vee r) \vee r$.

Sol.

p	q	r	$p \vee q$	$q \vee r$	$p \vee (q \vee r)$	$(p \vee q) \vee r$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	T	T	T	T
T	F	F	T	F	T	T
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

From the last two columns of the table we find that

$$p \vee (q \vee r) = (p \vee q) \vee r$$

Ex.2. *Using laws of the algebra of propositions, show that*

(i) $\sim (p \vee q) \vee (\sim p \wedge q) \equiv \sim p$

(ii) $\sim q \wedge (p \vee q) \equiv \sim q \wedge p$

Sol. ***(i)*** We have

$$\begin{aligned} \sim (p \vee q) \vee (\sim p \wedge q) &= (\sim p \wedge \sim q) \vee (\sim p \wedge q) \\ &= \sim p \wedge (\sim q \vee q) \\ &= \sim p \wedge T \\ &= \sim p \end{aligned}$$

(ii) We have

$$\begin{aligned} \sim q \wedge (p \vee q) &= (\sim q \wedge p) \vee (\sim q \wedge q) \\ &= (\sim q \wedge p) \vee F \\ &= \sim q \wedge p \end{aligned}$$

Self-learning exercise-3

1. The idempotent law is :

(a) $p \vee q = q \vee p$ *(b)* $\sim (\sim p) = p$ *(c)* $p \vee \sim q = T$ *(d)* $p \vee p = p$

2. $p \wedge (q \vee r)$ is equivalent to :

(a) $p \vee (q \wedge r)$ *(b)* $(p \wedge q) \vee (p \wedge r)$ *(c)* $(p \vee q) \wedge r$

3. Which of the following is true ?

(a) $p \vee F = p$ *(b)* $p \wedge F = p$ *(c)* $p \wedge T = F$

4. Which of the following is not true :

(a) $\sim (p \wedge q) \equiv \sim p \wedge \sim q$ *(b)* $\sim (p \wedge q) \equiv \sim p \vee \sim q$

(c) $\sim (p \vee q) \equiv \sim p \wedge \sim q$ *(d)* $p \vee p = p$

5. Prove that $p \wedge (q \wedge r) = (p \wedge q) \wedge r$

6. Prove that $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$

4.4 Conditional propositions and their negations

Many a times, we come across with the statements with imposed conditions. For example, "I dance if it rains" or "I dance if and only if it rains".

Such statements are called conditional and biconditional respectively. Study of these is important in the theory of logic.

4.4.1 Implication and its variations :

A statement of the form "If p then q" is called an implication or a conditional statement and is written as

$$p \rightarrow q$$

The other versions of $p \rightarrow q$ are :

(i) p only if q, *(ii)* p is sufficient for q,

(iii) q is necessary for p, *(iv)* p implies q.

The statement $p \rightarrow q$ is true barring the case that p is true and q is false *i.e.* $p \rightarrow q$ is false when p is true and q is false, otherwise it is true for the remaining possible values of p and q.

The truth values of $p \rightarrow q$ is shown in the following table :

p	q	$p \rightarrow q$	$\sim p$	$\sim p \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

From the above table, we observe that

$$p \rightarrow q \equiv \sim p \vee q$$

We, now describe the variations of $p \rightarrow q$. The conditionals $q \rightarrow p$, $\sim p \rightarrow \sim q$ and $\sim q \rightarrow \sim p$ are called respectively the **converse, inverse** and **contrapositive** of the conditional $p \rightarrow q$.

Ex.1. *Determine the truth values of the following statements*

(a) *If Jaipur is in India, then* $2 + 6 = 8$

(b) *If* $4 + 4 = 7$, *then* $8 + 8 = 16$

(c) *If* $3 + 3 = 6$, *then* $5 + 5 = 9$

(d) *If* $3 + 3 = 5$, *then* $4 + 4 = 7$

Sol. The given statements are of "$p \rightarrow q$" form. We know that $p \rightarrow q$ is true except in the case when p is true and q is false. Therefore, statements *(a), (b), (d)* are true and *(c)* is false.

Ex.2. *Find the truth value of* $(p \vee q) \rightarrow (p \rightarrow q)$.

Sol. We construct the following truth table :

p	q	$p \vee q$	$p \rightarrow q$	$(p \vee q) \rightarrow (p \rightarrow q)$
T	T	T	T	T
T	F	T	F	F
F	T	T	T	T
F	F	F	T	T

Ex.3. *Rewrite the following propositions without using the conditional :*

(a) *If share market sensex goes up, then prices rise.*

(b) *If it rains, he dances.*

Sol. We know that proposition "If p then q" stands for $p \to q$ which itself is logically equivalent to $\sim p \vee q$. Hence the given propositions can be written as

(a) Share market sensex does not go up or prices rise

(b) It does not rain or he dances.

4.4.2. Biconditional statement ($p \leftrightarrow q$) :

Let p and q are propositions then the compound proposition "p if and only if " is called the biconditional proposition and is denoted by $p \leftrightarrow q$. The other equivalents of $p \leftrightarrow q$ are :

1. "p implies q and q implies p" *i.e.* $p \leftrightarrow q$ is logically equivalent to $(p \to q) \wedge (q \to p)$

   and

2. p is a necessary and sufficient condition for q.

   Note that $p \leftrightarrow q$ is true when both p and q are true or both p and q are false. This is evident from the following truth table for $p \leftrightarrow q$.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Ex.1. *Determine the truth values of the following statements :*

(a) $5 + 7 = 6$ *if and only if* $2 + 3 = 8$

(b) $1 + 6 = 7$ *if and only if* $2 + 4 = 6$

(c) $2 + 3 = 8$ *if and only if* $2 + 2 = 4$

Sol. We know that $p \leftrightarrow q$ is true whenever both p and q have the same truth values. Therefore, following the reason we see that only statement *(a)* is true.

Ex.2. *Show that* $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$.

Sol. In order to prove that $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$ we construct following truth table :

p	q	$p \to q$	$q \to p$	$p \leftrightarrow q$	$(p \to q) \wedge (q \to p)$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Ex.2. *Write the negation of following statements :*

(a) *If it is humid, then he wears cotton shirt but no cap,*

(b) *If he makes money, then he will purchase a car or airship.*

Sol. ***(a)*** Let p denote "It is humid"

q denote "He wears cotton shirt"

r denote "He wears a cap"

Then the given proposition is $p \to (q \wedge \sim r)$

The negation of it is $\sim [p \to (q \wedge \sim r)]$

$\equiv \sim [\sim p \vee (q \wedge \sim r)]$

$\equiv p \wedge \sim (q \wedge \sim r)$

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

Therefore, the negation of the statement is –

It is humid and he wears a cap or no cotton shirt.

(b) Let p denote "He makes money"

q denote "He will purchase a car"

r denote "He will purchase an airship"

The given statement is of the form $p \to (q \vee r)$

Its negation is : $\sim [p \to (q \vee r)]$

$\equiv \sim [\sim p \vee (q \vee r)]$

$\equiv p \wedge (\sim q \wedge \sim r)$.

Thus the required negation is :

He makes money and he will neither purchase a car or an airship.

Ex.3. *Find the converse, inverse and contrapositive of the following conditional "only if Rama works hard will he get money".*

Sol. The given statement is equivalent to "If Rama gets money, then he worked hard"

Let p : Rama gets money

q : Rama worked hard.

The given statement is of $p \to q$ form whose converse, inverse and contrapositive are $q \to p$, $\sim p \to \sim q$ and $\sim q \to \sim p$ respectively.

Thus, the converse is :

If Rama worked hard, then he gets money.

Inverse is :

If Rama does not get money, then he did not work hard.

Contrapositive is :

If Rama did not work hard, then he does not get money.

Ex.4. *Write the negation of following statements in simplest possible form :*

(a) *He plays only if the weather is cold.*

(b) *If it rains, then he does not wear rain coat.*

Sol. ***(a)*** Let p be "He plays" and q be "the weather is cold".

The given statement is of $p \to q$ form.

Now, $\sim (p \to q) \equiv \sim (\sim p \vee q) \equiv p \wedge \sim q$

Hence the negation of the given statement is :

He plays and the weather is not cold.

(b) Let p be "It rains", q be "He does not wear raincoat"

The given statement is of $p \to q$ form

Since $\sim (p \to q) \equiv p \wedge \sim q$

The negation of the given statement is :

It rains and he wears raincoat.

Self-learning exercise-4

1. $p \to q$ is known as :

(a) Indication *(b)* Implication *(c)* Intimation *(d)* Inclination

2. $q \to p$ is equivalent to :

(a) $\sim q \vee p$ *(b)* $\sim p \wedge \sim q$ *(c)* $\sim p \vee q$ *(d)* $p \vee \sim q$

3. $p \to q$ is equivalent to :

(a) q is sufficient for p *(b)* p is necessary for q

(c) p is necessary and sufficient for q *(d)* p is necessary for $\sim q$

4. $p \leftrightarrow q$ is equivalent to :

(a) $(p \to q) \vee (q \to p)$ *(b)* $(q \to p) \wedge (p \to q)$

(c) $(p \vee \sim q) \vee (q \to p)$ *(d)* $(p \vee q) \wedge (p \wedge q)$

4.5 Arguments

Valid arguments and logic in proof :

An arguments is a sequence of propositions $P_1, P_2, \ldots P_n$ called premises that as a consequence yields another proposition Q. $P_1, P_2, \ldots, P_n$ are called premises or assumptions or hypothesis and Q is called the conclusion. An argument with premises $P_1, P_2, \ldots P_n$ and conclusion Q is denoted as

$$P_1, P_2, \ldots P_n \vdash Q$$

Valid argument : An argument is "valid" or "logical" if conclusion is true whenever all the premises are true. An argument which is not valid is called a fallacy.

Working method : 1. To ascertain the validity of argument $P_1, P_2, \ldots P_n \vdash Q$, make a truth table and find truth values of $(P_1 \wedge P_2 \wedge \ldots P_n) \rightarrow Q$. If it is a tautology, then the given argument is a valid statement, otherwise is a fallacy.

2. Another way of verifying that an argument is valid or not, it is sufficient to check only those rows of the truth table in which all the premises and conclusions have a true (T) as truth values.

We, now state some standard laws which are quite useful in the theory of logic.

Modus Ponens : It states that "If the proposition p is true and the implication $p \rightarrow q$ is also true, then, q must be true. Symbolically, we write

$$p \rightarrow q$$

$$\underline{p}$$

$$\therefore q$$

In the above symbolic representation, the statements above the line are the given premises and the premise below the line is the conclusion. The above law is also referred to as law of detatchment. The authenticity of the above law can be viewed by constructing a truth table.

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

Since $p \wedge (p \rightarrow q) \rightarrow q$ is a tautology, therefore, q is a conclusion of the premises $p \rightarrow q$ and p. Another way of verifying that an argument is valid or not, it is sufficient to check only those rows of the truth table in which all the premises and conclusion have a true (T) as truth values.

In the above table, we see that the first row has T for both premises p and $p \rightarrow q$ and the conclusion q.

Modus Tollens : If the proposition $p \rightarrow q$ is assumed as true and also the statement $\sim q$ is true, then, $\sim p$ must be true. Modus tollens is a Latin word meaning denying method simply because the conclusion is a denial. In symbolic form this law can be written as

$$p \rightarrow q$$

$$\underline{\sim q}$$

$$\therefore \sim p$$

The validity of the above law can be seen from the following truth table. Note that $[(p \rightarrow q) \wedge \sim q] \rightarrow \sim p$ is a tautology.

p	q	$\sim p$	$\sim q$	$p \to q$	$(p \to q) \wedge \sim q$	$[(p \to q) \wedge \sim q] \to \sim p$
T	T	F	F	T	F	T
T	F	F	T	F	F	T
F	T	T	F	T	F	T
F	F	T	T	T	T	T

3. Hypothetical syllogism : If two implications $p \to q$, $q \to r$ are true, then the implication $p \to r$ is also true. This law is called hypothetical syllogism.

Symbolically,

$$p \to q$$

$$\frac{q \to r}{\therefore p \to r}$$

The validity of the above law can be seen in the following table. Note that $[(p \to q) \wedge (q \to r)] \to (p \to r)$ is a tautology.

p	q	r	$p \to q$	$q \to r$	$p \to r$	$(p \to q) \wedge (q \to r)$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	T	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

4. Disjunctive Syllogism : It says that if propositions $p \vee q$ and $\sim p$ are considered to be true, then the conclusion q is also true. Symbolically,

$$p \vee q$$

$$\frac{\sim p}{\therefore q}$$

The validity of the above law can be seen in the following truth table. Note that $[(p \vee q) \wedge \sim p] \to q$ is a tautology.

p	q	$\sim p$	$p \vee q$	$(p \vee q) \wedge \sim p$	$[(p \vee q) \wedge \sim p] \rightarrow q$
T	T	F	T	F	T
T	F	F	T	F	T
F	T	T	T	T	T
F	F	T	F	F	T

5. Constructive dilemma : If propositions $p \rightarrow q \wedge (r \rightarrow s)$ and $p \vee r$ be considered as true, then the conclusion $q \vee s$ is also true. Symbolically,

$$p \rightarrow q \wedge (r \rightarrow s)$$

$$\frac{p \vee r}{\therefore q \vee s}$$

You can verify the validity of the above law by verifying from the truth table that $[p \rightarrow q \wedge (r \rightarrow s)] \wedge [p \vee r] \rightarrow q \vee s$ is a tautology.

6. Destructive dilemma : If propositions $p \rightarrow q \wedge (r \rightarrow s)$ and $(\sim q \vee \sim s)$ are considered to be true then the conclusion $\sim p \vee \sim r$ is also true. Symbolically,

$$p \rightarrow q \wedge (r \rightarrow s)$$

$$\frac{\sim q \vee \sim s}{\therefore \sim p \vee \sim r}$$

You can verify that $[p \rightarrow q \wedge (r \rightarrow s)] \wedge [\sim q \vee \sim s] \rightarrow \sim p \vee \sim r$ is a tautology.

7. Addition : This law is stated as

$$\frac{p}{\therefore p \vee q}$$

You can see that $p \rightarrow (p \vee q)$ is a tautology.

8. Simplification : This law is stated as

$$\frac{p \wedge q}{\therefore p}$$

You can verify that $(p \wedge q) \rightarrow p$ is a tautology.

Ex.1. *Prove the validity of the following argument "If I work hard and get rich then I will get promoted. If I get promoted, then I will be wiser. I will not be wiser. Hence, either I will not be rich or I will not work hard."*

Sol. Let the propositions are denoted by p, q, r and s as given below

p : I work hard

q : I get rich

r : I get promoted

s : I will be wiser

In symbolic form, the given argument is written as

$$(p \wedge q) \to r$$

$$r \to s$$

$$\sim s$$

Thus we have the following steps

(i) $(p \wedge q) \to r$ *(ii)* $r \to s$	given
(iii) $(p \wedge q) \to s$	[using hypothetical syllogism in *(i)*, *(ii)*]
(iv) $\sim s$	[given]
(v) $\sim (p \wedge q)$	[using modus tollens in *(iii)*, *(iv)*]
(vi) $\sim p \vee \sim q$	$[\because \sim (p \wedge q) \equiv \sim p \vee \sim q]$

Thus the conclusion is $\sim p \vee \sim q$

Therefore, the given argument is valid.

Ex.2. *Verify whether $p \to -s$ is valid conclusion of the premises*

$$p \to q,\ s \to \sim q$$

Sol. We have

(i) $p \to q$	
(ii) $s \to \sim q$	
(iii) $q \to \sim s$	$[\because s \to \sim q \equiv q \to \sim s]$
(iv) $p \to \sim s$	[using hypothetical syllogism in *(i)*, *(iii)*]

Hence $p \to \sim s$ is valid conclusion of the given premises

Ex.3. *"If I work hard, then I am rich*

I work hard, therefore I am rich"

Represent the above argument symbolically and verify its validity.

Sol. Let p be "I work hard" and

q be "I am rich"

Symbolic form can be written as

$$p \to q$$

$$\frac{p}{\therefore q}$$

According to the principle of modus ponens the argument is valid.

4.6 Summary

A proposition is a declarative sentence with truth value true or false but not both simultaneously. With logical connectives, two or more propositions give rise to another propositions. In this unit, you have learnt about compound propositions, conditional propositions and arguments. You have also learnt many laws of logic which help in solving word problems with tacit logical situations.

4.7 Answers to self-learning exercises

Self-learning exercise-1

1. *(d)* **2.** *(a)* **3.** *(i) (a), (ii) (b)* **4.** *(a)* **5.** *(a)*

Self-learning exercise-3

1. *(d)* **2.** *(b)* **3.** *(a)* **4.** *(a)*

Self-learning exercise-4

1. *(b)* **2.** *(a)* **3.** *(c)* **4.** *(b)*

4.8 Exercises

1. Assign a truth value to each of the following sentences :

   (i) $6 > 7 \vee 8 < 9$

   (ii) $(3 + 4 = 8) \vee (8 \times 4 = 20)$

   (iii) $(8 + 8 = 16) \wedge (4 \times 4 = 16)$

   (iv) $(9 + 9 = 12) \wedge (4 \times 4 = 16)$

   [Ans. *(i)* True *(ii)* False *(iii)* True *(iv)* False

2. Consider the following :

   p : Ram is tall

   q : Ram is strong

   Write the following statements in symbolic form :

   (a) Ram is tall and strong.

   (b) Ram is tall or strong.

   (c) Ram is neither tall nor strong.

   [Ans. *(a)* $p \wedge q$ *(b)* $p \vee q$ *(c)* $\sim p \wedge \sim q$**]**

3. Write the negation of the following :

   (a) If it rains, then they will not go for dinner.

   (b) If Ram works hard, he will make money.

[**Ans.** *(a)* It rains and they will go for dinner.

(b) Ram works hard and he will not make money.]

4. Prove that the following are tautologies :

(a) $(q \wedge p) \rightarrow (p \wedge q)$

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

(c) $[p \wedge (\sim p \vee q)] \rightarrow q$

(d) $(p \wedge q) \rightarrow p$

5. Prove that :

(i) $p \wedge (\sim q \vee q) \equiv p$

(ii) $(p \wedge q) \vee p \equiv q$

6. Prove that :

(i) $q \leftrightarrow p \equiv (\sim q \vee p) \wedge (\sim p \vee q)$

(ii) $[(p \vee q) \rightarrow r] \equiv [(p \rightarrow r) \wedge (q \rightarrow r)]$

7. Find the converse, Inverse and contrapositive of the following :

(a) If today is rainy day, then tomorrow is Sunday.

(b) If A is rectangle, then P is a square.

(c) If Ram is good, then he is honest.

8. Prove that :

$$(p \rightarrow \sim q) \wedge (r \rightarrow p) \wedge q \vdash \sim r$$

9. Test the validity of the following argument :

If Raju worked hard, then he purchased a car.

Raju purchased a car.

Therefore, Raju worked hard.

[**Ans.** Not valid]

10. Using laws of algebra for propositions, prove :

(a) $(p \rightarrow q) \wedge (q \rightarrow r) \wedge (r \rightarrow s) \wedge (p \vee t) \wedge \sim s \vdash t$

(b) $(p \rightarrow q) \wedge \sim q \vdash \sim p$

(c) $[p \rightarrow q \wedge (r \rightarrow s)] \wedge [\sim q \vee \sim s] \vdash \sim p \vee \sim r$

(d) $(p \vee q) \wedge (q \rightarrow r) \wedge (p \rightarrow t) \wedge \sim t \vdash r \wedge (p \vee q)$

□□□

Unit 5 : Relations

Structure of the Unit

5.0 Objectives

After reading this unit you will be able to

- Understand the notion of relation and its representation
- Learn about relations defined on a set and its various types

5.1 Introduction

The notion of relation is an important concept in mathematical sciences. A relation indicates association between two objects. For example, a is less than b. Infact, in daily life we come across with various types of relations. The notion of relation is amenable to mathematical treatment. A relation is denoted as ordered pairs. This unit entails mathematical conceptualization of relations on sets and their

classification. Equivalence relation and partial ordering relation are very important since equivalence relation induces partition of the set on which it is defined whereas partial ordering relation constitutes poset which give rise to concept of lattice in as much as that every lattice is a poset but converse is not necessarily true.

5.2.1 Relation and its representations :

A binary relation or simply relation R from a set A to set B is subset of $A \times B$, where ordered pair $(a, b) \in R$ means that $a \in A$ is related to $b \in B$ under relation R. If a is not related to b under the relation R, then we write $(a, b) \notin R$. Or $a \not R\ b$ or a is not R-related to b. If $(a, b) \in R$, then we write a is R-related to b or $a\ R\ b$.

Thus we conclude that if R is a relation from a set A to set B, then R is set of all those ordered pairs (a, b) where $a\ R\ b$ and hence obviously $R = \{(a, b) \mid a\ R\ b\} \subseteq A \times B$.

In this unit, we will emphasise on relations which are defined on a set A *i.e.* those relations which are subset of $A \times A$. Hence, we define the following.

Relation on a set A :

If R is a relation from a set A to set A then we say that R is a relation on the set A. Thus, in this case $R \subseteq A \times A$.

Domain and range of relation :

Let R be a binary relation

$$R = \{(a, b) \mid a\ R\ b\}$$

Then the set of all $a's$ is called the domain of R and the set of $b's$ is called the range of R.

Inverse relation : Let R be a relation from a set A to set B *i.e.* $R \subseteq A \times B$. Then inverse of R, denoted by R^{-1}, is the relation from set B to A. And is defined as

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}$$

i.e. $$bR^{-1}\ a \Leftrightarrow a\ R\ b$$

Thus to obtain R^{-1} of the relation R we have to reverse the order of the ordered pairs of R.

Consider the relation R on the set $A = \{2, 3, 4, 6\}$ defined by "$a\ R\ b$ if a divides b"

Then $R = \{(2, 2)\ (3, 3), (4, 4), (6, 6)\ (2, 4), (2, 6), (3, 6)\}$

Then $R^{-1} = \{(2, 2), (3, 3), (4, 4), (6, 6)\ (4, 2), (6, 2), (6, 3)\}$

Ex.1. *Let R be a relation from a set $A = \{a, b, c\}$ to set $B = \{x, y, z\}$ given by the set*

$$R = \{(a, x), (a, y), (b, z)\}$$

Then find the domain and range of the relation R.

Sol. The domain of a relation R is collection of first elements of ordered pairs which belong to relation set R. Similarly the collection of second elements of ordered pairs of R is the range of R.

Hence, domain $R = \{a, b\}$

Image $R = \{x, y, z\}$

Till now, we have described a relation as a set of ordered pairs. However, sometimes a pictorial representation of relations on finite sets is found convenient. This is done through arrow diagram. To explain, let us consider a relation $R \subseteq A \times B$. The finite sets A and B are represented by two non overlapping disks. If $(x, y) \in R$, then a directed arrow from x to y denotes that $x\ R\ y$. For example, the relation $R = \{(a, x), (b, y), (a, z)\}$ where $A = \{a, b, c\}$, $B = \{x, y, z\}$ is shown is the following figure.

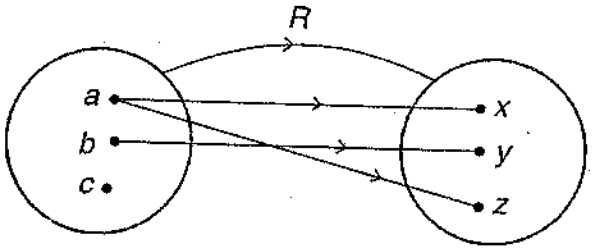


Fig. 1

Furthermore, matrix notation is also used to denote relations.

Let $R \subseteq A \times B$, where A and B are finite sets. Then we consider a rectangular array, where elements of A and B are placed in column and rows respectively outside the array. We put 1 in respective position if $(a, b) \in R$, where $a \in A$, $b \in B$ and other wise put 0 if $(a, b) \notin R$. The array thus found is called matrix of the relation R. Thus the relation R depicted in Fig. 1 can be presented in matrix notation as given below

	x	y	z
a	1	0	1
b	0	1	0
c	0	0	0

Fig. 2

We now consider the case where relation R is defined on a set A. *i.e.* $R \subseteq A \times A$. A relation defined on a set A can be depicted through "directed graph". In this representation of a relation, all the elements of the set A are placed encircled on a plane.

If $a\ R\ b$, then a is connected to b by a directed arrow. For example, consider the relation $R = \{(x, x), (y, y), (x, y), (x, z), (y, z)\}$ on the set $A = \{x, y, z\}$.

The directed graph of R is as given below

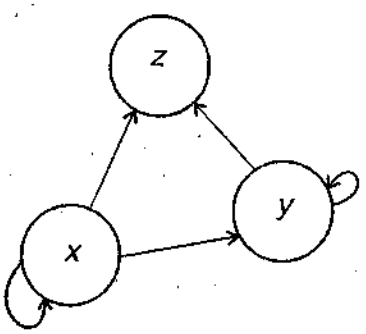


Fig. 3

Note that there is arrow from x to itself to represent $(x, x) \in R$.

Composition of relations :

Let R and S be relations from set A to B and set B to C respectively. *i.e.* $R \subseteq A \times B$ and $S \subseteq B \times C$. Then we can constitute a relation ROS or RS, from A to C, known as composite relation and defined by

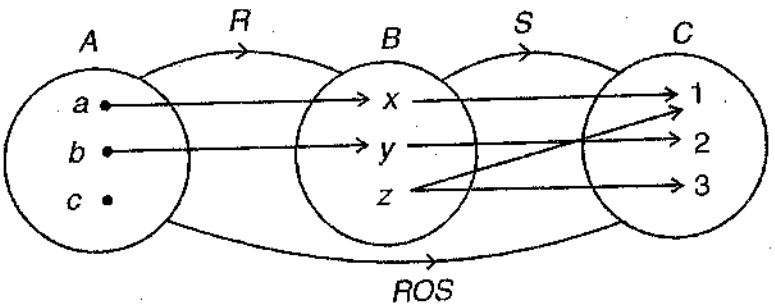
$ROS = \{(a, c) \mid \exists\, b \in B$, such that $(a, b) \in R, (b, c) \in S\}$

Ex. *Let $A = \{a, b, c\}$ $B = \{x, y, z\}$ $C = \{1, 2, 3\}$ be three sets. Let R and S are relations from A to B and B to C defined as*

$$R = \{(a, x), (b, y)\}, S = \{(x, 1), (y, 2), (z,1), (z, 3)\}$$

Then find composite relation ROS

Sol.



We set that $(a, x) \in R$ and $(x, 1) \in S$. Thus $(a, 1) \in ROS$. Similarly $(b, 2) \in ROS$. No other pairs belong to ROS. Thus

$$ROS = \{(a, 1), (b, 2)\}.$$

Note-1 : If M_R, M_S and M_{ROS} denote the matrix of relations R, S and ROS respectively, then

$$M_R \cdot M_S = M_{ROS}$$

This equality means that the matrices M_R M_S and M_{ROS} have the same zero entries implying that both M_R M_S and M_{ROS} denote the same composite relation ROS.

For an illustration, consider relations, given in the above examples

$$M_R = \begin{array}{c} \\ a \\ b \\ c \end{array}\!\!\begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{array} \qquad M_S = \begin{array}{c} \\ x \\ y \\ z \end{array}\!\!\begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \end{array}$$

$$M_{ROS} = \begin{array}{c} \\ a \\ b \\ c \end{array}\!\!\begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

Note that $M_R M_S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Thus $M_R M_S = M_{ROS}$.

Now, we state a theorem (without proof) that if R, S and T are relations from set A to B, set B to C and set C to D respectively, then

$RO(SOT) = (ROS) OT$.

This is known as associative law of composition of relations.

5.0 Types of relation

In this section, we will discuss various types of relations. Remember that the classifications to be presented here is defined for relations on a set.

Let R be a relation on a set A. Then we define :

5.3.1 Reflexive relation : R is reflexive if $(a, a) \in R \ \forall \ a \in A$. For example, consider relations R and S on the set $A = \{1, 2, 3\}$ given by

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

$S = \{(1, 1), (1, 2), (2, 1)\}$.

Here R is reflexive since every element of A is R-related to itself, but S is not reflexive since, for example $(2, 2) \notin S$.

Not reflexive : A relation $R \subseteq A \times A$ is not reflexive if there exists at least one element a in A such that $(a, a) \notin R$. For example, the relation R defined on the set $N = \{1, 2, 3, 4, ...\}$ such that "$(a, b) \in R$ if $a < b$ is not reflexive because $a \not< a \ \forall \ a \in N$.

Similarly, the relation $S = \{(a, a) (b, b)\}$ defined on the set $B = \{a, b, c\}$ is not reflexive. Since $(c, c) \notin S$.

5.3.2 Symmetric relation :

R is symmetric if $(a, b) \in R$ implies $(b, a) \in R$.

For example, let $A = \{1, 2, 3\}$. Let $R = \{(1, 1), (1, 2), (2, 1)\}$ and $S = \{(1, 1), (2, 2), (3, 2)\}$

Then R is symmetric since $(1, 2) \in R$ and $(2, 1) \in R$ but S is not symmetric since $(3, 2) \in S$ but $(2, 3) \notin S$.

Not symmetric : A relation R defined on the set A is not symmetric if $(a, b) \in R$ but $(b, a) \notin R$ for example, "Relation R of divisibility" on the set of natural numbers N is not symmetric since $2 \mid 4$ does not imply that $4 \mid 2$ *i.e.* $(2, 4) \in R$, but $(4, 2) \notin R$.

5.3.3 Transitive relation :

R is transitive if $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$

For an example, consider the relations

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

$S = \{(1, 1), (1, 2), (2, 3), (3, 3)\}$ on the set $A = \{1, 2, 3\}$. R is transitive but S is not transitive since

$$(1, 2) \in S, (2, 3) \in S \text{ but } (1, 3) \notin S.$$

Not transitive : A relation R defined on a set A is not transitive if there exist elements $a, b, c \in A$ such that $(a, b) \in R, (b, c) \in R$ but $(a, c) \notin R$ for example, let L be set of lines in a plane. Let R be a relation defined on the set L such that "$L_1 RL_2$ if lines $L_1, L_2 \in L$ are mutually perpendicular". Then this relation is not transitive since if

$L_1 RL_2, L_2 RL_3 \Rightarrow L_1$ is not perpendicular to L_3.

5.3.4 Antisymmetric relation :

R is antisymmetric if $(a, b) \in R$ and $(b, a) \in R$ implies $a = b$.

Note that antisymmetric relation is not "opposite" of symmetric relation. Infact, a relation can or can't simultaneously be symmetric and antisymmetric.

For example, let us consider following relations R, T and S on the set $A = \{1, 2, 3\}$

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

$S = \{(1, 1), (2, 2) (2. 3), (3, 2)\}$

Note that both R and S are not antisymmetric relations

Since $(1, 2) \in R, (2, 1) \in R$ but $1 \neq 2$

Similarly $(2, 3) \in S, (3, 2) \in S$ but $2 \neq 3$.

However, relation T is antisymmetric

Not antisymmetric : A relation R defined on the set A is not antisymmetric if $(a, b) \in R, (b, a) \in R$ but $a \neq b$.

For example, "Relation R of divisibility" on the set of integers Z is not antisymmetric since 3 divides -3 and -3 divides 3 but $3 \neq -3$.

Ex.1. *Let $Z^+ = \{1, 2, 3 \ldots.\}$ be the set of positive integers and a relation R on Z^+ is defined as follows*

$$R = \{(a, b) \mid a + 2b = 8\}$$

Is it reflexive ? Is it symmetric ?

Sol. We know that relation R on a set A is reflexive if $(a, a) \in R \ \forall \ a \in A$.

Following this, we find that here the given relation R is not reflexive since for example

$$1 + 2 \cdot 1 \neq 8$$

i.e. $(1, 1) \notin R$.

Also, R is not symmetric since $(6, 1) \in R$ [$\because 6 + 2 \cdot 1 = 8$]

but $(1, 6) \in R$ [because $1 + 2 \cdot 6 \neq 8$].

Ex.2. *Let* $R = \{(1, 1), (2, 2), (2, 3)\}$ *be a relation on the set* $A = \{1, 2, 3, 4, 5\}$. *Examine whether R is*

(a) reflexive (b) symmetric (c) antisymmetric (d) transitive.

Sol. R is not reflexive since $(a, a) \notin R \ \forall \ a \in A$. *e.g* $(3, 3) \notin R$, where $3 \in A$

R is not symmetric since $(2, 3) \in R$ but $(3, 2) \notin R$

R is antisymmetric

R is transitive.

Ex.3. *Let* $\leq$ *be a usual less than or equal to relation on the set of natural numbers N defined as*

$$R = \{(a, b) \mid a \leq b\}$$

Is R reflexive, symmetric, antisymmetric and transitive ?

Sol. R is reflexive since $a \leq a \ \forall \ a \in N$

R is not symmetric since $a \leq b$ does not imply $b \leq a$.

R is antisymmetric since $a \leq b$ and $b \leq a$ imply that $a = b$

R is transitive since $a \leq b, b \leq c$ imply $a \leq c$.

Ex.4. *Let P (A) denote the power set of a set A. Let* $\subseteq$ *denote the relation of inclusion (is subset of). Examine* $\subseteq$ *for various types of relations.*

Sol. Let $X, Y, Z \in P(A)$. Then obviously X, Y, Z are subsets of the set A.

Now, we know that every set is subset of itself *i.e.* $X \subseteq X \ \forall \ X \in P(A)$

$\Rightarrow \subseteq$ is reflexive

The relation $\subseteq$ is not symmetric since if $X \subseteq Y$.

Then it does not imply that $Y \subseteq X$.

However, $\subseteq$ is antisymmetric since

$$X \subseteq Y \text{ and } Y \subseteq X \Leftrightarrow X = Y.$$

The relation $\subseteq$ is transitive since

$$X \subseteq Y, \ Y \subseteq Z \ \Rightarrow X \subseteq Z.$$

Ex.5. *Show that the relation* $|$ *of division on the set integers is reflexive and transitive but it is not symmetric and anti symmetric.*

Sol. $Z = \{0, \pm 1, \pm 2 \ldots\}$ is the set of integers given that divisibility is the relation on Z. Let we denote this relation by R. Then

$R = \{(a, b) \mid a$ divides b *i.e.* $a \mid b\}$

R is reflexive since $a \mid a \ \forall \ a \in Z$.

R is transitive since $a \mid b$ and $b \mid c \Rightarrow a \mid c$

R is not symmetric since $a \mid b$ does not imply that $b \mid a$ *e.g.* 2 divides 4 but 4 does not divide 2

R is not antisymmetric since 4 divides -4 and -4 divides 4 but $4 \neq -4$.

Self-learning exercise-1

1. The relation R "$(a, b) \in R$ if $a \mid b$" defined on the set $A = \{1, 2\}$ is

(i) $\{(1, 1), (1, 2)\}$ *(ii)* $\{(1, 1), (2, 2), (1, 2)\}$

(iii) $\{(2, 1), (2, 2)\}$ *(iv)* None of these

2. The relation R "$(a, b) \in R$ if $a < b$" on the set N is

(i) Reflexive *(ii)* Not reflexive

(iii) Symmetric *(iv)* None of these

3. Which of the following is true ?

(i) A symmetric relation can never be antisymmetric.

(ii) An antisymmetric relation can never be symmetric.

(iii) If a relation is not symmetric then it is essentially an antisymmetric relation.

(iv) A relation can simultaneously be symmetric and antisymmetric.

4. Which of the following is true for the relation R "$(a, b) \in R$ if $a + b = 8$" on the set N

(i) R is reflexive *(ii)* R is antisymmetric

(iii) R is not symmetric *(iv)* R is not transitive

5.4 Equivalence relations and partitions

5.4.1 Equivalence relation :

A relation R on the set A is called equivalence relation if for $a, b, c \in A$,

(i) R is reflexive *i.e.* $(a, a) \in R$, $\forall\ a \in A$

(ii) R is symmetric *i.e.* $(a, b) \in R \Leftrightarrow (b, a) \in R$

(iii) R is transitive *i.e.* $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$.

Equivalence relation is an important concept in the theory of relation since it constitutes a partition of the set A in a unique manner that you would study in the coming pages.

Ex.1. *The relation $=$ of equality on the set Z of integers is an equivalence relation since for $a, b, c \in Z$ we have*

(i) $a = a$ *(Reflexivity)*

(ii) $a = b \Leftrightarrow b = a$ *(Symmetric)*

(iii) $a = b, b = c \Rightarrow a = c$ *(Transitivity)*

Ex.2. *The relation $\perp$ of perpendicularity on the set L of lines in the $X-Y$ plane is not an equivalence since $\perp$ is not reflexive simply because no line in the $X-Y$ plane is perpendicular to itself. Further, it is not transitive because if L_1, L_2, L_3 are three lines in the $X-Y$ plane such that*

$L_1 \perp L_2$ and $L_1 \perp L_2 \Rightarrow L_1$ is not perpendicular to L_3.

Thus we conclude that $\perp$ is not an equivalence relation although it is symmetric relation $[L_1 \perp L_2 \Leftrightarrow L_2 \perp L_1]$

Ex.3. *Let* $R = \{(x, x), (x, z), (z, x), (z, z)\}$ *be a relation on the set* $A = \{x, y, z\}$. *Determine whether R is an equivalence relation ?*

Sol. R is not reflexive because every element of A is not related to itself. Note that $(y, y) \notin R$. Hence R is not an equivalence relation although it is symmetric and transitive.

Ex.4. *Let* Z^+ *be the set of positive integers and R be a relation on* Z^+ *such that*

$R = \{(a, b) \mid a + b \text{ is even}\}$

Then determine whether R is an equivalence relation.

Sol. R is reflexive :

$\because$ $a + a$ is even $\forall\ a \in Z \Rightarrow (a, a) \in R$

$\Rightarrow$ R is reflexive

R is symmetric : Let $a + b$ is even, where $a, b \in Z^+$

$\Rightarrow$ $b + a$ is also even.

Thus we see that $(a, b) \in R \Leftrightarrow (b, a) \in R$

Hence R is symmetric

***R* is transitive :** Let $a, b, c \in Z^+$ such that $(a, b) \in R, (b, c) \in R$

$\Rightarrow$ $a + b$ is even and $b + c$ is even.

Now, $a + b$ is even if and only both a and b are even or odd. That is a and b have same parity. Following the reasoning, $b + c$ is even if and only if both b and c are even or odd thus $a + c$ will be even if and only if both a and c are even or odd *i.e.* a and c have the same parity. Thus we conclude that

$(a, b) \in R, (b, c) \in R\ (a, c) \in R$.

Hence R is transitive.

Ex.5. *Let R be a relation on the set Z of integers defined as*

$R = \{(a, b) \mid a, b \in Z, (a - b)$ *is divisible by* $4\}$

Then show that R is an equivalence relation.

Sol. 1. *R* is reflexive : Let $a \in Z$. Then $a - a = 0$ and 0 is divisible by 4. Then by definition of R we find that $(a, a) \in R\ \forall\ a \in Z$. Thus R is reflexive.

2. *R* is symmetric : Let $a, b \in Z$ such that $(a, b) \in R$

$\Rightarrow$ $(a - b)$ is divisible by 4.

$\Rightarrow$ $(b - a)$ is also divisible by 4.

$\Rightarrow$ $(b, a) \in R$

$\Rightarrow$ Thus $(a, b) \in R \Rightarrow (b, a) \in R$

Therefore, R is symmetric.

3. *R* is transitive : Let $(a, b) \in R, (b, c) \in R$

Thus, $(a - b)$ is divisible by 4 and $(b - c)$ is divisible by 4

$\Rightarrow$ $[(a-b)+(b-c)]$ is divisible by 4

$\Rightarrow$ $[a-c]$ is divisible by 4

$\Rightarrow$ $(a, c) \in R$

Thus, we find that $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$, R is transitive.

Accordingly, R is an equivalence relation.

Ex.6. *Let R be a relation on the set $A = \{1, 2, 3, 4, 5\}$ defined as*

$$R = \{(a, b) \mid |a - b| = 2\}$$

Determine whether R is an equivalence relation.

Sol. By the definition of R, we find

$$R = \{(1, 3), (2, 4), (3, 5), (3, 1), (4, 2), (5, 3)\}$$

1. Reflexivity : R is not reflexive since every element of A is not related to itself *e.g.* $(2, 2) \notin R$. Hence R is not an equivalence relation. You can see that R is symmetric but not transitive relation.

Ex.7. *Let $\simeq$ be a relation on $A \times A$ defined as follows*

$$(a, b) \simeq (c, d) \text{ whenever } ad = bc$$

where A is set of non zero integers. Determine whether $\simeq$ is an equivalence relation.

Sol. 1. $\simeq$ is reflexive : Let $a, b \in A$. Then $ab = ba$

[$\because$ Multiplication of integers is commutative]

$(a, b) \simeq (a, b)$ [by definition of $\simeq$]

$\Rightarrow$ every element $(a, b) \in A \times A$ is related to itself,

Therefore $\simeq$ is reflexive

2. $\simeq$ is symmetric : Let $(a, b), (c, d) \in A \times A$ such that

$(a, b) \simeq (c, d) \Rightarrow ad = bc$

$\Rightarrow da = cb$ [$\because$ multiplication of integers is commutative]

$\Rightarrow cb = da$

$\Rightarrow (c, d) \simeq (a, b)$

$\Rightarrow \simeq$ is symmetric

3. $\simeq$ is transitive : Let $(a, b), (c, d)$ and $(e, f) \in A \times A$ such that $(a, b) \simeq (c, d)$ and $(c, d) \simeq (e, f)$

$\Rightarrow$ $ad = bc$ and $cf = de$

$\Rightarrow$ $(ad)(cf) = (bc)(de)$

$\Rightarrow$ $af = be$

$\Rightarrow$ $(a, b) \simeq (e, f)$

Thus, we see that $(a, b) \simeq (c, d)$; $(c, d) \simeq (e, f) \Rightarrow (a, b) \simeq (e, f)$

Hence, $\simeq$ is transitive.

Therefore $\simeq$ is an equivalence relation

5.4.2 Partition of a set :

Let A be a non-empty set. A partition P of the set A is a collection of non-empty subsets $A_1, A_2 \ldots A_n$ of A such that every $a \in A$ belongs to one of the A_i and subsets A_i, $i = 1, 2 \ldots n$ are mutually disjoint. If $P = \{A_i\}$ is a partition of the set A, then the subsets A_i are called cells. To illustrate, we consider the set $A = \{1, 2, 3, 4, 5\}$

Let $P = \{\{1\}, \{1, 2, 3\}, \{4, 5\}\}$

$Q = \{\{1, 2\}, \{3, 4\}\}$

Here P is not a partition of the set A since $1 \in A$ belongs to two cells. Again Q is also not a partition of A since $5 \in A$ does not belong to any cell.

Ex.1 *Find all the partitions of the set* $A = \{a, b\}$.

Sol. The possible partitions of A are :

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

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

Ex.2 *Examine whether the following is partition of the set N of natural numbers.*

$$P = [\{n \mid n > 3\}, \{1, 2, 3, 4\}]$$

Sol. Given that

$$P = [\{4, 5, 6, 7 \ldots..\}, \{1, 2, 3, 4\}]$$
$$= [A_1, A_2]$$

where $A_1 = \{4, 5, 6, 7 \ldots.\}, A_2 = \{1, 2, 3, 4\}$.

P is not partition of N since A_1 and A_2 are not disjoint. [$\because$ 4 belongs to both A_1 & A_2]

Ex.3 *Let* $A = \{a, b\}$. Is $P = \{\phi, \{\{a\}, \{b\}\}, \{a, b\}\}$ a partition of A ?

Sol. No, since the empty set ϕ can not belong to a partition.

The concept of partition of a set is important in many practical applications. You will see that an equivalence relation partitions the set (on which it is defined). The cells of such partition are called equivalence classes.

5.4.3. Equivalence classes :

Let R be an equivalence relation on a set A. If $(a, b) \in R$, then a and b are called equivalent with respect to equivalence relation R.

An equivalence relation has a unique property in the sense that the set of all those elements of A that are equivalent to $a \in A$ constitute the equivalence class of a, denoted by $[a]$.

Thus, $[a] = \{x \in A \mid (a, x) \in R\}$

Thus for every element $a \in A$, we have an equivalence class. However it is to be noted that two equivalence classes are either identical or disjoint.

The set of all equivalence classes of elements of A under an equivalence relation R is called quotient set of A by R and is written as

$$\frac{A}{R} = \{[a] \mid a \in A\}.$$

The following theorem entails the important properties of equivalence classes.

Theorem. *Let R be an equivalence relation defined on the non-empty set A. Let $a, b \in A$. Then*

(i) $a \in [a]$

(ii) $b \in [a] \Rightarrow [b] = [a]$

(iii) $[a] = [b] \Leftrightarrow (a, b) \in R$

(iv) Either $[a] = [b]$ or $[a] \cap [b] = \phi$

Ex.1. *Let R_3 be an equivalence relation on the set Z of integers such that "$(a, b) \in R_3$ if $3 \mid (a - b)$". Then find the partitions induced by R_3 in Z.*

Sol. We know that

$$[x] = \{a \mid (a, x) \in R_3\}$$

Here $(a, x) \in R_3$ if $(a - x)$ is divisible by 3 *i.e.* $(a - x)$ is multiple of 3.

An equivalence class $A_r = [r]$, is obtained by adding r with multiples of 3.

Consequently,

$$A_0 = [0] = \{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}$$
$$A_1 = [1] = \{\ldots -8, -5, -2, 1, 4, 7, 10 \ldots\}$$
$$A_2 = [2] = \{\ldots -7, -4, -1, 2, 5, 8, 11 \ldots\}$$
$$A_3 = [3] = \{\ldots -6, -3, 0, 3, 6, 9 \ldots\}$$
$$A_4 = [4] = \{\ldots -5, -2, 1, 4, 7, 10 \ldots\}$$
$$A_5 = [5] = \{\ldots -4, -1, 2, 5, 8, 11 \ldots\} \text{ etc.}$$

We find that

$$A_0 = A_3 = A_6 = \ldots$$
$$A_1 = A_4 = A_7 = \ldots$$
$$A_2 = A_5 = A_8 = \ldots$$

Therefore $\frac{Z}{R_3}$ has there disjoint equivalence classes [0], [1] and [2]. That is

$$\frac{Z}{R_3} = \{[0], [1], [2]\}.$$

Ex.2. *Let* $R = \{(1, 1), (2, 2), (2, 3), (3, 2), (3, 3), (4, 4)\}$ be an equivalence relation on the set $A = \{1, 2, 3, 4\}$. Find $\frac{A}{R}$.

Sol. We know that

$$\frac{A}{R} = \{[a] \mid a \in A\}.$$

We have to find partitions induced by R in A *i.e.* We have to find equivalence classes $[a]$, $a \in A$. Recall that $[a] = \{x \in A \mid (a, x) \in R\}$.

Here 1 is R related to 1 only. This mean that $[1] = \{1\}$.

Now we choose which is not related to 1. We take 2, Now 2 is R related to 2 and 3.

Thus $[2] = \{2, 3\}$.

Now, further we take that element which is not related to 1 and 2. This element is 4 and 4 is R-related to itself only.

Thus $[4] = \{4\}$.

Hence partition of A induced by R is the set $\{\{1\}, \{2, 3\}, \{4\}\}$ and consequently $\frac{A}{R} = \{[1], [2], [4]\}$.

Ex.3. *Let* $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ *and an equivalence relation* $\sim$ "$(a, b) \sim (c, d)$ *if* $a + d = b + c$" *is defined on the set* $A \times A$. *Find an equivalence class of* $(2, 5)$.

Sol. We have to find ordered pairs $(x, y) \in A \times A$

Such that $(x, y) \sim (2, 5)$

i.e. $x + 5 = 2 + y$

or $y = 3 + x$

Now, on putting $x = 1, 2, 3 \ldots$ in the relation $y = 3 + x$, we obtain corresponding values as

$$x = 1, y = 3 + 1 = 4$$

$$x = 2, y = 3 + 2 = 5$$

$$x = 3, y = 3 + 3 = 6 \text{ etc.}$$

Thus $[(2, 5)] = \{(1, 4), (3, 6), (4, 7), (5, 8), (6, 9), (7, 10)\}$.

Self-learning exercise-2

1. Let the relation $R = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$ be defined on the set $A = \{1, 2\}$. Find $\frac{A}{R}$.
2. Let $A = \{1, 2, 3 \ldots. 15\}$ and an equivalence relation $\cong$ is defined on $A \times A$ such that $(a, b) \cong (c, d)$ if $ad = bc$, then find the equivalence class of $(3, 2)$.

5.5 Summary

This unit aimed to make you understand relations, their types and representation. You have seen that how an equivalence relation partitions the set on which it is defined. These partitions are called equivalence classes. Similarly, partial ordering relation is worth mentioning because it gives an idea of poset which in turn serves as a basis of theory of lattices. This will be dealt in the next unit. To make the learning process a happy journey you are advised to imbibe the concepts.

5.6 Answers to self-learning exercises

Self-learning exercise–1

1. *(ii)* **2.** *(ii)* **3.** *(iv)* **4.** *(iv)*

Self-learning exercise–2

1. $\frac{A}{R} = \{[1]\}$ **2.** $[(3, 2)] = \{(3, 2), (6, 4), (9, 6), (12, 8), (15, 10)\}$

5.7 Exercises

1. Let $A = \{0, 1, 2, 3, 4\}$, $B = \{0, 1, 2, 3\}$. A relation $R \subseteq A \times B$ is defined such that $(a, b) \in R$ if $a + b = 3$.

Then find the relation R. [**Ans.** $R = \{(0, 3), (1, 2), (2, 1), (3, 0)\}$]

2. A relation R is defined on the set of integers Z such that $(a, b) \in R$ if

(i) $a \leq b + 1$

(ii) $a \neq b$

(iii) a is multiple of b.

Then identify the type of relation R is

[**Ans.** *(i)* Reflexive, *(ii)* Symmetric, *(iii)* Reflexive, transitive]

3. Write the relations R and S defined on the set $A = \{1, 2, 3\}$ in matrix form.

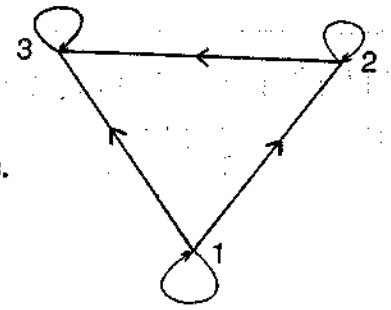
$R = \{(1, 1), (1, 2)\}$

$S = \{(1, 2), (2, 1), (1, 3)\}$

[**Ans.** $M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$, $M_S = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$]

4. Find the directed graph of the relation R "$(a, b) \in R$ if $a \leq b$" defined on the set $A = \{1, 2, 3\}$.

Ans.



5. Let a relation $R = \{(a, b) \mid a + 3b = 13\}$ is defined on the set of natural numbers. Then find R and R^{-1}.

[Ans. $R = \{(10, 1), (7, 2), (4, 3), (1, 4)\}$, $R^{-1} = \{(1, 10), (2, 7), (3, 4), (4, 1)\}$]

6. Examine whether the following are partitions of set of natural number N

(i) $\{n \mid n > 5\}, \{0\}, \{1, 2, 3, 4, 5\}$

(ii) $\{n \mid n > 6\}, \{n \mid n < 7\}$

(iii) $\{n \mid n^2 > 13\}, \{n \mid n^2 < 13\}$

[Ans. *(i)* No, since $0 \notin N$, *(ii)* No, *(iii)* Yes]

7. An equivalence relation $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$ is defined on the set $A = \{1, 2, 3\}$. Find $\frac{A}{R}$.

[Ans. $\{[1], [3]\}$]

8. Let N be set of natural members. Prove that the relation $\cong$ defined on N such that $(a, b) \cong (c, d)$ if $ad = bc$ is an equivalence relation.

9. Let a relation $\sim$ is defined on $Z \times Z$ such that "$(a, b) \sim (c, d)$ if $a + b = b + c$". Prove that $\sim$ is an equivalence relation.

□□□

UNIT 6 : Poset, Lattices and Functions

Structure of the Unit

6.0 Objectives

After reading this unit you will be able to :

- discuss poset and related concepts
- identify chains, antichain and lattices
- know types of lattices and their properties
- understand functions and their classification

6.1 Introduction

The study of posets is important because it is basis of a lattice. Note that every lattice is a poset and theory of lattices is founding stone of Boolean algebra whose importance is seriously felt in the digital age of computers. Similarly, theory of functions constitute a basis of many branches of Mathematics.

6.2 Poset

In the last unit you have studied about partial ordering relation on a set A. A non empty set A equipped with a partial ordering relation R is called a poset and is denoted as (A, R). To distinguish a partial ordering relation we use a symbol $\leq$. It is to be noted that the symbol $\leq$ would stand for a partial ordering relation and is not usual "less than or equal to" relation until and unless specified otherwise. Consequently in the forthcoming text $(A, \leq)$ stands for a poset.

Poset : A non empty set A equipped with a relation $\leq$ is a poset if for $a, b, c \in A$, the following hold good.

A_1 **reflexivity :** $a \leq a \quad \forall\, a \in A$

A_2 **Anti-symmetry :** $a \leq b, b \leq a \Leftrightarrow a = b$

A_3 **Transitivity :** $a \leq b, b \leq c \Rightarrow a \leq c$

Note 1 : If $\leq$ is a partial ordering relation on set A then $\leq$ is said to define partial ordering on A.

Note 2 : If two elements a and b of a poset $(A, \leq)$ are as $a \leq b$, then we say that a preceeds b.

Note 3 : The elements a and b of poset $(A, \leq)$ are said to be comparable if $a \leq b$ or $b \leq a$.

Ex.1. *The set N of natural numbers is a poset for the relation " \| " of divisibility i.e.*

$a \leq b$ *if* $a \mid b$; $\qquad a, b \in N$

Sol. $a \leq a \quad \forall\, a \in N$ since $a \mid a \quad \forall\, a \in N$ thus the given relation is reflexive

Let $\qquad a \mid b$ and $b \mid a \Leftrightarrow a = b$

i.e. $\qquad a \leq b$ and $b \leq a \Leftrightarrow a = b$

Thus the relation is antisymmetric

Again, let $\qquad a \mid b$ and $b \mid c \Rightarrow a \mid c$

Thus $\qquad a \leq b, b \leq c \Rightarrow a \leq c$

Hence the relation is transitive also

Thus $(N, \mid)$ is a poset.

6.2.1 Hasse diagram :

A finite poset is represented by a Hasse diagram. In Hasse diagram, elements of a poset are denoted by points and if a is related to b then b is placed a little higher than a and these are joined by a line segment. In Hasse diagram reflexivity and transitivity are not shown.

As an illustration let $a \leq b$, then its representation in Hasse diagram will be as shown in the following figure

Fig. 1

Note that a Hasse diagram does not have any horizontal line.

Ex.1. *Draw Hasse diagram of the poset* $(A, |)$

where $A = \{1,2, 3, 4\}$; $a\, R\, b$ *if* $a \mid b$.

Sol. The partial ordering relation R is given by

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

Then ordinary representation (arrow diagram) of the relation R will be as follows

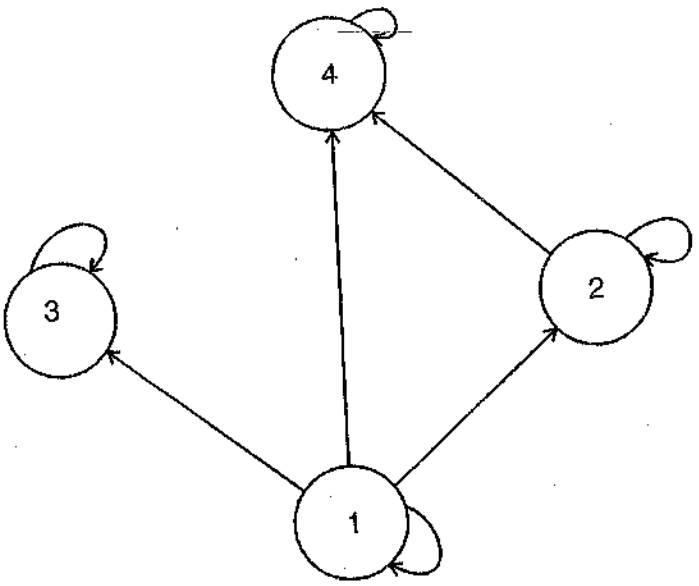


Fig. 2

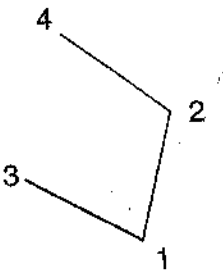


Fig. 3

The Hasse diagram would look like Fig. 3 after excluding arrow heads showing reflexivity and transitively.

Ex.2. *Find the relation R defined on the set*

where $A = \{1,2, 3, 4\}$; *which is exhibited in the following Hasse diagrams* :

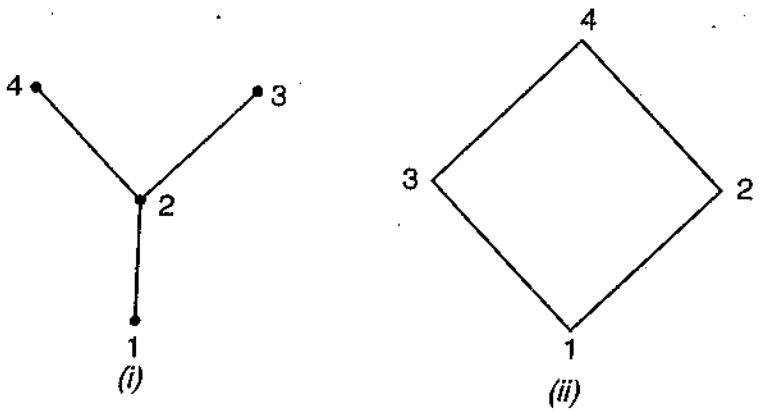


Fig. 4

Sol. We know that a Hasse diagram depicts partial ordering relation, therefore the given relation R is reflexive, antisymmetric and transitive. Thus we obtain

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

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

Ex.3. *$P(A)$ denote the power set of the set $A = \{a, b, c\}$. Draw the Hasse diagram of $(P(A), \subseteq)$, where $\subseteq$ is relation of set inclusion.*

Sol. Given that $A = \{a, b, c\}$ then

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

The Hasse diagram of $(P(A), \subseteq)$ is as follows

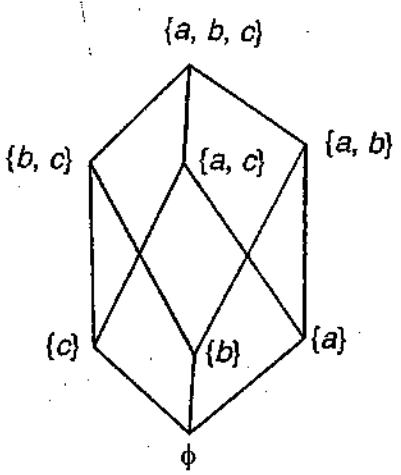


Fig. 5

6.2.2 Dual of a poset :

Let $(A, \leq)$ be a poset. A relation $\geq$ is called converse of relation $\leq$ if

$$a \leq b \Rightarrow b \geq a; \quad a, b \in A.$$

$(A, \geq)$ is called dual of $(A, \leq)$. The forthcoming theorem says that the dual of a post is also a poset.

Theorem. *The dual of a poset is again a poset.*

Proof : Let $(A, \leq)$ be a poset. Then to show that the dual $(A, \geq)$ of $(A, \leq)$ is also a poset, where $\geq$ is converse relation of $\leq$.

(i) **$\geq$ is reflexive :**

Since $a \leq a \quad \forall a \in A$ $[\because (A, \leq)$ is poset$]$

Therefore $a \geq a \quad \forall a \in A$

(ii) **$\geq$ is antisymmetric :**

$a \leq b,\ b \leq a \Leftrightarrow a = b$ $[\because (A, \leq)$ is poset$]$

$\Rightarrow$ $b \geq a,\ a \geq b \Leftrightarrow a = b$

$\Rightarrow$ $\geq$ is antisymmetric

(iii) **$\geq$ is transitive :** Since $(A, \leq)$ is a poset therefore for $a, b, c \in A$, we have

$a \leq b,\ b \leq c \Rightarrow a \leq c$

$\therefore$ $c \geq b,\ b \geq a \Rightarrow c \geq a$

Then $\geq$ is transitive

Thus $(A, \geq)$ is a poset.

6.2.3 Special elements in poset

Maximal and minimal elements :

An element a in a poset $(A, \leq)$ is called maximal element if no element succeeds it. That is, a is maximal element of the poset if there is **no other** element b such that $a \leq b$. Alternatively, we can say that a is maximal element of the poset if it does not preceed any other element of the poset. Note that a poset may have many maximal elements.

Similarly, an element x in a poset $(A, \leq)$ is called minimal element if it does not succeed any other element of the poset $(A, \leq)$.

For illustration, consider the following figure

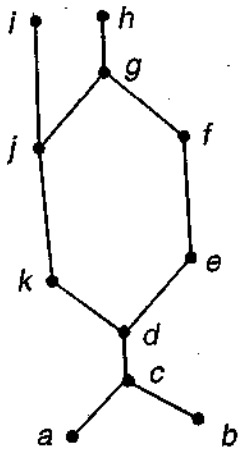


Fig. 6

In thus figure, i and h are the maximal elements since they don't preceed to any other element of the poset. Further, a and b are the minimal elements since no element of the poset preceeds them.

Greatest and least elements in poset : Let $(A, \leq)$ be a poset. An element x is called the greatest element of A if

$$a \leq x \quad \forall a \in A$$

The above definition implies that the greatest element (if it exists) is comparable with all the elements of the poset. It is to be noted that the greatest element (if it exists) is unique.

Similarly we define the least element of poset. An element y of the poset A is called the least element if

$$y \leq z \quad \forall z \in A.$$

Like greatest element, the least element is unique if it exists.

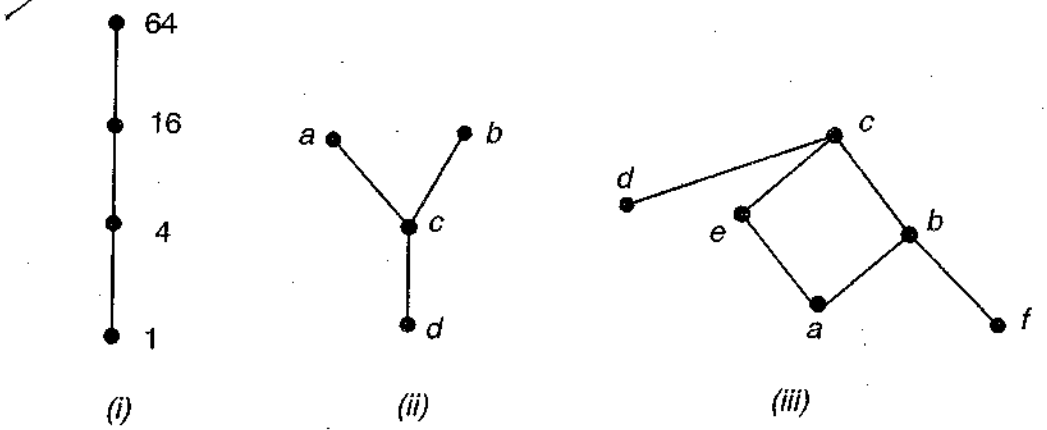
After going through the above mentioned special elements in a poset, a pertinent question arises. Is there anything to connect these elements. The following points are worth to reckon with.

(i) Maximal element of a poset need not necessarily be greatest element.

(ii) Minimal element of a poset need not necessarily be least element.

(iii) A poset may not have a maximal element at all.

Ex.1 *Find the special elements in the following posets :*



(i) *(ii)* *(iii)*

Fig. 7

Sol. ***(i)*** The greatest element is 64 and is the only maximal element. The least element is 1 and is the only minimal element.

(ii) The least element is d and is the only minimal element. There is no greatest element. a and b are maximal elements.

(iii) The greatest element is c. c and d are maximal elements. There is no least element and a and f are the only minimal elements.

6.2.4 Bounds :

Let $(A, \leq)$ be a poset. Then an element c is called an **upper bound of** $a, b \in A$ if

$$a \leq c \quad \text{and} \quad b \leq c.$$

Here it is to be noted that any pair of elements in poset may have more than one upper bound. Therefore we prescribe the notion of least upper bound or supremum. An element c is called least upper bound (*l.u.b.*) or supermum (sup) of a and b if

(i) c is upper bound of a and b.

(ii) if d is another upper bound of a and b then $c \leq d$.

similarly an element c is called lower bound of elements $a, b \in A$ if

$$c \leq a \text{ and } c \leq b$$

c will be greatest lower bound (Infimum) of a and b if there does not exist another lower bound d of a and b such that $d \leq c$.

Note 1 : A pair of elements in a poset may or may not have lower bound or upper bound.

Note 2 : The supremum and infimum of any pair of elements of a poset are unique, if they exist.

Note 3 : Supremum of a and b is denoted as $a \vee b$ and is read as a join b. Infimum of a and b is denoted as $a \wedge b$ and is read as a meet b.

Thus $\quad \text{sup. } \{a, b\} = a \vee b$

$\quad \text{Inf. } \{a, b\} = a \wedge b$

***Ex.*1.** *Find upper and lower bounds of pair of elements in the given poset*

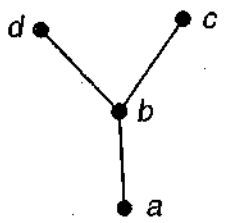


Fig. 8

Sol. Pair $\{a, b,\}$.

Since $\quad a \leq a$ and $a \leq b \Rightarrow a$ is lower bound of $\{a, b\}$

Again $\quad a \leq b,\ b \leq b \Rightarrow b$ is an upper bound of $\{a, b\}$

Again we see that $\quad [\because a \leq b \text{ and } b \leq c \Rightarrow a \leq c]$

$\quad a \leq c$

and $\quad b \leq c$

Thus c is also upper bound of $\{a, b\}$. Similarly d is also upper bound of $\{a, b\}$. Thus we have b, c and d as upper bounds of $\{a, b\}$. b is least upper bound of $\{a, b\}$ since b is comparable to other upper bounds c and d. *i.e.* $b \leq c$ and $b \leq d$.

6.2.5 Chains and Antichains :

Let $(A, \leq)$ be a poset. A subset B of A is said to form a chain iff every pair of elements of B is comparable. In case A itself is a chain then for any $a, b \in A$ we have $a \leq b$. If the chain A has n elements then the length of the chain is equal to $n-1$.

An antichain is the subset of a poset if any two elements of this subset are not comparable.

A chain is called the maximal chain if it is not part (subset) of a larger chain.

Ex.1. *Find the chains in the following lattice :*

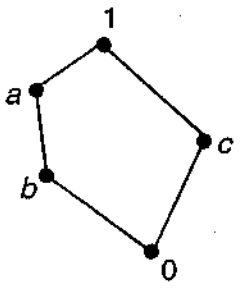


Fig. 9

Sol. We have $B_1 = \{0, 1\}$, $B_2 = \{0, a, 1\}$, $B_3 = \{0, b, 1\}$, $B_4 = \{0, c, 1\}$, $B_5 = \{0, a, b, 1\}$, as the five chains in the given lattice, since

$0 < 1;\ 0 < a < 1;\ 0 < b < 1;\ 0 < c < 1;\ 0 < b < a < 1$

Note that the chains B_4 and B_5 are maximal chains since these are not part of another larger chains.

Ex.2. *Find the chains in the following lattice*

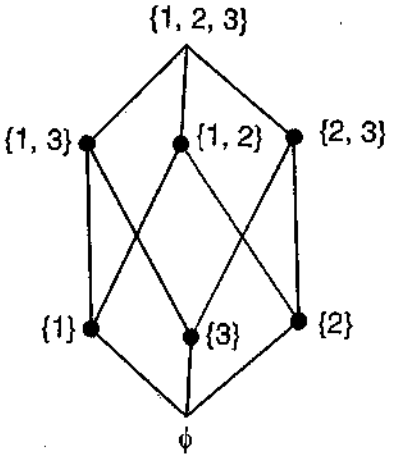


Fig. 10

Sol. There are numerous chains in this lattice for example, {ϕ, {1}, {ϕ, {2}}, {ϕ, {3}}, {ϕ, {1}, {1, 3}}, {ϕ, {1}, {1, 2}} and many more. You are advised to look into these.

We see that {ϕ , {2}, {2, 3}, {1, 2, 3}} is one of the maximal chain in this lattice. You can find other five maximal chains.

Ex.3. *Verify whether the following poset has an antichain :*

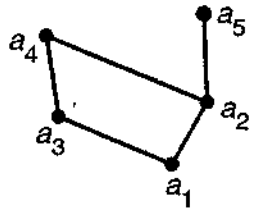


Fig. 11

Sol. We see that a_2, a_3; a_3, a_5, and a_4, a_5 are not comparable in this poset. Hence $\{a_2, a_3\}$ $\{a_3, a_5\}$ and $\{a_4, a_5\}$ constitute antichain.

6.3 Lattices

A lattice is a special kind of a poset. The notion of a lattice is associated with the bounds in a poset. Hence, we define.

Lattice : A poset $(A, \leq)$ is called a lattice if for any pair of elements a and b in A, $a \vee b \in A$, and $a \wedge b \in A$. *i.e.* sup $\{a, b\} \in A$, and Inf $\{a, b\} \in A$.

Note that every lattice is a poset but converse need not necessarily be true.

Ex.1 *The following poset is a lattice*

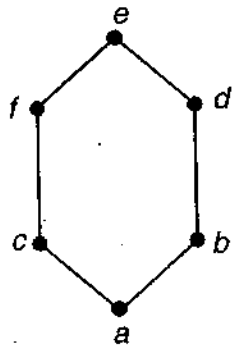


Fig. 12

Sol. To ensure whether a poset is a lattice examine that supremum and infimum of every pair of elements belong to the poset. We have examined for some of the supremums and infimums.

Supremums : Sup $\{a, c\} = c$

Sup $\{a, f\} = f$

Sup $\{b, f\} = e$ etc.

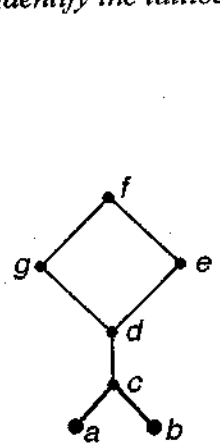
Infimums : Inf $\{a, c\} = a$

Inf $\{b, c\} = a$

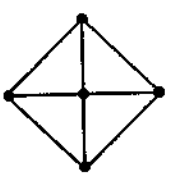
Inf $\{b, d\} = b$ etc.

You will see that supremum and infimum of every pair of elements of the given poset are in the poset. Hence, it is a lattice

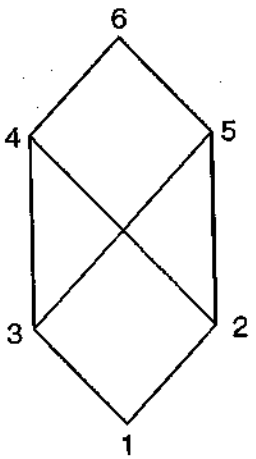
Ex.2. *Identify the lattices among the posets given below :*



(i)



(ii)



(iii)

Fig. 13

Sol. *(i)* The poset *(i)* is not a lattice because Inf $\{a, b\}$ does not exist.

(ii) The poset *(ii)* is a lattice.

(iii) The poset *(iii)* is not a lattice because 4, 5, 6 are upper bounds of $\{2, 3\}$ but 4 and 5 are incomparable. Consequently Sup $\{2, 3\}$ does not exist.

Self-learning exercise-1

1. Poset $(A, \leq)$ is a lattice if :

(i) $a \vee b \in A,\ a \wedge b \notin A$

(ii) $a \wedge b \in A,\ b \wedge a \in A$

(iii) $a \vee b \in A,\ a \wedge b \in A$

(iv) $a \vee b \notin A,\ a \wedge b \notin A$

2. Which if the following is not true :

(i) Every poset is a lattice

(ii) Poset has symmetric relation

(iiii) Hasse diagram depicts transitivity

(iv) All of the above are not true.

3. Which of the following is true :

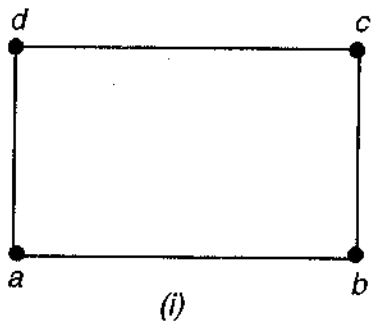
(i) Every poset has a greatest element necessarily

(ii) Every poset has a least element necessarily

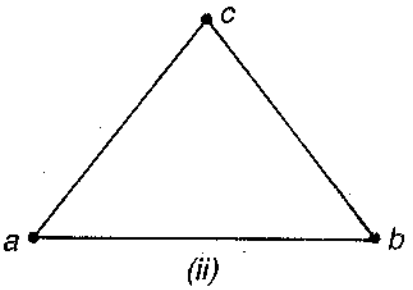
(iiii) A poset may have more than one maximal element

(iv) A poset may have no element

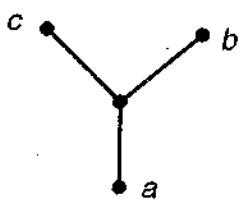
4. Which of the following is not a lattice ?



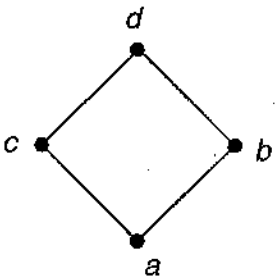
(i)



(ii)



(iii)



(iv)

Fig. 14

5. Find the universal upper bound and universal lower bound of the lattices given below :

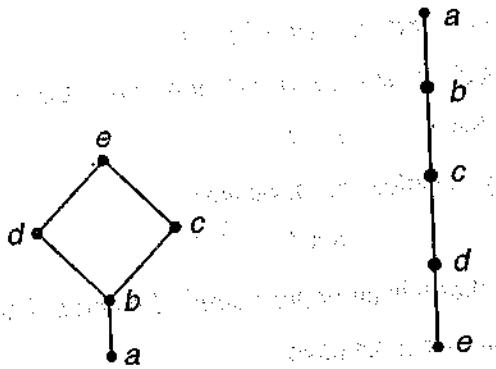


Fig. 15

6. Verify whether the posets given below are lattices :

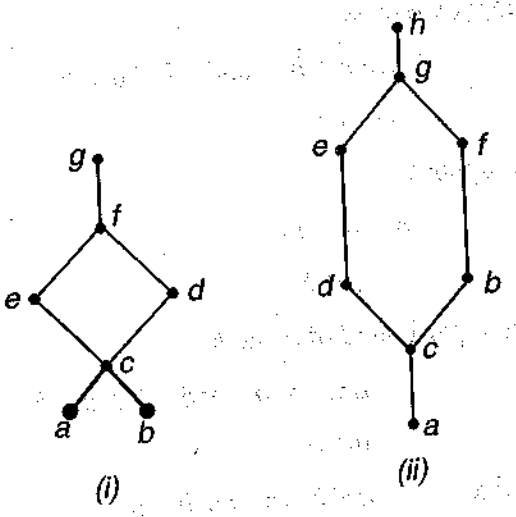


Fig. 16

7. Find maximal and minimal elements of the posets given in question no. 5 and 6.

8. Find upper and lower bounds of $\{a, b\}$ in the following poset :

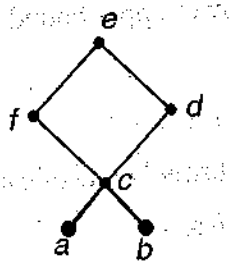


Fig. 17

6.3.1 Properties of lattices :

Theorem 1. *Let a, b, c and d be arbitrary elements of lattice* $(A, \leq)$. *Then*

(i) $a \leq b \Leftrightarrow a \vee b = b$.

(ii) $a \leq b \Leftrightarrow a \wedge b = a$.

(iii) $a \vee (b \vee c) = (a \vee b) \vee c$ *and* $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

(iv) $a \vee (a \wedge b) = a$ *and* $a \wedge (a \vee b) = a$.

(v) $a \leq b$ *and* $c \leq d \Rightarrow a \vee c \leq b \vee d$ *and* $a \wedge c \leq b \wedge d$.

Proof : *(i)* Given that $a \leq b$ .....(1)

Then by reflexivity in lattice $(A, \leq)$, we have

$$b \leq b \qquad \text{.....(2)}$$

(1) and (2) imply that b is an upper bound of a and b. But we know that $a \vee b$ is least upper bound of a and b. Therefore, we must have,

$$a \vee b \leq a \quad \text{and} \quad a \vee b \leq b \qquad \text{.....(3)}$$

Again, since $a \vee b$ is least upper bound of a and b

Therefore, $b \leq a \vee b, \quad a \leq a \vee b$ .....(4)

Thus from (3) and (4) we have

$$a \vee b \leq b \quad \text{and} \quad b \leq a \vee b$$

which yield $a \vee b = b$ [on using antisymmetry]

conversely, let us suppose

$$a \vee b = b$$

To show that $a \leq b$

Now $a \vee b$ is least upper bound of a and b

$\Rightarrow$ $a \leq a \vee b$ and $b \leq a \vee b$

$\Rightarrow$ $a \leq b$ $[\because a \vee b = b]$

Thus we conclude that $a \leq b \Leftrightarrow a \vee b = b$

(ii) Given that $a \leq b$ .....(1)

Then by reflexivity in lattice $(A, \leq)$, we have

$$a \leq a \qquad \text{.....(2)}$$

(1) and (2) imply that a is lower upper bound of a and b. But we know that $a \wedge b$ is greatest lower bound of a and b. Therefore,

$$a \leq a \wedge b \qquad \text{.....(3)}$$

Again, since $a \wedge b$ is greatest lower bound of a and b.

Therefore, $a \wedge b \leq a$ .....(4)

From (3) and (4), on using antisymmetry, we obtain

$$a \wedge b = a$$

conversely, by supposing $a \wedge b = a$, you can can prove $a \leq b$ to yield

$$a \leq b \Leftrightarrow a \wedge b = a$$

(iii) In order to show that

$$a \vee (b \vee c) = (a \vee b) \vee c$$

We shall show that

$$a \vee (b \vee c) \leq (a \vee b) \vee c \quad \text{and} \quad (a \vee b) \vee c \leq a \vee (b \vee c)$$

where result follows on using antisymmetry.

Let us consider $a \vee (b \vee c)$

$a \vee (b \vee c)$ is least upper bound of a and $(b \vee c)$

$$\Rightarrow \quad a \leq a \vee (b \vee c) \quad \text{and} \quad b \vee c \leq a \vee (b \vee c) \qquad \text{.....(1)}$$

Again $b \vee c$ is least upper bound of b and c

$$\Rightarrow \quad b \leq b \vee c \quad \text{and} \quad c \leq b \vee c \qquad \text{.....(2)}$$

From (1) and (2), we have.

$$b \leq b \vee c \leq a \vee (b \vee c) \Rightarrow b \leq a \vee (b \vee c) \qquad \text{.....(3)}$$

and $$c \leq b \vee c \leq a \vee (b \vee c) \Rightarrow c \leq a \vee (b \vee c) \qquad \text{.....(4)}$$

From (1) and (3) we see that $a \vee (b \vee c)$ is upper bound of a and b. But $a \vee b$ is least upper bound of a and b. Therefore,

$$a \vee b \leq a \vee (b \vee c) \qquad \text{.....(5)}$$

From (4) and (5) we see that $a \vee (b \vee c)$ is upper bound of $(a \vee b)$ and c. But $(a \vee b) \vee c$ is least upper bound of $a \vee b$ and c. Therefore,

$$(a \vee b) \vee c \leq a \vee (b \vee c) \qquad \text{.....(6)}$$

we will now show that

$$a \vee (b \vee c) \leq (a \vee b) \vee c \qquad \text{.....(7)}$$

Again, let us consider $(a \vee b) \vee c$. Then as above

we have, $$a \vee b \leq (a \vee b) \vee c \quad \text{and} \quad c \leq (a \vee b) \vee c \qquad \text{.....(8)}$$

Again $$a \leq a \vee b, \; b \leq a \vee b \qquad \text{.....(9)}$$

Thus $$a \leq a \vee b \leq (a \vee b) \vee c \Rightarrow a \leq (a \vee b) \vee c \qquad \text{.....(10)}$$

$$b \leq a \vee b \leq (a \vee b) \vee c \Rightarrow b \leq (a \vee b) \vee c \qquad \text{.....(11)}$$

From (8), (11) we find that

$$b \vee c \leq (a \vee b) \vee c \qquad \text{.....(12)}$$

From (10) and (12) we find that

$$a \vee (b \vee c) \leq (a \vee b) \vee c \qquad \text{.....(13)}$$

From (7), (13) we find on using antisymmetry

$$a \vee (b \vee c) = (a \vee b) \vee c$$

Similarly, we can show that

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

(iv) In order to prove that $a \vee (a \wedge b) = a$

We shall show that $a \vee (a \wedge b) \leq a$ and $a \leq a \vee (a \wedge b)$

whence result follows on using antisymmetry.

Now, we consider $a \vee (a \wedge b)$

$a \vee (a \wedge b)$ is least upper bound of a and $a \wedge b$

$\Rightarrow$ $a \leq a \vee (a \wedge b)$ .....(1)

and $a \wedge b \leq a \vee (a \wedge b)$ .....(2)

Again, $a \wedge b$ is greatest lower bound of a and b

$\Rightarrow$ $a \leq a \wedge b$ .....(3)

and $b \leq a \wedge b$ .....(4)

From (2) and (3),

$$a \leq a \wedge b \leq a \vee (a \wedge b)$$

$\Rightarrow$ $a \leq a \vee (a \wedge b)$ [using transitivity] .....(5)

Now we will show that

$$a \vee (a \wedge b) \leq a.$$

Now, $a \leq a$ (reflexivity)

and $a \wedge b \leq a$ [$\because$ $a \wedge b$ is g.l.b. of a and b]

$\Rightarrow$ a is upper bound of a and $a \wedge b$. But $a \vee (a \wedge b)$ is least upper bound of a and $a \wedge b$. There fore,

$$a \vee (a \wedge b) \leq a \quad \text{.....(6)}$$

From (5), (6) on using antisymmetry, we get

$$a \vee (a \wedge b) = a$$

Similarly, we can show that

$$a \wedge (a \wedge b) = a.$$

(v) Given that

$$a \leq b \quad \text{and} \quad c \leq d \quad \text{.....(1)}$$

Now, $b \leq b \vee d$ and $d \leq b \vee d$ .....(2)

[$\because$ $b \vee d$ is least upper bound of b and d]

From (1) and (2), we have

$$a \leq b \leq b \vee d \Rightarrow a \leq b \vee d \quad \text{.....(3)}$$

$$c \leq d \leq b \vee d \Rightarrow c \leq b \vee d \quad \text{.....(4)}$$

[on using transitivity]

(3) and (4) imply that $b \vee d$ is upper bound of a and c, but we know that $a \vee e$ is least upper bound of a and c. Therefore

$$a \vee c \leq b \vee d, \text{ hence the result}$$

Similarly, we can show that

$$a \wedge c \leq b \wedge d.$$

Theorem.2 *The dual of a lattice is again a lattice.*

Proof : Let $(A, \leq)$ be a lattice. Then obviously $(A, \leq)$ is also a poset since $\leq$ is partial ordering relation on the set A. We know that dual of a poset is also a poset. Let $(A, \geq)$ be dual of the poset $(A, \leq)$ where $\geq$ is converse relation on the set A and it is defined as

"A relation $\geq$ is called converse of relation $\leq$ if $a \leq b \Leftrightarrow b \geq a$" [That means b is comparable to a under relation $\geq$ when a is comparable to b under the relation $\leq$].

In order to prove the theorem we have to show that any pair of elements of A admit supremum and infimum with respect to $\geq$ in A.

Let $a, b \in A$. Then $a \vee b$ and $a \wedge b$ are supremum and infimum of a and b with respect to the relation $\leq$.

Thus $\quad a \leq a \vee b \quad$ and $\quad b \leq a \vee b$

$\Rightarrow \quad a \vee b \geq a \quad$ and $\quad a \vee b \geq b$

$\Rightarrow$ $a \vee b$ is lower bound of a and b with respect to the relation $\geq$. Now we will show that $a \vee b$ is greatest lower bound of a and b for the relation $\geq$. Let if possible, let c be another lower bound of a and b for the relation $\geq$. Then

$$\left.\begin{aligned} c \geq a \Rightarrow a \leq c \\ \text{and} \quad c \geq b \Rightarrow b \leq c \end{aligned}\right\} \quad \text{[by definition of } \geq \text{]}$$

$\Rightarrow$ c is bound of a and b for the relation $\leq$. But $a \vee b$ is least upper bound of a and b for the relation $\leq$. Hence

$$a \vee b \leq c \Rightarrow c \geq a \vee b$$

Thus we have shown that $a \vee b$ is greatest lower bound of $\{a, b\}$ for the relation $\geq$.

Similarly we can show that $a \wedge b$ is least upper bound of a and b for the relation $\geq$.

Since $a \vee b, a \wedge b \in A$. Thus $(A, \geq)$ is lattice.

Universal bounds in a lattice

Universal upper bound : An element u is called universal upper bound of a lattice $(A, \leq)$

$$a \leq u \qquad \forall\, a \in A$$

That is, u is universal upper bound of lattice $(A, \leq)$ if every element of A is comparable to u.

Universal lower bound : An element s is called universal lower bound of a lattice $(A, \leq)$ if

$$s \leq x \qquad \forall\, x \in A.$$

A lattice is called **bounded lattice** if

$$s \leq x \leq u \qquad \forall\, x \in A$$

where s and u are universal lower and upper bounds respectively.

Note 1 : Universal lower and universal upper bounds s and u are denoted by 0 and 1. Here it should be noted that these are merely symbols and are not ordinary numerals zero and one.

Note 2 : If a lattice possesses universal lower and upper bounds then these are unique.

***Ex.* 1.** *Find universal bounds in lattice* $(P(A), \subseteq)$ *where* $A = \{a, b, c\}$ *and* $P(A)$ *is power set of* A.

Sol. The lattice $(P(A), \subseteq)$ is shown in the following figure :

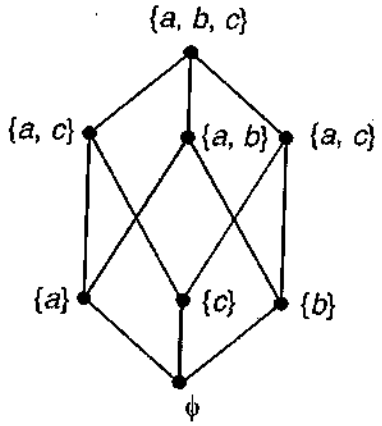


Fig. 18

Here $\{a, b, c\} = 1$, $\{\phi\} = 0$ are the universal bounds.

***Ex.* 2.** *Let* L *be set of all positive divisors of* 30. *Then find the universal lower bound and universal upper bound of the lattice* $(L, |)$.

Sol. The positive divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30.

Hence $L = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Recall that divisibility of positive integers is a partial ordering relation.

The lattice $(L, |)$ is shown below.

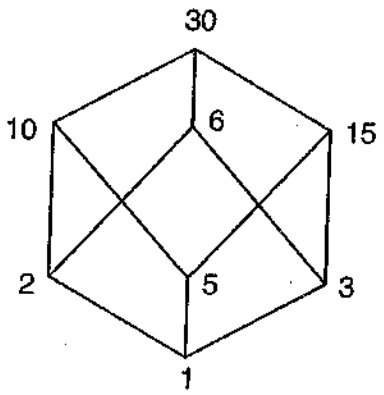


Fig. 19

Since $1 \leq x \leq 30 \quad \forall x \in L$

$\Rightarrow$ 1 and 30 are universal lower bound and universal upper bound of $(L, |)$.

Theorem. 3 *Let* $(A, \leq)$ *be a lattice, then* $\forall\ a \in A$

(i) $a \vee 1 = 1$ *and* $a \wedge 1 = a$

(ii) $a \vee 0 = a$ *and* $a \wedge 0 = 0$

where 0 and 1 are universal lower and universal upper bounds respectively.

Proof. *(i)* Let $a \in A$. Now, 1 is universal upper bound of A. Therefore

$$a \leq 1 \ \forall a \in A. \qquad \text{..... (1)}$$

Again, $1 \leq 1$ (reflexivity in $(A, \leq)$) .....(2)

From (1) and (2)

$$a \vee 1 \leq 1 \qquad \text{.....(3)}$$

Again, since $a \vee 1$ is least upper bound of a and 1. Therefore

$$a \leq a \vee 1 \text{ and } 1 \leq a \vee 1 \qquad \text{.....(4)}$$

Form (3) and (4),

$$a \vee 1 \leq 1, 1 \leq a \vee 1$$

$$\Rightarrow \quad a \vee 1 = 1$$

Similarly, we can show that $a \wedge 1 = a$.

(ii) Let $a \leq A$. Then $0 \leq a$ [$\because$ 0 is universal lower bound of A] .....(1)

Again, $a \leq a$ .....(2)

(1) and (2) imply that $a \vee 0 \leq a \vee a$ [using theorem 1 *(v)*]

or $a \vee 0 \leq a$ [$a \vee a = a$] .....(3)

Again, $a \vee 0$ is least upper bound of a and 0

$$\Rightarrow \quad a \leq a \vee 0 \text{ and } 0 < a \vee 0 \qquad \text{.....(4)}$$

Form (3) and (4), $a \vee 0 \leq a, a \leq a \vee 0$

$$\Rightarrow \quad a \vee 0 = a \qquad \text{[on using antisymmetry]}$$

Similarly, we can show $a \wedge 0 = 0$.

Distributive lattice :

A lattice $(A, \leq)$ is said to be distributive lattice if $\forall$ $a, b, c \in A$, we have

(i) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

(ii) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

The above two laws are called distributive laws of lattices.

Here, it is to be noted that lattices need not always be distributive as is evident form the following theorem.

Theorem 4 *Let a, b, c be arbitrary elements of a lattice* $(A, \leq)$. *Then*

(i) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$

(ii) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$

Proof. *(i)* Given that $a, b, c \in A$. Then

$$a \leq a \vee b \text{ and } b \wedge c \leq b \leq a \vee b$$

or $$a \leq a \vee b \text{ and } b \wedge c \leq a \vee b$$

$$\Rightarrow \quad a \vee b \text{ is upper bound of a and } (b \wedge c)$$

$\Rightarrow$ but $a \vee (b \wedge c)$ is least upper bound of a and $(b \wedge c)$. Therefore,

$$a \vee (b \wedge c) \leq a \vee b \quad \text{.....(1)}$$

Again, $a \leq a \vee c$ and $b \wedge c \leq c \leq a \vee c$

or $a \leq a \vee c$ and $b \wedge c \leq a \vee c$

$\Rightarrow$ $a \vee c$ is upper bound of a and $b \wedge c$

But $a \vee (b \wedge c)$ is least upper bound of a and $(b \wedge c)$. Therefore,

$$a \vee (b \wedge c) \leq a \vee c \quad \text{.....(2)}$$

Form (1) and (2), we find

$$a \vee (b \wedge c) \leq (a \wedge b) \wedge (a \vee c)$$

similarly we can show the result *(ii)*.

Complement of an element of a lattice :

Let $(A, \leq)$ be a bounded lattice. Let $a \in A$. Then an element $b \in A$ is called complement of $a \in A$ if

$$a \vee b = 1 \text{ and } a \wedge b = 0,$$

where 1 and 0 are universal upper bound and universal lower bound respectively of the lattice A.

The complement of a is denoted by $\overline{a}$ or by a'.

Note –1 : Only bounded lattice admits the notion of complement.

Note -2 : In a bounded lattice, any element may have no complement or more then one complement, but if the lattice is distributive also then an element (possessing complement) would have unique complement. Hence we state the following theorem.

Theorem 5 *If an element of bounded distributive lattice has a complement, then it is unique.*

Proof. Let $(A, \leq)$ be distributive and bounded lattice with 0 and 1 as its universal lower and universal upper bounds.

Let if possible b and c are two different complements of $a \in A$. Then by definition of complement of an element, we have

$$a \vee b = 1 \text{ and } a \wedge b = 0 \quad \text{.....(1)}$$

and $a \vee c = 1$ and $a \wedge c = 0$ .....(2)

Now, $c = c \vee 0$ [see theorem]

$= c \vee (a \wedge b)$ [using (1)]

$= (c \vee a) \wedge (c \vee b)$ [$(A, \leq)$ is distributive]

$= (a \vee c) \wedge (b \vee c)$ [$\because x \vee y = y \vee x$]

$= 1 \wedge (b \vee c)$

$= b \vee c$ [$\because 1 \wedge x = x \wedge 1 = x$]

Again, $b = b \vee 0$

$= b \vee (a \wedge c)$ [using (2)]

$= (b \vee a) \wedge (b \wedge c)$ [$\because (A, \leq)$ is distributive]

$= 1 \wedge (b \wedge c)$ [using (1)]

$= b \vee c$

Thus $b = c = b \vee c$

Hence our supposition that $a \in A$ has two different complements is wrong. Infact, $a \in A$ has unique complement in A.

Ex.1. *Give an example of a lattice where an element of it does not have complement.*

Sol. Let us consider the following bounded lattice.

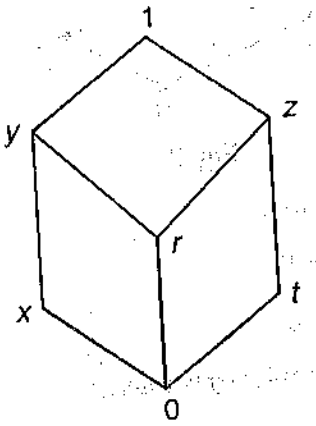


Fig. 20

Here note that the element r does not have complement since there does not exist any element b in the given lattice such that

$$r \vee b = 1 \quad \text{and} \quad r \wedge b = 0.$$

Where for example we see that x and y are complements of t. Note that

$$t \vee x = 1 \quad \text{and} \quad t \wedge x = 0$$

$$t \vee y = 1 \quad \text{and} \quad t \wedge y = 0$$

Ex.2. *Taking examples show that an element of a lattice may have different complements or unique complement.*

Sol. Consider the following lattice

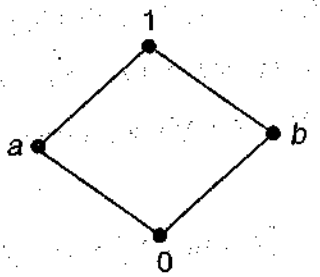


Fig. 21

In the above, we find that

$$a \vee b = 1 \text{ and } a \wedge b = 0$$

$\Rightarrow$ b is complement of a and vice-versa.

Thus complement of a and b are unique.

In the previous example we have seen that the element t has two different complements.

Ex.3. *Find the complements of x in the following lattice.*

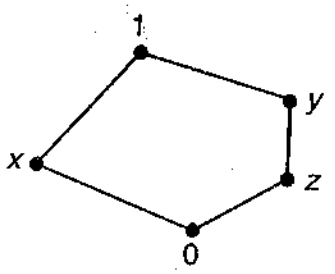


Fig. 22

Sol. From the given lattice we find that

$$x \vee y = 1 \text{ and } x \wedge y = 0$$

and $x \vee z = 1$ and $x \wedge z = 0$

$\Rightarrow$ x has two different complements y and z.

Ex.4. *Examine whether the lattice given above in the previous example is distributive.*

Sol. The lattice is not distributive since,

$$y \wedge (x \vee z) = y \wedge 1 = y$$

and
$$\begin{aligned} y \wedge (x \vee z) &= (y \wedge x) \vee (y \wedge z) \\ &= 0 \vee z \\ &= z \end{aligned}$$

$\Rightarrow$ $y \wedge (x \vee z) \neq (y \wedge x) \vee (y \wedge z)$

6.3.3 De'Morgan laws . Let $(A, \leq)$ be a complemented distributive lattice then for all $a, b, \in A$, we have

(i) $(a \vee b)' = a' \wedge b'$

(ii) $(a \wedge b)' = a' \vee b'$

Proof. ***(i)*** In order to prove that $(a \vee b)' = a' \wedge b'$ that is complement of $(a \vee b)$ is $a' \wedge b'$ we have to show that $(a \vee b) \vee (a' \wedge b') = 1$ and $(a \vee b) \vee (a' \wedge b') = 0$

we consider, $(a \vee b) \vee (a' \wedge b') = [(a \vee b) \vee a'] \wedge [(a \vee b) \vee b']$

(since A is distributive lattice)

$$= [a' \vee (a \vee b)] \wedge [a \vee (b \vee b')]$$

(on using commutativity and associativity)

$$= [(a' \vee a) \vee b] \wedge [a \vee (b \vee b')]$$

$$= [1 \vee b] \wedge [a \vee 1] \qquad [\because x \vee x' = 1 \ \forall x \in A]$$

$$= 1 \wedge 1 \qquad [\because x \vee 1 = 1 \ \forall \ x \in A]$$

$$= 1$$

Again, $(a' \wedge b') \wedge (a \vee b) = [(a' \wedge b') \wedge a] \vee [(a' \wedge b') \wedge b]$

$$= [a \wedge (a' \wedge b')] \vee [\, a' \wedge (b' \wedge b)]$$

$$= [(a \wedge a') \wedge b'] \vee [a' \wedge 0]$$

$$= [0 \wedge b'] \vee [a' \wedge 0]$$

$$= [0] \vee [0]$$

$$= 0$$

$\Rightarrow$ $(a \vee b)' = a' \wedge b'$

(ii) Simiarly to prove $(a \wedge b)' = a' \vee b'$ we shall show that $(a \wedge b) \vee (a' \vee b') = 1$ and $(a \wedge b) \wedge (a' \vee b') = 0$

we consider, $(a \wedge b) \vee (a' \vee b') = (a' \vee b') \vee (a \wedge b)$

$$= [(a' \vee b') \vee a] \wedge [(a' \vee b') \vee b]$$

$$= [(a \vee a') \vee b'] \wedge [a' \vee (b' \vee b)]$$

$$= [1 \vee b'] \wedge [a' \vee 1]$$

$$= 1 \wedge 1$$

$$= 1$$

Again, $(a \wedge b) \wedge (a' \vee b') = [(a \wedge b) \wedge a'] \vee [(a \wedge b) \wedge b']$

$$= [a' \wedge (a \wedge b)] \vee [\, a \wedge (b \wedge b')]$$

$$= [(a' \wedge a) \wedge b] \vee [\, a \wedge (b \wedge b')]$$

$$= [0 \wedge b] \vee [a \wedge 0] \qquad (\because x \wedge x' = 0 \ \forall x \in A)$$

$$= 0 \vee 0 \qquad [\because x \wedge 0 = 0 \wedge x = 0, \ \forall x \in A]$$

$$= 0$$

$\Rightarrow$ $(a \wedge b)' = a' \vee b'$

Complemented lattice : A bounded lattice $(A, \leq)$ is said to be a complemented lattice if every element of it contains a complement in the lattice.

Ex.1. *The lattice* $(P(A), \subseteq)$, where $P(A)$ *is power set of nonempty set* A, *is complemented and each subset* B *of* A *has the unique complement* $A - B$ *since*

$$B \vee (A - B) = B \cup (A - B) = A$$

$$B \wedge (A - B) = B \cap (A - B) = \phi$$

Note that in the lattice $(P(A), \subseteq)$ the set theoretic operations "union of sets denoted by $\cup$" and

intersection of sets denoted by "$\cap$" serve as join ($\vee$) and meet ($\wedge$) operations. Further A and ϕ are universal upper bound and universal lower bound of the lattice $(P(A), \subset)$.

Theorem . *The dual of a complemented lattice is again a complemented lattice. (left as an exercise for you)*

Ex.1. *Show that the following lattice is not distributive.*

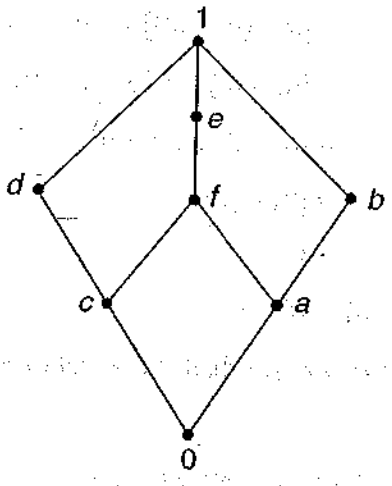


Fig. 23

Sol. In the given lattice, the element d has two complements a and b. Hence it is not distributive lattice. (Recall that in a distributive lattice complement (if it exists) of an element is unique).

Self-learning exercise-2

1. Which of the following is De-Morgan law

(i) $a \wedge a' = 1$ *(ii)* $a \wedge a' = 0$ *(iii)* $a \vee b = c \wedge 0$ *(iv)* $a \vee a' = 0$

2. If a' is complement of a. Then

(i) $a \vee a' = 0$ and $a \wedge a' = 0$

(ii) $a \vee a' = 1$ and $a \wedge a' = 0$

(iii) $a \vee a' = 0$ and $a \wedge a' = 1$

(iv) $a \vee a' = 1$ and $a \wedge a' = 1$

3. Which of the following is not true for a bounded lattice

(i) $a \vee 1 = a$ *(ii)* $a \vee 1 = 1$ *(iii)* $a \wedge 1 = a$ *(iv)* $a \wedge 0 = 0$

4. Which of the following is true for arbitrary elements a, b, c of a lattice $(A, \leq)$

(i) $a \vee (b \wedge c) \geq (a \vee b) \wedge (a \vee c)$

(ii) $a \vee (b \wedge c) \leq (a \wedge b) \vee (a \wedge c)$

(iii) $a \vee (b \wedge c) \leq (a \vee b) \vee (a \vee c)$

(iv) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$

6.4 Functions

A function is a specific case of relation. That is every function is a relation but converse need not be true. Now, we have a formal definition of function.

Let A and B be two non-void sets, then a function f from the set A to B is a collection of ordered pairs $f \subseteq A \times B$ in such a way that for every element $a \in A$, these exists unique element $b \in B$ such that $(a, b) \in f$.

Literally it means that every element of the set A is associated to unique element of B. If further inferences that there may be some element in B which is not associated to any element of A.

A function f form set A to set B is denoted as $f: A \to B$

The sets A and B are called domain and co-domain of the function f.

Range and Image : Let $(a, b) \in f$ then this implies that $f(a) = b$ Here, b is called f-image of a and a is called pre-image of b. The set of all the images of the elements of A under the function f is called the range of f. Symbolically, range of f is denoted by $f(A)$. Obviously $f(A) \subseteq B$.

A function $f : A \to B$ can be depicted as shown below

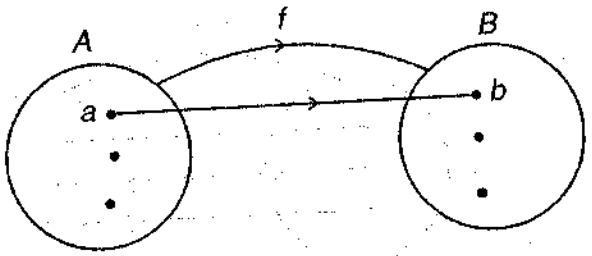


Fig. 24

6.4.1 Types of function :

***(i)* One-one or Injective function.**

A function from set A into set B is called one-one function if $\forall\ a, b, \in A$ such that

$$f(a) = f(b) \Rightarrow a = b$$

literally, it means that two different elements of A are not associated with the same element of B.

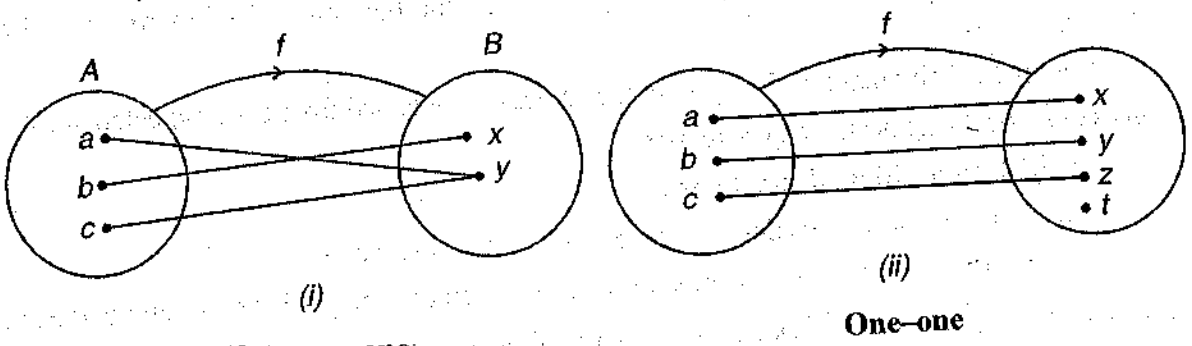


Fig. 25

Ex. Let $f(x) = 4x + 7$, where x is real number then f is one-one since for

$$f(x_1) = f(x_2) \Rightarrow 4x_1 + 7 = 4x_2 + 7$$
$$\Rightarrow x_1 = x_2.$$

***(ii)* Many-one :** A function $f: A \to B$ is many-one iff two or more elements of A are associated to the same element of B.

***(iii)* Onto or surjective function :** A function $f: A \to B$ is called onto if $f(A) = B$.

***(iv)* One-one onto or bijective function :** A function $f: A \to B$ is called bijective if f is one-one and onto function. Bijection is also referred to as one-one correspondence. Literally it means that Both A and B have same number of elements.

Following figures depict the types of functions discussed above

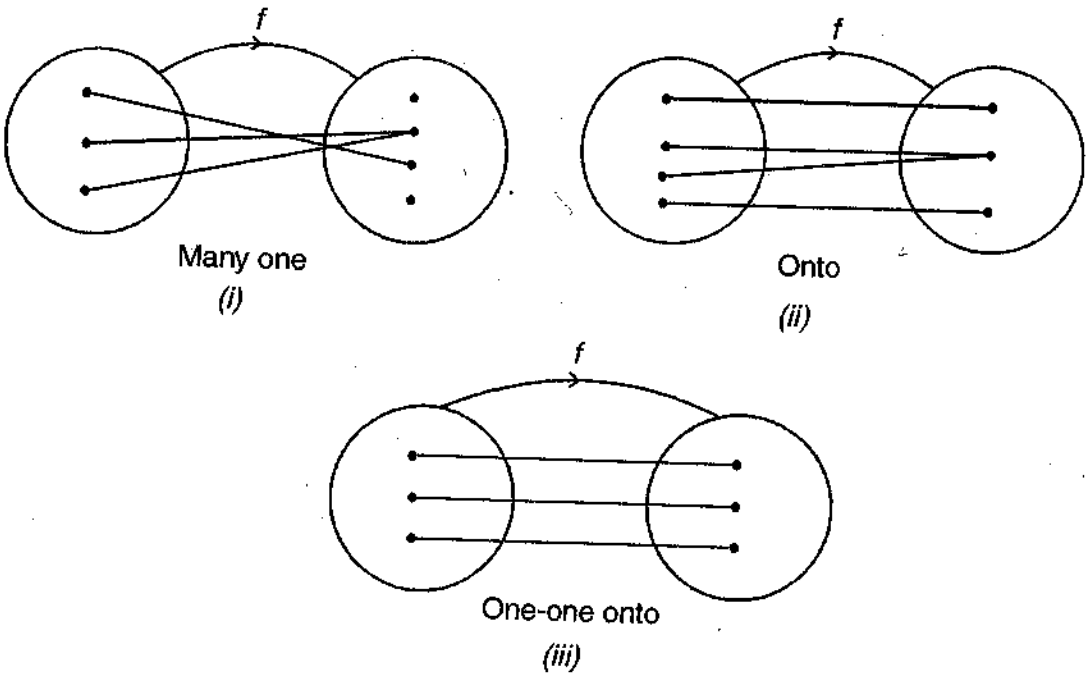


Fig. 26

Working method to test that a function is onto :

To verify that a function $f: A \to B$ is onto, the following procedure is followed.

Step 1 : Let $y \in B$ be any arbitrary element.

Step 2: Let $f(x) = y$.

Step 3 : Solve the equation $f(x) = y$ for x *i.e.* find the value of x in terms of y. Let it be $x = g(y)$.

Step 4 : Verify that for every $y \in B$, the values of x obtained from $x = g(y)$ belong to A. If such values of x exist then f is onto otherwise not.

6.4.2 Composition of functions :

With the help of composition of functions we get a new function.

Let $f: A \to B$ and $g: B \to C$ be two functions then the composition of f and g, read as gof and denoted by gof is another function $gof: A \to C$. Which is written as

$$gof(a) = g\{f(a)\} \ \forall \ a \in A.$$

Pictorially it is represented as in the following figure

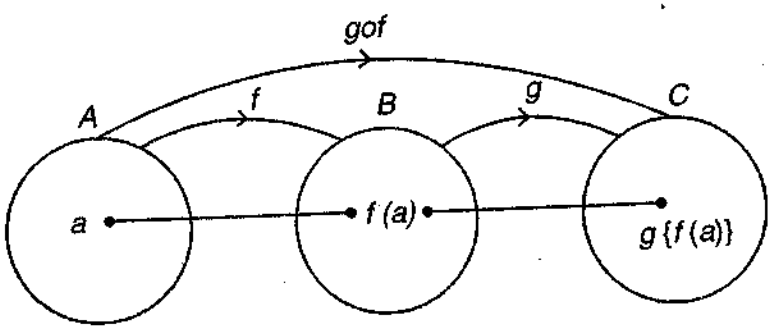


Fig. 27

Obviously for the function gof, A is the domain and C is co-domain. Whereas for g, range of f is its domain.

Note that in general $gof \neq fog$

Ex. *Let* $f : R \to R$ *and* $g : R \to R$ *be two functions such that*

$$f(x) = x-1,\ g(x) = \frac{x}{2}$$

Then find *fog* and *gof*

Sol. $$fog(x) = f\left[g(x)\right] = f\left(\frac{x}{2}\right) \qquad \because g(x) = \frac{x}{2}$$

Again, $$gof(x) = g\left\{f(x)\right\} = g(x-1) = \frac{x-1}{2} \qquad \because f(x) = x-1$$

Properties of composition of functions :

(i) Composition of functions, in general, is not commutative *i.e.* $fog \neq gof$

(ii) Composition of functions is associative *i.e.* for functions f, g, h we have

$$f\,o\,(goh) = (fog)\,oh$$

(iii) If functions f and g are onto then their compositions *gof*, *fog* are also onto.

6.4.3 Inverse function :

Let $f : A \to B$ be a one-one onto function then there exists a function f^{-1} form B to A, known as inverse function of f and is defined as for every $y \in B$, $x = f^{-1}(y)$, where $f(x) = y$.

This can be shown pictorially as given below

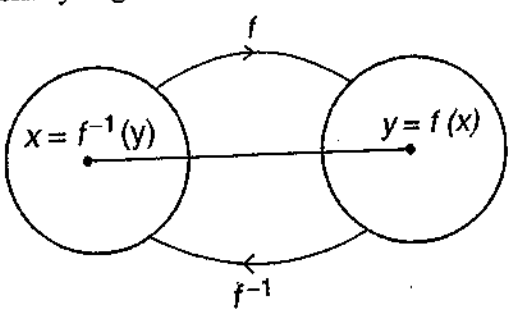


Fig. 28

Working method to get inverse function : Let $f: A \to B$ be one-one function. Then f^{-1} is obtained by following the given procedure.

Step -1 Let $y \in B$ is image of $x \in A$. Then $f(x) = y$

Step -2 Solve $y = f(x)$ for x is terms of y.

Step -3 Express x (obtained in step-2) as $f^{-1}(y)$. This gives f^{-1}.

Ex.1. *Find the inverse function of the function $f: R \to R$ defined as*

$$f(x) = 3x + 8 = y$$

Sol. Let x and y be elements of domain R and co-domain R such that $f(x) = y$.

Then $3x + 8 = y$

or $$x = \frac{y-8}{3} = f^{-1}(y)$$

Thus $f^{-1} : R \to R$ is defined as

$$f^{-1}(x) = \frac{x-8}{3}$$

Ex.2. *Let $A = \{0, 1, 2, 3...\}$ and a function $f: A \to A$ is defined as*

$$f(x) = \begin{cases} x-1, \text{ if } x \text{ is odd} \\ x+1, \text{ if } x \text{ is even} \end{cases}$$

show that $f = f^{-1}$

Sol. The given function f is one-one onto. Therefore f^{-1} exists. Let $x, y \in A$ exist such that $f(x) = y$.

Then $$\left.\begin{matrix} x-1 = y, \text{ if } x \text{ is odd} \\ x+1 = y, \text{ if } x \text{ is even} \end{matrix}\right\}$$

$\Rightarrow$ $$x = \begin{cases} y+1, \text{if } y \text{ is even} \\ y-1, \text{if } y \text{ is odd} \end{cases}$$

Thus $$x = f^{-1}(y) = \begin{cases} y+1, \text{ if } y \text{ is even} \\ y-1, \text{ if } y \text{ is odd} \end{cases}$$

or $$f^{-1}(x) = \begin{cases} x+1, \text{ if } x \text{ is even} \\ x-1, \text{ if } x \text{ is odd} \end{cases}$$

obviously, $f = f^{-1}$.

Ex.3. *Late $A = \{-2, 1, 3, 4\}$. A function $f: A \to A$ is defined such that*

$$f(x) = x^2 - 2x + 2$$

find ***(i)*** *range of f*

(ii) *pre-image of 5*

Sol. ***(i)*** Range of $f = f(A) = \{f(x) \mid x \in A\}$

Now, $f(-2) = (-2)^2 - 2(-2) + 2 = 10$

Similarly $f(-2) = 1, f(3) = 5, f(4) = 10$

Therefore $f(A) = \{1, 5, 10\}$

(ii) Let pre-image of 5 is x, then

$$f(x) = 5$$

Therefore, $x^2 - 2x + 2 = 5$

or $x^2 - 2x - 3 = 0$

or $(x + 1)(x - 3) = 0$

or $x = -1$ or $x = 3$

Since $-1 \notin A$, therefore 3 is pre-image of 5 under f.

Ex.4. *Show that a function $f : R \to R$ such that*

$f(x) = x^2$ *is not one-one.*

Sol. f is not one-one function because $2 \in R, -2 \in R$ but $f(2) = f(-2) = 4$.

However if we consider a function $f : R \to R$

such that $f(x) = x^3 + 2$,

Then it is one-one since if $x = y$

Then $x^3 = y^3$ or $x^3 + 2 = y^3 + 2$

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

consequently f is one-one.

Ex.5. $f : N \to N$, *such that*

$f(x) = 3x + 2$ *is not onto.*

Sol. Let $y \in N$ such that $f(x) = y$

$\Rightarrow$ $3x + 2 = y$

$\therefore$ $$x = \frac{y-2}{3}$$

Now for every $y \in N$, $\frac{y-2}{3} \notin N$.

e.g. for $$y = 1, \frac{1-2}{3} \notin N.$$

Thus, pre-image of every element of co-domain N does not belong to domain N. Consequently f is not onto.

Ex.6. *Let $A = R - \{3\}, B = R - \{1\}$. Show that function $f : A \to B$, such that*

$$f(x) = \frac{x-4}{x-3}$$ *is one-one onto.*

Sol. ***(i) f* is one-one**

Let x and y are arbitrary elements of A

such that $$f(x) = f(y)$$

Then $$\frac{x-4}{x-3} = \frac{y-4}{y-3}$$

$\Rightarrow$ $$(x-4)(y-3) = (x-3)(y-4)$$

or $$xy - 3x - 4y + 12 = xy - 3y - 4x + 12$$

or $$x = y$$

consequently f is one-one.

***(ii) f* is onto**

Let $y \in B$. Then

$$f(x) = y = \frac{x-4}{x-3}$$

$\therefore$ $$y(x-3) = x - 4$$

or $$x = \frac{4+3y}{y-1}$$

we see that for $y \neq 1$, $\frac{4+3y}{y-1} \in R$

Again we find that $\frac{4+3y}{y-1} \neq 3$

Since $\frac{4+3y}{y-1} = 3 \Rightarrow 4 = -3$. Which is not true.

Thus every element of B has pre-image in A. Thus f is onto.
Hence f is one-one onto.

6.5 Summary

In this unit you have gone through posets, lattices and functions. You must have observed that how a partial ordering relation defined on a set give rise to notion of a poset and lattice. In continuation of this you must appreciate the importance of Hasse diagram in representing a poset.

In this unit you also studied "function" which is a special case of a relation.

6.6 Answers to the self-learning exercises

Self-learning exercise-1

1. (*iii*) 2. (*iv*) 3. (*iv*)
4. Except (*iv*), (*i*), (*ii*), (*iii*) are not lattices. (*i*), (*ii*) are not even posets. (*iii*) is poset but not lattice because sup $\{a, c\}$ does not exist

5. Universal upper bound — *(i)* e — *(ii)* a

Universal lower bound — a — e

6. *(i)* is not a lattice — *(ii)* is a lattice

7. 5 *(i)* Maximal : e, Minimal : a

(ii) Maximal : a, Minimal : e

6 *(i)* Maximal : g, Minimal : a, b

(ii) Maximal : h, Minimal : a

8. Upper bound of $\{a, b\}$: c, d, e, f, e

least upper bound of $\{a, b\}$: c

lower bound of $\{a, b\}$: does not exist

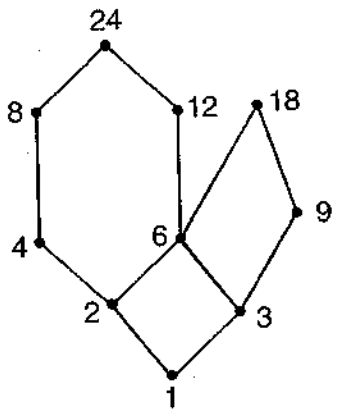
Self-learning exercise-2

1. *(ii)* **2.** *(ii)* **3.** *(i)* **4.** *(iv)*

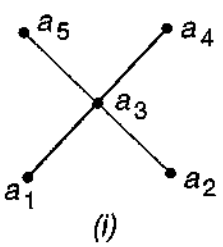
6.7 Exercises

1. Let $A = \{1, 2, 3, 4, 6, 8, 9, 12, 24\}$ and R be a relation defined on A such that " a R b if a devices b". Find the Hasse diagram of the poset (A, R)

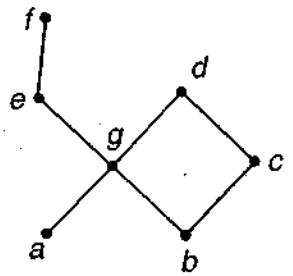
Ans.



2. Find minimal and maximal elements in the following posets :



(i)



(ii)

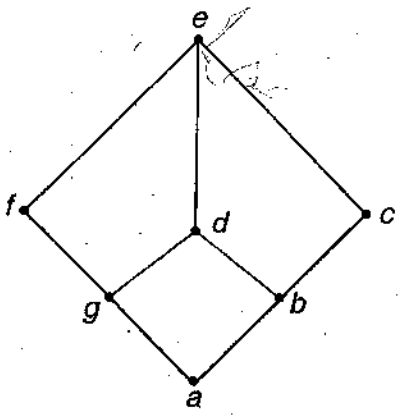
Ans. *(i)* Minimal elements : a_1, a_2

Maximal elements : a_4, a_5

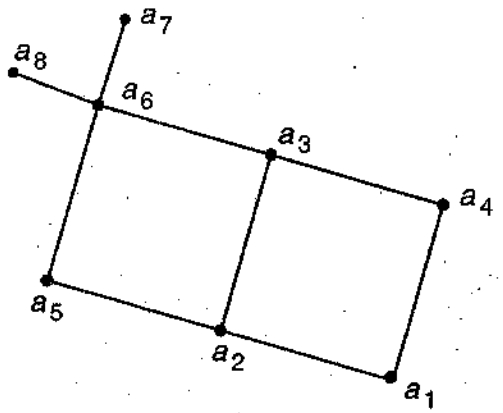
(ii) Minimal elements : a, b

Maximal elements : d, f

3. Show that the following lattice is not distributive



4. Find the superemum and infimum of $B = \{a_3, a_4, a_5\}$ in the following poset.



[Ans. sup : a_6, Inf : a_1]

5. Let $f: R \to R, g: R \to R, h: R \to R$ be functions

such that $f(x) = x + 2, g(x) = x^2, h(x) = x - 2$

Then show that $f \circ (g \circ h) = (f \circ g) \circ h$

Also find $g \circ f, f \circ g$ and $f \circ f$.

Ans. $(g \circ f)(x) = x^2 + 4x + 4$

$(f \circ g)(x) = x^2 + 2$

$(f \circ f)(x) = x + 4$.

6. Find inverse function of $f: R \to R$ such that

$$f(x) = x + 2$$

Ans. $f^{-1}(x) = x - 2$

7. Write the dual of $a \vee (b \wedge c)$ and $a \wedge (b \wedge c)$

Ans. $[a \wedge (b \vee c)]$ and $a \vee (b \vee c)$ respectively.

8. Show that function $f: A \to B$,

$f(x) = x \mid x \mid, \forall x \in A$ is one-one onto

where $A = B = \{x \in R \mid \mid x \mid \leq 1\}$.

□□□

UNIT 7 : Groups

Structure of the Unit

7.0 Objectives

After reading this unit you will be able to understand about binary operations and their properties, groupoids, quasigroups, semigroups, monoids, free monoids, homomorphism of semigroups and groups.

7.1 Introduction

In this unit we begin by defining binary operations and their properties. After this we proceed with the definitions of groupoids, quasigroups, semigroups, monoid, free semigroups, free monoids, homomorphism of semigroups and some important examples and results related to these topics. In the end of the unit we discuss about groups, examples of groups and elementary properties of groups.

7.2 Binary operations and tables

Let S be a nonempty set. A **binary operation** on S, denoted here by $*$, is a function from $S \times S$ into S. For any $a, b \in S$ we shall write $a * b$ or sometimes ab instead of $*(a, b)$, that is, the image of the ordered pair (a, b) under this function is denoted by $a * b$. Since a binary operation is a function only one element of S is assigned to each ordered pair $(a, b) \in S \times S$.

In other words we can say that a binary operation on a set S is a rule which assigns to each ordered pair of elements of S a unique element of S, that is, if a, b are elements in S, then $a * b$ is a unique element of S.

Examples :

1. Addition (+), subtraction (–) and multiplication (·) are binary operations on the set Z of integers because for each $a, b \in Z \Rightarrow a + b, a - b, ab$ are unique element of Z. However, division is not a binary operation on Z because the quotient of two integers is not always an integer. Division is not a binary operation on the set of rational numbers Q, on the set of real numbers R and on the set of complex numbers C, because division by 0 (zero) is not defined.
2. Let $P(S)$ be the collection of all subsets of S; for some set S. Then union ($\cup$) and intersection ($\cap$) are binary operations on $P(S)$ because for all $A, B \in P(S) \Rightarrow A \cup B$ and $A \cap B \in P(S)$.
3. Let $S = \{1, -1\}$. Then multiplication and division are binary operations on S but addition and subtraction are not binary operations on S.
4. Let $M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in R \right\}$ be a collection of all 2×2 matrices over R. Then matrix addition and matrix multiplication are binary compositions on M_2. Again, let

$$A = \left\{ \begin{bmatrix} a & b \\ c & 0 \end{bmatrix} \mid a, b, c \in R \right\} \text{ and}$$

$$B = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a, b, d \in R \right\}$$

be two subsets of M_2. Then matrix addition is a binary operation on A but matrix multiplication is not a binary operation on A, because $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix}$ are elements of A, where as $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 1 & 2 \end{bmatrix} \notin A$. On the other hand matrix addition and multiplication are binary operations on B.

5. On the set N of natural numbers, define $a * b$ is a number less than both a and b. Then $*$ is not a binary operation on N, since it does not assign a unique element of N to each ordered pair of elements of N, for example $4 * 3$ could be 2, 1.

6. Let $S = \{a, b, c, d\}$. Let the binary operation $*$ be defined on S by means of the following table :

$*$	a	b	c	d
a	a	b	c	d
d	b	a	d	c
c	c	d	a	b
d	d	c	b	a

The table is read in the following manner, for example, from the table

$$a * a = a,\ a * b = b,\ d * d = a,\ b * d = c.$$

7. Let $S = \{1, -1, i, -i\}$, where $i = \sqrt{-1}$. Let us consider the following tables

$+$	1	-1	i	$-i$
1	2	0	$1+i$	$1-i$
-1	0	-2	$-1+i$	$-1-i$
i	$1+i$	$-1+i$	$2i$	0
$-i$	$1-i$	$-1-i$	0	$-2i$

$-$	1	-1	i	$-i$
1	0	2	$1-i$	$1+i$
-1	-2	0	$-1-i$	$-1+i$
i	$i-1$	$i+1$	0	$2i$
$-i$	$-1-i$	$-i+1$	$-2i$	0

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$\div$	1	-1	i	$-i$
1	1	-1	$-i$	i
-1	-1	1	i	$-i$
i	i	$-i$	1	-1
$-i$	$-i$	i	-1	1

From above tables it is clear that multiplication ($\cdot$) and division ($\div$) are binary operations on S but addition ($+$) and subtraction ($-$) are not binary operations on S.

7.2.1 Properties of binary operations

A binary operation $*$ on a set S is said to be **commutative** if

$$a * b = b * a \qquad \forall\ a, b \in S.$$

A binary operation $*$ on a set S is said to be **associative** if

$$(a * b) * c = a * (b * c) \qquad \forall\ a, b, c \in S.$$

Examples :

1. Addition and multiplication are commutative and associative binary operations on the set Z of integers because for all $a, b, c \in Z$, we have

$$a + b = b + a,\quad ab = ba,\ a + (b + c) = (a + b) + c \text{ and } a(bc) = (ab)c.$$

On the other hand subtraction is neither commutative nor associative binary operation on Z, because

$$2 - 3 \neq 3 - 2 \quad \text{and} \quad 2 - (3 - 5) \neq (2 - 3) - 5.$$

2. $\cup$ and $\cap$ are commutative and associative binary operations on collection of all subset of S, *i.e.* $P(S)$, because for $A, B, C \in P(S)$, we have

$$A \cup B = B \cup A, \quad A \cap B = B \cap A$$

$$(A \cup B) \cup C = A \cup (B \cup C) \text{ and}$$

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

3. Consider the exponential operation $a * b = a^b$ on the set N of natural numbers. The operation $*$ is neither commutative nor associative because for $2, 3, \in N$,

$$2 * 3 = 2^3 = 8 \quad \text{but} \quad 3 * 2 = 3^2 = 9$$

$$\Rightarrow \qquad 2 * 3 \neq 3 * 2.$$

$$(2 * 2) * 3 = 2^2 * 3 = 4^3 = 64 \text{ but}$$

$$2 * (2 * 3) = 2 * 2^3 = 2 * 8 = 2^8 = 256$$

$$\Rightarrow \qquad (2 * 2) * 3 \neq 2 * (2 * 3).$$

4. Let M_n be a collection of all $n \times n$ matrices over R. Then matrix multiplication is associative on M_n but matrix multiplication is not commutative.

Identity element :

Let S be a nonempty set and let $*$ be a binary operation on S. An element $e_1 \in S$ is said to be **left identity** with respect to $*$ if $e_1 * a = a$ for all $a \in S$. An element $e_2 \in S$ is said to be **right identity** with respect to $*$ if $a * e_2 = a$ for all $a \in S$. An element $e \in S$ is said to be an **identity element** with respect to $*$ if

$$a * e = a = e * a \qquad \forall a \in S.$$

Thus an element $e \in S$ is called an identity in S if it left as well as right identity in S with respect to binary operation $*$ in S.

Inverse of an element :

Let S be a nonempty set and let $*$ be a binary operation on S. An element $b \in S$ is called a **left inverse** of a with respect to $*$ if $b * a = e$, where e is the identity element in S with respect to binary operation $*$ is S. An element $b \in S$ is called a **right inverse** of a with respect to $*$ if $a * b = e$. An element $b \in S$ is said to be the inverse of an element a $\in$ S if $b * a = e = a * b$. Thus an element $b \in S$ is called the inverse of a in S if b is left as well as right inverse of a in S and in this case we write $a^{-1} = b$.

Examples :

1. In the set Z of integers 0 (zero) is the identity element with respect to binary operation addition (+) because

$$a + 0 = a = 0 + a \qquad \forall a \in Z$$

and 1 (one) is the identity element in Z with respect to binary operation multiplication because $a \cdot 1 = a = 1 \cdot a \ \forall a \in Z$. zero is not an identity element with respect to binary operation subtraction (–) because $a - 0 = a \neq 0 - a$ unless $a = 0$.

2. In the set $P(S)$, empty se ϕ is the identity element with respect to binary operation $\cup$ because $\phi \cup A = A = A \cup \phi \ \forall \ A \in P(S)$ and set S is the identity element with respect to binary operation $\cap$ because $A \cap S = A = S \cap A \ \forall \ A \in P(S)$. If $\phi \neq A \in P(S)$, then inverse of A with respect to binary operation $\cup$ does not exist. Similarly $S \neq A \in P(S)$, then inverse of A with respect to binary operation $\cap$ does not exist. Since $\phi \cup \phi = \phi$ and $S \cap S = S$, so in the power set $P(S)$, ϕ and S are the only invertible elements for the union and intersection binary operations respectively.

3. In the set Q of rational numbers 1 and -1 are two left identifies with respect to binary operation $*$ defined by $a * b = a^2 b \ \forall \ a, b \in Q$, since $1 * x = x$ and $(-1) * x = x \ \forall \ x \in Q$.

7.2.2 Algebraic structures :

An **algebraic structure** is a system consisting of a nonempty set S and one or more operations defined on S. Thus, if $*$ is a binary operation on S, then $(S, *)$ is called an algebraic structure.

Examples : $(N, +)$, $(N, \cdot)$, $(Z, +)$, $(Z, \cdot)$, $(Z, -)$, $(Z, +, \cdot)$, $(Q, +)$, $(Q, \cdot)$, $(Q, -)$, $(Q, +, \cdot)$, $(R, +, \cdot)$, $(C, +, \cdot)$, $(P(S), \cup, \cap)$.

The set of natural number under subtraction is not an algebraic structure because subtraction is not a binary operation on N.

7.2.3 Groupoid, Quasigroup, Semigroup and Monoid :

Groupoid : If $*$ is a binary operation on a non-empty set S, then $(S, *)$ is known as **groupoid,** *i.e.* a nonempty set S equipped with one binary operation $*$ is called groupoid.

Examples : $(N, +)$, $(N, \cdot)$, $(Z, +)$, $(Z, \cdot)$, $(Z, -)$, $(Q, +)$, $(Q, \cdot)$, $(C, +)$, $(C, \cdot)$, $(R, +)$, $(R, \cdot)$, $(P(S), \cup)$ $(P(S), \cap)$.

Quasigroup : A nonempty set S equipped with a binary operation $*$ is called a **quasigroup** if for $x, y \in S$, the questions $a * x = b$ and $y * a = b$ have unique solutions in S.

For example, the algebraic structure $(Z, +)$ is a quasigroup, since the equation $a + x = b$ and $x + a = b$ have unique solutions in Z for $a, b \in Z$. However, the algebraic structure $(Z, \cdot)$ is not a quasigroup, since for $4, 7 \in X$, $4 \cdot x = 7$ has no solution in Z.

Semigroup : An algebraic structure $(S, *)$ is called a **semigroup** if binary operation $*$ is associative, *i.e.*,

$$a * (b * c) = (a * b) * c \qquad \forall \ a, b, c \in S.$$

Examples : $(N, +)$, $(N, \cdot)$, $(Z, +)$, $(Z, \cdot)$, $(Q, +)$, $(Q, \cdot)$, $(R, +)$, $(R, \cdot)$, $(C, +)$, $(C, \cdot)$, $(P(S), \cup)$ $(P(S), \cap)$.

The set Z of integers, Q of rationals, R of reals and C of complex numbers with binary operation of subtraction are not semigroups, since subtraction is not associative.

Monoid : A semigroup $(S, *)$ is called a **monoid** if there exists an identity element e in S with respect to binary operation $*$ in S, that is there exists $e \in S$ such that

$$c * a = a = a * e \qquad \forall\ a \in S.$$

Examples : The semigroup $(P(S), \cup)$ and $(P(S), \cap)$ are monoid because ϕ and S are the identities respectively for $\cup$ and $\cap$ in $P(S)$. The semigroup $(N, \cdot)$ is a monoid because $1 \in N$ is the identity element for multiplication. But the semigroup $(N, +)$ is not a monoid because 0, the identity for addition is not in N.

7.2.4 Subsemigroup and submonoid :

If $*$ is a binary operation on a nonempty set S and T is any nonempty subset of S, then T is said to be **closed** under the operation $*$ if $a * b \in T$ for all $a, b \in T$.

A nonempty subset T of a semigroup $(S, *)$ is called a **subsemigroup** of S if T itself is a semigroup with respect to the binary operation $*$ defined on S. Since T is a subset of S and $*$ is associative in S, so $*$ must be associative in T. In order to prove that a nonempty subset T of S to a subsemigroup of S, it is sufficient to show that T is closed under the binary operation $*$ in S.

Similarly, let $(S, *)$ be a monoid with identity e and let T be a nonempty subset of S. If T is closed under the operation $*$ and $e \in T$, then $(T, *)$ is called a **submonoid** of $(S, *)$.

Let $A = \{1, 3, 5, ..., 2n-1, ...\}$ where $n \in N$ be a collection of odd natural numbers. Then A is a nonempty subset of the semigroup $(Z, +)$ of integers. But A is not a subsemigroup of $(Z, +)$, since A is not closed under binary operation addition. Similarly the set N of natural numbers is a nonempty subset of the monoid $(Z, +)$ of integers. But N is not a submonoid of $(Z, +)$, since additive identity $0 \notin N$.

7.2.5 Cyclic monoid

A monoid $(S, *)$ is said to be a **cyclic monoid** if there exists an element $a \in S$ such that each element of S can be written as some integral power of a, *i.e.*, for any $b \in S$ there exists some $n \in Z$ such that $b = a^n$. In this case the element a is called **generator** of S. If addition is binary operation in S, then S is said to be a cyclic monoid generated by $a \in S$ if every element of S can be written as some integral multiple of a. For example the set $S = \{1, -1, i, -i\}$, where $i = \sqrt{-1}$ under multiplication as a binary operation is a cyclic monoid. The elements i and $-i$ are the generators. The set Z of integers under addition as a binary operation is a cyclic monoid. The elements -1 and 1 are the generators.

7.2.6 Homomorphism of semigroup

Let $(S, *)$ and $(S', 0)$ be any two semigroups. The a mapping $f: S \to S'$ is called a **semigroup homomorphism**, if

$$f(a * b) = f(a)\, 0\, f(b), \quad \text{for all } a, b \in S$$

or, simply

$$f(ab) = f(a) f(b), \quad \text{for all } a, b \in S.$$

If f is one-one then it is called a **semigroup monomorphism.** If f is onto, then it is called a **semigroup epimorphism.** If f is one-one, onto, *i.e.*, bijective, then it is called an **isomorphism** of semigroups. A homomorphism of a semigroup into itself is called a **semigroup endomorphism.** An isomorphism of a semigroup onto itself is called a **semigroup automorphism.**

Two semigroup S and S' are said to be **isomorphic,** if there exists an isomorphism between them, and then we write $S \cong S'$.

For example, let A be the set of all even integers, then the semigroups $(Z, +)$ and $(A, +)$ are isomorphic. We define a function $f: Z \to A$ by $f(a) = 2a$. f is one-one, since $f(a_1) = f(a_2) \Rightarrow 2a_1 = 2a_2 \Rightarrow a_1 = a_2$. Let b be any even integer. Then $a = \frac{b}{2} \in Z$ such that $f(a) = f\left(\frac{b}{2}\right) = b$, so f is onto.

For any $a, b \in Z$, we have

$$f(a + b) = 2(a + b)$$
$$= 2a + 2b = f(a) + f(b).$$

Hence $(Z, +)$ and $(A, +)$ are isomorphic semigroups, *i.e.* $Z \cong A$.

Similarly, let $A = \{0, 1\}$ and consider the semigroup $(A^*, \cdot)$ and $(A, +_2)$, where $\cdot$ is the concatenation operation and $+_2$ is defined by the table

$+_2$	0	1
0	0	1
1	1	0

Define the function $f: A^* \to A$ by

$$f(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ has odd number of 1's} \\ 0 & \text{if } \alpha \text{ has even number of 1's.} \end{cases}$$

If is easy to verify that α and β are any elements of A^*, then $f(\alpha \cdot \beta) = f(\alpha) +_2 f(\beta)$.

Thus f is a homomorphism. The function f is onto, since $f(0) = 0$ and $f(1) = 1$ but f is not an isomorphism, since it is not one to one.

7.2.7 Some important examples

Ex. **1.** *Show that the set Q^+ of positive rational numbers is a monoid with binary operation $*$ defined by*

$$a * b = \frac{ab}{2} \qquad \forall a, b \in Q^+.$$

Sol. Let a, b, c be three elements of Q^+. Then

$$(a * b) * c = \frac{ab}{2} * c$$
$$= \frac{(ab)c}{4}$$

$$= \frac{a}{2}\left(\frac{bc}{2}\right)$$

$$= \frac{a}{2}(b * c)$$

$$= a * (b * c)$$

$\Rightarrow$ $(a * b) * c = a * (b * c) \quad \forall\ a, b, c \in Q^+.$

Hence $*$ is associative.

Let e be the identity element in Q^+.

Then $a * e = a = e * a \quad \forall\ a \in Q^+$

$\Rightarrow$ $a * e = a \quad \forall\ a \in Q^+$

$\Rightarrow$ $\frac{ae}{2} = a$

$\Rightarrow$ $e = \frac{2}{a} \in Q^+$

So, $\frac{2}{a}$ is the identity element, and hence $(Q^+, *)$ is a monoid.

Ex.2. *Show that the set Z of integers with binary operation $*$ defined by*

$$a * b = a + b - ab, \text{ for all } a, b \in Z$$

is a commutative semigroup. Show also that it is a monoid.

Sol. Let a, b, c be three elements of Z. Then

$$a * (b * c) = a * (b + c - bc)$$
$$= a + (b + c - bc) - a(b + c - bc)$$
$$= a + b + c - bc - ab - ac + abc \quad \text{.....(1)}$$

and $(a * b) * c = (a + b - ab) * c$
$$= (a + b - ab) + c - (a + b - ab)c$$
$$= a + b + c - ab - ac - bc + abc$$
$$= a + b + c - bc - ab - ac + abc \quad \text{.....(2)}$$

From (1) and (2), we get

$$a * (b * c) = (a * b) * c \quad \forall\ a, b, c \in Z.$$

Hence $*$ associative.

Also $a * b = a + b - ab$

$= b + a - ab$

$= b * a$

$\Rightarrow$ $a * b = b * a \quad \forall\ a, b, c \in Z$

So it is also commutative.

Thus $(Z, *)$ is a commutative semigroup. Now, we observe that

$$a * 0 = a = 0 * a \quad \text{for all } a \in Z.$$

So 0 (zero) is the identity element in Z with respect to binary operation $*$ and hence $(Z, *)$ is also a monoid.

Ex.3. *Show that the set $N \times N = \{(a, b) \mid a, b \in N\}$ is a monoid with the binary operation $*$ defined by*

$$(a_1, b_1) * (a_2, b_2) = (a_1 a_2, b_1 b_2) \text{ for } (a_1, b_1), (a_2, b_2) \in N \times N.$$

Sol. Let (a_1, b_1), (a_2, b_2) and (a_3, b_3) be any three elements of $N \times N$. Then

$$(a_1, b_1) * [(a_2, b_2) * (a_3, b_3)]$$

$$= (a_1, b_1) * (a_2 a_3, b_2 b_3)$$

$$= [a_1 (a_2 a_3), b_1 (b_2 b_3)]$$

$$= [(a_1 a_2) a_3, (b_1, b_2) b_3],$$

since multiplication is associative in N

$$= (a_1 a_2, b_1, b_2) * (a_3, b_3)$$

$$= [(a_1, b_1) * (a_2, b_2)] * (a_3, b_3).$$

$\Rightarrow$ $*$ is associative in $N \times N$.

Now $1 \in N \Rightarrow (1, 1) \in N \times N$ such that

$$(a, b) * (1, 1) = (a, b) = (1, 1) * (a, b)$$

for every $(a, b) \in N \times N$. So $(1, 1)$ is the identity element in $N \times N$, and hence $(N \times N, *)$ is a monoid.

Ex.4. *Let $(S, *)$ be a semigroup with identity element e and let b and c be inverses of a. Then show that $b = c$, that is, the inverses are unique if they exist.*

Sol. Since b and c are inverses of $a \in S$, so

$$a * b = e = b * a \quad \text{.....(1)}$$

and

$$a * c = e = c * a \quad \text{.....(2)}$$

From (1) we have

$$a * b = e$$

$\Rightarrow$ $c * (a * b) = c * e$

$\Rightarrow$ $(c * a) * b = c$, since $*$ is associative

$\Rightarrow$ $e * b = c$, using (2)

$\Rightarrow$ $b = c$.

Ex.5. *Let $S = N \times N$. Let $*$ be a binary operation on S defined by*

$$(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \text{ for } (a_1, b_1), (a_2, b_2) \in S.$$

(i) *Show that $(S, *)$ is a semigroup.*

(ii) *$(S, *)$ is not a monoid.*

(iii) *Define a mapping $f: (S, *) \to (Z, +)$ by*

$$f(a, b) = (a - b), \ \forall \ (a, b) \in S. \text{ Show that } f \text{ is a homomorphism.}$$

Sol. Let (a_1, b_1), (a_2, b_2) and (a_3, b_3) be any three elements of S. Then

$$(a_1, b_1) * [(a_2, b_2) * (a_3, b_3)]$$

$$= (a_1, b_1) * [(a_2 + a_3, b_2 + b_3)$$

$$= [a_1 + (a_2 + a_3), b_1 + (b_2 + b_3)]$$

$$= [(a_1 + a_2) + a_3, (b + b_2) + b_3], \text{ since } + \text{ is associative in } N$$

$$= [(a_1 + a_2), (b_1 + b_2)] * (a_3, b_3)$$

$$= [(a_1, b_1) * (a_2, b_2)] * (a_3, b_3)$$

$\Rightarrow$ $*$ is associative in S and hence $(S, *)$ is a semigroup.

(ii) Since any $(a, b) \in S$, we have

$$(a, b) * (0, 0) = (a + 0, b + 0) = (a, b)$$

and $$(0, 0) * (a, b) = (0 + a, 0 + b) = (a, b).$$

But $0 \notin N \Rightarrow (0, 0) \notin S$, which shows that identity element with respect to binary operation $*$ is S does not exist and hence $(S, *)$ is not a monoid.

(iii) For any $(a_1, b_1), (a_2, b_2) \in S$, we have

$$f[(a_1, b_1) * (a_2, b_2)] = f(a_1 + a_2, b_1 + b_2)$$

$$= (a_1 + a_2) - (b_1 + b_2)$$

$$= (a_1 - b_1) + (a_2 - b_2)$$

$$= f(a_1, b_1) + f(a_2, b_2)$$

$\Rightarrow$ f is a homomorphism.

Self-learning exercise-1

1. Which one of the following is not a semigroup :

(a) $(N, +)$ ***(b)*** $(Z, +)$ ***(c)*** $(Z, -)$ ***(d)*** $(R, +)$

2. Which one of the following is not a monoid :

(a) $(N, +)$ ***(b)*** $(N, \cdot)$ ***(c)*** $(Z, \cdot)$ ***(d)*** $(Q, \cdot)$

3. Consider the set Q of rational numbers, and let $*$ be a binary operation on Q defined by $a * b = a + b - ab \quad \forall\ a, b \in Q$.

(i) Find $3 * 4$, $2 * (-5)$ and $7 * \frac{1}{2}$.

(ii) Is $*$ is commutative ?

(iii) Find the identity element for $*$

7.3 Groups

A monoid $(G, *)$ with identity e, is said to be a **group** if for every $a \in G$ there exists an element $b \in G$ such that $a * b = e = b * a$. b is known as inverse of a and we write $a^{-1} = b$. Note that if b is an inverse of a, then a is an inverse of b.

Thus a group is a nonempty set G together with a binary operation $*$ on G, if the following three properties are satisfied.

1. Associativity

$(a * b) * c = a * (b * c)$ for any elements a, b and c in G.

2. Identity

There is an element $e \in G$, such that $a * e = a = e * a \ \forall \ a \in G$. e is known as identity element is G with respect to binary operation $*$.

3. Inverses

For every $a \in G$, there is an element $b \in G$, called an inverse of a, such that

$$a * b = e = b * a.$$

Observe that if $(G, *)$ is a group, then $*$ is a binary operation on G, so G must be closed under $*$, that is $a * b \in G$ for any elements a and b in G.

A group $(G, *)$ is said to be **Abelian** or **commutative** if $a * b = b * a$ for all elements a and b in G. A group $(G, *)$ is **nonabelian** or **noncommutative**, if there is some pair of elements a and b in G for which $a * b \neq b * a$.

The number of elements in a group $(G, *)$ is called the **order** of the group. It is denoted by $0(G)$ or $|G|$. If G is a group that has a finite number of elements, we say that G is a **finite group,** otherwise the group is **infinite**. For example, the set $\{1, -1\}$ under multiplication is a finite group of order two. On the other hand Z, Q, R and C under addition are all infinite groups.

For an abstract group G, it is convention to write ab for $a * b$. Hence forth, except when necessary, $a * b$ will always be written as ab.

Examples of groups :

1. The set of all integers Z with the operation of ordinary addition is an abelian group. The identity element is 0 (zero) and $-a$ is the additive inverse of a in Z.
2. The set of all nonzero real numbers under the operation of ordinary multiplication is an abelian group. The number 1 is the identity element and an inverse of $0 \neq a$ is $\frac{1}{a}$.
3. The set $G = \{0\}$ is a group with the operation of ordinary addition and the set $G' = \{1\}$ is a group with the operation of ordinary multiplication. $0(G) = 1$ and $0(G') = 1$. In other words we can say that an identity element with respect to given binary operation is a group respect to that binary operation.
4. The set M_2 of all 2×2 matrices with real entries is a group under binary operation addition of matrices. The identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

5. The set M_2 of all 2×2 matrices with real entries is not a group under binary operation of matrix multiplication because inverse do not always exist. However, let G be a subset of 2×2 matrices with a nonzero determinant, that is, nonsingular matrices. Then G is a group under matrix multiplication. The identity element is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and the inverse of $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $A^{-1} = \frac{1}{|A|}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. This is an example of an infinite nonabelian group, since matrix multiplication is noncommutative.
6. The set $\{1, -1, i, -i\}$ where $i = \sqrt{-1}$ is a group under usual multiplication.
7. The set $Z_6 = \{0, 1, 2, 3, 4, 5\}$ is a group under addition modulo 6 but not a group under multiplication modulo 6. Here 1 and 5 have inverses, but the elements 0, 2, 3 and 4 do not have inverses.
8. The set $Z_n = \{0, 1, 2, ..., n-1\}$ for $n \geq 1$ is a group under addition modulo n. For $i > 0$ in Z_n, the inverse of i is $(n - i)$. Z_n is a group under multiplication modulo n if and only it n is prime.

7.3.1 Elementary properties of groups

Theorem 1. *If G is a group, then*

(i) *the identity of G is unique,*

(ii) *for each $a \in G$, a^{-1} is unique.*

Proof : ***(i)*** Let e_1 and e_2 be two identities of G. If e_1 be the identity element of G and $e_2 \in G$, then

$$e_1 * e_2 = e_2 \qquad \text{.....(1)}$$

Again, if e_2 be the identity element of G and $e_1 \in G$, then

$$e_1 * e_2 = e_1 \qquad \text{.....(2)}$$

Since $e_1 * e_2$ is unique element of G, so from (1) and (2) we get $e_1 = e_2$. Thus the identity element in G is unique.

(ii) Suppose b and c are two inverses of $a \in G$. Then

$$a * b = e = b * a \qquad \text{.....(3)}$$

and

$$a * c = e = c * a \qquad \text{.....(4)}$$

From (3), we have

$$a * b = e$$

$$\Rightarrow \quad c * (c * a) = c * e$$

$$\Rightarrow \quad (c * a) * b = c,$$

since $*$ is associative in G and e is the identity in G

$$\Rightarrow \quad e * b = c, \qquad \text{[using (4)]}$$

$$\Rightarrow \quad b = c$$

Hence inverse of $a \in G$ is unique.

Theorem 2. *In a group G*

(i) $(a^{-1})^{-1} = a$ *for all* $a \in G$, *and*

(ii) $(ab)^{-1} = b^{-1}a^{-1}$ *for* $a, b \in G$.

Proof : *(i)* Let e be the identity of G. Then $aa^{-1} = a^{-1}a = e$, and thus, a is the inverse of a^{-1}, that is

$$a = (a^{-1})^{-1}.$$

(ii) Here we have to show that $(ab)^{-1} = b^{-1}a^{-1}$. For this it is sufficient to show that

$$(ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})ab.$$

Now
$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(b(b^{-1}a^{-1})) \\ &= a((bb^{-1})a^{-1}) \\ &= a(ea^{-1}) \\ &= aa^{-1} \\ &= e \qquad \text{.....(1)}\end{aligned}$$

and, similarly

$$(b^{-1}a^{-1})(ab) = e \qquad \text{.....(2)}$$

From (1) and (2), we get

$$(ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})(ab)$$

$$\Rightarrow \quad (ab)^{-1} = b^{-1}a^{-1}$$

Theorem 3. *Let G be a group and let a, b and c be elements of G. Then*

(i) $ab = ac$ *implies* $b = c$ *(left cancellation low)*

(ii) $ba = ca$ *implies* $b = c$ *(right cancellation low)*

Proof : *(i)* Let $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$$\Rightarrow \quad (a^{-1}a)b = (a^{-1}a)c$$

$$\Rightarrow \quad eb = ec$$

$$\Rightarrow \quad b = c$$

(ii) Let $ba = ca \Rightarrow (ab)a^{-1} = (ca)a^{-1}$

$$\Rightarrow \quad b(aa^{-1}) = c(aa^{-1})$$

$$\Rightarrow \quad be = ce$$

$$\Rightarrow \quad b = c.$$

Theorem 4. *In a group G, for* $a, b \in G$ *the equations* $ax = b$ *and* $ya = b$ *have unique solutions in G.*

Proof : The element $x = a^{-1}b \in G$ is a solution of the equation $ax = b$, since

$$a(a^{-1}b) = (aa^{-1})b = eb = b.$$

For uniqueness, suppose that x_1 and x_2 are two solutions of the equation $ax = b$. Then $ax_1 = b$ and $ax_2 = b$. Hence

$$ax_1 = ax_2$$

$\Rightarrow$ $x_1 = x_2$, using left cancellation law.

Similarly we can show that $y = ba^{-1}$ is a unique solution of the equation $ya = b$ in G.

7.3.2 Order of an element

An element $a \in G$ is said to be of **finite order** if there exists a positive integer n such that $a^n = e$. If no such n exist then a is said to be of **infinite order**. The **least positive integer** n such that $a^n = e$ is called the **order** of a, denoted by $0(a)$ or $|a|$. Clearly the identity element of a group is the only element of order one. Note that if $0(a) = n$ and if for some positive integer m, $a^m = e$ then m is multiple of n.

Otherwise $m = nq + r$, $0 < r < n$, $q, r \in Z$ and

then $e = a^m = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$

$\Rightarrow$ $a^r = e$ with $0 < r < n$,

which contradicts the fact that $0(a) = n$.

If $0(a) = n$, then $0(a^{-1}) = n$. In additive group of integers $(Z, +)$, every non-identity element is of infinite order. In multiplicative group $(R - \{0\}, \cdot)$, the number -1 of order 2 and all other non-identity elements are of infinite order.

7.3.3 Cyclic groups

A group G is said to be **cyclic** if there exists an element $a \in G$ such that every element of G can be written in the form a^n for same $n \in Z$. a is known as **generator** of G and we write $G = \langle a \rangle$.

The additive group Z of integers is a cyclic group generated by 1, since $1 \in Z$ and for every integer n, we have $n = n \cdot 1$. We see that -1 is also a generator of Z, since $n = (-n)(-1)$ for every $n \in Z$. Thus $Z = \langle 1 \rangle = \langle -1 \rangle$.

The multiplicative group $G = \{1, w, w^2\}$, where w is non-real cube root of unity, is a cyclic group with w and w^2 as generators.

Theorem 5. *Every cyclic group is abelian, but converse is not necessarily true.*

Proof : Let $G = \langle a \rangle$ be a cyclic group with a as its generator. Also let x, y be any two elements of G. Then $x = a^m$ and $y = a^n$ for some, $m, n \in Z$. Now

$$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$$

$\Rightarrow$ $xy = yx \quad \forall x, y \in G$.

Hence G is abelian. However, converse is not necessarily tree. For example, the additive group R of real numbers is abelian but not cyclic.

7.4 Homomorphism of groups

Let $(G, *)$ and $(G', 0)$ be any two groups. Then a mapping $f: G \to G'$ is called a **group homomorphism,** if

$$f(a * b) = f(a)\, 0\, f(b), \text{ for all } a, b \in G.$$

Or simply $f(ab) = f(a) f(b)$, for all $a, b \in G$.

If f is one-one, then it is called a **monomorphism.** If f is onto, then it is called an **epimorphism.** If f is one-one and onto, *i.e.*, bijective, then it is called an **isomorphism.** A homomorphism of a group into itself is called an **endomorphism.** An isomorphism of a group onto itself is called an **automorphism.**

Two groups G and G' are said to be **isomorphic,** if there exists an isomorphism between them, and then we write $G \cong G'$.

The **Kernel** of a homomorphism f from a group G to a group G' is the set $\{x \in G \mid f(x) = e'\}$ and will be denoted by Ker f. Here, e' is the identity of G'. The image of f, denoted by $f(G)$ and it is the range of the map f. Thus

$$\text{im } (f) = f(G) = \{f(x) \in G' \mid x \in G\}.$$

If $f(G) = G'$, then G' is called a homomorphic image of G.

Theorem 6. *Let f be a homomorphism from a group G into a group G'. Then the following are true :*

(i) *$f(e) = e'$, where e and e' are identities of G and G', respectively,*

(ii) *$f(a^{-1}) = [f(a)]^{-1}$ for all a in G*

Proof : ***(i)*** Since e is the identity element in G and f in a homomorphism from G to G', so we have

$$f(e) = f(ee) = f(e) f(e)$$

$\Rightarrow$ $e' f(e) = f(e) f(e)$, since e' is the identity in G'

$\Rightarrow$ $e' = f(e)$, by right cancellation low

Hence $f(e) = e'$.

(ii) $a \in G \Rightarrow a^{-1} \in G$ such that

$$aa^{-1} = e = a^{-1}a$$

Now $f(e) = f(aa^{-1}) = f(a) f(a^{-1})$

$\Rightarrow$ $e' = f(a) f(a^{-1})$, by (i) $f(e) = e'$

Multiplying both sides on the left by $[f(a)]^{-1}$ and simplifying, we get

$$f(a^{-1}) = [f(a)]^{-1} \quad \text{for every} \quad a \in G.$$

Theorem 7. *Let f be a homomorphism from a group G into a group G'. Then f is a monomorphism if and only if Ker $f = \{e\}$.*

Proof : By definition of Kernel of f, Ker $f = \{x \in G \mid f(x) = e'\}$, where e' is the identity element in G'.

First suppose that f is a monomorphism. Let x be any, element of Ker f. Then

$$f(x) = e'$$

$\Rightarrow$ $f(x) = f(e)$, since $f(e) = e'$

$\Rightarrow$ $x = e$, since f is one-one

$\Rightarrow$ $\text{Ker } f = \{e\}$.

Conversely, suppose that $\text{Ker } f = \{e\}$. Let $x, y \in G$ such that $f(x) = f(y)$.

$\Rightarrow$ $f(x)\,[f(y)]^{-1} = f(y)\,[f(y)]^{-1}$

$\Rightarrow$ $f(x)\,f(y^{-1}) = e'$

$\Rightarrow$ $f(xy^{-1}) = e'$

$\Rightarrow$ $xy^{-1} \in \text{Ker } f$

$\Rightarrow$ $xy^{-1} = e$, since $\text{Ker } f = \{e\}$

$\Rightarrow$ $x = y$

Thus f is one-one and so f is a monomorphism.

Theorem 8. *Any infinite cyclic group G is isomorphic to the additive group $(Z, +)$ of integers.*

Proof : Let $G = \langle a \rangle$ be any infinite cyclic group with a as its generator, *i.e.*,

$$G = \{a^n \mid n \in Z\}.$$

Here G is infinite cyclic group, so the elements of G are all distinct, *i.e.*, $a^m, a^n \in Z$ then $a^m \neq a^n$ if $m \neq n$.

Let us consider a mapping

$$f : G \to Z \text{ defined by}$$

$$f(a^n) = n, \quad \text{for all } a^n \in G.$$

Let a^m, a^n be any two elements of G, then we have

$$f(a^m\, a^n) = f(a^{m+n})$$

$$= m + n$$

$$= f(a^m) + f(a^n).$$

Hence f is a homomorphism. Clearly f is onto, since for any $r \in Z$, there is $a^r \in G$ such that $f(a^r) = r$. f is also one-one, since for any $a^r, a^s \in G$ such that

$$f(a^r) = f(a^s) \Rightarrow r = s \Rightarrow, a^r = a^s.$$

Hence f is an isomorphism of G onto Z and consequently $G \cong Z$.

Ex.1. *Let $(R_0, \cdot)$ be the multiplicative group of non-zero real numbers, then show that the mapping $f : R_0 \to R_0$ defined by $f(2) = x^4$, for all $x \in R_0$ is a homomorphism. Also find its Kernel.*

Sol. Let x, y be any two elements of R_0, then

$$f(xy) = (xy)^4$$

$$= x^4\, y^4$$

$$= f(x)\, f(y).$$

Hence f is a homomorphism from R_0 to R_0.

$$\text{Ker } f = \{x \in R_0 \mid f(x) = 1\}$$
$$= \{x \in R_0 \mid x^4 = 1\}$$
$$= \{1, -1\}$$

Hence $\text{Ker } f = \{1, -1\}$.

Ex.2. *If f is a homomorphism of a group G to a group G' with Kernel K, then prove that for any $a, b \in G$;*

$$f(a) = f(b) \text{ if an only if } ab^{-1} \in K.$$

Sol. For any $a, b \in G$,

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

$\Leftrightarrow$ $f(a) f(b^{-1}) = e'$, where e' is the identity of G

$\Leftrightarrow$ $f(ab^{-1}) = e'$

$\Leftrightarrow$ $ab^{-1} \in K$.

Ex.3. *If m is fixed positive integer, then show that the mapping $f : (Z, +) \to (mZ, +)$ defined by $f(x) = mx$, for all $x \in Z$ is an isomorphism.*

Sol. Let x, y be any two elements of Z. Then

$$f(x + y) = m(x + y)$$
$$= mx + my$$
$$= f(x) f(y).$$

Hence f is a homomorphism. f is onto, because for any $my \in mZ$ there exists $y \in Z$ such that $f(y) = my$. f is also one-one, since

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

$\Rightarrow$ $x = y$.

Hence f is an isomorphism from Z onto mZ and consequently $Z \cong mZ$.

Ex.4. *The mapping $f : R \to R^+$ defined by $f(x) = e^x$, for all $x \in R$ is an isomorphism from the group $(R, +)$ to the group $(R^+, \cdot)$.*

Sol. Let x, y be any two elements of R. Then

$$f(x + y) = e^{x+y} = e^x e^y, \quad \text{for all} \quad x, y \in R.$$

$\Rightarrow f$ is a homomorphism.

f is onto, since for every $x \in R^+$, there exists $\log x \in R$ such that

$$f(\log x) = e^{\log x} = x.$$

We know that for any $x, y \in R$

$$x \neq y \Rightarrow e^x \neq e^y$$
$$\Rightarrow f(x) \neq f(y)$$
$$\Rightarrow f \text{ is one-one.}$$

Hence f is an isomorphism and consequently $(R, +) \cong (R^+, \cdot)$.

Self-learning exercise-2

1. Which one of the following is not a semigroup ?

   1. $(Z, +)$ 2. $(Q - \{0\}, \cdot)$ 3. $(\{1, -1\}, \cdot)$ 4. $(N, \cdot)$

2. Which one of the following is a group ?

   1. $(Z, -)$ 2. $(R, \cdot)$

   3. $(Z_2 = \{0, 1\}, +_2)$ 4. $(G = \{-1, 1\}, +)$

3. In the group $(Z_5 = \{0, 1, 2, 3, 4\}, +_5)$, inverse of 2 is :

   1. 0 2. 3 3. 4 4. 1

7.5 Summary

In this unit we have discussed binary operations and their properties. We have also discussed about groupoids, quasigroups, semigroups, monoids, free semigroup, free monoids, and results related to these topics. In the end of the unit we have explained groups and their elementary properties.

7.6 Answers to self-learning exercise

Self-learning exercise-1

1. (c) 2. (a)

3. *(i)* $3 * 4 = -5, 2 * (-5) = 7$ and $7 * \frac{1}{2} = 4$

   (ii) yes *(iii)* 0 (zero)

Self-learning exercise-2

1. (4) 2. (3) 3. (2)

7.7 Exercises

1. Which of the following subset of the set N of natural numbers are closed under the operation of multiplication ?

   (i) $A = \{1\}$

   (ii) $B = \{1, 2\}$

   (iii) $C = \{x \mid x \text{ is even natural number}\}$

   (iv) $D = \{x \mid x \text{ is prime number}\}$

   (v) $E = \{x \mid x \text{ is odd natural number}\}$ **[Ans.** Sets A, C and E are closed for multiplication]

2. Which of the above subsets of N are closed under the operation of addition ?

   [Ans. Set C is closed under addition]

3. Let S be a nonempty set with binary operation $*$ defined by $a * b = a$ for all $a, b \in S$. Show that S is a semigroup but it is not a monoid.

4. Show that set $S = \{1, 2, 3, 6\}$ is a monoid under the binary operation $*$ defined by $a * b =$ greatest common divisor of a and $b = gcd\,(a, b)$.

5. Consider the binary operation $*$ defined on the set $A = \{a, b, c, d\}$ by the following table :

$*$	a	b	c	d
a	a	c	b	d
b	d	a	b	c
c	c	d	a	a
d	d	b	a	c

Compute :

(i) $c * d$ and $d * c$

(ii) $b * d$ and $d * b$

(iii) $a * (b * c)$ and $(a * b) * c$

(iv) Is $*$ commutative, associative ? **[Ans.** *(i) a, a (ii) c, d (iii) c, a (iv)* neither]

6. Prove that the intersection of two submonoid of a monoid $(S, *)$ is a submonoid of $(S, *)$.

7. Let $A = \{a, b, c\}$ and consider the semigroup $(A^*, \cdot)$, where $\cdot$ is the operation of catenation. If $\alpha = abac$, $\beta = cba$ and $\gamma = babc$, commute

(i) $(\alpha \cdot \beta) \cdot \gamma$ *(ii)* $\gamma \cdot (\alpha \cdot \alpha)$ *(iii)* $(\gamma \cdot \beta) \cdot \alpha$

[Ans. *(i) abaccba babc (ii) babc abac abac (iii) babc cba abac*]

8. Prove that the set Z of all integers under the binary operation $*$ defined by $a * b = a + b + 1$ $\forall\, a, b \in Z$ is an abelian group.

9. Let G be the set of rational (real) numbers other than 1. Prove that G is an abelian group for the operation $*$ defined as

$$a * b = a + b - ab \quad \forall\, a, b \in G.$$

10. Show that the set Q^+ of the positive rational numbers forms an abelian group for the composition $*$ defined as

$$a * b = \frac{ab}{2} \quad \forall\, a, b \in Q^+.$$

□□□

UNIT 8 : Subgroups

Structure of the Unit

8.0 Objectives

After reading this unit you will be able to understand about subgroups, cyclic subgroups, cosets, permutation groups, alternating group A_n, normal subgroups and quotient groups.

8.1 Introduction

In this unit we begin by defining subgroups and their properties. After this we proceed with the definitions of complex of a group, cyclic subgroups, cosets, permutation group and some examples and results related to these topics. In the end of the unit we define normal subgroups, examples of normal subgroups, quotient group and elementary properties of normal subgroups.

8.2 Subgroups

A nonempty subset H of a group G is called a subgroup of G if H itself is a group under the binary operation defined in G.

We know that if e is the identity element in a group G, then $H = \{e\}$ is a group under the binary operation defined in G. $H = \{e\}$ is known as trivial subgroup of G. The group G itself is a subgroup of G, and any subgroup $H \neq G$ is called a proper subgroup of G. Thus every group G whose order > 1 has at least two subgroups $H = \{e\}$ and $H = G$.

The set E of even integers is a subgroup of the additive group $(Z, +)$ of integers but the set N of natural numbers is not a subgroup of $(Z, +)$, since additive identity 0 (zero) $\notin N$. The set $H = \{1, -1\}$ is a subgroup of the multiplicative group $< G = \{1, -1, i, -i\}, >$ but the set $K = \{-1\}$ is not a subgroup of G, since multiplication is not a binary operation in K.

From above we see that if H is a subgroup of G, then H is closed under the operation of G. However, this condition alone is not sufficient to guarantee that H is a subgroup of G.

Not that the identity of a subgroup is the same as that of the group. The inverse of any element of a subgroup is the same as the inverse of the element regraded as a member of the group. The order of any element of a subgroup is the same as the order of that element regarded as a member of the group. Every subgroup of an abelian group is abelian.

The following theorem gives a convenient condition to test when a subset of a given group is a subgroup of that group.

Theorem 1. *A nonempty subset H of a group G is a subgroup of G if and only if ab^{-1} is in H whenever a and b are in H.*

Proof : First suppose that H is a subgroup of G. If $a \in H$ and $b \in H$, then b^{-1} H. Since H is a subgroup of G, so $a \in H$, $b^{-1} \in H \Rightarrow ab^{-1} \in H$.

Conversely suppose that H is a non-empty subset of G such that $ab^{-1} \in H$, whenever $a \in H$ and $b \in H$. Since H is nonempty, so let $a \in H$. By given condition $a \in H$, $b = a \in H \Rightarrow aa^{-1} = e \in H$. Again by given condition $e \in H$, $a \in H \Rightarrow ea^{-1} = a^{-1} \in H$, which shows that every element of H is invertible. Finally let $a, b \in H$. Now $b \in H \Rightarrow b^{-1} \in H$. By given condition $a \in H$, $b^{-1} \in H \Rightarrow a(b^{-1})^{-1} = ab \in H$, which shows that H is closed for the binary composition defined in G. Since binary operation is associative in G, so it is associative in H. Hence H is a subgroup of G.

Note that if addition is binary operation in G, then H is a subgroup of G if and only if $(a - b)$ is in H whenever a and b are in H.

Theorem 2. *A nonempty subset H of a finite group G is a subgroup of G if and only if $ab \in H$ whenever $a, b \in H$.*

Proof : First suppose that H is a subgroup of G. If $a \in H$ and $b \in H$, then obviously $ab \in H$.

Conversely, suppose that $ab \in H$ whenever $a, b \in H$. Now we have to show that H is a subgroup of G. For this it is sufficient to show that $e \in H$ and for each $a \in H$, its inverse a^{-1} belongs to H. Let a be an arbitrary element of H. Then, by the repeated use of the given condition, it follows that $a, a^2, a^3, ..., a^n, ...$ are all belong to H. Since H is a finite set, at beast two of them coincide. Let $a^m = a^n$, for some $m \neq n$ and suppose $m > n$. Now

$$a^m = a^n \Rightarrow a^m a^{-n} = a^n a^{-n}$$

$$\Rightarrow a^{m-n} = e,$$

where e is the identity in G. Thus $a^{m-n} = e \in H$. Also

$a\, a^{(m-n)-1} = a^{(m-n)-1}\, a = a^{m-n} = e$ and hence $a^{-1} = a^{(m-n)-1} \in H$, which shows that every element of H is invertible. Hence H is a subgroup of G.

Theorem 3. *If H and K are subgroups of a group G, then $H \cap K$ is also a subgroup of G.*

Proof : Since H and K are subgroups of G, so $e \in H \cap K$ and hence $H \cap K \neq \phi$. Let a, b be any two elements of $H \cap K$. Then $a, b \in H$ and $a, b \in K$. Since H and K are subgroups of G, $ab^{-1} \in H$ and $ab^{-1} \in K$ and hence $ab^{-1} \in H \cap K$. Thus $a, b \in H \cap K$ implies $ab^{-1} \in H \cap K$ and hence $H \cap K$ is a subgroup of G.

Corollary : The intersection of an arbitrary collection of subgroups of a group is again a subgroup of the group.

Note that the union of two subgroups of a group is not necessarily a subgroup of the same group. For example, consider the additive group $(Z, +)$ of integers. Let

$H = \{2n \mid n \in Z\}$ and $K = \{3m \mid m \in Z\}$, then clearly H and K are subgroups of $(Z, +)$ but

$H \cup K = \{...., -4, -3, -2, 0, 2, 3, 4, 6, 8, 10, ...\}$ is not a subgroup of $(Z, +)$ because $2, 3 \in H \cup K$ but $2 + 3 = 5 \notin H \cup K$, that is, $H \cup K$ is not closed under binary operation defined in Z.

8.2.1 Complex of a group :

A nonempty subset H of a group G is called a complex of G. If H and K are two complex of a group G, then their product, denoted by HK, is defined as

$HK = \{ hk \mid h \in H, k \in K\}$.

Obviously $HK \subset G$, so it is also a complex of G. The inverse of a complex H is denoted by H^{-1} and $H^{-1} = \{h^{-1} \mid h \in H\}$. It can be easily verified that $(HK)^{-1} = K^{-1} H^{-1}$.

Theorem 4. *If H is a subgroup of a group G, then $H^{-1} = H$. However, the converse is not necessarily true.*

Proof : Let H be a subgroup of G. Now we have to show that $H^{-1} = H$. Let h be any element of H. Since H is a subgroup of G, so $h \in H$

$$\Rightarrow \quad h^{-1} \in H$$

$$\Rightarrow \quad (h^{-1})^{-1} = h \in H^{-1}$$

$$\Rightarrow \quad H \subseteq H^{-1} \qquad .....(1)$$

Again, let x be any element of H^{-1}, then $x = h^{-1}$ for some $h \in H$. Since H is a subgroup of G, so $h \in H \Rightarrow x = h^{-1} \in H$. Thus

$$h^{-1} \in H^{-1} \Rightarrow h^{-1} \in H \Rightarrow H^{-1} \subseteq H \qquad \text{.....(2)}$$

from (1) and (2) we get $H^{-1} = H$.

However, the converse of above is not necessarily true because if we consider the multiplicative group $G = \{1, -1\}$ and its complex $H = \{-1\}$, then $H^{-1} = \{-1\} = H$. But H is not a subgroup of G, since H is not closed for multiplication.

3.2.2 Cyclic subgroups :

A subgroup H of a group G is said to be a **cyclic subgroup** if there exists an element $a \in H$ such that every element of H can be written in the form a^n for some $n \in Z$. The element a is called **generator** of H and we write $H = < a >$.

For example, the subgroup $H = \{1, -1, i, -i\}$ is a cyclic subgroup of the multiplicative group $(C_o, \cdot)$ of nonzero complex members. i and $-i$ are two generators of H.

Again, let G be a cyclic group of order 6, generated by a, that is $G = < a > = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$. Then $H = < a^2 > = \{a^2, a^4, a^6 = e\}$ and $K = \{a^3, a^6 = e\}$ are cyclic subgroups of G generated by a^2 and a^3 respectively.

8.2.3 Cosets and Lagrange's theorem :

Let H be a subgroup of a group G. Then for $a \in G$, the set $Ha = \{ha \mid h \in H\}$ is called a **right coset** of H in G. The element $a \in G$ is called a representative of the coset. It is a subset of G. Similarly the set $aH = \{ah \mid h \in H\}$ is called a left coset of H in G. It in also a subset of G. If the group G is abelian, than $aH = Ha$ for all $a \in G$.

Note that the subgroup H itself is a right as well as a left coset, determined by the identity element $e \in G$, since

$$He = H = eH.$$

Further, since $e \in H \Rightarrow a = ea \in Ha$ and $a = ae \in aH$. Thus for all $a \in G$, $a \in aH$ and $a \in Ha$. If the group operation is addition (+), then a right coset of H in G is denoted as

$$H + a = \{h + a \mid h \in H\}$$

and a left coset of H in G is denoted as $a + H = \{a + h \mid h \in H\}$.

Ex.1. *Consider the multiplicative group* $< G = \{1, -1, i, -i\}, \bullet >$. *Let* $H = \{1, -1\}$ *be a subgroup of G. Since G is abelian, so each left cost of H in G is also a right coset of H in G. Now*

$$H \cdot 1 = \{1 \times 1, -1 \times 1\} = \{1, -1\} = 1 \cdot H = H$$

$$H \cdot (-1) = \{1 \times (-1), -1 \times (-1)\} = \{-1, 1\} = (-1) \cdot H = H$$

$$H \cdot i = \{i, -i\} = i \cdot H$$

$$H \cdot (-i) = \{-i, i\} = (-i) \cdot H$$

From above we see that $H \cdot 1 = H \cdot (-1)$ and $H \cdot i = H \cdot (-i)$. Thus $H \cdot 1$ and $H \cdot (i)$ are only two distinct cosets of H in G such that $G = H \cup Hi$ and $H \cdot \cap H \cdot i = \phi$.

Ex.2. *Consider the additive group $(Z, +)$ of integers. Let $H = \{3x \mid x \in Z\}$, then H is a subgroup of G. Since $(Z, +)$ is an abelian group, so each left coset of H in G is also a right coset of H in G. Now*

$$H = \{..., -12, -9, -6, -3, 0, 3, 6, 9, 12, ...\}$$

$$H + 0 = 0 + H = \{....., -12, -9, -6, -3, 0, 3, 6, 9, 12, ...\} = H$$

$$H + 1 = 1 + H = \{....., -8, -5, -2, 1, 4, 7, 10, ...\}$$

$$H + 2 = 2 + H \{....., -7, -4, -1, 2, 5, 8, 11, ...\}$$

$$H + 3 = 3 + H \{....., -6, -3, 0, 3, 6, 9, 12, ...\} = H + 0$$

$$H + 4 = 4 + H \{....., -5, -2, 1, 4, 7, 10, ...\} = H + 1$$

$$H + 5 = 5 + H \{....., -4, -1, 2, 5, 8, 11, ...\} = H + 2$$

From above we see that

$$H = H + 0 = H + 3 = H + 6 = H + 9 = ...$$

$$H + 1 = H + 4 = H + 7 = H + 10 = ...$$

$$H + 2 = H + 5 = H + 8 = H + 11 = ...$$

Thus $H + 0 = H$, $H + 1$ and $H + 2$ are only there distinct cosets of H in $(Z, +)$ such that

$$Z = H \cup (H + 1) \cup (H + 2) \text{ and } H \cap (H + 1) \cap (H + 2) = \phi.$$

Ex.3. *Let $H = \{0, 3\}$ be a subgroup of the group $< Z_6 = \{0, 1, 2, 3, 4, 5\}, +_6 >$ under addition moduls 6. Then the cosets of H in Z_6 are*

$$H +_6 0 = 0 +_6 H = \{0, 3\} = H +_6 3 = H$$

$$H +_6 1 = 1 +_6 H = \{1, 4\} = H +_6 4$$

$$H +_6 2 = 2 +_6 H = \{2, 5\} = H +_6 5.$$

Thus $H +_6 0 = H$, $H +_6 1$ and $H +_6 2$ are only three distinct cosets of H is Z_6 such that

$$Z_6 = H \cup (H +_6 1) \cup (H +_6 2) \quad \text{and} \quad H \cap (H +_6 1) \cap (H +_6 2) = \phi.$$

8.2.4 Properties of cosets :

Theorem 5. *If H is a subgroup of a group G, then $Ha = H$ if and only if $a \in H$.*

Proof : First suppose that $Ha = H$, then

$$a = ea \in Ha = H, \text{ i.e. } a \in H.$$

Conversely, suppose that $a \in H$. Now we have to show that $Ha = H$. Let x be any element of Ha. Then $x = ha$ for some $h \in H$. Since H is a subgroup of G, so $h \in H$, $a \in H$ implies $ha \in H$ and hence $x \in H$. Thus

$$Ha \subseteq H \qquad .....(1)$$

Again, let y be any element of H. Then

$$y = ye = ya^{-1}\, a = (ya^{-1})\, a \in Ha, \text{ since } ya^{-1} \in H$$

$$\Rightarrow \qquad H \subseteq Ha \qquad \text{.....(2)}$$

From (1) and (2) we get $Ha = H$.

Theorem 6. *Let H be a subgroup of a group G and let $a, b \in G$. Then $Ha = Hb$ if and only if $ab^{-1} \in H$ and $aH = bH$ if and only if $a^{-1} b \in H$.*

Proof : Let $Ha = Hb$, then $a = ea \in Ha = Hb$.

$$a \in Hb \Rightarrow a = hb \text{ for some } h \in H.$$

$$\Rightarrow \qquad ab^{-1} = h \in H.$$

Conversely, let $ab^{-1} \in H$. Then for any $ha \in Ha$, we have

$$ha = hab^{-1}b = h\,(ab^{-1})\, b \in Hb, \text{ since } h\,(ab^{-1}) \in H$$

$$\Rightarrow \qquad Ha \subseteq Hb. \text{ Similarly we can show that } Hb \subseteq Ha \text{ and hence } Ha = Hb.$$

Theorem 7. *Let H be a subgroup of a group G. Then*

(i) G is the union of the right (respectively left) cosets of H in G.

(ii) Two right (respectively left) cosets of H in G are either identical or disjoint.

Proof : We prove the theorem for right cosets of H in G. Analogous arguments apply to left coset.

(i) Since $Ha \subseteq G$ for all $a \in G$, therefore

$$\bigcup_{a \in G} Ha \subseteq G \qquad \text{.....(1)}$$

For any $a \in G$, $a = ea \in Ha$

As a varies in G, from above we get

$$G \subseteq \bigcup_{a \in G} Ha \qquad \text{.....(2)}$$

From (1) and (2), we get

$$G = \bigcup_{a \in G} Ha.$$

(ii) Let Ha and Hb be two right cosets of H in G such that $Ha \cap Hb \neq \phi$. Then there exists x such that $x \in Ha \cap Hb$, so that $x \in Ha$ and $x \in Hb$. Now $x \in Ha$ and $x \in Hb$ implies that $x = h_1 a = h_2 b$ for $h_1, h_2 \in H$. Thus

$$h_1 a = h_2 b \Rightarrow a = h_1^{-1} h_2 b$$

$$\Rightarrow Ha = Hh_1^{-1} h_2 b$$

$$\Rightarrow Ha = H\left(h_1^{-1} h_2\right) b$$

$$\Rightarrow Ha = Hb, \text{ since } h_1^{-1} h_2 \in H$$

Hence $Ha \cap Hb \neq \phi \Rightarrow Ha = Hb$.

Theorem 8. [*Lagrange's theorem*] *Let G be a finite group and H be a subgroup of G. Then the order of H divides the order of G.*

Proof : At first we shall show that $o(H) = o(Ha)$ for all $a \in G$. Let us consider a mapping $f: H \to Ha$ defined by $f(h) = ha \ \forall \ h \in H$. f is onto, since for any $ha \in Ha$, $h \in H$ such that $f(h) = ha$. f is also one-one

Since for $h_1, h_2 \in H$ $\quad f(h_1) = f(h_2) \Rightarrow h_1 a = h_2 a$

$\Rightarrow h_1 = h_2$, by right cancellation law.

Hence $o(H) = o(Ha) \ \forall \ a \in G$.

Since G is a finite group, the number of right (respectively left) cosets of H in G is finite. Let $\{Ha_1, Ha_2, ..., Ha_r\}$ be the set of all distinct right cosets of H in G. Then by theorem 7 we have

$$G = Ha_1 \cup Ha_2 \cup ..... \cup Ha_r.$$

Since all these cosets are pairwise disjoint, hence

$$\begin{aligned} o(G) &= o(Ha_1) + o(Ha_2) + ... + o(Ha_r) \\ &= o(H) + o(H) + ... + o(H), \ r \text{ times} \\ &= r\, o\,(H) \end{aligned}$$

Hence $o(H)$ divides $o(G)$.

Index of a subgroup :

Let H be a subgroup of a group G. The number of distinct right (left) cosets of H in G is called the index of H in G and is denoted by $[G : H]$. When G is finite by Lagrange's theorem we have

$$[G:H] = \frac{o(G)}{o(H)}.$$

For example, index of subgroup $H = \{1, -1\}$ of multiplicative group $G = \{1, -1, i, -i\}$ is two.

8.2.5 Some important examples :

Ex.1. *Let G be an abelian group with identity e. Then $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G.*

Sol. Since $e^2 = e$, so $e \in H$ and hence $H \neq \phi$. Let a, b be any two elements of H. Then $a^2 = e$ and $b^2 = e$. Now

$$\begin{aligned} (ab^{-1})^2 &= (ab^{-1})\,(ab^{-1}) \\ &= a\,(b^{-1}\,a)\,b^{-1} \\ &= a\,(ab^{-1})\,b^{-1}, \quad \text{since } G \text{ is abelian} \\ &= a^2\,(b^{-1})^2 \\ &= a^2\,(b^2)^{-1} \\ &= e\,e^{-1} = e \end{aligned}$$

$\Rightarrow \quad ab^{-1} \in H$ and have H is a subgroup of G.

Ex.2. *Prove that those elements of a group G which commute with a fixed element a of G, forms a subgroup of G.*

Sol. Let $N(a)$ be a collection of all those elements of G which commute with a, that is

$$N(a) = \{x \in G \mid ax = xa\}.$$

Now we have to show that $N(a)$ is a subgroup of

$$G.\ e \in G \Rightarrow ea = ae$$
$$\Rightarrow e \in N(a)$$
$$\Rightarrow N(a) \neq \phi.$$

Let $x, y \in N(a)$, then $ax = xa$ and $ay = ya$

$$ax = xa \Rightarrow x^{-1}(ax)\, x^{-1} = x^{-1}(xa)\, x^{-1}$$
$$\Rightarrow x^{-1}\, a\, (xx^{-1}) = (x^{-1}x)\, ax^{-1}$$
$$\Rightarrow x^{-1}ae = eax^{-1}$$
$$\Rightarrow x^{-1}\, a = ax^{-1}$$
$$\Rightarrow x^{-1} \in N(xa).$$

Now,

$$a(xy^{-1}) = (ax)\, y^{-1}$$
$$= (xa)\, y^{-1}$$
$$= x\, (ay^{-1})$$
$$= x\, (y^{-1}\, a)$$
$$= (xy^{-1})\, a$$

$\Rightarrow \quad xy^{-1} \in N(a)$

Thus $x,\ y \in N(a) \Rightarrow xy^{-1} \in N(a)$ and hence $N(a)$ is a subgroup of G.

Note that $N(a)$ is known as **normalizer** of a in G.

Ex.3. *Show that the elements in a group G which commute with every element of G forms a subgroup of G .*

Sol. Let $Z(G)$ be a collection of all those elements of G that commute with every element of G, that is

$$Z(G) = \{x \in G \mid xg = gx \text{ for all } g \text{ in } G\}.$$

Now we have to show that $Z(G)$ is a subgroup of G. $e \in G \Rightarrow eg = ge\ \forall\ g \in G$ and hence $Z(G) \neq \phi$ as $e \in Z(G)$. Let $x, y \in Z(G)$, then

$xg = gx$ and $yg = gy\ \forall\ g\ G.$

$$xg = gx \Rightarrow x^{-1}\, (xg)\, x^{-1} = x^{-1}\, (gx)\, x^{-1}$$
$$\Rightarrow (x^{-1}\, x)\, gx^{-1} = x^{-1}\, g\, (xx^{-1})$$
$$\Rightarrow egx^{-1} = x^{-1}\, ge$$

$$\Rightarrow gx^{-1} = x^{-1} g \ \forall g \in G$$
$$\Rightarrow x^{-1} \in Z(G).$$

Now,

$$\begin{aligned}(xy^{-1})\, g &= x\,(y^{-1} g)\\ &= x\,(gy^{-1})\\ &= (xg)\, y^{-1}\\ &= (gx)\, y^{-1}\\ &= g\,(xy^{-1})\end{aligned}$$

$(xy^{-1})\, g = g\,(xy^{-1}) \ \forall \ g \in G$ and hence $xy^{-1} \in Z(G)$. Thus $x, y \in Z(G) \Rightarrow xy^{-1} \in Z(G)$ and consequently $Z(G)$ is a subgroup of G.

Note that $Z(G)$ is known as **centre of G**. If G is a commutative group, than $Z(G)$ is G.

Ex.4. *Let Z be the group of integers under the operation of addition, and let* $H = \{mx \mid x \in Z\}$, *where m is a fixed positive integer. Show that H is a subgroup of G.*

Sol. $0 \in Z \Rightarrow m \cdot 0 = 0 \in H$

$$\Rightarrow H \neq \phi.$$

Let a, b be any two elements of H. Then $a = mx_1$ and $b = mx_2$ for some $x_1, x_2 \in Z$.

Now
$$\begin{aligned}a - b &= mx_1 - mx_2\\ &= m\,(x_1 - x_2)\\ &= mx_3, \quad \text{where} \quad x_3 = x_1 - x_2 \in Z\end{aligned}$$

$$\Rightarrow \quad a - b \in H.$$

Thus $a, b \in H \Rightarrow a - b \in H$ and hence H is a subgroup of Z.

Ex.5. *Let H be a subgroup of a group G. If index of H in G is two, then prove that* $Ha = aH$ *for all* $a \in G$.

Sol. Since index of H in G is two, so H has only two right (left) cosets in G. Again, since H itself is a right as well as left coset of H in G, so let $G = H \cup Ha$, where $H \cap Ha = \phi$. Again, if $G = H \cup bH$, where $H \cap bH = \phi$, then $Ha = bH$. Now $a \in Ha$ and $Ha = bH$, so $a \in bH$. $a \in aH$, $a \in bH \Rightarrow bH = aH$, since cosets are either identical or disjoint. Hence $Ha = aH$ for all $a \in G$.

Ex.6. *Let G be a finite group, H and K are subgroups of G such that* $K \subset H$. *Show that*

$$[G : K] = [G : H]\,[H : K].$$

Sol. Since H and K are subgroups of a finite group G, so

$$[G : H] = \frac{o(G)}{o(H)} \quad \text{and} \quad [G : K] = \frac{o(G)}{o(K)}.$$

Again, since $K \subset H$, so K is a subgroup of a finite group H and hence

$$[K : H] = \frac{o(K)}{o(H)}$$

Now $$[G:H][H:K] = \frac{o(G)}{o(H)}\frac{o(H)}{o(K)}$$

$$= \frac{o(G)}{o(K)} = [G:K]$$

Self-learning exercise-1

1. The set of even integers is a subgroup of the additive group of integers (Z, +). [True/False]
2. The set $\{1, i\}$ is a subgroup of the multiplicative group $< G = \{1, -1, i, -i\}, \cdot >$. [True/False]
3. The set $H = \{0, 2\}$ is a subgroup of the group $< Z_4 = \{0, 1, 2, 3\}, +_4 >$. [True/False]
4. The set of natural numbers is a subgroup of the multiplicative group $(Q_0, \cdot)$ of non-zero rational numbers. [True/False]
5. If $G = < a > = \{a, a^2, a^3, a^4 = 1\}$ and $H = \{1, a^2\}$ is a subgroup of G. Find all the cosets of H in G.

8.3 Permutation group

Let A be a nonempty set. Then a permutation of A is a function from A to A which is both one-one and onto. It A is a finite set of n elements, *i.e.*

$$A = \{a_1, a_2, \ldots\ldots, a_n\}$$

and f is a permutation on A, then $f(a_1), f(a_2), \ldots\ldots, f(a_n)$ are unique elements of A, then we write

$$f = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ f(a_1) & f(a_2) & \ldots & f(a_n) \end{pmatrix}$$

For example, $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ is a permutation on the set $A = \{1, 2, 3, 4\}$ such that $f(1) = 3, f(2) = 4, f(3) = 1$ and $f(4) = 2$.

Since composite of two one-one and onto functions defined on a set is again a one-one and onto function, so we can compose two permutations defined on a set. For example, if

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ and } g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

are two permutations on a set A = {1, 2, 3, 4}, then

$$(fog)(1) = f(g(1)) = f(1) = 3$$
$$(fog)(2) = f(g(2)) = f(3) = 1$$
$$(fog)(3) = f(g(3)) = f(4) = 2$$
$$(fog)(4) = f(g(4)) = f(2) = 4.$$

Thus,

$$(fog) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

and similarly $$gof = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

We observe that, $fog \neq gof$, in general. Let A be a nonempty set, and S_A be the collection of all permutations of A, then S_A is a group under permutation multiplication as binary operation. The identity function I_A is the identity element because for every $\sigma \in S_A, \sigma o I_A = \sigma = I_A o \sigma$. Since for each $\sigma \in S_A$, σ is a bijection from A to itself, so σ^{-1} is a bijection from A to itself and σ^{-1} is a permutation of A such that $\sigma o \sigma^{-1} = I_A = \sigma^{-1} o \sigma$.

If A is a finite set $\{1, 2, ..., n\}$, then the group of all permutations of A is the **symmetric group** on n symbols, and is denoted by S_n. The group S_n is called symmetric group because for $n = 3, 4$ etc. elements of S_n can be interpreted as symmetries of a triangle, a square, etc. S_n is non-abelian if $n > 2$. $o(S_n) = \lfloor n$.

***Ex.*1.** *Symmetric group* S_3.

Let S_3 denote the set of all one-one and onto functions from $\{1, 2, 3\}$ to itself. Then S_3 is a group under permutation multiplication as binary operation. All the six elements of S_3 are

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

We can construct an operation table as :

o	σ_0	σ_1	σ_2	τ_1	τ_2	σ_3
σ_0	σ_0	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	σ_0	τ_2	τ_3	τ_1
σ_2	σ_2	σ_0	σ_1	τ_3	τ_1	τ_2
τ_1	τ_1	τ_3	τ_2	σ_0	σ_2	σ_1
τ_2	τ_2	τ_1	τ_3	σ_1	σ_0	σ_2
τ_3	τ_3	τ_2	τ_1	σ_2	σ_1	σ_0

Above table shows that S_3 is a group under permutation multiplication. Since the table is not symmetric about leading diagonal, S_3 is a non-abelian group.

8.3.1 Cyclic permutation (cycles) :

Let A be a non-empty set. A permutation σ on A is said to be a **cyclic permutation** if there exists a finite subset $\{a_1, a_2, ..., a_r\}$ of A such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3, ..., \sigma(a_{r-1}) = a_r$, $\sigma(a_r) = a_1$ and $\sigma(a) = a$ if $a \in A$ but $a \notin \{a_1, a_2, ..., a_r\}$. We denote σ by the symbol $\sigma = (a_1, a_2, ..., a_r)$.

The number of elements that appear in such a representation of a cyclic permutation is called its length. Thus length of σ defined above is r. If r is length of a cycle σ, then order of σ is r. Any cycle of length one is called the **identity permutation.** A cyclic of length two is called a **transposition** and every transposition is inverse of itself.

For example, if $A = \{1, 2, 3, 4, 5, 6\}$, then $\sigma_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1)(2)(3)(4)(5)$ is identity permutation on A.

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 4 & 6 \end{pmatrix} = (4,5)$$

is a transposition and

$$\sigma_2 = (1,3,4,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 1 & 6 \end{pmatrix}$$

is a cyclic permutation of length four.

8.3.2 Even and odd permutations :

The sign of a permutation $\sigma \in S_n$, denoted by $\in(\sigma)$, is defined as the product

$$\prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{(i-j)}.$$

The value of $\in(\sigma)$ is either 1 or -1. A permutation $\sigma \in S_n$ is called an even permutation if $\in(\sigma) = 1$, and an odd permutation if $\in(\sigma) = -1$. For example, if

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Then

$$\in(\sigma_1) = \frac{\sigma(1)-\sigma(2)}{1-2} \times \frac{\sigma(1)-\sigma(3)}{1-3} \times \frac{\sigma(2)-\sigma(3)}{2-3}$$

$$= \frac{(3-1)}{(1-2)} \times \frac{(3-2)}{(1-3)} \times \frac{(1-2)}{(2-3)} = \frac{2 \times 1 \times -1}{-1 \times -2 \times -1} = 1$$

$\Rightarrow$ σ_1 is an even permutation.

$$\in(\sigma_2) = \frac{\sigma(1)-\sigma(2)}{1-2} \times \frac{\sigma(1)-\sigma(3)}{1-3} \times \frac{\sigma(2)-\sigma(3)}{2-3}$$

$$= \frac{(1-3)}{(1-2)} \times \frac{(1-2)}{(1-3)} \times \frac{(3-2)}{(2-3)}$$

$$= \frac{-2 \times -1 \times 1}{-1 \times -2 \times -1} = -1$$

$\Rightarrow$ σ_2 is an odd permutation.

Note that the product of two even permutations is even, the product of two odd permutations is even and product of one even and other odd permutation is an odd permutation.

8.3.3 Alternating group A_n:

The set of all even permutations of n distinct objects is denoted by A_n and it is a group with respect to permutation multiplication as binary operation. It is called the **alternating group** of degree n and $o(A_n) = \frac{\lfloor n}{2}$. For example on the set $\{1, 2, 3\}$,

$$A_3 = \left\{ \sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

is an alternating group of order 3. It is a subgroup of S_3. We can construct an operation table for A_3 as :

o	σ_0	σ_1	σ_2
σ_0	σ_0	σ_1	σ_2
σ_1	σ_1	σ_2	σ_0
σ_2	σ_2	σ_0	σ_1

Here σ_0 is the identity elements, $\sigma_1^{-1} = \sigma_2$ and $\sigma_2^{-1} = \sigma_1$. It is an abelian subgroup of a non abelian group S_3.

8.4 Normal subgroup

A subgroup N of a group G is said to be a normal subgroup (or invariant subgroup or self conjugate subgroup) of G if for all $n \in N$ and $x \in G$, $xnx^{-1} \in N$. If N is an normal subgroup of G, then symbolically we write it is $N \lhd G$.

Equivalently if $xNx^{-1} = \{xnx^{-1} \mid n \in N\}$, then N is a normal subgroup of G if and only if $xNx^{-1} \subset N$ for every $x \in G$. Every group G whose order greater than one has at least two normal subgroups $N = \{e\}$ and $N = G$. These two are known as improper normal subgroups of G and every normal subgroup other than these two is known as proper normal subgroup.

A group G is said to be **Simple group** if its only normal subgroups are $\{e\}$ and G. For example a group of prime order is simple, because such a group has no proper subgroups. If G is an abelian group, every subgroup N of G is normal in G, because for every

$$n \in N, x \in G, xnx^{-1} = xx^{-1}n = en = n \in N.$$

8.4.1 Elementary properties and examples :

Theorem 9. *A subgroup N of a group G is normal if and only if $xNx^{-1} = N$ for every $x \in G$.*

Proof : First suppose that N is a normal subgroup of G, then for every $x \in G$,

$$x N x^{-1} \subseteq N \qquad \text{.....(1)}$$

and for $x^{-1} \in G$,

$$x^{-1} Nx = x^{-1} N (x^{-1})^{-1} \subseteq N.$$

Now, for every $n \in N$, we have

$$\begin{aligned} n &= ene \\ &= xx^{-1} nxx^{-1} \\ &= x (x^{-1}nx) x^{-1} \in xNx^{-1}, \end{aligned}$$

$\Rightarrow$ $n \in xNx^{-1} \ \forall \ n \in N$ and hence

$$N \subseteq xNx^{-1} \ \forall \ x \in G \qquad \text{.....(2)}$$

from (1) and (2), we get

$$xNx^{-1} = N.$$

Conversely suppose that $xNx^{-1} = N$ for every $x \in G$, then obviously $xNx^{-1} \subseteq N$ and hence N is a normal subgroup of G.

Theorem 10. *A subgroup N of a group G is normal in G if and only if $xN = Nx$, for each $x \in G$.*

Proof : First suppose that $xN = Nx$ for each $x \in G$. Then for each $n \in N$, there is $m \in N$ such that

$$xn = mx \Rightarrow xnx^{-1} = m \in N$$

$\Rightarrow$ $xnx^{-1} \in N$ for every $n \in N$ and $x \in G$ and hence N is a normal subgroup of G. Conversely suppose that N is a normal subgroup of G, then

$$\begin{aligned} xNx^{-1} &= N \qquad \text{for every } x \in G \\ (xNx^{-1})\, x &= Nx \\ (xN)\, (x^{-1} x) &= Nx \\ xNe &= Nx \\ xN &= Nx \qquad \text{for every } x \in G. \end{aligned}$$

Theorem 11. *If N_1 and N_2 are normal subgroups of a group G, then $N_1 \cap N_2$ is a normal subgroup of G.*

Proof : Since intersection of two subgroups of a group is again a subgroup of that group, so $N_1 \cap N_2$ is a subgroup G. Let $x \in G$ and n be any element of $N_1 \cap N_2$, so $n \in N_1$ and $n \in N_2$. Since N_1 and N_2 are normal subgroups of G,

so $x \in G, n \in N_1 \Rightarrow xnx^{-1} \in N_1$

and $x \in G; n \in N_2 \Rightarrow xnx^{-1} \in N_2$.

Hence $xnx^{-1} \in N_1 \cap N_2$ for each $x \in G$ and $n \in N_1 \cap N_2$. Thus $N_1 \cap N_2$ is a normal subgroup of G.

Theorem 12. *Every subgroup N of a group G with index two is a normal subgroup.*

Proof : From example 5 of article 3.2.5, we have

$Nx = xN$ for all $x \in G$ and hence N is a normal subgroup of G.

Theorem 13. *If N is a normal subgroup of a group G, then the product of two right (Left) cosets of N in G is again a right (left) coset of N in G.*

Proof : Let Nx and Ny be two right cosets of N in G, then $x, y \in G$. Since N is a normal subgroup of G, so

$$Nx = xN \text{ for every } x \in G.$$

Now,

$$\begin{aligned} Nx\ Ny &= N\,(xN)\,y \\ &= N\,(Nx)\,y \\ &= N\,N\,x\,y \\ &= Nxy, \qquad \text{since } N \text{ is a subgroup, so } NN = N \end{aligned}$$

$$\Rightarrow \qquad Nx\ Ny = Nxy,\ xy \in G$$

Hence product of two right cosets of N in G is again a right coset of N in G. Similarly we can prove that product of two left cosets of N in G is again a left coset of N in G.

Ex.1. *Show that the centre of a group G, that is, $Z(G) = \{a \in G \mid ax = xa\ \forall\ x \in G\}$ is a normal subgroup of G.*

Sol. We know that $Z(G)$ is a subgroup of G. Let $x \in G$ and $n \in Z(G)$, then

$$\begin{aligned} xnx^{-1} &= (xn)\,x^{-1} \\ &= (nx)\,x^{-1} \\ &= n\,(xx^{-1}) \\ &= ne = n \in Z(G) \end{aligned}$$

Hence $xnx^{-1} \in Z(G)$ for all $x \in G, n \in Z(G)$, so $Z(G)$ is a normal subgroup of G.

Ex.2. *The alternating group A_n of all even permutations of degree n is a normal subgroup of the symmetric group S_n.*

Sol. We know that A_n is a subgroup of S_n. Let $\sigma \in S_n$ and $\tau \in A_n$. τ is an even permutation but $\tau \in S_n$ is either even or odd permutation. If τ is even, τ^{-1} is also even and hence $\sigma\,\tau\,\sigma^{-1}$ is even, so $\sigma\,\tau\,\sigma^{-1} \in A_n$. Again, if σ is odd, then σ^{-1} is also odd and hence $\sigma\,\tau\,\sigma^{-1}$ is even and so $\sigma\,\tau\,\sigma^{-1} \in A_n$. Thus, for every $\sigma \in S_n$ and $\tau \in A_n \Rightarrow \sigma\,\tau\,\sigma^{-1} \in A_n$ and $A_n \lhd S_n$.

Theorem 14. *If N is a normal subgroup of G and G/N is the set of all right cosets of N in G, then G/N is a group under the binary operation defined as $Nx\ Ny = N\ xy$ for all Nx, $Ny \in G/N$.*

Proof : Let $G/N = \{Nx \mid x \in G\}$. At first we show that binary operation defined in G/N is well defined. For this we show that, if $Na = Nc$ and $Nb = Nd$, then $Nab = Ncd$. Now, $Na = Nc$ shows that $ac^{-1} \in N$ and $Nb = Nd$ shows that $bd^{-1} \in N$.

Since $$(ab)(cd)^{-1} = abd^{-1}c^{-1}$$
$$= a(bd^{-1})a^{-1}(ac^{-1})$$

and N is a normal subgroup of G, so $a(bd^{-1})a^{-1}(ac^{-1}) \in N$ and hence $(ab)(cd)^{-1} \in N$.

This shows that $Nab = Ncd$. For $Na, Nb, Nc \in G/N$, we have

$$(Na\ Nb)\ Nc = (Nab)\ Nc$$
$$= N(ab)\ c$$
$$= Na(bc), \text{ since}$$
$$(ab)\ c = a(bc),\ \forall\ a, b, c \in G$$
$$= Na\ N(bc)$$
$$= Na\ (Nb\ Nc),$$

which shows that binary operation is associative in G/N.

Identity $e \in G$ implies $Ne = N \in G/N$ such that $Na\ Ne = Nae = Na = Nea = Ne\ Na$ for all $Na \in G/N$. This shows that N is the identity element in G/N. For each Na in G/N, $a \in G$ and $a^{-1} \in G$, so $Na^{-1} \in G/N$ such that

$$Na\ Na^{-1} = Naa^{-1} = Ne = N$$

and $$Na^{-1} = Na^{-1}a = Ne = N.$$

This shows that Na^{-1} is the inverse of Na. Hence G/N is a group. It is called the quotient or factor group of G by N.

Note that *(i)* for the existence of the quotient group G/N, N must be normal subgroup of G.

(ii) Every quotient group of an abelian group is abelian.

(iii) Every quotient group of a cyclic group is cyclic.

However, the converse of *(ii)* and *(iii)* results is not necessarily true because $o\left(\frac{S_3}{A_3}\right)$ is 2 (Prime) and so it is abelian and cyclic both but S_3 is neither abelian nor cyclic.

Ex.1. *Consider the multiplicative group $< G = \{1, -1, i, -i\}, \cdot >$ and its subgroup $H = \{1, -1\}$.*

From example 1 of article 8.2.5 we see that H and Hi are two distinct right cosets of H in G and hence $G/H = \{H, Hi\}$. We can construct an operation table as :

.	H	Hi
H	H	Hi
Hi	Hi	H

Ex.2. Consider the additive group (Z, +) of integers and its subgroup $H = \{3x \mid x \in Z\}$. Since Z is an abelian group, so H is a normal subgroup of Z and hence Z/H exists. From example 2 of article 8.2.5 we see that H, $H+1$ and $H+2$ are three distinct right cosets of H in Z and hence

$$Z/H = \{H, H+1, H+2\}.$$

We can construct an operation table as :

+	H	$H+1$	$H+2$
H	H	$H+1$	$H+2$
$H+1$	$H+1$	$H+2$	H
$H+2$	$H+2$	H	$H+1$

Self-learning exercise-2

1. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 2 \end{pmatrix}$ is a permutation on a set $A = \{1, 2, 3, 4\}$ [True/false]

2. Which one of the following is an identity permutation on a set $A = \{1, 2, 3\}$?

   (a) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *(b)* $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

   (c) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

3. In the quotient group G/N, the identity element is :

   (a) N *(b)* $N+1$

   (c) e (d) 0

4. Every subgroup of an abelian group is a normal subgroup. [True/false]

5. The union of two normal subgroup is again a normal subgroup. [True/false]

8.5 Summary

In this unit we have discussed subgroups and their properties. We have also discussed about cosets and Lagrange's theorem, permutation group and some important results related to these topics. In the end of the unit we have explained normal subgroups and their elementary properties.

8.6 Answers to self-learning exercises

Self-learning exercise-1

1. True 2. False 3. True 4. False

5. $Ha = \{a, a^3\}$, $H(1) = \{1, a^2\}$.

Self-learning exercise-2

1. False **2.** b **3.** a **4.** True

5. False

8.7 Exercises

1. Prove that set $H = \{a + ib \mid a, b \in Q\}$ is a subgroup the additive group $(C, +)$ of complex numbers.

2. If G is an abelian group, then prove that the set $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G.

3. Find all the cosets of $H = \{4x \mid x \in Z\}$ in the additive group $(Z, +)$ of integers.

[Ans. $H, H+1, H+2, H+3$**]**

4. Find all the right cosets of $H = \{(1), (1, 2)\}$ in the symmetric group S_3.

[Ans. $H, H(1, 2, 3), H(1, 3, 2)$**]**

5. Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ be two permutations on a set $A = \{1, 2, 3, 4\}$, then find fog and gof.

[Ans. $fog = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (23)$ and $gof = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12)$**]**

6. If H and K are two normal subgroup of a group G, then prove that HK is also a normal subgroup of G.

7. If H is a subgroup of G and N is a normal subgroup of G, then prove that $H \cap N$ is a normal subgroup of H.

8. Let G be a group and H be an normal subgroup of G such that G/H is abelian. Show that $\forall\ a, b \in G, aba^{-1}b^{-1} \in H$.

□□□

UNIT 9 : Ring, Integral Domain and Field

Structure of the Unit

9.0 Objectives

After reading this unit you will be able to understand about rings, integral domains, fields and their properties. You will be also able to understand about ring with zero divisors, ring without zero divisors, subrings, subfields and ring homomorphisms.

9.1 Introduction

In this unit we begin by defining rings and properties of rings. Alter this we proceed with the definitions of zero divisors, integral domains, fields, subrings, subfields and their properties. In the end of the unit we discuss about ring homomorphism and some important examples of this unit.

9.2 Rings

A ring is a nonempty set R equipped with two binary operations addition (+) and multiplication (·) such that

(i) $(R, +)$ is a commutative group,

(ii) $(R, \cdot)$ is a semigroup,

(iii) Multiplication distributes over addition, *i.e.* for all $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ (left distributive law)}$$

$$(b + c) \cdot a = b \cdot a + c \cdot a \text{ (right distributive law).}$$

R is called a ring with unit element if there exists an element $e \in R$. Such that $ea = a = ae$ for all $a \in R$. e is known as **unit element** in R. R is said to be **commutative ring** if $ab = ba$ for all $a, b \in R$. In a ring, the additive identity is called the **zero element** of the ring and the additive inverse of $a \in R$ is called the negative of a, to be denoted by $-a$. Also, we define $a - b = a + (-b)$ for all $a, b \in R$. Let $R = \{0\}$, then R is a ring with usual addition and multiplication defined as $0 + 0 = 0$ and $0 \cdot 0 = 0$. This ring $R = \{0\}$ is called the **zero** or **null** ring.

Ex.1. *The set Z of all integers is a ring with respect to usual addition and multiplication, because* $(Z, +)$ *is a commutative group,* $(Z, \cdot)$ *is a semigroup and for all* $a, b, c \in Z$, *the following are true :*

$$a(b + c) = ab + ac \text{ and } (b + c)\, a = ba + ca.$$

Ex.2. *The set Q of all rational numbers is a ring with respect to usual addition and multiplication, because* $(Q, +)$ *is a commutative group,* $(Q, \cdot)$ *is a semigroup and for all* $a, b, c \in Q$, *the following are true :*

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and } (b + c) \cdot a = b \cdot a + c \cdot a.$$

Note that the set R of real numbers and the set C of complex numbers are rings with respect to usual addition and multiplication. All the above rings are commutative ring with unity element 1.

Ex.3. *Let* M_2 *denotes the set of all* 2×2 *real matrices. Then* M_2 *is a ring with respect to usual addition and multiplication of matrices, because* $(M_2, +)$ *is an abelian group,* $(M_2, \cdot)$ is a semigroup and for all $A, B, C \in M_2$, *the following are true :*

$$A \cdot (B + C) = A \cdot B + A \cdot C \text{ and } (B + C) \cdot A = B \cdot A + C \cdot A.$$

It is an example of non-commutative ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Ex.4. *The set* $Z_n = \{0, 1, 2, \ldots, n - 1\}$ *is a ring with respect to addition and multiplication modulo n.*

9.2.1 Properties of Rings :

Theorem 1. *For any element a, b, c of a ring R,*

(i) $a \cdot 0 = 0 \cdot a = 0$,

(ii) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$

(iii) $(-a) \cdot (-b) = a \cdot b$

(iv) $a \cdot (b - c) = a \cdot b - a \cdot c$

(v) $(b - c) \cdot a = b \cdot a - c \cdot a$

Proof : *(i)* $a \cdot 0 = a \cdot (0 + 0)$

$= a \cdot 0 + a \cdot 0,$ by distributive law

$\Rightarrow \quad a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow \quad 0 = a \cdot 0,$ by left cancellation law in $(R, +)$

Similarly $0 \cdot a = 0.$

(ii) From *(i)*, we have

$a \cdot 0 = 0$

$\Rightarrow \quad a \cdot (-b + b) = 0$

$\Rightarrow \quad a \cdot (-b) + a \cdot b = 0$

$\Rightarrow \quad a \cdot (-b) = -(a \cdot b),$ by definition of additive inverse.

Again from *(i)*, we have

$0 \cdot b = 0$

$\Rightarrow \quad (-a + a) \cdot b = 0$

$\Rightarrow \quad (-a) \cdot b + a \cdot b = 0$

$\Rightarrow \quad (-a) \cdot b = -(a \cdot b)$

Thus $a(-b) = -(a \cdot b) = (-a) \cdot b.$

(iii) Using *(ii)*,

$(-a)(-b) = -[a(-b)]$

$= -(-ab)$

$= ab$

(iv) $a \cdot (b - c) = a \cdot [b + (-c)]$

$= a \cdot b + a \cdot (-c)$

$= a \cdot b - a \cdot c,$ [using *(ii)*]

(v) $(b - c) \cdot a = [b + (-c)] \cdot a$

$= b \cdot a + (-c) \cdot a$

$= b \cdot a - c \cdot a,$ [using *(ii)*]

9.2.2 Zero divisors :

If a and b are two non-zero elements in a ring R such that $a \cdot b = 0$, then a and b are called zero divisors or divisors of zero. a is known as left divisor of zero and b is known as right divisor of zero.

In a commutative ring R, every left divisor of zero is also a right divisor of zero and conversely.

A ring R is said to be **ring with zero divisors** if there exist non-zero elements a, b in R such that $a \cdot b = 0$, that is if $a \neq 0$, $b \neq 0$ but $ab = 0$. For example the set M_2 of all 2×2 matrices having their elements as integers forms a ring with zero divisors under addition and multiplication of matrices because

$A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, $B = \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix}$ are two non-zero elements in M_2 such that

$$A \cdot B = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

A ring *R* is said to be without zero divisors if product of two non-zero elements in *R* is not zero, *i.e.* if $a, b \in R$ such that $a \cdot b = 0$, than either $a = 0$ or $b = 0$. The ring of integers $(Z, +, \cdot)$ is a ring without zero divisors.

Cancellation laws in a ring :

In every ring the cancellation laws for addition composition always hold because it is always an abelian group. But the cancellation laws for multiplication composition may or may not hold in every ring.

Let *a* be *a* non-zero element of a ring *R* which is not a zero divisor. If *b* and *c* are in *R* and $ab = ac \Rightarrow b = c$, then it is known as **left cancellation** law and if $ba = ca \Rightarrow b = c$, then it is known as **right cancellation law**.

Theorem 2. *A ring R is without zero divisors if and only if cancellation taws hold in R.*

Proof : First suppose that *R* is without zero divisors. Let $a, b, c \in R$ such that $a \neq 0$ and $ab = ac$. Now

$$\begin{aligned} ab = ac &\Rightarrow ab - ac = 0 \\ &\Rightarrow a(b - c) = 0 \\ &\Rightarrow b - c = 0, \text{ since } a \neq 0 \text{ and } R \text{ is without zero divisors} \\ &\Rightarrow b = c \end{aligned}$$

Thus $ab = ac \Rightarrow b = c$.

Similarly $ba = ca \Rightarrow b = c$.

Hence cancellation laws hold in *R*.

Conversely, suppose that cancellation laws hold in *R*. Now we have to show that *R* is without zero divisors. Let $ab = 0$ with $a \neq 0$, then

$$\begin{aligned} ab = 0 &\Rightarrow ab = a \cdot 0, \text{ since } a \cdot 0 = 0 \ \forall \ a \in R \\ &\Rightarrow b = 0, \text{ by cancellation law.} \end{aligned}$$

Thus *R* is without zero divisors.

9.3 Integral domains and fields

A commutative ring *R* with unity and which is without zero divisors is called an **integral domain.**

The ring $(Z, +, \cdot)$ of integers is an integral domain, because it is a commutative ring with unity and without zero divisors. Similarly $(Q, +, \cdot)$, $(R, +, \cdot)$ and $(C, +, \cdot)$ are integral domains. The ring $< Z_6 = \{0, 1, 2, 3, 4, 5\}, +_6, \times_6 >$ is not an integral domain because it is a ring with zero divisors, since $0 \neq 2, 0 \neq 3 \in Z_6$ but $2 \times_6 3 = 6 = 0$. Note that

$< Z_p = \{0, 1, 2, ..., p-1\}, +_p, \times_p >$ is an integral domain if and only if p is prime.

A ring R with identity is called a division ring or skew field if all its non-zero elements are invertible. The rings $(Q, +, \cdot)$ of rational numbers. $(R, +, \cdot)$ of real numbers and $(C, +, \cdot)$ of complex numbers are division rings. The ring M_2 of all 2×2 non singular matrices over R is a division ring. The ring $(Z, +, \cdot)$ of integers is not a division ring, since for $0 \neq a \in Z$, $a \neq \pm 1$ multiplicative inverse of a does not exist in Z.

A commutative ring R with unity in which every non-zero element has multiplicative inverse is called a **field**. In other words we can say that a commutative division ring is a field.

Thus a field is a nonempty set R equipped with two binary operations (+) and multiplication $(\cdot)$ such that

(i) $(R, +)$ is a commutative group,

(ii) $(R - \{0\}, \cdot)$ is also a commutative group,

(iii) multiplication distributes over addition *i.e.*, for all $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

The set of rational numbers Q, the set of real numbers R and the set of complex numbers C are fields under usual addition and multiplication as binary operations. The ring of Gaussian integers $Z[i] = \{a + ib \mid a + b \in Z\}$ is an integral domain, because it is a commutative ring with unity and without zero divisors. But it is not a field, since for $0 \neq a + ib \in Z[i]$ its multiplicative inverse is $\frac{1}{a+ib}$

and $$\frac{1}{a+ib} = \frac{1}{(a+ib)} \frac{(a-ib)}{(a-ib)} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{ib}{a^2+b^2}$$

where $\frac{a}{a^2+b^2} \notin Z$, $\frac{b}{a^2+b^2} \notin Z$ for all $a, b \in Z$.

Theorem 3. *Every field is an integral domain but the converse is not necessarily true.*

Proof : Let F be a field. Then F is a commutative ring with unity in which every non-zero element has its multiplicative inverse. In order to prove that F is an integral domain, it is sufficient to show that F is without zero divisors. Let $a, b, \in F$ such that $a \neq 0$ and $ab = 0$. Then $a^{-1} \in F$ such that $aa^{-1} = 1 = a^{-1} a$. Now

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1} 0$$

$$\Rightarrow (a^{-1} a) b = 0, \quad \text{since} \quad x\,0 = 0 \ \forall\ x F$$

$$\Rightarrow 1 \cdot b = 0$$

$$\Rightarrow b = 0$$

Thus $0 \neq a, ab = 0 \Rightarrow b = 0$ and hence F is an integral domain.

The converse is not necessarily true because the ring $(Z, +, \cdot)$ of integers is an integral domain but it is not a field as its non-zero elements except 1 and –1 do not have their multiplicative inverse in Z.

Theorem 4. *Every finite commutative ring without zero divisors is a field.*

Proof : Let R be a finite commutative ring without zero divisors. In order to prove that R is a field, it is sufficient to show that R has unity and every non-zero element of R has a Multiplicative inverse in R. Since R is a finite set, so let us assume

$R = \{a_1, a_2, ..., a_n\}$ has n distinct elements. Let $a \neq 0$ be any non-zero arbitrary element of R. Then elements $aa_1, aa_2, ..., aa_n$ all belong to R and all are distinct, because

$$aa_i = aa_j \text{ for } i \neq j$$

$$\Rightarrow \quad aa_i - aa_j = 0$$

$$\Rightarrow \quad a(a_i - a_j) = 0$$

$$\Rightarrow \quad a_i - a_j = 0, \qquad \text{since } R \text{ is without zero divisor and } a \neq 0$$

$$\Rightarrow \quad a_i = a_j \text{ for } i \neq j, \text{ which contradicts}$$

the fact R has n distinct elements. Hence the set $\{aa_1, aa_2, ..., aa_n\}$ coincide with R. Now $a \in R$ implies that, there exists $a_k \in R$ such that $aa_k = a$. We shall show that a_k is the unity of R. Let a_l be any element of R. Then $a_l = aa_j$ for some $a_j \in R$. Now

$$\begin{aligned} a_l a_k = a_k a_l &= a_k (aa_j) \\ &= (a_k a) a_j \\ &= (aa_k) a_j, \text{ since } R \text{ is commutative} \\ &= aa_j = a_l \end{aligned}$$

Thus a_k is the unity of R.

Let $a_k = 1$. Since $1 \in R$, so $1 = aa_m = a_m a$ for some $a_m \in R$, which shows that a_m is the multiplicative inverse of a in R and hence R is a field.

Theorem 5. *Every finite integral domain is a field.*

Proof : Let R be a finite integral domain. Then R is a commutative ring with unity without zero divisors. In order to prove that R is a field, it is sufficient to show that every non-zero element of R has a multiplicative inverse in R.

Let a be any non-zero element of R. Then $a, a^2, ..., a^n, ...$ all are elements of R. They are infinite in number, so all can not be distinct as R is finite. Let

$$a^m = a^n \text{ for } m > n$$

$$\Rightarrow \quad a^m a^{-n} = a^n a^{-n}$$

$$\Rightarrow \quad a^{m-n} = a^0 = 1$$

$$\Rightarrow \quad a \cdot a^{m-n-1} = a$$

$$\Rightarrow \quad a^{-1} = a^{m-n-1}$$

$\Rightarrow$ Every non-zero element of R has multiplicative inverse in R and hence R is a field.

Theorem 6. *In a ring, an invertible element can not be a divisor of zero.*

Proof : Let a be an invertible element of a ring R. Then $a \neq 0$. Since a is invertible, these exists $a^{-1} \in R$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Now, let $ab = 0$ for some $b \in R$. Then

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}\,0$$
$$\Rightarrow (a^{-1}\,a)\,b = 0$$
$$\Rightarrow 1 \cdot b = 0$$
$$\Rightarrow b = 0.$$

This shows that a is not a left divisor of zero. Similarly we can show that a is not a right divisor of zero.

9.3.1 Characteristic of a ring, integral domain and field :

Let R be a ring with zero element '0' and suppose there exists a positive integer n such that $n \cdot a = 0$, for all $a \in R$, then the least such positive integer n is called the characteristic of the ring. If no such positive integer exists, then we say that characteristic of R is zero or infinite.

If R is a ring with unity e, then the least positive integer n such that $n \cdot e = 0$ is called the characteristic of R. If no such positive integer exist, then characteristic of R is zero or infinite. Since every integral domain (respectively a field) is a ring with unity, so the characteristic of an integral domain (respectively a field) is the least positive integer n such that $n \cdot e = 0$. If no such positive integer exist, then characteristic of an integral domain (respectively a field) is zero or infinite.

Note that in order to find the characteristic of an integral domain D (respectively a field F) we should find the order of the unity element e of D (respectively F) when regarded as a member of the additive group D (respectively F).

The ring Z of all integers has characteristic zero, since there is no positive integer m such that $m \cdot 1 = 0$. The characteristic of the ring $< Z_6 = \{0, 1, 2, 3, 4, 5\}, +_6, \times_6 >$ is 6 because order of 1 regarded as member of additive group $(Z_6, +_6)$ is 6. Similarly the fields Q, R and C all have characteristic zero.

Theorem 7. *The characteristic of an integral domain is zero or a prime number.*

Proof : Let D be an integral domain. If characteristic of D is zero, then the theorem is proved. Let characteristic of D be n and $n > 0$. Then n is the least positive integer such that $n \cdot 1 = 0$. We have to show that n is a prime number. If possible, let n be a composite number, *i.e.* $n = pq$ such that $1 < p < n$, $1 < q < n$ and $p, q \in N$. Now

$$n \cdot 1 = 0 \Rightarrow (pq) \cdot 1 = 0$$
$$\Rightarrow (p \cdot 1)(q \cdot 1) = 0$$

$\Rightarrow$ $p \cdot 1 = 0$ or $q \cdot 1 = 0$, since D is an integral

$\Rightarrow$ The characteristic of D is either p or q where $1 < p < n$ and $1 < q < n$, which contradicts the fact that characteristic of D is n. Hence n must be a prime number.

Note that every field is an integer domain, so the characteristic of a field is zero or a prime number.

9.4 Subrings and subfields

A nonempty subset S of a ring R is called a **subring** of R if S itself is a ring with respect to binary operations defined in R. Every non-zero ring R has atleast two subrings $S = \{0\}$ and $S = R$.$\{0\}$ is known as **trivial subring** of R and R is known as **improper** subring of R. Every subring of R other than these two is known as a **proper** subring of R.

The ring of integers is a proper subring of the ring $(Q, +, \cdot)$ $(R, +, \cdot)$ and $(C, +, \cdot)$. The ring of even integers is a proper subring of the ring of integers $(Z, +, \cdot)$.

A subset K, containing at beast two elements of a field F is called a subfield of F, if K itself is a field under binary operations defined in F. Every field F is a subfield of itself, known as **improper subfield** of F. All other subfields of F are known as a **proper** subfield.

A field F which has no proper subfield is called a **prime field**. For example, the field Q of rational numbers is a prime field. Similarly, the field $(Z_p, +_p, \times_p)$ where $Z_p = \{0, 1, 2, ..., p-1\}$ where p is prime, is a prime field.

The field of rational numbers $(Q, +, \cdot)$ and the field of real numbers $(R, +, \cdot)$ are subfields of the field of complex numbers $(C, +, \cdot)$ where as $(R, +, \cdot)$ is a subfield of $(C, +, \cdot)$.

Theorem 8. *A nonempty subset S of a ring R is a subring of R if and only if*

(i) $a - b \in S$ for all $a, b \in S$,

(ii) $ab \in S$ for all $a, b \in S$.

Proof : First suppose that S is a subring of R and let $a, b \in S$. Then $(S, +, \cdot)$ is a ring and hence $a + b \in S$. Again as S is a subring $b \in S \Rightarrow -b \in S$ and hence $a \in S, -b \in S \Rightarrow a + (-b) = a - b \in S$.

Conversely suppose that $a - b \in S$ and $ab \in S$ for all $a, b \in S$. Now $a - b \in S$ for all $a, b \in S$ implies that S is a subgroup of $(R, +)$. $ab \in S$ for all $a, b \in S$ shows that S is closed with respect to multiplication. Since multiplication in R is associative and it distributes over addition, the same is true for multiplication in S, since S is a subset of R. Hence S is a subring of R.

Form above theorem we can say that a subset S of a ring R is a subring of R if and only if S is an additive subgroup of $(R, +)$ and is closed under multiplication.

Note that the intersection of two subrings of a ring is again a subring of that ring. But the union of two subrings of a ring is not necessarily a subring of that ring. The union of two subrings of a rings is again a subring of that ring if and only if one is contained in the other.

A nonempty subset K of a field F is a subfield of F if and only if

(i) $a \in K, b \in K \Rightarrow a - b \in K$

(ii) $a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in K$.

From above we can say that a nonempty subset K of a field F is a subfield of F if and only if K is a subgroup of the additive abelian group $(F, +)$ and $K - \{0\}$ is a subgroup of the multiplicative abelian group $(F - \{0\}, \cdot)$.

9.5 Ring homomorphisms

A mapping ϕ from a ring R to another ring R' is called a homomorphism if for all $a, b \in R$

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a) \cdot \phi(b).$$

A ring homomorphism $\phi : R \to R'$ is an isomorphism if ϕ is one-one and onto, and we write $R \cong R'$.

A ring homomorphism is a monomorphism it is injective, an epimorphism if it is surjective.

A ring homomorphism $\phi : R \to R$ is known as endomorphism and is called an automorphism if ϕ is bijective.

If ϕ is a homomorphism from a ring R into a ring R', then $\phi(0) = 0'$ and $\phi(-a) = -\phi(a)$, for every $a \in R$. 0 and 0′ and are zero element of R and R' respectively. The kernel of ϕ is denoted by Ker ϕ and

Ker $\phi = \{r \in R \mid \phi(r) = 0'\}$. Since $0 \in R$ implies $\phi(0) = 0'$, so $0 \in$ Ker ϕ and hence Ker ϕ is a non-empty subset of R and it is a subring of R. The image set $\phi(R) = \{\phi(x) \mid x \in R\}$ is a subring of R'.

9.6 Some important examples

Ex.1. *Show that the set of all matrices of the form* $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$; $a, b \in R$ *is a ring for matrix addition and multiplication. It it without zero divisors.*

Sol. Let $M = \left\{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} : a, b \in R \right\}$. Let $x = \left\{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}, y = \begin{bmatrix} 0 & c \\ 0 & d \end{bmatrix} \right\}$ be any two elements of M. Then

$$x + y = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} + \begin{bmatrix} 0 & c \\ 0 & d \end{bmatrix} = \begin{bmatrix} 0 & a+c \\ 0 & b+d \end{bmatrix} \in M, \text{ since } a + c, b + d \in R.$$

and $$xy = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \begin{bmatrix} 0 & c \\ 0 & d \end{bmatrix} = \begin{bmatrix} 0 & ad \\ 0 & bd \end{bmatrix} \in M, \text{ since } ad, bd \in R.$$

Thus M is closed for the matrix addition and multiplication.

Since the matrix addition is commutative and associative, so matrix addition is also commutative and associative in M. $0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the zero element in M because for each $x = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \in M$, we have

$$x + 0 = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}.$$

For every $x = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \in M$, there exists $-x = \begin{bmatrix} 0 & -a \\ 0 & -b \end{bmatrix} \in M$ such that

$$x+(-x)=(-x)+x=\begin{bmatrix}0 & -a\\ 0 & -b\end{bmatrix}+\begin{bmatrix}0 & a\\ 0 & b\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

and hence every element of M has its additive inverse in M. Thus $(M, +)$ is an abelian group.

Since matrix multiplication is associative. So it is also associative in M and hence $(M, \cdot)$ is a semigroup. Again, since matrix multiplication is distributive over addition, therefore it is also true for M. Hence $(M, +, \cdot)$ is a ring.

We have non-zero element $\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix} \in M$ such that $\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$, therefore M ha zero divisors.

Ex.2. *If R is a ring such that $a^2 = a$, for all $a \in R$. Prove that*

(i) $a + a = 0 \ \forall \ a \in R$,

(ii) $a + b = 0 \Rightarrow a = b$, *for all* $a, b \in R$,

(iii) R is commutative ring.

Sol. ***(i)*** Since R is a ring, so $a \in R \Rightarrow a + a \in R$. By given condition, we have

$$\begin{aligned} a + a &= (a + a)^2 \\ &= (a + a)(a + a) \\ &= a(a + a) + a(a + a) \\ &= a^2 + a^2 + a^2 + a^2 \\ &= (a + a) + (a + a) \end{aligned}$$

$$\Rightarrow \quad 0 + (a + a) = (a + a) + (a + a)$$

$$\Rightarrow \quad 0 = a + a, \text{ by cancellation law for addition}$$

(ii) Now $a + b = 0 \Rightarrow a + b = a + a$, since $a + a = 0$

$$\Rightarrow b = a, \text{ by cancellation law for addition}$$

(iii) Since R is a ring, so $a \in R, b \in R \Rightarrow a + b \in R$. By given condition, we have

$$\begin{aligned} (a + b) &= (a + b)^2 \\ &= (a + b)(a + b) \\ &= a(a + b) + b(a + b) \\ &= a^2 + ab + ba + b^2 \\ &= a + ab + ba + b \end{aligned}$$

$$\Rightarrow \quad a + b = a + (ab + ba) + b$$

$$\Rightarrow \quad 0 = ab + ba, \text{ by cancellation laws for addition}$$

Hence by *(ii)*, we get

$$ab = ba \text{ for all } a, b \in R.$$

So, R is a commutative ring.

Note that such a ring is called a **Boolean ring**.

Ex.3, Show that the set

$$F = \{a + b\sqrt{2} \ : a, b \in Q\}$$

is a field.

Sol. *(i)* Let $x = a_1 + b_1\sqrt{2}$ and $y = a_2 + b_2\sqrt{2}$ be any two elements of F, then $a_1, a_2, b_1, b_2 \in Q$. Now

$$x + y = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})$$

$$= (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in F, \text{ since } a_1 + a_2 \in Q \text{ and } b_1 + b_2 \in Q.$$

and

$$xy = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$$

$$= a_1 a_2 + a_1 b_2\sqrt{2} + b_1 a_2\sqrt{2} + 2b_1 b_2,$$

$$= (a_1 a_2 + 2b_1 b_2) + (a_1 b_2 + b_1 a_2)\sqrt{2} \in F,$$

since $a_1 a_2 + 2b_1 b_2 \in Q$ and $a_1 b_2 + b_1 a_2 \in Q$.

Hence F is closed for addition and multiplication binary operations.

Since $a + b\sqrt{2}$ is a real number and addition and multiplication are commutative and associative in the set R of real numbers, so these are commutative and associative in F also. $0 = 0 + 0\sqrt{2}$ is the additive identity and $1 = 1 + 0\sqrt{2}$ is the multiplicative identity in F. Clearly the additive inverse of $x = a + b\sqrt{2}$ is $-x = (-a) + (-b)\sqrt{2}$.

Since in the set R of real numbers multiplication is distributive over addition, so distributive property hold in F. Let $x = a + b\sqrt{2}$ be a non-zero element of F. Then either $a \neq 0$ or $b \neq 0$ or both a and b are non-zero. Now we have

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \left(\frac{a}{a^2 - 2b^2}\right) + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2}.$$

Since $a, b \in Q$, then $a^2 = 2b^2$ only if $a = 0$ and $b = 0$, **but this is not possible** because either $a \neq 0$ or $b \neq 0$. Thus $\frac{a}{a^2 - 2b^2}$ and $\frac{-b}{a^2 - 2b^2}$ are both rational numbers and hence, we have

$$\frac{1}{a + b\sqrt{2}} \in F$$

such that

$$(a + b\sqrt{2}) \cdot \frac{1}{(a + b\sqrt{2})} = 1$$

$$= 1 + 0\sqrt{2}.$$

Hence $\frac{1}{a + b\sqrt{2}}$ is a multiplicative inverse of each non-zero element $a + b\sqrt{2}$ in F. Consequently $(F, +, \cdot)$ is a field.

Ex.4. *Let m be a fixed positive integer. Then the set*

$$S = mZ = \{mx | x \in Z\}$$

is a subring of the ring of integers $(Z, +, \cdot)$.

Sol. $0 \in Z \Rightarrow m \cdot 0 = 0 \in S$ and hence $S \neq \phi$. Let $x = ma$ and $y = mb$ be any two elements of S. Then $a, b \in Z$. Now

$$x - y = ma - mb$$

$$= m(a - b) \in S, \text{ since } a - b \in Z.$$

and

$$xy = (ma)(mb)$$

$$= m(amb) \in S, \text{ since } amb \in Z.$$

Hence S is a subring of $(Z, +, \cdot)$.

Ex.5. *Let* $Z(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in Z\}$. *With the help of example 2 of article 9.6 we can show that* $Z(\sqrt{2})$ *is a ring under usual addition and multiplication. Show that the mapping* $\phi : Z(\sqrt{2}) \to Z(\sqrt{2})$ *defined as* $\phi(a + b\sqrt{2}) = a - b\sqrt{2}$ *is a ring homomorphism. Determine Ker* ϕ.

Sol. Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ be any two elements of $Z(\sqrt{2})$, then $a, b, c, d \in Z$. Now

$$\phi(x + y) = \phi\left[(a + c) + (b + d)\sqrt{2}\right]$$

$$= (a + c) - (b + d)\sqrt{2}$$

$$= (a - b\sqrt{2}) + (c - d\sqrt{2})$$

$$= \phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2})$$

$$= \phi(x) + \phi(y)$$

and

$$\phi(x \cdot y) = \phi\left[(ac + 2bd) + (cd + bc)\sqrt{2}\right]$$

$$= (ac + 2bd) - (ad + bc)\sqrt{2}$$

$$= (a - b\sqrt{2})(c - d\sqrt{2})$$

$$= \phi(a + b\sqrt{2})\,\phi(c + d\sqrt{2})$$

$$= \phi(x) \cdot \phi(y)$$

Hence ϕ is a homomorphism.

$$\text{Ker } \phi = \left\{a+b\sqrt{2} \in Z\left(\sqrt{2}\right) : \phi\left(a+b\sqrt{2}\right) = 0+0\sqrt{2}\right\}$$

$$= \left\{a+b\sqrt{2} \in Z\left(\sqrt{2}\right) : a-b\sqrt{2} = 0+0\sqrt{2}\right\}$$

$$= \left\{a+b\sqrt{2} \in Z\left(\sqrt{2}\right) : a = 0 \text{ and } b = 0\right\}$$

$$= \{0\}$$

Hence Ker $\phi = \{0\}$.

Self-learning exercise-1

1. To form a ring, we require atleast :

(a) One element

(b) Two elements

(c) Three elements

(d) One elements which is additive identity

2. The correct statement is :

(a) Every integral domain is a field

(b) Every finite integral domain is a field

(c) Every ring is an integral domain

(d) A finite commutative ring with zero divisors is a field.

3. The ring $< Z_4 = \{0, 1, 2, 3\}, +_4, \times_4 >$ is a ring with zero divisors. [True/False]

4. $(Z_p, +_p, \times_p)$ is a field if

(a) p is a composite number

(b) p is a prime number

(c) p is even number

(d) p is odd number.

5. The characteristic of the ring $< Z_5 = \{0, 1, 2, 3, 4\}, +_5, \times_5 >$ is :

(a) 0 *(b)* 2

(c) 5 *(d)* 3

9.7 Summary

In this unit we have discussed rings, integral domains, fields and their properties. We have also discussed ring with zero divisors, ring without zero divisors, subrings, subfields and results related to these topics. In the end of the unit we have explained ring homomorphism and some important examples related to this unit.

9.8 Answers to self-learning exercises

Self-learning exercise-1

1. d 2. b 3. True 4. b
5. c

9.9 Exercises

1. Prove that the set R of numbers of the form $a+b\sqrt{3}$ where a, b are integers is a ring with respect to addition and multiplication.
2. If R is a commutative ring of characteristic 2, then prove that
$$(a+b)^2 = a^2 + b^2$$
3. Prove that the characteristic of a field is either zero or prime number.
4. If R is a ring and $a \in R$, then show that the set $N(a) = \{r \in R \mid ar = ra\}$ is a subring of R.
5. If R is a ring, then show that the set $S = \{x \in R \mid xy = yx \ \forall \ y \in R\}$ is a subring of R.
6. If $(Z, +, \cdot)$ and $(E, +, \cdot)$ are rings of integers and even integers respectively, then prove that the mapping $\phi : Z \to E$ defined as $\phi(a) = 2a \ \forall \ a \in Z$ is not a ring homomorphism.
7. Prove that the intersection of two subfields of a field is also a subfield of that field.

□□□

UNIT 10 : Boolean Lattices and Boolean Algebras

Structure of the Unit

10.0 Objectives

The purpose of writing this unit is to let the students familiar with a new algebraic system now called **Boolean algebra**, that deals with a systematic treatment of logic. Boolean algebra is widely used to analyse electrical circuits and also applied to computer electronics.

10.1 Introduction

In 1854 George Boole developed a new algebraic system which is now called Boolean algebra. In 1938 CE Shannon introduced two-valued Boolean algebra and demonstrated that properties of electrical switching circuits can be realized by this algebra. Later he called this **Switching algebra.** However a formal definition of Boolean algebra were given by EV Huntington in 1904, in which he formulated few postulates called the Huntington postulates.

This unit introduces the definition of Boolean lattice and Boolean algebra. The resemblance and deference between ordinary algebra and Boolean algebra are acknowledged so that the beginner should be careful not to apply the rules of ordinary algebra into the Boolean algebra where they are not applicable. The duality in Boolean algebra, various laws of Boolean algebra and related theorems are also discussed in length.

10.2 Boolean lattices

We recall that if L is a nonempty set and $\leq$ is a partial order relation defined on the set L, then the pair $(L, \leq)$ is said to be a partially ordered set or a poset. We also recall that a special type of poset $(L, \leq)$ in which every two elements x and y have a unique supremum (least upper bound) *i.e.* sup $\{x, y\}$ and unique infimum (greatest lower bound) *i.e.* inf $\{x, y\}$ in the nonempty set L, is said to be a **lattice.**

Thus a partially ordered set $(L, \leq)$ is a lattice if and only if for every pair of elements $a, b \in L$, there exist unique elements $l, u \in L$ such that

$$\sup \{a, b\} = u \text{ and } \inf \{a, b\} = l.$$

The sup $\{a, b\}$ is denoted by $a \vee b$ (a join b) and the inf $\{a, b\}$ is denoted by $a \wedge b$ (a meet b), where "$\vee$" and "$\wedge$" are the **binary operations** on the nonempty set L.

Before giving a formal definition of Boolean lattice we once again recall that :

(i) A lattice $(L, \leq)$ is said to be a **distributive lattice** if and only if for all element $a, b, c \in L$ $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ and $a \wedge (b \vee c) = (a \vee b) \vee (a \wedge c)$.

(ii) A lattice $(L, \leq)$ is said to be a **bounded lattice** if and only if it has a universal upper bound denoted by 1 and a universal lower bound denoted by 0.

(iii) A bounded lattice $(L, \leq)$ is said to be a **complemented lattice** if and only if for each element $a \in L$, there exists a unique element $a' \in L$ such that $a \vee a' = 1$ and $a \wedge a' = 0$. The element $a' \in L$ is called the complement of the element $a \in L$, where " ' " is a **unary operation** on the set L.

10.2.1 Boolean lattices :

A lattice $(B, \leq)$ is said to be Boolean lattice if $(B, \leq)$ is :

(i) distributive and

(ii) complemented.

If we take a finite set S, then we know that the relation "$\subseteq$" is a partial order relation on the power set $P(S)$ [$P(S)$ being the collection of all the subsets of S] It can be seen that the pair $(P(S), \subseteq)$ is a lattice which is complemented and distributive also. Hence $(P(S) \subseteq)$ is a Boolean lattice.

In a Boolean lattice $(B, \leq)$, every element in B has a unique complement. Therefore, there can be defined a unary operation on B, denoted by $'$ such that for each element $a \in B$, there exists a unique element $a' \in B$, called the complement of a. This unary operation then is called the complement operation.

Thus the Boolean lattice $(B, \leq)$ defines a lattice system $(B, +, \cdot, ')$ where + and $\cdot$ are the **meet** ($\vee$) and **join** ($\wedge$) operation and $'$ is the complement operation, such an algebraic system defined by the Boolean lattice $(B, \leq)$ is also known as **Boolean algebra.**

It is not possible to construct a finite Boolean lattice of any order. A finite Boolean lattice has exactly 2^n distinct elements for some integer $n \geq 1$. Moreover, there is a unique finite Boolean lattice of order 2^n for every positive integer $n \geq 1$.

10.2.2 Covers and atoms :

If a and b are any two elements in the Boolean lattice $(B, \leq)$, then we write $a < b$ if and only $a \leq b$ and $a \neq b$.

We say that the element $b \in B$ is a **cover** of the element $a \in B$ if and only if $a < b$ and there is no element $c \neq b$ in B, such that $a < c$ and $c < b$.

An element in the Boolean lattice $(B, \leq)$ is said to be an **atom** if it is a cover of the universal lower bound 0.

10.3 Boolean algebras

Algebraic system $< B, \vee, \wedge, ' >$ defined by the Boolean lattice $(B, \leq)$, where $\vee$, $\wedge$ and $'$ are the join, meet and the complement operations respectively, is called a Boolean algebra.

For the formal definition of Boolean algebra, we employ the postulates formulated by E.V. Huntington in 1904.

Let B be a nonempty set consisting of at least two distinct elements 0 and 1 (0 and 1 are not necessarily the ordinary integers 0 and 1). Let + and $\cdot$ be two binary operations and $'$ the unary operation (called the complement operation) defined on B. Then the algebraic structure $< B, +, \cdot, ', 0, 1 >$ is said to be a Boolean algebra if following laws hold in B :

(B1) For all elements $a, b \in B$

(i) $a + b = b + a$

(ii) $ab = ba$ [commutative laws]

(B2) For all elements $a \in B$

(i) $a + 0 = a = 0 + a$

(ii) $a \cdot 1 = a = 1 \cdot a$ [Identity laws]

0 and 1 are called the identity elements of B with respect to the + and the · operations respectively. We **also** call them to be 0 of B and 1 of B.

(B3) For all elements $a, b, c \in B$

(i) $a + (bc) = (a + b)(a + c)$

(ii) $a(b + c) = ab + ac$ [distributive laws]

(B4) For every element $a \in B$, there exists a unique element $a' \in B$ (called the complement of a) **such that**

(i) $a + a' = 1$

(ii) $aa' = 0$ [complementation laws]

The above postulates are due to EV Huntington. If we compare the definition of Boolean algebra with the arithmetic and ordinary algebra, we find that :

(i) The distributive law of + operation over · operation. *i.e.* the law $a + (bc) = (a + b)(a + c)$ is valid for Boolean algebra, though it does not hold true for ordinary algebra.

(ii) The elements of Boolean algebra do not have the additive inverse and the multiplicative inverse and so there are no subtraction or division operations in Boolean algebra.

(iii) The complement operation $'$ is defined on the Boolean algebra though it is not valid for ordinary algebra.

(iv) The ordinary algebra deals with the real numbers that include an infinite set of elements but Boolean algebra deals with undefined set of elements. The two-valued Boolean algebra deals with a set consisting of only two elements 0 and 1.

(v) The definition of Boolean algebra does not include the associative laws (is not a Huntington postulate). However these laws can be derived from other Huntington postulates.

In order to have a Boolean algebra B, we must show :

(i) The elements of the set B.

(ii) The rules of operation for the two binary operations " + " and " . "

(iii) that the set B, along with the two binary operations and the unary operation, satisfies the Huntington's postulates.

There can be formulated many Boolean algebras, depending upon the choice of elements of B and the rules of operations for the binary operations.

10.3.1 Two-valued Boolean algebra :

The structure $< B, +, \cdot, ' >$ where $B = \{0, 1\}$ and the operations +, · and $'$ defined on B are shown below :

x	x	$x+y$
0	0	0
0	1	1
1	0	1
1	1	1

;

x	x	xy
0	0	0
0	1	0
1	0	0
1	1	1

;

x	x'
0	1
1	0

is known as two-valued Boolean algebra, for we can show that all the Huntington postulates are valid for the set $B = \{0, 1\}$ and the operations defined above.

1. The closure property for the two operations + and · is obvious from the first two tables given above, since the result of each operation is 0 and 1 and both $0, 1 \in B$. So + and · are binary.
2. The commutative laws with respect to + and · are also obvious from the first two tables again as for all $a, b \in B$, we have

a	b	$a+b$	$b+a$	ab	ba
0	0	0	0	0	0
0	1	1	1	0	0
1	0	1	1	0	0
1	1	1	1	1	1

Thus $a + b = b + a$

and $ab = ba$ for all $a, b \in B$.

3. From the tables, we see that

(a) $0 + 0 = 0$ and $0 + 1 = 1 = 1 + 0$

(b) $1 \cdot 1 = 1$ and $1 \cdot 0 = 0 = 0 \cdot 1$

This proves that two identity elements, 0 for + operation and 1 for · operation as defined in (*B2*).

4. From the following table we see that for all possible values of a, b and c

$$a + (ac) = (a + b)(a + c)$$

a	b	c	(bc)	$a+(bc)$	$a+b$	$a+c$	$(a+b)(a+c)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	1	1	1	1	1

Therefore the distributive law of · over + is valid.

In a similar way we can show that the distributive law of + over · is also valid.

5. From the third given table *i.e.* the complement table we see that :

a	a'	$a+a'$	$a \cdot a'$
0	1	1	0
1	0	1	0

Thus for each $a \in B$, we have :

$$a + a' = 1 \quad \text{and} \quad aa' = 0$$

i.e. the complement laws are valid for each element in B.

6. Since the set $B = \{0, 1\}$ has two distinct elements 0 and 1 with $0 \neq 1$.

Hence $< B, +, \cdot, ' >$ is a Boolean algebra. This Boolean algebra (*i.e.* the two-valued Boolean algebra) is also called the smallest Boolean algebra.

Ex.1. *If $P(S)$ denote the power set of the nonempty finite set S, then $< P(S), \cup, \cap, \setminus, \phi, S >$ is a Boolean algebra, where the complement of any set $A \subseteq S$ is considered as $S \setminus A$, i.e., the complement of the set A with respect to S.*

Sol. For all elements $X, Y \in P(S)$ since $X \cup Y$ and $X \cap Y \in P(S)$ therefore $\cup$ and $\cap$ operation are the binary operations on $P(S)$ and the set $P(S)$ is closed under the operations $\cup$ and $\cap$. Also for all $X, Y \in P(S)$ we see that $X \cup Y = Y \cup X$ and $X \cap Y = Y \cap X$, therefore commutative laws hold for $P(S)$.

Since for all $\quad X \in P(S), \quad X \cup \phi = X$ and $X \cap S = X$,

therefore ϕ and X are the 0 and 1 of $P(S)$.

We know that the union is distributive over the intersection operation and also the intersection operation distributes the union *i.e.* for $X, Y, Z \in P(S)$

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

and $$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$

Thus distributive laws hold for $P(S)$.

Finally, for each $X \in P(S)$

$$X \cup (S \setminus X) = S \quad \text{and} \quad X \cap (S \setminus X) = \phi$$

therefore the complement laws also hold good.

Hence the given structure is a Boolean algebra.

Ex.2. *Let $B = \{1, 2, 3, 6\}$. If $+, \cdot$ and $'$ are defined as follows :*

For all $a, b \in B$ $\quad a + b = l.c.m\,(a, b)$

$$ab = g.c.d\,(a, b)$$

and $\quad a' = \dfrac{6}{a}, \quad$ *then* $< B, +, \cdot, ', 1, 6 >$ *is a Boolean algebra.*

Sol. Let us construct the composition tables with respect to $+$, $\cdot$ and $'$ operations respectively :

+	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

;

·	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

;

a	a'
1	6
2	3
3	2
6	1

From the above tables, we see that the 0 of the set B (*i.e.* the additive identity) is the integer 6, and 1 of the set B (*i.e.* the multiplicative identity) is the integer 1. It is also clear that the complement of each element of B does exist in B.

We can also see that the closure laws, commutative laws and the distributive laws also do hold for B.

Hence $<B, +, \cdot, ', 1, 6>$ is a Boolean algebra.

Ex.3. If $B = \{1, 2, 4, 8\}$ *and* $+, \cdot$ *and* $'$ *operations are defined as follows :*

For all $a, b \in B$

$$a + b = l.c.m\ (a, b)$$

$$ab = g.c.d\ (a, b)$$

and $$a' = \frac{8}{a}, \quad \textit{then} \quad \{B, +, \cdot, ', 1, 8\}$$

is not a Boolean algebra, since all the Huntington postulates except the complement laws hold good. We see that if we take $a \in B$, *where* $a = 4$, *then*

Sol. $$a + a' = \text{l.c.m}\left(4, \frac{8}{4}\right)$$

$$= \text{l.c.m}\ (4, 2)$$

$$= 4 \neq 8$$

and $$aa' = \text{g.c.d}\left(4, \frac{8}{4}\right)$$

$$= \text{g.c.d}\ (4, 2) = 2 \neq 1$$

where 8 and 1 are the 0 (additive identity) and 1 (multiplicative identity) of B. Thus of each $a \in B$

$$a + a' \neq 8 \quad \text{and} \quad aa' \neq 1.$$

Hence $<B, +, \cdot, ', 1, 8>$ is not a Boolean algebra.

10.3.2 Duality in Boolean algebras :

Each postulate in the definition of Boolean algebra does appear in pair. We can see that one part of the postulate can be obtained from the other if the binary operations and the identity elements are interchanged *i.e.*, if + operation be replaced by the $\cdot$ operation, $\cdot$ operation be replaced by + operation, the 0 of the Boolean algebra be replaced by 1 and 1 of the Boolean algebra be replaced by 0. This property is called the "**Duality principle**" in Boolean algebra and statements appearing in the pair are said to be the **dual** of each other. Thus

"The dual of a statement in a Boolean algebra B is a statement that is obtained by interchanging the + and $\cdot$ operations and interchanging the 0 and 1 in the statement."

For example the dual of the statement $a + ab = a$ is the statement $a \cdot (a + b) = a$.

10.3.3 Boolean sub-algebras :

Let $< B, +, \cdot, ', 0, 1 >$ be a Boolean algebra and $S \subseteq B$. Then the structure $< S, +, \cdot, ', 0, 1 >$ is said to be a **sub-algebra** or a **Boolean sub-algebra** of B if $< S, +, \cdot, ', 0, 1 >$ itself is a Boolean algebra with respect to the binary operations + and · and the unary operation ′ defined on B and consists of the elements 0 and 1 of B.

Note 1 A subset of a Boolean algebra B can be a Boolean algebra but it may or may not be a Boolean sub-algebra of B.

Note 2 Every Boolean sub-algebra of a Boolean algebra B is a Boolean algebra.

Note 3 The Boolean algebra B and $\{0, 1\}$ are always Boolean sub-algebras of B.

Ex.4. *Let D_{30} be the Boolean algebra where $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ [D_{30} is the set of all positive integers that are the divisor of 30], and +, · and ′ on D_{30} are defined as follows :*

$$a + b = l.c.m\,(a, b) \quad \text{for all} \quad a, b \in D_{30}$$

$$ab = g.c.d\,(a, b) \quad \text{for all} \quad a, b \in D_{30}$$

and

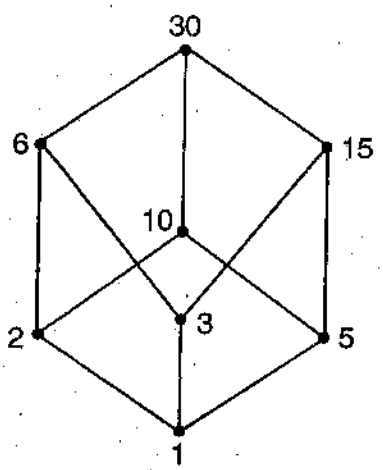
$$a' = \frac{30}{a} \quad \text{for each} \quad a \in D_{30}$$

Then construct

(a) *All the Boolean sub-algebras of D_{30}*

(b) *All Boolean algebras, that are not the Boolean sub-algebras of D_{30} and have atleast four elements*

Sol. Following figure show the Hasse-diagram of D_{30}



(a) **All the Boolean sub-algebras of D_{30} are :**

$$S_1 = \{1, 2, 15, 30\}$$

$$S_2 = \{1, 5, 6, 30\}$$

$$S_3 = \{1, 3, 10, 30\}$$

$S_4 = \{1, 30\}$

$S_5 = \{1, 2, 3, 5, 6, 10, 15, 30\}$

(b) All the Boolean algebras that are not the Boolean sub-algebras of D_{30} are :

$S_6 = \{1, 2, 3, 6\}$

$S_7 = \{1, 3, 5, 15\}$

$S_8 = \{3, 5, 6, 30\}$

$S_9 = \{1, 2, 5, 10\}$

$S_{10} = \{5, 10, 15, 30\}$

$S_{11} = \{2, 6, 10, 30\}$.

Self-learning exercise-1

1. The relation " $\leq$ " in the Boolean lattice $(B, \leq)$ is a .... on B.
2. A lattice $(B, \leq)$ is a Boolean lattice if and only if it is distributive and .... .
3. A finite Boolean lattice $(B, \leq)$ has exactly .... elements for some positive integer n.
4. In a Boolean lattice $(B, \leq)$ if there are two elements $a, b \in B$ such that $a \leq b$ and $a \neq b$. Also for all elements $c \in B$, either $a = c$ or $c = b$, then b is said to be .... of a.
5. In a Boolean lattice $(B, \leq)$, if an element a is a cover of the universal lower bound 0, then a is said to be .... .
6. In the Boolean algebra $< B, +, \cdot, ' >$, the set B consists of atleast .... elements.
7. Amongst the commutative laws, associative laws and the distributive laws, the .... are not the Huntington postulate for the Boolean algebra.
8. The distributive law .... is valid for Boolean algebra, though it is not valid for ordinary algebra.
9. Can we show that $< B, +, \cdot, ', 0, 1 >$ is a Boolean algebra if B consists of exactly six elements ?
10. The dual of the statement $a + (bc) = (a + b)(a + c)$ is ....
11. The dual of the statement $a + ab = a$ is ....
12. The dual of the expression $ab + ac'$ is .... .

10.4 Basic theorems and properties of Boolean algebra

Many theorems and properties of Boolean algebra $< B, +, \cdot, ', 0, 1 >$ can be derived using the postulates in the definition of Boolean algebra.

10.4.1 Idempotent laws :

In a Boolean algebra B, for all elements $a \in B$

(i) $a + a = a$ and *(ii)* $a + a \in B$

Proof : ***(i)*** By closure property for + operation

$$a \in B \Rightarrow a + a \in B$$

Now $a + a = (a + a) \cdot 1$ [by (*B*2)]

$= (a + a)\ (a + a')$ [by (*B*4)]

$= a + aa'$ [by (*B*3)]

$= a + 0$ [by (*B*4)]

$= a$ [by (*B*2)]

Hence $a + a = a.$

(ii) By closure property for · operation

$$a \in B \Rightarrow a \cdot a \in B$$

Now $a \cdot a = a \cdot a + 0$ [by (*B*2)]

$= a \cdot a + a \cdot a'$ [by (*B*4)]

$= a \cdot (a + a')$ [by (*B*3)]

$= a \cdot 1$ [by (*B*4)]

$= a$ [by (*B*2)]

Hence $a \cdot a = a.$

10.4.2 Boundedness laws (Dominance laws) :

In a Boolean algebra B, for all elements $a \in B$

(i) $a + 1 = 1$ and ***(ii)*** $a \cdot 0 \in 0$

Proof : ***(i)*** For all elements $a \in B$

we have $a + 1 = (a + 1) \cdot 1$ [by (*B*2)]

$= (a + 1)\ (a + a')$ [by (*B*4)]

$= a + 1 \cdot a'$ [by (*B*3)]

$= a + a'$ [by (*B*2)]

$= 1$ [by (*B*4)]

(ii) For all elements $a \in B$, we have

$a \cdot 0 = a \cdot 0 + 0$ [by (*B*2)]

$= a \cdot 0 + a\, a'$ [by (*B*4)]

$= a\,(0 + a')$ [by (*B*3)]

$= a\, a'$ [by (*B*2)]

$= 0.$ [by (*B*4)]

10.4.3 Absorption laws :

In the Boolean algebra B, for every two elements $a, b \in B$

(i) $a + a \cdot b = a$ and *(ii)* $a \cdot (a + b) = a$

Proof : *(i)* We have

$$a + ab = a \cdot 1 + ab \qquad \text{[by } (B2)\text{]}$$
$$= a(1 + b) \qquad \text{[by } (B3)\text{]}$$
$$= a(b + 1) \qquad \text{[by } (B1)\text{]}$$
$$= a \cdot 1 \qquad \text{[from 10.4.2]}$$
$$= a. \qquad \text{[by } (B2)\text{]}$$

(ii) $a(a + b) = (a + 0)(a + b) \qquad \text{[by } (B2)\text{]}$
$$= a + 0\,b \qquad \text{[by } (B3)\text{]}$$
$$= a + b \cdot 0 \qquad \text{[by } (B1)\text{]}$$
$$= a + 0 \qquad \text{[from 10.4.2]}$$
$$= a. \qquad \text{[by } (B2)\text{]}$$

10.4.4 Involution law :

In the Boolean algebra B, for each element $a \in B$

$$(a')' = a.$$

Proof : We have $a \in B \Rightarrow a' \in B$

and also $a + a' = 1 \; ; \quad aa' = 0 \qquad \ldots\ldots(1)$

Again $a' \in B \Rightarrow (a')' \in B$

and so $a' + (a')' = 1 \; ; \quad a'(a')' = 0$

or $(a')' + a' = 1 \; ; \quad (a')'\, a' = 0 \qquad \ldots\ldots(2)$

Comparing (1) and (2), we get

$$(a')' = a.$$

10.4.5 Cancellation laws :

In the Boolean algebra B, for all elements $a, b, c \in B$

(i) $b + a = c + a$ and $b + a' = c + a' \Rightarrow b = c$

(ii) $ba = ca$ and $ba' = ca' \Rightarrow b = c$

Proof : *(i)* Given that $b + a = c + a$ and $b + a' = c + a'$

Then $b = b + 0$

$$= b + aa'$$
$$= (b + a)(b + a') \qquad \text{[by } (B3)\text{]}$$
$$= (c + a)(c + a') \qquad \text{[by assumption]}$$

$= c + aa'$ [by $(B3)$]

$= c + 0$

$= c.$

Thus $b + a = c + a$ and $b + a' = c + a' \Rightarrow b = c.$

(ii) Given that $ba = ca$ and $ba' = ca'$

Then $b = b \cdot 1$

$= b \cdot (a + a')$

$= ba + ba'$ [by $(B3)$]

$= ca + ca'$ [by assumption]

$= c \cdot (a + a')$ [by $(B3)$]

$= c \cdot 1$

$= c.$

Thus $b \cdot a = ca$ and $ba' = ca' \Rightarrow b = c.$

10.4.6 Associative laws :

In the Boolean algebra B, for all elements $a, b, c \in B$

(i) $a + (b + c) = (a + b) + c$

(ii) $a\,(b\,c) = (a\,b)\,c$

Proof : *(i)* We have

$a + (b + c) = [a + (b + c)] \cdot 1$

$= [a + (b + c)]\,(c + c')$

$= [a + (b + c)]\,c + [a + (b + c)]\,c'$ [by $(B3)$]

$= [ca + c\,(b + c)] + [c'a + c'(b + c)]$ [by $(B3)$]

$= (ca + c) + (c'a + c'b + c'c)$ (by absorption laws)

$= (c + ca) + (c'(a + b) + 0)$

$= c + c'(a + b)$ [(by absorption laws) and $(B3)$]

$= (c + c')\,[c + (a + b)]$ [by $(B3)$]

$= 1\,[(a + b) + c]$ [by $(B4)$ and $(B1)$]

$= (a + b) + c$

Hence $a + (b + c) = (a + b) + c.$

(ii) We have

$a\,(b\,c) = [a\,(b\,c)] + 0$

$= [a\,(b\,c)] + c\,c'$

$= [a\,(b\,c) + c]\,[a\,(b\,c) + c']$ [by $(B3)$]

$= [(a + c)\,(bc + c)]\,[(a + c')\,(bc + c')]$ [by $(B3)$]

$= [(a + c) \cdot c]\ [(a + c')\ (b + c')\ (c + c')]$ (by absorption laws)

$= c\ [(a\ b + c') \cdot 1]$ [(by absorption laws) and (*B*3)]

$= c\ (a\ b) + cc'$ [by (*B*3)]

$= (a\ b)\ c + 0$ [by (*B*1) and (*B*4)]

$= (a\ b)\ c$

Hence $a\ (b\ c) = (ab)\ c.$

10.4.7 De-Morgan's laws :

In the Boolean algebra B, for all elements $a, b \in B$

(i) $(a + b)' = a'b'$

(ii) $(a\ b)' = a' + b'$

Proof : ***(i)*** In order to prove that

$(a + b)' = a'b'$, we must show that

$(a + b) + a'b' = 1$

and $(a + b)\ (a'b') = 0$

Now $(a + b) + a'b' = [(a + b) + a']\ [(a + b) + b']$ [by (*B*3)]

$= [a' + (a + b)]\ [(a + b) + b']$

$= [(a' + a) + b]\ [(a + (b + b')]$ (from 10.4.6)

$= (1 + b)\ (a + 1)$ [by (*B*4)]

$= 1 \cdot 1$

$= 1$ .....(1)

and $(a + b)\ (a'b') = a\ (a'b') + b\ (a'b')$

$= aa'\ b' + b\ (b'a')$ [by (*B*1) and 10.4.6]

$= 0\ b' + (bb')\ a'$ [by (*B*4) and 10.4.6]

$= 0 + 0\ a'$

$= 0 + 0$

$= 0$ .....(2)

From (1) and (2) we conclude that

$(a + b)' = a'b'$

(i) In order to prove that

$(a\ b)' = a' + b'$, we must show that

$ab + (a' + b') = 1$ and $ab\ (a' + b') = 0$

Now $ab + (a' + b') = [a + (a' + b')]\ [b + (a' + b')]$ [by (*B*3)]

$$= [(a + a') + b'] [(a' + b') + b] \qquad \text{[by 10.4.6 and } (B1)\text{]}$$

$$= [1 + b'] [a' + (b' + b)] \qquad \text{[by } (B4) \text{ and 10.4.6]}$$

$$= 1 \, (a' + 1)$$

$$= 1 \cdot 1$$

$$= 1 \qquad \text{.....(3)}$$

and $$a \, b \, (a' + b') = (a \, b) \, a' + (a \, b) \, b'$$

$$= a' (a \, b) + a \, (b \, b')$$

$$= (a' a) \, b + a \cdot 0$$

$$= 0 \cdot b + 0$$

$$= 0 + 0$$

$$= 0 \qquad \text{.....(4)}$$

From (3) and (4) we conclude that

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

Theorem 1. *In a Boolean algebra* $< B, +, \cdot, ', 0, 1 >$.

(i) *The additive identity (i.e. 0 of B) is unique*

(ii) *The multiplicative identity (i.e. 1 of B) is unique and*

(iii) *Complement of each element is unique.*

Proof : ***(i)*** If possible, let 0_1 and $0_2 \in B$ be two distinct 0 of the Boolean algebra B.

Now since 0_1 is the 0 of B, therefore for all $a \in B$,

$$a + 0_1 = a = 0_1 + a$$

and since $0_2 \in B$,

so $$0_2 + 0_1 = 0_2 = 0_1 + 0_2 \qquad \text{.....(1)}$$

Again since 0_2 is the 0 of B, so for all $a \in B$,

$$a + 0_2 = a = 0_2 + a$$

and since $0_1 \in B$,

therefore $$0_1 + 0_2 = 0_1 = 0_2 + 0_1 \qquad \text{.....(2)}$$

From (1) and (2) we have

$$0_1 = 0_2. \qquad \text{[using } (B1)\text{]}$$

i.e., 0 of B is unique.

(ii) If possible, let 1_1 and 1_2 be two distinct 1 of B.

Now since 1_1 is the 1, of B, therefore for all $a \in B$,

$$a \cdot 1_1 = a = 1_1 \cdot a$$

and since $1_2 \in B$,

so $$1_2 \cdot 1_1 = 1_2 = 1_1 \, 1_2 \qquad \text{.....(3)}$$

Again since 1_2 is also 1 of B, so for all $a \in B$,

$$a \cdot 1_2 = a = 1_2 \cdot a$$

and as $1_1 \in B$,

so $$1_1 \cdot 1_2 = 1_1 = 1_2 \cdot 1_1 \qquad \text{.....(4)}$$

From (3) and (4) we have

$$1_1 = 1_2.$$

Hence 1 of B is unique.

(iii) If possible, let b and $c \in B$ be two distinct complements of the element $a \in B$, then

$$a + b = 1 \; ; \; ab = 0$$

and $$a + c = 1 \; ; \; ac = 0$$

Now

$$\begin{aligned} b &= b + 0 = b + ac && (\because\ ac = 0) \\ &= (b + a)\,(b + c) && \text{[by } (B3)\text{]} \\ &= (a + b)\,(b + c) \\ &= 1\,(b + c) && (\because\ a + b = 1) \\ &= (a + c)\,(b + c) && (\because\ a + c = 1) \\ &= ab + c && \text{[by } (B3)\text{]} \\ &= 0 + c && (\because\ ab = 0) \\ &= c. \end{aligned}$$

Thus $b = c$, *i.e.*, the complement of $a \in B$ is unique.

Theorem 2. *In a Boolean algebra B, if* 0 *and* 1 *are the additive and multiplicative identities of B, then*

(i) $0' = 1$ ***(ii)*** $1' = 0$

Proof : ***(i)***

$$\begin{aligned} 0' &= (a\,a')', \quad \text{for} \quad a \in B \\ &= a'(a')' && \text{[by De-Morgan's laws]} \\ &= a' + a && [\because\ a = (a')'] \\ &= 1. && \text{[by } (B4)\text{]} \end{aligned}$$

(ii)

$$\begin{aligned} 1' &= (a + a')', \quad \text{for} \quad a \in B \\ &= a'(a')' && \text{[by De-Morgan's laws]} \\ &= a'a && (\because\ a = (a')') \\ &= 0. && \text{[by } (B4)\text{]} \end{aligned}$$

Ex.5. *In a Boolean algebra B, show that*

$$a = b \quad \text{if and only if} \quad a\,b' + a'b = 0.$$

Sol. Let $a\,b' + a'b = 0$.

Then

$$\begin{aligned} a &= a + 0 = a + a\,b' + a'b \\ &= a + a'b && \text{(by absorption law)} \\ &= (a + a')\,(a + b) \end{aligned}$$

$$= 1\,(a + b)$$

$$= a + b \qquad \text{.....(1)}$$

Again $b = b + 0 = b + a\,b' + a'b$

$$= a\,b' + a'b + b$$

$$= a\,b' + b \qquad \text{(by absorption law)}$$

$$= (a + b)\,(b' + b)$$

$$= (a + b) \cdot 1$$

$$= a + b \qquad \text{.....(2)}$$

From (1) and (2), we get

$$a = b$$

thus $a\,b' + a'b = 0 \Rightarrow a = b$

Now let $a = b$

then $a\,b' + a'b = b\,b' + a'a$

$$= 0 + 0$$

$$= 0$$

Thus $a = b \Rightarrow a\,b' + a'b = 0$

Hence $a = b$ if and only if $a\,b' + a'b = 0$.

Ex.6. *In a Boolean algebra B, the following are equivalent :*

(i) $a + b = b$ ***(ii)*** $a \cdot b = a$

(iii) $a' + b = 1$ ***(iv)*** $a\,b' = 0$

Sol. First of all let $a + b = b$

Then $a \cdot b = a\,(a + b)$

$$= a \qquad \text{(by absorption law)}$$

$\therefore$ $a + b = b \Rightarrow ab = a$

Now let $ab = a$

Then $a + b = ab + b$

$$= b + ba$$

$$= b \qquad \text{(by absorption law)}$$

therefore, $\boldsymbol{a + b = b \Leftrightarrow ab = a.}$

Now if $a + b = b$,

then $a' + b = a' + (a + b)$

$$= (a' + a) + b$$

$$= 1 + b$$

$$= 1$$

Therefore, $a + b \Rightarrow a' + b = 1$

Now if $a' + b = 1$,

then $a + b = (a + b) \cdot 1$

$= (a + b)(a' + b)$

$= aa' + b$ [by (*B*3)]

$= 0 + b$

$= b$

Therefore, $\boldsymbol{a + b = b \Leftrightarrow a' + b = 1}$

Now if $a' + b = 1$,

then $a' + b = 1 \Rightarrow (a' + b)' = 1'$

$\Rightarrow (a')' b' = 0$ (by De-Morgan's law)

$\Rightarrow ab' = 0$

Thus $a' + b = 1 \Rightarrow ab' = 0$

and if $ab' = 0$

Then $ab' = 0 \Rightarrow (ab')' = 0'$

$\Rightarrow a' + (b')' = 1$ (by De-Morgan's law)

$\Rightarrow a' + b = 1$

Thus $ab' = 0 \Rightarrow a' + b = 1$

Therefore, $\boldsymbol{a' + b = 1 \Leftrightarrow ab' = 0}$

Hence *(i)* $\Leftrightarrow$ *(ii)* $\Leftrightarrow$ *(iii)* $\Leftrightarrow$ *(iv)*.

Ex 7. *In the Boolean algebra B, for elements a, b, c* $\in B$,

$a + b = a + c$ and $ab = ac \Rightarrow b = c$.

Sol. Given that $a + b = a + c$ and $ab = ac$

Then $b = b \cdot (b + a)$ (by absorption law)

$= b(a + b)$

$= b(a + c)$ $(\because a + b = a + c)$

$= ba + bc$

$= ab + bc$

$= ac + bc$ $(\because ab = ac)$

$= (a + b)c$

$= (a + c)c$ $(\because a + b = a + c)$

$= c$ (by absorption law)

Hence $a + b = a + c$ and $ab = ac \Rightarrow b = c$.

Ex.8. *In the Boolean algebra B, prove that for elements a, b, c ∈ B*

(i) $(a+b)(a'+c)(b+c) = ac + a'b + bc$

(ii) $(a+b)' + (a+b')' = a'$

(iii) $ab + a'b' = (a+b')(a'+b)$

Sol. ***(i)*** $(a+b)(a'+c)(b+c) = (a+b)(a'b+c)$

$= (a+b)\,a'b + (a+b)\,c$

$= a(a'b) + b(a'b) + ac + bc$

$= (aa')\,b + a'(bb) + ac + bc$

$= 0 \cdot b + a'b + ac + bc$

$= 0 + ac + a'b + bc$

$= ac + a'b + bc$

(ii) $(a+b)' + (a+b')' = [(a+b)(a+b')]'$ (by De-Morgan's law)

$= (a + bb')'$ [by $(B3)$]

$= (a+0)'$

$= a'$

(iii) $ab + a'b' = [ab + a'][ab + b']$ [by $(B3)$]

$= [(a+a')(b+a')][(a+b')(b+b')]$

$= [1\,(b+a')][(a+b') \cdot 1]$

$= (a+b')(a'+b).$

Self-learning exercise-2

1. If $a + b, = b$ then $a'. + b = \ldots\ldots$.

2. If $a' + b = 1$ then $ab' = \ldots\ldots$.

3. In the Boolean algebra B, $a + b = b \Rightarrow ab = \ldots\ldots$.

4. In the Boolean algebra B,

$$a = b \Rightarrow ab' + a'b = \ldots\ldots .$$

5. In the Boolean algebra B, if

$$a + b = 1 \text{ and } ab = 0, \text{ then } b = \ldots\ldots .$$

6. In the Boolean algebra B, for all $a, b \in B$

$$(a'+b)(a'+b')(a+b') = \ldots\ldots .$$

7. In the Boolean algebra B, for all elements $a, b \in B$,

$$(a + a'b)(a' + ab) = \ldots\ldots .$$

8. In the Boolean algebra B,

$$a + a'b = \ldots\ldots .$$

10.5 Summary

In this unit we first defined the Boolean lattices and then the lattice system defined by the Boolean lattice, which is known as Boolean algebra. We also defined the Boolean algebra using the postulates formulated by Huntington.

We also studied the smallest Boolean algebra, having great importance in the field of switching algebra. Some theorems and basic laws of Boolean algebras were also derived followed by some examples.

10.6 Answers to the self-learning exercises

Self-learning exercise-1

1. partial order relation.

2. complemented.

3. 2^n

4. a cover

5. an atom

6. two distinct

7. associative laws

8. $a + (bc) = (a + b)(a + c)$

9. No (as 6 is not of the form 2^n for any positive integer n)

10. $a(b + c) = ab + ac$

11. $a(a + b) = a$.

12. $(a + b)(a + c')$

Self-learning exercise-2

1. 1 **2.** 0 **3.** a **4.** 0

5. a' **6.** $a'b'$ **7.** b **8.** $a + b$

10.7 Exercises

1. Demonstrate by means of truth table, the validity of the De-Morgan's laws for three variables, *i.e.*,

$$(a + b + c)' = a'b'c'$$

and $$(abc)' = a' + b' + c'$$

2. Demonstrate by means of truth table the validity of the distributive laws, *i.e.*,

$$a + bc = (a + b)(a + c)$$

and $$a(b + c) = ab + ac.$$

3. Prove the following Boolean identities :

(i) $acb + a\,b'c + a\,b\,c' = a\,(b + c)$

(ii) $[(ab)' + a' + ab)' = 0$

(iii) $ab + abc + a\,b\,c' + a\,b'c = b\,(a + c)$

(iv) $abc + a'b\,c + a\,b'c + a\,b\,c' = ab + bc + ca$

(v) $(a + a'b)\,(a' + ab) = b$

(vi) $a + b = a + c$ and $ab = ac \Rightarrow b = c$

4. Prove that, there can not exactly three distinct elements in any Boolean algebra.

□□□

Unit 11 : Boolean Expressions and Boolean Functions

Structure of the Unit

11.0 Objectives

This unit has been written to introduce the students with the expressions and the functions generated by the elements of the Boolean algebra. The unit intends too introduce the different standard forms of these expressions and the functions that help apply the Boolean algebra in a more specific way.

11.1 Introduction

This unit the definitions of Boolean expressions and Boolean functions and is progressed with various standard forms of the Boolean functions "sum of the minterms *i.e.* Disjunctive Normal Form" and "product of maxterms *i.e.* Conjunctive Normal Form". Boolean expressions are practically implemented in the form of digital logic gates in the electronic circuits. The cost of these circuits depends upon the numbers of gates in the circuits. Algebraic method is given for simplification of Boolean expressions that reduces the number of gates in a circuit, hence the cost of the circuit.

11.2 Boolean expressions

Before giving the definition of Boolean expression, we shall first define "Boolean variable" and "Literal".

11.2.1 Boolean variables :

A symbol x, representing an arbitrary element of a Boolean algebra $< B, +, \cdot, ', 0, 1 >$ is said to be a Boolean variable of the Boolean algebra B. Thus a variable x is a Boolean variable of B if it takes on only values in B. Consequently $x + x = x$ and $x\,x = x$, for every Boolean variable $x \in B$. Also if x and y are any two boolean variables in B, then

(i) $x + y = 0$ if and only if $x = y = 0$

(ii) $x\,y = 1$ if and only if $x = y = 1$.

11.2.2 Literals :

A literal x^* is defined to be a Boolean variable x or its complement x'. Thus $x^* = x$ or x'. The product of two or more literals, in which no two literals have the same variable is said to be a "fundamental product". Thus $x_1\,x_2\,x'_3, x'_1\,x_2\,x_3, x_1\,x'_2$ are all the fundamental products.

11.2.3 Boolean expressions :

By a Boolean expression over the Boolean algebra $< B, +, \cdot, ', 0, 1 >$, we mean an expression built up from the Boolean variables by applying the operations $+$, $\cdot$ and $'$ finite number of times. Thus a Boolean expression generated by elements of n-tuple $\overline{x} = (x_1, x_2, ..., x_n)$ over the Boolean algebra B can be defined as :

(i) Every Boolean variable name is a Boolean expression over B.

(ii) If x and y are any two Boolean expressions over the Boolean algebra B, then $x', y', x + y, x + y', xy, x'y, x + x'y$ etc.-etc. are also the Boolean expressions over B.

The Boolean expressions generated by elements of n-tuple $\overline{x} = (x_1, x_2, ..., x_n)$ are denoted by $E(x_1, x_2, ..., x_n)$. If $E(x_1, x_2, ..., x_n)$ is a Boolean expression over the Boolean algebra B, then it is not necessary that $E(x_1, x_2, ..., x_n)$ must involve all the n variables $x_1, x_2, ..., x_n$.

If $E = (x_1, x_2, ..., x_n)$ is a Boolean expression over the Boolean algebra B, then we can evaluate the expression $E = (x_1, x_2, ..., x_n)$ by substituting the variables in the expression by their values. For example if $E = (x_1, x_2, x_3) = (x_1 + x_2)(x'_1 + x'_2)(x'_1 + x_2)'$ is any Boolean expression over the Boolean algebra $< B, +, \cdot, ', 0, 1 >$, where $B = \{0, 1\}$, then assigning the values $x_1 = 0$, $x_2 = 0$ and $x_3 = 1$ the expression yields

$$E(0, 0, 1) = (0 + 0)(1 + 1)(1 + 0)'$$
$$= 0 \cdot 1 \cdot 0 = 0.$$

11.2.4 Equivalent Boolean expressions :

Two Boolean expressions generated by n variables, over the same Boolean algebra B are said to be equivalent if they assume the same value for every assignment of values to these n variables of B. For example the Boolean expressions $x_1 x_2 + x'_3$ and $(x_1 + x'_3)(x_2 + x'_3)$ are equivalent. We can write them as

$$x_1 x_2 + x'_3 = (x_1 + x'_3)(x + x'_3).$$

If the elements of the n-tuple $\bar{x} = (x_1, x_2, ..., x_n)$ are the Boolean variables that assume only values in the Boolean algebra B, then the Boolean expression $E = (x_1, x_2, ..., x_n)$ represents the elements in B. In such a case the Boolean expression is said to be a Boolean function over B generated by the n-tuple $\bar{x} = (x_1, x_2, ..., x_n)$ in B. We shall now give the formal definition of Boolean function.

11.2.5 Boolean functions :

Let $< B, +, \cdot, ', 0, 1 >$ be the Boolean algebra. Then the function $f : B^n \to B$, where $f(\bar{x})$ can be determined using the elements of n-tuple $\bar{x} = (x_1, x_2, ..., x_n)$, $x_i \in B$ for $i = 1, 2, ..., n$ and the operations $+$, $\cdot$ and $'$, is said to be a Boolean function of n-tuple $\bar{x} = (x_1, x_2, ..., x_n)$, over B. We write it as $f = (x_1, x_2, ..., x_n)$, Thus the Boolean function $f = (x_1, x_2, ..., x_n)$, of n variables is a function form B_n to B if it can be specified by the Boolean expression $E = (x_1, x_2, ..., x_n)$, for example if $E = (x_1, x_2, x_3) = x_1 x'_2 + x_2 x_3 + x'_1$ is the Boolean expression over the Boolean algebra $< B, +, \cdot, ', 0, 1 >$ where $B = \{0, 1\}$ then $f = (x_1, x_2, x_3) = x_1 x'_2 + x_2 x_3 + x'_1$ is the Boolean function from B^3 to B. The functional value of this function for the values $x_1 = 1, x_2 = 1, x_3 = 0$ is

$$f(1, 1, 0) = 1 \cdot 1' + 1 \cdot 0 + 1' = 0 + 0 + 0$$
$$= 0$$

The functional values of the above Boolean function $f = (x_1, x_2, x_3) = x_1 x_2' + x_2 x_3 + x'_1$ for all possible values of 3-tuple $\bar{x} = (x_1, x_2, x_3) \in B^3$ over $B = \{0, 1\}$ are :

$\bar{x} = (x_1, x_2, x_3)$	$f(x_1, x_2, x_3) = x_1 x_2' + x_2 x_3 + x_1'$
(0, 0, 0)	$0 \cdot 0' + 0 \cdot 0 + 0' = 1$
(0, 0, 1)	$0 \cdot 0' + 0 \cdot 1 + 0' = 1$
(0, 1, 0)	$0 \cdot 1' + 1 \cdot 0 + 0' = 1$
(0, 1, 1)	$0 \cdot 1' + 1 \cdot 1 + 0' = 1$
(1, 0, 0)	$1 \cdot 0' + 0 \cdot 0 + 1' = 1$
(1, 0, 1)	$1 \cdot 0' + 0 \cdot 1 + 1' = 1$
(1, 1, 0)	$1 \cdot 1' + 1 \cdot 0 + 1' = 0$
(1, 1, 1)	$1 \cdot 1' + 1 \cdot 1 + 1' = 1$

11.2.6 Complement of a Boolean function :

The dual of the Boolean function $f = (x_1, x_2, ..., x_n)$ on the Boolean algebra B is obtained by replacing 0's by 1's, 1's by 0's, + by · and · by + in the functional value of f. The complement $f' = (x_1, x_2, ..., x_n)$ of the Boolean function $f = (x_1, x_2, ..., x_n)$ is obtained by first taking the dual of the function $f = (x_1, x_2, ..., x_n)$ and then complementing each literal involved in the function. As an example the complement of the Boolean function

$$f = (x_1, x_2, x_3) = x_1'(x_2 + x_3) + x_1 \cdot x_3' \text{ is}$$

$$f'(x_1, x_2, x_3) = \left[x_1'(x_2 + x_3) + x_1 x_3'\right]'$$

$$= \left[x_1'(x_2 + x_3)\right]' \cdot \left[x_1 x_3'\right]'$$

$$= \left[x_1 + (x_2 + x_3)'\right]\left[x_1' + x_3\right]$$

$$= \left[x_1 + x_2' \; x_3'\right]\left[x_1' + x_3\right]$$

Self-learning exercise-1

1. A literal is defined to be a Boolean variable or its ..... .
2. If x is a Boolean variable, then x and x' are called ..... .
3. The product of two or more literals in which no two literals involve the same variable is called a ..... .
4. $x'_1 + x_2 x_3$ and $(x_1' + x_2)(x'_1 + x_3)$ are ..... Boolean expressions.
5. If x is a Boolean variable, then x is a Boolean expression : yes or no.

11.3 Representation of Boolean expressions

Consider the Boolean expression $f = (x_1, x_2, x_3) = x_1 x_2 + x_1 x_3$. In this expression, x_1, x_2 and x_3 are literals and we know that a literal is a primed or an unprimed Boolean variable. When the

Boolean expressions are implemented we need to minimize literals and the numbers of terms. Generally the literals and terms are arranged in one of the two standard forms.

(i) Sum of the products form (SOP) and

(ii) product of the sums form (POS).

11.3.1 Sum of Products form :

The words sum and products are derived form the symbolic forms of the OR and AND functions by + and · (addition and multiplication) respectively. These are not the arithmetic operators in usual sence. A product term is a sequence of literals that are ANDed together and a sum term ORed together. For example, x_1x_2, x_1x_3, $x_1'x_2'x_3$ etc.-etc. are the product terms where as $x_1 + x_2$, $x_1' + x_2 + x_3'$, $x_1' + x_3'$ etc.-etc. the sum terms. A sum of products form (SOP) is a sequence of product terms ORed together. For example

$$x_1 x_2 x_3 + x_1 x_3, x_1 x_2 + x_1 x_2' x_3' + x_2 x_3, x_1 x_2' + x_2 x_3' + x_1' x_2 x_3$$

are the sum of products form of the Boolean expressions.

Each of these sum of products forms consist of two or more product terms (AND) that are ORed together and each product term consists of one or more literals appearing in either primed or unprimed form.

11.3.2 Product of sums form :

A product of sums form of a Boolean expression is a sequence of sum terms that are ANDed together. For example $(x_1 + x_2)(x_2 + x'_3)$, $(x_1 + x_2 + x'_3)(x'_1 + x'_2 + x_3)$ are the product of sums form of the Boolean expressions. Each of these product of sums form consists of two or more sum terms (OR) that are ANDed together and each sum term consists of one or more literals appearing in either primed or unprimed form.

Ex.1. *Transform the Boolean expression* $x_1 x_2 + x_1 x'_2 (x'_1 x'_3)'$ *into sum of products form.*

Sol.
$$E(x_1, x_2, x_3) = x_1 x_2 + x_1 x_2' (x_1' x_3')'$$
$$= x_1 x_2 + x_1 x_2' (x_1 + x_3) \text{ (by De-Morgan's law)}$$
$$= x_1 x_2 + x_1 x_2' x_1 + x_1 x_2' x_3$$
$$= x_1 x_2 + x_1 x_2' + x_1 x_2' x_3.$$

Ex.2. *Transform the Boolean expression* $\left((x_1x_2)' x_3\right)' \cdot \left((x_1' + x_3)(x_2' + x_3')\right)'$ *into the sum of products form.*

Sol. Here $E(x_1, x_2, x_3) = \left((x_1 x_2')x_3\right)' \left((x_1' + x_3)(x_2' + x_3')\right)'$

$$= \left[\left((x_1\, x_2)'\right)' + x_3'\right]\left[(x_1' + x_3)' + (x_2' + x_3')'\right]$$

$$= [x_1\, x_2 + x_3'][x_1\, x_3' + x_2\, x_3]$$

$$= x_1\, x_2\, x_1\, x_3' + x_1\, x_2\, x_2\, x_3 + x_3'\, x_1\, x_3' + x_3'\, x_2\, x_3$$

$$= x_1\, x_2\, x_3' + x_1\, x_2\, x_3 + x_1\, x_3'$$

$$= x_1\, x_3' + x_1\, x_2\, x_3' + x_1\, x_2\, x_3$$

$$= x_1\, x_3' + x_1\, x_2\, x_3 \qquad \text{[by absorption law]}$$

Ex.3. *Transform the Boolean expression* $x_2\, x_3 + (x_2' x_3' + x_1'\, x_3)'$ *into product of sums form.*

Sol. $E(x_1, x_2, x_3) = x_2\, x_3 + (x_2' x_3' + x_1'\, x_3)'$

$$= x_2\, x_3 + (x_2'\, x_3')' \cdot (x_1'\, x_3)'$$

$$= x_2\, x_3 + (x_2 + x_3)(x_1 + x_3')$$

$$= [x_2\, x_3 + (x_2 + x_3)][x_2 x_3 + (x_1 + x_3')]$$

$$= (x_2 + x_2 + x_3)(x_3 + x_2 + x_3)(x_2 + x_1 + x_3') \cdot (x_3 + x_1 + x_3')$$

$$= (x_2 + x_3)(x_2 + x_3)(x_1 + x_2 + x_3')(x_1 + 1)$$

$$= (x_2 + x_3)(x_1 + x_2 + x_3') \cdot 1$$

$$= (x_2 + x_3)(x_1 + x_2 + x_3').$$

11.4 Minterms (standard products) and maxterms (standard sums)

The concept of the minterms and the maxterms yields to introduce a very convenient and shorthand notations to express logical functions.

11.4.1 Minterms (standard products) :

A Boolean expression (or a Boolean function) generated by n-tuple $\bar{x} = (x_1, x_2, ..., x_n)$ is said to be a **minterm** or a **standard product** if it can be expressed in the form of product of n distinct literals $x_1^*, x_2^*, ..., x_n^*$. Thus a minterm in n Boolean variables $x_1, x_2, ..., x_n$ is a Boolean expression of the form $x_1^*, x_2^*, ..., x_n^*$, where each x_i^* is either x_i or x_i' for $i = 1, 2, ..., n$.

For example, there can be formed four minterms $x_1' x_2', x_1' x_2, x_1 x_2'$ and $x_1 x_2$ generated by two variables x_1 and x_2 in $B = \{0, 1\}$. Similarly the 3-tuple $\bar{x} = (x_1, x_2, x_3)$ in B^3 where $B = \{0, 1\}$ generate in all 2^3, *i.e.*, eight minterms namely

$$x_1' x_2' x_3', x_1' x_2' x_3, x_1' x_2 x_3', x_1' x_2 x_3, x_1 x_2' x_3', x_1 x_2' x_3, x_1 x_2 x_3', \text{ and } x_1 x_2 x_3.$$

In general, n variables $x_1, x_2, \ldots, x_n$ in the Boolean algebra B, generate 2^n minterms, where each minterm is obtained from an "and" term (*i.e.* the standard product term) of n literals, with each literal being primed if the corresponding bit of the binary number is 0 and unprimed if the corresponding bit is 1. The minterm is symbolized as m_i ($i = 0, 1, 2, \ldots, n-1$). The minterms satisfy the following two properties :

(i) $m_i m_j = 0$; for all $i \neq j$

(ii) $\sum_{i=0}^{2^n-1} m_i = 1.$

11.4.2 Maxterms (Standard Sums) :

A Boolean expression (or a Boolean function), generated by n-tuple $\bar{x} = (x_1, x_2, \ldots, x_n)$ is said to be a **maxterm** or a **standard sum** if it can be expressed in the form of sum of n distinct literals $x_1^*, x_2^*, \ldots, x_n^*$. Thus a maxterm in n Boolean variables $x_1, x_2, \ldots, x_n$ is a Boolean expression of the form $x_1^* + x_2^* + \ldots + x_n^*$, where each x_i^* is either x_i or x'_i for $i = 1, 2, \ldots, n$.

Thus there are four maxterms $x_1 + x_2$, $x_1 + x_2'$, $x_1' + x_2$ and $x_1' + x_2'$, generated by two variables x_1 and x_2 in the Boolean algebra $B = \{0, 1\}$. Similarly three variables x_1, x_2, x_3 in $B = \{0, 1\}$ generate 2^3 *i.e.* eight maxterms namely

$x_1 + x_2 + x_3$, $x_1 + x_2 + x_3'$, $x_1 + x_2' + x_3$, $x_1 + x_2' + x_3'$, $x_1' + x_2 + x_3$, $x_1' + x_2 + x_3'$, $x_1' + x_2' + x_3$ and $x_1' + x_2' + x_3'$.

In general n variables $x_1, x_2, \ldots, x_n$ in the Boolean algebra $B = \{0, 1\}$, generate 2^n maxterms, where each maxterm is obtained from an "or" (*i.e.* the standard sum term) of n literals, with each literal being unprimed if the corresponding bit of the binary number is 0 and primed if the corresponding bit is 1. The maxterm is generally symbolized as M_i ($i = 0, 1, 2, \ldots, n-1$). It can also be noticed that the maxterms do satisfy the following two important properties

(i) $M_i + M_j = 1$; for all $i \neq j$,

(ii) $\prod_{i=0}^{2^n-1} M_i = 0.$

The definitions of minterms and the maxterms yield a close relationship between them. We can note that every maxterm can be obtained by complementing its corresponding minterm and vice-versa, as is clear form the following table of minterms and maxterms for three binary variables x_1, x_2, x_3 in $B = \{0, 1\}$:

x_1	x_2	x_3	Minterms		Maxterms	
			Term	m_i	Term	M_i
0	0	0	$x_1' x_2' x_3'$	m_0	$x_1 + x_2 + x_3$	M_0
0	0	1	$x_1' x_2' x_3$	m_1	$x_1 + x_2 + x_3'$	M_1
0	1	0	$x_1' x_2 x_3'$	m_2	$x_1 + x_2' + x_3$	M_2
0	1	1	$x_1' x_2 x_3$	m_3	$x_1 + x_2' + x_3'$	M_3
1	0	0	$x_1 x_2' x_3'$	m_4	$x_1' + x_2 + x_3$	M_4
1	0	1	$x_1 x_2' x_3$	m_5	$x_1' + x_2 + x_3'$	M_5
1	1	0	$x_1 x_2 x_3'$	m_6	$x_1' + x_2' + x_3$	M_6
1	1	1	$x_1 x_2 x_3$	m_7	$x_1' + x_2' + x_3'$	M_7

Any Boolean function can be expressed from the given truth table by forming a minterm for all possible combinations of the values of the Boolean variables that produce 1 as the functional value and than taking the sum of all the minterms corresponding these 1's. For example if we consider the functions $f_1(x_1, x_2, x_3)$ and $f_2(x_1, x_2, x_3)$ whose functional values for all possible combinations of variables x_1, x_2, x_3 are shown in the following table :

x_1	x_2	x_3	$f_1(x_1, x_2, x_3)$	$f_1(x_1, x_2, x_3)$
0	0	0	1	0
0	0	1	0	1
0	1	0	0	0
0	1	1	0	1
1	0	0	1	0
1	0	1	1	0
1	1	0	0	1
1	1	1	1	0

then the function $f_1(x_1, x_2, x_3)$ can be determined by expressing the combinations 000, 100, 101 and 111 (corresponding to the functional values 1) as $x_1' x_2' x_3'$, $x_1 x_2' x_3'$, $x_1 x_2' x_3$ and $x_1 x_2 x_3$ respectively.

Since each of these minterms has the functional value 1, therefore we can write $f_1(x_1, x_2, x_3)$ as

$$f_1(x_1, x_2, x_3) = x_1' x_2' x_3' + x_1 x_2' x_3' + x_1 x_2' x_3 + x_1 x_2 x_3$$

$$= m_0 + m_4 + m_5 + m_7$$

It is more convenient to express the above function as :

$$f_1(x_1, x_2, x_3) = \Sigma(0, 4, 5, 7)$$

Similarly the Boolean function $f_2(x_1, x_2, x_3)$ can be expressed as

$$\begin{aligned} f_2(x_1, x_2, x_3) &= x_1' x_2' x_3 + x_1' x_2 x_3 + x_1 x_2 x_3' \\ &= m_1 + m_3 + m_6 \\ &= \sum (1, 3, 6). \end{aligned}$$

The above example justifies the property of the Boolean algebra : "**Every Boolean function can be expressed as the sum of minterms**".

The complement of the function $f_1(x_1, x_2, x_3)$ in the table can be obtained by expressing the combination 001, 010, 011 and 110 as $x_1' x_2' x_3$, $x_1' x_2 x_3'$, $x_1' x_2 x_3$ and $x_1 x_2 x_3'$ respectively, where each one of the minterms assumes the value 0 of f_1. Therefore, we have

$$f'_1(x_1, x_2, x_3) = x_1' x_2' x_3 + x_1' x_2 x_3' + x_1' x_2 x_3 + x_1 x_2 x_3'$$

The complement of the above function $f'_1(x_1, x_2, x_3)$ is

$$\begin{aligned} f_1(x_1, x_2, x_3) &= (x_1 + x_2 + x_3')(x_1 + x_2' + x_3)(x_1 + x_2' + x_3')(x_1' + x_2' + x_3) \\ &= M_1 M_2 M_3 M_6 \\ &= \prod (1, 2, 3, 6). \end{aligned}$$

In a similar way the function $f_2(x_1, x_2, x_3)$ can also be expressed as

$$\begin{aligned} f_2(x_1, x_2, x_3) &= (x_1 + x_2 + x_3)(x_1 + x_2' + x_3)(x_1' + x_2 + x_3)(x_1' + x_2 + x_3')(x_1' + x_2' + x_3') \\ &= M_0 M_2 M_4 M_5 M_7 \\ &= \prod (0, 2, 4, 5, 7). \end{aligned}$$

This yields another important property of Boolean algebra – "**Every Boolean function can be expressed as the product of maxterms**".

The Boolean function when expressed as the sum of minterms or the product of maxterms are called in **"Canonical form"**.

11.5 Canonical forms of Boolean functions

We just saw that the Boolean algebra have properties that every Boolean function over the Boolean algebra B can be expressed as the sum of minterms and product of maxterms. These forms of the Boolean function are called the canonical forms. The canonical form of the Boolean function when it is represented as the sum of minterms is also called the "Disjunctive Normal Form" and when it is represented as the product of maxterms is called the "Conjunctive Normal Form" of the Boolean function.

11.5.1 Disjunctive normal form (DNF) :

A Boolean function $f(x_1, x_2, ..., x_n)$ over the Boolean algebra B is said to be in its **disjunctive normal form,** if it is expressible in the form $f(x_1, x_2, ..., x_n) = m_0 + m_1 + ... + m_k$ where each m_i ; $i = 0, 1, 2, ..., k$ is a minterm.

Now since the disjunctive normal form of the Boolean function is the sum of minterms and each minterm is the product of distinct literals, therefore, the disjunctive normal form is also called the **sum of standard product form** or the **minterm form.**

The representation of Boolean function in its disjunctive normal form is very simple as is described below :

(i) Simplify the given Boolean function, such that it has minimum number of terms in the form of sum.

(ii) Multiply each term in the sum by as many 1's equal to the number of missing literals in the respective term (For example if there are two literals x_j^* and x_k^* missing in a term of the Boolean function $f(x_1, x_2, ..., x_n)$ then multiply this term twice by 1).

(iii) Replace each 1 in the term by $x_i + x'_i$, if this 1 appears in the term due to the missing literal x_i^*, if this 1 appears in the term due to the missing literal x_i^*. (If there are two 1's in the term that correspond to the missing literals x_j^* and x_k^*, then replace the first 1 by $x_j + x'_j$ and the other 1 by $x_k + x'_k$)

(iv) Apply the distributive laws, commutative laws and the idempotent laws etc.

The resulting form is the disjunctive normal form of the given Boolean function.

For example if $f(x_1, x_2, x_3) = (x_1 + x_2' + x_3)(x_1' + x_2 + x_3')$ is the Boolean function generated by 3-tuple $\bar{x} = (x_1, x_2, x_3)$, then the disjunctive normal form of $f(x_1, x_2, x_3)$ is obtained as follows :

$$f(x_1, x_2, x_3) = (x_1 + x_2' + x_3)(x_1' + x_2 + x_3')$$

$$= x_1 x_1' + x_1 x_2 + x_1 x_3' + x_1' x_2' + x_2 x_2' + x_2' x_3' + x_1' x_3 + x_2 x_3 + x_3 x_3'$$

$$= x_1 x_2 + x_1 x_3' + x_1' x_2' + x_2' x_3' + x_1' x_3 + x_2 x_3$$

$$= x_1 x_2 \cdot 1 + x_1 x_3' \cdot 1 + x_1' x_2' \cdot 1 + x_2' x_3' \cdot 1 + x_1' x_3 \cdot 1 + x_2 x_3 \cdot 1$$

$$= x_1 x_2 (x_3 + x_3') + x_1 x_3' (x_2 + x_2') + x_1' x_2' (x_3 + x_3')$$

$$+ x_2' x_3' (x_1 + x_1') + x_1' x_3 (x_2 + x_2') + x_2 x_3 (x_1 + x_1')$$

$$= x_1 x_2 x_3 + x_1 x_2 x_3' + x_1 x_2 x_3' + x_1 x_2' x_3' + x_1' x_2' x_3 + x_1' x_2' x_3'$$

$$+ x_1 x_2' x_3' + x_1' x_2' x_3' + x_1' x_2 x_3 + x_1' x_2' x_3 + x_1 x_2 x_3 + x_1' x_2 x_3$$

$$= x_1 x_2 x_3 + x_1 x_2 x_3' + x_1 x_2' x_3' + x_1' x_2 x_3 + x_1' x_2' x_3' + x_1' x_2 x_3$$

$$= x_1' x_2' x_3' + x_1' x_2' x_3 + x_1' x_2 x_3 + x_1 x_2' x_3' + x_1 x_2 x_3' + x_1 x_2 x_3$$

$$= m_0 + m_1 + m_3 + m_4 + m_6 + m_7$$

$$= \Sigma(0, 1, 3, 4, 6, 7).$$

11.5.2 Conjunctive normal form (CNF) :

A Boolean function $f(x_1, x_2,..., x_n)$ over the Boolean algebra B is said to be in its **conjunctive normal form** if it is expressible in the form $f(x_1, x_2,..., x_n) = M_0\, M_1\, M_2,..., M_k$ where each M_i ; $i = 0, 1, 2,..., k$ is a maxterm.

As the conjunctive normal form of the Boolean function is the product of maxterms and each maxterm is the sum of distinct literals, therefore the conjunctive normal form is also called **product of standard sum form** or the maxterm form.

The procedure of representing the Boolean function $f(x_1, x_2,..., x_n)$ generated by n variables $x_1, x_2,..., x_n$ in B is described below :

(i) Simplify the Boolean function $f(x_1, x_2,..., x_n)$ so that it has minimum number of factors.

(ii) Add 0's to each factor, as many times, equal to the number of missing literals x_i^* in that factor (for example if a factor in the Boolean function $f(x_1, x_2,..., x_n)$ has two missing literals x_j^* and x_k^*, then add 0 twice to this factor).

(iii) Now replace every 0 in each factor, by $x_i x'_i$ if this 0 corresponds to the missing literal x_i^* in the factor (for example if there are two 0's in some particular factor, that are due to the missing literals x_j^* and x_k^*, then replace one 0 by $x_j x'_j$ and the other by $x_k x'_k$).

(iv) Apply now, the laws of Boolean algebra, for example distributive laws, commutative laws and idempotent laws etc.

The resulting function yields the conjunctive normal form of the given Boolean function.

We now take the Boolean function $f(x_1, x_2, x_3) = (x_1 + x_2)(x_1 + x_3) + x_1\, x_2\, x_3$ and wish to represent it in its conjunctive normal form :

$$
\begin{aligned}
f(x_1, x_2, x_3) &= (x_1 + x_2)\,(x_1 + x_3) + x_1\, x_2\, x_3 \\
&= x_1 + x_2\, x_3 + x_1\, x_2\, x_3 && \text{(by distributive law)} \\
&= x_1 + (x_2\, x_3 + x_1\, x_2\, x_3) \\
&= x_1 + x_2\, x_3 && \text{(by absorption law)} \\
&= (x_1 + x_2)\,(x_1 + x_3) \\
&= (x_1 + x_2 + 0)\,(x_1 + x_3 + 0) \\
&= (x_1 + x_2 + x_3\, x'_3)\,(x_1 + x_3 + x_2\, x'_2) \\
&= (x_1 + x_2 + x_3)\,(x_1 + x_2 + x'_3).(x_1 + x_2 + x_3)\,(x_1 + x'_2 + x_3) \\
&= (x_1 + x_2 + x_3)\,(x_1 + x_2 + x'_3).\,(x_1 + x'_2 + x_3) \\
&= M_0\, M_1\, M_2 \\
&= \prod(0, 1, 2).
\end{aligned}
$$

The disjunctive normal form and the conjunctive normal form of the Boolean function can be obtained simultaneous by constructing the truth table of the functional values of the Boolean function for all possible combinations of values of the variables $x_1, x_2,..., x_n$.

Consider the Boolean function $f(x_1, x_2, x_3) = (x_1 x_2' + x_1 x_3)' + x_1'$. The truth table of the functional values of the Boolean function f, for all possible combinations of values of x_1, x_2 and x_3 is :

x_1	x_2	x_3	$f(x_1, x_2, x_3) = (x_1 x_2' + x_1 x_3)' + x_1'$
0	0	0	$(0 \cdot 1 + 0 \cdot 0)' + 1 = 1$
0	0	1	$(0 \cdot 1 + 0 \cdot 1)' + 1 = 1$
0	1	0	$(0 \cdot 0 + 0 \cdot 0)' + 1 = 1$
0	1	1	$(0 \cdot 0 + 0 \cdot 1)' + 1 = 1$
1	0	0	$(1 \cdot 1 + 1 \cdot 0)' + 0 = 0$
1	0	1	$(1 \cdot 1 + 1 \cdot 1)' + 0 = 0$
1	1	0	$(1 \cdot 0 + 1 \cdot 0)' + 0 = 1$
1	1	1	$(1 \cdot 0 + 1 \cdot 1)' + 0 = 0$

Now we collect all the minterms that correspond to the functional values equal to 1 under f. We see that these minterms are corresponding to the combinations 000, 001, 010, 011 and 110, *i.e.*, the minterms are $x_1' + x_2' + x_3', x_1' x_2' x_3, x_1' x_2 x_3', x_1' x_2 x_3$ and $x_1 x_2 x_3'$, (Remember that in a minterm each variable is being primed if its corresponding bit is 0 and unprimed if the corresponding bit is 1). We now add up all these minterms. This sum gives rise the disjunctive normal form of $f(x_1, x_2, x_3)$. Thus the disjunctive normal form is

$$\begin{aligned} f(x_1, x_2, x_3) &= x_1' x_2' x_3', + x_1' x_2' x_3 + x_1' x_2 x_3' + x_1' x_2 x_3 + x_1 x_2 x_3' \\ &= m_0 + m_1 + m_2 + m_3 + m_6 \\ &= \Sigma(0, 1, 2, 3, 6). \end{aligned}$$

In order to obtain the conjunctive normal form of the same Boolean function

$$f(x_1, x_2, x_3) = (x_1 x_2' + x_1 x_3)' + x_1'$$

we read all those maxterms that are corresponding the functional values equal to 0 under f. In the table we see that these maxterms are corresponding to the combinations 100,101 and 111, *i.e.*, the maxterms are $x_1' + x_2 + x_3, x_1' + x_2 + x_3'$ and $x_1' + x_2' + x_3'$ (Remember that in a maxterm each variable is being primed if its corresponding bit is 1 and unprimed if the corresponding bit is 0). We now take the product of all these maxterms. This results the conjunctive normal form of the given Boolean function $f(x_1, x_2, x_3)$. Thus the conjunctive normal form of the given Boolean function is :

$$\begin{aligned} f(x_1, x_2, x_3) &= (x_1' + x_2 + x_3)(x_1' + x_2 + x_3')(x_1' + x_2' + x_3'). \\ &= M_4 M_5 M_7 \\ &= \Pi(4, 5, 7). \end{aligned}$$

Ex.4. *Transform the Boolean expression $x_1 + x_2$ into three variable disjunctive normal form.*

Sol. $E(x_1, x_2, x_3) = x_1 + x_2$

$$= x_1(x_2 + x_2') + x_2(x_1 + x_1')$$

$$= x_1 x_2 + x_1 x_2' + x_1 x_2 + x_1' x_2$$

$$= x_1 x_2 + x_1 x_2' + x_1' x_2$$

$$= x_1 x_2 (x_3 + x_3') + x_1 x_2' (x_3 + x_3') + x_1' x_2 (x_3 + x_3')$$

$$= x_1 x_2 x_3 + x_1 x_2 x_3' + x_1 x_2' x_3 + x_1 x_2' x_3' + x_1' x_2 x_3 + x_1' x_2 x_3'$$

$$= x_1' x_2 x_3' + x_1' x_2 x_3 + x_1 x_2' x_3' + x_1 x_2' x_3 + x_1 x_2 x_3' + x_1 x_2 x_3$$

$$= m_2 + m_3 + m_4 + m_5 + m_6 + m_7$$

$$= \Sigma (2, 3, 4, 5, 6, 7).$$

Ex.5. *Transform the Boolean expression $x_1 x_2$ into three variable conjunctive normal form.*

Sol. $E(x_1, x_2, x_3) = x_1 x_2$

$$= [x_1 + (x_2 x_2')][x_2 + (x_1 x_1')]$$

$$= (x_1 + x_2)(x_1 + x_2')(x_2 + x_1)(x_2 + x_1')$$

$$= (x_1 + x_2)(x_1 + x_2')(x_1' + x_2)$$

$$= (x_1 + x_2 + x_3 x_3')(x_1 + x_2' + x_3 x_3')(x_1' + x_2 + x_3 x_3')$$

$$= (x_1 + x_2 + x_3)(x_1 + x_2 + x_3')(x_1 + x_2' + x_3)$$
$$(x_1 + x_2' + x_3')(x_1' + x_2 + x_3)(x_1' + x_2 + x_3')$$

$$= M_0 M_1 M_2 M_3 M_4 M_5$$

$$= \prod (0, 1, 2, 3, 4, 5).$$

Ex.6. *Transform the following Boolean expressions into disjunctive normal form :*

(i) $E(x_1, x_2, x_3) = x_1 x_2 + x_2 x_3 + x_1 x_3$

(ii) $E(x_1, x_2, x_3) = x_1 + x_1 x_2 + x_1 x_2 x_3$

(iii) $E(x_1, x_2, x_3) = (x_1 + x_2)(x_1 + x_2')(x_1' + x_3)$

(iv) $E(x_1, x_2, x_3) = [(x_1' + x_2')(x_2 + x_3')]' + x_2 x_3$

Sol. ***(i)*** $E(x_1, x_2, x_3) = x_1\, x_2 + x_2\, x_3 + x_1\, x_3$

$= x_1\, x_2 (x_3 + x_3') + x_2\, x_3 (x_1 + x_1') + x_1\, x_3 (x_2 + x_2')$

$= x_1\, x_2\, x_3 + x_1\, x_2\, x_3' + x_1\, x_2\, x_3 + x_1'\, x_2\, x_3 + x_1\, x_2\, x_3 + x_1\, x_2'\, x_3$

$= x_1'\, x_2\, x_3 + x_1\, x_2'\, x_3 + x_1\, x_2\, x_3' + x_1\, x_2\, x_3$

$= M_3 + M_5 + M_6 + M_7$

$= \Sigma\,(3, 5, 6, 7)$

(ii) $E(x_1, x_2, x_3) = x_1 + x_1'\, x_2 + x_1\, x_2\, x_3$

$= x_1 (x_2 + x_2')(x_3 + x_3') + x_1\, x_2 (x_3 + x_3') + x_1\, x_2\, x_3$

$= (x_1\, x_2 + x_1\, x_2')(x_3 + x_3') + x_1\, x_2\, x_3 + x_1\, x_2\, x_3' + x_1\, x_2\, x_3$

$= x_1\, x_2\, x_3 + x_1\, x_2\, x_3' + x_1\, x_2'\, x_3$
$\quad + x_1\, x_2'\, x_3' + x_1\, x_2\, x_3 + x_1\, x_2\, x_3'$ (since $x + x = x$)

$= x_1\, x_2\, x_3 + x_1\, x_2\, x_3' + x_1\, x_2'\, x_3 + x_1\, x_2'\, x_3'$

$= x_1\, x_2'\, x_3' + x_1\, x_2'\, x_3 + x_1\, x_2\, x_3' + x_1\, x_2\, x_3$

$= m_4 + m_5 + m_6 + m_7$

$= \Sigma\,(4, 5, 6, 7)$

(iii) $E(x_1, x_2, x_3) = (x_1 + x_2)(x_1 + x_2')(x_1' + x_3)$

$= (x_1 + x_2\, x_2')(x_1' + x_3)$

$= (x_1 + 0)(x_1' + x_3)$

$= x_1\, x_1' + x_1 x_3$

$= x_1\, x_3$

$= x_1\, x_3 (x_2 + x_2')$

$= x_1\, x_2\, x_3 + x_1\, x_2'\, x_3$

$= m_7 + m_5$

$= \Sigma\,(5, 7).$

(iv) $E(x_1, x_2, x_3) = \left[(x_1' + x_2') + (x_2 + x_3')\right]' + x_2\, x_3$

$= (x_1' + x_2')'\,(x_2 + x_3')' + x_2\, x_3$

$= (x_1 x_2)(x_2' x_3) + x_2 x_3$

$$= x_1\, x_2\, x_2'\, x_3 + x_2\, x_3$$

$$= 0 + x_2\, x_3$$

$$= x_2\, x_3 (x_1 + x_1')$$

$$= x_1\, x_2\, x_3 + x_1'\, x_2\, x_3$$

$$= x_1'\, x_2\, x_3 + x_1\, x_2\, x_3$$

$$= m_3 + m_3$$

$$= \Sigma\,(3, 7)$$

Ex.7. *Transform the following Boolean functions into conjunctive normal form :*

(i) $E(x_1, x_2, x_3) = x_1\,(x_1 + x_2)\,(x_1 + x_2 + x_3)$

(ii) $E(x_1, x_2, x_3) = (x_1 + x_2)\,(x_2 + x_3)\,(x_1 + x_3)$

(iii) $E(x_1, x_2, x_3) = x_1\, x_2 + x_1'\, x_3$

(iv) $E(x_1, x_2, x_3) = (x_1'\, x_2)'\,(x_1 + x_3)$

Sol. ***(i)*** $E(x_1, x_2, x_3) = x_1\,(x_1 + x_2)\,(x_1 + x_2 + x_3)$

$$= (x_1 + x_2\, x_2' + x_3\, x_3')(x_1 + x_2 + x_3\, x_3')(x_1 + x_2 + x_3)$$

$$= (x_1 + x_2\, x_2' + x_3)(x_1 + x_2\, x_2' + x_3')\cdot$$
$$(x_1 + x_2 + x_3)(x_1 + x_2 + x_3')(x_1 + x_2 + x_3)$$

$$= (x_1 + x_2 + x_3)(x_1 + x_2' + x_3)(x_1 + x_2 + x_3')$$
$$(x_1 + x_2' + x_3')(x_1 + x_2 + x_3)(x_1 + x_2 + x_3')$$

$$= (x_1 + x_2 + x_3)(x_1 + x_2 + x_3')(x_1 + x_2' + x_3)(x_1 + x_2' + x_3')$$

$(\because\ x\,x = x)$

$$= M_0\, M_1\, M_2\, M_3$$

$$= \prod (0, 1, 2, 3).$$

(ii) $E(x_1, x_2, x_3) = (x_1 + x_2)\,(x_2 + x_3)\,(x_1 + x_3)$

$$= (x_1 + x_2 + x_3\, x_3')(x_2 + x_3 + x_1\, x_1').(x_1 + x_3 + x_2\, x_2')$$

$$= (x_1 + x_2 + x_3)(x_1 + x_2 + x_3')(x_1 + x_2 + x_3)$$
$$(x_1' + x_2 + x_3)(x_1 + x_2 + x_3)(x_1 + x_2' + x_3)$$

$$= (x_1 + x_2 + x_3)(x_1 + x_2 + x_3')(x_1 + x_2' + x_3)(x_1' + x_2 + x_3)$$

$(\because\ x\,x = x)$

$$= M_0\, M_1\, M_2\, M_4$$

$$= \prod (0, 1, 2, 3, 4).$$

(iii) $E(x_1, x_2, x_3) = x_1 x_2 + x_1' x_3$

$= (x_1 + x_1' x_3)(x_2 + x_1' x_3)$

$= (x_1 + x_1')(x_1 + x_3)(x_1' + x_2)(x_2 + x_3)$

$= 1 \cdot (x_1 + x_3 + x_2 x_2')(x_1' + x_2 + x_3 x_3')(x_2 + x_3 + x_1 x_1')$

$= (x_1 + x_2 + x_3)(x_1 + x_2' + x_3)(x_1' + x_2 + x_3)$

$(x_1' + x_2 + x_3')(x_1 + x_2 + x_3)(x_1' + x_2 + x_3)$

$= (x_1 + x_2 + x_3)(x_1 + x_2' + x_3)(x_1' + x_2 + x_3)(x_1' + x_2 + x_3')$

$= M_0 M_2 M_4 M_5$

$= \prod (0, 2, 4, 5).$

(iv) $E(x_1, x_2, x_3) = (x_1' x_2)'(x_1 + x_3)$

$= (x_1 + x_2')(x_1 + x_3)$

$= (x_1 + x_2' + x_3 x_3')(x_1 + x_3 + x_2 x_2')$

$= (x_1 + x_2' + x_3)(x_1 + x_2' + x_3')(x_1 + x_2 + x_3)(x_1 + x_2' + x_3)$

$= (x_1 + x_2 + x_3)(x_1 + x_2' + x_3)(x_1 + x_2' + x_3')$

$= M_0 M_2 M_3$

$= \prod (0, 2, 3).$

Ex.8. *Simplify the three variable Boolean expression* $\sum (1, 3, 5, 7)$, *using the Boolean algebra.*

Sol. $\sum (1, 3, 5, 7) = x_1' x_2' x_3 + x_1' x_2 x_3 + x_1 x_2' x_3 + x_1 x_2 x_3$

$= x_1' x_3 (x_2' + x_2) + x_1 x_3 (x_2' + x_2)$

$= x_1' x_3 + x_1 x_3$

$= x_3 (x_1' + x_1)$

$= x_3.$

Ex.9. *Simplify the three variable Boolean expression* $\sum (0, 1, 4, 5)$ *using the Boolean algebra.*

Sol. $\sum (0, 1, 4, 5) = x_1' x_2' x_3' + x_1' x_2' x_3 + x_1 x_2' x_3' + x_1 x_2' x_3$

$= x_1' x_2' (x_3' + x_3) + x_1 x_2' (x_3' + x_3)$

$= x_1' x_2' + x_1 x_2'$ $(\because x + x' = 1)$

$= (x_1' + x_2) x_2'$

$= x'_2.$

Ex.10. *Simplify the three variable Boolean expression* $\prod(1, 2, 4, 7)$ *using the Boolean algebra.*

Sol.

$$\prod(1, 2, 4, 7) = (x_1 + x_2 + x_3')(x_1 + x_2' + x_3)(x_1' + x_2 + x_3)(x_1' + x_2' + x_3')$$

$$= [x_1' + (x_2 + x_3')(x_2' + x_3)][x_1' + (x_2 + x_3)(x_2' + x_3')]$$

$$= [x_1 + x_2\, x_2' + x_2\, x_3 + x_2'\, x_3' + x_3\, x_3']$$

$$\cdot [x_1' + x_2\, x_2' + x_2\, x_3' + x_2'\, x_3 + x_3\, x_3']$$

$$= [x_1 + x_2\, x_3 + x_2'\, x_3'][x_1' + x_2\, x_3' + x_2'\, x_3]$$

$$= x_1\, x_1' + x_1\, x_2\, x_3' + x_1\, x_2'\, x_3 + x_1'\, x_2\, x_3 + x_2\, x_2\, x_3\, x_3'$$

$$+ x_2\, x_2'\, x_3\, x_3 + x_1'\, x_2'\, x_3' + x_2\, x_2'\, x_3'\, x_3' + x_2'\, x_2'\, x_3\, x_3'$$

$$= x_1\, x_2\, x_3' + x_1\, x_2'\, x_3 + x_1'\, x_2\, x_3 + x_1'\, x_2'\, x_3'.$$

Ex.11. *Simplify the three variable Boolean expression* $\prod(2, 4, 6)$ *using the Boolean algebra.*

Sol.

$$\prod(2, 4, 7) = (x_1 + x_2' + x_3)(x_1' + x_2 + x_3)\cdot(x_1' + x_2' + x_3)$$

$$= (x_1 + x_2' + x_3)((x_1' + x_3) + x_2)((x_1' + x_3) + x_2')$$

$$= (x_1 + x_2' + x_3)[(x_1' + x_3) + x_2\, x_2']$$

$$= (x_1 + x_2' + x_3)(x_1' + x_3)$$

$$= (x_1 + x_2')x_1' + x_3 \qquad \text{(by distributive property)}$$

$$= x_1\, x_1' + x_1'\, x_2' + x_3$$

$$= x_1'\, x_2' + x_3.$$

11.6 Minimization of Boolean expressions

In the earlier unit 10, we studied the basic laws of Boolean algebras and related theorems, that are used for the manipulations of logical expressions. In the next unit 12 we shall see that the logical expressions can be realized by using the logic gates. To implement a logical expression using logic gates, it is required that the expression be in more simplified manner. Therefore the simplification of the logical expressions is important as it saves the hardware required to design any system. In this section we shall use the basic laws, rules and the theorems of Boolean algebra for the simplification of Boolean expressions (*i.e.* the logical expressions).

Ex.12. *Minimize the Boolean expressions* :

(i) $x_1\, x_2 + x_1' + (x_1\, x_2)'$

(ii) $(x_1 + x_2)(x_1 + x_2')(x_1' + x_2)$

(iii) $x_1\, x_2\, x_3 + x_1\, x_2'\, x_3 + x_1\, x_2\, x_3'$

(iv) $x_1\,(x_1 + x_2)(x_1 + x_2 + x_3)$

(v) $x_1\, x_2 + x_1\,(x_2 + x_3) + x_2\,(x_2 + x_3)$

Sol. *(i)* $x_1\, x_2 + x_1' + (x_1\, x_2)' = x_1\, x_2 + x_1' + x_1' + x_2'$

$= x_1\, x_2 + x_1' + x_2'$

$= (x_1 + x_1')(x_1' + x_2) + x_2'$

$= 1 \cdot (x_1' + x_2) + x_2'$

$= x_1' + x_2 + x_2'$

$= x' + 1$

$= 1.$

(ii) $(x_1 + x_2)(x_1 + x_2')(x_1' + x_2) = (x_1 + x_2\, x_2')(x_1' + x_2)$

$= x_1\,(x_1' + x_2)$

$= x_1\, x_1' + x_1\, x_2$

$= x_1\, x_2$

(iii) $x_1\, x_2\, x_3 + x_1\, x_2'\, x_3 + x_1\, x_2\, x_3' = (x_1\, x_2\, x_3 + x_1\, x_2'\, x_3) + (x_1\, x_2\, x_3 + x_1\, x_2\, x_3')$ $(\because x + x = x)$

$= x_1\, x_3\,(x_2 + x_2') + x_1\, x_2\,(x_3 + x_3')$

$= x_1\, x_3 \cdot 1 + x_1\, x_2 \cdot 1$

$= x_1\,(x_2 + x_3)$

(iv) $x_1\,(x_1 + x_2)(x_1 + x_2 + x_3) = x_1\,(x_1 + x_2 + x_3)$ (by absorption law)

$= x_1.$ (by absorption law)

(v) $x_1\, x_2 + x_1\,(x_2 + x_3) + x_2\,(x_2 + x_3) = x_1\,(x_2 + (x_2 + x_3)) + x_2$ (by absorption law)

$= x_1\,(x_2 + x_3) + x_2$

$= x_1\, x_2 + x_1\, x_3 + x_2$

$= x_2 + x_1\, x_2 + x_1\, x_3$

$= x_2 + x_1\, x_3$ (by absorption law)

Self-learning exercise-2

1. A maxterm is the ..... of n literals.

2. The product of n literals is called a ..... .

3. There can be formed ..... minterms generated by n variables.

4. The sum of all the 2^n minterms generated by n variables is always ..... .

5. The product of all the 2^n maxterms generated by n variables is ..... .

6. If m_i and m_j are minterms and $i \neq j$, then $m_i\, m_j$ = ...

7. The disjunctive normal form of the expression $x_1 x_2$ in three variables x_1, x_2, x_3 is ..... .

8. The conjunctive normal form of the expression $x_1 + x_2$ in three variables x_1, x_2, x_3 is ..... .

9. Each individual term in the conjunctive normal form is called a ..... .

10. Each individual term in the disjunctive normal form is called a ..... .

11.7 Summary

In this unit we studied two specified forms of the Boolean expressions that is the disjunctive normal form and the conjunctive normal form of the Boolean expression. We also learned about procedures of transforming the Boolean expressions into these forms.

11.8 Answers to self-learning exercises

Self-learning exercise–1

1. complement. **2.** literals. **3.** fundamental product.

4. equivalent. **5.** yes.

Self-learning exercise–2

1. sum **2.** minterm **3.** 2^n

4. 1 **5.** 0 **6.** 0

7. $x_1\, x_2\, x_3 + x_1\, x_2\, x'_3$ **8.** $(x_1 + x_2 + x_3)\,(x_1 + x_2 + x'_3)$

9. maxterm **10.** minterm.

11.9 Exercises

1. Define minterm and maxterm.

2. Define the disjunctive normal form and the conjunctive normal form of the Boolean expression.

3. Transform the following Boolean expressions into disjunctive normal form :

(i) $x_1 + x_2\, x'_3$

(ii) $x_1 + x_2 + x_1\, x_3$

(iii) $x_3\,(x'_1 + x_2)$

(iv) $(x_1 + x_2)' + x_1\, x'_2 + x_3$

(v) $(x_1 + x_2 + x_3)(x_1\, x_2 + x'_1\, x'_3)'$.

[**Ans :** *(i)* $x_1\,x_2\,x_3 + x_1\,x_2\,x_3' + x_1\,x_2'\,x_3 + x_1\,x_2'\,x_3' + x_1'\,x_2\,x_3'$

(ii) $x_1\,x_2\,x_3 + x_1\,x_2\,x_3' + x_1\,x_2'\,x_3 + x_1\,x_2'\,x_3' + x_1'\,x_2\,x_3 + x_1'\,x_2\,x_3'$

(iii) $x_1\,x_2\,x_3 + x_1'\,x_2\,x_3 + x_1'\,x_2'\,x_3$

(iv) $x_1'\,x_2'\,x_3' + x_1'\,x_2'\,x_3 + x_1\,x_2'\,x_3' + x_1'\,x_2\,x_3 + x_1\,x_2'\,x_3 + x_1\,x_2\,x_3$

(v) $x_1'\,x_2\,x_3' + x_1\,x_2'\,x_3' + x_1\,x_2\,x_3$].

4. Transform the following Boolean expressions into conjunctive normal form :

(i) $(x_1 + x_2)\,(x_1 + x_3) + x_1\,x_2\,x_3$

(ii) $x_1\,x_2 + x_1\,x_2' + x_1\,x_3$

(iii) $(x_1\,x_2 + x_3)(x_1\,x_3 + x_2)$

(iv) $x_1(x_1 + x_2')(x_2 + x_3')$

(v) $(x_1 + x_2)(x_1 + x_3)(x_2 + x_3')$.

[**Ans :** *(i)* $(x_1 + x_2 + x_3)(x_1 + x_2 + x_3')(x_1 + x_2' + x_3)$

(ii) $(x_1 + x_2 + x_3)(x_1 + x_2 + x_3')(x_1 + x_2' + x_3)(x_1 + x_2' + x_3')$

(iii) $(x_1 + x_2 + x_3)(x_1 + x_2' + x_3)(x_1' + x_2 + x_3)(x_1 + x_2 + x_3')$

(iv) $(x_1 + x_2 + x_3)(x_1 + x_2' + x_3)(x_1 + x_2 + x_3')(x_1 + x_2' + x_3')(x_1' + x_2 + x_3')$

(v) $(x_1 + x_2 + x_3)(x_1 + x_2 + x_3')(x_1 + x_2' + x_3)(x_1' + x_2 + x_3')$].

5. Simplify the following three variable Boolean expressions. Using Boolean algebra :

(i) $\Sigma\,(1, 3, 4, 6)$

(ii) $\Sigma\,(0, 1, 3, 5)$

(iii) $\Pi\,(0, 1, 2, 3, 4, 6)$

(iv) $\Pi\,(0, 2, 4, 5)$.

[**Ans :** *(i)* $x_1'\,x_3 + x_1 x_3'$

(ii) $x_1'\,x_2' + x_1'\,x_3 + x_2'\,x_3$

(iii) $(x_1 + x_2)\,x_3$

(iv) $x_1\,x_2 + x_1'\,x_3 + x_2\,x_3$].

□□□

UNIT 12 : Switching Circuits and Digital Logic Gates

Structure of the Unit

12.0 Objectives

The purpose of writing this unit is to apply Boolean algebra to analyze electronic and electrical circuits. This was developed by scientist Shannon while analyzing telephone switching circuits.

12.1 Introduction

In Boolean algebra each variable has either of two values : true or false *i.e.*, 1 or 0. Many logical problems can be solved by using this two-state algebra. After Shannon's work, engineers realized that Boolean algebra could be applied to computer electronics. In this unit you will learn about the switching circuits, various digital logic gates and implementation of the Boolean expressions in the form of these logic gates. You will also learn, how these various logic gates are interrelated.

12.2 Switching circuits

One of the examples, where Boolean algebra can be applied, is the electronic circuit that involves two possible states. If we consider a simple on-off electric switch in a most elementary electric circuit, then it can be placed either in the off position or in the on position as shown below in the fig. 12.1 :

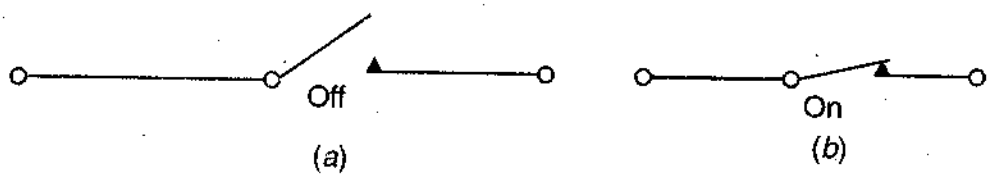
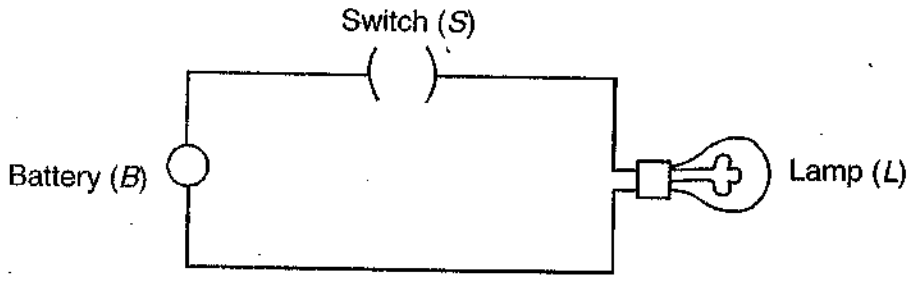


Fig. 12.1

One of the most elementary circuits is given below in fig. 12.2 :



(*a*)

S	*L*
0	0
1	1

(*b*) Condition table

Fig. 12.2

The battery *B*, the switch *S* and the indicating lamp *L* are connected in the simple most switching circuit. When the switch *S* in the off position, we say that the circuit is an open circuit and the lamp *L* does not glow, but when the switch *S* is in on position, we say that there is a closed circuit and the lamp *L* is seen glowing as the current flows in the circuit.

The condition, when the switch *S* is off, (*i.e.*, the switch is open) and the lamp *L* is off (*i.e.* does not glow), is indicated by the numeric value '0' and the switch is designated as *S'*. The condition when

the switch S is on (*i.e.* is closed) and the lamp L is on (*i.e.* glowing tamp), is indicated by the numeric value '1' and the switch is then designated as S. The condition table is the truth table, which lists all the possible combinations.

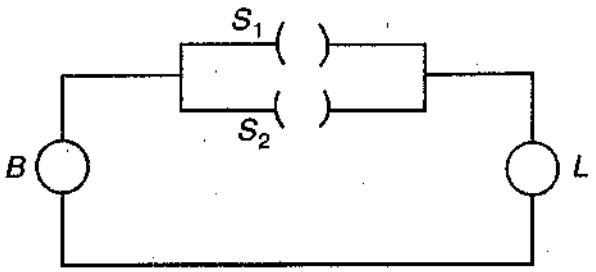
There can be constructed two-state devices that permit not only the electric current but any thing that can go through such as **'water'**, **'information'** etc. Later on, we shall replace the word **'switch'** by the word **'gate'**.

12.3 Interconnection of switches

Two or more switches can be connected in two most basic ways so as to form new switching circuits

12.3.1 In parallel :

Consider the switching circuit shown in fig. 12.3, in which two switches S_1 and S_2 are interconnected in parallel.



(*a*)

S_1	S_2	L
0	0	0
0	1	1
1	0	1
1	1	1

(*b*)

x	y	$x+y$
0	0	0
0	1	1
1	0	1
1	1	1

(c)

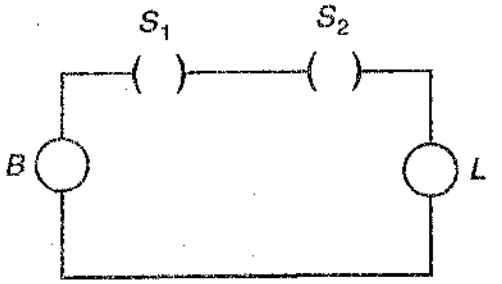
Fig. 12.3

When the switch S_1 is closed (and S_2 is open), then the current flows through S_1 and the lamp L is on. When the switch S_2 is closed (and S_1 is open), then the current flows through S_2 and again the lamp L is on. With both the switches S_1 and S_2, closed, the current is equally divided, between both the branches and permits the lamp to glow. But when both the switches are open, the circuit becomes an open circuit and the lamp is off.

Thus it can be said that two switches x and y are connected in parallel if the current does not flow when both x and y are open and the current flows when any one or both the switches x and y are closed. This shows that an "OR" function $x + y$ is obtained, when the switches x and y are connected in parallel.

12.3.2 In series :

Consider the switching circuit shown in fig. 12.4, in which two switches S_1 and S_2 are interconnected in series.



(a)

S_1	S_2	L
0	0	0
0	1	0
1	0	0
1	1	1

(b)

x	y	$x+y$
0	0	0
0	1	0
1	0	0
1	1	1

(c)

Fig. 12.4

When the switch S_1 is closed (and S_2 is open) or the switch S_1 is open (and S_2 is closed) or both S_1 and S_2 are open, then the circuit is open and the lamp is off. In only one case when both the switches S_1 and S_2 are closed the circuit permits the current to flow in and the lamp is on.

Thus when two switches x and y are connected in series, the current flows in series, the current flows only when both x and y are closed and it does not flow if any of x and y or both are open. This shows that an "AND" function $x \cdot y$ is obtained when the switches x and y are connected in series.

12.3.3 In series-parallel :

The series connection and the parallel connection of the switches can further be interconnected so as to form a new switching circuit called the "series-parallel circuit". Such a circuit is shown in the following figure 12.5 :

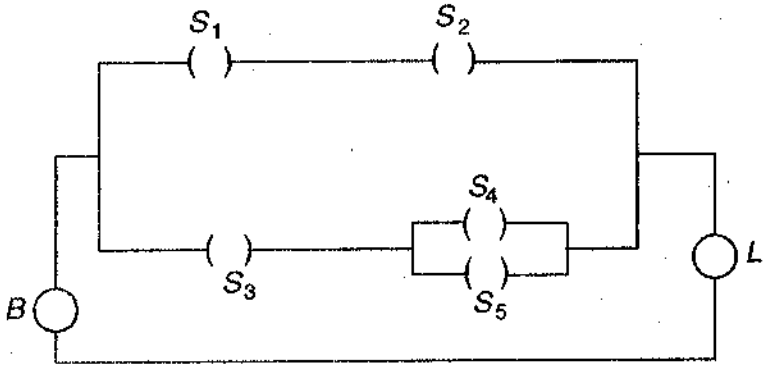


Fig. 12.5

12.3.4 Bridge-circuits :

There can be formed switching circuits that are not series-parallel circuits. Such switching circuits are called the bridge-circuits. Following circuit is one of the simple cases of bridge-circuits.

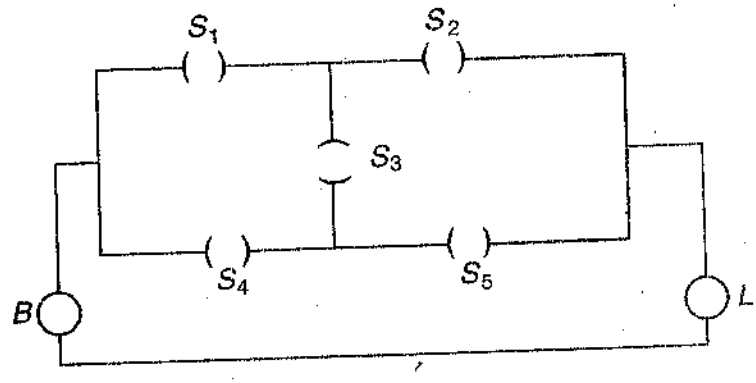


Fig. 12.6

It can be seen that the number of switches involved in the bridge-circuit is always less than that of number of switches involved in the equivalent (corresponding) series-parallel switching circuit. The switching circuit, equivalent to the bridge-circuit shown in fig. 12.6 is shown below in fig. 12.7 :

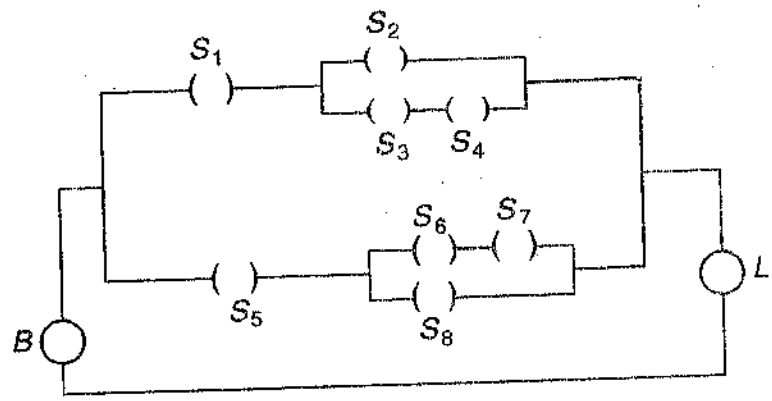


Fig. 12.7

Ex.1. *Construct the condition table for the following switching circuit and also prepare an equivalent simple circuit :*

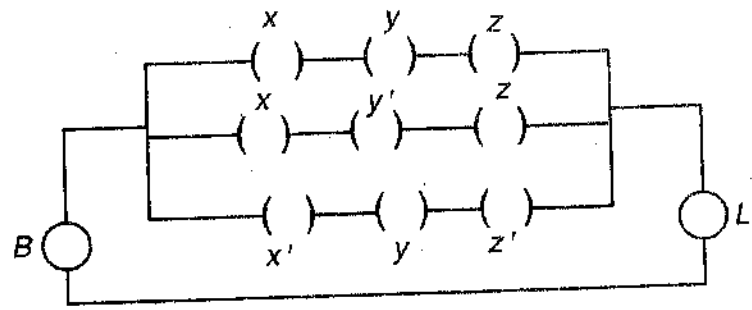


Fig. 12.8

Sol. The function (called the Boolean function) for the given switching circuit is :

$$f(x, y, z) = xyz + xy'z + x'yz'$$

The condition table (or the truth table) is

x	y	z	$f(x, y, z) = xyz + xy'z + x'yz'$
0	0	0	$0\cdot0\cdot0 + 0\cdot1\cdot0 + 1\cdot0\cdot1 = 0$
0	0	1	$0\cdot0\cdot1 + 0\cdot1\cdot1 + 1\cdot0\cdot0 = 0$
0	1	0	$0\cdot1\cdot0 + 0\cdot0\cdot0 + 1\cdot1\cdot1 = 1$
0	1	1	$0\cdot1\cdot1 + 0\cdot0\cdot1 + 1\cdot1\cdot0 = 0$
1	0	0	$1\cdot0\cdot0 + 1\cdot1\cdot0 + 0\cdot0\cdot1 = 0$
1	0	1	$1\cdot0\cdot1 + 1\cdot1\cdot1 + 0\cdot0\cdot0 = 1$
1	1	0	$1\cdot1\cdot0 + 1\cdot0\cdot0 + 0\cdot1\cdot1 = 0$
1	1	1	$1\cdot1\cdot1 + 1\cdot0\cdot1 + 0\cdot1\cdot0 = 1$

The Boolean function can be simplified as

$$\begin{aligned} f(x, y, z) &= xyz + xy'z + x'yz' \\ &= xz(y + y') + x'yz' \\ &= xz\cdot1 + x'yz' \\ &= xz + x'yz' \end{aligned}$$

Hence the equivalent simpler circuit is :

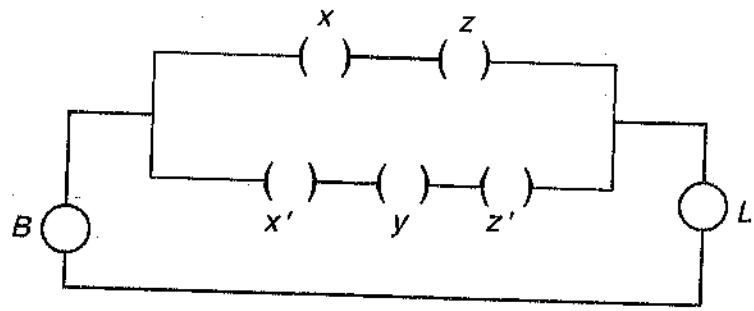


Fig. 12.9

Ex.2. *Find the Boolean function for the following switching circuit and simplify it to construct an equivalent circuit :*

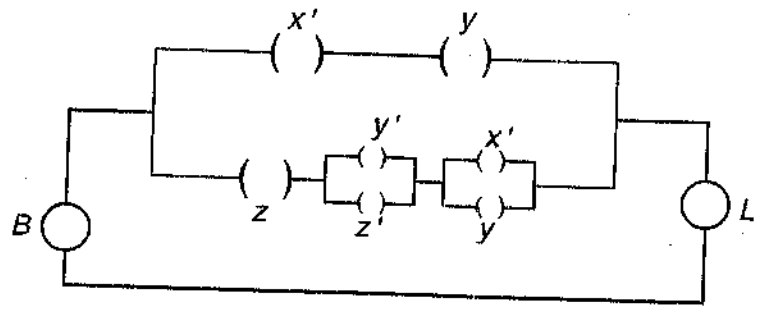


Fig. 12.10

Sol. The Boolean function for the given switching circuit is :

$$\begin{aligned} f(x, y, z) &= x'y + z(y' + z') + (x' + y) \\ &= x'y + z(x'y' + yy' + x'z' + yz') \end{aligned}$$

$$= x'y + z(x'y' + 0 + x'z' + yz')$$
$$= x'y + x'y'z + x'zz' + yzz'$$
$$= x'y + x'y'z + 0 + 0$$
$$= x'(y + y'z)$$
$$= x'(y + y')(y + z)$$
$$= x' \cdot 1 \cdot (y + z)$$
$$= x'(y + z).$$

Hence the equivalent circuit is :

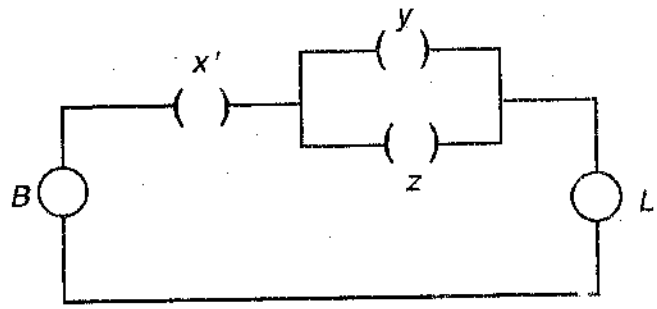


Fig. 12.11

Self-learning exercise-I

1. If the switches are interconnected in series, then the current flows through the circuit when and only when .... .
2. Out of five switches, connected in parallel, two switches are open. Does the current flow through the circuit ?
3. In the switching circuit, shown in Fig. 12.7, all the switches except the switches S_1 and S_5 are open. In order that the current flows in the circuit, which are the switches that should also be closed ?

12.4 Digital logic gates

A switching network governs the flow of current through the circuit. The logic gates are basically the electronic circuits that are used to implement the most elementary logical expressions. A digital electronic circuit with one or more input signals but only one output signal is said to be a logic gate.

Since logic gate is a switching circuit, therefore the output of any logic gate can have one and only one of the two possible states namely 1 or 0.

To understand the basic idea of logic gates, consider the switching circuit shown in Fig. 12.3*(a)*. We have four possible combinations of switches S_1 and S_2 as shown below :

Inputs		Output
S_1	S_1	
open (0)	open (0)	lamp off (0)
open (0)	closed (1)	lamp on (1)
closed (1)	open (0)	lamp on (1)
closed (1)	closed (1)	lamp on (1)

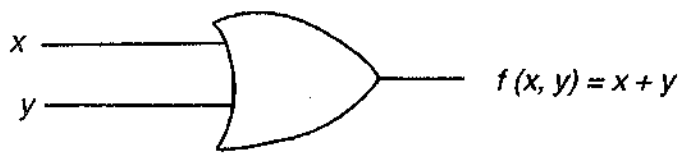
Here, when either of the switches S_1 and S_2 or both S_1 and S_2 are closed, the lamp glows. In binary language, when any one of the inputs or both the inputs are 1, the output is 1. When both switches are open, the lamp is off, *i.e.*, when both inputs are 0, the output is 0.

12.5 Three basic logic gates

There are three basic logic gates, the OR-gate, the AND-gate and the NOT-gate (or Inverter). Other logic gates, the NAND-gate, the NOR-gate, the EX-OR gate and the EX-NOR are derived from these three gates only.

12.5.1. OR-gate :

The OR-gate performs logical addition, more commonly known as the OR-function. The OR-gate has two or more inputs and one output. The output of the OR-gate is 0 only when all the inputs are at logic 0. If any one of the input is at logic 1, the output of the OR-gate is 1. The logic symbol for the OR-gate is shown in Fig. 12.12.

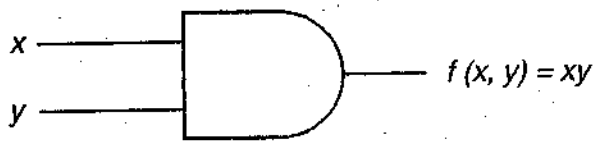


Inputs		Output
x	y	$x + y$
0	0	0
0	1	1
1	0	1
1	1	1

Fig. 12.12

12.5.2. AND-gate :

The AND-gate performs logical multiplication, more commonly known as the AND-function. It has two or more inputs but one output. The output of the AND-gate is 1 only when all the inputs in the gate are at logic 1. If any one of the input is at logic 0, the output of the AND-gate is 0. The logic symbol for the AND-gate is shown in Fig. 12.13.

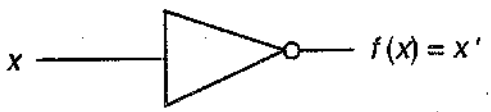


Inputs		Output
x	y	xy
0	0	0
0	1	0
1	0	0
1	1	1

Fig. 12.13

12.5.3. NOT-gate (Inverter) :

The NOT-gate or the inverter has only one input signal and one output signal which is just opposite of the input signal. The NOT-gate (inverter) performs a basic logic function called the "inversion" or "complementation". In terms of bits, the NOT-gate changes a logic 1 to logic 0 and logic 0 to logic 1. Fig. 12.14 shows the logic symbol for the NOT-gate. The bubble [0] placed on the output indicates the negation (inversion). The function performed by the NOT-gate is commonly known as the NOT-function.



Inputs	Output
x	x'
0	1
1	0

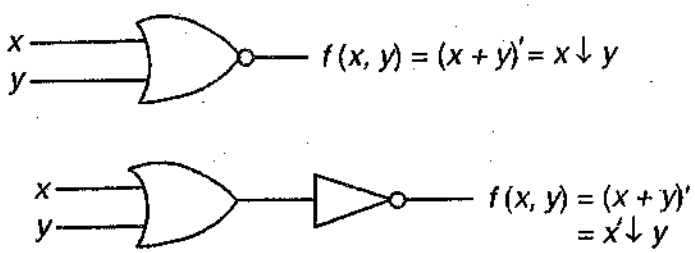
Fig. 12.14

12.6 Combination of basic logic gates

The combination of the basic logic gates, the OR-gate, the AND gate and the NOT-gate, give rise new digital logic gates. We discuss these gates in the following text.

12.6.1. NOR-gate :

The NOR-gate has two or more inputs but only one output. The NOR is a contraction of the words NOT and OR and implies an OR function with an inverted output. The output of the NOR-gate is at logic 1 only when all the input signals are of logic 0. If any of the input signal is at logic 1, then the output of the NOR-gate is at logic 0. The NOR-gate is a "Universal" gate as it can be used to construct an AND-gate, an OR-gate and an inverter or any combination of these functions. The logic symbol for a two input NOR-gate is shown below in Fig. 12.15

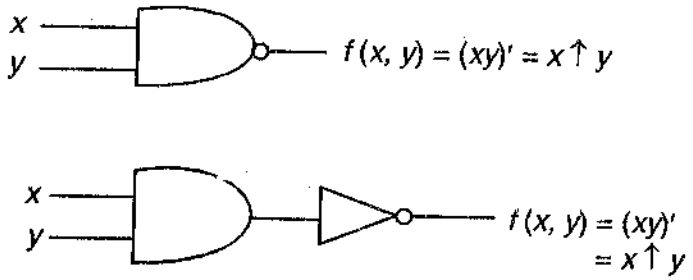


Inputs		Output
x	y	$(x+y)'$
0	0	1
0	1	0
1	0	0
1	1	0

Fig. 12.15

12.6.2. NAND-gate :

The term NAND is the contraction of words NOT and AND. The NAND-gate implies an AND function with an inverted output. It is a universal gate as it can be used to construct an AND-gate, an OR-gate, an inverter or any other combination of these. The output of the NAND-gate is at logic 0, only when all the inputs are at logic 1. If any of the input is at logic 0, the output of the NAND-gate is at logic 1. The logic function for a two-input NAND-gate is shown below in Fig. 2.16



Inputs		Output
x	y	$(x\,y)'$
0	0	1
0	1	1
1	0	1
1	1	0

Fig. 12.16

12.6.3. Exclusive-OR-gate (XOR-gate) :

The Exclusive-OR-gate or the XOR-gate is the combination of OR, AND and NOT-gates. It has two or more inputs but one output. A two-input XOR-gate is symbolically shown in Fig. 12.17

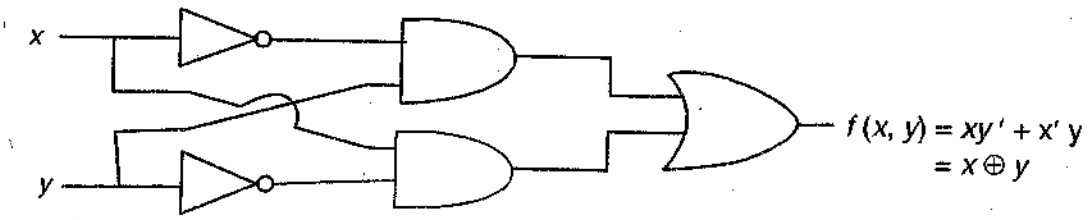
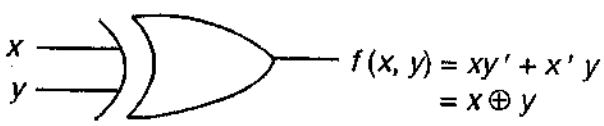


Fig. 12.17

The output of the *XOR*-gate is at logic 1, if any one but not all the inputs are at logic 1. Logically, the *XOR*-gate recognizes only words that have an odd number of inputs at logic 1, *i.e.* for odd number of inputs of logic 1, the output of the *XOR*-gate is at logic 1. The *XOR*-gate does not recognize the words that have even number of inputs at logic 1 or all the inputs at logic 0. The logic symbol for a two-input *XOR*-gate is shown in fig 12.18.



Inputs		Output
x	y	$x\,y' + x\,y'$
0	0	0
0	1	1
1	0	1
1	1	0

Fig. 12.18

12.6.4. Exclusive NOR-gate (XNOR-gate) :

The Exclusive NOR-gate is logically equivalent to inverted Exclusive OR-gate, i.e. an XOR-gate followed by a NOT-gate. An XNOR-gate has two or more inputs but only one out put. The out put of XNOR-gate is at logic 0 if any one, but not all the inputs are at logic 0. If recognizes only those words that have an even number of 1 or words that have all 0. This means that for all inputs at logic 0 or for even number of inputs at logic 1, the output of the XNOR-gate is at logic 1. The construction of XNOR-gate for a two-input system can be represented as follows :

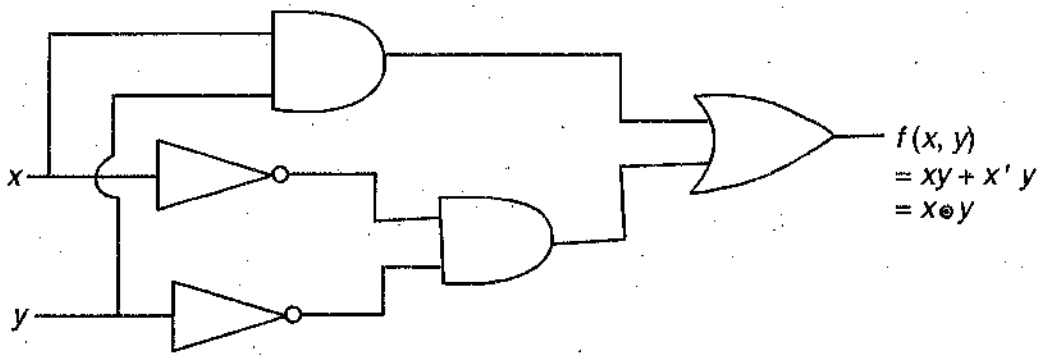
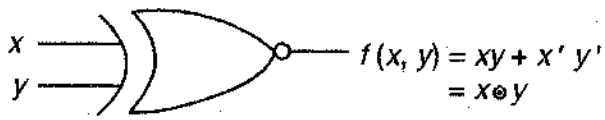


Fig. 12.19

The logical symbol for a two-input XNOR-gate is shown in fig 12.20.



Inputs		Output
x	y	$x\,y + x\,y'$
0	0	1
0	1	0
1	0	0
1	1	1

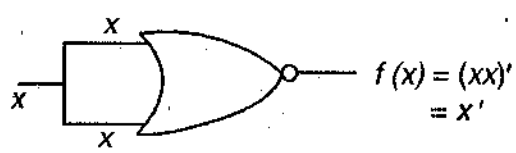
Fig. 12.20

12.7 Universal property of NOR and NAND-gates

Since any logic function can be generated using the NOR or NAND gate, for this reason the NOR gate and the NAND gate are called the universal gates.

12.7.1. NOT function using NAND-gate :

The NOT function (Inverter) can be constructed, using NAND-gate by connecting all the inputs together and creating a single common input as shown in the following figure :

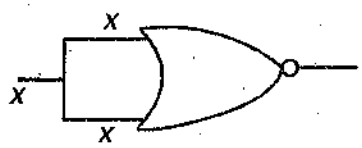


	Inputs		Output	
	x	x	$(x\,x)'$	
$x = 0$	0	0	1	$f(x) = 1$
	0	1	1	
	1	0	1	
$x = 1$	1	1	0	$f(x) = 0$

Fig. 12.21

12.7.2. NOT function using NOR-gate :

The NOT function can be constructed using NOR gate by connecting all the inputs together and making a single input as shown below in Fig. 12.22.



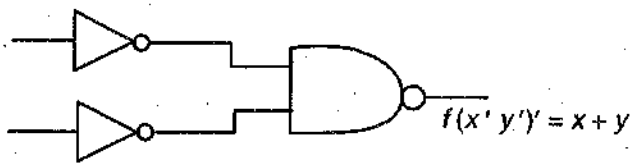
	Inputs		Output	
	x	x	$(x+x)'$	
$x = 0$	0	0	1	$f(x) = 1$
	0	1	0	
	1	0	0	
$x = 1$	1	1	0	$f(x) = 0$

Fig. 12.22

12.7.3. OR function using NAND-gate :

The OR function can be constructed using only NAND gate as follows :

$$x + y = (x')' + (y')' = (x'y')'$$



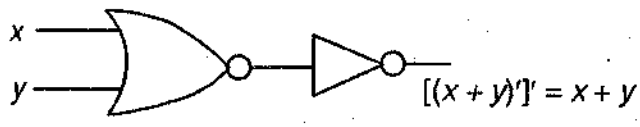
x	y	$x+y$	$x'+y'$	$(x'y')'$
0	0	0	1	0
0	1	1	0	1
1	0	1	0	1
1	1	1	0	1

Fig. 12.23

12.7.4. OR function using NOR-gate :

The OR function can be generated using the NOR-gate, just inverting the output of the NOR gate as shown below :

$$x + y = \left[(x + y)'\right]'$$



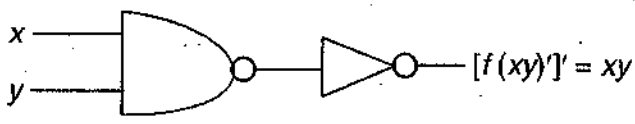
x	y	$x+y$	$(x+y)'$	$[(x+y)']'$
0	0	0	1	0
0	1	1	0	1
1	0	1	0	1
1	1	1	0	1

Fig. 12.24

12.7.5. AND function using NAND-gate :

The AND function can be generated using and NAND gate by inverting the output of the NAND gate.

$$xy = \left[(xy)'\right]'$$



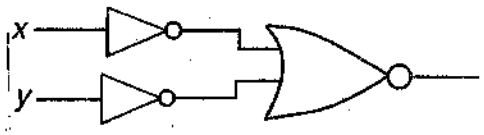
x	y	xy	$(xy)'$	$((xy)')'$
0	0	0	1	0
0	1	0	1	0
1	0	0	1	0
1	1	1	0	1

Fig. 12.25

12.7.6. AND function using NOR-gate :

The AND function can be generated using only NOR-gate as follows :

$$xy = (x')'\ (y')' = (x' + y')'$$



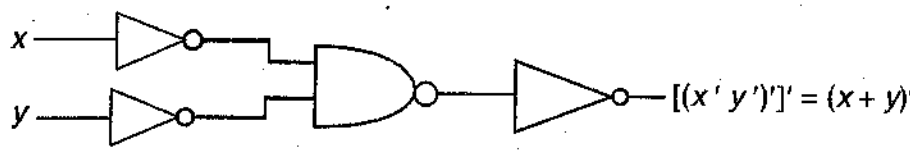
x	y	xy	$x' + y'$	$(x' + y')'$
0	0	0	1	0
0	1	0	1	0
1	0	0	1	0
1	1	1	0	1

Fig. 12.26

12.7.7. NOR function using NAND-gate :

The NOR function can be generated using only NAND-gates as follows :

$$(x + y)' = x'y' = \left[(x'y')'\right]'$$



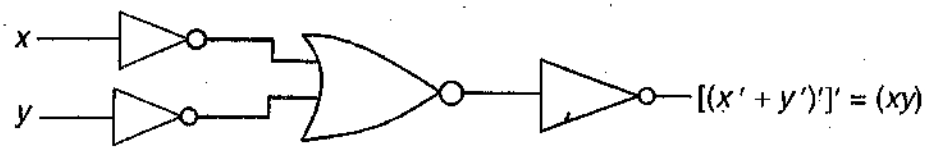
x	y	$(x + y)'$	$x'y'$	$(x'y')'$	$((x'y')')'$
0	0	1	1	0	1
0	1	0	0	1	0
1	0	0	0	1	0
1	1	0	0	1	0

Fig. 12.27

12.7.8. NAND function using NOR-gate :

The NAND function can be constructed using only NOR-gate as follows :

$$(xy)' = x' + y' = \left[(x' + y')'\right]'$$



x	y	$(xy)'$	$x'+y'$	$(x'+y')'$	$[(x'+y')']'$
0	0	1	1	0	1
0	1	1	1	0	1
1	0	1	1	0	1
1	1	0	0	1	0

Fig. 12.28

Ex.3. *Implement the Boolean expression for XOR-gate using only NAND-gates.*

Sol. $$E(x, y) = x \oplus y = xy' + x'y$$

$$= \left[(xy')' \cdot (x'y)'\right]'$$

which can be generated by developing the logic circuit using only NAND-gates.

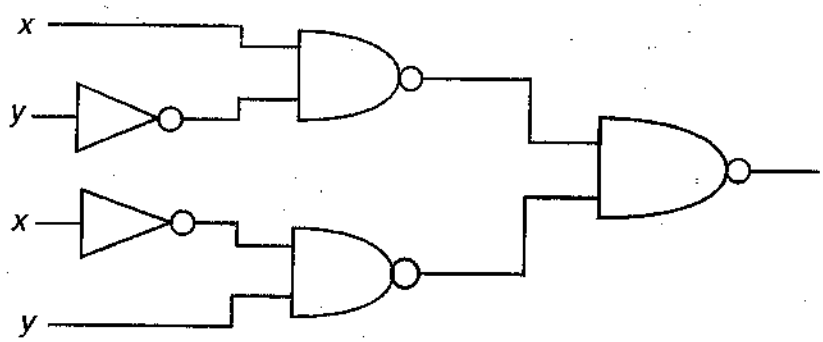


Fig. 12.29

Ex.4. *Implement the Boolean expression for XNOR-gate using only NOR-gates.*

Sol. $$E(x, y) = x \odot y = xy + x'y'$$

$$= (x' + y')' + (x + y)'$$

$$= \left[\left((x' + y')' + (x + y)'\right)'\right]'$$

The logic circuit for the above function using only NOR gates is :

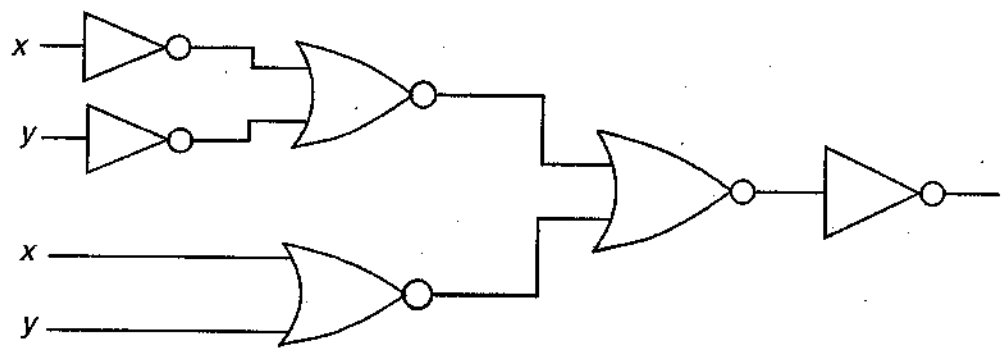


Fig. 12.30

Ex.5. *Show that the logic circuits (a) and (b) shown in Fig.* 12.31 *are equivalent :*

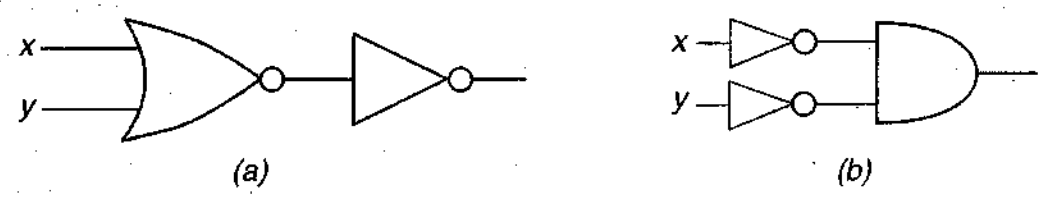


Fig. 12.31

Sol. The condition tables for the logic circuits shown in Fig. 12.31 are :

x	y	$x+y$	$(x+y)'$
0	0	0	1
0	1	1	0
1	0	1	0
1	1	1	0

and

x	y	x'	y'	$x'y'$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	0	0	0

which are identical. Hence the two circuits are equivalent.

Ex.6. *Use NAND gates only to draw a logic circuit for the Boolean expression*

$$E(x, y, z) = xy'z + yz'$$

Sol. Here the given Boolean expression can be written as

$$E(x, y, z) = xy'z + yz' = \left[(xy'z)'\ (yz')'\right]'$$

Therefore the logic circuit using only NAND gates is

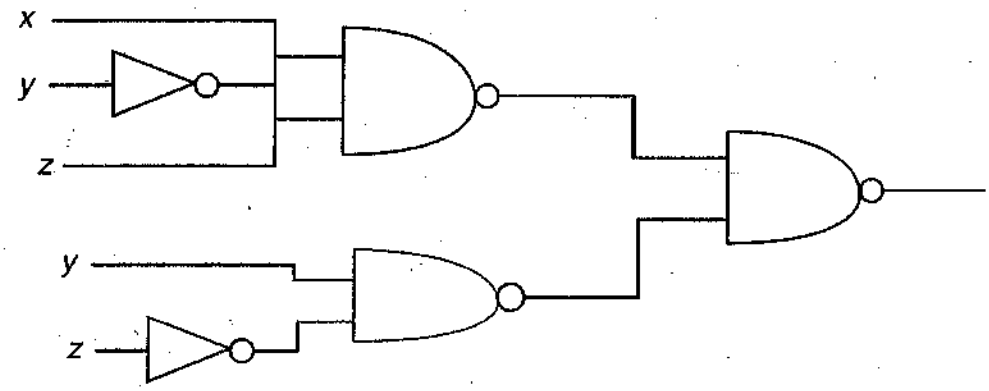


Fig. 12.32

Ex.7. *Construct the logic circuit using only NAND gates for the Boolean expression*

$$E(x, y, z) = (x' + y)z + y' + xz$$

Sol. Here the given expression is

$$\begin{aligned} E(x, y, z) &= (x' + y)z + y' + xz \\ &= (x \cdot y')'z + y' + xz \\ &= \left[\left((xy')'z\right)'y(xz)'\right]' \end{aligned}$$

The logic circuit using the NAND-gates is therefore

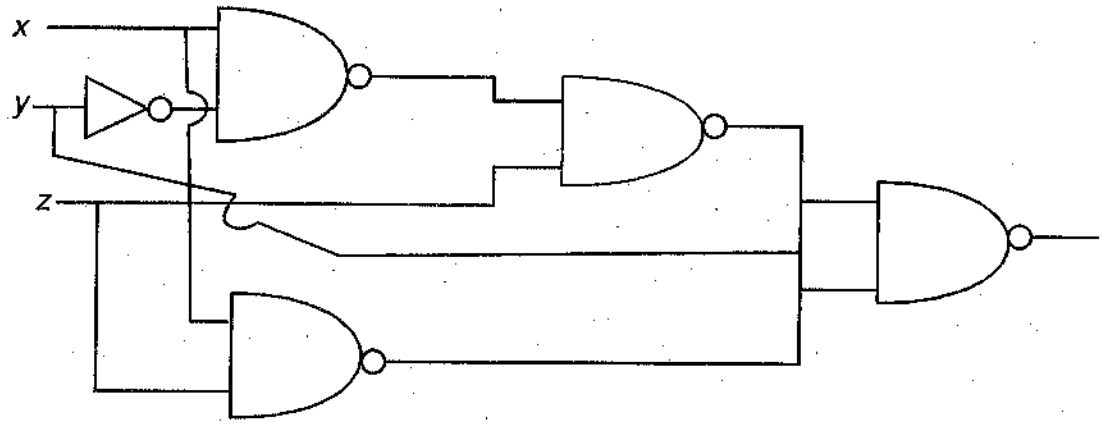


Fig. 12.33

Ex.8. *Draw the logic circuit for the Boolean expression*

$$E(x, y, z) = (x + y)(y + z)(z + x),$$

using only NOR-gates.

Sol. $$E(x, y, z) = (x + y)(y + z)(z + x)$$

$$= \left[(x + y)' + (y + z)' + (z + x)'\right]'$$

Therefore the logic circuit using only NOR gates is :

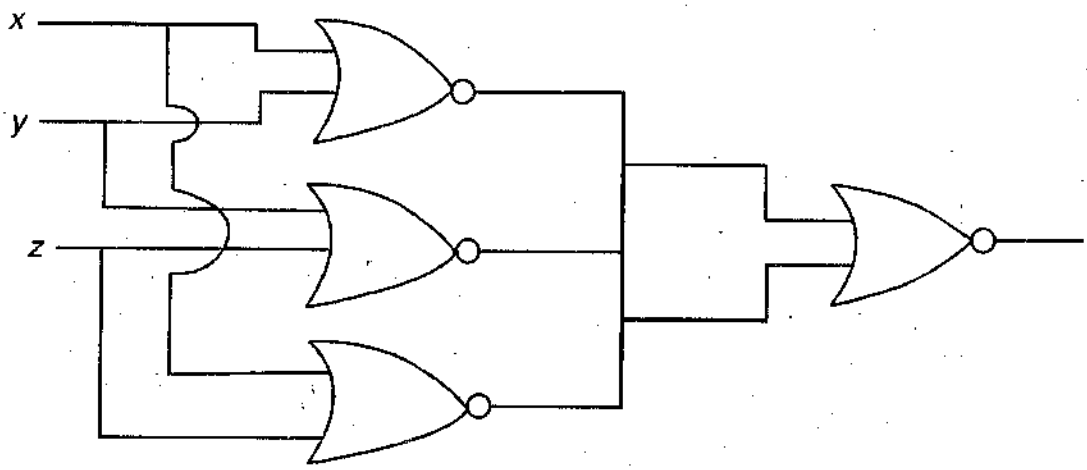


Fig. 12.34

Ex.9. *Draw a logic circuit for the Boolean expression*

$$E(x, y, z) = (x + yz)' + y$$

Sol. The logic circuit for expression is :

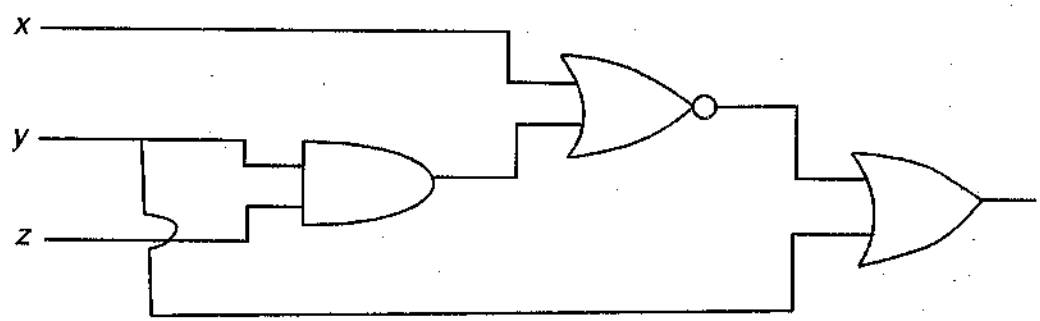


Fig. 12.35

Ex.10. *Determine the condition table for the logic circuit in fig* 12.36

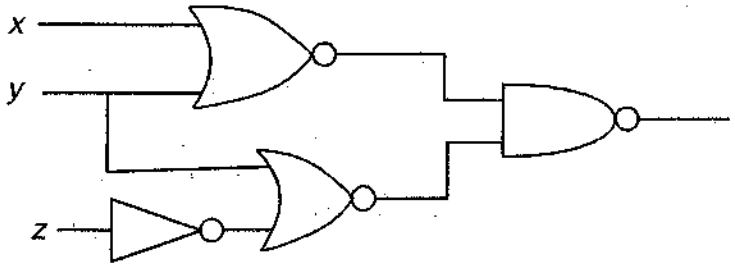


Fig. 12.36

Sol. Here $E(x, y, z) = \left[(x+y)' (y+z')' \right]'$

$= (x+y)+(y+z')$

[De-Morgan's law and since $(a')' = a$]

$= x+y+z'$

The condition table for the given expression is :

x	y	z	z'	$x+y+z'$
0	0	0	1	1
0	0	1	0	0
0	1	0	1	1
0	1	1	0	1
1	0	0	1	1
1	0	1	0	1
1	1	0	1	1
1	1	1	0	1

Ex.11. *Show that the Boolean expression E (x, y, z) = x y z ' can be implemented with one two-input NOR gate and one two-input NAND gate.*

Sol. Here $E(x, y, z) = x\, y\, z'$,

$= \left((x\, y)' \right)' z'$,

$= \left((x\, y)' + z \right)'$

Therefore the logic circuit is :

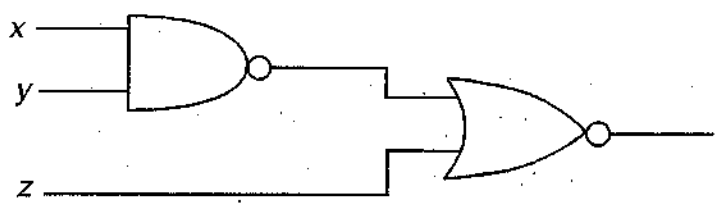


Fig. 12.37

Ex.12. *Implement the expression* $E(x, y, z, t) = x\,y\,z\,t$ *using only NAND gates.*

Sol. Here $E(x, y, z, t) = x\,y\,z\,t$

$$= \left[(x\,y\,z\,t)' \right]'$$

$$= \left[(x\,y)' + (z\,t)' \right]'$$

$$= \left[\left[\left((x\,y)' \right)' \left((z\,t)' \right)' \right]' \right]'$$

The logic circuit, therefore is :

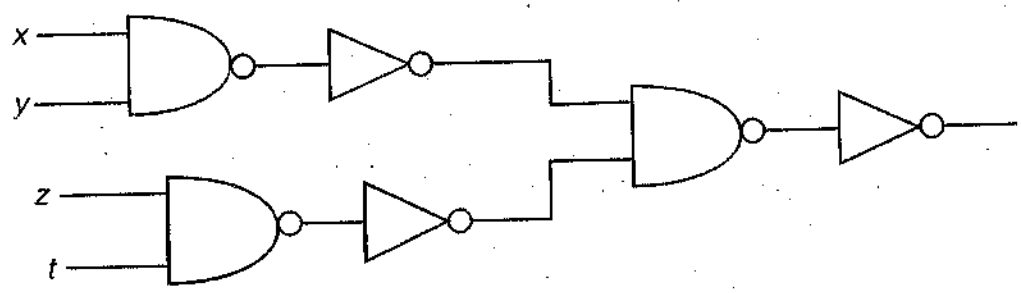


Fig. 12.38

Self-learning exercise-1

1. The NAND gate and the NOR gates are known as the ..... gates.
2. The Boolean expression for a two-input NOR gate is ..... .
3. The Boolean expression for a two-input NAND gate is ..... .
4. The Boolean expression for a two-input XOR-gate is ..... .
5. The Boolean expression for a two-input XNOR-gate is ..... .
6. Two ..... and one ..... gates are needed to implement the Boolean expression

$$E(x, y, z) = x\,y + y\,z.$$

7. If one input of the OR gate is at logic 1, then the out-put of the gate is at logic ..... .
8. If one input of the AND gate is at logic 0 then the output is at logic ..... .
9. An AND gate output will always differ form an OR gate output if the input conditions are same-true or false ?

12.8 Summary

In the current unit, we studied the switching circuits, the two-state devices and the logic gates. Three basic logic gates the NOT-gate *i.e.* the Inverter, the NOR-gate and the AND-gate are the basic

elements that make up a digital system. The universal gates i.e. the NOR gate and the NAND gate are used to construct the basic logic gates. Also the other combinations of logic gates namely the XOR-gate and XNOR-gate are of no less importance as they are the reduced digital logic circuits.

12.9 Answers to self-learning exercises

Self-learning exercise-1

1. All the switches are closed.
2. Yes
3. S_2 or S_3 and S_4 or S_6 and S_7 or S_8.

Self-learning exercise-2

1. Universal gates
2. $f(x, y) = (x + y)' = x' y'$
3. $f(x, y) = (x \cdot y)' = x' + y'$
4. $f(x, y) = x \oplus y = x y' + x' y$
5. $f(x, y) = x \odot y = x y + x' y'$
6. AND, OR
7. 1
8. 0
9. False

12.10 Exercises

1. Why are NOR gate and NAND gate known as the universal gates ?
2. Develop the digital logic circuit for each of the following Boolean expressions, using OR, AND and NOT-gates :

   (a) $E(x, y, z) = x y + yz$

   (b) $E(x, y, z) = x (y' + z)$

   (c) $E(x, y, z, t) = x y (z + t)$
3. Using only the NAND gate, develop logic circuit for each of the Boolean expression :

   (a) $E(x, y, z, t) = (x + z) (y' + t)$

   (b) $E(x, y, z, t) = x y (z + t)$
4. Develop a digital logic circuit for each of the following Boolean expression using only NOR-gates :

   (a) $E(x, y, z, t) = x y z + x t.$

   (b) $E(x, y, z) = x (y' + z).$

□□□

Reference Books

1. **Elements of Discrete Mathematics**

   C.L. Liu

   McGraw-Hill Book Company, Newyork, 1985

2. **Discrete Mathematics**

   Schaum's Outlines

   S. Litschutz and Lars Lipson

   Tata McGraw-Hill Pub. Company, New Delhi, 1997

3. **Elements of Discrete Mathematics**

   Dileep S. Chauhan and Rakesh Pandey

   Jaipur Publishing House, Jaipur, 2007