GMA S2 01

Abstract Algebra and Discrete Mathematics

SEMESTER - II

Mathematics

BLOCK - 2



KRISHNA KANTA HANDIQUI STATE OPEN UNIVERSITY

Subject Experts

Prof. N. R. Das, Dept of Mathematics, Gauhati University
Dr. Dillip Kumar Sarma, Former Head, Cotton College

Course Coordinator : Harekrishna Deka, Academic consultant, KKHSOU

SLM Preparation Team

UNITS	CONTRIBUTORS
9, 10, 11, 12, 14	Dr Dilip Kumar Sarma Cotton College, Guwahati
13	Harekrishna Deka KKHSOU

Editorial Team

Content : Prof. Biswajit Bhagawati,Former Head, ,Cotton college
Structure & Format : Harekrishna Deka, KKHSOU

January, 2018, Review: (if any)

© Krishna Kanta Handiqui State Open University.
This Self Learning Material (SLM) of the Krishna Kanta Handiqui State Open University is made available under a Creative Commons Attribution-NonCommercial-ShareAlike4.0 License (international): http://creativecommons.org/licenses/by-nc-sa/4.0/
For the avoidance of doubt, by applying this license KKHSOU does not waive any privileges or immunities from claims that it may be entitled to assert, nor does KKHSOU submit to the jurisdiction, courts, legal processes or laws of any jurisdiction.

Printed and published by Registrar on behalf of the Krishna Kanta Handiqui State Open University.

Headquarters : Patgaon, Rani Gate, Guwahati - 781017
City Office : Housefed Complex, Dispur, Guwahati-781006; Web: www.kkhsou.in

BLOCK INTRODUCTION

This is the second block of the course ;Abstract Algebra and Discrete Mathematics'. The block consists of six unit.

In ninth unit, we will discuss ring and its properties.

The tenth unit consists of Integral domains and Field. In this unit, you will know about properties of Integral domains and Field.

The eleventh unit deals with the concept of vector space. In this unit, we will discuss properties of vector space and subspace of a vector space. We will also discuss linear dependence and independence of a vactor space. Finally, we also define basis and dimension of a vector space in this unit.

The twelvth unit deals with the concept of combintorics. After going through this unit, you will be able to know permutations and combinations.

In thirteenth unit, we will discuss the concept of Mathematical logic. In this unit, we will discuss the different logical connectives.

The concept of Boolean Algebra will be discussed in the fourtheenth unit. In this unit, we will discuss some basic laws of Boolean Algebra and Boolean Expression.

While going through a unit, you wll notice some along side boxes, which have been included to help you know some of the difficult, unseen terms. At the end of each section, you will get "CHECK YOUR PROGRESS" questions. These have been designed to self-check your progress of study. It will be better if you solve the problems put in these boxes immediately after you go through the sections of the units and then match your answers with " ANSWERS TO CHECK YOUR PROGRESS" Given the end of each unit.

CONTENTS

UNIT 9: Ring **Page : 121-132**

Definitions and Examples of Rings, Properties of Ring.

UNIT 10: Integral domain & Field **Page : 133-140**

Integral domains, Field and their properties.

UNIT 11: Vector space **Page : 141-166**

Defintion and examples of vector space, Elementary properties, subspace of a vector space, Linear dependence and Independence, Basis and Dimension.

UNIT 12: Cominatorics **Page : 167-183**

The Rule of Sum, The Rule of product, Permutation, Combination.

UNIT 13: Mathematical Logic **Page : 184-201**

Definition of Statements, Examples of Statements, Logical Connectives : Negation, Conjunction, Disjunction Conditional, Biconditional.

UNIT 14: Boolean Algebra **Page : 102-232**

Definition, Properties and Examples, Basic Laws of Boolean Algebra, Boolean Expression.

UNIT 9: RING

UNIT STRUCTURE

9.1 Learning objectives

9.2 Introduction

9.3 Ring

9.4 Properties of Ring

9.5 Let us Sum up

9.6 Answers to "Check Your Progress"

9.7 Further Readings

9.8 Model Questions

9.1 LEARNING OBJECTIVES

After going through this unit, you will be able to know

- ring
- properties of ring.

9.2 INTRODUCTION

We have discussed group and its various properties, sub group, coset, cyclic group, normal sub groups and quotient group. In this unit we will study ring. Ring is an algebraic structure, i,e., a non-empty set equipped with two binary operations and satisfying certain postulates.

9.3 RING

A non-empty set R, equipped with two binary operations, called addition (+) and multiplication (·) is called a ring if the following postulates are satisfied.

(1) R is an additive Abelian group,

(2) R is an multiplicative semigroup

(3) The two distributive laws hold good, viz

a. (b + c) =a.b + a.c. (left distributive law)

(a + b). c = a.c + b.c, (right distributive law) for all a, b, c $\in$ R

Note : 1. In order to be a ring, there must be a non-empty set equipped with two binary operations, viz, + and . , satisfying the postulates mentioned above. Later on we will simply write ''Let R be a ring''. It should be borne in mind that there are two binary operations, viz, + and . , on R.

2. It should also be borne in mind that the binary operations + and . may not be known usual addition and multiplication.

3. Since R is an additive Abelian group, the additive identity, denoted by 0, belongs to R. It is called the zero element of R. Here 0 is a symbol. It should not be confused with the real number zero.

4. If a , b $\in$ R, then - b $\in$ R ($\because$ R is an additive group). a+ (– b) is, generally, denoted by a – b.

5. a.b is, generally, written as ab.

Commutative Ring: A ring R is said to be commutative if ab = ba, for all a, b $\in$ R.

Ring with unity : A ring R is said to be a ring with unity (or identity) if there exists an element e $\in$ R such that

ae = a = ea, for all a $\in$ R.

Note 1. A ring may or may not have a unity.

2. If R is a ring with unity, unity may be same as the zero element. For example, {0} is a commutative ring with unity . Here 0 is the additive as well as the multiplicative identity. It is known as the zero ring.

Theorem 1 : If R is a ring with unity, then unity is unique.

Proof Let R be a ring with unity. If possible, let e and f be two identities of R.

ef = e = fe [$\because$ f is unity]

ef = f = fe [$\because$ e is unity]

$\therefore$ e = f

Note: In view of the above theorem, we write ''the unity''.

Example 1. Let R = $\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$: a, b are integers$\}$

I (i) Let $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R$, $\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in R$,

a, b, c, d $\in$ Z

Now $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 0 & 0 \end{pmatrix} \in R$

$\therefore$ Matrix addition is a binary operation on R.

(ii) We know that matrix addition is associative.

(iii) We have $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$,

and $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(iv) For every $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R$, we have $\begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} \in R$ such that

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

$\therefore \begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix}$ is the additive inverse of $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$.

(v) We know that matrix additive is commutative.

$\therefore$ R is an Abelian group under matrix addition.

II. (i) We have $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} \in R$

$\therefore$ matrix multiplication is a binary operation on R

(ii) We know that matrix multiplication is associative.

$\therefore$ R is a semigroup under matrix multiplication.

III. We know that matrix multiplication is distributive over matrix addition.

The two distributive laws are satisfied.

$\therefore$ R is a ring under matrix addition and matrix multiplication.

We have $\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \in R$, $\begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix} \in R$

$$\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}=\begin{pmatrix}3 & 6\\ 0 & 0\end{pmatrix}$$

$$\therefore \begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}\begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix}\neq\begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}$$

$\therefore$ R is a non- commutative ring.

Again, there does not exist any element $X \in G$ such that

$$x\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}x \text{, for all } \begin{pmatrix}a & b\\ 0 & 0\end{pmatrix} \in R$$

$\therefore$ R is a ring without unity.

Example 2 Let R be the set of all 2 x 2 matrices over integers.

I. Clearly R is an Abelian group under matrix addition.

II. R is a semigroup under matrix multiplication.

III. The two distributive laws are satisfied.

$\therefore$ R is a ring under matrix addition and matrix multiplication.

We know that matrix multiplication is not, in general, commutative.

$\therefore$ R is a non-commutative ring.

We have $I = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \in R$, and

$AI = A = IA$, for all $A \in R$.

$\therefore$ R is a ring with unity.

Example 3: Let 2Z be the set of all even integers

I. 2Z is an Abelian group under usual addition.

II. 2Z is a multiplicative semigroup.

III. The two distributive laws are satisfied.

$\therefore$ 2Z is a ring under usual addition and multiplication.

Moreover, 2Z is a commutative ring.

2Z is a ring without unity, for $1 \notin 2Z$.

Example 4: Let Z be the set of integers.

I. Z is an Abelian group under usual addition.

II. Z is a multiplicative semigroup.

III. The two distributive laws are satisfied.

$\therefore$ Z is a ring under usual addition and scalar multiplication.

Moreover, Z is a commutative ring . It is also a ring with unity, $1 \in Z$.

Other examples of commutative rings with unity are

- the ring Q of rational numbers
- the ring IR of real numbers.
- the ring C of complex numbers.

Example 5: Let C [a, b] denote the set of all real-valued continuous functions defined on [a, b] ; a, $b \in R$

Let $f, g \in C[a, b]$

We define $(f + g)(x) = f(x) + g(x)$

$(fg)(x) = f(x)\, g(x),\ x \in [a, b]$

I. (i) We have $(f + g)(x) = f(x) + g(x) \in R$

Also, the sum of two continuous functions is continuous.

$\therefore$ f + g is continuous and so $f + g \in C[a, b]$

$\therefore$ addition of functions is a binary operation on C [a, b].

(ii) Let $f, g, h \in C[a, b]$, $x \in [a, b]$

$$\begin{aligned}((f+g)+h)(x) &= (f+g)(x) + h(x)\\ &= (f(x) + g(x)) + h(x)\\ &= f(x) + (g(x) + h(x))\\ &= f(x) + (g+h)(x)\\ &= (f + (g+h))(x), \forall x \in [a, b]\end{aligned}$$

$\therefore (f + g) + h = f + (g + h)$

(iii) We have $0 : [a, b] \to R$, $0(x) = 0$, $\forall\, x \in [a, b]$

Clearly $0 \in C[a, b]$, and

$0 + f = f = f + 0$

(iv) For every $f \in C[a, b]$, we define

$-f : [a, b] \to R$, $(-f)(x) = -f(x)$

Clearly $-f \in C[a, b]$, and

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0 = 0(x)$$

$\therefore f + (-f) = 0$

Similarly $(-f) + f = 0$

(v) $(f + g)(x) = f(x) + g(x)$

$= g(x) + f(x)$

$= (g + f)(x),\ \forall\, x \in [a, b]$

$\therefore f + g = g + f$

$\therefore$ C [a, b] is an Abelian group under addition of functions.

II. (i) (fg) (x) = f (x) g (x) $\in \mathbb{R}$

Also, the product of two continous functions is continuous.

$\therefore$ fg is continuous and so fg $\in$ C [a, b].

$\therefore$ Multiplication of functions is a binary operation on C [a, b]

(ii) ((fg) h) (x) = (fg) (x) h (x)

= (f (x) g (x)) h (x)

= f (x) (g (x) h (x))

= f (x) (gh) (x)

= (f (gh)) (x), $\forall x \in [a, b]$

$\therefore$ (fg)h = f (gh)

$\therefore$ C [a, b] is a semigroup under multiplication of functions.

III. ((f+g) h) (x) = (f + g) (x) h (x)

= (f (x) + g (x)) h (x)

= f (x) h (x) + g (x) h(x)

= (f h) (x) + (gh) (x)

= (fh + gh)(x)

$\therefore$ (f + g) h = fh + gh

Similarly f (g + h) = fg + fh

$\therefore$ C [a , b] is a ring under addition and multiplication of functions.



CHECK YOUR PROGRESS - 1

Q 1: Give an example of a commutative ring with unity having only one element.

Q 2: Give an example of a non-commutative ring without unity.

Q 3: Give an example of a commutative ring without unity.

Q 4: Give an example of a non-commutative ring with unity.

Q 5: Give an example of an infinite commutative ring with unity.

Q 6: Let $IR^2 = \{(a, b) : a, b \text{ are reals}\}$

We define

(a, b) + (c, d) = (a + c, b + d),

(a, b) (c, d) = (ac, bd);

a, b, c, d are reals.

Show that IR^2 is a commutative ring with unity.

9.4 PROPERTIES OF RING

Let R be a ring. Then

(i) $a0 = 0a = 0$; for all $a \in R$

(ii) $a(-b) = (-a)b = -(ab)$; for all $a, b \in R$

(iii) $(-a)(-b) = ab$; for all $a, b \in R$

(iv) $a(b - c) = ab - ac$; for all $a, b, c \in R$

Proof (i) we have

$a0 = a(0 + 0)$

$= a0 + a0$, by left distributive law

$\therefore a0 + 0 = a0 + a0$

$\Rightarrow 0 = a0$, by left cancellation law in the additive group R

i. e $a0 = 0$

Similarly $0a = 0$

(ii) We have $a0 = 0$

This $\Rightarrow a((-b) + b) = 0$, $[\because (-b) + b = 0]$

$\Rightarrow a(-b) + ab = 0$, by left distributive law

$\Rightarrow a(-b)$ is the additive inverse of ab

$\therefore$ i.e., $a(-b) = -(ab)$

Similarly $(-a)b = -(ab)$

(iii) We have $(-a)(-b) = l(-b)$, taking $l = -a$

$= -(lb)$, using (ii)

$= -((-a)b)$

$= -(-(ab))$, using (ii)

$= ab$

(iv) $a(b - c) = a(b + (-c))$

$= ab + a(-c)$, by left distributive law

$= ab - ac$, by (ii)

Boolean Ring: Let R be a ring and $a \in R$.

a is called an idempotent element of R if $a^2 = a$.

A ring R is called a Boolean ring, if every element of it is idempotent.

Note: George Boole (1815-1864) of the nineteenth century was ‘‘an essentially self-taught Britisher’’. He is famous for his epoch - making book The Laws of Thought.

Theroem 3: Let R be a Boolean ring. Then

(i) $a + a = 0$, for all $a \in R$

i. e. every element of R is its own additive inverse

(ii) $a + b = 0 \Rightarrow a = b$, for all $a, b \in R$

(iii) R is a commutative ring.

Proof : (i) Let $a \in R$. $\therefore a^2 = a$

Also $a + a \in R$

$\therefore (a + a)^2 = a + a$ [$\because$ R is a Boolean ring]

$\Rightarrow (a + a)(a + a) = a + a$

$\Rightarrow (a + a)a + (a + a)a = a + a$, By left distributive law

$\Rightarrow (a^2 + a^2) + (a^2 + a^2) = a + a$, by right distributive law

$\Rightarrow (a + a) + (a + a) = (a + a) + 0$

$\Rightarrow a + a = 0$, by left cancellation law in the additive group R

(ii) We have $a + a = 0$

$\therefore a + b = a + a$, by (i)

$\Rightarrow b = a$, by left cancellation law in the additive group R

i.e. $a = b$

(iii) Let $a, b \in R \therefore a^2 = a, b^2 = b$

Also $a + b \in R$

$\therefore (a + b)^2 = a + b$

$\Rightarrow (a + b)(a + b) = a + b$

$\Rightarrow (a + b)a + (a + b)b = a + b$, by left distributive law

$\Rightarrow (a^2 + ba) + (ab + b^2) = a + b$

$\Rightarrow (a + ba) + (ab + b) = a + b$

$\Rightarrow (a + b) + ba + ab = (a + b) + 0$, by associative and commutative law of addition.

$\Rightarrow ba + ab = 0$, by left cancellation law in the additive group R.

$\Rightarrow ab = ba$, by (ii)

$\therefore$ R is a commutative ring.



CHECK YOUR PROGRESS - 2

Q 1: Let $R = \{a + b\sqrt{2} : a, b \in Z\}$. Show that R is a commutative ring with unity under usual operations of addition and multiplication.

Q 2: If in a ring R, $a^2 = a$ for all $a \in R$, show that $2a = 0$ and $a + b = 0 \Rightarrow a = b$

Q 3: In z,define $\oplus$ and $\otimes$ as $a \oplus b = a + b + 1, a \otimes b = a + b + ab$. Show that Z is a commutative ring under the operations $\oplus$ and $\otimes$. Is it a ring with unity ?



9.5 LET US SUM UP

- A non-empty set R, equipped with two binary operations, called addition (+) and multiplication (·), is called a ring if the following postulates are satisfied.

(i) R is an additive Abelian group

(ii) R is a multiplicative semigroup

(iii) The two distributive laws hold good, viz.,

a . (b + c) = a.b + a.c, (left distributive law)

(a + b).c = a.c + b.c, (right distributive law)

for all a, b, $c \in R$

- A ring R is said to be commutative if ab = ba, for all a, $b \in R$
- A ring R is said to be a ring with unity (or identity) if there exists an element $e \in R$ such that

ae = a = ea, for all $a \in R$



9.6 ANSWERS TO "CHECK YOUR PROGRESS"

CHECK YOUR PROGRESS-1

Ans to Q No1: {0} is a commutative ring with unity. It should be noted that, in this ring, 0 is the additive as well as the multiplicative identity.

Ans to Q No 2: The ring R = $\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$: a, b are integers$\}$ is a non-commutative ring without unity.

Ans to Q No 3: The ring 2Z of even integers is a commutative ring without unity.

Ans to Q No 4: The ring R of all 2 x 2 matrices over integers is a non-commutative ring with unity.

Ans to Q No 5: The ring Z of integers is an infinite commutative ring with unity.

Ans to Q No 6: $IR^2 = \{(a, b) : a, b \text{ are reals}\}$

I. (i) Let $(a, b), (c, d) \in IR^2$, where a, b, c, d are reals

Now $(a, b) + (c, d) = (a + c, b + d) \in IR^2$

(ii) Let $(a, b), (c, d), (e, f) \in IR^2$

$((a, b) + (c, d)) + (e, f) = (a + c, b + d) + (e, f)$

$= ((a + c) + e, (b + d) + f)$

$= (a + (c + e), b + (d + f))$

$= (a, b) + (c + e, d + f)$

$= (a, b) + ((c, d) + (e, f))$

$\therefore$ addition is associative.

(iii) We have $(0, 0) \in IR^2$,

and $(0, 0) + (a, b) = (a, b) = (a, b) + (0, 0)$

$\therefore$ (0, 0) is the additive identity.

(iv) For every $(a, b) \in IR^2$, we have $(-a, -b) \in IR^2$ such that $(a, b) + (-a, -b) = (0, 0) = (-a, -b) + (a, b)$

$\therefore$ (–a, – b) is the additive inverse of (a, b).

(v) (a, b) + (c, d) = (a + c, b + d)

= (c + a, d + b)

= (c, d) + (a, b)

$\therefore$ addition is commutative.

$\therefore$ IR^2 is an additive Abelian group.

II. (i) (a, b) (c, d) = (ac, bd) $\in IR^2$

(ii) ((a, b) (c, d)) (e, f) = (ac, bd) (e, f)

= ((ac) e, (bd) f)

= (a (ce), b (df))

= (a, b) (ce, df)

= (a, b) ((c, d) (e, f))

$\therefore$ multiplication is associative.

$\therefore$ IR^2 is a multiplicative semigroup.

III. (a, b) ((c, d) + (e, f)) = (a, b) (c + e ,d + f)

= (a (c + e), b (d + f))

= (ac + ae, bd + bf)

= (ac, bd) + (ae, bf)

= (a, b) (c, d) + (a, b) (e, f)

Similarly ((a, b) + (c, d)) (e, f) = (a, b) (e, f) + (c, d) (e, f)

$\therefore$ IR^2 is a ring

Furthermore, (a, b) (c, d) = (ac, bd)

= (ca, db)

= (c, d) (a, b)

$\therefore$ IR^2 is a commutative ring.

Again, (1, 1) $\in IR^2$, and

(a, b) (1, 1) = (a1, b1) = (a, b) = (1, 1) (a, b)

$\therefore$ (1, 1) is the unity.

$\therefore$ IR^2 is a ring with unity.

Thus, IR^2 is a commutative ring with unity

CHECK YOUR PROGRESS - 2

Ans to Q No 1: It can be easily verified that R is a commutative ring with

$$0 = 0 + 0\sqrt{2}$$

as additive identity and $1 = 1 + 0\sqrt{2}$ as the multiplicative identity or unity R.

Ans to Q No 2: Properties of Rings ((i), (ii))

Ans to Q No 3: It can be easily verified that Z is a commutative ring under the given operations.Also $a \otimes 0 = 0 = 0 \otimes a \ \ \forall a \in Z$ .Hence,it is a ring with unity 0.



9.7 FURTHER READINGS

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.

2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).

3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).

4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.

5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.



9.8 MODEL QUESTIONS

Q 1: Let Z be the set of integers, We define (+) and (·) on Z as follows

a (+) b = a + b – 1,

a (·) b = a + b – ab, for all a, b $\in$ Z

Examine Z is a commutative ring with unity under (+), (·).

Q 2: Prove that a ring R is commutative if and only if

$(a + b)^2 = a^2 + 2ab + b^2$, for all a, b $\in$ R

[Here a^2 means aa]

*** ***** ***

UNIT 10: INTEGAL DOMAIN & FIELD

UNIT STRUCTURE

10.1 Learning objectives

10.2 Introduction

10.3 Integral Domain

10.4 Field

10.5 Let us Sum up

10.6 Answers to "Check Your Progress"

10.7 Further Readings

10.8 Model Questions

10.1 LEARNING OBJECTIVES

After going through this unit you will be able to know

- Integral domain and its properties
- Field and their properties.

10.2 INTRODUCTION

In Unit 9, we have discussed ring and its various properties. In this unit we will study Integral domain and Field. Integral domain and Field are also a Ring satisfying certain postulates.

10.3 INTEGRAL DOMAIN

Let us consider the ring R of all 2 x 2 matrices over integers.

Let $A = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \in R$ and $B = \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix} \in R$

Here A is not a null matrix, B is not a null matrix, i.e. $A \neq 0$, $B \neq 0$

But $AB = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}$

$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$

i.e, AB is a null matrix.

Thus, we see that $A \neq 0$, $B \neq 0$; but AB = O.

Again, let us consider the ring Z of integers. If $a, b \in Z$ and

$a \neq 0$, $b \neq 0$, then $ab \neq 0$

Definition: An element $a (\neq 0)$ in a ring R is called a zero divisor if there exists an element $b (\neq 0)$ in R such that ab = 0 or ba = 0.

We see that the ring R of all 2 x 2 matrices over integers has zero divisors whereas the ring Z of integers has no zero divisors, for if $a \in Z$, $b \in Z$, $a \neq 0$, $b \neq 0$, then $ab \neq 0$, $ba \neq 0$.

Concellation Laws: Let R be a ring. The additive cancellation laws hold good in R, since R is an additive Abelian group.

So, by cancellation laws in a ring, we mean multiplication laws (cancellation of non zero elements).

The cancellation laws hold good in R if $ab = ac \Rightarrow b = c$, $ba = ca \Rightarrow b = c$; where $a, b, c \in R$, $a \neq 0$.

Theorem 1: The cancellation laws hold good in a ring R if and only if R has no zero divisors.

Proof: Let the cancellation laws hold good in a ring R.

Let $a, b \in R$ such that ab = 0

If $a \neq 0$, $ab = 0 \Rightarrow ab = a0 \Rightarrow b = 0$, by cancellation law.

Similarly, if $b \neq 0$, $ab = 0 \Rightarrow ab = 0b \Rightarrow a = 0$.

So there can be no zero divisor.

Conversely, let there be no zero divisors in R.

Let $a, b, c \in R$ and $ab = ac$, $a \neq 0$

$\therefore ab - ac = 0$

$a(b - c) = 0$

$\therefore a \neq 0$ and R is without zero divisors

$\therefore b - c = 0 \Rightarrow b = c$

Thus, if $a \neq 0$, $ab = ac \Rightarrow b = c$

similarly, if $a \neq 0$, $ba = ca \Rightarrow b = c$

Thus, the cancellation laws hold good in R.

Definition A commutative ring with unity $e \neq 0$ and containing no zero divisors is called an Integral Domain.

The simplest example of an integral domain is the ring Z of integers. It is a commutative ring, has unity and is without zero divisors.

Note: An integral domain may be considered as a generalisation of Z.

Example 1: Let us consider the set R = {a + bi : a, b are integers, $i = \sqrt{-1}$} of Gaussian integers, after the name of C. F. Gauss (1777-1855).

I. (i) Let a + bi, c + di $\in$ R,

a, b, c, d are integers, i = $\sqrt{-1}$

(a + bi) + (c + di) = (a + c) + (b + d)i $\in$ R

(ii) Addition of complex numbers is associative.

(iii) We have 0 = 0 + 0i $\in$ R

and 0 + (a + bi) = a + bi = (a + bi) + 0

(iv) For every a + bi $\in$ R, we have (–a) + (–b)i $\in$ R such that

(a + bi) + ((–a) + (–b)i) = 0 =((–a) + (–b)i) + (a + bi)

(v) Addition of complex numbers is commutative.

$\therefore$ R is an Abelian group under addition of complex numbers.

II. (i) (a + bi) (c + di) = (ac – bd) + (ad + bc)i $\in$ R

(ii) Multiplication of complex numbers is associative

$\therefore$ R is a semigroup under multiplication of complex numbers.

III. Clearly the two distributive laws hold good.

$\therefore$ R is a ring

Furthermore, multiplication of complex numbers is commutative.

$\therefore$ R is a commutative ring.

Also R possesses 1 (1=1 + oi)

$\therefore$ R is a ring with unity.

Again we know that the product of two non-zero complex numbers cannot be zero.

$\therefore$ R is without zero divisors.

Thus, R is an integral domain.

10.4 FIELD

Definition: Let R be a ring with unity e $\neq 0$. If every non-zero element of R has multiplicative inverse in R, then R is called a Division Ring (or a Skew

Field).

A commutative division ring is called a field.

The simplest example of a field is the ring IR of real numbers.

It is commutative, has unity and every non-zero element has multiplicative inverse in IR.

Therefore, IR is a field.

Similarly, the ring C of complex numbers is also a field.

Note: The ring z of integers is not a field. (why?)

Example 2: Examine if the ring

R = {a + bi : a, b, are integers, i = $\sqrt{-1}$ }

of Gaussian integers is a field.

Solution: We know that R is a commutative ring with unity.

(Ref. Example 6)

Let a + bi $\in$ R such that a + bi $\neq 0$

Now the multiplicative inverse of a + bi is $\frac{a}{a^2+b^2}+\left(-\frac{b}{a^2+b^2}\right)i$ which is not an element of R.

$\therefore$ R is not a field.

Theorem 2: Every field is an integral domain.

Proof: Let F be a field.

Let a, b $\in$ F such that a $\neq 0$ and ab = 0

$\therefore$ a $\neq$ 0, $a^{-1} \in$ F (F is a field)

Now ab = 0

$\Rightarrow$ a^{-1} (ab) = a^{-1} 0

$\Rightarrow$ (a^{-1} a) b = 0

$\Rightarrow$ b = 0

Similarly, if b $\neq 0$ and ab = 0, then a = 0

$\therefore$ F has no zero divisors.

Thus, F is a commutative ring with unity and containing no zero divisors.

$\therefore$ F is an integral domain.

Note: The converse of the above theorem is not true, i.e, every integral domain is not a field.

Let us consider the ring Z of integers. We know that Z is an integral domain. But only two elements, viz, –1 and 1 have multiplicative inverses in Z. $\therefore$ Z is not a field.

However we have the following

Theorem 3: A non-zero finite integral domain is a field.

Proof: Let R = $\{a_1, a_2, a_3, ... a_n\}$ be a finite non-zero integral domain, where all the a_i's are distinct.

Let a_1 be the zero element of R.

Let us consider the non zero elements $a_2, a_3, ..., a_n$.

Let a_p be not the unity of R ($p \neq 1$),i.e., $a_p \neq e$, the unity of R.

Let us consider the products

$a_p a_2$, $a_p a_3$, ..., $a_p a_n$

All these elements belong to R. Also all the elements are distinct, for if

$a_p a_i = a_p a_j$, $2 \leq i \leq n$, $2 \leq j \leq n$, $i \neq j$

then $a_p a_i - a_p a_j = 0$

$a_p \neq e$,

$\Rightarrow a_p (a_i - a_j) = 0$

$\Rightarrow a_i - a_j = 0$, [$\because a_p \neq 0$ and R is without zero divisors]

$\Rightarrow a_i = a_j$, which is a contradiction

Now one of $a_p a_2$, $a_p a_3$, ..., $a_p a_n$ must be unity, Let $a_p a_q = e$, where e is the unity of R

Then $a_p a_q = e = a_q a_p$.

$\therefore a_p$ has multiplicative inverse in R. If a_p is the unity of R, then a_p has multiplicative inverse in R.

Thus, every non-zero element of R has multiplicative inverse in R.

$\therefore$ R is a field.

Theorem 4: A division ring has no zero divisors.

Proof: Let R be a division ring.

Let a, b $\in$ R such that $a \neq 0$ and ab=0

$\therefore a \neq 0$, $a^{-1} \in$ R ($\because$ R is a division ring)

Now ab = 0

$\Rightarrow a^{-1} (ab) = a^{-1} 0$

$\Rightarrow (a^{-1}a)b = 0$

$\Rightarrow b = 0$

Similarly, if $b \neq 0$ and $ab = 0$, then $a = 0$.

$\therefore$ R is without zero divisors



CHECK YOUR PROGRESS

Q 1: Does the ring Q of rational numbers contain zero divisors?

Q 2: Let R be the ring of all 2 x 2 matrices over integers, Does the cancellation laws hold good in R?

Q 3: Is the ring 2Z of even integers an integral domain?

Q 4: Give an example of an integral domain which is not a field.

Q 5: Does the ring $IR^2 = \{(a, b) : a, b \in IR\}$ contain zero divisiors?



10.5 LET US SUM UP

- An element $a(\neq 0)$ in a ring R is called a zero divisor if there exists an element $b (\neq 0)$ in R such that $ab = 0$ or $ba = 0$
- A commutative ring with unity $e \neq 0$ and containing no zero divisors is called an integral domain
- Let R be a ring with unity $e \neq 0$.
  If every non-zero element of R has multiplicative inverse in R, then R is called a division ring (or a skew field).
  A commutative division ring is called a field.
- Every field is an integral domain, but every integral domain is not a field.
- A non-zero finite integral domain is a field.

10.6 ANSWERS TO "CHECK YOUR PROGRESS"

CHECK YOUR PROGRESS

Ans to Q No 1: No. If a, b $\in$ Q and a $\neq 0$, b $\neq 0$, then ab $\neq 0$

Ans to Q No 2: No. Cancellation laws hold good in a ring if and only if it has no zero divisors. The ring of all 2 x 2 matrices over integers contains zero divisors. So cancellation laws do not hold good in the ring of all 2 x 2 matrices over integers.

For example

$$\begin{pmatrix}1 & 3\\ 3 & 9\end{pmatrix}\begin{pmatrix}3 & 3\\ 5 & 7\end{pmatrix}=\begin{pmatrix}18 & 24\\ 54 & 72\end{pmatrix}$$

$$\begin{pmatrix}1 & 3\\ 3 & 9\end{pmatrix}\begin{pmatrix}6 & 9\\ 4 & 5\end{pmatrix}=\begin{pmatrix}18 & 24\\ 54 & 72\end{pmatrix}$$

i. e. $\begin{pmatrix}1 & 3\\ 3 & 9\end{pmatrix}\begin{pmatrix}3 & 3\\ 5 & 7\end{pmatrix}=\begin{pmatrix}1 & 3\\ 3 & 9\end{pmatrix}\begin{pmatrix}6 & 9\\ 4 & 5\end{pmatrix}$,

i. e. AB = AC, but B $\neq$ C,

where $A=\begin{pmatrix}1 & 3\\ 3 & 9\end{pmatrix}$, $B=\begin{pmatrix}3 & 3\\ 5 & 7\end{pmatrix}$, $C=\begin{pmatrix}6 & 9\\ 4 & 5\end{pmatrix}$

Ans to Q No 3: The ring 2Z of even integers is not an integral domain, since it does not contain the multiplicative identity.

Ans to Q No 4: The ring Z of integers is an integral domain, but not a field. Only –1 and 1 have multiplicative inverses in Z,

Ans to Q No 5: Yes.

(7, 0) $\in$ IR^2, (0, 13) $\in$ IR^2 ,(7, 0) $\neq$ (0, 0), (0, 13) $\neq$ (0, 0).

But (7, 0) (0, 13) = (0, 0).



10.7 FURTHER READINGS

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.



10.8 MODEL QUESTIONS

Q 1: Let R = {(a, b) : a, b are reals}. We define

(a, b) + (c, d) = (a + c, b + d)

(a, b) (c, d) = (ac – bd, bc + ad)

Prove that R is a field.

Q 2: Let R = {a + b $\sqrt{2}$: a, b are rational numbers}. show that R is a field under usual addition and multiplication.

Q 3: Let R be a commutative ring with unity and is without zero divisors. Show that the only idempotent elements are the zero element and the unity element.

*** ***** ***

UNIT 11: VECTOR SPACE

UNIT STRUCTURE

11.1 Learning objectives

11.2 Introduction

11.3 Defintion and examples of vector space

11.4 Elementary properties

11.5 Subspace of a vector space

11.6 Linear dependence and Independence

11.7 Basis and Dimension

11.8 Let us Sum Up

11.9 Answers to Check Your Progress

11.10 Further Readings

11.11 Model Questions

11.1 LEARNING OBJECTIVES

After going through this unit, you will be able to know :

- definition and examples of vector space
- elementary properties of vector space
- subspace of a vector space
- linear dependence and independence of vectors
- basis and dimension of a vector space

11.2 INTRODUCTION

We know the notion of a vector. The concept of a vector space comes from the notion of a vector.In vectors, we have addition of vectors, multiplication of a vector by a scalar, and the scalar product of vectors.In vector space also, we find the addition of vectors,multiplication of a vector by a scalar and the scalar product of vectors.Thus a vector space may be regarded as a generalisation of a vector that is found in mechanics or Analytical geometry.

11.3 DEFINITION AND EXAMPLES OF VECTOR SPACE

Definition : Let V be an Abelian group under " + ". Let F be a field under "+, $\bullet$ ".

For each element $\alpha \in F$, $x \in V$,we have $\alpha x \in V$, called scalar multiplication.

Then V is said to be a vector space over the field F if the following conditions are satisfied.

1. $\alpha(x+y) = \alpha x + \alpha y$
2. $(\alpha + \beta)x = \alpha x + \beta x$
3. $(\alpha\beta)x = \alpha(\beta x)$
4. $1x = x$

where $\alpha, \beta \in F$, $x, y \in V$ and 1 is the unit element of F.

We write "$V(F)$ is a vector space".

Note

1. The element of V are called vectors, and the elements of F are called scalars.
2. $x+y$ denotes the "addition " (+) of two vectors $x, y \in V$, whereas $\alpha+\beta$ denotes "addition " (+) of two scalars $\alpha, \beta \in F$. It should be borne in mind that these two additions are different, though they are denoted by the same symbol.
3. αx denotes the "multiplication" of a vector $x \in V$ by a scalar $\alpha \in F$;whereas $\alpha\beta$ denotes the "multiplication"of two scalars $\alpha, \beta \in F$. It should be borne in mind that these two multiplication are also different ,though they are denoted by the same symbol.
4. V is an Abelian group under " + ". So,we have the operation " + "in V .F is a field under "+, $\bullet$ ".Also,we have multiplication of a vector by a scalar.Thus ,we have altogether four operations in a vector space.
5. V is an Abelian group under " + ".So,we have the additive identity 0 under +,called the zero element.Again F is a field.So,we have the zero element $0 \in F$ .These two zeroes are different,though they are dented by the same symbol.Again F contains the unit element 1.It should be borne in mind that 1 is not necessarily the real number 1.

6. If $F = R$,i.e., if F is the field of real numbers,then $V(R)$ is called a real vector space.

   If $F = C$,i.e., if F is the field of complex numbers,then $V(C)$ is called a complex vector space.

7. We define the "subtraction"in V as follows $x - y = x + (-y)$,where $-y$ is the additive inverse of y ; $x, y \in V$.

Example 1 : Let $R^2 = \{(x_1, x_2) : x_1, x_2 \text{ are reals}\}$,and R be the field of real numbers.We define addition and scalar multiplication in R^2 as follows

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \quad \text{... (1)}$$

$$\alpha(x_1, x_2) = (\alpha x_1, \alpha x_2) \quad \text{... (2)}$$

where $x = (x_1, x_2)$, $y = (y_1, y_2) \in R^2$, $\alpha \in R$.

Then R^2 is a vector space over R,i.e. R^2 is a real vector space.

Solution : I.First we prove that R^2 is an Abelian group under + defined by (1)

(i) $x + y = (x_1 + y_1, x_2 + y_2) \in R^2$

(ii) Let $x = (x_1, x_2)$, $y=(y_1,y_2), z=(z_1,z_2) \in R^2$

Now
$$\begin{aligned}(x + y) + z &= (x_1 + y_1, x_2 + y_2) + (z_1, z_2)\\ &= ((x_1 + y_1) + z_1, (x_2 + y_2) + z_2)\\ &= (x_1 + (y_1 + z_1), x_2 + (y_2 + z_2))\\ &= (x_1, x_2) + (y_1 + z_1, y_2 + z_2)\\ &= x + (y + z)\end{aligned}$$

$\therefore$ "+" is associative.

(iii) We have $0 = (0,0) \in R^2$

and $x + 0 = (x_1, x_2) + (0,0) = (x_1 + 0, x_2 + 0) = (x_1, x_2) = x$

Similarly, $0 + x = x$

i.e., $x + 0 = x = 0 + x$

[Note that in $0 = (0,0)$, 0 in the L.H.S is a symbol,not the real number 0]

(iv) For every $x = (x_1, x_2) \in R^2$, there exists $-x = (-x_1, -x_2) \in R^2$ such that

$$\begin{aligned}x + (-x) &= (x_1, x_2) + (-x_1, -x_2)\\ &= (x_1 - x_1, x_2 - x_2)\\ &= (0,0)\\ &= 0\end{aligned}$$

Similarly, $(-x) + x = 0$

i.e. $x+(-x)=0=(-x)+x$

(v) $x+y=(x_1,x_2)+(y_1,y_2)$

$=(x_1+y_1,x_2+y_2)$

$=(y_1+x_1,y_2+x_2)$

$=(y_1,y_2)+(x_1,x_2)$

$=y+x$

$\therefore R^2$ is an abelian group under "+".

II. we have $\alpha\in R, x=(x_1,x_2)\in R^2$

$\alpha x=\alpha(x_1,x_2)$

$=(\alpha x_1,\alpha x_2)\in R^2$

III. (i) $\alpha(x+y)=\alpha(x_1+y_1,x_2+y_2)$

$=(\alpha x_1+\alpha y_1,\alpha x_2+\alpha y_2)$

$=(\alpha x_1,\alpha x_2)+(\alpha y_1,\alpha y_2)$

$=\alpha(x_1,x_2)+\alpha(y_1,y_2)$

$=\alpha x+\alpha y$

(ii) $(\alpha+\beta)x=(\alpha+\beta)(x_1,x_2)$

$=((\alpha+\beta)x_1,(\alpha+\beta)x_2)$

$=(\alpha x_1+\beta x_1,\alpha x_2+\beta x_2)$

$=(\alpha x_1,\alpha x_2)+(\beta x_1,\beta x_2)$

$=\alpha(x_1,x_2)+\beta(x_1,x_2)$

$=\alpha x+\beta x \quad ,\alpha,\beta\in R, x=(x_1,x_2)\in R^2$

(iii) $(\alpha\beta)x=\alpha\beta(x_1,x_2)$

$=((\alpha\beta)x_1,(\alpha\beta)x_2)$

$=(\alpha(\beta x_1),\alpha(\beta x_2))$

$=\alpha(\beta x_1,\beta x_2)$

$=\alpha(\beta(x_1,x_2))$

$=\alpha(\beta x)$

(iv) We have $1\in R$

$1x=1(x_1,x_2)=(1x_1,1x_2)=(x_1,x_2)=x$

$\therefore R^2$ is a vector space over R,i.e., R^2 is a real vector space .

Example 2 : Let $R^n=\{(x_1,x_2,...,x_n): x_i\text{'s are reals}\}$, and R be the field

of real numbers. R^n is a real vector space if we define

$$x+y=(x_1,x_2,...,x_n)+(y_1,y_2,...,y_n)=(x_1+y_1,x_2+y_2,...,x_n+y_n)$$

and $\alpha x=\alpha(x_1,x_2,...,x_n)=(\alpha x_1,\alpha x_2,...,\alpha x_n)$

where $x=(x_1,x_2,...,x_n), y=(y_1,y_2,...,y_n)\in R^n$ and $\alpha\in R^n$.

It can be shown as in the previous example.

Example 3 : Let V be the set of all real-valued continuous functions defined on $[a,b]$.Then V is a real vector space if we define addition and scalar multiplication as follows

$$(f+g)(x)=f(x)+g(x),$$
$$(\alpha f)(x)=\alpha f(x),$$

where $f,g\in V$, and $\alpha\in R$.

I. First we prove that V is an Abelian group under addition.

(i) Let $f,g\in V$

$\therefore$ f and g are real valued continuous functions defined on $[a,b]$

$\therefore$ $f+g$ is also a real valued continous function defined on $[a,b]$

$y\in W_1$ $\therefore$ $f+g\in V$.

(ii) Let $f,g,h\in V$ and $x\in[a,b]$

Now, $((f+g)+h)(x)=(f+g)(x)+h(x)$

$$=(f(x)+g(x))+h(x)$$
$$=f(x)+(g(x)+h(x))$$
$$=f(x)+(g+h)(x)$$
$$=(f+(g+h))(x),\ \forall x\in[a,b]$$

$\therefore (f+g)+h=f+(g+h),\ \forall f,g,h\in V$

(iii) Let $\theta:[a,b]\to R$, $\theta(x)=0$, $\forall x\in[a,b]$.

Clearly $\theta\in V$

Now $(\theta+f)(x)=\theta(x)+f(x)$

$$=0+f(x)$$
$$=f(x)$$

$\therefore \theta+f=f$

Similarly, $f+\theta=f$

$\therefore f+\theta=f=\theta+f$.

This shows that θ is the additive identity in V.

(iv) For every $f \in V$, we define $-f$ by the rule

$$(-f)(x) = -f(x), \forall x \in [a,b]$$

Clearly, $(f + (-f))(x) = f(x) + (-f)(x)$

$$= f(x) - f(x)$$
$$= 0$$
$$= \theta(x), \quad \forall x \in [a,b]$$
$$\therefore f + (-f) = \theta$$

Similarly, $(-f) + f = \theta$

$$\therefore f + (-f) = \theta = (-f) + f$$

(v) $(f+g)(x) = f(x) + g(x)$

$$= g(x) + f(x)$$
$$= (g+f)(x), \forall x \in [a,b]$$
$$\therefore f + g = g + f$$

$\therefore$ V is an abelian group under addition.

II.Let $\alpha \in R$, $f \in V$, $x \in [a,b]$

$$(\alpha f)(x) = \alpha f(x) \in R$$

Since f is continuous, $\therefore \alpha f$ is also continous.

$$\therefore \alpha f \in V$$

III. (i) $(\alpha(f+g))(x) = \alpha(f+g)(x), \alpha \in R, f, g \in V$

$$= \alpha(f(x) + g(x)), x \in [a,b]$$
$$= \alpha f(x) + \alpha g(x)$$
$$= (\alpha f + \alpha g)(x), \quad \forall x \in [a,b]$$
$$\therefore \alpha(f+g) = \alpha f + \alpha g$$

(ii) $((\alpha + \beta)f)(x) = (\alpha + \beta)f(x)$

$$= \alpha f(x) + \beta f(x)$$
$$= (\alpha f)(x) + (\beta f)(x)$$
$$= (\alpha f + \beta f)(x) \quad , \forall x \in [a,b]$$
$$\therefore (\alpha + \beta)f = \alpha f + \beta f$$

(iii) $((\alpha\beta)f)(x) = (\alpha\beta)f(x)$

$$= \alpha(\beta f(x))$$
$$= \alpha(\beta f)(x), \quad \forall x \in [a,b]$$

$\therefore (\alpha\beta)f = \alpha(\beta f)$

(iv) $(1f)(x) = 1f(x)$

$= f(x), \forall x \in [a,b]$

$\therefore 1f = f$

$\therefore$ V is a vector space over R,i.e.,V is a real vector space.



CHECK YOUR PROGRESS 1

Q 1: Show that the field of real numbers R is a vector space over R.

Q 2: Show that the field of complex numbers C is a vector space over C.

Q 3: Show that the field of complex numbers C is a vector space over R. Is R is a vector space over C?

Q 4: Let V be the set of all $m \times n$ matrices over reals. Show that V is a vector space over R.

Q 5: Let $V = \{(x_1, x_2) : x_1, x_2 \text{ are reals}\}$, and $\alpha \in R$. Define addition and scalar multiplication in V as follows

$x + y = (x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$

$\alpha x = \alpha(x_1, x_2) = (\alpha x_1, x_2)$

where $x = (x_1, x_2)$, $y = (y_1, y_2) \in V$, $\alpha \in R$

Show that V is not a vector space.

11.4 ELEMENTARY PROPERTIES

Let V be a vector space over a field F.Let $\alpha, \beta \in F$, $x, y \in V$ .Then

(i) $\alpha 0 = 0$ (This"0" is the zero element of the Abelian group V)

(ii) $0x = 0$ (The "0" on the left is the zero element of the field F,and the"0" on the right is the zero element of V.)

(iii) if $\alpha x = 0$,then $\alpha = 0$ or $x = 0$

(iv) $(-\alpha)x = \alpha(-x) = -\alpha x$

(v) $\alpha(x - y) = \alpha x - \alpha y$

(vi) $(\alpha - \beta)x = \alpha x - \beta x$

Proof : (i) We have $0 + 0 = 0$

We note that this $0 \in V$

Now $\alpha 0 = \alpha(0 + 0)$

$= \alpha 0 + \alpha 0$

$\therefore \alpha 0 + (-\alpha 0) = \alpha 0 + \alpha 0 + (-\alpha 0)$

$\Rightarrow 0 = \alpha 0$

i.e. $\alpha 0 = 0$

(ii) We have $0 + 0 = 0$

We note that this $0 \in F$

Now $0x = (0 + 0)x$

$= 0x + 0x$

$\therefore 0x + (-0x) = 0x + 0x + (-0x)$

$\Rightarrow 0 = 0x$

i.e. $0x = 0$

(iii) Here $\alpha x = 0$

If $\alpha = 0$, there is nothing to prove.

Let $\alpha \neq 0$, α^{-1} exists.

Now $x = 1x$

$= (\alpha \alpha^{-1})x$

$= \alpha^{-1}(\alpha x)$

$= \alpha^{-1} 0$

$= 0$

(iv) We have $x + (-x) = 0$, the zero element of V

$\alpha + (-\alpha) = 0$, the zero element of F

Now, $\alpha 0 = \alpha(x + (-x))$

$\Rightarrow 0 = \alpha x + \alpha(-x)$

$\therefore (-\alpha x) + 0 = (-\alpha x) + \alpha x + \alpha(-x)$

$\Rightarrow -\alpha x = \alpha(-x)$

Again $0x = (\alpha + (-\alpha))x$

$\Rightarrow 0 = \alpha x + (-\alpha)x$

$(-\alpha x) + 0 = (-\alpha x) + \alpha x + (-\alpha)x$

$\Rightarrow -\alpha x = (-\alpha)x$

Thus, $(-\alpha)x = \alpha(-x) = -\alpha x$.

(v) We have $x - y = x + (-y)$

Also,we have $\alpha(-y) = -\alpha y$

Now $\alpha(x-y)=\alpha(x+(-y))$

$=\alpha x+\alpha(-y)$

$=\alpha x-\alpha y$

(vi) Proceed as above.

Example 4 : Let V be a vector space over the field F.Show that

$x+x=2x\,,\forall x\in V$

Solution : we have

$x+x=1x+1x$

$=(1+1)x$

$=2x\,.$



CHECK YOUR PROGRESS 2

Q 1: Let V be a vector space over the field F.Let $x,y\in V$ and $\alpha,\beta\in F$. Show that (i) if $\alpha x=\beta x$, Then $\alpha=\beta\,,x\neq 0$

(ii) if $\alpha x=\alpha y$, then $x=y\,,\alpha\neq 0$

(iii) if $\alpha x=0$, and $x\neq 0$, then $\alpha=0$

(iv) if $\alpha x=0$, and $\alpha\neq 0$, then $x=0$

(v) if $\alpha x=x$, then $\alpha=1$ or $x=0$.

11.5 SUBSPACE OF A VECTOR SPACE

Let V be a vector space over a field F.Let W be a nonempty subset of V.W is called a subspace of V if W itself is a vector space over F under the same addition and scalar multiplication in V.

Note: 1. V itself is a subspace of V.

2. The set $\{0\}$ consisting of the zero element of the additive group V is a vector space,called the null space. $\{0\}$ is a supspace of V.

Theorem : A non-empty subset W of a vector space V(F) is a subspace of V if and only if W is closed under addition and scalar multiplication.

Proof : Let W be a subspace of V(F).Then,by definition,W is closed under addition and scalar multiplication.

Conversely, let W be closed under addition and scalar multiplication.

Let $a,b\in W$

Now $1 \in F$

$\therefore -1 \in F$

Now $-1 \in F, b \in W$

$\therefore (-1)b \in W$ i.e. $-b \in W$

Thus, $a \in W, -b \in W$

$\therefore a - b \in W$

$\therefore$ W is a subgroup of the additive abelian group V.

All the other conditions for a vector space are satisfied in W, as they are satisfied in V.

$\therefore$ W is a vector space over F.

Theorem : A non-empty subset W of a vector space V(F) is a subspace of V if and only if $\alpha x + \beta y \in W$,for all $\alpha, \beta \in F; x, y \in W$.

Proof : Let W be a subspace of V.

Let $x, y \in W$, $\alpha, \beta \in F$

$\therefore \alpha x \in W$, $\beta y \in W$

$\therefore \alpha x + \beta y \in W$

Conversely, let W be a non-empty subset of V such that for all $\alpha, \beta \in F$; $x, y \in W$, $\alpha x + \beta y \in W$.

Now $1 \in F$

$\therefore 1x + 1y \in W$

i.e., $x + y \in W$

$\therefore$ W is closed under addition.

Again $\alpha \in F$, $0 \in F$

$\therefore \alpha x + 0y \in W$

i.e., $\alpha x \in W$

$\therefore$ W is closed under scalar multiplication.

$\therefore$ W is a subspace of V. (by previous theorem)

Example 5 : Let us consider the vector space $R^2(R)$.

Let $W = \{(a,0) : a \in R\}$

Clearly $W \subseteq R^2$,and $W \neq \phi$

Let $\alpha, \beta \in R$; $(a,0), (b,0) \in W$

$$\alpha(a,0) + \beta(b,0) = (\alpha a, 0) + (\beta a, 0)$$

$$= (\alpha a + \beta a, 0 + 0)$$

$$= (\alpha a + \beta a, 0) \in W$$

$\therefore$ W is a subspace of R^2.

Example 6 : Let us consider the vector space $R^3(R)$.

Let $W = \{(x_1, x_2, x_3) : x_1 + x_2 + x_3 = 0, x_1, x_2, x_3 \in R\}$

Clearly, $W \subseteq R^3, W \neq \phi$

Let $\alpha, \beta \in R$; $x = (x_1, x_2, x_3) \in W$, $y = (y_1, y_2, y_3) \in W$

$$\therefore x_1 + x_2 + x_3 = 0$$

$$y_1 + y_2 + y_3 = 0$$

Now, $\alpha x + \beta y = \alpha(x_1, x_2, x_3) + \beta(y_1, y_2, y_3)$

$$= (\alpha x_1, \alpha x_2, \alpha x_3) + (\beta y_1, \beta y_2, \beta y_3)$$

$$= (\alpha x_1 + \beta y_1, \alpha x_2 + \beta y_2, \beta y_3 + \alpha x_3)$$

Now, $(\alpha x_1 + \beta y_1) + (\alpha x_2 + \beta y_2) + (\beta y_3 + \alpha x_3)$

$$= \alpha(x_1 + x_2 + x_3) + \beta(y_1 + y_2 + y_3)$$

$$= \alpha 0 + \beta 0$$

$$= 0$$

$\therefore \alpha x + \beta y \in W$

$\therefore$ W is a subspace of V.

Theorem : Intersection of two subspaces of a vector space is a subspace.

Proof : Let V be a vector space over a field F.

Let W_1 and W_2 be two subspaces of V.

$$\therefore W_1 \neq \phi, W_2 \neq \phi$$

$\therefore W_1 \cap W_2 \neq \phi$, since at least the zero element 0 of W is in $W_1 \cap W$.

Let $\alpha, \beta \in F; x, y \in W_1 \cap W_2$

$x \in W_1 \cap W_2 \Rightarrow x \in W_1$ and $x \in W_2$

$y \in W_1 \cap W_2 \Rightarrow y \in W_1$ and $y \in W_2$.

Now $\alpha, \beta \in F$; $x, y \in W_1$ and W_1 is a subspace of V.

$$\therefore \alpha x + \beta y \in W_1$$

Again $\alpha, \beta \in F$; $x, y \in W_2$ and W_2 is a subspace of V.

$$\therefore \alpha x + \beta y \in W_2$$

Thus, $\alpha x + \beta y \in W_1$ and $\alpha x + \beta y \in W_2$

$$\therefore \alpha x + \beta y \in W_1 \cap W_2$$

$\therefore W_1 \cap W_2$ is a subspace of V.

Note : Union of two subspaces may not be a subspace.

We know R^3 is a vector space over R under componentwise addition and componentwise scalar multiplication.

Let $W_1 = \{(x,0,0) : x \in R\}$

$W_2 = \{(0, y,0) : x \in R\}$

Clearly, W_1 is a subspace of R^3, W_2 is a subspace of R^3.

Now $(5,0,0) \in W_1$, $(0,5,0) \in W_2$

But $(5,0,0)+(0,0,5) = (5,5,0) \notin W_1 \cup W_2$

i.e., $(5,0,0) \in W_1 \cup W_2$, $(0,5,0) \in W_1 \cup W_2$

but $(5,0,0)+(0,0,5) \notin W_1 \cup W_2$

$\therefore W_1 \cup W_2$ is not a subspace of R^3.

Theorem: Union of two subspaces is a subspace if and only if one of them is contained in the other.

Proof : Let V be a vector spae over a field F.

Let W_1, W_2 be two subspace of V.

Let $W_1 \subseteq W_2$ .Then $W_1 \cup W_2 = W_2$

$\because W_2$ is a subspace of V,

$\therefore W_1 \cup W_2$ is a subspace of V.

Conversely, let W_1, W_2 be a subspace of V such that $W_1 \cup W_2$ is also a subspace of V.

We are to prove that $W_1 \subseteq W_2$ or $W_2 \subseteq W_1$

If possible,let it not be the true.

$\therefore W_1 \not\subset W_2$ and $W_2 \not\subset W_1$

$\therefore$ there exists $x \in W_1$ such that $x \notin W_2$ .Also, there exists $y \in W_2$ such that $y \notin W_1$.

Now $x \in W_1 \Rightarrow x \in W_1 \cup W_2$

$y \in W_2 \Rightarrow y \in W_1 \cup W_2$

$\because W_1 \cup W_2$ is a subspace of V.

$\therefore x + y \in W_1 \cup W_2$

This $\Rightarrow x + y \in W_1$ or $x + y \in W_2$

Let $x + y \in W_1$

Now $-x \in W_1$ $(\because x \in W_1), x + y \in W_1$

$\therefore (-x) + x + y \in W_1$

$\Rightarrow (-x+x)+y \in W_1$

$\Rightarrow 0+y \in W_1$

$\Rightarrow y \in W_1$

which is a contradiction.

Similarly,let $x+y \in W_2$

Now $x+y \in W_2, -y \in W_2 \ (\because y \in W_2)$

$\therefore (x+y)+(-y) \in W_2$

$\Rightarrow x+(y+(-y)) \in W_2$

$\Rightarrow x+0 \in W_2$

$\Rightarrow x \in W_2,$

which is a contradiction.

So,our assumption is wrong.

$\therefore$ either $W_1 \subseteq W_2$ or $W_2 \subseteq W_1$.



CHECK YOUR PROGRESS 3

Q 1: Let $R^3(R)$ be the vector space under componentwise addition and componentwise scalar multiplication.

(i) Let $W=\{(a,2b,3c): a,b,c \in R\}$. Show that W is a subspace of R^3.

(ii) Let $W=\{(x,y,z): x-3y+4z=0, x,y,z \in R\}$. Show that W is a subspace of R^3.

(iii) Let $W=\{(x,y,z): x^2+y^2=z^2, x,y,z \in R\}$. Show that W is not a subspace of R^3.

Q 2: Let $R^n(R)$ be the vector space under componentwise addition and componentwise scalar multiplication.

Let $W=\{(x_1,x_2,\cdots,x_n): x_1+x_2+\cdots+x_n=1\}$.Show that W is not a subspace of R^n.

11.6 LINEAR DEPENDENCE AND INDEPENDENCE

Let V be a vector space over a field F. Vectors $x_1,x_2,x_3,\cdots,x_n \in V$ are said to be linearly dependent over F if there exist scalars

$\alpha_1, \alpha_2, \cdots, \alpha_n \in F$ (not all of them zero) such that $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$.

Thus,the vectors $x_1, x_2, x_3, \cdots, x_n \in V$ are linearly dependent if

$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$

$\Rightarrow$ at least one of $\alpha_1, \alpha_2, \cdots, \alpha_n$ is not zero.

If $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$

$\Rightarrow \alpha_1 = 0, \alpha_2 = 0, \cdots, \alpha_n = 0$;

the vectors $x_1, x_2, x_3, \cdots, x_n$ are linearly independent.

A finite set $\{x_1, x_2, x_3, \cdots, x_n\}$ is said to be linearly dependent or linearly independent according as its n elements are linearly dependent or linearly independent.

A subset W of V is called linearly independent if the elements of W are linearly independent .Otherwise it is said to be linearly dependent.

Note

1. Let $x \in V$,and $x \neq 0$

   Let $\alpha \in F$

   Now $\alpha x = 0$

   $\Rightarrow \alpha x = 0x$

   $\Rightarrow \alpha = 0$,[$\alpha x = \beta x \Rightarrow \alpha = \beta$, if $x \neq 0$]

$\therefore$ x is linearly independent i.e.a non-zero vector is always linearly independent.

2. We have $1.0 = 0$,but $1 \neq 0$,where 1 is the unity of F.

$\therefore$ zero vetor is always lineraly dependent.

3. A superset of a linearly dependent set of vectors is linearly dependent.

4. A subset of a linearly independent set of vectors is linearly independent.

Example 7 : Let us consider the vector space R^2 over R under componentwise addition and componentwise scalar multiplication.

Let us consider the vectors $e_1 = (1,0), e_2 = (0,1)$ in R^2.

Let $\alpha_1, \alpha_2 \in R$

Now, $\alpha_1 e_1 + \alpha_2 e_2 = 0$

$\Rightarrow \alpha_1(1,0) + \alpha_2(0,1) = (0,0)$

$\Rightarrow (\alpha_1, 0) + (0, \alpha_2) = (0,0)$

$\Rightarrow (\alpha_1, \alpha_2) = (0,0)$

$\Rightarrow \alpha_1 = 0, \alpha_2 = 0$

$\therefore$ the vectors $e_1=(1,0), e_2=(0,1)$ are linearly independent.

Example 8 : Let us consider the vector space R^3 over R under componentwise addition and componentwise scalar multiplication.

Let us consider the vectors $x=(1,2,-1), y=(2,2,1), z=(1,-2,3)$ in R^3.

Let $\alpha_1,\alpha_2,\alpha_3 \in R$

Now $\alpha_1 x+\alpha_2 y+\alpha_3 z=0$

$\Rightarrow \alpha_1(1,2,-1)+\alpha_2(2,2,1)+\alpha_3(1,-2,3)=(0,0,0)$

$\Rightarrow (\alpha_1,2\alpha_1,-\alpha_1)+(2\alpha_2,2\alpha_2,\alpha_2)+(\alpha_3,-2\alpha_3,3\alpha_3)=(0,0,0)$

$\Rightarrow (\alpha_1+2\alpha_2+\alpha_3, 2\alpha_1+2\alpha_2-2\alpha_3, -\alpha_1+\alpha_2+3\alpha_3)=(0,0,0)$

$\Rightarrow \alpha_1+2\alpha_2+\alpha_3=0$ ... (1)

$2\alpha_1+2\alpha_2-2\alpha_3=0$

i.e. $\alpha_1+\alpha_2-\alpha_3=0$ ... (2)

$-\alpha_1+\alpha_2+3\alpha_3=0$ ... (3)

Now $\begin{vmatrix} 1 & 2 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{vmatrix}$

$=1(1+1)-2(1-1)+1(1+1)$

$=4\neq 0$

$\therefore$ the only solution of the equations (1),(2),(3) is $\alpha_1=0,\alpha_2=0,\alpha_3=0$.

$\therefore$ the vectors $(1,2,-1),(2,2,1),(1,-2,3)$ are linearly independent.

Example 9: Let us consider the vector space $R^3(R)$.Let us consider the vectors $x=(1,1,2), y=(1,2,5), z=(5,3,4)$ in R^3.

Let $\alpha_1,\alpha_2,\alpha_3 \in R$

Now $\alpha_1 x+\alpha_2 y+\alpha_3 z=0$

$\Rightarrow \alpha_1(1,1,2)+\alpha_2(1,2,5)+\alpha_3(5,3,4)=(0,0,0)$

$\Rightarrow (\alpha_1,\alpha_1,2\alpha_1)+(\alpha_2,2\alpha_2,5\alpha_2)+(5\alpha_3,3\alpha_3,4\alpha_3)=(0,0,0)$

$\Rightarrow (\alpha_1+\alpha_2+5\alpha_3, \alpha_1+2\alpha_2+3\alpha_3, 2\alpha_1+5\alpha_2+4\alpha_3)=(0,0,0)$

$\Rightarrow \alpha_1+\alpha_2+5\alpha_3=0$ ... (1)

$\alpha_1+2\alpha_2+3\alpha_3=0$ ... (2)

$2\alpha_1+5\alpha_2+4\alpha_3=0$ ... (3)

Now $\begin{vmatrix} 1 & 1 & 5 \\ 1 & 2 & 3 \\ 2 & 5 & 4 \end{vmatrix}$

$=1\times(8-15)-1\times(4-6)+5\times(5-4)$

$= -7 + 2 + 5 = 0$

$\therefore$ the system of equations possesses non zero solution.

From (1) and (2)

$$\frac{\alpha_1}{3-10} = \frac{\alpha_2}{-(3-5)} = \frac{\alpha_3}{2-1}$$

$$\Rightarrow \frac{\alpha_1}{-7} = \frac{\alpha_2}{2} = \frac{\alpha_3}{1}$$

$\Rightarrow \alpha_1 = -7k, \alpha_2 = 2k, \alpha_3 = k, k \in R$

From (3), $2 \times (-7k) + 5 \times 2k + 4k = 0$

$\therefore$ $(-7k, 2k, k)$ satisfies (3)

Thus, $(-7,2,1)$ is a solution.

$\therefore$ $-7x + 2y + z = 0$

$\therefore$ the vectors $(1,1,2), (1,2,5), (5,3,4)$ are linearly dependent.

Example 10 : Let us consider the vector space R over Q.

We have $1, \sqrt{3} \in R$

Let $\alpha, \beta \in Q$ such that $1\alpha + \sqrt{3}\beta = 0$

If possible, let $\beta \neq 0$

$$\therefore \sqrt{3} = -\frac{\alpha}{\beta}$$

Now $\alpha \in Q, \beta \in Q$ $\therefore -\frac{\alpha}{\beta} \in Q$

$\therefore$ $\sqrt{3} \in Q$, which is a contradiction.

$\therefore$ $\beta = 0$

This $\Rightarrow \alpha = 0$

$\therefore$ $\{1, \sqrt{3}\}$ is linearly independent in R over Q.

Proposition : If two vectors of a vector space are linearly dependent,one of them is a scalar multiple of the other.

Proof : Let V be a vector space over a field F.

Let $x, y \in V$ such that x, y are linearly dependent.

Then there exist scalars α, β not both zero such that

$$\alpha x + \beta y = 0$$

Let $\alpha \neq 0, \therefore \alpha^{-1} \in F$

Now $\alpha x = -\beta y$

$\Rightarrow \alpha^{-1}(\alpha x) = \alpha^{-1}(-\beta y)$

$\Rightarrow (\alpha^{-1}\alpha)x = (-\alpha^{-1}\beta)y$

$\Rightarrow x = \delta y$,taking $-\alpha^{-1}\beta = \delta$

Thus, x is a scalar multiple of y .

Similarly,if $\beta \neq 0$,y is a scalar multiple of x .



CHECK YOUR PROGRESS 4

Q 1: Show that the vectors $(1,1,2),(1,2,5),(5,3,4)$ are linearly dependent in $R^3(R)$.

Q 2: Show that the vectors $(2,3,1),(2,1,3),(1,1,1)$ are linearly dependent in $R^3(R)$.

Q 3: Show that the vectors $(0,1,1),(1,0,1),(1,1,0)$ are linearly independent in $R^3(R)$.

Q 4: Show that the vectors $(1,2,-1),(2,2,1),(1,-2,3)$ are linearly independent in $R^3(R)$.

11.7 BASIS AND DIMENSION

Definition : Let V be a vector space over a field F.Let $x_1, x_2, x_3, \cdots, x_n \in V$. Any vector $x = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$;where $\alpha_1, \alpha_2, \cdots, \alpha_n \in F$ is called a linear combination of the vectors $x_1, x_2, x_3, \cdots, x_n$.

Definition : Let V be a vector space over a field F.A subset S of V is called a basis of V if

(i) any finite number of elements in S are linearly independent,

(ii) each vector in V is a linear combination of a finite number of elements of S.

Example 11 : Let us consider the vector space $R^2(R)$.Let us consider the subset $S = \{e_1, e_2\}$ of R^2 ,where $e_1 = (1,0), e_2 = (0,1)$

Let $\alpha_1, \alpha_2 \in R$ such that

$\alpha_1 e_1 + \alpha_2 e_2 = 0$

$\Rightarrow \alpha_1(1,0) + \alpha_2(0,1) = (0,0)$

$\Rightarrow (\alpha_1, 0) + (0, \alpha_2) = (0,0)$

$\Rightarrow (\alpha_1, \alpha_2) = (0,0)$

$\Rightarrow \alpha_1 = 0, \alpha_2 = 0$

$\therefore$ S is linearly independent.

Let $x = (x_1, x_2) \in R^2$

Now $x = (x_1, x_2)$

$= x_1(1,0) + x_2(0,1)$

$= x_1 e_1 + x_2 e_2$

Thus, each vector in R^2 is a linear combination of the elements of S.

$\therefore$ S is a basis of R^2 ,known as the standard basis.

Example 12 : $S = \{e_1, e_2, e_3\}$ is the standard basis of $R^3(R)$,where $e_1 = (1,0,0)$, $e_2 = (0,1,0)$, $e_3 = (0,0,1)$.

Example 13 : $S = \{e_1, e_2, \cdots, e_n\}$is the standard basis $R^n(R)$, where $e_1 = (1,0,0,\cdots,0)$, $e_2 = (0,1,0,\cdots,0)$, $\cdots, e_n = (0,0,0,\cdots,1)$.

Example 14 : Let us consider the vector space $R^3(R)$.

Let $T = \{u_1, u_2, u_3\}$be a subset of R^3 , where

$u_1 = (1,1,0), u_2 = (1,0,0), u_3 = (0,1,1)$.

Let $\alpha_1, \alpha_2, \alpha_3 \in R$ such that

$\alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 = 0$

$\Rightarrow \alpha_1(1,1,0) + \alpha_2(1,0,0) + \alpha_3(0,1,1) = (0,0,0)$

$\Rightarrow (\alpha_1, \alpha_1, 0) + (\alpha_2, 0, 0) + (0, \alpha_3, \alpha_3) = (0,0,0)$

$\Rightarrow (\alpha_1 + \alpha_2, \alpha_1 + \alpha_3, \alpha_3) = 0$

$\therefore \alpha_1 + \alpha_2 = 0$

$\alpha_1 + \alpha_3 = 0$

$\alpha_3 = 0$

$\therefore \alpha_1 = \alpha_2 = \alpha_3 = 0$

$\therefore$ T is linearly independent.

Let $x = (x_1, x_2, x_3) \in R^3$ such that

$x = \beta_1 u_1 + \beta_2 u_2 + \beta_3 u_3$, where $\beta_1, \beta_2, \beta_3 \in R$

$\Rightarrow (x_1, x_2, x_3) = \beta_1(1,1,0) + \beta_2(1,0,0) + \beta_3(0,1,1)$

$\Rightarrow (x_1, x_2, x_3) = (\beta_1, \beta_1, 0) + (\beta_2, 0, 0) + (0, \beta_3, \beta_3)$

$\Rightarrow (x_1, x_2, x_3) = (\beta_1 + \beta_2, \beta_1 + \beta_3, \beta_3)$

$\therefore \beta_1 + \beta_2 = x_1$

$\beta_1 + \beta_3 = x_2$

$\beta_3 = x_3$

$\therefore\ \beta_1 = x_2 - \beta_3 = x_2 - x_3$

$\beta_2 = x_1 - \beta_1 = x_1 - x_2 + x_3$

$\therefore\ (x_1, x_2, x_3) = (x_2 - x_3)(1,1,0) + (x_1 - x_2 + x_3)(1,0,0) + x_3(0,1,1)$

Thus, each vector in R^3 is a linear combination of the element of T.

$\therefore$ T is a basis of R^3.

Note : From Example 12 and Example 14,we see that a vector may have more than one basis.

Example 15 : Show that the set $\{(1,1,2),(1,2,5),(5,3,4)\}$ is not a basis of $R^3(R)$.

Solution : We have already proved that the set $\{(1,1,2),(1,2,5),(5,3,4)\}$ is linearly dependent. (Example 9)

$\therefore$ the given set is not a basis of R^3.

Theorem : Let V be a vector space over the field F. If $S = \{u_1, u_2, \cdots, u_n\}$ is a basis of V, then each element of V can be uniquely expressed as a linear combination of $u_1, u_2, \cdots, u_n$.

Proof : By definition of basis, we know that each element of V can be expressed as a linear combination of $u_1, u_2, \cdots, u_n$.

We show that the expression is unique.

Let $x \in V$

If possible, let

$x = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$

$x = \beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_n u_n$

where $\alpha_i \in F$, $\beta_i \in F$, $i = 1,2,\cdots,n.$

$\therefore\ \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n = \beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_n u_n$

$\Rightarrow (\alpha_1 - \beta_1)u_1 + (\alpha_2 - \beta_2)u_2 + \cdots + (\alpha_n - \beta_n)u_n = 0$

$\because\ \{u_1, u_2, \cdots, u_n\}$ is linearly independent,

$\therefore\ \alpha_1 - \beta_1 = 0, \alpha_2 - \beta_2 = 0, ..., \alpha_n - \beta_n = 0$

$\Rightarrow \alpha_1 = \beta_1, \alpha_2 = \beta_2, ..., \alpha_n = \beta_n$

Thus, the expression is unique.

Definition : Let V be a vector space over a field F.

If the number of elements in a basis of V is finite, then V is said to be a finite dimensional vector space.It is said to be a of finite dimension.Other vector spaces are said to be infinite dimensional.We note that any two bases of finite dimensional vector space have the same number of elements.

The number of elements in a basis of a vector space V is said to be the dimension of V.Generally it is denoted by dimV.THe null space is said to be of 0 dimension.

Example 16 : We know that the standard basis $\{(1,0),(0,1)\}$ of the vector space $R^2(R)$ has two elements.

$\therefore$ dim $R^2 = 2$

Example 17: Dimension of $R^3(R)$ is 3.

Example 16: Dimension of $R^n(R)$ is n.

Example 19 : Show that $\{1, i\}$ forms a basis of $C(R)$.What is the dimension of $C(R)$?

Solution : Let $\alpha, \beta \in R$ such that

$$1\alpha + i\beta = 0$$
$$\Rightarrow \alpha + i\beta = 0 + i0$$
$$\Rightarrow \alpha = 0, \beta = 0$$

$\therefore \{1, i\}$ is linearly independent.

Now $\alpha + i\beta \in C$

$$\alpha + i\beta = 1\alpha + i\beta$$

Thus, each vector in C is a linear combination of the elements of $\{1, i\}$.

$\therefore \{1, i\}$ is a basis.

Number of elements of $\{1, i\}$ is 2.

$\therefore$ dimension of $C(R)$ is 2.

Example 20 : If x, y are elements in a vector space $V(F)$,and $\alpha, \beta \in F$;Show that the set $\{x, y, \alpha x + \beta y\}$ is linearly dependent.

Solution : We have

$$(-\alpha)x + (-\beta)y + 1(\alpha x + \beta y) = 0$$

Hence $1 \neq 0$

$\therefore$ the set is linearly dependent.



11.8 LET US SUM UP

- Let V be an Abelian group under " + ". Let F be a field under "+, $\bullet$ ". For each element $\alpha \in F$, $x \in V$, we have $\alpha x \in V$, called scalar multiplication.

  Then V is said to be a vector space over the field F if the following conditions are satisfied.

  1. $\alpha(x+y)=\alpha x+\alpha y$
  2. $(\alpha+\beta)x=\alpha x+\beta x$
  3. $(\alpha\beta)x=\alpha(\beta x)$
  4. $1x=x$

  where $\alpha,\beta \in F$, $x, y \in V$ and 1 is the unit element of F.
- The set $\{0\}$ consisting of the zero element of the additive group V is a vector space,called the null space.
- Let V be a vector space over a field F.Let W be a nonempty subset of V.W is called a subspace of V if W itself is a vector space over F under the same addition and scalar multiplication in V.

  V itself is a subspace of V.

  $\{0\}$ is a supspace of V.
- Intersection of two subspaces of a vector space is a subspace, whereas union of two subspaces may not be a subspace.
- The vectors $x_1, x_2, x_3, \cdots, x_n$ in a vector space V over a field Fare linearly dependent over F if $\alpha_1 x_1+\alpha_2 x_2+\cdots+\alpha_n x_n=0$.

  $\Rightarrow$ at least one of $\alpha_1, \alpha_2, \cdots, \alpha_n$ is not zero.

  If $\alpha_1 x_1+\alpha_2 x_2+\cdots+\alpha_n x_n=0$

  $\Rightarrow \alpha_1=0, \alpha_2=0, \cdots, \alpha_n=0$;

  The vectors $x_1, x_2, x_3, \cdots, x_n$ are linearly independent.
- A non-zero vector is always linearly independent.
- Zero vector is always linearly dependent.

- Let V be a vector space over a field F.Let $x_1, x_2, x_3, \cdots, x_n \in V$.
  Any vector $x = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$;where $\alpha_1, \alpha_2, \cdots, \alpha_n \in F$ is called a linear combination of the vectors $x_1, x_2, x_3, \cdots, x_n$.
- Let V be a vector space over a field F.A subset S of V is called a basis of V if
  (i) any finite number of elements in S are linearly independent,
  (ii) each vector in V is a linear combination of a finite number of elements of S.
- The number of elements in a basis of a vector space V is said to be the dimension of V.Generally it is denoted by dimV.The null space is said to be of 0 dimension.



11.9 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS – 1

Ans to Q No 1: I. We know that R is an abelian additive group.

II. If $\alpha \in R, x \in R$, then $\alpha x \in R$.

III. (i). $\alpha(x+y) = \alpha x + \alpha y$

(ii). $(\alpha+\beta)x = \alpha x + \beta x$

(iii). $(\alpha\beta)x = \alpha(\beta x)$

(iv). $1x = x$

where $\alpha, \beta \in R$, $x, y \in R$ and 1 is the unit element of R.

$\therefore$ R is a vector space over R.

Ans to Q No 2: Left as an exercise.As above.

Ans to Q No 3: First part : Left as an exercise.

Second Part : R is not a vector space over C

$2+3i \in C$, $5 \in R$

But $(2+3i)5 \notin R$, i.e. R is not closed with repect to scalar multiplication.

Ans to Q No 4: I. We know that V be an Abelian group under matrix addition.

II.If $\alpha \in R, A \in V$,then $\alpha A \in V$.

III.(i). $\alpha(A+B)=\alpha A+\alpha B$

(ii). $(\alpha+\beta)A=\alpha A+\beta A$

(iii). $(\alpha\beta)A=\alpha(\beta A)$

(iv). $1A=A$

where $\alpha, \beta \in R$; $A, B \in V$,1 is the unity element of R.

$\therefore$ V is a vector space over R.

Ans to Q No 5 : Let $\alpha, \beta \in R$, $x=(x_1, x_2) \in V$

Now $(\alpha+\beta)x=(\alpha+\beta)(x_1, x_2)$

$=((\alpha+\beta)x_1, x_2)$

$=(\alpha x_1+\beta x_1, x_2)$

$\alpha x+\beta x=\alpha(x_1, x_2)+\beta(x_1, x_2)$

$=(\alpha x_1, x_2)+(\beta x_1, x_2)$

$=(\alpha x_1+\beta x_1, x_2+x_2)$

$=(\alpha x_1+\beta x_1, 2x_2)$

$\therefore (\alpha+\beta)x \neq \alpha x+\beta x$

$\therefore$ V is not a vector space over R.

CHECK YOUR PROGRESS – 2

Ans to Q No 1: (i) $\alpha x=\beta x$, $x \in V; \alpha, \beta \in F, x \neq 0$

$\Rightarrow \alpha x+(-\beta x)=\beta x+(-\beta x)$

$\Rightarrow \alpha x-\beta x=0$

$\Rightarrow (\alpha-\beta)x=0$

$\Rightarrow \alpha-\beta=0 \quad [\because x \neq 0, 0x=0]$

$\Rightarrow \alpha=\beta$

(ii) $\alpha x=\alpha y$, $x, y \in V; \alpha \in F, \alpha \neq 0$

$\Rightarrow \alpha x-\alpha y=0$

$\Rightarrow \alpha(x-y)=0$

$\Rightarrow x-y=0$ $[\because \alpha \neq 0, \alpha 0=0]$

$\Rightarrow x=y$

(iii) $\alpha x=0, x \neq 0$

$\Rightarrow \alpha x=0x$

$\Rightarrow \alpha=0$

(iv) $\alpha x = 0, \alpha \neq 0$

$\Rightarrow \alpha x = \alpha 0$

$\Rightarrow x = 0$

(v) $\alpha x = x$

$\Rightarrow \alpha x - x = 0$

$\Rightarrow \alpha x - 1x = 0$

$\Rightarrow (\alpha - 1)x = 0$

$\Rightarrow \alpha - 1 = 0$ or $x = 0$

$\Rightarrow \alpha = 1$ or $x = 0$

CHECK YOUR PROGRESS – 3

Ans to Q No 1: (i) Let $\alpha, \beta \in R$, and $x = (a_1, 2b_1, 3c_1) \in W$,

$y = (a_2, 2b_2, 3c_2) \in W$

Now $\alpha x + \beta y = \alpha(a_1, 2b_1, 3c_1) + \beta(a_2, 2b_2, 3c_2)$

$= (\alpha a_1, 2\alpha b_1, 3\alpha c_1) + (\beta a_2, 2\beta b_2, 3\beta c_2)$

$= (\alpha a_1 + \beta a_2, 2\alpha b_1 + 2\beta b_2, 3\alpha c_1 + 3\beta c_2)$

$= (\alpha a_1 + \beta a_2, 2(\alpha b_1 + \beta b_2), 3(\alpha c_1 + \beta c_2))$

$\in W$

$\therefore W$. is a subspace of R^3.

(ii) Left as an exercise.

(iii) Left as an exercise.

Ans to Q No 2: Let $\alpha, \beta \in R$

$x = (x_1, x_2, \cdots, x_n) \in W, y = (y_1, y_2, \cdots, y_n) \in W$

$\therefore x_1 + x_2 + \cdots + x_n = 1$

$y_1 + y_2 + \cdots + y_n = 1$

Now $\alpha x + \beta y$

$= \alpha(x_1, x_2, \cdots, x_n) + \beta(y_1, y_2, \cdots, y_n)$

$= (\alpha x_1, \alpha x_2, \cdots, \alpha x_n) + (\beta y_1, \beta y_2, \cdots, \beta y_n)$

$= (\alpha x_1 + \beta y_1, \alpha x_2 + \beta y_2, \cdots, \alpha x_n + \beta y_n)$

Now $(\alpha x_1 + \beta y_1) + (\alpha x_2 + \beta y_2) + \cdots + (\alpha x_n + \beta y_n)$

$= \alpha(x_1 + x_2 + \cdots + x_n) + \beta(y_1 + y_2 + \cdots + y_n)$

$= \alpha + \beta$

$\neq 0$, if $\alpha \neq 1-\beta$

$\therefore \alpha x + \beta y \notin W$, if $\alpha \neq 1-\beta$

$\therefore$ W is not a subspace of R^n.

CHECK YOUR PROGRESS – 4

1. Left as an exercise.
2. Left as an exercise.
3. Left as an exercise.
4. Left as an exercise.



11.10 FURTHER READINGS

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society.
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd. Hyderabad 500029.



11.11 MODEL QUESTION

Q 1: Prove that a field F is a vector space over any subfield K of F.

Q 2: Let $R^3(R)$ be the vector space under componentwise addition and componentwise scalar multiplication.

Let $\alpha_1, \alpha_2, \alpha_3$ be three fixed elements of R.

Define $W = \{(x_1, x_2, x_3) : \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = 0, x_1, x_2, x_3 \in R\}$

Show that W is a subspace of $R^3(R)$.

Q 3: Let $R^3(R)$ be the vector space under componentwise addition and componentwise scalar multiplication.

Let $W = \{(x_1, x_2, x_3) : x_2 + 4x_3 = 0, x_1, x_2, x_3 \in R\}$

Examine if W is a subspace of $R^3(R)$.

Q 4: Let R(R) be the vector space of real numbers.Let $x, y, z \in R$. Show that the set $\{x, y, z\}$ is linearly dependent if the set $\{x + ay + bz, y, z\}$ is linearly dependent.

[$\{x + ay + bz, y, z\}$ is linearly dependent,there exist scalar α, β, γ ,not all zero such that $\alpha(x + ay + bz) + \beta y + \gamma z = 0$

This $\Rightarrow \alpha x + (\alpha a + \beta) y + (\alpha b + \gamma) z = 0$

If $\alpha \neq 0$, then clearly $\{x, y, z\}$ is linearly dependent.

If $\alpha = 0$, then at least one of β, γ is not zero; When $\alpha = 0$; $\alpha a + \beta = \beta$, $\alpha b + \gamma = \gamma$.

$\therefore$ at least one of $\alpha a + \beta$, $\alpha b + \gamma$ is not zero.

$\therefore$ the set $\{x, y, z\}$ is linearly dependent.

Q 5: Consider the vector space $R^3(R)$ under componentwise addition and componentwise scalar multiplication.

Examine if the set $\{(1,2,1), (2,1,0), (1,-1,2)\}$ is a basis of $R^3(R)$.

Q 6: Consider the vector space $R^4(R)$ under componentwise addition and componentwise scalar multiplication.

Show that $\{e_1, e_2, e_3, e_4\}$ is a basis of $R^4(R)$, where $e_1 = (1,0,0,0)$, $e_2 = (0,1,0,0)$, $e_3 = (0,0,1,0)$, $e_4 = (0,0,0,1)$.

*** ***** ***

UNIT 12 : COMBINATORICS

UNIT STRUCTURE

12.1 Learning Objectives

12.2 Introduction

12.3 The Rule of Sum

12.4 The Rule of product

12.5 Permutation

12.6 Combination

12.7 Let Us Sum Up

12.8 Answers To Check Your Progress

12.9 Further Readings

12.10 Model Questions

12.1 LEARNING OBJECTIVES

After going through this unit, you will able to know

- the rule of sum
- the rule of product
- permutation
- combination

12.2 INTRODUCTION

Combinatorics is an important branch of discrete mathematics. It deals with counting the number of ways of arranging or selecting objects from a finite collection under specified rules, i.e. it deals with problems of permutation and combinations. Combinatorics is widely applied in computer science.

12.3 THE RULE OF SUM

If there are n_1 ways to do a work A and distinct from them, n_2 ways to do work B,then the number of ways to do A or B is n_1+n_2. Here the two works cannot be done at the same time.

Note : The rule can be extended to any finite number of works. Thus, if r works can be done in n_1, n_2, ...,n_r ways and if they cannot be done simultaneously, then any one of the r works can be performed in $n_1+n_2+n_3$ . . . . .+ n_r ways.

Example 1 : There are 26 boys and 28 girls in a class. Find the number of ways of selecting one student as class representative.

Solution : One boy can be selected in 26 ways (we can select any one of these 26 boys). One girl can be selected in 28 ways.

$\therefore$ One student (a boy or a girl, not both of them) can be selected in 26+28 i.e. 54 ways.

Example 2 : There are 30 mathematics books and 25 science books in a library. In how many ways a mathematics book or a science book can be selected ?

Solution : We are to select one book, a mathematics book or a science book.

One mathematics book can be selected in 30 ways. One science book can be selected in 25 ways.

$\therefore$ a mathematics book or a science book can be selected in 30+25 i.e. 55 ways.

Example 3 : In how many ways a heart or a club can be selected from a pack of cards ?

Solution : A pack of cards contains 52 cards out of which there are 13 hearts, 13 diamonds, 13 clubs, 13 spades.

$\therefore$ One heart can be selected in 13 ways, one club can be selected in 13 ways.

$\therefore$ a heart or a club can be selected in 13+13 i.e, 26 ways.

12.4 THE RULE OF PRODUCT (OR SEQUENTIAL RULE)

If a work can be done in two successive steps, and the first step can be done in n_1 ways, the second step can be done in n_2 ways, then the work can be done in $n_1 \times n_2$ ways.

Note : The rule can be extended to any finite number of works. Thus, if a work can be done in r successive steps, and the first step can be done in n_1

ways, the second step can be done in n_2 ways, and in this way, the r th step can be done in n_r ways, then the work can be done in $n_1 \times n_2 \times \ldots\ldots\ldots \times n_r$ ways.

Example 4 : There are 25 boys and 20 girls in a class. A teacher wants to select one boy and one girl. In how many ways can this be done ?

Solution : One boy can be selected in 25 ways. One girl can be selected in 20 ways. Thus, the first step (i.e. to select one boy) can be done in 25 ways, the second step (i.e. to select one girl) can be done in 20 ways.

$\therefore$ One boy and one girl can be selected in 25×20 i.e. 500 ways.

Example 5 : What is the number of two-digit odd positive integers ?

Solution : Ones place can be filled up in 5 ways (any one of the five digits 1, 3, 5, 7, 9). Tens place can be filled up in 9 ways (any one of the nine digits 1, 2, 3, 4, 5, 6, 7, 8, 9). Thus, the first step can be done in 5 ways, the second step can be done in 9 ways.

$\therefore$ the work can be done in 5×9 i.e. 45 ways.

$\therefore$ the number of two odd-digit positive integers = 45



CHECK YOUR PROGRESS 1

Q 1: One man or a woman is to be selected from 24 men and 12 women. In how many ways can this be done ?

Q 2: There are 24 boys and 12 girls in a class. A teacher wants to select one boy and one girl. In how many ways can this be done ?

Q 3: Find the number of two-digit even positive integers.

Q 4: Find the number of three-digit odd positive integers.

Q 5: Find the number of three-digit even positive integers.

Q 6: Find the number of four-digit odd positive integers.

Q 7: Find the number of four-digit even positive integers.

Q 8: There are 40 mathematics books and 28 science books in a library. In how many ways one mathematics book or one science book can be selected ?

Q 9: There are 40 mathematics books and 28 science books in a library. In how many ways one mathematics book and one science book can be selected ?

Q 10: A big hall has 12 doors. In how many ways can a person enter the hall by one door and come out by a different door ?

Q 11: There are 15 buses plying between Guwahati and Dibrugarh. In how many ways can a man go from Guwahati to Dibrugarh and return by a different bus ?

Q 12: In how many ways can 7 students stand in a queue ?

Q 13: A man has six letters and there are three latter boxes. In how many ways can he post the letters ?

Q 14: In how many ways can three prizes be distributed among six students, if each of the students is eligible for each of the prizes ?

Q 15: Find the number of license plates that can be made where each plate contains two distinct English letters followed by four distinct digits.

Q 16: In how many ways a condidate can answer all the questions of a true-false test consisting of 10 question ?

Q 17: How many functions are there from a set with 5 elements to a set with 7 elements ?

Q 18: How many functions are there from a set with 7 elements to a set with 5 elements ?

Q 19: How many one-one functions are there from a set with 5 elements to a set with 7 elements ?

Q 20: How many one-one functions are there from a set with m elements to a set with n elements ?

Q 21: Find the number of seven-character palindromes that can be formed using the letters of the English alphabet such that no letter appears more than twice in each of them.

12.5 PERMUTATION

Let there be a set containing n distinct elements. An ordered arrangement of r elements of the set is called a permutation (or an r-permutation of n elements), $r \leq n$.

Symbolically it is denoted by ${}^nP_r$, or P(n, r), or $P(n_r)$.

Theorem : (Number of r-permutations without repetition) The number of r-permutations of n distinct objects is

P(n, r) = n(n-1) n(-2) . . . . . (n-r+1)

$$= \frac{n!}{(n-r)!},\ r \leq n$$

Proof : The first object can be closen in n different ways. So, we are left with (n-1) objects. Therefore, the second object can be chosen in (n-1) ways. Similarly, the third object can be chosen in (n-2) ways. In this way, the last object, i.e. the rth object can be chosen in (n-r+1) ways .Consequently, by the product rule, there are n(n-1)(n-2) . . . . (n-r+1) way of ordered arrangment Thus,

P(n, r) = n(n-1)(n-2) . . . . . (n-r+1)

$$= \frac{n(n-1)(n-2)\ .....(n-r+1)(n-r)(n-r-1).....3.2.1}{(n-r)(n-r-1)....\ 3.2.1}$$

$$= \frac{n!}{(n-r)!}$$

Note : $P(n,n) = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!,\ 0!=1$

Example 6: Find the value of n if P(n, 4) = 360

Solution : P (n, 4) = 360

or, $\frac{n!}{(n-4)!} = 360$

or, $\frac{n(n-1)(n-2)(4-3)(n-4)!}{(n-4)!} = 360$

or, n(n-1)(n-2)(n-3) = 6 x 5 x 4 x 3

$\therefore$ n = 6

Note : Left hand side is the product of 4 consecutive positive integers.

Therefore, the right hand side has also been expressed as the product of 4 consecutive positive integers.

Example 7 : How many four-digit numbers can be formed from the six digits 1, 2, 3, 5, 7, 8, if repetitions of digits are not allowed ?

Solution : The number of 4 digit numbers.

= the number of 4-permutations of 6 objects (digits)

= P (6, 4)

$= \frac{6!}{(6-4)!} = \frac{6!}{2!}$ = 6 x 5 x 4 x 3 = 360

Example 8: In how many ways can 10 different examination answer scripts be arranged so that the best and the worst always come together ?

Solution : The best and the worst come together. So, we can consider the best script and the worst script as a single script. Thus, we can consider 10 objects to be '9' objects. So, these '9' objects can be arranged in ${}^{9}P_{9}$ i.e. 9! ways.

Again, the best script and the worst script can be arranged among themselves in 2! ways.

$\therefore$ the reqiored number of ways

= 9! $\times$ 2!

= 725760.



CHECK YOUR PROGRESS 2

Q 1: Three persons enter a railway carriage, where there are 6 vacant seats. In how many ways can they seat themselves ?

Q 2: A gentleman has 6 friends to invite. In how many ways can he send invitation cards to them, if he has three bearers to carry the cards ?

Q 3: There are 20 candidates in an examination for awarding 5 prizes. In how many ways can the prizes be distributed, each candidate being eligible for one prize ?

Q 4: How many numbers lying between 100 and 1000 can be formed with the digits 1, 2, 3, 4, 5 if the digits in the same

number are not repeated ? Fund also the number of numbers lying between 100 and 10,000.

Q 5: How many four-digits even numbers cab be formed from the digits 1, 2, 3, 5, 7, 8 if repetition of digits are not allowed ?

Q 6: How many four-digit odd numbers can be formed from the digits 1, 2, 3, 5, 7, 8 if repetition of digits are not allowed ?

Q 7: How many four-digit numbers divigible by 5 can be formed from the digits 1, 2, 3, 5, 7, 8 if repetition of digits are not allowed ?

Q 8: In how many ways can 10 different examination answer scripts be arranged so that the best and the worst never come together ?

Q 9: Mr X has 4 mathematics books, 3 statistics book and 5 economics books. In how many ways can he arrange them on a shelf of books if books of each subject are placed together, and in the following order : mathematics, statistics, economics ?

Q 10: Find the number of ways in which letters of the word TRIANGLE can be arranged among themselves, if each arrangement begins with T and ends with E.

12.6 COMBINATION

Let there be a set containing n distinct elements. An unordered selection of r elements of the set is called a combination (or an r-combination of n elements), $r \leq n$.

Symblically it is denoted by ${}^{n}C_{r}$, or C(n, r), or $C(n_{r})$

Theorem : (Number of r-combinations without repetition) The number of r-combinations of n distinct objects is

$$C(n, r) = \frac{P(n, r)}{n!} = \frac{n!}{r!(n-r)!}, \quad r \leq n$$

Proof : By r-combination we mean an unerdered selection of r-objects from n distinct objects. Each r-combination contains r objects. These r objects can be ananged among themseleves in ${}^{r}P_{r}$, i.e., r! ways.

Therefore, each r-combination yields r! permutations.

$\therefore$ C(n, r) combinations will yoeld C(n, r) r! permutations.

We know that the number of r-permutations of n distinct objects is given by P(n, r)

$\therefore$ C (n, r) r ! = P (n, r)

or, C(n, r) = $\frac{P(n, r)}{r!}$

$= \frac{n!}{r!(n-r)!}$

Note : $C(n, n) = \frac{n!}{n!(n-n)!} = 1,\ 0.! = 1$

Theorem : C(n, r) = C(n, n-r), $r \leq n$

Proof : If r objects are chosen from n objects, then (n-r) objects are left.

Thus, selection of r objects from n objects is the same as leaving (n-r) objects.

Thus, to each r-combination there corresponds an (n-r) combination.

$\therefore$ C(n, r) = C(n, n-r)

Theorem : (Pascal's Identity)

C(n+1, r) = C(n, r) + C(n, r-1), $r \leq n$

Proof : Let us counsider a finite set A having (n+1) elements.

Let B be a subset of A, and let the number of elements of A be n.

Let $p \in A$ such that $p \notin B$

Clearly $A = B \cup \{p\}$

Every r-element subset of A is either an r-element subset of B or the union of an (r-1) element subset of B and the singleton set {p}.

In the first case, the number of subsets is C(n, r); whereas in the second case, the number of subsets is C(n, r-1).

$\therefore$ the total number of r-element subsets of A is C(n, r) + C(n, r-1).

But we know that the total number of r-element subsets of A is C(n+1, r).

$\therefore$ C(n+1, r) = C(n, r) + C(n, r-1).

Note : Blaise pascal was a famous french mathematician of the seventeenth century.

Example 9 : In how many ways can a committee of 6 gentlemen and 3 ladies be formed out of 9 gentlemen and 6 ladies?

Solution : 6 gentlemen can be selected from 9 gentlement in ${}^9C_6$ ways. 3 ladies can be selected from 6 ladies can be selected in ${}^6C_3$ ways.

$\therefore$ by the product rule, the number of committees = ${}^9C_6 \times {}^6C_3$

$$= \frac{9!}{6!\ 3!} \times \frac{6!}{3!\ 3!}$$

$$= \frac{9\times 8\times 7}{3\times 2\times 1} \times \frac{6\times 5\times 4}{3\times 2\times 1}$$

$= 3\times 4\times 7\times 5\times 4$

$= 1680$

Example 10 : A question paper contains 3 different sections A, B and C containing 4, 5 and 6 questions respectively. In how many ways a caudidate can make a selection of 7 questions, selecting at least 2 questions from each sections ?

Solution : There are three possibilities.

I 2 questions from A, 2 from B, 3 from C

II 2 from A, 3 from B, 2 from C

III 3 from A, 2 from B, 2 from C

The number of ways in I

$= {}^4C_2 \times {}^5C_2 \times {}^6C_3 = 6\times 10\times 20 = 1200$

The number of ways in II

${}^4C_2 \times {}^5C_3 \times {}^6C_2 = 6\times 10\times 15 = 900$

The number of ways in III

${}^4C_3 \times {}^5C_2 \times {}^6C_2 = 4\times 10\times 20 = 800$

$\therefore$ the required number of ways

$= 1200 + 900 + 800$

$= 2900$



CHECK YOUR PROGRESS 3

Q 1: There are 6 men and 7 women working in an office. In how many ways can a committee of 3 men and 4 women be selected ?

Q 2: There are 6 men and 7 women working in an office. In how many ways can a committee of 4 persons which has at least one woman be selected ?

Q 3: There are 6 men and 7 women working in an office. In how many ways can a committee of 4 persons which has at most one man be selected ?

Q 4: From 8 gentlemen and 4 ladies, a team of 5 is to be formed. In how many ways can this be done so as to include at least one lady?

Q 5: A man has 7 friends, 4 of them are ladies and 3 men. His wife has also 7 friends, 3 of them are ladies and 4 men. In how many ways can they invite a dinner party of 3 ladies and 3 men so that there are 3 of man's friends and 3 of wife's friends ?



12.7 LET US SUM UP

- If there are n_1 ways to do a work A and distinct from them, n_2 ways to do another work B, then the number of ways to do A or B is n_1+n_2. Here the two works cannot be done at the same time. This is known as the rule of sum.
- If a work can be done in two successive steps, and the first step can be done in n_1 ways, the second step can be done in n_2 ways, then the work can be done in $n_1 \times n_2$ ways, This is known as the rule of product.
- Let there be a set containing n distinct elements. An ordered arrangement of r elements of the set is called an r-permutation of n elements, $r \leq n$. An unordered selection of r elements of the set is called an r-combination of n elements, $r \leq n$.
- The number of r-permutations of n distinct objects is
  P(n, r) = n(n-1)(n-2) . . . . (n-r+1)

$$= \frac{n!}{(n-r)!},\ r \le n$$

- The number of r-combinations of n distinct objects is

$$C(n, r) = \frac{P(n, r)}{n!} = \frac{n!}{r!(n-r)!},\ r \le n$$

- C(n, r) = C(n, n-r), $r \le n$
- C(n+1, r) = C(n, r) + C(n, r-1)



12.8 ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress 1

Ans to Q No 1: One man can be selected in 24 ways,

One woman can be selected in 12 ways.

$\therefore$ One woman or one woman can be selected in 24+12 i. e. 36 ways.

Ans to Q No 2: One boy can be selected in 24 ways.

One girl can be selected in 12 ways.

$\therefore$ One boy and one girl can be selected in 24×12 i.e. 288 ways.

Ans to Q No 3: Ones place can be filled up in 5 ways (any one of the digits 0, 2, 4, 6, 8).

Tens place can be filled up in 9 ways (any one of the digits 1, 2, 3, 4, 5, 6, 7, 8, 9).

$\therefore$ the required number of numbers

$= 5 \times 9 = 45$

Ans to Q No 4: Ones place can be filled up in 5 ways (any one of the digits 1, 3, 5, 7, 9).

Tens place can be filled up in 10 ways (any one of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9)

Hundreds place can be filled up in 9 ways (any one of the digits 1, 2, 3, 4, 5, 6, 7, 8, 9).

$\therefore$ the required number of numbers = $5 \times 10 \times 9 = 450$

Ans to Q No 5: Ones place can be filled up in 5 ways (any one of the digits 0, 2, 4, 6, 8).

Tens place can be filled up in 10 ways. (any one of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9).

Hundreds place can be filled up in 9 ways (any one of the digits 1, 2, 3, 4, 5, 6, 7, 8, 9).

$\therefore$ the required number of numbers

$= 5 \times 10 \times 9 = 450$

Ans to Q No 6: Do yourself. Ans 4500

Ans to Q No 7: Do yourself. Ans 4500

Ans to Q No 8: One mathematies book or one science book can be selected in 40+28 i.e 69 ways.

Ans to Q No 9: One mathematies book and one science book can be selected in 40×28 i.e. 1120 ways.

Ans to Q No 10: A person can enter the hall in 12 ways, i.e, the first step can be performed in 12 ways. the person can come out from the hall in 11 ways, i.e., the second step can be performed in 11 ways.

$\therefore$ the required number of ways.

$= 12 \times 11 = 132$

Ans to Q No 11: Do yourself. Ans 210

Ans to Q No 12: Do yourself. Ans 5040

Ans to Q No 13: Do yourself. Ans $3^6 = 729$

Ans to Q No 14: Do yourself. Ans $6^3 = 216$

Ans to Q No 15: First letter can be filled up in 26 ways.

Second letter can be filled up in 25 ways.

First digit can be filled up in 10 ways.

Second digit can be filled up in 9 ways.

Third digit can be filled up in 8 ways.

Fourth digit can be filled up in 7 ways.

$\therefore$ the required number of ways

$= 26 \times 25 \times 10 \times 9 \times 8 \times 7$

Ans to Q No 16: First question can be answered in 2 ways (either true of

false).

Similarly, each of the questions can be answered in 2 ways.

$= 2\times2\times2\times2\times2\times2\times2\times2\times2\times2$

$= 2^{10} = 1024$

Ans to Q No 17: Number of elements in the domain = 5

Number of elements in the codomain = 7

First element can be associated in 7 ways.

Similarly each of the elements of the domain can be associated in 7 ways.

$\therefore$ the required number of functions

$= 7\times7\times7\times7\times7 = 7^5$

Ans to Q No 18: Number of elements in the domain = 7

Number of elements in the codomain = 5

Each of the elements of the domain can be associated in 5 ways.

$\therefore$ the required number of functions

$= 5\times5\times5\times5\times5\times5\times5 = 5^7$

Ans to Q No 19: Number of elements in the domain = 5

Number of elements in the codomain = 7

First element can be associated in 7 ways

Second element can be associated in 6 ways

Third element can be associated in 5 ways

Fourth element can be associated in 4 ways

Fifth element can be associated in 3 ways

$\therefore$ the required number of one-one functions

$= 7\times6\times5\times4\times3 = 2520$

Ans to Q No 20: We note that ; if m > n, there cannot be one-one function from the first set to the second set.

$\therefore m \le n$

Now, 1st element can be associated in n ways

2nd element can be associated in (n-1) ways

3rd element can be associated in (n-2) ways.

In this way, mth element can be associated in (n-m+1) ways.

$\therefore$ the required number of one-one functions.

= n(n-1)(n-2) . . . . (n-m+1)

Ans to Q No 21: [Dictionary meaning of the word palindrome is given below.

'A word, phrase, number or any other sequence of units which has the property of reading the same forwards as it does backwards, character for character, sometimes disregarding punctuation, capitalization and diacritics.']

The required number of palindromes

$= 26 \times 25 \times 24 \times 23$

= 358800

Check Your Progress 2

Ans to Q No 1: Number of ways $= {}^{6}P_3 = \frac{6!}{(6-3)!} = \frac{6!}{3!} = \frac{6 \times 5 \times 4 \times 3!}{3!}$

= 120

Ans to Q No 2: Number of ways = $3 \times 3 \times 3 \times 3 \times 3 \times 3 = 729$

Ans to Q No 3: Number of ways $= {}^{20}P_5 = \frac{20!}{(20-5)!}$

$= \frac{20!}{15!} = \frac{20 \times 19 \times 18 \times 17 \times 16 \times 15!}{15!}$

= 1860480

Ans to Q No 4: Do yourself. Ans 60,180

Ans to Q No 5: Ones place can be filled up in 2 ways (one of the digits 2, 8). The other three places can be filled up in ${}^{5}P_3$ ways.

$\therefore$ the required number of numbers

$= 2 \times {}^{5}P_3 = 2 \times \frac{5!}{(5-3)!} = 2 \times \frac{5!}{2!} = 2 \times \frac{5 \times 4 \times 3 \times 2!}{2!}$

= 120

Ans to Q No 6: Ones place can be filled up in 4 ways (one of the digits 1, 3, 5, 7). The other three places can be filled up in ${}^{5}P_3$ ways.

$\therefore$ the required number of numbers

$= 4 \times {}^{5}P_3 = 4 \times 5 \times 4 \times 3 = 240$

Ans to Q No 7: Ones place can be filled up in 1 way (5). The other three places can be filled up in ${}^{5}P_3$ ways.

$\therefore$ the required number of numbers

$= 1 \times {}^5P_3 = 1 \times 5 \times 4 \times 3 = 60$

Ans to Q No 8: If there is no restriction, 10 answer scripts can be arranged among themselves in ${}^{10}P_{10}$ i.e. 10! ways.

Again, we know that if the best and the worst scripts come together, the number of arrangements $= 9! \times 2!$

$= 725760$ (Example 8)

$\therefore$ if the best and the worst do not come together, the number of arrangements

$= 10! - 2 \times 9!$

$= 3628809 - 725760$

$= 2903040$

Ans to Q No 9: Number of ways

$= 4! \times 3! \times 5!$

$= 4 \times 3 \times 2 \times 1 \times 3 \times 2 \times 1 \times 5 \times 4 \times 3 \times 2 \times 1$

$= 17280$

Ans to Q No 10: Each arrangement begins with T, and ends with E. So, we are left with six letters R. I. A, N, G, L.

These six letters can be arranged among themselves in ${}^6P_6$ ways, i.e. 6! ways, i.e., $6 \times 5 \times 4 \times 3 \times 2 \times 1$ ways, i.e. 729 ways.

$\therefore$ the number of ways = 720

Check Your Progress 3

Ans to Q No 1: 3 men can be selected from 6 men in ${}^6C_3$ ways.

4 women can be selected from 7 women in ${}^7C_4$.

$\therefore$ the required number of ways

$$= {}^6C_3 \times {}^7C_4 = \frac{6!}{3!\,3!} \times \frac{7!}{4!\,3!} = \frac{6 \times 5 \times 4}{3 \times 2 \times 1} \times \frac{7 \times 6 \times 5}{3 \times 2 \times 1}$$

$= 20 \times 35 = 700$

Ans to Q No 2: At least one woman is to be selected. Therefore number of women may be 1, or 2 or 3 or 4. So we have the following possibilities

Men (6)	Women (7)
3	1
2	2

1	3
0	4

$\therefore$ the required number of ways

$= {}^6C_3 \times {}^7C_1 + {}^6C_2 \times {}^7C_2 + {}^6C_1 \times {}^7C_3 + {}^6C_0 \times {}^7C_4$

$= 20 \times 7 + 15 \times 21 + 6 \times 35 + 1 \times 35$

$= 140 + 315 + 210 + 35$

$= 700$

Ans to Q No 3: At most one man is to be selected. Therefore number of men may be 0, or 1. So, we have the following possibilities

Men (6)	Women (7)
0	4
1	3

$\therefore$ the required number of ways

$= {}^6C_0 \times {}^7C_4 + {}^6C_1 \times {}^7C_3 = 1 \times 35 + 6 \times 35 = 35 + 210 = 245$

Ans to Q No 4: Do yourself. Ans 736

Ans to Q No 5: We have the following possibilities.

Man		Wife	
Men (3)	Ladies (4)	Men (4)	Ladies (3)
3	0	0	3
2	1	1	2
1	2	2	1
0	3	3	0

$\therefore$ the required number of ways

$= ({}^3C_3 \times {}^4C_0 \times {}^4C_0 \times {}^3C_3) + ({}^3C_2 \times {}^4C_1 \times {}^4C_1 \times {}^3C_2) + ({}^3C_1 \times {}^4C_2 \times {}^4C_2 \times {}^3C_1)$

$+ \quad ({}^3C_0 \times {}^4C_3 \times {}^4C_3 \times {}^3C_0)$

$=$ 485, after simplification.



12.9 FURTHER READINGS

1) *Discrete Mathematical Structures with Application to Computer Science.* J.P Tremblay & R. Manohar.

2) *Discrete Structures and Graph Theory,* G. S. S. Bhishma Rao.



12.10 MODEL QUESTIONS

Q 1: Write down the sum rule for counting.

Q 2: Write down the product rule for countting

Q 3: Prove using combinational argument that

C(2n, 2) = 2 C (n, 2) + n^2

Q 4: Prove, using combinational argument, that

$C(n+m,r)=\sum_{i=0}^{r} C(m,r-i)C(n,i)$ for integers $n \geq r \geq 0$, and $m \geq r \geq 0$.

Q 5: Two distinguishable dice are rolled. In how many ways can we get a sum of 7 or 9 ?

Q 6: In how many way can we draw a king or a queen from a pack of cards ?

Q 7: A license plate contains two English letters, followed by two digits, followed by two English letters, followed by four digits. How many license plates can be made if repetition of letters and digits are allowed?

Q 8: There are 10 married couple in a group. Find the number of ways of selecting a woman and a man who is not her husband from this group.

Q 9: From 8 boys and 6 girls a team of 8 players is to be forwed. In how many ways can the team be formed so that exactly 3 girls are included excluding a paiticular girl and including a particular boy ?

Q 10: Find the number of one-one functions from a set with n elements to itself.

*** ***** ***

Unit 13: MATHEMATICAL LOGIC

UNIT STRUCTURE

13.1 Learning Objectives

13.2 Introduction

13.3 Definition of Statements

13.3.1 Examples of Statements

13.4 Logical Connectives

13.4.1 Negation

13.4.2 Conjunction

13.4.3 Disjunction

13.4.5 Conditional

13.4.6 Biconditional

13.5 Let Us Sum Up

13.6 Answers to Check Your Progress

13.7 Further Reading

13.8 Model Questions

13.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- define statements and examples of statements
- define truth tables about different statements
- know about negation of statements
- know about conjuction, disjunction, conditional and bi-conditional of two statements

13.2 INTRODUCTION

Mathematical logic is the discipline that deal with the methods of reasoning. As all of us know that the main asset that makes humans far more superior than other species is the ability of reasoning. Logic provides rules and techniques for determining whether a given argument or mathematical proof or conclusion in a scientific theory is valid or not. Logic

is concerned with studying arguments and conclusions. Logic is used in mathematics to prove theories and to draw conclusions from experiments in physical science in our every day life to solve many types of problem. Logic is used in computer science to verify the correctness of programs. The rules of logic or techniques of logic are called rules of inference because the main aim of logic is to draw conclusions inferences from given set of hypothesis. In this unit, we will introduce you to the definition and examples of statements, truth table of different statements. We will allso discuss about the logical connectives. Moreover, we will discuss about the converse, opposite and contrapositive of statements.

13.3 DEFINITION OF STATEMENTS

In logic we communicate our ideas or thoughts with the help of sentences in a particular language. The following types of sentences are normally used in our everyday communication.

Assertive sentence : A sentence that makes an assertion is called an assertive sentence or declerative sentence.

For example, " Mars supports life ".is an assertive or a declerative sentence

Imperative sentence : A sentence that expresses a request or a command is called an imperative sentence .

For example, "please bring me a cup of tea." is an imperative sentence.

Exclamatory sentence : A sentence that express some strong feeling is called an exclamatory sentence.

For example, "How big is the whale fish !." is an exclamatory sentence .

Interrogative sentence : A sentence that asks some questions is called an interrogative sentence.

For example, "What is your age ? "is an interrogative sentence .

STATEMENT : *A sentence or proposition is an assertive (or decleartive) sentence which is either true or false but not both. A sentence cannot both true and false at the same time .*

13.3.1 Examples of Statements

IIIUSTRATION 1 : Consider the following sentences :

i) Washington D .C is not in America.

ii) Every rectangle is a square.

iii) The earth is a planet.

iv) Three plus six is 9.

v) The sun is a star.

Each of sentences (iii), (iv) & (v) is a true declerative sentence and so each of them is a statement.

Each of sentences (i) & (ii) is a false declerative sentence and so each of them is a statement.



To denote statements we use the capital letters P, Q, R, ... etc

IIIUSTRATION 2 : Consider the following sentences :

i) Do your home work.

ii) Give me a glass of water.

iii) How are you ?

iv) Have you ever seen Taj Mahal ?

v) May god bless you !

vi) May you live long !

Sentences (i) & (ii) are imperative sentences. so they are not statements. Each of sentences (iii) & (iv) is asking a question. So they cannot be assigned true or false. Hence they are not statements. Each of sentences (v) & (vi) is an imperative optive. So we cannot assign true or false of them and hence none of them is a statement.



CHECK YOUR PROGRESS

1: Find out which of the following sentences are statements and which are not - justify your answer.

i) Paris is in England.

ii) May god bless you ?

iii) 6 has three prime factors .

iv) 18 is less than 16 .

v) How far is chennai from here?

vi) Every rhombus is a square .

vii) There are 35 days in a month.

viii) Two plus three is five.

ix) x +2 = 9

x) The moon is made of green cheese.

13.4 LOGICAL CONNECTIVES

Till now, we have considered primary statements. We often combine simple (primary) statements to form compound statements by using certain connecting words known as logical connectives. Primary statements are combined by means of connectives : *AND , OR, IF---- THEN ,* and *IF AND ONLY IF,* lastly *NOT.*

Now we will discuss in details about logical connectives with their truth tables.

13.4.1 Negation

The denial of a statement P is called its negation and is written as **~P** and read as 'not P'. Negation of any statement P is formed by writing "It is not the case that -------" or "It is false that ---------" before P or inserting in P the word "not".

Let us consider the statement

P : All integers are rational numbers .

The negation of this statement is :

~ P : It is not the case that all integers are rational numbers.

or

~ P : It is false that all integer are not rational number.

or

~ P : At least one integer is not a rational number.

or

Consider now the statement ,

P : 7> 9

The negation of this statement is

~ P : 7 < 9

or

~ P : 7= 9

TRUTH TABLE OF NEGATION

If the truth value of "P " is T, then the truth value of ~P is F. Also if the truth value of "P " is F, then the truth value of ~p is T .

This definion of the negation is summarized as follows by a table .

The truth table of ~P is :

P	~ P
T	F
F	T

Table 2.1

IIUSTRATION EXAMPLES :

Write the negation of the following statements :

(i) $\sqrt{7}$ is a rational.

(ii) $\sqrt{2}$ is not a complex number.

(iii) Every natural number is greater than zero.

(iv) All primes are odd.

(v) All mathematicians are man .

Solution : (i) Let *r* denotes the given statement i.e

r : $\sqrt{7}$ is a rational.

The negation ~ r of this statement is given by

~ r : It is not the case that $\sqrt{7}$ is a rational.

or

~ r : $\sqrt{7}$ is not a rational.

or

~ r : It is false that $\sqrt{7}$ is rational .

(ii) Let the given statement be denoted by *u* i.e

u : $\sqrt{2}$ is not a complex number.

The negation ~ u of this statement is given by

~u : $\sqrt{2}$ is a complex number.

or

~u : It is false that $\sqrt{2}$ is not a complex number.

(iii) The negation of the given statement is :

It is false that every natural number is greater than 0.

or

There exists a natural number which is not greater than 0.

(iv) The negation of the given statement is

There exists a prime which is not odd.

or

Some primes are not odd.

or

At least one prime is not odd.

(v) The negation of the given statement is :

Some mathematician is not man.

or

There exists a mathematician who is not man.

or

At least one mathematician is not man.

or

It is false that all mathematicians are man.



CHECK YOUR PROGRESS

Q 2: Write the negation of the following statements -

i) Bangalore is the capital of Karnataka.

ii) The Earth is round.

iii) The Sun is cold.

iv) Some even integers are prime.

v) Both the diagonals of a rectangle have the same length.

13.4.2 Conjunction

The conjunction i.e joining of two statements P and Q is the statement P $\wedge$ Q which is read as "*P and Q*"

IIIUSTRATION EXAMPLES :

(i) The conjunction of the statements :

P : It is raining.

Q : 2+2 = 4 is P $\wedge$ Q.i.e

It is raining and 2+2=4 .

(ii) Consider the statement

P : The Earth is round and the Sun is cold.

Its components are :

Q : The Earth is round.

R : The Sun is cold.

Truth table : The statement P $\wedge$ Q has the truth value T whenever both P and Q have the truth value T ; Other wise it has the truth value F.

The truth table for conjunction as follows :

P	Q	P $\wedge$ Q
T	T	T
T	F	F
F	T	F
F	F	F

Table 2.2

IIIUSTRATION EXAMPLES :

Translate the following statement into symbolic form :

Ramu and Raghu went to school.

Solution : In order to write it as a conjunction of two statements, it is necessary first to paraphrase the statement as Ramu went to school and Raghu went to school.

Now write P : Ramu went to school.

Q : Raghu went to school

Then the given statement can be written in symbolic form as $P \wedge Q$.

13.4.3 Disjunction

The disjunction of the two statements P and Q is the statement $P \vee Q$ which is read as "*P or Q*".

IIUSTRATION 3 :

(i) Consider the compound statement

P : Two lines intersect at a point or they are parallel.

The component statements of this statement are :

Q : Two lines intersect at a point.

R : Two lines are parallel.

(ii) Consider another statement

P : 45 is a multiple of 4 or 6.

Its component statements are :

Q : 45 is a multiple of 4 .

R : 45 is a multiple of 6.

Truth table : The statement $P \vee Q$ has the truth value F only when both P and Q have the truth value F, $P \vee Q$ is true if either P is true or Q is true (or both Pand Q are true). Truth table for disjunction :

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Table 2.3



CHECK YOUR PROGRESS

Q 3: Write the following statements in symbolic form :

(i) Pavan is rich and Raghav is not happy.

(ii) Pavan is not rich and Raghav is happy.

(iii) Naveen is poor but happy.

(iv) Naveen is rich or unhappy

(v) Naveen and Amal are both smart .

(vi) It is not true that Naveen and Amal are both smart

(vii) Naveen is poor or he is both rich and unhappy

(vii) Naveen is neither rich nor happy.

IIIUSTRATIVES EXAMPLES :

Write the components statements of the following compound statements and check the compound statement is true or false.

(i) 50 is a multiple of both 2and 5.

(ii) All living things have two legs and two eyes .

(iii) Mumbai is the capital of Gujrat or Maharashtra.

(iv) A rectangle is a quadrilatateral or a 5 sided polygon.

(v) $\sqrt{2}$ is a rational number or an irrational



The connective is not always the same as the word "or "because the fact that the word "or " in English language can be used in two different senses :
i) Inclusive OR (one or the other or both) and
ii) Exclusive OR (one or the other but not both)

Solution : (i) The components statements of the given statement are

P : 50 is multiple of 2

Q : 50 is multiple of 5

we observe that both P and Q are true statements. Therfore the compound statement is true.

(ii) The component statements of the given statement are

P : All living things have two legs.

Q : All living things have two eyes.

we find that both P and Q are false statements. Therefore, the compound statement is false.

(iii) The components statements of the given statement are

P : Mumbai is the capital of Gujrat.

Q : Mumbai is the capital of Maharashtra.

we find that P is false and Q is true. Therefore, the compound statement is true.

(iv) The components statement are

P : A rectangle is a quadrilateral.

Q : A rectangle is a 5 sided polygon.

we observe that P is true and Q is false . Therefore, the compound statement is true.

(v) The compound statement are

P : $\sqrt{2}$ is a rational number.

Q : $\sqrt{2}$ is an irrational number.

clearly P is false and Q is true, therefore the compound statement is true.



CHECK YOUR PROGRESS

Q 4: Write the component statements of the following compound statements and check the compound statement is true or false.

(i) Delhi is in India and 2+2=4.

(ii) Delhi is in England and 2+2=4.

(iii) Delhi is in India and 2+2=5 .

(iv) Delhi is in England and 2+2=5.

(v) Square of an integer is positive or negative.

(vi) The sky is blue and the grass is green .

(vii) The earth is round or the sun is cold.

(viil) All rational numbers are real and all real numbers are complex.

(ix) 25 is a multiple of 5 and 8.

(x) 125 is a multiple of 7or 8.

13.4.5 Conditional

If P and Q are any two statements, then the statement $P \rightarrow Q$ read as "*if P , then Q*", is called a conditional statement.

Example : Let P : Amulya works hard.

Q : Amulya will pass the examination.

Then $P \rightarrow Q$: If Amulya works hard, then he will pass the exam.

The statement P is called the *antecedent* and Q is called the *consequent* in $P \rightarrow Q$. The sign $\rightarrow$ is called the sign of implication.

We will also write $P \rightarrow Q$ for P only if Q.

Truth table for conditional '$P \rightarrow Q$ ' as follows :

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

we will also write $P \rightarrow Q$ for (i) P only if Q (ii) Q If P (iii) Q provided that P, (iv) P is sufficient for Q, (v) Q is necessary conditions for P, (vi) P implies Q, (vii) Q is implied by P.

IIIUSTRATIVES EXAMPLES :

1. Write each of the following statements in the form " If--then"
   (i) You get job implies that your credentials are good.
   (ii) A quadrilateral is a parallogram if its diagonals bisect each other.
   (iii) To get A+ in the class, it is necessary that you do all the excercisesof the book.

Solution :

(i) we know that "If P, then Q" is equivalent to "$P \rightarrow Q$"
Therefore,the given statement can be written as
"If you get a job , then your credentials are good."

(ii) The given statement can be written as-
"If the diagonal of a quadrilateral bisect each other, then it is parallogrm".

(iii) The given statement can be written as

"If you get A+ in the class, then you do all the exercise of the books".

2. Write the component statements of each of the following statements. Also check whether the statements are true or not.

(i) If a triangle ABC is equilateral , then it is isosceles.

(ii) If a and b are integers , then ab is a rational number.

Solution :

(i) The component statements of the given statement are:

P : The triangle ABC is equilateral.

Q : The triangle ABC is isosceles.

Since an equilateral triangle is isosceles, so the given statement is true.

(ii) The component statements are :

P : a and b are integers.

Q : ab is a rational number.

Since the product of two integers is an integer and therefore a rational number. So, the compound statement is true.



CHECK YOUR PROGRESS

Q 5: Write down the truth value of each of the following implication.

(i) If 3+2=7, then Paris is the capital of india.

(ii) If 3+4=7,then 3 $\rangle$ 7.

(iii) If 4 $\rangle$ 5,then 5 $\langle$ 6.

(iv) If 7 $\rangle$ 3, then 6 $\langle$ 14.

(v) If two integers a and b are such that a>b, then a-b is always a positive integer.

13.4.6 Biconditional (If and only if implication)

If P and Q are any two statements , then the statement $P \leftrightarrow Q$ which is read as"P If and only if Q" and abbreviated as "Piff Q" is called a biconditional.

The following table defines the biconditional :

The statement $P \leftrightarrow Q$ has the truth value T whenever both P and Q have identical truth values.

Truth table for biconditional ($P \leftrightarrow Q$):

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

The biconditional $P \leftrightarrow Q$ is the conjunction of the conditionals $P \rightarrow Q$ and $Q \rightarrow P$ i.e $(P \rightarrow Q) \wedge (Q \rightarrow P)$ is an alternate notation for $P \leftrightarrow Q$

Also, truth table for $(P \rightarrow Q) \leftrightarrow (Q \rightarrow P)$

P	Q	$P \rightarrow Q$	$Q \rightarrow P$	$(P \rightarrow Q) \wedge (Q \rightarrow P)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Note that both truth tables are identical.

IIIUSTRATIVES EXAMPLES :

1. Consider the statement :

   A triangle is equilateral if and only if it is equiangular.

   This is if and only if implication with the component statements:

   P : A triangle is equilateral.

   Q : A triangle is equiangular.

2. 8 $\rangle$ 4 if and only if 8 -4 is positive.
3. 2+ 2=4 if and only if it is raining.
4. Two lines are parallel if and only if they have the same slope.

Biconditional $P \leftrightarrow Q$ may be read by following way :

a. P if and only if Q

b. P is equivalent to Q

c. P is necessary and sufficient condition for Q

d. Q is necessary and sufficient condition for P

IIIUSTRATION EXAMPLES :

Write the truth value of each of the following biconditional statements.

(i) 4 $\rangle$ 2 if and only if 0 $\langle$ 4-2 .

(ii) 3 $\langle$ 2 if and only if 2 $\langle$ 1.

(iii) 3+5 $\rangle$ 7 if and only if 4+6 $\langle$ 10.

Solution :

(i) Let P : 4 $\rangle$ 2

Q : 0 $\langle$ 4-2

Then, the given statement is $P \leftrightarrow Q$.

Clearly, P is true and Q is true and therefore, $P \leftrightarrow Q$ is true. Hence, the given statement is true, and its truth value is T.

(ii) Let P : 3 < 2

Q : 2<1

Then, the given statement is $P \leftrightarrow Q$.

Clearly, P is false and Q is false and therefore, $P \leftrightarrow Q$ is true. Hence, the given statement is true, and its truth value is T.

(iii) Let P : 3+5 > 7

Q : 4+6<10

Then, the given statement is $P \leftrightarrow Q$



Clearly, P is true and Q is false and therefore, $P \leftrightarrow Q$ is false. Hence, the given statement is false and therefore, its truth value is F.

CHECK YOUR PROGRESS

Q 6: Write down the truth value of each of the following

(i) 3+5=8 if and only if 4+3=7.

(ii) 4 is even if and only if 1 is prime.

(iii) 6 is odd if and only if 2 is odd.

(iv) 2+3=5 if and only if 3>5.

(v) 4+3=8 if and only if 5+4=10.

(vi) 2<3 if and only if 3<4.



13.5 LET US SUM UP

- Mathematical logic is concerned with all kinds of reasoning, whether they be legal arguments or mathematical proofs or conclusions in a scientific theory based upon a set of hypotheses.
- Sentences are usually classified as declarative, exclamatory, interrogative and imperative. In our study of logic, we will confine ourselves to declarative sentences only i.e. we begin by assuming that the object language contains a set of declarative sentences. A primary statement is a declarative sentence which cannot be further broken down or analyzed into simpler sentences.
- New statements can be formed from primary statements through the use of sentential connectives. The resulting statements are called *compound statements.*
- The sentential connectives are called logical connectives.the different types of connectives are: *negation(~), AND(conjunction),OR (disjunction), IF---THEN (conditional), IF AND ONLY IF (Bi-conditional) etc.*

- Truth tables have already been introduced in the definitions of the connectives Our basic concern is to determine the truth value of a statement formula for each possible combination of the truth values of the component statements. A table showing all such truth values is called the truth table of the formula. we constructed the truth table for ~P, $P \vee Q$, $P \wedge Q$, $P \rightarrow Q$ and $P \leftrightarrow Q$. Observe that if the truth values of the components are known, then the truth value of the resulting statement can be readily determined from the truth table by reading along the row which corresponds to the correct truth value of the component statements.
- The statement P is called the antecedent and Q is called the consequent in $P \rightarrow Q$.



13.6 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Statement : (i), (iii), (iv), (vi), (vii), (viii) & (x).

Ans to Q No 2: (i) Bangalore is not the capital of Karnataka.

(ii) The earth is not round.

(iii) The sun is not cold.

(iii) No even integer is prime.

(iv) There is at least one rectangle whose both diagonals do not have the same length.

Ans to Q No 3: (i) $P \wedge \sim Q$ where P : Pavan is rich
Q : Raghav is happy

(ii) $\sim P \wedge Q$

(iii) $\sim R \wedge H$ where R : Naveen is rich
H : Naveen is happy

(iv) $R \vee \sim H$

(v) $P \wedge Q$ where P : Naveen is smart

Q : Amal is smart

(vi) $\sim(P \wedge Q)$

(vii) $\sim R \vee (R \wedge \sim H)$ where R : Naveen is rich

R : Naveen is happy

(viii) $\sim R \wedge \sim H$

Ans to Q No 4: (i) P : Delhi is in india

Q : 2+2=4

the compound statement is true

(ii) P : Delhi is in England

Q : 2+2=4

the compound statement is false.

(iii) P : Delhi is in india

Q : 2+2=5

the compound statement is false

(iv) P : Delhi is in England

Q : 2+2=5

the compound statement is false

(v) P : Square of an integer is positive

Q : Square of an integer is negative

the compound statement is true.

(vi) P : The sky is blue

Q : The grass is green

The compound statement is true.

(vii) P : The earth is round

Q : The sun is cold

The compound statement is true.

(viii) P : All rational numbers are real

Q : All real numbers are complex.

The compound statement is true.

(ix) P : 25 is a multiple of 5

Q : 25 is a multiple of 8

The compound statement is false.

(x) P : 125 is a multiple of 7

Q : 125 is a multiple of 8

The compound statement is false.

Ans to Q No 5: (i) True (ii) False (iii) True (iv) False (v)True

Ans to Q No 6: (i) True (ii) False (iii) True (iv) False (v) True (vi) True.



13.7 FURTHER READING

1) C. L. Liu, Elements of Diserete Mathemathics, Tata McGraw-Hill Edition

2) Seymour Lipschutz, Marc Lars Lipson, Discrete Mathematics, Tata McGraw-Hill Edition.



13.8 MODEL QUESTIONS

Q 1: Find out which of the following sentences are statements and which are not. Justify your answer.

(i) The real number x is less than 2.

(ii) All real numbers are complex numbers.

(iii) Listen to me, Ravi !

Q 2: Find the component statements of the following and check whether they are true or not:

(i) A line is staight and extends indefinitely in both directions.

(ii) The sky is blue and the grass is green.

(iii) The earth is round or the sun is cold.

(iv) All rational numbers are real and all real numbers are complex

(v) 25 is a multiple of 5 and 8.

Q 3: Write the component statements of each of the following statements.Also, check whether the statements are true or not.

(i) Sets A and B are equal if and only if ($A \subseteq B$ and $B \subseteq A$).

(ii) $|a|<2$ if and only if ($a>-2$ and $a<2$)

(iii) Δ ABC is isosceles if and only if $\angle B = \angle C$.

(iv) $7<5$ if and only if 7 is not a prime number.

(v) Δ ABC is a triangle if and only if AB+BC>AC.

*** ***** ***

UNIT 14 : BOOLEAN ALGEBRA

UNIT STRUCTURE

14.1 Learning Objectives

14.2 Introduction

14.3 Definition, Properties and Examples

14.4 Basic Laws of Boolean Algebra

14.5 Boolean Expression

14.6 Let Us Sum Up

14.7 Answers To Check Your Progress

14.8 Further Readings

14.9 Model Questions

14.1 LEARNING OBJECTIVES

After going through this unit, you will able to know

- boolean algebra, its properties, examples
- basic laws of boolean algebra
- boolean expression.

14.2 INTRODUCTION

Boolean Algebra is an algebraic structure after the name of British logician George Boole (1813-1864). By an algebraic structure we mean a set equipped with one or more binary operations defined on it satisfying certain axioms. Though it is an abstract algebraic sturucture, it can be used for analysing electrical circuits. Nowadays it is immensely used for the analysis and design of electronic computers.

14.3 DEFINITION, PROPERTIES AND EXAMPLES

Definition : Let B a non-empty set equipped with two binary operations + and . , a unary operation $'$, and two distinct elements 0 and 1. Then B is called a Boolean Algebra if the following conditions are satisfied.

1. Commutative laws

   (i) a + b = b + a, (ii) a.b = b.a, $\forall a, b \in B$

2. Distributive laws

   (i) a + (b.c) = (a + b).(a + c)

   (ii) a. (b + c) = (a.b) + (a.c), $\forall a, b, c \in B$

3. Identity laws

   (i) a + 0 = a, (ii) a.1 = a

4. Complement laws

   (i) a + $a^{/}$ = 1, (ii) a.$a^{/}$ = 0

Note : 1. From the definition it is clear that there cannot a Boolean Algebra with one element.

2. 1 is called unit element, and 0 is called zero element.
3. $a^{/}$ is called complement of a.
4. A Boolean Algebra is generally denoted by (B, + , . , $^{/}$, 0, 1) or (B, +, . ,$^{/}$) or simply by B.
5. The symbols 0 and 1 are not necessaily real numbers 0 and 1 respectively.

Example 1 : B = {0, 1} is a Boolean Algebra under +, . , $^{/}$ defined by

+	1	0
1	1	1
0	1	0

.	1	0
1	1	0
0	0	0

	/
1	0
0	1

Solution : From the definition of +, . , $^{/}$, it follows that

1. (i) a + b = b + a

   (ii) a.b = b.a, $\forall a, b \in B$

2. (i) a + (b.c) = (a+b).(a + c)

   (ii) a.(b+c) = (a.b) + (a.c), $\forall a, b, c \in B$

3. (i) a + 0 = a, (ii) a.1 = a, $\forall a \in B$

4. (i) a + $a^{/}$ = 1 (1 + $1^{/}$ = 1 + 0 = 1),

   0 + $0^{/}$ = 0 + 1 = 1)

   (ii) a. $a^{/}$ = 0 (1. $1^{/}$ = 1.0 = 0,

   0.$0^{/}$ = 0.1 = 0)

   $\therefore$ (b, + , . , $^{/}$) is a Boolean Algebra.

Properties

1. In a Boolean Algebra B, zero element is unique.

Proof : Let (B, + , . , $^{/}$) be a Boolean Algebra.

If possible, let there be two zero elements 0 and 0_1

$\therefore$ a + 0 = a, $\forall a \in B$

a + 0_1 = a, $\forall a \in B$

$\therefore$ 0_1 + 0 = 0 ($\because$ 0 is zero element)

Again 0_1+0 = 0 + 0_1 (by commutative law)

= 0 ($\because$ 0_1 is zero element)

$\therefore$ 0_1 = 0

i.e. zero element is unique.

Note : In view of the above property, we will write as “the” zero element.

2. In a Boolean Algebra B, unit element is unique.

Proof : Let (B, +, . , $^{/}$) be a Boolean Algebra.

If possible, let there be two unit elements 1, and 1_u.

$\therefore$ $a.1 = a, \forall a \in B$

$a.1_u = a, \forall a \in B$

$\therefore$ 1_u.1 = 1_u ($\because$ 1 is unit element)

$\therefore$ 1_u = 1

i.e unit element is unique.

Note : In view of the above theorem, we will write as “the” unit element.

3. In a Boolean Algebra B, complement of each element is unique.

Proof : Let (B, + , . , $^{/}$) be a Boolean Algebra.

Let 0 be the zero element, and

1 be the unit element.

Let $a \in B$

If possible, let $a^{/}$ and a_1 be complements of a

$\therefore$ a + $a^{/}$ = 1, a . $a^{/}$ = 0 ($\because$ $a^{/}$ is complement of a)

a + a_1 = 1,a . a_1 = 0 ($\because$ a_1 is complement of a)

Now $a^{/}$ = $a^{/}$.1

= $a^{/}$. (a + a_1)

= ($a^{/}$.a) + ($a^{/}$.a_1)

= (a.$a^{/}$) + ($a^{/}$.a_1)

$= 0 + (a^{/}.a_1)$

$= (a^{/}.a_1) + 0$

$= a^{/}.a_1$ (1)

Again $a_1 = a_1.1$

$= a_1.(a + a^{/})$

$= (a_1.a) + (a_1.a^{/})$

$= (a.a_1) + (a_1.a^{/})$

$= 0 + (a_1.a^1)$

$= (a^{/}.a_1) + 0$

$= a^{/}.a_1$ (2)

From (1) and (2), we get

$a^{/} = a_1$

Note : In view of the above theorem, we write as "$a^{/}$" is the complement of a.

4. In a Boolean Algebra B,

(i) $1^{/} = 0$, (ii) $0^{/} = 1$, where 0 is the zero element, and 1 is the unit element.

Proof : (i) Let B be a Boolean Algebra,

Now, by identity laws, we have a + 0 = 1 and a.1 = a, $\forall a \in B$

Replacing a by 1 in a + 0 = a, we get 1 + 0 = 1.

Replacing a by 0 in a.1 = 1, we get 0.1 = 0

i.e. 1.0 = 0 (0.1 = 1.0, by commutative law)

Thus, 1 + 0 = 1 (1)

1.0 = 0 (2)

From (1) and (2), we conclude that $0 = 1^{/}$ i.e. $1^{/} = 0$ (complement laws)

(ii) Let B be a Boolean Algebra.

Now, by identity laws, we have a.1 = 1 and a + 0 = a, $\forall a \in B$

Replacing a by 0 in a.1 = a, we get 0.1 = 0.

Replacing a by 1 in a + 0 = a, we get 1 + 0 = 1.

i.e. 0 + 1 = 1, (1+ 0 = 0 + 1, by commutativeled)

Thus, 0.1 = 0 (1)

0 + 1 = 1 (2)

From (1) and (2), we conclude that $0^{/} = 1$ (complement law)

Note : The property (ii), viz $0^{/} = 1$ can be derived from property (i), viz $1^{/} = 0$ by interchanging the binary operations + and . , and by interchanging 0 and 1. Here (ii) is called the dual of (i), and vice versa, i.e. (i) is the dual of (ii) This principle is known as the principle of duality. The principle holds good for every statement and every theorem in a Boolean Algebra.

Example 2 : Let X be a non-empty set Let P(x) be the power set of A, i.e P(x) is the set of all subsets of x.

Let $A, B \in P(x)$, i.e. $A \subseteq X,\ B \subseteq X$

We define

$A + B = A \cup B,$

$A.B = A \cap B$

$A^{/}$ = the complement of A.

Clearly, union is a binary operation on P(x), intersection is a binary operation on P(x), complementation is a unary operation on P(x).

Now 1. (i) $A + B = A \cup B = B \cup A = B + A$

(ii) $A.B = A \cap B = B \cap A = B.A,\ \forall A, B \in P(x)$

2. (i) $A + (B.C) = A \cup (B \cap C)$

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

$= (A + B).(A + C),\ \forall A, B, C \in P(x)$

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

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

$= (A.B) + (A.C)$

3. (i) $A + \phi = A \cup \phi = A,\quad \phi \in P(x)$

(ii) $A.X = A \cap X = A$

4. (i) $A + A^{/} = A \cup A^{/} = X$

(ii) $A.A^{/} = A \cap A^{/} = \phi$

$\therefore (P(x), \cup, \cap, {}^{/})$ is a Boolean Algebra, where ϕ is the zero element and X is the unit element.

Example 3: Let B = {1, 2, 5, 10, 11, 22, 55, 110} be the set of all positive divisiors of 110. We define

a + b = l.c.m. of a, b,

a.b = g.c.d. of a, b,

$a^{/} = \frac{110}{a}, \quad a, b \in B$

We construct the composition tables for +, . , $^{/}$ as follow?

+	1	2	5	10	11	22	55	110
1	1	2	5	10	11	22	55	110
2	2	2	10	10	22	22	110	110
5	5	10	5	10	55	110	55	110
10	10	10	110	10	110	110	110	110
11	11	22	110	110	11	22	55	110
22	22	22	110	110	22	22	110	110
55	55	55	110	110	55	110	55	110
110	110	110	110	110	110	110	110	110

.	1	2	5	10	11	22	55	110
1	1	1	1	1	1	1	1	1
2	1	2	1	2	1	2	1	2
5	1	1	5	5	1	1	5	5
10	1	2	5	10	1	2	5	10
11	1	1	1	1	11	11	11	11
22	1	2	1	2	11	22	11	22
55	1	1	5	5	11	11	55	55
110	1	2	5	10	11	22	55	110

/	1	2	5	10	11	22	55	110
	110	55	22	11	10	5	2	1

From the above tables, we see that + is a binary operation on B. .

is a binary operation on B, and $^{/}$ is a unary operation on B.

Again 1 (i) a+b = l.c.m. of a, b

= l. c. m. of b, a

= b+a, $\forall a, b \in B$

(ii) a, b = g.c.d. of a, b

= g.c.d. of b, a

= b.a, $\forall a, b \in B$

2. From the tables, we have

(i) a + (b.c) = (a+b).(a+c)

(ii) a.(b+c) = (a.b) + (a.c), $\forall a, b, c \in B$

3. (i) a+1 = l .c.m of a, 1

= a, $\forall a \in B$

(ii) a.110 = g.c.d. of a, 110

= a, $\forall a \in B$

4. (i) $a+a^{/}$ = l.c.m of a, $a^{/}$

= l.c.m. of $a, \frac{110}{a}$

= 110, $\forall a \in B$

(ii) $a.a^{/}$ = g.c.d. of a, $a^{/}$

= g.c.d. of $a, \frac{110}{a}$

= 1, $\forall a \in B$

$\therefore$ (B, + , . , /) is a Boolean Algebra; where 1 is the zero element, and 110 is the unit element.



CHECK YOUR PROGRESS

Q 1: Let X ={1}. Show that the set P(x) = {{1}, ϕ } is a Boolean Algebra under operations of union, intersection, and complementation in P(x).

Q 2: Let X = {1, 2, 3}, and Let P(X) be the power set of X. Show that P(X) is a Boolean Algebra under operations of union, intersection, and complementation in P(X).

Q 3: Let B = {1, 2, 3, 5, 6, 10, 30} be the set of all positive divisors of 30. Define

a+b = l.c.m. of a, b; $a, b \in B$

a.b = g.c.d. of a, b

$a^{/} = \frac{30}{a}$

Show that (B, +, . , /) is a Boolean Algebra

Q 4: Let B = {1, 2, 5, 7, 10, 14, 35, 70} be the set of all positive

divisors of 70. Define

a+b = l.c.m of a, b, $a, b \in B$

a.b = g.c.d. of a, b

$a^{/} = \frac{70}{a}$

Show that (B, +, . , /) is a Boolean Algebra.

Q 5: Give an example of a Boolean Algebra with 16 elements.

Q 6: Let B = {0, a, b, 1}. Define +, . , / in B as follows.

+	0	a	b	1
0	0	a	b	1
a	a	a	1	1
b	b	1	b	1
1	1	1	1	1

.	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

/	0	a	b	1
	1	b	a	0

Show that (B, +, . , /) is a Boolean Algebra.

Q 7: Let B = { 1, 2, 4, 5, 10, 20} be the set of all positive divisors of 20. Define

a+b = l.c.m. of a, b $\forall a, b \in B$

a.b = g.c.d. of a, b $\forall a, b \in B$

$a^{/} = \frac{20}{a}, \ \forall a \in B$

Examine if (B, +, . , /) is a Boolean Algebra.

14.4 BASIC LAWS OF BOOLEAN ALGEBRA

Let (B, +, . , /) be a Boolean Algebra. Let 0 be the zero element, and 1 be the unit element of B.

1. Idempotent Laws.

(i) a+a = a, (ii) a.a = a, $\forall a \in B$

Proof : (i) a = a+0

= a + (a.a$^{/}$)

= (a+a).(a+a$^{/}$), by associative law

= (a+a).1

= a+a

i.e. a+a = a

(ii) a = a.1

= a.(a + $a^{/}$)

= (a.a) + (a.$a^{/}$), by associative law

= (a.a) + 0

= a.a

Note : The result (ii) is a dual of the result (i), and vice versa. The result (ii) can be obtained from (i) by replacing + by . , . by + , 0 by 1, 1 by 0.

2. Boundedness Laws

(i) a+1 = 1, (ii) a.0 = 0, $\forall\ a \in B$

Proof : (i) a+1 = (a+1) . 1

= (a+1).(a+$a^{/}$)

= a+(1.$a^{/}$), by associative law

= a+$a^{/}$, (1.$a^{/}$ = $a^{/}$.1 = a)

= 1

(ii) a.0 = (a.0) + 0

= (a.0) + (a.$a^{/}$)

= a.(0+$a^{/}$), by associative law

= a.$a^{/}$, (0+$a^{/}$ = $a^{/}$+0 = $a^{/}$)

= 0

3. Absorption Laws

(i) a+(a.b) = a, (ii) a.(a+b) = a, $\forall a, b \in B$

Proof : (i) a+(a.b) = (a.1) + (a.b)

= a.(1 + b)

= a.1, (1+b = b+1 = 1, by boundedness law)

= a

(ii) a.(a+b) = (a+0).(a+b)

= a+(0.b)

= a+0, (0.b = b.0 = 0, by boundedness law)

=a

4. Associative Laws

(i) (a+b)+c = a + (b+c)

(ii) (a.b).c = a.(b.c)

Proof : (i) Let L = (a+b) + c

R = a + (b+c)

Now a.L = a.((a+b)+c)

= a.(a+b) + a.c, by distributive law

= a + (a.c), by absorption law

= a, by absorption law

a . R = a.(a+(b+c))

= (a.a)+(a.(b+c)), by distributive law

= a+(a.(b+c)), by idempotent law

= a, by absorption law

$\therefore$ a.L = a.R

Again a'.L =a'.((a+b) + c)

= a'.(a+b) + (a'.c), by distributive law

= (a'.a) + (a'.b) + (a'.c), by distributive law

= 0 + (a'.b) + (a'.c)

= (a'.b) + (a'.c)

= a'.(b+c)

a'.R = a'.(a + (b+c))

= (a'.a) + a'.(b+c), by distributive law

= 0 + a'.(b+c)

= a'.(b+c)

$\therefore$ a'.L = a'.R

Now L = 1.L

= (a+a').L

= (a.L) + (a'.L)

= (a.R) + (a'.R)

= (a+a').R

= 1.R

= R

$\therefore$ L = R

i. e. (a+b) + c = a+(b+c)

(ii) Let L = (a.b).c

R = a. (b.c)

Now a + L = a + ((a.b).c)

= (a + (a.b)).(a+c), by distributive law

= a.(a+c), by absorption law

= a, by absorption law

a + R = a +(a.(b.c))

= (a+a).(a+(b.c)), by distributive law

= a.(a+(b.c)), by idempotent law

= a, by absorption law

$\therefore$ a + L = a+R

Again a'+L = a' + (a.b).c)

= (a' + (a.b)).(a'+c), by distributive law

= ((a'+a).(a'+b)).(a'+c), by distributive law

= 1.(a'+b).(a'+c)

= (a'+b).(a'+c)

= a' + (b.c)

a' + R = a' +(a.(b.c))

= (a'+a).(a' + (b.c)), by distributive law

= 1.(a' + (b.c))

= a' + (b.c)

$\therefore$ a' + L = a' + R

Now L = 0 + L

= (a.a') + L

= (a+L).(a'+L)

= (a+R).(a'+R)

= (a.a') + R

= 0 + R

= R

$\therefore$ L = R

i.e. (a.b).c = a.(b.c)

5. Involution Law : $\left(a'\right)' = a$

Proof : By definition of complement, we have

a+a' =1, and a.a' = 0

i. e. $a'+a = 1$, and $a'.a = 0$, by commutative law

$\therefore$ by uniquences of complement, a is the complement of a', i. c., $(a')' = a$.

6. De Morgan's Laws

(i) $(a+b)' = a'.b'$, (ii) $(a.b)' = a'+b'$

Proof : (i) $(a+b) + (a'.b') = b+a + (a'.b')$, by commutative law

$= b +(a+a').(a+b')$, by distributive law

$= b+1.(a+b')$

$= b + (a+b')$

$= b + (b'+a)$, by commutative law

$= (b+b') +a$, by associative law

$= 1+a$

$= 1$, by boundedness law

$(a + b).(a'.b') = ((a+b).a').b'$, by associative law

$= ((a.a') + (b.a')).b'$, by distributive law

$= (0 + (b.a')).b'$

$= (b.a').b'$

$= b.(a'.b')$, by associative law

$= b.(b'.a')$, by commutative law

$= (b.b').a'$, by associative law

$= 0.a'$

$= 0$

Thus, we see that $a'.b'$ is the complement of a+b,

i. e. $(a+b)' = a'.b'$

[Augustus De Morgan (1806 – 1871) was a famous mathematician. He was born in Madurai, India]

Corollary (i) $a+b = (a'.b')'$, (ii) $a.b = (a'+b')'$

Proof : (i) $(a'.b')' = (a')'+(b')'$, by De morgan's law

$= a+b$, by involution law

(ii) $(a'+b') = (a')'.(b')'$, by De morgan's law

$= a.b$, by involution law

7. (i) If $b+a = c+a$, and $b+a' = c+a'$, then $b = c$.

(ii) If $b.a = c.a$, and $b.a' = c.a'$, then $b = c$.

Proof : (i) $b = b+0$

$= b + (a.a^{/})$

$= (b+a).(b+a^{/})$, by distributive law

$= (c+a).(c+a^{/})$, (given)

$= c+(a.a^{/})$, by distributive law

$= c+0$

$= c.$

(ii) $b = b.1$

$= b.(a+a^{/})$

$= (b.a) + (b.a^{/})$, by distributive law

$= (c.a) + (c.a^{/})$, given

$= c.(a + a^{/})$

$= c.1$

$= c$

8. (i) $a+b^{/} = 1$ if and only if $a+b = a$

(ii) $a.b^{/} = 0$ if and only if $a.b = a$

Proof : (i) Let $a+b^{/} = 1$

Now $a + b = (a+b) . 1$

$= (a+b).(a+b^{/})$, given

$= (a+(b.b^{/})$, by distributive law

$= a+0$

$= a$

Conversely, Let $a+b = a$

Now $a+b^{/} = 1.(a+b^{/})$

$= (a+a^{/}).(a+b^{/})$

$= a+(a^{/}.b^{/})$, by distributive law

$= a+(a+b)^{/}$, by De morgan's law

$= a+a^{/}$, given

$= 1.$

(ii) Let $a.b^{/} = 0$

Now $a.b = a.b + 0$

$= a.b+a.b^{/}$, given

$= a.(b+b^{/})$, by distributive law

$= a . 1$

= a

Conversely, let a.b = a

Now $a.b' = 0 + a.b'$

$= (a.a') + (a.b')$

$= a.(a'+b')$, by distributive law

$= a.(a.b)'$, by De Mergan's law

$= a.a'$, given

= 0.

9. (i) $a+(a'.b) = a+b$

(ii) $a.(a'+b) = a.b$

Proof : (i) $a+(a'.b) = (a+a').(a+b)$, by distributive law

$= 1.(a+b)$

$= a+b$

(ii) $a.(a'+b) = (a.a') + (a.b)$

$= 0 + (a.b)$

$= a.b$

Example 4: Let B be a Boolean Algebra.

Let $a, b \in B$. Show that

$a.(a.b)' = a.b'$

Solution : $a.(a.b)'$

$= a.(a'+b')$, by De Morgan's law

$= (a.a') + (a.b')$

$= 0 + (a.b')$

$= a.b'$

Example 5: Let B be a Boolean Algebra, and $a, b, c \in B$. Show that

$(a+b).(b+c).(c+a) = a.b + b.c + c.a$

Solution : $(a+b).(b+c).(c+a)$

$= (a+b).(b.c + b.a + c.c + c.a)$

$= (a+b).(b.c + b.a + c + c.a)$

$= a.(b.c) + a.(b.a) + a.c + a.(c.a) + b.(b.c) + b.(b.a) + b.c + b.(c.a)$

$= a.b.c + a.(a.b) + a.c + a.(a.c) + (b.b).c + (b.b).a + b.c + a.b.c$

$= (a.b.c + a.b.c) + (a.a).b + a.c + (a.a).c + b.c + b.a + b.c)$

$= a.b.c + a.b + a.c + a.c + b.c + b.a + b.c$

= a.b.c + (a.b + a.b) + (a.c + a.c) + (b.c + b.c)

= a.b.c + a.b + a.c + b.c

= a.b. (c+1) + a.c + b.c

= a.b.1 + c.a + b.c

= a.b + b.c + c.a

Example 6 : Let B be a Boolean Algebra, and a, b $\in$ B Prove that a+b = 0 if and only if a = 0 and b = 0 Write the dual of the above proposition and prove it

Solution : Let a = 0, and b = 0

$\therefore$ a+b = 0+0

= 0

Converselt, Let a+b = 0

Now a = a+0

= a+(b.b$^{/}$)

= (a+b).(a+b$^{/}$), by distributive law

= 0.(a+b$^{/}$), given

=0

b = b+0

= b + (a.a$^{/}$)

= (b+a).(b+a$^{/}$)

= (a+b).(b+a$^{/}$)

= 0.(b+a$^{/}$)

= 0

2nd Part

Dual of the above proposition is a.b = 1 $\Leftrightarrow$ a = 1, and b = 1

If a = 1, b = 1,

a.b = 1.1 = 1

Conversely, Let a.b = 1

Now a = a.1

= a.(b+b$^{/}$)

= (a.b) + (a.b$^{/}$)

= 1 + (a.b$^{/}$)

= 1

b = b.1

= b.(a+a$^{/}$)

= (b.a) + (b.a$^{/}$)

= (a.b) + (b.a$^{/}$)

= 1 + (b.a$^{/}$)

= 1

Example 7 : Let B be a Boolean Algebra and a, b, c$\in$B. Prove that the following expressions are equal.

(i) (a+b).(a$^{/}$+c).(b+c)

(ii) a.c + a$^{/}$.b + b.c

(iii) (a+b).(a$^{/}$+c)

(iv) a.c + a$^{/}$.b

Solution : (a+b).(a$^{/}$+c).(b+c)

= (a+b).(a$^{/}$.b + a$^{/}$.c + c.b + c.c)

= (a+b).(a$^{/}$.b + a$^{/}$.c + c.b + c)

= a.a$^{/}$.b + a.a$^{/}$.c + a.c.b + a.c + b.a$^{/}$.b + b.a$^{/}$.c + b.c.b + b.c

= 0.b + 0.c + a.c.b + a.c + b.a$^{/}$ + b.a$^{/}$.c + b.c + b.c

= b.c.(a + a$^{/}$) + a.c + b.c + b.a$^{/}$

= b.c.1 + a.c + b.c + a$^{/}$.b

= b.c + a.c + b.c + a$^{/}$.b

= a.c + a$^{/}$.b + b.c (1)

Again, (a+b).(a$^{/}$+c)

= a.a$^{/}$ + a.c + b.a$^{/}$ + b.c

= 0 + a.c + a$^{/}$.b + b.c

= a.c + a$^{/}$.b + b.c (2)

Again, a.c + a$^{/}$.b + b.c

= a.c + a$^{/}$.b + 1.b.c

= a.c + a$^{/}$.b + (a+a$^{/}$).b.c

= a.c + a$^{/}$.b + a.b.c + a$^{/}$.b.c

= ((a.c) + (a.c).b) + ((a$^{/}$.b) + (a$^{/}$.b).c)

= a.c + a$^{/}$.b, by absortion law (3)

From (1), (2) and (3), we conclude that

(a+b).((a$^{/}$+c).(b+c)

= a.c + $a^{/}$.b + b.c

= (a+b).($a^{/}$+c)

= a.c + $a^{/}$.b



CHECK YOUR PROGRESS

Q 8: Prove that there cannot be a Boolean Algebra with 3 elements.

Q 9: Let B be a Boolean Algebra, and let a, b, c $\in$ B. If a+c=a, b+c=b, show that (a.b) + c = a.b

Q 10: Let B be a Boolean Algebra. Let a, b $\in$ B. Show that a+(a+b)$^{/}$ = a+$b^{/}$.

Q 11: Let B be a Boolean Algebra, and let a, b $\in$ B. Prove that the following properties are equivalent

(i) a+b=a, (ii) a+$b^{/}$=1, (iii) a.b=b

Write the dual of the above proposition and prove it.

Q 12: Let B be a Boolean Algebra, and let a, b, c $\in$ B. Show that

[(abc+$a^{/}b^{/}$)$^{/}$ + bc]$^{/}$ = $a^{/}b^{/}$

[Here abc means a.b.c]

14.5 BOOLEAN EXPRESSION

Let us consider the Boolean Algebra B={0, 1}, where +, . , and $^{/}$ are defined by

+	0	1
0	0	1
1	1	1

.	0	1
0	0	0
1	0	1

/	0	0
	1	0

A literal symbol that is used to represent an element of B is called a Boolean variable. Thus, if x denotes a Boolean variable, then x will have the value 0 or 1. If x is a Boolean variable, $x^{/}$ is also a Boolean variable.

Let x, y be two Boolean variables. The values of x, y may be given by the following table.

x	y

1	1
1	0
0	1
0	0

Let x, y, z be three Boolean variables. The values of x, y, z may be given by the following table.

x	y	z
1	1	1
1	1	0
1	0	1
0	1	1
1	0	0
0	1	0
0	0	1
0	0	0

By a Boolean expression, we mean an expression that is construted by a finite set of symbols, each representing a Boolean variable, by applying the binary operations +, and . , and the unary operation /. Thus. $x.y + x^{/}$ is a Boolean expression of two variables. Similarly x.y+y.z+z.x is a Boolean expression of three variables.

We note that 0 and 1 are Boolean expressions. Any variable is a Boolean expression.

Corresponding to a Boolean expression, we can construct a table known as the truth table (or the assignment table or the value table).

We construct a truth table for the Boolean expression $xy+x^{/}$ (By xy we mean x.y).

x	y	xy	$x^{/}$	$xy+x^{/}$
1	1	1	0	1
1	0	0	0	0
0	1	0	1	1
0	0	1	1	1

Two Boolean expressions of variables $x_1, x_2, \ldots, x_n$ are said to be

equal if they assume the same values for every assignment of values 0, 1 to the variables $x_1, x_2, \ldots, x_n$.

The equality of two Boolean expressions is denoted by " = ".

Example 8: Construct the truth table for the Boolean expression xy + xz of the variables x, y, z.

Solution :

x	y	z	xy	xz	xy+xz
1	1	1	1	1	1
1	1	0	1	0	1
1	0	1	0	1	1
0	1	1	0	0	0
1	0	0	0	0	0
0	1	0	0	0	0
0	0	1	0	0	0
0	0	0	0	0	0

Example 9: Construct the truth table for the Boolean expression $xy+x'y+xy'+x'y'$ of the variables x, y.

Solution :

x	y	x'	y'	xy	$x'y$	xy'	$x'y'$	$xy+x'y+xy'+x'y'$
1	1	0	0	1	0	0	0	1
1	0	0	1	0	0	1	0	1
0	1	1	0	0	1	0	0	1
0	0	1	1	0	0	0	1	1

Example 10: Prove that the Boolean expressions $(xy+x)'$ and $(x'+y')x'$ are equal.

Solution :

x	y	xy	xy+x	$(xy+x)'$
1	1	1	1	0
1	0	0	1	0
0	1	0	0	1
0	0	0	0	1

Again,

x	y	x'	y'	$x'+y'$	$(x'+y')x'$
1	1	0	0	0	0
1	0	0	1	1	0
0	1	1	0	1	1
0	0	1	1	1	1

Looking at the last column of the above two tables, we conclude that $(xy+x)' = (x'+y')x'$.



CHECK YOUR PROGRESS

Q 13: Let $f(x, y, z) = xy + z'$ be a Boolean expression of three variables x, y, z. Find the values of f(1, 1, 0), f(0, 1, 1), f(0, 1, 0), f(1, 1, 1), f(0, 0, 0).

Q 14: Construct truth tables for the following Boolean expressions.

(i) $x + yx'$ (ii) $x(x+y')$

(iii) $xy + yz + zx$ (iv) $xy' + x(y'+z)$

Q 15: Examine if the following Boolean expressions are equal

(i) $(x+y)'$, $x'y'$

(ii) $(xy)'$, $x' + y'$

(iii) $x(y+z)$, $xy+xz$

(iv) $xz + (x'+y')'$, $x(y+z)$



14.6 LET US SUM UP

- Let B be a non-empty set equipped with two binary operations + and . , a unary operation /, and two distinct elements 0 and 1. Then B is called a Boolean Algebra if the following conditions are satisfied.

  1. (i) a+b = b+a, (ii) a.b = b.a, $\forall\ a, b \in B$

  2. (i) a+ (b.c) = (a+b).(a+c)

     (ii) a.(b+c) = (a.b)+(a.c), $\forall\ a, b, c \in B$

  3. (i) a+0 = a, (ii) a.1 = 1, $\forall\ a \in B$

(ii) $a+a^{/} = 1$, (ii) $a.a^{/} = 0$, $\forall\ a \in B$

0 is called the zero element.

1 ia called the unit element.

$a^{/}$ is the complement of a.

- In a Boolean Algebra, zero element is unique.
- In a Boolean Algebra, unit element is unique.
- In a Boolean Algebra, complement of each element is unique.
- In a Boolean Algebra B, $1^{/} = 0$, $0^{/} = 1$.
- Every statement and every theorem in a Boolean Algebra remains valid if the binary operations + and . , and the zero element 0 and the unit element 1 are interchanged. This principle is known as the principle of duality.
- In a Boolean Algebra B,

  1. (i) $a+a = a$, (ii) $a.a = a$, $\forall\ a \in B$
  2. (i) $a+1 = 1$, (ii) $a.0 = 0$
  3. (i) $a+(a.b) = a$, (ii) $a.(a+b) = a$
  4. (i) $(a+b)+c = a+(b+c)$
     (ii) $(a.b).c = a.(b.c)$,
  5. $(a^{/})^{/} = a$
  6. (i) $(a+b)^{/} = a^{/}.b^{/}$, (ii) $(a.b)^{/} = a^{/}+b^{/}$
  7. (i) If $b+a=c+a$, and $b+a^{/} = c+a^{/}$, then $b=c$
     (ii) If $b.a. = c.a$, and $b.a^{/} = c.a^{/}$, then $b=c$
  8. (i) $a+b^{/}=1$ if and only if $a+b = a$
     (ii) $a.b^{/} = 0$ if and only if $a.b = a$
  9. (i) $a+(a^{/}.b) = a+b$
     (ii) $a.(a^{/}+b) = a.b$

- A literal symbol that is used to represent an element of the Boolean Algebra B = {0, 1} is called a Boolean variable. In B, +, . , / are defined by

+	0	1
0	0	1
1	1	1

.	0	1
0	0	0
1	0	1

/	0	
	1	0

- By a Boolean expression, we mean an expression that is constructed by a finite set of symbols, each representing a Boolean variable, by

applying the binary operations + and . , and the unary operation /.

- 0 and 1 are Boolean expressions.
- Any variable is a Boolean expression.
- Two Boolean expressions of variables $x_1, x_2, \ldots, x_n$ are said to be equal if they assume the same values for every assignment of values 0, 1 to the variables $x_1, x_2, \ldots, x_n$.

  The equality of two Boolean expressions is denoted by " = ".



14.7 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Here x = {1}

P(x) = {{1}, ϕ }

$\cup$	{1}	ϕ
{1}	{1}	{1}
ϕ	{1}	ϕ

$\cap$	{1}	ϕ
{1}	{1}	ϕ
ϕ	ϕ	ϕ

	$\cap$	/
	{1}	ϕ
	ϕ	{1}

From the tables, we see that $\cup$ is a binary operation on P(x), $\cap$ is a binary operation on P(x), / is a unary operation on P(x).

Now, 1. (i) $A \cup B = B \cup A$

(ii) $A \cap B = B \cap A, \ \forall \ A, B \in P(x)$

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

(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \ \forall \ A, B, C \in P(x)$

3. (i) $A \cup \phi = A$

(ii) $A \cap \{1\} = \{1\}, \forall \ A \in P(x)$

4. (i) $A \cup A' = \{1\}$

(ii) $A \cap A' = \phi, \ \forall \ A \in P(x)$

$\therefore (P(x), \cup, \cap, /)$ is a Boolean Algebra, where ϕ is the zero element and {1} is the unit element.

Ans to Q No 2: Left as an exercise.

Ans to Q No 3: We construct the composition tables for +, . , / as follows.

+	1	2	3	5	6	10	15	30
1	1	2	3	5	6	10	15	30
2	2	2	6	10	6	10	30	30
3	3	6	3	15	6	30	15	30
5	5	10	15	5	30	10	15	30
6	6	6	6	30	6	30	30	30
10	10	10	30	10	30	10	30	30
15	15	30	15	15	30	30	15	30
30	30	30	30	30	30	30	30	30

.	1	2	3	5	6	10	15	30
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
3	1	1	3	1	3	1	3	3
5	1	1	1	5	1	5	5	5
6	1	2	3	1	6	2	3	6
10	1	2	1	5	3	5	15	15
15	1	1	3	5	3	5	15	15
30	1	2	3	5	3	10	15	30

/	1	2	3	5	6	10	15	30
	30	15	10	6	5	3	2	1

From the above tables, we see that + is a binary operation on B, . is a binary operation on B, and $'$ is a unary operation on B.

Again, 1. (i) a+b = l.c.m of a, b

= l.c.m of b, a

= b+a, $\forall\ a, b \in B$

(ii) a.b = g.c.d of a, b

= g.c.d of b, a

= b.a, $\forall\ a, b \in B$

2. From the tables, we have

(i) a+(b.c) = (a+b).(a+c)

(ii) a.(b+c) = (a.b)+(a.c), $\forall\ a, b, c \in B$

3. (i) a+1 = l.c.m of a, 1 = a, $\forall\ a \in B$

   (ii) a. 30 = g.c.d of a, 30 = 1, $\forall\ a \in B$

4. (i) $a+a^{/}$ = l.c.m of a, $a^{/}$

   = l.c.m of a, $\frac{30}{a}$

   = 30

   (ii) $a.a^{/}$ = g.c.d of a, $a^{/}$

   = g.c.d of a, $\frac{30}{a}$

   =1

   $\therefore$ (B, +, . , /) is a a Boolean Algebra, where 1 is the zero element, and 30 is the unit element.

Ans to Q No 4: Left as an exercise.

Ans to Q No 5: Let X = {1, 2, 3, 4}

Then the power set P(x) of x contains 2^4 i.e. 16 elements.

The set P(x) is a Boolean Algebra under operations of union, intersection, and complementation in P(x).

Ans to Q No 6: Here B = {0, a, b, 1}

+, . , / are defined in B as follows

+	0	a	b	1
0	0	a	b	1
a	a	a	1	1
b	b	1	b	1
1	1	1	1	1

.	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

/	0	a	b	1
	1	b	a	0

From the tables, we see that + is a binary operation on B, . is a binary operation on B, $^{/}$ is a unary operation on B.

Now,

1. (i) + is commutative on B.

   (ii) . is commutative on B.

2. (i) + is distributive over . in B

   (ii) . is distributive over + in B

3. (i) a+0 = a

   (ii) a.1 = 1, $\forall\ a \in B$

4. (i) $a+a^{/} = 1$

(ii) $a.a^{/} = 0, \ \forall \ a \in B$

$\therefore$ (B, +, . , /) is a Boolean Algebra, where 0 is the zero element, and 1 is the unit element.

Ans to Q No 7: Here B = {1, 2, 4, 5, 10, 20} is the set of all positive divisors of 20.

We construct the composition tables as follows.

+	1	2	4	5	10	20
1	1	2	4	5	10	20
2	2	2	4	10	10	20
4	4	4	4	20	20	20
5	5	10	20	5	10	20
10	10	10	20	10	10	20
20	20	20	20	20	20	20

.	1	2	4	5	10	20
1	1	1	1	1	1	1
2	1	2	2	1	2	2
4	1	2	4	1	2	4
5	1	1	1	5	5	5
10	1	2	2	5	10	10
20	1	2	4	5	10	20

/	1	2	4	5	10	20
	20	10	5	4	2	1

From the tables, we see that + is a binary operation on B, . is a binary operation on B, / is a unary operation on B.

Now, 1 (i) a+b = l.c.m of a, b

= l.c.m of b, a

= b+a

(ii) a.b = g.c.d of a, b

= g.c.d of b, a

= b.a

2. From the tables, we have

(i) a+(b.c) = (a+b), (a+c)

(ii) a.(b+c) = (a.b) + (a.c), $\forall \ a, b, c \in B$

3. (i) a+1 = l.c.m of a, 1=a

(ii) a.20 = g.c.d of a, 20

= a, $\forall \ a \in B$

The conditions 4 (i), and 4 (ii) are not satisfied. For

$10+10^{/}$ = l.c.m of 10, $10^{/}$

= l.c.m of 10, 2=10

$\therefore$ B is not a Boolean Algebra.

Note : We state the following theorem without proof.

Let n > 1 be a natural number. Let B be the set of all positive divisors of n. We define +, . , / in B as follows.

a+b = l.c.m of a, b

a.b = g.c.d of a, b

$a' = \frac{n}{a}$

Then B is a Boolean Algebra if and only n is not divisible by any square intager.

In the above example, n = 20 and 20 is divisible by 4, which is a square integer.

Ans to Q No 8: If possible, let B be a Boolean Algebra with 3 elements.

Let B {0, 1, a}, where $a \neq 0,\ a \neq 1$

We know that $0' = 1$, $1' = 0$

$\therefore$ $a' = a$

Now a = a.a

= $a.a'$

= 0, which is a contradition

$\therefore$ there cannot be a Boolean Algebra with 3 elements.

Ans to Q No 9: (a.b) + c = c+(a.b), by commutative law

= (c+a).(c+b), by distributive law

= (a+c). (b+c), by commutative law

= a.b, (given)

Ans to Q No 10: $a+(a+b)' = a+(a'.b')$

$= (a+a').(a+b')$

$= 1.\ (a+b')$

$= a+b'$

Ans to Q No 11: First we prove that (i) $\Rightarrow$ (ii)

We have a+b = a

$\therefore$ $a+b' = 1.\ (a+b')$

$= (a+a').(a+b')$

$= a+(a'.b')$

$= a+(a+b)'$

$= a+a'$

$= 1$

Next we prove that (ii) $\Rightarrow$ (iii)

We have $a+b' = 1$

$\therefore a+b = (a+b).1$

$= (a+b).(a+b')$

$= a+(b.b')$

$= a+0$

$= a$

Now $a.b = (a+b).b$

$= b.(a+b)$

$= b.(b+a)$

$= b$, by absorption law

Next we prove that (iii) $\Rightarrow$ (i)

We have $a.b = b$

Now $a+b = a+ (a.b)$

$= a$, by absorption law

Thus, we see that the properties (i), (ii), and (iii) are equivalent.

2nd Part : The dual of the above proposition is

(i) $a.b = a$, (ii) $a.b' = 0$, (iii) $a+b = b$

It can be proved by replacing . by + , + by . , 1 by 0, and 0 by 1 in the first part.

Ans to Q No 12: $[(abc+a'b')' + bc]'$

$= (abc+a'b') (b'+c')$, by De Mergan's law

$= abc\, b' + abc\, c' + a'b'b'+a'b'c'$

$= ac\, 0 + ab\, 0 + a'b' + a'b'c'$, $[bb'=0, cc' = 0, b'b'=b']$

$= a'b' + a'b'c'$

$= a'b'\, I + a'b'c'$

$= a'b' (1+c')$

$= a'b'$, $1+c'=1$

Ans to Q No 13: $f(x, y, z) = xy+z'$

$\therefore$ $f(1, 1, 0) = 1.1 + 0'$

$= 1+1$

$= 1$

$f(0, 1, 1) = 0.1 + 1'$

$= 0 + 0$

$= 0$

$f(0, 1, 0) = 0.1 + 0'$

$= 0+1$

$= 1$

$f(1, 1, 1) = 1.1.+1'$

$= 1+0$

$= 1$

$f(0, 0, 0) = 0.0 + 0'$

$= 0+1$

$= 1$

Ans to Q No 14:

(i)

x	y	x'	yx'	$x+yx'$
1	1	0	0	1
1	0	0	0	1
0	1	1	1	1
0	0	1	0	0

(ii)

x	y	y'	$x+y'$	$x(x+y')'$
1	1	0	1	1
1	0	1	1	1
0	1	0	0	0
0	0	1	1	0

(iii)

x	y	z	xy	yz	zx	xy+yz+zx
1	1	1	1	1	1	1
1	1	0	1	0	0	1
1	0	1	0	0	1	1
0	1	1	0	1	0	1
1	0	0	0	0	0	0
0	1	0	0	0	0	0
0	0	1	0	0	0	0
0	0	0	0	0	0	0

(iv) Left as an exercise

Ans to Q No 15:

(i)

x	y	x+y	$(x+y)'$	x'	y'	$x'y'$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

From column 4 and column 7, we conclude that $(x+y)' = x'y'$

(ii) Left as an exercise.

(iii) Left as an exercise.

(iv)

x	y	z	xz	x'	y'	$x'+y'$	$(x'+y')'$	$xz+(x'+y')'$	y+z	x(y+z)
1	1	1	1	0	0	0	1	1	1	1
1	1	0	0	0	0	0	1	1	1	1
1	0	1	1	0	1	1	0	1	1	1
0	1	1	0	1	0	1	0	0	1	0
1	0	0	0	0	1	1	0	0	0	0
0	1	0	0	1	0	1	0	0	1	0
0	0	1	0	1	1	1	0	0	1	0
0	0	0	0	1	1	1	0	0	0	0

From column 9 and column 11, we conclude that

$xz + (x'+y')' = x(y+z)$



14.8 FURTHER READINGS

1) Sen, M. K, Chakraborty B. C. : *Introduction to Discrete Mathematies* (2010), Books and Allied (P) Ltd, Kolkata 700010.

2) Dasgupta Asok : *Abstract and Linea Algebra* (2014), Asoke Prakasan, Kolkata 700007.



14.9 MODEL QUESTIONS

Q 1: Let X = {1, 2}. Let P (x) be the power set of X. Show that the set P(x) is a Boolean Algebra under union, intersection, and complementation in P(x).

Q 2: Let B = {1, 2, 5, 10, 17, 34, 85, 170} be the set of all positive divisors of 170. Define +, . , / in B as follows.

a+b = l.c.m of a, b

a.b = g.c.d of a, b

$a^{/} = \frac{170}{a}$

Examine if (B, +, . , /) is a Boolean Algebra.

Q 3: Let B = {1, 2, 3, 4, 6, 8, 12, 24} be the set of all positive divisors of 24. Define +, . , / in B as follows.

a+b = l.c.m of a, b

a.b = g.c.d of a, b

$a^{/} = \frac{24}{a}$

Examine if (B, +, . , /) is a Boolean Algebra.

Q 4: Let (B, +, . , /) be a Boolean Algebra, and let a, b $\in$ B. Express the following in simplied form

(i) $(a+b).(a^{/}+b^{/}).(a^{/}+b).(a+b^{/})$

(ii) $(a.b)+(a^{/}.b)+(a.b^{/})+(a^{/}.b^{/})$

Q 5: Let (b, +, . , /) be a Boolean Algebra, and let a, b, c, d $\in$ B. Prove that a.c + b.d = (a+b).(b+c).(c+d).(d+a)

Q 6: Give an example of a Boolean Algebra that has infinite number of elements.

Q 7: Let (B, +, . , /) be a Boolean Algebra, and let a, b, c $\in$ B. Prove that $(a+b')(b+c')(c+a')=(a'+b)(b'+c)(c'+a)$

Q 8: Let $f(x, y, z) = x.y.z + x.y'.z + x'.y.x + x'.y'.z'$ be a Boolean expression of three variables x, y, z. Find the values of f(1, 1, 1), f(1, 1, 0), f(1, 0, 1), f(0, 1, 1), f(0, 0, 0).

Q 9: Construct truth tables for the following Boolean expressions

(i) $xy+x(x+y)$ (ii) $x'y+xy'+x(x+y')$ (iii) $xyz+xy'z+x'yz+xyz'$

Q 10: Examine if the following Boolean expressions are equal

(i) $(x+y+z)'$, $x'y'z'$

(ii) $(xyz)'$, $x'+y'+z'$

(iii) $x.(x+y)$, x

(iv) $(x+y)z'$, $xz'+yz'$

*** ***** ***



PEFERENCES

- Fraleigh, John B : A First in Abstract Algebra (First Indian Reprit, 2003, Person Education (Singapore) Pvt. Ltd., Indian Delhi 110, 092.

- Mapa, S. K. : Higher Algebra (Abstract and Linear) (1994), Ashok Prakashan, Calcutta 700 007.

- Khanna, V. K. and Bhambri, S. K. : A Course in Abstract Algebra (2006), Vikas Publishing House Pvt. Ltd, New Delhi 110 014.

- Singh, Surajeet and Zameeruddin, Qazi Modern Algebra (2006, Vikas Publishing House Pvt. Ltd, New Delhi 110 014.

- Tamuli B. K. : Contemporary Algebra (1977), New Book Stall, Guwahati- 781 001.

- Pundir S . K. : Advance Abstract Algebra, Krishna Prakashan Media (P) Ltd, Meerut 250 001

- Sharma, J. K. : Discrete Mathematics, Macmillian Publishing India Ltd., New Delhi- 110002