Biyani's Think Tank

Concept based notes

Abstract Algebra

(B.Sc)

Dr. Radhika

Lecturer

Deptt. of Science

Biyani Girls College, Jaipur

Published by :

Think Tanks

Biyani Group of Colleges

Sector-3, Vidhyadhar Nagar,

Jaipur-302 023 (Rajasthan)

Ph : 0141-2338371, 2338591-95 • Fax : 0141-2338007

E-mail : acad@biyanicolleges.org

Website :www.gurukpo.com; www.biyanicolleges.org

ISBN: 978-93-83462-84-1

Edition: 2015

Price:

Leaser Type Setted by :

Biyani College Printing Department

Preface

I am glad to present this book, especially designed to serve the needs of the students. The book has been written keeping in mind the general weakness in understanding the fundamental concepts of the topics. The book is self-explanatory and adopts the "Teach Yourself" style. It is based on question-answer pattern. The language of book is quite easy and understandable based on scientific approach.

Any further improvement in the contents of the book by making corrections, omission and inclusion is keen to be achieved based on suggestions from the readers for which the author shall be obliged.

I acknowledge special thanks to Mr. Rajeev Biyani, *Chairman* & Dr. Sanjay Biyani, *Director* (*Acad.*) Biyani Group of Colleges, who are the backbones and main concept provider and also have been constant source of motivation throughout this Endeavour. They played an active role in coordinating the various stages of this Endeavour and spearheaded the publishing work.

I look forward to receiving valuable suggestions from professors of various educational institutions, other faculty members and students for improvement of the quality of the book. The reader may feel free to send in their comments and suggestions to the under mentioned address.

Author

Unit-I

Group and Subgroup

1 **The set of all real numbers under the usual multiplication operation is not a group since**

a) multiplication is not a binary operation
b) multiplication is not associative
c) identity element does not exist
d) zero has no inverse

Ans. d)

2 **If (G,·) is a group s.t. $(ab)^{-1} = a^{-1} b^{-1}$, ∀ a, b ϵ G then G is**

a) commutative semi group
b) abelian group
c) non-abelian group
d) None of these

Ans. b)

3 **The inverse of -i in the multiplicative group {1, -1, i, -i} is**

a) 1
b) -1
c) i
d) -i

Ans. c)

4 **If (G,·) is a group s.t. a^2 = e, a ϵ G then G is**

a) semi group b) abelian group
c) non-abelian group d) none of these

Ans. **b)**

5 **The set of integers Z with the binary operation a⋆b = a+b+1, a ,b ϵ Z is a group. The identity element of this group is**

a) 0 b) 1
c) -1 d) 12

`Ans. c)

6 **In the group (G,·) the value of $(a^{-1}b)^{-1}$ is**

a) ab^{-1} b) b^{-1} c) a^{-1}b d) ba^{-1}

Ans. **b)**

7 **Let G denotes the set of all n×n singular matrices with rational numbers as entries. Then under multiplication G is**

a) Subgroup b) finite abelian group

c) infinite non abelian group d) infinite abelian group

Ans. c)

8 **If a, b are positive integers, define as a⋆b = a where a b = a (modulo 7) then inverse of 3 in G = {1, 2, 3, 4, 5, 6} is**

a) 3 b) 1 c) 5 d) 4

Ans. c)

9 **In the group G = {2, 4, 6, 8} under multiplication modulo 10 the identity element is**

a) 6 b) 8 d) 4 d) 2

Ans. a)

10 **The set of all n^{th} root of unity under multiplication of complex numbers form**

a) Semi group with unity
b) commutative semi group with unity
c) group
d) abelian group

Ans. d)

Q .1 Define order of an element of a group and prove that order of every element of a finite group is finite and less than or equal to the order of the group.

Ans. Order of an element of a group -

Let a be an element of a group G if n is a least positive integer s.t.

a^n = e, where e is identity of G then n is called order of a. And it is denoted by

O (a) = n

Statement of Theorem -

Order of every element of a finite group is finite and less than or equal to the order of the group.

Proof - Let (G, *) be a finite group whose order is n.

Let a ϵ G then $a \star a = a^2 \epsilon$ G

$a^2 \star a = a^3 \epsilon$ G

So on $a^n \epsilon$ G

a° = e, a, a^2-------- a^n are elements of G

But G has only n elements. So there exist two elements a^r and a^s

s.t. $a^r = a^s$, r < s

$\Rightarrow a^r . (a^r)^{-1} = a^s . (a^r)^{-1}$

$\Rightarrow$ e = a^{s-r} where s - r $\neq$ 0

$\Rightarrow a^K$ = e where k $\neq$ 0

$\Rightarrow$ O (a) $\leq$ ——— (1)

now since k = s - r $\leq$ n

$\Rightarrow$ k $\leq$ n ——— (2)

from (1) & (2)

O (a) $\leq$ k $\leq$ n

$\Rightarrow$ O (a) $\leq$ O (G) $\because$ O (G) = n

Hence proved that order of every element of a finite group is finite and less than or equal to the order of the group.

Q.2 Give the definition of cyclic group with example and prove that every infinite cyclic group has two and only two generators

Ans. **Cyclic group** -

Let G be a group then G is called cyclic group of G if there exist a element a in such a way that every element of G can be written as some integral power of a

or G = $\{a^n / n \epsilon Z\}$.

Then a is called generator of group G.

Example -

Set {1, -1, i, - i } is a multiplicative group. This is cyclic group because it has two generators i and -i.

1 = i^4, -1 = i^2, i = i^1, - i = i^3

1 = $(-i)^4$, -1 = $(-i)^2$, i = $(-i)^3$, - i = $(-i)^1$

Statement of Theorem -

Every infinite cyclic group has two and only two generators.

proof Let G be a cyclic group and a be its generator i.e. G = [a].

Now let x ϵ G then $\exists$ m ϵ s.t.

x = a^m

$\Rightarrow$ x = $(a^{-1})^{-m}$

$\Rightarrow$ x can also be written as some integral power of a^{-1}

so a^{-1} is also generator of G.

If possible

Let $a = a^{-1} \Rightarrow a.\ a = a^{-1}.\ a$

$\Rightarrow a^2$ = e

$\Rightarrow$ O (a) = 2

$\Rightarrow$ O (G) = 2

But this contradict that G is infinite so $a \neq a^{-1}$.

Now we prove that there does not exist any other generator.

Let if possible a^m, m $\neq \pm$ 1 is also generator of G.

So for $a \in$ G, $\exists$ n $\in$ s.t.

$a = (a^m)^n$

$\Rightarrow a.\ a^{-1} = a^{mn}.\ a^{-1}$

$\Rightarrow$ e = a^{mn-1}

$\Rightarrow$ O (a) $\leq$ mn-1

$\Rightarrow$ O (G) $\leq$ mn-1

which is contradiction

Hence a and a^{-1} are only two generators of Z.

Hence proved that every infinite cyclic group has two and only two generators.

Q.3 Prove that set P_n of n! permutations on n symbols is a finite group under the operation of permutation multiplication.

Proof Let S = {x_1, x_2----- x_n} be a finite set of n elements. Let f, g $\in$ P_n be two permutations defined on S. Since we know that permutation is one - one on - to mapping so fog is also one - one and on - to mapping. $\Rightarrow$ fog $\in$ P_n

$\Rightarrow$ permutation multiplication is closed under P_n

1 <u>Associativity</u> -

We know that one - one and on - to function satisfy associative property.

i.e. fo (goh) = (fog) oh

so permutation multiplication is associative in P_n

2 <u>Existence of identity element</u> -

Since I $\in$ P_n so

(foI) (x_i) = f [I(x_i)]

= f (x_i] $\forall\ x_i \in$ S, f $\in P_n$

(Iof) (x_i) = I [f(x_i]

= f (x_i) $\forall\ x_i \in$ S, f $\in P_n$

Hence I is identity

3 <u>Existence of inverse</u> -

Let f $\in P_n$. Since f is one - one and on - to so inverse of f i.e. f^{-1} exist which is also one - one and on - to on S so $f^{-1} \in P_n$

Now fof^{-1} (x) = f[f^{-1}(x)] = x = I (x)

$f^{-1}Of$ (x) = f^{-1} [f (x)] = x = I (x)

$\Rightarrow fof^{-1}$ = I = $f^{-1}Of$

$\Rightarrow$ Every permutation has its inverse permutation in P_n

Hence P_n set of n! permutation is a finite group under the operation of permutation multiplication.

This is called **"Symmetric Group".**

Q.4 Define cyclic Permutation and order of a cycle with example.

Ans <u>Cyclic Permutation</u> -

Let S = {x_1, x_2------ x_n} be a finite set then permutation f defined on S is called cyclic permutation if

f (x_i) = x_{i+1} , i = 1, 2, 3-----k – 1, k ≤ n

f (x_k) = x_1

and f (x_j) = x_j , j ≠ 1, 2, 3,------k

<u>Example</u> - f = (1 2 4 6) $\in S_7$ is cyclic permutation of length 4 s.t.

f(1) = 2, f (2) = 4, f(4) = 6, f(6) = 1

f(3) = 3, f (5) = 5, f (7) = 7

Thus f = (1 2 4 6) = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 6 & 5 & 1 & 7 \end{pmatrix}$

<u>Order of a cycle</u> -

If f is cycle of length n then $f^n \equiv$ I, where n is least positive integer then n is called order of cycle f.

Example

Let f = (1 2 5 7) ϵ S_7

f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 4 & 7 & 6 & 1 \end{pmatrix}$

f^2 = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 3 & 4 & 1 & 6 & 2 \end{pmatrix}$

f^3 = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 3 & 4 & 2 & 6 & 5 \end{pmatrix}$

f^4 = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$

Hence order of a cycle is equal to length of a cycle.

Transposition -Any cycle permutation whose length is 2 is called transposition.

Even and odd Permutation -We know that every permutation can be expressesd as a composite of transpositions so if in this expression number of transpositions is even then permutation is even and if number of transposition is odd then permutation is called odd. permutation.

Ex.

f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 3 & 1 & 8 & 7 & 6 & 9 & 5 \end{pmatrix}$

= (1 2 4) (5 8 9) (6 7)

= (1 4) (1 2) (5 9) (5 8) (6 7)

Here number of transposition is 5 which is odd so permutation f is odd permutation

Q.5 Prove that the set A_n of all even permutations of degree n is a group of order $\frac{n!}{2}$

Proof We know that multiplication of two even permutation is even so set A_n is closed for multiplication.

1 Associativity - We know that function satisfy associative property. Since even permutation are also function so multiplication is associative in A_n.

2 Existence of Identity - Identity permutation is even permutation i.e. I ϵ A_n. So I is identity of multiplication in A_n.

3 Existence of inverse - Since inverse of even permutation is also a even permutation so every even permutation has its inverse in A_n.

Hence Set A_n of all even permutation is a group.

Now we have to prove that order of this group A_n is $\frac{n!}{2}$

Let Set S_n has e_1, e_2-------- e_m even permutation and O_1, O_2,------ O_r odd permutations then

S_n = { e_1, e_2,------ e_m, O_1, O_2------ O_r}

∴ m + r = n! ---------- (1)

Now let α be any transposition then α e_1, α e_2--------α e_m are odd permutations and

α O_1, α O_2--------α O_r are even permutation because transposition is odd permutation.

Now since α e_1, α e_2-------- α e_m are odd permutations but number of odd permutation is r in S_n so

m ≤ r ----------(2)

similarly α O_1, α O_2------- α O_r are even permutation but number of even permutation is m in S_n so

r ≤ m ----------(3)

By (2) & (3)

m = r

Now from (1)

m = r = $\frac{n!}{2}$

⇒ Order of A_n (set of even permutation) is $\frac{n}{2}$!

Q. 6 If σ = (1 7 2 6 3 5 8 4)

$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 4 & 3 & 8 & 7 & 6 & 1 \end{pmatrix}$

then prove that

$\rho\sigma\rho^{-1}$ = (ρ(1) ρ(7) ρ(2) ρ(6) ρ(3) ρ(5) ρ(8) ρ(4))

Also express ρ is a product of disjoint cycles

Find whether ρ is an even or odd permutation

Also give its order

Ans σ= (1 7 2 6 3 5 8 4)

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 5 & 1 & 8 & 3 & 2 & 4 \end{pmatrix}$$

$$\rho\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 4 & 3 & 8 & 7 & 6 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 5 & 1 & 8 & 3 & 2 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 8 & 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

$$\rho^{-1} = \begin{pmatrix} 2 & 5 & 4 & 3 & 8 & 7 & 6 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 4 & 3 & 2 & 7 & 6 & 5 \end{pmatrix}$$

Now

$$(\rho\sigma)\,\rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 8 & 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 4 & 3 & 2 & 7 & 6 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 2 & 8 & 7 & 5 & 4 & 1 \end{pmatrix}$$

= (1 3 2 6 5 7 4 8)

= (2 6 5 7 4 8 1 3)

= (ρ(1) ρ(7) ρ(2) ρ(6) ρ(3) ρ(5) ρ(8) ρ(4))

Now

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 4 & 3 & 8 & 7 & 6 & 1 \end{pmatrix}$$

= (1 2 5 8) (3 4) (6 7)

= (1 8) (1 5) (1 2) (3 4) (6 7)

number of transposition is 5 so ρ is odd.

Q .7 Define Subgroup of a group with example and prove that necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is a ϵ H, b ϵ H $\Rightarrow$ $ab^{-1} \epsilon$ H

Ans **Subgroup -**

A non-empty subset H of a group G is said to be a subgroup of G if

i) H is closed for the composition defined on G.

ii) H itself is a group for the composition induced by G.

Ex. i) Set of integers (Z, +) is subgroup of rational numbers (Q, +)

ii) Set ({1, -1}, ·) is subgroup of set ({1, -1, i, -i}, ·)

Now proof of the Statement

Necessary condition -

Let H be a subgroup of G and a, b ϵ H

Now b ϵ H $\Rightarrow$ $b^{-1} \epsilon$ H

$\because$ $a \epsilon$ H and $b^{-1} \epsilon$ H $\Rightarrow$ $ab^{-1} \epsilon$ H

$\therefore$ condition is necessary

Sufficient condition -

Let $a \epsilon$ H, b ϵ H $\Rightarrow$ $ab^{-1} \epsilon$ H

Then we have to prove that H is a subgroup of G.

since H is non-empty set there exist at least one element (say a) in H.

Now $a \epsilon$ H, $a \epsilon$ H $\Rightarrow$ $aa^{-1} \epsilon$ H

$\Rightarrow$ e ϵ H

$\therefore$ H has identity element

Now Let b be any arbitrary element of H then e ϵ H, b ϵ H $\Rightarrow$ $eb^{-1} \epsilon$ H

$\Rightarrow$ $b^{-1} \epsilon$ H

since b is any arbitrary element of H so every element of H has its inverse in H.

Now $a \in$ H, b $\in$ H $\Rightarrow a \in$ H, $b^{-1} \in$ H

$\Rightarrow a(b^{-1})^{-1} \in$ H

$\Rightarrow a$ b $\in$ H

thus H is closed for the composition of G.

Lastly $\forall\ a$, b, c $\in$ H $\Rightarrow a$, b, c $\in$ G

$\Rightarrow a$ (bc) = (a b) c

H is associative

Hence H is subgroup

Thus condition is sufficient

Q .8 The union of two subgroups of a group G is a subgroup iff one is contained in the other.

Proof **<u>Necessary condition</u>** -

Let H_1 and H_2 be any two subgroup of G.

Let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$ then

$H_1 \cup H_2 = H_2$ or H_1 ----------(1)

Since H_1 and H_2 are subgroup so by

(1) $H_1 \cup H_2$ is also a subgroup of G.

<u>Sufficient condition</u> -

Let H_1 and H_2 are two subgroup of G and $H_1 \cup H_2$ is also a subgroup of G then we have to prove that either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Now by contradiction let us suppose that

$H_1 \not\subseteq H_2$ and $H_2 \not\subseteq H_1$

Now $H_1 \not\subseteq H_2 \Rightarrow \exists\ a \in H_1$ and $a \notin H_2$

$H_2 \not\subseteq H_1 \Rightarrow \exists\ b \in H_2$ and $b \notin H_1$

but $a \in H_1 \cup H_2$ and b $\in H_1 \cup H_2$

$\Rightarrow a$ b ϵ H_1U H_2 ($\because$ H_1U H_2 is subgroup)

$\Rightarrow a$ b ϵ H_1 or a b ϵ H_2

Now if a b ϵ H_1

$a \epsilon H_1$ and a b ϵ $H_1 \Rightarrow a^{-1} \epsilon H_1$ and a b ϵ H_1

$\Rightarrow a^{-1}(a$ b) ϵ H_1

$\Rightarrow$ e b ϵ H_1

$\Rightarrow$ b ϵ H_1

which is contradiction

Now if a b ϵ H_2

a b ϵ H_2 and b ϵ $H_2 \Rightarrow a$ b ϵ H_2 and $b^{-1} \epsilon H_2$

$\Rightarrow (a$ b) $b^{-1} \epsilon H_2$

$\Rightarrow a$ e ϵ H_2

$\Rightarrow a \epsilon H_2$

which is contradiction

$\Rightarrow$ Our assumption is wrong

$\Rightarrow H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Q.9 Define cosets and find all the cosets of H = {0,4} in the group G = $(Z_8, +_8)$.

Ans **<u>Coset</u>**

Let H be any subgroup of G and a ϵ G then set

a H = $\{ah/h \in H\}$

is called left coset of H in G

and

H a = $\{ha/h \epsilon$ H$\}$

is called right coset of H in G

Now

$(Z_8, +_8)$ =

$(\{0, 1, 2, 3, 4, 5, 6, 7\}, +_8\}$

Here G = {0,1, 2, 3, 4, 5, 6, 7}

H = {0, 4}

Here H is subgroup of G for $+_8$ and it is commutative so all left cosets are equal to right cosets.

Now

$0 \in G$ and $0 + H = H + 0$

$= \{0 +_8 0, 0 +_8 4\} = \{0,4\} = H$

$1 \in G$ and $1 + H = H + 1$

$= \{1 +_8 0, 1 +_8 4\} = \{1,5\}$

$2 \in G$ and $2 + H = H + 2$

$= \{2 +_8 0, 2 +_8 4\} = \{2,6\}$

$3 \in G$ and $3 + H = H + 3$

$= \{3 +_8 0, 3 +_8 4\} = \{3,7\}$

$4 \in G$ and $4 + H = H + 4$

$= \{4 +_8 0, 4 +_8 4\} = \{4,0\} = H$

$5 \in G$ and $5 + H = H + 5$

$= \{5 +_8 0, 5 +_8 4\} = \{5,1\} = H+1$

$6 \in G$ and $6 + H = H + 6$

$= \{6 +_8 0, 6 +_8 4\} = \{6,2\} = H+2$

$7 \in G$ and $7 + H = H + 7$

$= \{7 +_8 0, 7 +_8 4\} = \{7,3\} = H+3$

Hence there are only 4 different cosests which are

H, H+1, H+2, H+3

Q.10 State and prove Lagrange's theorem.

Ans **Statement -**

Order of each subgroup of a finite group is a divisor of the order of the group.

Proof -

Let G be a finite group of order n and H be a subgroup of order m.

i.e. O(G) = n, O(H) = n ----------(1)

Now let us define a mapping f: H→ a H

s.t. f(h) = a h $a \in G$

This mapping is one-one and on-to mapping so

O(H) = O(a H) = O(H a)

We know that G = $\underset{a \in G}{U} a H$

But we know that all the left cosets are not distinct so let H has only k different cosets

a_1H, a_2H, ------a_kH

so G = a_1H U a_2H U------Ua_kH

O(G) = O($a_1 H$) + O(a_2H) + O(a_3H)------O(a_kH)

= O(H) + O(H) +-------+ O(H) k times using (1)

= kO(H)

⇒ n = km

⇒ order of H is a divisor of the order of the group.

Q. 11 Prove that every group of prime order is a cyclic group.

Ans Let G be a group of prime order p then we have to prove that G is cyclic since p is prime

p >1 i.e. O(G) > 1 ⇒ G has at least two elements. So there exist an element a s.t. $a \neq$ e.

Now $a \neq$ e so O(a) ≥ 2

let O(a) = m

then let H = [a] be a cyclic subgroup of G and

$$O(H) = O(a) = m$$

since H is subgroup of G by Lagrange's theorem m is divisor of p but p is prime so m = 1 or p. But O(H) > 1 so m = p i.e.

$$O(H) = O(G) \Rightarrow H = G$$

H is cyclic so G is cyclic group.

Q.12 If H is a subgroup of G and (G: H) = 2 prove that a H = H a , $\forall$ $a \in$ G.

Proof Given that (G: H) = 2 i.e. H has two different right coset or left costs in G. We know that H is left and right coset of itself. So

G = H U H a H $\cap$ H a = $\emptyset$

and G = H U bH H $\cap$ bH = $\emptyset$

so H a = bH

Now $a \in$ H a, H a = bH $\Rightarrow$ $a \in$ bH

$a \in$ aH, $a \in$ bH $\Rightarrow$ bH = a H

Since two left coset are either identical or disjoint

$\therefore$ H a = b H = a H

$\Rightarrow$ H a = a H. , $\forall$ $a \in$ G

****

Unit-II

Homomorphism, Normal Subgroup and Quotient Subgroup

Q. 1 Define Homomorphism. If f is a homomorphism of a group G into a group G', then prove that

i) H is a subgroup of G

$\Rightarrow$ f(H) is a subgroup of G'

ii) H' is a subgroup of G'

$\Rightarrow f^{-1}(H') = \{x \in G / + (x) \in H'\}$ is a subgroup of group G.

Proof i) Since f is homomorphism from G to G' and

H is any subset of G so f(H) $\subset G'$.

f(H) is non-empty set because

$e \in$ H s.t. f(e) = e' $\in$ f(H)

Now Let a', $b' \in$ f(H)

then $\exists$ a, b $\in$ H s.t.

f(a) = a' and f(b) = b'

Now $a'\ b'^{-1}$ = f(a) of$(b)^{-1}$

= f(a) Of (b^{-1})

= f$(a \star b^{-1})$ ---------(1) {f is homomorphism}

Since H is subgroup so if

$a \in$ H b $\in$ H $\Rightarrow a \star b^{-1} \in$ H

$\Rightarrow$ f$(a \star b^{-1}) \in$ f(H)

$\therefore a'\ b'^{-1} \in$ f(H) from ---------(1)

Thus if a^1, $b^1 \in$ f(H) $\Rightarrow a^1\ b^{1-1} \in$ f(H)

ii> We have to prove $f^{-1}(H')$ is subgroup of G where H' is subgroup of G'

Now $f^{-1}(H')$ is non-empty set

because $e' \in H'$ s.t. f(e) = $e' \in H'$

$\Rightarrow$ e $\in f^{-1}(H')$

Now let a, b $\in f^{-1}(H')$

$\Rightarrow$ f(a) $\in H'$, f(b) $\in H'$

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

= f(a) O[$f(b)$]$^{-1}$ ----------(2)

$\therefore$ f(a) $\in H^1$ f(b) $\in H'$

$\Rightarrow$ f(a) O[$f(b)$]$^{-1} \in H'$

Thus from (1)

f($a \star b^{-1}$) $\in H'$

$\Rightarrow a \star b^{-1} \in f^{-1}(H')$

Thus $a \in f^{-1}(H')$, b $\in f^{-1}(H') \Rightarrow a \star a \star b^{-1} \in f^{-1}(H')$

Hence $f^{-1}(H')$ is subgroup of G.

Q .2 Define Kernel of Homomorphism and show that A homomorphism of a group G into a group G' is a monomorphism iff Kernel of f = {e}, where e is the identity in G.

Ans Kernel of homomorphism -

Let (G, +) and (G', o) be two groups and f is homomorphism defined from G to G' then Kernel of f is denoted by K and it is defined as

K = { x / f(x) = e', x $\in$ G and e^1 is identity element of G'}

Proof of Statement

Let f be a monomorphism i.e. f is one-one homomorphism there we have to prove that Kernel of f ={e}.

Let K be Kernel of f and x $\in$ K

$\Rightarrow$ f(x) = e'

We know that f(e) = e'

so f(x) = f(e) ⇒ x = e {∵ f is one-one)

so K = {e}

Conversely

Let K = {e} then we have to prove that f is one-one

Let x, y ϵ G s.t.

f(x) = f(y)

⇒ f(x) o $[f(y)]^{-1}$ = f(y) o $[f(y)]^{-1}$

⇒ f(x) o $f(y^{-1})$ = f(y) o $f(y^{-1})$

⇒ f (x⋆ y^{-1}) = f (y⋆ y^{-1})

⇒ f (x⋆ y^{-1}) = f (e)

⇒ f (x⋆ y^{-1}) = e'

⇒ x⋆ y^{-1} ϵ K

But K = {e}

so x⋆ y^{-1} = e

⇒ x = y

Thus f is one-one homomorphism

Q.3 Define Normal subgroup.

Prove that a subgroup N of a group (G, o) is normal iff for every n ϵ N and every g ϵ G,

g n g^{-1} ϵ N.

Ans Normal subgroup

Let G be a group then a subgroup N of G is called normal subgroup of G if Ng = gN

∀g ϵ G.

Proof of statement -

Let N be a normal subgroup of G.

then by $definition$ of normal subgroup

Ng = gN , $\forall$ g ϵ G

Now let n ϵ N, g ϵ G

gn ϵ gN$\Rightarrow$gn ϵ Ng. ($\because$ Ng = gN)

$\Rightarrow$ gn ϵ Ng.

$\Rightarrow \exists\ n_1 \epsilon$ N s.t.

gn = n_1 g

$\Rightarrow$ g n g^{-1} = n_1 g g^{-1}

$\Rightarrow$ g n g^{-1} = $n_1 \epsilon$ N

$\Rightarrow$ g n $g^{-1} \epsilon$ N

Conversely - Let N be a subgroup of G s.t. g n $g^{-1} \epsilon$ N then we have to prove that N is normal.

Let g ϵ G then g n $g^{-1} \epsilon$ N $\forall$ n ϵ N

Now n g ϵ NG

n g = (g g^{-1}) n g

= g (g^{-1} n g) ϵ gN

$\Rightarrow$ Ng $\subseteq$ gN ----------(1)

Now g $n_1 \epsilon$ gN

g n_1 = g n_1 (g^{-1} g)

= (g $n_1 g^{-1}$) g. ϵ Ng

$\Rightarrow$ gN $\subseteq$Ng ----------(2)

From (1) & (2) Ng = g N.

$\Rightarrow$ N is normal in G.

Q.4 A subgroup N of a group G is normal subgroup iff g N g^{-1} = N, $\forall$ g ϵ G.

Proof Let N is normal is normal subgroup of G

Let $x \in N$, $g \in G$, then we know that

$g x g^{-1} \in N$

$\Rightarrow g N g^{-1} \subseteq N$ ---------- (1)

this is true for all element of G

so this is also true for g^{-1}

i.e. $g^{-1} N g \subseteq N$

$\Rightarrow g g^{-1} N g g^{-1} \subseteq g N g^{-1} \Rightarrow N \subseteq g N g^{-1}$ ----------(2)

from (1) & (2)

$N = g N g^{-1}$

Conversely - Let $g N g^{-1} = N$ $\forall g \in G$

$\Rightarrow g N g^{-1} \subset N$

$\Rightarrow g x g^{-1} \in N$ $\forall g \in G, x \in N$

Q .5 The intersection of any two normal subgroups of a group is normal subgroup.

Proof Let N_1 and N_2 are two normal subgroup of G then we know that $N_1 \cap N_2$ is subgroup of G. Now we have to prove that $N_1 \cap N_2$ is normal subgroup of G.

Let $n \in N_1 \cap N_2 \Rightarrow n \in N_1$ and $n \in N_2$

Let $g \in G$

then $g \in G, n \in N_1 \Rightarrow g n g^{-1} \in N_1$ $\{\because N_1$ is normal$\}$

$g \in G, n \in N_2 \Rightarrow g n g^{-1} \in N_2$ $\{\because N_2$ is normal$\}$

$\Rightarrow g n g^{-1} \in N_1 \cap N_2$

$\Rightarrow N_1 \cap N_2$ is normal in G.

Q.6 If H is subgroup of G and N is a normal subgroup of G. then $H \cap N$ is a normal subgroup of H. Where $H \cap N$ need not be normal in G.

Proof Let H be a subgroup of G and N is normal subgroup of G. then $H \cap N$ is subgroup of G we want to prove that $H \cap N$ is normal subgroup of H.

Firstly we will prove that H ⋂ N is subgroup of H.

Let x ϵ H ⋂ N and h ϵ H

⇒ x ϵ H and x ϵ N, h ϵ H

x ϵ H, h ϵ H ⇒ h x h^{-1} ϵ H

x ϵ N, h ϵ H ⇒ h x h^{-1} ϵ N {∵ N is normal}

⇒ h x h^{-1} ϵ H ⋂ N

⇒ H ⋂ N is normal in H.

Q .7 Prove that the Kernel of a homomorphism f of a group G to a group G is a normal subgroup of G.

Proof Let f be a homomorphism defined from G to G' and K is Kernel of f then we have to prove that K is normal in G.

K = {x ϵ G / f(x) = e'} where e' is identity of G'

since f(e) = e' ⇒ e ϵ K so K ≠ ∅

Let a, b ϵ K then f(a) = e', f(b) = e'

Now

f (ab^{-1}) = f(a) f(b^{-1}) {∵ f is homomorphism}

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

= e'. e'^{-1}

= e'

⇒ $a\ b^{-1}$ ϵ K

⇒ K is subgroup of G.

Now let a ϵ K and x ϵ G

f (x a x^{-1}) = f(x) f(a) f(x^{-1}) {f is homomorphism}

= f(x) e' [$f(x)$]$^{-1}$

= f(x) [$f(x)$]$^{-1}$

$= e'$

$\Rightarrow$ x $a\ x^{-1} \in$ K

$\Rightarrow$ K is normal in G.

Q.8 **If H and K are two normal subgroups of G, then HK is also a normal subgroup of G.**

Solution **Let H and K are two normal subgroups of G then we have to prove that HK is normal in G.**

Firstly we will prove that HK is subgroup of G.

Let $h_1\ k_1, h_2\ k_2 \in$ HK where $h_1, h_2 \in$ H

$k_1, k_2 \in$ K

Now $(h_1\ k_1)\ (h_2\ k_2)^{-1} = h_1\ k_1\ (k_2^{-1}\ h_2^{-1})$

$= h_1\ (k_1\ k_2^{-1})\ h_2^{-1}$

$= h_1\ k_3\ h_2^{-1}$ $\{k_1\ k_2^{-1} = k_3$ (say)

$= h_1\ (h_2^{-1} h_2)\ k_3\ h_2^{-1}$

$= (h_1\ h_2^{-1})\ (h_2\ k_3\ h_2^{-1})$ ----------(1)

since $k_3 \in$ K, $h_2 \in$ H $\Rightarrow h_2 \in$ G

$\Rightarrow h_2\ k_3\ h_2^{-1} \in$ K $\{\because$ K is normal in G$\}$

and $h_1 \in$ H, $h_2 \in$ H $\Rightarrow h_1\ h_2^{-1} \in$ H

So from ----------(1)

$(h_1 h_2^{-1})\ (h_2\ k_3\ h_2^{-1}) \in$ HK

$\Rightarrow (h_1 k_1)\ (h_2\ k_2^{-1}) \in$ HK

$\Rightarrow$ HK is subgroup of G

Let h k $\in$ HK and x $\in$ G

$\Rightarrow$ h $\in$ H, x $\in$ G and k $\in$ K, x $\in$ G

$\Rightarrow$ x h $x^{-1} \in$ H and x K $x^{-1} \in$ K

$\Rightarrow$ (x h x^{-1}) (x k x^{-1}) ϵ H K

$\Rightarrow$ x h(x^{-1} x) k x^{-1} ϵ H K

$\Rightarrow$ HK is normal subgroup of G.

Q.9 Define Quotient Group and cosets. Prove that the set of all cosets of a normal subgroup H of a group G. is a group with respect to multiplication of cosets defined as Ha H b = H ab $\forall$ a, b ϵ G

Ans Coset -

Let G be a group and H be its normal subgroup then

Hx = {h x / $\forall$ h ϵ H, x ϵ G}

is called right coset of H in G.

Set of all right (left) cosets of H in G is denoted by G/H.

Quotient group or factor group

Let H be a normal subgroup of G.

then set of all right (left) cosets of H in G with operation

H a H b = H a b

is called Quotient group it is denoted by G/H.

Proof Let H be any normal subgroup of G and set of all right cosets of H in G is

G/H = {H a / $\forall$ a ϵ ϵ}

Now we want to prove that G/H is group.

1 Closure -

Let H a, H b ϵ G/H where a, b ϵ G then H a H b = H a b ϵ G/H because a b ϵ G

2 Associativity -

Let H a, H b, H c ϵ G/H where a, b, c ϵ G

then

H a (H b H c) = H a H b c

= H a (b c)

= H (a b) c

= H a b H c

= (H a H b) H c

3 <u>Identity element</u> –

Let H x be identity element of $^{G}/_{H}$ where x ϵ G then for H a ϵ $^{G}/_{H}$

H a H x = H a

$\Rightarrow$ H a x = H a $\Rightarrow$ a x = a $\Rightarrow$ x = e

Thus He = H is identity

4 <u>Existence of inverse</u> –

Let H x be inverse element of Ha then

H a H x = H

$\Rightarrow$ H a x = He $\Rightarrow$ a x = e

$\Rightarrow$ x = $a^{-1}\epsilon$ G

Thus H x = Ha^{-1} is inverse element of H a in $^{G}/_{H}$

Thus $^{G}/_{H}$ is a group

Q .10 Find the quotient group $^{G}/_{H}$ when G = (Z, +) and H = (4Z, +). Also prepare the composition table of $^{G}/_{H}$.

Ans We know that (Z, +) is abelian group so every subgroup of it is normal subgroup. So H is normal subgroup of G so $^{G}/_{H}$ is quotient group whose element are all possible right (left) cosets of H in G.

Cosets of H in G are

0+H = H+0 = {------ -8,-4, 0, 4, 8} = H

1+H = {------ -7, -3, 1, 5, 9------} = H+1

2+H = {------- -6, -2, 2, 6, 10 -----} = H+2

3+H = {------- -5, -1, 3, 7, 11 -------} = H+3

4+H = {-------- -4, 0, 4, 8, -------} = H+4 = H

Similarly 5+H = H+5 = H+1

-1 +H = {------ -9, -5, -1, 3, 7------} = 3+H

-2+H = {------ -10, -6, -2, 2, 6-----} = 2+H

and so.

So we can see here that distint cosets are

G/H = {H, H+1, H+2, H+3}

Composition table of G/H

+	H	H+1	H+2	H+3
H	H	H+1	H+2	H+3
H+1	H+1	H+2	H+3	H
H+2	H+2	H+3	H	H+1
H+3	H+3	H	H+1	H+2

Q.11 Every group is homomorphic to its quotient group.

Proof Let G be a group and N be its normal subgroup.

Let us define a mapping

$\emptyset : G \to G/N$

s.t.

$\emptyset(x) = Nx, \quad \forall x \in G$

For homomorphism

$\emptyset(xy) = Nxy$

$= Nx\ Ny$

$= \emptyset(x)\ \emptyset(y)$

$\Rightarrow \emptyset$ is homomorphism

For each Nx ϵ $G/_N$, $\exists$ x ϵ G s.t.

$\emptyset$ (x) = Nx

$\Rightarrow$ $\emptyset$ is on-to

$\Rightarrow$ $\emptyset$ is on-to homomorphism

Q.12 ***If is a homomorphism of G on to*** $G/_N$ ***defined as f(x) = Nx,*** $\forall$ ***x*** ϵ ***G, then the Kernel of*** **f = N.**

Proof Let f: G $\rightarrow$ $G/_N$

s.t. f(x) = Nx, $\forall$ x ϵ G

then

Ker f = {x ϵ G / f(x) = N}

$\because$ N is identity of $G/_N$

= {x ϵ G / Nx = N}

= {x ϵ G / x ϵ N}

= N

$\Rightarrow$ Ker f = N

Q.13 ***<u>Fundamental Theorem of Homomorphism.</u>***

Prove that every homomorphic image of a group G is isomorphic to some quotient group of G.

Proof Let G be a group and f (G) be its homomorphic image. Let K be Kernel of f then K is normal subgroup of K so we can define quotient group $G/_K$. then we have to prove that

$G/_K \cong$ f (G)

Let us define a mapping

$\emptyset$: $G/_K \rightarrow$ f (G)

s.t. $\emptyset$ (K x) = f(x)

For well defined

Let Ka = K b $\Rightarrow ab^{-1} \in K$

$\Rightarrow$ f $(ab^{-1}) = e'$ { where e' is identity of f(G)}

$\Rightarrow$ f (a) f $(b^{-1}) = e'$ {f is homomorphic}

$\Rightarrow$ f (a) $[f\ (b)]^{-1} = e'$

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

$\Rightarrow$ $\emptyset$ (Ka) = $\emptyset$ (Kb)

$\Rightarrow$ $\emptyset$ is well-defined

For homomorphism

$\emptyset$ (Kab) = f $(a$b)

= f (a) f (b)

= $\emptyset$ (Ka) $\emptyset$ (Kb)

$\Rightarrow$ $\emptyset$ is homomorphic

For one-one.

Let $\emptyset$ (Ka) = $\emptyset$ (Kb)

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

$\Rightarrow$ f (a) $[f\ (b)]^{-1} = e'$

$\Rightarrow$ f (a) f $(b^{-1}) = e'$

$\Rightarrow$ f $(ab^{-1}) = e'$

$\Rightarrow ab^{-1} \in K$

$\Rightarrow$ K a = K b

$\Rightarrow$ $\emptyset$ is one-one

Now For on-to:-

Let b $\in$ f (G) then $\exists$ x $\in$ G s.t.

b = f (x) = ∅ [K x]

⇒ ∅ is on-to

Thus ∅ is isomorphic

i.e $G/K \cong$ f (G)

Q .14 Show that the mapping f: G → G' s.t. f(x) = 2x, ∀ x ϵ G is an isomorphism where G is the additive group of integers and G' is the additive group of even integers including zero.

Proof Here f: G → G' or f: (Z, +) → (2Z, +)

s.t. f (x) = 2x, ∀ x ϵ Z

We have to prove that f is isomorphism. For this we will prove that f is well-defined, homomrphic, one-one and on-to.

For well defined

Let $x_1 = x_2$

⇒ $2x_1 = 2x_2$

⇒ f (x_1) = f (x_2)

f is well defined

For homomorphic:-

f $(x_1+x_2) = 2(x_1+x_2)$

$= 2\ x_1 + 2\ x_2$

= f (x_1) + f (x_2)

f is homomorphic

For one-one:-

Let f (x_1) = f (x_2)

⇒ $2\ x_1 = 2\ x_2$

⇒ $x_1 = x_2$

⇒ f is one-one

For on-to:-

for each element y of G' , ∃ x ϵ G.

s.t. y = 2x = f(x)

⇒ f is on-to

Hence f is isomorphism.

****

Unit-III

Ring and Field

Q .1 Define ring and type of rings.

Ans A non-empty set R with two binary operation (+) and (-) is called ring if it satisfy following portulats.

i) Associativity of addition

$(a + b)+c = a + (b + c), \quad \forall a\ b, c \in R$

ii) Existence of identity

$a +0 = a = 0 +a, \quad \forall\ a \in R$

iii) Existence of inverse

for each $b \in R \quad \exists\ a \in R$ s.t.

$a +b = 0 = b +a$

iv) Commutativity of addition

$a +b = b +a, \quad \forall\ a, b \in R$

v) Associativity of Multiplication

$a. (b. c) = (a. b) .c, \quad \forall\ a, b, c \in R$

vi)Distributivity of Multiplication over addition

$a. (b +c) = a. b + a. c$

$(b +c) . a = b. a +c. a, \quad \forall\ a, b, c \in R$

Types of Ring

i) Commutative ring –

A ring Commutative for multiplication

i.e. $a. b = b. a \quad \forall\ a, b \in R$

is called Commutative ring

ii) Ring with unity –

A ring which have identity element for multiplication is called Ring with unity. Here identity element is called unity, which is 1.

iii)Ring with zero divisor –

A ring is called with zero divisor

if $\exists$ a, b ϵ R s.t.

$a \neq 0, b \neq 0$ and $a. b = 0$

iv) Ring without zero divisor –

A ring which not have any two element a, b. such that

$a \neq 0, b \neq 0$ and $a. b = 0$

is called ring without zero divisor

v) Integral domain –

A commutative ring with unity and without zero divisor is called integral domain.

vi) Field –

A Commutative ring R is field if it has unity element and every non-zero element has its inverse in R.

vii) Division ring or skew field.

A ring is division ring if it has unity and inverse of each element

Q .2 Prove that a ring R without zero-divisor iff the cancellation laws hold in R

Proof Necessary condition –

Let R be a ring without zero-divisor

Let x, y, z ϵ R.

s.t. $x. y = x. z, \quad x \epsilon 0$

$\Rightarrow x. y + [-(x. z)] = x. z + [-(x. z)]$

$\Rightarrow x. y + x. (-z) = 0$

$\Rightarrow x. (y-z) = 0$

R is ring without zero divisor and $x \neq 0$

so $y-z = 0$

$\Rightarrow y = z$

$\Rightarrow$ R holds left cancellation law

similarly R holds right cancellation law

Sufficient Condition –

Let R holds cancellation law

then if possible. let a, b ϵ R s.t.

$a. b = 0 \quad a \neq 0, b \neq 0$

we know that $a. 0 = 0$

$\Rightarrow a. b = a. 0$

$\Rightarrow b = 0$ {by cancellation law}

which is contradiction

so R is without zero divisor

Q .3 Prove that a finite commutative ring without zero divisor is a field.

Prof Let R be a finite commutative ring without zero divisor.

Now we want to prove that this is a field for this we have to prove that R has unity element and every element of R has its multiplicative inverse in R.

Let R has a_1, a_2------a_n n elements

Let x be any non-zero element of R

then $a_1. x$, $a_2. x$, $a_3. x$------$a_n.x \epsilon$ R

There all elements are different

If possible

let $a_i. x = a_j. x$

$\Rightarrow a_i. x - a_j. x = 0$

$\Rightarrow (a_i - a_j) . x = 0$

$\Rightarrow a_i - a_j = 0$ because $x \neq 0$

R is without zero divisor

$\Rightarrow a_i = a_j$

$\Rightarrow$ all elements are different.

Thus $R = \{a_1, a_2 \text{------} a_n\} = \{a_1 . x, a_2 . x \text{ ------ } a_n . x\}$

If $y \in R$ then $\exists\ a_m \in R$ s.t.

$y = a_m . x = x . a_m$

and $x \in R$ so $\exists\ a_l \in R$ s.t.

$x = a_l . x = x . a_l$

Now

$a_l . y = y . a_l = (a_m . x) . a_l$

$= a_m . (x . a_l) = a_m . x$

$= y$

$\Rightarrow a_l$ is identity element of R.

Now

$a_l \in R$ so $\exists\ a_r \in R$

s.t. $a_l = a_r . x = x . a_r$

$\Rightarrow a_r$ is multiplicative inverse of x

here x is any arbitrary element of R so every element of R has its multiplicative inverse in R.

Hence R is field.

Q .4 Define characteristic of a ring. Prove that the characteristic of an integral domain is either zero or prime number.

Proof **<u>Characteristic of a ring</u> –**

Let (R, +, ·) be a ring then a least positive integer n is called characteristic of R if

$$n\,a = 0, \quad \forall\, a \in R$$

where 0 is additive identity.

Proof of Theorem –

Let D be a integral domain at $a \neq 0$ be any element of D then if 0 (a) = 0 then characteristic of D is zero if characteristic of D is non-zero say p then

$$O\,(a) = p$$

we have to prove that p is prime.

Let p is not prime then let $p = p_1\, p_2$

where $p_1 \neq 1$, $p_2 \neq 1$, $p_1 < p$, $p_2 < p$.

Now $a \neq 0 \quad \Rightarrow a.\, a \neq 0$

$$\Rightarrow a^2 \neq 0 \quad \text{and} \quad a^2 \in D$$

We know that order of two non-zero element of an integral domain is same so

$0\,(a) = p \Rightarrow 0\,(a^2) = p$

$\Rightarrow 0\,(a^2) = p_1\, p_2$

$\Rightarrow p_1\, p_2\, a^2 = 0$

$\Rightarrow (p_1\, a)\,(p_2\, a) = 0$

$\Rightarrow$ either $p_1\, a = 0$ or $p_2\, a = 0$

{$\because$ D is without zero divisor

but $p_1\, a \neq 0$. {$\because a \neq 0$ and $p_1 \neq 0$

$p_2\, a \neq 0$ {$\because a \neq 0$ and $p_2 \neq 0$}

which is contradiction

So our assumption that p is not prime is wrong.

Hence p is prime.

Q. 5 Prove that the set of all real numbers of the form m + n$\sqrt{2}$, where m and n are integers with ordinary addition and multiplication forms a ring. Is it field?

Proof Let R = { m + n$\sqrt{2}$ / m, n ϵ Z}

Now let

$m_1 + n_1 \sqrt{2}$; $m_2 + n_2 \sqrt{2}$ ϵ R.

where m_1, n_1, m_2, n_2 ϵ Z

then $(m_1 + n_1 \sqrt{2}) + (m_2 + n_2 \sqrt{2}) = (m_1 + n_1) + (n_1 + n_2) \sqrt{2}$ ϵ R

$\because (m_1 + n_1), (n_1 + n_2)$ ϵ Z

$(m_1 + n_1 \sqrt{2}) . (m_2 + n_2 \sqrt{2}) = (m_1 m_2 + 2 n_1 n_2) + (m_1 n_2 + n_1 m_2) \sqrt{2}$ ϵ R

$\because (m_1 m_2 + 2 n_1 n_2), (m_1 n_2 + n_1 m_2)$ ϵ Z

We know that for addition and multiplication real number are associative here R is set of real numbers so R is associative for addition and multiplication.

Now let m + n$\sqrt{2}$ be any element of R

then (m + n$\sqrt{2}$) + (0 + 0 $\sqrt{2}$) = (m +0) + (n + 0) $\sqrt{2}$

= m + n $\sqrt{2}$

$\Rightarrow$ 0 + 0 $\sqrt{z}$ is additive identity.

(m + n $\sqrt{2}$) + [- m + (-n) $\sqrt{2}$] = (m – m) + (n – n) $\sqrt{2}$

= 0 + 0 $\sqrt{2}$

m + n $\sqrt{2}$ have its additive inverse in R. m + n $\sqrt{2}$ is any arbitrary element of R so every element of R has its additive inverse in R.

Since for real number distributive law for multiplication over addition is true so R has distributive properly.

Hence R form a ring.

Now

(m + n $\sqrt{2}$) . (1 + 0 $\sqrt{2}$) = m + n $\sqrt{2}$

$\Rightarrow 1 + 0\sqrt{2} \quad \epsilon$ R is identity for multiplication.

$(m + n\sqrt{2}) . \frac{1}{(m+n\sqrt{2})} = 1 + 0\sqrt{2}$

$\Rightarrow \frac{1}{m+n\sqrt{2}}$ is multiplicative inverse of $m + n\sqrt{2}$

$\frac{1}{m+n\sqrt{2}} = \frac{m-n\sqrt{2}}{(m+n\sqrt{2})(m+n\sqrt{2})} = \frac{m-n\sqrt{2}}{m^2-2n^2}$

$= \frac{m}{m^2-2n^2} - \frac{n}{m^2-2n^2}\sqrt{2}$

this is element of R if

$\frac{m}{m^2-2n^2} \quad \epsilon Z$ and $\frac{-n}{m^2-2n^2} \quad \epsilon Z$

which is not necessary true.

because if m = 5, n = 3 then

$\frac{1}{5+3\sqrt{2}} = \frac{5}{7} - \frac{3}{7}\sqrt{2} \quad \notin R.$

$\Rightarrow$ R is not a field.

Q. 6 For a ring R in which $a^2 = a$, $\forall\, a \epsilon$ R prove that

i> $a + a = 0$, $\forall\, a \epsilon$ **R**

ii> $a + b = 0 \Rightarrow a = b$

iii> R is commutative ring

Proof i) Let $a \epsilon$ R

then $a + a \epsilon$ R {$\because$ R is ring

$\Rightarrow (a + a)^2 = (a + a)$ {$\because a^2 = a$

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

$\Rightarrow a^2 + a^2 + a^2 + a^2 = a + a$

$\Rightarrow a + a + a + a = a + a$

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

$\Rightarrow (a + a) = 0$ {$\because$ by left cancellation law}

ii) Let $a, b \in R$

and $a + b = 0 \quad \rightarrow$

$\Rightarrow a + b = a + a$ {from i)

$\Rightarrow b = a$

ii) Let $a, b \in R$ then $a + b \in R$

so $(a + b)^2 = a + b$

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

$\Rightarrow a^2 + a.b + b.a + b^2 = a + b$

$\Rightarrow a + a.b + b.a + b = a + b$

$\Rightarrow a.b + b.a = 0$ {by cancellation law}

$\Rightarrow a.b = b.a$ {from ii)}

$\Rightarrow$ R is commutative ring

Q .7 Define subring. Let < R, +, . > be a ring and S be a non-empty subset of R. Prove that S is a subring iff

i) $a \in S, \ b \in S \Rightarrow a - b \in S$

ii) $a \in S, \ b \in S \Rightarrow a\,b \in S$

Proof **Subring –**

Let R be a ring and S be any non empty subset of R then S is called subring of R if

i> $a \in S, \ b \in S \Rightarrow a + b \in S$

ii> $a \in S, \ b \in S \Rightarrow a\,b \in S$

iii> S is also a ring for induced composition by R.

Proof of Statement -

Firstly let S be a subring of ring R.

Let $a, b \in S \Rightarrow a, -b \in S$ {S is a ring

$\Rightarrow a + (-b) \in S$ {S is closed

$\Rightarrow a - b \in S$

S is closed for multiplication so

$a \in S,\ \ b \in S \Rightarrow a\, b \in S$

Conversely - Let S be any non-empty subset of R and

$a, b \in S \Rightarrow a - b \in S$ and $a.\, b \in S$

Then we have to prove that S is subring

Now

$a \in S,\ \ a \in S \Rightarrow a - a \in S$

$\Rightarrow 0 \in S$

$\Rightarrow 0 - a \in S$

$\Rightarrow - a \in S$

and $a \in S, - b \in S \Rightarrow a - (-b) \in S$

$\Rightarrow a + b \in S$

and $a \in S,\ \ b \in S \Rightarrow a - b \in S$

Thus S is closed for addition and multiplication. S has identity element for addition. Every element in S has its additive inverse in S and since S $\underline{c}$ R so S is commutative for addition, associative for addition and hold distributive law.

Hence S is subring of R.

Q.8 Define subfield and Prime-field. Prove that the necessary and sufficient conditions for a non-empty subset K of a field F to be a subfield are

i> $\boldsymbol{a \in K, b \in K \Rightarrow a - b \in K}$

ii> $\boldsymbol{a \in K, 0 \neq b \in K \Rightarrow a\, b^{-1} \in K}$

Ans **Subfield**

Let F be a field and K be its non-empty set then K is called subfield of F if

i> $a \in K, b \in K \Rightarrow a + b \in K$

ii> $a \in K, b \in K \Rightarrow a\, b \in K$

iii> K is also a field for induced composition by F.

Prime Field -

If a field does not have any proper subfield then field is called prime field.

Proof of Theorem –

Necessary condition –

Let K be a subfield of field F.

Let $a \epsilon$ K, b ϵ K $\Rightarrow a \epsilon$ K, - b ϵ K {K is field}

$\Rightarrow a$ + (- b) ϵ K {K is closed}

$\Rightarrow a$ – b ϵ K

$a \epsilon$ K, 0 ≠ b ϵ K $\Rightarrow a \epsilon$ K, $b^{-1} \epsilon$ K {K is field }

$\Rightarrow a\, b^{-1} \epsilon$ K {K is closed}

Sufficient condition –

Let K be a non-empty subset of field F

and $a \epsilon$ K, b ϵ K $\Rightarrow a$ – b ϵ K, $a\, b^{-1} \epsilon$ K.

then

$a \epsilon$ K,$a \epsilon$ K $\Rightarrow a - a \epsilon$ K

$\Rightarrow 0 \epsilon$ K [additive identity]

0 ϵ K, $a \epsilon$ K $\Rightarrow 0 - a \epsilon$ K

$\Rightarrow - a \epsilon$ K [additive inverse]

$a \epsilon$ K, - b ϵ K $\Rightarrow a$ - (- b) ϵ K

$\Rightarrow a$ +b ϵ K [closed for addition]

$a \epsilon$ K, $a \epsilon$ K $\Rightarrow a\, a^{-1} \epsilon$ K

$\Rightarrow 1 \epsilon$ K [multiplicative identity]

1.ϵ K. $a \epsilon$ K $\Rightarrow 1.a^{-1} \epsilon$ K

$\Rightarrow a^{-1} \epsilon$ K [multiplicative inverse]

$a \epsilon$ K, $b^{-1} \epsilon$ K $\Rightarrow a\,(b^{-1})^{-1} \epsilon$ K

$\Rightarrow a$ b ϵ K [closed for multiplication]

And K $\subseteq$ F so K is commutative, associative for addition, associative for multiplication and hold distributive law.

Hence K is subfield.

Q .9 Prove that the set S = { $a + 2^{1/3}$ b + $4^{1/3}$ c / a, b, c ϵ Q} is a subfield of R.

Ans Let x ϵ S and y ϵ S

where x = $a + 2^{1/3}$ b + $4^{1/3}$ c , a, b, c ϵ Q

y = d + $2^{1/3}$ e + $4^{1/3}$ f, d, e, f ϵ Q

then

x –y = ($a + 2^{1/3}$ b + $4^{1/3}$ c) – (d + $2^{1/3}$ e + $4^{1/3}$ f)

= (a – d) + $2^{1/3}$ (b – e) + $4^{1/3}$ (c – f) ϵ S

{$\because$ a – d, b – e, c – f ϵ Q

Now if x $\neq$ 0 then inverse of x is $1/x$

$$x^{-1} = \frac{1}{x}$$

$$= \frac{1}{a+2^{1/3}b+4^{1/3}c} \times \frac{a^2+(2^{1/3}b)^2+(4^{1/3}c)^2-(a)(2^{1/3}b)-(2^{1/3}b)(4^{1/3}c)-a(4^{1/3}c)}{a^2+(2^{1/3}b)^2+(4^{1/3}c)^2-a(2^{1/3}b)-(2^{1/3}b)(4^{1/3}c)-a(4^{1/3}c)}$$

$$= \frac{a^2+4^{1/3}b^2+2.2^{1/3}c^2-2^{1/3}ab-2bc-4^{1/3}ac}{a^3+2b^3+4c^3-3a.2^{1/3}b+4^{1/3}c}$$

$$= \frac{(a^2-2bc)+2^{1/3}(2c^2-ab)+4^{1/3}(b^2-ac)}{a^3+2b^3+4c^3-6abc} \quad \epsilon \text{ S}$$

Now

x ϵ S, y ϵ S

then x. y = (a d + 2 b f + 2 c e) + $2^{1/3}$(a e + b d + 2 c f)

+ $4^{1/3}$ (a f + b e + c d) ϵ S

so we already proved that if y ϵ S $\Rightarrow y^{-1} \epsilon$ S

Now

x ϵ S, y ϵ S $\Rightarrow$ x ϵ S, $y^{-1} \epsilon$ S

$\Rightarrow$ x $y^{-1} \epsilon$ S

Hence S is a Subfield of R.

Q.10 Define i) Ring homomorphism

ii) Embedding of Ring

Ans. **Ring homomorphism –**

Let R and S be two ring and f be a function defined from R to S then f is called ring homomorphism if

f (a +b) = f (a) + f(b)

f (a b) = f (a) f(b), $\forall$ a, b ϵ R

Embedding of Ring

Let R and R' be two ring then if there exist subring S of R' such that S is monomorphic to R then R is embedded in R' and R' is Extension of R.

Q .11 Prove that every ring can be embedded in a ring with unity.

Ans Let R be a ring and Z be a ring of integers.

Let R' = Z $\times$ R = {(m, a) / m ϵ Z, a ϵ R}

s.t. (m, a) + (n, b) = (m + n, a + b)

(m, a) (n, b) = (m n, n a + m b + a b)

where m, n ϵ Z, a, b ϵ R

Now we want to prove that R' is a ring for these compositions.

i) Associative for addition

Let (p, a), (q, b), (r, c) $\epsilon R'$

then [(p, a) + (q, b)] + (r, c) = (p + q, a +b) + (r, c)

$= [(p + q) + r, (a + b) + c]$

$= (p + q + r, a + b + c)$

$= (p + (q + r), a + (b + c))$

$= (p, a) + [(q + r), (b + c)]$

$= (p, a) + [(q, b) + (r, c)]$

ii) additive identity –

since $0 \in Z$ and $0 \in R$

so $(0, 0) \in R'$ Let $(m, a) \in R$

Now $(0, 0) + (m, a) = (0 + m, 0 + a)$

$= (m, a)$

$\Rightarrow$ (0, 0) is additive identity of R'.

iii)additive inverse –

$(m, a) \in R' \Rightarrow m \in Z, \quad a \in R$

$\Rightarrow - m \in Z, \quad -a \in R$

$\Rightarrow (- m, - a) \in R'$

Now

$(m, a) + (- m, - a) = (m + (- m), a + (- a))$

$= (m - m, a - a)$

$= (0, 0)$

$\Rightarrow$ (- m, - a) is additive inverse of (m, a)

iv) commutative for addition

$(m, a) + (n, b) = (m + n, a + b)$

$= (n + m, b + a)$

$= (n, b) + (m, a)$

v)Associative for multiplication –

$[(p, a) (q, b)] (r, c) = (p q, q a + p b + a b) (r, c)$

$= [p q r, r (q a) + r (p b) + r (a b) + p g c + (q a + p b + a b) c]$ ---------(1)

$(p, a) [(q, b) (r, c)]$

$= (p, a) (q r, r b + q c + b c)$

$= (p (q r), (q r) a + p (r b + q c + b c) + a (r b + q c + b c))$

$= (p q r, r q a + r p b + p q c + p b c + r a b + q a c + a b c)$----------(2)

from (1) & (2)

$[(p, a) (q, b)] (r, c) = (p, a) [(q, b) (r, c)]$

vi) Multiplicative identity –

$1 \in Z, 0 \in R$ so $(1, 0) \in R'$

Now let $(m, a) \in R'$

then $(m, a) (1, 0) = (1. m, a. 1 + m. 0 + a. 0)$

$= (m, a)$

$\Rightarrow (1, 0)$ is multiplicative identity

Hence R' is ring with unity

Let

$S = \{0\} \times R = \{(0, a) / a \in R\}$

Clearly S is a non-empty subset of R'

Now Let $(0, a), (0, b) \in S$

then $(0, a) – (0, b) = (0, a) + (0, - b)$

$= (0, a - b) \in S$

and $(0, a) (0, b) = (0.0, a. 0 + 0. b + a. b)$

$= (0, a b) \in S$

$\Rightarrow$ S is subring of R'.

Let us define a mapping

$\emptyset : R \to S$

s. t. $\emptyset$ (a) = (0, a), $\quad \forall$ a ϵ R

For homomorphism

$\emptyset$ (a + b) = (0, a + b)

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

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

and $\emptyset$ (a b) = (0, a b)

= (0, a) (0, b)

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

$\Rightarrow \emptyset$ is homomorphism

For one-one

Let $\emptyset$ (a) = $\emptyset$ (b)

$\Rightarrow$ (0, a) = (0, b)

$\Rightarrow$ a = b

$\Rightarrow \emptyset$ is one-one

Thus. R' has a subring S which is monomorphic to R so R is embedded in $R^{'}$.

Q .12 Prove that the field < Q, +, · > of rational numbers is a prime field.

Proof We have to prove that field < Q, +, · > of rational numbers is prime field. i.e. it has no any proper subfield. Let S be any subfield of Q.

then $S \subseteq Q$ -------(1)

and 1 ϵ S

Now 1 ϵ S $\Rightarrow$ 1+1+1+-----m times = m ϵ S

1+1+1-----n times = n ϵ S

$\frac{m}{n} \epsilon$ Q where m, n ϵ Z, n $\neq$ 0

m ϵ S and n ϵ S $\Rightarrow$ $\frac{1}{n}$ ϵ S {S is subfield

m ϵ S and $\frac{1}{n}$ ϵ S $\Rightarrow$ $\frac{m}{n}$ ϵ S

i.e. $\frac{m}{n}$ ϵ Q $\Rightarrow$ $\frac{m}{n}$ ϵ S

$\Rightarrow$ Q $\subseteq$ S ----------(2)

from (1) & (2)

Q = S

$\Rightarrow$ S is not a proper subfield of Q

$\Rightarrow$ < Q, +, · > is prime field.

Q .13 Field of quotient of an integral domain is the smallest field containing it.

Proof **Field of quotient** –

Let D be a integral domain with more than one element then (F, f) is called field of quotient of D where F is a field and f is a monomorphism defined from D to F. Here every element of a ϵ F can be represent as $\frac{f(x)}{f(y)}$ where x, y ϵ D y $\neq$ 0.

Proof of statement

Let D be a integral domain and K be a field containing it.

Let a, b ϵ D, b $\neq$ 0 $\Rightarrow$ a, b ϵ K, b $\neq$ 0 {$\because$ D$\subset$K

$\Rightarrow$ a $b^{-1}\epsilon$ K {$\because$ K is a field

Let K^1 = {a b^{-1} / a, b ϵ D, b $\neq$ 0}

then $K^1 \subset$ K . Now we have to prove that K^1 is subfield of K and $K^1 \cong$ F where F is quotient field of D.

Let x, y ϵ K

$\Rightarrow \exists$ a, b, c, d ϵ D s. t.

x = a b^{-1}, y = c d^{-1} b, d $\neq$ 0

Now x – y = a b^{-1} - c d^{-1}

= a d d^{-1} b^{-1} - c b b^{-1} d^{-1}

= (a d – c b) b^{-1} d^{-1} (D is commutative

$\Rightarrow$ x – y ϵ K^1

Now x y^{-1} = (a b^{-1}) $(c\ d^{-1})^{-1}$

= (a b^{-1}) $[(d^{-1})^{-1}\ c^{-1}]$

= (a b^{-1}) (d c^{-1})

= a (b^{-1}d) c^{-1}

= a d ($b^{-1}c^{-1}$) [D is commutative

= a d $(c\ b)^{-1}$ a d, c b ϵ D

$\Rightarrow$ x y^{-1} ϵ K

Hence K^1 is subfield of K.

Now we will prove that

F $\cong$ K^1

Let us define a mapping

f: F $\rightarrow$ K^1.

s. t. f (a/b) = a b^{-1} $\forall$ a/b ϵ F

For homomorphism

f $\left(\frac{a}{b}+\frac{c}{d}\right)$ = f $\left(\frac{a\,d+c\,b}{b\,d}\right)$

= (a d + c b) $(b\ d)^{-1}$

= (a d + c b) $(d^{-1}b^{-1})$

= a d d^{-1} b^{-1} + c b $d^{-1}b^{-1}$

= a b^{-1}+ c d^{-1}

= f (a/b) + f (c/d)

f $\left(\frac{a}{b}.\frac{c}{d}\right)$ = f $\left(\frac{a\,c}{b\,d}\right)$

$= (a\ c)\ (b\ d)^{-1}$

$= (a\ c)\ (d^{-1}b^{-1})$

$= a\ (c\ d^{-1})\ b^{-1}$

$= (a\ b^{-1})\ (c\ d^{-1})$

$= f\ (a/b)\ .\ f\ (c/b)$

$\Rightarrow$ f is homomorphism

For one-one

$f\ (a/b) = f\ (c/b)$

$\Rightarrow a\ b^{-1} = c\ d^{-1}$

$\Rightarrow a\ b^{-1}\ b = c\ d^{-1}\ b$

$\Rightarrow a = c\ b\ d^{-1}$

$\Rightarrow a\ d = c\ b$

$\Rightarrow (a, b) = (c, d)$

$\Rightarrow (a, b) \sim (c, d)$

$\Rightarrow a/b = c/d$

$\Rightarrow$ f is one-one.

For on - to –

For each $a\ b^{-1} \in K^1\ \exists\ a/b \in F$

s. $t.$ $f\ (a/b) = a\ b^{-1}$

$\Rightarrow$ f is on to

Hence $F \cong K^1$

Now if D is contained in a field K then F is also contained in K.

Hence, field of quotient of an integral domain is the smallest field containing it.

Unit-IV

Ideal and Vector Space

Q .1 Define ideal. Prove that if I_1 and I_2 be two ideals of a ring R, then prove that $I_1 + I_2 = \{a_1 + a_2 / a_1 \in I_1, a_2 \in I_2\}$ is an ideal containing both I_1 and I_2.

Ans Ideal

A non-empty subject I of a ring R is called ideal of R if

i> I is a subgroup for addition operation induced by R.

ii> $\forall$ a $\in$ I, r $\in$ R $\Rightarrow$ r. a $\in$ I

and a. r $\in$ I

Proof of Theorem –

Let $x = a_1 + a_2 \in I_1 + I_2$, $a_1 \in I_1$, $a_2 \in I_2$

and $y = b_1 + b_2 \in I_1 + I_2$, $b_1 \in I_1$, $b_2 \in I_2$

Now $a_1, b_1 \in I_1 \Rightarrow a_1 - b_1 \in I_1$ {$\because I_1$ is ideal

$a_2, b_2 \in I_2 \Rightarrow a_2 - b_2 \in I_2$ {$\because I_2$ is ideal

Now

$x - y = (a_1+a_2) - (b_1+b_2)$

$= (a_1-b_1) + (a_2-b_2) \in I_1 + I_2$

$\Rightarrow I_1 + I_2$ is a subgroup of R.

Now Let r $\in$ R, $x = a_1+a_2 \in I_1+I_2$

$\Rightarrow$ r $\in$ R, $a_1 \in$ I, and r $\in$ R, $a_2 \in I_2$

$\Rightarrow$ r. $a_1 \in I_1$ and r. $a_2 \in I_2$

and a_1. r $\in I_1$ and a_2. r $\in I_2$

$\Rightarrow$ r a_1+r $a_2 \in I_1 + I_2$ and a_1. r + a_2. r $\in I_1+I_2$

$\Rightarrow$ r (a_1+a_2) ϵ I_1+I_2 and (a_1+a_2) r ϵ I_1+I_2

Hence I_1+I_2 is a ideal.

Now we have to prove that I_1+I_2 contains I_1 and I_2 both.

Let $a_1 \epsilon I_1 \Rightarrow a_1 = a_1+0 \epsilon I_1+I_2$

$\Rightarrow I_1 \subseteq I_1 + I_2$

similarly $a_2 \epsilon I_2 \Rightarrow a_2 = 0 + a_2 \epsilon I_1+I_2$

$\Rightarrow I_2 \subseteq I_1 + I_2$

Theorem ***Prove that a commutative ring with unity is a field if it has no proper ideal or if it is a simple ring.***

Proof Let R be a commutative ring with unity and it has no proper ideal.

Let Ra = {r a / r ϵ R}, where a ϵ R

then this is an ideal.

But R is simple so

Ra = {0} or Ra = R

but r = 1 ϵ R $\Rightarrow$ 1. a = a ϵ Ra

$\Rightarrow$ Ra $\neq$ {0}

$\Rightarrow$ Ra = R

For providing that R is a field we have to that R has multiplicative inverse of each of its elements.

Since every element R can be expressed as ra where r ϵ R then since 1 ϵ R so for 1 ϵ R $\exists$ x ϵ R s. t.

x a = 1 $\Rightarrow$ x = $a^{-1} \epsilon$ R

$\Rightarrow$ every non-zero element has its inverse in R

$\Rightarrow$ R is a field

Q .2 Define Principal ideal and Principal ideal domain.

Prove that every ideal I in a ring Z of integers is a principal ideal or the ring Z of integers is a principal ideal ring and principal ideal domain.

Proof **Principal ideal** –

An ideal I of a ring R is called principal ideal if it can be generate by a single element i.e. if R has an element a s. *t*. I = [a].

Principal ideal domain –

If every ideal of an integral domain is principal ideal then integral domain is called principal ideal domain.

Proof of the theorem –

Let I be an ideal of Z then

if $I = \{0\}$ then $\exists\ 0 \in Z$ s. *t*.

$I = [0]$ then I is principal ideal

Let $I \neq \{0\}$ then $m \in I, m \neq 0$

if $m \in I \Rightarrow -m \in I$ {$\because$ I is ideal

$\Rightarrow$ I has positive integer.

Let a be smallest integer of I and b be any other integer then by division algorithm

$b = a q + r$ where $0 \leq r < a$

Now $a \in I, q \in Z \Rightarrow a q \in I$ {$\because$ I is ideal

$b \in I, a q \in I \Rightarrow b - a q \in I$

$\Rightarrow r \in I$

which is contradiction of being a smallest integer so r = 0

$\Rightarrow$ $b = a q$

so $I = \{a q / q \in Z\}$

$\Rightarrow$ I is a principal ideal

⇒ Z is a principal ring

since Z is commutative ring with unity

so Z is a principal integral domain.

Q .3 Define quotient ring. Prove that an ideal of a commutative ring R with unity is prime iff R/I is an integral domain

Ans Quotient ring – Let R be a ring and I be its ideal. Since R is a ring so it is commutative for addition. I is it's a subgroup of R for addition so I is also commutative subgroup of R. we know that every commutative subgroup is normal subgroup so I is a normal subgroup of R. So we can define

R/I = {I + a / a ϵ R} whose elements are cosets of I in R. This R/I is called quotient ring.

Proof of the theorem –

Let R be a commutative ring with unity and I be its prime ideal so R/I is also a commutative ring with unity. Now we have to prove that R/I is an integral domain for this we will prove that R is without zero divisor.

Let I + a, I + b ϵ R/I

s. ϵ. (I + a) + (I + b) = I

⇒ I + a b = I

⇒ a b ϵ I ⇒ a ϵ I or b ϵ I {∵ I is prime

⇒ I + a = I or I + b = I

⇒ R/I is without zero divisor.

Conversely Let R/I is an integral domain then we have to prove that I is a prime ideal of R.

Now since R/I is an integral domain

so R/I is without zero divisor.

Let a b ϵ I then we have to prove

either a ϵ I or b ϵ I

Now a b ϵ I

$\Rightarrow$ I + a b = I

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

$\Rightarrow$ I + a = I or I + b = I $\{\because R/I$ is without zero divisor

$\Rightarrow$ a ϵ I or b ϵ I

$\Rightarrow$ I is prime ideal.

Q .4 State and prove fundamental Theorem of ring homomorphism.

or

Prove that every homomorphic image of a ring R is isomorphic to some Quotient ring.

Ans Let R be a ring and f (R) be its homomorphic image. K be Kernel of f then K be ideal of R. So we can define R/K which is quotient ring of R. We have to prove that

$$R/K \cong f(R)$$

Let us define a mapping

$$\emptyset: R/K \to f(R)$$

s. ε. $\emptyset$ (K + a) = f (a) a ϵ R

For well-defined

Let K + a = K + b, a, b ϵ R

$\Rightarrow$ a – b ϵ K

$\Rightarrow$ f (a – b) = 0′ {0′ is identity of f (R)}

$\Rightarrow$ f (a) – f (b) = 0′

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

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

$\Rightarrow$ $\emptyset$ is well-defined

For homomorphism

$\emptyset$ [(K + a) + (K + b)] = $\emptyset$ [K + (a + b)]

= f (a + b)

= f (a) + f (b)

= $\emptyset$ (K + a) + $\emptyset$ (K + b)

and $\emptyset$ [(K + a) (K + b)] = $\emptyset$ [K + a b]

= f (a b)

= f (a) f (b)

= $\emptyset$ (K + a) $\emptyset$ (K + b)

$\Rightarrow$ $\emptyset$ is homomorphism

For one-one

Let $\emptyset$(K + a) = $\emptyset$ (K + b)

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

$\Rightarrow$ f (a) – f (b) = 0′

$\Rightarrow$ f (a - b) = 0′

$\Rightarrow$ a – b $\in$ K

$\Rightarrow$ K a = K b

$\Rightarrow$ $\emptyset$ is one-one

For on-to – For each f (a) ϵ f (R), $\exists$ K + a ϵ R/K

s. t. $\emptyset$ (K + a) = f (a)

$\Rightarrow$ $\emptyset$ is on-to

Hence $R/_K \cong$ f (R)

Q.5 Prove that an ideal I of a commutative ring R with unit is maximal iff the quotient ring $R/_I$ is a field.

Ans Let R be a commutative ring with unity and I be its maximal ideal, then we have to prove that $R/_I$ is a field.

Since R is a commutative ring with unity so $R/_I$ is also commutative with unity.

where I is zero and I + e is unity. element of $R/_I$. where e is unity of I.

Now if $I + a \neq I + 0 = I$

$\Rightarrow$ $a \notin I$

We know that [a] is an ideal of R.

so I + [a] is also an ideal of R.

then $a \notin I \Rightarrow I \subset I + [a] \subset R$

but I + [a] is maximal ideal so

$I + [a] = R$

$\Rightarrow R = \{i + r. a / i \in I, r \in R\}$

since $e \in R$ so $\exists$ $i_1 \in I, r_1 \in R$ s. $\in$.

$e = i_1 + r_1 . a \Rightarrow e - r_1 . a = i_1 \in I$

$\Rightarrow e - r_1 . a \in I$

$\Rightarrow I + e = I + r_1 a$

$\Rightarrow I + e = (I + r_1)(I + a)$

$\Rightarrow$ If I + a is multiplicative inverse of $I + r_1$

$\Rightarrow$ every element of $R/_I$ has its multiplicative inverse in $R/_I$

$\Rightarrow$ $R/_I$ is a field.

Conversely – Let I be an ideal of commutative ring with unity and $R/_I$ is a field.

Then we have to prove that I is maximal ideal.

Let N be any ideal of R s.t. $I \subseteq N \subseteq R$

and $I \neq N$ then we have to prove that N = R for providing I is maximal ideal of R.

Since $I \neq N$ so $\exists\ a \in N$ s. t. $a \notin I$

$\Rightarrow$ $I + a \neq I$

Now $I + a \in {}^{R}/_{I}$ and ${}^{R}/_{I}$ is a field so

I + a has its multiplicative inverse say I + b i.e.

(I +a). (I + b) = I + e

$\Rightarrow I + a\,b = I + e$

$\Rightarrow e - a\,b \in I$

$\Rightarrow e - a\,b \in N$ $\because I \subseteq N$ $a.\,b \in N$

$\Rightarrow e \in N \Rightarrow N = R$

$\Rightarrow$ I is maximal ideal

Q .6 Define vector space.

Prove that the matrix set

V = $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} / a, b \in R \right\}$ is a vector space over the field R of real numbers with respect to matrix addition and matrix scalar multiplication.

Ans **<u>Vector Space</u> –**

An algebraic structure $(V, \oplus)$ where V is non-empty set is called vector space over field $(F, \oplus, \odot)$ if

I) $(V, \oplus)$ is abelian group

II) if $\alpha \in F, v \in V$

then $\alpha \odot v \in V$

III) $\alpha \odot (v_1 \oplus v_2) = \alpha \odot v_1 \oplus \alpha \odot v_2$ where $\alpha \in F$

and $v_1, v_2 \in V$

IV) $(\alpha_1 \oplus \alpha_2) \odot v_1 = \alpha_1 \odot v_1 + \alpha_2 \odot v_4$

where $\alpha_1, \alpha_2 \in F$ and $v_1 \in V$

V) $\alpha_1 \odot (\alpha_2 \odot v_1) = (\alpha_1 \odot \alpha_2) v_1$

where $\alpha_1, \alpha_2 \in F$ and $v_1 \in V$

VI) $1 \odot v_1 = v_1$ where 1 is identity for multiplication in F.

Here elements of V are called vectors and elements of F are called scalar.

Proof

I Let $v_1 = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix}$, $v_2 = \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} \in V$

where $a_1, a_2, b_1, b_2 \in R$

then

$$v_1 + v_2 = \begin{pmatrix} a_1 + a_2 & 0 \\ 0 & b_1 + b_2 \end{pmatrix} \in V$$

since $(a_1 + a_2), (b_1 + b_2) \in R$

$\Rightarrow$ V is closed for addition.

We know that matrix addition is commutative and associative so V is commutative and associative.

Now Since $0 \in R$ so

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in V$

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

$\Rightarrow \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is identity for addition in V

And for each $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in V$, $\exists \begin{pmatrix} -a & 0 \\ 0 & -b \end{pmatrix} \in V$

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

$\Rightarrow$ every element of V has its additive inverse.

Hence (V, +) is commutative group.

II Let $v = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $\alpha \in R$

then $\alpha . v = \alpha \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} \alpha a & 0 \\ 0 & \alpha b \end{pmatrix} \in V$

$\Rightarrow$ V is closed for scalar multiplication in R

III $\alpha(v_1 + v_2) = \alpha \left[\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} + \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} \right]$

$= \alpha \begin{pmatrix} a_1 + a_2 & 0 \\ 0 & b_1 + b_2 \end{pmatrix}$

$= \begin{pmatrix} \alpha(a_1 + a_2) & 0 \\ 0 & \alpha(b_1 + b_2) \end{pmatrix}$

$= \begin{pmatrix} \alpha a_1 + \alpha a_2 & 0 \\ 0 & \alpha b_1 + \alpha b_2 \end{pmatrix}$

$= \begin{pmatrix} \alpha a_1 & 0 \\ 0 & \alpha b_1 \end{pmatrix} + \begin{pmatrix} \alpha a_2 & 0 \\ 0 & \alpha b_2 \end{pmatrix}$

$= \alpha \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} + \alpha \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix}$

$= \alpha v_1 + \alpha v_2$

IV $(\alpha_1 + \alpha_2) v = (\alpha_1 + \alpha_2) \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$

$= \begin{pmatrix} (\alpha_1 + \alpha_2) a & 0 \\ 0 & (\alpha_1 + \alpha_2) b \end{pmatrix}$

$= \begin{pmatrix} \alpha_1 a + \alpha_2 a & 0 \\ 0 & \alpha_1 b + \alpha_2 b \end{pmatrix}$

$= \begin{pmatrix} \alpha_1 a & 0 \\ 0 & \alpha_1 b \end{pmatrix} + \begin{pmatrix} \alpha_2 a & 0 \\ 0 & \alpha_2 b \end{pmatrix}$

$= \alpha_1 \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + \alpha_2 \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$

$= \alpha_1 v + \alpha_2 v$

V> $(\alpha_1\ \alpha_2)\ v$ $= \alpha_1\ \alpha_2 \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$

$= \begin{pmatrix} \alpha_1\alpha_2\ a & 0 \\ 0 & \alpha_1\alpha_2 b \end{pmatrix}$

$= \alpha_1 \begin{pmatrix} \alpha_2\ a & 0 \\ 0 & \alpha_2\ b \end{pmatrix}$

$= \alpha_1 \left\{\alpha_2 \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right\}$

$= \alpha_1(\alpha_2\ v)$

VI> $1.\ v = 1\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$

$= \begin{pmatrix} 1.a & 0 \\ 0.1 & b \end{pmatrix}$

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

Hence V is a vector space.

Q .7 Let V be the set of all positive real numbers and R be the field of real numbers.

We define the following operations for any positive real numbers x and y

$x \oplus y = x.\ y$

and $a \odot x = x^a$, $a \in R$.

Then prove that V(R) is a vector space with $\oplus$ and $\odot$ as vector addition and scalar multiplication respectively.

Poof I i) Let x, y ϵ V

so x and y are real positive integer

so $x \oplus y = x.\ y$ is also a positive integer

i.e. $x \oplus y \in V$

$\Rightarrow$ V is closed for vector addition.

ii> For commutative -

x, y ϵ V

x $\oplus$ y = x. y

= y. x

= y $\oplus$ x

V is commutative for addition.

iii) For associative

Let x, y, z ϵV

then

(x $\oplus$ y) $\oplus$ z = (x. y) $\oplus$ z

= (x. y). z

= x. (y. z)

= x $\oplus$ (y $\oplus$ z)

iv) For additive identity

1 is a real positive number so 1 ϵ V.

Now 1 $\oplus$ x = 1. x = x

= x. 1 = x $\oplus$ 1

$\Rightarrow$ 1 is additive identity of V.

v) For inverse element

We know that if x is a real positive integer then $\frac{1}{x}$ is also real positive integer.

if x ϵ V $\exists$ $\frac{1}{x}$ ϵ V

s.t. x $\oplus \frac{1}{x}$ = x. $\frac{1}{x}$ = 1

$\Rightarrow$ every element of V has its additive inverse.

Hence (V, $\oplus$) is an abelian group.

II let $r \in R$ and $x \in V$

then $r \odot x = x^r \in V$

because we know that the value of a real power of real positive number is again a real positive number.

Hence V is closed for scalar multiplication

III $\alpha \odot (x \oplus y) = \alpha \odot (x.y)$

$= (x.y)^{\alpha}$

$= x^{\alpha}.y^{\alpha}$

$= (\alpha \odot x) \oplus (\alpha \odot y)$

IV $(\alpha + \beta) \odot x = (\alpha + \beta) \odot x$

$= x^{\alpha+\beta}$

$= x^{\alpha}.x^{\beta}$

$= (\alpha \odot x) \oplus (\beta \odot x)$

V> $\alpha \odot (\beta \odot x) = (\beta \odot x)^{\alpha}$

$= (x^{\beta})^{\alpha}$

$= x^{\alpha\beta}$

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

VI> $1 \odot x = x^1 = x$

Hence V is a vector space over R.

Q .8 If (V, $\oplus$) be a vector space over the field (F, +, ·) and $0^{\star}$ be the zero vector of V and 0 be the additive identity in F, then

i> $\alpha \odot 0^{\star} = 0, \quad \forall\, a \in F$

ii> $0 \odot v = 0^{\star}, \quad \forall\, v \in V$

iii> $(-\alpha) \odot v = -(\alpha \odot v), \quad \forall\, \alpha \in F, v \in V$

Proof **i>** Since $0^\star$ is zero element so

$$0 \oplus 0^\star = 0$$

Now $\alpha \odot (0 \oplus 0^\star) = \alpha \odot 0$

$$\Rightarrow (\alpha \odot 0) \oplus (\alpha \cdot 0^\star) = \alpha \odot 0$$

$$\Rightarrow (\alpha \odot 0) \oplus (\alpha \cdot 0^\star) = (\alpha \odot 0) \oplus 0$$

$$\Rightarrow \alpha \cdot 0^\star = 0$$

ii> $0 \odot v = (0 \oplus 0) \odot v$

$$= (0 \odot v) \oplus (0 \odot v)$$

$$\Rightarrow 0^\star \oplus (0 \odot v) = (0 \odot v) \oplus (0 \odot v)$$

$$\Rightarrow 0 \odot v = 0^\star$$

iii> $[\alpha + (-\alpha)] \odot v = (\alpha \odot v) \oplus (-\alpha \odot v)$

$$0 \odot v = (\alpha \odot v) \oplus [(-\alpha) \odot v]$$

$$0^\star = (\alpha \odot v) \oplus (-\alpha) \odot v$$

$\Rightarrow$ $(-\alpha) \odot v$ is inverse of $(\alpha \odot v)$ for $\oplus$

$\Rightarrow$ $(-\alpha) \odot v = -(\alpha \odot v)$

Q .9 **Define Vector Subspace.**

Prove that the necessary and sufficient conditions for a non-empty subset W of a vector space V(F) to be a subspace of V are

i> $w_1 \in W,\ w_2 \in W \Rightarrow w_1 - w_2 \in W$

ii> $\alpha \in F,\ w \in W \Rightarrow \alpha \odot w \in W$

Ans Let $(V, \oplus)$ be a vector space over a field $(F, +, \cdot)$ and $W \subset V$ then W is called vector subspace of V if

i> W is a vector space over F under the operation of V.

Proof of theorem –

Let W (F) be vector subspace of V (F) then $(W, \oplus)$ is abelian group

and W is closed for scalar multiplication.

so $w_1 \in W, w_2 \in W \Rightarrow w_1 \in W, -w_2 \in W$

$\Rightarrow w_1 \oplus (-w_2) \in W$

$\Rightarrow w_1 - w_2 \in W$

and $\alpha \in F, w \in W \Rightarrow \alpha \odot w \in W$

Sufficient condition –

Let $W \subseteq V, w \neq \emptyset$ and i> and ii> are satisfied then we have to prove that W is vector subspace of V.

Now $w \in W, w \in W \Rightarrow w - w \in W$

$\Rightarrow 0 \in W$

$\Rightarrow$ W has identity for addition

Now $0 \in w, \quad w \in W \Rightarrow 0 - w \in W$

$\Rightarrow -w \in W$

$\Rightarrow$ every element of W has its additive inverse.

Now $w_1 \in W, w_2 \in W \Rightarrow w_1 \in W, -w_2 \in W$

$\Rightarrow w_1 - (-w_2) \in W$

$\Rightarrow w_1 + w_2 \in W$

$\Rightarrow$ W is closed for addition.

Now since $W \subseteq V$ so every element of W is element V. And V is vector space so V is commutative and associative. Thus W is commutative and associative.

Hence $(W, \oplus)$ is abelian group.

ii) condition says that W is closed for scalar multiplication.

Since $W \subseteq V$ elements of W satisfies all postulats.

Hence W is itself a vector space over F

$\Rightarrow$ W (F) is vector subspace of V (F).

Q .10 Prove that the union of two subspaces W_1 and W_2 of a vector space V is a subspace iff either $W_1 \subseteq W_2$ or $W_2 \subseteq W_1$

Proof Let W_1 and W_2 be two subspaces of V s. t. either $W_1 \subset W_2$ or $W_2 \subset W_1$

then $W_1 \cup W_2 = W_2$ or $W_1 \cup W_2 = W_1$

$\Rightarrow W_1 \cup W_2$ is vector subspace of V.

Conversely –

Let $W_1 \cup W_2$ is vector subspace then we have to prove that $W_1 \subset W_2$ or $W_2 \subset W_1$

Let $W_1 \not\subset W_2$

$\Rightarrow \exists\ w_1 \in W_1$ and $w_1 \notin W_2$ ----------(1)

$\Rightarrow w_1 \in W_1 \cup W_2$

if $W_2 \not\subset W_1$ then $\exists\ w_2 \in W_2$ and $w_2 \notin W_1$

$\Rightarrow w_2 \in W_1 \cup W_2$ ----------(2)

but $w_1 \in W_1 \Rightarrow w_1 \in W_1 \cup W_2$

$w_2 \in W_2 \Rightarrow w_2 \in W_1 \cup W_2$

Now since $W_1 + W_2$ is a subspace so

$w_1 \in W_1 \cup W_2,\ w_2 \in W_1 \cup W_2 \Rightarrow w_1 + w_2 \in W_1 \cup W_2$

$\Rightarrow w_1 + w_2 \in W_1$ or $w_1 + w_2 \in W_2$

if $w_1 + w_2 \in W_1$ and $w_1 \in W_1 \Rightarrow -w_1 \in W_1$

$\Rightarrow (w_1 + w_2) - w_1 \in W_1$

$\Rightarrow w_2 \in W_1$

which is contradiction.

if $w_1 + w_2 \in w_2$ and $w_2 \in W_2 \Rightarrow -w_2 \in W_2$

$\Rightarrow (w_1 + w_2) + (-w_2) \in W_2$

$\Rightarrow w_1 \in W_2$

which is again contradiction

So our assumption is wrong.

$\Rightarrow \quad W_1 \subset W_2$ or $W_2 \subset W_1$

Q . 11 Show that the set

W = {(x, y, z) / x – 3y + 4z = 0, x y, z ϵ R} of 3 – tuples is a subspace of the vector space V_3 (R).

Ans W = {(x, y, z) / x – 3y + 4z = 0 , x, y, z ϵ R} and V_3 = {(x, y, z) / x, y, z ϵ R}

then we have to prove that W (R) is subspace of V_3 (R).

Let $w_1 = (x_1, y_1, z_1) \ \epsilon$ W

$w_2 = (x_2, y_2, z_2) \ \epsilon$ W

then $x_1 - 3y_1 + 4z_1 = 0 \ \Rightarrow \ x_1 = 3y_1 - 4z_1$

and $x_2 - 3y_2 + 4z_2 = 0 \ \Rightarrow \ x_2 = 3y_2 - 4z_2$

Let $\alpha, \beta, \epsilon R$

then $\alpha w_1 + \beta w_2 = \alpha (x_1, y_1, z_1) + \beta (x_2, y_2, z_2)$

$= \alpha (3y_1 - 4z_1, y_1, z_1) + \beta (3y_2 - 4z_2, y_2, z_2)$

$= (\alpha(3y_1 - 4z_1), \alpha y_1, \alpha z_1) + (\beta(3y_2 - 4z_2), \beta y_2, \beta z_2)$

$= (\alpha(3y_1 - 4z_1) + \beta (3y_2 - 4z_2), \alpha y_1 + \beta y_2, \alpha z_1 + \beta z_2)$

$= (3 (\alpha y_1 + \beta y_2) - 4 (\alpha z_1 + \beta z_2), \alpha y_1 + \beta y_2, \alpha z_1 + \beta z_2)$

Now $3 (\alpha y_1 + \beta y_2) - 4 (\alpha z_1 + \beta z_2) - 3(\alpha y_1 + \beta y_2) + 4 (\alpha z_1 + \beta z_2)$

$= 3\alpha y_1 + 3\beta y_2 - 4 \alpha z_1 - 4\beta z_2 - 3 \alpha y_1 - 3 \beta y_2 + 4 \alpha z_1 + 4 \beta z_2$

$= 0$

Thus $\alpha w_1 + \beta w_2 \epsilon$ W

$\Rightarrow$ W is vector subspace.

Q .12 If V(F) is a vector space over the field F . v_1 and v_2 are fixed elements of V, show that the set S = {$\alpha v_1 + \beta v_2 / \alpha, \beta \epsilon F \ v_1 \ v_2 \epsilon V$} is a subspace of V.

Ans V (F) is a vector space over F.

S= { $\alpha v_1 + \beta v_2 / \alpha, \beta \epsilon F, v_1 \ v_2 \epsilon V$}

then we have to prove that S is a vector subspace of V.

Let x, y ϵ S then

x = $\alpha_1 v_1 + \beta_1 v_2$, where $\alpha_1, \beta_1 \epsilon$ F

y = $\alpha_2 v_1 + \beta_2 v_2$, where $\alpha_2, \beta_2 \epsilon$ F

Let $\alpha, \beta, \epsilon F$

then $\alpha x + \beta y =$ $\alpha (\alpha_1 v_1 + \beta_1 v_2 + \beta (\alpha_2 v_1 + \beta_2 v_2)$

$= (\alpha \alpha_1 + \beta \alpha_2) v_1 + (\alpha \beta_1 + \beta \beta_2) v_2$ ----------(1)

here $\alpha, \beta, \alpha_1, \alpha_2, \beta_1, \beta_2 \epsilon F$ and F is

a field so $(\alpha \alpha_1 + \beta \alpha_2) \epsilon F$

and $(\alpha \beta_1 + \beta \beta_2) \epsilon F$

from (1)

$(\alpha \alpha_1 + \beta \alpha_2) v_1 + (\alpha \beta_1 + \beta \beta_2) v_2 \epsilon S$

$\Rightarrow$ $\alpha x + \beta y \epsilon S$

$\Rightarrow$ S is a subspace of V over F.

Unit – V

Vector Space and Subspace

Q.1 Define Linear Combination of vectors. In vector space V_3 (R) express v = (1, - 2, 5) as a linear combination of the given vectors v_1 = (1, 2, 3), v_2 = (2, -1, 1), v_3 = (1, 1, 1)

Ans Linear Combination –

Let V be a vector space over the field F. then if any element $v \in V$ can be written as

$v = \alpha_1 v_1 + \alpha_2 v_2 +$------$+ \alpha_n v_n$

where $\alpha_1, \alpha_2, \alpha_3$-------$\alpha_n \in F$

and v_1, v_2------$v_n \in$ V

then v is called linear combination

of v_1, v_2------v_n.

Let v_1 = (1, - 2, 5)

v is linear combination of v_1, v_2, v_3 if

$v = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3, \alpha_1, \alpha_2, \alpha_3 \in F$ ----------(1)

$\Rightarrow$ (1, - 2, 5) = α_1(1, 2, 3) +α_2(2, - 1, 1) + α_3(-1, 1, 1)

= (α_1+ 2α_2+α_3, 2α_1 - α_2+α_3, 3α_1 +α_2+α_3)

$\Rightarrow \alpha_1$+ 2α_2 +α_3 = 1----------(2)

2α_1 - α_2 + α_3= -2----------(3)

3α_1 + α_2 + α_3 = 5 ----------(4)

(1) - (2)

$\Rightarrow$ - α_1 + 3α_2 = 3 ----------(5)

(2) - (3)

$\Rightarrow$ $-\alpha_1 - 2\alpha_2 = -7$ ----------(6)

(5) - (6) $\Rightarrow$ $5\alpha_2 = 10$

$\Rightarrow \alpha_2 = 2$

from (5) $\alpha_1 = 3$

from (2) $\alpha_3 = -6$

using values of $\alpha_1, \alpha_2, \alpha_3$ in (1) , we get

$v = 3v_1 + 2v_2 - 6v_3$

which is Linear Combination of v.

Q.2 For which value of k will the vector

u = (5, k,7) ϵ V_3(R), is a linear combination of u_1 = (1, -5, 3) and u_2 = (3, 2, 1).

Ans. Let

$u = \alpha u_1 + \beta u_2$ --------(1)

$\Rightarrow$ (5, k,7) = α (1, -5, 3) + β (3, 2, 1)

= (α, -5 α, 3 α) + (3 β, 2 β, β)

(5, k,7) = (α+3 β, -5 α+2 β, 3 α+ β)

$\Rightarrow$ α+3 β = 5 ---------(2)

- 5 α+2 β = k ----------(3)

3 α+ β= 7 ----------(4)

from (2) - (3)$\times$ (4)

- 8 α = - 16

$\Rightarrow$ α = 2

from (1) β = 1

using values of α and β in (3)

- 10 + 2 = k

⇒ k = - 8

⇒ u is linear combination of u_1 and u_2 for k = - 8.

Q.3 Define Linear span. Show that the following vectors span the vector space V_3(R)

u_1 = (1, 2, 3), u_2 = (0, 1, 2), u_3 = (0,0,1)

Linear Span

Ans. Let V (F) be a vector space over F and S = $\{v_1, v_2 \text{-----} v_n\}$ be its non-empty subset then collection of all possible linear combination of finite elements of S is called linear Span L (S).

i.e.

$$L(S) = \left\{ \sum_{i=1}^{n} \alpha_i v_i \,/\, \alpha_i \epsilon F, i = 1, 2 \text{ ---} n \right\}$$

This is also called space generated by S.

Now we have to prove that L (S) = V_3 (R)

where S = $\{u_1, u_2, u_3\}$

u_1 = (1, 2, 3), u_2 = (0, 1, 2), u_3 = (0, 0, 1)

Let (x, y, z) ϵ V_3 (R)

then

(x, y, z) = $\alpha\, u_1 + \beta\, u_2 + \gamma\, u_3$

= α (1, 2, 3) + β (0, 1, 2) + γ (0, 0, 1)

= (α, 2 α + β, 3α +2 β + γ)

⇒ α = x

2 α + β = y

3α +2 β + γ= z

⇒ This is echelon.

α = x

β = y – 2x

γ = z – 3x – 2y

⇒ u_1, u_2, u_3 span V_3 (R)

Q .4 Define Linear dependence and Linear independence of vectors in vector space.

Ans **Linear dependence –**

Let V be a vector space over the field F and S = $\{v_1, v_2$-----$v_n\}$ be any subset of V then S is called linear dependent if there exist α_1, α_2-----α_n not all zero s.t.

$$\alpha_1 v_1 + \alpha_2 v_2 + \text{------}+\alpha_n v_n = 0$$

Linear independence

Let V be a vector space over the field F and S = $\{v_1, v_2$------$v_n\}$ be any subset of V then S is called linear independent if

$$\alpha_1 v_1 + \alpha_2 v_2 + \text{------}+\alpha_n v_n = 0$$

$$\Rightarrow \alpha_1 = \alpha_2 = \alpha_3\text{------} = \alpha_n = 0$$

Th* .1** ***The set of non-zero vectors v_1, v_2------v_n of a vector space V(F) is linearly dependent iff some v_K, $2 \le K \le n$ is a linear combination of the preceding ones.

Proof Firstly let $\{v_1, v_2$------$v_n\}$ is linearly dependent. Let K be the first integer for which v_1, v_2------v_K is linear dependent

i.e. $\alpha_1 v_1 + \alpha_2 v_2 + \text{-------}+\alpha_K v_K = 0$

⇒ where $\alpha_K \neq 0$

$$\Rightarrow v_K = -\frac{\alpha_1}{\alpha_K} v_1 + -\frac{\alpha_2}{\alpha_K} v_2 + \text{------}+ -\frac{\alpha_{K-1}}{\alpha_K} v_{K-1}$$

⇒ v_K is linear combination of its preceding

Conversely- Let any vector v_K be linear combination of its preceding ones.

i.e.

$$v_K = \alpha_1 v_1 + \alpha_2 v_2 + \text{------} + \alpha_{K-1} v_{K-1}$$

$$\Rightarrow \quad \alpha_1 v_1 + \text{------} + \alpha_{K-1} v_{K-1} + (-1)\, v_K = 0$$

$\Rightarrow$ there exist one coefficient (-1) which is not zero so $\{v_1, v_2\text{-----}v_K\}$ is linearly dependent.

$$\Rightarrow \quad \alpha_1 v_1 + \text{------} + (-1)\, v_K + \alpha_{K-1} v_{K-1} + \text{------} + \alpha_n v_n = 0$$

$\Rightarrow$ Since all coefficient are not zero so

$\{v_1, v_2\text{------}v_n\}$ is linearly dependent.

Th ***If V (F) is a vector space and S = $\{v_1, v_2\text{-----}v_n\}$ is a subset of some non-zero vectors of V, then S is L.D. iff some of elements of S can be expressed as a linear combination of the others.***

Proof Firstly let us assume S = $\{v_1, v_2\text{------}v_n\}$ is L.D. so there exist $\alpha_1, \alpha_2\text{------}\alpha_n$ not all zero s.t.

$$\alpha_1 v_1 + \alpha_2 v_2 + \text{-------} + \alpha_n v_n = 0 = \sum_{i=1}^{n} \alpha_i v_i = 0$$

$\Rightarrow$ Let $\alpha_K \neq 0$ then

$$\Rightarrow \quad \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1\, i \neq K}^{n} \alpha_i v_i + \alpha_K v_K = 0$$

$$\Rightarrow \quad v_K = - \sum_{i=1\, i \neq K}^{n} \frac{\alpha_i}{\alpha_K} v_K$$

$\Rightarrow v_K$ is linear combination of others

Conversely – let $v_K \in$ S which is linear combination of others i.e.

$$v_K = \beta_1 v_1 + \beta_2 v_2 + \text{------} + \beta_{K-1} v_{K-1} + \beta_{K+1} v_{K+1} + \text{------} + \beta_n v_n$$

$$\Rightarrow \quad \beta_1 v_1 + \text{------} + \beta_{K-1} v_{K-1} + (-1)\, v_K + \beta_{K+1} v_{K+1} + \text{------} + \beta_n v_n = 0$$

since coefficient of v_K is not zero

so $\{v_1, v_2\text{-----}v_n\}$ is linearly dependent.

Q .5 Prove that the four vectors v_1= (1, 0, 0) v_2= (0, 1, 0) v_3= (0, 0, 1) and v_4= (1,1,1) in V_3(C) form a L.D. set but any three of them are L.I.

Ans. Let $\alpha, \beta, \gamma, \delta \in C$ s.t.

$\alpha v_1 + \beta v_2 + \gamma v_3 + \delta v_4 = 0$

$\Rightarrow \alpha (1, 0, 0) + \beta (0, 1, 0) + \gamma (0, 0, 1) + \delta (1,1,1) = (0, 0, 0)$

$\Rightarrow (\alpha+ \delta, \beta+ \delta, \gamma+ \delta) = (0, 0, 0)$

$\Rightarrow \alpha = \beta = \gamma = - \delta$

Let $\delta = - 1$ then $\alpha = 1, \beta = 1, \gamma = 1$ s.t.

$\alpha v_1 + \beta v_2 + \gamma v_3 + \delta v_4 = 0$

so v_1, v_2, v_3, v_4 are L.D.

Now let

$\alpha v_1 + \beta v_2 + \gamma v_3 = 0$

$\Rightarrow \alpha (1, 0, 0) + \beta (0, 1, 0) + \gamma (0, 0, 1) = (0, 0, 0)$

$\Rightarrow (\alpha, \beta, \gamma) = (0, 0, 0)$

$\Rightarrow \alpha = 0, \beta = 0, \gamma = 0$

$\Rightarrow v_1, v_2, v_3$ are L.I.

Q .6 Define Basis and dimension of a vector space.

Prove that set S = {(1, 2, 1), (2, 1, 0) (1, -1, 2)} form a basis of V_3 (R).

Ans Basis –

Let V (F) be a vector space then a subset S of vectors of V is called basis of V if

i> S is Linearly independent

ii> S span V(F)

Dimension-

Number of elements in the basis of a vector space V (F) is called dimension of V.

It is denoted by

dim V

Now Let S = {(1, 2, 1), (2, 1, 0), (1, -1, 2)}

then we have to prove that S is basis of V. For this we will prove that

S is Li I and S pan V_3 (F).

Since $S \subseteq V_3$ (R)

Let α (1, 2, 1) + β (2, 1, 0) + γ (1, -1, 2) = (0, 0, 0)

$\Rightarrow$ $(\alpha + 2\beta + \gamma, 2\alpha + \beta - \gamma, \alpha + 2\gamma) = (0, 0, 0)$

$\Rightarrow$ $\alpha + 2\beta + \gamma = 0$

$2\alpha + \beta - \gamma = 0$

$\alpha + 2\gamma = 0 \quad \Rightarrow \alpha = -\gamma/2$

$\alpha = -\beta, \beta = 0$

$\Rightarrow$ $\alpha = 0, \beta = 0, \gamma = 0$

$\Rightarrow$ S is L.I

Now let $(\alpha, \beta, \gamma) \in V_3$ (R)

then (α, β, γ) = α (1, 0, 0) + β (0, 1, 0) + γ (0, 0, 1)

(1, 0, 0) = a (1, 2, 1) + b (2, 1, 0) + c (1, -1, 2)

$\Rightarrow$ (1, 0, 0) = (a + 2b +c, 2a + b – c, a + 2c)

$\Rightarrow$ a + 2b + c = 1

2a + b – c = 0

a + 2c = 0

$\Rightarrow$ a= $-\frac{2}{9}$, b = $\frac{5}{9}$, c = $1/9$

similarly (0, 1, 0) = $\frac{4}{9}$ (1, 2, 1) - $\frac{1}{9}$ (2, 1, 0) - $\frac{2}{9}$ (1, -2, 2)

(0, 0, 1) = $\frac{1}{3}$ (1, 2, 1) - $\frac{1}{3}$ (2, 1, 0) + $\frac{1}{3}$ (1, -1, 2)

so (α, β, γ) can be expressed as linear combination of vectors of S.

$\Rightarrow$ S is basis of V_3 (R)

Th.3 ***Prove that every finite dimensional vector space has a basis.***

Proof Let V (F) be a finite dimensional vector space and S = $\{v_1, v_2 \text{----} v_n\}$ be a finite subset of V s.t. L(S) = V.

Now either S is L.I or L.D.

If S is L.I then S is basis but if S is L.D. then there exist a vector $v_i \in$ S in such a way that it can be written as linear combination of its previous vectors.

Now we exclude v_i from S then

S – $\{v_i\}$ = S' has (n - 1) elements

S' also generate V i.e. L (S') = V

let $v \in$ V then

$v = \alpha_1 v_1 + \alpha_2 v_2 + \text{-------} + \alpha_n v_n$

but $v_i = \beta_1 v_1 + \text{------} + \beta_{i-1} v_{i-1}$

$\Rightarrow$ $v = \alpha_1 v_1 + \text{------} + \alpha_i(\beta_1 v_1 + \text{------} + \beta_{i-1} v_{i-1}) + \text{------} + \alpha_n v_n$

$= (\alpha_1 + \alpha_1 \beta_1) v_1 + \text{------} + (\alpha_{i-1} + \alpha_i \beta_{i-1}) v_{i-1}$

$+ \alpha_{i+1} v_{i+1} + \text{-----} + \alpha_n v_n$

$\Rightarrow$ v is linear combination of vectors

$v_1, v_2 \text{-----} v_{i-1}, v_{i+1} \text{------} v_n$

Thus L (S') = V

Now if S' is L.I then S' is basis but if it is L.D. then there exist an element a_j which is linear combination of its previous vectors.

Excluding this from S' we get a new set S'' of n – 2 elements.

Repeating this process we can get a subset of S which is L.I and generate V.

Morever we get a subset of S which has a single element and this is not zero element so this is L.I. and this span V.

so this is basis of V.

Th.4 ***If W is a subspace of a finite dimensional vector space V (F) then***

i> ***dim W ≤ dim V***

ii> ***W = V ⇒ dim V = dim W.***

Proof Let dim V = n and W be any subspace of V.

Since dim V = n so any set of (n +1) elements or more than (n +1) elements is L.D. so if let S = $\{v_1, v_2 \text{-----} v_m\}$ be greatest set of L.I. vectors where m ≤ n.

Now we want to prove that S is basis of W. S is L.I. Since W is greatest L.I. set so

$v, v_1, v_2 \text{-----} v_m$ is L.D.

⇒ $v \in$ W is linear combination of

$v_1, v_2 \text{-----} v_m$

⇒ L (S) = W

⇒ dim W = m where m ≤ n

⇒ dim W ≤ dim V

ii> if W= V then W is subspace of V and V is subspace of W so

dim W ≤ dim V and dim V ≤ dim W

⇒ dim V = dim W

Th.5 ***If S and T are finite-dimensional subspace of a vector space, then***

dim S + dim T = dim (S+T) + dim (S ∩ T).

Proof Let dim (S ∩ T) = K

and W = $\{\gamma_1, \gamma_2 \text{-----} \gamma_K\}$ is basis of S ∩ T.

then W ⊆S and W ⊆ T.

Since W ⊆S and W is L.I so W can be extended to basis of S let

$\{\gamma_1, \gamma_2\text{-----}\gamma_K, \alpha_1, \alpha_2\text{-----}\alpha_m\}$

be basis of S then dim S = m + K

Similarly W ⊆T and W is L.I so W can be extended to basis of S let

$\{\gamma_1, \gamma_2, \text{---}\gamma\text{----}\gamma_K, \beta_1 \text{-----}\beta_n\}$ be basis of T then dim T = K + n

Now dim S + dim T – dim (S ∩ T) =

= (m + K) + (n + k) – K

= m + n + K

Combining basis of S and T we get a

set $W_1 = \{\gamma_1, \gamma_2\text{---}\gamma_K, \alpha_1\text{----}\alpha_m, \beta_1\text{----}\beta_n\}$

Now we will prove that this is basis of (S+T). For this we will prove that

W_1 is L.I and L(W_1) = S+T.

Let $C_1\,\gamma_1 + C_2\,\gamma_2 + \text{------} + C_K\,\gamma_K + a_1\,\alpha_1 + \text{-----} + a_m\,\alpha_m$

$+ b_1\,\beta_1 + \text{-----} + b_n\,\beta_n = 0$

$$\Rightarrow \sum_{i=1}^{n} b_i\,\beta_i = -\sum_{i=1}^{K} C_i\,\gamma_i - \sum_{i=1}^{m} a_i\,\alpha_i \text{ ----------(1)}$$

$$\Rightarrow \text{Now } -\sum_{i=1}^{K} C_i\,\gamma_i - \sum_{i=1}^{m} a_i\,\alpha_i \in S$$

and $\sum_{i=1}^{n} b_i\,\beta_i \in T$

$$\Rightarrow \sum_{i=1}^{n} b_i\,\beta_i \in S \qquad \{\text{using (1)}$$

$$\Rightarrow \sum_{i=1}^{n} b_i\,\beta_i \in S \cap T$$

so $\sum_{i=1}^{n} b_i \beta_i = \sum_{i=1}^{K} d_i \gamma_i$

$\Rightarrow \quad b_1 \beta_1 + b_2 \beta_2 + \text{-----} + b_n \beta_n - d_1 \gamma_1 \text{ -----} d_K \gamma_R = 0$

but $\{\beta_1, \beta_2 \text{-----} \beta_n, \gamma_1 \text{----} \gamma_K\}$ is L.I. so

$b_1 = \text{-------} = b_n = d_1 = d_2 = \text{-------} = d_k = 0$

$\Rightarrow \quad b_1 = b_2 \text{-----} = b_n = 0$

using this in (1)

$C_1 \gamma_1 + C_2 \gamma_2 + \text{------} + C_K \gamma_K + a_1 \alpha_1 + \text{-----} + a_m \gamma_m = 0$

$\Rightarrow$ Since $\{\gamma_1, \gamma_2 \text{-----} \gamma_K, \alpha_1, \text{-----} \alpha_m\}$ is L.I

so $C_1 = C_2 = \text{-----} C_K = a_1 = a_2 = \text{-------} = a_m = 0$

Hence $\{\gamma_1, \text{-----} \gamma_K, \alpha_1 \text{-----} \alpha_m, \beta_1 \text{-----} \beta_n\}$ is L.I.

Let $\alpha \in$ S + T then

$\alpha =$ any element of S + any element of T

= linear combination of elements of basis

of S + linear combination of elements

of basis of T

$\Rightarrow \alpha =$ linear combination of elements of W_1

$\Rightarrow \alpha \in L(W_1)$

$\Rightarrow$ S + T $\subseteq L(W_1)$

but $L(W_1) \subseteq$ S + T

$\Rightarrow L(W_1) =$ S + T

thus dim (S + T) = K + m + n

Hence

dim S + dim T = dim (S + T) + dim (S $\cap$ T).

Th **.6** ***A vector space V(F) of dimension n is isomorphic to*** F^n

Proof Let $\{v_1, v_2 \text{-----} v_n\}$ be basis of V (F) then $v \in$ V can be expressed as

$v = \alpha_1 v_1 + \alpha_2 v_2 + \text{------} + \alpha_n v_n$ where $\alpha_{i \in F}$

Let us define a mapping

f: V $\rightarrow$ F^n s.t.

f $(v) = (\alpha_1, \alpha_2 \text{ -----} \alpha_n)$

For homomorphism

Let u, $v \in$ V then u = $\sum_{i=1}^{n} a_i v_i$, $v = \sum_{i=1}^{n} \beta_i v_i$

$$f(\lambda u + \mu v) = f\left[\lambda \sum_{i=1}^{n} a_i v_i + \mu \sum_{i=1}^{n} \beta_i v_i\right]$$

$$= f\left[\sum_{i=1}^{n} (\lambda a_i + \mu \beta_i) v_i\right]$$

$$= (\lambda a_1 + \mu \beta_1, \lambda a_2 + \mu \beta_2, \text{-----} \lambda a_n + \mu \beta_n)$$

$$= (\lambda a_1, \lambda a_2 \text{----- } \lambda a_n) + (\mu \beta_1, \text{----- } \mu \beta_n)$$

$$= \lambda (a_1, a_2 \text{-----} a_n) + \mu (\beta_1, \beta_2 \text{-----} \beta_n)$$

$$= \lambda \sum_{i=1}^{n} a_i v_i + \mu \sum_{i=1}^{n} \beta_i v_i$$

$$= \lambda f(u) + \mu f(v)$$

f is homomorphic

<u>For one-one</u>

Let f (u) = f (v)

$$\Rightarrow f\left(\sum_{i=1}^{n} a_i v_i\right) = f\left(\sum_{i=1}^{n} \beta_i v_i\right)$$

$$\Rightarrow (a_1, a_2 \text{-----} a_n) = (\beta_1, \beta_2 \text{-----} \beta_n)$$

$\Rightarrow \quad a_i = \beta_i$

$\Rightarrow \quad \sum_{i=1}^{n} a_i v_i = \sum_{i=1}^{n} \beta_i v_i$

$\Rightarrow$ u = v

$\Rightarrow$ f is one - one

For on-to Since for $(a_1, a_2 \text{-----} a_n) \in F^n$

then $\exists\, v \in V$ s.ϵ.

f (v) = $(a_1, a_2 \text{-----} a_n)$

$\Rightarrow$ f is on-to

Hence f is isomorphism.

Th.7 Prove that if W (F) is any subspace of a vector space V (F), then the set V/W of all cosets W + v, v being an arbitrary element of V, is a vector space over the field F for the addition and scalar multiplication compositions defined as follows

$(W + v_1) + (W + v_2) = W + (v_1 + v_2)$

$\alpha \cdot (W + v) = W + \alpha v \qquad v, v_1, v_2 \in V$

Proof We will prove that V/W is vector space

i> Commutative for addition

(W + u) + (W + v) = W + (u + v)

= W + (v + u) {V is commutative

= (W + v) + (W + v)

ii> Associative for addition

(W +u) + $[(W + v) + (W + w)]$ = (W + u) + [W + (v + w)]

= [W + (u + (v + w))]

= W + (u +v) + w

$= (W + u + v) + (W + w)$

$= [(W + u) + (W + v)] + (W + w)$

iii> additive identity

$0 \in V$ so $W + 0 \in V/W$

Now $(W + v) + (W + 0) = W + (v + 0) = W + v$

$W + 0$ i.e. W is additive identity.

iv> additive inverse

$v \in V \Rightarrow -v \in V \Rightarrow W + (-v) \in V/W$

Now

$(W + v) + (W + (-v)) = W + [v + (-v)]$

$= W + 0$

$\Rightarrow$ additive inverse of $W + v$ is $W + (-v)$ in V/W

$(\frac{V}{W}, +)$ is abelian group.

Now

i> $\alpha [(W + u) + (W + v)] = \alpha [W + (u + v)]$

$= W + \alpha (u + v)$

$= W + (\alpha u + \alpha v)$

$= (W + \alpha u) + (W + \alpha v)$

$= \alpha (W + u) + \alpha (W + v)$

ii> $(\alpha + \beta)(W + u) = W + (\alpha + \beta) u$

$= W + (\alpha u + \beta u)$

$= (W + \alpha u) + (W + \beta u)$

$= \alpha (W + u) + \beta (W + u)$

iii> $(\alpha \beta)(W + u) = W + \alpha \beta u$

$= \quad \alpha\,(W + \beta u) \;=\; \alpha\,[\beta\,(W + u)]$

iv) $1.\,(W + u) \;=\; W + 1.u \;=\; W + u$

Hence V/W is a vector space. This is called quotient space.

Th.8 ***If W (F) is a subspace of finite dimensional vector space V (F), then the quotient space (V/W) is also a finite dimensional and dim V/W = dim V – dim W.***

Proof Since W (F) is a subspace of finite dimension so let dim W = n with basis $\{w_1, w_2\text{-----}w_n\}$ since W is subspace of V so it can extened to basis of V

$\{w_1, w_2\text{-----}w_n, v_1, v_2\text{-----}v_m\}$

dim V = n + m

so any $v \in V$ can be expressed as

$v = \alpha_1 w_1 + \text{-----} + \alpha_n w_n + \beta_1 v_1 + \text{-----} + \beta_m v_m \;\; \alpha_i, \beta_i \in F$

$\Rightarrow$ $W + v = W + (\alpha_1 w_1 + \alpha_2 w_2 + \text{----} + \alpha_n w_n + \beta_1 v_1 + \text{-----} + \beta_m v_m)$

$= W + (\alpha_1 w_1 + \text{-----} + \alpha_n w_n) + W + (\beta_1 v_1 + \text{-----} + \beta_m v_m)$

$= W + (\beta_1 v_1 + \text{-----} + \beta_m v_m)$

$= \beta_1\,(W + v_1) + \beta_2\,(W + v_2) + \text{-----} + \beta_m\,(W + v_m)$

$\Rightarrow$ every element of V/W can be expressed as linear combination of $\{W+v_1, \text{-----} W+v_m\}$

Now we will prove that this is L.I.

Let $\alpha_1\,(W+v_1) + \alpha_2\,(W+v_2) + \text{-------} + \alpha_m\,(W+v_m) = W$

$\Rightarrow$ $W + (\alpha_1 v_1 + \alpha_2 v_2 + \text{-----} + \alpha_m v_m) = W$

$\Rightarrow$ $\alpha_1 v_1 + \alpha_2 v_2 + \text{-----} + \alpha_m v_m \in W$

$\Rightarrow$ $\alpha_1 v_1 + \text{------} + \alpha_m v_m = \beta_1 w_1 + \beta_2 w_2 + \text{-----} + \beta_n w_n$

$\Rightarrow$ $\beta_1 w_1 + \text{------} + \beta_n w_n + (-\alpha_1) v_1 + \text{------} + (-\alpha_m) v_m = 0$

$\Rightarrow$ $\beta_1 = \text{------} = \beta_n = \alpha_1 = \text{------} = \alpha_m = 0$

$\{\because \{w_1\text{-----}w_n, v_1\text{-----}v_m$ is L.I.$\}$

$\Rightarrow \quad \alpha_1 = \text{------} = \alpha_m = 0$

$\Rightarrow$ $\{W + v_1, W + v_2, \text{------} W + v_m\}$ is L.I.

Hence $\{W + v_1, W + v_2 + \text{------} W + v_m\}$ is basis of V/M

$\Rightarrow \dim V/M = m$

$= (m + n) - n$

$\Rightarrow \dim V/M = \dim V - \dim W$

****