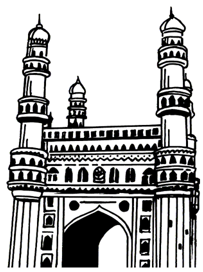
Rahul's ✔
Topper's Voice

AS PER CBCS SYLLABUS



B.Sc.

II Year IV Sem

Latest 2021-22 Edition

ALGEBRA

MATHEMATICS PAPER - IV

- **Study Manual**
- **FAQ's and Important Question**
- **Solved Problems**
- **Short Question & Answers**
- **Multiple Choice Questions**
- **Fill in the blanks**
- **Solved Previous Question Papers**
- **Solved Model Papers**

Syllabus covered for :
Osmania University
Kakatiya *University*
Mahatma Gandhi University
Palamuru University
Useful for :
Telangana University
Satavahana *University*

Price ` 159-00

Rahul Publications™
Hyderabad. Ph : 66550071, 9391018098

B.Sc.

II Year IV Sem

ALGEBRA

MATHEMATICS PAPER - IV

Price `. 159-00

Sole Distributors : ☎ : **66550071, Cell : 9391018098**

VASU BOOK CENTRE

Shop No. 3, Beside Gokul Chat, Koti, Hyderabad.

Maternity Hospital Opp. Lane, Narayan Naik Complex, Koti, Hyderabad.
Near Andhra Bank, Subway, Sultan Bazar, Koti, Hyderabad -195.

CONTENTS

ALGEBRA

MATHEMATICS PAPER - IV

STUDY MANUAL

SOLVED PREVIOUS QUESTION PAPERS

SOLVED MODEL PAPERS

SYLLABUS

UNIT - I

Groups: Definition and Examples of Groups - Elementary Properties of Groups- Finite Groups - Subgroups - Terminology and Notation - Subgroup Tests -Examples of Subgroups.

Cyclic Groups: Properties of Cyclic Groups -Classification of Subgroups Cyclic Groups.

UNIT - II

Permutation Groups: Definition and Notation - Cycle Notation - Properties of Permutations - A Check Digit Scheme Based on D5. Isomorphisms; Motivation - Denition and Examples - Cayley's Theorem Properties of Isomorphisms - Automorphisms - Cosets and Lagrange's Theorem Properties of Cosets 138 - Lagrange's Theorem and Consequences - An Application of Cosets to Permutation Groups - The Rotation Group of a Cube and a Soccer Ball.

UNIT - III

Normal Subgroups and Factor Groups: Normal Subgroups - Factor Groups - Applications of Factor Groups - Group Homomorphisms - Definition and Examples - Properties of Homomorphisms - The First Isomorphism Theorem.

Introduction to Rings: Motivation and Definition - Examples of Rings -Properties of Rings - Subrings.

Integral Domains: Definition and Examples -Fields - Characteristics of a Ring.

UNIT - IV

Groups: Definition and Examples of Groups - Elementary Properties of Groups - Finite Groups - Subgroups - Terminology and Notation -Subgroup Tests - Examples of Subgroups.

Cyclic Groups: Properties of Cyclic Groups -Classication of Subgroups Cyclic Groups.

Contents

UNIT - I

UNIT - II

Topic		Page No.

UNIT - III

UNIT - IV

Frequently Asked & Important Questions

UNIT - I

1. Prove that the set GL (2, R) = $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle/ a, b, c, d \in R, ad - bc \neq 0 \right\}$ is a non abelian group with respect to matrix multiplication.

Ans : **(May/June-2019)**

Refer Unit-I, Q.No.6

---

2. Let G be a group and let H be a non empty subset of G. If ab is in H whenever a and b are in H and a^{-1} is in H whenever a is in H then H is a subgroup of G.

Ans : **(June-2019)**

Refer Unit-I, Q.No.27

---

3. Let G be a group and let a be an element of order n in G, if $a^k = e$ then n divides K.

Ans : **(Jan.-2021)**

Refer Unit-I, Q.No.38

---

4. Let 'a' be an element of order n in a group and let k be a positive integer. Then prove that

(a) $\langle a^k \rangle = \langle a^{\gcd(n, k)} \rangle$ (b) $|a^k| = \dfrac{n}{\gcd(n, k)}$

Ans : **(Jan.-21)**

Refer Unit-I, Q.No.39

---

5. State and prove fundamental theorem of cyclic group.

Ans : **(Jan.-21)**

Refer Unit-I, Q.No.43

UNIT - II

1. Prove that for n > 1, A_n has order $\dfrac{n!}{2}$.

Ans : **(May/June-19)**

Refer Unit-II, Q.No.13

---

2. Let ϕ be an isomorphism from G to $\bar{G}$. If K is a subgroup of G. Then $\phi(k) = \{\phi(k) / k \in K\}$ is a subgroup of $\bar{G}$

Ans : **(Jan.-21)**

Refer Unit-II, Q.No.33

3. The set of Automorphism of a group and the set of inner Automorphism of group are both group under the operation of function composition.

Ans : **(Jan.-21)**

Refer Unit-II, Q.No.39

4. The order of a subgroup of a finite group divides the order of the group

Ans : **(Jan.-21, May/June-19)**

Refer Unit-II, Q.No.54

5. Prove that a group of prime order is cyclic.

Ans : **(Jan.-21)**

Refer Unit-II, Q.No.57

6. Prove that the group rotation of a cube is isomorphic to S_4.

Ans : **(May/June-19)**

Refer Unit-II, Q.No.67

UNIT - III

1. Prove that a subgroup N of a group G is a normal subgroup of G iff $g N g^{-1} = N \ \forall \ g \in G$.

Ans : **(May/June-19)**

Refer Unit-III, Q.No.5

2. If G is a group and N is a normal subgroup of G. Then prove that $\frac{G}{N} = \{Nx / x \in G\}$ forms a group w.r.to coset multiplication as the binary operation

Ans : **(Imp.)**

Refer Unit-III, Q.No.8

3. Let $f : G \to \bar{G}$ be an onto homomorphism then prove that f is an isomorphism iff $K = \{e\}$

Ans : **(Imp.)**

Refer Unit-III, Q.No.17

4. Fundamental theorem of homomorpic in group.

Ans : **(Imp.)**

Refer Unit-III, Q.No.20

5. A nonempty subset S of a ring R. is a subring if S is closed subtraction and multiplication i.e., (i) $a - b \in S$ (ii) $ab \in S$ when $a, b \in S$

Ans : **(Imp.)**

Refer Unit-III, Q.No.30

6. **Prove that $Q\left[\sqrt{2}\right] = \{a + b\sqrt{2} \,/\, a, b \in Q\}$ is a field with respect to ordinary addition and multiplication of numbers.**

Sol : **(Imp.)**

Refer Unit-III, Q.No.43

---

7. **The characteristic of an integral domain is the 0 or prime.**

Ans : **(Jan-21, May/June-19)**

Refer Unit-III, Q.No.46

---

8. **If D is an integral domain, Then prove that D[x] is an integral domain.**

Sol : **(May/June-19)**

Refer Unit-III, Q.No.48

---

9. **Prove that Z_3 [i] = {a + ib / a,b$\in Z_3$ } is a field of order 9?**

Sol : **(May/June-19)**

Refer Unit-III, Q.No.50

UNIT - IV

1. **Let R be a commutative ring with Unity and let A be an ideal of R. Then $\frac{R}{A}$ is an integral domain if and only if A is Prime**

Ans : **(May/June-19)**

Refer Unit-IV, Q.No.8

---

2. **Let R be a commutative ring with Unity and Let A be an ideal of R.**

Then $\frac{R}{A}$ is a field if and only if A is maximal.

Ans : **(Nov.-20)**

Refer Unit-IV, Q.No.10

---

3. **Let ϕ be a ring homomarphism from a ring R to a ring S. Let A be a subring of R and Let B be an ideal of S If ϕ is an isomurphism If and only if ϕ is onto and Ker $\phi = \{r \in R \,/\, \phi(r) = 0\} = \{0\}$**

Ans : **(May/June-19)**

Refer Unit-IV, Q.No.16

---

4. **Let R be a commutative Ring of characteristics 2,**

Then prove that the mapping $a \to a^2$ is a ring homomorphism from R to R.

Ans : **(Nov.-20)**

Refer Unit-IV, Q.No.22

5. Let ϕ be a ring homomorphism from Ring R to ring S. If R is commutative ring prove that $\phi(R)$ is commutative.

Ans : **(Jan.-21)**

Refer Unit-IV, Q.No.26

6. Prove that ring with unity contains z_n or z.

Ans : **(Jan.-21, May/June.-19)**

Refer Unit-IV, Q.No.27

7. Let ϕ be a ring homomorphism from a ring R to a ring S. Then Ker $\phi = \{r \in R / \phi(r) = 0\}$ is an ideal of R.

Ans : **(May/June-19)**

Refer Unit-IV, Q.No.28

8. If F is a field of characteristic zero then prove that F contains a subfield isomorphic to the rational numbers.

Ans : **(Jan.-21)**

Refer Unit-IV, Q.No.29

9. Show that the set $M_2(z)$ of 2 × 2 matrices with integer entries is a non commutative ring with unity.

Ans : **(Jan.-21)**

Refer Unit-IV, Q.No.32

10. Define ring homomorphism show that $\phi : C \to M_2[R]$ given by

$\phi(a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ $\forall$ a, b $\in$ R, is an isomorphism of C into M_2 [R].

Sol : **(May/June-19)**

Refer Unit-IV, Q.No.33

11. Prove that Z_7, the ring of integers modulo 7 is a field.

Ans : **(Jan.-21)**

Refer Unit-IV, Q.No.34

UNIT I	**Groups:** Definition and Examples of Groups - Elementary Properties of Groups- Finite Groups - Subgroups - Terminology and Notation - Subgroup Tests -Examples of Subgroups. **Cyclic Groups:** Properties of Cyclic Groups -Classification of Subgroups Cyclic Groups.

1.1 Groups

1.1.1 Binary Operation

Q1. Define binary operation with examples.

Ans :

A binary operation (*) on any non empty set 'G' is a mapping * : G × G $\rightarrow$ G is the Cartesian product of G into itself. They are also denoted by o, ., $\oplus$, etc.

Properties

(i) A binary operation (*) is commutative on a set 'G' iff

$$a * b = b * a \ \forall \ a, b \in G$$

(ii) A binary operation (*) is associative on a set 'G' iff

$$(a * b) * c = a * (b * c) \ \forall \ a, b, c \in G$$

Example

i) Natural numbers

$* = +$

$a \in N, b \in N$

$a + b \in N \Rightarrow \qquad 1 + 2 \in N$

$a = 1; b = 2 \qquad 3 \in N$

$1 * 2 \in N$

$2 \in N$

$\therefore$ + is binary operation on S

ii) N

$* = -$

$a \in N, b \in N$

$a * b \notin N$

$a - 1 \notin N$

$a = 1; b = 2$

$1 - 2 \notin N$

'–' is not binary operations on S

iii) Whole Numbers

$a * b \in N \qquad * = +$

$a = 1, b = 2$

$a + b \in W$

'+' is binary operation on W

iv) $a * b \in W$

$* = X$

$a = 1, b = 2$

$a * b = a \times b$

$= 1 \times 2$

$= 2 \in W$

$\therefore$ X is binary operation on W.

1.1.2 Definition and Examples of Groups

Q2. Write some examples of groups.

Ans :

Let 'G' be any non-empty set, * be binary operation on G. If (G, $*$) is said to be group it satisfies four properties.

1. Closure law
2. Associative law
3. Identity law
4. Inverse law

1. Closure Law

If 'G' is any non-empty set and '*' is binary operation, then for $a \in G$, $b \in G \Rightarrow a * b \in G$ it is called closure law.

Note: If '$*$' is a binary operation on G if and only if it satisfies closure law.

Ex: (N, +) (R, –)

2. Associative Law

If '*' is any binary operation on non empty set 'G' If $a,b,c \in G$; $(a * b) * c = a * (b * c)$ is called associative law, otherwise '$*$' is not satisfies associative law on G.

Example

i) N

$* = +$

$a = 2, b = 3, c = 5$

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

$(2+3)+5 = 2+(3+5)$

$5+5 = 2+8$

$10 = 10$

'+' satisfies associative law on N.

Q = Rational

$* = -$

$a = \frac{5}{3}, b = \frac{10}{3}, c = -\frac{7}{2}$

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

$$\left(\frac{5}{3}-\frac{10}{3}\right)-\left(-\frac{7}{2}\right) = \frac{5}{3}-\left(\frac{10}{3}+\frac{7}{2}\right)$$

$$-\frac{5}{3}+\frac{7}{2}=\frac{5}{3}-\left(\frac{20+21}{6}\right)$$

$$-\frac{10+21}{6} = \frac{5}{3}-\frac{41}{6}$$

$$\frac{11}{6} = \frac{10-41}{6}$$

$$\frac{11}{6} \pm -\frac{31}{6}$$

$\therefore$ – does not satisfies associative law on Q.

3. Identity Law

Let 'G' be any non empty set and '*' be any binary operation on G. $\forall a \in G\ \exists e \in G \ni e * a = a * e = a$. Here 'e' is called identity element.

Eg:

i) (N, •), '1' is identity element

$a = 2$

$1 \times 2 = 2 \times 1 = 2$

$a = 3 \Rightarrow 1 \times 3 = 3 \times 1 = 3$

$\therefore$ (N, •) here '1' is identity element

ii) (W, +) + {0, 1, 2, ...}

$0 + 2 = 2 + 0 = 2$

$\therefore$ (W, +) has an identity with respect to addition i.e., '0'

Note:

(i) '0' is called additive identity element.

(ii) '1' is called multiplicative identity element.

4. Inverse Law

An element 'a' is said to be invertible $\exists x \in G \ni x * a = e = a * x$, here 'a' is called invertible, 'x' is inverse of a.

i.e., $a^{-1} * a = e = a * a^{-1}$

Q3. Define Commutative Law with an example.

Ans :

Let 'G' be any non empty set, $*$ be binary operation on G. Hence '$*$' is commutative on G.

If $a, b \in G \Rightarrow a * b = b * a$

Example :

1. (Z, +) is an abelian group

We know that (Z, +) is group

$\forall$ a, b, $\in$ Z $\Rightarrow$ a + b = b + a

$\Rightarrow$ Satisfies commutative property

$\therefore$ (Z, +) is abelian group.

Key Point :

1. Let $R^* = R - \{0\}$ set of all non zero real number. Then $(R^+, \cdot)$ is a group.
2. Let $R^* = Q - \{0\}$ = set of all non zero rational numbers then $(Q^*, \cdot)$ is a group.

1.1.3 Elementary Properties of Groups

Q4. What are the Elementary Properties of Groups?

Ans :

(i) Uniqueness of the Identity

It states that "in a group G, there exists only one identity element".

(ii) Cancellation Laws

Let a, b, c be the elements of a group G.

$ba = ca \Rightarrow b = c$ (Right cancellation law)

$ab = ac \Rightarrow b = c$ (Left cancellation law)

(iii) Uniqueness of Inverse

It states that "For each element a in a group G, there is a unique element b in G such that $ab = ba = e$".

(iv) If a, b are the elements of a group G, then $(ab)^{-1} = b^{-1} a^{-1}$.

Q5. A rectangular array of the form $\begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{bmatrix}$ is called 2 × 2 matrix. Prove that the array is group under addition.

Ans :

Given array is $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle/ a, b, c, d \in R \right\}$$

Required to prove that (G, +) is a group.

Let us consider,

$$A_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \ A_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

Where $A_1, A_2, A_3, \in G$

To prove (G, +) is group

It is enough to prove the following properties.

1. Closure Properties :

$\forall A_1, A_2, \in G \rightarrow A_1 + A_2 \in G$

$$\Rightarrow \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} \in G$$

2. Associate Property :

$\forall A_1, A_2, A_3 \in G$

$\Rightarrow A_1 + (A_2 + A_3) = (A_1 + A_2) + A_3$

$$\Rightarrow \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \left\{ \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right\}$$

$$= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 + a_3 & b_2 + b_3 \\ c_2 + c_3 & d_2 + d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 + a_2 + a_3 & b_1 + b_2 + b_3 \\ c_1 + c_2 + c_3 & d_1 + d_2 + d_3 \end{bmatrix}$$

Similarly

$(A_1 + A_2) + A_3$

$$= \begin{bmatrix} a_1 + a_2 + a_3 & b_1 + b_2 + b_3 \\ c_1 + c_2 + c_3 & d_1 + d_2 + d_3 \end{bmatrix}$$

$\therefore A_1 + (A_2 + A_3) = (A_1 + A_2) + A_3$

3. Identity Property :

Identity element under addition is '0'

So, here identity of 2 × 2 matrix is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$\Rightarrow \ni A_1 + I = I + A_1 = A_1$

$$\Rightarrow \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

4. Inverse Property :

Inverse of element 'a' under addition is '–a'

So, Let $A_1 \in G$

$\Rightarrow$ $A + (-A_1) = (-A_1) + A_1 = e$

$\Rightarrow$ $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix}$ which is an inverse of a matrix A_1

$\Rightarrow$ $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = e$

$\therefore$ 2 × 2 is satisfies the all above 4 properties under addition

$\therefore$ $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is group under addition

---

Q6. Prove that the set GL (2, R) = $\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Big/ a, b, c, d \in R, ad - bc \neq 0\right\}$ is a non abelian group with respect to matrix multiplication.

Ans : **(May/June-2019)**

Given set is GL (2, R)

$= \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Big/ a, b, c, d \in R, ad - bc \neq 0\right\}$

Required to prove GL(2, R) is a non abelian group under multiplication :

Which is enough to prove that not a commutative property.

Let $A_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $A_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ &

$A_3 = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \in R$

1. Closure Properties :

Let $A_1, A_2, \in G \Rightarrow A_1 \cdot A_2$

$\Rightarrow$ $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} \in R$

2. Associative Property :

Clearly, Associative property satisfies

$\forall$ $A_1, A_2, A_3 \in G \Rightarrow A_1 (A_2 A_3) = (A_1 A_2) A_3$

In matrix multiplication. The associative property satisfies.

3. Identity Property :

Identity of matrix under multiplication is $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$

$\forall\ A_1 \in G \Rightarrow A_1 I = I A_1 = A1$

$$\Rightarrow \begin{bmatrix}a_1 & b_1\\c_1 & d_1\end{bmatrix}\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = \begin{bmatrix}a_1 & 0\\0 & d_1\end{bmatrix} \in G$$

4. Inverse Property :

Inverse of $\begin{bmatrix}a & b\\c & d\end{bmatrix}$ is $\Rightarrow$ Let $A = \begin{bmatrix}a & b\\c & d\end{bmatrix}$

$|A| = ad - bc \neq 0$

$$\frac{1}{|A|}\begin{bmatrix}d & -b\\-c & a\end{bmatrix} = \begin{bmatrix}\frac{b}{ad-bc} & \frac{-b}{ad-bc}\\ \frac{-c}{ad-bc} & \frac{a}{ad-bc}\end{bmatrix}$$

$\therefore$ GL (2, R) is a group

5. Commutative Property :

In general matrix multiplication need not to be commutative.

For example : 2 × 2 matrix

Let $A_1 = \begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}$, $A_2 = \begin{bmatrix}4 & 2\\3 & 1\end{bmatrix}$

$A_1 A_2 = A_2 A_1$

$$\Rightarrow \begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}4 & 2\\3 & 1\end{bmatrix} = \begin{bmatrix}4+6 & 2+2\\12+12 & 6+4\end{bmatrix}$$

$$A_1 A_2 = \begin{bmatrix}10 & 4\\24 & 10\end{bmatrix}$$

$$A_3 A_1 = \begin{bmatrix}4 & 2\\3 & 1\end{bmatrix}\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix} = \begin{bmatrix}4+6 & 8+8\\3+3 & 6+4\end{bmatrix}$$

$$= \begin{bmatrix}10 & 16\\9 & 10\end{bmatrix}$$

$\therefore\ A_1 A_2 \neq A_2 A_1$

$\therefore$ GL (2, R) is not an abelian group.

So, which is a non abelian group under matrix multiplication.

Q7. Prove that the set of R* of non zero real numbers is an abelian group under ordinary multiplication.

Ans :

Given set is R* $\Rightarrow$ non zero real number

i.e., $R^* = R - \{0\}$

Required to prove R* is abelian group under multiplication.

So, it is enough to prove the following properties.

1. Closure Property :

Let $a, b, \in R - \{0\}$

$\Rightarrow\ a . b \in R - \{0\}$

Let $a = 1, \quad b = 2$

$\Rightarrow\ a. b = 1(2) = 2 \in R^*$

2. Associative Property

Let $a, b, c \in R^* \Rightarrow a(bc) = (ab) . c$

Let us consider $a = 1,\ b = 2,\ c = 3$

$a(b c) = 1(2 . 3) \Rightarrow 1(6) = 6$

$(a . b) . c = (1 . 2) . 3 \Rightarrow 2 . 3 = 6$

$\therefore\ a . (b . c) = (a . b) . c$

3. Identity Property :

Identify element under multiplication is '1'

So, let $a = 2,\ I = 1$

$\forall\ a . I = I . a = a \qquad \forall a \in R^*$

$a . I = 2 . 1 = 2$

$I . a = 1 . 2 = 2$

4. Inverse Property :

Inverse element 'a' under multiplication is $\frac{1}{a}$.

$\forall\ a . \frac{1}{a} = \frac{1}{a} . a = I \qquad a \in R^*$

Let a = 2

$$2 . \frac{1}{2} = \frac{1}{2} . 2 = 1 \in I$$

∴ R* is forms a group

To prove R* is abelian group

It is enoug to prove commutative property.

$\forall$ a, b $\in$ R* $\Rightarrow$ a . b = b . a

Let a = 1, b = 2

a . b = 1 . 2 = 2 $\in$ R*

b . a = 2 . 1 = 2 $\in$ R*

∴ R* of non zero real numbers also satisfies the commutative property.

∴ R* is forms a abelian group under multiplication.

1.1.4 Addition Modulo "$\oplus$" and Multiplication Modulo "$\otimes$"

Q8. Define Addition Modulo.

Ans :

If a and b are any two integers and m is a fixed positions integer. Then a + b under addition modulo 'm' is denoted by a $\underset{m}{\oplus}$ b and it is defined as, a $\underset{m}{\oplus}$ b = a + b if a + b < m

$$a \underset{m}{\oplus} b = r$$

where 'r' is the least non negative ($\geq$ 0) reminder by dividing a + b by m if

a + b $\geq$ m.

Example :

1. $2 \underset{3}{\oplus} 7 = 0$

(i) 2 + 7 = 9

(ii) a + b $\geq$ m $\Rightarrow$ 9 $\geq$ 3

(iii) divide $\frac{9}{3}$ $\Rightarrow$ reminder '0'

2. $3 \underset{4}{\oplus} 1 = 0$

3. $3 \underset{5}{\oplus} 3 = 1$

Q9. Define multiplication modulo.

Ans :

If a and b are any two integers.

Then a into b under multiplication modulo 'm' is denoted by a $\underset{m}{\otimes}$ b and is defined as

$$a \underset{m}{\otimes} b = a \times b \quad \text{if} \quad a \times b < m$$

$$a \underset{m}{\otimes} b = r$$

where

'r' is a the least non negative reminder obtained by dividing

a × b by m if a × b $\geq$ m

Example :

1. $2 \underset{4}{\otimes} 8 = 0$

(i) 2 × 8 = 16

(ii) 16 $\geq$ 4

(iii) $\frac{16}{4}$ $\Rightarrow$ reminder '0'

2. $2 \underset{4}{\otimes} 4 = 2$

(i) 2 × 4 = 8

(ii) 8 > 6

(iii) $\frac{8}{6}$ reminder is '2'

Q10. Define Cayley's Table.

Ans :

Sometimes an operation $*$ on a finite set conveniently be specified by a table called the composition table.

The construction of composition table is explained below :

Let $S = \{a_1, a_2 ... a_i, a_j ... a_n\}$ be a finite set with 'n' elements.

Let a table with n + 1 rows & n + 1 columns be taken.

Let the squares in the first row be filled in with $a_1, a_2, ..., a_n$ & the squares in the first column be filled in with $a_1, a_2, ..., a_n$

Let a_i $(1 \leq i \leq n)$ and a_j $(1 \leq j \leq n)$ be any two elements of S.

Let the product $a_i * a_j$ obtained by operating a_i with a_j be placed in the square which is at the integer section of the row headed by a_i and the column headed by a_j.

Q11. Check G {0, 1, 2, 3} is a group under multiplication modulo 4.

Ans :

G = {0, 1, 2, 3} under multiplication modulo '4'.

By composition table :

$\otimes_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

To check G is group or not. It is enough to satisfies the given following properties.

1. Closure Property :

This property satisfies, as the all entries in the table are the elements of G.

2. Associative Property :

$\forall$ a, b, c $\in$ G

$\Rightarrow$ $(a \otimes_4 b) \otimes_4 c = a \otimes_4 (b \otimes_4 c)$

which leaves the same reminder when divided by '4'.

3. Identity Property :

Since the top most row coincide with the second row corresponding to the elements 1. We have e = 1 is the identity element.

4. Inverse Property :

From the composition table, it is clear that the Inverse of 1 is 1,

Inverse of 3 is 3.

where the inverse of '0' and '2' can't find the it

$\therefore$ Here Inverse Property is does not exists in G.

$\therefore$ G is not group under multiplication modulo '4'.

Q12. Show that {1, 2, 3} under multiplication modulo 4 is not a group but that {1, 2, 3, 4} under multiplication modulo 5 is a group.

Ans :

G = {1, 2, 3}

(i) To show that 'G' is multiplication modulo 4 is not group.

By composition table

$\otimes_4$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

1. Closure Property :

By the given table, we can observe that, all the entries of the table except '0' is included in the set 'G'.

So, here closure property is not satisfies as closure property not satisfied. Then we need not to proceed for other property.

$\therefore$ G = {1, 2, 3} is not group under multiplication modulo 4.

(ii) To prove that 'G' is multiplication modulo '5' is group.

G = {1, 2, 3, 4}

By composition table

$\otimes_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1. Closure Property :

This property satisfies, as the all entries in the table are the elements of G.

2. Associative Property :

$\forall$ a, b, $\in$ G

$\Rightarrow$ $(a \underset{4}{\otimes} b) \underset{4}{\otimes} c = a \underset{4}{\otimes} (b \underset{4}{\otimes} c)$

which leaves the same reminder when divided by 5

3. Identity Property :

Since the top most row coincide with the 1st row corresponding elements we have e = 1 is the identity element.

4. Inverse Property :

From the composition table, It is clear that the

Inverse of 1 is 1

Inverse of 2 is 3

Inverse of 3 is 2

Inverse of 4 is 4

$\therefore$ Under multiplication modulo 5, each element has inverse.

$\therefore$ All 4 properties are satisfied.

Then G = {1, 2, 3, 4} is a group under multiplication modulo '5'.

Q13. Show that the set {5, 15, 25, 35} is a group under multiplication modulo 40. What is the identity element of this group ?

Ans :

G = {5, 15, 25, 35} under multiplication modulo 40.

Required to prove (G, $\otimes_{40}$) is a group

By composition table

$\underset{40}{\otimes}$	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

1. Closure Property :

This property is satifices, as all entries in the table are the elements of 'G'.

2. Associative Property :

$\forall$ a, b, c $\in$ G

$\Rightarrow$ $(a \underset{40}{\otimes} b) \underset{40}{\otimes} c = a \underset{40}{\otimes} (b \underset{40}{\otimes} c)$

which leaves the same reminder when divided by '40'.

3. Identity Property :

Since the top most row coincide with the 3rd row corresponding elements. e = 25 is an identity element of the group.

4. Inverse Property :

From the composition table, It is clear that the inverse of 5 is 25

Inverse of 15 is 15

Inverse of 25 is 25

Inverse of 35 is 35

$\therefore$ G is group under multiplication modulo '40'. and the identity element of this group is '25'.

Q14. What is Relatively prime ?

Ans :

If n is a positive integer. Then, we define U(n) = Set of all positive integers less than n and relatively prime 'n'

Relatively Prime :

If two integers are said to be relatively prime if there gcd is 1.

Q15. Show that (U(10), $\underset{10}{\otimes}$) is a group.

Ans :

Here U(10) = Set of all positive integers less than 10 and relatively prime '10'

$\therefore$ U(10) = {1, 3, 7, 9}

By composition table

$\underset{10}{\otimes}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

1. Closure Property :

Closure property is satisfied, since all the elements are present in the U(10)

2. Associative Property :

$\forall$ a, b, c $\in$ U(10)

$\Rightarrow$ $(a \underset{10}{\otimes} b) \underset{10}{\otimes} c = a \underset{10}{\otimes} (b \underset{10}{\otimes} c)$

which leaves the same reminder when divided by '10'.

3. Identity Property :

Identity element under multiplication is '1'. Since the top most row coincide with first row corresponding element.

4. Inverse Property :

From the composition table, It is clear that the

Inverse of 1 is 1

Inverse of 3 is 7

Inverse of 7 is 3

Inverse of 9 is 9

$\therefore$ All 4 properties are satisfied. Then U(10) form a group under multiplication modulo '10'.

Q16. Prove that {1, 2, 3, ... n – 1} is a group under multiplication modulo 'n'.

Ans :

Let Z_n = {1, 2, 3, ... n – 1}

Required to show that (Z_n, $\otimes_n$) is a group.

Key Points :

1. If n is prime number and if n/ab $\Rightarrow$ n/a or n/b
2. A prime number n does not divide 'a' where $1 \leq a \leq p - 1$

1. Closure Property :

$\forall$ a, b $\in Z_n \Rightarrow a \underset{n}{\otimes} b = r \in Z_n$

where $1 \leq r \leq n - 1$

where r = 0 is not possible because 'n' does not divide a × b

2. Associative Property :

$\forall$ a, b, c $\in Z_n$

$\Rightarrow$ $(a \underset{n}{\otimes} b) \underset{n}{\otimes} c = a \underset{n}{\otimes} (b \underset{n}{\otimes} c)$

which leaves the reminder when divided by 'n'

3. Identify Property :

Let $a \in Z_n \ \exists\ e = 1 \in Z_n \ \exists\ a \underset{n}{\otimes} 1$

$= 1 \underset{n}{\otimes} a = a$

4. Inverse Property :

Let $S \in Z_n$ $(1 \leq S \leq n - 1)$

Now, consider the products

$1 \underset{n}{\otimes} S,\ 2 \underset{n}{\otimes} S,\ \ldots\ (n - 1) \underset{n}{\otimes} s$

The above product are elements of Z_n by closure property.

Also, we have the above products are distinct. Because,

If $i \underset{n}{\otimes} S = j \underset{n}{\otimes} S$ where $i \neq S$

$\Rightarrow$ P / (i × S – j × S)

$\Rightarrow$ P / S (i – J)

$\Rightarrow$ P / i – j or P / S

Which is not possible because 'n' cannot divide i – j and 'n' cannot divide 'S' because 1 $\leq$ i – j $\leq$ n – 1, 1 $\leq$ S $\leq$ n – 1

$\therefore$ The product $1 \underset{n}{\otimes} S,\ 2 \underset{n}{\otimes} S, \ldots (n-1) \underset{n}{\otimes} S.$

are distinct,

Since as the elements of Z_n

We have $S' \underset{n}{\otimes} S = 1$

Where $1 \leq S' \leq n - 1$

$\Rightarrow$ S' is the inverse of S

$\therefore$ $(Z_n, \underset{n}{\otimes})$ is group.

Q17. In a group G, there is a only one identity element.

Ans :

Given that (G, •) is a group.

Assume e & e' are the identity elements

Since e is identity element of G

$\forall$ a $\in$ G $\exists$ e $\in$ G

$\Rightarrow$ a . e = e . a = a ... (1)

Similarly

e' $\in$ G $\ni$ a . e' = e' . a = a ... (2)

By (1) $\Rightarrow$ a . e = a Put a = e'

e' . e = e' ... (3)

By (2) $\Rightarrow$ e' . a = a Put a = e

e' . e = e ... (4)

From equation (3) and (4), e' = e

$\therefore$ We can conclude that

There is a only one identity element in a group G.

Q18. Define Cancellation Laws.

Ans :

If a, b $\in$ G.

Then we define cancellation law holds.

1. Left cancellation law

   a . b = a . c

   b = c

2. Right cancellation law

   b . a = c . a

   b = c where a $\neq$ 0

Q19. In a group G the left & right cancellation laws hold i.e.,

(i) a . b = a . c $\Rightarrow$ b = c

(ii) b . a = c . a $\Rightarrow$ b = c

Ans :

Given that (G, •) is a group

Left cancellation law : Let a, b, c $\in$ G

$\Rightarrow$ a . b = a . c ... (1)

Since a $\in$ G and G is a group

$\Rightarrow$ $a^{-1} \in G$

Multiply equation (1) with a^{-1}

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

$(a^{-1}a)$. b = $(a^{-1}.a)$ c $\rightarrow$ [by Associative property (ab) c = a(bc)]

e . b = e . a $\rightarrow$ $a^{-1}a = e = aa^{-1}$

$\Rightarrow$ b = c $\rightarrow$ [By Identity property a . e = e . a = a

$\therefore$ Left cancellation law proved

Right Cancellation Law :

Let a, b, c $\in$ G

$\Rightarrow$ b . a = c . a ... (2)

a $\in$ G and G is a group

$\Rightarrow$ $a^{-1} \in G$

Multiply a^{-1} to equation (2) on right side

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

$b(aa^{-1}) = c(aa^{-1})$ By Associative property

$b.e = c.e$

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

$a.e = e.a = a$

$\therefore$ Right cancellation law proved.

Q20. For each element in a group G there is a unique element b in G such that

ab = ba = e

Ans :

Let $a \in G$

Given that $a . b = b . a = e$ ... (1)

$\Rightarrow$ b is a inverse of a

Suppose that

c is also inverse of $a \in G$

$\Rightarrow$ $a . c = c . a = e$ ... (2)

From (1) and (2) $a . b = a . c$

By left cancellation law

$b = c$

Q21. For group elements a & b,

$(ab)^{-1} = b^{-1}\, a^{-1}$

Ans :

Suppose that $(G, \cdot)$ is a group

$a, b \in G$

Required to prove $(ab)^{-1} = b^{-1}a^{-1}$

Since $a, b \in G \Rightarrow a . b \in G$

(Closure property)

$a \in G \Rightarrow b^{-1} \in G$

$b \in G \Rightarrow b^{-1} \in G$

$\therefore$ $b^{-1} \in G,\ a^{-1} \in G \Rightarrow b^{-1} . a^{-1} \in G$

(Closure property)

Let $ab = c$ and $b^{-1}a^{-1} = d$

To prove $(a\, b)^{-1} = b^{-1}\, a^{-1}$

It is enough to prove $c^{-1} = d$

$\Rightarrow$ $c\, d = e$

Consider

$c.d \Rightarrow (ab)\, (b^{-1}a^{-1})$

$= [(ab)\, b^{-1}]\, a^{-1}$ Associative property

$= [a\, (bb^{-1})\, a^{-1}$ Associative property

$= [ae]a^{-1}$ $bb^{-1} = b^{-1}b = e$

$= aa^{-1}$ $a.e = e.a = G$

$cd = e$

$c^{-1} = d$

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

Hence proved

Q22. Prove that in a group $(a^{-1})^{-1} = a\ \forall\ a$

Ans :

By the definition of Inverse

$\forall\ a \in G \Rightarrow aa^{-1} = a^{-1}\, a = e$

Inverse of $a^{-1} = a$

$(a^{-1})^{-1} = a$

1.2 Finite Groups : Subgroups

Q23. Define order of a group with example.

Ans :

If $(G, \cdot)$ is a group then the number of elements of a group (finite or infinite) is called its order.

It is denoted as the order of G (or) $|G|$

Example :

$U(10) = \{1, 3, 7, 9\}$ is a group

Then the order of G $\Rightarrow$ $|G| = 4$

1.2.1 Order of Element

Q24. Define order of element with example.

Ans :

The order of element 'a' in a group G is a smallest positive integer n such that $a^n = e$. Then we say that 'a' has infinite order. The order of an element 'a' is denoted by $|a|$.

Example :

U(15) = {1, 2, 4, 7, 8, 9, 11, 13, 14} under the multiplication modulo 15. Here order 8.

The order of element 7 is

$7^1 = 7$

$7^2 = 4$

$7^3 = 13$

$7^4 = 1$

So, $|7| = 4$

1.3 Subgroup Tests - Examples of Subgroups

Q25. What is subgroup.

Ans :

Let (G, ·) be a group. Let H be a nonempty subset of G such that (H, ·) be a group then H is called subgroup of G and it is denoted by $H \le G$.

Q26. Let G be a group and H a non empty subset of G. If ab^{-1} is in H, then H is a subgroup of G.

Ans :

Given that (G, ·) is a group

and 'H' is nonempty subset of G

Required to prove H is a subgroup of G

$\Leftrightarrow \quad ab^{-1} \in H \quad \forall\ a, b \in H$

Suppose that

H is subgroup of G, Prove that $ab^{-1} \in H$ $\forall\ a, b \in H$

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

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

Conversely suppose that,

$\forall\ a, b \in H \Rightarrow ab^{-1} \in H$ ... (1)

Prove that H is a subgroup of G

(a) Associative Property :

$\forall\ a, b, c \in H \Rightarrow (a.b) . c = a(b.c)$

(b) Identity Property :

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

$= e \in H$ ... (2)

(c) Inverse Property :

$e \in H$ by (2)

$e \in H,\ a \in H \Rightarrow e.a^{-1} \in H$ by (1)

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

$\therefore \quad \forall\ a \in H \Rightarrow a^{-1} \in H$ ... (3)

(d) Closure Property :

$\forall\ a, b \in H \Rightarrow a.b \in H$

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

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

$= ab \in H$

Q27. Let G be a group and let H be a non empty subset of G. If ab is in H whenever a and b are in H and a^{-1} is in H whenever a is in H then H is a subgroup of G.

Ans : **(June-2019)**

Given that H is a non empty subset of G

Required to prove H is a subgroup of G

$\Leftrightarrow \quad \forall\ a \in H \Rightarrow a^{-1} \in H$

$\forall\ a, b \in H \Rightarrow ab \in H$

Suppose that

H is a subgroup of G

By the definition of elements of H satisfy all the properties of a group.

Conversely suppose that

$\forall\ a \in H \Rightarrow a^{-1} \in H$

$\forall\ a, b \in H \Rightarrow ab \in H$

Required to prove 'H' is a subgroup of G.

(a) Closure Property :

$\forall\ a, b \in H \Rightarrow ab \in H$

(by Assumptions)

(b) Associative Property :

$\forall$ a, b, c $\in$ H $\Rightarrow$ (ab) . c = a(b.c)

H is a subset of G

(c) Identify Property :

By (i) $\Rightarrow a^{-1} \in H \ \forall \ a \in H$

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

$\Rightarrow e \in H$

(d) Inverse Property :

$\forall \ a^{-1} \in H,\ \forall \ a \in H$

Q28. If G is an abelian group and H, K are subgroup of G then prove that H.K = {h.k / h $\in$ H, k $\in$ K} is again a subgroup of G.

Ans :

Given that HK = {h.k / h $\in$ H, k $\in$ K}

H & K are subgroups of G

i.e., HK $\neq$ 0, e $\in$ HK

as e = e . e where e $\in$ H, e $\in$ k.

By applying two step subgroup test required to prove HK is an subgroup of G

1. Let x, y $\in$ HK

$x = h_1k_1$ where $h_1 \in H,\ k_1 \in K$

$y = h_2k_2$ where $h_2 \in H,\ k_2 \in K$

Consider

$xy = (h_1 k_1) (h_2 k_2)$

$= h_1 (k_1 h_2) k_2$ Associative

$= h_1 (h_2 k_1) k_2$ Commutative

$= (h_1 h_2) (k_1 k_2)$ Associative

$\in$ H K

2. Show that $\forall$ x $\in$ HK $\Rightarrow x^{-1} \in$ HK

$x = h_1 k_1$

$\Rightarrow x^{-1} = (h_1 k_1)^{-1}$

$= K_1^{-1} h_1^{-1}$ (Socks shoe property)

$= h_1^{-1} k_1^{-1}$ Abelian

$\in$ H K

$\therefore$ H K is an subgroup of G.

Q29. Let H be a non empty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

Ans :

Given that

H is non empty finite subset of a group G.

Required to prove that, H is a subgroup of G.

Also, given that,

H is a closed with respect to multiplication i.e., H satisfy closure property with respect to multiplication.

Apply - two step subgroup test

1. Closure Property :

From equation (1) it is satisfied

2. Inverse Property :

i.e, To show, $a^{-1} \in H,\ \forall \ a \in H$

Case (i) :

If a = e then $a^{-1} \in H \ \forall \ a \in H$

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

Case (ii) :

Let a $\neq$ e

Now consider the products a, a^2, a^3, a^4, ... which are elements of H

H is finite

Say, $a^i = a^j$ where i > j

$\Rightarrow a^i . a^{-j} = a^j . a^{-j}$

$\Rightarrow a^{i-j} = a^0 = e$

$\Rightarrow a^{i-j} = e$

Consider

$a . a^{i-j-1} = a^{i-}j$

$= e$

a^{i-j-1} $\therefore$ The required multiplication.

$\Rightarrow$ Inverse of a $\Rightarrow$ whenever $a^{i-j-1} \in$ H

Because $a^{i-j} = e$

Since $e \neq a$

$i - j \neq 1 \Rightarrow i - j > 1$

$i - j - 1 \geq 1$

$\therefore$ a^{i-j-1} is a^{-1}

Q30. Let G be a group and let a be any element of G. Then, <a>, is a subgroup of G

Ans :

Given that $<a> = \{a^n / n \in Z\}$

Obviously $<a>$ constains the elements 'a'

Now, we shall prove that,

$<a>$ is subgroup of G

Apply one step subgroup test.

Let $a^m, a^n \in <a>$, where $m, n \in Z$

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

$\Rightarrow$ $a^m a^{-n}$

$\Rightarrow$ $a^{m-n} \in <a>$ $[\because m - n \in Z]$

Let 'T' be a another subgroup of G

Containing the same element 'a'

Required to prove $<a>$ is smallest.

$<a> \subset T$

Let $x \in <a>$

$\Rightarrow$ $x = a^r$

Since $a \in T$

We have by closure property

$a^r \in T$

$x \in T$

$<a> \subset T$

$<a>$ is the smallest subgroup of G

Containing 'a'

Q31. What is a center of group?

Ans :

The center, Z(G) of a group G is the subset of elements in G that commute with every element of G, In symbols,

$Z(G) = \{a \in G / ax = xa \ \forall \ x \text{ in } G\}$

Q32. The center of a group G is a subgroup of G.

Ans :

By the definition of center of group

$Z(G) = \{a \in G / ax = xa \ \forall \ x \text{ in } G\}$

$\because$ $e \in Z(G)$ as $ea = ae$ $\forall$ $a \in G$

(i) $Z(G) \neq \phi$

Required to prove Z(G) is subgroup of G.

Apply two step subgroup test.

1. Closure Property :

Let $a_1, a_2 \in Z(G)$

$\Rightarrow$ $a_1 \in Z(G)$

$\Rightarrow$ $a_1x = xa_1 \ \forall x \in Z$ ... (1)

$\Rightarrow$ $a_2 \in Z(G)$

$\Rightarrow$ $a_2x = xa_2 \ \forall x \in Z$ ... (2)

We shall show that $a_1, a_2 \in Z(G)$

It is enough to show $(a_1 \, a_2) \, x = x(a_1 \, a_2)$

$\forall x \in Z$

Consider

$(a_1 \, a_2) \, x = a_1(a_2 \, x)$ Associative

$= a_1(x \, a_2)$ from (2)

$= (x \, a_1) \, a_2$ Associative

$= (a_1 \, x) \, a_2$ from (1)

$= x(a_1 \, a_2)$ Associative

2. Inverse Property :

Requuired to show,

$\forall$ $a_1 \in Z(G) \Rightarrow a_1^{-1} \in Z(G)$

i.e., to show,

$a_1^{-1} x = x \, a_1^{-1} \ \forall x \in Z$

From (1)

$a_1x = xa_1$ $\forall x \in G$

$a_1^{-1} (a_1 \, x) = a_1^{-1} (x \, a_1)$

$\Rightarrow$ $(a_1^{-1} \, a_1) \, x = (a_1^{-1}x) \, a_1$ Associative

$\Rightarrow \quad ex = (a_1^{-1} x)\, a_1$

$\Rightarrow \quad x = (a_1^{-1} x)\, a_1$

$\Rightarrow \quad xa_1^{-1} = (a_1^{-1} x)\, a_1\, a_1^{-1}$

$\Rightarrow \quad a_1^{-1} = (a_1^{-1} x)\, e$

$\Rightarrow \quad xa_1^{-1} = a_1^{-1} (x\, .\, e)$

$\Rightarrow \quad xa_1^{-1} = a_1^{-1}\, x$

$\therefore$ Z(G) is a subgroup of G.

Q33. Define centralizer of 'a' in G.

Ans :

Let a be a fixed element of a group G

The centralizes of a in G_1 c(a), is the set of all elements in G that commute with a. In symbols,

$c(a) = \{x \in G \mid xa = ax\}$

Q34. For each a in a group G, the centralizer of a is a subgroup of G.

Ans :

Given that G is a group

From 1.4.2

$C(a) = \{x \in G \mid a\, .\, x = ax\}$

Required to prove,

C(a) is a subgroup of G

$C(a) \neq \phi$

$\because e \in c(a)$ as $e.a = a.e$

Apply the two step subgroup test.

1. Closure Property :

$\forall\ x_1, x_2 \in c(a)$

$\Rightarrow \quad x_1x_2 \in c(a)$

$x_1 \in c(a) \Rightarrow$ By the definition

$\Rightarrow \quad x_1a = ax_1$ ... (1)

Similarly

$x_2 \in c(a) \Rightarrow x_2a = ax_2$ ... (2)

Now, to show that

$x_1, x_2 \in c(a)$

Required to show,

$a(x_1\, x_2) = (x_1\, .\, x_2)\, a$

Consider

$a(x_1\, x_2)$

$a(x_1\, x_2) = (a\, x_1)\, x_2$ Associative

$= (x_1\, a)\, x_2$ from (2)

$= x_1\, (a\, x_2)$ Associative

$= x_1\, (x_2\, a)$ from (2)

$= (x_1\, x_2)\, a$ Associative

$\therefore \quad a(x_1\, x_2) = (x_1\, x_2)\, a$

2. Inverse Property :

Here, required to show,

$\forall\, x_1 \in c(a) \Rightarrow x_1^{-1} \in c(a)$

So, prove,

$x_1^{-1}a = ax_1^{-1}$

$x_1 \in c(a) \Rightarrow$ from (1)

$x_1a = ax_1$

$\Rightarrow \quad x_1^{-1} (x_1a) = x_1^{-1} (ax_1)$

$\Rightarrow \quad (x_1^{-1} x_1)\, a = (x_1^{-1}a)\, x_1$

$\Rightarrow \quad ea = (x_1^{-1}\, a)\, x1$

$\Rightarrow \quad a = (x_1^{-1}a)\, x_1$

Apply x_1^{-1}

$\Rightarrow \quad ax_1^{-1} = (x_1^{-1}a)\, x_1\, x_1^{-1}$

$\Rightarrow \quad ax_1^{-1} = (x_1^{-1}a)\, e$

$\Rightarrow \quad ax_1^{-1} = x_1^{-1}\, (a\, .\, e)$

$\Rightarrow \quad ax_1^{-1} = x_1^{-1}\, a$

$\therefore$ c(a) is subgroup of G.

1.4 Cyclic Group - Properties of Cyclic Groups

Q35. Derive cyclic group with example.

Ans :

A group G is said to be a cyclic group if there is an element $a \in G$.

Such that $G = \{a^n \mid n \in z\}$ such an element 'a' is called a generator of G.

Example :

$G = \{1, -1, i, -i\}$ is a cyclic group generated by 'i'

Because $i^1 = i$

$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

$\therefore$ 'i' is a generator of G.

Q36. Find whether $(U(10), \underset{10}{\otimes})$ is a cyclic or not : find its generator ?

Sol :

$U(10) = \{1, 3, 7, 9\}$

We know that U(10) is a group under $\underset{10}{\otimes}$

$3^1 = 3$

$3^2 = 3 \underset{10}{\otimes} 3 = 9$

$3^3 = 3^2 \underset{10}{\otimes} 3 = 9 \underset{10}{\otimes} 3 = 7$

$3^4 = 3^3 \underset{10}{\otimes} 3 = 7 \underset{10}{\otimes} 3 = 1$

$\therefore \langle 3 \rangle = \{3, 9, 7, 1\}$

i.e., $(U(10), \underset{10}{\otimes})$ is a cyclic group and '3' its a generator.

$7^1 = 7$

$7^2 = 7 \underset{10}{\otimes} 7 = 9$

$7^3 = 7^2 \underset{10}{\otimes} 7 = 9 \underset{10}{\otimes} 7 = 3$

$7^4 = 7^3 \underset{10}{\otimes} 7 = 3 \underset{10}{\otimes} 7 = 1$

$\therefore \langle 7 \rangle = \{7, 9, 3, 1\}$

7 is also generator of $(U(10), \underset{10}{\otimes})$

$9^1 = 9$

$9^2 = 9 \underset{10}{\otimes} 9 = 1$

$9^3 = 9^2 \underset{10}{\otimes} 9 = 1 \underset{10}{\otimes} 9 = 9$

$9^4 = 9^3 \underset{10}{\otimes} 9 = 9 \underset{10}{\otimes} 9 = 1$

Here 1, 9 one only the elements which included in the U(10), but not 3 & 7.

So, 9 is not a generator of $(U(10), \underset{10}{\otimes})$

Q37. Let G be a group, and let a belong to G.

(i) if a has infinite order, then $a^i = a^j$ if and only if $i = j$

(ii) If a has finite order, say n, then $\langle a \rangle = \{e, a, a^2 \ldots a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$

Ans :

Given that G is a group

and $a \in G$

(i) Given that a is a infinite order

By the definition,

It is not possible to find a +ve integer 'n' such that $a^n = e$

So, consider

$a^i = a^j$

$a^{i-j} = 1 \ (= e)$

$a^{i-j} = a^0$

$i - j = 0$

$i = j$

(ii) Given that 'a' has finite order say 'n'

i.e., $|a| = n$

By the definition ;

$a^n = e,$

where n is lest positive integer satisfying the condition.

To show that $\langle a \rangle = \{e, a, a^2, \ldots a^{n-1}\}$

Consider a^k where $k \in z$

Apply division algorithm

$k = nq + r$ where $0 \le r < n$

Consider

$a^k = a^{nq+r}$

$= a^{nq} . a^r$

$= (a^n)^q . a^r$

$= e^q . a^r$

$= e . a^r$

$a^k = a^r$ where $0 \le r < n$

$<a> = \{e, a, a^2, ... a^{n-1}\}$

Given that order of $a = n$

i.e., $|a| = n$

By definition, $a^n = e$ where 'n' is the least positive integer.

To prove that $a^i = a^j$ iff n divides $i - j$

Case (i)

Suppose that $a^i = a^j$ to show that n divides $i - j$

Consider

$a^i = a^j$

$a^{1-j} = e$

Now, we shall apply division algorithm to $i - j$ & n

$i - j = nq + r$ where $0 \le r < n$

$a^{i-j} = a^{nq+r}$

$e = a^{nq+r}$

$= a^{nq} a^r$

$= (a^n)^q, a^r$

$= ea^r$

$e = a^r$

$\therefore$ $a^r = e$

$r < n$ is not possible because 'n' is the least positive integer such that $a^n = e$

$\Rightarrow$ $r = 0$

Substitute $r = 0$ in the equation

$i - j = nq + r$

$i - j = nq$

$\Rightarrow$ n divides $i - j$

Case (ii)

Conversely suppose that,

n divides $i - j$

Required to prove that $a^i = a^j$

Again n divides $i - j \Rightarrow i - j = nq$

Consider

$a^{i-j} = a^{nq}$

$= (a^n)^q$

$= e^q$

$a^{i-j} = e = a^0$

Now, multiply both side with a^j

$a^{i-j} . a^j = a^0 . aj$

$a^i = a^j$

(1) Give an example

For any group element a, $|a| = |<a>|$

G is a cyclic group

Which is generated by a

Consider $G = \{1, -1, i, -i\}$

$\Rightarrow$ $(G, *)$ is a group

Also, cyclic group

$\because$ $G = <i>$ where 'i' is the generator

$|G| = 4$ also $|i| = 4$

Because '4' is the least positive integer

Such that $i^4 = 1$

$\therefore$ $|G| = |i|$

$|<i>| = |i|$

Q38. Let G be a group and let a be an element of order n in G, if $a^k = e$ then n divides K.

Ans : **(Jan.-2021)**

Given that G is a group

a is an element of order n in G

We know that,

If a has finite order, $a^i = a^j \Leftrightarrow$

n divides (i – j)

Given that $|a| = n$

Also $a^k = e$

$a^k = a^0$

$\Rightarrow$ n divides k = 0

n divides k

Q39. Let 'a' be an element of order n in a group and let k be a positive integer. Then prove that

(a) $<a^k> = <a^{gcd\ (n,\ k)}>$

(b) $|a^k| = \dfrac{n}{gcd\ (n, k)}$

Ans : **(Jan.-21)**

Given, 'a' is an element of order 'n'

$\Rightarrow$ i.e., $|a| = n$

We know that 'n' is the least positive integer

Such that $a^n = e$

(a) Let gcd (n, K) = d

$\Rightarrow$ d divides k

$\Rightarrow$ K = dr where $r \in z$

Required to prove, $<a^k> = <a^{gcd\ (n,\ k}>$

i.e., $<a^k> = <a^d>$

i.e., We shall prove that

(i) $<a^k> \subset <a^d>$

(ii) $<a^d> \subset <a^k>$

(i) Consider

$a^k = a^{dr}$

$a^k = (a^d)^r$

$\therefore$ $<a^k> \subset <a^d>$ ... (1)

To prove (ii) $<a^d> \subset <a^k>$

Since d = gcd (n, k)

$\Rightarrow$ $\exists$ s, t $\in$ Z $\ni$ d = ns + kt

$a^d = a^{ns + kt}$

$= a^{ns} a^{kt}$

$= (a^n)^s a^{kt}$

$= e^s a^{kt}$

$= ea^{kt}$

$= a^{kt}$

$a^d = (a^k)^t$

$<a^d> \subset <a^k>$ ... (2)

From (1) and (2)

$<a^d> = <a^k>$

$\Rightarrow$ $<a^k> = <a^d>$

$= <a^{gcd\ (n,\ k)}>$

$\therefore$ $<a^k> = <a^{gcd\ (n,\ k)}>$

(ii) $|a^k| = \dfrac{n}{gcd\ (n, k)} = \dfrac{n}{d}$

Required to prove that result, determine $|a^d|$

Consider,

$$\left(a^d\right)^{\frac{n}{d}} = a^n = e$$

$$\left(a^d\right)^{\frac{n}{d}} = e$$

$\Rightarrow$ $|a^d| \leq \dfrac{n}{d}$ ... (3)

Let 'i' be an integer where $i < \dfrac{n}{d}$

$\Rightarrow$ $(a^d)^i = a^{di} \neq e$

Because n is the least positive integer

Such that $a^n = e$

We have id < n

$(a^d)^i \neq e$

$|a^d| = \dfrac{n}{d}$

Now, consider $|a^k|$

$|a^k| = |<a^k>|$

$<a^k> = |<a^{gcd(n, k)}>|$

$<a^k> = |<a^d>|$

$= |a^d|$

$= \frac{n}{d}$

$<a^k> = \frac{n}{gcd\ (n,\ k)}$

Q40. Prove that every cyclic group is abelian group.

Ans :

G is a cyclic group

and say 'a' is its generator

$\Rightarrow$ G = <a>

By definition, we know that $G = \{a^n \mid n \in z\}$

Required to prove

The commutative property true

Let $x, y \in G$

$\Rightarrow x = a^r$

$\Rightarrow y = a^s$

Consider,

$xy = a^r . a^S$

$= a^{r+S}$

$= a^{S+r}$

$= a^S . a^r$

$xy = yx$

$\therefore$ G is abelian group

Q41. If G is a cyclic group generator by an element 'a' then prove that 'G' is also generated by a^{-1}

Ans :

Given that, G is a cyclic group

i.e., G = <a>

Required to prove $G = <a^{-1}>$

Let $x \in G$

$\Rightarrow x = a^r$ where $r \in Z$

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

$\therefore$ Every element of G is expressed as integral part of a^{-1}

$\therefore$ a^{-1} is the generator of G

$\therefore$ $G = <a^{-1}>$

Q42. Find all subgroups of Z_{30}

Ans : **(Jan.-21)**

$Z_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$

<1> = {0, 1, 2, ... 29} order is 30

<2> = {0, 2, 4, ... 38} order 15

<3> = {0, 3, 6 ..... 27} order 10

<5> = {0, 5, 10, 15, 20, 25} order 5

<6> = {0, 6, 12, 18, 24} order 5

<10> = {0, 10, 20} order 3

<15> = {0, 15} order 2

<30> = {0} order 2

1.4.1 Classification of Subgroups of Cyclic Groups

Q43. State and prove fundamental theorem of cyclic group.

Ans : **(Jan.-21)**

(G, ·) is a cyclic group

Let H be a subgroup of G

Case (i)

If H = G

or H = {e}

$\because$ G is cyclic and H = G

$\Rightarrow$ H is also cyclic

If H = {e} then H = <e>

$= \{e^n \mid n \in Z\}$

$\Rightarrow$ H is cyclic

Case (ii)

Let $H \neq G$ and $H \neq \{e\}$

$\Rightarrow \exists\ a \neq e \in H$

Since $a \in H$ and H is a subgroup of G

We have the elements of H are the form a^t

Now, $a^m \in H$,

m is a least positive integer

Required to prove,

$H = <a^m>$

Let $a^m = C$

i.e., $H = <C>$

$b \in H$ is expressed as integral power of C

$\because\ b \in H \Rightarrow b \in G$

$b = a^n$

Apply division algorithm to 'n' and 'm'

$n = mq + r$ where $0 \leq r < m$

By substituting

$b = a^n$

$= a^{mq + r}$

$a^n = a^{mq + r}$

$a^n . a^{-mq} = a^r$ ... (1)

$a^n \in H$ [$\because\ b = a^n \in H$]

$a^m \in H \Rightarrow (a^m)^q \in H$

$\Rightarrow a\text{–}mq \in H$

$a^n \in H,\ a^{-mq} \in H$

$\Rightarrow a^n a^{-mq} \in H$

$\Rightarrow a^{n-mq} \in H$

$\Rightarrow a^r \in H$

$r < m$ is not possible

Because $a^m \in H$, m is least positive integer

$\therefore\ r = 0$

Substituting $r = 0$ in $b = a^{mq + r}$

$b = a^{mq}$

$b = (a^m)^r$

$b = C^r$

$H = <C>$

H is a cyclic group.

Q44. If G is a cyclic group generated by an element 'a' of order 'n' and if |<a>| = n. Then prove that the order of the subgroup of group generated by a is a divisor of 'n'.

Ans :

G is a cyclic group

and $G = <a>$, also, $|a| = n$

$\Rightarrow$ $a^n = e$ where 'n' is the least positive integer

Required to prove,

The order of the subgroup of <a> is a divisor of 'n'.

Means, the order of the subgroup of G is a divisor of $n = |a|$

Now, by fundamentals theorem of cyclic group.

If $b \in H$

$\Rightarrow b = a^n = a^{mq+r}$

$a^n = a^{mq} = e$

$n = mq$

Also we have H is the subgroup of G generated by a^m

$\therefore\ H = <a^m>$

$H = \{a^m, (a^m)^2 ..... (a^m)^q = e\}$

$H = q$

$n = mq \Rightarrow q / n$

$\Rightarrow |H| / |G|$

Q45. An integer K in Z_n is a generator of Z_n iff gcd (K, n) = 1

Ans :

If G is a cyclic group generated by an element 'a' of 0 order 'n'

Then a^m is generator of G

$\Leftrightarrow$ gcd (m, n) = 1

Z_n = {0, 1, 2, ... (n –1} is group with respect to $\oplus_n$ also Z_n is generated by '1'

$\Rightarrow$ Z_n is cyclic group

$Z_n = \langle 1 \rangle$

Also, |1| = n

Z_n is a cyclic group generated by 1 of order 'n'

Then 1^k is generator of

$G = Z_n \Leftrightarrow$ gcd (K, n) = 1

$\therefore$ K is generator of G

$= Z_n \Leftrightarrow$ gcd (K, n) = 1

Q46. If d is a positive divisor of n. The number of elements of order 'd' in a cyclic group of order 'n' is ϕ(d)

Ans :

Let $G = \langle a \rangle$ be a finite cyclic group of order 'n'.

$\therefore$ |a| = n

a, d is positive integer

If d is divisor of n,

Then n = dm

Now, $|a| = n \Rightarrow a^n = e$

$\Rightarrow a^{dm} = e$

$\Rightarrow (a^m)^d = e$

$\Rightarrow |a^m| \leq d$

Let $|a^m| = S$ where $S < d$

Then $(a^m)^S = e$

$\Rightarrow$ $a^{ms} = e$ where $ms < md$

Since |a| = n

Where ms < n

$a^{ms} = e$ is abscrd

$\therefore$ $S \nless d$ i.e, S = d

$\therefore$ $a^m \in G$ where $|a^m| = d$

Thus $\langle a^m \rangle$ is a cyclic subgroup of order d.

Q47. Every group of prime order is cyclic.

Ans :

Let 'p' be a prime

and G be a group

Such that $|G| = p$

Then G contains more than one element

Let $g \in G$

Such that $g \neq e$

Then $<g>$ contains more than one element

Since $<g> \leq G$

By Lagrange's theorem

$|<g>|$ divides P

Since $|<g>| > 1$ and $|<g>|$ divides a prime,

$|<g>| = P = |G|$

Hence $<g> = G$

G is cyclic

Q48. Let G be the group of polynomial under addition with coefficients from Z_{10}. Find the orders of

$f(x) = 7x^2 + 5x + 4$

$g(x) = 4x^2 + 8x + 6$

and $f(x) + g(x)$

Sol :

Let $G = \{\phi(x) = a_0 + a_2x^1 + a_2x^2 + ... + a_nx^n + ...$ where $a_0, a_1, ... a_n ... \in Z_{10}\}$

be the given group under addition modulo 10.

Let $f(x) = 7x^2 + 5x + 4$ and

$g(x) = 4x^2 + 8x + 6 \in G$

Then

$f(x) + g(x) = (7 + 4) x^2 + (5 + 8) x + (4 + 6)$

$= 1x^2 + 3x + 0$

$= x^2 + 3x$

By the definition of order of an element n,

$\phi(x) = 0 \Rightarrow |\phi(x)| = n$

$\Rightarrow$ Now, $10 f(x) = 10 [7x^2 + 5x + 4]$

$= 0x^2 + 0x + 0$

$= 0$

$\therefore$ $|f(x)| = 10$

$\Rightarrow$ $5\,g(x) = 5[4x^2 + 8x + 6]$

$= 0x^2 + 0x + 0$

$\therefore$ $|g(x)| = 5$

$\Rightarrow$ $10\,[f(x) + g(x)] = 10\,(x^2 + 3x)$

$= 0$

$|f(x) + g(x)| = 10$

$\therefore$ The order of f(x), g(x) and f(x) + g(x) are

10, 5 and 10 respectively.

Q49. If a is an element of a group G and |a| = 7. Show that a is the cube of some elements of G.

Sol :

Let (G, ·) is a group

and e be the identify element of G

Let $a \in G$ and $|a| = 7$

i.e., $a^7 = e$

Consider $a = a\,.\,e$

$= a\,.\,a^7$

$= a^8$

$= a^8\,.\,e$

$= a^8\,.\,a^7$

$= a^{15}$

$= (a^5)^3$

Hence a is the cube of a^5 of G.

Q50. Suppose that <a>, <b> and <c> are cyclic groups of order 6, 8 and 20 respectively. Find all the generator of <a>, <b> and <c>.

Sol :

Let <a>, <b> and <c> be cyclic group order 6, 8 and 20 respectively.

i.e,, $|<a>| = 6$; $|<b>| = 8$;

$|<c>| = 20$

Now, gcd (6, 1) = gcd (6, 5) = 1

$\therefore$ The generator of <a> are a and a^5

Now, gcd (8, 1) and gcd (8, 5) = gcd (8, 7)=1

$\therefore$ The generator of <b> are b, b^3, b^5 and b^7

Now,

gcd (20, 1) = gcd (20, 3) = gcd (20, 7)

= gcd (20, 9) = gcd (20, 11)

= gcd (20, 13) = gcd (20, 17)

= gcd (20, 19) = 1

∴ The generator of <c> are

$c, c^3, c^7, c^9, c^{11}, c^{13}, c^{17}, c^{19}$

Q51. How many subgroups does Z_{10} have? List a generator for each of these subgruops.

Sol :

Let Z_{20} = {0, 1, 2, ... 19} be a group

By definition of generator of a

is $\langle a \rangle = \{a^n \mid n \in Z\} = Z_{20}$

Now,

$\langle 1 \rangle = Z_{20}$

<2> = {0,2,4,6,8,10,12,14,16,18}

<4> = {0, 4, 8, 12, 16}

<5> = {0, 5, 10, 15}

<10> = {0, 10}

<20> = {0}

∴ There are six subgroups of Z_{20}

The generator for the subgroups are

1, 2, 4, 8, 10, 20.

Q52. Consider the set {4, 8, 12, 16}. Show that this set is a group under multiplication modulo Q_{20} by cons-tructing its Cayley table.

What is the identity element? Is the group cyclic ?

If So, find all of its generator.

Sol :

Let G = {4, 8, 12, 16} be a set under multiplication modulo 20

$\otimes_{20}$	4	8	12	16
4	16	12	8	4
8	12	4	16	8
12	8	16	4	12
16	4	8	12	16

$\therefore$ (G, $\otimes_{20}$) is satisfies. Closure, Associative identity and inverse properties.

Here, identities element is e = 16

and the inverse element of 4, 8, 12, 16 are

4, 12, 8, 16 respectively.

$\therefore$ (G, $\otimes_{20}$) is a group

By definition of cyclic group

$<a> = G = \{a^n / n \in Z\}$

$8 \in G \Rightarrow 8^1 = 8$

$\Rightarrow 8^2 = 8 \underset{20}{\otimes} 8 = 4$

$8^3 = 8^2 \underset{20}{\otimes} 8 = 4 \underset{20}{\otimes} 8 = 12$

$8^4 = 8^3 \underset{20}{\otimes} 8 = 12 \underset{20}{\otimes} 8 = 16$

$\therefore$ 8 is the generator of G.

and the inverse element of 8 is 12.

Also, generator of G.

$\therefore$ G = <8> = <12> is a cyclic group

$\therefore$ 8 and 12 are generator of G.

Short Question and Answers

1. Let G be a group and let a be an element of order n in G, if $a^k = e$ then n divides K.

Ans :

Given that G is a group

a is an element of order n in G

We know that,

If a has finite order, $a^i = a^j \Leftrightarrow$

n divides (i – j)

Given that $|a| = n$

Also $a^k = e$

$a^k = a^0$

$\Rightarrow$ n divides k = 0

n divides k

2. Find all subgroups of Z_{30}

Ans :

Z_{30} = {1, 2, 3, 5, 6, 10, 15, 30}

<1> = {0, 1, 2, ... 29} order is 30

<2> = {0, 2, 4, ... 38} order 15

<3> = {0, 3, 6 ..... 27} order 10

<5> = {0, 5, 10, 15, 20, 25} order 5

<6> = {0, 6, 12, 18, 24} order 5

<10> = {0, 10, 20} order 3

<15> = {0, 15} order 2

<30> = {0} order 2

3. Let G be a group and let H be a non empty subset of G. If ab is in H whenever a and b are in H and a^{-1} is in H whenever a is in H then H is a subgroup of G.

Ans :

Given that H is a non empty subset of G

Required to prove H is a subgroup of G

$\Leftrightarrow \quad \forall\, a \in H \Rightarrow a^{-1} \in H$

$\forall\, a, b \in H \Rightarrow ab \in H$

Suppose that

H is a subgroup of G

By the definition of elements of H satisfy all the properties of a group.

Conversly suppose that

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

$\forall\, a, b \in H \Rightarrow ab \in H$

Required to prove 'H' is a subgroup of G.

(a) Closure Property

$\forall\, a, b \in H \Rightarrow ab \in H$

(by Assumptions)

(b) Associative Property

$\forall\, a, b, c \in H \Rightarrow (ab) \,.\, c = a(b.c)$

H is a subset of G

(c) Identify Property

By (i) $\Rightarrow a^{-1} \in H \;\forall\; a \in H$

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

$\Rightarrow e \in H$

(d) Inverse Property

$\forall\, a^{-1} \in H, \;\forall\, a \in H$

4. Prove that the set GL (2, R) = $\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle/ a, b, c, d \in R, ad - bc \neq 0\right\}$ is a non abelian group with respect to matrix multiplication.

Ans :

Given set is GL (2, R)

$$= \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle/ a, b, c, d \in R, ad - bc \neq 0\right\}$$

Required to prove GL(2, R) is a non abelian group under multiplication :

Which is enough to prove that not a commutative property.

Let $A_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $A_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ &

$A_3 = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \in R$

i) Closure Properties

Let $A_1, A_2, \in G \Rightarrow A_1 . A_2$

$$\Rightarrow \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} \in R$$

ii) Associative Property

Clearly, Associative property satisfices

$\forall A_1, A_2, A_3 \in G \Rightarrow A_1 (A_2 A_3) = (A_1 A_2) A_3$ In matrix multiplication. The associative property satisfices.

iii) Identity Property

Identity of matrix under multiplication is

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\forall A_1 \in G \Rightarrow A_1 I = I A_1 = A1$

$$\Rightarrow \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 & 0 \\ 0 & d_1 \end{bmatrix} \in G$$

iv) Inverse Property

Inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\Rightarrow$ Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$|A| = ad - bc \neq 0$

$$\frac{1}{|A|} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} \frac{b}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

$\therefore$ GL (2, R) is a group

5. Define binary operation with examples.

Ans :

A binary operation (*) on any non empty set 'G' is a mapping * : G × G $\rightarrow$ G is the Cartesian product of G into itself. They are also denoted by o, ., $\oplus$, etc.

Properties

(i) A binary operation (*) is commutative on a set 'G' iff

$a * b = b * a \ \forall \ a, b \in G$

(ii) A binary operation (*) is associative on a set 'G' iff

$(a * b) * c = a * (b * c) \ \forall \ a, b, c \in G.$

6. Write some examples of groups.

Ans :

Let 'G' be any non-empty set, * be binary operation on G. If (G, $*$) is said to be group it satisfies four properties.

a) Closure law

b) Associative law

c) Identity law

d) Inverse law

a) Closure Law

If 'G' is any non-empty set and '*' is binary operation, then for $a \in G, b \in G \Rightarrow a * b \in G$ it is called closure law.

Note: If '$*$' is a binary operation on G if and only if it satisfies closure law.

Ex: (N, +) (R, –)

b) Associative Law

If '*' is any binary operation on non empty set 'G' If $a,b,c \in G$; $(a * b) * c = a * (b * c)$ is called associative law, otherwise '$*$' is not satisfies associative law on G.

Example

i) N

$* = +$

$a = 2, b = 3, c = 5$

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

$(2+3)+5 = 2+(3+5)$

$5+5 = 2+8$

$10 = 10$

'+' satisfies associative law on N.

Q = Rational

$* = -$

$a = \frac{5}{3}, b = \frac{10}{3}, c = -\frac{7}{2}$

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

$\left(\frac{5}{3}-\frac{10}{3}\right)-\left(-\frac{7}{2}\right) = \frac{5}{3}-\left(\frac{10}{3}+\frac{7}{2}\right)$

$-\frac{5}{3}+\frac{7}{2}=\frac{5}{3}-\left(\frac{20+21}{6}\right)$

$-\frac{10+21}{6} = \frac{5}{3}-\frac{41}{6}$

$\frac{11}{6} = \frac{10-41}{6}$

$\frac{11}{6} \pm -\frac{31}{6}$

$\therefore$ – does not satisfies associative law on Q.

c) Identity Law

Let 'G' be any non empty set and '*' be any binary operation on G. $\forall a \in G\ \exists e \in G \ni e * a = a * e = a$. Here 'e' is called identity element.

Eg:

i) (N, •), '1' is identity element

$a = 2$

$1 \times 2 = 2 \times 1 = 2$

$a = 3 \Rightarrow 1 \times 3 = 3 \times 1 = 3$

$\therefore$ (N, •) here '1' is identity element

ii) (W, +) + {0, 1, 2, ...}

$0 + 2 = 2 + 0 = 2$

$\therefore$ (W, +) has an identity with respect to addition i.e., '0'

Note

(i) '0' is called additive identity element.

(ii) '1' is called multiplicative identity element.

d) Inverse Law

An element 'a' is said to be invertible $\exists x \in G \ni x * a = e = a * x$, here 'a' is called invertible, 'x' is inverse of a.

i.e., $a^{-1} * a = e = a * a^{-1}$

7. What are the Elementary Properties of Groups?

Ans :

(i) Uniqueness of the Identity

It states that "in a group G, there exists only one identity element".

(ii) Cancellation Laws

Let a, b, c be the elements of a group G.

$ba = ca \Rightarrow b = c$ (Right cancellation law)

$ab = ac \Rightarrow b = c$ (Left cancellation law)

(iii) Uniqueness of Inverse

It states that "For each element a in a group G, there is a unique element b in G such that ab = ba = e".

(iv) If a, b ar the elements of a group G, then $(ab)^{-1} = b^{-1} a^{-1}$.

8. Define Addition Modulo.

Ans :

If a and b are any two integers and m is a fixed positions integer. Then a + b under addition modulo 'm' is denoted by $a \oplus_m b$ and it is defined as, $a \oplus_m b = a + b$ if $a + b < m$

$a \oplus_m b = r$

where 'r' is the least non negative (≥ 0) reminder by dividing a + b by m if

$a + b \geq m$.

9. Define multiplication modulo.

Ans :

If a and b are any two integers.

Then a into b under multiplication modulo 'm' is denoted by $a \otimes_m b$ and is defined as

$a \otimes_m b = a \times b$ if $a \times b < m$

$a \otimes_m b = r$

where

'r' is a the least non negative reminder obtained by dividing

$a \times b$ by m if $a \times b \geq m$

Example :

1. $2 \otimes_4 8 = 0$

(i) $2 \times 8 = 16$

(ii) $16 \geq 4$

(iii) $\frac{16}{4} \Rightarrow$ reminder '0'

2. $2 \otimes_4 4 = 2$

(i) $2 \times 4 = 8$

(ii) $8 > 6$

(iii) $\frac{8}{6}$ reminder is '2'

10. Define Cayley's Table.

Ans :

Sometimes an operation $*$ on a finite set conveniently be specified by a table called the composition table.

The construction of composition table is explained below :

Let $S = \{a_1, a_2 \ldots a_i, a_j \ldots a_n\}$ be a finite set with 'n' elements.

Let a table with n + 1 rows & n + 1 columns be taken.

Let the squares in the first row be filled in with $a_1, a_2, \ldots, a_n$ & the squares in the first column be filled in with $a_1, a_2, \ldots, a_n$

Let a_i $(1 \leq i \leq n)$ and a_i $(1 \leq j \leq n)$ be any two elements of S.

Let the product $a_i * a_j$ obtained by operating a_i with a_j be placed in the square which is at the integer section of the row headed by a_i and the column headed by a_j.

11. Define order of element with example.

Ans :

The order of element 'a' in a group G is a smallest positive integer n such that $a^n = e$. Then we say that 'a' has infinite order. The order of an element 'a' is denoted by $|a|$.

Example :

U(15) = {1, 2, 4, 7, 8, 9, 11, 13, 14} under the multiplication modulo 15. Here order 8.

The order of element 7 is

$7^1 = 7$

$7^2 = 4$

$7^3 = 13$

$7^4 = 1$

So, $|7| = 4$

12. Derive cyclic group with example.

Ans :

A group G is said to be a cyclic group if there is an element $a \in G$.

Such that $G = \{a^n \mid n \in z\}$ such an element 'a' is called a generator of G.

Example :

$G = \{1, -1, i, -i\}$ is a cyclic group generated by 'i'

Because $i^1 = i$

$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

$\therefore$ 'i' is a generator of G.

13. Every group of prime order is cyclic.

Ans :

Let 'p' be a prime

and G be a group

Such that $|G| = p$

Then G contains more than one element

Let $g \in G$

Such that $g \neq e$

Then $<g>$ contains more than one element

Since $<g> \leq G$

By Lagrange's theorem

$|<g>|$ divides P

Since $|<g>| > 1$ and $|<g>|$ divides a prime,

$|<g>| = P = |G|$

Hence $<g> = G$

G is cyclic

Choose the Correct Answers

1. In a group (G, •) for a, b $\in$ G $\Rightarrow$ $(ab)^{-1}$ = ________ [c]

   (a) $(ba)^{-1}$ (b) $a^{-1}b^{-1}$

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

2. If every element of (G, •) is its own ________ [c]

   (a) Identity (b) Associative

   (c) Inverse (d) Group

3. Additive identity is ________ [a]

   (a) 0 (b) 1

   (c) –1 (d) ∞

4. Multiplicate identity is ________ [b]

   (a) 0 (b) 1

   (c) –1 (d) ∞

5. The order of a infinite group is ________ [c]

   (a) 1 (b) –1

   (c) 0 (d) commutative

6. Every cyclic group is ________ [a]

   (a) commutative (b) normal

   (c) cyclic (d) homomorphism

7. Every subgroup of a cyclic group is ________ [a]

   (a) cyclic (b) subgroup

   (c) normal (d) abelian

8. Group satisfies ________ conditions. [d]

   (a) 1 (b) 2

   (c) 3 (d) 4

9. If H is any subgroup of group 'G' then H^{-1} = ________ [b]

   (a) H^{-1} (b) H

   (c) G (d) G^{-1}

10. H is any subgroup of group G. Then HH = ________ [c]

    (a) H^2 (b) H^{-1}

    (c) H (d) O

Fill in the Blanks

1. Every permutation of a finite set can be written as a cycle or ________.
2. Every permutation in s_n, n > 1 is a ________.
3. The set of even permutation in s_n forms a ________.
4. $<ak> = <a^{gcd(n, k)}>$ and $|a^k|$ = ________.
5. In a finite cyclic group, the order of an element divides the ________.
6. In a finite group, the number of elements of order d is a ________.
7. If 'x' is a binary operation on G if and only if it satisfies ________.
8. Additive identity element is ________.
9. Multiplicative identity element is ________.
10. Let $(G_1.)$ be a group for a, $b \in G (ab)^2 = a^2 b^2$ iff ________.
11. The identity element of subgroup H of G is same as the ________ of group G.
12. If H is any subgroup of group G Then HH = ________.
13. Intersection of two subgroup of group G is ________.
14. The union of two subgroups is again a subgroup of group iff ________.
15. Any two left (right) cosets of subgroup either ________ (or) ________.

Answers

1. Product of disjoint cycles
2. Product of two-cycles
3. Subgroup of Sn
4. n/gcd(n, k)
5. $\because$ order of the group
6. Multiple of $\phi(d)$
7. Closure law
8. Zero
9. 1
10. G is an abelian group
11. Identity element
12. H
13. Again a subgroup of group G
14. $\because$ one is continent in another
15. Disjoint, Identical

UNIT II	**Permutation Groups:** Definition and Notation - Cycle Notation - Properties of Permutations - A Check Digit Scheme Based on D5. Isomorphisms; Motivation - Denition and Examples - Cayley's Theorem Properties of Isomorphisms - Automorphisms - Cosets and Lagrange's Theorem Properties of Cosets 138 - Lagrange's Theorem and Consequences - An Application of Cosets to Permutation Groups - The Rotation Group of a Cube and a Soccer Ball.

2.1 Permutation Groups

2.1.1 Definition and Notation

Q1. Define Permutation group.

Ans :

Let S = $a_1, a_2, \ldots a_n$ be finite set then a permutation is a mapping $f : S \to S$ which is both one – one and onto (or)

If $S = \{a_1, a_2, \ldots a_n\}$ then a one-one mapping from S onto itself is called a permutation of degree n.

The number n of elements in S is called the degree of permutation.

Q2. Write examples for permutation.

Ans :

A Permutation of set A is a function from A to A is both one to one and onto. A permutation of a set A is a set of permutation of A that forms a group under function composition.

Example :

1. Define a permutation of set {1, 2, 3, 4} by Specifying.

$\alpha(1) = 2, \quad \alpha(2) = 3$

$\alpha(3) = 1, \quad \alpha(4) = 4$

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

2. Define a permutation α of the set {1, 2, 3, 4, 5, 6} given by

$\beta(1) = 5, \quad \beta(2) = 3, \quad \beta(3) = 1,$

$\beta(4) = 6, \quad \beta(5) = 2, \quad \beta(6) = 4$

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$$

Q3. Define composition of permutation with example.

Ans :

Let $f = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{bmatrix}$ and

$g = \begin{bmatrix} b_1 & b_2 \ldots\ldots & b_n \\ c_1 & c_2 \ldots\ldots & c_n \end{bmatrix}$ be two elements.

Here $b_1, b_2 \ldots\ldots b_n$ (or) $c_1, c_2, \ldots\ldots c_n$ are nothing but the elements $a_1, a_2 \ldots\ldots a_n$ of S in some order.

None, $f(a_1) = b_1, \; g(b_1) = c_1,$

$f(a_2) = b_2, \; g(b_1) = c_2 \ldots\ldots$

By definition we have

$c_1 = g(b_1) = g(f(a_1)) = (gf)(a_1)$

i.e,. $(gf)(a_1) = c_1$

Similarly

$(gf)(a_2) = c_2, \; (gf)(a_3) = c_3 \ldots\ldots$

$(gf)(a_n) = c_n$

$$\therefore \quad gf = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ c_1 & c_2 & \cdots & c_n \end{bmatrix}$$

Example :

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} \text{ and } \gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \text{ find } \gamma\sigma$$

Sol :

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}, \gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$$

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$$

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

2.2 Cycle Notation

Q4. Write notation for cycle.

Ans :

Let $S = \{a_1, a_2, \ldots a_n\}$

$= \{a_1, a_2, \ldots a_k, a_{k+1}, a_{k+2} \ldots a_n\}$

Consider a permutation which is of the form

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \cdots & a_k & a_{k+1} & \cdots & a_n \\ a_2 & a_3 & a_4 & \cdots & & a_1 & a_{k+1} & \cdots & a_n \end{pmatrix}$$

is called as cyclic permutation whose length is K and degree 'n'

where $f(a_1) = a_2$, $f(a_2) = a_3$ ..... $f(a_k) = a_1$

$f(a_{k+1}) = a_{k+1}$ ..... $f(a_n) = a_n$

The above cyclic permutation is expressed as $f = (a_1, a_2, \ldots a_k)$

2.3 Properties of Permutations

Q5. Every permutation of a finite set can be written as a cycle or as a product of disjoint cycle.

Ans :

Let A be a set,

$A = \{1, 2, 3 \ldots n\}$

Let α be a permutation on set A

Let a_1 be an element of A

i.e., $a_1 \in A$

The element a_2 is obtained as,

$a_2 = \alpha(a_1)$ ... (1)

Similarly,

$a_3 = \alpha(\alpha(a_1))$

$= \alpha^2 (a_1)$ and so on.

$\Rightarrow$ Then the sequence

$a_1, \alpha(a_1), \alpha^2(a_1)$ ..... must be finite

$\Rightarrow$ $a_1 = \alpha^m(a_1)$ for some $m \leq n$.

Consider

Case (i) :

If $m = n$ then there is no repetition

$a_1 = \alpha^0(a_1)$

$= a_1$

$a_2 = (\alpha) (a_1) = \alpha a_1$

$a_3 = (\alpha)^2 (a_1) = \alpha^2 a_1$

$\Rightarrow$ $\alpha = (a_1, a_2 ..... a_n)$ ..... (2)

Equation (2) represents a single cycle.

Hence, a permutation of a finile set can be expressed as a cycle.

Case (ii) :

If $m < n$,

Then there must be repetition

i.e., If $\alpha^i(a_1) = \alpha^j(a_1)$ for some $i < j$

Then $a_1 = \alpha^m (a_1)$

Where $m = j - i$

$a_1 = \alpha^0, a_2 = \alpha\, a,$

$a_3 = \alpha^2 a_1 .....$

$a_m = \alpha^m a_1$

The sequence obtained is,

$\alpha_1 = (a_1, a_2 ..... a_m)$ ... (3)

Equation (3) represents a cycle

Let b_1 be an element of a which is not present in first cycle. i.e., α_1

$b_2 = \alpha(b_1)$

$b_3 = \alpha^2(b_2)$

The sequence obtained

b_1, b_2 ..... is a finite sequence.

$b_1 = a^k (b_1)$ for some K.

The second cycle and first cycle does not contain common elements as they are disjoint cycles.

If $\alpha^i(a_1) = \alpha^j(b_1)$ for some i and j

$$\frac{\alpha^i}{\alpha^i} a_1 = b$$

$\Rightarrow \quad \alpha^{i-j} a_1 = b_1$

$\Rightarrow \quad a_1 = b_1$ is a contradiction

The cycle is,

$\alpha_2 = (b_1, b_2 \text{ ..... } b_k)$ ... (4)

Similarly, the third cycle will be of the for m

$\alpha_3 = c_1, c_2 \text{ ..... } c_s$

The process is continued till the elements of A get exhausted.

Multiplying equation (3), (4) & (5)

$\alpha_1 , \alpha_2 , \alpha_3 = (a_1, a_2 \text{ ..... } a_{nm})\ (b_1, b_2 \text{ ..... } b_k)\ (c_1, c_2 \text{ ..... } c_s)$

If $\alpha_1 . \alpha_2 . \alpha_3 = \alpha$ then

$\alpha = (a_1, a_2, a_3 \text{ ..... } a_m)\ (b_1, b_2, \text{ ..... } b_k)\ (c_1, c_2 \text{ ..... } c_s)$

$\alpha = (a_1, a_2, a_3 \text{ ..... } a_m)\ (b_1, b_2, \text{ ..... } b_k)\ (c_1, c_2, \text{ ..... } c_s)$

If can be seen for equation (6). That the permutation of A is a product of disjoint cycles. If there are 'n' number of disjoint cycles,

Then.

$\alpha = (a_1, a_2 \text{ ..... } a_m)\ (b_1, b_2 \text{ ..... } b_k)\ (c_1, c_2 \text{ ..... } c_s) \text{ ..... } (d_1, d_2 \text{ ..... } d_n)$

Hence, every permutation of a finite set can be expressed as a product of disjoint cycles.

Q6. If the pair of cycles, $\alpha = (a_1, a_2 \text{ .... } a_m)$ and $\beta = (b_1, b_2 \text{ .... } b_n)$ have no entries in common, Then $\alpha\beta = \beta\alpha$.

Ans :

Let $\alpha = (a_1, a_2 \text{ ..... } a_m)$

Let $\beta = (b_1, b_2 \text{ ..... } b_n)$

& $S = (c_1, c_2 \text{ ..... } c_k)$

Let us say that α and β are permutation of the set

$S = \{a_1, a_2 \text{ .... } a_m,\ b_1, b_2 \text{ .... } n_n,\ c_1, c_2 \text{ .... } a_k\}$

Where C's are the numbers of S left fixed by both a and β.

To prove, $\alpha\beta = \beta\alpha$

i.e., to prove that $(\alpha\,\beta)(x) = (\beta\,\alpha)(x)$ for $x \in S$

For $x \in A$ the following cases carries.

Case (i)

Let $x \in \{x_1, x_2 \ldots\ldots x_k\}$

$\therefore$ $f(x) \in \{x_1, x_2 \ldots\ldots x_k\}$

Since α, β are disjoint cycles.

$\{a_1, a_2 \ldots a_k\} \cap \{y_1, y_2 \ldots\ldots y_t\} = \phi$

$\therefore$ $x_1, f(x) \notin \{y_1, y_2 \ldots\ldots y_r\}$

$\therefore$ $\beta(x) = x$ & $\beta((\alpha(x)) = \alpha(x)$

Now, $(\beta\alpha)(x) = \beta(\alpha(m)) = \alpha(x)$

and $((\alpha\beta)(x)) = (\alpha(\beta(x))) = \alpha(x)$

and hence, $(\beta\alpha)(x) = (\alpha\beta)(x)$ for $x \in s$.

Case (ii) :

Let $x \in \{y_1, y_2 \ldots\ldots y_t\}$

$\therefore$ $\beta(x) \in \{y_1, y_2 \ldots\ldots y_t\}$

Since

α, β are disjont cycle.

$\{x_1, x_2 \ldots x_k\} \cap \{y_1, y_2 \ldots y_t\} = \phi$

$\therefore$ $x, \beta(x) \notin (x_1, x_2 \ldots x_k)$

Now,

$(\beta\,\alpha)(x) = \beta(\alpha(x)) = \beta(x)$

and

$(\alpha\,\beta)(x) = \alpha(\beta(x)) = \beta(x)$

and, Hence $\beta\alpha(x) = \alpha\beta\,(x)$

Case (iii) :

Let $x \notin \{x_1, x_2 \ldots x_k\}$ and $x \notin \{y_1, y_2 \ldots y_t\}$

$\therefore$ $\alpha(x) = x$ and $\beta(x) = x$

Now,

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

and $(\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(x) = x$

Hence,

$(\beta\alpha)(x) = \alpha\beta\,(x)$

$\therefore$ $\beta\alpha = \alpha\beta$ for $x \in S$.

Q7. Every permutation in S_n, n > 1, is a product of 2 - cycles with example.

Ans :

The identity can be expressed as (1 2) (1 2) and so it is a product of 2 - cycle.

We know that by product of disjont cycles every permutation can be written in the form

$(a_1, a_2 \ldots a_k)(b_1, b_2 \ldots b_t) \ldots (c_1, c_2 \ldots c_s)$

A direct computation show that this is same as

$(a_1a_k)(a_1a_{k-1}) \ldots (a_1a_2)(b_1b_t)(b_1b_{t-1}) \ldots (b_1b_2) \ldots (c_1c_s)(c_1c_{s-1}) \ldots (c_1c_2)$

Example :

Let f = (2 3 4) of degree 4

Then f = (2 3) (2 4)

$$\because \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2\ 4\ 3)$$

Also

We have f = (2 3) (1 2) (2 1) (2 4)

f = (1 3) (3 1) (2 3) (2 4) etc.

This every cycle can be expressed as a produt of transposition.

Q8. If $\varepsilon = \beta_1 \beta_2 \ldots \beta_r$, where the β's are 2 - cycles, Then 'r' is even.

Ans :

Clearly $r \neq 1$,

Since a 2 - cycles is not the identity

If r = 2, we are done.

We suppose that r > 2,

and we proceed by induction.

Suppose that the right most 2 - cycle is (a b)

Then, sine (i j) = (j i)

The product $\beta_{r-1} \beta_r$ can be Expressed in one of the following forms.

ε = (a b) (a b)

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

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

(a b)(c d) = (c d) (a b)

If the first case occurs,

We may delete $\beta_{r-1} \beta_r$ from the original product to obtain

$\varepsilon = \beta_1 \beta_1 \ldots \beta_{r-2}$

and therefore, by the second principle of mathematical induction.

$r - 2$ is even.

In the other three cases, we replace the form of $\beta_{r-1}\ \beta_r$ on the right by its counters part on the left to obtain a new product of 2 - cycle.

Now, we repeat the procedure just described with $\beta_{r-2}\ \beta_{r-1}$

and as before, we obtain (r – 2) 2 - cycles equal to the identity

or new product of 'r' 2 - cycles.

Where the right most occurrence of a is in the third 2 cycle from the right.

Continuing this process, we must obtain a product of (r – 2) 2 cycles equal to identity,

Because otherwise we have a product equal to the identity in which the only occurrence of the integer 'a' is the left most 2 - cycle.

and such a product does not fix 'a', where as the identity does.

Hence, by the second principle of mathematical induction

r – 2 is even and 'r' is even as well.

Q9. If a permutation α can be expressed as a product of an even (odd) numbers of 2 - cycles, Then every decomposition of α into a product of 2 - cycles must have an even (odd) number 2-cycle. In symbols, If

$$\alpha = \beta_1\beta_2 \ldots\ldots \beta_r \quad \text{and} \quad \alpha = \gamma_1\, \gamma_2 \ldots\ldots \gamma_s$$

where we β's and the γ's are 2- cycles

Then r and S are both even or both odd.

Ans :

Let the polynomial in x corresponding to S

Let $P_n(x) = (x_1 - x_2)(x_1 - x_3) \ldots\ldots (x_1 - x_n)$

$(x_2 - x_3) \ldots\ldots (x_2 - x_n)$

....

....

$(x_{n-1} - x_n)$

$= \Pi\,(x_1 - x_j)$ where $i < j$, $1 \leq i \leq n - 1$ and $2 \leq j \leq n$.

Now,

$P_n(x)$ can be split into the following three types of product corresponding to a transposition (r, S).

(i) $L = \prod_{i,\, j \neq r,\, S} (x_i - x_j)$

(ii) $M = \prod_{i \neq r,\, S} (x_i - x_r)\ (x_i - x_s)$

(iii) $x_r - x_s$

$\therefore \quad p_n(x) = \pm\ LM\,(x_r - x_s)$

We considers the effect of transposition (r, s) on $p_n(x)$.

Then $(r, s)\ L = L$

$$(r, s)\ M = (r, s)\left[\pm \prod_{i \neq r, S} (x_i - x_r)(x_i - x_j)\right] = M$$

$$(r, s)\ [(x_r - x_s)] = x_s - x_r = -(x_r - x_s)$$

$$(r, s)\ [p_n(x)] = (r, s)\ [\pm\ LM\ (x_r - x_s)]$$

$$= \pm\ (r, s)\ L\ .\ (r, s)\ M\ .\ (r, s)\ (x_r - x_s)$$

$$= \pm\ [L\ M\ \{x_r - x_s\}]$$

$$= \pm\ [L\ M - \{x_s - x_r\}]$$

$$= -p_n(x)$$

$\therefore$ A transposition (r, s) changes $p_n(x)$ to $p_n(x)$

Let f be a permutation on S.

If f can be expressed as a product of r permutation.

Say $f_1, f_2 \ldots. f_r$ then

$$f(p_n(x)) = f_1, f_2 \ldots f_r\ [p_n\ (x)]$$

$$= f_1, f_2 \ldots.. f_{r-1}\ ((-1)'\ p_n(x)) = (-1)^r\ p_n(x)$$

Again if f can be expressed as a product of S transpositions,

Then $f(p_n(x)) = (-1)^r\ p_n(x)$

Since f is a permutation

$f(p_n(x))$ is Unique

$\therefore\ (-1)^r\ p_n(x) = (-1)^s\ p_n(x)$

For this to be true,

Both r, s must be even (or) odd.

Q10. What is odd and even permutation?

Ans :

Even and odd permutation.

$\rightarrow$ A permutation that can be expressed as a product of an even number of 2 - cycles is called an Even permutation.

$\rightarrow$ A permutation that can be Expressed as a product of an odd number of 2- cycles is called an odd permutation.

Q11. Determine whether the following permutation even or odd.

(a) (1 3 5)

(b) (1 3 5 6)

(c) (1 3 5 6 7)

(d) (1 2) (1 3 4) (1 5 2)

(e) (1 2 4 3) (3 5 2 1)

Sol :

(a) (1 3 5) = (1 3) (1 5)

= Product of two permutation.

(b) (1 3 5 6) = (1 3) (1 5) (1 6)

= Product of three permutation.

∴ (1 3 5 6) is odd permutation

(c) (1 3 5 6 7) = (1 3) (1 5) (1 6) (1 7)

Product of four permutation.

(d) (1 2) (1 3 4) (1 5 2) = (1 2) (1 3) (1 4) (1 5) (1 2)

Product of five permutation

∴ (1 2) (1 3 4) (1 5 2) is an odd permutation.

(e) (1 2 4 3) (3 5 2 1) = (1 2) (1 4) (1 3) (3 5) (3 2) (3 1)

Product of six permutation

∴ It is a even permutation.

Q12. Define Alternating group of degree 'n'.

Ans : **(June-19)**

The group of even permutation of n symbols is denoted by A_n and is called the alternating group of degree n.

Q13. Prove that for n > 1, A_n has order $\frac{n!}{2}$.

Ans : **(May/June-19)**

Let $S_n = \{e_1, e_2 .... e_p, o_1, o_2 .... o_q\}$ be the permutation group on 'n'.

Where $e_1, e_2 ..... e_p$ are even permutataion .

and $o_1, o_2 .... o_q$ are odd permutataion.

∴ p + q = n!

Let $t \in s_n$ and 't' be a transpontion since permutataion multiplication follows closure law in S_n.

We have $te_1, te_2 ..... te_p, to_1, to_2 ..... to_q$ as elementn of S_n

Since 't' is an odd permutation.

$te_1, te_2 .... te_p$ are all odd and

$to_1, to_2....to_q$ are even.

Let $te_i = te_j$ for $i \leq p, j \leq p$

Since S_n is a group by left cancellation law. $e_i = e_j$

∴ $te_i \neq te_j$ and hence the p permutation

$te_1, te_2 ..... te_p$ are all distinct in S_n.

But S_n contains exactly q odd permutation

$\therefore$ $p \leq q$ ... (1)

Similarly we can should that q even permutation to_1, to_2 ..... to_q are all distinct even permutation in S_n

$\therefore$ $q \leq p$ ... (2)

$\therefore$ from (1) & (2)

$$p = q = \frac{n!}{2}$$

Number of even permutation in S_n = number of odd permutation in S_n = $\frac{n!}{2}$

2.4 A Check Digit Scheme based on D_5

Q14. What is Digit Scheme based on D_5.

Ans :

The international standard book Number (ISBN) method was capable of detecting all single - digit errors and all transposition eross involving adjacent digits.

Q15. Let the Bank note A G 8 5 3 6 8 2 7 11 7.

To nesify that 7 is the appropriate check digit.

Sol :

Using Verhoeff's check -- digit scheme

$\sigma(a_1) * \sigma^2(a_2) * ..... * \sigma^{10}(a_{10}) * a_{11} = 0$ ... (1)

Where $a_1 a_2 .... a_{10}$ is a string with digits is a_{11}

Here

a_1 = A, a_2 = G, a_3 = 8, a_4 = 5, a_3 = 3, a_6 = 6, a_7 = 8, a_8 =2, a_9 = 7, a_{10} = 11, a_{11} = 7

Let α = (0 1 5 8 9 4 2 7) (3 6)

Then from (1)

$\Rightarrow$ $\sigma(A) * \sigma^2(G) * \sigma^3(8) * \sigma^4(5) * \sigma^6(6) * \sigma^7(8) * \sigma^8(2) * \sigma^9(7) * \sigma^{10}(U) * 7$

$\Rightarrow$ $\sigma(0) * \sigma^2(2) * \sigma^3(8) * \sigma^4(5) * \sigma^5(3) * \sigma^6 * (6) * \sigma^7(8) * \sigma^8(2) * \sigma^9(7) * \sigma^{10}(7) * 7$

$\Rightarrow$ $(1 * 0) * 2 * 2 * 6 * 6 * 5 * 2 * 0 * 1 * 7$

$\Rightarrow$ $(1 * 2) * 2 * 6 * 6 * 5 * 2 * 0 * 1 * 7$

$\Rightarrow$ $(3 * 2) * 6 * 6 * 5 * 2 * 0 * 1 * 7$

$\Rightarrow$ $(0 * 6) * 6 * 5 * 2 * 0 * 1 * 7$

$\Rightarrow$ $(6 * 6) * 5 * 2 * 0 * 1 * 7$

$\Rightarrow$ $(0 * 5) * 2 * 0 * 1 * 7$

$\Rightarrow$ $(8 * 2) * 0 * 1 * 7$

$\Rightarrow$ (8 $*$ 0) $*$ 1 $*$ 7

$\Rightarrow$ (8 $*$ 1) $*$ 7

$\Rightarrow$ 7 $*$ 7 = 0

Hence, the given banknote number is the appropriate check digit 7

2.5 Isomorphism, Motivation - Definition & Example - Cayley's Theorem

Q16. Define Homomorphism.

Ans :

Let (G, $\cdot$) and ($\bar{G}$, $*$) be two groups then a mapping ϕ from G $\to$ $\bar{G}$ is said to be a homomorphism

Q17. Define Isomorphism.

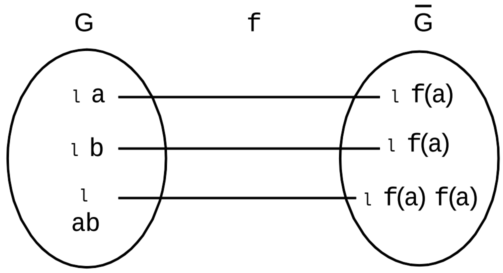
Ans :

A mapping ϕ G $\to$ $\bar{G}$ is said to be an isomorphism

If ϕ is homomorphism, one - one & onto

Here the group G & $\bar{G}$ are said to be isomorphism to each other and donoted as G $\simeq$ $\bar{G}$ isomasphism to each other 4 donoted as G $\simeq$ G

i.e., ϕ(a b) = ϕ(a) ϕ (b) $\forall$ a, b in G.



'G' Operation	'$\bar{G}$' operation	Operation Preservation
•	•	ϕ(a . b) = ϕ(a) . ϕ(b)
•	+	ϕ(a . b) = ϕ(a) + ϕ(b)
+	•	ϕ(a + b) = ϕ(a) ϕ(b)
+	+	ϕ(a + b) = ϕ(a) + ϕ(b)

Q18. ϕ : G $\to$ $\bar{G}$ when $\phi = 2^x$. Show that ϕ is a isomorphism.

Sol :

$\phi = 2^x$

To prove Isomorphism

1. To prove Homomorphism
2. one - one and onto.

Suppose $2^x = 2^y$

Apply log

$\log 2^x = \log 2^y \Rightarrow x \log 2 = y \log 2$ (right commutation law)

$\Rightarrow \quad x = y.$

$\therefore \quad \phi$ is one - one

For onto, we must find for any positive real number y some real number x.

$\phi(x) = y$

i.e., $2^x = y \Rightarrow x = \log_2 y.$

$\therefore \quad \phi$ is onto.

$\Rightarrow \quad \phi$ is Homomorphism

Suppose $\phi(x+y) = 2^{x+y}$

$= 2^x . 2^y$

$= \phi(x) . \phi(y)$

$\therefore \quad \phi$ is Homomorphism $\forall x, y \in G$

Q19. Prove that U(10) $\approx$ Z_4 and U (5) $\approx z_4$

Sol :

Let $Z_4 = \{0, 1, 2, 3\}$

$(Z_4, +) = \{0, 1, 2, 3, +\}$

$(U(5)) = \{1, 2, 3, 4\}$

$(U(5), +) = \{1, 2, 3, 4, +\}$

$U(10) = \{1, 3, 7, 9 , .\}$

are groups

Let the mapping. $\phi : Z_4 \rightarrow U(10)$

$\phi(e) = e'$ and $\phi(a^{-1}) = [\phi(a)]^{-1}$

Where $e = o \in z_4$

$e' = 1 \in U(10)$ are identity elements and $a \in z_4$

That $\phi(0) = 1$

$\phi(1) = 3$

$\phi(2) = 4$

$\phi(3) = 2$

Here $\phi : z_4 \rightarrow U_{10}$ is an isomorphisms

i.e., $z_4 \approx U(10)$

Now, let the mapping $\psi : z_4 \to U(5)$ is defined as

$\psi(e) = e'$ & $\psi(a^{-1}) = [\psi(a)]^{-1}$

Where $e = 0 \in z_4$

$e' = 1 \in U(5)$ are identity

Elements and $a \in z_4$

Then $\phi(0) = 1$, $\phi(1) = 7$, $\phi(2) = 9$, $\phi(3) = 3$

Hence $\psi : z_4 \to U(5)$ is an isomorphism

i.e., $z_4 \approx U(5)$

Q20. Prove that U(10) $\approx$ U(12)

Sol :

Let $U(10) = (\{1, 3, 7, 9\}, .)$

and $U(12) = (\{1, 5, 7, 11\}, .)$ are groups

There doesn't exist any mapping

$\phi : U(10) \to U(12)$ is an isomorphism.

Since,

$\forall a \in U(12) \to a^2 = 1$

i.e, 1, 5, 7, 11 $\in U(12) \Rightarrow 1^2 = 1$

$3^2 = 5$

$7^2 = 1$

$11^2 = 1$

Now $\phi(9) = \phi(3 . 3) = \phi(3) \ \phi(3) = 1$

$\phi(1) = \phi(1 . 1) = \phi(1) . \phi(1) = 1$

But $\phi(9) = \phi(1) \Rightarrow 9 \neq 1$

$\therefore$ $U(10) \approx U(12)$

Q21. Let G = SL (2, R) be a group of 2 × 2 real matrices with determinant 1.

Show that the mapping $\phi_M : G \to G$ be defined by $\phi_M(A) = MAM^{-1}$, $\forall A \in G$ is an isomorphism.

Sol :

$$\text{Let } G = SL(2, R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Big/ ad - bc = 1 \ \&\ a, b, c, d \in R \right\}$$

Be a group under multiplication

Let M be any 2 × 2 real matrix with determinant 1.

i.e., $M = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \Rightarrow \det M = ps - qr = 1$ for $p, q, r, s \in R$.

Let the mapping $\phi_m : G \to G$ be defined by $\phi_m(A) = MAM^{-1}$ then prove that ϕ_m is an isomorphism.

Now consider $(MAM^{-1}) = (\det M)(\det A)(\det M)^{-1}$

$= 1 . 1 . 1^{-1}$

$= 1$

$\therefore$ $\det(MAM^{-1}) = 1$

$\Rightarrow$ $MAM^{-1} \in G$

$\Rightarrow$ $\phi_m(A) = MAA^{-1}$

$\therefore$ ϕ_m is well defined.

Let $A, B \in G \Rightarrow \phi_m(A) = MAM^{-1}$

and $\phi_m(B) = MBM^{-1}$

Consider $\phi_m(A) = \phi_m(B)$

$MAM^{-1} = MBM^{-1}$

$\Rightarrow$ $A = B$ [By left & light cancellation law]

$\therefore$ ϕ_m is one - one

$\forall\ B \in G \Rightarrow B = MAM^{-1}\ \exists\ A \in G$ such that $\det B = \det MAM^{-1} = 1$

$\Rightarrow$ $A = MAM^{-1} \in G$

$\Rightarrow$ $\phi_m(A) = MAM^{-1}$

$\Rightarrow$ $M(M^{-1}BM)M^{-1}$

$\Rightarrow$ $(MM^{-1})B(MM^{-1})$

$\Rightarrow$ I B 1

$\Rightarrow$ B

ϕ_m is onto.

Let $A, B \in G \Rightarrow \phi_m(A) = MAM^{-1}$ and $\phi_m(B) = MBM^{-1}$

Then $AB \in G \Rightarrow \phi_m(AB) = M(AB)M^{-1}$

$= MA . I . M^{-1}$

$= MAM^{-1} . MBM^{-1}$

$= \phi_m(A) . \phi_m(B)$

$\therefore$ $\phi_m(AB) = \phi_m(A) . \phi_m(B)$

ϕ_m is homomorphism.

$\therefore$ ϕ_m is Isomorphism.

Q22. Every group is isomorphic to a group of permutations.

Ans :

Given that G is a finite group.

Consider $f_a : G \to G$ defined by $f_a(x) = ax$

$\forall\ x \in G$

Required to prove f_a is a permutation on G

i.e, to prove

(i) f_a is well defined

(ii) f_a is one - one

(iii) f_a is onto

(i) Let x, y $\in$ G

$ax, ay \in G$

$x = y \Rightarrow ax = ay$

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

$\therefore$ f_a is well defined

(ii) Let x, y $\in$ G

We have $f_a(x) = f_a(y)$

$\Rightarrow ax = ay$

$\Rightarrow x = y$

$\therefore$ f_a is one - one

(iii) f_a is onto

$x \in G, \exists\ a^{-1} x \in G$

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

$= (aa^{-1})x$

$= e . x$

$= x$

$f_a : G \to G$ is onto

$\therefore$ f_a is $G \to G$ is permutation on G

Let us define $G' = \{f_a / a \in G\}$

Let G' be the set of all permutation defined on G.

Here, we required to prove,

G' is a group w.r.to permutation multiplications.

(a) Closure Property

Let $a, b \in G$, $f_a, f_b \in G'$

for $x \in G$,

Consider $(f_a f_b)(x) = f_a(f_b(x))$

$= f_a(bx)$

$= a(bx)$

$= (ab)x$

$(f_a f_b)(x) = f_{ab}(x)$

$f_{ab} \in G' \Rightarrow f_a f_b \in G'$

(b) Associative Property

For $a, b, c \in G$, $f_a, f_b, f_c \in G'$

For $x \in G$

Consider

$((f_a f_b) f_c)(x) = f_a((f_b) f_c(x))$

$= f_a f_b ((f_c)(x))$

$= f_a f_b (f_c(x))$

$= f_a(f_b f_c(x))$

$(f_a f_b) f_c = f_a (f_b f_c)$

(c) Existence of Identity

Let e be the identity in G

$f_e \in G$ & $f_e f_a = f_{ea} = f_a$

$f_a f_e = f_{ae}$

$= f_a$

Identity in G' is exists

(d) Existence of Inverse

If $a \in G \Rightarrow a^{-1} \in G'$

$f_{a^{-1}} \in G^1$ and $f_{a^{-1}} f_a = f_{a^{-1}a}$

$= f_e$

G' is invertible

G' is a group

Next to show that $G \cong G'$

Consider $\phi : G \to G'$ defined by $\phi(a) : f_a$ for $a \in G$

ϕ is one one

Consider ϕ (a) = ϕ . (b)

$f_a = f_b$

$f_a(x) = f_b(x)$

ax = bx

a = b for x $\in$ G,

a, b $\in$ G

ϕ is onto

Consider $f_a \in G'$, $a \in G$ such that

$\phi(a) = f_a$

ϕ is structure preserving

Since a, b $\in$ G

ab $\in$ G

ϕ (ab) = f_{ab}

$= f_a f_b$

$= \phi(a)\, \phi(b)$

$\therefore$ G $\cong$ G'

G' is called permutation group.

$\therefore$ Every finite group G is a isomorphic to the permutation group G'

Q23. Find the regular permutation group $\overline{U(12)}$ for U(12)

Sol :

Let U(12) = {1, 5, 7, 11}

Which is a group under multiplication

By Cayley`s Table.

U(12)	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

By Caylay`s Theorem

T_f : U(12) $\rightarrow$ U(12) which is defined by

$T_f(x) = f(x) \ \forall \ x \in U(12)$

If $f = 1 \in U(12) \Rightarrow T_1 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{pmatrix}$

If $f = 5 \in U(12) \Rightarrow T_2 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{pmatrix}$

If $f = 7 \in U(12) \Rightarrow T_7 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{pmatrix}$

If $f = 11 \in U(12) \Rightarrow T_{11} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 11 & 5 & 7 & 1 \end{pmatrix}$

Then the permutation group is

$U(12) = \{T_1, T_5, T_7, T_{11}\}$ under multiplication

Then the regular representation of $\overline{U(12)}$

•	T_1	T_5	T_7	T_{11}
T_1	T_1	T_5	T_7	T_{11}
T_5	T_5	T_1	T_{11}	T_7
T_7	T_7	T_{11}	T_1	T_5
T_{11}	T_{11}	T_7	T_5	T_1

Here $U(12) \approx \overline{U(12)}$

2.6 Properties of Isomorphism

Q24. Suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$ then ϕ carries the identity of G to the identity of $\bar{G}$

Ans :

Let us denote the identity in G by e and identity in $\bar{G}$ by $\bar{e}$

Then, Since, e = ee

Then we have $\phi(e) = \phi(ee)$

$\phi(ee) = \phi(e)$

$\Rightarrow \phi(e)\, \phi(e) = \bar{e}\, \phi(e)$

(ϕ is homomorphism

$\bar{e}$, $\phi(e) \in \bar{G}$)

$\Rightarrow$ $\phi(e) = \bar{e}$ By right can cancellation done in $\bar{G}$

Q25. Suppose that ϕ is an isomorphism from group G onto a group $\bar{G}$ than for every integer n and for every group element a in G, $\phi(a^n) = [\phi(a)]^n$

Ans :

Let (G, $\circ$) and ($\bar{G}$, $\cdot$) be two groups.

Let $\phi : G \to \bar{G}$ is an isomaplism required to prove

$\phi(a^n) = [\phi(a)]^n \ \forall \ a \in G \ \& \ \forall \ n \in Z$ ... (1)

Case (i) :

Let $n \in z^+$

By using mathematical induction

for $n = 1$

L. H. S = $\phi(a^1) = \phi(a)$

$= [\phi(a)]^1$

= R. H. S

$\therefore$ equation (1) is true for $n = 1$

Assume that equation (1)

is true for $n = k$

i.e., $\phi(a^k) = [\phi(a)]^k$ ... (2)

$\phi(a^{k+1}) = \phi(a^k . a)$

$= \phi(a^k) \ \phi(a)$

[$\because$ ϕ homomorphism]

$= [\phi(a)]^k \ \phi(a)$

[$\because$ equation (2)]

$= [\phi(a)]^{k+1}$

Equation (1) is true for $n = k+1$

$\therefore$ $\phi(a^n) = [\phi(a)]^n \quad \forall \ n \in z^+$

Case (ii) :

Let $n \in z^-$ Then $m = -n$

$\therefore$ $m \in z^+$

$\Rightarrow$ $\phi(a^m) = [\phi(a)]^m$ [$\because$ Case (i)]

$\Rightarrow$ $\phi(a^{-n}) = [\phi(a)]^{-n}$

$\therefore$ $\phi(a^n) = [\phi(a)]^n \quad \forall \ n \in z^-$

Case (iii)

Let $n = o \in z$

$\phi(a^o) = \phi(e)$

$= e^1 = [\phi(a)]^0$

$\therefore$ $\phi(a^n) = [\phi(a)]^n \quad \forall \ n \in z^-$

Q26. Suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$ for any elements a & b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commutes.

Ans :

Let 'G' be a group, a, b $\in$ G

$\Rightarrow$ (G, $\cdot$) be an abelian group

($\bar{G}$, $\cdot$) be an isomorphic group.

$\phi : G \to \bar{G}$ be a onto

$\forall$ a, b $\in$ $\Rightarrow$ ab = ba ... (1)

Required to prove $\phi(a). \phi(b) = \phi(b) . \phi(a)$

Consider

$\phi(a) . \phi(b) = \phi(ab)$ $\phi$is homomorphic

$= \phi(b \ a)$

$= \phi(b) . \phi(a)$

f is homomorphic

$\therefore$ $\phi(a) . \phi(b) = \phi(b) . \phi(a)$

Conversely suppose that,

$\phi(a) . \phi(b) = \phi(b) . \phi(a)$

Then required to prove ab = ba.

Consider

$\phi(a) \ \phi(b) = \phi(b) \ \phi(a)$

$\Rightarrow$ $\phi(ab) = \phi(ba)$

(ϕ is homomorphism)

$\Rightarrow$ ab = ba

(ϕ is one one)

Q27. Let ϕ be an isomorphism from group G onto group $\bar{G}$. Then G = <a> if and only if $\bar{G}$ = <ϕ(a)>.

Ans :

Let (G, $\cdot$) & ($\bar{G}$, $\cdot$) ba a two groups

$\phi : G \to \bar{G}$ is an isomorphism.

Suppose that : G = <a> then prove that

$\bar{G} = \langle\phi(a)\rangle = \{(\phi(a))^n / n \in z\}$ is a cyclic group

Let $G = \langle a \rangle = \{a^n / n \in z\}$ be a cyclic group

$\forall\ \phi(a) \in \bar{G}$

$\Rightarrow \exists\ a \in G \Rightarrow a^n \in G$

$\Rightarrow \phi(a^n) \in \bar{G}$

$\Rightarrow \phi(a^n) = [\phi(a)]^n \quad \forall\ n \in z$

$\therefore \bar{G} = \langle\phi(a)\rangle$ is a cyclic group

Conversely suppose that

Let $\bar{G} = \langle\phi(a)\rangle$ is a cyclic group

Required to prove

G = <a> is a cyclic group

$\forall\ a \in G \Rightarrow \phi(a) \in \bar{G}$

$\Rightarrow [\phi(a)]^n \in \bar{G} \ \forall\, n \in z$ [$\because \bar{G}$ is a cyclic]

$\Rightarrow \phi(a^n) \in \bar{G} \quad \forall\ n \in z$

$\Rightarrow a^n \in G$ ϕ is onto

$\therefore G = \langle a \rangle = \{a^n / n \in z\}$

Which is a cyclic group.

Q28. Suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$ then |a| = |ϕ(A)| $\forall$ a in G (isomorphism preserve orders).

Ans :

Let G, $\bar{G}$ be a two group.

$\phi : G \to \bar{G}$ is an isomorphism.

Let $a \in G$ of order n

i.e., |a| = n

Then, Required to prove $|a| = n$

By definition $a^n = e$ where e is an identity in G

$\Rightarrow \phi(a^n) = \phi(e)$

$\Rightarrow \phi(a . a .... a) = e'$ $e' \in \bar{G}$

$\Rightarrow \phi(a) . \phi(a) .... \phi(a) = e'$

$[\phi(a)]^n = e'$

Order of $\phi(a) \leq n$ ... (1)

Suppose that the orders of $\phi(a)$ is m

where $m < n$

Then $[\phi(a)]^m = e'$

$\phi(a^m) = \phi(e)$ $[\because \phi(e) = e']$

$a^m = e$ $[\because \phi$ is one one]

which is a contradiction

Since n is the least integer such that $a^n = e$

$\therefore$ $m = n$

$\therefore$ Hence $|\phi(a)| = m = n = |a|$

$\therefore$ $|\phi(a)| = n$

$\therefore$ $|\phi(a)| = |a|$

Q29. Let ϕ be an isomorphism from a group G onto a group $\bar{G}$, then for a fixed integer K and a fixed group elements b in G. The equation $x^k = b$ has the same number of solution in G as does the equation $x^k = \phi(b)$ in $\bar{G}$.

Ans :

Let G , $\bar{G}$ be two groups.

Let $\phi : G \rightarrow \bar{G}$. be an isomorphism for a fixed integer K, and fixed group elements b in G.

Then the equation $x^k = b$ has the same in G.

But $x^k = \phi(b)$ does not have same number of solutions in $\bar{G}$.

Example :

Let $G = C^*$ & $\bar{G} = R^*$

$K = 4$ & $b = 1$ (identity)

Then $x^4 = 1$ has four solutions in C^*

i.e., $x = \{-1, \pm, i, -i\}$

But the equation $x^4 = \phi(1) = 1$

has two solutions in R^*

Q30. Suppose that ϕ is isomorphism from a group G onto a group $\bar{G}$. Than If G is finite, Then G and $\bar{G}$ have exactly the same number of elements of every order.

Ans :

Let G & $\bar{G}$ be a two groups

$\phi : G \to \bar{G}$ is an isomorphism

Let G be a finite

The order of G be 'n'

i.e., $|G| = n$

$a \in G, \Rightarrow |a| = n \Rightarrow a^n = e = 1$

$\therefore \quad \phi(G) = \bar{G} \qquad \because \phi$ is onto

$1 = \phi(1) = \phi(a^n) = [\phi(a)]^n$

$\therefore$ G & $\bar{G}$ have exactly the same number of elements of every order.

Q31. Suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$. Then ϕ^{-1} is an isomorphism from $\bar{G}$ onto G.

Ans :

Let G, $\bar{G}$ be a two groups.

$\phi : G \to \bar{G}$ is an isomorphism

and $\phi|G| = \{\phi(a) \in \bar{G} \ / \ a \in G\}$

$a \in G \Rightarrow b = \phi(a) \in \phi(G)$

$= \bar{G}$

Then $\phi^{-1}(\bar{G}) = \{\phi^{-1}(b) \ / \ b \in \bar{G}\}$

$\Rightarrow \quad a = \phi^{-1}(b) \in \phi^{-1}(\bar{G}) = G$

Consider

$\phi^{-1}(b_1) = \phi^{-1}(b_2)$

$\Rightarrow \phi(\phi^{-1}(b_1)) = \phi(\phi^{-1}(b_2)) \qquad [\because \phi$ one - one]

$\Rightarrow eb_1 = eb_2$

$\Rightarrow b_1 = b_2$

$\therefore \phi^{-1}$ is one one.

$\forall g \in G \Rightarrow \phi(g) \in \phi(G) = \bar{G}$

$\Rightarrow \quad \phi(g) = g'$

$\exists\ g' \in \bar{G} \Rightarrow \phi^{-1}(\phi(g))$

$\Rightarrow \phi^{-1}(g^{-1})$

$\Rightarrow g = \phi^{-1}(g^{-1})$

$\therefore$ ϕ^{-1} is onto

$\forall\ x, y \in \bar{G} = \phi(G)$

$\Rightarrow x^1 = \phi(x)\ \&\ y^1 = \phi(y)\ \exists\ X, Y \in G$

$\Rightarrow \phi^{-1}(x^1) = x\ \&\ \phi^{-1}(y^1) = y$ [$\because$ ϕ^{-1} is one one.]

Now $x', y' \in \bar{G} \Rightarrow \phi^{-1}(x'y')$

$= \phi^{-1}(\phi(x) . \phi(y))$

$= \phi^{-1}(\phi(xy))$ [$\because$ ϕ is homomorphism]

$= e(xy)$

$= xy$

$= \phi^{-1}(x')\ \phi^{-1}(y')$

$\therefore$ $\phi^{-1}(x'y') = \phi^{-1}(x')\ \phi^{-1}(y')$

$\therefore$ ϕ^{-1} is a homomorphism.

Hence ϕ^{-1} is an isomorphism.

Q32. Suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$ then G is abelian if and only if $\bar{G}$ is Abelian.

Ans :

Let G & $\bar{G}$ be a two groups

$\phi : G \to \bar{G}$ is an isomorphic

Let G be an abelian group

Then required to prove $\bar{G}$ is an abelian group.

Let $a, b \in G$ abd $a', b' \in \bar{G}$

$\forall\ a'\ b' \in \bar{G} \Rightarrow a' = \phi(a)\ \exists\ a \in G$

$\&\ \ b' = \phi(b)\ \exists\ b \in G$

Consider

$a^1b^1 = \phi(a)\ \phi(b)$

$= \phi(ab)$

$= \phi(ba)$

$= \phi(b) . \phi(a)$

$= b^1 . a^1$

$\therefore \quad a^1b^1 = b^1a^1$

$\therefore \quad \bar{G}$ is abelian group.

Conversely suppose that

$\bar{G}$ is an abelian group then prove that G is an abelian group.

$\forall\ a, b \in G \Rightarrow a = \phi^{-1}(a^1) \qquad \exists\ d \in \bar{G}$

$\Rightarrow a = \phi^{-1}(b^1) \qquad \exists\ b' \in \bar{G}$

Consider

$ab = \phi^{-1}(a^1)\,\phi^{-1}(b^1)$

$= \phi^{-1}(a^1b^1)$ [$\because \phi$ is homomorphism]

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

$= \phi^{-1}(b^1)\,\phi^{-1}(a^1)$

$= b\,.\,a$

$\therefore \quad ab = ba. \qquad \forall\ a, b \in G$

$\therefore$ G is an abelian group

Q33. Let ϕ be an isomorphism from G to $\bar{G}$. If K is a subgroup of G. Then $\phi(k) = \{\phi(k) / k \in K\}$ is a subgroup of $\bar{G}$

Ans : **(Jan.-21)**

Let G and $\bar{G}$ be the two groups.

and $\phi : G \to \bar{G}$ is isomorphism.

Let K be a subgroup of G.

Then $\phi(K) = \{\phi(k) / k \in K\}$ is subset of $\bar{G}$

i.e., $e = 1 \in G$

$\phi(e) = e' = 1 \in \phi(k)$

$\phi(k) \neq \phi$ and $\in \phi(k) \in \bar{G}$

$\forall\ \phi(k_1), \phi(k_2) \in \phi(k) \Rightarrow \exists\ k_1, k_2 \in k.$

$\Rightarrow \quad k_1 - k_2 \in k$ and $k_1 . k_2 \in k$

$\Rightarrow \quad \phi(k_1 - k_2) \in \phi(k)$ and $\phi(k_1 . k_2) \in \phi(k)$

Consider

$\phi(k_1) - \phi(k_2) \in \phi(k_1 - k_2) \in \phi(k)$

& $\quad \phi(k_1) . \phi(k_2) \in \phi(k_1\ k_2) \in \phi(k)$

$\therefore \quad \phi(k)$ is a subgroup of $\bar{G}$.

Q34. Suppose that is an isomorphism from a group G onto a group $\bar{G}$ then, If $\bar{K}$ is a subgroup of $\bar{G}$ then $\phi^{-1}(\bar{K}) = \{g \in G / \phi(g) \in \bar{K}\}$ is a subgroup of G.

Ans :

Let G & $\bar{G}$ be a two groups.

Let $\phi : G \to \bar{G}$ be an isomorphism.

Let $\bar{K}$ be a subgroup of $\bar{G}$

Then required to prove that

$\phi^{-1}(\bar{K})$ is a subgroup of G.

Let $e' = 1 \in \bar{G} \Rightarrow e' \in \bar{K}$

$\Rightarrow \phi(e) = e' = 1$

$\Rightarrow \quad e' = \phi^{-1}(e) = 1 \in \phi^{-1}(\bar{K})$

$\therefore \quad \phi^{-1}(\bar{K}) = \phi$ and $\phi^{-1}(\bar{K}) \in G$

$\phi(g_1) = g_1' \ \forall \ g_1 \in \phi^{-1}(\bar{K})$

$\phi(g_2) = g_2' \ \forall \ g_2 \in \phi^{-1}(\bar{K})$

$\Rightarrow \quad g_1 = \phi^{-1}(g_1') \ \& \ g_1 = \phi^{-1}(g_2') \qquad \exists \ g_1', g_2' \in \bar{K}$

$\Rightarrow \quad g_1' - g_2', \in \bar{K} \ \& \ g_1'.\ g_2' \in \bar{K}$

$\Rightarrow \quad \phi(g_1' - g_2') \in \phi(\bar{K})$ and $\phi(g_1'.\ g_2') \in \phi(\bar{K})$

Consider

$\phi(g_1 - g_2) = \phi^{-1}(g_1') - \phi(g_2')$

$= \phi^{-1}(g_1' - g_2') \in \phi(\bar{K})$

and $g_1 g_2 = \phi^{-1}(g_1')\ \phi(g_2')$

$= \phi^{-1}(g_1'.\ g_2') \in \phi^{-1}(\bar{K})$

$g_1 g_2 = \phi^{-1}(g_1'.\ g_2')$

$\therefore \quad \phi^{-1}(\bar{K})$ is a subgroup of G.

2.7 AUTOMORPHISM

Q35. Define Automorphism.

Ans :

An isomorphism from a group G onto it self is called an automorphism of G.

Q36. The function $\phi : C \rightarrow C$ given by $\phi(a + bi) = a - bi$ be an automorphism of the group of complex number under addition.

Sol :

Let (C. +) be a group

$\phi : C \rightarrow C$ is define by $\phi(a + bi) = a - bi \ \forall \ a, b \in R$.

To prove ϕ is automorphism required to prove one - one, onto & homomorphism (i.e., to prove isomorphism).

$\forall \ a_1 + i b_1, a_2 + b_2 i \in C$

Consider

$\phi(a_1 + b_1 i) = \phi(a_2 + b_2 i)$

$\Rightarrow \ a_1 - i b_1 = a_2 - i b_2$

$\Rightarrow \ a_1 = a_2$ and $b_1 = b_2$

$\Rightarrow \ a_1 + b_1 i = a_2 + b_2 i$

$\therefore$ ϕ is one - one

$\forall a - b i \in C \Rightarrow a + (-b) i \in C$

$\Rightarrow \ \phi(a + i(-b)) = a - i(-b)$

$= a + ib \in C$

$\therefore$ ϕ is onto

$\forall \ a_1 + ib_1, a_2 + ib_2 \in C$

$\Rightarrow \ (a_1 + ib_1) + (a_2 + ib_2)$

$\Rightarrow \ (a_1 + a_2) + i(b_1 + b_2)$

$= \ \in C$

Consider

$\phi[(a_1 + ib_1) + (a_2 + ib_2)] = \phi[(a_1 + a_2) + i(b_1 + b_2)]$

$\Rightarrow \ (a_1 + a_2) - (b_2 + b_2)i$

$\Rightarrow \ (a_1 - bi) + (a_2 - b_2 i)$

$\Rightarrow \ \phi(a_1 + ib_1) + \phi(a_2 + ib_2)$

$\therefore$ ϕ is Homomorphism.

$\therefore$ ϕ is an isomorphic

$\therefore$ $\phi : c \rightarrow c$ is Automorphism,

Q37. $R^2 = \{(a, b) / a, b \in R\}$. Then $\phi(a, b) = (b, a)$ is an automorphism of the group R^2 under component wise addition.

Sol :

Given, $R^2 = \{(a, b) / a, b \in R\}$

$\phi : R^2 \rightarrow R^2$, defined as $\phi(a, b) = (b, a)\ \forall (a, b) \in R^2$

$\phi(a_1, b_1) = (b_1, a_1)$ & $\phi(a_2, b_2) = (b_2, a_2)\ \forall (a_1, b_1)$ & (a_2, b_2) & $\in R^2$

Consider

$\phi(a_1, b_1) = \phi(a_2, b_2)$

$\Rightarrow (b_1, a_1) = (b_2, a_2)$

$\Rightarrow b_1 = b_2,\ a_1 = a_2$

$\Rightarrow (a_1, b_1) = (a_2, b_2)$

ϕ is one one.

$\Rightarrow \phi(a, b) = (b, a) \in R^2\ \forall\ (a, b) \in R^2$

ϕ is onto

Now , Consider

$\phi[(a_1, b_1) + (a_2, b_2)] = \phi[(a_1 + a_2) + (b_1 + a_2)]i$

$= (a_1 + a_2) - (b_1 + b_2)i$

$= (a_1 - b_1 i) + (a_2 - b_2 i)$

$= \phi(a_1, b_1) + \phi(a_2, b_2)$

$\therefore$ ϕ is Homomorphim

$\therefore$ ϕ is an automorphism of group R^2

Q38. What is Inner Automorphism?

Ans :

Let G be a group, & Let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}\ \forall\ x \in G$ is called the inner automorphism of G induced by a.

Q39. The set of Automorphism of a group and the set of inner Automorphism of group are both group under the operation of function composition.

Ans : **(Jan.-21)**

Let $\phi_a : G \rightarrow G$ is an isomorphism.

Let $a \in G$ & the set of all inner Automorphism of G induced by a

$Inn(G) = \{\phi_a / \phi_a(x) = axa^{-1}\ \forall\ x \in G\}$

Closure Property :

Let $\phi_a, \phi_b \in Inn(G) \Rightarrow \phi_a(x) = axa^{-1}$

$\Rightarrow \phi_a(x) = bxb^{-1}\ \forall\ x \in G$

Consider

$(\phi_b \circ \phi_a)(x) = \phi_b[\phi_a(x)]$

$= \phi_b[axa^{-1}]$

$= b[axa^{-1}]b^{-1}$

$= (b\,a)\,x\,(a^{-1}\,b^{-1})$

$= (b\,a)\,x\,(b\,a)^{-1}$

$\therefore \quad (bxb^{-1})\,(axa^{-1}) = (ba)x\,(ba)^{-1} \in \text{Inn}\,(G)$

Associative Property :

Let $\phi_a, \phi_b, \phi_c \in \text{Inn}\,(G)$

$\phi_c(x) = cxc^{-1}, \;\forall\; x \in G$

Consider

$[(\phi_a \circ \phi_b) \circ \phi_c]\,(x) = (\phi_a \circ \phi_b)\,[\phi_c(x)]$

$= \phi_a[\phi_b(\phi_c(x))]$

$= \phi_a[\phi_b(cxc^{-1})]$

$= \phi_a[b(cxc^{-1})b^{-1}]$

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

$= [(ab)\,c]\,x\,[c^{-1}(a^{-1}b^{-1})]$

$= [(ab)\,c]\,x\,[c^{-1}(ab)^{-1}]$

$= [(ab)\,c]\,x\,[(a\,b)\,c]^{-1}$

$= [(a\,(bc]\,x\,[a\,(bc)]^{-1}$

$= [\phi_a \circ (\phi_b \circ \phi_c)]\,(x)$

$\therefore$ Inn (G) is satisfies the Associative.

Identity Property :

$\therefore \quad e \in G \Rightarrow \phi_2 \in \text{Inn}(G)$

$\phi_2(x) = e\,x\,e^{-1}$

$= e\,x\,e$

$= x$

$(\phi_e \circ \phi_a)\,(x) = \phi_e\,[\phi_a(x)]$

$= \phi_e\,(ax\,a^{-1})$

$= e(ax\,a^{-1})\,e^{-1}$

$= (e\,a)\,x\,(a^{-1}\,e^{-1})$

$= (e\,a)\,x\,(ea)^{-1}$

$= ax\,a^{-1}$

$(\phi_e \circ \phi_a)\,(x) = \phi_a\,(x)$

By $(\phi_a \circ \phi_e)\,(x) = \phi_a\,(x)$

$\therefore \quad \phi_e = I$ is an identity element of Inn(G)

Inverse Property :

Consider $(\phi_a \circ \phi_{a^{-1}})(x) = \phi_a [\phi_{a-1}(x)]$

$= \phi_a [a^{-1} xa^{-1}]^{-1}$

$= (a^{-1} xa^{-1})^{-1}$

$= (aa^{-1})\, x\, (aa^{-1})^{-1}$

$= ex\, a^{-1}$

$= \phi_e (x)$

Similarly

$(\phi_{a^{-1}} \circ \phi_a)(x) = \phi_e (x)$

$\therefore$ Inn(G) is satifies the inverse property

$\therefore$ Inn(G) is group under the operation of composition of function.

Q40. Compute Aut (Z_{10}).

Sol :

Let $Z_{10} = \{0, 1, 2, 3, ... 9\}$ be a group

Under addition modulo 10.

By definition of Automorphism of G

Aut (G) = $\{\alpha / \alpha : Z_{10} \to Z_{10}$ is isomorphism$\}$

Consider

$\alpha(K) = \alpha(1 + 1 + ... + 1$ (K times)

$= \alpha(1) + \alpha(1) + ... + \alpha(1)$

$= K \,.\, \alpha(1)$

$|\alpha(1)| = 10$ and $\alpha(1) = 1$, $\alpha(1) = 3$, $\alpha(1) = 7$, $\alpha(1) = 9$

Aut (Z_{10}) = $\{\alpha_1, \alpha_3, \alpha_7, \alpha_9\}$ is group under multiplication with identity α_1

By Cayley's table

	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

Q41. From every positive integer n, Aut (Z_n) is isomorphic to U(n).

Ans :

Let 'n' be a positive integer

and Aut (Z_n) & U(n) are groups under multiplication.

T : Aut (Z_n) $\rightarrow$ U(n) be defined by $T(\alpha) = \alpha(1)$ with $\alpha(K) = K \cdot \alpha(1) \quad \forall\ K \in Z_n$

$\alpha, \beta \in$ Aut (Z_n)

$\alpha(1) = \beta(1)$

$\Rightarrow \quad \alpha(K) = K \cdot \alpha(1)$

$K \cdot \beta(1) = \beta(K)$

$\therefore \quad \alpha(K) = \beta(K) \quad \forall\ K \in Z_n$

Consider

$T(\alpha) = T(\beta)$

$\Rightarrow \quad \alpha(1) = \beta(1)$

$\Rightarrow \quad \alpha = \beta$

$\therefore$ T is one - one

Let $r \in U(n)$

Consider

$\alpha : Z_n \rightarrow Z_n$

$\alpha(S) = Sr \pmod n \quad \forall\ S \in Z_n$

Then α is an isomorphism of Z_n

$\therefore \quad T(\alpha) = \alpha(1) = r$

T is onto from Aut (Z_n) to U(n)

Let $\alpha, \beta \in$ Aut (Z_n)

Then $T(\alpha\beta) = (\alpha\beta)(1) = \alpha(\beta(1))$

$= \alpha(1 + 1 + ... + 1)$

$= \alpha(1) + \alpha(1) + ... + \alpha(1)$ ($\beta(1)$ times))

$= \alpha(1) \cdot \beta(1)$

$= T(\alpha) \cdot T(\beta)$

$\therefore$ T is homomorphim

Hence Aut (Z_n) $\approx$ U(n)

2.8 Cosets and Lagrange's Theorem - Properties of Cosets

Q42. Define right coset of H in G and left coset of H in G.

Ans :

Let G be a group and let H be a non empty subset of G. For any $a \in G$. The set $\{ah / h \in H\}$ is denoted by aH, is called left coset of H in G generated by a and the set $Ha = \{ha / h \in H\}$ is called right coset of H in G generated by a.

Q43. Let G = S_3 and H = {(1), (1, 3)}. Then find left cosets of H in G are

Sol :

Let G = S_3

= $\{f_1\ f_2\ f_3\ f_4\ f_5\ f_6\}$

= {(1) (1 2) (1 3) (2 3) (1 2 3) (1 3 2)}

is a group under permutation, multiplication and

$$H = \{(1), (1\ 3)\} = \left\{\begin{pmatrix}1\\2\end{pmatrix}\begin{pmatrix}1 & 3\\3 & 1\end{pmatrix}\right\} \text{ is a subgroup of G}$$

(1) ∈ G ⇒ (1) H ⇒ {(1) (1), (1) (1 3)}

= ((1), (1 3)} = H

(1 2) ∈ G ⇒ (1 2) H ⇒ {(1 2) (1), (1 2) (1 3)}

= {1 2), (1 3 2)}

= (1 3 2)

= H

(1 3) ∈ G ⇒ (1 3) H = {1 3) (1), (1 3) (1 3)}

= {(1 3), (1 3)}

= H

(2 3) ∈ G ⇒ (2 3) H = {2 3) (1), (2 3) (1 3)}

= {(2 3), (1 2 3)}

= (1 2 3) H

Q44. Let H = {0, 3, 6} is Z_9 under addition. Then find the left cosets of H is Z_9.

Sol :

Let Z_9 = {0, 1, 2, 3, 4, 5, 6, 7, 8}

is group under addition modulo 9

and H = {0, 3, 6} is a subgroup of Z_9

$0 \in Z_9 \Rightarrow 0 + H = \{0, 3, 6\} = 3 + H = 6 + H$

$1 \in Z_9 \Rightarrow 1 + H = \{1, 4, 7\} = 4 + H = 7 + H$

$2 \in Z_9 \Rightarrow 2 + H = \{2, 5, 8\} = 5 + H = 8 + H$

Q45. Let H be a subgroup of G, and let a belong to G. Then, a H = subgroup of G ⇔ a ∈ H

Ans :

Let (G, ·) be group

H be a subgroup of G

Let a ∈ G

Then the left coset H in G is

$aH = \{ah / h \in H\}$ is a subset of G

i.e., $e \in H \Rightarrow a \,.\, e = a \in a H$

$\therefore \quad aH \neq \phi$ and $aH \subseteq G$

Let aH be a subgroup of G

Then required to prove $a \in H$

$aH = eH \Leftrightarrow a \in e H$

$aH = H$ is subgroup $\Leftrightarrow a \in H$

Q46. Let H be a subgroup of group G and a, b $\in$ G then (ab) H = a(bH) and H(ab) = (Ha) b

Ans :

Let (G, ·) be group

H be a subgroup of G

Let $a, b \in H$ then the left cosets of G

is $bH = \{bh / h \in H\}$

Consider

$$a\,(bH) = \{a\,(bh) / h \in H\}$$
$$= \{(ab)\,h / h \in H\}$$
$$= (ab)\,H$$

$\therefore \quad (ab)\,H = a(bH)$

Similarly,

The right coset H of G is $Ha = \{ha / h \in H\}$

Consider $(Ha)\,b = \{(ha)\,b / h \in H\}$

$$= \{h\,(ab) / h \in H\}$$
$$= H\,(ab)$$

$\therefore \quad (Ha)\,b = H(ab)$

Q47. Let H be a subgroup of G, and Let a & b belong to G aH = bH if and only if a $\in$ bH

Ans :

H be a subgroup of G

$a, b \in H$

Suppose that $aH = bH$

Required to prove $a \in bH$

$\because \quad a \in aH$ where $a \in bH \qquad (\because\ aH = bH)$

Conversely suppose that $a \in bH$

Required to prove $aH = bH$

$a \in bH \Rightarrow a = bH$

Consider $aH = (bh)H$

$= b(hH)$

$= bH$

$aH = bH$

Q48. Let H be a subgroup of G, & a, b $\in$ G

Then aH = bH or aH $\cap$ bH = ϕ

Ans :

Let H be a subgroup of G

& $a, b \in G$

Here aH & bH are left cosets of H in G

1. If aH & bH are dijoint

i.e., $aH \cap bH = \phi$. Then there is nothing to prove.

2. If aH & bH are not adjust

i.e., $aH \cap bH \neq \phi$

$\exists\ c \in aH \cap bH$

$c \in aH \Rightarrow c = a.h_1$ where $h_1 \in H$

$c \in bH \Rightarrow c = b.h_2$ where $h_2 \in H$

$\therefore$ $ah_1 = bh_2$

Multiply with h_1^{-1} both sides

$(ah_1)\, h_1^{-1} = (bh_2)\, h_1^{-1}$

$a(h_1 h_1^{-1}) = b(h_2 h_1^{-1})$

$ae = bh_2 h_1^{-1}$

$a = bh_3$

We shall prove that

$aH = bH$

Consider $aH = (bh_3)H$

$= b(h_3H)$

$= bH$

$\therefore$ $aH = bH$

Q49. Let H be a subgroup of G, & a, b $\in$ G

Then $aH = bH \Leftrightarrow a^{-1}b \in H$

Ans :

H subgroup of G

Required to prove $aH = bH \Leftrightarrow a^{-1}b \in H$

Suppose that $aH = bH$

i.e., to prove $a^{-1}b \in H$

Consider bH & $b \in H$

$\Rightarrow \quad b \in aH$

$= \quad b = ah$ where $h \in H$

Multiply with a^{-1} on both sides

$a^{-1}b = a^{-1}(ah)$

$a^{-1}b = (a^{-1}a)\,h$

$a^{-1}b = eh$

$a^{-1}b = h$

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

Conversely suppose that $a^{-1}b \in H$

Required to prove $aH = bH$

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

$\Rightarrow a(a^{-1}bH) = aH$

$\Rightarrow (aa^{-1})\,bH = aH$

$\Rightarrow e\,b\,H = aH$

$\Rightarrow bH = aH$

$\therefore \quad aH = bH \Leftrightarrow a^{-1}b \in H$

Q50. Let H be a subgroup of G & a, b $\in$ G

Then $|aH| = |bH|$

Ans :

Let $(G, \cdot)$ be a group

& Let H be a subgroup of G

Let $|H| = n$

Let $a, b \in G$ then the left cosets of H in G are aH & bH

$aH = \{ah / h \in H\} \Rightarrow |aH| = |H| = n$

$bH = \{bh / h \in H\} \Rightarrow |bH| = |H| = n$

$\therefore \quad |aH| = |bH|$

$\forall \; a, b \in G$

Q51. Let H be a subgroup of G, & a, b ∈ G

Then aH = Ha if and only if H = aH a^{-1}

Ans :

Let (G, •) be a group

& Let H be a subgroup of G

Let a ∈ G then the left and right cosets of G are aH & Ha

Consider aH = Ha ⇔ (aH) a^{-1}

⇔ (Ha)a–1 [∵ a^{-1} ∈ G]

⇔ $aHa^{-1} = H(aa^{-1})$

⇔ $aHa^{-1} = He$

⇔ $aHa^{-1} = H$

∴ aH = Ha ⇔ $H = aHa^{-1}$

Q52. Find all the left cosets of {1, 11} in U(30).

Sol :

Let U(30) = {1, 7, 11, 13, 17, 19, 23, 29} be a group under multiplication modulo 30 of order 8.

i.e., |U(30)| = 8

Let H = {1, 11} be a subgroup of U(30) of order 2

i.e., |H| = 2

The number of left cosets = $\frac{|U(30)|}{|H|} = \frac{8}{2} = 4$

1H = 11H = H = {1, 11}

7H = 17H = {7, 17}

13H = 23H = {13, 23}

19H = 29H = {19, 29}

∴ The required left cosets are

1H, 7H, 13H, 19H.

Q53. Find the cosets of H = {1, 15} in G = U(32)

Sol :

Let G = U(32)

= {1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31} is a group under multiplication

& H = {1, 15} is a subgroup of U(32)

1 ∈ G ⇒ 1.H = {1.1, 1.15} = {1, 15} = H

$3 \in G \Rightarrow 3H = \{3, 13\} = 13H$

$5 \in G \Rightarrow 5.H = \{5, 11\} = 11H$

$7 \in G \Rightarrow 7.H = \{7, 9\} = 9H$

$17 \in G \Rightarrow 17.H = \{17, 31\} = 31H$

$19 \in G \Rightarrow 19.H = \{19, 29\} = 29H$

$21 \in G \Rightarrow 21.H = \{21, 27\} = 27H$

$23 \in G \Rightarrow 23.H = \{23, 25\} = 25$

2.9 LAGRANGE'S THEOREM AND CONSEQUENCES

Q54. The order of a subgroup of a finite group divides the order of the group

(or)

If H is subgroup of a finite group G then, $|H| / |G|$

Ans : **(Jan.-21, May/June-19)**

Given that H is subgroup of a finite group G

Case (i)

Let $H = \{e\}$

& $|G| = n$

$\Rightarrow |H| = 1 \qquad \therefore |H| / |G| = \frac{1}{n}$

If $H = G \Rightarrow |H| = |G|$

$= n$

$\Rightarrow |H| / |G|$

Case (ii)

Let $H \neq \{e\}$ and $H \neq G$

Suppose that $H = \{h_1, h_2, ... h_m\}$

$\Rightarrow |H| = m$

also H has m distinct elements

i.e., $h_i \neq hj$ where $i \neq j$

Now, required to prove the right costs, so let us construct right cosets

Let $e \in G \Rightarrow$ H.e is the right coset

$\because He = H$

H e has 'm' distinct elements

If $h_i a = h_j a$ for $i \neq j$

$h_i = h_j$ for $i \neq j$

which is a contradiction because

$h_i \neq h_j$ when $i \neq j$

$\Rightarrow$ If H & H a are only two distinct right cosets then

$$G = H \cup H a$$

$$|G| = |H| + |Ha|$$

$$n = m + m$$

$$n = 2m \Rightarrow m/n$$

$$\Rightarrow |H| / |G|$$

Q55. If G is a finite and H is a subgroup of G

Then $|G : H| = |G| / |H|$

Ans :

Let G be a finite group

and H is a subgroup of G

and H is also finite group.

By definition of index of subgroup of a finite group is G : H

Then $|G : H|$ = No. of distinct cosets of H in G

$$= \frac{\text{No. of elements in G}}{\text{No. of elements in H}}$$

$$= \frac{|G|}{|H|}$$

$\therefore$ $|G : H| = |G| / |H|$

Q56. In a finite group, the order of each element of the group divides the order of the group.

Ans :

Let G be a finite group

and the orders of G is n

i.e., $|G| = n$

Let $a \in G$

and the order of an element $a \neq e \in G$

$|a| = m$ then

$|H| = <a>$ is a subgroup of G

and $|H| = m$

$\therefore$ $|H|$ divides $|G|$

$\Rightarrow$ $|a|$ divides $|G|$

Q57. Prove that a group of prime order is cyclic.

Ans : **(Jan.-21)**

Given that G is a group of prime orders

$\Rightarrow$ $|G| = P$

$|G| = P \geq 2$

Case (i)

Let $P = 2$

$\Rightarrow$ $|G| = 2$

$\Rightarrow$ $G = \{e, a\}$ where $a \neq e$

We required to prove that

G is cyclic

$a \in G$, $a \in G$ $\Rightarrow$ $a^2 \in G$

$\Rightarrow$ $a^2 = e$ (or) $a^2 = a$

If $a^2 = e$

$G = \{e, a\}$

$= \{a^2, a\}$

$= \{a, a^2\}$

$G = <a>$

$\therefore$ G is a cyclic group

If $a^2 = a$

$a.a = a.e$

$a = e$ By left cancellation Law

Which is not possible because $a \neq e$

Case (ii) :

Let $|G| = P > 2$

$\exists\ a \neq e \in G \Rightarrow |a| > 1$

Let $|a| = m \Rightarrow m > 1$

By definition, $a^m = e$ where 'm' is least positive integer,

Consider

$H = \{a, a^2, a^3 \ldots a^m = e\}$

H is a subgroup of G

By Lagrange's theorem

$$|H| \,/\, |G| \Rightarrow m \,/\, p$$

$\Rightarrow$ m = 1 or m = p

$\Rightarrow$ m = p

(m = 1 is not possible because we have m > 1)

$\Rightarrow |H| = |G|$

$\Rightarrow G = H = \langle a \rangle$

G is cyclic

$\therefore$ Every group of prime order is cyclic

Q58. Let G be a finite group, and let $a \in G$. Then $a^{|G|} = e$.

Ans :

Let G be a finite group

We know that $|a| \,/\, |G|$ ... (1)

Suppose that $|a| = m$

By definition $a^m = e$ where 'm' is the least positive integer

Substitute $|a| = m$ in (1)

$$\Rightarrow m \,/\, |G|$$

$|G| = K.m$ where k is the positive integer

Consider

$$\text{LHS } a^{|H|} = a^{mk}$$
$$= (a^m)^k$$
$$= e^k$$
$$a^{|G|} = e^k$$
$$\therefore a^{|G|} = e$$

Q59. State and prove for every integer 'a' and every prime 'p', a^p mod p = a mod p

Ans :

Given that, 'a' is integer and p is a prime number

To prove

Apply division algorithm to 'a' and 'p'

$\exists$ m and r which are integer

$\exists$ a = pm + r where $0 \le r < p$

a – r = pm

$\Rightarrow$ p / a–r

By congruence, we have a = r (mod m)

Required to prove r^p = r (mod p) ... (1)

Case (i)

Let r = 0

Substitute r = 0 in (1)

So, that to prove $0^p \equiv 0 \pmod p$

$0 \equiv 0 \pmod p$

$\because$ $p / 0 - 0$

i.e., $p / 0$

Case (ii)

Let r = 1, 2, 3, ... p – 1

Also, By definition

U(p) = Set of all positive integer less than p and relatively prime to p

U(p) = {1, 2, 3 ..... (p – 1)}

Also, we have U(p) is a group with respect to multiplication modulo p

$r \in U(p)$ and $|U(p)| = p - 1$

$\because$ $a^{|G|} = e$

$\Rightarrow$ $r^{|U(p)|} = e = 1$

$r^{p-1} = 1$

$r^{p-1} - 1 = 0$

$\because$ $p / 0$ we have $p / r^{p-1} - 1$

By congruences definition

$r^{p-1} = 1 \pmod p$

$r^p = r \pmod p$

Q60. For two finite sub groups H and K of a group, define the set HK = {hk / h $\in$ H, k $\in$ K}

Then |HK| = $|H|\ |K| / |H \cap K|$

Ans :

Let (G, $\cdot$) be a group

Let H & K be two finite subgroup of G

The set HK = {hk / h $\in$ H, k $\in$ K} is also finite subgroup of G and $\exists$ h k = h' k'

Where h $\neq$ h' and k = K'

The intersection of H & K is H $\cap$ K

is also finite subgroup of G

The product of order of HK and order of H $\cap$ K is the product of order of H and the order of K

i.e., $|HK| \cdot |H \cap K| = |H| \cdot |K|$

$$|HK| = \frac{|H|.|K|}{|H \cap K|}$$

Q61. A group of order 75 can have at most one subgroup of order 25

Sol :

Let (G, $\cdot$) is a finite group of order 75

i.e, $|G| = 75$

Let H & K be two subgroup of G

Then $|H \cap K|$ divides $|H| = 25$

and $|H \cap K|$ divides $|K| = 25$

i.e., $|H \cap K| = 1$ or 5

$$\therefore \quad |HK| = \frac{|H||K|}{|H \cap K|} = \frac{25 . 25}{1} \text{ or } (\frac{(25)(25)}{5}$$

$= 625$ (or) 125

Hence $|H \cap K| = 25$

and H = K

2.10 An Application of Cosets of Permutation Groups

Q62. Define stabilizer of a point.

Ans :

Let G be a group of permutation of a set S, for each i in S, let $Stab_G$ (i) = {$\phi \in G$ / ϕ(i) = i}

Q63. Define Orbit of a point.

Ans :

Let G be a group of permutation of a set S. For each s in S, but

$Orb_G(S) = \{\phi \in (S) / \phi \in G\}$ The set $Orb_G(S)$ is a subset of S called the Orbit of S

Under G, we use $|Orb_G(S)|$ to denote the number of elements in $Orb_G(S)$

Q64. Let G = {(1), (1 3 2) (4 6 5) (7 8), (1 2 3) (4 5 6), (1 2 3) (4 5 6) (7 8), (7 8)}

Then find stabilizer of 1, 2, 4 and 7 in G.

Sol :

Stab of (1) = $Stab_G(1)$ = {(1), (7 8)}

Stab of (2) = $Stab_G(2)$ = {(1), (7 8)}

Stab of (4) = $Stab_G(4)$ = {(1), (7 8)}

Stab of (7) = $Stab_G(7)$ = {(1), (1 3 2), (4 5 6), (1 2 3) (4 5 6)}

Q65. Let G = {(1), (1 3 2), (4 5 6) (7 8), (1 2 3) (4 5 6), (1 2 3) (4 5 6) (7 8), (7 8)}

Then find orbit of 1, 2, 4 and 7 in G

Sol :

Orbit of 1 in G = $Orb_G(1)$ = {1, 3, 2}

Orbit of 2 in G = $Orb_G(2)$ = {2, 1, 3}

Orbit of 4 in G = $Orb_G(4)$ = {4, 6, 5}

Orbit of 7 in G = $Orb_G(7)$ = {7, 8}

Q66. Let G be a finite group of permutation of a set. Then, for any i from S,

$$|G| = |Orb_G(i)|\ |Stab_G(i)|$$

Ans :

Given that 'G' is a finite group of permutation defined on S

Required to prove that

$|G| = |Stab_G(i)|\ |Orb_{(G)}(i)|$

Let $H = Stab_G(i)$

$K = Orb_G(i)$

$\because$ $Stab_G(i)$ is a subgroup of G

H is a subgroup of G

To prove the result, it is enough to prove

$|G| = |H|\ |K|$ ... (1)

By Lagrange's theorem

Number of left cosets = $\frac{|G|}{|H|}$

$\Rightarrow$ $|G| = |H| \times$ No. of left cosets ... (2)

Definite a mapping

$T : \{\alpha H / \alpha \in G\} \rightarrow \{\alpha(i) / \alpha \in G\}$

Defined as $T(\alpha H) = \alpha(i)$

(i) T is well defined

if $\alpha H = \beta H$

Required to show that

$T(\alpha H) = T(\beta H)$

Consider

$\alpha H = \beta H \qquad \alpha, \beta \in G$

$\Rightarrow$ $\alpha^{-1}\beta \in H$

$\Rightarrow$ $\alpha^{-1}\beta\,(i) = i$

$\Rightarrow$ $\alpha \,.\, \alpha^{-1}\beta\,(i) = \alpha(i)$

$\Rightarrow$ $\beta(i) = \alpha(i)$

$\therefore$ $T(\alpha H) = T(\beta H)$

(ii) T is one - one :

If $T(\alpha H) = T(\beta H) \Rightarrow \alpha H = \beta H$

Consider

$T(\alpha H) = T(\beta H)$

$\alpha(i) = \beta(i)$

$\Rightarrow$ $\alpha^{-1}\alpha\,(i) = \alpha^{-1}\beta\,(i)$

$\Rightarrow$ $I\,(i) = \alpha^{-1}\beta\,(i)$

$\Rightarrow$ $i = \alpha^{-1}\beta\,(i)$

$\Rightarrow$ $\alpha^{-1}\beta \in Stab_G(i)$

$\Rightarrow$ $\alpha^{-1}\beta \in H$

$\alpha H = \beta H$

T is one - one

(iii) T is onto

Let $j \in K$

$\exists\, i \in S \ni \alpha(i) = j$

$\Rightarrow$ $T(\alpha H) = j$

T is onto

∴ The number of left cosets |K|

∴ $|G| = |K|\ |H|$

$|G| = |Stab_G(i)|\ \ |Orb_G(i)|$

2.11 The Rotation Group of a Cube and a Soccer Ball

Q67. Prove that the group rotation of a cube is isomorphic to S_4.

Ans : **(May/June-19)**

Let G be the group of rotions of a cube and Lable the six faces of the cube

1, 2, 3, 4, 5 and 6

Then G be a group of permutation on the set

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

Required to prove. G is isomorphic to a subgroup of S_4.

∴ Cube has four diagonals and labelling the consecutive diagonals 1, 2, 3, 4

∴ The rotation 90° that yields the permutation $a = (1\ 2\ 3\ 4)$

∴ The another 90° rotation about the axis perpendicular to first axis yields the permutaiton on $\beta = (1\ 4\ 2\ 3)$

The group of permutation included by rotation contains the eight element subgroup

$\{\varepsilon, \alpha, \alpha^2, \alpha^3, \beta^2, \beta^2\alpha, \beta^2\alpha^2, \beta^2\alpha^3\}$ of G and the order of $\alpha\beta$ is 3.

i.e., $(\alpha\beta)^3 = \varepsilon$

The order of the rotation group must be divisible by both 8 and 3

∴ The rotation yields all 24 permutation

i.e., $|G| = 24\ \ |S_4|$

Hence $G \approx S_4$

Short Question and Answers

1. The set of Automorphism of a group and the set of inner Automorphism of group are both group under the operation of function composition.

Ans :

Let $\phi_a : G \to G$ is an isomorphism.

Let a $\in$ G & the set of all inner Automorphism of G induced by a

$\text{Inn}(G) = \{\phi_a / \phi_a(x) = axa^{-1} \ \forall \ x \in G\}$

Closure Property

Let $\phi_a, \phi_b \in \text{Inn}(G) \Rightarrow \phi_a(x) = axa^{-1}$

$\Rightarrow \phi_a(x) = bxb^{-1} \ \forall \ x \in G$

Consider

$(\phi_b \circ \phi_a)(x) = \phi_b[\phi_a(x)]$

$= \phi_b[axa^{-1}]$

$= b[axa^{-1}]b^{-1}$

$= (b\,a)\,x\,(a^{-1}b^{-1})$

$= (b\,a)\,x\,(b\,a)^{-1}$

$\therefore \quad (bxb^{-1})(axa^{-1}) = (ba)x(ba)^{-1} \in \text{Inn}(G)$

Associative Property

Let $\phi_a, \phi_b, \phi_c \in \text{Inn}(G)$

$\phi_c(x) = cxc^{-1}, \ \forall \ x \in G$

Consider

$[(\phi_a \circ \phi_b) \circ \phi_c](x) = (\phi_a \circ \phi_b)[\phi_c(x)]$

$= \phi_a[\phi_b(\phi_c(x))]$

$= \phi_a[\phi_b(cxc^{-1})]$

$= \phi_a[b(cxc^{-1})b^{-1}]$

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

$= [(ab)\,c]\,x\,[c^{-1}(a^{-1}b^{-1})]$

$= [(ab)\,c]\,x\,[c^{-1}(ab)^{-1}]$

$= [(ab)\,c]\,x\,[(a\,b)\,c]^{-1}$

$= [(a\,(bc]\,x\,[a\,(bc)]^{-1}$

$= [\phi_a \circ (\phi_b \circ \phi_c)](x)$

$\therefore \quad$ Inn (G) is satisfies the Associative.

Identity Property

$\therefore \quad e \in G \Rightarrow \phi_2 \in Inn(G)$

$\phi_2(x) = e\,x\,e^{-1}$

$= e\,x\,e$

$= x$

$(\phi_e \circ \phi_a)(x) = \phi_e\,[\phi_a(x)]$

$= \phi_e\,(ax\,a^{-1})$

$= e(ax\,a^{-1})\,e^{-1}$

$= (e\,a)\,x\,(a^{-1}\,e^{-1})$

$= (e\,a)\,x\,(ea)^{-1}$

$= ax\,a^{-1}$

$(\phi_e \circ \phi_a)(x) = \phi_a\,(x)$

By $(\phi_a \circ \phi_e)(x) = \phi_a\,(x)$

$\therefore \quad \phi_e = I$ is an identity element of Inn(G)

Inverse Property

Consider $(\phi_a \circ \phi_{a^{-1}})(x) = \phi_a\,[\phi_{a-1}(x)]$

$= \phi_a\,[a^{-1}\,xa^{-1}]^{-1}$

$= (a^{-1}\,xa^{-1})^{-1}$

$= (aa^{-1})\,x\,(aa^{-1})^{-1}$

$= ex\,a^{-1}$

$= \phi_e\,(x)$

Similarly

$(\phi_{a^{-1}} \circ \phi_a)(x) = \phi_e\,(x)$

$\therefore$ Inn(G) is satifies the inverse property

$\therefore$ Inn(G) is group under the operation of composition of function.

2. Let ϕ be an isomorphism from G to $\overline{G}$. If K is a subgroup of G. Then $\phi(k) = \{\phi(k) / k \in K\}$ is a subgroup of $\overline{G}$

Ans :

Let G and $\overline{G}$ be the two groups.

and $\phi : G \to \overline{G}$ is isomorphism.

Let K be a subgroup of G.

Then $\phi(K) = \{\phi(k) / k \in K\}$ is subset of $\bar{G}$

i.e., $e = 1 \in G$

$\phi(e) = e' = 1 \in \phi(k)$

$\phi(k) \neq \phi$ and $\in \phi(k) \in \bar{G}$

$\forall\ \phi(k_1), \phi(k_2) \in \phi(k) \Rightarrow \exists\ k_1, k_2 \in k.$

$\Rightarrow$ $k_1 - k_2 \in k$ and $k_1 . k_2 \in k$

$\Rightarrow$ $\phi(k_1 - k_2) \in \phi(k)$ and $\phi(k_1 . k_2) \in \phi(k)$

Consider

$\phi(k_1) - \phi(k_2) \in \phi(k_1 - k_2) \in \phi(k)$

& $\phi(k_1) . \phi(k_2) \in \phi(k_1 k_2) \in \phi(k)$

$\therefore$ $\phi(k)$ is a subgroup of $\bar{G}$.

3. The order of a subgroup of a finite group divides the order of the group

(or)

If H is subgroup of a finite group G then, $|H| / |G|$

Ans :

Given that H is subgroup of a finite group G

Case (i)

Let $H = \{e\}$

& $|G| = n$

$\Rightarrow$ $|H| = 1$ $\therefore$ $|H| / |G| = \frac{1}{n}$

If $H = G \Rightarrow |H| = |G|$

$= n$

$\Rightarrow$ $|H| / |G|$

Case (ii)

Let $H \neq \{e\}$ and $H \neq G$

Suppose that $H = \{h_1, h_2, ... h_m\}$

$\Rightarrow$ $|H| = m$

also H has m distinct elements

i.e., $h_i \neq hj$ where $i \neq j$

Now, required to prove the right costs, so let us construct right cosets

Let $e \in G \Rightarrow H.e$ is the right coset

$\because \quad He = H$

H e has 'm' distinct elements

If $h_i a = h_j a$ for $i \neq j$

$h_i = h_j$ for $i \neq j$

which is a controdiction because

$h_i \neq h_j$ when $i \neq j$

$\Rightarrow$ If H & H a are only two distinct right cosets then

$$G = H \cup Ha$$

$$|G| = |H| + |Ha|$$

$$n = m + m$$

$$n = 2m \Rightarrow m/n$$

$$\Rightarrow |H| / |G|$$

4. Define Permutation group.

Ans :

Let S = $a_1, a_2, \ldots a_n$ be finite set then a permutation is a mapping $f : S \to S$ which is both one – one and onto (or)

If S = $\{a_1, a_2, \ldots a_n\}$ then a one-one mapping from S onto itself is called a permutation of degree n.

The number n of elements in S is called the degree of permutation.

5. Write notation for cycle.

Ans :

Let $S = \{a_1, a_2, \ldots a_n\}$

$= \{a_1, a_2, \ldots a_k, a_{k+1}, a_{k+2} \ldots a_n\}$

Consider a permutation which is of the form

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \cdots & a_k & a_{k+1} & \cdots & a_n \\ a_2 & a_3 & a_4 & \cdots & & a_1 & a_{k+1} & \cdots & a_n \end{pmatrix}$$

is called as cyclic permutation whose length is K and degree 'n'

where

$f(a_1) = a_2,\ f(a_2) = a_3 \ldots\ldots f(a_k) = a_1$

$f(a_{k+1}) = a_{k+1} \ldots\ldots f(a_n) = a_n$

The above cyclic permutation is expressed as $f = (a_1, a_2, \ldots a_k)$.

6. Define Isomorphism.

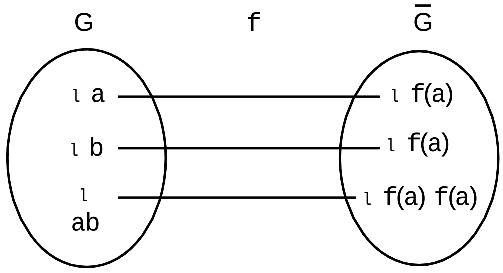
Ans :

A mapping ϕ $G \to \bar{G}$ is said to be an isomorphism

If ϕ is homomorphism, one - one & onto

Here the group G & $\bar{G}$ are said to be isomarphism to each other and donoted as $G \simeq \bar{G}$ isomasphism to each other 4 donoted as $G \simeq G$

i.e., $\phi(a\,b) = \phi(a)\,\phi(b)\ \forall$ a, b in G.



'G' Operation	'$\bar{G}$' operation	Operation Preservation
•	•	$\phi(a\,.\,b) = \phi(a)\,.\,\phi(b)$
•	+	$\phi(a\,.\,b) = \phi(a) + \phi(b)$
+	•	$\phi(a + b) = \phi(a)\,\phi(b)$
+	+	$\phi(a + b) = \phi(a) + \phi(b)$

7. Compute Aut (Z_{10}).

Sol :

Let $Z_{10} = \{0, 1, 2, 3, ... 9\}$ be a group

Under addition modulo 10.

By definition of Automorphism of G

Aut (G) = $\{\alpha / \alpha : Z_{10} \to Z_{10}$ is isomorphism$\}$

Consider

$\alpha(K) = \alpha(1 + 1 + ... + 1$ (K times)

$= \alpha(1) + \alpha(1) + ... + \alpha(1)$

$= K\,.\,\alpha(1)$

$|\alpha(1)| = 10$ and $\alpha(1) = 1$, $\alpha(1) = 3$, $\alpha(1) = 7$, $\alpha(1) = 9$

Aut (Z_{10}) = $\{\alpha_1, \alpha_3, \alpha_7, \alpha_9\}$ is group under multiplication with identity α_1

By Cayley's table

	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

8. Let H = {0, 3, 6} is Z_9 under addition. Then find the left cosets of H is Z_9.

Sol :

Let $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

is group under addition modulo 9

and $H = \{0, 3, 6\}$ is a subgroup of Z_9

$0 \in Z_9 \Rightarrow 0 + H = \{0, 3, 6\} = 3 + H = 6 + H$

$1 \in Z_9 \Rightarrow 1 + H = \{1, 4, 7\} = 4 + H = 7 + H$

$2 \in Z_9 \Rightarrow 2 + H = \{2, 5, 8\} = 5 + H = 8 + H$

9. A group of order 75 can have at most one subgroup of order 25.

Sol :

Let $(G, \cdot)$ is a finite group of order 75

i.e, $|G| = 75$

Let H & K be two subgroup of G

Then $|H \cap K|$ divides $|H| = 25$

and $|H \cap K|$ divides $|K| = 25$

i.e., $|H \cap K| = 1$ or 5

$$\therefore \quad |HK| = \frac{|H||K|}{|H \cap K|} = \frac{25 \cdot 25}{1} \text{ or } (\frac{(25)(25)}{5}$$

$$= 625 \text{ (or) } 125$$

Hence $|H \cap K| = 25$

and $H = K$

10. List the applications of factor groups.

Sol :

Let G be a finte group and H be the subgroup of G and $H \neq \{e\}$. The factor group is denoted by $\frac{G}{H}$.

(i) The structure of group G and factor group $\frac{G}{H}$ is same. Hence, a less complicated approximation of G can be obtained from the approximation of $\frac{G}{H}$ because $\frac{G}{H}$ is smaller than G.

ii) The properties of a group G can be obtained by examing the properties of factor group $\frac{G}{H}$.

iii) The position of element in a factor group gives the costs of group.

iv) The order of subgroup can be obtained by means of factor group.

11. If H and K are subgroups of a group G with $|H| = 24$, $|K| = 20$ then show that $H \cap K$ is an abelian group.

Sol :

Given,

H and K are subgroups of a group G

$|H| = 24$

$|K| = 20$

Then, $H \cap K \neq \phi$, as identity element 'e' is comon to H and K.

According to Lagrange's theorem, the order of a subgroup of a finite group divides the order of the group.

$\therefore$ $|H \cap K|$ divides both $|H| = 24$ and $|K| = 20$

Since, $|H| = 24$ and $|K| = 20$ are relatively prime,

$\therefore$ $|H \cap K| = 1$

i.e., the order of $H \cap K = 1$

Hence, $H \cap K$ is as abelian group.

12. Find all idempotent elements in the ring $(Z_{10}, +_{10}, \times_{10})$

Sol :

Given,

$(Z_{10}, +_{10}, \times_{10})$ is a ring.

Here, $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

a2 = a

Then

$0^2 = 0 \times_{10} 0 = 0$

$1^2 = 1 \times_{10} 1 = 1$

$2^2 = 2 \times_{10} 2 = 4$

$3^2 = 3 \times_{10} 3 = 9$

$4^2 = 4 \times_{10} 4 = 6$

$5^2 = 5 \times_{10} 5 = 5$

$6^2 = 6 \times_{10} 6 = 6$

$7^2 = 7 \times_{10} 7 = 9$

$8^2 = 8 \times_{10} 8 = 4$

$9^2 = 9 \times_{10} 9 = 1$

$\therefore$ $0^2 = 0$, $1^2 = 1$, $5^2 = 5$, $6^2 = 6$ are the idempotent elements.

Choose the Correct Answers

1. $f(ab)$ = ________ [c]
   (a) $f(ba)$ (b) $f(b)\ f(a)$
   (c) $f(a)\ f(b)$ (d) 0

2. Ker f = $\{x \in G / f(x)$ = ________ [d]
   (a) e (b) 0
   (c) 1 (d) e'

3. hH = ________ [a]
   (a) H (b) G
   (c) S (d) None of the above

4. $aH \cap bH$ = ________ [c]
   (a) 0 (b) 1
   (c) ϕ (d) H

5. The order of any subgroup of finite group divides order ________ [b]
   (a) element (b) group
   (c) subgroup (d) none

6. A group of prime order is ________ [c]
   (a) commutative (b) normal
   (c) cyclic (d) subgroup

7. $|H|\ |K| / (H \cap K)$ ________ [b]
   (a) $|KH|$ (b) $|HK|$
   (c) $|H|$ (d) $|K|$

8. If a is self conjugate element of group G is ________, $\forall\ x \in G$ [b]
   (a) $a = xax$ (b) $a = x^{-1}ax$
   (c) $a = xax^{-1}$ (d) $a = xx^{-1}a$

9. If a is said to be a normalizer if N(a) = ________ [a]
   (a) $xa = ax$ (b) $x^{-1}a = x$
   (c) $x^{-1}a = a$ (d) $xa = x^{-1}a$

10. Intersection of two normal subgroups of G is ________ [b]
    (a) commutative (b) normal
    (c) cyclic (d) zero

Fill in the Blanks

1. Let ϕ be a group homomorphism from G to $\bar{G}$. Then kerϕ is a ________.
2. If ϕ is a homomorphism from a finite group G to $\bar{G}$, then $|\phi(G)|$ is ________.
3. If H is cyclic, then ϕ(H) is ________.
4. If H is abelian, then ϕ(H) is ________.
5. $\phi(g^n)$ = ________ $\forall$ n in Z.
6. $\phi(a) = \phi(b)$ if and only if ________.
7. If $\bar{K}$ is a subgroup of $\bar{G}$, then $\phi'(\bar{K})$ = ________.
8. If G is a group of order p^2, where p is a prime, then G is ________.
9. For any group G, G / Z(G) is ________.
10. Let G be a group and let Z(G) be the center of G. If G / Z(G) is cyclic then G is ________.
11. A subgroup H of G is normal in G if and only if ________.
12. If G is a finite group and H is a subgroup of G, then ________.
13. A group of prime order is ________.
14. For every integer 'a' and every prime p, a^p modp = ________.
15. Let G be a finite group, and let a $\in$ G, then ________.

ANSWERS

1. Normal subgroup of G
2. Divides |G| and $|\bar{G}|$
3. Also cyclic
4. Also abelian
5. $(\phi(g))^n$
6. akerϕ = bkerϕ
7. $\{K \in G / \phi(K) \in \bar{K}\}$ is a subgroup of G
8. Abelian
9. Isomorphic to Inn(G)
10. Abelian
11. $x H x^{-1} \subseteq H, \forall x \in (G)$
12. $|G : H| = |G| / |H|$
13. Cyclic
14. a modp
15. $a^{|G|} = e$

UNIT III	**Normal Subgroups and Factor Groups:** Normal Subgroups - Factor Groups - Applications of Factor Groups - Group Homomorphisms - Definition and Examples - Properties of Homomorphisms - The First Isomorphism Theorem. **Introduction to Rings:** Motivation and Definition - Examples of Rings - Properties of Rings - Subrings. **Integral Domains:** Definition and Examples -Fields - Characteristics of a Ring.

3.1 Normal Subgroups and Factor Groups

3.1.1 Definition

Q1. Define Normal subgroup with example.

Sol :

A subgroup 'N' of a group 'G' is said to be a normal subgroup of 'G' $\forall\ g \in G,\ \forall\ n \in N$

$\Rightarrow$ $g\,n\,g^{-1} \in N$

Eg.

Let $G = \{1, -1, i, -i\}$

$\Rightarrow$ G is group w.r.to multiplication

Sol :

We have $N = \{1, -1\}$ is a subgroup of G

Let $g = 1,\ n = -1 \Rightarrow g\,n\,g^{-1} = 1 \times (-1)\,(1) = -1 \in N$

Let $g = -1,\ n = -1 \Rightarrow g\,n\,g^{-1} = (-1) \times (-1) \times (-1) = -1 \in N$

$g = i,\ n = -1 \Rightarrow g\,n\,g^{-1} = (i) \times (-1)\,(-i) = -1 \in N$

$g = -i,\ n = -1 \Rightarrow g\,n\,g^{-1} = (-i) \times (-1) \times (i) = -1 \in N$

$\therefore$ N is a normal subgroup of 'G'.

Note :

If 'N' is a normal subgroup of 'G' then we write it as $N \triangleleft G$

Q2. Prove that every subgroups of an abelian group is always normal.

Ans :

Let 'G' be an abelian group

Suppose that 'N' is a subgroup of 'G'

To proe that 'N' is a normal subgroup of G

We shall show that $\forall\ g \in N,\ \forall\ n \in N \Rightarrow g\,n\,g^{-1} \in N$

Consider

$g\,n\,g^{-1} = (gn)\,g^{-1}$

$= (ng)\,g^{-1}$ [gn = ng as G is abelian]

$= n(gg^{-1})$ Associative property

$= ne$ $gg^{-1} = e = g^{-1}g$

$g\,n\,g^{-1} = n$

$g\,n\,g^{-1} \in N'$

$\therefore$ N is a normal subgroup of G

Q3. Prove that intersection of any two normal subgroup of 'G' is again a normal subgroup of 'G'.

Ans :

Let 'G' be a group

and suppose that H & K are two normal subgrop of 'G'.

$\because$ H and K are subgroups of G

$\Rightarrow$ $H \cap K$ is also subgrop of G

[intersection of two subgroups of group is again a subgroup]

Required to prove $H \cap K$ is a normal subgroup of G

We shall show that

$$\boxed{\forall\, g \in G,\ \forall\, x \in H \cap K \Rightarrow g\,x\,g^{-1} \in H \cap K}$$

$x \in H \cap K \Rightarrow x \in H \ \&\ x \in K$

$\because$ H is a normal subgroup of G

We have by definition

$\forall\ g \in G,\ \forall\ x \in H \Rightarrow g\,x\,g^{-1}$ ... (1)

Similarly

$\because$ K is normal subgroups of G

By definition $\forall\ g \in G,\ \forall\ x \in H \Rightarrow g\,x\,g^{-1} \in K$ ... (2)

(1) and (2) $\Rightarrow g\,x\,g^{-1} \in H \cap K$

$\therefore$ $H \cap K$ is a normal subgroup of 'G'

Q4. Write a condition for normal subgroup.

Sol :

Second definition of normal subgroup of : A subgroup 'N' of a group 'G' is said to be a normal subgroup 'G' if $\forall\ g \in G \Rightarrow g\,n\,g^{-1} \subset N$

Q5. Prove that a subgroup N of a group G is a normal subgroup of G iff $g N g^{-1} = N \ \forall \ g \in G$.

Ans : **(May/June-19)**

Given that N is a subgroup of of 'G'

To prove that N is normal suubgroup of G

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

Ist Part :

Suppose that $g N g^{-1} = N \ \forall \ g \in G$

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

$\Rightarrow$ N is a normal subgroup of G (by definition)

Conversely suppose that

N is a normal subgroup of G

To prove that $g N g^{-1} = N \ \forall \ g \in G$

N is a normal subgroup of G

$\Rightarrow$ By definition $g N g^{-1} \subset N \ \ \forall \ g \in G$,,, (1)

$g \in G \ \Rightarrow \ g^{-1} \in G$

$\therefore$ Writing the condition (1) for 'g^{-1}'

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

$\Rightarrow \ g^{-1} N g \subset N \qquad [\because (g^{-1})^{-1} = g]$

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

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

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

$\Rightarrow \ N e \subset g N g^{-1} \qquad [eN = N]$

$\Rightarrow \ N \subset g N g^{-1} \qquad [Ne = N]$ ... (2)

equations (1) & (2)

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

Q6. Prove that a subgroup 'N' of a group 'G' is a normal subgroup of G iff product of two right (left) cosets of N in G is again a right (left) coset of 'N' in 'G'.

Ans :

Note : If 'H' is a subgroup of a group G w.r. to multiplication

Then $H H = H$

Similarly if H is a subgroup of G under addition then $H + H = H$

Given that 'N' is a subgroup of G

To prove that N is a normal subgroup of G $\Leftrightarrow$

Consider product of two right cosets of N is again a right cosets of N.

Ist Part :

Suppose that 'N' is a normal subgroup of G.

By definition aN = Na $\forall$ a $\in$ G ... (1)

for a, b $\in$ G

Na and Nb are the two right cosets.

Now consider the product of two right cosets = Na . Nb

$\Rightarrow$ N (aN) b

$\Rightarrow$ N (Na) b by (1)

$\Rightarrow$ N N a b

Na . Nb $\Rightarrow$ N a b (N N = N)

Which is again a right coset because a, b $\in$ G

Conversely suppose that

Product of two right cosets is again a right coset.

To Prove that 'N' is a normal subgroup of G we shall verify that 'N' is a normal subgroup

By 1st definition i.e.,

To prove that $\forall$ g $\in$ G, n $\in$ N $\Rightarrow$ g n g^{-1} $\in$ N

Consider g n g^{-1}

$\Rightarrow$ e . g n g^{-1} [eg = g]

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

= N g g^{-1} [N a . N b = N ab product of 2 left cosets is again a right coset]

= Ne

= N

$\therefore$ g n g^{-1}N

$\Rightarrow$ N is a normal subgroup of 'G'.

3.2 Factor Group (or) Quotient Group

Q7. Define factor group.

Ans :

Let 'G' be a group and 'N' be a normal subgroup of 'G'. Then the factor group or the Quotient group denoted by

$$\frac{G}{N} = \{Nx / x \in G\}$$

i.e., the set of all right cosets of N in G forms a group know as factor group

or Quotient group w,r, to the binany operation multiplication of two right cosets.

Q8. If G is a group and N is a normal subgroup of G. Then prove that $\frac{G}{N}$ = {Nx / x $\in$ G} forms a group w.r.to coset multiplication as the binary operation

Ans : **(Imp.)**

Given that

'N' is a normal subgroup of G

$\frac{G}{N} = \{Nx / x \in G\}$

Let Nx, Ny & Nz $\in \frac{G}{N}$, where x, y, z $\in$ G

1. Closure Property

$\forall$ Nx, Ny $\in \frac{G}{N} \Rightarrow$ Nx Ny $\in \frac{G}{N}$

Because x, y $\in$ G $\Rightarrow$ xy $\in$ G

2. Associative Property

$\forall$ Nx, Ny, Nz $\in \frac{G}{N}$

Consider $(N_x N_y) N_z = (N_{xy}) \in N_z$ $\quad$ $N_x (N_y N_z) = N_x (N_{yz})$

$= N_{xyz}$ ... (1) $\quad$ $= N_{xyz}$ ... (2)

3. Identity Property

$\forall$ Nx $\in \frac{G}{N}$ $\exists$ Ne $\in \frac{G}{N}$ [e $\in$ G]

$\ni$ Nx Ne = Ne Nx = Nx

Nx Ne = Nxe = Nx

Ne = N acts as the identity element of $\frac{G}{N}$

4. Inverse Property

$\forall$ Nx $\in \frac{G}{N}$ $\exists$ N $x^{-1} \in \frac{G}{N}$

$\ni$ Nx . Nx^{-1} = Nx x^{-1} = Ne [$\because$ x $\in$ G $\Rightarrow$ x^{-1}]

Similarly

Nx^{-1} Nx = Nx^{-1} x = Ne

$\therefore$ $\frac{G}{N}$ forms a group

Q9. Prove that if G is a abelian group and N is a normal subgroup of G then $\frac{G}{N}$ is also an abelian group.

Ans :

Given that

G is an abelian group and

N is a normal subgroup of G

$\therefore \quad \frac{G}{N} = \{Nx / x \in G\}$ forms a group known as Quotient group (or) factory group w.r.to cosets multiplication as a binary operation.

Commutative Property $\forall$ Nx, Ny $\in \frac{G}{N}$

Consider

$N_x N_y$

$= N_{xy}$

$= N_{yx}$ [xy = y, as G is abelian]

$N_x N_y = N_y N_x$

Q10. Prove that if G is a cyclic group then $\frac{G}{N}$ is also a cyclic group.

Ans :

Given that G is a cyclic group

Let N be a subgroup of G

$\because$ G is a cyclic group $\Rightarrow$ G is abelian

$\Rightarrow$ N is a normal subgroup of G

[$\because$ every subgroup of an abelian group is normal]

$\therefore \quad \frac{G}{N} = \{Nx / x \in G\}$

$\because$ G is a cyclic group

$\forall\ x \in G \Rightarrow x = a^n$ where $n \in z$ and

a is a generator of G

i.e., G = <a>

Let $Nx \in \frac{G}{N}$ (where $x \in G$)

$\Rightarrow$ $Nx = Na^n$ $[\because x = a^n]$

$= Na\ Na \ldots Na$ $[N_{ab} = N_a N_b]$

$Nx = (Na)^n$

$\frac{G}{N}$ is also a cyclic group.

Q11. Let H be a normal subgroup of G and K be any subgroup of G then prove that $HK = \{hk / h \in K, k \in K\}$ is also subgroup of G

Ans :

Given that

H is a normal subgroup of G

K is a subgroup of G

$HK = \{hk / h \in K, k \in K\}$

$HK \neq \phi$

$\because$ $e \in HK$

and $e = e . e$ where $e \in H$, $e \in K$

Now, we shall show that HK is a subgroup of G by applying "one stop subgroup test".

Let $h_1, K_1, h_2, K_2 \in HK$ where $h_1 h_2 \in H, K_1, K_2 \in H$

Consider

$(h_1 K_1)\ (h_2 K_2)^{-1}$

$= h_1 K_1\ K_2^{-1} h_2^2$ [Socks - Shoes property]

$= h_1 (K_1 K_2^{-1}) h_2^{-1}$

$= h_1 h_2^{-1} (K_1 K_2^{-1}) \in HK$

$\Rightarrow$ HK is subgroup of G $\Leftrightarrow$ $Ha = aH$ i.e., $h_1 a = ah_1$

3.3 Group Homomorphism - Definition, Examples

3.3.1 Applications of Factor Groups

Q12. List the applications of factor groups.

Ans :

Let 'G' be a finite group and 'H' be the subgroup of G and $H \neq \{e\}$. The factor group is denoted by $\frac{G}{H}$.

(i) The structure of group G and factor group $\frac{G}{H}$ is same. Hence, a less complicated approximation of G can be obtained from the approximation of $\frac{G}{H}$ because $\frac{G}{H}$ is smaller than G.

(ii) The properties of a group G can be obtained by examining the properties of factor group $\frac{G}{H}$.

(iii) The position of element in a factor group gives the cosets of group.

(iv) The order of a subgroup can be obtained by means of factor group.

Q13. Define Homomorphism.

Sol :

A Homomorphism ϕ from a group G to a group $\bar{G}$ is mapping from G into $\bar{G}$ that preserves the group operation.

i.e., $\phi(ab) = \phi(a)\, \phi(b) \quad \forall$ a, b in G

3.4 Properties of Homomorphism

Q14. Let $\phi : G \to \bar{G}$ be a homomorphism then prove that

(i) $\phi(e) = \bar{e}$ where e & $\bar{e}$ are the identity element of G and $\bar{e}$

(ii) $\phi(a^{-1}) = [\phi(a)]^{-1} \ \forall \ a \in G$, $\phi(g^n) = (\phi(g))^n$

(iii) If |g| is finite then |ϕ(g)| divides |g|

Ans :

1. Given that

Let $\phi : G \to \bar{G}$ be a homomorphism

To prove that $\phi(e) = \bar{e}$

Let $a \in G$

$\phi(a) \in \bar{G}$

Consider

$\bar{e} \,.\, \phi(a) = \phi(a) \qquad (\because \ ea = a)$

$= \phi(e \,.\, a)$

$= \phi(e)\, \phi(a)$

$\bar{e} \,.\, \phi(a) = \phi(e)\ \phi(e)$

$\bar{e} = \phi(e)$ (By Right cancellation law)

2. To prove that $\phi(a^{-1}) = [\phi(a)]^{-1} \ \forall \ a \in G$

from (i) we have $\bar{e} = \phi(e)$

$= \phi(aa^{-1})$

$= \phi(a)\ \phi(a^{-1})$

$= e$

Using the definition of inverse

We get $[\phi(a)]^{-1} = \phi(a^{-1})$

3. To prove that $\phi(g^n) = [\phi(g)]^n$

We shall apply the principle of mathematical induction on n.

The result is obvious for n = 1

Put n = 2 LHS = $\phi(g^2) = \phi(g \cdot g)$

$= \phi(g)\ \phi(g)$

$= [\phi(g)]^2$

$\therefore$ The result is true for n = 2

Let the given result be true for n = k

$\therefore$ We have $\phi(g^k) = [\phi(g)]^K$ ... (1)

To prove that $\phi(g^{K+1}) = [\phi(g)]^{K+1}$

LHS = $\phi(g^{K+1}) = \phi(g^K \cdot g)$

$= \phi(g^K)\ \phi(g)$

$= [\phi(g)]^K\ \phi(g)$

$= [\phi(g)]^{K+1}$

By the principle of mathematical induction

We have $\phi(g^n) = [\phi(g)]^n$

4. Given that $|g|$ is finite

Let $|g| = n$ [finite number]

By definition $g^n = e$, where n is the least the integral

Consider

$[\phi(g)]^n = \phi(g^n)$ From equation ... (2)

$= \phi(e)$ $g^n = e$

$[\phi(g)]^n = \bar{e}$ $\phi(e) = \bar{e}$

By the definition of order of an element

We have $|\phi(g)| / n$

$\Rightarrow$ $|\phi(g)| / (g) \rightarrow |g|$

Hence Proved the Properties of Homomorphism

Q15. Define Kernel of Homomorphism

Sol :

Let $f : G \rightarrow \bar{G}$ be a homomorphism then the Kernel of f denoted by Kerf (or) K_f (or) K is defined as Kerf = $\{x \in G / \phi(x) = \bar{e}\}$

Note :

1. i.e., In other words $x \in Kerf \Leftrightarrow \phi(x) = \bar{e}$
2. Kerf is non empty because $e \in$ Kerf as $\phi(x) = \bar{e}$

Q16. If $f : G \to \bar{G}$ is a homomorphism with Kernel K then prove that K is a normal subgroup of G.

Ans :

Given that

$f : G \to \bar{G}$ is a homomorphism

$Kerf = K = \{x \in G / f(x) = \bar{e}\}$

To prove that K is a normal subgroup of G

1. K is non empty (or) $K \neq \phi$

$K \neq \phi$

$\because$ $e \in K$ $[\in f(fe) = \bar{e}]$

2. To show that K is subgroup of G [Applying 2 step subgroup test]

(i) Closure Property

Let $x, y \in K$ to show that $xy \in K$

$$\left.\begin{array}{l} x \in K \Rightarrow f(x) = \bar{e} \\ y \in K \Rightarrow f(y) = \bar{e} \end{array}\right\} \quad \ldots (1)$$

Consider

$f(xy) = f(x) \ f(y)$ $\because$ f is homomorphism

$= \bar{e} \ . \ \bar{e}$

$f(xy) = \bar{e}$

$xy \in K$

$\therefore$ Closure propery holds good.

(ii) Inverse Property

To show that $x^{-1} \in K$ $\forall \ x \in K$

Consider

$f(x^{-1})$

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

$= (\bar{e})^{-1}$ From (1)

$= \bar{e}$ Inverse of an identity element is itself

$\therefore$ Inverse property holds good.

(iii) We shall show that

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

Now, consider

$f(g x g^{-1})$

$= f(g) f(x) f(g^{-1})$ $\because$ f is homomorphism

$= f(g)\ \bar{e}\ f(g^{-1})$ From (1)

$= f(g) . f(g^{-1})$ $\because$ f is homomorphism $gg^{-1} = g^{-1}g = e$

$= f(g . g^{-1})$

$= f(e)$

$f(g x g^{-1}) = \bar{e}$ ($\because$ property of homomorphism)

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

K is normal subgroup of G

Q17. Let $f : G \to \bar{G}$ be an onto homomorphism then prove that f is an isomorphism iff K = {e}

Ans : **(Imp.)**

Given that $f : G \to \bar{G}$ is homomorphism and onto

To prove that f is an isomorphism $\Leftrightarrow$ Kerf = K = {e}

Ist Part

Suppose that f is an isomorphism

To proe that K = {e}

Let $x \in K$

$\Rightarrow$ $f(x) = \bar{e}$ [$\bar{e}$ is identity of $\bar{G}$]

$\Rightarrow$ $f(x) = f(e)$ [$\because$ $f(e) = \bar{e}$]

$\Rightarrow$ $x = e$ f is isomorphism $\Rightarrow$ f is one - one

$\therefore$ K = {e}

Conversely suppose

K = {e}

To prove that f is an isomorphism

It is enough to prove that f is one one

$\because$ Given that f is homomorphism and onto

f is one - one

Let $x, y \in G$

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

Multiply both sides $f(y^{-1})$ to the right side

$f(x)\, f(y^{-1}) = f(y)\, f(y^{-1})$

$f(xy^{-1}) = f(yy^{-1})$ f is homomorphism

$\Rightarrow f(xy^{-1}) = f(e)$ $yy^{-1} = y^{-1}y = e$

$\Rightarrow f(xy^{-1}) = \bar{e}$ $\because$ property of homomorphism

$\Rightarrow xy^{-1} \in K$ $[\because K = \{e\}]$

$\Rightarrow xy^{-1} = e$

Multiply 'y' to the right side

$xy^{-1}y = ey$

$xe = ey$

$x = y$

f is one - one

Hence f is isomorphism.

Q18. Let $f : G \to \frac{G}{N}$ be defined as $f(x) = Nx \ \forall \ x \in G$

Where N is a normal subgroup of G then prove that

(i) f is a homomorphism and also (ii) Kerf = N

Ans :

Given that

$f : G \to \frac{G}{N}$ defined as $f(x) = Nx$

(i) f is homomorphism

To show that $f(xy) = f(x)\, f(y)$

Consider $f(xy)$

$= Nxy$ $\because$ Coset multiply $Na \,.\, Nb = Nab$

$= Nx\, Ny$

$f(xy) = f(x)\, f(y)$

(ii) Kerf = N

Let $\text{Kerf} = K = \{x \in G \,/\, f(x) = N\}$

To prove that $K = N$ which is to prove (i) $K \subset N$ (ii) $N \subset K$

(a) To show that $K \subset N$

Let $x \in K$

$\Rightarrow$ f(x) = N

$\Rightarrow$ Nx = N   f(x) = Nx

$\Rightarrow$ $x \in N$ Ha = H = aH $\Leftrightarrow$ $a \in H$

(b) To show that $K \subset N$

Let $x \in N$

$\Rightarrow$ $Nx \in N$

$\Rightarrow$ f(x) = N $a \in H \Leftrightarrow aH = H = Ha$

$\Rightarrow$ $x \in K$ f(x) = Nx

$\Rightarrow$ $N \subset K$ By definition of K

$\therefore$ K = N is Kerf = N

Q19. Define Automorphism Homomorphism Image and Isomorphic Image.

Sol :

(i) Automorphism

A mapping $f : G \to \bar{G}$ is said to be an automorphism if 'f' is an isomorphism i.e., in other words 'f' is homomorphism, 1 – 1, & onto

(ii) Homomorphic Image

If $f : G \to \bar{G}$ is homomorphism & onto

Then $\bar{G}$ is called as homomorphic image of G

(iii) Isomorphic Image

If $f : G \to \bar{G}$ is isomorphism. Then we say that G and $\bar{G}$ are isomorphic to each other and denotes as $G \simeq \bar{G}$ and $\bar{G}$ is called is isomorphic image of G.

3.4.1 The First Isomorphism Theorem

Q20. Fundamental theorem of homomorpic in group.

(OR)

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

Ans : **(Imp.)**

Let $\bar{G}$ be the homomorphic image of G

By definition we have $f : G \to \bar{G}$ such that 'f' is homomorphism and 'f' is onto

Let 'K' be the Kernel of f

$\Rightarrow$ K is normal subgroup of G

Where $K = \{x \in G / f(x) = \bar{e}\}$

$\Rightarrow \quad \dfrac{G}{K} = \{Kx \,/\, x \in G\}$ is a Quotient group or factor group.

Now, define a mapping $\phi : \dfrac{G}{K} \to \bar{G}$ as $\phi(Kx) = f(x) \quad \forall\ x \in G$

(i) ϕ is well defined :

Let $Kx, Ky \in \dfrac{G}{K} \ni Kx = Ky$

To prove that $\phi(Kx) = \phi(Ky)$

Consider

$Kx = Ky$

$\Rightarrow \quad xy^{-1} \in K$

$\Rightarrow \quad f(xy^{-1}) = \bar{e}$

$\Rightarrow \quad f(x)\, f(y^{-1}) = \bar{e}$

$\Rightarrow \quad f(x)\, f(y^{-1})\, f(y) = \bar{e}\ f(y)$

$\Rightarrow \quad f(x)\, f(y^{-1}y) = f(y)$

$\Rightarrow \quad f(x)\, f(e) = f(y)$

$\Rightarrow \quad f(xe) = f(y)$

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

$\therefore \quad \phi$ is well defined

(ii) ϕ is homomorphism :

To show that $\phi(Kx.\ Ky) = \phi(Kx)\ \phi(Ky)$

LHS $= \phi(Kx\ .\ Ky) = \phi(Kxy)$ ($\because$ By coset multiply) ($\because$ Ha Hb = Ha)

$= f(xy)$ ($\because$ By definition ϕ) ($\because$ f is homomorphism by definition ϕ)

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

$\phi(Kx\ Ky) = \phi(Kx)\ \phi(Ky)$

(iii) ϕ is one - one

Let $Kx, Ky \in \dfrac{G}{K} \ni \phi(Kx) = \phi(Ky)$

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

$\Rightarrow \quad f(x)\ .\ f(y^{-1}) = f(y)\ .\ f(y^{-1})$

$\Rightarrow \quad f(xy^{-1}) = f(yy^{-1})$ ($\because$ Multiply $f(y^{-1})$)

$\Rightarrow \quad f(xy^{-1}) = f(e)$

$\Rightarrow \quad f(xy^{-1}) = \bar{e}$ ($\because$ f(e) = e)

$\Rightarrow \quad xy^{-1} \in K$

$\Rightarrow \quad Kx = Ky \qquad (\because Ha = Hb \Leftrightarrow ab^{-1} \in H)$

$\therefore \quad \phi$ is 1 – 1

(iv) ϕ is onto

Since $f : G \rightarrow \bar{G}$ is onto

We have $\forall\ y \in \bar{G}\ \exists\ x \in G \Rightarrow y = f(x)$

$\Rightarrow \quad y = \phi(Kx) \qquad [\because f(x) = \phi(Kx)]$

ϕ is onto

Q21. Let ϕ be a homomorphism from a group G to a group $\bar{G}$.

Let H be a subgroup of G then prove that the following

(i) $\phi(H) = \{\phi(h) / h \in H\}$ is subgroup of $\bar{G}$

(ii) If H is cyclic then $\phi(H)$ is cyclic

(iii) If 'H' is abelian. Then $\phi(H)$ is abelian

(iv) If 'H' is normal in G. Then $\phi(H)$ is also normal

Ans :

1. Given that H is subgroup of G

$\phi(H) = \{\phi(h) / h \in H\}$

To prove that $\phi(H)$ is subgroup of $\bar{G}$

(i) $\phi(H) \neq \phi$

$\because \quad e \in \phi(H)$

or $\quad \bar{e} = \phi(e)$ where $e \in H$

(ii) Now we shall apply "2 step subgroup test"

(a) Closure Property

Let $\phi(h_1), f(h_2) \in \phi(H)$, where $h_1, h_2 \in H$

To show that $\phi(h_1), \phi(h_2) \in \phi(H)$

Consider

$\phi(h_1)\ \phi(h_2)$

$\Rightarrow \quad \phi(h_1\ h_2) \qquad (\because \phi$ is homomorphism)

$\in \quad \phi(H) \qquad (\because h_1\ h_2 \in H$ as H is subgroup)

(b) Existence of Inverse

To show that $\forall\ \phi(h_1) \in \phi(H) \Rightarrow [\phi(h_1)]^{-1} \in \phi(H)$

Consider

$[\phi(h_1)]^{-1}$ ($\because$ Property of homomorphism)

$\Rightarrow$ $\phi(h_1^{-1})$ ($\because$ $h_1^{-1} \in H,\ h_1 \in H$)

$\in \phi(H)$

$\therefore$ $\phi(H)$ is subgroup of $\bar{G}$

2. If H is cyclic then $\phi(H)$ is cyclic

Given that H is cyclic

By definition $H = \langle a \rangle$ where a is generator of H

Let $a^1, a^2 \ldots\ldots \in H$

$\Rightarrow$ $\phi(a), \phi(a^2) \ldots\ldots \phi(H)$

$\Rightarrow$ $\phi(a) \,.\, [\phi(a)]^2, \ldots\ldots \in \phi(H)$ $\phi(g^n) = [\phi(y)]^n$

$\therefore$ $\phi(H) = \langle \phi(a) \rangle$

$\Rightarrow$ $\phi(H)$ is cyclic group

3. If H is abelian then $\phi(H)$ is abelian

Given that

H is abelian to show that $\phi(H)$ is abelian

H is abelian $\Rightarrow h_1 h_2 = h_2 h_1$ $\forall\ h_1 h_2 \in H$

To prove that $\phi(H)$ is abelian we shall show that $\phi(h_1)\,\phi(h_2) = \phi(h_2)\,\phi(h_1)$

Consider

$\phi(h_1\ h_2) = \phi(h_1)\ \phi(h_2)$ ($\because$ ϕ is homomorphism) ... (1)

Also

$\phi(h_2\ h_1) = \phi(h_2)\ \phi(h_1)$

$= \phi(h_2)\ \phi(h_1)$ ... (2)

By (1) and (2)

$\phi(h_1)\ \phi(h_2) = \phi(h_2)\ \phi(h_1)$

4. If 'H' is normal then $\phi(H)$ is normal

Given that H is normal in G

$\Rightarrow$ By definition $\forall\ g \in H,\ \forall\ h \in H \Rightarrow g\,h\,g^{-1} \in H$

To prove that

$\phi(H)$ is normal in $\bar{G}$

We shall that

$\forall\ \phi(g) \in \bar{G},\ \forall\ \phi(h) \in \phi(H)$

$\Rightarrow$ $\phi(g)\ \phi(h)\ \phi(g^{-1}) \in \phi(H)$

Consider

$\phi(g)\ \phi(h)\ \phi(g)^{-1}$

$\phi(g)\ \phi(h)\ \phi(g^{-1})$

$= \phi(g\ h\ g^{-1})$

$\in\ \phi(H) \qquad \because\ g\ h\ g^{-1} \in H$

3.5 Introduction to Rings - Motivation and Definition

Q22. Define Ring, Commutative Ring & Ring with Unity.

Ans :

A ring R is set with two binary operations, addition (denoted by a + b) and multiplication (denoted by ab). Such that for all a, b, c in R.

1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. $\exists\ o \in R \ni a + o = a \qquad \forall\ a \in R$
4. $\exists\ -a \in R \ni a + (-a) = o$
5. $a\ (b\ c) = (ab)\ c$
6. $a\ (b + c) = ab + ac$ and $(b + c)\ a = ba + ca$.

In a Ring (R, +, ·) if a . b = b . a

for a, b $\in$ R Then we say that R is commutative ring.

A ring (R, +, .) is said to be a ring with Unity if R has Unit element

i.e., $\forall\ a \in R\ \exists\ 1 \in R \ni a\,.\,1 = 1.a = a$

3.5.1 Examples of Rings

Q23. State the examples of Rings.

Ans :

Example 1:

The set Z of integers Under ordinary addition and multiplication is a commutative ring with Unity 1. The Unity of Z are 1 and –1

Example 2:

The set M_2 (Z) of 2 × 2 matrices with integer entries is a non commutative ring with Unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Example 3:

The set 2 Z of even integers under ordinary addition and multiplication is a commutative ring with out Unity.

Example 4:

The set Z [x] of all polynomials in the variable x with integer coefficients under Ordinary addition and multiplication is a commutative ring with Unity f(x) = 1

3.5.2 Properties of Rings

Q24. Let a, b & c belong to a ring R.

Then a.o = o.a = o

Ans :

Ginen that a, b, c $\in$ R

Consider a . o = a .(o + o)

= a . o + o . a (by identity)

a . o = o

$\Rightarrow$ a .(o + o) = a.o + a.o [a . o $\in$ R $\Rightarrow$ a . o $\in$ R]

a.o + o = o + a.o = a.o

$\therefore$ By Applying the left canellection law in (R, +)

We get a.o = o

Similarly o.a = o.

Q25. Let a, b, c, $\in$ R Then a(–b) = (–a)b = –(ab)

Ans :

Given that a, b, c $\in$ R

Required to prove a(–b) = –(ab)

Consider

a(–b) + ab = a[–b + b]

a(–b) + (ab) = a(o)

= o

a(–b) + ab = o

$\Rightarrow$ a(–b) = –(ab)

Similarly (–a)b = –(ab)

Q26. Let a, b, c $\in$ R Then (–1)(–a) = –a

Ans :

Ginen that a, b, c $\in$ R.

Required to prove (–1)(–a) = –a

Consider

(–1) a + a = (–1) a + 1 . a

= [–1+1]a

= o . a

= o

(–1)a+a = o $\Rightarrow$ (–1) a = –a

Q27. Let a, b, & c $\in$ R Then

(–a)(–b) = ab $\forall$ a , b $\in$ R

Ans :

Given that a, b, C $\in$ R

Consider

L H S $\Rightarrow$ (–a)(–b)

$\Rightarrow$ –[(–a)b]

$\Rightarrow$ – [–(ab)] $\because$ [a(–b) = –(ab)]

$\Rightarrow$ ab

$\therefore$ (–a)(–b) = ab

Q28. Let a, b & c $\in$ R Then a (b – c) = ab – ac & (b – c) a = ba – ca

Ans :

Given that a, b ,C $\in$ R

Required to prove a(b – c) = ab – ac

Consider

a(b – c) = a [b + (–c)]

= ab + a (–c)

a(b – c) = ab – ac $\because$ a(–b) = –ab

Similarly we can also prove (b – c) a = ba – ca

3.6 Subrings

Q29. What is subring?

Ans :

A subset S of ring R. is a subring of R if S is itself a ring with the operation of R.

Q30. A nonempty subset S of a ring R. is a subring if S is closed subtraction and multiplication

i.e., (i) a – b $\in$ S

(ii) ab $\in$ S when a, b $\in$ S

Ans : **(Imp.)**

Suppose S be a subring of R.

Required to prove

(i) a – b $\in$ S

(ii) a b $\in$ S When a, b $\in$ S

(i) Let a, b $\in$ S

b $\in$ S $\Rightarrow$ –b $\in$ S $\quad\because$ S is subring

a $\in$ S, –b $\in$ S $\Rightarrow$ a + (–b) $\in$ S

a – b $\in$ S

(ii) a, b $\in$ S $\forall$ a, b $\in$ S $\quad\because$ S is subring

(S, .) is semi group

Conversely suppose that a – b $\in$ S & ab $\in$ S

Required to prove S is a subring of R.

(i) (S, +) is an Abelian group

(a) Associative property

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

(a+b)+c=a+ (b+c) $\quad\because$ S C R

(b) Existence of Identity :

a $\in$ S, – a $\in$ S $\Rightarrow$ a – a $\in$ S

$\Rightarrow$ o $\in$ S $\quad\because$ (i)

(c) Existence of Inverse :

o $\in$ S,

$\therefore$ o $\in$ S, a $\in$ S $\Rightarrow$ o – a $\in$ S

$\Rightarrow$ o +(–a) $\in$ S

$\Rightarrow$ –a $\in$ S

(d) Closure Property :

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

b $\in$ S $\Rightarrow$ – b $\in$ S

a $\in$ S, – b $\in$ S $\Rightarrow$ a – (– b) $\in$ S

$\Rightarrow$ a + b $\in$ S

(e) Commutative Property :

$\forall$ a, b $\in$ S $\Rightarrow$ a+ b = b + a $\quad\because$ S C R

$\therefore$ (S, +) is a abelian group.

(ii) (S, .) is a semi group

(a) Closure property :

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

(b) Associatine property

$\forall$ a, b c$\in$ S

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

(c) Distributive property

L D L : a (b + c) = ab + ac

$\forall$ a, b c $\in$ S

R D L : (b + c) . a = b . a + c . a

$\forall$ a, b $\in$ c S

Q31. Show that the set of matrices $\begin{bmatrix} a & b \\ o & c \end{bmatrix}$ is a subring of the ring of 2 × 2 matrices whose elements are integers and S = $\left\{ \begin{bmatrix} a & b \\ o & c \end{bmatrix} o, ab, c \in Z \right\}$

Sol :

Then S $\neq \phi$ and S C R .

Let A, B $\in$ S so that A = $\begin{bmatrix} a_1 & b_1 \\ o & c_1 \end{bmatrix}$ B = $\begin{bmatrix} a_2 & b_2 \\ o & c_2 \end{bmatrix}$ where

o, a_1, b_1, c_1, a_2, b_2, c_2, $\in$ Z

$\therefore$ A – B = $\begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ o & c_1 - c_2 \end{pmatrix}$ and AB = $\begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ o & c_1 c_2 \end{pmatrix}$

Sine $a_1 - a_2$, $b_1 - b_2$, $c_1 - c_2$ $\in$ Z

$a_1 b_1$ + b_1 c_2, $c_1 c_2$ $\in$ Z

we have A, B $\in$ S $\Rightarrow$ A – B $\in$ S and AB $\in$ S

Hence S is a Subring of R.

Q32. Let a $\in$ R. Let S = {x $\in$ R | ax = o} show that S is a Subring of R.

Sol :

Given, a $\in$ R

S = {x $\in$ R| ax = o}

Required to show, S is a Subring of R.

If o $\in$ R is the Zero element of R.

and a $\in$ R

we have a o = o $\Rightarrow$ o $\in$ S

$\therefore$ S $\neq \phi$ and S C R

Let x, y $\in$ S Then x, y $\in$ R and ax = o, ay = o

Now a(x – y) = ax – ay

= o – o

= o

$x - y \in S$

Also $a(xy) = (ax)y$

$= oy$

$= o$

$= xy \in S$

$\therefore$ S is a subring of R.

Q33. If R is a ring and C (R) = $\{x \in R / xa = ax \ \forall \ a \in R\}$ Than Prove that C (R) is a Subring of R.

Sol :

For $O \in R$

The Zero element of the ring

we have $oa = ao \ \forall a \in R$

By the definition of C(R), $O \in C(R)$

$\therefore \quad C(R) \neq \phi$ & $C(R) \subset R$

Let $x, y \in C(R)$

Then $x, y \in R$ and $xa = ax$

$ya = ay \ \forall a \in R$

$\forall a \in R, a(x-y) = ax - ay$

$= xa - ya$

$= (x-y)a$

$\forall a \in R, a(xy) = (ax)y$

$= (xa)y$

$= x(ay)$

$= x(ya)$

$= (xy)a$

$\therefore x, y \in C(R)$ is a subring of R.

Q34. Let M_2 (Z) be the ring of all 2 × 2 matrices over the integers and Let R = $\left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} \Big/ a, b \in Z \right\}$

prove or disprove that R is a Subring of M_2 (Z)

Sol :

Let $M_2(Z) = \left\{ \begin{bmatrix} p & q \\ r & s \end{bmatrix} \Big/ p, q, r, s \in z \right\}$ be a ring.

Hence R = $\left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} \middle/ a, b \in Z \right\}$ is a subset of M_2 (Z)

if a = b = o $\in Z$

$\Rightarrow \begin{bmatrix} o & o \\ o & o \end{bmatrix} = o \in R$

$R \neq \phi$

Let $A = \begin{bmatrix} a_1 & a_1 \\ b_1 & b_1 \end{bmatrix}$ & $B = \begin{bmatrix} a_2 & a_2 \\ b_2 & b_2 \end{bmatrix} \in R$,

$a_1, b_1, a_2, b_2 \in Z$

Then $A - B = \begin{bmatrix} a_2 - a_2 & a_1 - a_2 \\ b_1 - b_2 & b_1 - b_2 \end{bmatrix} \in R.$

$[\therefore a_1 - a_2 \in Z$ and $b_1 - b_2 \in Z]$

and $A.B = \begin{bmatrix} a_1a_2 + a_1b_2 & a_1a_2 + a_1b_2 \\ a_2b_1 + b_1b_2 & a_2b_1 + b_1b_2 \end{bmatrix} \in R$

$[\therefore a_1a_2 + a_1b_2 \in Z \ \& \ a_2 b_1 + b_1b_2 \in Z]$

Thus $\forall A . B \in R \Rightarrow A - B \in R$

$\Rightarrow A . B \in R$

$\therefore$ R is a Subring of M_2 (Z)

3.7 Integral Domains

3.7.1 Definition and Examples

Q35. Define zero divisors with example

Ans :

A Zero divisor is a non Zero element 'a' of a commutative ring R. Such that there is a non zeco element $b \in R$ with ab = o

Example :

In the ring, $(z_6, \oplus_6, \otimes_6)$ where

$z_6 = \{0,1, 2, 3, 4, 5,\}$ with Zero divisors

$2 \neq 0, \quad 3 \neq 0 \Rightarrow 2 \otimes 3 = 0$

$3 \neq 0, \quad 4 \neq 0 \Rightarrow 3 \otimes 4 = 0$

Q36. Define integral domain with example.

Ans :

An Integral domain is a commutative ring with Unity and no Zero divisors.

Example 1:

(Z, +, ·) is an Integral domain

Example 2:

$(Z_5, \oplus_5, \oplus_5)$ is an example of finite integral domain

Example 3:

The ring Z(x) of polynomials with integer coefficients is an integral domain.

Example 4:

$Z \oplus Z$ is not an integral domain.

Q37. Define Cancellation Law.

Ans :

If $(R, +, \circ)$ is a ring, then $(R, +)$ is an abelian group. So cancellation law with respect to addition all true in R.

Left cancellation Law :

$a . b = a . c \Rightarrow b = c$

Where $a, b, c \in R, \; a \neq 0$

Right cancellation law

$b . a = c . a \Rightarrow b = c$

where $a, b, c \in R, \; a \neq 0$

Q38. A ring R has no zero divisors if and only if the cancellation laws hold in R.

Ans :

Suppose that R has no zero divisors required to prove the cancellation laws hold in

i.e., To prove

(i) Left cancellation law

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

(ii) Right cancellation law

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

(i) Let $a, b, c \in R$ where $a \neq 0$

Consider

$a.b = a.c$

$a.b = a.c = 0$

$a(b - c) = 0$

$\because \; a \neq 0$

and R is without zero divisors

$b - c = 0$

$b = 0 \quad \because \; a.b = 0 \Rightarrow a = 0$ or $b = 0$

(ii) We can also prove right cancellation laws as (i)

$\therefore$ If R has a no zero divisors then the cancellation laws hold in R.

Conversely suppose that

If cancellation laws hold in R

Then Ring R has no zero divisors

Suppose that R is with zero divisors

By definition

$\exists \; a \neq 0 \in R, \; b \neq 0 \in R$ but $a.b = 0$

$\Rightarrow$ $a.b = a.0$

$b = 0$ LCL as $a \neq 0$

Which is a contradiction because $b \neq 0$

$\therefore$ Our assumption is wrong

$\therefore$ R is without zero divisors.

3.7.2 Fields

Q39. What is field? Write some examples.

Ans :

A field is commutative ring with unity in which every non zero element is a unit.

Example 1 :

$(Z, +, \cdot)$ where $Z =$ the set of all integers is not a field, because all non-zero elements of Z are not units.

Example 2 :

$(Z_7, +, \cdot)$ where $Z_7 =$ the set of integers under modulo 7 is a filed.

Q40. A finite integral domain is a field

Ans :

Let us consider a finite integral domain

i.e, $D = \{0, 1, a_1, a_2 \ldots a_n\}$ be all elements of the integral domain D.

and it containing $n + 2$ distinct elements

i.e., $a_i \neq a_j$ for $i \neq j$

Required to prove D is a field

i.e., To prove every non-zero element of 'D' has multiplicative inverse in D.

Let $a \neq 0 \in D$

$a.D = \{a, a.1, a.a_1, a.a_2 ... a.a_n\}$

$a \in D, a_i \in D \Rightarrow a.a_i \in D$

Also the elements of a.D are distinct because

If $a.a_i = a.a_j$ for $i \neq j$

$a_i = a_i$ for $i \neq j$

[$\because$ D is without zero divisors applying LCL as $a \neq 0$]

Which is a contradiction as the elements of D are distinct

$\because$ The elements of a.D are same as elements of D

We have $1 \in a . D$

$\Rightarrow a.1 = 1$ or $a . a_i = 1$

$a = 1$ or $a . a_i = 1$

$a^{-1} = 1$ or a_i is the required

Multiplication of inverse of $a \neq D$

$\therefore$ A finite integral domain is a field.

Q41. Every field is an integral domain.

Ans :

Suppose that (F, +, $\cdot$) is a field

Required prove F is a integral domain i.e., to prove F is without zero divisors

Case (i) :

Consider $a, b \in F$, where $a \neq 0$ and $a.b = 0$

$\therefore$ $a \neq 0 \in F$

We have $a^{-1} \in F$

Consider

$a.b = 0$

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

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

$\Rightarrow 1 b = 0$

$\Rightarrow b = 0$

Case (ii) :

Consider $a, b \in F$, where $b \neq 0$ and $a.b = 0$

$\because$ $b \neq 0 \in F$

We have

$b^{-1} \in F$

Consider

$a \, . \, b = 0$

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

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

$a(1) = 0$

$a = 0$

$\therefore$ By case (i) and case (ii)

$a.b = 0 \Rightarrow a = 0 \text{ or } b = 0$

Q42. For every prime p, Z_p the ring of integers modulo p is a field.

Ans :

$(Z_p, +, \cdot)$ is a ring.

Sine $Z_p = (0, 1, 2, ... p - 1)$ has p distinct elements, Z_p is a finite ring.

Required to prove Z_p is an integral domain

Clearly,

$1 \in Z_p$ is the unity element

for $a, b \in Z_p$

$ab \pmod p \equiv ba \pmod p$

$ab = ba$

Hence Z_p is commutative

for $a, b \in Z_p$

and $ab = 0 \Rightarrow ab = 0 \pmod p$

$\Rightarrow p \mid ab \Rightarrow p \mid a \text{ or } p \mid b$

$\Rightarrow a \equiv 0 \pmod p \text{ or } b \equiv 0 \pmod p$

$\Rightarrow a = 0 \text{ or } b = 0$

$\therefore$ Z_p has no zero divisors

Thus, $(Z_p, +, \cdot)$ is a finite integral domain

$\therefore$ Z_p is a field.

Q43. Prove that $Q\left[\sqrt{2}\right] = \{a + b\sqrt{2} \, / \, a, b \in Q]$ is a field with respect to ordinary addition and multiplication of numbers.

Sol : **(Imp.)**

Let $x, y, z \in Q\left[\sqrt{2}\right]$

So that

$$x = a_1 + b_1\sqrt{2},\ y = a_2 + b_2\sqrt{2},\ z = a_3 + b_3\sqrt{2}$$

where $a_1, b_1, a_2, b_2, a_3, b_3 \in Q$

$$x + y = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})$$

$$= (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

where $a_1 + a_2 = a,\ b_1 + b_2 = b \in Q$

$$x . y = (a_1 + b_1\sqrt{2}) . (a_2 + b_2\sqrt{2})$$

$$= (a_1 a_2) + a_1 b_2\sqrt{2} + a_2b_1\sqrt{2} + b_1 b_2$$

$$= (a_1 a_2 + 2b_1 b_2) + \sqrt{2}\ (a_1 b_2 + a_2 b_1)$$

$$x . y = c + d\sqrt{2}$$

where $c = a_1a_2 + 2b_1b_2 \in Q$

and $d = a_2b_2 + a_2 b_1 \in Q$

$\therefore$ Addition and multiplication of numbers are binary operations in $Q\sqrt{2}$

$$x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} = (a_2 + a_1) + (b_2 + b_1)\sqrt{2}$$

$$= (a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2})$$

$$= y + x$$

= addition is commutative

$$(x + y) + z = (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{2}$$

and $x + (y + z) = (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{2}$

$\Rightarrow$ $(x + y) + z = x + (y + z)$

Addition is associative

for $0 \in Q$

We have $0 + 0\sqrt{2} = 0 \in Q\sqrt{2}$

So that

$x + 0 = x$ for $x \in Q\sqrt{2}$ $\Rightarrow$ $0 \in Q\sqrt{2}$ is the zero element

for $x = a_1 + b_1\sqrt{2} \in Q\sqrt{2}$

We have

$$-x = (-a_1) + (-b_1)\sqrt{2} \in Q\sqrt{2}$$

So that

$x + (-x) = 0$

$\Rightarrow$ Additive inverse exists

$\therefore$ $(Q\sqrt{2}, +)$ is commutative group

$x \cdot y = (a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$

$= (a_2a_1 + 2b_2b_1) + (a_2b_1 + b_2a_1)\sqrt{2}$

$= y \cdot x$

Commutative under multiplication

$(x \cdot y)\, z = (\overline{a_1a_2 + 2b_1b_2} + \overline{a_1b_2 + a_2b_1\sqrt{2}}) \cdot (a_3 + b_3\sqrt{2})$

$= (a_1 a_2 a_3 + 2b_1 b_2 a_3 + 2a_1 b_2 b_3 + 2a_3 b_1 b_3) + (a_1 a_2 b_3 + 2b_1 b_2 b_3 + a_1 a_3 b_2 + a_2 a_3 b_1)\sqrt{2}$

and

$x.(y \cdot z) = (a_1 + b_1\sqrt{2})\,(\overline{a_2a_3 + 2b_2b_3} + \overline{a_2b_3 + a_3b_2}\sqrt{2})$

$= (a_1 a_2 a_3 + 2a_1 b_2 b_3 + 2a_2 b_1 b_3 + 2a_3 b_1 b_2) + (a_1 a_2 b_3 + a_1 a_3 b_2 + a_2 a_3 b_1 + 2b_1 b_2 b_3)\sqrt{2}$

$\therefore$ $x, (y \cdot z) = x \cdot (y \cdot z)$ multiplication is associative

$x \cdot (y + z) = (a_1 + b_2\sqrt{2})\ (\overline{a_2 + a_3} + \overline{b_2 + b_3}\sqrt{2})$

$= (a_1 a_2 + a_1 a_3 + 2b_1 b_2 + 2b_1 b_3) + (a_1 b_2 + a_1 b_3 + a_2 b_1 + a_3 b_1)\sqrt{2}$

and

$x \cdot y + x \cdot z = (\overline{a_1a_2 + 2b_1b_2} + \overline{a_1b_2 + a_2b_1}\sqrt{2}) + (\overline{a_1a_3 + 2b_1b_3} + \overline{a_1b_3 + a_3b_1}\sqrt{2}$

$= (a_1a_2 + 2b_1b_2 + a_1a_3 + 2b_1b_3) + (a_1b_2 + a_2b_1 + a_1b_3 + a_3b_1)\sqrt{2}$

$\therefore$ $x \cdot (y + z) = x \cdot y + x \cdot z$

Distributivity is true

Hence $(Q\sqrt{2}, +, \cdot)$ is a ring.

$1 = 1 + 0\sqrt{2} \in Q\sqrt{2}$

So that

$x \cdot 1 = (a_1 + b_1\sqrt{2})\,(1 + 0\sqrt{2})$

$= x \quad \forall\ x \in Q\sqrt{2}$

$\therefore$ $Q\sqrt{2}$ is a commutative ring with unity element to show that $Q\sqrt{2}$ is a filed we have to prove further every non-zero element in $Q\sqrt{2}$ has multiplicative inverse

Let $a + b\sqrt{2} \in Q\sqrt{2}$ and $a \neq 0$ & $b \neq 0$

Then

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}$$

Since $a^2 - 2b^2 \neq 0$ for $a \neq 0$ and $b \neq 0$

$$a, b \in Q \Rightarrow \frac{a}{a^2-2b^2} \cdot \frac{-b}{a^2-2b^2} \in Q$$

for $a + b\sqrt{2} \neq 0 \in Q\sqrt{2}$ there exists $\left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \in Q\sqrt{2}$

Such that

$$(a + b\sqrt{2})\left[\left(\frac{a}{a^2-2b^2}\right)+\left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}\right] = 1 = 1 + 0\sqrt{2}$$

$\therefore$ Every non zero element of $Q\sqrt{2}$ is invertible

Hence $Q\sqrt{2}$ is a field

Q44. For every prime p, Z_p **the ring of integers modulo p is a field.**

Ans :

We know that

$(Z_p, +, \cdot)$ is a ring

Since Z_p = {0, 1, 2, ... p – 1) has p distinct elements.

Z_p is a finite ring

We prove now

Z_p is an integral domain

Clearly, $1 \in Z_p$ is the unity element

for $a, b \in Z_p$

$a\,b \pmod p \equiv b\,a \pmod p$

$\Rightarrow$ $a\,b = b\,a$

and hence Z_p is commutative

For $a, b \in Z_p$ and $ab = 0 \Rightarrow ab = 0 \pmod p$

$\Rightarrow p / ab$

$\Rightarrow p / a$ or p/b

$\Rightarrow$ $a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$

$\Rightarrow$ a = 0 or b = 0

$\therefore$ Z_p has zero divisors

Thus $(Z_p, +, \cdot)$ is a finite integral domain

$\therefore$ Z_p is a field

3.8 Characteristic of a Ring

Q45. State the characteristic of a ring with example.

Ans :

The characteristic of ring R is the least positive integer n such that $nx = 0 \ \forall$ x in R.

If no such integer exists, we say that R has characteristic 0. The characteristic of R denoted by char R

Example 1:

For any element $x \in Z_3 [i]$ ring

We have

$3x = 0 \ \forall \ x \in Z_3 [i] \Rightarrow$ Characteristic of $Z_3 [i] = 3$

Example 2:

The Set R = {0, 2, 4, 6, 8} is field under addition and multiplication modulo 10.

Q46. The characteristic of an integral domain is the 0 or prime.

Ans : **(Jan-21, May/June-19)**

Let $(R, +, \cdot)$ be an integral domain

Let the characteristic of $R = P(\neq 0)$

If possible. Suppose that P is not a prime

Then P = m n where 1 < m, n < p

$a \neq 0 \in R \Rightarrow a.a = a^2 \in R$ and $a^2 \neq 0$

$\because$ R is integral domain

$Pa^2 = 0 \Rightarrow (mn)\, a^2 = 0 \Rightarrow (ma)\,(na) = 0$

$\Rightarrow ma = 0$ or $na = 0$

Let ma = 0 for any $x \in R$

$(ma)\, x = 0 \Rightarrow a(mx) = 0 \Rightarrow mx = 0$

This is absard

$1 < m < p$ and characteristic of R = P

$\therefore$ $ma \neq 0$

Similarly, we can prove that na $\neq$ 0

This is contradictional

Hence P is a prime.

Q47. If R is a commutative ring with unity of characteristic = 3. Then prove that $(a + b)^3 = a^3 + b^3 \ \forall$ a, b $\in$ R.

Sol :

R is a ring with characteristic = 3

$3x = 0$, zero element of R $\forall x \in R$

Since R is a commutative ring.

By Binomial theorem

$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

$a, b \in R \Rightarrow a^2b,\ ab^2 \in R \Rightarrow 3a^2b = 0$

$3ab^2 = 0$

$\therefore \quad (a + b)^3 = a^3 + b^3$

Q48. If D is an integral domain, Then prove that D[x] is an integral domain.

Sol : **(May/June-19)**

Suppose that,

D is an integral domain

i.e., commutative ring with Unity and has zero divisors.

Since D [x] is ring

If D is commutative rivg with Unit element

f (x) = 1

required to prove D [x] has no zero divisors.

Let f (x), g (x) be non zero polynomials in D [x] where

$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0,\ a_n \neq 0$

$g(x) = b_m x^m + b_{m-1} x^{m-1} + ... + b_0,\ b_n \neq 0$

Since D is an integral domain

$a_n, b_m \neq 0$

$f(x) \neq 0,\ \ g(x) \neq 0$

$f(x)\ \ g(x) \neq 0$

Thus, D [x] has zero divisors.

$\therefore$ If D is an integral domain,

Then D [x] is an integral domain.

Q49. Let G be the group and let Z (G) be the Centre of G. If $\frac{G}{Z(G)}$ is cyclic. Then G is abelian.

Sol : **(May/June-19)**

Given that,

G is a group

and Z (G) is a Centre of G.

If $\frac{G}{Z(G)}$ is cyclic required to prove G is abelian.

i.e., ab = ba,

$\Rightarrow$ < g Z (g) > = $\frac{G}{Z(G)}$

a, b are arbitrary elements of G

Then, $\exists$ integers i and j Such that

$a\,Z(G) = (g\,Z(G))^i = g^i\,Z(G)$ for some 'i'

$b\,Z(G) = (g\,Z(G))^j = g^i\,Z(G)$ for some 'j'

$a\,Z(G) = g^i\,Z(G)$

$a = g^i Z_1$ for some $Z_1 \in Z(G)$

Similarly

$b = g^j Z_2$ for some $Z_2 \in Z(G)$

Consider $ab = (g^i Z_1)(g^j Z_2)$

$= g^i g^j (Z_1 Z_2)$

$ab = g^{i+j} (Z_1 Z_2)$

$= g^{i+j} (Z_1 Z_2)$

$= g^j g^i (Z_1 Z_2)$

$= g^j Z_2 g^i Z_1$

$= ba$

$\therefore$ ab = ba.

$\therefore$ G is Commutative

i. e., G is abelian

$\therefore$ G is abelian when $\frac{G}{Z(G)}$ is cyclic

Q50. Prove that Z_3 [i] = {a + ib / a,b $\in Z_3$ } is a field of order 9?

Sol : **(May/June-19)**

Z_3 [i] = { a + ib / a,b $\in$ Z_3}, & the elements of Z_3 are 0, 1, 2

ie., Z_3 = 0, 1, 2

for a=0, b = 0 $\Rightarrow$ 0 + i 0 = 0

a=0, b = 1 $\Rightarrow$ 0 + 1 (i) = i

a=0, b = 2 $\Rightarrow$ 0 +2 i = 2 i

a=1, b = 0 $\Rightarrow$ 0 + 0 i = 1

a=1, b = 2 $\Rightarrow$ 1 + 2 i = 1 + 2 i

a=1, b = 1 $\Rightarrow$ 1 + i (1) = 1 + i

a=2, b = 0 $\Rightarrow$ 2 + 0 i = 2

a=2, b = 1 $\Rightarrow$ 2 + i (1) = 2 + i

a=2, b = 2 $\Rightarrow$ 2 + 2 i = 2 + 2 i

$\therefore$ Z_3 [i] = {0, i, 2i, 1, 1 + 2i,1 + i, 2, 2 + i, 2 + 2i}

$\Rightarrow$ Z_3 [i] is a field As Z_3 [i] has q elements

$\Rightarrow$ It order is 9

$\therefore$ Z_3 [i] is a field of order 9.

Q51. Prove that the ring of Gaussian integers z[i] = {a + ib / a, b $\in$ z} is an integral domain.

Ans : **(Jan.-21)**

Given that

z[i] = {a + ib / a, b $\in$ z}

c is a ring of complex numbers

z[i] = $\neq$ ϕ

and z[i] $\subset$ c

Let a + ib, c + id $\in$ z[i]

z[i] is said to be the subring of c,

It is satisfies the following conditions

i.e., a, b $\in$ z[i] $\Rightarrow$ a – b $\in$ z[i]

a, b $\in$ z[i] $\Rightarrow$ a b $\in$ z[i]

Let a, b, c, d $\in$ z[i]

Consider

$(a + bi) - (-(c + di)) = (a + bi) + (-c - di)$

$= (a + (-c)) + (b + (-d))i$

$= (a - c) + (b - d)\,i$ ... (1)

Since a, b, c, d $\in$ z

$\Rightarrow$ $(a - c) \in z$ and $(b - d) \in z$

$(a - c) + (b - d)i \in z[i]$

$a - c + bi - di \in z[i]$

$(a + bi) - (c + di) \in z[i]$

Consider

$(a + bi)(c + di) = ac + adi + bci + bdi^2$

$= ac + (ad + bc)i + bd(-1)$

$= (ac - bd) + (ad + bc)i \in z[i]$

$\therefore$ $(a + bi)(c + di) \in z[i]$ ... (2)

$\therefore$ from equation (1) and (2) are satisfied

Hence z[i] is a subring of complex number c

Q52. Let G be a group and let Z(G) be the centre of G. If $\frac{G}{Z(G)}$ cyclic then G is abelian.

Ans :

Given,

G is a group

Z(G) is the centre of G

G is said to be abelian if it satisfies the following condition

ab = ba

Let $\frac{G}{Z(G)}$ is cyclic, then three exists some generator gZ(G) such that,

$$<gZ(g)> = \frac{G}{Z(G)}$$

Let a, b are arbitrary elements of G

Then, there exists integers i and j such that,

$aZ(G) = (gZ(G))^i = g^iZ(G)$ for some 'i'

$bZ(G) = (gZ(G)^i = g^iZ(G)$ for some 'j'

$aZ(G) = g^iZ(G)$

$\Rightarrow$ $a = g^i Z_1$ for some $Z_1 \in Z(G)$

Similarly,

$bZ(G) = g^i Z(G)$

$\Rightarrow$ $b = g^i Z_2$ for some $Z_{21} \in Z(G)$

Consider,

ab = (g'ZJ (gZ_2)

$\Rightarrow$ $ab = g^i g^i Z_1 Z_2$

As the elements of centre Z(G) commute with all elements of G

$\therefore$ $ab = g^i g^i Z_1 Z_2 = g^{i+j} Z_1 Z_2$

$= g^{j+i} Z_2 Z_1 = g^i g^i Z_2 Z_1$

$= g^i Z_2 g^i Z_] = ba$

$\therefore$ ab = ba

$\Rightarrow$ G is commutative i.e., abelian

Hence, G is abelian when $\frac{G}{Z(G)}$ is cyclic

Short Question and Answers

1. The characteristic of an integral domain is the 0 or prime.

Ans :

Let $(R, +, \cdot)$ be an integral domain

Let the characteristic of $R = P(\neq 0)$

If possible. Suppose that P is not a prime

Then $P = m\,n$ where $1 < m, n < p$

$a \neq 0 \in R \Rightarrow a.a = a^2 \in R$ and $a^2 \neq 0$

$\because$ R is integral domain

$Pa^2 = 0 \Rightarrow (mn)\,a^2 = 0 \Rightarrow (ma)\,(na) = 0$

$\Rightarrow ma = 0$ or $na = 0$

Let $ma = 0$ for any $x \in R$

$(ma)\,x = 0 \Rightarrow a(mx) = 0 \Rightarrow mx = 0$

This is absard

$1 < m < p$ and characteristic of $R = P$

$\therefore$ $ma \neq 0$

Similarly, we can prove that $na \neq 0$

This is contradictional

Hence P is a prime.

---

2. If D is an integral domain, Then prove that D[x] is an integral domain.

Sol :

Suppose that,

D is an integral domain

i.e., commutative ring with Unity and has zero divisors.

Since D [x] is ring

If D is commutative rivg with Unit element

$f(x) = 1$

required to prove D [x] has no zero divisors.

Let f (x), g (x) be non zero polynomials in D [x] where

$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0,\ a_n \neq 0$

$g(x) = b_m x^m + b_{m-1} x^{m-1} + ... + b_0, b_n \neq 0$

Since D is an integral domain

$a_n, b_m \neq 0$

$f(x) \neq 0, \; g(x) \neq 0$

$f(x) \; g(x) \neq 0$

Thus, D [x] has zero divisors.

$\therefore$ If D is an integral domain,

Then D [x] is an integral domain.

---

3. Define Normal subgroup with example.

Sol :

A subgroup 'N' of a group 'G' is said to be a normal subgroup of 'G' $\forall \; g \in G, \; \forall \; n \in N$

$\Rightarrow \; g \, n \, g^{-1} \in N$

Eg.

Let $G = \{1, -1, i, -i\}$

$\Rightarrow$ G is group w.r.to multiplication

Sol :

We have $N = \{1, -1\}$ is a subgroup of G

Let $g = 1, \; n = -1 \; \Rightarrow g \, n \, g^{-1} = 1 \times (-1)(1) = -1 \in N$

Let $g = -1, \; n = -1 \Rightarrow g \, n \, g^{-1} = (-1) \times (-1) \times (-1) = -1 \in N$

$g = i, \; n = -1 \Rightarrow g \, n \, g^{-1} = (i) \times (-1)(-i) = -1 \in N$

$g = -i, n = -1 \Rightarrow g \, n \, g^{-1} = (-i) \times (-1) \times (i) = -1 \in N$

$\therefore$ N is a normal subgroup of 'G'.

---

4. Define factor group.

Ans :

Let 'G' be a group and 'N' be a normal subgroup of 'G'. Then the factor group or the Quotient group denoted by

$$\frac{G}{N} = \{Nx \, / \, x \in G\}$$

i.e., the set of all right cosets of N in G forms a group know as factor group

or Quotient group w,r, to the binany operation multiplication of two right cosets.

5. List the applications of factor groups.

Ans :

Let 'G' be a finite group and 'H' be the subgroup of G and H $\neq$ {e}. The factor group is denoted by $\frac{G}{H}$.

(i) The structure of group G and factor group $\frac{G}{H}$ is same. Hence, a less complicated approximation of G can be obtained from the approximation of $\frac{G}{H}$ because $\frac{G}{H}$ is smaller than G.

(ii) The properties of a group G can be obtained by examining the properties of factor group $\frac{G}{H}$.

(iii) The position of element in a factor group gives the cosets of group.

(iv) The order of a subgroup can be obtained by means of factor group.

6. Define Automorphism Homomorphism Image and Isomorphic Image.

Sol :

(i) Automorphism

A mapping $f : G \rightarrow \bar{G}$ is said to be an automorphism if 'f' is an isomorphism i.e., in other words '**f**' is homomorphism, 1 – 1, & onto

(ii) Homomorphic Image

If $f : G \rightarrow \bar{G}$ is homomorphism & onto

Then $\bar{G}$ is called as homomorphic image of G

(iii) Isomorphic Image

If $f : G \rightarrow \bar{G}$ is isomorphism. Then we say that G and $\bar{G}$ are isomorphic to each other and denotes as $G \simeq \bar{G}$ and $\bar{G}$ is called is isomorphic image of G.

7. State the examples of Rings.

Ans :

Example 1:

The set Z of integers Under ordinary addition and multiplication is a commutative ring with Unity 1. The Unity of Z are 1 and –1

Example 2:

The set M_2 (Z) of 2 × 2 matrices with integer entries is a non commutative ring with Unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Example 3:

The set 2 Z of even integers under ordinary addition and multiplication is a commutative ring with out Unity.

Example 4:

The set Z [x] of all polynomials in the variable x with integer coefficients under Ordinary addition and multiplication is a commutative ring with Unity f(x) = 1

8. Define integral domain with example.

Ans :

An Integral domain is a commutative ring with Unity and no Zero divisors.

Example 1:

(Z, +, ·) is an Integral domain

Example 2:

$(Z_5, \oplus_5, \oplus_5)$ is an example of finite integral domain

Example 3:

The ring Z(x) of polynomials with integer coefficients is an integral domain.

Example 4:

$Z \oplus Z$ is not an integral domain.

9. Define Cancellation Law.

Ans :

If $(R, +, \circ)$ is a ring, then (R, +) is an abelian group. So cancellation law with respect to addition all true in R.

Left cancellation Law :

$a . b = a . c \Rightarrow b = c$

Where $a, b, c \in R, a \neq 0$

Right cancellation law

$b . a = c . a \Rightarrow b = c$

where $a, b, c \in R, a \neq 0$

10. What is field? Write some examples.

Ans :

A field is commutative ring with unity in which every non zero element is a unit.

Example 1 :

(Z, +, ·) where Z = the set of all integers is not a field, because all non-zero elements of Z are not units.

Example 2 :

$(Z_7, +, \cdot)$ where Z_7 = the set of integers under modulo 7 is a filed.

Choose the Correct Answers

1. Characterstic of a ring of the farm ________. [a]

   (a) $na = 0$ (b) $na \neq 0$

   (c) $a = 0$ (d) $n = 0$

2. The intersection of subgroup of a ring is ________. [b]

   (a) ring (b) subring

   (c) closed (d) commutative

3. $(a+U)+(b+U) =$ ________. [a]

   (a) $a+b+U$ (b) $a-b+U$

   (c) $-a+b+U$ (d) $a+b-U$

4. Ring satisfies ________ conditions. [d]

   (a) commutative ring (b) field

   (c) ideal (d) group

5. $a \cdot a^{-1} =$ ________. [b]

   (a) 0 (b) 1

   (c) a (d) none

6. $a + a^{-1} =$ ________. [a]

   (a) 0 (b) 1

   (c) a (d) none

7. Multipliative identity is ________. [b]

   (a) 0 (b) 1

   (c) a (d) e

8. Additive identity is ________. [d]

   (a) 1 (b) e

   (c) a (d) 0

9. Set of all integers satisfies ________. [a]

   (a) prime ideal ring (b) group

   (c) maximal (d) ring

10. $R = (Z_6, +, \cdot)$ is a ________ [d]

    (a) ring (b) group

    (c) maximal ideal ring (d) principle ideal ring

Fill in the Blanks

1. $a \cdot e$ = ________.
2. If $(R_1 +, \cdot)$ is said to be boalean ring if ________.
3. Commutative property is ________ with respect to multiplication
4. Distributive laws ________.
5. The intersection of the subgroups of a ring is ________.
6. A commutative ring with unity is containing no zero divisors is called ________.
7. If every non-zero elements of R has a ________.
8. Characteristic of a ring of the farm ________.
9. $\frac{R}{U}$ is commutative, if R is ________.
10. $(a+U)+(b+U)$ = ________ $\forall\, a, b \in R$.
11. $(a+U)(b+U)$ = ________ $\forall\, a, b \in R$.
12. If $\frac{R}{U}$ has a unity element, If R is ________.
13. The ideals is generated by a prime number is ________ .
14. Let 'U' be an ideal of commutative ring R. U is a ________ . Iff $\frac{R}{U}$ is an ________ .
15. Let R be a commutative ring & $U \neq R$ is a prime ideal. If ________.

ANSWERS

1. $\because$ As – a
2. $a^2 = a, a^2 = a, \forall a \in R$
3. $a.b = b.a,\ \forall a, b \in R$
4. $a(b+c) = ab + ac$
5. agian a sub ring
6. Integral domain
7. multiplicative inverse
8. $na = 0,\ \forall a \in R$
9. commutative
10. $(a+b)+U$
11. $ab+U$
12. unity element
13. a maximal ideal
14. prime ideal, integral domain
15. $\forall\, a, b \in R$ & $ab \in U \ni a \in U$ (or) $b \in U$

UNIT IV	**Groups:** Definition and Examples of Groups - Elementary Properties of Groups - Finite Groups - Subgroups - Terminology and Notation -Subgroup Tests - Examples of Subgroups. **Cyclic Groups:** Properties of Cyclic Groups -Classication of Subgroups Cyclic Groups.

4.1 Ideals and Factors Rings

Q1. Define ideals.

Ans :

A non empty subset 'S' of a ring 'R' (R, +, ·) is said to be an ideal of R.

If 1. S is a group of R, w.r.to addition

2. $\forall$ r $\in$ R, $\forall$ s $\in$ S $\Rightarrow$ r.s & s r $\in$ S

Q2. Define improper ideals.

Ans :

The ideals S = {0} and S = R are Known as improper ideals of R. The ideals other Than S = {0} and S = R are known are proper ideals of R.

Q3. If R is a Unity and 'U' is an idel of R. Where 1 $\in$ U. Then prove that U = R.

Ans :

Given that

'R' is a ring with Unity

U is an ideal of R

1 $\in$ U

$\therefore$ U is an ideal of R

By definition U $\subset$ R ..... (1)

Required to prove R $\subset$ U

$\because$ U is an ideal of R

We have by definition

$\forall$ r $\in$ R, 1 $\in$ U $\Rightarrow$ r . 1 & 1 . r $\in$ U

$\Rightarrow$ r $\in$ U

$\Rightarrow$ R $\subset$ U ..... (2)

From equation (1) and (2)

We can conclude that U = R

Q4. If R is a commutative ring and $a \in R$ then $Ra = \{ra / r \in R\}$ is an ideal of R.

Ans :

For $0 \in R$, $0a = 0 \in R a$

$\therefore$ $Ra \in \phi$ & $R a \subset R$

Let $x, y \in R a$

Then $x = r_1 a$

$y = r_2 a$ where $r_1, r_2 \in R$

$x - y = r_1 a - r_2 a$

$= (r_1 - r_2) a$ when $r_1, r_2 \in R$

$x, y \in R a \Rightarrow x - y \in R a$ .... (1)

Let $x \in R a$ and $r \in R$

$x . r = (r_1 a) r$ ($x = r_1 a$ whene $r_1 \in R$)

$= r_1(a r)$

$= r_1 (r a)$

$= (r_1 r) a$

$= r' a$ where $r' = r_1 r \in R$ ..... (2)

Sinec R is commutative ring,

$\Rightarrow$ $x, r = r . x$

$\therefore$ $x \in R a,$ $r \in R$

$\Rightarrow$ $x r = r x \in R a$

Hence from (1) & (2)

Ra is an ideal of R

4.1.1 Factor Rings

Q5. Define factor Ring.

Ans :

Let (R, +, **.**) be a ring and 'U' be an ideal of R Then $\frac{R}{U} = \{u + x / x \in R\}$ form a ring known as a factor ring with respect to the operations defined as follows

(i) $(u + x) + (u + y) = u + (x + y)$

(ii) $(u + x) . (u + y) = u + xy$

Q6. (R, +, .) be a ring, 'U' be an idea of R. Then $\frac{R}{U}$ is factor ring.

Ans :

(R, +, **.**) be a ring.

U be an ideal of R.

Required to prove $\frac{R}{U}$ forms a factor ring

1. $\left(\frac{R}{U}, +\right)$ is an abelian group

2. $\left(\frac{R}{U}, \bullet\right)$ is an semi group

1. $\left(\frac{R}{U}, +\right)$ is an abelian group

Let $U + x,\ U + y,\ U + Z \in \frac{R}{U}$ where $x, y, z \in R$

(a) Closure Property :

$$\forall\ U + x,\ U + y, \in \frac{R}{U} \Rightarrow (U + x) + (U + y)$$

$$\Rightarrow U + (x + y) \in \frac{R}{U}$$

(b) Associative Property :

$[(U + x) + (U + y)] + U + Z = (U + x) [(U + y) + (U + z)]$

Consider

$$\begin{aligned}[(U + x) + (U + y)] + (U + z) &= [U + (x + y)] + (U + z)\\ &= U + (x + y) + z\\ &= U + (x + (y + z))\\ &= (U + x) + (U + (y + z))\\ &= (U + x) + [(U + y) + (U + z)]\end{aligned}$$

L H S = R H S

(c) Identity Property :

$$\forall\, a + x \in \frac{R}{U}\ \exists\ U + 0 \in \frac{R}{U}$$

$$\ni U + x + (U + 0) = U + (x + 0)$$
$$= U + x$$

Similarly $(U + 0) + (U + x) = U + x$

(d) Inverse Property :

$$\forall\ U + x \in \frac{R}{U}\ \exists\ U + (-x) \in \frac{R}{U}$$

$\ni$ (U + x)+ U + (–x) = U + (x +(–x))

= U + 0

Similarly (U + (–x)) + (U + x) = U + 0

(e) Commutative Proparty :

$\forall$ U + x, U + y $\in \frac{R}{U}$

(U + x) + (U + y) = U + (x + y)

= U + (y + x)

= (U +y) + (U + x)

$\left(\frac{R}{U}, +\right)$ is abelian group

2. $\left(\frac{R}{U}, \bullet\right)$ is a semi group

(a) Closure Property

$\forall$ U + x , U + y $\in \frac{R}{U}$

$\Rightarrow$ (U + x) + (U + y) = U + x y $\in \frac{R}{U}$

(b) Associative Property

$\forall$ U + x , U + y & U + Z $\in \frac{R}{U}$

Consider

[(U + x) + (U + y)] (U + z) =(U + xy) (U + z)

= U + (xy) z

= U + x (yz)

= (U + x) + (U + yz)

= (U + x) (U + y) (U + z)

$\left(\frac{R}{U}, \bullet\right)$ is a semi group

Distributive Law

LDL : $\forall$ U + x, U + y, U + z $\in \frac{R}{U}$

(U + x) [(U + y) (U + z)] = (U + x) (U + y) + (U + x) (U + z)

L H S = (U + x) [(U + y) + (U+ z)]

= (U + x) [(U + (y + z)]

= U + x (y + z)

= U +xy + xz

= (U + xy) + (U + xz)

= (U + x) (U + y) + (U + x) (U + z)

R H S

Similarly R D L is also holds good

4.2 Prime Ideal and Maximal Ideal

Q7. Define Principal Ideal.

Ans :

If R is a commutative ring with Unity, we observe for a given a $\in$ R the set {ra / r $\in$ R} is an ideal in R that contains the element 'a' here 'a' is called principal ideal generated by 'a'. is denoted by (a) or $\langle a \rangle$.

Q8. Let R be a commutative ring with Unity and let A be an ideal of R. Then $\frac{R}{A}$ is an integral domain if and only if A is Prime

Ans : **(May/June-19)**

Given that

'R' is a commutative ring with Unity and 'S' is ideal of 'R.'

To prove that $\frac{R}{S}$ is an Integral domain $\Leftrightarrow$ S is prime ideal of R.

Suppose that $\frac{R}{S}$ is an Integral domain

$\Rightarrow$ $\frac{R}{S}$ is without zero divisors.

By definiton

We have if S + a, S + b $\in \frac{R}{S}$ such that

(S + a) . (S + b) = S = S + o

$\Rightarrow$ S + a = S or S + b = S ..... (1)

Now we shall prove that

S is a prime ideal of R

Let $S \in S$ when $S = a.\ b$ when $a, b \in R$

To show that $a \in s$ or $b \in s$

$S \in S \Rightarrow S + S = S$

$\Rightarrow S + ab = S$

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

$\Rightarrow S + a = S$ or $S + b = S$ by ..... (1)

$\Rightarrow a \in S = S$ or $b \in S$

S is a prime ideal of R

Conversely suppose That

'S' is a prime ideal of 'R'

Required to show $\frac{R}{S}$ is an Integral domain

It is required to show that

$\frac{R}{S}$ is with out zero divisors.

Let $S + a , S + b + \frac{R}{S}$

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

$\Rightarrow S + (ab) = S$

$ab \in S$

$a \in s$ or $b \in s$

$\Rightarrow S + a \in S$ or $S + b \in S$

$\frac{R}{S}$ is without zero divisors.

Q9. Define maximal ideal.

Ans :

A maximal ideal M of a ring R is an ideal different from R such that there is no proper ideal U of R properly containing M.

Q10. Let R be a commutative ring with Unity and Let A be an ideal of R.

Then $\frac{R}{A}$ is a field if and only if A is maximal.

Ans : **(Nov.-20)**

Given that

R is a commutative ring with unity and 'S' is an ideal of R.

Required to prove $\frac{R}{S}$ is field

If and only if S is a maximal ideal of R

Suppose that $\frac{R}{S}$ is a field.

Let S' be an ideal of R when S $\neq$ S' and S $\subset$ S' $\subset$ R

i.e., to prove S is maximal ideal of R

Consider

$S \subset R \Rightarrow \exists\, a \in R \ni a \notin s$

$\Rightarrow S + a \neq S$

$\Rightarrow$ S + a is non zero element of $\frac{R}{S}$

Similalry

$S \subset S' \Rightarrow \exists\, b \in S`$

$\exists\; b \notin S$

$S + b \neq S$

$\Rightarrow$ S + b is an non zero element of $\frac{R}{S}$

$\therefore$ $\frac{R}{S}$ is a field.

$\frac{R}{S}$ is an integral domain

$\therefore$ $\frac{R}{S}$ is without zero divisors

We can find $S + C \in \frac{R}{S}$

$\ni$ S + a = (S + b) (S + c)

$\Rightarrow$ S + a = S + bc

a – bc $\in$ S'

$\because$ S $\in$ S' ..... (1)

we have S` is an edeal of R

we have b $\in$ s` & c $\in$ R

bc $\in$ S` .... (2)

Apply closure property to the element

$a - bc$ & bc

$\Rightarrow$ $a - bc + bc \in S'$

$a \in S'$

$\therefore$ $\forall$ $a \in R$ we have $a \in S'$

$R \subset S'$

$S' = R$

Hence 'S' is maximal ideal of R

Connversely suppose that

S is maximal ideal of R

Required to prove $\frac{R}{S}$ is a field.

$\because$ R is a commutative ring with Unity

We have $\frac{R}{S}$ is also commutative ring with Unity .

Required to prove

$\frac{R}{S}$ is field it is enough the show, every non zero element of $\frac{R}{S}$ has multiplication inverse of $\frac{R}{S}$

Let $S + a$ be a non zero element of $\frac{R}{S}$

Consider the principle ideal generated by 'a'

i.e., $<a> = \{ax / x \in R\}$

$\because$ The sum of two ideals is again an ideal.

We have $S + <a>$ is also an ideal.

$S \subset S + <a> \subset R$

$\because$ S is maximal ideal of R

We have

$S + <a> = R$

$R \subset S + <a>$

$1 \in R \Rightarrow 1 + S + <a>$

$1 = d + ax$

$d \in S \Rightarrow S + d = S$

$S + (1 - ax) = S$

$S + 1 = S + ax$

$\quad = S + (1 - ax) = S$

$S + 1 = S + ax$

$S + 1 = (S + a)(S + x)$

$S + x$ is required multiplication inverse

$\therefore \quad \frac{R}{S}$ is a field

4.3 Ring Homomorphism

4.3.1 Definition and Examples

Q11. Define Ring homomorphism.

Ans :

A ring homomorphism from a ring R to ring S is a mapping from R to S that preserves the two ring operations.

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

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

$\phi(a\ b) = \phi(a) \cdot \phi(b)$

Let R & S be two rings w.r. to the binary operations '+' & '$\cdot$' defined on them, then ϕ is said to be an isomorphism if ϕ is homomorphism, ϕ is one one & ϕ is onto.

Q12. Let n be an integer with decimal representation $a_k\ a_{k-1} + \ldots\ldots a_1\ a_0$ is divisible by 9 if and only if $a_k + a_{k-1} + \ldots\ldots a_1\ a_0$ is divisible by 9.

Sol :

Let $n = a_k\ a_{k-1} + \ldots\ldots a_1\ a_0$

$\quad = a_k\ 10^k + 1\ a_{k-1}\ 10^{k-1} + \ldots.. + a_1 . 10 + a_0$

Let the natural mapping

$\alpha : z \to z_9$ be defined by

$\alpha(x) = \gamma(\text{mod } 9) \quad \forall\ x \in z$

$\alpha(10) = 1$ is a homomorphism

$\therefore$ n is divisible by 9

$\alpha(n) = 0$

$\Leftrightarrow \alpha[a_k\ 10^k + a_{k-1}\ 10^{k-1} + \ldots.. + a_1 10 + a_0] = 0$

$\Leftrightarrow \alpha(a_k)\ [\alpha(10)]^k + \alpha(a_{k-1})\ [(10)]^{k-1} + \ldots.. + \alpha(a_0) = 0$

$\Leftrightarrow \alpha(a_k) + \alpha(a_{k-1})\ 1 + \ldots.. + \alpha(a_0) = 0$

$\Leftrightarrow \alpha(a_k + a_{k-1} + \ldots.. + a_1 + a_0) = 0$

$\Leftrightarrow a_k + a_{k-1} + \ldots.. + a_1 + a_0$ is divisible by 9

4.4 Properties of Ring Homomorphism

Q13. Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S. Then for any r $\in$ R and any position integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(n))^n$.

Ans :

Let R and S are two rings

$\phi : R \to S$ be a ring homomorphism for any $r \in R$

and any positive integer $n \Rightarrow n . r \in z$

Consider

$\phi(n . r) = \phi(r + r ..... + r)$ n times

$= \phi(r) + \phi(r) + ... + \phi(r)$

$\phi(nr) = n . \phi(r)$

$\phi(r^n) = \phi(r . r ..... r)$ (n times)

$= \phi(r)\ \phi(r)\ .....\ \phi(r)$

$\therefore \quad \phi(r^n) = [\phi(r)]^n$

Q14. Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R then $\phi(A) = \{\phi(x) / x \in A\}$ is a subring of S.

Ans :

Let R and S are two rings

Let A a subring of R.

$\phi(A)$ is a non empty

$\bar{0} \in \phi(A)$ as $\bar{0} = \phi(0)$

Let $\phi(a_1),\ \phi(a_2) \in \phi(A)$

where $a_1, a_2 \in A$

(i) Required to show that

$\phi(a_1) - \phi(a_2) \in \phi(A)$

$= \phi(a_1) + \phi(-a_2)$

$= \phi(a_1 + (-a_2))$

$= \phi(a_1 - a_2) \in \phi(A)$

(ii) Required to show $\phi(a_1),\ \phi(a_2) \in \phi(A)$

Consider $\phi(a_1) . \phi(a_2) = \phi[a_1\ a_2] \in \phi(A)\ \ a_1, a_2 \in A$

Q15. Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S. If A is an ideal and ϕ is onto S, then ϕ(A) is an ideals.

Ans :

Let S & R be two rings

$\phi : R \to S$ be a ring onto homomorphism

Let A be an ideal of R.

Then the range set $\phi(A) = \{\phi(x) / x \in A\}$ is Subset of S

i.e., The identity element

$0 \in R \Rightarrow 0 \in A \Rightarrow \phi(0) = 0' \phi(A)$

and $0' \in S$ where 0' is an identity element in S

$\therefore \quad \phi(A) \neq \phi$ and $\phi(A) \subseteq S$

$\forall \; \phi(x), \; \phi(y) \in \phi(A) \Rightarrow \exists \; x, y \in A$

$\Rightarrow x - y \in A$

$\Rightarrow \phi(x - y) \in \phi(A)$

Consider

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

$= \phi(x) + \phi(y)$

$= \phi(x) - \phi(y) \in \phi(A)$

Let $r \in R$ and $x \in A \Rightarrow rx$ and $xr \in A$

$r' \in R$ and $x' \in \phi(A) \Rightarrow r' = \phi(r) \; \exists \; r \in R$ and $x' = \phi(x) \; \exists \; x \in A$

Consider

$r' . x' = \phi(r) . \phi(x)$

$= \phi(rx) \in \phi(A)$

$x' . r' = \phi(x) . \phi(r)$

$= \phi(xr) \in \phi(A)$

Hence $\phi(A)$ is an ideal of R

4.4.1 Kernel of Homomorphism

Let ϕ be a ring homomorphism from a ring R to a ring S. Then Ker $\phi = \{r \in R / \phi(r) = 0\}$ is an ideal of R.

Q16. Let ϕ be a ring homomarphism from a ring R to a ring S. Let A be a subring of R and Let B be an ideal of S If ϕ is an isomurphism If and only if ϕ is onto and Ker $\phi = \{r \in R / \phi(r) = 0\} = \{0\}$

Ans : **(May/June-19)**

Let ϕ be an into isomarphism i.e., f is one one homomorphism

We prove that Ker $\phi = \{0\}$

a $\in$ R, ϕ (a) = d $\Rightarrow$ ϕ (a) = ϕ (0)

$\Rightarrow$ a = 0

0 $\in$ R is the only element in R

So that $\phi(0) = 0$

By definition Ker ϕ = {0}

Conversely Suppore

Let Ker ϕ = {0}

Required to prove ϕ is one – one

a, b $\in$ R and ϕ(a) = ϕ(b)

$\phi(a) - \phi(b) = 0' \Rightarrow \phi(a - b) = 0'$

$\Rightarrow$ a – b $\in$ Ker ϕ = {0}

a – b = 0

a = b

$\therefore$ ϕ is one – one

Q17. Let ϕ be an isomorphism from a ring R onto a ring S, Then ϕ^{-1} is an isomorphism from S onto R.

Ans :

Let R and S are two rings

Let ϕ : R $\rightarrow$ S is an isomorphism then the range set $\phi(R) = \{\phi(x) / x \in R\} = S$

ϕ^{-1} : S $\rightarrow$ R is an inverse function of ϕ

$\phi^{-1}(s) = \{\phi^{-1}(x^1) / x^1 \in s\}$ is also subring of R

Now, $\forall$ x', y' $\in$ S $\Rightarrow$ $\phi^{-1}(x') = x$ & $\phi^{-1}(y') = y \ \exists\ x + y \in R$

$\Rightarrow$ x + y $\in$ R & xy $\in$ R

$\Rightarrow$ $\phi(x + y) = \phi(x) + \phi(y)$

$= x' + y'$

$\phi(xy) = \phi(x) . \phi(y)$

$= x' y'$

Consider

$\phi^{-1}(x' + y') = x + y$

$= \phi^{-1}(x) + \phi^{-1}(y)$

& $\phi^{-1}(x' y') = xy = \phi^{-1}(x)\, \phi^{-1}(y)$

$\therefore$ ϕ^{-1} : S $\rightarrow$ R is a homomorphism

Let $\phi : R \to S$ is 1 –1

and onto then $\phi^{-1} : S \to R$ is also one one and onto

$\therefore$ $\phi^{-1} : S \to R$ is an isomorphism.

Q18. Let R be a ring with Unity 1. The mapping $\phi : Z \to R$ given by $n \to n.1$ is a ring homomorphism.

Ans :

Let R be a ring with Unity 1

Then mapping $\phi : Z \to R$ be defined by

$\phi(n) = n .1 \quad \forall n \in z$

$\forall$ m, n $\in$ z $\Rightarrow \phi(m) = m . 1$ & $\phi(n) = n . 1$

Now, $m + n \in z \Rightarrow \phi(m + n) = (m + n) . 1$

$= m . 1 + n . 1$

$= \phi(m) + \phi(n)$

and m, n $\in$ z $\Rightarrow \phi(m . n)$

$= (m . n) . 1$

$= (m . 1) (m . 1)$

$\phi (m . n) = \phi(m) + \phi(n)$

$\phi : Z \to R$ is a homomorphim

Q19. For any positive integer n. The mapping $\phi : Z \to Z_n$ defined as $\phi(x) = \overline{r}$ where x = r (mod n) is a ring homomorphism.

Ans :

Given that

$\phi : Z \to Z_n$

defined $\phi(x) + \overline{r}$ where $x = r(\text{mod } n)$

Required to show,

$\phi (x + y) = \phi(x) + \phi(y)$

Let $\phi(y) = \overline{s}$

where $y = s \text{ (mod n)}$

$x + y = r + s(\text{mod n})$

Similarly

$x . y = r . s \text{ (mod n)}$

$\overline{r+s} = \overline{r} + \overline{s}$

$\overline{rs} = \overline{r} . \overline{s}$

L H S $\phi(x + y) = \overline{r+s}$

$= \overline{r} + \overline{s}$

$= \phi(x) + \phi(y)$

$\phi(xy) = \overline{rs}$

$= \overline{r} + \overline{s}$

$\phi(xy) = \phi(x) + \phi(y)$

$\therefore$ ϕ is homomorphism

Q20. If A is an ideal of a ring R . Then show that the Quotient ring $\frac{R}{A}$ is a homomorphic image of R.

Ans :

Let R be a ring

A be an ideal of R.

$\frac{R}{A}$ = {r +A / r $\in$ R} is ring with respect to addition and multiplication of cosets

(a + A) + (b + A) = (a + b) + A and (a + A) (b + A)

$= ab + A$ for $a + A, b + A \in \frac{R}{A}$

Let 'f' be a mapping from a ring R to the ring $\frac{R}{A}$.

i.e., $f : R \to \frac{R}{A}$

$\frac{R}{A}$ is said to be homomorphic image of R.

If it satisfices the following conditions

(i) f is well defined

$f : R \to \frac{R}{A}$ defined by

$f(a) = a + A \quad \forall\ a \in R$

$\forall\ a, b \in R, a = b \Rightarrow a + A = b + A$

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

f is well defined

(ii) f is homomorphism

$\forall$ a, b $\in$ R

$f(a+b) = (a + b) + A$

$= (a + A) + (b + A)$

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

$\therefore$ $f(a + b) = f(a) + f(b)$

Consider

$f(ab) = ab + A$

$= (a + A)(b + A)$

$= f(a) f(b)$

$f(ab) = f(a) f(b)$

$\therefore$ f is ring homomorphism.

(iii) f is an onto mapping

of $x + A \in \frac{R}{A}$ then $x \in R$

$x \in A \Rightarrow f(x) = x + A$

$\forall\ x + A \in \frac{R}{A}$ $\exists\ x \in R$ for which $f(x) = x + A$

f is an onto

$f : R \to \frac{R}{A}$ is an onto homomorphim

f is well defined and homomorphism and onto mapping

$\frac{R}{A}$ is homomorphic image of R.

Hence, the Quotient ring $\frac{R}{A}$ is an homomorphic image

Q21. Prove that every homomorphic image of a ring R is isomorphic to some Quotient Ring of R.

Ans :

Let $\bar{R}$ be the homomorphic image of ring R.

$f : R \to \bar{R}$ such that f is homomorphism and f is onto

Let S be the Kernel of f

$S = \{x \in R / f(x) = \bar{0}\}$

S is one ideal of R

$$\frac{R}{S} = \{S + x / x \in R\}$$

$$\frac{R}{S} \simeq \overline{R}$$

Define a mapping $\phi : \frac{R}{S} \to R$ as $\phi (s + x) = f(x)$

(i) ϕ is well defined,

Let $S + x,\ S + y \in \frac{R}{S}$

Such that S + x, S + y required show, $\phi(S + x) = \phi(x + y)$

Consider

$S + x = x + y$

$x - y \in S$

$f(x - y) = \overline{0}$

$f(x) - f(y) = \overline{0}$

$f(x) - f(y) + f(y) = \overline{0} + f(y)$

$f(x) = f(y)$

$\phi(S + x) = \phi(S + y)$

ϕ is well defined mapping.

(ii) ϕ is homomorphism.

Required to show

$\phi[(S + x) + (S + y)] = \phi(S + x) + \phi(S + y)$

Consider

$$\begin{aligned}\phi[(S + x) + (S + y)] &= \phi[S + (x + y)] \\ &= f(x + y) \\ &= f(x) + f(y) \\ &= \phi(S + x) + \phi(S + y)\end{aligned}$$

L H S = R H S

(iii) ϕ is one – one

Let $(S + x) . (S + y) \in \frac{R}{S}$

$\Rightarrow \quad \phi(S + x) = \phi(S + y)$

$f(x) = f(y)$

$f(x) - f(y) = \bar{0}$

$f(x - y) = \bar{0}$

$x - y \in S$

$S + x . S + y$

(iv) ϕ is onto

$\because$ f is onto, we have $\forall\ y \in \bar{R}$

$\exists\ x \in R \ni y = f(x)$

$\Rightarrow \quad \phi(S + x)$

$y = \phi(S + x)$

ϕ is onto

$\therefore \quad \frac{R}{S} \simeq \bar{R}$

Q22. Let R be a commutative Ring of characteristics 2,

Then prove that the mapping a $\rightarrow$ a² is a ring homomorphism from R to R.

Ans : **(Nov.-20)**

Given that

R is commutative ring and char is 2

$\phi : R \rightarrow R$ and $\phi(a) = a^2 \quad \forall\ a \in R$ ... (1)

Let $a, b \in R \Rightarrow 2a = 0$ and $2b = 0$ ... (2)

$a + b \Rightarrow 2ab = 0$ ... (3)

$f(b) = b^2 \quad \forall\ b \in R$

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

$= a^2 + b^2 + 2ab$

$= a^2 + b^2 + 0$ by (2)

$= a^2 + b^2$

$\phi(a + b) = \phi(a) + \phi(b)$ by (1)

Also, $\phi(ab) = (ab)^2$

$= a^2 b^2$

$= \phi(a)\ \phi(b)$

Hence ϕ is a ring homomorphism.

Q23. Is the ring 2z is isomorphic to ring 3z.

Ans :

Given,

2z and 3z are rings

Let z = {n / n ∈ z} then

2z = {2n / n ∈ z}

3z = {3n / n ∈ z}

ϕ is a mapping from 2z to 3z

i.e., $\phi : 2z \to 3z \ni \phi(2.h) = 3h \quad \forall\ h \in z$

$\forall$ 2a, 2b ∈ 2z

Then the ring 2z is isomorphic to ring 3z, if ϕ is isomorphism, ϕ is one one

ϕ is well defined and ϕ is onto

$\phi(2a + 2b) = \phi(2(a + b))$

$= 3(a + b)$

$= 3a + 3b$

$= \phi(2a) + \phi(2b)$

$\therefore \quad \phi(2a + 2b) = \phi(2a) + \phi(2b)$

$\phi(2a \,.\, 2b) = \phi(2\ (2ab))$

$= 3(2ab)$

$\neq \phi(2a)\ \phi(2b)$

$\therefore$ The ring 2z is not isomorphic to the ring 3z.

Q24. Prove that the subset S of all matrices of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ with a and b integers forms a subring of the M_2 of all 2 × 2 matrices with integers as entries. Is it and ideal.

Ans :

Let, $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$,

$B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$ are any two elements of S

Where,

a, b, c, d ∈ Z

$$A - B = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} - \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$$

$$\Rightarrow \quad A - B = \begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in S$$

$$AB = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$$

$$= \begin{bmatrix} a\times c+0\times 0 & a\times 0+0\times d \\ 0\times c+b\times 0 & 0\times 0+b\times d \end{bmatrix}$$

$$= \begin{bmatrix} ac+0 & 0+0 \\ 0+0 & 0+bd \end{bmatrix}$$

$$\Rightarrow \quad AB = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in S$$

$\therefore$ S is a subring of M_2

Let, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$, $\begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \in R$,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1\times 3+0\times 2 & 1\times 4+0\times 1 \\ 0\times 3+1\times 2 & 0\times 4+1\times 1 \end{bmatrix}$$

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

$$= \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \notin S$$

$\therefore$ S is not an ideal of M_2

Q25. If a map $\phi : R \to R'$ is a homomorphism with Ker ϕ. Then prove that Ker ϕ is an ideal of R.

Ans :

Given that $\phi : R \to R'$ is a homomorphism with Ker ϕ.

S is a nonempty subset of R

Then if is satisfies the following conditions.

(i) Subset S is a subgroup of R with respect to addition

(ii) $r s \in S$ and $sr \in S \ \forall \ r \in S$ and $s \in S$

Required to show that S is an ideal of R

Let O, O' $\in$ R and R' respectively.

Let S be a Kernel of f.

$\therefore$ S = {x $\in$ R : f(x) = O'}

O $\in$ S

f(O) = O'

$\therefore$ S is non empty

If a, b $\in$ S

Then

f(a) = O' = f(b) ... (1)

f(a – b) = f(a + [–b])

= f(a) + f(–b)

= f(a) – f(b)

= O' – O'

a –b $\in$ S

If r is any element of R

Then f(ar) = f(a) . f(r)

= 0' f(r)

f(ar) = 0' ... (2)

and, f(ra) = f(r) f(a)

= f(r) . 0'

f(ra) = 0' ... (3)

From (2) and (3) ar $\in$ S, r a $\in$ S

Hence a, b $\in$ S, r $\in$ S $\Rightarrow$ (a – b) $\in$ S, ar $\in$ S, ra $\in$ S

$\therefore$ S is a ideal of R.

Q26. Let ϕ be a ring homomorphism from Ring R to ring S. If R is commutative ring prove that ϕ(R) is commutative.

Ans : **(Jan.-21)**

Let R and S be a two rings

$\phi : R \to S$

and R is a commutative ring

Let the homomorphic image of R be ϕ(R)

Let x, y $\in$ ϕ(R)

$\Rightarrow$ x, y $\in$ ϕ(R) $\Rightarrow$ $\exists$ a, b $\in$ R

ϕ(a) = x, ϕ(b) = y

$\Rightarrow$ xy = ϕ(a) ϕ(b)

$= \phi(ab)$

$= \phi(ba)$ $\because$ R is commutative ring

$= \phi(b)\,\phi(a)$

$= yx$

$\therefore$ $xy = yx$

Let $\phi : R \to S$ is a ring homomorphism

Let '1' be the unity element of R

$\Rightarrow$ $\phi(1) \in S$

Let a, be an element of R.

$a \in R$

$a' \in R$

$\Rightarrow$ $a' = \phi(a)$ for some $a \in R$

Consider

$\phi(1)\,a' = \phi(1)\,\phi(a)$

$= \phi(1a)$

$= \phi(a)$

$= a'$

$\phi(1)\,a' = a'$ ... (1)

Consider

$a'\,\phi(1) = \phi(a)\,\phi(1)$

$= \phi(a1)$

$= \phi(a)$

$= a'$

$\therefore$ $a'\,\phi(1) = a'$ ... (2)

From (1) and (2)

$\phi(1)\,a' = a'\,\phi(1) = a'$

$\therefore$ $\phi(1)$ is a unity element of S

Q27. Prove that ring with unity contains z_n or z.

(OR)

If R is a ring with unity and the characteristics of R is n > 0 then prove that R contains a subring is isomorphic to Z_n. If the characteristics of R is 0 then R contains a subring isomorphic to Z.

Ans : **(Jan.-21, May/June.-19)**

Given that, R is a ring with unity

S be a subring of R

S = {K.1 / K $\in$ z}

From the definition of Ring homomorphism

$\phi : z \to$ S given by ϕ(K) = K.1 is a homomorphism

By the first isomorphism of ring

$$\frac{z}{\text{Ker } \phi} \approx S \qquad \text{But Ker } \phi = <n>$$

where n – additive order of 1 from the property of characteristic of a ring with unity.

Let R be a ring with unity 1.

Let 1 has order n under addition

Then R has characteristic n

If R has characteristic 'n'

$$\text{Then } S \approx \frac{z}{\text{Ker } \phi} \approx \frac{Z}{< n >} \approx z_n$$

R contains, a subring isomorphic to z_n

When the characteristic of R is n.

If R has characteristic

$$\text{Then } S \approx \frac{z}{\text{Ker } \phi} \approx \frac{Z}{< 0 >}$$

$$\approx Z$$

Z_n contains a ring with unity.

Q28. Let ϕ be a ring homomorphism from a ring R to a ring S. Then Ker ϕ = {r $\in$ R / ϕ(r) = 0} is an ideal of R.

Ans : **(May/June-19)**

Given that

ϕ is a ring homomorphism

i.e., $\phi : R \to S$

Required to show that Ker ϕ is an ideal of R

Let 0 $\in$ R and 0' $\in$ S

Let ϕ be a Kernel of f

$\therefore \quad \phi$ = {r $\in$ R : ϕ(r) = 0}

0 $\in \phi$, Since f(0) = 0'

ϕ is non empty

If $a, b \in \phi$ then

$f(a) = 0' = f(b)$

$f(a - b) = f(a + (-b))$

$= f(a) + f(-b)$

$= f(a) - f(b)$

$= 0' - 0' \qquad \because f(a) = 0' = f(b)$

$a - b \in \phi$

If r is any element of R.

$f(ra) = f(r)\ f(a)$

$= f(r)\ 0$

$= 0$

$f(ra) = 0$

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

$= 0\ f(r)$

$= 0$

$\therefore \quad f(ra) = 0$ and $f(ar) = 0 \Rightarrow ar \in \phi$ and $ra \in \phi$

Hence $a, b \in \phi, \quad r \in \phi, \quad r \in R$

$\Rightarrow \quad (a - b) \in \phi, \ ar \in \phi, \ ra \in \phi$

$\therefore \quad \phi$ is ideal of R

i.e., Ker ϕ is an ideal of R.

Q29. If F is a field of characteristic zero then prove that F contains a subfield isomorphic to the rational numbers.

Ans : **(Jan.-21)**

Given that, F is a field of characteristic zero

S is isomorphic to Z

Let g be the ring isomorphic to S to Z

Let $T : \left\{ \frac{a}{b} \Big/ a, b \in s, \ b \neq 0 \right\}$ be the subfield

$f : T \to Q$ be defined by $= f\left(\frac{a}{b}\right) = \frac{g(a)}{g(b)}$ ... (A)

By the definition of ring homomorphism

ϕ is a ring homomorphism, it should satisfied the given two conditions.

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(a\ b) = \phi(a) + \phi(b)$

Let $S, t \in T \ \exists\ a, b, c, d \in S$ where $b = d \neq 0$

Such that $S = \dfrac{a}{b}$ and $t = \dfrac{c}{d}$

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

$$= \frac{g(a)}{g(b)} + \frac{g(c)}{g(d)} \text{ from (A)}$$

$$= \frac{g(a)\, g(d) + g(c)\, g(b)}{g(b)\, g(d)}$$

$$= \frac{g(ad + bc)}{g(bd)}$$

$$= f\left(\frac{ad + bc}{bd}\right)$$

$$= f\left(\frac{ad}{bd} + \frac{bc}{bd}\right)$$

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

$\therefore \quad f(S) + f(t) = f(S + t)$

Consider

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

$$= \frac{g(a)}{g(b)} \cdot \frac{g(c)}{g(d)}$$

$$= \frac{g(ac)}{g(bd)}$$

$$= f\left(\frac{ac}{bd}\right)$$

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

$$= f(S\, t)$$

$\therefore$ f(S) f(t) = f(St)

$\therefore$ f is ring homomorphism

Now to prove f is Ring Isomorphism, it is enough to prove f is one - one and f is onto

1. 'f' is one - one

Let f(S) = f(t)

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

$\Rightarrow \frac{g(a)}{g(b)} = \frac{g(c)}{g(d)}$

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

$\Rightarrow$ g(ad) = g(cb)

$\Rightarrow$ ad = bc

$\Rightarrow \frac{a}{b} = \frac{c}{d}$

$\therefore$ f is one - one

2. 'f' is onto

Let $p \in Q$. Then there exist $m, n \in z$, $n \neq 0$ such that $p = \frac{m}{n}$

Since g is a ring homomorphism from S to z

$\exists$ a, b $\in$ S, b $\neq$ 0 $\ni$ g(a) = m, g(b) = n

$\Rightarrow f\left(\frac{a}{b}\right) = \frac{g(a)}{g(b)} = \frac{s}{t}$

$\therefore$ 'f' is onto

$\therefore$ 'f' is ring homomorphism

Then 'f' contains a subfield isomorphic to the rational number.

Q30. Find all the maximal ideals in Z_{12}.

Sol :

Given that, Z_{12} is a ring

Let I be the ideal of Z_{12}

The divisors of 12 are 1, 2, 3, 4, 6 and 12

$\therefore$ The ideals in Z_{12} are

$<1> = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0\} = Z_{12}$

$<2> = \{0, 2, 4, 6, 8, 10\}$

$<3> = \{0, 3, 6, 9\}$

$<4> = \{0, 4, 8\}$

$<6> = \{0, 6\}$

$<12> = \{0\}$

$<1>$ and $<12>$ are not maximals.

$\therefore$ Maximal ideals = $<2>, <3>$

Q31. Let R, S be any two rings and $\phi : R \to S$ is a homomorphism. If R is commutative. Then show that $\phi(R)$ is commutative.

Ans :

Given that, R, S are two rings

$\phi : R \to S$ is a homomorphism

Suppose that, R is commutative ring

Required to prove $\phi(R)$ is commutative ring

Let $\phi(r_1), \phi(r_2) \in \phi(R)$, where $r_1, r_2 \in R$

Consider

$$\phi(r_1)\ \phi(r_2) = \phi(r_1\ r_2)$$
$$= \phi(r_2\ r_1)$$
$$= \phi(r_2)\ \phi(r_1)$$

$\therefore$ $\phi(r_1)\ \phi(r_2) = \phi(r_2)\ \phi(r_1)$

$\therefore$ $\phi(R)$ is commutative ring

Q32. Show that the set $M_2(z)$ of 2 × 2 matrices with integer entries is a non commutative ring with unity.

Ans : **(Jan.-21)**

Given that

$M_2(z)$ is a set of 2 × 2 matrices with integer

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ $\forall$ A, B $\in M_2(z)$

$\Rightarrow$ $A + B = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}$

and

$$A \cdot B = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

From the above we can conclude that closed binary operations $M_2(z)$ is a ring.

Let $0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ be the additive identity

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ be the multiplicative identity

Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in M_2(z)$

$B = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \in M_2(z)$

Consider $AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1+1 & 0+0 \\ 0+1 & 0+0 \end{bmatrix}$

$= \begin{bmatrix} 2 & 0 \\ 1 & 0 \end{bmatrix}$

Consider $BA = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$= \begin{bmatrix} 1+0 & 1+0 \\ 1+0 & 1+0 \end{bmatrix}$

$= \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

$\therefore \quad AB \neq BA$

So, multiplication is not commutative

$\therefore \quad M_2(z)$ is a non commutative ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Q33. Define ring homomorphism show that $\phi : C \to M_2[R]$ given by

$$\phi(a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \ \forall\ a, b \in R, \text{ is an isomorphism of C into } M_2[R].$$

(OR)

Let $S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \Big/ a, b \in R \right\}$ **then show that**

$\phi : C \to S$ **given by,** $\phi : (a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ **is a ring isomorphism.**

Sol : **(May/June-19)**

Given that

$\phi : C \to S$ given by, $\phi : (a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \ \forall\ a, b \in R.$

Let $h_1, h_2 \in C$

$h_1 = a_1 + ib_1, h_2 = a_2 + ib_2$

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

Consider

$h_1 + h_2 = (a_1 + ib_1) + (a_2 + ib_2)$

$\therefore \quad h_1 + h_2 = (a_1 + a_2) + i(b_1 + b_2)$

Consider

$h_1 h_2 = (a_1 + ib_1)(a_2 + ib_2)$

$= a_1 a_2 + i a_1 a_2 + i b_1 a_2 - b_1 b_2$

$\therefore \quad h_1 h_2 = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2)$

$\phi(h_1) = \phi(a_1 + ib_1)$

$$= \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix}$$

$$\phi(h_2) = \phi(a_2 + ib_2) = \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix}$$

$$\phi(h_1) + \phi(h_2) = \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ -b_1 - b_2 & a_1 + a_2 \end{bmatrix} \quad \text{... (1)}$$

$$\phi(h_1 + h_2) = \phi[(a_1 + a_2) + i(b_1 + b_2)] = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ -(b_1 + b_2) & a_1 + a_2 \end{bmatrix} \quad \text{... (2)}$$

From (1) + (2)

$\phi(h_1) + \phi(h_2) = \phi(h_1 + h_2)$

Similarly

$\phi(h_1 \ h_2) = \phi(h_1)\ \phi(h_2)$

$\therefore$ ϕ is ring homomorphism from C to S

$\therefore$ $\phi(h_1) = \phi(h_2)$

$$\Rightarrow \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix}$$

Compare the matrices

$\Rightarrow a_1 = a_2 \qquad b_1 = b_2$

$\Rightarrow a_1 + ib_1 = a_2 + ib_2$

$\therefore h_1 = h_2$

ϕ is one - one and homomorphism.

$\therefore$ ϕ is not an onto homomorphism

$\therefore$ ϕ is an into isomorphism

Q34. Prove that Z_7, the ring of integers modulo 7 is a field.

Ans : **(Jan.-21)**

Given, $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

with integer modulo 7. Under addition and multiplication.

Z_7 Under addition modulo, By composition table

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Z_7 Under multiplication modulo By composition table.

$\bullet_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

1. here Associative property is satisfied Under $\oplus_7$ and $\otimes_7$
2. Distributive property also holds good.
3. Commutative property also holds good.

   i. e., $0 \in Z$ be the additive identity element

   $1 \in Z$ be the multiplicative identity element.
4. The additive inverse of 0,1, 2, 3, 4, 5, 6 are 0, 6, 5, 4, 3, 2, 1 respectively.
5. The multiplicative inverse of 1, 2, 3, 4, 5, 6 are 1, 4, 5, 2, 3, 6 respectively.

   $\therefore$ Z is commutative

   $\therefore$ Z_7 is the ring of integer modulo 7 is a field.

Short Question and Answers

1. Prove that Z_7, the ring of integers modulo 7 is a field.

Ans :

Given, $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

with integer modulo 7. Under addition and multiplication.

Z_7 Under addition modulo, By composition table

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Z_7 Under multiplication modulo By composition table.

$\bullet_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

1. here Associative property is satisfied Under $\oplus_7$ and $\otimes_7$
2. Distributive property also holds good.
3. Commutative property also holds good.

   i. e., $0 \in Z$ be the additive identity element

   $1 \in Z$ be the multiplicative identity element.
4. The additive inverse of 0,1, 2, 3, 4, 5, 6 are 0, 6, 5, 4, 3, 2, 1 respectively.
5. The multiplicative inverse of 1, 2, 3, 4, 5, 6 are 1, 4, 5, 2, 3, 6 respectively.

$\therefore$ Z is commutative

$\therefore$ Z_7 is the ring of integer modulo 7 is a field.

2. Let ϕ be a ring homomorphism from a ring R to a ring S. Then Ker ϕ = {r $\in$ R / ϕ(r) = 0} is an ideal of R.

Ans :

Given that

ϕ is a ring homomorphism

i.e., $\phi : R \rightarrow S$

Required to show that Ker ϕ is an ideal of R

Let $0 \in R$ and $0' \in S$

Let ϕ be a Kernel of f

$\therefore \quad \phi = \{r \in R : \phi(r) = 0\}$

$0 \in \phi$, Since $f(0) = 0'$

ϕ is non empty

If $a, b \in \phi$ then

$f(a) = 0' = f(b)$

$f(a - b) = f(a + (-b))$

$= f(a) + f(-b)$

$= f(a) - f(b)$

$= 0' - 0' \qquad \because f(a) = 0' = f(b)$

$a - b \in \phi$

If r is any element of R.

$f(ra) = f(r)\, f(a)$

$= f(r)\, 0$

$= 0$

$f(ra) = 0$

$f(ar) = f(a)\, f(b)$

$= 0\, f(r)$

$= 0$

$\therefore \quad f(ra) = 0$ and $f(ar) = 0 \Rightarrow ar \in \phi$ and $ra \in \phi$

Hence $a, b \in \phi, \quad r \in \phi, \quad r \in R$

$\Rightarrow \quad (a - b) \in \phi,\ ar \in \phi,\ ra \in \phi$

$\therefore \quad \phi$ is ideal of R

i.e., Ker ϕ is an ideal of R.

3. Let ϕ be a ring homomorphism from Ring R to ring S. If R is commutative ring prove that ϕ(R) is commutative.

Ans :

Let R and S be a two rings

$\phi : R \to S$

and R is a commutative ring

Let the homomorphic image of R be $\phi(R)$

Let $x, y \in \phi(R)$

$\Rightarrow$ $x, y \in \phi(R) \Rightarrow \exists\ a, b \in R$

$\phi(a) = x, \quad \phi(b) = y$

$\Rightarrow$ $xy = \phi(a)\,\phi(b)$

$= \phi(ab)$

$= \phi(ba)$ $\quad \because$ R is commutative ring

$= \phi(b)\,\phi(a)$

$= yx$

$\therefore$ $xy = yx$

Let $\phi : R \to S$ is a ring homomorphism

Let '1' be the unity element of R

$\Rightarrow$ $\phi(1) \in S$

Let a, be an element of R.

$a \in R$

$a' \in R$

$\Rightarrow$ $a' = \phi(a)$ for some $a \in R$

Consider

$\phi(1)\,a' = \phi(1)\,\phi(a)$

$= \phi(1a)$

$= \phi(a)$

$= a'$

$\phi(1)\,a' = a'$ ... (1)

Consider

$a'\,\phi(1) = \phi(a)\,\phi(1)$

$= \phi(a1)$

$= \phi(a)$

$= a'$

$\therefore$ a' $\phi(1)$ = a' ... (2)

From (1) and (2)

$\phi(1)$ a' = a' $\phi(1)$ = a'

$\therefore$ $\phi(1)$ is a unity element of S

4. Define Ring homomorphism.

Ans :

A ring homomorphism from a ring R to ring S is a mapping from R to S that preserves the two ring operations.

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

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

$\phi(a\ b) = \phi(a) \cdot \phi(b)$

Let R & S be two rings w.r. to the binary operations '+' & '•' defined on them, then ϕ is said to be an isomorphism if ϕ is homomorphism, ϕ is one one & ϕ is onto.

5. Let R be a ring with Unity 1. The mapping ϕ : Z $\to$ R given by n $\to$ n.1 is a ring homomorphism.

Ans :

Let R be a ring with Unity 1

Then mapping $\phi : Z \to R$ be defined by

$\phi(n) = n .1 \quad \forall n \in z$

$\forall$ m, n $\in$ z $\Rightarrow \phi(m) = m . 1$ & $\phi(n) = n . 1$

Now, m + n $\in$ z $\Rightarrow \phi(m + n) = (m + n) . 1$

$= m . 1 + n . 1$

$= \phi(m) + \phi(n)$

and m, n $\in$ z $\Rightarrow \phi(m . n)$

$= (m . n) . 1$

$= (m . 1) (m . 1)$

$\phi(m . n) = \phi(m) + \phi(n)$

$\phi : Z \to R$ is a homomorphim

6. Is the ring 2z is isomorphic to ring 3z.

Ans :

Given,

2z and 3z are rings

Let z = {n / n $\in$ z} then

$2z = \{2n / n \in z\}$

$3z = \{3n / n \in z\}$

ϕ is a mapping from 2z to 3z

i.e., $\phi : 2z \to 3z \ni \phi(2.h) = 3h \quad \forall\ h \in z$

$\forall\ 2a, 2b \in 2z$

Then the ring 2z is isomorphic to ring 3z, if ϕ is isomorphism, ϕ is one one

ϕ is well defined and ϕ is onto

$\phi(2a + 2b) = \phi(2(a + b))$

$= 3(a + b)$

$= 3a + 3b$

$= \phi(2a) + \phi(2b)$

$\therefore \quad \phi(2a + 2b) = \phi(2a) + \phi(2b)$

$\phi(2a \,.\, 2b) = \phi(2\ (2ab))$

$= 3(2ab)$

$\neq \phi(2a)\ \phi(2b)$

$\therefore$ The ring 2z is not isomorphic to the ring 3z.

7. Find all the maximal ideals in Z_{12}.

Ans :

Given that, Z_{12} is a ring

Let I be the ideal of Z_{12}

The divisors of 12 are 1, 2, 3, 4, 6 and 12

$\therefore$ The ideals in Z_{12} are

$<1> = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0\} = Z_{12}$

$<2> = \{0, 2, 4, 6, 8, 10\}$

$<3> = \{0, 3, 6, 9\}$

$<4> = \{0, 4, 8\}$

$<6> = \{0, 6\}$

$<12> = \{0\}$

$<1>$ and $<12>$ are not maximals.

$\therefore$ Maximal ideals = $<2>, <3>$

8. If R is a Unity and 'U' is an idel of R. Where $1 \in U$. Then prove that U = R.

Ans :

Given that

'R' is a ring with Unity

U is an ideal of R

$1 \in U$

$\therefore$ U is an ideal of R

By definition $U \subset R$ ..... (1)

Required to prove $R \subset U$

$\because$ U is an ideal of R

We have by definition

$\forall\ r \in R,\ 1 \in U \Rightarrow r.1\ \&\ 1.r \in U$

$\Rightarrow r \in U$

$\Rightarrow R \subset U$ ..... (2)

From equation (1) and (2)

We can conclude that U = R

9. Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S. Then for any $r \in R$ and any position integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(n))^n$.

Ans :

Let R and S are two rings

$\phi : R \to S$ be a ring homomorphism for any $r \in R$

and any positive integer $n \Rightarrow n.r \in z$

Consider

$\phi(n.r) = \phi(r + r ..... + r)$ n times

$= \phi(r) + \phi(r) + ... + \phi(r)$

$\phi(nr) = n.\phi(r)$

$\phi(r^n) = \phi(r.r ..... r)$ (n times)

$= \phi(r)\ \phi(r) ..... \phi(r)$

$\therefore\ \phi(r^n) = [\phi(r)]^n$

10. Let R, S be any two rings and $\phi : R \to S$ is a homomorphism. If R is commutative. Then show that $\phi(R)$ is commutative.

Ans :

Given that, R, S are two rings

$\phi : R \to S$ is a homomorphism

Suppose that, R is commutative ring

Required to prove $\phi(R)$ is commutative ring

Let $\phi(r_1), \phi(r_2) \in \phi(R)$, where $r_1, r_2 \in R$

Consider

$$\phi(r_1)\ \phi(r_2) = \phi(r_1\ r_2)$$

$$= \phi(r_2\ r_1)$$

$$= \phi(r_2)\ \phi(r_1)$$

$\therefore \quad \phi(r_1)\ \phi(r_2) = \phi(r_2)\ \phi(r_1)$

$\therefore \quad \phi(R)$ is commutative ring

Choose the Correct Answers

1. $f(a + b)$ = ________. [b]

(a) f(a) – f (b) (b) f(a) + f(b)

(c) $\frac{f(a)}{f(b)}$ (d) none

2. $f(-a)$ = ________. [b]

(a) $f(-a)$ (b) $-f(a)$

(c) f(a) (d) $\frac{1}{f(a)}$

3. Kernel f = [c]

(a) $f(x) = 0$ (b) $f(x) = x$

(c) $f(x) = 0'$ (d) $f(x) = -x$

4. Every homomorphic image of a commutative ring is ________. [d]

(a) Closed (b) Open

(c) Bounded (d) Commutative

5. $\phi(A)$ = ________. [a]

(a) $\phi(a)$ (b) $\phi(-a)$

(c) $-\phi(a)$ (d) 0

6. If A is an ideal and ϕ is onto 'S'. Then $\phi(A)$ = ________. [c]

(a) field (b) ring

(c) ideal (d) 0

7. $T = ab^{-1}$, $a, b \in S$, is ________. [c]

(a) $b = 0$ (b) $b = -1$

(c) $b \neq 0$ (d) $b = 1$

8. If ϕ is homomorphism $\phi(x) = x$, where a^2 = ________. [c]

(a) 0 (b) 1

(c) a (d) –a

9. 176, 825, is divisible by ________. [a]

(a) 9 (b) 2

(c) 11 (d) 5

10. Ring isomorphism z_2 to a subring z_{2n} iff n is ________. [b]

(a) prime (b) odd

(c) even (d) (a) and (b)

Fill in the Blanks

1. Degree $f_1(x) < p$ degree $f(x)$ = ________.
2. f(a + b) = ________.
3. f(ab) = ________.
4. If f is homomorphism it satisfies ________.
5. f is automorphism if f is ________.
6. f(m + n) = ________.
7. f(–a) = ________.
8. f(0) = ________.
9. The homomorphic image of a ring R is ________.
10. Every homomorphic image of a ring is ________.
11. z_7 = ________.

Answers

1. $f_1(x) = 0$
2. f(a) + f(b)
3. ∴ f(a) . f(b)
4. (i) f(a + b) = f(a) + f(b)

   (ii) f(ab) = f(a) . f(b)
5. One – one and onto
6. f(m) + f(n)
7. –f(a)
8. 0'
9. Subring of R
10. ∴ Ring R
11. {0, 1, 2, 3, 4, 5, 6}

FACULTY OF SCIENCE

B.Sc. IV-Semester(CBCS) Examination

January - 2021

Subject: Mathematics

Paper - IV : ALGEBRA

Time : 2 Hours] **[Max. Marks : 80**

SECTION - A (4 × 5 = 20 Marks)

[Short Answer Type]

Note : Answer any **FOUR** questions.

ANSWERS

1. Let G be a group and let "a" be an element of order n in G. If $a^k = e$ then prove that n divides K. **(Unit-I, SQA-1)**
2. Find all subgroups of Z_{30}. **(Unit-I, SQA-2)**
3. Suppose $\phi : G \to \bar{G}$ is an isomorphism from a group G onto group $\bar{G}$. If K is a subgroup of G then prove that $\phi(K) = (\phi(R) \mid R \in K)$ is a subgroup of $\bar{G}$. **(Unit-II, SQA-2)**
4. Prove that the set of all inner automorphisms of a group G is a group under composition of functions. **(Unit-II, SQA-1)**
5. Prove that Z_7, the ring of integers modulo 7 is a field. **(Unit-IV, SQA-1)**
6. Show that the characteristic of an integral domain is zero or a prime. **(Unit-III, SQA-2)**
7. Let ϕ be a ring homomorphism from a ring R to a ring S. If R is commutative ring, prove that $\phi(R)$ is commutative. **(Unit-IV, SQA-3)**
8. In the ring Z_5, find the quotient and remainder upon dividing $f(x) = 3x^4 + x^3 + 2x^2 + 1$ by $g(x) = x^2 + 4x + 2$ where $f(x), g(x) \in Z_5[x]$. **(Out of Syllabus)**

SECTION - B (3 × 20 = 60 Marks)

[Essay Answer Type]

Note : Answer any **THREE** questions.

9. State and prove fundamental theorem of cyclic groups. **(Unit-I, Q.No.43)**
10. Let G be a group and aeG such that $|a| = n$. If K is a positive integer then prove that $<a^k> = <a^{gcd(n,k)}$ and $|a^k| = \frac{n}{gcd(n,k)}$. **(Unit-I, Q.No.39)**
11. State and prove Lagrange's theorem for groups. **(Unit-II, Q.No.54)**
12. Prove that a group up of prime order is cyclic. **(Unit-II, Q.No.57)**

13. Show that the set $M_2(Z)$ of 2 × 2 matrices with integer entries is a non-commutative ring with unity. **(Unit-IV, Q.No.32)**
14. Show that the set of Gaussian integers $Z[i] = \{a + ib \mid a, b \in Z\}$ is a sub ring of the ring of complex numbers. **(Unit-III, Q.No.51)**
15. Prove that ring with unity contains Z_n or Z. **(Unit-IV, Q.No.27)**
16. If F is a field of characteristic zero then prove that F contains a subfield isomorphic to the rational numbers. **(Unit-IV, Q.No.29)**

FACULTY OF SCIENCE

B.Sc. IV-Semester(CBCS) Examination

May / June - 2019

Subject: Mathematics

Paper - IV : ALGEBRA

Time : 3 Hours] **[Max. Marks : 80**

SECTION - A (5 × 4 = 20 Marks)

[Short Answer Type]

Note : Answer any **FIVE** of the following questions.

ANSWERS

1. Prove that the set

   $GL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Big/ a,b,c,d \in R, ad - bc \neq 0 \right\}$ is a non abelian group with

   respect to matrix multiplication. **(Unit-I, SQA-4)**

2. Let G be a group and H be a nonempty subset of G. If $ab \in H \ \forall a,b \in H$ and $a^{-1} \in H \ \forall a \in H$ then prove that H is a subgroup of G. **(Unit-I, SQA-3)**

3. State and prove Lagrange's theorem. **(Unit-II, SQA-3)**

4. Define Automorphism Homomorphism Image and Isomorphic Image. **(Unit-III, SQA-6)**

5. Prove that the characteristic of an integral domain in either zero or prime. **(Unit-III, SQA-1)**

6. Let R[x] denotes the set of all polynomials with real coefficients and let A denotes the subset of the all polynomials with constant term 0 then prove that A is an ideal of R[x] and $A = < x >$. **(Out of Syllabus)**

7. Let ϕ be a ring homomorphism from a ring R to a ring S then Ker $\phi = \{r \in R \,]\, \phi(r) = 0\}$ is an ideal of R. **(Unit-IV, SQA-2)**

8. If D is an integral domain then prove that D[x] is an integral domain. **(Unit-III, SQA-2)**

SECTION - B (4 × 15 = 60 Marks)

[Essay Answer Type]

Note : Answer **ALL** from the questions.

9. (a) Every subgroup of a cyclic group is cyclic more over if $|< a >| = n$ then the order of any subgroup of $< a >$ is a divisor of n and for each positive divisor k of n, the group $< a >$ has exactly one subgroup of order k namely $< a >$. **(Unit-I, Q.No.43)**

OR

(b) Define Alternating group of degree n. Also prove that A_n has order $\frac{n!}{2}$ if $n > 1$. **(Unit-II, Q.No.13)**

10. (a) Prove that the group of rotations of a cube is isomorphic to S_4. **(Unit-III, Q.No.67)**

OR

(b) Let G be a group and let Z(G) be the centre of G. If $\frac{G}{Z(G)}$ is cyclic then G is abelian. **(Unit-III, Q.No.49)**

11. (a) Prove that $Z_3[i] = \{a + ib \mid a,b \in Z_3\}$ is a field of order 9. **(Unit-III, Q.No.50)**

OR

(b) Let R be a commutative ring with unity and let A be an ideal of R $\frac{R}{A}$ then is an integral domain if and only if A is prime ideal. **(Unit-III, Q.No.52)**

12. (a) If R is a ring with unity and the characteristic of R is $n > 0$ then prove that R contains a subring isomorphic to Z_n. If the characteristic of R is 0 then R contains a subring isomorphic to Z. **(Unit-IV, Q.No.27)**

OR

(b) Let $S = \left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \Big/ a, b \in R\right\}$ then show that $\phi : C \to S$ given by $\phi(a + i(b)) =$ is a ring isomorphism. **(Unit-IV, Q.No.33)**

FACULTY OF SCIENCE

B.Sc. IV-Semester (CBCS) Examination

Model Paper - I

Paper - IV : ALGEBRA

Subject: Mathematics

Time : 3 Hours] [Max. Marks : 80

PART - A (8 × 4 = 32 M)

[Short Answer Type]

Note : Answer any Eight of the following questions

1. Let G be a group and let a be an element of order n in G, if $a^k = e$ then n divides K. **(Unit-I, SQA-1)**
2. Let G be a group and let H be a non empty subset of G. If ab is in H whenever a and b are in H and a^{-1} is in H whenever a is in H then H is a subgroup of G. **(Unit-I, SQA-3)**
3. Define binary operation with examples. **(Unit-I, SQA-5)**
4. A group of order 75 can have at most one subgroup of order 25. **(Unit-II, SQA-9)**
5. Compute Aut (Z_{10}). **(Unit-II, SQA-7)**
6. Write notation for cycle. **(Unit-II, SQA-5)**
7. Define Cancellation Law **(Unit-III, SQA-9)**
8. State the examples of Rings. **(Unit-III, SQA-7)**
9. List the applications of factor groups. **(Unit-III, SQA-5)**
10. Prove that Z_7, the ring of integers modulo 7 is a field. **(Unit-IV, SQA-1)**
11. Let ϕ be a ring homomorphism from Ring R to ring S. If R is commutative ring prove that $\phi(R)$ is commutative. **(Unit-IV, SQA-3)**
12. Let R be a ring with Unity 1. The mapping $\phi : Z \to R$ given by $n \to n.1$ is a ring homomorphism. **(Unit-IV, SQA-5)**

SECTION - B (4 × 12 = 48 M)

[Essay Answer Type]

Note : Answer all the following questions

13. (a) Prove that the set of R* of non zero real numbers is an abelian group under ordinary multiplication. **(Unit-I, Q.No. 7)**

(OR)

(b) State and prove fundamental theorem of cyclic group. **(Unit-I, Q.No. 43)**

14. (a) Prove that for $n > 1$, A_n has order $\frac{n!}{2}$. **(Unit-II, Q.No. 13)**

(OR)

(b) State and prove for every integer 'a' and every prime 'p', a^p mod p = a mod p. **(Unit-II, Q.No. 59)**

15. (a) Prove that a subgroup N of a group G is a normal subgroup of G iff $g N g^{-1} = N \ \forall \ g \in G$. **(Unit-III, Q.No. 5)**

(OR)

(b) Fundamental theorem of homomorpic in group. **(Unit-III, Q.No. 20)**

16. (a) Let R be a commutative ring with Unity and let A be an ideal of R. Then $\frac{R}{A}$ is an integral domain if and only if A is Prime **(Unit-IV, Q.No. 8)**

(OR)

(b) Let R be a commutative Ring of characteristics 2, Then prove that the mapping $a \to a^2$ is a ring homomorphism from R to R. **(Unit-IV, Q.No. 22)**

FACULTY OF SCIENCE

B.Sc. IV-Semester (CBCS) Examination

Model Paper - II

Paper - IV : ALGEBRA

Subject: Mathematics

Time : 3 Hours] [Max. Marks : 80

PART- A (8 × 4 = 32 M)

[Short Answer Type]

Note : Answer any Eight of the following questions

1. Define Cayley's Table **(Unit-I, SQA-10)**
2. Find all subgroups of Z_{30} **(Unit-I, SQA-2)**
3. Write some examples of groups. **(Unit-I, SQA-6)**
4. The set of Automorphism of a group and the set of inner Automorphism of group are both group under the operation of function composition. **(Unit-II, SQA-1)**
5. The order of a subgroup of a finite group divides the order of the group. **(Unit-II, SQA-3)**
6. Define Permutation group. **(Unit-II, SQA-4)**
7. The characteristic of an integral domain is the 0 or prime. **(Unit-III, SQA-1)**
8. Define Normal subgroup with example. **(Unit-III, SQA-3)**
9. Define factor group. **(Unit-III, SQA-4)**
10. Let R, S be any two rings and $\phi : R \to S$ is a homomorphism. If R is commutative. Then show that $\phi(R)$ is commutative. **(Unit-IV, SQA-10)**
11. Let ϕ be a ring homomorphism from a ring R to a ring S. Then Ker $\phi = \{r \in R / \phi(r) = 0\}$ is an ideal of R. **(Unit-IV, SQA-2)**
12. Is the ring 2z is isomorphic to ring 3z. **(Unit-IV, SQA-6)**

SECTION - B (4 × 12 = 48 M)

[Essay Answer Type]

Note : Answer all the following questions

13. (a) If G is a cyclic group generated by an element 'a' of order 'n' and if $|<a>| = n$. Then prove that the order of the subgroup of group generated by a is a divisor of 'n'. **(Unit-I, Q.No. 44)**

(OR)

(b) Show that {1, 2, 3} under multiplication modulo 4 is not a group but that {1, 2, 3, 4} under multiplication modulo 5 is a group. **(Unit-I, Q.No. 12)**

14. (a) Let H be a subgroup of G & $a, b \in G$ **(Unit-II, Q.No. 50)**

Then $|aH| = |bH|$

(OR)

(b) Suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$. **(Unit-II, Q.No. 31)**

Then ϕ^{-1} is an isomorphism from $\bar{G}$ onto G.

15. (a) If G is a group and N is a normal subgroup of G. Then prove **(Unit-III, Q.No. 8)**

that $\frac{G}{N} = \{Nx / x \in G\}$ forms a group w.r.to coset multiplication

as the binary operation

(OR)

(b) A nonempty subset S of a ring R. is a subring if S is closed subtraction and multiplication **(Unit-III, Q.No. 30)**

i.e., (i) $a - b \in S$

(ii) $ab \in S$ when $a, b \in S$

16. (a) Let ϕ be a ring homomarphism from a ring R to a ring S. Let A be a subring of R and Let B be an ideal of S If ϕ is an isomurphism If and only if ϕ is onto and Ker $\phi = \{r \in R / \phi(r) = 0\} = \{0\}$ **(Unit-IV, Q.No. 16)**

(OR)

(b) Let ϕ be a ring homomorphism from Ring R to ring S. If R is commutative ring prove that $\phi(R)$ is commutative. **(Unit-IV, Q.No. 26)**

FACULTY OF SCIENCE

B.Sc. IV-Semester (CBCS) Examination

Model Paper - III

Paper - IV : ALGEBRA

Subject: Mathematics

Time : 3 Hours] [Max. Marks : 80

PART- A (8 × 4 = 32 M)

[Short Answer Type]

Note : Answer any Eight of the following questions

1. Prove that the set $GL(2, R) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle/ a, b, c, d \in R, ad - bc \neq 0\right\}$ **(Unit-I, SQA-4)**

   is a non abelian group with respect to matrix multiplication.

2. What are the Elementary Properties of Groups? **(Unit-I, SQA-7)**
3. Define multiplication modulo. **(Unit-I, SQA-9)**
4. Let ϕ be an isomorphism from G to $\bar{G}$. If K is a subgroup of G. Then **(Unit-II, SQA-2)**

   $\phi(k) = \{\phi(k) / k \in K\}$ is a subgroup of $\bar{G}$.

5. Let $H = \{0, 3, 6\}$ is Z_9 under addition. Then find the left cosets of H is Z_9. **(Unit-II, SQA-8)**
6. Define Isomorphism. **(Unit-II, SQA-6)**
7. If D is an integral domain, Then prove that D[x] is an integral domain. **(Unit-III, SQA-2)**
8. Define integral domain with example. **(Unit-III, SQA-8)**
9. Define Automorphism Homomorphism Image and Isomorphic Image. **(Unit-III, SQA-6)**
10. Define Ring homomorphism. **(Unit-IV, SQA-4)**
11. Find all the maximal ideals in Z_{12}. **(Unit-IV, SQA-7)**
12. Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S. Then for any $r \in R$ and any position integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(n))^n$. **(Unit-IV, SQA-9)**

SECTION - B (4 × 12 = 48 M)

[Essay Answer Type]

Note : Answer all the following questions

13. (a) Let G be a group, and let a belong to G.

    (i) if a has infinite order, then $a^i = a^j$ if and only if $i = j$ **(Unit-I, Q.No. 37)**

    (ii) If a has finite order, say n, then $\langle a \rangle = \{e, a, a^2 \ldots a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$

(OR)

(b) Let G be the group of polynomial under addition with coefficients from Z_{10}. **(Unit-I, Q.No. 48)**

Find the orders of

$f(x) = 7x^2 + 5x + 4$

$g(x) = 4x^2 + 8x + 6$

and $f(x) + g(x)$

14. (a) The set of Automorphism of a group and the set of inner Automorphism of group are both group under the operation of function composition. **(Unit-II, Q.No. 39)**

(OR)

(b) Prove that a group of prime order is cyclic. **(Unit-II, Q.No. 57)**

15. (a) The characteristic of an integral domain is the 0 or prime. **(Unit-III, Q.No. 46)**

(OR)

(b) Prove that $Z_3 [i] = \{a + ib / a,b \in Z_3\}$ is a field of order 9? **(Unit-III, Q.No. 50)**

16. (a) Prove that ring with unity contains z_n or z. **(Unit-IV, Q.No. 27)**

(OR)

(b) Define ring homomorphism show that $\phi : C \rightarrow M_2 [R]$ given by **(Unit-IV, Q.No. 33)**

$\phi (a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ $\forall$ a, b $\in$ R, is an isomorphism of C into $M_2 [R]$.