PITHAPUR RAJAH'S GOVERNMENT COLLEGE(A)

KAKINADA

GROUP THEORY-SEM- III

By

G. PRASADA RAO
Lecturer in Mathematics

GROUP THEORY

UNIT 1: GROUPS

Binary Operation – Algebraic structure – semi group-monoid – Group definition and elementary properties Finite and Infinite groups – examples – order of a group. Composition tables with examples.

UNIT 2: SUBGROUPS

Complex Definition – Multiplication of two complexes Inverse of a complex-Subgroup definition – examples-criterion for a complex to be subgroups.

Criterion for the product of two subgroups to be a subgroup-union and Intersection of subgroups.

Co-sets and Lagrange's Theorem:

Co-sets Definition – properties of Co-sets–Index of subgroups of a finite groups–Lagrange's Theorem.

UNIT 3: NORMAL SUBGROUPS:

Definition of normal subgroup – proper and improper normal subgroup–Hamilton group – criterion for a subgroup to be a normal subgroup – intersection of two normal subgroups – Sub group of index 2 is a normal sub group – simple group – quotient group – criteria for the existence of a quotient group.

UNIT4: HOMOMORPHISM

Definition of homomorphism – Image of homomorphism elementary properties of homomorphism – Isomorphism – auto morphism definitions and elementary properties–kernel of a homomorphism – fundamental theorem on Homomorphism and applications.

UNIT 5: PERMUTATIONS AND CYCLIC GROUPS

Definition of permutation – permutation multiplication – Inverse of a permutation – cyclic permutations – transposition – even and odd permutations – Cayley's theorem.

Definition of cyclic group – elementary properties – classification of cyclic groups.

Activities

Seminar/ Quiz/ Assignments/ Applications of Group Theory to Real life Problem /Problem Solving Sessions

Text Book

Modern Algebra by A.R.Vasishtha and A.K.Vasishtha, KrishnaPrakashanMedia Pvt. Ltd., Meerut.

Reference Books

1. Abstract Algebra by J.B. Fraleigh, Published by Narosa publishing house.
2. Modern Algebra by M.L. Khanna, Jai Prakash and Co. Printing Press, Meerut
3. Rings and Linear Algebra by Pundir&Pundir, published by PragathiPrakashan

UNIT-1: GROUPS

INTRODUCTION: A group is commonly studied as an abstraction of the number systems and the system of permutations on set (i.e. the study of algebraic structures is called group)

$\mathbb{N} = The\ set\ of\ natural\ numbers = \{1,2,3, \dots \dots \dots\}$

$\mathbb{Z} = The\ set\ of\ integers = \{\dots \dots . . -3,-2,-1,0,1,2,3, \dots \dots \dots\}$

$\mathbb{Z}^{+} = The\ set\ of\ positive\ integers = \{1,2,3, \dots \dots \dots . .\}$

$\mathbb{Z}^{-} = The\ set\ of\ negative\ integers = \{\dots \dots . . -3,-2,-1\}$

$\mathbb{Q} = The\ set\ of\ rational\ numbers = \{\frac{p}{q}/p, q \in \mathbb{Z}\ and\ q \neq 0\}$

$= \{\dots -\frac{1}{2}, \frac{3}{2}, -\frac{2}{5}, \frac{3}{7} \dots . .\}$

$\mathbb{Q}^{+} = The\ set\ of\ positive\ rational\ numbers = \{\frac{1}{2}, \frac{3}{5} \dots \dots\}$

$\mathbb{R} - \mathbb{Q} = The\ set\ of\ irrational\ number = \{\sqrt{2}, \sqrt{3}, \sqrt{5}, \pi\ e, \dots \dots \dots . .\}$

$\mathbb{R} = The\ set\ of\ real\ numbers = \mathbb{N} \cup \mathbb{Z} \cup \mathbb{Q} \cup \mathbb{R} - \mathbb{Q}$

$\mathbb{R}^{+} = The\ set\ of\ positive\ real\ numbers$

$\mathbb{Q}_0 = \mathbb{Q} - \{0\} = The\ set\ of\ non - zero\ rational\ numbers$

$\mathbb{R}_0 = \mathbb{R} - \{0\} = The\ set\ of\ non - zero\ real\ numbers$

$\mathbb{C} = \{x + iy/, y \in \mathbb{R}\ and\ i^2 = -1\}$

Non-empty set: A set contains at least one element is called non-empty set.

Ex: $A = \{1,-1,2,3,5,8,\}\ is\ a\ finite\ set.$

Prime number: A number P (>1) which divides 1 and itself is called as a prime number.

Ex: Prime numbers are 2, 3, 5, 7 ……..

Composite number: A number P (>1) which is not a prime number is called as a composite number.

Ex: Composite numbers are 4, 6, 8, 9……

Note: 1 is neither a prime number nor a composite number

2 is the only even prime

Binary operation (closure property): A non-empty set G with a operation $(*: G \times G \to G)$ is said to be a binary operation if $a * b \in G \quad \forall a, b \in G$

Ex: $(i)(\mathbb{N}, +)$: $1 + 2 = 3 \in \mathbb{N}; 2 + 4 \in \mathbb{N}$

$Let\ a, b \in \mathbb{N},\ \ a + b \in \mathbb{N} \Longrightarrow' +' is\ a\ binary\ operation\ on\ \mathbb{N}.$

$(ii)(\mathbb{N}, -)\ is\ not\ a\ binary\ opertion\ because\ Let\ a = 1, b = 2\ now\ a - b = -1 \notin \mathbb{N}$

$(iii)(\mathbb{N}, \times)\ is\ \ a\ binary\ opertion.\ Let\ a, b \in\ \mathbb{N} \Longrightarrow ab \in \mathbb{N}$

$(iv)(\mathbb{N}, \div)\ is\ not\ a\ binary\ opertion\ because\ Let\ a = 1,\ = 2\ now\ a \div b = {}_{2} \notin \mathbb{N}$

$Hence\ (\mathbb{N}, +), (\mathbb{N}, \times)\ are\ binary\ operations\ but\ (\mathbb{N}, -), (\mathbb{N}, \div)\ \ are\ not\ binary\ operations.$

$(\mathbb{Z}, +), (\mathbb{Z}, -), (\mathbb{Z}, \times)\ are\ binary\ operations\ but\ , (\mathbb{Z}, \div)\ \ is\ not\ binary\ operation$

$(\mathbb{Q}, +), (\mathbb{Q}, -), (\mathbb{Q}, \times)\ , (\mathbb{Q}, \div)\ are\ binary\ operations$

Algebraic system: A non-empty set G is said to be algebraic system if it contains one or more binary operations.

Ex: $(i)\ (\mathbb{N}, +), (\mathbb{Z}, -), (\mathbb{Q}, +), (\mathbb{R}, +) \qquad (ii)\ \ (\mathbb{N}, +, \times), (\mathbb{Z}, +, -), (\mathbb{Q}, +, -, \times), (\mathbb{R}, +, -, \times, \div)$

Groupoid: A non-empty set G is said to be groupoid if it contains a binary operation.

Remark: 1.Every groupoid is always an algebraic system but an algebraic system need not be groupoid.

Associative property: A non-empty set G with a binary operation $*$ is said to be associative if $(a * b) * c = a * (b * c)\ \ \forall a, , c \in G$

Ex:

$(i)\ (\mathbb{N}, +), (\mathbb{N}, \times)\ are\ all\ satisfies\ associative\ property.\ but (\mathbb{Z}, -)\ is\ not\ an\ associative$

$(ii) The\ set\ of\ all\ matrices\ is\ an\ associative\ under\ addition\ and\ multiplication.$

$i.e. (i)\ A + (B + C) = (A + B) + C (ii)\ A(BC) = (AB)C \quad \forall A, B, C$

$(iii)\ The\ set\ of\ all\ complex\ numbers\ is\ an\ associative\ under\ addition\ and\ multiplication.$

$i.e. (i)\ z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3 (ii)\ z_1(z_2 z_3) = (z_1 z_2) z_3 \quad \forall z_1, z_2, z_3 \in \mathbb{C}$

3. Composition of mapping is an associative $i.e. (f \circ g) \circ h = f \circ (g \circ h)\ \forall f, g, h$

4. $(\mathbb{Q}, -)$ is not associative. Since 3, -4, 6, $\in \mathbb{Q} \Rightarrow 3 - (-4\ -6) = (3 - (-4)) - 6 \Rightarrow 13 \neq 1.$

Semi group: A non – empty set G with a binary operation $*$ is said to be a semi group if it satisfies associative property.

Ex: 1. $(\mathbb{N},+),(\mathbb{N},\times)$ are all semi groups.

2. $(\mathbb{Q},-)$ is not semi group

Identity property: Let G be non –empty set and $*$ be a binary operation on G then there exist an element $e \in G$ such that $a * e = a = e * a \quad \forall a \in G$ Here 'e' is called the identity element

Remark: (i) If $* = +$ (Addition) then '0' is the additive identity. i.e. $a + 0 = 0 + a = a \; \forall \; a \in G$

(ii) If $* = \times$ (Multiplication) then '1 'is the multiplicative identity i.e. $a.1 = 1.a = a \; \forall \; a \in G$

Monoid: A non-empty set G is said to be Monoid if (i) $*$ is a binary operation (ii) Associative property (iii) Identity property

Ex: $(i)(\mathbb{N},+),(\mathbb{Z},-)$ are not a Monoids

$(ii)(\mathbb{N},\times),(\mathbb{Z},+),(\mathbb{Z},\times),(\mathbb{Q},+),(\mathbb{Q},\times),(\mathbb{Q},\div),(\mathbb{R},+),(\mathbb{R},\times),(\mathbb{R},\div)$ are all a Monoids

Inverse property: Let G be non – empty set and $*$ be a binary operation on G then for each $a \in G$ so there exist $b \in G$ such that $a * b = e = b * a$ where e is identity element.

Remark:

1. $-a$ is the additive inverse of a. since $a + (-a) = 0 = (-a) + a$.

2. $\frac{1}{a}$ is the multiplicative inverse of a for $a \neq o$ since $a\left(\frac{1}{a}\right) = 1 = \left(\frac{1}{a}\right)a$.

3. $a * b = ab$, $\forall$ a, b$\in$ R, Identity = K, Inverse = $\frac{1}{a}$, $\forall$ a $\in$R, a$\neq$0

GROUP: A non – empty set G with a operation $*$ is said to be a group if it satisfies

1. Closure property: $a * b \in G \quad \forall a, b \in G$

2. Associative property: $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$

3. Identity property: $so \; \exists \; e \in G \ni a * e = a = e * a \quad \forall a \in G \; here \; e \; is \; called \; the \; idntity$

4. Inverse property: $For \; each \; a \in G \; so \; \exists \; b \in G \; such \; that \; a * b = e = b * a$

$here \; b \; is \; the \; inverse \; of \; a$

Ex:(i) $(\mathbb{N},+)$ $is \; not \; a \; group \; as \; 0 \notin \mathbb{N}$

$(ii)(\mathbb{N},\times)$ *is not a group as inverse property is failure* $(\because\ 2 \in \mathbb{N}, 2\,(\frac{1}{2}) = 1\ but \frac{1}{2} \notin \mathbb{N})$

$(iii)(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ *are all groups but* $(\mathbb{Z},\times)$ *is not a group as inverse failure.*

$(iv)(\mathbb{Q},\times)$, $(\mathbb{R},\times)$ *are not groups as* 0 *does not has inverse.*

(v) ($\mathbb{Q}_0,\times),(\mathbb{R}_0,\times)$ *are all groups*

Note: $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),$ ($\mathbb{Q}_0,\times),(\mathbb{R}_0,\times)$ *are all groups*

Commutative property: A non – empty set G with a operation $*$ is said to be commutative if

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

Abelian group: A group G is said to be an abelian group if it satisfies the commutative property.

Ex: $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),$ ($\mathbb{Q}_0,\times),(\mathbb{R}_0,\times)$ *are all abelian groups*

Finite group: A group G is said to be finite group if number of elements in group is finite

Ex: $(i)\ G = \{1,-1\}, G = \{1,,^2\}, G = \{1,-1,i,-i\}$ *are all finite groups under multiplication.*

Infinite group: A group G is said to be infinite group if number of elements in group is infinite

Ex: $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),$ ($\mathbb{Q}_0,\times),(\mathbb{R}_0,\times)$ *are all infinite groups*

Order of group: Number of elements in a group is called order of group. And it is denoted by o (G) or |G|

Ex: $(i)\ G = \{1,-1\}$ *is a group under multiplication so* $(G) = 2$

Problems:

1. Prove that the set of positive rational numbers form an abelian group under $*$ is defined by a$*$ $b = {}^{ab}$

Sol: G = The set of all positive rational numbers = $\mathbb{Q}^+$

and $*$ is defined by a$*$ $b = {}^{ab}$ $\forall\ a, b \in \mathbb{Q}^+$

To prove that $(G,*)$ is an abelian group

(i) Closure property: $Let\ a, b \in \mathbb{Q}^+ \Rightarrow ab \in \mathbb{Q}^+ \Rightarrow \frac{ab}{3} \in \mathbb{Q}^+ \Rightarrow$ a $* b \in \mathbb{Q}^+$

$\therefore$ a $* b \in G \quad \forall a, b \in G$

(ii) Associative property: $Let\ a,,c \in \mathbb{Q}^+$

$$(a*b)*c = (\frac{ab}{3})*c = \frac{(\frac{ab}{3})c}{3} = \frac{abc}{9} \quad and \quad a*(b*c) = a*(\frac{bc}{3}) = \frac{a(\frac{bc}{3})}{3} = \frac{abc}{9}$$

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

(iii) Existence of identity: $Let\ a \in G\ and\ 'e'\ be\ the\ identity\ element$

$Now\ a*e = a \Longrightarrow {}^{ae} = a \Longrightarrow e = 3$

$Now\ a*e = a*3 = a.{}^{3} = a$ similarly we can prove $e*a = a \Longrightarrow {}^{ea} = a \Longrightarrow e = 3$

$\therefore The\ identity\ element\ is\ 3$

(iv) Existence of inverse: $Let\ a \in G\ and\ 'b'\ be\ the\ inverse\ of\ a$

$Now\ a*b = e \Longrightarrow {}^{ab} = 3 \Longrightarrow b = {}^{9}$

$The\ inverse\ of\ a\ is\ {}_{a}\ \ so\ every\ element\ has\ invertiable$

(v) Commutative property: $Let\ a,\ \in G\ Now\ a*b = {}^{ab} = {}^{ba} = b*a$

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

$\therefore (G,*)\ is\ an\ abelian\ group.$

2. Prove that the set $\mathbb{Z}$of all integers form an abelian group w.r.t the operation defined by $a*b = a+b+2\ \forall\ a,\ \in \mathbb{Z}$

Sol: G = The set of all integers = $\mathbb{Z}$

$and\ *$ is defined by a$*\ b = a+b+2\ \forall\ a,\ \in \mathbb{Z}$

To prove that $(G,*)$is an abelian group

(i) Closure property: $Let\ a,b \in \mathbb{Z} \Longrightarrow a+b \in \mathbb{Z} \Longrightarrow a+b+2 \in \mathbb{Z} \Longrightarrow$ a$*\ b \in \mathbb{Z}$

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

(ii) Associative property: $Let\ a,,c \in \mathbb{Z}$

$(a*b)*c = (a+b+2)*c = (a+b+2)+c+2 = a+b+c+4$

$and\ \ a*(b*c) = a*(b+c+2) = a+(b+c+2)+2 = a+b+c+4$

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

(iii) Existence of identity: *Let* $a \in G$ *and* $'$e$'$ *be the identity element*

$Now\ a * e = a \Longrightarrow a + e + 2 = a \Longrightarrow e = -2$

$Now\ a * e = a * (-2) = a + (-2) + 2 = a$ similarly we can prove

$e * a = a \Longrightarrow e + a + 2 = a \Longrightarrow e = -2$

$\therefore$ *The identity element is* -2

(iv) Existence of inverse: *Let* $a \in G$ *and* $'$ b'*be the inverse of* a

$Now\ a * b = e \Longrightarrow a + b + 2 = -2 \Longrightarrow b = -4 - a$

The inverse of a *is* $-4 - a$ *so every element has invertiable*

(v) Commutative property: *Let* $a, b \in G$ $Now\ a * b = a + b + 2 = b + a + 2 = b * a$

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

$\therefore (G,*)$ *is an abelian group.*

3. Prove that the set $\mathbb{Z}$of all integers form an abelian group w.r.t the operation defined by $a * b = a + b + 1\ \forall\ a, \in \mathbb{Z}$

Sol: G = The set of all integers = $\mathbb{Z}$

and $*$ is defined by a$* b = a + b + 1\ \forall\ a, \in \mathbb{Z}$

To prove that $(G,*)$is an abelian group

(i) Closure property: *Let* $a, b \in \mathbb{Z} \Longrightarrow a + b \in \mathbb{Z} \Longrightarrow a + b + 1 \in \mathbb{Z} \Longrightarrow$ a $* b \in \mathbb{Z}$

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

(ii) Associative property: *Let* $a, , c \in \mathbb{Z}$

$(a * b) * c = (a + b + 1) * c = (a + b + 1) + c + 1 = a + b + c + 2$

and $\ a * (b * c) = a * (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 2$

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

(iii) Existence of identity: *Let* $a \in G$ *and* $'$e$'$ *be the identity element*

$Now\ a * e = a \Longrightarrow a + e + 1 = a \Longrightarrow e = -1$

$Now\ a * e = a * (-1) = a + (-1) + 1 = a$ similarly we can prove

$e * a = a \Longrightarrow e + a + 1 = a \Longrightarrow e = -1$

$\therefore The\ identity\ element\ is - 1$

(iv) Existence of inverse: $Let\ a \in G\ and'\ b'be\ the\ inverse\ of\ a$

$Now\ a * b = e \Longrightarrow a + b + 1 = -1 \Longrightarrow b = -2 - a$

$The\ inverse\ of\ a\ is - 2 - a\ \ so\ every\ element\ has\ invertiable$

(v) Commutative property: $Let\ a, \in G\ Now\ a * b = a + b + 1 = b + a + 1 = b * a$

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

$\therefore (G,*)\ is\ an\ abelian\ group.$

4. P.T the set G of rational (real) numbers other than 1 with operation

$a \oplus b = a + b - ab\ \ \forall a, b \in G$ is an abelian group. Hence show that $x =$ $_2$ is a solution of the equation $(4 \oplus 5) \oplus x = 7$

Sol: $G = \mathbb{R} - \{1\}$

$and\ \oplus$ is defined by $a \oplus b = a + b - ab\quad \forall a, b \in G$

To prove that $(G,\oplus)$is an abelian group

(i) Closure property: $Let\ a, b \in G\ where\ a \neq 1 \in \mathbb{R},\ \neq 1 \in \mathbb{R}$

$since\ a, \in G \Longrightarrow a + b \in G\ and\ ab \in G\ where\ a + b - ab \neq 1$

$\Longrightarrow a + b - ab \in G \Longrightarrow a \oplus b \in G$

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

(ii) Associative property: $Let\ a, , c \in G$

$(a \oplus b) \oplus c = (a + b - ab) \oplus c = \ (a + b - ab) + c - (a + b - ab)c$

$= a + b + c - ab - bc - ac + abc$

$Next\ \ a \oplus (b \oplus c) = a \oplus (b + c - bc) = a + (b + c - bc) - a(b + c - bc)$

$= a + b + c - ab - bc - ac + abc$

$\therefore (a \oplus b) \oplus c = a(\oplus (b \oplus c) \quad \forall a, b, c \in G$

(iii) Existence of identity: *Let* $a \in G$ *and* $'e'$ *be the identity element*

$Now\ a \oplus e = a \Longrightarrow a + e - ae = a \Longrightarrow (1 - a) = 0 \Longrightarrow e = 0 \ \ since\ \ a \neq 1$

$Now\ a \oplus e = a \oplus (0) = a + (0) - (0) = a$ similarly we can prove

$e \oplus a = a \Longrightarrow e + a - ea = a \Longrightarrow (1 - a) = 0 \Longrightarrow e = 0 \ \ since\ \ a \neq 1$

$\therefore The\ identity\ element\ is\ 0$

(iv) Existence of inverse: *Let* $a \in G$ *and* $'b'$*be the inverse of* a

$Now\ a \oplus b = e \Longrightarrow a + b - ab = 0 \Longrightarrow (1 - a) = -a \ \Longrightarrow b = \ _{1 - a} = \ _{a - 1}$

$The\ inverse\ of\ a\ is\ \ _{a-1}\ so\ every\ element\ has\ invertiable$

(v) Commutative property: $Let\ a, b \in G\ Now\ a \oplus b = a + b - ab = b + a - ba = b \oplus a$

$\therefore a \oplus b = b \oplus a\ \ \forall\ a, b \in G$

$\therefore (G,\oplus)\ is\ an\ abelian\ group.$

$(\ 4 \oplus 5) \oplus x = 7 \Longrightarrow (4 + 5 - 20) \oplus x = 7$

$\Longrightarrow -11 \oplus x = 7 \Longrightarrow (-11 + x + 11x) = 7 \Longrightarrow 12x = 18 \Longrightarrow x = \ _{2}$

5. P.T the set G of rational (real) numbers other than -1 with operation $a \oplus b = a + b + ab\ \forall a,\ \in G$ is an abelian group. Hence show that $x = -\ _{3}$ is a solution of the equation $(2 \oplus x) \oplus 3 = 7$

Sol: $G = \mathbb{R} - \{-1\}$

$and\ \ \oplus$ is defined by $\ a \oplus b = a + b + ab\ \ \forall a, b \in G$

To prove that $(G,\oplus)$is an abelian group

(i) Closure property: $Let\ a, b \in G\ where\ a \neq -1 \in \mathbb{R}, b \neq -1 \in \mathbb{R}$

$since\ a,\ \in G \Longrightarrow a + b \in G\ and\ ab \in G\ where\ a + b + ab \neq 1$

$\Longrightarrow a + b + ab \in G \Longrightarrow a \oplus b \in G$

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

(ii) Associative property: $Let\ a,,c \in G$

$(a \oplus b) \oplus c = (a + b + ab) \oplus c = (a + b + ab) + c + (a + b + ab)c$

$= a + b + c + ab + bc + ac + abc$

$Next\ \ a \oplus (b \oplus c) = a \oplus (b + c + bc) = a + (b + c + bc) + a(b + c + bc)$

$= a + b + c + ab + bc + ac + abc$

$\therefore (a \oplus b) \oplus c = a(\oplus (b \oplus c) \qquad \forall a, b, c \in G$

(iii) Existence of identity: $Let\ a \in G\ and\ 'e'\ be\ the\ identity\ element$

$Now\ a \oplus e = a \Longrightarrow a + e + ae = a \Longrightarrow (1 + a) = 0 \Longrightarrow e = 0 \ \ since\ \ a \neq -1$

$Now\ a \oplus e = a \oplus (0) = a + (0) + (0) = a$ similarly we can prove

$e \oplus a = a \Longrightarrow e + a + ea = a \Longrightarrow (1 + a) = 0 \Longrightarrow e = 0 \ \ since\ \ a \neq -1$

$\therefore The\ identity\ element\ is\ 0$

(iv) Existence of inverse: $Let\ a \in G\ and'\ b'be\ the\ inverse\ of\ a$

$Now\ a \oplus b = e \Longrightarrow a + b + ab = 0 \Longrightarrow (1 + a) = -a \ \Longrightarrow b = \dfrac{}{1 + a}$

$The\ inverse\ of\ a\ is\ \ _{a+1}\ so\ every\ element\ has\ invertiable$

(v) Commutative property: $Let\ a, b \in G\ Now\ a \oplus b = a + b + ab = b + a + ba = b \oplus a$

$\therefore a \oplus b = b \oplus a\ \ \forall\ a, b \in G$

$\therefore (G,\oplus)\ is\ an\ abelian\ group.$

$(\ 2 \oplus x) \oplus 3 = 7 \Longrightarrow (2 + x + 2x) \oplus 3 = 7$

$\Longrightarrow (2 + 3x) \oplus 3 = 7 \Longrightarrow [(2 + 3x) + 3 + 3(2 + 3x)] = 7$

$\Longrightarrow [2 + 3x + 3 + 6 + 9x] = 7$

$\Longrightarrow 12x + 11 = 7 \Longrightarrow 12x = -4 \Longrightarrow x = -\dfrac{}{3}$

6. P.T the set of matrices $A_\alpha = \begin{bmatrix} cos\alpha & -sin\alpha \\ sin\alpha & cos\alpha \end{bmatrix}$ $where\ \alpha \in \mathbb{R}$ forms a group w.r.t. matrix multiplication if $cos\theta = cos\varphi \Longrightarrow \theta = \varphi$.Is it abelian?

Sol: $G = \{A_\alpha / \alpha \in \mathbb{R} \; and \; A_\alpha = \begin{bmatrix} cos\alpha & -sin\alpha \\ sin\alpha & cos\alpha \end{bmatrix}\}$

To prove that $(G,\cdot)$ is a group

(i) Closure property: $Le\ , \ \in G$

$where\ A_\alpha = \begin{bmatrix} & -sin\alpha \\ sin\alpha & \end{bmatrix}\ and\ A_\beta = \begin{bmatrix} cos\beta & -sin\beta \\ sin\beta & cos\beta \end{bmatrix}$

$Now A_\alpha \cdot A_\beta = \begin{bmatrix} & -sin\alpha & cos\beta & -sin\beta & \cos(\alpha+\beta) & -sin(\alpha+\beta) \\ sin\alpha & cos\alpha & sin\beta & cos\beta & sin(\alpha+\beta) & cos(\alpha+\beta) \end{bmatrix}_{\alpha+\beta}$

$since \quad \alpha, \beta \in \mathbb{R} \Longrightarrow \alpha + \beta \in \mathbb{R}$

$\therefore \cdot$ is a binary operation on G

$\therefore$ G has closed under multiplication

(ii) Associative property: $A_\alpha\ , A_\beta, A_\gamma \in G \; where \; \alpha, \beta, \gamma \in \mathbb{R}$

$(A_\alpha \cdot A_\beta) \cdot A_\gamma = (A_{\alpha+\beta}) \cdot A_\gamma = A_{(\alpha+\beta)+\gamma}$

$= A_{\alpha+(\beta+\gamma)} = A_\alpha \cdot A_{(\beta+\gamma)} = A_\alpha \cdot (A_\beta \cdot A_\gamma)$

$\therefore \cdot$ is an associative on G

(iii) Existence of identity: $Let A_\alpha \; where \; \alpha \in \mathbb{R}$

$we\ have\ \ A_0 = \begin{bmatrix} & -sin0 & 1 \\ sin0 & cos0 & 0 \quad 1 \end{bmatrix}$

$Now\ A_\alpha \cdot\ A_0 = A_{\alpha+0} = A_\alpha$

$also\ A_0 \cdot\ A_\alpha = A_{0+\alpha} = A_\alpha$

$\therefore The\ identity\ element\ is\ \begin{bmatrix} 0 & 1 \end{bmatrix}$

(iv) Existence of inverse: $Let A_\alpha \; where \; \alpha \in \mathbb{R}$

$since\ \alpha \in \mathbb{R} \implies -\alpha \in \mathbb{R} \Longrightarrow\ A_{-\alpha} \in G$

$Now\ A_\alpha \cdot\ A_{-\alpha} = A_{\alpha+(-\alpha)} = A_0$

$also\ A_{-\alpha} \cdot\ A_\alpha = A_{-\alpha+(\alpha)} = A_0$

$A_{-\alpha}\ is\ the\ inverse\ of\ A_\alpha$

$\therefore$ *Every element in G has multiplicative inverse.*

$\therefore$ $(G,\cdot)$ *is an abelian group.*

(v) Commutative property: *Le* , $\in G$

Now $A_\alpha \cdot A_\beta = A_{\alpha+\beta} = A_{\beta+\alpha} = A_\beta \cdot A_\alpha$

$\therefore$ $A_\alpha \cdot A_\beta = A_\beta \cdot A_\alpha \ \forall A_\alpha , A_\beta \ \in G$

$\therefore$ $(G,\cdot)$ *is an abelian group.*

7. If G is the set of even integers i.e. $G = \{\ldots\ldots -4,-2,0,2,4,\ldots\ldots\}$ then prove that G is an abelian group w.r.t addition as the operation.

Sol: $G = \{\ldots\ldots -4,-2,0,2,4,\ldots\ldots\} = \{2n/n \in \mathbb{Z}\} = Set\ of\ Even\ integers$

To prove that $(G,+)$ is an abelian group

(i) Closure property: *Let* $a,b \in G$ *then* $a = 2n, = 2m$ *where* $n, \in \mathbb{Z}$

$\Longrightarrow a+b = 2n+2m = 2(n+m) = 2l \in G$ *where* $l = m+n \in \mathbb{Z}$

$\Longrightarrow$ a $+ b \in G$

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

(ii) Associative property: *Let* $a,,c \in G$ *then* $a = 2n, b = 2m\ , c = 2p$ *where* $n,m,p \in \mathbb{Z}$

$(a+b)+c = (2n+2m)+2p = 2[(n+m)+p]$

$= 2[(n+(m+p)] = 2n+(2m+2p) = a+(b+c)$

$\therefore (a+b)+c = \ a+(b+c) \qquad \forall a,b,c \in G$

(iii) Existence of identity: *Let* $a \in G$ *then* $a = 2n$ *where* $n \in \mathbb{Z}$

we have $2(0) \in G$

Now $a+e = 2n+2(0) = 2(n+0) = 2n = a$

$\therefore$ *The identity element is* $2(0) = 0$

(iv) Existence of inverse: *Let* $a \in G$ *then* $a = 2n$ *where* $n \in \mathbb{Z}$

since $n \in \mathbb{Z} \Longrightarrow -n \in \mathbb{Z} \Longrightarrow -2n \in \mathbb{Z} \Longrightarrow -a \in G$

now $\ a+(-a) = 2n-2n = 2(0) = 0$

$The\ inverse\ of\ a\ is - a$

$\therefore Every\ element\ in\ G\ has\ additive\ \ inverse.$

(v) Commutative property: $Let\ a, b \in G$

$Now\ a + b = 2n + 2m = 2m + 2n = b + a$

$\therefore a + b = b + a\ \ \forall\ a, b \in G$

$\therefore (G, +)$ is an abelian group

8. S.T the set $G = \{x/x = 2^a 3^b\ and\ a,\ \in \mathbb{Z}\}$ is an abelian group under multiplication.

Sol: $G = \{x/x = 2^a 3^b\ and\ a, b \in \mathbb{Z}\}$

To prove that $(G, \cdot)$ is an abelian group

(i) Closure property: $Let\ x, y \in G\ then\ x = 2^a 3^b, y = 2^c 3^d\ where\ a, b, , d \in \mathbb{Z}$

$\Longrightarrow xy = (2^a 3^b)(2^c 3^d) = 2^{a+c} 3^{c+d} = 2^l 3^m \in G\ since\ l = a + c \in \mathbb{Z}, m = c + d \in \mathbb{Z}$

$\Longrightarrow$ xy $\in G$ $\quad\quad$ $\therefore$ xy $\in G\ \ \forall x, y \in G$

(ii) Associative property:

$Let\ x, y, \in G\ then\ x = 2^a 3^b, = 2^c 3^d, = 2^e 3^f\ where\ a, b, c, d, e, f \in \mathbb{Z}$

$(xy)z = [(2^a 3^b)(2^c 3^d)]2^e 3^f = 2^{(a+c)+e} 3^{(b+d)+f}$

$= 2^{a+(c+e)} 3^{b+(d+f)}$

$= 2^a 3[(2^{c+e} 3^{d+f}]$

$= 2^a 3[(2^c 3^d)(2^e 3^f)] = x(yz)$

$\therefore (xy)z = \ x(yz) \quad \forall x, y, z \in G$

(iii) Existence of identity: $Let\ x \in G\ then\ x = 2^a 3^b\ where\ a, b \in \mathbb{Z}$

$we\ have\ 1 = 2^0 3^0 \in G\ \ since\ 0 \in \mathbb{Z}$

$Now\ x \cdot 1 = (2^a 3^b)(2^0 3^0) = 2^{a+0} 3^{b+0} = 2^a 3^b = x$

$\therefore The\ identity\ element\ is\ 1 = 2^0 3^0$

(iv) Existence of inverse: $Let\ x \in G\ then\ x = 2^a 3^b\ where\ a, b \in \mathbb{Z}$

$since\ a, \in \mathbb{Z} \Longrightarrow -a, -b \in \mathbb{Z} \Longrightarrow 2^{-a}3^{-b} \in G$

$now\ \ x \cdot (2^{-a}3^{-b}) = (2^a 3^b)(2^{-a}3^{-b}) = 2^{a-a}3^{b-b} = 2^0 3^0$

$The\ inverse\ of\ 2^a 3^b\ is\ 2^{-a}3^{-b}$

$\therefore Every\ element\ in\ G\ has\ multiplicative\ inverse.$

v) Commutative property: $Let\ x, \in G\ then\ x = 2^a 3^b, = 2^c 3^d\ where\ a,, c, d \in \mathbb{Z}$

$\Longrightarrow xy = (2^a 3^b)(2^c 3^d) = 2^{a+c}3^{c+d} = 2^{c+a}3^{d+c} = (2^c 3^d)(2^a 3^b) = yx$

$\therefore$ xy = yx $\ \forall x, y \in G$

$\therefore (G,\cdot)$ is an abelian group

9. S.T the set $G = \{\ldots\ldots 2^{-3}, 2^{-2}, 2^{-1},, 2^1, 2^2, 2^3\ \ldots\ldots\}$ is an abelian group under multiplication.

Sol: $G = \{\ldots\ldots 2^{-3}, 2^{-2}, 2^{-1}, 1, 2^1, 2^2, 2^3\ \ldots\ldots\} = \{2^n / n \in \mathbb{Z}\}$

To prove that $(G,\cdot)$ is an abelian group

(i) Closure property: $Let\ x, y \in G\ then\ x = 2^a,\ y = 2^b\ where\ a, \in \mathbb{Z}$

$\Longrightarrow xy = (2^a 2^b) = 2^{a+b} = 2^l \in G\ since\ l = a + b \in \mathbb{Z},$

$\Longrightarrow$ xy $\in G$ $\qquad\qquad$ $\therefore$ xy $\in G\ \ \forall x, y \in G$

(ii) Associative property:

$Let\ x, y, \in G\ then\ x = 2^a, y = 2^b, = 2^c\ where\ a, b, \in \mathbb{Z}$

$(xy)z = (2^a 2^b)2^c = [2^{(a+b)}]2^c = 2^{a+(b+c)}$

$= 2[2^{b+c}]$

$= 2(2^b 2^c)$

$= x(yz)$

$\therefore (xy)z = x(yz) \qquad \forall x, y, z \in G$

(iii) Existence of identity: $Let\ x \in G\ then\ x = 2^a\ where\ a \in \mathbb{Z}$

$we\ have\ 1 = 2^0 \in G\ \ since\ 0 \in \mathbb{Z}$

$Now\ x \cdot 1 = (2^a)(2^0) = 2^{a+0} = 2^a = x$

$\therefore$ *The identity element is* $1 = 2^0$

(iv) Existence of inverse: *Let* $x \in G$ *then* $x = 2^a$ *where* $a \in \mathbb{Z}$

since $a \in \mathbb{Z} \Longrightarrow -a \in \mathbb{Z} \Longrightarrow 2^{-a} \in G$

now $x \cdot (2^{-a}) = (2^a)(2^{-a}) = 2^{a-a} = 2^0$

The inverse of 2^a *is* 2^{-a}

$\therefore$ *Every element in G has multiplicative inverse.*

(v) commutative property: *Let* $x, y \in G$ *then* $x = 2^a, y = 2^b$ *where* $a, b \in \mathbb{Z}$

$\Longrightarrow xy = (2^a)(2^b) = 2^{a+b} = 2^{b+a} = (2^b)(2^a) = yx$

$\therefore$ xy = yx $\forall x, y \in G$

$\therefore (G, \cdot)$ is an abelian group

10. S.T the set of all ordered pairs (a, b) of real numbers for which $a \neq 0$ w.r.t the operation $\times$ defined by $(a, b) \times (c, d) = (ac, bc + d)$ is a group.

Is the group commutative?

Sol: $G = \{(a,) \,/\, a \neq 0 \in \mathbb{R}, b \in \mathbb{R}\}$

The operation $\times$ defined by $(a, b) \times (c,) = (ac, bc + d)$

To prove that $(G, \times)$ is a group

(i) Closure property: *Let* $(a, b), (c, d) \in G$ *where* $a \neq 0 \in \mathbb{R}, c \neq 0 \in \mathbb{R}$

$\Longrightarrow (a,) \times (c, d) = (ac, \ + d) \in G$ *since* $a \neq 0 \in \mathbb{R}, c \neq 0 \in \mathbb{R} \Longrightarrow ac \neq 0 \in \mathbb{R}$

$\Longrightarrow (a, b) \times (c, d) \in G \qquad \therefore (a, b) \times (c, d) \ \forall x, y \in G$

(ii) Associative property:

Let $(a, b), (c, d), (e, f) \in G$ *where* $a \neq 0 \in \mathbb{R}, c \neq 0 \in \mathbb{R}, e \neq 0 \in \mathbb{R},$

$[(a, b) \times (c, d)] \times (e, f) = (ac, bc + d) \times (e, f) = [(ac)e, (bc + d)e + f]$

$= (ace, bce + de + f)$

Next $(a,) \times [(c,) \times (e, f)] = (a, b) \times (ce, de + f) = ((ce), bce + de + f)$

$= (ace, bce + de + f)$

$[(a,b)\times(c,d)]\times(e,f)=(a,b)\times[(c,d)\times(e,f)]$

(iii) Existence of identity: $Let\ (a,b)\in G\ (x,y) be\ the\ identity\ in\ G$

$Now\ (a,b)\times(x,y)=(a,b)\Longrightarrow(ax,bx+y)=(a,b)$

$\Longrightarrow ax=a, bx+y=b\Longrightarrow x=1, y=0$

$\therefore The\ identity\ element\ is\ (1,0)$

(iv) Existence of inverse: $Let\ (a,b)\in G\ (c,d) be\ the\ inverse\ \ in\ G$

$(a,b)\times(c,d)=(1,0)\Longrightarrow(ac,bc+d)=(1,0)$

$\Longrightarrow ac=1, bc+d=0\Longrightarrow c=\ ,\qquad -b(\ )=d$

$(c,d)=(_{a},-_{a})\ is\ the\ inverse\ of\ (a,b)$

$\therefore Every\ element\ in\ G\ has\ \ inverse.$

(v) Commutative property: $Let\ (a,b),(c,d)\in G\ where\ a\neq 0\in\mathbb{R}, c\neq 0\in\mathbb{R}$

$\Longrightarrow(a,b)\times(c,d)=(ac,bc+d)$

$\Longrightarrow(c,d)\times(a,b)=(ca,da+b)$

$\therefore(a,b)\times(c,d)\neq(c,d)\times(a,b)$

$\therefore (G,\times)$ is not an abelian group

11. P.T the set of n^{th} root of unity under multiplication forms a finite abelian group. (OR)

P.T the set $G=\{a/a^n=1\}$er multiplication form a finite abelian group.

Sol: $G=\{x/x=\sqrt{1}\}=\{x/x=1^{\frac{1}{n}}\}=\{x/x^n=1\}$

$we\ have\ 1=cos0+isin0=cos2\pi+isin2\pi$

$=cos2k\pi+isin2k\pi\ \ where\ k=0,1,2,\dots n-1$

$x=1^{\frac{1}{n}}=(cos2k\pi+isin2k\pi)^{\frac{1}{n}}$

$\Longrightarrow x=\cos(\frac{2k\pi}{n})+isin(\frac{2k\pi}{n})=e^{i(\frac{2k\pi}{n})}\ \ where\ k=0,1,2,\dots n-1$

$G = \{1, , ^2, \ldots \omega^{n-1}\}$ $where\ \omega = e^{i(\frac{2\pi}{n})} \Rightarrow \omega^n = 1$

To prove that $(G,\cdot)$is an abelian group

(i) Closure property: $Let\ a, b \in G\ then\ a^n = 1,\ b^n = 1$

$now\ (ab) = a^n b^n = 1.1 = 1$

$\therefore (ab) = 1 \Longrightarrow ab \in G\ \ \forall a, b \in G$

(ii) Associative property: Since all elements in G are complex numbers and hence multiplication is associative in G

(iii) Existence of identity: $Let\ \omega^r \in G\ \ where\ 0 \leq r \leq n-1$

$we\ have\ 1 = \omega^0 \in G$

$Now\ \omega^r \cdot \omega^0 = \omega^{r+0} = \omega^r$

$\therefore The\ identity\ element\ is\ 1 = \omega^0$

(iv) Existence of inverse: we have 1.1=1

$Let\ \omega^r \in G\ be\ any\ elementof\ G\ where\ r = 1,2, \ldots n-1$

$\therefore \omega^{n-r} \in G$

$now\ \omega^r \cdot \omega^{n-r} = \omega^n = 1$

$The\ inverse\ of\ \omega^r\ is\ \omega^{n-r}$

$\therefore Every\ element\ in\ G\ has\ multiplicative\ inverse.$

(v) Commutative property: $Let\ a, \in G\ then\ a = \omega^r, b = \omega^s\ where\ 0 \leq r, \leq n-1$

$\Longrightarrow ab = \omega^r \omega^s = \omega^{r+s} = \omega^{s+r} = \omega^s \omega^r = ba$

$\therefore$ ab = ba $\forall a, b \in G$

$\therefore (G,\cdot)$ is finite an abelian group

12. P.T the set of 4^{th} root of unity under multiplication forms a finite group. (OR)

P.T the set $G = \{1, -1, i, -i\}$*under multiplication form a finite abelian goup*.

Sol: $G = \{x/x = \sqrt[4]{1}\} = \{x/x = 1^{\frac{1}{4}}\} = \{x/x^4 = 1\} = \{1, -1, , -i\}$

$\cdot$	$\mathbf{1}$	$\mathbf{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$
$\mathbf{-1}$	$\mathbf{-1}$	$\mathbf{1}$	$\boldsymbol{-i}$	$\boldsymbol{i}$
$\boldsymbol{i}$	$\boldsymbol{i}$	$\boldsymbol{-i}$	$\mathbf{-1}$	$\mathbf{1}$
$\boldsymbol{-i}$	$\boldsymbol{-i}$	$\boldsymbol{i}$	$\mathbf{1}$	$\mathbf{-1}$

To prove that $(G,\cdot)$is an abelian group

Construct a composition table for G under multiplication

(i) Closure property: We observe that all elements in C.T

are the elements of $G. \therefore \cdot \; is \; a \; binary \; operation \; on \; G.$

(ii)Associative property: From C.T we observe that all the elements are complex numbers and hence multiplication is associative

(iii) Existence of identity: From C.T we observe that the row headed by 1 is coincide with the top row of C.T. $\therefore 1 \; is \; the \; identity \; element \; in \; G.$

(iv) Existence of inverse: From C.T we observe that the identity elements 1 contains in each row.

The inverse of $1, -1, i, -i \; are \; 1, -1, -i, i \; respectively.$

$\therefore Each \; element \; in \; G \; has \; multilicative \; inverse$

(v) Commutative property: From C.T we observe that all the rows identical with their corresponding columns. Hence $(G,\cdot)$ is finite an abelian group.

13. P.T the set of cube root of unity under multiplication forms a finite group. (OR)

P.T the set $G = \{1, , \omega^2\}$ *under multiplication form a finite abelian group.*

Sol: $G = \{x/x = \sqrt[3]{1}\} == \{x/x^3 = 1\} = \{1, , \omega^2\}$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

To prove that $(G,\cdot)$is an abelian group

Construct a composition table for G under multiplication

(i) Closure property: We observe that all elements in C.T

are the elements of $G. \therefore \cdot \; is \; a \; binary \; operation \; on \; G.$

(ii)Associative property: From C.T we observe that all the elements are complex numbers and hence multiplication is associative

(iii) Existence of identity: From C.T we observe that the row headed by 1 is coincide with the top row of C.T. $\therefore 1 \; is \; the \; identity \; element \; in \; G.$

(iv) Existence of inverse: From C.T we observe that the identity elements 1 contains in each row.

The inverse of $are\ 1, \omega, \omega^2\ are\ 1, ^2, \omega\ respectively.$

$\therefore Each\ element\ in\ G\ has\ multilicative\ inverse$

(v) Commutative property: From C.T we observe that all the rows identical with their corresponding columns. Hence $(G,\cdot)$ is finite an abelian group.

14. P.T the set of square root of unity under multiplication forms a finite group. (OR)

P.T the set $G = \{1, -1\}$ *under multiplication form a finite abelian group*

15. S.T $G = \{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \}$ is a group w.r.t matrix multiplication.

Find the identity and the inverse of every element

Sol: $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, D = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

To show that $G = \{A, B, , D\}$ is a group under multiplication.

Construct a composition table for G under multiplication

$\cdot$	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

(ii)Associative property: From C.T we observe that all the elements are complex numbers and hence multiplication is associative

(iii) Existence of identity: From C.T we observe that the row headed by A is coincide with the top row of C.T. $\therefore A\ is\ the\ identity\ element\ in\ G.$

(iv) Existence of inverse: From C.T we observe that the identity elements A contains in each row.

The inverse of $A, B, , D\ are\ A, B, C, D\ respectively.$

$\therefore Each\ element\ in\ G\ has\ multilicative\ inverse\ Th(G,\cdot)$ is a group

(v) Commutative property: From C.T we observe that all the rows identical with their corresponding columns. Hence $(G,\cdot)$ is finite an abelian group.

Klein-4 group: A group of order 4 whose every element is its own inverse is called kleins-4 group Ex: The above group is kleins-4 group

Cancellation laws: Let G be a non-empty set and $*$ be a binary operation on G .For each a, b, c, $\in G$ then (i) a∗b=a∗c⇒ b=c left cancellation laws and(ii) b∗a=c∗a ⇒b=c right cancellation law

Theorem1: In a group $(G,\cdot)$ cancellation laws holds

Proof: Given that $(G,\cdot)$is a group. Let $a \in G$ so $\exists\ a^{-1} \in G\ \ni aa^{-1} = e = a^{-1}a$

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

$Now\ ab = ac$

$Multiplying\ with\ a^{-1}$

$\Longrightarrow\ a^{-1}(ab) = a^{-1}(ac)$

$\Longrightarrow (a^{-1}) = (a^{-1}a)c \qquad [\cdot\ is\ associative\ ]$

$\Longrightarrow eb = ec \Longrightarrow b = c \qquad [\ ^{-1} = e = a^{-1}a\ ]$

$\therefore\ ab = ac \Longrightarrow b = c\ (left\ cancellation)$

Similarly :
$Let\ a, b, c \in G$

$Now\ ba = ca \Longrightarrow (ba)^{-1} = (ca)a^{-1} \Longrightarrow b(aa^{-1}) = c(aa^{-1}) \Longrightarrow be = ce \Longrightarrow b = c$

$\therefore\ ba = ca \Longrightarrow b = c\ (right\ cancellation)$

Theorem2: The identity element in group $(G,\cdot)$ is unique.

Proof: Given that $(G,\cdot)$ is a group

If possible suppose that e_1, e_2 be two identities in $(G,\cdot)$

Since e_1 is the identity element $\therefore e_2e_1 = e_2 = e_1e_2 \longrightarrow (1)$

$Also\ e_2$ is the identity element $\therefore e_1e_2 = e_1 = e_2e_1 \longrightarrow (2)$

Now $e_2 = e_1e_2 \quad from\ (1)$

$= e_1 \quad f(2)$

$\therefore e_2 = e_1$

$\therefore$ The identity element in group $(G,\cdot)$ is unique

Theorem 3: Every element in a group $(G,\cdot)$ has unique inverse

Proof: Given that $(G,\cdot)$ is a group. Let a $\in G$, e be the identity element in G
If possible suppose that a have two invertible elements b, c.

Since a is the inverse of 'c' $\therefore$ ac=e=ca …….. (1)

Also a is the inverse of 'b' $\therefore$ ab=e=ba …….. (2)

From (1) and (2) ac=ab $\Longrightarrow$c=b ($\because$ By left cancellation law)

$\therefore$ 'a' has unique inverse.

It follows that every element in a group G has unique inverse.

Theorem4: If$(G,\cdot)$ is a group then $(ab)^{-1} = b^{-1}a^{-1}$ $\forall$ a, b, $\in G$

Proof: Given that $(G, \cdot)$ is a group. Let a, b $\in G$,

Let a^{-1}be the multiplicative inverse of 'a'$\Longrightarrow aa^{-1} = e = a^{-1}a$

Let b^{-1} be the multiplicative inverse of 'b' $\Longrightarrow b\,b^{-1} = e = b^{-1}b$

Claim: $(ab)^{-1} = b^{-1}a^{-1}$

Now (ab)$(b^{-1}a^{-1}) = [(ab)b^{-1}]a^{-1}$ ($\because \cdot$ is an associative)

$= [a(bb^{-1})]\ a^{-1}$ (Again $\cdot$ is an associative)

$= [ae]a^{-1}$

$= aa^{-1} = e$ (e is the identity element)

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

Now $(b^{-1}a^{-1})(ab) = [(b^{-1}a^{-1})a]b$ ($\because \cdot$ is an associative)

$= [b^{-1}(a^{-1}a)]b$ (Again $\cdot$ is an associative)

$= (b^{-1}e)b$

$= b^{-1}b = e$ (e is the identity element)

$\therefore$ $(b^{-1}a^{-1})(ab) = e$ ---------- (2)

From (1) & (2) $(b^{-1}a^{-1})(ab) = e$ = (ab)$(b^{-1}a^{-1})$

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

$\therefore$ $(ab)^{-1} = b^{-1}a^{-1}$ $\forall$ a, b, $\in G$

Theorem5: In group (G, ·) for x, y, a, b, $\in$ G then the equations ax=b and ya=b have a unique solution.

Proof: Given that (G, ·) is a group. Let a, b $\in$G,

Since a, b ∈G $ax = b$

$\Longrightarrow a^{-1}(ax) = a^{-1}b$

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

$\Longrightarrow ex = a^{-1}b$

$\Longrightarrow x = a^{-1}b$

But if $x = a^{-1}b$

Now $ax = b$

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

$\Longrightarrow (aa^{-1}) = b$

$\Longrightarrow eb = b$

$\Longrightarrow b = b$

$\boldsymbol{x = a^{-1}b}$ is the solution of the equation ax=b.

Uniqueness part: If possible suppose that $\boldsymbol{x_1}$, be two solutions of ax=b,

$\boldsymbol{ax_1 = b \; and \; ax_2 = b}$

$\Longrightarrow \boldsymbol{ax_1 = ax_2}$

$\Longrightarrow \boldsymbol{x_1 = x_2}$ (By left cancellation law)

∴ Solution is unique.

Similarly $y = ba^{-1}$ is the solution of ya =b.

If possible suppose that y_1, y_2 be the solution of ya=b.

$\therefore \; \boldsymbol{y_1a = b \; and \; y_2a = b}$

$\Longrightarrow \boldsymbol{y_1a = y_2a}$

$\Longrightarrow \boldsymbol{y_1 = y_2}$ (By Right cancellation law)

∴ Solution is unique.

Hence the equations ax=b and ya=b have unique solution.

Theorem6: If (G, ·) is a group then $\boldsymbol{(ab) = a^2b^2 \Leftrightarrow}$ (G, ·) is an abelian group.

Proof: Let a, b ∈G ⇒ ab ∈G

$(ab)^2 = a^2b^2 \Leftrightarrow (ab)(ab) = (aa)(bb)$

$\Leftrightarrow [(ab)] = [(aa)]b$ ($\because \cdot$ is an associative)

$\Leftrightarrow [a(ba)]b = [a(ab)]b$

$\Leftrightarrow a(ba) = a(ab)$

$\Leftrightarrow ba = ab$

$\Leftrightarrow$ (G, ·) is an abelian group

Theorem7: In a group (G, ·) ∀ a, ∈ G $a^2 = e$ then prove that G is an abelian.

(OR)

In a group (G, ·) every element has its own inverse (i.e. $a = a^{-1} \Longrightarrow a^2 = e$ ∀ a, ∈ G) then (G, ·) is an abelian group.

Proof: Let a, b, ∈ G ∴ ab∈ G

Since ∀ a ∈ G $a^2 = e$,

we have $(ab)^2 = e$
$\Longrightarrow (ab)(ab) = e$
$\Longrightarrow ab = (ab)^{-1} = b^{-1}a^{-1}$
$\Longrightarrow ab = b^{-1}a^{-1} \longrightarrow (1)$

But $a^2 = e \Longrightarrow aa = e \Longrightarrow a = a^{-1}$ Similarly $b^2 = e \Longrightarrow bb = e \Longrightarrow b = b^{-1}$

From (1) ab=ba⇒ G is an abelian

(OR)

Let a, b ∈ G ∴ ab∈ G By hypothesis $a = a^{-1}$ $b = b^{-1}$ and $ab = (ab)^{-1}$

Since $ab = (ab)^{-1}$
$\Longrightarrow ab = b^{-1}a^{-1}$
$\Longrightarrow ab = ba$ ($a = a^{-1}$ $b = b^{-1}$)

∴ ab=ba ∀ a, b ∈ G

Theorem8: An algebraic system (G, ·) is a group $\Leftrightarrow (i).(b.c) = (a.b).c \ \forall a, b, c \in G$

(ii) The equations $ax = b, ya = b$ have unique solution for each $x, y, a, b \in G$

Necessary condition ($\Longrightarrow$): Given that (G, ·) is a group

Since (G, ·) is a group$\Longrightarrow a.(b.c) = (a.b).c \ \forall a, b, c \in G$

To prove that in a group (G, ·) $The\ equations\ ax = b,\ = b\ have\ unique$

$solution\ for\ each\ x, y, a, b \in G.$ Let a, b ∈G,

Since a, b ∈G $ax = b$

$\Longrightarrow a^{-1}(ax) = a^{-1}b$

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

$\Longrightarrow ex = a^{-1}b$

$\Longrightarrow x = a^{-1}b$

But if $x = a^{-1}b$

Now $ax = b$

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

$\Longrightarrow (aa^{-1}) = b$

$\Longrightarrow eb = b$

$\Longrightarrow b = b$

$\boldsymbol{x = a^{-1}b}$ is the solution of the equation ax=b.

Uniqueness part: If possible suppose that $\boldsymbol{x_1}$, be two solutions of ax=b,

$\boldsymbol{ax_1 = b\ and\ ax_2 = b}$

$\Longrightarrow \boldsymbol{ax_1 = ax_2}$

$\Longrightarrow \boldsymbol{x_1 = x_2}$ (By left cancellation law)

∴ Solution is unique.

Similarly $y = ba^{-1}$ is the solution of ya =b.

If possible suppose that y_1, y_2 be the solution of ya=b.

$\therefore\ \boldsymbol{y_1a = b\ and\ y_2a = b}$

$\Longrightarrow \boldsymbol{y_1a = y_2a}$

$\Longrightarrow \boldsymbol{y_1 = y_2}$ (By Right cancellation law)

∴ Solution is unique.

Hence the equations ax=b and ya=b have unique solution.

Sufficient condition (⟸): Conversely given that (G, ·) is an algebraic system such that

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

$(ii) The\ equations\ ax = b, ya = b\ have\ unique\ solution\ for\ each\ x, y, a, b \in G$

To prove that (G, ·) is a group. For this we have to show that (i) G has identity element($\forall b \in G, \exists e \in G \ni b.e = b = e.b$)

(ii) Every element in G has multiplicative inverse ($\forall a \in G \; so \; \exists b \in G \ni a.b = e$)

Since $the\ equations\ ax = b, ya = b\ have\ unique\ solution\ for\ each\ x, y, , b \in G$

$The\ equations\ ax = a\ has\ unique\ solution\ for\ each\ \ a \in G$

$Let\ it\ be\ e \in G \therefore ae = a$

Also $the\ equations\ \ ya = b\ has\ unique\ solution\ for\ each\ a, \in G$

$Let\ it\ be\ d \in G \therefore da = b$

$Let\ b \in G$

$Now\ be = (da)e$

$= d(ae)$

$= da = b$

$\therefore be = b \Longrightarrow e\ is\ the\ identity\ element\ in\ G.$

$Let\ a \in G, and\ e \in G$

Since $\ the\ equation\ ax = e\ has\ unique\ solution\ for\ each\ \ a, e \in G$

$Let\ it\ be\ b \in G \qquad \therefore ab = e \Longrightarrow b\ is\ the\ inverse\ of\ a.$

$Each\ element\ in\ G\ has\ multiplicative\ inverse.$

$\therefore (G,\cdot)\ is\ a\ group$

Theorem9: In finite semi group (G, ·) cancellation laws holds then (G, ·) is a group

Proof: we know that in semi group (G, ·) the equations ax=b and

ya =b have a unique solution for each x, y, a, b, ∈ G then (G, ·) is a group.

We prove this theorem it is enough to show that the equations ax=b and

ya =b have a unique solution for each x, y, a, b, ∈ G.

Let $G = \{a_1, a_2, , \ldots a_n\}$ be have 'n' distinct elements and (G, ·) is a semi group satisfies cancellation laws.

Let a≠0∈ G

Consider let $aG = \{aa_1, _2, , \ldots aa_n\}$

To show that aG=G, Let p∈aG ⇒p=a x_k for some $x_k \in G$ $1 \leq k \leq n$

Since a∈ G , $x_k \in G \Rightarrow a\, x_k \in G$ ⇒p∈ G $\Longrightarrow aG \subseteq G$

If possible suppose that $aa_i = aa$ for i≠j

$\Longrightarrow \boldsymbol{a_i = a_j}$ (By left cancellation laws)

Which is contradiction to G has 'n' distinct elements

∴ aG has 'n' distinct elements and G has 'n' distinct elements. and $aG \subseteq G$

∴ aG =G

Let b∈ G ⇒b ∈a G (aG = G)

$\Longrightarrow b = ax_p$ for somex_p $where\ 1 \leq p \leq n$

To show thatx_p will be a unique solution.

If possible suppose thatx_p, x_q be the solutions of ax=b.

∴ ax_p=b ax_q=b

∴ ax_p= ax_q

⇒x_p=x_q (By left cancellation laws)

Hence there exist unique solution x_p∈G for ax=b.

∴ The equations ax=b has a unique solution for each a, b ∈G.

Next consider a set $Ga = \{a_1 a, _2 a, , \ldots a_n a\}$

Similarly we can prove that the equation ya=b has a unique solution for each a, b ∈G

∴ (G, ·) is a group.

Theorem10: Let G be a group .Let a, b ∈ G. Then prove that $(ab) = a^n b^n$ when G is abelian and n ∈ℕ

Proof: For n ∈ℕ we prove that this result by mathematical induction on n ∈ℕ

Let s (n) be $(ab) = a^n b^n$

For n=1 $(ab)^1 = ab$

$= a^1 b^1$

$\therefore$ s (1) is true.

We can assume that the s(n) is true for some n=k$\in \mathbb{N}$

$(\boldsymbol{ab})^{\boldsymbol{k}} = \boldsymbol{a^k b^k}$

Now$(\boldsymbol{ab})^{\boldsymbol{k+1}} = (\boldsymbol{ab})^{\boldsymbol{k}}(\boldsymbol{ab})$

$= (\boldsymbol{a^k b^k})(\boldsymbol{ab})$

$= (\boldsymbol{a^k b^k})(\boldsymbol{ba})$ **(G is an abelian)**

$= \boldsymbol{a^k}(\boldsymbol{b^k b})\boldsymbol{a}$ **('·' is an associative)**

$= a^k a(b^k b)$ (Again G is an abelian)

$= a^{k+1} b^{k+1}$

$\therefore$ S (k+1) is true.

Theorem11: If G is a group such that $(\boldsymbol{ab}) = \boldsymbol{a^m b^m}$ for three consecutive integers m for all a, b, $\in$ G, show that G is abelian.

Proof: To prove that ab=ba $\forall$ a, b$\in$ G

Let a, b$\in$ G and m, m+1, m+2 be three consecutive integers

$(ab)^m = a$; $(ab)^{m+1} = a^{m+1} b^{m+1}$ $(ab)^{m+2} = a^{m+2} b^{m+2}$

Now $(ab)^{+2} = (ab)^{m+1}(ab)$

$\Longrightarrow (ab)^{+2} = a^{m+1} b^{m+1}(ab)$

$\Longrightarrow aa^{m+1} b^{m+1} b = aa^m (ab)$

$\Longrightarrow a^{m+1} b^{m+1} b = a^m (ab)$ $(By\ L.C.L)$

$\Longrightarrow a^{m+1} b^{m+1} = a^m b^m ba$ $(By\ R.C.L)$

$\Longrightarrow (ab)^{+1} = (ab)^m (ba)$

$\Longrightarrow (ab)^m (ab) = (ab)^m (ba)$

$\Longrightarrow ab = ba\ By\ L.C.L$

$ab = ba \ \forall$ a, b$\in$ G

$\therefore$ G is abelian.

Addition modulo M: *Let* $a, \in \mathbb{Z}$ *and* M*be fixed positive integer. If* r *is the remainder* $(0 \leq r < M)$*when* $a + b$ *is divided by* M*. We define* $a +_m b = r$.

We read it as "a addition modulo M b"

Ex: 1) $3 +_4 5 = 0$ $(3 + 5 = \frac{8}{4} = 0)$ 2) $3 +_4 7 = 2$ $(3 + 7 = \frac{10}{4} = 2)$

3) $5 +_5 6 = 1$ $(5 + 6 = {}^{11} = 1)$

Multiplication modulo P: *Let* $a, \in \mathbb{Z}$ *and* P*be fixed positive integer. If* r *is the remainder* $(0 \leq r < P)$*hen* ab *is divided by* P*. We define* $a \times_P b = r$.

We read it as "a multiplication modulo P b"

Ex: 1) $3 \times_4 5 = 3$ $(3 \times 5 = {}^{15} = 3)$ 2) $3 \times_4 7 = 1$ $(3 \times 7 = {}^{21} = 1)$

3) $5 \times_5 6 = 0$ $(5 \times 6 = {}^{30} = 0)$

A congruent to b modulo M: *Let* $a, \in \mathbb{Z}$ *and* M*be fixed positive integer. If* r *is the remainder* $(0 \leq r < M)$*. If* $a - b$ *is divisible by* M*.* $(or\ divides\ by\ M)$

then we say that a *is congruent to* b *moduloM and it is denoted by* $a \equiv b\ (mod M)$

$i.e.\ a \equiv b\ (mod M) \Leftrightarrow M|(a - b)$

Ex: . $4 \equiv 2\ (mod 2) = (2|(4 - 2) = 2|2)$

Theorem1: ***The set*** $G = \{0, , 2, 3, \ldots . (m - 1)\}$ ***of first m positive integers form an abelian group under addition moduloM***

Proof: *If* $a, \in \mathbb{Z}$ *and* $m \in \mathbb{N}$ *then* $a +_m b = r$ *where* r *is the remainder when* $a + b$ *is divided by* m *when* $0 \leq r \leq m - 1$

(i) Closure property: *Let* $a, b \in G$ *then* $0 \leq a \leq m - 1$ and $0 \leq b \leq m - 1$

$\therefore a +_m b = r \in G$ *since* $0 \leq r \leq m - 1$

$\therefore a +_m b \in G$ $+_m$ *is a binary on* G

(ii) Associative property: *Let* $a, b, c \in G$

Now $(+_m b) +_m c = (a+b)+_m c = remainder\,'r'\,when (a+b)+c\ is\ divided\ by\ 'm'$

$= remainder\,'r'\,when\ a+(b+c)\ is\ divided\ by\ 'm'$

$= a+_m(b+c)$

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

$\therefore (a+_m b) +_m c = a+_m(b+_m c)$

(iii) Existence of identity: We have $0 \in G$

$Let\ a \in G\ then\ 0 \le a \le m-1$

$Now\ a+_m 0 = a = 0+_m a$

$\therefore The\ identity\ element\ is\ e = 0$

(iv) Existence of inverse: we have $0+_m 0 = 0$

$Let\ a \in G\ then\ 1 \le a \le m-1 \therefore m-a \in G$

$Now\ a+(m-a) = 0 = (m-a)+_m a$

$\therefore m-a\ is\ the\ additive\ inverse\ of\ 'a'$

$Each\ element\ in\ G\ has\ additive\ inverse.$

(v) Commutative property: $Let\ a, b \in G$

$Now\ a+_m b = r\ \ when\ a+b\ is\ divided\ by\ m$

$= r\ \ when\ b+a\ is\ divided\ by\ m$

$= b+_m a$

$\therefore (G, +_m) isan\ abelian\ group$

Theorem2: ***The set of $(p-1)egers\ G = \{1, 2, 3, \ldots (p-1)\}$ where p is aprime form an abelian group of order $(p-1)$ under multiplication modulo p.***

Proof: $If\ a, b \in \mathbb{Z}\ and\ p \in \mathbb{N}\ then\ a \times_p b = r\ where\ r\ is\ the\ remainder\ when\ ab$ $is\ divided\ by\ p\ when\ 0 \le r < P$

(i) Closure property: $Let\ a, b \in G\ then\ 1 \le a \le p-1$ and $1 \le b \le p-1$

$since\ p\ is\ aprime\ number\ so\ ab\ cannot\ be\ divisible\ by\ p.$

$so\ the\ remainder\ cannot\ be\ equal\ to\ zero.\ so\ we\ shall\ have\ 1 \leq r \leq p-1$

$\therefore a \times_p b = r \in G \ \ since 1 \leq r \leq p-1$

$\therefore a \times_p b \in G \qquad \therefore \times_p \ is\ a\ binary\ on\ G$

(ii) Associative property: $Let\ a, b, c \in G$

Now $(\ \times_p b) \times_p c = (ab) \times_p c = remainder'r'when(ab)c\ is\ divided\ by\ 'p'$

$= remainder'r'when\ a(bc)\ is\ divided\ by\ 'p'$

$= a \times_p (bc)$

$= a \times_p (b \times_p c)$

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

(iii) Existence of identity: We have $1 \in G$

$Let\ a \in G\ then\ 1 \leq a \leq p-1$

$Now\ a \times_p 1 = a = 1 \times_p a$

$\therefore The\ identity\ element\ is\ e = 1$

(iv) Existence of inverse: $Let\ s \in G\ then\ 1 \leq s \leq m-1$

$Considr\ the\ product\ of\ p-1 \Longrightarrow 1 \times_p s, 2 \times_p s, 3 \times_p s \ldots . (p-1) \times_p s$

$All\ these\ elements\ ar\ the\ elements\ of\ G\ by\ binary\ operation\ and$

$all\ these\ elements\ are\ distinct$

$If\ possible\ suppose\ that\ two\ elements\ are\ equl$

$i \times_p s = j \times_p s\ where\ i \neq j\ and\ 1 \leq i \leq p-1\ and\ 1 \leq j \leq p-1$

$\Longrightarrow is\ and\ js\ have\ the\ same\ remainder\ when\ each\ is\ divided\ by\ 'p'$

$\Longrightarrow is - js\ is\ divisible\ by\ 'p'$

$\Longrightarrow p|is - js \Longrightarrow p|(i-j)s \Longrightarrow p|i-j\ or\ p|s$

$which\ is\ a\ contrdict\ to\ 1 \leq i-j \leq p-2$

$Hence\ i \times_p s \neq j \times_p s \qquad \therefore all\ \ elements\ are\ distinct$

And also one of these elements must be equal to 1

since $1 \in G$ *so* $\exists\, k \in G \ni k \times_p s = 1 = s \times_p k \Longrightarrow k$ *is the inverse of* s

Each element in G *has multiplicative inverse.*

(v) Commutative property: *Let* $a, b \in G$

Now $a \times_p b = r$ *when* ab *is divided by* p

$= r$ *when* ba *is divided by* p

$= b \times_p a$

$\therefore (G, \times_p)$ *is an abelian group*

Problems:

1. P.T the set $G = \{0, , 2, 3, 4\}$ is an abelian group of order '5' w.r.t. addition modulo'5'

Sol: Given $G = \{0,1,2,3,4\}$ *under* $'+_5'$

Construct a composition table for G

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(i) Closure property: we observe that all elements in C.T are the elements of G

$'+_5'$is binary on G

(ii) Associative property: *Let* $a, b, c \in G$

Now $(+_5 b) +_5 c = (a + b) +_5 c = remainder\,'r'\,when (a + b) + c$ *is divided by* $'5'$

$= remainder\,'r'\,when\ a + (b + c)$ *is divided by* $'5'$

$= a +_5 (b + c)$

$= a +_5 (b +_5 c)$

$\therefore (+_5 b) +_5 c = a +_5 (b +_5 c)$

(iii) Existence of identity: From C.T we observe that the row headed by 0 is coincide with the top row of C.T. $\therefore 0$ *is the identity element in* G.

(iv) Existence of inverse: From C.T we observe that the identity elements 0 contains in each row.

The inverse of $0,1,2,3,4\ are\ 0,4,3,2,1\ respectively.$

$\therefore$ *Each element in G has additive inverse* $Th(G,+_5)$ is a group

(v) commutative property: From C.T we observe that all the rows identical with their corresponding columns. Hence $(G,+_5)$ is an abelian group of order 5

2. P.T the set $G=\{1,,3,4\}$ is an abelian group of order '4' w.r.t. multiplication modulo'5'

Sol: Given $G=\{1,2,3,4\}\ under\ '\times_5'$

Construct a composition table for G

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(i) Closure property: we observe that all elements in C.T are the elements of G

$'\times_5'$ is binary on G

(ii) Associative property: *Let* $a,b,c\in G$

Now $(\ \times_5 b)\times_5 c=(ab)\times_5 c=remainder'r'when(ab)c\ is\ divided\ by\ '5'$

$=remainder'r'when\ (bc)\ is\ divided\ by\ '5'$

$=a\times_5(bc)$

$=a\times_5(b\times_5 c)$

$\therefore(\ \times_5 b)\times_5 c=a\times_5(b\times_5 c)$

(iii) Existence of identity: From C.T we observe that the row headed by 1 is coincide with the top row of C.T. $\therefore 1\ is\ the\ identity\ element\ in\ G.$

(iv) Existence of inverse: From C.T we observe that the identity elements 1 contains in each row.

The inverse of $1,2,3,4\ are\ 1,3,2,4\ respectively.$

$\therefore$ *Each element in G has additive inverse* $Th(G,\times_5)$ is a group

(v) commutative property: From C.T we observe that all the rows identical with their corresponding columns. Hence $(G,\times_5)$ is an abelian group of order 4

3. P.T the set $G = \{1, , 5, 7\}$ is an abelian group of order '4' w.r.t. multiplication modulo'8'

Sol: Given $G = \{1,3,5,7\}\ under\ '\times_8'$

Construct a composition table for G

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

(i) Closure property: we observe that all elements in C.T are the elements of G

$'\times_8'$ is binary on G

(ii) Associative property: $Let\ a, b, c \in G$

Now $(\ \times_8 b) \times_8 c = (ab) \times_8 c = remainder\ 'r'\ when (ab)c\ is\ divided\ by\ '8'$

$= remainder\ 'r'\ when\ (bc)\ is\ divided\ by\ '8'$

$= a \times_8 (bc)$

$= a \times_8 (b \times_8 c)$

$\therefore (\ \times_8 b) \times_8 c = a \times_8 (b \times_8 c)$

(iii) Existence of identity: From C.T we observe that the row headed by 1 is coincide with the top row of C.T. $\therefore 1\ is\ the\ identity\ element\ in\ G.$

(iv) Existence of inverse: From C.T we observe that the identity elements 1 contains in each row.

The inverse of $1,3,5,7\ are 1,3,5,7\ respectively.$

$\therefore Each\ element\ in\ G\ has\ additive\ inverse\ Th(G,\times_8)$ is a group

(v) commutative property: From C.T we observe that all the rows identical with their corresponding columns. Hence $(G,\times_8)$ is an abelian group of order 4

Order of an element: Let (G, ·) be a group and a ∈ G then there exist a least positive integer 'n' such that a^n=e. then n is said to be order of 'a 'and it is denoted by 0(a). In case such a positive integer does not exist then we say that 0(a) is zero (or) infinite.

Note: (i) We have $e^1 = e \Longrightarrow (e) = 1$

$\therefore The\ orer\ of\ identity\ element\ is\ 1$

(ii) In addition we have $na = 0 \Longrightarrow (a) = n$

Ex: 1. Find the order of each element in a group $G = \{1, -1\}$ under multiplication.

Sol: $G = \{1, -1\}$ *is group under multiplication. Here* $e = 1$

Let $a = 1$ *now* $(1)^1 = 1, (1)^2 = 1, (1)^3 = 1 \ \therefore o(1) = 1$

Let $a = -1$ *now* $(-1)^1 = -1, (-1)^2 = 1, (-1)^3 = -1 \ \therefore o(-1) = 2$

$\therefore (1) = 1, (-1) = 2$

2. Find the order of each element in a group $G = \{1, \omega, \}$ under multiplication

Sol: $G = \{1, , ^2\}$ *is group under multiplication. Here* $e = 1$

Let $a = 1$ *now* $(1)^1 = 1, (1)^2 = 1, (1)^3 = 1 \ \therefore o(1) = 1$

Let $a = \omega$ *now* $(\omega)^1 = \omega, (\omega)^2 = \omega^2, \ (\omega)^3 = \omega^3 = 1 \ \therefore o(\omega) = 3$

Let $a = \omega^2$ *now* $(\omega^2)^1 = \omega^2, (\omega^2)^2 = \omega, \ (\omega^2)^3 = \omega^6 = 1 \ \therefore (\omega^2) = 3$

$\therefore (1) = 1, (\omega) = 3, o(\omega^2) = 3$

3. Find the order of each element in a group $G = \{1, -1, , -i\}$ under multiplication

Sol: $G = \{1, -1, , -i\}$ *is group under multiplication. Here* $e = 1$

Let $a = 1$ *now* $(1)^1 = 1, (1)^2 = 1, (1)^3 = 1 \ \therefore o(1) = 1$

Let $a = -1$ *now* $(-1)^1 = -1, (-1)^2 = 1, (-1)^3 = -1 \ \therefore o(-1) = 2$

Let $a = i$ *now* $(i)^1 = i, (i)^2 = -1, \ (i)^3 = -i, \ (i)^4 = 1 \therefore o(i) = 4$

Let $a = -i$ *now* $(-i)^1 = -i, (-i)^2 = -1, \ (-i)^3 = i, \ (-i)^4 = 1 \therefore o(-i) = 4$

$\therefore (1) = 1, (-1) = 2, o(i) = 4, o(-i) = 4$

4. Find the order of each element in a group $G = Z_6 = \{0, 1, , 3, 4, 5\}$ under addition modulo 6

Sol: $G = Z_6 = \{0,1,2,3,4,5\}$ is a group under addition modulo 6 *Here* $e = 0$

Let $a = 0$ *now* $1.(0) = 0, \ \ 2.(0) = 0, \ \ 3.(0) = 0$ *so* $o(0) = 1$

Let $a = 1$ *now* $1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 6.(1) = 0, \qquad 12(1) = 0, \ldots$ *so* $o(1) = 6$

Let $a = 2$ *now* $2 +_6 2 +_6 2 = 3.(2) = 0, \qquad 6(2) = 0, \ldots$ *so* $o(2) = 3$

Let $a = 3$ *now* $3 +_6 3 = 2.(3) = 0, \qquad 4(3) = 0, \ldots$ *so* $o(3) = 2$

$Let\ a = 4\ now\ 4+_6 4+_6 4 = 3.(4) = 0, \qquad 6(4) = 0, \ldots so\ o(4) = 3$

$Let\ a = 5\ now\ 5+_6 5+_6 5+_6 5+_6 5+_6 5 = 6.(5) = 0, \qquad 12(5) = 0, \ldots so\ o(5) = 6$

$\therefore o(0) = 1, o(1) = 6, o(2) = 3, o(3) = 2, o(4) = 3, o(5) = 6$

5. *In a $gr(G,\cdot)$, if $a, b \in G$ then $o(a) = 5, b \neq e$ and $aba^{-1} = b^2$ find $o(b)$?*

Sol: Given $(a) = 5 \Longrightarrow a^5 = e \ \ and\ aba^{-1} = b^2$

$Now\ (aba^{-1})^2 = (aba^{-1})(aba^{-1}) = ab^2a^{-1} = a(aba^{-1})a^{-1} = a^2ba^{-2}$

$\therefore (aba^{-1})^2 = a^2ba^{-2}$

$\Longrightarrow [(aba^{-1})^2]^2 = (a^2ba^{-2})^2 \Longrightarrow (aba^{-1})^4 = a^2b^2a^{-2} = a^2(aba^{-1})a^{-2} = a^3ba^{-3}$

$\therefore (aba^{-1})^4 = a^3ba^{-3} \Longrightarrow (aba^{-1})^8 = a^4ba^{-4}$

$\Longrightarrow (aba^{-1})^{16} = a^5ba^{-5} \Longrightarrow (b^2)^{16} = ebe^{-1} \Longrightarrow b^{32} = b \Longrightarrow b^{31} = e \Longrightarrow (b)|31$

$since\ 31\ is\ a\ prime\ so\ (b) = 1\ or\ 31$

$If\ (b) = 1\ then\ b = e\ which\ is\ contradict\ to\ \ b \neq e\ \ \therefore (b) = 31$

6. If every element of a group *G* except the identity is of order 2 then prove that *G*is an abelian.

Proof: $Let\ (G,\cdot)\ be\ group\ and\ 'e'be\ the\ identity\ element\ of\ G$

$We\ have\ (e) = 1\ also\ e^2 = e$

$Let\ a \neq e$

$since\ the\ order\ of\ the\ element\ a \neq e\ is\ 2 \Longrightarrow (a) = 2 \Longrightarrow a^2 = e \Longrightarrow a = a^{-1}$

$Let\ a, b \in G \Longrightarrow ab \in G \Longrightarrow (ab)^2 = e$

$$\Longrightarrow ab = (ab)^{-1}$$

$$\Longrightarrow ab = b^{-1}a^{-1} = ba$$

$\therefore ab = ba \Longrightarrow (G,\cdot)\ is\ an\ abelian\ group.$

Theorem1: ***The order of every element of a finite group $(G,\cdot)$ is also finite and is always less than or equal to order of G***

Proof: $(G,\cdot)$ *be a group and* $'a'$*be any element of* G.

By binary operation the set of all positive integral power of $'a'$ *are* $a^1, ^2, a^3 \ldots . \in G$

are all cannot be distinct (since G is finite group)

$Let\ a^r = a^s \ \ where\ r, s \in \mathbb{N}\ and\ r > s$

$\Longrightarrow a^r a^{-s} = a^s a^{-s} \Longrightarrow a^{r-s} = a^0 = e \Longrightarrow a^m = e \ \ where\ m = r - s > 0$

$\therefore m\ is\ a\ positive\ integer\ such\ that\ a^m = e$

By well ordering principal "Every positive integer set has a least member"

Thus the set of all those positive integer m such that $a^m = e$ *has least number say* $'n'$

$\therefore'\ n'is\ a\ least\ positive\ integer\ such\ that\ a^n = e \ \Longrightarrow o(a) = n \ \ i.e. finite$

$Next\ to\ prove\ that\ o(a) \leq o(G)$

$Let o(a) = p \Longrightarrow p\ is\ a\ leat\ positive\ integer\ such\ that\ a^p = e$

$If\ possible\ suppose\ that\ o(a) > o(G)$

By binary operation the set of all positive integral power of $'a'$ *are* $a^1, ^2, a^3 \ldots . a^p \in G$

The set of all these elements are distinct

$Let\ a^r = a^s \ \ where\ 1 \leq r \leq p, 1 \leq s \leq p\ and\ r > s$

$\Longrightarrow a^r a^{-s} = a^s a^{-s} \Longrightarrow a^{r-s} = a^0 = e \Longrightarrow (a) = r - s \qquad (\therefore 1 \leq r - s \leq p - 1 < p)$

$which\ is\ a\ contradict\ to\ o(a) = p. Hence\ a^r \neq a^s$

$\therefore a^1, a^2, a^3 \ldots . a^p \in Gare\ all\ distinct$

$since\ o(a) > o(G) \Longrightarrow p > o(G) which\ is\ not\ possible$

$Hence\ o(a) \leq o(G)$

Theorem2: ***In a*** $gr(G,\cdot), if\ a \in G\ then\ o(a) = o(a^{-1})$

Proof: $Let\ (a) = n \Longrightarrow n\ is\ a\ least\ positive\ integer\ such\ that\ a^n = e$

$Let\ (a^{-1}) = m \Longrightarrow m\ is\ a\ least\ positive\ integer\ such\ that\ (a^{-1}) = e$

$To\ prove\ that\ (a) = (a^{-1})\ i.e.\ n = m\ (n \leq m\ and\ m \leq n\ )$

$since\ a^n = e \Longrightarrow (a^n)^{-1} = e^{-1} \Longrightarrow (a^{-1})^n = e \Longrightarrow o(a^{-1}) \leq n \Longrightarrow m \leq n \rightarrow (1)$

$also\ (a^{-1}) = e \Longrightarrow a^{-m} = e \Longrightarrow (a^{-m})^{-1} = e^{-1} \Longrightarrow a^m = e \Longrightarrow o(a) \leq m \Longrightarrow n \leq m \rightarrow (2)$

$From\ (1)\ (2)\ n = m\ i.e.(a) = o(a^{-1})$

Theorem3: $\boldsymbol{In\ a\ gr(G,\cdot), if\ a \in G\ then\ o(a) = n\ then\ a^m = e \Leftrightarrow n|m}$

Necessary condition ($\Longrightarrow$): $Given\ that\ (a) = n\ \Longrightarrow n$
$is\ a\ least\ positive\ integer\ such\ that\ a^n = e$

$By\ division\ algorithm\ m, (\neq 0) \in \mathbb{Z}\ so\ \exists\ q, r \in \mathbb{Z}\ such\ that\ m = nq + r\ where\ 0 \leq r < n$

$since\ a^m = e \Longrightarrow a^{nq+r} = e \Longrightarrow a^{nq}a^r = e \Longrightarrow (a^n)^q a^r = e \Longrightarrow (e)^q a^r = e \Longrightarrow a^r = e$

$\Longrightarrow r\ is\ a\ least\ positive\ integer\ such\ that\ a^r = e\ \ where\ \ 0 \leq\ r < n$

$If\ 0 <\ r < n\ then\ it\ is\ contradict\ to\ (a) =\ .Hence\ r = 0$

$\therefore m = nq + 0 \Longrightarrow n|m$

Sufficient condition ($\Longleftarrow$): $conversely\ given\ that\ (a) = n\ such\ that\ n|m$

$To\ prove\ that\ a^m = e$

$since\ o(a) = n \Longrightarrow n\ is\ a\ least\ positive\ integer\ such\ that\ a^n = e$

$since\ \ n|m\ by\ definition\ so\ \exists\ a\ positive\ integer\ p\ such\ that\ m = np$

$Now\ a^m = a^{np} = (a^n)^p = e^p = e$

$\therefore a^m = e$

UNIT-2: SUB GROUPS

Complex: Any subset of a group G is called as a complex.

Ex (i) The set $A = \{1, -1\}$ is a complex of group $G = \{1, -1, i, -i\}$ under multiplication

(ii) The set of integers is a complex of a group $(\mathbb{Q}, +)$

Multiplication of a complex: Let M, N be the complex of a group $(G, \cdot)$ then $MN = \{mn \,/\, m \in M, n \in N\}$ is called as multiplication of complex.

Inverse of complex: Let M be the complex of a group $(G, \cdot)$ then $M^{-1} = \{m^{-1} \in G / m \in M\}$ is called as the inverse of element of M

Sub group: A non empty subset H is said to be a subgroup of a group $(G, \cdot)$ if H itself is a group under the same operation of G

Ex: The set of integers is a subgroup of $(\mathbb{Q}, +)$ i.e. $(\mathbb{Z}, +)$ $is\ a\ sub\ group\ of$ $(\mathbb{Q}, +)$

Note: 1. Every group contains at least two sub groups. They are $H = \{e\}$ and $H = G$ are the subgroup of G itself. These two subgroups are called improper/trivial subgroups of G. If any other subgroups exist then it is called proper/non trivial subgroups.

Ex: 1. Find all subgroups of a group $G = \{1, -1, i, -i\}$ under multiplication.

Sol: Given $G = \{1, -1, i, -i\}$ is group under multiplication.

$\cdot$	1	-1
1	1	-1
-1	-1	1

$H_1 = \{1\}\ and\ H_2 = G$ are trivial subgroups of G

Clearly $H_3 = \{1, -1\}$ is also a group.

Hence H_3 is a non-trivial subgroup of G

2 Find all subgroups of a group $Z_6 = \{0, 1, , 3, 4, 5\}$ under addition.

Sol: Given $Z_6 = \{0,1,2,3,4,5\}$ is a group under $+_6$

$+_6$	0	3
0	0	3
3	3	0

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$H_1 = \{0\}\ and\ H_2 = G$ are trivial subgroups of G

Clearly $H_3 = \{0,2,4\}$ is also a group.

Clearly $H_4 = \{0,3,\}$ is also a group

Hence $H_{3,4}$ is a non-trivial subgroup of G

Theorem1: The identity of a subgroup H of a group $(G,\cdot)$ is same as the identity element of G

Proof: $Let\ a \in H\ and\ e^1\ be\ the\ identity\ element\ of\ H.$

$Since\ \ H\ is\ a\ subgroup\ of\ G \Longrightarrow\ (H,\cdot)\ is\ a\ group\quad \therefore ae^1 = a \rightarrow (1)$

$Since\ a \in H \Longrightarrow a \in G\ (H \subseteq G)\ and\ e\ is\ the\ identity\ element\ of\ G\quad \therefore ae = a \rightarrow (2)$

$Since\ e^1 \in H \Longrightarrow e^1 \in G\ From\ (1)\ (2)\ \ ae^1 = ae \Longrightarrow e^1 = e$

Theorem2: The inverse of any element of a subgroup H of a group $(G,\cdot)$ is same as the inverse element in a group G

Proof: $Let\ a \in H\ and\ e\ be\ the\ identity\ element\ of\ G.$

$Since\ \ H\ is\ a\ subgroup\ of\ G \Longrightarrow\ (H,\cdot)\ is\ a\ group\ \ since\ a \in H \Longrightarrow a \in G\ \ (\because H \subseteq G)$

$Let\ 'b'\ be\ the\ inverse\ of\ 'a' \Longrightarrow ab = e \rightarrow (1)$

$Let\ 'c'\ be\ the\ inverse\ of\ 'a' \Longrightarrow ac = e\ \rightarrow (2)$

$From\ (1)\ (2)\ \ ab = ac \Longrightarrow b = c$

Theorem3: If H is a subgroup of a group G then $H^{-1} = H$

Proof: Given that H is a subgroup of a group G

To prove that $H^{-1} = H\ (^{-1} \subseteq H\ and\ H \subseteq H^{-1})$

$Let\ h^{-1} \in H^{-1} \Longrightarrow h \in H\ since\ H\ is\ a\ subgroup\ and\ \ h \in H \Longrightarrow h^{-1} \in H$

$\therefore h^{-1} \in H^{-1} \Longrightarrow h^{-1} \in H \Longrightarrow H^{-1} \subseteq H \rightarrow (1)$

$Let\ h \in H, ce\ H\ is\ a\ subgroup\ \Longrightarrow h^{-1} \in H \Longrightarrow (h^{-1})^{-1} \in H^{-1}\ \Longrightarrow h \in H^{-1}$

$\therefore h \in H \Longrightarrow h \in H^{-1} \Longrightarrow H \subseteq H^{-1} \rightarrow (2)$

$From\ (1)\ (2)\ \ H^{-1} = H$

$The\ converse\ of\ above\ theorem\ need\ not\ be\ true\ i.e.\ H\ is\ a\ complex\ of\ G\ such\ that$

$H^{-1} = H\ then\ H\ need\ not\ be\ a\ subgroup.$

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

$Clearly\ H\ is\ non-empty\ \ subset\ of\ G.$

$H^{-1}=\{(-1)^{-1}\}=\{-1\}=H$

$But\ (-1)(-1)=1\notin H\Longrightarrow binary\ operation\ fails.Hence\ H\ is\ not\ a\ group$

$Thus\ H\ is\ not\ a\ subgroup\ of\ G.$

Theorem4: If H is a subgroup of a group G then $HH=H$

Proof: Given that H is a subgroup of a group G

To prove that $HH=H\ (.e.HH\subseteq H\ and\ H\subseteq HH)$

$Let\ x\in HH\ then\ x=h_1h_2\ where\ h_1\in H,h_2\in H$

$Since\ H\ is\ a\ subgroup\ of\ G\ \ By\ closure\ property\ h_1\in H,h_2\in H\Longrightarrow h_1h_2\in H\ \Longrightarrow x\in H$

$\therefore x\in HH\ \Longrightarrow x\in H\Longrightarrow HH\subseteq H\ \rightarrow(1)$

$Leth_3\in H,e\ is\ the\ identity\ element\ in\ H\ \therefore h_3=h_3e\in HH\Longrightarrow h_3\in HH$

$\therefore h_3\in H\Longrightarrow h_3\in HH\Longrightarrow H\subseteq HH\rightarrow(2)$

$From\ (1)\ (2)\ HH=H$

$The\ converse\ of\ above\ theorem\ need\ not\ be\ true\ i.e.H\ is\ a\ complex\ of\ G\ such\ that$

$HH=H\ \ then\ H\ need\ not\ be\ a\ subgroup.$

$Consider\ G=\{2^n/n\in\mathbb{Z}\}\ \ is\ a\ group$

$and\ H=\{1,2^1,2^2,2^3,\ldots.\}$

$Clearly\ H\ is\ non-empty\ subset\ of\ G.$

$HH=\{h_1h_2/h_1\in H,h_2\in H\}=\{1,2^1,2^2,2^3,\ldots.\}=H$

$But\ 2\in H\ so\ \exists\ _2\notin H\ni 2.(_2)=1\Longrightarrow inverse\ \ fails.Hence\ H\ is\ not\ a\ group$

$Thus\ H\ is\ not\ a\ subgroup\ of\ G.$

Theorem5: A non-empty subset H of a group G is a subgroup of G

$\Leftrightarrow(i)\ a\in H,b\in H\Longrightarrow ab\in H\ (ii)\ a\in H\Longrightarrow a^{-1}\in H$

Necessary condition ($\Longrightarrow$): $Given\ that\ H\ is\ a\ subgroup\ of\ G.$

$To\ prove\ th(i)\ a \in H, b \in H \Longrightarrow ab \in H\ (ii)\ a \in H \Longrightarrow a^{-1} \in H$

$Since\ H\ is\ a\ subgroup\ of\ G \Longrightarrow (H,\cdot)\ \ is\ a\ group$

$By\ closure\ property\colon a \in H, b \in H \Longrightarrow ab \in H$

$By\ inverse\ property\colon a \in H \Longrightarrow a^{-1} \in H$

Sufficient condition ($\Longleftarrow$): $Conversely\ given\ that\ H\ is\ a\ non-empty\ subset\ of\ G$

$such\ th(i)\ a \in H, b \in H \Longrightarrow ab \in H\ (ii)\ a \in H \Longrightarrow a^{-1} \in H$

$To\ prove\ that\ H$ is a subgroup of G

(i)By (i) $a \in H, b \in H \Longrightarrow ab \in H\ \ \therefore closure\ property\ holds\ in\ H$

$(ii) Since\ all\ elements\ of\ H\ are\ the\ elements\ of\ G\ \ (H \subseteq G). We\ know\ that$

$multiplication\ is\ associative\ in\ G\ and\ hence\ multiplication\ is\ associative\ in\ H.$

$(iii)\ Since\ H \neq \phi\ \ Let\ a \in H$

$Let\ a \in H, a \in H\ \ (ii)\ a^{-1} \in H$

$\therefore a \in H, a^{-1} \in H\ \ (i)\ aa^{-1} \in H \Longrightarrow e \in H$

$(iv)\ By\ (ii)\ a \in H \Longrightarrow a^{-1} \in H$

$\therefore (H,\cdot)\ is\ a\ group$

$Hence\ H\ is\ a\ subgroup\ of\ G$

Theorem6: A non-empty subset H of a group G is a subgroup of G

$\Leftrightarrow (i)\ a \in H, b \in H \Longrightarrow ab^{-1} \in H\ \ where\ b^{-1}\ is\ the\ inverse\ of\ b\ in\ G$

Necessary condition ($\Longrightarrow$): $Given\ that\ H\ is\ a\ subgroup\ of\ G.$

$To\ prove\ th(i)\ a \in H, b \in H \Longrightarrow ab^{-1} \in H$

$Since\ H\ is\ a\ subgroup\ of\ G \Longrightarrow (H,\cdot)\ \ is\ a\ group$

$Let\ a \in H, b \in H,\qquad H\ is\ a\ subgroup\ of\ G \Longrightarrow a \in H, {}^{-1} \in H \Longrightarrow ab^{-1} \in H$

Sufficient condition ($\Longleftarrow$): $Conversely\ given\ that\ H\ is\ a\ non-empty\ subset\ of\ G$

$such\ th(i)\ a \in H, b \in H \Longrightarrow ab^{-1} \in H$

$To\ prove\ that\ H$ is a subgroup of G

(i) $Since\ H \neq \phi \quad Let\ a \in H$

$Let\ a \in H, a \in H\ By\ Hypothesis \quad aa^{-1} \in H \Longrightarrow e \in H$

$\therefore e\ is\ the\ identity\ element\ in\ H$

(ii) $Since\ e \in H, a \in H\ \ by\ Hyp\ \ ea^{-1} \in H \Longrightarrow a^{-1} \in H$

$\therefore a \in H \Longrightarrow a^{-1} \in H$

(iii)Let $a \in H, b \in H \Longrightarrow a \in\ , b^{-1} \in H\ By\ Hyp \quad a(b^{-1})^{-1} \in H \Longrightarrow ab \in H$

$\therefore Closure\ property\ holds\ in\ H$

(ii) $Since\ all\ elements\ of\ H\ are\ the\ elements\ of\ G\ (H \subseteq G). We\ know\ that$

$multiplication\ is\ associative\ in\ G\ and\ hence\ multiplication\ is\ associative\ in\ H.$

$\therefore (H,\cdot)\ is\ a\ group$

$Hence\ H\ is\ a\ subgroup\ of\ G$

Theorem7: A non-empty subset H of a group G is a subgroup of $G \Leftrightarrow HH^{-1} \subseteq H$

Necessary condition ($\Longrightarrow$): $Given\ that\ H\ is\ a\ subgroup\ of\ G.$

$To\ prove\ that\ \ HH^{-1} \subseteq H$

$Let\ x \in HH^{-1} \Longrightarrow x = ab^{-1}\ where\ a \in H, b^{-1} \in H^{-1}\ since\ a \in H, b \in H$

$Since\ H\ is\ a\ subgroup\ of\ G\ so\ a \in H, \in H \Longrightarrow ab^{-1} \in H \ \ \Longrightarrow x \in H$

$\therefore x \in HH^{-1} \ \Longrightarrow x \in H \ \Longrightarrow HH^{-1} \subseteq H$

Sufficient condition ($\Longleftarrow$): $Conversely\ given\ that\ H\ is\ a\ non-empty\ subset\ of\ G$

$such\ that\ HH^{-1} \subseteq H$

$To\ prove\ that\ H$ is a subgroup of G

(i) $Since\ H \neq \phi \quad Let\ a \in H$

$Let\ a \in H, b \in H\ \Longrightarrow a \in H, b^{-1} \in H^{-1}\ \Longrightarrow ab^{-1} \in HH^{-1} \Longrightarrow ab^{-1} \in H \quad since\ HH^{-1} \subseteq H$

$\therefore\ a \in H, b \in H \Longrightarrow ab^{-1} \in H$

$Hence\ H\ is\ a\ subgroup\ of\ G$

Theorem8: A non-empty subset H of a group G is a subgroup of $G \Leftrightarrow HH^{-1} = H$

Necessary condition ($\Longrightarrow$): $Given\ that\ H\ is\ a\ subgroup\ of\ G.$

$To\ prove\ that\ HH^{-1} = H\ i.e.(\ ^{-1} \subseteq H\ \ and\ H \subseteq HH^{-1})$

$Let\ x \in HH^{-1} \Longrightarrow x = ab^{-1}\ where\ a \in H, b^{-1} \in H^{-1} since\ a \in H, b \in H$

$Since\ H\ is\ a\ subgroup\ of\ G\ so\ a \in H,\ \in H \Longrightarrow ab^{-1} \in H\ \ \Longrightarrow x \in H$

$\therefore x \in HH^{-1}\ \Longrightarrow x \in H\ \Longrightarrow HH^{-1} \subseteq H\ \rightarrow (1)$

$Lety \in H \Longrightarrow y = ab\quad where\ a \in H, b \in H$

$Since\ H\ is\ a\ subgroup\ of\ G\ so\ y \in H$

$Since\ a \in H,\ \in H, since\ H\ is\ a\ subgroup\ of\ G\ \Longrightarrow ab^{-1} \in H$

$According\ to\ definition\ of\ complex\ \ a \in H,\ \in H, \Longrightarrow\ a \in H, b^{-1} \in H^{-1}$

$\Longrightarrow ab^{-1} \in HH^{-1}$

$\therefore ab^{-1} \in H\ \Longrightarrow ab^{-1} \in HH^{-1} \Longrightarrow H \subseteq HH^{-1} \rightarrow (2)$

From (1) and (2) $HH^{-1} = H$

Sufficient condition ($\Longleftarrow$): $Conversely\ given\ that\ H\ is\ a\ non-empty\ subset\ of\ G$

$such\ that\ HH^{-1} = H\ (HH^{-1} \subseteq H\ \ and\ H \subseteq HH^{-1})$

$To\ prove\ that\ H$ is a subgroup of G

$(i) since\ H \neq \phi\ \ Let\ a \in H$

$Let\ a \in H, b \in H\ \Longrightarrow a \in H, b^{-1} \in H^{-1}\ \Longrightarrow ab^{-1} \in HH^{-1} \Longrightarrow ab^{-1} \in H\quad since\ HH^{-1} \subseteq H$

$\therefore\ a \in H, b \in H \Longrightarrow ab^{-1} \in H$

$Hence\ H\ is\ a\ subgroup\ of\ G$

Theorem9: A non-empty finite subset H of a group G is a subgroup of G

$\Leftrightarrow (i) a \in H, b \in H \Longrightarrow ab \in H$

Necessary condition ($\Longrightarrow$): $Given\ that\ H\ is\ a\ subgroup\ of\ G.$

$To\ prove\ that (i)\ a \in H, b \in H \Longrightarrow ab \in H$

$Since\ H\ is\ a\ subgroup\ of\ G \Longrightarrow (H, \cdot)\ is\ a\ group$

$By\ closure\ property:\ a \in H, b \in H, \Longrightarrow ab \in H$

Sufficient condition ($\Longleftarrow$): $Conversely\ given\ that\ H\ is\ a\ finite\ subset\ of\ G$

$such\ that (i)\ a \in H, b \in H \Longrightarrow ab \in H$

To prove that H is a subgroup of G

(i)By Hyp $a \in H, b \in H \Longrightarrow ab \in H$

$(ii)\ Since\ all\ elements\ of\ H\ are\ the\ elements\ of\ G\ (H \subseteq G).We\ know\ that$

$multiplication\ is\ associative\ in\ G\ and\ hence\ multiplication\ is\ associative\ in\ H.$

$(iii)\ Since\ H \neq \phi, \qquad Let\ a \in H$

$By\ Hyp\ a \in H, a \in H \Longrightarrow a^2 \in H$

$Again\ a^2 \in\ , a \in H\ By\ Hyp\ a^3 \in H$

$Also\ a^3 \in\ ,\ \in H\ By\ Hyp\ a^4 \in H$

$By\ induction\ we\ prove\ that\ a^n \in H\ where\ n\ is\ a\ positive\ integer$

$The\ set\ of\ all\ positive\ integral\ powers\ of\ 'a' are\ a^1, a^2, ^3, a^4, \ldots a^n, a^{n+1}, \ldots \in H$

$Since\ H\ is\ a\ finite\ so\ the\ set\ of\ all\ these\ elements\ a^1, ^2, a^3, a^4, \ldots a^n, a^{n+1}, \ldots \in H$

$can\ not\ be\ distinct.$

$Let\ a^r = a^s\ \ where\ r > s\ and\ r, s \in \mathbb{N}$

$\Longrightarrow a^{r-s} = a^0 = e\ \ since\ \ r > s\ \Longrightarrow r - s > 0 \Longrightarrow r - s\ is\ a\ positive\ integer.$

$\therefore a^{r-s} \in H \Longrightarrow e \in H$

$(iv) Since\ \ r > s\ \Longrightarrow r - s > 0 \Longrightarrow r - s - 1 \geq 0\ \therefore a^{r-s-1} \in H$

$Let\ a \in H$

$Now\ a.a^{r-s-1} = a^{r-s} = a^0 = e$

$\therefore a^{r-s-1}\ is\ the\ iverse\ of\ 'a'$

$Each\ element\ in\ H\ has\ multiplicative\ inverse\ .$

$Hence\ (H, \cdot) is\ a\ group$

Theorem10: A non-empty subset H of a finite group G is a subgroup of G

$\Leftrightarrow (i)\ a \in H, b \in H \Rightarrow ab \in H$

Necessary condition ($\Rightarrow$): $Given\ that\ H\ is\ a\ subgroup\ of\ a\ finite\ group G.$

$To\ prove\ that (i)\ a \in H, b \in H \Rightarrow ab \in H$

$Since\ H\ is\ a\ subgroup\ of\ G \Rightarrow (H,\cdot)\ is\ a\ group$

$By\ closure\ property:\ a \in H, b \in H, \Rightarrow ab \in H$

Sufficient condition ($\Leftarrow$): $Conversely\ given\ that\ H\ is\ a\ non-empty\ subset\ of\ a\ finite\ group\ G\ \ such\ that (i)\ a \in H, b \in H \Rightarrow ab \in H$

To prove that H is a subgroup of G

(i)By Hyp $a \in H, b \in H \Rightarrow ab \in H$

$(ii)\ Since\ all\ elements\ of\ H\ are\ the\ elements\ of\ G\ (H \subseteq G). We\ know\ that\ multiplication\ is\ associative\ in\ G\ and\ hence\ multiplication\ is\ associative\ in\ H.$

$(iii)\ Since\ H \neq \phi, Let\ a \in H$

$By\ Hyp\ a \in H, a \in H \Rightarrow a^2 \in H$

$Again\ a^2 \in\ , a \in H\ By\ Hyp\ a^3 \in H$

$Also\ a^3 \in\ ,\ \in H\ By\ Hyp\ a^4 \in H$

$By\ induction\ we\ prove\ that\ a^n \in H\ where\ n\ is\ a\ positive\ integer$

$since\ a \in H \Rightarrow a \in G$

$We\ know\ that\ the\ order\ of\ every\ element\ of\ a\ finite\ group\ G\ is\ also\ finite.$

$It\ follows\ that\ order\ of\ 'a'\ be\ n\ \ i.e. o(a) = n \Rightarrow a^n = e$

$where\ n\ is\ a\ least\ positive\ integer$

$\therefore a^n \in H \Rightarrow e \in H\ \therefore e\ is\ the\ identity\ element.$

$(iv)\ since\ n > 0 \Rightarrow n - 1 \geq 0 \Rightarrow a^{n-1} \in H$

$Let\ a \in H,$

$Now\ a.a^{n-1} = a^n = e$

$\therefore a^{n-1}$ *is the iverse of* $'a'$

Each element in H *has multiplicative inverse .*

Hence $(H,\cdot)$*is a group*

Theorem11: ***If*** H, ***are two subgroups of a group*** G ***then*** HK ***is a subgroup of*** G

$\Leftrightarrow HK = KH$

Necessary condition ($\Longrightarrow$): *Given that* H, *are two subgroups of a group* G *such that* HK *is a subgroup of* G.

To prove that $HK = KH$

since HK *is a subgroup of* $G \Longrightarrow (HK)^{-1} = HK$ $\quad (\because H < G \Longrightarrow H^{-1} = H)$

$\Longrightarrow K^{-1}H^{-1} = HK$ $\quad (\because K < G \Longrightarrow K^{-1} = K)$

$\Longrightarrow KH = HK$

$\therefore HK = KH$

Sufficient condition ($\Longleftarrow$): *Conversely given that* H, K *are two subgroups of a group* G *such that* $HK = KH$

To prove that HK *is a sbgroup of* G. *For this we have to show that* $(HK)(HK)^{-1} = HK$

Now $(HK)(HK)^{-1} = HK(K^{-1}H^{-1})$

$= [(HK)^{-1}]H^{-1}$

$= [(KK^{-1})]^{-1}$

$= (HK)^{-1}$ $\quad (\because K < G \Longrightarrow KK^{-1} = K)$

$= (KH)^{-1}$ $\quad (\because HK = KH)$

$= (HH^{-1})$

$= KH$ $\quad (\because H < G \Longrightarrow HH^{-1} = H)$

$= HK$

$\therefore (HK)(HK)^{-1} = HK$

$\therefore HK$ *is a sbgroup of* G

Theorem12: The intersection of two subgroups of a group G is also a subgroup of G

Proof: $Let\ H, K\ are\ two\ subgroups\ of\ a\ group\ G$

$To\ prove\ that\ \ H \cap K\ is\ a\ subgroup\ of\ G$

$(i) since\ H, K\ are\ two\ subgroups\ of\ G$

$\therefore\ e \in H\ and\ e \in K \Longrightarrow e \in H \cap K\ \Longrightarrow H \cap K\ \neq \emptyset$

$(ii)\ Clearly\ H \cap K\ \subseteq G\ \ (\because H \subseteq G, K \subseteq G)$

$(iii)\ Let\ a, b \in H \cap K\ \Longrightarrow a, b \in H\ and\ a, b \in K$

$Since\ a, b \in H, H\ is\ a\ subgroup\ of\ G \Longrightarrow ab^{-1} \in H$

$also\ since\ a, b \in K, K\ is\ a\ subgroup\ of\ G \Longrightarrow ab^{-1} \in K$

$\therefore ab^{-1} \in H\ and\ ab^{-1} \in K \Longrightarrow ab^{-1} \in H \cap K$

$\therefore H \cap K\ is\ a\ subgroup\ of\ G$

The union of two subgroups of a group G need not be a subgroup of G

Ex: $G = (\mathbb{Z}, +)\ be\ a\ group\ under\ addition.$

$Let\ H = \{\ldots . -6, -4, -2, 0, 2, 4, 6, \ldots\}$

$and\ K = \{\ldots . -9, -6, -3, 0, 3, 6, 9, \ldots\}\ be\ two\ subgroups.$

$H \cup K = \{\ldots -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9, \ldots .\}$

$Let\ 3{,}4 \in H \cup K \Longrightarrow 3 + 4 = 7 \notin H \cup K \Longrightarrow'\ +'$ is not a binary operation on $H \cup K$

$\therefore H \cup K\ is\ not\ subgroup\ of\ G$

$Let\ H = \{\ldots . -6, -4, -2, 0, 2, 4, 6, \ldots\}\ and\ K = \{\ldots ., -8, -4, , 0\ , 4, 8, , \ldots\}\ be\ two\ subgroups.$

$H \cup K = \{\ldots -8, -6, -4, -2, , 0, 2, 4, 6, 8, \ldots .\}$

$Let\ 2, 4 \in H \cup K \Longrightarrow 2 + 4 = 6 \in H \cup K \therefore H \cup K\ is\ a\ subgroup\ of\ G$

Note: $K \subseteq H\ then\ H \cup K\ is\ a\ subgroup\ of\ G$

Theorem13: The union of two subgroups of a group G is a subgroup of $G \Leftrightarrow$ one is contained in other. (OR)

Let H, K are two subgroups of a group G then $H \cup K$ is a subgroup of $G \Leftrightarrow$ $H \subseteq K$ or $K \subseteq H$.

Necessary condition ($\Longrightarrow$): *Let H, K are two subgroups of a group of G such that $H \cup K$ is a subgroup of G*

To prove that $H \subseteq K$ or $K \subseteq H$

If possible suppose that $H \nsubseteq K$ and $K \nsubseteq H$

Since $H \nsubseteq K \Longrightarrow$ so $\exists$ atleast one element $a \in H$ but $a \notin K$

also $K \nsubseteq H \Longrightarrow$ so $\exists$ atleast one element $b \in K$ but $b \notin H$

$\therefore a, b \in H \cup K \quad (\because H \subseteq H \cup K, \quad K \subseteq H \cup K)$

$\Longrightarrow ab \in H \cup K \ (\because H \cup K$ is a subgroup$) \Longrightarrow ab \in H$ or $ab \in K$ or $ab \in H \cap K$

If $ab \in H$:

Since $ab \in H, \in H,$ H is a sub group $\Longrightarrow a^{-1} \in H$

$a^{-1} \in H, ab \in H,$ *H is a subgroup of $G \Longrightarrow a^{-1}(ab) \in H \Longrightarrow b \in H$*

which is a contradict to $b \notin H \therefore ab \notin H$

If $ab \in K$:

since $ab \in K,$ $b \in K, K$ is a sub group $\Longrightarrow b^{-1} \in K$

$ab \in K, b^{-1} \in K,$ *K is a subgroup of $G \Longrightarrow (ab)^{-1} \in K \Longrightarrow a \in K$*

which is a contradict to $a \notin K \therefore ab \notin K$

$\therefore ab \notin H$ and $ab \notin K \Longrightarrow ab \notin H \cap K$ which is a contradict to $ab \in H \cap K$

Hence our supposition is wrong

Thus $H \subseteq K$ or $K \subseteq H$

Sufficient condition ($\Longleftarrow$): *Conversely given that H, K are subgroups of G such that $H \subseteq K$ or $K \subseteq H$*

$To\ prove\ that\ H \cup K\ is\ a\ subgroup\ of\ G$

$Since\ H \subseteq K \implies H \cup K = K\ since\ K\ is\ a\ subgroup$

$\implies H \cup K\ is\ a\ subgroup\ of\ G$

$Also\ K \subseteq H \implies H \cup K = H$

$Since\ H\ is\ a\ subgroup \implies H \cup K\ is\ a\ subgroup\ of\ G$

Ex: 1. ***Let H be a subgroup of G and Let*** $T = \{x \in G / xH = Hx\}$

show that T is a subgroup of G

Proof: $T = \{x \in G / xH = Hx\}$

$To\ prove\ that\ T is\ a\ subgroup\ of\ G$

$(i)\ since\ e \in G, \quad we\ have\ eH = He$

$\therefore e \in T \implies T \neq \emptyset$

$(ii)\ clearly\ T \subseteq G\ (by\ \text{def}\ of\ T)$

$(iii)\ Let\ x, y \in T\ then\ xH = xH\ and\ Hy = yH$

$To\ prove\ that\ xy^{-1} \in T\ For\ this\ we\ have\ to\ show\ that\ (xy^{-1}) = (xy^{-1})$

$First\ we\ prove\ that\ y^{-1} \in T$

$since\ Hy = yH$

$\implies y^{-1}(Hy)y^{-1} = y^{-1}(yH)y^{-1}$

$\implies y^{-1}(yy^{-1}) = (y^{-1}y)Hy^{-1}$

$\implies y^{-1}H = Hy^{-1}$

$\implies y^{-1} \in T$

$Now\ (xy^{-1}) = (Hx)^{-1}$

$= (xH)^{-1}$

$= (Hy^{-1})$

$= (y^{-1}H)$

$= (xy^{-1})$

$\therefore (xy^{-1}) = (xy^{-1}) \Longrightarrow xy^{-1} \in T$

$\therefore T is a subgroup of G$

2. If H is a subgroup of a group G and if $g \in G$ and $gHg^{-1} = \{ghg^{-1}/h \in H\}$ then prove that gHg^{-1} is asubgroup of G.

proof: $Given\ H\ is\ a\ subgroup\ of\ a\ group\ G\ and\ gHg^{-1} = \{ghg^{-1}/h \in H\}$

$To\ prove\ that\ \ gHg^{-1}\ is\ a\ subgroup\ of\ G$

$(i)\ since\ e \in H,\qquad we\ have\ \ geg^{-1} \in gHg^{-1} \Longrightarrow gHg^{-1} \neq \phi$

$(ii)\ clearly\ \ gHg^{-1} \subseteq H\quad (by\ \text{def}\ of\ gHg^{-1})$

$(iii)\ Let\ x, y \in gHg^{-1}\ then\ x = gh_1g^{-1},\ \ y = \ gh_2g^{-1}\ where\ h_1, h_2 \in H$

$To\ prove\ that\ xy^{-1} \in gHg^{-1}$

$Now\ xy^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1}$

$= (gh_1g^{-1})(gh_2{}^{-1}g^{-1})$

$= gh_1(g^{-1}g)h_2{}^{-1}g^{-1}$

$= gh_1h_2{}^{-1}g^{-1}$

$= (h_1h_2{}^{-1})^{-1}$

$= gHg^{-1}\qquad (\because h_1h_2{}^{-1} \in H)$

$\therefore\ xy^{-1} \in gHg^{-1}$

$\therefore gHg^{-1}\ is\ asubgroup\ of\ G$

CO-SETS & LAGRANGE'S THEOREM

Co-set (def): Let $(H,\cdot)$ be a subgroup of $(G,\cdot)$ and $a \in G$ then the set $Ha = \{ha/h \in H\}$ is called as right co-set of H in G generated by $'a'$ and the set $aH = \{a\,h/h \in H\}$ is called as left co-set of H in G generated by $'a'$ and it is called as co-set of H in G generated by $'a'$.

Note:

1.For addition, we have $H + a = \{h + a/h \in H\}$ is called as right co-set of H in G generated by $'a'$ and the set $a + H = \{a + h/h \in H\}$ is called as left co-set of H in G generated by $'a'$ and it is called as co-set of H in G generated by $'a'$.

2. If e is the identity element of G and $H < G$ then $eH = \{eh/h \in H\} = \{h/h \in H\} = H$ And $He = \{he/h \in H\} = \{h/h \in H\} = H$

3. Every subgroup H of G itself is a left and right co-sets of H in G

Ex: 1. Find the distinct right or left co-sets of $H = \{0,,4\}$ in Z_6 under $+_6$

Sol: $Z_6 = \{0,1,2,3,4,5\}, under\ +_6\ is\ a\ group\ and\ H = \{0,2,4\}$

$Clearly\ H\ is\ \ a\ subgroup\ of\ G\ since\ a = 0 \in\ ,H = \{0,2,4\}$

$(i)H + 0 = \{h +_6 0/h \in H\} = \{0,2,4\} = H$ $(ii)H + 1 = \{h +_6 1/h \in H\} = \{1,3,5\}$

$(iii)H + 2 = \{h +_6 2/h \in H\} = \{2,4,0\}$ $(iv)H + 3 = \{h +_6 3/h \in H\} = \{3,5,1\}$

$(v)H + 4 = \{h +_6 4/h \in H\} = \{4,0,2\}$ $(vi)H + 5 = \{h +_6 5/h \in H\} = \{5,3,1\}$

$\therefore\ H + 0,\quad H + 1\ are\ distinct\ right/left\ cosets\ of\ H\ in\ G$

2. Find the distinct right or left co-sets of $H = \{1,4\}$ Z_5 under $\times_5$

Sol: $Z_5 = \{1,2,3,4\}, under\ \times_5\ is\ a\ group\ and\ H = \{1,4\}$

$Clearly\ H\ is\ \ a\ subgroup\ of\ G\ since\ a = 1 \in\ ,H = \{1,4\}$

$(i)H1 = \{h \times_5 1/h \in H\} = \{1,4\} = H$ $(ii)H2 = \{h \times_5 2/h \in H\} = \{2,3\}$

$(iii)H3 = \{h \times_5 3/h \in H\} = \{3,2\}$ $(iv)H4 = \{h \times_5 4/h \in H\} = \{4,1\}$

$\therefore\ H1,\quad H2\ are\ distinct\ right/left\ cosets\ of\ H\ in\ G$

Note: $1.The\ number\ of\ distinct\ right\ or\ left\ cosets\ of\ H\ in\ G = \frac{o(G)}{(H)}$

$2.Every\ right\ or\ left\ cosets\ of\ H\ in\ G\ have\ the\ same\ number\ of\ elements.i.e\ (Ha) = (Hb)$

3. $G = Ha \cup Hb$

Theorem1: ***Let H be a subgroup of G and $h \in G$ then $h \in H \Leftrightarrow Hh = H = hH$***

Necessary condition ($\Longrightarrow$): *Given that H is a subgroup of G and $h \in G$ such that $h \in H$*

To prove that $Hh = H = hH \quad (Hh \subseteq H, H \subseteq Hh)$

Let $x \in Hh$ *then* $x = h_1 h \quad where\ h_1 \in H$

since $h_1 \in H, \quad h \in H, \quad H$ *is a subgroup of* $G \Longrightarrow h_1 h \in H \Longrightarrow x \in H$

$\therefore Hh \subseteq H \rightarrow (1)$

Let $h_2 \in H$ *and e be the identity element in G*

Since H is a subgroup of G so $e \in H$

Now $h_2 = h_2 e = h_2(h^{-1}h) = (h_2 h^{-1})h \in Hh \quad (\because h_2 \in H, h^{-1} \in H, H < G \text{ so } h_2 h^{-1} \in H)$

$\therefore H \subseteq Hh \rightarrow (2)$

From (1) (2) $Hh = H$

Next to prove that $hH = H \ (hH \subseteq H \ , H \subseteq hH)$

Let $y \in hH$ *then* $y = hh_3 \quad where\ h_3 \in H$

since $h_3 \in H, \quad h \in H, \quad H$ *is a subgroup of* $G \Longrightarrow hh_3 \in H \Longrightarrow y \in H$

$\therefore hH \subseteq H \rightarrow (3)$

Let $h_4 \in H$ *and e be the identity element in G*

since H is a subgroup of G so $e \in H$

Now $h_4 = eh_4 = (hh^{-1})h_4 = h(h^{-1}h_4) \in hH \quad (\because h^{-1} \in H, h_4 \in H, H < G \text{ so } h^{-1}h_4 \in H)$

$\therefore H \subseteq hH \rightarrow (4)$

From (3) (4) $hH = H$

Sufficient condition ($\Longleftarrow$): *Conversely given that H is a subgroup of G and*

$h \in G$ *such that* $Hh = H = hH$

To prove that $h \in H$

Let e be the identity element in G

$since\ H\ is\ a\ subgroup\ of\ G\ so\ e \in H$

$Now\ h = he \in hH \Longrightarrow h \in hH \Longrightarrow h \in H \quad (\because H = hH)$

$Next\ \ h = eh \in Hh = H \Longrightarrow h \in H$

Theorem2: ***If a and b are two elements of a group G and H is a subgroup of G then*** $(i)Ha = Hb \Leftrightarrow ab^{-1} \in H \quad (ii)aH = bH \Leftrightarrow a^{-1}b \in H$

(i) N.C (⟹): $Given\ that\ H\ is\ a\ sub\ group\ of\ G\ such\ that\ Ha = Hb$

$To\ prove\ that\ ab^{-1} \in H$

$Let\ e\ be\ the\ identity\ element\ of\ G\ since\ H < G\ so\ e \in H$

$Now\ Ha = Hb \Longrightarrow Hab^{-1} = Hbb^{-1}$

$\Longrightarrow Hab^{-1} = He = H$

$\Longrightarrow Hab^{-1} = H$

$\Longrightarrow ab^{-1} \in H \qquad (\because H < G, Hh = H \Leftrightarrow h \in H)$

S.C (⟸): $Conversely\ given\ that\ H\ is\ a\ subgroup\ of\ G\ such\ that\ ab^{-1} \in H$

$To\ prove\ that\ Ha = Hb$

$since\ ab^{-1} \in H \Longrightarrow Hab^{-1} = H$

$\Longrightarrow Hab^{-1}b = Hb$

$\Longrightarrow Ha = Hb$

(ii) N.C (⟹): $Given\ that\ H\ is\ a\ subgroup\ of\ G\ such\ that\ aH = bH$

$To\ prove\ that\ a^{-1}b \in H$

$Let\ e\ be\ the\ identity\ element\ of\ G\ since\ H < G\ so\ e \in H$

$Now\ aH = bH \Longrightarrow a^{-1}aH = a^{-1}bH$

$\Longrightarrow H = a^{-1}bH$

$\Longrightarrow a^{-1}bH = H$

$\Longrightarrow a^{-1}b \in H \qquad (\because H < G, hH = H \Leftrightarrow h \in H)$

S.C (⟸): $Conversely\ given\ that\ H\ is\ a\ subgroup\ of\ G\ such\ that\ a^{-1}b \in H$

$To\ prove\ that\ aH = bH$

$since\ a^{-1}b \in H \Longrightarrow a^{-1}bH = H$

$\Longrightarrow aa^{-1}bH = aH$

$\Longrightarrow bH = aH$

Theorem3: ***If a and b are two elements of a group G and H is a subgroup of G then*** $(i)a \in Hb \Leftrightarrow Ha = Hb$ $(ii)a \in bH \Leftrightarrow aH = bH$

(i) N.C (⟹): $Given\ that\ H\ is\ a\ subgroup\ of\ G\ such\ that\ a \in Hb$

$To\ prove\ that\ Ha = Hb$

$since\ a \in Hb \Longrightarrow ab^{-1} \in Hbb^{-1}$

$\Longrightarrow ab^{-1} \in He$

$\Longrightarrow ab^{-1} \in H \qquad (\because H < G, Hh = H \Leftrightarrow h \in H)$

$\Longrightarrow Ha = Hb$

S.C (⟸): $Conversely\ given\ that\ H\ is\ a\ subgroup\ of\ G\ such\ that\ Ha = Hb$

$To\ prove\ that\ a \in Hb$

$Let\ e \in G, since\ H < G \therefore e \in H$

$Now\ a = ea \in Ha$

$\Longrightarrow a \in Ha$

$\Longrightarrow a \in Hb \quad (\because Ha = Hb)$

(ii) N.C (⟹): $Given\ that\ H\ is\ a\ subgroup\ of\ G\ such\ that\ a \in bH$

$To\ prove\ that\ aH = bH$

$since\ a \in bH \Longrightarrow b^{-1}a \in b^{-1}bH$

$\Longrightarrow b^{-1}a \in eH$

$\Longrightarrow b^{-1}a \in H \qquad (\because H < G, hH = H \Leftrightarrow h \in H)$

$\Longrightarrow aH = bH$

S.C (⟸): $Conversely\ given\ that\ H\ is\ a\ subgroup\ of\ G\ such\ that\ aH = bH$

$To\ prove\ that\ a \in bH$

$Let\ e \in G, since\ H < G\ \therefore e \in H$

$Now\ a = ae \in aH$

$\Longrightarrow a \in aH$

$\Longrightarrow a \in bH \quad (\because aH = bH)$

Theorem4: ***Let H be a subgroup of G then there exist a bijection between any two left or right cosets of H in G*** **(OR)**

Let H be a subgroup of G then there exist one − one correspondance between any two left or right coset of H in G.

Proof: $Let\ H\ be\ a\ subgroup\ .For\ any\ a, b \in G.$

$Let\ aH, bH\ be\ two\ left\ cosets\ of\ H\ in\ G$

$Define\ a\ mapping\ f: aH \to bH\ by\ f(ah) = bh \quad \forall ah \in aH$

(i) f is one − one and well − define: $Let\ ah_1, ah_2 \in aH\ such\ that\ (ah_1) = (ah_2)$

$To\ prove\ that\ \ ah_1 = ah_2$

$since\ (ah_1) = (ah_2) \Leftrightarrow bh_1 = bh_2$

$\Leftrightarrow h_1 = h_2$

$\Leftrightarrow ah_1 = ah_2$

$\therefore f\ is\ one - one\ and\ well - defined$

(ii) f is on − to: $Let\ bh \in bH\ then\ h \in H$

$For\ this\ h \in H, we\ have\ ah \in aH \Longrightarrow f(ah) = bh$

$\therefore \forall bh \in bH\ so\ \exists\ ah \in aH\ such\ that\ f(ah) = bh$

$\therefore \quad f\ is\ on - to$

$Thus\ f\ is\ bijective.$

Theorem5: ***Let H be a subgroup of Gthen there is one − one correspondance between the set of all distinct left cosets of H in G and the set ofall distinct***

right cosets of H in G.

Proof: *Let H be a subgroup of G. For any $a, b \in G$.*

Let Ha, Hb be two right cosets of H in G

Let G_1 be the set of all distinct left cosets of H in G.

Let G_2 be the set of all distinct rihgt cosets of H in G.

Define a mapping $f: G_1 \to G_2$ by $(aH) = Ha^{-1} \quad \forall aH \in G_1$

(i) f is one − one and well − define: *Let $aH, \in G_1$ such that $(aH) = f(bH)$*

To prove that $aH = bH$

$since\ (aH) = (bH) \Leftrightarrow Ha^{-1} = Hb^{-1}$

$\Leftrightarrow a^{-1}(b^{-1})^{-1} \in H \quad (\because Ha = Hb \Leftrightarrow ab^{-1} \in H\ )$

$\Leftrightarrow a^{-1}b \in H$

$\Leftrightarrow a^{-1}bH = H$

$\Leftrightarrow aa^{-1}bH = aH$

$\Leftrightarrow bH = aH$

$\Leftrightarrow aH = bH$

$\therefore f\ is\ one - one\ and\ well - defined$

(ii) f is on − to: *Let $Ha \in G_2$ then $a \in G \Longrightarrow a^{-1} \in G \Longrightarrow a^{-1}H \in G_1$*

For this $a^{-1}H \in G_1 \Longrightarrow (a^{-1}H) = (a^{-1})^{-1} = Ha$

$\therefore \forall\ Ha \in G_2 so\ \exists\ a^{-1}H \in G_1 such\ that\ (a^{-1}H) = Ha$

$\therefore\ \ f\ is\ on - to$

Thus f is bijective.

Index of a subgroup of a finite group: -If H is a subgroup of a group G then the number of distinct left/right co-sets of H in G is called as index of H in G and it is denoted by $[G: H]$ or $i_G(H)$

LAGRANGE'S THEOREM: The order of a subgroup of a finite group divides the order of a group. (OR)

If H is any subgroup of a finite group G then $(H)|o(G)$. *Is the converse true? justify your answer?*

Proof: Given that H is any subgroup of a finite group G

$\therefore$ H is also finite.

To prove that $(H)|o(G)$

If $H = G \Longrightarrow (H) = (G) \Longrightarrow (H)|o(G)$

If $H \neq G$ to prove that $(H)|o(G)$

Let $(G) = n$ and $(H) = m$ to prove that $m|n$

We know that every right/left co-set of H in G has the same number of elements and the number of right co-sets of H in G is also finite and also $H = He$, H is also right co-set of H in G.

If Ha, Hb, Hc ... ... H are right co-sets of H in G (n terms) then $(Ha) = (Hb) = (Hc) = \cdots = o(H) = m$

Let the number of distinct right co-sets of H in G be k and all these right co-sets of H in G are disjoint.

$\therefore G = Ha \cup Hb \cup Hc \cup \ldots . \cup H(k\ times) \Longrightarrow o(G) = o(Ha) + o(Hb) + o(Hc) + \cdots + o(H)$

$\Longrightarrow n = m + m + m + .. + m(\ k\ times) \Longrightarrow n = mk \Longrightarrow k = \frac{n}{m}$

$\therefore m|n \Longrightarrow o(H)|o(G)$

Hence the order of a subgroup of a finite group divides the order of a group

The converse of this theorem need not be true i.e. if G is a finite group and $(H)|o(G)$ then H need not be a subgroup.

For example: Consider $G = \{1, -1, i, -i\}\ so\ o(G) = 4 \therefore$

Let $H = \{i, -i\} hen\ o(H) = 2$

Clearly $(H)|o(G)$ $(2|4)$

But H is not a group as $(i) = -1 \notin H$

$\therefore H\ is\ not\ a\ subgroup\ of\ G$

Theorem7: *If G is a finite group and $a \in G$ then $(a)|o(G)$*

Proof: G *is a finite group and* $a \in G$.

Let $o(a) = n$

we know that G *is a finite group and* $a \in G$ *such that* $o(a) = n$

then $H = \{e = a^0, ^1, a^2, \dots a^{n-1}\}$ *form a group under multiplication.*

Hence H *is a subgroup of* G *such that* $o(H) = n$

By Lagrange's theorem $o(H)|o(G) \Longrightarrow n|o(G) \Longrightarrow o(a)|o(G)$

Theorem8: ***If a is an element of a finite group G then*** $^{(G)} = e$ $(or)^{|G|} = e$

(OR)

If G is a finite group of order n and if $a \in G$ ***then*** $a^n = e$ $(or)a^{|G|} = e$

Proof: *Given* G *is a finite group of order* n *i.e.* $o(G) = n$

Let $o(a) = d \Longrightarrow a^d = e$ *and since* $o(a) \leq o(G)$ $(since\ G\ is\ finite)$

we know that G *is a finite group and* $a \in G$ *such that* $o(a) = d$ *then*

$H = \{e = a^0, a^1, a^2, \dots ^{-1}\}$ *form a group under multiplication.*

Hence H *is a subgroup of* G *such that* $o(H) = d$

By Lagrange's theorem $o(H)|o(G) \Longrightarrow d|o(G) \Longrightarrow d|n \Longrightarrow n = kd$ *forsome* $k \in \mathbb{N}$

Now $a^n = a^{kd} = (a^d)^k = e^k = e$

$\therefore a^n = e$ $(or)a^{|G|} = e$

Theorem9: ***Every group of prime order has no proper subgroups.***

Proof: *Let* G *be a group such that* $(G) = p$ *where* p *is aprime.*

Let H *be subgroup of* G *such that* $o(H) = m$

By Lagranges theorem $o(H)|o(G) \Longrightarrow m|p$

Since p *is a prime so* $m = 1$ *or* $m = p$

$\Longrightarrow (H) = 1$ *or* $(H) = (G) \Longrightarrow H = \{e\}$ *or* $H = G$

These are improper or trivial subgroup.

i.e. G *has only improper subgroups*

Thus G has no proper subgroups

Normalizer of an element: *Let G be a group and $a \in G$ then the set of all elements in G which are commutes with an element of $'a'$ in G and it is denoted by $N(a)$*

i.e. $N(a) = \{x \in G / ax = xa\}$

Centre of a group: *Let G be a group and $a \in G$ then the set of all elements in G which are commutes with every element of G and it is denoted by $C(G)$ or $Z(G)$*

i.e. $C(G) = \{x \in G / ax = xa \ \forall a \in G\}$

Theorem 10: ***Let G be a group and $a \in G$ then (a) a subgroup of G***

Proof: $(a) = \{x \in G / ax = xa\}$

To prove that $N(a)$ is a subgroup of G

(i) *Since* $e \in G$, *we have* $ae = ea$

$\therefore e \in N(a) \Longrightarrow N(a) \neq \emptyset$

(ii) *Clearly* $(a) \subseteq G$ *(by def of* (a)*)*

(iii) *Let* $x, y \in N(a)$ *then* $ax = xa$ *and* $ay = ya$

To prove that $xy^{-1} \in (a)$.

For this we have to show that $(xy^{-1}) = (xy^{-1})$

First we prove that $y^{-1} \in (a)$

since $ay = ya$

$\Longrightarrow y^{-1}(ay)y^{-1} = y^{-1}(ya)y^{-1}$

$\Longrightarrow y^{-1}(yy^{-1}) = (y^{-1}y)ay^{-1}$

$\Longrightarrow y^{-1}a = ay^{-1}$

$\Longrightarrow y^{-1} \in (a)$

Now $(xy^{-1}) = (ax)^{-1}$

$= (xa)^{-1}$

$= (ay^{-1})$

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

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

$\therefore (xy^{-1}) = (xy^{-1}) \Longrightarrow xy^{-1} \in (a)$

$\therefore N(a)\ is\ a\ subgroup\ of\ G$

UNIT-3: NORMAL SUBGROUPS

Normal subgroup (def): -A subgroup $H$of a group is said to be a normal subgroup G if $\forall h \in H$and $\forall x \in G \Longrightarrow xhx^{-1} \in H$. It is denoted by $H \rhd G$ we read it as H is a normal subgroup of G

Note: From the def of normal subgroup. We observe that

1.$H \rhd G \Leftrightarrow xHx^{-1} \subseteq H, \forall x \in G \quad (\because xHx^{-1} = \{xhx^{-1}/h \in H\})$

2.$H \rhd G \Leftrightarrow x^{-1}Hx \subseteq H, \forall x \in G \qquad (\because x \in G \Longrightarrow x^{-1} \in G, \rhd G)$

3. Every group contains at least two normal subgroups {e} and G itself is called as improper or trivial normal subgroups of G. If any other normal subgroups exist then it is called as proper or non-trivial normal subgroups.

Theorem1: ***A subgroup H of group G is a normal subgroup of G*** $\Leftrightarrow$

$\boldsymbol{xHx^{-1} = H \; \forall x \in G}$

N.C ($\Longrightarrow$): $Given\ that\ H\ is\ a\ normal\ subgroup\ of\ G$

$To\ prove\ that\ xHx^{-1} = H \; \forall x \in G$

$Since\ H\ is\ normal\ subgroup\ of\ G \Longrightarrow xHx^{-1} \subseteq H, \qquad \forall x \in G \rightarrow (1)$

$since \quad xHx^{-1} \subseteq H, \qquad \forall x \in G$

$\Longrightarrow x^{-1}(x^{-1})^{-1} \subseteq H, \; \forall x \in G$

$\Longrightarrow x^{-1}Hx \subseteq H, \; \forall x \in G$

$\Longrightarrow (x^{-1}Hx)^{-1} \subseteq xHx^{-1}, \; \forall x \in G$

$\Longrightarrow (^{-1})H(xx^{-1}) \subseteq xHx^{-1}, \; \forall x \in G$

$\Longrightarrow H \subseteq xHx^{-1}, \; \forall x \in G \rightarrow (2)$

$From\ (1)\ (2) \quad xHx^{-1} = H \qquad \forall x \in G$

S.C ($\Longleftarrow$): $Conversely\ given\ that\ H\ is\ a\ subgroup\ of\ G\ such\ that\ xHx^{-1} = H \quad \forall x \in G$

$To\ prove\ that\ His\ a\ normal\ subgroup\ of\ G$

$since\ xHx^{-1} = H \quad \forall x \in G \Longrightarrow x^{-1}Hx \subseteq H \;\; and \;\; H \subseteq xHx^{-1} \quad \forall x \in G$

$x^{-1}Hx \subseteq \; , \forall x \in G \Longrightarrow H\ is\ a\ normal\ subgroup\ of\ G$

Theorem2: ***A subgroup H of a group G is a normal subgroup of G $\Leftrightarrow$ each left coset of H in G is a right coset of H in G***

N.C ($\Longrightarrow$): *Given that H is a normal subgroup of G*

To prove that each left coset of H in G is a right coset of H in G

Since H is normal subgroup of G $\Longrightarrow xHx^{-1} = H, \quad \forall x \in G$

$$\Longrightarrow (xHx^{-1}) = Hx, \ \forall x \in G$$

$$\Longrightarrow (xH)^{-1}x = Hx, \ \forall x \in G$$

$$\Longrightarrow xH = Hx, \ \forall x \in G$$

S.C ($\Longleftarrow$): *Conversely given that H is a subgroup of G such that each left coset of H in G is a right coset of H in G*

To prove that His a normal subgroup of G

Let $x \in G$ then $xH = Hy$ for some $y \in H$

since $e \in H$, so $x = xe \in xH$

$$\Longrightarrow x \in xH$$

$$\Longrightarrow x \in Hy \quad (\therefore xH = Hy)$$

$$\Longrightarrow xy^{-1} \in Hyy^{-1}$$

$$\Longrightarrow xy^{-1} \in H$$

$$\Longrightarrow Hx = Hy$$

$$\Longrightarrow Hx = xH$$

$$\Longrightarrow Hxx^{-1} = xHx^{-1}$$

$$\Longrightarrow H = xHx^{-1}$$

$$\Longrightarrow xHx^{-1} = H \ \forall x \in G$$

$\therefore$ *His a normal subgroup of G*

Theorem3: ***A subgroup H of a group G is a normal subgroup of G ⇔***

The product of two right cosets of H in G is again a right coset of H in G

N.C (⟹): $Given\ that\ H\ is\ a\ normal\ subgroup\ of\ G$

$To\ prove\ that\ the\ product\ of\ two\ right\ cosets\ of\ H\ in\ G\ is\ again$

$a\ right\ coset\ of\ H\ in\ G\ .$

$For\ any\ a,b \in G\ then\ Ha, Hb\ be\ two\ right\ cosets\ of\ H\ in\ G.$

$$Now\ (Ha)(Hb) = H(aH)b$$

$$= H(Ha)b \qquad (\because H \rhd G \Leftrightarrow Ha = aH\ )$$

$$= HHab$$

$$= Hab \qquad (\because H < G then\ HH = H\ )$$

$since\ a \in G, b \in G \Longrightarrow ab \in G$

$\therefore Hab\ is\ a\ right\ coset\ of\ H\ in\ G$

S.C (⟸): $Conversely\ given\ that\ H\ is\ a\ subgroup\ of\ G\ such\ that\ the\ product\ of$

$two\ right\ cosets\ of\ H\ in\ G\ is\ again\ a\ right\ coset\ of\ H\ in\ G$

$To\ prove\ that\ H\ is\ a\ normal\ subgroup\ of\ G\ i.e. \forall h \in H, \forall x \in G \Longrightarrow xhx^{-1} \in H$

$Let\ h \in H\ and\ x \in G$

$$Now\ \ xhx^{-1} = (hx^{-1}) \in HxHx^{-1}$$

$$\Longrightarrow xhx^{-1} \in HxHx^{-1}$$

$$\Longrightarrow xhx^{-1} \in Hxx^{-1} \qquad (\because Ha \cdot Hb = Hab\ )$$

$$\Longrightarrow xhx^{-1} \in He$$

$$\Longrightarrow xhx^{-1} \in H$$

$\therefore \forall h \in H, \forall x \in G \Longrightarrow xhx^{-1} \in H$

$Thus\ H\ is\ a\ normal\ subgroup\ of\ G$

Theorem4: Every subgroup of an abelian is always normal subgroup

Proof: Let G be an abelian group and H be a subgroup

To prove that H is a normal subgroup of G (i.e.$\forall h \in H, \forall x \in G \Longrightarrow xhx^{-1} \in H$)

Let $h \in H,\ and\ x \in G$

$xhx^{-1} = (x^{-1}h)$ $(\because x \in G \Longrightarrow x^{-1} \in G, h \in H \Longrightarrow h \in G \Longrightarrow h^{-1}x = x^{-1}h, G\ is\ abelian)$

$= (xx^{-1})h$

$= eh$

$= h \in H$

$\therefore xhx^{-1} \in H$ $\therefore$ H is a normal subgroup of G

Theorem5: The intersection of any two normal subgroups of a group is a normal subgroup

(OR)

Let H, K be two normal subgroups of a group$G$ then $H \cap K$ is also normal subgroup of G.

Proof: $Let\ H,\ are\ two\ normal\ subgroups\ of\ a\ group\ G$

$To\ prove\ that\ H \cap K\ is\ a\ normal\ subgroup\ of\ G$

$(i) Since\ H, K\ are\ two\ subgroups\ of\ G$

$\therefore\ e \in H\ and\ e \in K \Longrightarrow e \in H \cap K\ \Longrightarrow H \cap K\ \neq \phi$

$(ii) Clearly\ H \cap K\ \subseteq G\ (\because H \subseteq G, K \subseteq G)$

$(iii)\ Let\ a, b \in H \cap K\ \Longrightarrow a, b \in H\ and\ a, b \in K$

$Since\ a, b \in H, H\ is\ a\ subgroup\ of\ G \Longrightarrow ab^{-1} \in H$

$also\ since\ a, b \in K, K\ is\ a\ subgroup\ of\ G \Longrightarrow ab^{-1} \in K$

$\therefore ab^{-1} \in H\ and\ ab^{-1} \in K \Longrightarrow ab^{-1} \in H \cap K$

$\therefore H \cap K\ is\ a\ subgroup\ of\ G$

$Let\ x \in G, y \in H \cap K\ \Longrightarrow y \in H\ and\ y \in K$

$since\ x \in G, y \in\ ,\ \triangleright\ G \Longrightarrow xyx^{-1} \in H$

$Also\ x \in G, y \in\ ,\ \triangleright G \Longrightarrow xyx^{-1} \in K$

$\therefore xyx^{-1} \in H \cap K \quad \forall x \in G, \quad \forall y \in H \cap K$

$\therefore H \cap K\ is\ a\ normal\ subgroup\ of\ G$

Theorem6: ***Let N and M be normal subgroups of a groupG then NM is a normal subgroup of G.***

Proof: $Since\ N\ is\ a\ normal\ subgroup\ of\ G,\ have\ Na = aN \quad \forall a \in G$

$In\ particular\ for\ any\ a \in M\ , \qquad NM = MN\ and$

$hence\ NM\ is\ a\ subgroup\ of\ G \qquad (\because H < G, K < G\ then\ HK < G \Leftrightarrow HK = KH)$

$For\ any\ a \in G, we\ have$

$$(NM)a = N(Ma)$$

$$= N(aM) \qquad (\because M\ is\ a\ normal\ )$$

$$= (Na)M$$

$$= (aN)M \qquad (\because N\ is\ a\ normal\ )$$

$$= a(NM)$$

$\therefore\ (NM)a = a(NM) \Longrightarrow NM\ is\ a\ normal\ subgroup\ of\ G$

Theorem7: If *G* is a group and *H* is a subgroup of index 2 in *G* then *H* is a normal subgroup of *G*. **(OR)**

Let H be a subgroup of a group G such that there are exactly two left cosets of H in G then prove that every right coset of H in G is a left coset and vice − versa

Proof: $Given\ that\ H\ is\ a\ subgroup\ of\ index\ 2$

$\therefore The\ number\ of\ distinct\ right\ or\ left\ cosets\ of\ H\ in\ G\ is\ 2$

$To\ prove\ that\ H\ is\ a\ normal\ subgroup\ of\ G.$

$For\ this\ we\ have\ to\ show\ that\ \ xH = Hx \quad \forall x \in G$

$Let\ x \in G$

$If\ x \in H\ then\ xH = Hx\ (H < G, h \in H \Leftrightarrow hH = Hh = H)$

$\therefore H\ is\ a\ normal\ subgroup\ of\ G$

$If x \notin H\ then\ xH \neq H \neq Hx\ (\ h \notin H \Leftrightarrow hH \neq Hh \neq H)$

$Since\ index\ of\ H\ in\ G\ is\ 2$

$\therefore G = xH \cup H = Hx \cup H$

$= There\ is\ no\ element\ in\ common\ Hx\ and\ H\ also\ xH\ and\ H$

$\therefore We\ must\ have\ Hx = xH \Longrightarrow H\ is\ a\ normal\ subgroup\ of\ G$

Simple group: A group G is said to be simple if it has no proper normal subgroups.

Theorem8: Every group of prime order is simple

Proof: $Let\ G\ be\ a\ group\ such\ that\ (G) = p\ where\ p\ is\ aprime.$

$Let\ H\ be\ subgroup\ of\ G\ such\ that\ o(H) = m$

$By\ Lagranges\ theorem\ o(H)|o(G) \Longrightarrow m|p$

$Since\ p\ is\ a\ prime\ so\ m = 1\ or\ m = p$

$\Longrightarrow (H) = 1\ or\ (H) = (G) \Longrightarrow H = \{e\}\ or\ H = G$

$These\ are\ improper\ or\ trivial\ \ normal\ subgroup.$

$i.e.\ G\ has\ only\ improper\ normal\ subgroups$

$Thus\ G\ has\ no\ proper\ normal\ subgroups$

$Thus\ G\ is\ a\ simple\ group.$

Centre of a group: $Let\ G\ be\ a\ group\ and\ a \in G\ then\ the\ set\ of\ all\ elements\ in\ G$

$which\ are\ commutes\ with\ every\ element\ of\ \ G\ and\ it\ is\ denoted\ by\ C(G)\ or\ Z(G)$

$i.e. C(G) = \{x \in G / ax = xa\ \ \forall a \in G\}$

Theorem9: $\boldsymbol{Let\ G\ be\ a\ group\ and\ a \in G\ then\ (G)\ is\ a\ normal\ subgroup\ of\ G}$

Proof: $(G) = \{x \in G / ax = xa\ \ \forall a \in G\}$

$To\ prove\ that\ C(G)\ is\ a\ normal\ subgroup\ of\ G$

$(i) Since\ \ e \in G,\qquad we\ have\ \ ae = ea\ \ \ \forall a \in G$

$\therefore e \in C(G) \Longrightarrow C(G) \neq \phi$

$(ii) Clearly\ (G) \subseteq G\ (by \text{ def } of\ (G))$

$(iii) Let\ x, y \in C(G)\ then\ ax = xa\ and\ ay = ya$

$To\ prove\ that\ xy^{-1} \in (G)$

$For\ this\ we\ have\ to\ show\ that\ (xy^{-1}) = (xy^{-1})$

$First\ we\ prove\ that\ y^{-1} \in (G)$

$since\ ay = ya$

$\Longrightarrow y^{-1}(ay)y^{-1} = y^{-1}(ya)y^{-1}$

$\Longrightarrow y^{-1}(yy^{-1}) = (y^{-1}y)ay^{-1}$

$\Longrightarrow y^{-1}a = ay^{-1}$

$\Longrightarrow y^{-1} \in (G)$

$Now\ (xy^{-1}) = (ax)^{-1}$

$= (xa)^{-1}$

$= (ay^{-1})$

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

$= (xy^{-1})$

$\therefore (xy^{-1}) = (xy^{-1}) \Longrightarrow xy^{-1} \in (G)$

$\therefore C(G)\ is\ a\ subgroup\ of\ G$

$Now\ we\ show\ that\ C(G)\ is\ a\ normal\ subgroup\ of\ G$

$Let\ a \in G, x \in C(G)$

$Now\ axa^{-1} = (ax)^{-1} = (xa)a^{-1} = x(aa^{-1}) = xe = x \in C(G)$

$\therefore axa^{-1} \in (G) \Longrightarrow (G)\ is\ a\ normal\ subgroup\ of\ G$

Theorem10: ***Let H be a normal subgroup of G then the set*** $\frac{G}{H} = \{Ha/a \in G\}$

is a group under coset multiplication

Proof: $Given\ that\ H\ is\ a\ normal\ subgroup\ of\ G.$

$For\ a \in G, Ha = aH$

$The\ set \frac{G}{H} = \{Ha/a \in G] = The\ set\ of\ all\ cosets\ of\ H\ in\ G$

$Define\ a\ coset\ multiplication\ by\ Ha \cdot Hb = Hab \quad \forall Ha, Hb \in \frac{G}{H}$

$To\ prove\ that\ {}_{H} = \{Ha/a \in G]\ is\ a\ group\ under\ coset\ multiplication.$

(i)By closure property: $Let\ Ha, Hb \in {}_{H}\ where\ a, b \in G$

$Now\ Ha \cdot Hb = Hab \in {}_{H} \quad (\because a, b \in G \Longrightarrow ab \in G)$

$\therefore '\cdot'\ is\ a\ binary\ operation$

(ii)Associative property: $Let\ Ha, Hb, Hc \in {}_{H}$

$$(Ha \cdot Hb) \cdot Hc = Hab \cdot Hc$$
$$= H(ab \cdot c)$$
$$= Ha \cdot (bc)$$
$$= Ha \cdot (Hbc)$$
$$= Ha \cdot (Hb \cdot Hc)$$

(iii)Identity property: $We\ have\ e \in G \Longrightarrow He \in {}_{H}$

$Let\ Ha \in {}_{H}$

$Now\ He \cdot Ha = Hea = Ha$

$also\ Ha \cdot He = Hae = Ha$

$\therefore He\ is\ the\ identity\ element\ in\ {}_{H}$

(iv)Inverse property: $Let\ Ha \in \frac{G}{H} \Longrightarrow a \in G$

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

$\Longrightarrow Ha^{-1} \in \frac{G}{H}\ Now\ Ha \cdot Ha^{-1} = Haa^{-1} = He$

$\therefore Ha^{-1}$ *is the inverse of* Ha

$\therefore$ *Every element in* $\frac{G}{H}$ *has multiplicative inverse.*

Hence $\frac{G}{H} = \{Ha/a \in G\}$ *is a group under coset multiplication.*

Quotient group or factor group: *Let* H *be a normal subgroup of* G *then the*

$set_{H} = \{Ha/a \in G\}$ *is a group under coset multiplication is called as Quotient group .*

Theorem11: Every quotient group of an abelian group is abelian.

Proof: *Given that* H *is a normal subgroup of* G.

For $a \in G, Ha = aH$

The set $_{H} = \{Ha/a \in G] =$ *The set of all cosets of* H *in* G

Define a coset multiplication by $Ha \cdot Hb = Hab \quad \forall Ha, Hb \in {}_{H}$

To prove that $_{H} = \{Ha/a \in G]$ *is a group under coset multiplication.*

(i)By closure property: *Let* $Ha, Hb \in {}_{H}$ *where* $a, b \in G$

Now $Ha \cdot Hb = Hab \in {}_{H} \quad (\because a, b \in G \Longrightarrow ab \in G)$

$\therefore '\cdot'$ *is a binary operation*

(ii)Associative property: *Let* $Ha, Hb, Hc \in {}_{H}$

$$(Ha \cdot Hb) \cdot Hc = Hab \cdot Hc$$
$$= H(ab \cdot c)$$
$$= Ha \cdot (bc)$$
$$= Ha \cdot (Hbc)$$
$$= Ha \cdot (Hb \cdot Hc)$$

(iii)Identity property: *We have* $e \in G \Longrightarrow He \in \frac{G}{H}$

Let $Ha \in \frac{G}{H}$

$Now\ He \cdot Ha = Hea = Ha$

$also\ Ha \cdot He = Hae = Ha$

$\therefore He\ is\ the\ identity\ element\ in \frac{G}{H}$

(iv)Inverse property: $Let\ Ha \in \frac{G}{H} \Longrightarrow a \in G$

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

$\Longrightarrow Ha^{-1} \in {}_{H}\ Now\ Ha \cdot Ha^{-1} = Haa^{-1} = He$

$\therefore Ha^{-1}\ is\ the\ inverse\ of\ Ha$

$\therefore Every\ element\ in\ {}_{H}\ has\ multiplicative\ inverse.$

$Hence\ {}_{H} = \{Ha/a \in G\}\ is\ a\ group\ under\ coset\ multiplication.$

(v)Commutative property: $Let\ Ha, Hb \in {}_{H}$

$Now\ Ha \cdot Hb = Hab$

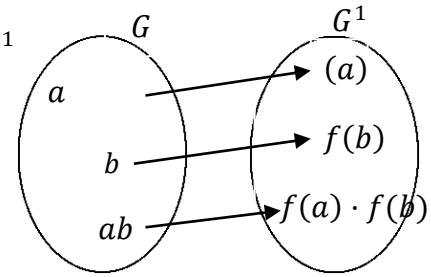
$= Hba \qquad (\because G\ is\ n\ abelian\ )$

$= Hb \cdot Ha$

$\therefore {}_{H} = \{Ha/a \in G\}\ is\ an\ abelian\ group$

UNIT-4: HOMOMORPHISM FOR GROUPS

Homomorphism: Let G, G^1 be two groups. A mapping $f: G \to G^1$ is said to be homomorphism if $(a \cdot b) = (a) \cdot (b)$



Homomorphic image set: If $f: G \to G^1$ is a homomorphism then the image of G is called as homomorphic image set. i.e. $(G) = \{(a) \in G^1 / a \in G\}$

Monomorphism: A homomorphism $f: G \to G^1$ is said to be monomorphism if f is one-one mapping.

Epimorphism: A homomorphism $f: G \to G^1$ is said to be Epimorphism if f is on-to mapping.

Isomorphism: A homomorphism $f: G \to G^1$ is said to be isomorphism if f is one-one and on-to mapping.

Endomorphism: If $f: G \to G$ is a homomorphism then f is called as endomorphism.

Automorphism: If $f: G \to G$ is an isomorphism then f is called as Automorphism.

Notations: If $f: G \to G^1$ is a homomorphism then G^1 is the homomorphic image of G

(I.e. f is homo and onto) we write $G^1 \simeq G$ (i.e. $G^1$is the homomorphic image of G)

If $f: G \to G^1$ is an isomorphism then G^1 is the isomorphic image of G and $G, G^1$are isomorphic images to each other. We write $G^1 \cong G$

***Theorem1**: Let $f: G \to G^1$ be a homomorphism then*

(i) $f(e) = e^1$ where e, e^1 are identity elements of G and G^1 respectively

(ii) $f(a^{-1}) = [f(a)]^{-1}$ $\forall a \in G$

***Proof**: Given that $f: G \to G^1$ is a homomorphism*

(i) since $e \in G$, we have $e \cdot e = e$

$\Rightarrow f(e \cdot e) = f(e)$ ($\because f$ *is mapping*)

$\Rightarrow f(e) \cdot f(e) = f(e)$ ($\because f$ *is homo*)

$\Rightarrow (e)\cdot(e)=(e)\cdot e^1 \qquad (\because f(e)\in G^1, e^1\in G^1)$

$\Rightarrow (e)=e^1 \qquad (\because By\ l.c.l)$

$(ii) Let\ a\in G \Rightarrow a^{-1}\in G\ such\ that\ aa^{-1}=e=a^{-1}a$

$\therefore aa^{-1}=e$

$\Rightarrow (aa^{-1})=(e)$

$\Rightarrow (a)(a^{-1})=e^1 \qquad by(i) f(e)=e^1$

$\Rightarrow (a^{-1})=[(a)]^{-1}$

***Theorem2*: The homomorphic image of a group is also a group.**

(OR)

If f is homomorphism from a group G into a group G^1 then $((G),\cdot)$ is a subgroup of G^1

***Proof*:** $Given\ that\ f: G\to G^1 is\ a\ homomorphism$

$(G)=\{(a)\in G^1/a\in G\}=Homomorphic\ image\ set$

$To\ prove\ that\ (G)\ is\ \ group. For\ this\ we\ have\ to\ show\ that\ (G)\ is\ a\ subgroup\ of\ G^1$

$since\ \ (i): G\to G^1 is\ a\ homo, we\ have\ (e)=e^1$

$\Rightarrow e^1=(e)\in(G)$

$\Rightarrow e^1\in(G)\Rightarrow(G)\neq\phi$

$(ii)\ By\ the\ definition\ of\ (G) \qquad clearly\ (G)\subseteq G^1$

$(iii)\ Let\ a^1,^1\in f(G)\ so\ \exists\ a,b\in G\ such\ that\ f(a)=a^1, f(b)=b^1$

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

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

$=(ab^{-1})$

$=(ab^{-1})\in(G)$

$\therefore a^1(b^1)^{-1}\in f(G)$

$\therefore (G)\ is\ subgroup\ of\ G^1$

$Hence\ f(G)\ is\ a\ group$

Theorem3: The homomorphic image of an abelian group is also an abelian group

Proof: $Given\ that\ f: G \to G^1 is\ a\ homomorphism$

$(G) = \{(a) \in G^1 / a \in G\} = Homomorphic\ image\ set$

$To\ prove\ that\ f(G)\ is\ an\ abelian\ \ group.$

$For\ this\ we\ have\ to\ show\ that\ (G)\ is\ a\ subgroup\ of G^1$

$since\ \ (i): G \to G^1 is\ a\ homo, we\ have\ (e) = e^1$

$$\Longrightarrow e^1 = (e) \in (G)$$

$$\Longrightarrow e^1 \in (G) \Longrightarrow (G) \neq \phi$$

$(ii) By\ the\ definition\ of\ (G) \qquad clearly\ (G) \subseteq G^1$

$(iii)\ Let\ a^1, ^1 \in f(G)\ so\ \exists\ a, b \in G\ such\ that\ f(a) = a^1, f(b) = b^1$

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

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

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

$$= (ab^{-1}) \in (G)$$

$\therefore a^1(b^1)^{-1} \in f(G)$

$\therefore (G)\ is\ subgroup\ of\ G^1$

$Hence\ f(G)\ is\ a\ group$

$(iv) Commutative\ property: Let\ a^1, ^1 \in f(G) so\ \exists\ a, b \in G\ such\ that\ f(a) = a^1, f(b) = b^1$

$Now\ a^1 \cdot b^1 = (a)(b)$

$$= f(ab)$$

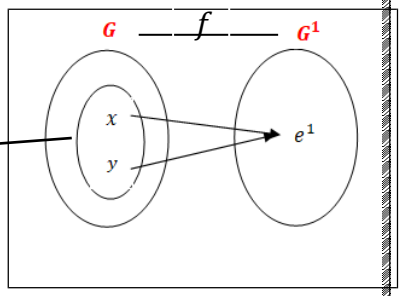
$$= f(ba) \quad (\because G\ is\ an\ abelian\ )$$

$$= f(b)f(a)$$

$$= b^1 \cdot a^1$$

$\therefore$ The homomorphic image of an abelian group is also an abelian group

Kernel of a homomorphism: Let $f: G \to G^1$ be a homomorphism then the set of elements in G which are mapped with the identity element of G^1 is called as kernel of the homomorphism. It is denoted by Ker f



$Kerf = \{x \in G/(x) = e^1 \; where \; e^1 \; is \; the \; identity \; element \; in \; G^1\}$

Note: 1. $p \in kerf \Leftrightarrow (p) = e^1$

2. $f: G \to G^1 is \; a \; homo, we \; have \; (e) = e^1 \Longrightarrow e \in kerf \Longrightarrow kerf \neq \phi$

3. $By \; the \; defintion \; of \; kerf, arly \;\; kerf \subseteq G$

***Theorem4**: If $f: G \to G^1$ is homomorphism then kerf is a normal subgroup of G.*

***Proof**: $Given \; that \; f: G \to G^1 \; is \; a \; homomorphism$*

$Kerf = \{x \in G/(x) = e^1 \; where \; e^1 \; is \; the \; identity \; element \; in \; G^1\}$

$To \; prove \; that \; kerf \; is \; a \; normal \; subgroup \; of \; G$

$(i) since \; f: G \to G^1 is \; a \; homo, we \; have \; (e) = e^1 \Longrightarrow e \in kerf \Longrightarrow kerf \neq \phi$

$(ii). By \; the \; defintion \; of \; kerf, clearly \; kerf \subseteq G$

$(iii) Let \; a, b \in kerf \Longrightarrow (a) = e^1, (b) = e^1$

$To \; prove \; that \; ab^{-1} \in kerf \;\; (i.e. (ab^{-1}) = e^1)$

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

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

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

$= e^1$

$\therefore ab^{-1} \in kerf$

$(iv) \; Let \; a \in G, x \in kerf \Longrightarrow (x) = e^1$

$To \; prove \; that \; axa^{-1} \in kerf \; (i.e. (axa^{-1}) = e^1)$

$Now \; (axa^{-1}) = (a)(x)f(a^{-1})$

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

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

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

$= e^1$

$\therefore\ axa^{-1} \in kerf$

$\therefore kerf$ *is a normal subgroup of* G

Problems:

1. *If* G *is a group of non* $-$ *zeo real numbers under multiplication then prove that* $\phi: G \to G$ *where* $(x) = x^2\ \forall x \in G$ *is homo, determine kernel*ϕ

sol: *Given that* $\phi: G \to G$ *by* $(x) = x^2\ \ \forall x \in G$

Let $a, b \in G \Longrightarrow (a) = a^2$ *and* $(b) = b^2$ *also* $ab \in G \Longrightarrow (ab) = a^2b^2$

Now $(ab) = a^2b^2 = (a)(b)$

$\therefore \phi$ *is homomorphism*

$ker\phi = \{x \in G/(x) = e^1$ *where* e^1 *is the identity element in* $G\}$

$= \{x \in G/x^2 = 1\}$

$= \{x \in G/x = \pm 1\}$

$\therefore ker\phi = \{\pm 1\}$

2.$(\mathbb{Z}, +)$*is agroup of integers. P.T* $f: \mathbb{Z} \to \mathbb{Z}$ *by* $(x) = 2x\ \forall x \in \mathbb{Z}$ *is a homo and also find* $kerf$?

Sol: *Given tha* $f: \mathbb{Z} \to \mathbb{Z}$ *by* $(x) = 2x\ \forall x \in \mathbb{Z}$

Let $x, y \in \mathbb{Z} \Longrightarrow x + y \in \mathbb{Z}$

$\therefore (x) = 2x,\ \ (y) = 2y$

$(x + y) = 2(x + y)$

$= 2x + 2y$

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

$\therefore f$ *is homomorphism*

$kerf = \{x \in G/(x) = e^1$ *where* e^1 *is the identity element in* $\mathbb{Z}\}$

$= \{x \in \mathbb{Z}/2x = 0\}$

$= \{x \in \mathbb{Z}/x = 0\}$

$\therefore kerf = \{0\}$

3. *If G is a group under multiplication and $\phi: G \to G$ is defined by $(x) = x^{-1} \quad \forall x \in G$ then show that ϕ is not homomorphism.*

Sol: *Given that $\phi: G \to G$ by $(x) = x^{-1} \quad \forall x \in G$*

Let $x, y \in G \Longrightarrow (x) = x^{-1}$ and $(y) = y^{-1}$ also $xy \in G \Longrightarrow (xy) = (xy)^{-1}$

Now $(xy) = (xy)^{-1} = y^{-1}x^{-1} = \phi(y)\phi(x) \neq \phi(x)\phi(y)$

$\therefore \phi$ is not a homomorphism

4. *If G is a group under addition and $f: G \to G$ is defined by $(a) = a + 2 \quad \forall a \in G$ then show that ϕ is not homomorphism.*

Sol: *Given that $f: G \to G$ by $(a) = a + 2 \quad \forall a \in G$*

Let $a, b \in G \Longrightarrow (a) = a + 2$ and $(b) = b + 2$ also $a + b \in G \Longrightarrow (a + b) = a + b + 2$

Now $(a + b) = a + b + 2$

$(a) + (b) = a + 2 + b + 2 \neq (a + b)$

$\therefore f$ is not a homomorphism

5. *If $f: G \to G$ defined by $(x) = \{_{-1,\ x < 0}$ where G is set of non − zero real numbers and $G = \{-1,1\}$ are groups under multiplication. P.T f is homo and find $kerf$.*

Sol: *Given that $f: G \to G$ defined by $(x) = \{_{-1,\ x < 0}$*

Toprove that f is homo

Let $x, y \in G$

c(i) *If $x > 0, y > 0 \Longrightarrow xy > 0$*

$(x) = 1, (y) = 1$ *and* $f(xy) = 1$ *and also* $f(x)f(y) = 1.1 = 1$

$\therefore f(xy) = f(x)f(y) \Longrightarrow f$ is homo

c(ii) $If\ x < 0, y < 0 \Rightarrow xy > 0$

$(x) = -1, (y) = -1\ and\ f(xy) = 1\ and\ also\ f(x)f(y) = (-1)(-1) = 1$

$\therefore f(xy) = f(x)f(y) \Rightarrow f\ is\ homo$

c(iii) $If\ x < 0, y > 0 \Rightarrow xy < 0$

$(x) = -1, (y) = 1\ and\ f(xy) = -1\ and\ also\ f(x)f(y) = (-1)1 = -1$

$\therefore f(xy) = f(x)f(y) \Rightarrow f\ is\ homo$

c(iv) $If\ x > 0, y < 0 \Rightarrow xy < 0$

$(x) = 1, (y) = -1\ and\ f(xy) = -1\ and\ also\ f(x)f(y) = 1.(-1) = -1$

$\therefore f(xy) = f(x)f(y) \Rightarrow f\ is\ homo$

$In\ all\ above\ 4\ cases\ \ (xy) = (x)(y) \Rightarrow f\ is\ homo$

$kerf = \{x \in G/(x) = e^1\ where\ e^1\ is\ the\ identity\ element\ in\ G\}$

$= \{x \in \mathbb{R} - \{0\}/f(x) = 1\}$

$= \{x \in \mathbb{R} - \{0\}/x > 0\}$

$\therefore kerf = \{\mathbb{R}^+\}$

6. $If\ f: G \to G defined\ by\ (x) = \{_{-1,\ x > 0}\ where\ G\ is\ set\ of\ non - zero\ real\ numbers$

$and\ \{-1,1\}\ are\ groups\ under\ multiplication.\ P.T\ f\ is\ homo\ and\ find\ kerf$ Ans) $\{\mathbb{R}^-\}$

7. $If\ G\ is\ a\ group\ under\ multiplication\ and\ f: G \to G\ is\ defined\ by\ (x) = x^{-1}\ \ \forall x \in G$

$P.T\ f\ is\ one - one\ and\ on - to.\ Also\ prove\ that\ f\ is\ homo\ iff\ G\ is\ abelian.$

Sol: $Given\ f: G \to G\ is\ defined\ by\ (x) = x^{-1}\ \ \forall x \in G$

(i) f is one − one: $Let\ x, y \in G\ such\ that\ f(x) = f(y)$

$To\ prove\ that\ x = y$

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

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

$\Rightarrow x = y$

(ii) f is on − to: Let $y \in G$ $(co-domain)$ $\exists\ y^{-1} \in G$ $(domain)$.

For this $y^{-1} \in G$ wehave $(y^{-1}) = (y^{-1})^{-1} = y$

$\therefore \forall y \in G\ \exists\ y^{-1} \in G\ \ni (y^{-1}) = y \Longrightarrow f$ is on − to

Next prove that f is homo if f G is abelian

N. C($\Longrightarrow$): Given that f is homo.

To prove that G is abelian $(i.e.\ xy = yx\ \ \forall x, y \in G\ )$

Let $x, y \in G \Longrightarrow xy \in G$

since f is homo $\Longrightarrow f(xy) = f(x)f(y)$

$$\Longrightarrow (xy)^{-1} = x^{-1}y^{-1}$$

$$\Longrightarrow y^{-1}x^{-1} = x^{-1}y^{-1}$$

$$\Longrightarrow (y^{-1}x^{-1})^{-1} = (x^{-1}y^{-1})^{-1}$$

$$\Longrightarrow xy = yx$$

S.C ($\Longleftarrow$): Conversely given that G is an abelian.

To prove that f is homo

Let $x, y \in G \Longrightarrow xy \in G \therefore (x) = x^{-1}, (y) = y^{-1}, and\ (xy) = (xy)^{-1}$

Now $(xy) = (xy)^{-1}$

$$= y^{-1}x^{-1}$$

$$= x^{-1}y^{-1}$$

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

$\therefore f$ is homo

8. If f for a group $G, : G \to G$ is given by $f(x) = x^2$ is a homomorphism.

P.T G is abelian.

Sol: Given that $f: G \to G$ by $(x) = x^2\ \ \forall x \in G$

To prove that G is abelian$(i.e.\ xy = yx\ \forall\ x, y \in G)$

Let $x, y \in G \Longrightarrow xy \in G$

$since\ f\ is\ homo \implies f(xy) = f(x)f(y)$

$\implies (xy)^2 = x^2y^2$

$\implies (xy)(xy) = (xx)(yy)$

$\implies x(yx)y = x(xy)y$

$\implies xy = yx \qquad \therefore G\ is\ abelian$

9. *Show that the groups* $G = (\{0,1,2,3\}, +_4)$, $G^1 = (\{1,-1,i,-i\},\cdot)$ *are isomorphic*.

Sol: $G = (\{0,1,2,3\}, +_4)$ $\qquad$ $G^1 = (\{1,-1,i,-i\},\cdot)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

we have to find an isomorphism $f: G \to G^1$

The identity in G *is* 0 *and the identity in* G^1 *is* 1.

Let $(0) = 1 also\ (a) = [(a)]^{-1}\ \forall a \in G$

Define $(1) = i$

$(3) = (1^{-1}) = [(1)]^{-1} = (i)^{-1} = -i\ and\ f(2) = -1$

$[(2) = (2^{-1}) = [(2)]^{-1} = (-1)^{-1} = -1]$

$\therefore\ (0) = 1, (1) = i\ , f(2) = -1, f(3) = -i$

$Let\ a, b \in G \implies a+_4 b \in G$

$(a+_4 b) = f(a)f(b)$

For example $(0+_4 2) = (2) = -1\ and \qquad (0)f(2) = 1(-1) = -1$

$\therefore\ f\ is\ homo\ .$

f is one – one : *different elements have different images*

f is on − to: $For\ all\ y \in G^1\ so\ \exists\ atleast\ one\ element\ \ x\ in\ G\ such\ that\ (x) = y$

$\therefore f: G \to G^1 is\ an\ isomorphism\ such\ that\ \ (0) = 1, (1) = i\ , f(2) = -1, f(3) = -i$

$\therefore\ G^1 \cong G$

***Theorem5*: If *f* is homomorphism from a group *G* onto a groupG^1 with *kerf* then *f* is one-one $\Leftrightarrow$ *kerf* $= \{e\}$**

***N*. ($\Longrightarrow$)**: $Given\ that\ f: G \to G^1\ is\ an\ isomorphism$

$To\ prove\ that\ kerf = \{e\}$

$Let\ a \in Kerf\ then\ (a) = e^1$

$Since\ f\ is\ homo. we\ have\ (e) = e^1$

$\therefore f(a) = f(e) \Longrightarrow a = e\ \ (\therefore f\ is\ one - one\ )$

$\therefore kerf = \{e\}$

S.C ($\Longleftarrow$): $Conversely\ given\ that\ f$ is homomorphism from a group G onto a group G^1

with $kerf = \{e\}$.

$To\ prove\ that\ f\ is\ one - one$

$Let\ a, b \in G\ such\ that\ f(a) = f(b)$

$To\ prove\ that\ a = b$

$Since\ f(a) = f(b) \Longrightarrow f(a)[f(b)]^{-1} = f(b)[f(b)]^{-1}$

$\Longrightarrow (a)(b^{-1}) = e^1$

$\Longrightarrow (ab^{-1}) = e^1$

$\Longrightarrow ab^{-1} \in kerf = \{e]$

$\Longrightarrow ab^{-1} = e$

$\Longrightarrow a = b$

$\therefore f\ is\ one - one$

Thorem6*: *The set of all automorphism of a group G from a group G w.r.t composition mapping is group.

Proof: $Let\ A(G) = \{f/f\ is\ an\ isomorphism\ from\ G\ to\ G\}$

$Let\ '\circ'be\ the\ composition\ of\ bijection\ over\ G$

$To\ prove\ that\ A(G)\ is\ a\ group\ when\ '\circ'$

(i)Closure property: $Let\ f, g \in A(G) \Longrightarrow f, g\ are\ bijection$

$$\Longrightarrow gof\ is\ also\ bijection$$

$Let\ a, b \in G \Longrightarrow ab \in G$

$$Now\ gof(ab) = g[f(ab)]$$

$$= g[f(a)f(b)]$$

$$= g[f(a)]g[f(b)]$$

$$= gof(a).gof(b)$$

$\therefore gof\ is\ homomorphism \Longrightarrow gof \in A(G)$

(ii)Associative property: $We\ know\ that\ composition\ of\ a\ mapping\ in\ A(G)\ is\ an\ associative.$

(iii)Identity property: $Let\ I: G \to G\ be\ the\ identity\ mapping.$

$Since\ I\ is\ one-one\ and\ on-to\ and\ structure\ is\ preserving\ i.e. I \in A(G)$

$Let f \in A(G) \Longrightarrow f\ is\ bijection\ and\ f\ is\ homo.$

$we\ have\ foI = Iof = f \Longrightarrow Identity\ exists\ in\ A(G) and\ it\ is\ I$

(iv)Inversproperty: $Let\ f \in A(G) \Longrightarrow fis\ one-one\ and\ on-to$

$\Longrightarrow f^{-1} is\ also\ one-one\ and\ on-to$

$we\ have\ to\ show\ that\ f^{-1}\ is\ homo.$

$Let\ f^{-1}(a) = a^1, f^{-1}(b) = b^1\ for\ a^1, b^1 \in G$

$\Longrightarrow (a^1) = a, (b^1) = b$

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

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

$= a^1 b^1$

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

$\therefore f^{-1}$ *is homo*

we have $f^{-1}of = fof^{-1} = I$

$\therefore f^{-1}$ *is the inverse of* f.

Each element in $A(G)$ *has invertiable element*

$\therefore A(G)$ *is a group under composition of mapping*

Theorem7: ***If N is a normal subgroup of G and a mapping*** $f: G \to_N$ ***by*** $(x) = Nx \ \forall x \in G$ ***then f is on − to homomorphism and kerf = N***

Proof: *Given that* $f: G \to_N$ *by* $(x) = Nx \ \forall x \in G$

(*i*)*f is homo*: *Let* $x, y \in G \Longrightarrow xy \in G$

$f(xy) = Nxy$

$= Nx.Ny$

$= f(x)f(y)$

$\therefore f$*is homo*

(*ii*)*f is on − to*: *Let* $Nx \in_N \Longrightarrow x \in G$

For this $x \in G$, *we have* $f(x) = Nx$

$\forall Nx \in_N$ *so* $\exists\, x \in G \ \ni f(x) = Nx \therefore f$*is on − to*

To prove that $kerf = N$ $(i.e.\, kerf \subseteq N$ *and* $N \subseteq kerf)$

Let $p \in Kerf \Longrightarrow f(p) = Ne = N$

since $p \in kerf \Longrightarrow p \in G \ (\because kerf \subseteq G)$

$\Longrightarrow f(p) = Np$

$\Longrightarrow Ne = Np$

$\Longrightarrow pe^{-1} \in N$

$\Longrightarrow p \in N$

$\therefore kerf \subseteq N \rightarrow (1)$

$Next\ let\ q \in N$

$since\ q \in N \Longrightarrow q \in G \quad (\because N \rhd G)$

$\Longrightarrow f(q) = Nq$

$\Longrightarrow f(q) = N \quad (\because h \in H, Hh = H = hH) \Longrightarrow q \in kerf$

$\therefore N \subseteq kerf \rightarrow (2)$

$From\ (1)\ and\ (2)\ kerf = N$

Fundamental theorem of homomorphism for groups: (first isomorphism theorem)

Statement: If f is homomorphism from a group G onto a group G^1 with $Kerf$ then $_{Kerf}$ is isomorphic to the group G^1

(Or)

Every homomorphic image of a group G is isomorphic to some quotient group of the group G

Proof: Given that $f: G \rightarrow G^1$ is on-to homomorphism.

$kerf = \{x \in G/(x) = e^1\ where\ e^1\ is\ the\ identity\ element\ in\ G^1\}$

We know that ker f is a normal subgroup of G, write $kerf = K$

$_K = \{Kx/x \in G\}\ is\ a\ \underset{g}{r}\ \underset{o}{up}\ under\ Kx \cdot Ky = Kxy \qquad \forall\ Kx, Ky \in\ _K$

This group is called quotient group.

$Define\ \psi: {}_K \rightarrow G^1\ by\ (Kx) = (x), \quad \forall Kx \in\ _K$

i) ψ is well-define and one-one: - $Let\ Kx = Ky \in\ _K \ni Kx = Ky$

$Since\ Kx = Ky \Leftrightarrow xy^{-1} \in K = Kerf \quad (\because Ha = Hb \Leftrightarrow ab^{-1} \in H)$

$\Leftrightarrow xy^{-1} \in Kerf$

$\Leftrightarrow (xy^{-1}) = e^1$

$$\Leftrightarrow (x)(y^{-1}) = e^1 \quad (\because f \text{ is homo})$$

$$\Leftrightarrow (x)[f(y)]^{-1} = e^1$$

$$\Leftrightarrow (x)[f(y)]^{-1} f(y) = e^1 f(y)$$

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

$$\Leftrightarrow \psi(Kx) = \psi(Ky)$$

$\therefore \psi$ *is well defined and one − one*

ii) ψ is homomorphism: *Let* $Kx, \in {}_K$

$Now\ \psi(Kx \cdot Ky) = \psi(Kxy)$

$$= f(xy) \quad (\because f \text{ is homo})$$

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

$$= \psi(Kx)\psi(ky)$$

$\therefore \psi$ is homomorphism

iii) ψ is on-to: - *Let* $y^1 \in G^1$

Since f is on-to so $\exists\ y \in G \ni (y) = y^1$

For this $y \in G \Longrightarrow ky \in {}_K \Longrightarrow (ky) = (y) = y^1$

Thus $\forall y^1 \in G^1 \exists\ ky \in {}_K \Longrightarrow (ky) = (y) = y^1$

$\therefore \psi$ is on-to. Hence ψ is an isomorphism from ${}_K$ to G^1 i.e. ${}_K \cong G^1$

Second isomorphism theorem: -Let N be a normal subgroup of G and H be a subgroup of G then H N is a normal subgroup of H and HN is a subgroup of G and $\frac{H}{H\ K} \cong N$

$HN = \{hn / h \in H, n \in N\}$

Proof: Given that H, N are subgroups of G, clearly H N is a subgroup of H or N

Let $n \in H \bigcap N$ and $h \in H \Rightarrow n \in H$ and $n \in N$ and $h \in H$

$\therefore hnh^{-1} \in N$ (Since $N \triangleright G$ and $h \in G$)

And $hnh^{-1} \in H$ (since $n \in H, h \in H \Rightarrow nh^{-1} \in H, h \in H \Rightarrow hnh^{-1} \in H$, H is a subgroup of G)

And hence $hnh^{-1} \in H \bigcap K$ Therefore H$\bigcap$ N is a normal subgroup of H.

To prove that HN is a subgroup of G

Let $x_{1,} x_2 \in HN$ then $x_1 = h_1 n_1 \quad x_2 = h_2 n_2$ where $h_1, h_2 \in H$ and $n_1, n_2 \in N$

Now $x_1 x_2^{-1} = (h_1 n_1)(h_2 n_2)^{-1}$

$= (h\, n\,)(n_2{}^1 h_2{}^1)$

$= h\, n_3 h_2{}^1$ Where $n_3 = n\, n_2{}^1 \in N$

$= h\, e n_3{}_2{}^1$

$= h\, h^{-1} h\, n_3 h^{-1}$

$= h h_2 n_3 h^{-1}$ Since $h = {}_1 h_2{}^1$

$= hn_4 \in HN$ Where $n_4 = h_2 n_3 h_2{}^1 \in N$ as $N \quad G$

$\therefore x\, x_2{}^1 \in HN \Rightarrow HN$ is a subgroup of G.

And that N is a normal subgroup of HN so that the quotient group $^{HN} = \{Nx / x \in HN\}$

Define $f : H \to {}^{HN}$ by $f(x) = Nx, \forall x \in H$

i) f is homo: Let $x, y \in H \in \Rightarrow xy \in H$

$f(xy) = Nxy = (Nx)(Ny)$

$= f(x) f(y)$

$\therefore f$ is homo

ii) f is on-to: Any element ${}_N$ is of the form Nax,where $a \in H$ and $x \in N$

and $f(a) = Na = Nax$ (since N is a normal, $a^{-1} xa \in N$)

$\therefore f$ is on-to

$\ker f = \{x \in H / f(x) = \text{the identity in } \frac{HN}{N}\}$

$= \{x \in H / Nx = N\}$

$= \{x \in H / x \in N\} = N \bigcap H$

Therefore, by the fundamental theorem of homomorphism, $\frac{H}{H \cap K} \cong \frac{HN}{N}$

Third isomorphism theorem: -Let N and K be normal subgroups of a group G such that $N \subseteq K$ .Then $\frac{K}{N}$ is a normal subgroup of $\frac{G}{N}$ and $\frac{\frac{G}{N}}{\frac{K}{N}} \cong \frac{G}{K}$

Proof: -For any Na, and Nb$\in \frac{K}{N}$ where a, b$\in$K.

We have $(Na)(Nb)^{-1} = (Na)(Nb^{-1}) = N(ab^{-1}) \in \frac{K}{N}$

And also $(Nx)(Na)(Nx)^{-1} = N(xax^{-1}) \in \frac{K}{N}, \forall x \in G$

$\therefore \frac{K}{N} \triangleright \frac{G}{N}$

Now define $f : \frac{G}{N} \to \frac{G}{K}$ by $f(Na) = Ka, \forall a \in G$

i) f **is well-define:** -Let $Na, Nb \in \frac{G}{N}$ ∋ $Na = Nb, \forall a, b \in G$

$$= \{Na / Ka = K\}$$

$$= \{Na / a \in K\} = \frac{K}{N}$$

Since $Na = Nb \Rightarrow ab^{-1} \in N \subseteq K$

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

$$\Rightarrow ka = Kb$$

$$\Rightarrow f(Na) = f(Nb)$$

$\therefore f$ is well-defined

ii) f **is homo:** -Let $Na, Nb \in \frac{G}{N} \Rightarrow Nab \in \frac{G}{N}$

$f(Nab) = Kab = (Ka)(Kb) = f(Na)\, f(Nb)$

$\therefore f$ is homo

ii) f **is on-to**: -Let $Ka \in \frac{G}{K}$ where $a \in G$

For this $a \in G \Rightarrow Na \in \frac{G}{N}$, we have $f(Na) = Ka$

$\forall Ka \in \frac{G}{K}\, so \exists Na \in \frac{G}{N} \ni f(Na) = Ka$

$\therefore$ f is on-to

$\ker f = \{Na \in \frac{G}{N} / f(Na) = \text{the identity in } \frac{G}{N}\}$

$= \{Na / Ka = K\}$

$= \{Na / a \in K\} = \frac{K}{N}$

Therefore, by fundamental theorem of homomorphism $\frac{\frac{G}{N}}{\frac{K}{N}} \cong \frac{G}{K}$

UNIT-5: PERMUTATION GROUPS

Permutation : *Let S be a finite set containing n distinct elements then there exist a bijective mapping $f: S \to S$ is called as a permutation on S. The number of elements in S called as dgree of permutation*

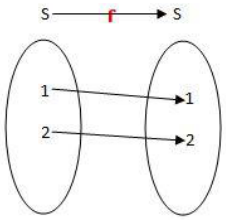
Notation: *Let S be a finite set having n elements $i.e. S = \{a_1, a_2, \dots\}$ then the permutation* $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ (a_1) & (a_2) & \dots & f(a_n) \end{pmatrix}$

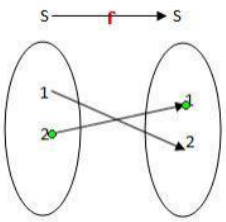
$i.e.$ each element in second row is the f image of the elements in first row.

Ex: *Let $S = \{1,2,3\}$ and $f: S \to S$ such that $f(1) = 2, f(2) = 3, f(3) = 1$*

then $f = \begin{pmatrix} 1 & 2 & 3 \\ (1) & (2) & (3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *is permutation of degree* 3.

Example: $S = \{1,2\}$ *then the permutations are*





$\therefore$ *Total number of distinct permutation of S is* 2

Note: *Total number of distinct permutation of S in n symbols is $n!$ the set of all these permutation of degree n form a group under permutation multiplication. This group is called as symmetric group and it is denoted by S_n.*

$i.e$ $S_n = \{f / f$ *is a permutation of degree* $n\}$

Ex: $S = \{1,2,3\}$ be a finite set then find S_3

Sol: *The number of distinct permutations of degree* 3 *is* $3! = 6$

$s_3 = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$ *is a group under permutation of multiplications.*

Equality of two permutation: *Let f and g be two permutation then they are called equal* $\Leftrightarrow f(a) = g(a) \quad \forall a \in S$

i.e. image of every element of S under both f and g are equal.

Example: $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ *and* $g = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix}$

Here $(1) = 3 = (1)$

$(2) = 2 = (2)$

$(3) = 1 = (3)$

Identity permutation: *A permutation f is said to be identity permutation of S if* $(a) = a \quad \forall a \in S$ **Ex**: $I = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ *or* $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$

Product of permutations (or)multiplication of permutations:

Let $S = \{a_1, _2, \dots a_n\}$ *be a finite set containing n distinct elements.*

Let $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ *and* $g = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$ *be two permutations of degree n*

then the product of two permutations is also a composition of permutations

i.e. $(gof)(x) = gof(x) = g[f(x)]$

$gof = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & \end{pmatrix}$

Ex: 1. $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ **and** $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ **then find fg and gf**

Sol: $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *and* $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$fg = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $gf = \begin{pmatrix} & 1 & 2 & 3 \\ 3 & & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$\therefore fg = gf$

2. Compute $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 2 & 5 & 1 & 7 & 4 \end{pmatrix}$

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

3. $S = \{1,2,3,4,5,6\}$ ***and*** $f = (2\ 3\ 6), g = (1\ 4\ 6)$ ***find*** fg ***and*** gf

Sol: $fg = (2\ 3\ 6)(1\ 4\ 6) = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 1 & 3 & 6 & 4 & 5 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 2 & 3 & 6 & 5 & 1\end{pmatrix}$

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

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

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

Cyclic permutation: *Consider a set* $S = \{a_1, a_2, \dots\}$ *and*

$f = \begin{pmatrix}a_1 & a_2 & \dots a_k & a_{k+1} & \dots & a_n\\ a_2 & a_3 & \dots a_1 & a_{k+1} & \dots & a_n\end{pmatrix}$ *is a permutation of degree n then* $(a_1) = a_2$,

$(a_2) = a_3, \dots (a_k) = a_1, f(a_{k+1}) = a_{k+1}, \dots f(a_n) = a_n$

This type of permutation f *is called as cyclic permutation of length* k *and degree* n.

It is denoted by $(a_1\ a_2\ \dots a_k)$ *or* $(a_2\ a_3\ \dots a_k\ a_1)$

Ex*: 1.** $f = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 1 & 2 & 3 & 5 & 6\end{pmatrix}$ ***be a permutation then f ***is a cyclic permutation***

i.e. $f = (1\ 4\ 3\ 2)$ *is a cyclic permutation of length* 4 *of degree* 6

2. $f = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 1 & 2 & 3 & 6 & 5\end{pmatrix} = (1\ 4\ 3\ 2)(5\ 6)$ *is not a cyclic permutation.*

3. ***Express*** $f = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 2 & 4 & 6 & 7 & 3 & 1 & 5 & 8\end{pmatrix}$ ***in cyclic form.***

Sol: $f = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 2 & 4 & 6 & 7 & 3 & 1 & 5 & 8\end{pmatrix} = (1\ 2\ 4\ 7\ 5\ 3\ 6)$

Length of cycle: *The number of elements in cycle is called as length of cycle.*

Ex: $f = (1\ 2\ 3\ 4\ 5)$ *then length of* f *is* 5

If length of cycle is " r "*then it is called* $r-$*cycle. Above example is* $5-$*cycle*

Note: 1. *A cycle of length* 1 *is called as Identity permutation.*

Ex: $f = \begin{pmatrix}1,2,\dots & n\\ 1,2,\dots & n\end{pmatrix} = (1)(2)(3)\dots(n)$

2. *A length of cycle is called order of cycle*

Ex: $f = (1\ 2\ 3\ 4)\ then\ (f) = 4$

3.*Inverse of a cycle*: $Let\ f = (1\ 2\ 3\ 4)\ then\ f^{-1} = (4\ 3\ 2\ 1)$

2.*Write down the inverse of* $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$

: $(i)\ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix} \Rightarrow f^{-1} = \begin{pmatrix} 5 & 3 & 4 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$

Disjoint cycles: $Let\ S = \{a_1, _2, \dots a_n\}\ be\ a\ finite\ set.$

$Two\ cycles\ f\ and\ g\ are\ said\ to\ be\ disjoint\ cycles\ if\ they\ have\ no\ common\ elements$

Ex: $Let\ S = \{1,2,3,4,5,6\}\ and\ f = (1\ 3\ 5)\ \ g = (2\ 4\ 6)\ are\ disjoint\ \ cycles\ and$

$f = (1\ 3\ 5\ 4)\ and\ \ g = (2\ 4\ 6)\ are\ not\ disjont\ cycles.$

Product of disjoint cycles are commutes: $Let f, g\ are\ disjoint\ cycles$

$then\ they\ have\ \ no\ common\ elements.$

$(a) \neq a\ \ then\ (a) = a \Rightarrow (fg)(a) = f[g(a)] = f(a) \Rightarrow fg = f \rightarrow (1)$

$Next\ (a) = a\ then\ (a) \neq a \Rightarrow (gf)(a) = g[f(a)] = f(a) \Rightarrow gf = f \rightarrow (2)$

$\therefore fg = gf$

Ex: $Let\ S = \{1,2,3,4,5,6\}\ and\ f = (1\ 3\ 5)\ \ g = (2\ 4\ 6)\ are\ disjoint\ \ cycles\ \ then$

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

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

$\therefore fg = gf$

Note: $Every\ permutation\ can\ be\ expressed\ as\ the\ product\ of\ disjoint\ cycles$

Ex: $Let\ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}\ then\ f = (1\ 6\ 2\ 5)(3\ 4)$

1.*Write down the product of disjoint cycles*

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

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

$(iii)(4\ 5)(1\ 2\ 3)(3\ 2\ 1)(5\ 4)(2\ 6)(1\ 4) = (2\ 6)(1\ 4)$

Order of a permutation: *Let S_n be a permutation group on a set S. If $f \in S_n$ suchthat $f^n = I$ where I is the identity pemutation and n is a least positive integer then the order of a permutation is n*

Note: *A permtation can be exprssed as $K-$ disjoint cycles whose lengths are $M_1, M_2, \dots M_n$ then order of the permutation is $L.C.M$ of $\{_1, M_2, \dots M_n\}$*

Ex: *Let* $f == \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 4 & 3 & 1 & 2\end{pmatrix}$ *then* $f = (1\ 6\ 2\ 5)(3\ 4)$

$\therefore O(f) = L.C.\{4,2\} = 4$

1. *Find the order of the permutation* $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 4 & 3 & 1 & 2 & 6 & 7 & 5\end{pmatrix}$ ***in*** S_7

Sol: *Given* $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 4 & 3 & 1 & 2 & 6 & 7 & 5\end{pmatrix} = (1\ 4\ 2\ 3)(5\ 6\ 7) = L.C.\{3,4\} = 12$

2. *Find the order of* $f = (1\ 3\ 5\ 7)(2\ 3\ 4)(1\ 2\ 3\ 5)$

Sol: $f = (1\ 3\ 5\ 7)(2\ 3\ 4)(1\ 2\ 3\ 5) \rightarrow$ *These are not disjoint cycles*

$= \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 5 & 4 & 7 & 2 & 3 & 6 & 1\end{pmatrix} = (1\ 5\ 3\ 7)(2\ 4) = L.C.\{2,4\} = 4$

Transposition: . *A cycle of length 2 is called as transposition*

Ex: $f =$ $(2\ 4), (i\ j)$ *both are transpositions.*`

Note: 1. *Order of every tranposition is* $2 \Longrightarrow$ *Every transposition is self inverse*

2. *Every permutation can be expressed as a product of transposition.*

Let a cycle $(_1, a_2, a_3, \dots a_{n-1}, a_n) = (a_1\ a_2)(a_1\ a_3)(a_1\ a_4) \dots (a_1\ a_{n-1})(a_1\ a_n)$

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

$O(f) = L.C.\{3,4\} = 12$

Inversion: *Let f be a permutation then the pair (i,j)* $0 < i < j \leq n$ *is an inversion*

$for\ f\ if\ f(i) > f(j)$

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

$Here\ 1 < 2\ but\ (1) > (2) = 3 > 1$

$Here\ 1 < 3\ but\ (1) > (3) = 3 > 2$

$Here\ 1 < 4\ but\ (1) < (4) = 3 < 4\ \ this\ not\ a\ inversion\ pair$

$Here\ 5 < 6\ but\ (5) > (6) = 6 > 5$

$Then\ the\ pair\ (1\ 2), (1\ 3)\ are\ called\ inversion$

Signature: $The\ total\ number\ of\ such\ inversion\ for\ the\ permutation\ f\ is\ called\ signature\ and\ it\ is\ denoted\ by\ Sig\ f.$

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

$Here\ the\ iversion\ pairs\ are\ (1\ 3), (2\ 3), (2\ 4), (5\ 6) so\ Sig\ f = 4$

Inverse permutation: $If\ f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ $is\ a\ permutation\ then\ inverse\ permutation\ of\ f\ is\ f^{-1} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ $here\ f^{-1}\ is\ also\ bijective.$

$\therefore ff^{-1} = f^{-1}f = I$

Ex: If $f = (2\ 3\ 4\ 1)$ of degree 5 then find f^{-1}

Sol: $f = (2\ 3\ 4\ 1) \Rightarrow f^{-1} = (1\ 4\ 3\ 2)$

2. *Write down the inverse of the following permutations*

$(i)\ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$ $(ii) = \begin{pmatrix} 4 & 2 & 3 & 1 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

: $(i)\ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix} \Rightarrow f^{-1} = \begin{pmatrix} 5 & 3 & 4 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$

$(ii)\ g = \begin{pmatrix} 4 & 2 & 3 & 1 \\ 2 & 4 & 1 & 3 \end{pmatrix} \Rightarrow g^{-1} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

3. *Express the product $(2\ 5\ 4)(1\ 4\ 3)(2\ 1)$ as a product of disjoint cycles and find its inverse.*

Sol: $Given\ (2\ 5\ 4)(1\ 4\ 3)(2\ 1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} = (1\ 5\ 4\ 3)(2)$

$\Rightarrow f^{-1} = (3\ 4\ 5\ 1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}$

4. ***Express the*** $f = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} \\ \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{4} & \mathbf{6} & \mathbf{5} \end{pmatrix}$ ***as a product of transpositions.***

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

$(ii) f = (1\ 2\ 3\ 4\ 5\ 6) = (1\ 6)(1\ 5)(1\ 4)(1\ 3)(1\ 2)$

Even and odd permutation: *A permutation* f *is called even* (odd) *permutation if the total number of transposition are even*(odd) .

Ex: $Let\ f = (1\ 2\ 3\ 4\ 5\ 6\ 7) = (1\ 2)(1\ 3)(1\ 4)(1\ 5)(1\ 6)(1\ 7) = 6\ (transposition)$

$Even\ transposition = Even\ permutation$

Note: **1.** *A cycle of length n is called even pemutation*(odd) *if n is* $odd(even)$

: () $3-cycle\ is\ even\ pemutation\ i.e.\ f = (1\ 2\ 3\ ) = (1\ 2)(1\ 3)$

$= Even\ number\ of\ transposition$

$(ii)\ 4-cycle\ is\ odd\ permutation.\ i.e.\ f = (1\ 2\ 3\ 4) = (1\ 2)(1\ 3)(1\ 4)$

$= odd\ number\ of\ transposition$

2. $Every\ transposition\ is\ an\ odd\ permutation.$: $(2\ 4), (5\ 6)\ are\ odd\ permutation.$

3. $The\ identity\ permutation\ is\ always\ even\ permutation\ because\ I\ can\ be\ expressed\ as\ a\ product\ of\ 2\ transposition.$: $(1\ 2)(2\ 1) = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$,

$(1\ 2)(2\ 1)(3\ 1)(1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

4. $The\ product\ of\ two\ odd\ permutation\ is\ even.\ Ex$: $(12)(3\ 4)$

5. $The\ product\ of\ two\ even\ permutation\ is\ even.$

Ex: $f = (1\ 2\ 3),\ = (3\ 4\ 5)\ then\ fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5)$

6. *The product of even and odd permutation is odd.*

Ex: $f = (1\ 2\ 3) \rightarrow even\ and\ g = (1\ 2\ 3\ 4) \rightarrow odd$

$then\ fg = (1\ 2\ 3)(1\ 2\ 3\ 4) = (1\ 3\ 4\ 2) \rightarrow odd$

7. *The inverse of odd permutation is odd*

8. *The inverse of even permutation is even*

1. *Examine weather the following permutation are even or odd*?

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

$= 5\ transposition$

$\therefore\ f\ is\ odd\ permutation.$

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

$= 4\ tranposition\ \ \therefore\ f\ is\ even\ permutation.$

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

$= 3\ transposition\ \ \therefore\ f\ is\ odd\ permutation$

Theorem1: ***Let S_n be the permutation set of degree n of order n! form a finite group under product of permutation. If $n \leq 2$ then S_n is abelian group and if $n \geq 3$ then S_n is non − abelian group.***

Proof: *Let $S = \{a_1, a_2, \dots\}$ be a finite set containing n distinct elements*

$\therefore S_n = \{f / f\ is\ a\ permutation\ of\ degree\ n\}$

To prove that S_n is a group under product of permutation.

(i)Closure property: *Let* $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ *and* $g = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c^n \end{pmatrix}$ *be two permutations of degree n then* $gof = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix} \in S_n$

(ii)Associative property: *Let* $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ *and* $g = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ {}_1 & c_2 & \dots & c^n \end{pmatrix}$,

$h = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$ *be three permutations of degree* n

Now $h(gof) = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$ *and* $(hog)of = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$

$\therefore ho(gof) = (hog)of$

(iii)Identity permutation: *Let* $I = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ *be a permutation of degree* n

Let $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ *be a permutation of* S_n

$foI = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = f$

also $Iof = f \therefore I = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ *is the identity permutation of degree* n.

(iv)Inverse property: *Let* $f \in S_n \Longrightarrow f$ *is bijective* $\Longrightarrow f^{-1}$ *is bijective so* $f^{-1} \in S_n$

$fof^{-1} = I$ *or* $f^{-1}of = I$

$\therefore f^{-1}$ *is the inverse of* f

Every permutation in S_n *has invertiable permutation* $\therefore S_n$ *is a group of order* $n!$

If $n = 1$ *then* $(S_n) = 1! = 1$

i.e. Every group of order 1 *is always abelian.*

If $n = 2$ *then* $(S_n) = 2! = 2$

$\therefore$ *Every group of order* 2 *is always abelian*

If $n \geq 3$ *then* $f = \begin{pmatrix} 1 & 2 & 3 \dots & n-1 & n \\ 2 & 3 & 4 \dots & n & 1 \end{pmatrix}$ $g = \begin{pmatrix} 1 & 2 & 3 \dots & n-1 & n \\ 2 & 1 & 3 \dots & n-1 & n \end{pmatrix}$

$fg = \begin{pmatrix} 1 & 2 & 3 \dots & n \\ 3 & 2 & 4 \dots & 1 \end{pmatrix}$ *and* $gf = \begin{pmatrix} 1 & 2 & 3 \dots & n \\ 1 & 3 & 4 \dots & 2 \end{pmatrix}$

$\therefore fg \neq gf \Longrightarrow S_n$ *is non* $-$ *abelian group if* $n \geq 3$

Theorem2: ***Let*** S_n ***be a permutation group of degree n then of*** $n!$ ***elements in*** $\frac{n!}{2}$

elements are even permutation and $\frac{n!}{2}$ elements are odd perutation of degree n.

Proof: *Given that S_n is a permutation group of degree n of order n!*

i.e. $S_n = \{e_1, _2, \dots e_p, o_1, o_2, \dots o_q\}$ *is a permutation group of degree n*

$(S_n) = n!$ *here* $e_1, e_2, \dots e_p$ *are even permutation of degree n.*

and $o_1, _2, \dots o_q$ *are odd permutation of degree n.*

$\therefore p + q = n!$

Since every permutation in S_n *is either even or odd but not both.*

Let $t \in S_n$ *whre t is a transposition.*

Since S_n *is a permutation group.*

By closure property: $te_1, te_2, \dots te_p, to_1, to_2, \dots to_q \in S_n$

Since t is odd permutation and $e_1, _2, \dots e_p$ *are even permutation*

$\therefore te_1, te_2, \dots te_p$ *are p odd permutations.*

If possible suppose that $te_i = te_j \Longrightarrow e_i = e_j$

which is a contraduct to p even permutation $\therefore\ te_i \neq te_j$

$\therefore te_1, te_2, \dots te_p$ *are p odd permutations*

$\therefore p \leq q \rightarrow (1)$ $\quad (\because S_n$ *contains exactly q odd permutations*$)$

similarly we can prove that $to_1, to_2, \dots$ *are q distinct even permutations*

$\therefore q \leq p \rightarrow (2)$ $\quad (\because S_n$ *contains exactly p even permutations*$)$

From $(1)\ (2)$ $p = q$

Since $p + q = n! \Longrightarrow p + p = n! \Longrightarrow 2p = n! \Longrightarrow p = \frac{n!}{2}$

$\Longrightarrow p = q = \frac{n!}{2}$

$\therefore q = \frac{n!}{2}$

$\therefore$ *Every permutaion group* S_n *contains* $\frac{n!}{2}$ *even permutations and* $\frac{n!}{2}$ *odd permutations*

Alternating set: *Let* S_n *be a permutation group of order* $n!$. *The set of all even permutation is called as alternating set and it is denoted by* A_n

Theorem3: ***The alternating set*** A_n ***form a group of order*** $\frac{n!}{2}$ ***under product of permutation.***

Proof: $A_n = \{f/f \text{ is an even permutation of degree } n\}$

To prove that A_n *is a group under product of permutation.*

(i)***Closure property***: *Let* $f, g \in A_n \Longrightarrow f$*and* g *are even permutation*

. The product of two even permutation is also even permutation. $\therefore fg \in A_n$

(ii)***Associative property***: *Since permutation is a mapping and hence product of permutation is always associative. i. e.* $(fog)oh = fo(goh) \quad \forall f, g, h \in A_n$

(iii)***Identity property***: *Let* $I \in A_n \Longrightarrow I$ *is an even permutation.*

we know that every identity permutation is always even permutation.

Let $f \in A_n \Longrightarrow f$ *is even permutation* $\therefore foI = f = Iof$

(iv)***Inverse property***: *Let* $f \in A_n \Longrightarrow f$ *is even permutation*

We know that the inverse of even permutation is also even permutation. $\therefore f^{-1} \in A_n$

$\therefore fof^{-1} = I = f^{-1}of \quad \forall f \in A_n$

$\therefore$ *The alternating set* A_n *form a group of order* $\frac{n!}{2}$ *under product of permutation*

Theorem4: ***The alternating group*** A_n ***is a normal subgroup of*** S_n

proof: $S_n = \{f/f \text{ is a permutation of degree } n\}$ *is group of order* $n!$

$A_n = \{f/f \text{ is an even permutation of degree } n\}$ *is a group of order* $\frac{n!}{2}$

To prove that A_n *is a normal subgroup of* S_n

$(i) A_n \neq \phi, A_n \subseteq S_n$ (ii) *Let* $f, g \in A_n \Longrightarrow f$ *and* g *are even permutation*

$\Rightarrow f,^{-1} \in A_n \Rightarrow fg^{-1} \in A_n \therefore A_n$ *is a sbgroup of* S_n

$(iii) Let f \in S_n$ *and* $g \in A_n$ *since* $f \in S_n \Rightarrow f$ *is either even or odd*

Case(i) *If* f *is even*

Since f *is even* $\Rightarrow f^{-1}$*is also even.* f *is even, is even* $\Rightarrow fg$ *is also even*

$\therefore fg$ *is even,* $^{-1}$*is even* $\Rightarrow fgf^{-1}$ *is also even* $\therefore fgf^{-1} \in A_n$

Case(ii) *If* f *is odd*

Since f *is odd* $\Rightarrow f^{-1}$*is also odd.* f *is odd,* g *is even* $\Rightarrow fg$ *is odd*

$\therefore fg$ *is odd,* $^{-1}$*is odd* $\Rightarrow fgf^{-1}$ *is also even* $\therefore fgf^{-1} \in A_n$

$\forall f \in S_n, \forall g \in A_n \Rightarrow fgf^{-1} \in A_n$

$\therefore A_n$ *is a normal subgroup of* S_n

Theorem5: ***For any*** $n > 1$ *the set of all even permutaion in* S_n ***is a normal subgroup of*** S_n ***and order of*** A_n ***is*** $\frac{n!}{2}$ ***and the index of*** A_n ***in*** S_n ***is*** 2

Proof: *Let* $n > 1$ *and* $A_n = \{f \in S_n / f$ *is an even permutation of degree* $n\}$

we know that $G = \{1, -1\}$ *is a group under multiplication and* 1 *is the identity of* G.

Define $\phi: S_n \to G$ *by* $(f) = \{_{-1,}^{1,}$ $\begin{matrix} if\ f\ is\ even \\ if\ f\ is\ odd \end{matrix}$

we prove that $\phi: S_n \to G$ *is on − to homomorphism with* A_n *as kernel*

Case(i) *Let* f, g *are even* $\Rightarrow fg$ *is also even*

$\therefore (f) = 1, (g) = 1, (fg) = 1$

$(f)(g) = 1.1 = 1 = (fg)$

Case(ii) *Let* f, g *are odd* $\Rightarrow fg$ *is also even*

$\therefore (f) = -1, (g) = -1, \phi(fg) = 1$

$(f)(g) = (-1)(-1) = 1 = \phi(fg)$

Case(iii) *Let* f *is even,* g *are odd* $\Rightarrow fg$ *is odd*

$\therefore (f) = 1, (g) = -1, (fg) = -1$

$(f)(g) = 1(-1) = -1 = (fg)$

Case(iv) *Let* f *is odd,* g *is even* $\Longrightarrow fg$ *is odd*

$\therefore\ (f) = -1, (g) = 1, \phi(fg) = -1$

$(f)(g) = (-1).1 = -1 = (fg)$

In all above cases $\phi(fg) = \phi(f)\phi(g) \Longrightarrow \phi$ *is homomorphism*

Since $n > 1$, *he transposition* $(1\ 2)$ *in* S_n *is odd permutation and hence*

$(1\ 2) = -1$ *This shows that* ϕ *is on* $-$ *to*

$ker\phi = \{f \in S_n / \phi(f) = identity\ element\ in\ G\}$

$= \{f \in S_n / (f) = 1\}$

$= \{f \in S_n / f\ is\ even\}$

$= The\ set\ of\ all\ even\ permutations$

$= A_n$

By fundamental theorem of isomorphism, $\frac{S_n}{\ker \phi} \cong G \Longrightarrow \frac{S_n}{A_n} \cong G \Longrightarrow o\left(\frac{S_n}{A_n}\right) = o(G)$

$\Longrightarrow o\left(\frac{S_n}{A_n}\right) = 2 \Longrightarrow \frac{(S_n)}{(A_n)} = 2 \Longrightarrow o(A_n) = \frac{o(S_n)}{2} \Longrightarrow o(A_n) = \frac{n!}{2}$

Cayley's theorem 6: Every finite group is isomorphic to some permutation group

(OR)

Prove that a permutation group is isomorphic to a group on suitable finite set

Proof: *Let* G *be a finite group and* $a \in G$.

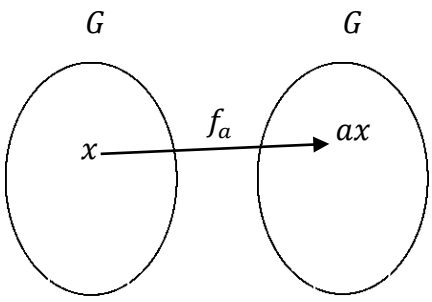
Define $f_a : G \to G$ *by* $f_a(x) = ax \quad \forall x \in G$

(i) f_a **is well − define and one − one:**

Let $x, y \in G \Longrightarrow x = y$

since $x = y \Leftrightarrow ax = ay \quad \forall a \in G$

$\Leftrightarrow f_a(x) = f_a(y)$



$\therefore f_a$ *is well defined and one* $-$ *one*

(*ii*)f_a *is on* $-$ *to:

Let $y \in G$ $(co - domain)$

since $a \in G, y \in G \Longrightarrow a^{-1}y \in G$

$\therefore f_a(a^{-1}y) = (a^{-1}y) = y$

$\forall y \in G$ *so* $\exists\ a^{-1}y \in G\ \ni f_a(a^{-1}y) = y$

$\therefore f_a$ *is on* $-$ *to and hence* f_a *is a permutation.*

Write $G^1 = \{f_a \in G / a \in G\}$

$=$ *The set of all permutations of* G *corresponding to every element of* G

To prove that G^1 *is a group under product of permutation.*

(*i*)*Closure property*: $L\ , f_a \in_b G^1$

since $a, b \in G$ *and* $x \in G$

$$f_a f_b(x) = f_a[f_b(x)]$$
$$= f_a(bx)$$
$$= a(bx)$$
$$= (ab)x$$
$$= f_a(x) \in G^1$$

$\therefore f_a f_b(x) = f_a(x) \in G^1 \Longrightarrow f\ f_a\ = f\ _b{}_a \in G^1 \longrightarrow (1)$

(*ii*)*Associative property*: $L\ , f_a, f_b \in_c G^1$

$Now\ (f_a f_b) f_c = (f_a{}_b) f_c$
$$= f^{(ab)c}$$
$$= f_{a(bc)}$$
$$= f_a(f_{bc})$$
$$= f_a(f_b f_c)$$

(*iii*)*Identity property*: *since* $e \in G \Longrightarrow f_e \in G^1$

$Let f_a \in G^1 \quad Now\ f_a f_e = f_{ae} = f_a$

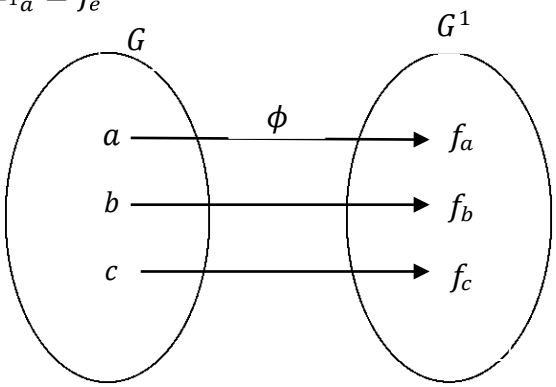
$similarly\ f_e f_a = f_{ea} = f_a$

(iv)Inverse property: $Let\ f_a \in G^1 \Longrightarrow a \in G \Longrightarrow a^{-1} \in G \Longrightarrow f_{a^{-1}} \in G^1$

$Now\ f_a f_{a^{-1}} = f_{aa^{-1}} = f_e\ similarly\ f_{a^{-1}} f_a = f_{a^{-1}a} = f_e$

$G^1\ is\ a\ permutation\ group.$

$Define\ \phi: G \to G^1\ by\ (a) = f_{\ a} \quad \forall a \in G$



$(i)\phi$ is well define and one − one:

$Let\ a, b \in G\ such\ that\ a = b$

$since\ a = b \Leftrightarrow ax = bx \quad \forall x \in G$

$\Leftrightarrow f_a(x) = f_b(x)$

$\Leftrightarrow f_a = f_b$

$\Leftrightarrow \phi(a) = \phi(b)$

$(ii)\phi$ is homo: $Let\ a, b \in G \Longrightarrow ab \in G$

$Now\ \phi(ab) = f_{ab}$

$= f_a f_b$

$= \phi(a)\phi(b)$

$\therefore \phi\ is\ homo$

$(ii)\phi$ is on − to:

$Let\ f_{\ b} \in G^1 \Longrightarrow b \in G$

$For\ this\ b \in G, we\ have\ \phi(b) = f_{\ b}$

$Thus \forall f_{\ b} \in G^1\ so\ \exists\ b \in G\ such\ that\ \ (b) = f_{\ \ b}$

$\therefore Every\ finite\ group\ is\ isomorphic\ to\ some\ permutation\ group$

Problems:

1.*Find the permutation group is isomorphic to the multiplicative group*

$G = \{1, \omega, \omega^2\}$

Sol: *Given that* $G = \{1, \omega, \omega^2\}$

By using Cayley's theorem, consider $f_a: G \to G$ *by* $f_a(x) = ax \quad \forall a \in G$

and x *is any element of* G

$\therefore f_a$ *is a permutation*

The permutation group is $G^1 = \{ , , \}$

where $f_1 = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1.1 & 1.\omega & 1.\omega^2 \end{pmatrix} = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega & \omega^2 \end{pmatrix}$ $f_\omega = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega.1 & \omega.\omega & \omega.\omega^2 \end{pmatrix} =$
$\begin{pmatrix} 1 & \omega & \omega^2 \\ \omega & \omega^2 & 1 \end{pmatrix}$

$f^{\omega^2} = \begin{pmatrix} 1 & \omega & \omega^2 \\ .\omega^2 1 & \omega^2.\omega & \omega^2.\omega^2 \end{pmatrix} = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \end{pmatrix}$

2. *Find the permutation group is isomorphic to the multiplicative group*

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

Sol: *Given that* $G = \{1, -1, , -i\}$

By using Cayleys theorem, consider $f^a: G \to G$ *by* $f^a(x) = ax \quad \forall a \in G$

and x *is any element of* G

$\therefore f^a$ *is a permutation*

The permutation group is $G^1 = \{ , , , \}$

where $f^1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1.1 & 1(-1) & 1.i & 1.(-i) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix}$

$f_{-1} = \begin{pmatrix} 1 & -1 & i & -i \\ -1.1 & -1(-1) & -1.i & -1.(-i) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix}$

$f_i = \begin{pmatrix} 1 & -1 & i & -i \\ i.1 & (-1) & i.i & i.(-i) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix}$

$f_{-i} = \begin{pmatrix} 1 & -1 & i & -i \\ -i.1 & -(-1) & -i.i & -i.(-i) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix}$

3. Find A_3 is a normal subgroup of S_3

Sol: $Given\ S = \{1,2,3\}$

$$S_3 = \{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\}$$

$A_3 = The\ set\ of\ even\ permtation$

$f_1 = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = Identity\ permutation\ so\ this\ is\ even$

$f_2 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} = (2\ 3) \rightarrow This\ transposition\ so\ it\ is\ odd$

$f_3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = (1\ 3\ ) \rightarrow odd$

$f_4 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = (1\ 2)) \rightarrow odd$

$f_5 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = (1\ 2\ 3) = (1\ 2)(1\ 3) = 2\ transposition\ so\ \ this\ is\ even$

$f_6 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = (1\ 3\ 2) = (1\ 3)(1\ 2) = 2\ transposition\ so\ \ this\ is\ even$

$A_3 = \{\ , f_1, f_5, f_6\}$ $is\ a\ normal\ subgroup\ of S_3$

CYCLIC GROUPS

Cyclic group: *Let* $(G,\cdot)$ *be a group and* $a \in G$ *then* $G = \{a^n / n \in \mathbb{Z}\}$ *is called as cyclic group generated by* $'a'$ *and is denoted by* $G =< a >$ *or* (a)

Note: *When we have taken addition* $G = \{na / n \in \mathbb{Z}\}$ *is a cyclic group generated by* $'a'$

Ex: 1. $P.T\ G = \{1, -1\}$ *is a cyclic group under multiplication.*

Sol: *Given that* $G = \{1, -1\}$

$Let\ a = 1 \quad Now\ 1^1 = 1, (1) \neq -1\ for\ any\ n \in \mathbb{Z} \Longrightarrow a = 1\ is\ not\ a\ generator\ of\ G$

$Let\ a = -1 \quad (-1)^1 = -1, (-1)^2 = 1 \Longrightarrow a = -1\ is\ a\ generator\ of\ G$

$\therefore G =< -1 > \Longrightarrow G\ is\ a\ cyclic\ group$

2. $P.T\ G = \{1, \omega, \omega^2\}$ *is a cyclic group under multiplication*.

Sol: *Given that* $G = \{1, \omega, ^2\}$

$Let\ a = 1 \quad Now\ 1^1 = 1, (1) \neq \omega, \omega^2\ for\ any\ n \in \mathbb{Z} \Longrightarrow a = 1\ is\ not\ a\ generator\ of\ G$

$Let\ a = \omega \quad (\omega\ )^1 = \omega, (\omega)^2 = \omega^2, (\omega)^3 = 1 \Longrightarrow a = \omega\ is\ a\ generator\ of\ G$

$Let\ a = \omega^2 \quad (\omega^2\ )^1 = \omega^2, (\omega^2)^2 = \omega, (\omega^2)^3 = 1 \Longrightarrow a = \omega^2\ is\ a\ generator\ of\ G$

$\therefore G =< \omega > \ and < \omega^2 > \Longrightarrow G\ is\ a\ cyclic\ group$

3. $P.T\ G = \{1, -1, , -i\}$ *is a cyclic group under multiplication*.

Sol: *Given that* $G = \{1, -1, , -i\}$

$Let\ a = 1 \quad Now\ 1^1 = 1, (1) \neq -1, , -i\ for\ any\ n \in \mathbb{Z} \Longrightarrow a = 1\ is\ not\ a\ generator\ of\ G$

$Let\ a = -1 \quad (-1\ )^1 = -1, (-1)^2 = 1, (-1)^n \neq i, -i$

$\Longrightarrow a = -1\ is\ not\ a\ generator\ of\ G$

$Let\ a = i \quad (i\ )^1 = i, (i)^2 = -1, (i)^3 = -i, (i)^4 = 1 \Longrightarrow a = i\ is\ a\ generator\ of\ G$

$Let\ a = -i \quad (-i\ )^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$

$\Longrightarrow a = -i\ is\ a\ generator\ of\ G$

$\therefore G =< i > \ and < -i > \Longrightarrow G\ is\ a\ cyclic\ group$

4. $P.T\ the\ n^{th}\ roots\ of\ unity\ is\ a\ cyclic\ group\ under\ multiplication$.

Sol: $Let\ G = \{e^{\frac{2k\pi i}{n}}/k = 0,1,2,\ldots(n-1)\}\ where\ \omega = e^{\frac{2\pi i}{n}}\ so\ G = \{1,\omega,\omega^2,\ldots\omega^{n-1}\}$

$Let\ a = \omega \quad Now\ (\ )^1 = \omega,\ (\omega)^2 = \omega^2,\ (\omega)^3 = \omega^3 \ldots (\omega)^{n-1} = \omega^{n-1}$

$\Longrightarrow a = \omega\ is\ a\ generator\ of\ G\ .i.e.\ G =< \omega >$

$\therefore G\ is\ a\ cyclic\ group.$

$Hence\ the\ n^{th}\ roots\ of\ unity\ is\ a\ cyclic\ group\ under\ multiplication$

5. $S.T\ Z_6 = \{0,1,2,3,4,5\}\ is\ a\ cyclic\ group\ of\ order\ 6\ under\ +_6$

Sol: $Z_6 = \{0,1,2,3,4,5\}$

$Let a = 1\ \ G = \{0(1),1(1),2(1),3(1),4(1),5(1)\} = \{0,1,2,3,4,5\}$

$\therefore G =< 1 > \Longrightarrow\ G\ is\ a\ cyclic\ group$

$Let a = 5\ \ G = \{0(5),1(5),2(5),3(5),4(5),5(5)\} = \{0,5,4,3,2,1\}$

$\therefore G =< 5 > \Longrightarrow\ G\ is\ a\ cyclic\ group$

6. $P.T\ (\mathbb{Z},+)\ have\ only\ two\ generators\ (OR)\ P.T\ (\mathbb{Z},+)\ is\ a\ cyclic\ group$

Sol: $Let\ \mathbb{Z} = \{\ldots -3,-2,-1,0,1,2,3\ldots.\}\ clearly\ (\mathbb{Z},+)\ is\ a\ group$

$Let\ a = 1\ then\ \{\ldots -3(1),-2(1),-1(1),0(1),1(1),2(1),3(1)\ldots.\}$

$= \{\ldots -3,-2,-1,0,1,2,3\ldots.\} = \mathbb{Z} \therefore \mathbb{Z} =< 1 > \Longrightarrow \mathbb{Z}\ is\ a\ cyclic\ group$

$Also -1\ is\ the\ additive\ inverse\ of\ 1 \therefore \mathbb{Z} =< -1 > \Longrightarrow \mathbb{Z}\ is\ a\ cyclic\ group$

$\therefore 1,-1\ are\ the\ generators\ of\ (\mathbb{Z},+)$

S.No	Infinite cyclic groups	Generators
1	$(\mathbb{Z},+)$	$1,-1$
2	$(2\mathbb{Z},+)$	$2,-2$
3	$(n\mathbb{Z},+)$	$n,-n$
4	$G = \{a^n/n \in \mathbb{Z}\}$	$a,\frac{-}{a}$
5	$G = \{2^n/n \in \mathbb{Z}\}$	$2,\frac{-}{2}$

Theorem1: *If 'a' is a generator of a cyclic group then a^{-1} is also generator of cyclic group*

(OR)

If $G =< a >$ then P.T $G =< a^{-1} >$

Proof: *Let $G =< a >$ be a cyclic group generated by' a'*

i.e. $G = \{a^n / n \in \mathbb{Z}\}$ Let $a^r \in G$ where $r \in \mathbb{Z}$

Now $a^r = (a^{-1})^{-r}$ where $-r \in \mathbb{Z}$

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

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

Theorem2: *Any infinite cyclic group G has exactly two generators*

Proof: *Let G be an ifinite cyclic group generated by a. Thus $(a) = 0$ or ∞*

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

Let a^m be a genrator of G since $a \in G$ so $\exists\, p \in \mathbb{Z}$ such that $(a^m)^p = a$

$\Longrightarrow a^{mp-1} = e \Longrightarrow (a) = mp - 1$

[*$p - 1 > 0$ then $\exists\, q = mp - 1 \ \ni a^q = e \Longrightarrow G$ is finite*]

$\therefore$ *G is infinite so $mp - 1 = 0 \Longrightarrow mp = 1 \Longrightarrow m = \pm 1$ or $p = \pm 1$*

$\therefore$ *G has exactly two generators*

Theorem3: *Every cyclic group is always an abelian. Is the converse true? justify your answer*

Proof: *Let $G =< a >$ be a cyclic group generated by a*

i.e. $G = \{a^n / n \in \mathbb{Z}\}$ Let $x, y \in G$ then $x = a^r, y = a^s$ where $r, s \in \mathbb{Z}$

Now $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$

$xy = yx \quad \forall x, y \in G \therefore G$ *is an abelian group*

The converse of the theorem need not be true

i.e. Every abelian group need not be a cyclic group.

Ex: $G = \{e, a, b, c\}$ *is an abelian group undermultiplication*

$Now\ (i)(e)^1 = e, (e)^2 = e \ldots (e)^n = e$

$\Longrightarrow e$ *is not a generator of* G

$(ii)(a)^1 = a, (a)^2 = e, (a)^3 = a, (a)^4 = e, (a)^5 = a \ldots$

$\Longrightarrow a$ *is not a generator of* G

$(iii)(b)^1 = b, (b)^2 = e, (b)^3 = b, (b)^4 = e, (b)^5 = b \ldots$

$\Longrightarrow b$ *is not a generator of* G

$(iv)(c)^1 = c, (c)^2 = e, (c)^3 = c, (c)^4 = e, (c)^5 = c \ldots$

$\Longrightarrow c$ *is not a generator of* G

$\therefore G$ *is not a cyclic group*

Hence every abelian group need not be a cyclic group

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Consider $G = \{A = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, B = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, = \begin{bmatrix}1 & -0\\ -0 & 1\end{bmatrix}, D = \begin{bmatrix}0 & 1\\ 1 & -0\end{bmatrix}\}$

Clearly is G an Abelian group w.r.t matrix multiplication.

$B = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, ^2 = \begin{bmatrix}-0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix} = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix} = C$

$B^3 = BB^2 = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix} = D$

$B^4 = B^2.B^2 = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = A$

$\cdot$	A	B	C	D
A	A	B	C	D
B	B	C	D	A
C	C	D	A	B
D	D	A	B	C

$G =< B > \Longrightarrow\ G$ *is a cyclic group*

***Theorem4**: Let G be a finite cyclic group of order n. Then for any* $1 \leq m \leq n$,

a^m ***is a generator of*** $G \Leftrightarrow m$ ***is relatively prime to*** $n.\ (i.e\ (m, n) = 1)$

Proof: *Given that* $G =< a >$ *and* $o(a) = |G| = n.$

For any $b \in G$, *we have* $< b > \subseteq G =< a >$ *and hence*

$G =< b > \Leftrightarrow < a > \subseteq < b > \Leftrightarrow a \in < b >$

$\therefore b$ is a generator of $G \Leftrightarrow a = b^S$ for some integer s.

Now, us fix $1 \leq m \leq n$. Then

a^m is a generator of $G \Leftrightarrow a = (a^m)^S$ for some $s \in \mathbb{Z}$

$\Leftrightarrow a^{ms-1} = e$ for some $s \in \mathbb{Z}$

$\Leftrightarrow (a)|ms - 1$

$\Leftrightarrow n|ms - 1$

$\Leftrightarrow ms - 1 = nt$ for some $t \in \mathbb{Z}$

$\Leftrightarrow ms - nt = 1$ for some $t \in \mathbb{Z}$

$\Leftrightarrow m$ is relatively prime to n. $(i.e\ (m,n) = 1)$

Theorem5*: *A cyclic group of order 'n' has exactly $\phi(n)$ generators

Proof: we know that $G =< a^m > \Leftrightarrow (m,) = 1$

$\Longrightarrow a^m$ is the generator of $G \Leftrightarrow m$ is a positive integer lessthan n and

which is relatively prime to n

The number of generators in $G \Leftrightarrow$ The number of positive integers less than n and

which are relatively prime to $n \Leftrightarrow \phi(n)$

$\therefore$ A cyclic group of order $'n'$ has exactly $\phi(n)$ generators

Eulerϕ function: Euler ϕ function is a function $\phi: \mathbb{N} \to \mathbb{N}$ defined as follows

$(i)\ (1) = 1\ \ (ii) r\ n(> 1) \in N$

$\phi(n) =$ The number of positive integers less than n and which are relatively

prime to n

Note: 1. If G is a cyclic group then $n = {p_1}^1 {p_2}^2 \ldots {p_k}^k$ where $p_{1,2}, \ldots p_k$ are primes

and $1 < p_1 < p_2 < \cdots < p_k$, $\alpha_{1,2}, \ldots \alpha_k$ are positive integers then

$(n) = n\,(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k})$

2. Further $n = p^\alpha$ where p is a prime and less than n then

$(n) = n\left(1 - \frac{1}{p}\right) = p^{\alpha}\left(\frac{p-1}{p}\right) = p^{\alpha-1}(p-1)$

3. *If p is a prime then* $(n) = n\left(1 - \frac{1}{p}\right) = p\left(\frac{p-1}{p}\right) = p - 1$

1. *Find the number of generators of a cyclic group of order* 10

Sol: $n = 10$ *then* $(10) = ?$ $\quad n = 10 = 2 \times 5 = 2^1 \times 5^1$

$(n) = n\left(1 - \frac{}{p_1}\right)\left(1 - \frac{}{p_2}\right) \Rightarrow \phi(10) = 10\left(1 - \frac{}{2}\right)\left(1 - \frac{}{5}\right) = 10\left(\frac{}{2}\right)\left(\frac{}{5}\right) = 4$

$\therefore (10) = 4$ $\quad$ *Generators are* $a^1, a^3, ^7, a^9$

2. *Find the number of generators of a cyclic group of order* 5,6,8,12,15,36,60,72,100,256 ?

Sol: $n = 5 \rightarrow$ *prime then* $(5) = 5 - 1 = 4$

$(ii) n = 6 = 2 \times 3 = 2^1 \times 3^1 \Rightarrow (6) = 6\left(1 - \frac{}{2}\right)\left(1 - \frac{}{3}\right) = 6\left(\frac{}{2}\right)\left(\frac{}{3}\right) = 2$

$(iii) n = 8 = 2^3 \Rightarrow (8) = 8\left(1 - \frac{}{2}\right) = 8\left(\frac{}{2}\right) = 4$

$(iv) n = 100 = 10 \times 10 = 2^2 \times 5^2 \Rightarrow (100) = 100\left(1 - \frac{}{2}\right)\left(1 - \frac{}{5}\right) = 100\left(\frac{}{2}\right)\left(\frac{}{5}\right) = 40$

$(iii) n = 256 = 2^8 \Rightarrow (256) = 256\left(1 - \frac{}{2}\right) = 256\left(\frac{}{2}\right) = 128$

Theorem6: ***Every subgroup of a cyclic group is cyclic***

Proof: *Let* $G = < a >$ *be a cyclic group generated by* $'a'$ *i.e.* $G = \{a^n / n \in \mathbb{Z}\}$

Let H be a subgroup of G

To prove that H is a cyclic group

Since $H \subseteq G \Rightarrow$ *Every element of H is an element of G*

Thus it follows that $a^n \in H$ *for some* $n \in \mathbb{Z}$

Let $'d'$ *be a least positive integer such that* $a^d \in H$

To prove that H is a generated by a^d $(i.e. H = < a^d >)$

Let a^m *be the generator of H for some* $m \in \mathbb{Z}$

$By\ division\ algorithm\ so\ \exists\ q, r \in\in \mathbb{Z}\ suchthat\ m = dq + r\ where\ 0 \leq r < d$

$Now\ a^m = a^{dq+r} = (a^d)^q a^r$

$since\ a^m \in H, a^d \in H \Longrightarrow a^{dq} \in H \Longrightarrow a^{-dq} \in H$

$By\ closure\ property\ a^m \in H, a^{-dq} \in H \Longrightarrow a^m a^{-dq} \in H \Longrightarrow a^{dq} a^r a^{-dq} \in H$

$\Longrightarrow a^r \in H\ \ where\ 0 \leq r < d$

$If\ \ 0 < r < d\ then\ a^r \in H\ \ \ which\ is\ a\ contraduct\ to\ a^d\ is\ \ least$

$\therefore r = 0$

$a^m = a^{dq+0} = (a^d)$

$which\ impies\ that\ every\ element\ in\ H\ is\ of\ the\ form\ (a^d)^q$

$\therefore H =< a^d >\ Hence\ H\ is\ a\ cyclic\ group.$

Theorem7: *Every subgroup of a cyclic group is a normal subgroup*

proof: 1. *Every subgroup of a cyclic group is cyclic*

2. *Every cyclic group is always abelian*

3. *Every subgroup of an abelian group is a normal subgroup*

Proof1: $Let\ G =< a >\ be\ acyclic\ group\ generated\ by\ 'a'\ i.e. G = \{a^n / n \in \mathbb{Z}\}$

$Let\ H\ be\ a\ subgroup\ of\ G$

$To\ prove\ that\ H\ is\ a\ cyclic\ group$

$Since\ H \subseteq G \Longrightarrow Every\ element\ of\ H\ is\ an\ element\ of\ G$

$Thus\ it\ follows\ that\ a^n \in H\ for\ some\ n \in \mathbb{Z}$

$Let\ 'd'\ be\ a\ least\ positive\ integer\ such\ that\ a^d \in H$

$To\ prove\ that\ H\ is\ a\ generated\ by\ a^d\ \ (i.e. H =< a^d >)$

$Leta^m\ be\ the\ generator\ of\ H\ forsome\ m \in \mathbb{Z}$

$By\ division\ algorithm\ so\ \exists\ q, r \in\in \mathbb{Z}\ suchthat\ m = dq + r\ where\ 0 \leq r < d$

$Now\ a^m = a^{dq+r} = (a^d)^q a^r$

$since\ a^m \in H, a^d \in H \Longrightarrow a^{dq} \in H \Longrightarrow a^{-dq} \in H$

$By\ closure\ property\ a^m \in H, a^{-dq} \in H \Longrightarrow a^m a^{-dq} \in H \Longrightarrow a^{dq} a^r a^{-dq} \in H$

$\Longrightarrow a^r \in H\ \ where\ 0 \leq r < d$

$If\ \ 0 < r < d\ then\ a^r \in H\ \ \ which\ is\ a\ contraduct\ to\ a^d\ is\ \ least$

$\therefore r = 0$

$a^m = a^{dq+0} = (a^d)$

$which\ implies\ that\ every\ element\ in\ H\ is\ of\ the\ form\ (a^d)^q$

$\therefore H =< a^d > Hence\ H\ is\ a\ cyclic\ group.$

Proof2: $Let\ G =< a > be\ a\ cyclic\ group\ generated\ by\ a$

$i.e. G = \{a^n / n \in \mathbb{Z}\}\ \ Let\ x, y \in G\ then\ x = a^r, y = a^s\ where\ r, s \in \mathbb{Z}$

$Now\ xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$

$xy = yx \quad \forall x, y \in G \therefore G\ is\ abelian\ group$

Proof3: Let G be an abelian group and H be a subgroup

To prove that H is a normal subgroup of G (i.e.$\forall h \in H, \forall x \in G \Longrightarrow xhx^{-1} \in H$)

Let.$h \in H,\ x \in G$

$xhx^{-1} = (x^{-1}h) \quad (\because x \in G \Longrightarrow x^{-1} \in G, h \in H \Longrightarrow h \in G \Longrightarrow x^{-1}h = hx^{-1},\ is\ abelian)$

$= (xx^{-1})h$

$= eh$

$= h \in H$

$xhx^{-1} \in H$ $\quad H$ is a normal subgroup of G

Theorem8: ***Evey quotient group of a cyclic group is also a cyclic group***

Proof: $Let\ G =< a > be\ a\ cyclic\ group\ generated\ by\ 'a'$

$i.e. G = \{a^n / n \in \mathbb{Z}\}$

$Let\ N\ be\ a\ subgroup\ of\ G$

$since\ G\ is\ cyclic\ and\ hence\ N\ is\ abelan\ (\because Every\ cyclic\ group\ is\ always\ abelian)$

$\therefore N\ is\ a\ normal\ subgroup\ of\ G\ (\because Every\ subgrop\ of\ an\ abelian\ is\ a\ normal\ subgroup\ )$

$\frac{G}{N} = \{Na/a \in G\}$ *is a quoti nt group u d r* $a \cdot Nb = Nab \quad \forall Na, \; b \in \frac{G}{N}$
e *n e N* *N*

To prove that $\frac{G}{N}$ *is a cyclic group*

$i.e.\frac{G}{N} =< Na >$ $(i.e.\frac{G}{N} \subseteq < Na > \; , < Na > \subseteq \frac{G}{N})$

$Let\ a \in G \Longrightarrow Na \in {}_N \Longrightarrow < Na > \in {}_N \Longrightarrow < Na > \subseteq {}_N \rightarrow (1)$

$Let\ Nx \in {}_N \Longrightarrow x \in G \Longrightarrow x = a^p\ where\ p \in \mathbb{Z}$

$Nx = Na^p = Na \cdot Na \cdot Na \cdot \ldots Na\ (p\ times)$

$= (Na)^p \in < Na >$

$\Longrightarrow Nx \in < Na >$

$\therefore {}_N \subseteq < Na > \rightarrow (2)$

$F(1) and\ (2)\ {}_N =< Na >$

$\therefore {}_N$ *is a cyclic group*

***Theorem9**: **Every group of prime order is a cyclic. Is the converse true**?*

***justify your answer**?*

***Proof**: Let G be a group such that $o(G) = p$ where p is a prime*

Let G be contains at least two elements, ce 2 is the least positive prime number.

Let $'a'$ be any element of G which is not an identity element $((e) = 1)$

$\therefore (a) \geq 2$ *Let* $(a) = m \Longrightarrow a^m = e$ *where m is the least positive integer*

$\therefore m \geq 2$

Let $H =< a >$ *is a cyclic subgroup of* G

$i.e.\, H = \{a^m/m \in \mathbb{Z}\} = \{a^1, ^2, a^3, \ldots a^m, a^{2m} \ldots\} = \{a^1, a^2, a^3, \ldots a^m = e\}$

$o(H) = m = o(a)$

By Lagranges theorem $o(H)|o(G) \Longrightarrow m|p$

since p is a prime and $m \geq 2$

$\therefore m = p \Longrightarrow o(H) = o(G)$

$\Longrightarrow H = G \Longrightarrow G$ *is a cyclic*

$\therefore$ *Every group of prime order is a cyclic*

The converse of above theorem need not be true

i.e. Every cyclic group of order need ot be prime

For example $G = \{1, -1, i, -i\}$ *is a cyclic group of order* 4 *but* 4 *is not a prime.*

Theorem10: ***Every group of prime order is abelian***

Proof: *First we prove that* 1. *Every group of prime order is a cyclic*

2. *Every cyclic group is always abelian*

Proof1: *Let G be a group such that* $o(G) = p$ *where p is a prime*

Let G be contains at least two elements, ce 2 *is the least positive prime number.*

Let $'a'$*be any element of G which is not an identity element* $((e) = 1)$

$\therefore (a) \geq 2$ *Let* $(a) = m \Longrightarrow a^m = e$ *where m is the least positive integer*

$\therefore m \geq 2$

Let $H =< a >$ *is a cyclic subgroup of G*

i.e. $H = \{a^m / m \in \mathbb{Z}\} = \{a^1, ^2, a^3, \ldots a^m, a^{2m} \ldots\} = \{a^1, a^2, a^3, \ldots a^m = e\}$

$o(H) = m = o(a)$

By Lagranges theorem $o(H)|o(G) \Longrightarrow m|p$

since p is a prime and $m \geq 2$

$\therefore m = p \Longrightarrow o(H) = o(G)$

$\Longrightarrow H = G \Longrightarrow G$ *is a cyclic*

$\therefore$ *Every group of prime order is a cyclic*

Proof2: *Let* $G =< a >$ *be a cyclic group generated by a*

$i.e. G = \{a^n / n \in \mathbb{Z}\}$ *Let* $x, y \in G$ *then* $x = a^r, y = a^s$ *where* $r, s \in \mathbb{Z}$

Now $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$

$xy = yx \quad \forall x, y \in G \therefore G$ *is an abelian group*

Theorem11: ***Any infinite cyclic group is isomorphic to the additive group of integer.***

proof: *Let G be an infinte group generated by'* a'.

Thus $(a) = 0$ *or* $\propto$ *and* $a^0 = e$

$\therefore \ G = \{a^n / n \in \mathbb{Z}\}$ *and let* $(\mathbb{Z}, +)$*be group under addition.*

Define $f: G \to \mathbb{Z}$ *by* $f(a^n) = n \quad \forall a^n \in G$

f is 1 − 1: *Let* $a^i, a^j \in G \ \ni f(a^i) = f(a^j)$

Since $f(a^i) = f(a^j) \Longrightarrow i = j \Longrightarrow a^i = a^j$

f is on − to: *Let* $k \in \mathbb{Z}$

$\therefore a^k \in G$ *and* $f(a^k) = k$

f is homo: *Let* $a^i, a^j \in G \ \Longrightarrow a^i a^j \in G$

Now $f(a^i a^j) = f(a^{i+j}) = i + j = f(a^i) + f(a^j)$

$\therefore f$ *is an isomorphism from G to* $\mathbb{Z}$

Theorem12: ***Every finite cyclic group G of order n is isomorphic to group*** $(\mathbb{Z}_n, +_n)$

Proof: *Let G be a finite cyclic group of order n generated by a. so* $o(a) = n$

$G = \{a^0 = e, ^1, a^2, \ldots a^{n-1}\}$

$\therefore G = \{a^m / m \in \ \mathbb{Z}$ *and* $0 \leq m < n\}$

$\mathbb{Z}_n = \{0,1,2, \ldots n-1\}$ *is a group under* $+_n$

Define $f: G \to \mathbb{Z}_n$ *by* $f(a^m) = m \quad \forall a^m \in G$

f is 1 − 1: *Let* $a^i, a^j \in G \ \ni f(a^i) = f(a^j)$

Since $f(a^i) = f(a^j) \Longrightarrow i = j \Longrightarrow a^i = a^j$

f is on − to: *Let* $k \in \mathbb{Z}$

$\therefore a^k \in G \text{ and } f(a^k) = k$

f is homo: $Let\ a^i, a^j \in G \implies a^i a^j \in G \implies a^{i+j} \in G$

$By\ division\ algorithm\ \exists\ q, r \in \mathbb{Z}\ \ni i + j = nq + r\ \ where\ 0 \leq r < n$

$a^{i+j} = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$

$f(a^i a^j) = f(a^{i+j}) = f(a^r) = r = f(a^i) +_n f(a^j)$

$\therefore f\ is\ an\ isomorphism\ from\ G\ to\ \mathbb{Z}_n$