5. Introduction to Groups Theory

5.1 Properties of groups

Groups:

Let G be a non-empty set and * be a binary operation on G.

G is called a group under the operation * if

(i) **Closed:** $a * b \in G, \forall a, b \in G$

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

(iii) **Identity:** There exists $e \in G$ such that $a * e = e * a = a, \forall a \in G$

(iv) **Inverse:** For every $a \in G$, there exists $a^{-1} \in G$ such that $a^{-1} * a = a * a^{-1} = e$.

It is denoted by $(G,*)$.

Abelian group:

A group $(G,*)$ is said to be an abelian group if it satisfies commutative property $a * b = b * a, \forall a, b \in G$.

Finite and infinite groups:

A group $(G,*)$ is said to be a finite group if G has a finite number of elements. Otherwise, it is called as an infinite group. If G has n elements, then $O(G) = n$.

1. **Check whether the set of integers under addition is an abelian group.**

   (i) $a + b \in Z, \forall a, b \in Z$

   (ii) $a + (b + c) = (a + b) + c, \forall a, b, c \in Z$

   (iii) There exists $0 \in Z$ such that $a + 0 = 0 + a = a, \forall a \in Z$

   (iv) For every $a \in G$, there exists $-a \in G$ such that $(-a) + a = a + (-a) = 0$.

   (v) $a + b = b + a, \forall a, b \in G$.

   Therefore, $(Z, +)$ is closed, associative, identity, inverse and commutative.

   Hence, $(Z,*)$ is an abelian group.

2. **Check whether the set of integers under subtraction is a group.**

   (i) $a - b \in Z, \forall a, b \in Z$

   (ii) $a - (b - c) \neq (a - b) - c, \forall a, b, c \in Z$

   Therefore, $(Z, -)$ is closed but not associative.

   Hence, $(Z, -)$ is not a group.

3. Check whether the set of integers under multiplication is a group.

(i) $a \times b \in Z, \forall a, b \in Z$

(ii) $a \times (b \times c) = (a \times b) \times c, \forall a, b, c \in Z$

(iii) There exists $1 \in Z$ such that $a \times 1 = 1 \times a = a, \forall a \in Z$

(iv) For every $a \in G$, $\frac{1}{a} \times a = a \times \frac{1}{a} = 1$. But $\frac{1}{a} \notin Z$

Therefore, $(Z,\times)$ is closed, associative, identity, but not inverse.

Hence, $(Z,\times)$ is not a group.

4. Check whether the set of all non-zero rational numbers under multiplication is a group.

(i) $a \times b \in Q - \{0\}, \forall a, b \in Q - \{0\},$

(ii) $a \times (b \times c) = (a \times b) \times c, \forall a, b, c \in Q - \{0\},$

(iii) There exists $1 \in Q - \{0\},$ such that $a \times 1 = 1 \times a = a, \forall a \in Q - \{0\},$

(iv) For every $a \in Q - \{0\}$, there exists $\frac{1}{a} \in Q - \{0\}$ such that $\frac{1}{a} \times a = a \times \frac{1}{a} = 1$.

Therefore, $(Q - \{0\},\times)$ is closed, associative, identity and inverse.

Hence, $(Q - \{0\},\times)$ is a group.

5. Prove that the set of all $n \times n$ non-singular matrices under matrix multiplication is a group but not abelian.

Let M be the set of all $n \times n$ non-singular matrices.

(i) $AB \in M, \forall A, B \in M$

(ii) $A(BC) = (AB)C, \forall A, B, C \in M$

(iii) There exists $I \in M$ such that $AI = IA = A, \forall A \in M$

(iv) For every $A \in M$, there exists $A^{-1} \in M$ such that $AA^{-1} = A^{-1}A = I$.

Therefore, $(M, \times)$ is closed, associative, identity and inverse.

Hence, $(M, \times)$ is a group.

Since $AB \neq BA$, $(M, \times)$ is not an abelian group.

6. Check whether the set of all fourth roots of unity under multiplication is a group.

Let $W = \{1, -1, i, -i\}$

(i) $a \times b \in W, \forall a, b \in W$

(ii) $a \times (b \times c) = (a \times b) \times c, \forall a, b, c \in W$

(iii) There exists $1 \in W$ such that $a \times 1 = 1 \times a = a, \forall a \in W$

(iv) For every $a \in W$, there exists $b \in W$ such that $b \times a = a \times b = 1$.

Therefore, $(W, \times)$ is closed, associative, identity and inverse.

Hence, $(W, \times)$ is a group.

7. Let G be a set of all non-zero real numbers and let $a * b = \frac{1}{2}(ab)$.

Show that $(G, *)$ is an abelian group.

(i) $a * b = \frac{1}{2}(ab) \in G, \forall a, b \in G$

(ii) $a * (b * c) = a * \frac{1}{2}(bc) = \frac{1}{2}\left\{a\frac{1}{2}(bc)\right\} = \frac{1}{4}\{a(bc)\} = \frac{1}{4}\{(ab)c\}$

$(a * b) * c = \frac{1}{2}(ab) * c = \frac{1}{2}\left\{\frac{1}{2}(ab)c\right\} = \frac{1}{4}\{(ab)c\}$

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

(iii) There exists $2 \in G$ such that

$a * 2 = \frac{1}{2}(a \times 2) = a, \forall a \in G$

$2 * a = \frac{1}{2}(2 \times a) = a, \forall a \in G$

(iv) For every $a \in G$, there exists $b = \frac{4}{a} \in G$ such that

$a * b = \frac{1}{2}(ab) = \frac{1}{2}\left(a \times \frac{4}{a}\right) = 2$

$b * a = \frac{1}{2}(ba) = \frac{1}{2}\left(\frac{4}{a} \times a\right) = 2$

(v) $a * b = \frac{1}{2}(ab) = \frac{1}{2}(ba) = b * a, \forall a, b \in G$

Therefore, $(G, *)$ is closed, associative, identity, inverse and commutative.

Hence, $(G, *)$ is an abelian group.

8. Let $\circ$ be an operation on Z defined by $x \circ y = x + y + 1$, prove that $(Z,\circ)$ is an abelian group.

(i) $x \circ y = x + y + 1 \in Z, \forall x, y \in Z$

(ii) $x \circ (y \circ z) = x \circ (y + z + 1) = x + y + z + 1 + 1$

$(x \circ y) \circ z = (x + y + 1) \circ z = x + y + 1 + z + 1$

Therefore, $x \circ (y \circ z) = (x \circ y) \circ z, \forall x, y, z \in Z$.

(iii) There exists $-1 \in Z$ such that

$x \circ (-1) = x - 1 + 1 = x, \forall x \in Z$

$(-1) \circ x = -1 + x + 1 = x, \forall x \in Z$

(iv) For every $x \in Z$, there exists $-x - 2 \in Z$ such that

$x \circ (-x - 2) = x - x - 2 + 1 = -1$

$(-x - 2) \circ x = -x - 2 + x + 1 = -1$

(v) $x \circ y = x + y + 1 = y + x + 1 = y \circ x, \forall x, y \in Z$

Therefore, $(Z,\circ)$ is closed, associative, identity, inverse and commutative.

Hence, $(Z,\circ)$ is an abelian group.

9. Let G be the set of all real numbers not equal to -1 and $*$ be defined by $a * b = a + b + ab$ then prove that $(G, *)$ is an abelian group.

(i) $a * b = a + b + ab \in G, \forall a, b \in G$

(ii) $a * (b * c) = a * (b + c + bc)$

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

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

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

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

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

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

(iii) There exists $0 \in G$ such that

$a * 0 = a + 0 + a(0) = a, \forall\ a \in G$

$0 * a = 0 + a + (0)a = a, \forall\ a \in G$

(iv) For every $a \in G$, there exists $-\frac{a}{1+a} \in G$ such that

$a * \left(-\frac{a}{1+a}\right) = a - \frac{a}{1+a} + a\left(-\frac{a}{1+a}\right) = \frac{a+a^2-a-a^2}{1+a} = 0$

$\left(-\frac{a}{1+a}\right) * a = -\frac{a}{1+a} + a + \left(-\frac{a}{1+a}\right)a = \frac{-a+a+a^2-a^2}{1+a} = 0$

(v) $a * b = a + b + ab = b + a + ba = b * a, \forall a, b \in G$

Therefore, $(G,*)$ is closed, associative, identity, inverse and commutative.

Hence, $(G,*)$ is an abelian group.

10. Theorem 1: In a group, prove that there exists only one identity element.

Suppose there are two identity elements $e_1, e_2 \in G$.

Since e_1 is an identity element, $e_1 a = a e_1 = a, \forall a \in G$.

Since e_2 is an identity element, $e_2 a = a e_2 = a, \forall a \in G$.

This shows that $a e_1 = a = a e_2$ and hence $e_1 = e_2$.

This means that e_1 and e_2 are not different.

Therefore, there exists only one element.

11. Theorem 2: In a group G, prove that every element has only one inverse.

Suppose a' and a'' are two inverse elements of $a \in G$.

Since a' is an inverse of a, $aa' = a'a = e$, where e is an identity element of G.

Since a'' is an inverse of a, $aa'' = a''a = e$, where e is an identity element of G.

Therefore, $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$.

This means that a' and a'' are not different.

Therefore, every element has only one inverse.

12. Theorem 3: For any elements a, b in a group G,

Prove that $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.

(i) Let $a^{-1} = c$. Then $ca = a^{-1}a = e$ and $ac = aa^{-1} = e$.

Therefore, $ca = ac = e$.

Hence, $a = c^{-1} = (a^{-1})^{-1}$

(ii) $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = (ae)a^{-1} = aa^{-1} = e$.

$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}(eb) = b^{-1}b = e$.

Therefore, $b^{-1}a^{-1}$ is the inverse of ab.

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

13. Theorem 4: Let G be a group and $a, b, x \in G$. Prove that left cancellation law and right cancellation law hold.

(i) To prove: $xa = xb \Rightarrow a = b$ (Left cancellation law)

$xa = xb \Rightarrow x^{-1}(xa) = x^{-1}(xb)$

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

$\Rightarrow ea = eb$

$\Rightarrow a = b$

Therefore, left cancellation law holds.

(ii) To prove: $ax = bx \Rightarrow a = b$ (Right cancellation law)

$ax = bx \Rightarrow (ax)x^{-1} = (bx)x^{-1}$

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

$\Rightarrow ae = be$

$\Rightarrow a = b$

Therefore, left cancellation law holds.

14. Theorem 5: Let G be a graph and $a, b \in G$. Then (i) The equation $ax = b$ has a unique solution in G. (ii) The equation $ya = b$ has a unique solution in G.

(i) $ax = a(a^{-1}b) = (aa^{-1})b = eb = b$

Therefore, $x = a^{-1}b$ is the solution of $ax = b$.

Suppose x_1 and x_2 are the two solutions of $ax = b$.

Then $ax_1 = b$ and $ax_2 = b$.

This implies that $ax_1 = ax_2$

By left cancellation law, $x_1 = x_2$.

Therefore, the two solutions of $ax = b$ are not different.

Hence, the equation $ax = b$ has a unique solution in G.

(ii) $ya = (ba^{-1})a = b(a^{-1}a) = be = b$

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

Suppose y_1 and y_2 are the two solutions of $ya = b$.

Then $y_1a = b$ and $y_2a = b$.

This implies that $y_1a = y_2a$

By right cancellation law, $y_1 = y_2$.

Therefore, the two solutions of $ya = b$ are not different.

Hence, the equation $ya = b$ has a unique solution in G.

15. Prove that a group G in which every element is its own inverse is abelian.

Let $a, b \in G$. By data, $a = a^{-1}, b = b^{-1}$ and $ab = (ab)^{-1}$

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

Therefore, G is an abelian group.

16. Prove that a group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}, \forall a, b \in G$

If part: Suppose G is abelian.

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

Only if part: Suppose $(ab)^{-1} = a^{-1}b^{-1}$

$ab = (a^{-1})^{-1}(b^{-1})^{-1}$ [Since $a = (a^{-1})^{-1}, b = (b^{-1})^{-1}$]

$= (a^{-1}b^{-1})^{-1}$ [Since $a^{-1}b^{-1} = (ab)^{-1}$]

$= (b^{-1})^{-1}(a^{-1})^{-1}$ [Since $(ab)^{-1} = b^{-1}a^{-1}$ in G]

$= ba$ [Since $(a^{-1})^{-1} = a$]

Therefore, G is abelian.

17. In a group G having more than one element if $x^2 = x$ for every $x \in G$.

Prove that G is abelian.

Let $a, b \in G$. By data, $a^2 = a, b^2 = b$ and $(ab)^2 = ab$

$a(ab)b = (aa)(bb) = a^2b^2 = ab = (ab)^2 = (ab)(ab) = a(ba)b$

By left cancellation law, $(ab)b = (ba)b$

By right cancellation law, $ab = ba$

Therefore, G is an abelian group.

18. Prove that a group G is an abelian if and only if $(ab)^2 = a^2b^2, \forall a, b \in G$

If part: Suppose G is an abelian.

$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$

Only if part: Suppose $(ab)^2 = a^2b^2$

$(ab)(ab) = (aa)(bb)$

$a(ba)b = a(ab)b$

By left cancellation law, $(ba)b = (ab)b$

By right cancellation law, $ba = ab$

Therefore, G is abelian.

5.2 Particular groups

1. The Klein 4-group

Consider a set $A = \{e, a, b, c\}$ on this set, suppose we define a binary operation described by the following table:

It is easy to verify that A is an abelian group under the binary operation defined.

e is the identity element of G and every element is its own inverse.

This group is of order 4.

It is called as the Klein 4-group or Quadratic group.

It is denoted by K_4 or V_4.

$\bullet$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Additive group of Integers modulo n

Let n be a specified positive integer ≥ 2. It is known that Congruent to modulo n is an equivalence relation on Z. This relation induces a partition of Z with the congruence classes. For any $a \in Z$, Additive group of Integers modulo the congruence class determined by the expression $[a] = \{x \in Z | x \equiv a \ (mod\ n)\} = \{a + nx | x \in Z\}$.

Now $[0] = \{0 + nx | x \in Z\}, [1] = \{1 + nx | x \in Z\}, \ldots , [n-1] = \{n - 1 + nx | x \in Z\}$

Let Z be the set of these equivalence classes. That is, $Z = \{[0], [1], [2], \ldots, [n-1]\}$.

Consider Z under the binary operation $addition\ modulo\ n$, denoted by $\oplus_n$.

This group is called additive group of integers modulo n and is denoted by $(Z_n, \oplus_n)$.

The order of this group is n.

Example: Operation table for $(Z_6, +)$ is given by

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	6	1	2	3	4

2. Multiplicative group of integers mod p

Let n be a given integer > 1 and Z_n denote the set of all congruence classes modulo n.

That is, $Z_n = \{[0], [1], [2], \ldots, [n-1]\}$.

Multiplication modulo n denoted by $\otimes_n$ *is* defined as

$[x] \otimes_n [y] = [x \times y], \forall [x], [y] \in Z_n$.

Consider Z_n under the binary operation multiplication modulo n denoted by $\otimes_n$.

(i) $[x] \otimes_n [y] \in Z_n, \forall [x], [y] \in Z_n$

(ii) $[x] \otimes_n \{[y] \otimes_n [z]\} = \{[x] \otimes_n [y]\} \otimes_n [z], \forall [x], [y], [z] \in Z_n$

(iii) There exists $[1] \in Z_n$, such that $[x] \otimes_n [1] = [1] \otimes_n [x] = [x]$.

(iv) For any $[x] \in Z_n$, there exists $[y] \in Z_n$ such that $[x] \otimes_n [y] = [y] \otimes_n [x] = [1]$, if n is a prime number.

(v) $[x] \otimes_n [y] = [y] \otimes_n [x], \forall [x], [y] \in Z_n$

Therefore, $(Z_n, \otimes_n)$ is an abelian group only if n is a prime number.

Note:

$(Z_p^+, \otimes_p)$ is the multiplicative group of integers modulo p.

It is also denoted by $(Z_p^+, \times)$.

$Z_p^+ = \{[0], [1], [2], \ldots, [p-1]\}$. Order of the group $O(Z_p^+) = p - 1$.

Operation table for $(Z_7^+, \times)$ is

Example 1: Find the operation table for $(Z_7^+, \times)$.

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	4	6	4	2
6	6	5	1	3	2	1

Example 2: Find all x in $(Z_{11}^{+}, \times)$ such that $x = x^{-1}$.

×	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

From the above table $x.x = 1$ is true only if $x = 1$ *or* 10.

1 and 10 are only elements of $(Z_{11}^{+}, \times)$ which are their own inverses.

That is, 1 and 10 are only solutions of $x^2 \equiv 1(mod\ 11)$

Example 3: If p is a prime, prove that $(p-1)! \equiv -1(mod\ p)$

[Wilson's theorem]

Consider the group $(Z_p^{+}, \times)$.

$Z_P^{+} = \{[1], [2], [3], \dots, [p-1]\}$

In Z_P^{+} , only $[1]$ and $[p-1]$ have their own inverses. $([x] = [x]^{-1})$

Remaining $(p-3)$ elements have $\frac{p-3}{2}$ pairs of the form $[x], [x]^{-1}$with $[x] \neq [x]^{-1}$.

Multiplying all these elements,

$2 \times 3 \times \dots \times (p-2) \equiv 1^{\frac{p-3}{2}}\ (mod\ p)$

$2 \times 3 \times \dots \times (p-2) \equiv 1\ (mod\ p)$

$2 \times 3 \times \dots \times (p-2) \times (p-1) \equiv 1 \times (p-1)\ (mod\ p)$

$(p-1)! \equiv (p-1)\ (mod\ p)$

$(p-1)! \equiv -1\ (mod\ p)$

This proves the result.

4. Permutation groups

Example : Permutation group of degree 3

Consider that set $A = \{1, 2, 3\}$. These 3 elements can be permuted in $3! = 6$ ways.

These permutations are $123, 132, 213, 231, 312, 321$. That is,

$$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Since these six permutations are 1-1 and onto functions from A to A, the composition of any two of these permutations is also a permutation.

If $S_3 = \{P_0, P_1, P_2, P_3, P_4, P_5\}$, composition table for S_3 is as below.

$\times$	P_0	P_1	P_2	P_3	P_4	P_5
P_0	P_0	P_1	P_2	P_3	P_4	P_5
P_1	P_1	P_2	P_0	P_5	P_3	P_4
P_2	P_2	P_0	P_1	P_4	P_5	P_3
P_3	P_3	P_4	P_5	P_0	P_1	P_2
P_4	P_4	P_5	P_3	P_2	P_0	P_1
P_5	P_5	P_3	P_4	P_1	P_2	P_0

S_3 is closed and associative under composition of permutations.

S_3 contains identity element P_0. S_3 contains inverse of each element.

By table, $P_0^{-1} = P_0, P_1^{-1} = P_2, P_2^{-1} = P_1, P_3^{-1} = P_3, P_4^{-1} = P_4, P_5^{-1} = P_5$.

Therefore, S_3 is a group under composition of permutations.

S_3 is a symmetric group of order 3. S_3 is not commutative.

Problem : Consider the symmetric group S_4 consists of all the permutations of the set $A = \{1, 2, 3, 4\}$.

What is the order of S_4? What is the identity element of S_4?

If $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix}$ verify that $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$.

(i) The order of $S_4 = 4! = 24$.

(ii) Identity element of $S_4 = P_0 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}$

(iii) $(\alpha\beta)^{-1} = \left(\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix}\right)^{-1}$

$= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix}$

$\beta^{-1}\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix}^{-1}\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}^{-1}$

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

Therefore, $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$.

5.3 Subgroups

Definition: A non-empty subset H of a group G is called a subgroup of G whenever H itself is a group under the binary operation in G.

Examples:

1. Under the usual addition, the set of all even integers is a subgroup of the group of integers.
2. Under the usual multiplication, the set of all even integers is the subgroup of the group of all non-zero real numbers.
3. Under the composition of permutations, $\{P_0, P_1, P_2\}, \{P_0, P_3\}, \{P_0, P_4\}$are the subgroups of the symmetric group $S_3 = \{P_0, P_1, P_2, P_3, P_4, P_5\}$.
4. Let $H = \{0, 2, 4\} \subseteq Z_0$, $(H, +)$ is a subgroup of $(Z_6, +)$.

Remarks:

1. For any group G, $e \in G$ and $\{e\} \subseteq G$.
   Since $\{e\}$ is a group under the operation in G, $\{e\}$ is a subgroup of G.
2. For any group G, $G \subseteq G$. Thus every group is a subgroup to itself.
3. $\{e\}$ and G are called **trivial subgroups** of a group G .
   All the other subgroups are called **proper subgroups** of G.

1. **Theorem 1: Prove that H is a subgroup of G if and only if $ab \in H$ and $a^{-1} \in H, \forall a, b \in H$.**

   If part:

   Suppose H is a subgroup of G.

   $\Longrightarrow H$ is a group under the same operation of G.

   $\Longrightarrow H$ is closed and H has inverse for each element of H.

   $\Longrightarrow ab \in H$ and $a^{-1} \in H, \forall a, b \in H$.

   Only if part:

   Suppose $ab \in H$ and $a^{-1} \in H, \forall a, b \in H$.

   Since $ab \in H$, H is closed.

   Since $H \subseteq G, a(bc) = (ab)c, \forall a, b, c \in H$. H is associative.

   Since $a, a^{-1} \in H, aa^{-1} = e \in H$ by given conditions. Hence H has identity element.

   Since $a^{-1} \in H$, for any $a \in H$, H has inverse.

   Therefore, H is a group.

   Since H is a group and $H \subseteq G$, H is a subgroup of G.

2. **Theorem 2: Prove that H is a subgroup of G if and only if $ab^{-1} \in H, \forall a, b \in H$.**

   If part:

   Suppose H is a subgroup of G.

   Then clearly, H is a group under the same operation of G.

   Hence, for any $a, b \in H, b^{-1} \in H$ and $ab^{-1} \in H$.

   Only if part:

   Suppose $ab^{-1} \in H, \forall a, b \in H$.

   By taking $b = a, aa^{-1} \in H$. Thus $e \in H$. Identity property holds.

   By taking $a = e$ and $b = a, ea^{-1} = a^{-1} \in H$. Inverse property holds.

   Since $b \in H, b^{-1} \in H,\ a(b^{-1})^{-1} \in H$, by given condition.

   Therefore, $ab \in H$. Closed property holds under the binary operation of G.

   Since associative property holds for all the elements of G, this holds for $H \subseteq G$.

   Therefore, H is a subgroup of G.

3. **Theorem 3: When H is finite, P.T. H is a subgroup of G if and only if $ab \in H, \forall a, b \in H$.**

If part:

H is a subgroup of G.

$\Longrightarrow$ H is a group.

$\Longrightarrow$ H is closed.

$\Longrightarrow ab \in H, \forall a, b \in H.$

Only if part:

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

That is, H is **closed.**

Since $H \subseteq G$ and G is associative, H is also **associative.**

Consider a set $aH = \{ah | h \in H\}$, for any $a \in H$.

Since $a \in H, ah \in H, for\ any\ h \in H.$

Therefore, $aH \subseteq H$. Since H is finite, aH is also finite.

Define a function $f: H \to aH$ by $f(h) = ah, \forall h \in H$.

Then $f(h_1) = f(h_2) \Longrightarrow ah_1 = ah_2 \Longrightarrow h_1 = h_2$, by left cancellation law.

Therefore, f is 1-1 from H to aH. Since f s finite, $|H| = |aH|$.

$aH \subseteq H, |H| = |aH| \Longrightarrow H = aH.$

Since $a \in H, a = ah_1$, for some $h_1 \in H$.

Since $a = ae, ae = ah_1$, for some $h_1 \in H$.

By left cancellation law, $e = h \in H$. **Identity** law holds.

$e \in H \Longrightarrow e \in aH \Longrightarrow e = ah_2$, for some $h_2 \in H$. $h_2 = a^{-1}$. **Inverse** property holds.

Therefore, H is a group. Since $H \subseteq G$, H is a subgroup of G.

This completes the proof of the theorem.

4. **Prove that the intersection of two groups of a group is a subgroup of the group.**

Let G be a group and H and K be two subgroups of G.

$a, b \in H \cap K \Longrightarrow a, b \in H\ and\ a, b \in K$

$\Longrightarrow ab^{-1} \in H\ and\ ab^{-1} \in K$

$\Longrightarrow ab^{-1} \in H \cap K$

Therefore, $H \cap K$ is a subgroup of G.

5. **Check whether the union of two subgroups of a group a subgroup?**

   Consider two subgroups of a symmetric group S_3 as $T_1 = \{P_0, P_3\}, T_2 = \{P_2, P_4\}$.

   But $T_1 \cup T_2 = \{P_0, P_2, P_3, P_4\}$ is not closed. Because $P_3P_4 = P_1 \notin T_1 \cup T_2$.

   Therefore, $T_1 \cup T_2$ is not a group.

6. **Let G be a group and $J = \{x \in G | xy = yx, \forall y \in G\}$. P.T. J is a subgroup of G.**

   $e \in G \Longrightarrow ey = ye, \forall y \in G$

   $\Longrightarrow e \in J$

   $\Longrightarrow J$ is non-empty.

   For any $a, b \in J$ and any $y \in G$,

   $(ab)y = a(by) = a(yb) = (ay)b = (ya)b = y(ab)$

   Therefore, $ab \in J$.

   $ya = ay$

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

   $\Longrightarrow (a^{-1}y)(aa^{-1}) = (a^{-1}a)(ya^{-1})$

   $\Longrightarrow (a^{-1}y)e = e(ya^{-1})$

   $\Longrightarrow a^{-1}y = ya^{-1}$

   Therefore, $a^{-1} \in J$

   Thus, $ab \in J, a^{-1} \in J, \forall a, b \in J$

   Therefore, J is a subgroup of G.

7. **Consider the subset H of the symmetric group S_4 consisting of the following elements of S_4. $P_0 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}, P_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}, P_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}$, $P_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$. Construct a table to show that H is an abelian group of S_4.**

$\times$	P_0	P_1	P_2	P_3
P_0	P_0	P_1	P_2	P_3
P_1	P_1	P_0	P_3	P_2
P_2	P_2	P_3	P_0	P_1
P_3	P_3	P_2	P_1	P_0

   This table shows that H is closed under permutation.

   Therefore, by theorem 3, H is a subgroup of S_4.

   The table also shows that the commutative law holds in H.

   Therefore, H is an abelian group.

8. **For the group Z_6^3, find subgroups of orders 6, 12 and 36.**

   Consider the group Z_6 of order 6.

   $Z_6^3 = Z_6 \times Z_6 \times Z_6$ is a group of order $6^3 = 216$.

   Every element of Z_6^3 is of the form (a, b, c) , where $a, b, c \in Z_6$.

   $H_1 = \{(a, 0, 0) | a \in Z_6\}$ is a subgroup of order 6.

$H_2 = \{(a, b, 0) | a \in Z_6, b = 0, 3\}$ is a subgroup of order 12.

$H_3 = \{(a, b, 0) | a, b \in Z_6\}$ is a subgroup of order 36.

5.4 Cyclic group

Definition:

A group is said to be the cyclic group if for some $a \in G$, every element $x \in G$ is of the form a^n, for some $n \in Z$. The element a is called the generator of the cyclic group G. It is denoted by $G =< a >$.

Example:

$G = \{i, -i, -1, 1\}$ is the cyclic group generated by i.

Every element of G is of the form i^n, for some $n \in Z$.

Hence, i is the generator of the cyclic group G.

Theorem 1:

If a is a generator of a cyclic group G, show that inverse of a is also a generator.

Proof:

a is a generator of the cyclic group G.

$\Longrightarrow$ If $g \in G$ then $g = a^n$, for some $n \in Z$.

$\Longrightarrow g = a^n = \{(a^{-1})^{-1}\}^n = (a^{-1})^{-n}$, for some $n \in Z$.

$\Longrightarrow$ a^{-1} is also a generator of the cyclic group G.

Examples:

1. **Show that the group $(G,*)$ is a cyclic group whose multiplication table is**

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

a is an identity element of G.

$b^2 = b * b = c$

$b^3 = b^2 * b = c * b = d$

$b^4 = b^3 * b = d * b = e$

$b^5 = b^4 * b = e * b = f$

$b^6 = b^5 * b = f * b = a$

Every element of G is an integral power of b.

Therefore, $(G,*)$ is a cyclic group.

2. **Prove that the Klein-4 group is not cyclic.**

In the Klein-4 group, every element is its own inverse.

$x^2 = x.x = e$

$x^3 = x^2.x = ex = x$

If n is even, $x^n = x^{2r} = (x^2)^r = e^r = e$

If n is odd, $x^n = x^{n-1}.x = ex = x$

Therefore, every integral power of x is equal to either e or x.

$\Longrightarrow$ No element in this group can be a generator.

$\Longrightarrow$ Klein-4 group is not cyclic.

3. **Prove that the multiplicative group of non-zero rational numbers are not cyclic.**

Consider $(Q^*,\times)$.

Q^* is the set of all non-zero rational numbers and $\times$ is the usual multiplication.

Suppose $(Q^*,\times)$ is cyclic.

$\Longrightarrow$ There is a non-zero rational number $\frac{p}{q} \neq 1$ as a generator.

$\Longrightarrow$ Since $2, 3 \in Q^*$, we have $2 = \left(\frac{p}{q}\right)^m$ and $3 = \left(\frac{p}{q}\right)^n$ for some $m, n \in Z$.

$\Longrightarrow$ This gives $2^n = 3^n$, which is impossible.

Therefore, $(Q^*,\times)$ is not cyclic.

4. **Prove that the group $(Z_4, +)$ is cyclic. Find all its generators.**

The elements of Z are the congruent classes $[0], [1], [2], [3]$.

The operator $+$ is $'addition\ modulo\ 4'$.

$$[1] = [1]^1$$

$$[2] = [1] + [1] = [1]^2$$

$$[3] = [1] + [1] + [1] = [1]^3$$

$$[4] = [1] + [1] + [1] + [1] = [1]^4$$

Therefore, every element of Z is an integral power of $[1]$.

Therefore, $(Z_4, +)$ is a cyclic group.

$[1]$ is the generator of Z_4.

$[1]^{-1} = [-1] = [4 - 1] = [3]$ is also a generator of Z_4.

$[0]^n \neq [1]$, for any $n \in Z$.

$[2]^n \neq [1]$, for any $n \in Z$.

Therefore, $[1]$ and $[3]$ are the only generators of Z_4 .

5.5 Lagrange's theorem

If G is a finite group and H is a subgroup of G, then $O(G)|O(H)$.

Proof:

H is a subgroup of a finite group G.

$\Longrightarrow$ H is also finite.

$\Longrightarrow H = \{h_1, h_2, h_3, \dots, h_n\}$, where each h_i is distinct.

$\Longrightarrow Ha = \{h_1a, h_2a, h_3a, \dots, h_na\}$, where each h_ia is distinct.

$\Longrightarrow$ The right coset Ha has n distinct elements.

Since G is finite, there are a finite number of distinct right cosets.

Let $G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k$

$\Longrightarrow O(G) = |Ha_1| + |Ha_2| + \cdots + |Ha_k| = n + n + \cdots k\ times = nk$

$\Longrightarrow\ n|O(G)$

$\Longrightarrow\ O(H)|O(G)$