SOUTH EASTERN UNIVERSITY OF SRI LANKA
Faculty of Applied Sciences
Department of Mathematical Sciences

MTM 12221 GROUP THEORY 1
2021/ 2022

Course Contents:
Binary operations, Groups, Subgroups , Order of an element, Order of a group, Cyclic groups, Permutation groups, Even and odd permutations

1. Binary Operation and Group Axioms

1.1 Binary operation

Definition 1.1 Let G be a non-empty set. Any mapping (or rule) $*: G \times G \to G$ is called a binary operation (or binary composition) on G which we will usually denote by $*(a,b) = a * b$. If $*$ is a binary operation on G, we say that G is closed under $*$.

Remark: If $*$ is a binary operation on G, then
(i) the operation $*$ is **well-defined**: for any $a, b \in G$, there is exactly one $c \in G$ such that $a * b = c$.
(ii) G is **closed** under $*$: for all $a, b \in G$, $a * b = c \in G$.

Examples 1.1 Tick (√) if $*$ is a binary operation on the given set or give a counter example:

Set	**Operation**	**Binary**
$\mathbb{Z}$	Addition	
	Subtraction	
	Multiplication	
	Division	
Set of all $m \times n$ matrices with real entries: $M_{m\times n}(\mathbb{R})$	Matrix Addition	
Set of all square matrices of order n	Matrix Multiplication	
set of all polynomials of degree less than or equal to n : $P_n(x)$	Polynomial Addition	
	Polynomial Multiplication	
$\mathbb{R}$	division	
$\mathbb{N}$	subtraction	

1.2 Groups

Definition 1.2 A non-empty set G together with a binary operation $*: G \times G \to G$ is called a ***group*** if the following axioms hold:

G1: Associative property.
That is, for every $a, b, c \in G$,

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

G2: Existence of identity
That is, for all $a \in G$, there exist an element $e \in G$ such that

$$a * e = e * a = a$$

G3: Existence of inverse
That is, for each $a \in G$, there exist an element $b \in G$ such that

$$a * b = b * a = e.$$

A group is said to be **abelian** if the axiom

G4: Commutativity
That is, for all $a, b \in G$

$$a * b = b * a$$

holds in addition to group axioms G1, G2 and G3.

Remarks:

(i) We'll often write $(G,*)$ to distinguish the operation on G. If the operation is understood, we'll just write G for the group.

(ii) One should verify that G is non-empty and $*$ is a binary operation before check the axioms G1, G2, G3 and G4.

(iii) Identity element e depends only on both the set G and the binary operation $*$.

(iv) Inverse element b of an element $a \in G$ depends on a, G and $*$.

(v) To check G2 and G3, it is enough to check <u>both</u> identity element and inverse only <u>in one direction</u>: that is check

$$e * a = a \quad \text{and} \quad b * a = e$$

[In this case, we say that e is the left identity of G and b is the left inverse of a in G] or check

$$a * e = a \quad \text{and} \quad a * b = e$$

[In this case, e is the right identity of G and b is the right inverse of a in G].

Example 1.2 Well-known abelian Groups

(i) $(\mathbb{Z}, +)$ is an abelian group. Identity element is $0(\in \mathbb{Z})$ and the inverse of $n \in \mathbb{Z}$ is $-n$.

(ii) $(M_n(\mathbb{R}), +)$ is an abelian group.
If $A = (a_{ij}) \in M_n(\mathbb{R})$, then the zero matrix is the identity element and $-A = (-a_{ij})$ is the additive inverse.

(iii) $(\wp_n(x), +)$ is an abelian group. zero polynomial is additive identity and for any $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \wp_n(x)$, $-p(x) = -a_0 - a_1x - a_2x^2 - \cdots - a_nx^n \in \wp_n(x)$ is the additive inverse.

Example 1.3 Non-Groups

(i) $(\mathbb{Z}, \times)$ is not a group. Multiplication on $\mathbb{Z}$ is associative, 1 is the identity element $(1 \times n = n \times 1 = n$ for any $n \in \mathbb{Z})$ but for any $n\backslash\{1\} \in \mathbb{Z}$, inverse element does not exist. That is, $n \times \frac{1}{n} = 1$ however $\frac{1}{n} \notin \mathbb{Z}$ if $n \neq 1$.

(ii) $M_n(\mathbb{R}),\times)$ is not a group because a matrix with zero determinant has no inverse. However, set of all invertible matrices of same size is a group but not abelian as matrix multiplication is not commutative.

(iii) $\mathbb{Q}$ = set of all rational numbers $= \left\{\frac{p}{q} \middle| p, q \in \mathbb{Z}, q \neq 0\right\}$, $\mathbb{R}$ = set of all real numbers, $\mathbb{C}$ = set of all complex numbers $= \{a + ib | a, b \in \mathbb{R}$, and $i^2 = -1\}$ are additive abelian groups but not multiplicative groups.

(iv) $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}, \mathbb{C}\backslash\{0\}$ are multiplicative abelian groups. 1 is the identity element and $\frac{1}{a}$ is the inverse of a.

Remark: Let G be a nonempty set and H be a nonempty subset of G. Let $*$ be an operation defined on both G and H.

(i) If $*$ is a binary operation on one set (G or H), then it need not to be binary on the other.

(ii) If $*$ is associative on the super set G, it is associative on the subset H, but the converse need not to be true.

(iii) If e is the identity element of G and if $e \in H$, then e is the identity element of H.

(iv) If a^{-1} is the inverse of $a \in G$ and $a, a^{-1} \in H$, then a^{-1} is the inverse of $a \in H$.

Example 1.4 A binary operation on $\mathbb{Z}$ is defined as $a * b = a + b + 1$ for all $a, b \in \mathbb{Z}$. Show that $(\mathbb{Z},*)$ is an group.

Example 1.5 Let $G = \{(a, b) \mid a, b \in \mathbb{R}$ with $a \neq 0\}$. Define an operator $*$ on G by

$$(a, b) * (c, d) = (ac, bc + d).$$

Show that $(G,*)$ is a group. Is it Abelian? Justify your answer.

1.3 Group Tables

An easy way to handle a (small) finite group is preparing *group table* (or *Cayley table*). Let us explain it using the following example.

Example 1.6 Construct the Cayley table for the set of all solutions A of the equation $x^4 = 1$ under (complex) multiplication and show that this forms a group.

Notation:

- If there is no confusion between the binary operations $*$ and the usual multiplication $\times$, we usually write ab instead of $a * b$. Further,

$$a^n = \underbrace{a * a * \cdots * a}_{n \text{ times}} \quad \text{and} \quad a^{-n} = (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * \cdots * a^{-1}}_{n \text{ times}} .$$

- However, in additive type groups we use na for $a * a * \cdots * a$ (n times). That is,

$$na = \underbrace{a * a * \cdots * a}_{n \text{ times}} \quad \text{and} \quad -na = n(-a) = \underbrace{(-a) * (-a) * \cdots * (-a)}_{n \text{ times}}.$$

- We may write 1 for the identity element of multiplicative type groups and 0 for the additive type groups, if there is no confusion with real numbers 1 and 0.
  For example, 0 element of the group $(M_2(\mathbb{R}), +)$ is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

1.4 Order of a Group and element

Definition 1.3 The order of a group G, denoted by $|G|$, is the number of elements in G. If a group G has infinitely many elements, we will write $|G| = \infty$.

A group G is said to be finite if $|G| < \infty$.

$(\mathbb{Z}, +), (M_n(\mathbb{R}), +), (\mathbb{Q}\backslash\{0\}, \times), (\mathbb{R}\backslash\{0\}, \times), (\mathbb{C}\backslash\{0\}, \times)$ are examples for infinite group.
Order of the group G in example 1.6 is 4 and hence it is a finite group.

Definition 1.4 Order of an element of a group
Let a be an arbitrary element of a group G. The least positive integer m ,if it exists, such that $a^m = e$ (or $ma = e$), where e is the identity element of G, is called the order of the element a and is denoted by $\circ(a) = m$ or $|a| = m$. If there is no such m for an element $a \in G$, we say that a has infinite order and denote $\circ(a) = \infty$ or $|a| = \infty$.

Theorem 1.1 Every element of a finite group has finite order.

Example 1.7 Find the order of the group G and the order of each of the element 1, i given in example 1.6.

Observations:
- ✓ Order of the identity element is 1.
- ✓ Order of an element is equal to order of its inverse.
- ✓ Order of an element divides order of the group.

EXERCISES 1

1. Determine whether each of the following operation $*$ is a binary operation on the corresponding sets. If $*$ is a binary operation, determine whether $*$ is associative and whether $*$ is commutative. Also, decide whether the given set is a group under the respective operation
   (i) On $\mathbb{N}$, define $*$ by $a * b = a^b$.

(ii) On $\mathbb{R}\backslash\{1\}$, define $*$ by $a * b = 2(a+b) - ab$.
(iii) On $\mathbb{N}$, define $*$ by $a * b =$ the largest integer less than ab.
(iv) On $\mathbb{Q}$, define $*$ by $a * b = 2a + b + 1$.
(v) On $\mathbb{N}$, define $*$ by $a * b = |ab| - a$.
(vi) On $\mathbb{Q}$, define $*$ by $a * b = ab/2$.
(vii) On $\mathbb{N}$, define $*$ by $a * b = (ab)^2$.
(viii) On $\mathbb{Q}$, define $*$ by $\frac{a}{b} * \frac{c}{d} = \frac{a+c}{bd}$.
(ix) On $\mathbb{Z}$, define $*$ by $a * b = 1$.
(x) On $\mathbb{Z}$, define $*$ by $a * b = 1 - 2ab$.

2. Show that set of all 2×2 matrices of the form $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, b, d \in \mathbb{R},\ ad \neq 0 \right\}$ is a group under ordinary matrix multiplication. Is this group abelian? Justify your answer.

3. A binary operation on $\wp_2(x) = \{a + bx + cx^2 \mid a, b, c \in \mathbb{R}\}$ is defined as $p_1(x) * p_2(x) = 2p_1(x) - p_2(x)$ for all $p_1(x), p_2(x) \in \wp_2(x)$. Determined whether $(\wp_2(x), *)$ is a group.

4. A binary operation on $\mathbb{R}\backslash\{-\frac{1}{2}\}$ is defined as $a * b = a + b + 2ab$ for all $a, b \in \mathbb{R}\backslash\{-\frac{1}{2}\}$. Show that $\left(\mathbb{R}\backslash\{-\frac{1}{2}\}\ , *\right)$ is a group. Is this group abelian? Justify your answer.

5. Let $G = \{(x, y) \in \mathbb{R}^2 | y \neq 0\}$. Define an operation $*$ on G such that
$$(a, b) * (x, y) = (a + x, by).$$
Show that $(G, *)$ is an abelian group.

6. Let the operation $*$ be defined on a set $A = \{a, b, c, d, e\}$ by means of the following composition table.

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

(i) Is $*$ a binary operation on A? Give a reason.
(ii) Compute $[(b * c) * (d * a)] * e$
(iii) Is $*$ associative on A? Give a reason.
(iv) Prove or disprove: $*$ commutative on A.

7. Let G consists of all roots (real or complex) of the equation $x^3 = 1$. Construct the composition table for G under multiplication and show that G is an abelian group. What is the order of G? Find the orders of the roots other that $x = 1$.

2. Basic Theorems of Groups

Theorem 2.1 Uniqueness of identity
The identity element of a group is unique.

Theorem 2.2 Cancellation laws

Let a, b, c be arbitrary elements of a group G. Then,

Left cancellation law: $a * b = a * c \Longrightarrow b = c$.

Right cancellation law: $b * a = c * a \Longrightarrow b = c$.

Theorem 2.3 Uniqueness of inverse

The inverse of each element of a group is unique.

Theorem 2.4 Let G be a group. Then, for any $a, b \in G$

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

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

EXERCISES 2

1. Let G is a set and $*$ is a binary operation on G such that the following conditions are satisfied:
   (i) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
   (ii) There exists an element e in G such that $e * e = e$.
   (iii) For each $a \in G$, there exists b in G such that $b * a = e$.
   (iv) For $a, b, c \in G$, if $a * b = e$ and $a * c = e$, then $b = c$.
   Show that G is a group.
   (Hint: Show that e is the left identity).

2. If G is a group and $a, b \in G$, then show that the equation $ax = b$ has a unique solution.

3. Suppose that $(G,*)$ is a group and $a \in G$. If $a * a = e$, then show that $a = e$, where e is the identity element of G.

3. Subgroups

Definition 3.1 Subgroups

Let $(G,*)$ be a group and let H be a non-empty subset of G. Then, H is said to be a subgroup of G if H is also a group under the same binary operation $*$. If H is a subgroup of G, we denote it by $H \leq G$.

Definition 3.2 Trivial and proper subgroups

The sets $\{e\}$ and G itself are subgroups of any group G. They are called the trivial subgroups of G. The subgroups which are not trivial, if any, are known as proper subgroups.

Theorem 3.1 Let H be a non-empty subset of a group G. Then,

i. $H \leq G$ if and only if $ab^{-1} \in H$ for all $a, b \in H$.

ii. In particular, if H is finite, then $H \leq G$ if and only if $ab \in H$ for all $a, b \in H$.

Theorem 3.2 Let G be a finite group and H be any subgroup of G. Then $|H|$ divides $|G|$.

Theorem 3.3 Every subgroup of an abelian subgroup is always abelian. Subgroup of a non-abelian group may or may not be abelian.

Example 3.1 Let $G = \{(a,b)|a,b \in \mathbb{R} \text{ with } a \neq 0\}$. Let the peration $*$ be defined on G such that

$$(a,b) * (c,d) = (ac, bc + d).$$

Show that G is a non-abelian group. Define $H_1 = \{(a,b)|a,b \in \mathbb{Q} \text{ with } a \neq 0\}$ and $H_2 = \{(a,0) \mid a \in \mathbb{R}\backslash\{0\}\}$. Show that H_1 is a non-abelian subgroup whereas H_2 is abelian subgroup.

EXERCISES 3

1. Let $G = \{(a,b) \mid a \in \mathbb{Z}, b \in \mathbb{Q}\}$. An operator on G is defined by
   $$(a,b) * (c,d) = (a + c, 2^c b + d).$$
   Show that $*$ is a binary operation and that $(G,*)$ is a group. Is G abelian?
   Show that $H = \{(a,0)|a \in \mathbb{Z}\}$ is a subgroup of G.

2. Let g be a fixed element of a group G and let $C(G) = \{x \in G|xg = gx\}$. Show that $C(G)$ is a subgroup of G. (This subgroup is called *centralizer* of g).

3. Let G be a group and let $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$. Show that $Z(G)$ is a subgroup of G. (This subgroup is called the *centre* of the group G)

4. Let g be a fixed element of a group G and let $H = \{x \in G \mid x = g^n, n \in \mathbb{N}\}$. Show that H is a subgroup of G.
   Let G be the set of all 2×2 matrices with unit determinant under usual matrix multiplication. Form a subgroup H of G which contains the element $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
   Construct the group table. Is H abelian?

5. Show that intersection of two subgroups of a group G is a subgroup of G.

6. Let n be any fixed integer. Show that the set $H_n = \{nx \mid x \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$. Is it abelian? Justify your answer.

   Hence show that the union of two subgroups of a group G need not to be a subgroup of G.

4 Cyclic Groups

Definition 4.1 Cyclic Groups

A group is said to be cyclic if there exists an element $a \in G$ such that any element $b \in G$ can be obtained by operating a by itself several times. That is, G is cyclic if $b = a^n$ or $b = na$ according as the operation is of multiplicative or additive type.
In this case, we say that a is a generator of G and write $G =< a >$.

Theorem 4.1 For any positive integer m, let $\mathbb{Z}_m$ be the set of all residue classes of integers modulo m. Then, $(\mathbb{Z}_m, +)$ is a cyclic group and $\mathbb{Z}_m =< [1] >$.

Recall: $\mathbb{Z}_m = \{[0],\ [1],\ [2],\ \cdots,\ [m-1]\}$.
For example, $\mathbb{Z}_8 = \{[0],\ [1],\ [2],\ \cdots,\ [7]\}$.
Then, $[3] + [6] = [9] = [1]$ as when you divide 9 by 8, the reminder is 1.
$[3] \times [6] = [18] = [2]$ as when you divide 18 by 8, the reminder is 2.

Identity element of the group is $[0]$ as $[a] + [0] = [0] + [a] = [a]$.

Inverse of $[a]$ is $[m-a]$ as $[m-a] + [a] = [0]$.

Example 4.1 Complete Cayley table for $(\mathbb{Z}_6, +)$. Is this group abelian?
Find $|2|$ and $|3|$.
$[1]$ is a generator. Find another generator for this group.
Find the subgroups of $(\mathbb{Z}_6, +)$.
Complete composition table for $\mathbb{Z}_6$ under $\times$ and verify that $\mathbb{Z}_6$ is not a group under multiplication modulo 6.

Theorem 4.2 For any positive integer m, let

$$\mathbb{Z}_m^* = \{[a] \mid 1 \leq a \leq m \text{ and } \gcd(a, m) = 1\}.$$

Then, $\mathbb{Z}_m^*$ is an abelian group with respect to multiplication modulo m.
In particular, if m is prime, then it is cyclic.

If m is prime, then $\mathbb{Z}_m^* = \{[1],\ [2],\ \cdots,\ [m-1]\}$.

Example 4.2 Complete Cayley table for $(\mathbb{Z}_{12}^*, \times)$. Is this a group? If so is it abelian and find $|5|$ and $|7|$.

Example 4.3 Complete Cayley table for $(\mathbb{Z}_5^*, \times)$. Is this group abelian?
Find all the generators and subgroups of $(\mathbb{Z}_5^*, \times)$.

Theorem 4.3 Any cyclic group is abelian.

Theorem 4.4 A subgroup of a cyclic group is cyclic.

Definition 4.2 Euler-phi function

The Euler-phi function $\phi(n)$ is the number of positive integers x $(\leq n)$ that have no common divisors with n.

For example, $\phi(12) = 4$ as 1, 5, 7, 11 are relatively prime to 12.

How many generators are there for a finite cyclic group?

Theorem 4.5 Let G be a cyclic group of order n. Then, G has $\phi(n)$ generators. Moreover, If d divides n, the number of elements of order d in G is $\phi(d)$. It is 0 otherwise.

Example 4.4 Verify the theorem 4.5 for the example 4.3

EXERCISES 4

1. Define the terms *cyclic group* and *generator* of a cyclic group.
   Prove each of the following:
   (a) A cyclic group is abelian.
   (b) A subgroup of a cyclic group is cyclic.
   (c) Inverse of a generator of a cyclic group is again a generator.

Note:- Let G be a cyclic group of order n generated by an element $a \in G$. The element a^m (or ma) is also a generator if $\gcd(m,n) = 1$.

2. How many generators are there of the cyclic group of order (i) 8, (ii) 10.

3. Show that the group $(\mathbb{Z}_{10}^{\times},\times)$ is a cyclic group of order 4.
   Find all generators of this cyclic group. Verify that order of the group is equal to order of each generator.
   Find the subgroup of $\mathbb{Z}_{10}^{\times}$ generated by the element $[9] \in \mathbb{Z}_{10}^{\times}$.

4. Show that additive group of residue classes $\mathbb{Z}_8 = \{[0],[1],[2],\cdots,[7]\}$ modulo 8 is a cyclic group.
   Find all generators of this cyclic group.
   Verify that order of the group is equal to order of each generator.
   Verify also that inverse of each generator is again a generator.
   Find the subgroup of generated by the element $[9] \in \mathbb{Z}_{10}^{\times}$.

5. Show that the set U_n of n^{th} roots of unity (i.e. the solutions of the equation $x^n = 1$) forms a cyclic group with respect to multiplication. Find all generators of U_4 and U_5.

6. Show that the abelian group $\mathbb{Z}_8^{\times}$ under multiplication is not cyclic.

7. Show that $H = \{a^k \mid k \in \mathbb{Z}, a \in G\}$ is a cyclic subgroup of a group G.

   Let G be the group of 2×2 invertible matrices under multiplication. Find all subgroups of G generated by $\begin{pmatrix} 0 & \frac{1}{3} \\ 3 & 0 \end{pmatrix}$.

8. Show that the group $G = \{2^n \mid n \in \mathbb{Z}\}$ under multiplication is cyclic. Give two generators.

9. Let G be a cyclic group of order 6 and let a be a generator. Show that a^5 is also a generator of G where as a^4 cannot be a generator. Find all subgroups of G defined whose order is 3.

5. PERMUTATION GROUPS

Definition 5.1 Permutation

Let A be a non-empty subset. Any bijective mapping from A to A is called a *permutation*.

Notation: The set of all permutations of the set is denoted by S_A. If A is finite and has n elements, we shall write S_n instead of S_A.

Theorem 5.1 There are $n!$ Permutations in S_n. i.e. $|S_n| = n!$.

Let's consider the set $A = \{a_1, a_2, a_3\}$. For simplicity, we may write this as $\{1, 2, 3\}$. That is, the integer i represents i^{th} element in the set. Then there are $3! = 6$ permutations in S_3.

Consider a permutation $\rho_1 \in S_3$ defined as $\rho_1(1) = 2$, $\rho_1(2) = 3$ and $\rho_1(3) = 1$. For simplicity, we write this as

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

i.e. the image of each element is written immediately below that element. Even simply, since $1 \to 2$, $2 \to 3$ and $3 \to 1$ under ρ_1, we may write it as

$$\rho_1 = (1\ 2\ 3).$$

Remark: An element that goes to the same element is not written.

If we consider the permutation $\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 3 \end{pmatrix}$, we may write this $\mu_1 = (2\ 3)$.

Example 5.1 Write down all 6 permutations of the set S_3.

Composition of Permutations

Let ρ and μ be two permutations defined on a set A. The com[position $\rho \circ \mu$, simply $\rho\mu$ is defined by

$$\rho \circ \mu(x) = \rho\mu(x) = \rho[\mu(x)]$$

for all $x \in A$.

Example 5.2 Let $\rho = (1\ 2\ 5\ 4\ )$ and $\mu = (1\ 2\ 3\ 4\ 5)$. Verify that $\rho\mu \neq \mu\rho$.

Theorem 5.2

Let A be a finite set containing n distinct elements. Then, S_n of A forms a finite group of order $n!$ with respect to composition of permutations as the operation.

- Closure Property: Composition of two bijective mappings is again a bijective mapping.
- Associativity: Assosiativity holds for the composition of mappings
- Identity element: A mapping which maps an element to itself is the identity permutation and is denoted by ω or (1).

  For example, in S_3 $\omega = (1) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$. Note that $\omega\rho = \rho\omega = \rho$ for all $\rho \in S_n$.

- Inverse element: The inverse of a permutation ρ is obtained by reversing it and is denoted by ρ^{-1}.

Definition 5.2 cycles of length r

- A subset $\rho = \{i_1, i_2, \cdots, i_r\}$ of $(1, 2, \cdots, n)$, usually written as $((i_1, i_2, \cdots, i_r)$, is called a *cycle of length* r (or an $r-$cycle), if $\rho(i_j) = \rho(i_{j+1})$ for $j = 1, 2, \cdots, r-1,$ and $\rho(i_r) = i_1$ and $\rho(k) = k$ for all $k \notin \rho$.

- A cycle of length 2 is called a *transposition*.

Theorem 5.3

i. $(i_1, i_2, \cdots, i_r) = (i_2, \cdots, i_r, i_1) = (i_3, \cdots, i_r, i_1, i_2) = \cdots = (i_r, i_1, i_2, \cdots, i_{r-1})$.

ii. $(i_1, i_2, \cdots, i_r)^{-1} = (i_r, i_{r-1}, \cdots, i_1)$.

iii. $(i_1, i_2, \cdots, i_r) = (i_1, i_2, \cdots, i_j)(i_j, i_{j+1}, \cdots, i_r)$.

Example 5.3 Let $\rho = (1\ 2\ 5\ 4)$. Find ρ^{-1} and check that $\rho\rho^{-1} = \omega$.

Definition 5.3 $\rho-$ orbits

- If there is no common element between two permutations, they are said to be disjoint.
- The collection of disjoint cycles of a permutation ρ in S_n is called the set of $\rho-$ orbits.

Theorem 5.4

Any permutation can be written as a product of disjoint cycles.
Any permutation can be written as a product of transpositions.

Definition 5.4 Parity or Signature of a permutation

If a permutation ρ can be expressed as a product of odd number of transpositions, we say that the parity of ρ (or simply, ρ) is odd. This fact is denoted by $\varepsilon_\rho = -1$, where ε_ρ is read as the signature of ρ.

Theorem 5.5 For any permutations ρ and σ,

i. $\varepsilon_\rho = \varepsilon_{\rho^{-1}}$ *ii.* $\varepsilon_{\rho\sigma} = \epsilon_\rho \varepsilon_\sigma$

Definition 5.5 order of a permutation

The smallest positive integer m such that $\rho^m = \omega$ is called the order of the permutation ρ and this fact is denoted by $|\rho| = m$.

Theorem 5.6

i. If $\rho,\ \sigma$ are disjoint cycles, then $\rho\sigma = \sigma\rho$.

ii. order of $(i_1, i_2, \cdots, i_r) = r$.

iii. $|\rho| = |\rho^{-1}|$.

iv. If $\rho,\ \sigma$ are disjoint cycles of lengths l and m respectively, then $|\rho\sigma| = \text{lcm}\ (l, m)$.

v. If $\rho,\ \sigma$ are disjoint cycles such that $(\rho\sigma)^r = \omega$, then $\rho^r = \sigma^r = \omega$.

Theorem 5.7

i. Let $\sigma = (i_1, i_2, \cdots, i_r)$ be a given cycle in S_n and m be a given positive integer. Then,

$$\sigma^m = \begin{pmatrix} i_1 & i_2 & \cdots & i_4 \\ i_{\overline{m+1}} & i_{\overline{m+2}} & \cdots & i_{\overline{m+r}} \end{pmatrix},$$

where $\overline{m+k}$ denotes the residue of $(m+k)$ modulo r and $i_0 = i_r$.

ii. for any $\rho \in S_n$, $\rho\sigma\rho^{-1} = \rho(i_1, i_2, \cdots, i_r)\rho^{-1} = \big(\rho(i_1),\ \rho(i_2),\ \cdots,\ \rho(i_r)\big)$.

Example 5.4 Let $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 4 & 7 & 8 & 6 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 4 & 6 & 2 & 7 & 3 & 8 \end{pmatrix}$.

i. Decompose ρ, σ, $\rho\sigma$ and $\sigma\rho$ as a product of disjoint cycles.

ii. Express $\rho\sigma$, $\sigma\rho$ and $\rho\sigma\rho^{-1}$ as a product of transpositions.

iii. Find the signatures of $\rho\sigma$, $\sigma\rho$ and $\rho\sigma\rho^{-1}$.

iv. What are the $\rho-$ orbits and $\sigma-$ orbits?

v. Find the order of $\rho\sigma$, $\sigma\rho$ and $\rho\sigma\rho^{-1}$.

Example 5.5 Let $\rho = (2\ 3\ 5\ 6\ 8)$ and $\sigma = (1\ 3\ 4)(2\ 6\ 7)$. Find ρ^{18} and $\rho\sigma\rho^{-1}$.

EXERCISES 5

1. Let $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 6 & 9 & 7 & 1 & 8 & 10 & 2 \end{pmatrix}$ be a permutation in S_{10}.
   (a) Express ρ as a product of disjoint cycles and as a product of transpositions.
   (b) What is the parity and order of ρ?
   (c) Find ρ^{-1} and ρ^{99}.
   (d) Find a permutation $\sigma\ (\neq \omega, \rho, \rho^{-1})$ such that $\rho^{-1}\sigma\,\rho = \sigma$.

2. Let $\alpha = (1\ 3)(2\ 5\ 7\ )$, $\beta = (1\ 3\ 4\ 6)$ and $\gamma = (1\ 5\ 7\ 3\ 4\ 6\ 2)$ be permutations in S_7.
   (a) Find $\alpha\beta$, $\alpha\gamma\alpha^{-1}$ and $\gamma^{-1}\beta^{-1}\alpha\beta\gamma$.
   (b) Find a permutation θ in S_7 such that $\theta\gamma^8\theta^{-1} = (1\ 7\ 5\ 3\ 2\ 6\ 4)$.

3. Let $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 4 & 1 & 2 & 7 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 3 & 4 & 2 & 1 & 7 \end{pmatrix}$ be permutations in S_7.
   (a) What is the parity and order of ρ?
   (b) Find $\rho\sigma$, $\rho^{-1}, \rho\sigma\rho^{-1}$ and ρ^{40}.
   (c) Show that it is not possible to find a permutation μ in S_7 such that $\mu^{-1}\rho\mu = (1\ 6)(2\ 5)$.

4. Let $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 4 & 1 & 6 & 7 & 5 & 2 \end{pmatrix}$ be two permutations in S_8.
   (a) Express ρ as a product of transpositions.
   (b) Write σ as a product of transpositions.
   (c) Find the order and the parity of $\rho\sigma$.

(d) Find ρ^{-26}.

(e) Find a permutation $\alpha\ (\neq \omega)$ in S_8 such that $\rho\sigma\alpha\sigma^{-1}\rho^{-1} = \alpha$.

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

(a) Express ρ, σ and $\rho\sigma$ as the products of disjoint cycles.

(b) Decompose ρ, σ and $\rho\sigma$ as the products of transpositions.

(c) What are the $\rho-$ orbits and $\sigma-$ orbits?

(d) Calculate $|\rho|, |\sigma^{-1}|$ and $|\rho\sigma|$.

(e) Find ρ^{-1} and ρ^{206}.

(f) Find a non-trivial permutation α such that $\rho^{-1}\sigma^{-1}\alpha\sigma\rho = \alpha$.

(g) Show that a permutation β cannot be found such that $\beta^{-1}\rho\beta = \sigma$.

(h) Calculate the parity of the permutations ρ, σ and $\rho\sigma$.