# Study Material on Group Theory - I

Department of Mathematics, P. R. Thakur Govt. College
MTMACOR06T: (Semester - 3)

**University Syllabus**

Unit-1: Symmetries of a square, Dihedral groups, definition and examples of groups including permutation groups and quaternion groups (through matrices), elementary properties of groups.

Unit-2: Subgroups and examples of subgroups, centralizer, normalizer, center of a group, product of two subgroups.

Unit-3: Properties of cyclic groups, classification of subgroups of cyclic groups, Cycle notation for permutations, properties of permutations, even and odd permutations, alternating group, properties of cosets, Lagrange's theorem and consequences including Fermat's Little theorem.

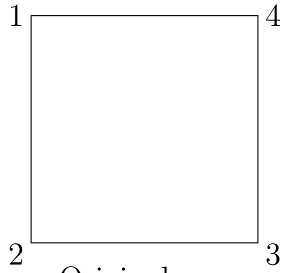
Unit-4: External direct product of a finite number of groups, normal subgroups, factor groups, Cauchy's theorem for finite abelian groups.

Unit-5: Group homomorphisms, properties of homomorphisms, Cayley's theorem, properties of isomorphisms, First, Second and Third isomorphism theorems.

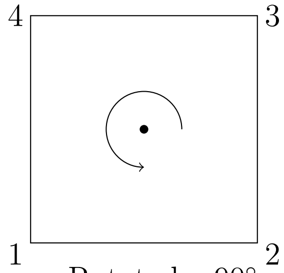
# 1 Definition and Examples

## 1.1 Symmetric transformations of a square

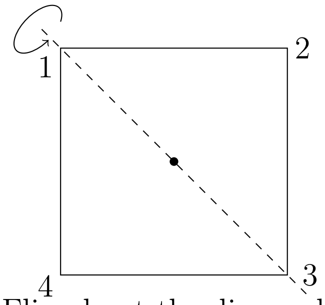
Before defining groups we look at some examples. Consider a square $ABCD$ in plane. Apply the following transformation on the square: (1) Rotate the square anticlockwise about it center by an angle 90°, denote it by $r$ and (2) flip the square about a straight line through one of the vertices and the center of the square, denote it by $s$. Then what will be the position of the square? let us see it.



Original square



Rotate by 90°



Flip about the diagonal line

We observe that all possible symmetric positions of the square can be obtained by applying repeatedly the above mentioned rotation and reflection. It is also observed that there can be exactly eight possible symmetric positions of the square. If we write a position of the square by counting the corners in anticlockwise direction, the initial position is 1234. After repetead rotations by 90° the subsequent positions are 4123, 3412 and 2341. Then again to 1234. After flipping about the diagonal 1-3 the position becomes 1432 which reverts to the initial position by a second flip. If we apply rotations after a flip the positions are 1432, 2143, 3214 and 4321. Thus, the all eight symmetric positions of the square are given by $\{1234, 4123, 3412, 2341, 1432, 2143, 3214, 4321\}$. The transformation of the square from its original position to any of its symmetric position is called a symmetric transformation.

Now consider the set $S = \{1, 2, 3, 4\}$ and consider the set of all permutations of $S$. A permutation is a bijection from the set $S$ to $S$. If $f : S \to S$ is a permutation we write it as $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}$, where $f(1) = i_1, f(2) = i_2$ etc. Composition of two permutations is another permutation, for example if $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ then the composition $g \circ f$ is given by $g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$. To find the calculation, see by $f$, 1 goes to 2 and by $g$, 2 goes to 4, hence by $g \circ f$, 1 goes to 4. In brief, the movement of other elements are as follows: $2 \xrightarrow{f} 4 \xrightarrow{g} 2$, i.e. $2 \xrightarrow{g \circ f} 2$, $3 \xrightarrow{f} 3 \xrightarrow{g} 1$, i.e. $3 \xrightarrow{g \circ f} 1$, $4 \xrightarrow{f} 1 \xrightarrow{g} 3$, i.e. $4 \xrightarrow{g \circ f} 3$. Similarly $f \circ g$ is given by $f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$. The identity mapping is called the identity permutation, denoted by $i$, i.e., $i = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$. An easy calculation shows that there are $4! = 24$ permutations on the set $S = \{1, 2, 3, 4\}$.

The set of all permutations on the set has the following properties:

1. Composition of two permutations is also a permutation.
2. For permutations $f, g, h$, $(f \circ g) \circ h = f \circ (g \circ h)$, this is called associative property.
3. Composition of any permutation with the identity permutation $i$ leaves it unchanged.
4. Every permutation $f$ has an inverse permutation $f^{-1}$ in the sense that $f \circ f^{-1} = f^{-1} \circ f = i$.

To find the inverse of a permutation, just interchange the rows and arrange columns accordingly. For example, if $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ then $f^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

Now, back to symmetric transformations of a square. The rotation $r$ and the flip $s$ are permutations which are be written as $r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ and $s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$. Any symmetric transformation is repeated compositions of $r$ and $s$. All the symmetric transformations are $i = r^4 = s^2, r, r^2, r^3, s, r \circ s, r^2 \circ s$ and $r^3 \circ s$. We write $f^k = f \circ f \circ \cdots \circ f$ ($k$-times) for any permutation $f$. We observe that The set of all symmetric transformations of the square satisfies all the four properties listed above that satisfied by the set of all permutations of $S$.

The set of all permutations of the set $\{1, 2, 3, 4\}$, denoted by $S_4$, is called permutation group of degree 4 and the set of symmetric transformations of the square is denoted by $D_4$ called the dihedral group of degree 4. It can be noted that $D_4$ is a subset of $S_4$ but both satisfy the above four properties.

## 1.2 Definition and examples

We are in a position to define group.

Definition. 1.1 Let $S$ be a non empty set. A function defined on $S \times S$ is called a *binary operation* or a *binary composition* on the set $S$.

Example. 1.2 Usual addition, multiplication on the set of real or complex numbers or their subsets are examples of binary operations. The compositions of functions on some set $S$ is also an example of binary operation on the set of all the functions from $S$ to $S$.

Notation. 1.3 If $*$ is a binary operation on a set $S$, as it is a function on $S \times S$, i.e., $* : S \times S \to S'$, for $a, b \in S$ instead of writing $*(a, b)$ we write it as $a * b$. We are already familiar with it, such as for addition we write $a + b$ instead of $+(a, b)$.

Definition. 1.4 A binary operation $*$ defined on a set $S$ is said to satisfy the *closure property* if the codomain set of $*$ is $S$ itself, i.e., $* : S \times S \to S$. In other words, if for all $a, b \in S$, $a * b \in S$. If $*$ satisfy the closure property, we say that $S$ *is closed under* $*$.

Example. 1.5 On the set $\mathbb{N}$ of all natural numbers addition and multiplication satisfy the closure property but the subtraction or division does not satisfy it, as for $a, b \in \mathbb{N}$, $a + b$ and $a \cdot b$ are members of $\mathbb{N}$ but $a - n$ or $a/b$ may bot be a member of $\mathbb{N}$.

Definition. 1.6 A binary operation $*$ on a set $S$ is said to *satisfy associative property* if for all $a, b, c \in S$, $a * (b * c) = (a * b) * c$. We say $*$ is *associative* if it satisfy the associative property.

Example. 1.7

1. On the set $\mathbb{Z}$ of integers, $+$ and $\cdot$ are associative where $-$ is not associative.

2. On the set $\mathbb{R} - \{0\}$ of non-zero real numbers division and subtraction are not associative, whereas addition and multiplication are associative.

Definition. 1.8 An ordered pair $(S, *)$ is called a *semigroup* if $S$ is a non-empty set $*$ is a binary operation on $S$ and $*$ satisfies the closure property and associative property. If $*$ satisfies only the closure property then it is called a *groupoid.*

Example. 1.9

1. $(\mathbb{N}, +), (\mathbb{N}, \cdot)$ are simplest examples of semigroup.

2. $(\mathbb{R}_+, \cdot)$ is a semigroup, where $\mathbb{R}_+$ is the set of all positive real numbers.

Definition. 1.10 An element $e$ on a groupoid $(S, *)$ is called a *left identity element* if $e * a = a$ for all $a \in S$. $e$ is called a *right identity element* if $a * e = a$ for all $a \in S$. $e$ is called an *identity element* if it is both a right identity element and a left identity element, i.e., if $e * a = a * e = a$ for all $a \in S$.

Example. 1.11

1. In the system $(\mathbb{Z}, +)$, $0$ is the identity element, since for $a \in \mathbb{Z}$, $a + 0 = 0 + a = a$.

2. In the system $(\mathbb{R} - \{0\}, \cdot)$, 1 is the idntity element, since for $a \in \mathbb{R} - \{0\}$, $a \cdot 1 = 1 \cdot a = a$.

3. If $S$ is the set of all $2 \times 2$ non-singular matrices over the real numbers then the identity matrix $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the left identity element as well as the right identity element with respect to matrix multiplication.

4. Consider the set $\mathbb{Z}$ of all the integers. Define a binary operation $*$ by $a * b = 2a + b$ for all $a, b \in \mathbb{Z}$. Then for any $a \in \mathbb{Z}$, $0 * a = 2 \cdot 0 + a = a$. Thus 0 is a left identity element of $(\mathbb{Z}, *)$. But for any $a \in \mathbb{Z}$, $a * 0 = 2a + 0 \neq a$. Thus 0 is not a right identity element. In fact, for this binary operation there is no right identity element, for $a * e = a$ implies that $2a + e = a$, i.e., $e = -a$. Thus $e$ is dependent on $a$ and hence can not be a right identity element of the system.

Definition. 1.12 Let $G$ be a set, $*$ be a binary operation on $G$. Then the pair $(G, *)$ is called a *group* if it satisfies the following axioms:

1. $G$ is closed under $*$,

2. $*$ is associative,

3. There is a left identity element $e$ in $G$ such that $e * a = a$ for all $a \in G$,

4. For every $a \in G$ there exists an element $b \in G$ such that $b * a = e$, $b$ is called a left inverse of $a$ and is denoted by $a^{-1}$. Thus we have $a^{-1} * a = e$.

It has not been mentioned exclusively that $G$ is non empty, as it follows from the existence of left identity element. Before providing any example of a group we write some elementary results which will help us to modify the definition of a group.

Theorem. 1.13 *In a group $(G, *)$*

1. *every left identity element is also a right identity element.*

2. *left inverse of an element is also a right inverse of that element.*

Proof. 1. Let $e$ be a left identity element of $G$, i.e., $e * x = x$ for all $x \in G$. Assume that $a \in G$, $b$ is a left inverse of $a$ and $c$ is a left inverse of $b$, i.e., $b * a = e$ and

$c * b = e$. Now,

$$\begin{aligned} e * a = a \;&\Rightarrow\; (e * a) * e = a * e \;\Rightarrow\; ((c * b) * a) * e = a * e \\ &\Rightarrow\; (c * (b * a)) * e = a * e \quad \text{(by associative property)} \\ &\Rightarrow\; (c * e) * e = a * e \;\Rightarrow\; c * (e * e) = a * e \;\Rightarrow\; c * e = a * e. \qquad (1) \end{aligned}$$

$$\text{Again, } e * a = a \;\Rightarrow\; (c * b) * a = a \;\Rightarrow\; c * (b * a) = a \;\Rightarrow\; c * e = a. \qquad (2)$$

From (1) and (2) above we have $a * e = a$. Since this is true for every $a \in G$, $e$ is a right identity element of $G$.

2. Again, $e = c*b = c*(e*b) = (c*e)*b = (a*e)*b$ (by (1) above) $= a*(e*b) = a*b$. Thus $b$ is right inverse of $a$. ■

In view of the above result without any loss of generality we may assume the existence of identity element and inverse of each element in a group instead of left identity element and left inverse of each element in the group. Hence we modify the definition of a group as follows:

Definition. 1.14 Let $G$ be a set, $*$ be a binary operation on $G$. Then the pair $(G, *)$ is called a *group* if it satisfies the following axioms:

1. $G$ is closed under $*$,
2. $*$ is associative,
3. There is an identity element $e$ in $G$ such that $e * a = a * e = a$ for all $a \in G$,
4. For every $a \in G$ there exists an element $b \in G$ such that $b * a = a * b = e$, $b$ is called inverse of $a$ and is denoted by $a^{-1}$. Thus we have $a^{-1} * a = a * a^{-1} = e$.

Example. 1.15 1. $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are examples of group.

2. $(\mathbb{R} - \{0\}, \,\cdot\,), (\mathbb{C} - \{0\}, \,\cdot\,)$ are also examples of group.
3. Let $M_n(\mathbb{R})$ denote the set of all $n \times n$ matrices with real number entries. Then $M_n(\mathbb{R})$ is a group under matrix addition, zero matrix being the identity element and negative of a matrix is its inverse.
4. Let $GL_n(\mathbb{R})$ denote the set of all $n \times n$ non-singular matrices over $\mathbb{R}$. Then $GL_n(\mathbb{R})$ is a group with respect to matrix multiplication, the identity matrix $I_n$ being the identity element and the inverse of each matrix is the inverse of it.

5. Let $S_n$ denote the set of all permutations of the set $\{1, 2, \ldots, n\}$. Then $(S_n, \circ)$ is a group, here $\circ$ denotes the composition of functions.

6. It has already been proved that $D_4$, the set of all symmetric transformations of the square is a group with respect to composition of transformations. For any positive integer $n > 2$, $D_n$ denotes the set of all symmetric transformations of a regular $n$-gon and is called the *dihedral group* of order $n$. The symmetric transformations are compositions of rotation by an angle $2\pi/n$ about its center ($90^\circ$ for the case of square) and a flip about an axis of symmetry (such as a straight line through the centre and a vertex of the polygon, a diagonal in the case of square).

7. Let $\omega$ denote the cube root of unity, $S = \{1, \omega, \omega^2\}$. Then $(S, \cdot)$ is a group. Note that $\{1, \omega, \omega^2\}$ is the set of all roots of the equation $x^3 = 1$.

   Similarly, the set $B = \{1, -1, i, -i\}$, where $i^2 = -1$, forms a group under multiplication of complex numbers. Here $B = \{1, i, i^2, i^3\}$ is the set of all roots of the equation $x^4 = 1$

   In general, for $n \in \mathbb{N}$ let $\Omega_n$ denote the set of the roots of the equation $x^n = 1$. Then $(\Omega_n, \cdot)$ is a group. Note that $\Omega_n$ can be written as $\Omega_n = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ where $\alpha = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

8. Consider the set $Q_8 = \{1, -1, i, j, k, -i, -j, -k\}$. Define multiplication on $Q$ as follows: $1{\cdot}x = x{\cdot}1 = x$, $-1{\cdot}x = x{\cdot}-1 = -x$ for all $x \in Q$, $i{\cdot}i = j{\cdot}j = k{\cdot}k = -1$, $i \cdot j = k, j \cdot k = i, k \cdot i = j$ and $j \cdot i = -k, k \cdot j = -i, i \cdot k = -j$. All these operations can be written in the following composition table:

| $\cdot$ | $1$ | $i$ | $j$ | $k$ | $-1$ | $-i$ | $-j$ | $-k$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $i$ | $j$ | $k$ | $-1$ | $-i$ | $-j$ | $-k$ |
| $i$ | $i$ | $-1$ | $k$ | $-j$ | $-i$ | $1$ | $-k$ | $j$ |
| $j$ | $j$ | $-k$ | $-1$ | $i$ | $-j$ | $k$ | $1$ | $-i$ |
| $k$ | $k$ | $j$ | $-i$ | $-1$ | $-k$ | $-j$ | $i$ | $1$ |
| $-1$ | $-1$ | $-i$ | $-j$ | $-k$ | $1$ | $i$ | $j$ | $k$ |
| $-i$ | $-i$ | $1$ | $-k$ | $j$ | $i$ | $-1$ | $k$ | $-j$ |
| $-j$ | $-j$ | $k$ | $1$ | $-i$ | $j$ | $-k$ | $-1$ | $i$ |
| $-k$ | $-k$ | $-j$ | $i$ | $1$ | $k$ | $j$ | $-i$ | $-1$ |

   In this table $x \cdot y$ means $x$ is taken from leftmost column and $y$ is taken from header row. With this operation $(Q_8, \cdot)$ is a group, called the *quaternion group.*

9. Let $p \in \mathbb{N}$. Consider a relation $\rho_p$ on $\mathbb{Z}$ by $a\rho_p b$ if and only if $a - b$ is divisible by $p$. It can easily be verified that $\rho_p$ is an equivalence relation on $\mathbb{Z}$ (verify it

by yourself, to ensure that it is really easy). The set of all equivalence classes is denoted by $\mathbb{Z}_p = \{(0), (1), \ldots, (p-1)\}$. Define addition $+$ on $\mathbb{Z}_p$ by for all $(a), (b) \in \mathbb{Z}_p$, $(a) + (b) = (a+b)$. Then $(\mathbb{Z}_p, +)$ is a group, called the *residue class group modulo p*. Here $(0)$ is the identity element and for $(k) \in \mathbb{Z}_p$ since $(k) + (p-k) = (p) = (0)$, $(p-k)$ is the inverse of $(k)$.

Definition. 1.16 A group $(G, *)$ is called *abelian group* or *commutative group* if for all $a, b \in G$, $a * b = b * a$.

Example. 1.17

1. The groups $(\mathbb{Z}, +), (\mathbb{R}, +)$ are abelian groups.
2. The group $(Gl_n(\mathbb{R}), \cdot\ )$ is not abelian, since matrix multiplication is not commutative.
3. The group $(S_n, \circ)$ is not abelian, since composition of functions is not commutative.

Notation. 1.18

1. Let $(G, *)$ be a group and $a \in G$. For $n \in \mathbb{N}$ the element $a * a * \cdots * a$ ($n$-times) is denoted by $a^n$. When the binary operation is denoted by $+$ then the element $a + a + \cdots + a$ ($n$ times) is denoted by $na$.
2. Usually the identity element is denoted by $e$. When the binary operation is taken as multiplication '$\cdot$' the identity element is written as 1. When the binary operation is taken as $+$, the identity element is written as 0, in this case the inverse of an element $a$ is written as $-a$.

Definition. 1.19 A group $(G, *)$ is called a *finite group* if $G$ has a finite number of elements otherwise it is called an infinite group. The number of elements in the group $G$ is called the *order of the group* and is denoted by $|G|$ or by $o(G)$.

Example. 1.20 $(\mathbb{Z}, +), (\mathbb{R}, +), (M_n(\mathbb{R}), +)$ etc. are infinite group. For $n \in \mathbb{N}$, $S_n$ is an example of finite group and $|S_n| = n!$. The dihedral group $D_n$ is also a finite group with $|D_n| = 2n$.

## 1.3 Elementary Properties

So far we have talked of *an* identity element of a group or *an* inverse of an element of the group. The following result shows that a group has exactly one identity element and every element have only one inverse. Hence we shall talk of *the* identity element and *the* inverse of an element of a group.

THEOREM. 1.21 *In a group the identity element and the inverse of every element are unique.*

PROOF. Let $(G, *)$ be a group and if possible, let it has two identity elements say, $e$ and $e'$. Then $e = e * e'$ ($e'$ is taken as (right) identity element). Also $e' = e * e'$ (here $e$ is taken as (left) identity element). Thus $e = e * e' = e'$.

Let $a \in G$ and if possible suppose that $a$ has two inverses $b$ and $b'$, i.e., $a*b = b*a = e$ and $a * b' = b' * a = e$. Then $b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$. Thus $b = b'$. ■

THEOREM. 1.22 *In a group $(G, *)$,*

1. *for $a \in G$, $(a^{-1})^{-1} = a$,*

2. *for $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$.*

PROOF. 1. We have $a * a^{-1} = a^{-1} * a = e$, where $e$ is the identity element. This implies that $a$ is the inverse of the element $a^{-1}$, i.e., $(a^{-1})^{-1} = a$.

2. By using associative property, $(a * b) * (b^{-1} * a^{-1}) = ((a * b) * b^{-1}) * a^{-1} = (a * (b * b^{-1})) * a^{-1} = (a * e) * a^{-1} = a * a^{-1} = e$. Similarly $(b^{-1} * a^{-1}) * (a * b) = e$. Thus $b^{-1} * a^{-1}$ is the inverse of $a * b$, i.e., $(a * b)^{-1} = b^{-1} * a^{-1}$. ■

THEOREM. 1.23 *The left and right cancellation laws hold in a group $(G, *)$:*

1. *for $a, b, c \in G$, if $a * b = a * c$ then $b = c$.*

2. *for $a, b, c \in G$, if $b * a = c * a$ then $b = c$.*

PROOF. For the first part $a * b = a * c \Rightarrow a^{-1} * (a * b) = a^{-1} * (a * c) \Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c \Rightarrow e * b = e * c \Rightarrow b = c$. The second part is done similarly, the reader may easily work out it. ■

When there is no chance of ambiguity about the binary operation $*$, instead of writing $(G, *)$ we write simply $G$. We also write $ab$ instead of writing $a * b$ if we agree that $ab$ is not actually the multiplication of $a$ and $b$ it is the binary operation of $a$ and $b$ in $G$.

THEOREM. 1.24 *If $G$ is a group and $a, b \in G$ then the equations $ax = b$ and $ya = b$ have unique solutions in $G$.*

Proof. Taking $x = a^{-1}b$ we have $ax = a(a^{-1}b) = (aa^{-1})b = eb = b$, where $e$ is the identity element. Thus $x = a^{-1}b$ is a solution of the equation $ax = b$. To check the uniqueness of the solution let $x_1$ and $x_2$ be two solutions of the equation $ax = n$. Then $ax_1 = b$ and $ax_2 = b$ which implies that $ax_1 = ax_2$. Taking binary operation by $a^{-1}$ from left on both sides and using associative property we have $a^{-1}(ax_1) = a^{-1}(ax_2) \Rightarrow (a^{-1}a)x_1 = (a^{-1}a)x_2 \Rightarrow ex_1 = ex_2 \Rightarrow x_1 = x_2$. Thus the solution is unique.

The second part is similar and left to the reader. ■

Converse of the above theorem is also true in the sense that in a semigroup if the equations $ax = b$ and $ya = b$ have unique solutions then it becomes a group.

Theorem. 1.25 *Let $G$ be a non-empty semigroup such that for each $a, b \in G$ the equations $ax = b$ and $ya = b$ have unique solutions in $G$. Then $G$ is a group.*

Proof. As $G$ is a semigroup the closure and associative properties hold. To complete the proof we have to check that $G$ has the identity element and every element of $G$ has inverse in $G$.

Let us choose $a \in G$ arbitrarily. The the equations $ya = a$ has a solutions in $G$, let $e$ be the solution. Then $ea = a$. Let $b$ be an arbitrary element of $G$. Then the equation $ax = b$ has a solution, say $c$. Then $ac = b$. Then $eb = e(ac) = (ea)c = ac = b$. Since $b$ has been chosen arbitrarily in $G$ it follows that $e$ is the left identity element of $G$.

To check the existence of inverse of each element of $G$, Choose $a \in G$. Then the equation $ya = e$ has a solution in $G$, let $b$ be the solution. Then $ba = e$ and hence $b$ is the left inverse of $a$. So every element of $G$ has a left inverse in $G$. Thus $G$ is a group. ■

Definition. 1.26 The order of an element $a$ in a group $G$ is the smallest positive integer $n$ such that $a^n = e$ where $e$ is the identity element. If no such integer exists the order of $a$ is defined to be infinite. Order of the element $a$ is denoted by $|a|$ or by $o(a)$.

In case the binary operation is '+' where the identity element is denoted by 0, the order of the element $a$ is the smallest positive integer $n$ such that $na = 0$.

Example. 1.27

1. Each non-zero element of $(\mathbb{Z}, +)$ has order infinity.
2. In the group $(\mathbb{R} - \{0\}, \cdot)$, $o(-1) = 2, o(1) = 1$ and $o(x) = \infty$ for all other elements $x$.

3. In the multiplicative group of $n$-th root of unity, where $n$ is a prime number, every element other than 1 has order $n$.

4. In the multiplicative group $\{1, -1, \omega, \omega^2, -\omega, -\omega^2\}$ (roots of the equation $x^6 = 1$) $o(-1) = 2, o(\omega) = o(\omega^2) = 3, o(-\omega) = o(-\omega^2) = 6$.

5. In a group $G$, $o(x) = o(x^{-1})$ for any $x \in G$.

## 1.4 Exercises

1. Verify whether the set $\{a + b\sqrt{2} : a, b \in \mathbb{Q}, |a| + |b| \neq 0\}$ forms a group under multiplication.

2. Let $I = \{x : 0 \leq x \leq 1, x \in \mathbb{R}\}$. Define an operation $*$ on $I$ by $x * y = x + y - [x + y]$ for all $xy \in I$. Prove that $(I, *)$ is a group.

3. Write down the composition table of $\mathbb{Z}_6$.

4. If $p$ is prime show that the non-zero elements of $\mathbb{Z}_p$ froms a group under multiplication, defined by $(a).(b) = (a.b)$ for all $(a), (b) \in \mathbb{Z}_p - \{(0)\}$.

5. If $o(a) = 2$ for some element $a$ in a group $G$ prove that $a = a^{-1}$.

6. In a group $G$ if $(ab)^2 = a^2b^2$ for all $a, b \in G$ then prove that $G$ is abelian.

7. If in a group $o(a) = n$ then prove that $a^{-1} = a^{n-1}$.

8. If $G$ is a finite group of even order prove that there exists an element $a \in G$ such that $a = a^{-1}$.

# 2 Subgroups

## 2.1 Definition and Examples

We have already seen that $S_4$, the set of all permutations of the set $\{1, 2, 3, 4\}$ is a group and $D_4$, the group of all symmetric transformations of the square can be regarded as subset of $S_4$. A subset of a group which itself is also a group with respect to the same operation is called a subgroup.

Definition. 2.1 Let $(G, *)$ be a group. A set $H \subset G$ is called a *subgroup* of $G$ if $(H, *)$ is also a group, where the binary operation $*$ on $H$ is the restriction of $*$ on $G$ to $H$. If $H$ is a subgroup of $G$ it is written as $H < G$.

Example. 2.2

1. For every group $G$, $G$ itself and $\{e\}$ are subgroups of $G$, called the trivial subgroups where $e$ is the identity element.
2. Let $n \in \mathbb{N}, n > 1$, $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$. Then $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.
3. $\{1, \omega, \omega^2\}$ is a subgroup of the group $\{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.
4. As we have mentioned earlier, $D_n$ is a subgroup of $S_n$, $n \geq 3$.
5. for $n \in \mathbb{N}$, $SL_n(\mathbb{R})$ the set of all $n \times n$ matrices with determinant 1 is a subgroup of $GL_n(\mathbb{R})$, the multiplicative group of all non-singular $n \times n$ matrices.

The necessary and sufficient condition for a subset of a group to be a subgroup is the following:

Theorem. 2.3 *Let $G$ be a group. A non-empty subset $H \subset G$ is a subgroup of $G$ if and only if (i) for all $a, b \in H$, $ab \in H$ and (ii) for all $a \in H, a^{-1} \in H$.*

Proof. If $H$ is a subgroup of $G$ then $H$ itself is a group with respect to the same binary operation as in $G$. By closure property of $H$, $a, b \in H \Rightarrow ab \in H$. Also for $a \in H$, $H$ being a group, $a^{-1} \in H$. Thus conditions (i) and (ii) are satisfied.

Conversely, assume that $H$ is a subset of the group $G$ satisfying the conditions (i) and (ii). Condition (i) says that $H$ satisfies the closure property. As the binary operation in $H$ is the same as that in $G$ and associative property holds in $G$ it follows that associative property holds also in $H$ (this is called hereditary property). As $H \neq \emptyset$, choose $a \in H$. By condition (ii) $a^{-1} \in H$ and by condition (i) $aa^{-1} = e \in H$. Thus H has the identity element. The existence of inverse of each element of $H$ follows from condition (ii). Thus $H$ is a group under the same binary operation as in $G$ and hence $H$ is a subgroup of $G$. ■

In the above theorem the conditions (i) and (ii) can be written in a combined form as follows:

THEOREM. 2.4 *A non empty subset $H$ of a group $G$ is a subgroup of $G$ if and only if for all $a, b \in H$, $a^{-1}b \in H$.*

EXAMPLE. 2.5

1. Prove for $n \in \mathbb{N}$, $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

   Let $a, b \in n\mathbb{Z}$. Then there exist $n_1, n_2 \in \mathbb{Z}$ such that $a = nn_1$ and $b = nn_2$. Then $a+b = nn_1+nn_2 = n(n_1+n_2)$. Since $n_1+n_2 \in \mathbb{Z}$ it follows that $a+b \in n\mathbb{Z}$. Thus condition (i) is satisfied. Also for $a = nn_1 \in n\mathbb{Z}$, $-a = -nn_1 = n(-n_1)$. Since $-n_1 \in \mathbb{Z}$, $n(-n_1) \in n\mathbb{Z}$, i.e., $-a \in n\mathbb{Z}$. Thus condition (ii) also hold. hence $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

2. Prove that $SL_2(\mathbb{R})$ is a proper subgroup of $GL_2(\mathbb{R})$.

   $GL_2(\mathbb{R})$ denotes the set of all $2 \times 2$ non-singular matrices over $\mathbb{R}$ and $SL_2(\mathbb{R})$ denotes the set of all $2\times2$ matrices whose determinant is 1. Let $A, B \in SL_2(\mathbb{R})$, then $|A| = |B| = 1$. Now, $|AB| = |A| \cdot |B| = 1 \cdot 1 = 1$ hence $AB \in SL_2(\mathbb{R})$. Also $A \in SL_2(\mathbb{R}) \Rightarrow |A| = 1 \Rightarrow |A^{-1}| = \frac{1}{1} = 1$, i.e., $A^{-1} \in SL_2(\mathbb{R})$. Hence $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$. To check it is proper (i.e., non-trivial) we have to check $\{I_2\} \subsetneqq SL_2(\mathbb{R}) \subsetneqq GL_2(\mathbb{R})$. Consider the matrix $A = \begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix}$. Then $|A| = 8 - 7 = 1$ shows that $A \in SL_2(\mathbb{R})$. Also $B = \begin{pmatrix} 2 & 3 \\ 5 & 6 \end{pmatrix} \in GL_2(\mathbb{R}) - SL_2(\mathbb{R})$. Hence the subgroup is proper.

3. Let $S^1 = \{z \in \mathbb{C} : |z| = 1\}$, the circle in complex plane with center at origin and radius 1. Prove that $S^1$ is a group under multiplication and for any $n \in \mathbb{N}, n > 1$, the roots of the equation $x^n = 1$ form a subgroup of $S^1$.

   That $S^1$ is a group with respect to complex multiplication is a routine check, students are asked to do it. Let $\Omega_n = \{z \in \mathbb{C} : z^n = 1\}$ denote the set of all the roots of the equation $x^n = 1$. It has been shown that $\Omega_n$ can be written as $\Omega_n = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ where $\alpha = \cos\theta + i \sin\theta, \theta = \frac{2\pi}{n}$. (i) If $\alpha^k, \alpha^l \in \Omega_n$ then $\alpha^k \cdot \alpha^l = \alpha^{k+l} = \alpha^r \in \Omega_n$, where $r$ is the remainder when $k+l$ is divided by $n$. (if $k + l > n$ then dividing $k + l$ by $n$ we have $k + l = dn + r$,

$0 \leq r < n$, hence $\alpha^{dn+r} = (\alpha^n)^d \cdot \alpha^r = 1^d \cdot \alpha^r = \alpha^r$). (ii) Also for $\alpha^k \in \Omega_n$, $(\alpha^k)^{-1} = \alpha^{n-k} \in \Omega_n$. Hence $\Omega_n$ is a subgroup of $S^1$.

## 2.2 Some special subgroups

DEFINITION. 2.6 Let $G$ be a group and $A$ be a non-empty subset of $G$. Then the set $\{g \in G : gag^{-1} = a \; \forall a \in A\}$ is called the *centralizer* of the set $A$ and is denoted by $C_G(A)$. If $A = \{a\}$ is a singleton set we write its centralizer as $C_G(a)$ instead of $C_G(\{a\})$.

It can be noted that for $a \in A$ and $g \in G$, $gag^{-1} = a$ if and only if $ga = ag$. Thus the centralizer of a set $A$ is actually those elements of $G$ which commute with every member of $A$.

THEOREM. 2.7 *The centralizer of a subset is a subgroup.*

PROOF. Let $G$ be a group and $A \subset G, A \neq \emptyset$. To prove that $C_G(A)$ is a subgroup of $G$ choose $g, h \in C_G(A)$. Then $gag^{-1} = hah^{-1} = a$ for all $a \in A$. For $a \in A$ we have $(gh)a(gh)^{-1} = (gh)a(h^{-1}g^{-1}) = g(hah^{-1})g^{-1} = gag^{-1} = a$. Hence $gh \in C_G(A)$. Also, for $g \in C_G(A), a \in A$, since $gag^{-1} = a$ we have $g^{-1}(gag^{-1})g = g^{-1}ag \Rightarrow (g^{-1}g)a(g^{-1}g) = g^{-1}ag \Rightarrow eae = g^{-1}ag \Rightarrow a = g^{-1}ag$, where $e$ is the identity element. Since this is true for all $a \in A$ it follows that $g^{-1} \in C_G(A)$. Thus $C_G(A)$ is a subgroup of $G$. ■

EXAMPLE. 2.8

1. For an abelian group $G$, for any element $a$, $C_G(a) = G$.
2. Find the centralizer of $i$ in the group $Q_8$, the group of quaternions.

   From the composition table of $Q_8$ it is observed that $C_{Q_8}(i) = \{\pm 1, \pm i\}$.
3. In $S_4$, if $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, then $C_{S_4}(\sigma) = \{i, \sigma, \rho\}$, where $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ and $i$ denotes the identity permutation. One can observe that the members of $C_{S_4}(\sigma)$ other than $\sigma$ move only those members of $\{1, 2, 3, 4\}$ which are not effected by $\sigma$, we call those permutations *disjoint* from $\sigma$. Keeping this in mind, find $C_{S_5}(f)$ where $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} \in S_5$.

DEFINITION. 2.9 The *center* of a group $G$ is the set of all those members of $G$ which commute with every member of $G$ and is denoted by $Z(G)$. Thus $Z(G) = \{x \in G : xg = gx \; \forall g \in G\}$.

It can be observed that $Z(G)$ is nothing but the centralizer of the whole group, i.e., $Z(G) = C_G(G)$ for any group $G$. Since centralizer of a subset of $G$ is a subgroup of $G$ as a particular case we can conclude immediately that

Theorem. 2.10 *The center of a group is a subgroup of it.*

For a set $A \subset G$ and $g \in G$ define $gA = \{ga : a \in A\}$ and $Ag = \{ag : a \in A\}$.

Definition. 2.11 Let $A$ be a subset of a group $G$. The *normalizer* of $A$, denoted by $N_G(A)$, is the set $\{g \in G : gA = Ag\}$.

If can be noted that though the definitions are looking similar, the centralizer and normalizer of a set $A$ are different. For $g \in G$, $g \in C_G(A)$ if and only if $ga = ag$ for all $a \in A$, on the other hand $g \in N_G(A)$ if and only if $gA = Ag$, i.e., for all $a \in A$ there exists $b \in A$ such that $ga = bg$. However if $g \in C_G(A)$ then obviously $g \in N_G(A)$, i.e., $C_G(A) \subset N_G(A)$.

Example. 2.12 Consider $G = S_3$ the group of permutations on the set $\{1, 2, 3\}$. Let us consider the set $A = \{i, f, g\}$ where $i$ is the identity mapping, $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Then one can easily check that $C_G(A) = A$ whereas $N_G(A) = G$. [Check it by yourself to verify that it is really easy. First write down all the six members of $S_3$ and then calculate the compositions from both sides with the members of $A$].

## 2.3 Properties of Subgroups

We study some more elementary properties of subgroups.

Theorem. 2.13 *Intersection of two subgroups of a group is again a subgroup.*

Proof. Let $G$ be a group and $H, K$ are subgroups of $G$. If $H \cap K = \{e\}$, where $e$ is the identity element of $G$, then it is a subgroup. Otherwise choose $a, b \in H \cap K$. Then since $H$ is a subgroup and $a, b \in H$ it follows that $ab \in H$. Similarly $ab \in K$. Thus $ab \in H \cap K$.

Also for $a \in H \cap K$, since $H, K$ are subgroups and $a \in H, a \in K$ it follows that $a^{-1} \in H, a^{-1} \in K$ and hence $a^{-1} \in H \cap K$. Thus $H \cap K$ is a subgroup of $G$. ■

Union of two subgroups need not be a subgroup, the following example shows it.

Example. 2.14 Consider the groups $(2\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$, both are subgroups of $(\mathbb{Z}, +)$. Then $2 \in 2\mathbb{Z} \subset 2\mathbb{Z} \cup 3\mathbb{Z}$ and $3 \in 3\mathbb{Z} \subset 2\mathbb{Z} \cup 3\mathbb{Z}$, but $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Thus $2\mathbb{Z} \cup 3\mathbb{Z}$ can not be a subgroup of $\mathbb{Z}$.

The above result can be extended to an arbitrary collection of subgroups.

Theorem. 2.15 *Let $\{H_i : i \in I\}$ be a collection of subgroups of a group $G$. Then the intersection $\cap_{i \in I} H_i$ is also a subgroup.*

Proof is similar to that one already proved.

Definition. 2.16 let $G$ be a group, $a \in G$. Then the set $\{a^n : n \in \mathbb{Z}\}$ is a group, called the *cyclic subgroup generated by* $a$ and is denoted by $\langle a \rangle$. $a$ is called a *generator* of the cyclic subgroup or the subgroup is called *generated by* $a$.

Example. 2.17

1. The cyclic subgroup generated by $i$ in $Q_8$ is $\{\pm 1, \pm i\}$, since it is the set $\{i, i^2, i^3, i^4\}$. $i^5 = i$ and hence the same elements are repeated for all other powers. This is why it is called cyclic.

2. In the group $(\mathbb{Z}, +)$ for any $n \in \mathbb{Z}$, $\langle n \rangle = \{nk : k \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \ldots\} = n\mathbb{Z}$. Note that here $\mathbb{Z}$ being an additive group we write $nk$ instead of $n^k$.

3. If in a group $G$ an element $a \in G$ has order $n$, i.e., $a^n = e$ then $\langle a \rangle = \{a, a^2, a^3, \ldots, a^{n-1}, a^n = e\}$. All other powers will give the same elements, i.e., $a^{n+1} = a, a^{n+2} = a^2, a^0 = e, a^{-1} = a^{n-1}, a^{-2} = a^{n-2}$ etc.

4. Consider $\mathbb{Z}_6$, the additive group of residue class modulo 6. The elements are $\{(0), (1), (2), \ldots, (5)\}$. Then $\langle (2) \rangle = \langle (4) \rangle = \{(2), (4), (0)\}$. So different elements may generate the same cyclic subgroup.

Definition. 2.18 If $G$ is a group and $a \in G$ such that $\langle a \rangle = G$, i.e., the cyclic subgroup generated by $a$ is $G$ itself, we call $G$ a *cyclic group* and write it as $G = \langle a \rangle$. $a$ is called the generator of $a$.

Example. 2.19

1. The group $(\mathbb{Z}, +)$ has two generators 1 and $-1$.

2. For $n \in \mathbb{N}$, let $\alpha = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. Then the roots of the equation $x^n = 1$ are $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ which is a group under multiplication. Obviously $\alpha$ is a generator of this group. It can be observed that if $n$ is prime then any $\alpha^k$ can be a generator.

We shall study more on cyclic groups in course of time.

Definition. 2.20 Let $G$ be a group, $H, K$ be two subgroups of $G$. Then the set $HK = \{ab : a \in H, b \in K\}$ is called the *internal direct product* of $H$ and $K$. Similarly $KH = \{kh : k \in K, h \in H\}$.

We say that $HK = KH$ if the two sets are equal, it does not mean that $hk = kh$ for all $h \in H$ for all $k \in K$, it means that for $h \in H, k \in K$ there exist $h_1 \in H, k_1 \in K$ such that $hk = k_1h_1$ so that $hk \in KH$, i.e., $HK \subset KH$. Similarly $kh = h_2k_2$ for some $h_2 \in H, k_2 \in K$ so that $kh \in HK$, i.e., $KH \subset HK$. This makes the two sets equal.

Theorem. 2.21 *If $H$ and $K$ are subgroups of a group $G$ then the product $HK$ is also a subgroup of $G$ provided $HK = KH$.*

Proof. Choose $a, b \in HK$. Then $a = h_1k_1$ and $b = h_2k_2$ for some $h_1, h_1 \in H$ and $k_1, k_2 \in K$. Then

$$\begin{aligned} a^{-1}b &= (h_1k_1)^{-1}(h_2k_2) = (k_1^{-1}h_1^{-1})(h_2k_2) \\ &= k_1^{-1}(h_1^{-1}h_2)k_2 \text{ (by associative property)} \\ &= k_1^{-1}h_3k_2 \text{ (where } h_3 = h_1^{-1}h_2) \\ &= k_1^{-1}k_3h_4 \text{ (where } h_3k_2 = k_3h_4, \text{ since } HK = KH) \\ &= k_4h_4 \text{ (where } k_1^{-1}k_3 = k_4) \ . \end{aligned}$$

Thus $a^{-1}b \in KH = HK$. Hence $KH$ is a subgroup of $G$. ■

The condition $HK = KH$ is necessary, the following example explains it.

Example. 2.22 Consider $G = S_3$ the permutation group on the set $\{1, 2, 3\}$. Let $H = \{i, \rho\}$ and $K = \{i, \sigma\}$, where $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Here note that $\rho^{-1} = \rho$ and $\sigma^{-1} = \sigma$, i.e., $\rho^2 = \sigma^2 = i$. Now $HK = \{i, \rho, \sigma, \rho\sigma\}$ is not a subgroup of $S_3$ since $\rho\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ has no inverse in $HK$. (Calculate $(\rho\sigma)^{-1}$ and see it).

## 2.4 Exercises

1. Find the cyclic subgroup of $\mathbb{Z}_{30}$ generated by (25).

2. Show that a group with no proper nontrivial subgroup is cyclic.

3. Show that any subgroup of a cyclic group is cyclic.

4. Show that the elements $(1), (5), (7), (11), (13)$ and $(17)$ are generators of $\mathbb{Z}_{18}$.

# 3 Cyclic Group

The cyclic subgroup of a group and in particular the cyclic group have already been defined in previous section. We recall the definition of cyclic group once again.

Definition. 3.1 A group generated by a single element is called a *cyclic group*. If an element $a$ is a generator of a group $G$ then it is written as $G = \langle a \rangle$.

If $a$ is a generator of the group $G$ then $G = \{a^k : k \in \mathbb{Z}\}$. Recall that for any positive integer $k$, $a^k = a \circ a \circ \cdots \circ a$ ($k$-times) and $a^{-k} = a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}$ ($k$-times). When the binary operation is $+$ we write $ka$ instead of $a^k$ and $-a$ for $a^{-1}$. Hence we can say the group $(\mathbb{Z}, +)$ is cyclic group generated by 1. Also $-1$ is another generator of $(\mathbb{Z}, +)$ as $\mathbb{Z} = \{k.(-1) : k \in \mathbb{Z}\}$.

Example. 3.2

1. Consider the multiplicative group $G$ of all the roots of the equation $x^n = 1$, where $n > 1$ is an integer. Taking $\theta = \frac{2\pi}{n}$ and $\alpha = \cos\theta + i\sin\theta$, the roots are $\alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n = 1$. Thus $\alpha$ is a generator of the group, i.e., $G = \langle \alpha \rangle$.

2. In the above example if $n$ is a prime integer then for any $k$, not a multiple of $n$, $\alpha^k$ is a generator of $G$. However, for a composite $n$ some $\alpha^k$ may generate a proper subgroup of $G$. For example let $n = 6$, then $-\omega$ is a generator of the group of all the roots of $x^6 = 1$. But $(-\omega)^4 = \omega$ generates a proper subgroup $\{1, \omega, \omega^2\}$ of it.

3. Consider a regular $n$-gon in plane, Let $r$ denotes the rotation about the centre of the polygon by an angle $\frac{2\pi}{n}$. Then $\langle r \rangle$ is a group and is a subgroup of $D_n$.

4. $D_n$, the dihedral group of order $n$ is not a cyclic group, since the flip of the plane about a symmetric axis can not be obtained from rotation, on the other hand a rotation can not be obtained from flip.

Theorem. 3.3 *If $a$ is a generator of a group $G$ then $o(G) = o(a)$, in particular if $G$ is finite and $o(G) = n$ then $G = \{e, a, a^2, \ldots, a^{n-1}\}$.*

Proof. Let $o(a) = n < \infty$. Then $a^n = e$, where $e$ is the identity element of $G$. Also $a, a^2, \ldots, a^{n-1}, e$ are distinct elements of $G$, for if $a^i = a^j$, $1 \leq i < j < n$ then $a^{i-j} = a^0 = e$ contradicting the fact that $n$ is the smallest positive integer such that $a^n = e$. Also if $k > n$ then by division algorithm $k = nr + q$, $r \in \mathbb{N}$, $0 \leq q < n$. Hence $a^k = a^{nr+q} = (a^n)^r a^q = e^r a^q = ea^q = a^q$ where $0 \leq q < n$. Hence $a, a^2, \ldots, a^{n-1}, e$ are the only elements of $G$ and hence $o(G) = n$.

When $o(a) = \infty$ then there exists no $n$ for which $a^n = e$. Hence for $i, j \in \mathbb{Z}$, $i =\neq j$, if $a^i = a^j$ then $a^{i-j} = e$ showing that $o(a)$ is finite – a contradiction. Hence $\{a^i : i \in \mathbb{Z}\}$ is an infinite set and hence $o(G) = \infty$. ■

Theorem. 3.4 *In a group $G$ if $a^m = a^n = e$ for $m, n \in \mathbb{N}$ then $a^d = e$ where $d = \gcd(m, n)$. Also if $a^m = e$ where $m \in \mathbb{N}$ then $o(a)$ divides $m$.*

Proof. Since $d = \gcd(m, n)$ there exist integers $x, y$ such that $d = mx + ny$. Hence $a^d = a^{mx+ny} = a^{mx}a^{ny} = (a^m)^x(b^n)^y = e^x e^y = e$.

Now, assume that $a^m = e$ and $o(a) = n$. Then, since $a^n = e$, by above $a^d = e$ where $d = \gcd(m, n)$. But $n$ being the smallest positive integer such that $a^n = e$ and $0 < d \leq n$, we must have $d = n$. Hence $\gcd(m, n) = n$, i.e., $n$ divides $m$. ■

# 4 Permutation

We have already been introduced with permutation before defining the group. Here we study it formally.

The set of all the bijective maps on a set $S$ is denoted by $A(S)$. $A(S)$ forms a group with respect to the composition of mappings. For a finite set $S = \{x_1, x_2, \ldots, x_n\}$ we write $S_n$ instead of $A(S)$. The elements of $S_n$ are called the permutations on $S$. Here also without any loss of generality we may take $S = \{1, 2, \ldots, n\}$ as we are not interested of the elements of the set rather the effect of permutation on the elements.

Definition. 4.1 A *permutation* on a finite set $S$ is a bijection map on the set onto itself. The group of all the permutations on the set is called the *group of symmetry of order n.*

If $f \in S_n$ we write it as $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ where $f(1) = i_1$, $f(2) = i_2$, ..., $f(n) = i_n$. Writing the inverse of $f$ is simple, just interchange the rows and arrange columns accordingly. for example take $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ in $S_4$. Then $f^{-1}$ is given by,

$$f^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

The product (actually composition) of two permutations is obtained by applying the right first and then the left. For example, if $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$ then their products are $gf = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_{i_1} & j_{i_2} & \cdots & j_{i_n} \end{pmatrix}$ and $fg = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_{j_1} & i_{j_2} & \cdots & i_{j_n} \end{pmatrix}$.

Example. 4.2 Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$. Find (i) $f^{-1}$, (ii) $fg$ and (iii) $gf$.

(i) $f^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

(ii) $fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

Here $1 \xrightarrow{g} 3 \xrightarrow{f} 4$, $2 \xrightarrow{g} 2 \xrightarrow{f} 3$, $3 \xrightarrow{g} 1 \xrightarrow{f} 2$, and $4 \xrightarrow{g} 4 \xrightarrow{f} 1$.

(iii) $gf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

## 4.1 Cycles and transpositions

Definition. 4.3 Let $i_1, i_2, \ldots, i_k \in S = \{1, 2, \ldots, n\}$ and $f \in S_n$ be such that $f(i_1) = i_2, f(i_2) = i_3, \ldots, f(i_{k-1}) = i_k$, $f(i_k) = i_1$ and $f(i) = i$ for $i \neq i_j, 1 \leq j \leq k$. Then $f$ is called a *k-cycle* or a *cycle of length k* and is denoted by $f = (i_1 \quad i_2 \quad \ldots \quad i_k)$.

In the notation of a $k$-cycle the only order of the elements is important. Hence $f = (i_1 \quad i_2 \quad \ldots \quad i_k) = (i_2 \quad i_3 \quad \ldots \quad i_k \quad i_1) = (i_3 \quad i_4 \quad \ldots \quad i_k \quad i_1 \quad i_2)$ and so on.

Example. 4.4 If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$. Then in cycle notation $f = (1 \quad 2 \quad 3 \quad 4) = (2 \quad 3 \quad 4 \quad 1) = (3 \quad 4 \quad 1 \quad 2) = (4 \quad 1 \quad 2 \quad 3)$, this is a 4-cycle and $g = (1 \quad 3) = (3 \quad 1)$ which is a 2-cycle..

Definition. 4.5 A 2-cycle is called a *transposition*

Definition. 4.6 Two cycles are called *disjoint* if they have no integer in common.

Example. 4.7 (i) The cycles $(2 \quad 3 \quad 6)$ and $(1 \quad 5 \quad 4 \quad 7)$ in $S_7$ are disjoint as there is no common element.

(ii) $(2 \quad 3 \quad 6)$ and $(1 \quad 5 \quad 3)$ in $S_7$ are not disjoint cycles as there is a common element 3.

Theorem. 4.8 *If $f$ and $g$ are disjoint cycles then $fg = gf$.*

Proof. Let $f = (i_1 \quad i_2 \quad \dots \quad i_k)$ be a $k$-cycle and $g = (j_1 \quad j_2 \quad \dots \quad j_m)$ be an $m$-cycle in $S_n$, $f$ and $g$ are disjoint. Let $x \in S = \{1, 2, \dots, n\}$. Note that $A = \{i_1, i_2, \dots, i_k\} \subset S$ and $B = \{j_1, j_2, \dots, j_m\} \subset S$ and $A \cap B = \emptyset$. Also for $x \notin A$, $f(x) = x$ and for $x \notin B, g(x) = x$.

If $x \in A$ then $x \notin B$ and hence $f(x) \in A$ and $g(x) = x$. Thus $gf(x) = g(f(x)) = f(x)$ and $fg(x) = f(g(x)) = f(x)$. Thus $fg(x) = gf(x)$.

If $x \in b$ then $x \notin A$ and hence $g(x) \in B$ and $f(x) = x$. Thus $gf(x) = g(f(x)) = g(x)$ and $fg(x) = f(g(x)) = g(x)$. Thus $fg(x) = gf(x)$.

If $x \in S - (A \cup B)$ then $f(x) = g(x) = x$ and hence $fg(x) = gf(x)$.

Thus for all $x \in S$, $fg(x) = gf(x)$. Hence $fg = gf$. ■

Example. 4.9 Take $f, g \in S_7$ as follows: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 6 & 5 & 3 & 7 \end{pmatrix} = (3\ 4\ 6)$, a 3-cycle and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 4 & 7 & 6 & 1 \end{pmatrix} = (1 \quad 5 \quad 7)$ is also a 3-cycle. Here $S = \{1, 2, 3, 4, 5, 6, 7\}, A = \{3, 4, 6\}$ and $B = \{1, 5, 7\}$. Obviously, $f$ and $g$ are disjoint and it can easily be verified that for all $x \in S$, $fg(x) = gf(x)$, i.e., $fg = gf = (3 \quad 4 \quad 6)(1 \quad 5 \quad 7) = (1 \quad 5 \quad 7)(3 \quad 4 \quad 6)$.

Example. 4.10 For a $k$-cycle $f = (i_1 \quad i_2 \quad \dots \quad i_k)$ its inverse is given by, $f^{-1} = (i_k \quad i_{k-1} \quad \dots \quad i_2 \quad i_1)$.

It can be easily verified that

$$ff^{-1} = (i_1 \quad i_2 \quad \dots \quad i_k)(i_k \quad i_{k-1} \quad \dots \quad i_2 \quad i_1) = i.$$

where $i$ is the identity permutation. Hence the result follows.

Example. 4.11 The inverse of a transposition is itself.

Theorem. 4.12 *If $f$ is a $k$-cycle then $o(f) = k$.*

Proof. Let $f = (i_1 \quad i_2 \quad \dots \quad i_k)$ be a $k$-cycle. Then $f(x) = x$ for all $x \notin \{i_1, i_2, \dots, i_k\}$. Also $f(i_1) = i_2, f^2(i_1) = f(f(i_1)) = f(i_2) = i_3, f^3(i_1) = f(f^2(i_1)) = f(i_3) = i_4$, proceeding this way, $f^{k-1}(i_1) = i_k$ and $f^k(i_1) = f(f^{k-1}(i_1)) = f(i_k) = i_1$. Hence we can write $f$ as $f = (i_1 \quad f(i_1) \quad f^2(i_1) \quad \dots \quad f^{k-1}(i_1))$.

Thus we have $f^k(i_1) = i_1$, $f^k(i_2) = f^k(f(i_1)) = f^{k+1}(i_1) = f(f^k(i_1)) = f(i_1) = i_2$. For $2 < r < k$, $f^k(i_r) = f^k(f^{r-1}(i_1)) = f^{k+r-1}(i_1) = f^{r-1}(f^k(i_1)) = f^{r-1}(i_1) = i_r$. Hence we have $f^k(x) = x$ for all $x$ in the domain of $f$. Thus $f^k = i$, the identity element of $S_n$.

Since for $r < k$, $f^r(i_1) = i_{r+1} \neq i_1$, i.e., $f^r \neq i$ for any positive integer $r$ less than $k$ we have $o(f) = k$. ■

Theorem. 4.13 *Every permutation is a product of disjoint cycles.*

Proof. Take any $f \in S_n$, $S = \{1, 2, \dots, n\}$. Let $A_1 = \{1, f(1), f^2(1), \dots, \}$ Then $A_1$ is finite since $S$ is finite. Let $a$ be the first integer in $S$ which is not in $A_1$ and set $A_2 = \{a, f(a), f^2(a), \dots\}$. Then $A_2$ is also finite. Take $b \in S$ as the first element of $S$ which is not in $A_1 \cup A_2$ and set $A_3 = \{b, f(b), f^2(b), \dots\}$. This process terminates after a finite number of steps as $S$ is a finite set and we have $S = A_1 \cup A_2 \cup \cdots \cup A_k$, $A_i \cap A_j = \emptyset$ for $i \neq j$. Some $A_i$'s may be singletons.

For each $i = 1, 2, \dots, k$ define $\sigma_i \in S_n$ by $\sigma_i(x) = f(x)$ if $x \in A_i$ and $\sigma_i(x) = x$ otherwise. Then each $\sigma_i$ is a cycle, and $f = \sigma_1 \sigma_2 \cdots \sigma_k$. Since $A_1, A_2, \dots, A_k$ are disjoint the cycles $\sigma_1, \sigma_2, \dots, \sigma_k$ are disjoint. ■

Example. 4.14 Decompose the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 3 & 9 & 7 & 8 & 1 & 6 & 2 \end{pmatrix}$ into disjoint cycles.

Here $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Starting with 1, $A_1 = \{1, 5, 7\}$. First element of $S$ not in $A_1$ is 2, so $A_2 = \{2, 4, 9\}$. The first member not in $A_1 \cup A_2$ is 3. So $A_3 = \{3\}$. The first member not in $A_1 \cup A_2 \cup A_3$ is 6. So $A_4 = \{6, 8\}$.

Hence $\sigma_1 = (1 \quad 5 \quad 7), \sigma_2 = (2 \quad 4 \quad 9), \sigma_3 = (3)$ and $\sigma_4 = (6 \quad 8)$. Here $\sigma_3 = (3)$ is an one-cycle and we can omit it. Hence $f = \sigma_1\sigma_2\sigma_4 = (1 \quad 5 \quad 7)(2 \quad 4 \quad 9)(6 \quad 8)$. As the cycles are disjoint, they can be placed in any order.

Theorem. 4.15 *Every $k$-cycle can be decomposed as a product of $k-1$ transpositions.*

Proof. If $(i_1 \quad i_2 \quad \ldots \quad i_k)$ is a $k$-cycle then it can be written as:

$(i_1 \quad i_2 \quad \ldots \quad i_k) = (i_1 \quad i_k)(i_1 \quad i_{k-1})(i_1 \quad i_{k-2}) \cdots (i_1 \quad i_3)(i_1 \quad i_2)$. ■

Here it can be observed that transpositions are not disjoint and hence the order of the product can not be altered.

In the last two theorems we have seen that a permutation can be decomposed into disjoint cycles and each cycle can again be decomposed into transpositions. Thus combining these we have the following theorem.

Theorem. 4.16 *Every permutation in $S_n$ can be expressed as a product of transpositions.*

Proof. Follows from those of the last two theorems. ■

Example. 4.17 If $f = (i_1 \quad j_1)(i_2 \quad j_2) \cdots (i_k \quad j_k)$ is a product of $k$ transpositions then $f^{-1} = (i_k \quad j_k)(i_{k-1} \quad j_{k-1}) \cdots (i_1 \quad j_1)$.

$$\begin{aligned} f^{-1} &= ((i_1 \quad j_1)(i_2 \quad j_2) \cdots (i_k \quad j_k))^{-1} \\ &= (i_k \quad j_k)^{-1}(i_{k-1} \quad j_{k-1})^{-1} \cdots (i_1 \quad j_1)^{-1} \\ &= (i_k \quad j_k)(i_{k-1} \quad j_{k-1}) \cdots (i_1 \quad j_1). \end{aligned}$$

Example. 4.18 Decompose the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 3 & 9 & 7 & 8 & 1 & 6 & 2 \end{pmatrix}$ into transpositions. Also find the inverse of $f$.

We have already decomposed the permutation into disjoint cycles as

$f = (1 \quad 5 \quad 7)(2 \quad 4 \quad 9)(6 \quad 8)$.

Now $(1 \quad 5 \quad 7) = (1 \quad 7)(1 \quad 5)$, $(2 \quad 4 \quad 9) = (2 \quad 9)(2 \quad 4)$. Also $(6 \quad 8)$ is already a transposition.

Hence $f = (1 \quad 5 \quad 7)(2 \quad 4 \quad 9)(6 \quad 8) = (1 \quad 7)(1 \quad 5)(2 \quad 9)(2 \quad 4)(6 \quad 8)$.

Hence $f^{-1} = (6 \quad 8)(2 \quad 4)(2 \quad 9)(1 \quad 5)(1 \quad 7) = (6 \quad 8)(2 \quad 9 \quad 4)(1 \quad 7 \quad 5)$ which can be expressed as $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 3 & 2 & 1 & 8 & 5 & 6 & 4 \end{pmatrix}$

## 4.2 Odd and Even Permutations

Consider a polynomial $P$ of $n$ variables $x_1, x_2, \dots, x_n$,

$$\begin{aligned} P(x_1, x_2, \dots, x_n) &= (x_1 - x_2)(x_1 - x_3)\cdots(x_1 - x_n)(x_2 - x_3)\cdots(x_{n-1} - x_n) \\ &= \prod_{1 \le i < j \le n} (x_i - x_j). \end{aligned}$$

Any permutation of the variables only changes the sign of $P$ without changing the value. Let $f \in S_n$, then define $f^*P$ by

$$\begin{aligned} f^*P(x_1, x_2, \dots, x_n) &= P(x_{f(1)}, x_{f(2)}, \dots, x_{f(n)}) \\ &= \prod_{1 \le i < j \le n} (x_{f(i)} - x_{f(j)}). \end{aligned}$$

Then it can be observed that for any $f \in S_n$, either $f^*P = P$ or $f^*P = -P$.

For example consider a transposition $\sigma = (1 \quad 2) \in S_3$. Then

$$\begin{aligned} P(x_1, x_2, x_3) &= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \\ \sigma^*P(x_1, x_2, x_3) &= (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) \ = \ -P(x_1, x_2, x_3). \end{aligned}$$

For another example consider a 3-cycle $\tau = (1 \quad 3 \quad 4)$ in $S_4$. Then

$$\begin{aligned} P(x_1, x_2, x_3, x_4) &= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4) \\ \sigma^*P(x_1, x_2, x_3, x_4) &= (x_3 - x_2)(x_3 - x_4)(x_3 - x_1)(x_2 - x_4)(x_2 - x_1)(x_4 - x_1) \\ &= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4) \\ &= P(x_1, x_2, x_3, x_4). \end{aligned}$$

Definition. 4.19 A permutation $f$ in $S_n$

1. is called an *odd permutation* if $f^*P(x_1, x_2, \dots, x_n) = -P(x_1, x_2, \dots, x_n)$ and

2. is called an *even permutation* if $f^*P(x_1, x_2, \dots, x_n) = P(x_1, x_2, \dots, x_n)$.

Note that any transposition changes the sign of $P$ and hence is an odd permutation. It is known that any permutation $f$ can be expressed as a product of transpositions $f = \sigma_1\sigma_2 \dots \sigma_k$. Now applying $f$ on $P$ means applying $k$ number transpositions on $P$ and will change the sign of $P$ $k$ number of times. Thus $f^*P = (-1)^k P$, i.e., $f$ is even if $k$ is even and odd if $k$ is odd. So we can redefine odd and even permutation as follows:

Definition. 4.20 A permutation is called an *even permutation* if it is a product of even number of transpositions and is called an *odd permutation* if it is a product of odd number of transpositions.

Theorem. 4.21 *A $k$-cycle is even if and only if $k$ is odd.*

Proof. Any $k$-cycle $(i_1 \quad i_2 \quad \ldots \quad i_k)$ can be expressed as

$$(i_1 \quad i_2 \quad \ldots \quad i_k) = (i_1 \quad i_k)(i_1 \quad i_{k-1}) \cdots (i_1 \quad i_3)(i_1 \quad i_2)$$

which is a product of $k-1$ transpositions. Hence $(i_1 \quad i_2 \quad \ldots \quad i_k)$ is even if and only if $k-1$ is even if and only if $k$ is odd. ■

Theorem. 4.22 *All the even permutations in $S_n$ forms a subgroup of it.*

Proof. Note that the identity permutation $i$ is an even permutation. Also if $f$, $g$ are even permutations then both are product of even number of transpositions and hence $fg$ is also a product of even number of transpositions, i.e., $fg$ is an even permutation.

Finally if $f$ is an even permutation then it is a product of even number of transpositions and hence $f^{-1}$ is also a product of even number of transpositions. Thus $f^{-1}$ is an even transposition.

Thus the set of all the even permutations is a subgroup of $S_n$. ■

Definition. 4.23 The subgroup of all the even permutations in $S_n$ is called the *alternating group* of order $n$ and is denoted by $A_n$.

Note that $o(S_n) = n!$, half of which are odd permutations and rest half are even permutations. So $o(A_n) = \frac{n!}{2}$.

## 4.3 Exercise

1. Decompose the into disjoint cycles and find the parity (odd or even) of the following permutations. Also find the inverse of each of them.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 5 & 2 & 1 & 6 & 8 & 7 & 9 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 5 & 7 & 2 & 4 & 6 & 1 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 3 & 5 & 7 & 1 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 2 & 4 & 6 & 9 & 1 & 8 \end{pmatrix}$

2. Find the alternating group $A_4$.

3. Find the missing entries so that the following permutations are (i) odd (ii) even:

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

# 5 Lagrange's Theorem

This is a famous theorem regarding the order of subgroups of finite group. It has many important consequences.

Theorem. 5.1 *If $G$ is a finite group and $H$ is a subgroup of $G$ then order of $H$ divides the order of $G$.*

Proof. Define a relation $\sim$ on $G$ as follows: for all $a, b \in G$, $a \sim b$ iff $a^{-1}b \in H$. Then (i) since for all $a \in G$, $a^{-1}a = e \in H$, $a \sim a$ and hence $\sim$ is reflexive. (ii) For $a, b \in G$, $a \sim b \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H$ (since $H$ is a subgroup) $\Rightarrow b^{-1}a \in H \Rightarrow b \sim a$. Hence $\sim$ is symmetric. (iii) For $a, b, c$ assume that $a \sim b$ and $b \sim c$. Then $a^{-1}b \in H$ and $b^{-1}c \in H$ which implies that $(a^{-1}b)(b^{-1}c) \in H \Rightarrow a^{-1}(bb^{-1})c \in H \Rightarrow a^{-1}c \in H \Rightarrow a \sim c$. Thus $\sim$ is transitive.

Hence the relation $\sim$ is an equivalence relation and so it divides $G$ into equivalence classes. Note that for $a \in G$ the equivalence class containing $a$ is

$$\begin{aligned} [a] &= \{b \in G : a^{-1}b \in H\} = \{b \in G : a^{-1}b = h \text{ for some } \in H\} \\ &= \{b \in G : b = ah \text{ for some } \in H\} = \{ah : h \in H\} \\ &= aH. \end{aligned}$$

In particular, if $a \in H$ then $[a] = H$. Now, for $a \in G$ consider the mapping $\psi_a : H \to [a]$ defined by $\psi_a(h) = ah$ for all $h \in H$. For $h_1, h_2 \in H$, $\psi_a(h_1) = \psi_a(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$. Hence $\psi_a$ is injective. Also for $ah \in [a]$ we have $\psi_a(h) = ah$, thus $\psi_a$ is surjective. Thus $\psi_a$ is a bijection from $H$ onto $[a] = aH$.

$H$ being a finite set, let $o(H) = k$. So the class $[a]$ has also $k$ number of elements. Thus every equivalence class have the same number of elements $k$. If then number of equivalence classes is $m$ then $n = km$. Thus $k|n$, i.e., $o(H)$ divided $o(G)$. ■

Definition. 5.2 If $G$ is a finite group and $H$ is a subgroup of $G$ then the number $o(G)/o(H)$ is called the *index* of $H$ in $G$.

Definition. 5.3 If $H$ is a subgroup of $G$ then for $a \in G$ the set $aH = \{ah : h \in H\}$ is called a *left coset* of $H$. The set $Ha = \{ha : h \in H\}$ is called a right coset of $H$.

Usually a left coset need not be a right coset, however if $G$ is abelian group then for any $a \in G$ and for any subgroup $H$ of $G$, $aH = Ha$.

Example. 5.4 Let us consider the group $S_3$ and $H = \{i, f\}$ where $i$ is the identity permutation and $f = (1 \quad 2)$. Then $H$ is a subgroup of $S_3$. Now $S_3 = \{i, f, g, h, \rho, \sigma\}$ where $g = (2 \quad 3), h = (1 \quad 3)$, $\rho = (1 \quad 2 \quad 3)$ and $\sigma = (1 \quad 3 \quad 2)$.

The left cosets are $fH = H, gH, hH, \rho H$ and $\sigma H$.

$$\begin{aligned}
gH &= \{gi, gf\} = \{g, \sigma\} \text{ since } gf = (2 \quad 3)(1 \quad 2) = (1 \quad 3 \quad 2) = \sigma. \\
hH &= \{hi, hf\} = \{h, \rho\} \text{ since } hf = (1 \quad 3)(1 \quad 2) = (1 \quad 2 \quad 3) = \rho. \\
\rho H &= \{\rho i, \rho f\} = \{\rho, h\} \text{ since } \rho f = (1 \quad 2 \quad 3)(1 \quad 2) = (1 \quad 3) = h. \\
\sigma H &= \{\sigma i, \sigma f\} = \{\sigma, g\} \text{ since } \sigma f = (1 \quad 3 \quad 2)(1 \quad 2) = (2 \quad 3) = g.
\end{aligned}$$

There are three distinct left cosets, $gH = \sigma H, hH = \rho H$ and $H$ itself.

The right cosets are $Hf = H, Hg, Hh, H\rho$ and $H\sigma$.

$$\begin{aligned}
Hg &= \{ig, fg\} = \{g, \rho\} \text{ since } fg = (1 \quad 2)(2 \quad 3) = (1 \quad 2 \quad 3) = \rho. \\
Hh &= \{ih, fh\} = \{h, \sigma\} \text{ since } fh = (1 \quad 2)(1 \quad 3) = (1 \quad 3 \quad 2) = \sigma. \\
H\rho &= \{i\rho, f\rho\} = \{\rho, g\} \text{ since } f\rho = (1 \quad 2)(1 \quad 2 \quad 3) = (2 \quad 3) = g. \\
H\sigma &= \{i\sigma, f\sigma\} = \{\sigma, h\} \text{ since } f\sigma = (1 \quad 2)(1 \quad 3 \quad 2) = (1 \quad 3) = h.
\end{aligned}$$

There are three distinct right cosets, $Hg = H\rho, Hh = H\sigma$ and $H$ itself.

Hence from the above we see that $gH \neq Hg, hH \neq Hh, \rho H \neq H\rho, \sigma H \neq H\sigma$. Hence all the left cosets are different from the corresponding right coset. However the number of left cosets is equal to the number of right cosets, which is the index of $H$ in $G$, i.e., $o(G)/o(H) = 6/2 = 3$.

Theorem. 5.5 *A group of prime order is cyclic.*

Proof. Let $G$ be a group of prime order $p$. For any $a \in G$, $a$ is not the identity element of $G$, the cyclic group $\langle a \rangle$ is a non-trivial subgroup of $G$. By Lagrange's Theorem $o(\langle a \rangle)$ divides $o(G)$. Since $o(G) = p$ is prime and $o(\langle a \rangle) > 1$, we have $o(\langle a \rangle) = p$, i.e., $G = \langle a \rangle$. Hence $G$ is cyclic. ■

Corollary. 5.6 *For a finite group $G$ and $a \in G$, $o(a)$ divides $o(G)$.*

## 5.1 Euler's Theorem and Fermat's Theorem

Consider the group $\mathbb{Z}_n$ the groups of integers modulo $n$. Then $\mathbb{Z}_n$ forms a group under addition modulo $n$. Now define multiplication on $\mathbb{Z}_n$ as follows: for $[p], [q] \in \mathbb{Z}$, $[p].[q] = [pq]$. Though this multiplication is well defined, $\mathbb{Z}_n$ does not form a group under multiplication as it contains *divisors of zero* for example in $\mathbb{Z}_6$, $[2].[3] = [6] = [0]$, but $[2] \neq [0], [3] \neq [0]$.

For $n \in \mathbb{N}$, let $U_n$ denote the set of all those members $[p]$ for which $p$ is prime to $n$, i.e., $U_n = \{[p] \in \mathbb{Z}_n : \gcd(p, n) = 1\}$. Then it can be easily be verified that $U_n$ is a group with respect to multiplication modulo $n$ with the identity element $[1]$.

Definition. 5.7 The group $U_n = \{[p] \in \mathbb{Z}_n : \gcd(p, n) = 1\}$ is called the *group of units* in $\mathbb{Z}_n$.

Example. 5.8

1. $U_6 = \{[1], [5]\}$, Here only 1 and 5 are the numbers less than 6 and prime to 6.
2. $U_7 = \{[1], [2], [3], [4], [5], [7]\}$, here 7 being a prime number all non-zero numbers less than 7 is prime to 7 and hence $U_7$ contains 6 elements.
3. For any prime number $p$, $U_p = \{[1], [2], \ldots, [p-1]\}$ whcih contains $p-1$ elements.
4. $U_8 = \{[1], [3], [5], [7]\}$.

Definition. 5.9 Euler's $\phi$-function is defined as follows: For any $n \in \mathbb{N}$, $n > 1$, $\phi(n)$ is the number of positive integers $m$ such that $1 \leq m < n$ and $\gcd(m, n) = 1$. For $n = 1$, $\phi(1)$ is defined as 1.

It immediately follows that if $n$ is a prime number then $\phi(n) = n - 1$.

Hence for $n \in \mathbb{N}$ the order of the group $U_n$ is $\phi(n)$.

Theorem. 5.10 (Euler) *If $a$ is an integer relatively prime to $n$ then $a^{\phi(n)} \equiv 1(\text{mod } n)$.*

Proof. Note that $U_n$ is an abelian group under multiplication modulo $n$ and the order $U_n$ is $\phi(n)$. Then $[a] \in U_n$ since $\gcd(a, n) = 1$. Hence $[a]^{\phi(n)} = [1]$. But $[a]^{\phi(n)} = [a^{\phi(n)}] = [1]$ if and only if $a^{\phi(n)} - 1$ is divisible by $n$. This shows that $a^{\phi(n)} \equiv 1(\text{mod } n)$. ■

A special case of Euler's Theorem is the Fermat's Little Theorem is which states that if $p$ is prime then for any $a$ not divisible by $p$, $a^{p-1}$ is divisible by $p$.

THEOREM. 5.11 (FERMAT) *If $p$ is a prime number and if $p$ does not divide $a$, then $a^{p-1} \equiv 1(\text{mod } p)$.*

PROOF. Since $p$ is a prime number $\phi(p) = p - 1$ and also $\gcd(a, p) = 1$. Hence by applying Euler's Theorem $a^{p-1} \equiv 1(\text{mod } p)$. Hence $a.a^{p-1} \equiv a.1(\text{mod } p)$, i.e., $a^p \equiv a(\text{mod } p)$. ■

It can be noted that if $p|a$ then $a \equiv 0(\text{mod } p)$ which implies that $a^p \equiv 0(\text{mod } p)$. Hence $a^p \equiv p(\text{mod } p)$ for all integer $a$.

## 5.2 Exercise

1. Let $G = S_4$. Find all the right cosets of $H = \{i, f\}$ where $f = (1\ 2)$.

2. In $\mathbb{Z}_8$ find the right cosets of the subgroup $H = \{[0], [3], [6]\}$.

3. Write down the composition table of the group $U_9$. Also find the order of all the elements of $U_9$.

4. If $G = \{a_1, a_2, \dots, a_n\}$ is a finite abelian group and $x = a_1 a_2 \cdots a_n$, then show that $x^2 = e$.

# 6 Normal Subgroups

It has been observed that for some subgroup $H$ of a group $G$ the left coset may not be equal to the corresponding right coset. If a subgroup $H$ be such that every left coset is equal to the corresponding right coset then that subgroup is called an *invariant subgroup* or a *normal subgroup* of $G$.

DEFINITION. 6.1 A subgroup $N$ of a group $G$ is called a *normal subgroup* of $G$ if for all $g \in G$, $gNg^{-1} \subset N$ and is denoted by $N \lhd G$.

It can be observed that for a subgroup $N$ of a group $G$, if the condition $gNg^{-1} \subset N$ is satisfied for all $g \in G$ then $N = eNe = (g^{-1}g)N(g^{-1}g) = g^{-1}(gNg^{-1})g \subset g^{-1}Ng \subset N$ and hence $N = gNg^{-1}$. Thus we can alternatively say that $N$ is a normal subgroup of $G$ if for all $g \in G$, $gNg^{-1} = N$.

THEOREM. 6.2 *A subgroup $N$ of a group $G$ is a normal subgroup if and only if every left coset of $N$ is also a right coset.*

PROOF. Assume that $N$ is a normal subgroup of $G$. Then for $g \in G$, $gNg^{-1} = N$. Multiplying both sides by $g$ from right, $gN = Ng$, hence every left coset is also a right coset.

Conversely, assume that every left coset is also a right coset. Let $a \in G$, Then $aN = Na$. This implies that $aNa^{-1} = N$. Since this is true for every $a \in G$ it follows that $N$ is a normal subgroup of $G$. ■

If $N \lhd G$ then the set of all the cosets of $N$ is called the quotient set and is denoted by $G/N$. It can be remembered that the relation $\sim$ on $G$ defined by $a \sim b$ if and only if $ab^{-1} \in N$ is an equivalence relation and the equivalence classes are exactly the cosets of $N$. Hence $G/N = G/\sim$.

THEOREM. 6.3 *If $N \lhd G$ then the $G/N$ is also a group with respect to the operation $Na \cdot Nb = Nab$ for all $a, b \in G$.*

PROOF. First to see whether the operation $\cdot$ is well defined, i.e., if $Na = Na'$ and $Nb = Nb'$ then $Na \cdot Nb = Na' \cdot Nb'$. If $Na = Na'$ then $aa'^{-1} \in N$ and if $Nb = Nb'$ then $bb'^{-1} \in N$. Now $(ab)(a'b')^{-1} = (ab)(b'^{-1}a'^{-1}) = a(bb'^{-1})a'^{-1} = ana'^{-1}$ where $n = bb'^{-1} \in N$. Now $N$ being a normal subgroup every left coset is also a right coset, hence $an = n'a$ for some $n' \in N$. Thus $(ab)(a'b')^{-1} = n'aa'^{-1} = n'n'' \in N$ where $n'' = aa'^{-1} \in N$. Thus $Nab = Na'b'$, i.e., $Na \cdot Nb = Na' \cdot Nb'$, i.e., the operation $\cdot$ is well defined.

Closure and associative properties are inherited from those in $G$. $N$ acts as the identity element of $G/N$. in G/N the inverse of $NainG/N$ is $Na^{-1}$ as $Na \cdot Na^{-1} = Naa^{-1} = Ne = N$. Thus $G/N$ is a group. ■

EXAMPLE. 6.4

1. For $n \in \mathbb{N}$, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, since $\mathbb{Z}$ is abelian ever subgroup is normal subgroup. Then $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$, the group of residue classes of $\mathbb{Z}$ modulo $n$.

2. Consider $S_n$, the symmetric group of order $n$. The subgroup $A_n$ of all the even permutations in $S_n$ is a normal subgroup of $S_n$.

3. If $G$ is a group of even order and $N$ is a subgroup of $G$ such that $o(G)/o(N) = 2$ then $N$ is a normal subgroup of $G$. The only cosets are $N$ and $G - N$.

Lagrange's Theorem states that order of a subgroup divides the order of the group. Question arises is the converse true? The answer if no in general. For example, there are groups of order 12 (group of symmetries of a regular tetrahedron) having no subgroup of order 6. However for some special cases the result is true. One such result is the Cauchy's Theorem.

Theorem. 6.5 (Cauchy) *If $G$ is a finite abelian group and $p$ is a prime integer dividing $o(G)$ then $G$ has an element of order $p$.*

Proof. Let $o(G) = n$, then $p \mid n$. We shall prove the theorem by induction. If $n = 1$ then there is no prime integer less than $n$ and hence result is vacuously true for $n = 1$.

Assume $n > 1$. If $n = p$ then $G$ is cyclic and hence every generator of $G$ is of order $p$. Thus the result is true.

Assume $p < n$. Then choose $a \in G$ such that $a \neq e$ where $e$ is the identity element of $G$. If $o(a) = p$ then the result is proved. Now assume that $o(a)$ is a multiple of $p$, i.e., $o(a) = m = pk$ for some $k \in \mathbb{N}$. Then $a^m = e$ and hence $e = a^m = a^{kp} = (a^k)^p$. Thus $o(a^k) = p$ and hence the result is proved.

Now assume that $p \nmid m = o(a)$. Since $a \neq e$, $\langle a \rangle = N$ is a proper subgroup of $G$. Also $G$ being abelian $N$ is a normal subgroup of $G$. Hence $G/N$ is a group and $1 < o(G/N) < o(G) = n$. Now $o(G/N) = o(G)/o(N) = \frac{n}{m} = k$(say), i.e., $n = mk$. Since $p \mid n$ and $p \nmid m$ we must have $p \mid k$. Thus $p \mid o(G/N)$. By induction hypothesis there exists a member $Nx \in G/N$ such that $o(Nx) = p$. Hence $(Nx)^p = N$, i.e., $Nx^p = N$ which implies that $x^p \in N$. Also $Nx$ being a nontrivial element of $G/N$ we have $x \notin N$. Thus $\langle x^p \rangle$ is a proper subgroup of $\langle x \rangle$ and hence $p \mid o(x)$. Then since $o(x)$ is a multiple of $p$, by the process shown above, $o(x^l) = p$ where $l = o(x)/p$. This completes the induction.

Hence in all the cases there is an element in $G$ of order $p$. ■

# 7 Homomorphisms and related theorems

## 7.1 External Direct Product

Let $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$ be $n$ groups, $G = \prod_{i=1}^n G_i = G_1 \times G_2 \times \cdots \times G_n$ be the cartesian peoduct of the underlying sets. A binary operation $*$ on $G$ can be introduced as follows: for $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in G$, define

$x * y = (x_1 *_1 y_1, x_2 *_2 y_2, \dots, x_n *_n y_n)$, i.e., the composition is componentwise. With this definition one can easily verify the following result.

Theorem. 7.1 *If $(G_1, *_1), (G_2, *_2), \dots, (G_k, *_k)$ are $n$ groups, with $o(G_i) = n_i$, $1 \leq i \leq k$, and $G = \prod_{i=1}^{k}$ then $(G, *)$ is a group of order $n_1 n_2 \dots n_n$, where $*$ is defined by: $x * y = (x_1 *_1 y_1, x_2 *_2 y_2, \dots, x_k *_n y_k)$ for all $x = (x_1, x_2, \dots, x_k), y = (y_1, y_2, \dots, y_k)$ in $G$.*

We omit the proof as any reader can verify it easily.

Definition. 7.2 The group $(\prod G_i, *)$ is called the em external direct product of the groups $(G_1, *_1), (G_2, *_2), \dots, (G_k, *_k)$.

Example. 7.3 1. Let $G = (\mathbb{Z}, +)$, then $G \times G$ with the operation $+$ defined by $(a, b) + (c, d) = (a + c, b + d)$ for all $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$ is the direct product of $\mathbb{Z}$ with itself.

2. Let $G_1 = S_3$, the symmetric group of order 3 and $G_2 = M_2$, the set of all the $2 \times 2$ matrices over real numbers. Then

$$G_1 \times G_2 = \{(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) : f \in S_3, \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in M_2\}.$$

The operation $*$ on $G_1 \times G_2$ is defined as follows: for all $(f, \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]), (g, \left[\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right])$ in $G_1 \times G_2$, $(f, \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]) * (g, \left[\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right]) = (fg, \left[\begin{smallmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd', \end{smallmatrix}\right])$. With this operation $G_1 \times G_2$ is a group.

Here we note a few properties of direct product without proof. Some other properties will be dealt in course of time.

Theorem. 7.4 *The order of the group $\prod_{i=1}^{n} (G_i, *_i)$ is $o(G_1).o(G_2).\dots.o(G_n)$.*

Theorem. 7.5 *The external product of the groups $(G_1, *_1), (G_2, *_2), \dots, (G_n, *_n)$ is abelian if and only if each $(G_i, *_i)$ is abelian.*

Theorem. 7.6 *Let $G$ be the external product of the groups $(G_1, *_1), (G_2, *_2), \dots, (G_n, *_n)$, $e_k$ be the identity element of $G_k$, $1 \leq k \leq n$. Then for each $i$, $i \leq i \leq n$, the set $G'_i = \{(e_1, e_2, \dots, e_{i-1}, x_i, e_{i+1}, \dots, e_n) : x_i \in G_i\}$, is a normal subgroup of $G$.*

## 7.2 Homomorphisms

Homomorphisms of groups are the functions between the groups which preserve the compositions of the groups.

Definition. 7.7 Let $(G, \circ), (G', *)$ be two groups. Then a mapping $\phi : G \to G'$ is called a *homomorphism* if for all $a, b \in G$, $\phi(a \circ b) = \phi(a) * \phi(b)$.

Definition. 7.8 Let $\phi : G \to G'$ be a homomorphism. If $\phi$ is one-one (injective) then it is called a *monomorphism.* If $\phi$ is onto (surjective) then it is called a *epimorphism.* If $\phi$ is one-one and onto, i.e., bijective then it is called an *isomorphism.* Two groups $G, G'$ are said to be *isomorphic* if there exists an isomorphism from $G$ onto $G'$ and is denoted by $G \simeq G'$.

Example. 7.9

1. For every group $G$ the identity map $1_G : G \to G$, defined by $1_G(x) = x$ for all $x \in G$, is a homomorphism, in fact is an isomorphism.
2. The function $f : G \to G'$ defined by $f(x) = e'$ for all $x \in G$, where $e'$ is the identity element of $G'$, is a homomorphism.
3. For $n \in \mathbb{N}$ the mapping $\phi_n : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by $\phi_n(x) = nx$ for all $x \in \mathbb{Z}$ is a homomorphism.
4. Let $S^1$ be the multiplicative group $\{z \in \mathbb{C} : |z| = 1\}$. The mapping $\phi : (\mathbb{R}, +) \to (S^1, \cdot)$ defined by $\phi(t) = \cos t + i \sin t$, for all $t \in \mathbb{R}$. Then for $t_1, t_2 \in \mathbb{R}$, $\phi(t_1 + t_2) = \cos(t_1 + t_2) + i \sin(t_1 + t_2) = (\cos t_1 + i \sin t_1) \cdot (\cos t_2 + i \sin t_2) = \phi(t_1) \cdot \phi(t_2)$. Thus $\phi$ is a homomorphism.

Theorem. 7.10 *If $\phi : G \to G'$ is a homomorphism then (i) $\phi(e) = e'$ where $e$ and $e'$ are respectively the identity elements of $G$ and $G'$ and (ii) for all $x \in G$, $\phi(x^{-1}) = (\phi(x))^{-1}$.*

Proof. (i) For an arbitrary $x \in G$, $\phi(x) = \phi(xe) = \phi(x)\phi(e)$. By left cancellation on $G'$ we have $e' = \phi(e)$. (ii) For $x \in G$, $e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$. Hence $\phi(x^{-1})$ is the inverse of $\phi(x)$, i.e., $(\phi(x))^{-1} = \phi(x^{-1})$. ■

Theorem. 7.11 *If $\phi : G \to G'$ and $\psi : G' \to G''$ are two homomorphisms the the composition $\psi \circ \phi : G \to G''$ is also a homomorphism.*

Proof is easy and hence omitted.

Theorem. 7.12 *If $\phi : G \to G'$ is a homomorphism then $\phi(G) = \{\phi(x) : x \in G\}$ is a subgroup of $G'$.*

Proof. Take $y_1, y_2 \in \phi(G)$. Then there exist $x_1, x_2 \in G$ such that $\phi(x_1) = y_1$ and $\phi(x_2) = y_2$. Now $y_1 y_2^{-1} = \phi(x_1)(\phi(x_2))^{-1} = \phi(x_1)\phi(x_2^{-1}) = \phi(x_1 x_2^{-1})$. Since $G$ is a group, $x_1 x_2^{-1} \in G$ and hence $y_1 y_2^{-1} \in \phi(G)$. Thus $\phi(G)$ is a subgroup of $G'$. ■

Theorem. 7.13 (Cayley) *Every group is isomorphic to a subgroup of some symmetric group $A(S)$.*

Proof. Recall that for a non-empty set $S$, the symmetric group $A(S)$ is the set of all bijections from $S$ to $S$, where the binary operation is the composition of mappings.

Here we take $S = G$ itself. For each $a \in G$ define a mapping $T_a : G \to G$ by $T_a(x) = ax$ for all $x \in G$. Then we have the following observations:

1. For $x_1, x_2 \in G$, $T_a(x_1) = T_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. Thus $T_a$ is injective.
2. For $y \in G$ take $x = a^{-1}y$ so that $T_a(x) = ax = aa^{-1}y = y$, hence $T_a$ is onto.

Thus for each $a \in G$, $T_a \in A(G)$. Define a mapping $\phi : G \to A(G)$ by $\phi(a) = T_a$ for all $a \in G$. We shall show that $\phi$ is a homomorphism.

For $a, b \in G$, $x \in G$, $T_a \circ T_b(x) = T_a(T_b(x)) = T_a(bx) = a(bx) = (ab)x = T_{ab}(x)$. Hence $Ta \circ T_b = T_{ab}$. Now, $\phi(ab) = T_{ab} = T_a \circ T_b = \phi(a) \circ \phi(b)$. Thus $\phi$ is a homomorphism.

Hence $\phi(G) = \{T_a : a \in G\}$ is a subgroup of $A(G)$.

Also for $a, b \in G$, $\phi(a) = \phi(b) \Rightarrow T_a = T_b \Rightarrow T_a(x) = T_b(x)$ for all $x \in G \Rightarrow ax = bx$ for all $x \in G$ and hence $a = b$. Thus $\phi$ is injective. Hence $\phi : G \to \phi(G)$ is an isomorphism. Thus $G$ is isomorphic to the subgroup $\phi(G)$ of $A(S)$. ■

Definition. 7.14 Let $\phi : G \to G'$ be a homomorphism Then the *kernel of the homomorphism* $\phi$ is defined as the set $\ker\phi = \{x \in G : \phi(x) = e'\}$, where $e'$ is the identity element of $G'$.

Theorem. 7.15 *For a homomorphism $\phi : G \to G'$, the kernel* $\ker\phi$ *is a normal subgroup of $G$.*

Proof. If $a, b \in \ker\phi$ then $\phi(a) = \phi(b) = e'$ where $e'$ is the identity element of $G'$. Hence $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = e'e'^{-1} = e'$. Hence $ab^{-1} \in \ker\phi$. This shows that $\ker\phi$ is a subgroup of $G$.

For $g \in G, a \in ker\phi$, we have $\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)e'\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = e'$. Thus $gag^{-1} \in \ker\phi$ for all $g \in G$, for all $a \in \ker\phi$. Thus $\ker\phi$ is a normal subgroup of $G$. ■

Corollary. 7.16 *A homomorphism $\phi : G \to G'$ is a monomorphism if and only if* $\ker\phi = \{e\}$*, where $e$ is the identity element of $G$.*

Proof. Since $\phi(e) = e'$ we have $e \in \ker\phi$. Also $\phi$ is injective if and only if $\phi^{-1}(e')$ can contain at most one element. Hence $\phi$ is a monomorphism if and only if $\ker\phi = \{e\}$. ■

Example. 7.17 1. Let $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$ be $n$ groups and $G = \prod_{i=1}^{n} G_i$ be their external direct product. For $1 \leq k \leq n$ define $\pi_k : G \to G_k$ by

$$\pi_k(x_1, x_2, \ldots, x_n) \;=\; x_k \text{ for all } (x_1, x_2, \ldots, x_n) \in G$$

Then it can easily be verified that $\pi_k$ is a homomorphism for each $k, 1 \leq k \leq n$. Also

$$\begin{aligned} \ker\pi_k &= \{(x_1, x_2, \ldots, x_{k-1}, e_k, x_{k+1}, \ldots, x_n) : x_i \in G_i : 1 \leq i \leq n\} \\ &= G_1 \times G_2 \times \cdots \times G_{k-1} \times \{e_k\} \times G_{k+1} \times \cdots \times G_n. \end{aligned}$$

Here $e_k$ is the identity element of $(G_k, *_k)$.

2. Let $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$ be $n$ groups and $G = \prod_{i=1}^{n} G_i$ be their external direct product. For $1 \leq k \leq n$ define $\phi_k : G_k \to G$ by

$$\phi_k(x) \;=\; (e_1, e_2, \ldots, e_{k-1}, x, e_{k+1}, \ldots, e_n), \text{ for all } x \in G_k,$$

where $e_i$ is the identity element of $(G_i, *_i)$. Then $\phi_k$ is a monomorphism of $G_k$ into $G$. If we put $G'_k = \phi_k(G) = \{e_1\} \times \{e_2\} \times \cdots \{e_{k-1}\} \times G_k \times \{e_{k+1}\} \times \cdots \{e_n\}$ then $G'_k$ is isomorphic to $G_k$.

3. We can prove that $G'_k$, as defined above, is a normal subgroup of $G$. Define $\overline{G_k} = G_1 \times \cdots G_{k-1} \times G_{k+1} \times \cdots \times G_n$ and a mapping $\psi_k : G \to \overline{G_k}$ by

$$\begin{aligned} \psi_k(x_1, x_2, \ldots, x_n) \;=\; & (x_1, x_2, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n), \\ & \text{for all } (x_1, x_2, \ldots, x_n) \in G, \end{aligned}$$

i.e., $\psi_k$ just erases the $k$-th component of $(x_1, x_2, \ldots, x_n)$. Then it is easy to verify that $\psi_k$ is a homomorphism and $\ker\psi_k = G'_k$. Hence $G'_k$ is a normal subgroup of $G$.

## 7.3 Isomorphism Theorems

Here we study the three isomorphism theorems of groups. We begin with the following.

Theorem. 7.18 (First Isomorphism Theorem) *Let $\phi : G \to G'$ be a homomorphism from $G$ onto $G'$ with kernel $K$. Then the quotient group $G/K$ is isomorphic to $G'$.*

Proof. Define a map $\psi : G/K \to G'$ by $\psi(Ka) = \phi(a)$ for all $Ka \in G/K$. First we show that $\psi$ is well defined, i.e., if $a, b \in G$ such that $Ka = Kb$ then $\psi(Ka) = \psi(Kb)$.

Choose $a, b \in G$ such that $Ka = Kb$. Then $Kab^{-1} = K$, i.e., $ab^{-1} \in K$. Since $K = \ker\phi$, $\phi(ab^{-1}) = e'$ where $e'$ is the identity element of $G'$. Thus, $\phi(a)\phi(b^{-1}) = e'$ which implies that $\phi(a)(\phi(b))^{-1} = e'$, i.e., $\phi(a) = \phi(b)$. Hence $\psi(Ka) = \psi(Kb)$.

To show that $\psi$ is a homomorphism, let $Ka, Kb \in G/K$. Then $\psi(Ka.Kb) = \psi(Kab) = \phi(ab) = \phi(a)\phi(b) = \psi(Ka)\psi(Kb)$. Thus $\psi$ is a homomorphism.

To show $\psi$ is injective, take $Ka, Kb \in G/K$ such that $\psi(Ka) = \psi(Kb)$. Then $\phi(a) = \phi(b)$ which implies that $\phi(a)(\phi(b))^{-1} = e'$, i.e., $\phi(ab^{-1}) = e'$ and hence $ab^{-1} \in \ker\phi = K$. This implies that $Ka = Kb$. Thus $\psi$ is injective.

Finally, for any $c \in G'$, since $\phi$ is onto, there exists $a \in G$ such that $\phi(a) = c$, hence $\psi(Ka) = c$. Thus $\psi$ is onto.

So $\psi$ is an isomorphism of $G/K$ onto $G'$, i.e., $G/K$ is isomorphic to $G'$. ■

Theorem. 7.19 (Correspondence Theorem) *Assume that $\phi : G \to G'$ is a homomorphism of $G$ onto $G$ with kernel $K$. Let $N'$ be a subgroup of $G'$. Define $N = \phi^{-1}(N') = \{a \in G : \phi(a) \in N'\}$. Then $N$ is a subgroup of $G$ such that $K \subset N$ and $N/K$ is isomorphic to $N'$. Moreover if $N'$ is a normal subgroup of $G'$ then $N$ is a normal subgroup of $G$.*

Proof. Take $a, b \in N$. Then $\phi(a), \phi(b) \in N'$. Since $N'$ is a subgroup of $G'$ we have $\phi(a)(\phi(b))^{-1} \in N'$, i.e., $\phi(ab^{-1} \in N'$ and hence $ab^{-1} \in N$. Thus $N$ is a subgroup of $G$. Also if $a \in K$ then $\phi(a) = e' \in N'$ which implies that $a \in N$. Thus $K \subset N$.

Since $K \lhd G$ and $K \subset N \subset G$ we have $K \lhd N$. Let $\phi_N$ denote the restriction of $\phi$ on $N$. Then $\phi_N : N \to N'$ is an onto homomorphism with kernel $K$, hence by first isomorphism we have $N/K \simeq N'$.

Finally, if $N' \lhd G'$ then for any $a \in G$, for any $y \in N'$ we have $\phi(a)y(\phi(a))^{-1} \in N'$, i.e., $\phi(a)y\phi(a^{-1}) \in N'$. In particular, if $x \in N$ then $\phi(x) \in N'$, hence we have

$\phi(a)\phi(x)\phi(a^{-1}) \in N'$, or $\phi(axa^{-1}) \in N'$ and hence $axa^{-1} \in N$. Since this is true for any $a \in G$ for any $x \in N$ we have $N \lhd G$. ■

The above result says that an onto homomorphism $\phi$ induces an one-to-one correspondence between the subgroups of $G'$ and those subgroups of $G$ which contain the kernel $K$. Moreover this correspondence assigns normal subgroups of $G'$ to normal subgroups of $G$ containing $K$.

Theorem. 7.20 (Second isomorphism Theorem) *let $H$ be a subgroup of $G$ and $N$ be a normal subgroup of $G$. Then $HN = \{hn : h \in H, n \in N\}$ is a subgroup of $G$ and $H \cap N$ is a normal subgroup of $H$ and $H/(H \cap N) \simeq HN/N$.*

Proof. First to show that $HN$ is a subgroup of $G$. Note that $e \in H, e \in N$ hence $e \in HN$, thus $HN \neq \emptyset$. Let $x = h_1n_1, y = h_2n_2 \in HN$. Then $xy^{-1} = (h_1n_1)(h_2n_2)^{-1} = (h_1n_1)(n_2^{-1}h_2^{-1}) = h_1(n_1n_2^{-1})h_2^{-1} = h_1n_3h_2^{-1}$ where $n_3 = n_1n_2^{-1} \in N$. $N$ being a normal subgroup $Nh_2^{-1} = h_2^{-1}N$ hence there exists there is $n_4 \in N$ such that $n_2h_2^{-1} = h_2^{-1}n_4$. Thus $xy^{-1} = h_1n_3h_2^{-1} = h_1h_2^{-1}n_4 = h_3n_4 \in HN$ where $h_3 = h_1h_2^{-1} \in H$. Thus $HN$ is a subgroup of $G$.

Note that $N \lhd G$ and $N < HN < G$, hence $N \lhd HN$. So the quotient group $HN/N$ is defined. Consider the mapping $\phi : H \to HN/N$ defined by $\phi(h) = hN$ for all $h \in H$. For $h \in H, n \in N$ $hnN = hN$ since $n \in N$. Let $h_1, h_2 \in H$, then $\phi(h_1h_2) = h_1h_2N = h_1Nh_2N = \phi(h_1)\phi(h_2)$. Thus $\phi$ is a homomorphism. Now,

$$\begin{aligned} \ker\phi &= \{h \in H : \phi(h) = e_{HN/N}\} = \{h \in H : \phi(h) = N\} \\ &= \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N. \end{aligned}$$

Hence $H \cap N$ is a normal subgroup of $H$ and by first isomorphism theorem $H/\ker\phi \simeq$ Image$\phi$, i.e., $H/(H \cap N) \simeq HN/N$. ■

Theorem. 7.21 (Third Isomorphism Theorem) *If $\phi : G \to G'$ is an onto homomorphism with $\ker\phi = K$ and $N' \lhd G'$ then $N = \{x \in G : \phi(x) \in N'\}$ is a normal subgroup of $G$ containing $K$ and $G/N \simeq G'/N'$. Equivalently, $(G/K)/(N/K) \simeq G/N$.*

Proof. Define a mapping $\psi : G \to G'/N'$ by $\phi(a) = \phi(a)N'$ for all $a \in G$. Then for $a, b \in G$, $\psi(ab) = \phi(ab)N' = \phi(a)\phi(b)N' = \phi(a)N'\phi(b)N' = \psi(a)\psi(b)$. Thus $\psi$ is a homomorphism. Also

$$\begin{aligned} \ker\psi &= \{a \in G : \psi(a) = N'\} = \{a \in G : \phi(a)N = N'\} \\ &= \{a \in G : \phi(a) \in N'\} = N. \end{aligned}$$

Hence by first isomorphism $G/N \simeq G'/N'$. Also since $\ker\phi = K$ and the restriction of $\phi on N$ is a homomorphism with kernel $K$ we again have $G/K \simeq G'$ and $N/K \simeq N'$. Hence $G'/N' \simeq (G/K)/(N/K)$. Thus $G/N \simeq (G/K)/(N/K)$. ■