THIRUVALLUVAR UNIVERSITY COLLEGE OF ARTS AND SCIENCE
TIRUPATTUR

# STUDY MATERIALS

# BMA51-ABSTRACT ALGEBRA

For
III YEAR, V SEMESTER

Prepared by

Dr. NARASIMMAN PASUPATHI

ASSISTANT PROFESSOR
DEPARTMENT OF MATHEMATICS
THIRUVALLUVAR UNIVERSITY COLLEGE OF ARTS AND SCIENCE
TIRUPATTUR-635 901, TAMIL NADU, INDIA

## SEMESTER - V

## PAPER - 7

## ABSTRACT ALGEBRA

**Objectives**

This course aims to impart emphasis on concepts and technology of the groups and rings as these algebraic structures have applications in Mathematical Physics, Mathematical Chemistry and Computer Science.

**UNIT-I: Groups**

Definition of a Group - Examples - Subgroups;

**UNIT-II: Groups (Contd)**

Counting Principle - Normal Subgroups - Homomorphisms.

**UNIT-III: Groups (Contd)**

Automorphisms - Cayley's Theorem - Permutation Groups.

**UNIT-IV: Rings**

Definition and Examples - Integral Domain - Homomorphism of Rings - Ideals and Quotient Rings.

**UNIT-V: Rings (Contd)**

Prime Ideal and Maximal Ideal - The field of quotients of an Integral domain – Euclidean rings.

**Recommended Text**

I.N.Herstein (1989), Topics in Algebra, (2nd Edn.)Wiley Eastern Ltd. New Delhi

Chapter-2: Sections 2.1-2.10 (Omit Applications 1 and 2 of 2.7)

Chapter-3: Sections 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7

**Reference Books**


1. S.Arumugam. (2004) *Modern Algebra.*Scitech Publications, Chennai.
2. J.B.Fraleigh (1987). *A First Course in Algebra* (3rd Edition) Addison Wesley, Mass. (Indian Print)
3. Lloyd R.Jaisingh and Frank Ayres,Jr. (2005) *Abstract Algebra*, (2nd Edition), Tata McGraw Hill Edition, New Delhi.
4. M.L.Santiago (2002) *Modern Algebra*, Tata McGraw Hill, New Delhi.
5. Surjeet Singh and QaziZameeruddin. (1982) *Modern Algebra*. Vikas Publishing House Pvt. Ltd. New Delhi.

## ABSTRACT ALGEBRA

Abstract Algebra is the study on algebraic structure. Algebraic structure is an ordered pair $(A, \star)$ of a non-empty set $A$ together with binary operation $\star$.

An $n-$Array operation is a mapping $f : A^n \to A$. If $n = 1$, the mapping $f : A \to A$ is said to be an Unary operation. If $n = 2$, the mapping $f : A \times A \to A$ is said to be an Binary operation, and so on.

The Binary operation is denoted by $\star$ and based on the Binary operation we have various Algebraic Structures like Group, Field, Rings, Vector Spaces, etc.,

Group is an algebraic structure with one Binary Operation.

Field, Rings, Vector Spaces are all algebraic structures with two Binary operations.

### UNIT I

### GROUPS

Definition of a Group - Examples - Subgroups

**Definition 1. Group:** A non empty set $G$ together with a binary operation $\star$ defined on the set $G$ is said to be a Group if it satisfies the following axioms

(i) Closed Property: For all $a, b \in G$ implies that $a \star b \in G$

(ii) Associative Property: For all $a, b, c \in G$ implies that $a \star (b \star c)$=$(a \star b) \star c$.

(iii) Existance of Identity: There exist an element $e \in G$ sucht that $a \star e$=$e \star a$=$a$ for all $a \in G$.

(iv) Existance of Inverse: For every $a \in G$ there exist an element $a^{-1} \in G$ such that $a \star a^{-1}$=$a^{-1} \star a$=$e$.

**Definition 2. Abelian Group:** A group is said to be an abelian group if it satisfies a commutative property.

- Commutative Property: For all $a, b \in G$ implies that $a \star b$=$b \star a$.

**Example 1.**

(i) $(\mathbb{R}, +)$ *is an infinite abelian group.*
(ii) $(\mathbb{R} - 0, \cdot)$ *is an infinite abelian group.*
(iii) $(\mathbb{C}, +)$ *is an infinite abelian group.*
(iv) $(\mathbb{C} - 0, \cdot)$ *is an infinite abelian group.*
(v) *Set of all* $2 \times 2$ *matrices with real numbers* $a, b, c, d$, *such that* $ad - bc \neq 0$ *is an infinite non-abelian group.*

**Example 2.** *The integers* $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ *form a group under the operation of addition.*

*Consider two integers* $m, n \in \mathbb{Z}$. *Sum of two integers is an integer hence it is closed. The identity is* $0$, *and the inverse of* $n \in \mathbb{Z}$ *is written as* $-n$ *and it is exist. Notice that the set of integers under addition have the additional property that* $m + n = n + m$ *and therefore form an abelian group.*

**Definition 3. Order of a Group:** The number of elements present in the group $G$ is said to be order of a group and it is denoted by $|G|$ or $o(G)$.

**Definition 4. Finite Group:** If $|G|$ or $o(G)$ is finite, the group $G$ is said to be finite group. Otherwise it is said to be infinite group.

**Example 3.**

(i) $G = \{-1, 1\}$ *is an finite abelian group*
(ii) $(\mathbb{Z}, +)$ *is an infinite abelian group*

**Definition 5. Quasi group** A algebraic structure is said to be an Quasi group if it satisfies only the closed Property.

**Definition 6. Semi group** A algebraic structure is said to be an Semi group if it satisfies the closed Property and Associative Property.

**Example 4.** $(\mathbb{N}, +)$ *is an Semi-group.*

**Definition 7. Monoid** A algebraic structure is said to be an Monoid if it satisfies the closed Property, Associative Property and Existance of Identity.

**Example 5.**

(i) $(\mathbb{Z}, \cdot)$ *is an Monoid but not an group.*
(i) $(\mathbb{N}, \cdot)$ *is an Monoid.*

**Definition 8. Cancellation Law's:** Let $G$ be a group, then the Left Cancellation Law is defined as

$$a \cdot u = a \cdot w \implies u = w$$

and the Right Cancellation Law is defined as

$$u \cdot a = w \cdot a \implies u = w$$

for all $a, u, w \in G$.

**Theorem 1.** *State and prove Left and Right Cancellation Law's*

*Proof.* Let $G$ be a group, then the Left Cancellation Law is defined as

$$a \cdot u = a \cdot w \implies u = w \tag{1}$$

Pre-multiply by $a^{-1}$ on both side of equation (1), we arrive

$$\begin{aligned} &a^{-1}(a \cdot u) = a^{-1}(a \cdot w) \\ &\implies (a^{-1}a) \cdot u = (a^{-1}a) \cdot w \\ &\implies e \cdot u = e \cdot w \\ &\implies u = w. \end{aligned}$$

The Right Cancellation Law is defined as

$$u \cdot a = w \cdot a \implies u = w \tag{2}$$

Post-multiply by $a^{-1}$ on both side of equation (2), we arrive

$$\begin{aligned} &(u \cdot a)a^{-1} = (w \cdot a)a^{-1} \\ &\implies u \cdot (aa^{-1}) = w \cdot (aa^{-1}) \\ &\implies u \cdot e = w \cdot e \\ &\implies u = w. \end{aligned}$$

□

**Problem 1.** *Let $G$ denote the set of all matrices of the form* $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$ *where* $x \in \mathbb{R}^\star$. *Then show that $G$ is a group under matrix multiplication.*

**Solution:** Let $A, B \in G$ where $A = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$ and $B = \begin{pmatrix} y & y \\ y & y \end{pmatrix}$. Then

$$AB = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in G.$$

We know that matrix multiplication is associative. Let $E = \begin{pmatrix} e & e \\ e & e \end{pmatrix} \in G$ such that $AE = A$. Therefore

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} e & e \\ e & e \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

$\implies$

$$\begin{pmatrix} 2xe & 2xe \\ 2xe & 2xe \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

$\implies$

$$2xe = x.$$

Hence $e = \frac{1}{2}$ and hence $E = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ is the identity element of $G$. Let $\begin{pmatrix} y & y \\ y & y \end{pmatrix}$ be the inverse of $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$. Then

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Therefore,

$$\begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Hence $2xy = \frac{1}{2}$ which implies $y = \frac{x}{4}$. Therefore, inverse of $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$ is $\begin{pmatrix} \frac{x}{4} & \frac{x}{4} \\ \frac{x}{4} & \frac{x}{4} \end{pmatrix}$. Hence $G$ is a Group.

**Problem 2.** *Show that the set* $G = \{1, -1, i, -i\}$ *is a group under multiplication.*

*Proof.* **Closure Property:**

$$1 \cdot -1 = -1 \in G, \qquad -1 \cdot i = -i \in G,$$
$$i \cdot -i = 1 \in G, \qquad -i \cdot 1 = -i \in G.$$

Hence $G$ is closed under multiplication.

**Associative Property:** Consider $1, -1, i \in G$

$$1 \cdot (-1 \cdot i) = (1 \cdot -1) \cdot i$$
$$1 \cdot -i = -1 \cdot i$$
$$-i = -i$$

Hence $\cdot$ is Associative.

**Existance of Identity:**

$$1 \cdot 1 = 1 \in G, \qquad -1 \cdot 1 = -1 \in G,$$
$$i \cdot 1 = i \in G, \qquad -i \cdot 1 = -i \in G$$

The identity element is 1 and it exists in $G$.
Hence $\cdot$ is Associative.
**Existance of Inverse:**

$$1 \cdot 1 = 1 \in G, \qquad -1 \cdot -1 = 1 \in G,$$
$$i \cdot -i = 1 \in G, \qquad -i \cdot i = 1 \in G.$$

Hence Inverse exists. Therefore, $G$ is a group under multiplication.
**Commutative Property:**

$$1 \cdot -1 = -1 \cdot 1 = -1, \qquad 1 \cdot -i = -i \cdot 1 = -i,$$
$$i \cdot -i = -i \cdot i = 1, \qquad -1 \cdot i = i \cdot -1 = -i.$$

Hence Inverse exists. Therefore, $G$ is an finite abelian group under multiplication.

□

It is often convenient to describe a group in terms of an addition or multiplication table. Such a table is called a Cayley table.

| · | 1 | -1 | i | -i |
|---|---|---|---|---|
| 1 | 1 | -1 | i | -i |
| -1 | -1 | 1 | -i | i |
| i | i | -i | -1 | 1 |
| -i | -i | i | 1 | -1 |

**Closed:** There is no new element is formed in the composition table. Therefore, Multiplication is closed

**Associative:** A composition table under multiplication of integers
are always associative. Therefore, multiplication is associative.

**Identity:** From the first row or column, the identity element is 1. Therefore, Identity exists.

**Inverse:** From the composition table $1, -1$ are self inverses and $i, -i$ are inverse to each other. Therefore, Inverse exists.

**Commutative:** The composition table is symmetric about leading diagonal. Therfore Multiplication is commutative.

Hence, $G$ is a abelian group under multiplication.

**Problem 3.** *Show that the cube root of unity is a group.*

| · | 1 | a | $a^2$ |
|---|---|---|---|
| 1 | 1 | a | $a^2$ |
| a | a | $a^2$ | 1 |
| $a^2$ | $a^2$ | 1 | a |

**Closed:** There is no new element is formed in the composition table. Therefore, Multiplication is closed

**Associative:** A composition table under multiplication of integers
are always associative. Therefore, multiplication is associative.

**Identity:** From the first row or column, the identity element is 1. Therefore, Identity exists.

**Inverse:** From the composition table 1 is the self inverse and $a, a^2$ are inverse to each other. Therefore, Inverse exists.

**Commutative:** The composition table is symmetric about leading diagonal. Therfore Multiplication is commutative.
Hence, $G$ is a abelian group under multiplication.

**Problem 4.** *Show that the set* $(\mathbb{C}, +)$ *is an abelian group.*

**Solution:** Let $\mathbb{C} = \{\dots, 1+i, -1+i, 2+i, -2-i, \dots\}$
**Closure Property:** $(2+i)+(3+i) = 5+2i \in \mathbb{C}$.
Hence $\mathbb{C}$ is closed under $+$.
**Associative Property:**
Consider $1+i, -1+2i, i \in G$

$$1+i+(-1+2i+i) = (1+i+-1+2i)+i$$
$$1+i-1+3i = 3i+i$$
$$4i = 4i$$

Hence $+$ is Associative.
**Existance of Identity:** $e = 0+0i$

The identity element is $e = 0+0i$ and it exists in $\mathbb{C}$.
Hence identity exists.
**Existance of Inverse:**

$$1+i+(-1-i) = 0+0i$$
$$1+3i+(-1-3i) = 0+0i$$

Hence Inverse exists. Therefore, $\mathbb{C}$ is a group under multiplication.
**Commutative Property:**

$$(1+i)+(3+4i) = (3+4i)+(1+i) = 5+5i$$

Hence Inverse exists. Therefore, $\mathbb{C}$ is an infinite abelian group under addition.

**Problem 5.** *Show that identity element of a Group is unique.*

*Proof.* Let $e_1$ and $e_2$ be any two identity elements of $G$. If $e_1$ be the identity element, then

$$e_1 \star e_2 = e_2 \star e_1 = e_2. \quad (3)$$

If $e_2$ be the identity element, then

$$e_1 \star e_2 = e_2 \star e_1 = e_1. \quad (4)$$

Now, from (3) and (4), we arrive $e_1 = e_2$. Hence, identity element of a Group is unique. □

**Problem 6.** *Show that in a group $G$, for every $a \in G$, inverse of $G$ is unique.*

*Proof.* Let $e$ be the identity of $G$. Let $a_1$ and $a_2$ be any two inverses of $a \in G$. If $a_1$ be the inverse $a$, then

$$a_1 \star a = a \star a_1 = e. \tag{5}$$

If $a_2$ be the inverse $a$, then

$$a_2 \star a = a \star a_2 = e. \tag{6}$$

Now, from (5) and (6), we arrive $a_1 = a_2$. Hence, inverse of $G$ is unique. □

**Problem 7.** *Let $G$ be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.*

*Proof.* Let

$$a, b \in G.$$

Then

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

Similarly,

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

Hence, $(ab)^{-1} = b^{-1}a^{-1}$. □

**Problem 8.** *Let $G$ be a group. For any $a \in G$, $(a^{-1})^{-1} = a$.*

*Proof.* Now

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

Multiplying both sides of this equation by $a$, we have

$$\begin{aligned} (a^{-1})^{-1} &= e(a^{-1})^{-1} \\ &= aa^{-1}(a^{-1})^{-1} \\ &= ae \\ &= a. \end{aligned}$$

□

**Problem 9.** *Let $G$ be a group and $a$ and $b$ be any two elements in $G$. Then the equations $ax = b$ and $xa = b$ have unique solutions in $G$.*

*Proof.* Let $ax = b$. Pre-multiply by $a^{-1}$, we get

$$a^{-1}ax = a^{-1}b$$
$$ex = a^{-1}b$$
$$x = a^{-1}b.$$

Hence, the solution of $ax = b$ is exist. To prove uniqueness, let $x_1$ and $x_2$ are both solutions of $ax = b$, then

$$ax_1 = b = ax_2.$$

So

$$\begin{aligned} x_1 &= a^{-1}ax_1 \\ &= a^{-1}ax_2 \\ &= x_2. \end{aligned}$$

Hence, $ax = b$ has unique solution.

Let $xa = b$ and post-multiply by $a^{-1}$, we get

$$xaa^{-1} = ba^{-1}$$
$$xe = ba^{-1}$$
$$x = ba^{-1}.$$

Hence, solution of $xa = b$ is exist. To prove uniqueness, let $y_1$ and $y_2$ are both solutions of $xa = b$, then

$$y_1a = b = y_2a.$$

So

$$\begin{aligned} y_1 &= a^{-1}y_1a \\ &= a^{-1}y_2a \\ &= y_2. \end{aligned}$$

Hence, $xa = b$ has unique solution. □

**Assignment: Group**

**Assignment: Part A**

(1) Define Group
(2) Give an example for group
(3) Define abelian group
(4) Show that identity element of a group is unique
(5) Show that in a group $G$, for every $a \in G$, inverse of $a$ is unique.
(6) In a group $G$, show that $(ab)^{-1} = b^{-1}a^{-1}$ for $a, b \in G$.

**Assignment: Part B**

(1) Show that $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$ where $x \in \mathbb{R}^{\star}$ then $G$ is a group under matrix multiplication.
(2) Prove that $(a \cdot b)^n = a^n b^n$ if $G$ is an abelian group for all $a, b \in G$ and all integers $n$.
(3) If $G$ is a group in which $(ab)^i = a^i b^i$ for three consecutive integers $i$ for all $a, b \in G$, show that $G$ is abelian.
(4) If $G$ is a group prove that
    (i) The identity element of $G$ is unique.
    (ii) For all $a, b \in G, (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

**Assignment: Part C**

(1) Show that set of all $2 \times 2$ matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with real numbers $a, b, c, d$, such that $ad - bc \neq 0$ is a non-abelian group under multiplication matrices.
(2) Verify that the set of all Natural numbers is Group with respect to addition and multiplication.
(3) Show that the cube root of unity is a group.
(4) Show that $(\mathbb{R} - \{0\}, \cdot)$ is an abelian group.

**Definition 9. Subgroup:** If a subset $H$ of a group $G$ is itself a group under the operation of $G$, then we say that $H$ is a subgroup of $G$.

**Example 6.** *(i)* $(2\mathbb{Z},+)$ *is a subgroup of* $(\mathbb{Z},+)$. *(ii) For any* $n \in \mathbb{Z}^+$*, we have* $(\mathbb{Z}_n,+) < (\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$.

**Notation:**

(i) We write $H \leq G$ to mean $H$ is a subgroup of $G$.
(ii) If $H$ is not equal to $G$, we write $H < G$. Then, we say $H$ is a proper subgroup of $G$.
(iii) $\{e\}$ and $G$ are called the trivial subgroups. All other subgroups are nontrivial.

**Problem 10.** *Let $H$ be a subgroup of $G$. Then*

(i) *the identity element of $H$ is the same as that of $G$.*
(ii) *for each $a \in H$ the inverse of $a$ in $H$ is the same as the inverse of $a \in G$.*

*Proof.*

(i) Let $e$ and $e'$ be the identities of $G$ and $H$ respectively. Let $a \in H$ and $e'$ is the identity of $H$, we have

$$e'a = a.$$

Since $e$ is the identity of $G$ and $a \in G$, we have

$$a = ea.$$

Therefore $e'a = ea$. By right cancellation law, we have

$$e' = e.$$

(ii) Let $a'$ and $a''$ be the inverse of $a$ in $G$ and $H$ respectively. Since by (i), $G$ and $H$ have the same identity element $e$, we have

$$a'a = e = a''a.$$

Hence by cancellation law

$$a' = a''.$$

□

**Problem 11.** *A subset $H$ of a group $G$ is a subgroup of $G$ iff*

(i) *it is closed under the binary operation in $G$.*
(ii) *The identity $e$ of $G$ is in $H$.*
(ii) $a \in H \implies a^{-}1 \in H$.

*Proof.* Let $H$ be a subgroup of $G$. The result follows immediately from the Problem-10.

Conversely let $H$ be a subset of $G$ satisfying cinditions (i),(ii)and (iii). Then, obviously $H$ itselt is a group with respect to the binary operarion in $G$. Therefore $H$ is a subgroup of $G$. □

**Problem 12.** *A non-empty subset $H$ of a group $G$ is a subgroup of $G$ iff $a, b \in H \implies ab^{-1} \in H$.*

*Proof.* $\implies$ Let $H$ be a subgroup of $G$. Then

$$\begin{aligned} &a, b \in H \\ &\implies a, b^{-1} \in H \\ &\implies ab^{-1} \in H. \end{aligned}$$

Therefore,

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

Conversely, let $H$ be a non-empty subset of $G$ such that

$$a, b \in H \implies a, b^{-1} \in H.$$

To prove: $H$ is subgroup of $G$. Since $H \neq \Phi$, there exists an element $a \in H$. Hence

$$aa^{-1} \in H.$$

Thus $e \in H$. Also, since $e, a \in H$, $ea^{-1} \in H$. Hence $a^{-1} \in H$.

Now let $a, b \in H$. Then $a, b^{-1} \in H$. Hence

$$a(b^{-1})^{-1} = ab \in H.$$

Thus $H$ is closed under the binary operation in $G$. Thus by above theorem $H$ is a subgroup of $G$. □

**Problem 13.** *If $H$ and $K$ are subgroups of a group $G$ then $H \cap K$ is also a subgoup of $G$.*

*Proof.* Clearly $e \in H \cap K$ and hence $H \cap K$ is non-empty. Now let $a, b \in H \cap K$. Then

$$a, b \in H$$

and

$$a, b \in K.$$

Since $H$ and $K$ are subgroups of $G$,

$$ab^{-1} \in H$$

and

$$ab^{-1} \in K$$

.

Therefore,

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

Hence by the above theorem $H \cap K$ is a subgroup of $G$. □

**Definition 10.** Let $G$ be a group, $H$ a subgroup of $G$; for $a, b \in G$ we say $a$ is congruent to $b \mod H$, written as

$$a \equiv b \mod H$$

if

$$ab^{-1} \in H$$

.

**Definition 11. Left coset:** Let $H$ be a subgroup of a group $G$. Let $a \in G$. Then the set

$$aH = \{ah | h \in H\}$$

is called the Left coset of $H$ defined by $a$ in $G$.

**Definition 12. Right coset:** Let $H$ be a subgroup of a group $G$. Let $a \in G$. Then the set

$$Ha = \{ha | h \in H\}$$

is called the Left coset of $H$ defined by $a$ in $G$.

**Definition 13. Order(or)Period:** If $G$ is a group and $a \in G$, the Order(or)Period of $a$ is the least positive integer $m$ such that

$$a^m = e$$

.

**Definition 14.** If $H$ is a subgroup of $G$ and $a \in G$, then $Ha$ consists of all elements in $G$ of the form $ha \in H$. If $H$, $K$ are two subgroups of $G$, then

$$HK = \{x \in G | x = hk, h \in H, k \in K\}$$

.

**Definition 15. Index:** Let $H$ be a subgroup of $G$. The number of distinct left(right) cosets of $H$ in $G$ is called the index of $H$ in $G$ and is denoted by $[G : H]$.

**Example 7.** $(Z_8, \bigoplus)$. *$H = \{0, 4\}$ is a subgroup. The left cosets of $H$ are given by*

(i) $0 + H = \{0, 4\} = H$

(ii) $1 + H = \{1, 5\}$

(iii) $2 + H = \{2, 6\}$

(iv) $3 + H = \{3, 7\}$.

*These are the four distinct left cosets of $H$. Hence the index of the subgroup $H$ is 4.*

**Theorem 2.** *Let $G$ be a group and $H$ ba a subgroup of $G$. Then*

(i) $a \in H \implies aH = H$.
(ii) $aH = bH \implies a^{-1}b \in H$.
(iii) $a \in bH \implies a^{-1} \in Hb^{-1}$.
(iv) $a \in bH \implies aH = bH$.

*Proof.* (i) Let $a \in H$. We claim that

$$aH = H.$$

Let $x \in aH$. Then

$$x = ah$$

for some $h \in H$. Now, $a \in H$ and $h \in H \implies ah = x \in H$(Since $H$ is a subgroup). Hence,

$$aH \subset H.$$

Let $x \in H$. Then

$$x = a(a^{-1}x) \in aH.$$

Hence,

$$H \subset aH.$$

Thus,

$$H = aH.$$

Conversly, let $aH = H$. Now $a = ae \in aH$. Therfore

$$a \in H.$$

(ii) Let $aH = bH$. Therefore,

$$a^{-1}(aH) = a^{-1}(bH).$$

Therefore,

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

. Therefore, (by i)

$$a^{-1}b \in H.$$

Conversely, let $a^{-1}b \in H$. Then, (by i)

$$a^{-1}bH = H.$$

Therefore,

$$aa^{-1}bH = aH$$

and hence

$$bH = aH$$

.

(iii) Let $a \in bH$. Then

$$a = bh$$

for some $h \in H$. Therefore

$$a^{-1} = (bh)^{-1} = h^{-1}b^{-1} \in Hb^{-1}.$$

(iv) Let $a \in bH$. We claim that $aH = bH$. Let $x \in aH$. Then

$$x = ah_1$$

for some $h_1 \in H$. Also $a \in bH \implies a = bh_2$ for some $h_2 \in H$—(1). Therefore,

$$x = (bh_2)h_1 = b(h_2h_1) \in bH.$$

Therefore,

$$aH \in bH$$

. Now, let $x = bh_3$ for some $h_3 \in H$. Also from (1), $b = ah_2^{-1}$. Therefore,

$$x = ah_2^{-1}h_3 \in aH.$$

Therefore,

$$bH \subset aH.$$

Hence,

$$aH = bH.$$

Then,

$$a = ae \in aH.$$

Therefore,

$$a \in bH.$$

□

**Theorem 3.** *Let $H$ ba a subgroup of $G$. Then*

(i) *any two left cosets of $H$ are either identical or disjoint.*
(ii) *union of all the left cosets of $H$ is $G$*
(iii) *the number of slements in any left coset $aH$ is the same as the number of elements in $H$.*

*Proof.* (i) Let $aH$ and $bH$ be two left cosets. Suppopse $aH$ and $bH$ are not disjoint. We claim that

$$aH = bH.$$

Since $aH$ and $bH$ are not disjoint. that is $aH \cap bH \neq \Phi$. Therefore there exists an element

$$c \in aH \cap bH.$$

Therefore

$$c \in aH \text{ and } c \in bH.$$

Therefore,

$$aH = cH \text{ and } bH = cH.$$

Therefore,

$$aH = bH.$$

(ii) Let $a \in G$. Then

$$a = ae \in aH.$$

Therefore, Every element of $G$ belongs to a left coset of $H$. Therefore, the union of all the left cosets of $H$ is $G$.

(iii) The map $f : H \to aH$ defined by

$$f(h) = ah$$

is clearly a bijection. Hence every left coset has the same number of elements as $H$. □

**Theorem 4.** *Let $H$ be a subgroup of $G$. The number of left cosets of $H$ is the same as the number of right cosets of $H$.*

*Proof.* Let $L$ and $R$ respectively denotethe set of left and right cosets of $H$. We define a map $f : L \to R$ by

$$f(aH) = Ha^{-1}.$$

$f$ **is well defined:** Let

$$\begin{aligned} aH &= bH \\ &\implies a^{-1}b \in H \\ &\implies a^{-1} \in Hb^{-1} \\ &\implies Ha^{-1} = Hb^{-1} \\ &\implies f(aH) = f(bH). \end{aligned}$$

$f$ **is** $1-1$**:** Let

$$\begin{aligned} f(aH) = f(bH) \\ &\implies Ha^{-1} = Hb^{-1} \\ &\implies a^{-1} \in Hb^{-1} \\ &\implies a^{-1} = bh^{-1} \\ &\implies a \in bH \\ &\implies aH = bH. \end{aligned}$$

$f$ **is onto:** For, every right coset $Ha$ has a pre-image under $f$ namely $a^{-1}H$.
Hence $f$ is a bijection from $L$ to $R$. Hence the number of left cosets is the same as the number of right cosets. □

**Theorem 5. Lagrange's theorem:** *Let $G$ be a finite group of order $n$ and $H$ be any subgroup of $G$. Then the order of $H$ divides the order of $G$.*

*Proof.* Let $|H| = m$ and $[G : H] = r$. Then the number of distinct left cosets of $H$ in $G$ is $r$. By the Theorem-3, these $r$ left cosets are mutually disjoint, they have the same number of elements namely $m$ and their union is $G$. Therefore, $n = rm$. Hence $m$ divides $n$. □

**Theorem 6.** *The order of any element of a finite group $G$ divides the order of $G$.*

*Proof.* Let $G$ be a group of order $n$. Let $a \in G$ be an element of order $m$. Then the order of $a$ is the same as the order of the cyclic group $< a >$. Now by lagrange's theorem the order the subgroup $< a >$ divides the order of $G$. □

**Theorem 7.** *let $G$ be a group of order $n$. Let $a \in G$, then $a^n = e$.*

*Proof.* Let the order of $a$ be $m$. Then $m$ divides $n$. Hence

$$n = mq.$$

Therefore

$$a^n = a^{mq} = (a^m)^q = e^q = e.$$

□

**Theorem 8.** *In a group $G$, show that $G$ is abelian group iff $(a \cdot b)^2 = a^2 \cdot b^2$, for all $a, b \in G$.*

*Proof.* Given that $G$ is abelian group

$$\implies a \cdot b = b \cdot a \text{ for all } a, b \in G.$$

Now,

$$\begin{aligned}(a \cdot b)^2 &= (a \cdot b)(a \cdot b)\\ &= a(ba)b\\ &= a(ab)b\\ &= (aa)(bb)\\ &= a^2b^2.\end{aligned}$$

Therefore, $(a \cdot b)^2 = a^2 \cdot b^2$, for all $a, b \in G$.

Conversely, let $G$ be a group satisfying

$$(a \cdot b)^2 = a^2 \cdot b^2$$

for all $a, b \in G$.

$$\implies (ab)(ab) = (aa)(bb)$$
$$\implies a(ba)b = a(ab)b.$$

Now, pre-multiply by $a^{-1}$ and post-multiply by $b^{-1}$, we get

$$ba = ab$$

for all $a, b \in G$. Therefore, $G$ is an abelian group. □

**Theorem 9.** *In a group $G$, let $(ab)^i = a^i b^i$ for three consecutive integers, for all $a, b \in G$. Prove that $G$ is an abelian group.*

*Proof.* Let

$$(ab)^m = a^m b^m \tag{7}$$
$$(ab)^{m+1} = a^{m+1} b^{m+1} \tag{8}$$
$$(ab)^{m+2} = a^{m+2} b^{m+2} \tag{9}$$

for some integers m, and for all $a, b \in G$.
**Claim**: $G$ is abelian.

$\implies$ ab=ba, for all $a, b \in G$. Using (7) and (8), we get

$$(ab)^{m+1} = a^{m+1} b^{m+1}$$
$$\implies (ab)(ab)^m = aa^m bb^m$$
$$\implies (ab)a^m b^m = aa^m bb^m$$
$$\implies a(ba^m)b^m = a(a^m b)b^m.$$

By left and right cancellation laws,

$$b(a^m) = a^m b$$

for all $a, b \in G$.

Similarly, we get $ba^{m+1} = a^{m+1}b$, for all $a, b \in G$. Therefore,

$$b(a^m a) = (a^m a)b$$
$$\implies (ba^m)a = a^m(ab)$$
$$\implies (a^m b)a = a^m(ab)$$
$$\implies a^m(ba) = a^m(ab).$$

By left cancellation law,

$$ba = ab,$$

for all $a, b \in G$. Therefore, $G$ is an abelian group. □

**Theorem 10.** *Let $G$ be group. Let $a, b \in G$. Then*

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

*and*

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

*Proof.*

$$\begin{aligned} &(ab)(b^{-1}a^{-1}) \\ &= a(bb^{-1})a^{-1} \\ &= aea^{-1} \\ &= aa^{-1} = e. \end{aligned}$$

Similarly

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

Hence,

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

(ii) $aa^{-1} = e$ and $a^{-1}a = e \implies (a^{-1})^{-1} = a.$

□

**Theorem 11.** *Let $G$ be a group of order $n$. Let $a \in G$ then $a^n = e$.*

*Proof.* Let the order of $a$ be $m$. Then $m$ divides $n$. Hence,

$$n = mq.$$

Therefore,

$$a^n = a^{mq} = (a^m)^q = e^q = e.$$

□

**Theorem 12. Euler's Theorem:** *If $n$ is any integer and $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 (mod n)$.*

*($\phi(n)$ is the number of positive integers less than $n$ relatively prime to $n$).*

*Proof.* Let
$$G = \{m/m < n \; \& \; (m,n) = 1\}.$$
$G$ is a group under multiplication modulo $n$. This group is of order $\phi(n)$.

Now, Let $(a,n) = 1$. Let $a = qn + r;\; 0 \le r < n$ so that $a \equiv r(\mod n)$.

Since $(a,n) = 1$ we have $(n,r) = 1$ so that $r \in G$.. Therefore
$$r^{\phi(n)} = 1.$$
Therefore,
$$r^{\phi(n)} \equiv 1(\mod n).$$
Also,
$$a^{\phi(n)} \equiv r^{\phi(n)}(\mod n).$$
Since $\equiv$ is transitive, we get
$$a^{\phi(n)} \equiv 1(\mod n).$$
□

**Theorem 13. Fermat's Theorem** *Let $p$ be a prime number and $a$ be any integer relatively prime to $p$. Then, $a^{p-1} \equiv 1(modp)$.*

*Proof.* Since $p$ is prime, $\phi(p) = p - 1$. Now, by Euler's Theorem

$$a^{\phi(p)} \equiv 1(\mod p).$$
$$\implies a^{p-1} \equiv 1(\mod p).$$
□

**Problem 14.** *Let $A$ and $B$ be subgroups of a finite group $G$ such that $A$ is a subgroup of $B$. Show that*
$$[G : A] = [G : B][B : A].$$

**Solution:**
$$[G : A] = \frac{|G|}{|A|}$$
$$[G : B] = \frac{|G|}{|B|}$$
and
$$[B : A] = \frac{|B|}{|A|}.$$

Therefore,

$$[G:B][B:A] = \frac{|G|}{|B|}\frac{|B|}{|A|} = \frac{|G|}{|A|} = [G:A].$$

Hence,

$$[G:A] = [G:B][B:A].$$

**Problem 15.** *Let $H$ and $K$ be two finite subgroups of a group $G$. Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

*(or)*

$$O(HK) = \frac{O(H)O(K)}{O(H \cap K)}.$$

*Proof.* Let $L = H \cap K$. Since $H$ and $K$ are subgroups of $G$, $L$ is also a subgroup of $G$ and $L \subseteq H \text{ and } K$.

Now, let $Lx_1, Lx_2, \ldots, Lx_m$ be the distinct right cosets of $L$ in $K$ so that

$$K = Lx_1 \cup Lx_2 \cup, \ldots, \cup Lx_m. \tag{10}$$

and

$$m = [K:L] = \frac{|K|}{|L|} = \frac{|K|}{|H \cap K|}. \tag{11}$$

Now, from equation (10), we get

$$\begin{aligned} HK &= HLx_1 \cup Hx_2 \cup \ldots Hx_m \\ &= Hx_1 \cup Hx_2 \cup \ldots Hx_m (Since L \subseteq H.) \end{aligned} \tag{12}$$

**Claim:** The cosets $Hx_1, Hx_2, \ldots, Hx_m$ are distinct.

Suppose

$$Hx_i = Hx_j.$$

$$\implies x_i x_j^{-1} \in H.$$

Also $x_i, x_j \in K$ and hence

$$x_i x_j^{-1} \in H \cap K = L.$$

Hence

$$Lx_i = Lx_j$$

which is a contradiction since the cosets $Lx_1, Lx_2, \dots, Lx_m$ are distinct. Thus, from equation (12) and using (11), we have

$$\begin{aligned}|HK| &= |Hx_1| + |Hx_2| + \cdots + |Hx_m| \\ &= m|H| \\ &= \frac{|H||K|}{|H \cap K|}.\end{aligned}$$

Hence,

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

□

**Theorem 14.** *Let $H$ and $K$ be two subgroups of a group $G$. Then $HK$ is a subgroup of $G$ iff $HK = KH$.*

*Proof.* Let $HK$ is a subgroup of $G$.
Claim: $HK = KH$.

Let $x \in HK$
$\implies x^{-1} \in HK$, Since $HK$ is a subgroup.

Let $x^{-1} = hk$, where $h \in H, k \in K$. Therefore,

$$x = (hk)^{-1} = k^{-1}h^{-1} \in KH,$$

since $H$ and $K$ are subgroups. Therefore,

$$HK \subseteq KH. \tag{13}$$

Now, let $x \in KH \implies x = kh$ for $k \in K, h \in H$.
$\implies x^{-1} = (kh)^{-1} = h^{-1}k^{-1} \in HK$,

Now, since $HK$ is a subgroup and $x^{-1} \in HK$, we have $x \in HK$. Therefore,

$$KH \subseteq HK. \tag{14}$$

From (13) and (14), we get

$$HK = KH$$

Conversely, let $HK = KH$.

Claim: $HK$ is subgroup of $G$.

Clearly $e \in HK$ and hence $HK$ is non-empty.

Let $x, y \in HK$. Then $x = h_1k_1$ and $y = h_2k_2$, where $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

Now, $xy^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$.

Where $k_2^{-1}h_2^{-1} \in KH$, since $KH = HK$ we get $k_2^{-1}h_2^{-1} \in HK$. Therefore,

$$k_2^{-1}h_2^{-1} = h_3k_3,$$

for $h_3 \in H, k_3 \in K$. Hence,

$$xy^{-1} = h_1k_1h_3k_3.$$

Now $k_1h_3 \in KH$, since $KH = HK$ we have $k_1h_3 \in HK$.

$$\implies k_1h_3 = h_4k_4,$$

for $h_4 \in H, k_4 \in K$. Therefore,

$$xy^{-1} = h_1(h_4k_4)k_3 = (h_1h_4)(k_4k_3) \in HK.$$

Hence, $HK$ is subgroup of $G$.

□

**Assignment: Part A**

(1) Give an example of a subgroup of the group of set of all integers with operation addition
(2) Define subgroup of a group
(3) For a subgroup $H$ of a group $G$, when do you say that $a \equiv b (\mod H)$ for $a, b \in G$.
(4) State the Fermat's theorem

**Assignment: Part B**

(1) If $H$ and $K$ are subgroups of a group $G$ prove that $H \cap K$ is also a subgroup of $G$.
(2) Show that a non-empty subset $H$ of a group $G$ is a subgroup of $G$ if and only if $ab^{-1} \in H$ for all $a, b \in H$.
(3) If $H$ is a non-empty finite subset of a group $G$ and if the closure property is satisfied in $H$, show that $H$ is a subgroup.
(4) Prove that a non empty subset $H$ of a group is a subgroup of $G$ if and only if
    (i) $a, b \in H$ implies that $ab \in H$
    (ii) $a \in H$ implies that $a^{-1} \in H$
(5) Show that if $H$ is a subgroup of a group $G$ the relation $a \equiv b \mod H$ is an equivalence relation.

**Assignment: Part C**

(1) State and prove Lagranges theorem
(2) If $G$ is a finite group and $a \in G$ prove that $O(a)/O(G)$
(3) Prove that $HK$ is a subgroup of G if and only if $HK = KH$.