“Group and Subgroup”

Dissertation submitted to the Department of Mathematics in partial fulfillment of the requirements for the award of the degree of Master of Science in Mathematics

Mahapurusha Srimanta Sankaradeva Viswavidyalaya

Department of Mathematics

Submitted By:

Partha Jyoti Bora

Roll No: MAT-10/23

Registration No: MSSV-0023-101-001357

M.sc 4^{th} Semester

Session : 2023-2025

Department of Mathematics
MSSV, Nagaon

Under The Guidance:

Dr. Raju Bordoloi, HOD

Department of Mathematics, MSSV, Nagaon

Certificate

This is to certify that the dissertation entitled **"Group and Subgroup"**, submitted by **Partha Jyoti Bora**, Roll No. **MAT-10/23**, Registration No. **MSSV-0023-101-001357**, in partial fulfillment for the award of the degree of **Master of Science in Mathematics**, is a bonafide record of original work carried out under my supervision and guidance.

To the best of my knowledge, the work has not been submitted earlier to any other institution for the award of any degree or diploma.

Dr. Raju Bordoloi
Head of Department
Department of Mathematics
Mahapurusha Srimanta Sankaradeva Viswavidyalaya,Nagaon

Date: Signature of Guide
Place:

Declaration

I, **Partha Jyoti Bora**, hereby declare that the dissertation titled **"Group and Subgroup"**, submitted to the Department of Mathematics, **Mahapurusha Srimanta Sankaradeva Viswavidyalaya**, is a record of original work carried out by me under the supervision of **Dr. Raju Bordoloi**, HOD,Department of Mathematics.

This work has not been submitted earlier to any other institution or university for the award of any degree or diploma.

Place: Partha Jyoti Bora

Date: Roll No.: MAT-10/23

Acknowledgement

First and foremost, I would like to express my sincere gratitude to my guide, **Dr. Raju Bordoloi**, HOD, Department of Mathematics, Mahapurusha Srimanta Sankaradeva Viswavidyalaya, for his valuable guidance, continuous support, and encouragement throughout the course of this dissertation.

I also extend my heartfelt thanks to the faculty members of the Department of Mathematics for their constant academic support and the friendly learning environment they provided.

I am deeply grateful to my family and friends for their unwavering moral support and motivation throughout my academic journey. Their encouragement gave me the strength to successfully complete this work.

Lastly, I thank all those who directly or indirectly helped me during this project.

Place: Partha Jyoti Bora

Date: Roll No.: MAT-10/23

Table of Contents

Chapter 1

Introduction and examples

1.1 Introduction

This section provide some idea of the "nature of abstract algebra". I shall provide a brief outline only.Following are some of the salient points :

1. The section forms an introduction to "binary operations",which are define in the next section.
2. To achieve this, it treats multiplication of complex numbers.
3. It present Euler's Formula :

$$e^{i\theta} = \cos\theta + i\sin\theta$$

4. For any complex number $z \in \mathbb{C}$ we have :

$$z = |z|e^{i\theta}$$

5. It expounds the algebra of the Unit circle :
   (a) The Unit circle:

$$U = \{z \in \mathbb{C} : |z| = 1\} = \{z \in \mathbb{C} : z = e^{i\theta} \text{ where } \theta \in \mathbb{R}\}$$

(b) Observe, for $z, w \in U$, the product $zw \in U$. We say that the unit circle U is closed under multiplication.

(c) Let the map $f : [0, 2\pi) \to U$ be defined by $f(\theta) = e^{i\theta}$. Then, f is a bijection.

(d) Indeed, $f(x + y)$ sends sum to the product. In this case, addition $x + y$ in $[0, 2\pi)$ is defined "modulo 2π".

6. Algebra of Roots of Unity : We consider the algebra of roots of unity. Choose a positive integer n.

(a) Let U_n denote the set of all roots of the equation $z^n = 1$ in $\mathbb{C}$.

(b) Let $\zeta = e^{\frac{2\pi i}{n}}$. Then,

$$U_n = \{\zeta^0, \zeta^1, \zeta^2, \ldots, \zeta^{n-1}\}.$$

(c) Let the map $\varphi : \mathbb{Z}_n \to U_n$ be defined by

$$\varphi(r) = \zeta^r = e^{\frac{2\pi i r}{n}}.$$

is a bijection.It requires a proof that φ is well-defined.

(a) Actually, $\varphi(x + y) = \varphi(x)\varphi(y)$ maps sum to the product.

7. Also, $U_n \subseteq U$, the unit circle.

1.2 Binary Operation

Addition and multiplication are examples of *binary operations* in all the situations where we operated on them:

$$\mathbb{Z},\ \mathbb{Z}_n,\ \mathbb{R},\ \mathbb{C},\ M_n(\mathbb{R}),\ M_n(\mathbb{C})$$

where $M_n(\mathbb{R})$, $M_n(\mathbb{C})$ are the set of $n \times n$ matrices with coefficients in $\mathbb{R}$ or $\mathbb{C}$. Multiplication on U, U_n is also a binary operation. They are referred to as binary operations since to each ordered pair (x, y) they assign another element $x + y$ or xy.

We provide a rigorous definition of binary operations.

Definition 1.2.1. Let S be any set. A binary operation $*$ on S is a function

$$* : S \times S \to S.$$

Temporarily, we employ the notation $x * y := *(x, y)$.

Definition 1.2.2. Let $*$ be a binary operation on S and H be a subset of S. We say H is *closed under* $*$, if for any $x, y \in H$ we also have $x * y \in H$. Notationally,

$$\text{if } x, y \in H \implies x * y \in H.$$

Example 1.2.3. (§I.2, 2.7). Let $\mathcal{F}$ be the set of all continuous real-valued functions on $\mathbb{R}$. We give four binary operations:

(a) Sum: $(f + g)(x) = f(x) + g(x)$

(b) Product: $(fg)(x) = f(x)g(x)$

(c) Composition: $(f \circ g)(x) = f(g(x))$

(d) Subtraction: $(f - g)(x) = f(x) - g(x)$

Note division f/g is not defined in general (except when $g(x) \neq 0$ for all x). Therefore, division isn't a binary operation on $\mathcal{F}$.

1.3 Properties of Binary Operations

Definition 1.3.1. A binary operation $*$ on S is *commutative* if

$$x * y = y * x \quad \forall x, y \in S.$$

Remark and Examples: To my knowledge, matrix multiplication and composition are the only "natural" binary operations that are not commutative. Most counterexamples are artificially constructed.

1. On $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{R}$, and $\mathbb{C}$, both addition and multiplication are commutative.

2. On $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$, addition is commutative, but multiplication is **not** commutative. For example:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

   More generally:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ x & y \end{bmatrix} \neq \begin{bmatrix} a & b \\ x & y \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

   The left-hand side (LHS) is:

$$\begin{bmatrix} x & y \\ a & b \end{bmatrix}$$

   The right-hand side (RHS) is:

$$\begin{bmatrix} b & a \\ y & x \end{bmatrix}$$

3. Let F be the set of all continuous functions on $\mathbb{R}$. Then:

   (a) Addition $(+)$ is commutative.

   (b) Subtraction is **not** commutative.

   (c) Composition is **not** commutative. For example, let:

$$f(x) = e^x, \quad g(x) = x^2$$

   Then:

$$(f \circ g)(x) = e^{x^2}, \quad (g \circ f)(x) = (e^x)^2 = e^{2x}$$

Thus:

$$f \circ g \neq g \circ f$$

Definition 1.3.2. A binary operation $*$ on S is said to be *associative* if:

$$a * (b * c) = (a * b) * c \quad \forall a, b, c \in S.$$

Remarks and Examples.

1. To begin with, only when an operation is **associative**, we are not required to use parentheses to indicate the order of multiplication. We can represent $a * b * c$ for both $a * (b * c)$ and $(a * b) * c$.

2. I know (well, I do) no natural instance of binary operations which is not associative.

Example 1.3.3: Addition $(+)$ is a binary operation on the set of natural numbers $\mathbb{N}$, the set of integers $\mathbb{Z}$, and the set of real numbers $\mathbb{R}$.

Example 1.3.4: Multiplication $(\times)$ is a binary operation on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

Example 1.3.5: Union, intersection, and difference are binary operations on $\mathcal{P}(A)$, the power set of A.

Theorem 1.3.6.

The identity element of a binary operation $*$ on a set A, if it exists, is unique.

Proof: Let e' and e'' be two identity elements of A relative to the binary operation $*$.

Since e' is an identity element, for all $a \in A$:

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

In particular, taking $a = e''$, we get:

$$e' * e'' = e''$$

Similarly, since e'' is also an identity element, for all $a \in A$:

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

In particular, taking $a = e'$, we get:

$$e'' * e' = e'$$

Thus, we have:

$$e' * e'' = e'' \quad \text{and} \quad e'' * e' = e'$$

Therefore:

$$e' = e''$$

Hence, the identity element is unique.

Theorem 1.3.7. Suppose that $*$ is a binary operation on a set A that is associative. Then, each invertible element in A has a unique inverse.

Proof: Let $a \in A$ be an invertible element with respect to the binary operation $*$. Suppose, to the contrary, that b and c are two different inverses of a in A.

Let e be the identity element in A with respect to $*$. Then, by definition:

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

Since $*$ is associative on A, we have:

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

Substituting the known identities:

$$e * c = b * e$$

But, since e is the identity element:

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

Thus:

$$c = b$$

Therefore, the inverse of a is unique.

1.4 Cancellation Law

Definition 1.4.1.
A binary operation $*$ on a set A is said to satisfy:

1. **Left Cancellation Law:** For all $a, b, c \in A$,

$$a * b = a * c \implies b = c$$

2. **Right Cancellation Law:** For all $a, b, c \in A$,

$$b * a = c * a \implies b = c$$

Theorem 1.4.2.

Let $*$ be an associative binary operation on a set A such that each element of A is invertible. Then $*$ satisfies both the left and right cancellation laws, i.e.,

$a * b = a * c \implies b = c$ and $b * a = c * a \implies b = c, \quad \forall\ a, b, c \in A.$

Proof: Let e be the identity element of A with respect to $*$. Since all elements of A are invertible, each $a \in A$ has an inverse, denoted by $a' \in A$.

Assume:

$$a * b = a * c$$

Multiplying both sides on the left by a':

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

Since $*$ is associative:

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

But a' is the inverse of a, so $a' * a = e$, the identity element:

$$e * b = e * c$$

Using the identity property:

$$b = c$$

Thus, the left cancellation law holds.

Similarly, for the right cancellation law, assume:

$$b * a = c * a$$

Multiplying both sides on the right by a':

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

Using associativity:

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

Since a' is the inverse of a, $a * a' = e$:

$$b * e = c * e$$

Using the identity property:

$$b = c$$

Thus, the right cancellation law also holds.

1.5 Isomorphic Binary Structures

We establish **isomorphic binary structures**. The point is, if two binary structures are isomorphic, then properties of one carry over to the properties of the other through the isomorphism. Therefore, if we know one, we know the other. We do not need to study two of them separately.

Definition 1.5.1. By a **binary structure** $\langle S, * \rangle$, we will mean a set S with a binary operation $*$ on it.

Definition 1.5.2. Let $\langle S, * \rangle$ and $\langle T, *' \rangle$ be two binary structures.

1. A map $\varphi : S \to T$ is called a **homomorphism of binary structures** if

$$\varphi(x * y) = \varphi(x) *' \varphi(y) \quad \forall\, x, y \in S.$$

2. A map $\varphi : S \to T$ is called an **isomorphism of binary structures** if

$$\varphi(x * y) = \varphi(x) *' \varphi(y) \quad \forall\, x, y \in S,$$

and φ is a bijection.

(Emphasis in this section is on isomorphic structures; not on homomorphisms.)

Example 1.5.3. Let $U = \{z \in \mathbb{C} : |z| = 1\}$ be the **unit circle**. Then, with usual multiplication, $\langle U, \cdot \rangle$ is a binary structure.

On the interval $[0, 2\pi)$, the addition modulo 2π gives a binary structure $\langle [0, 2\pi), + \rangle$.

The map

$$\varphi : [0, 2\pi) \to U \quad \text{defined by} \quad \varphi(t) = e^{it}$$

is a binary structure isomorphism.

Example 1.5.4. Let n be an arbitrary positive number. Define

$$\psi : \mathbb{Z}_n \to U_n \quad \text{by} \quad \psi(k) = e^{\frac{2k\pi i}{n}} \quad (= \zeta_n)$$

Then, ψ is an isomorphism of binary structures.

Example 1.5.6. The mapping

$$\exp : \langle \mathbb{R}, + \rangle \to \langle (0, \infty), \cdot \rangle \quad \text{defined by} \quad \exp(t) = e^t$$

is an isomorphism of binary structures. Its inverse

$$\ln : \langle (0, \infty), \cdot \rangle \to \langle \mathbb{R}, + \rangle, \quad t \mapsto \ln(t)$$

is also an isomorphism of binary structures.

Definition 1.5.7. Let $\langle S, * \rangle$ be a binary structure. An element $e \in S$ is said to be an *identity element* for $*$ if

$$e * x = x * e = x, \quad \forall x \in S.$$

Theorem 1.5.8. Let $\langle S, * \rangle$ be a binary structure. Then, $\langle S, * \rangle$ possesses at most one identity element.

Proof. Let e, ϵ be identity elements in S. We shall prove that $e = \epsilon$.

Since e is an identity element:

$$\epsilon = \epsilon * e.$$

Since ϵ is also an identity element:

$$e = \epsilon * e.$$

Thus, $\epsilon = e$. The proof is complete.

Theorem 1.5.9. Let $\varphi : S \to T$ be an isomorphism of two binary structures $\langle S, * \rangle$ and $\langle T, *' \rangle$. Let $e \in S$ be the identity for $*$. Then, $\varphi(e)$ is an identity element in $\langle T, *' \rangle$.

Proof:

For $x \in T$, we must show $x *' \varphi(e) = \varphi(e) *' x = x$.

Because φ is onto, $\varphi(a) = x$ for some $a \in S$.

We have:

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

Apply φ:

$$\varphi(e) *' \varphi(a) = \varphi(a) *' \varphi(e) = \varphi(a)$$

Which is:

$$\varphi(e) *' x = x *' \varphi(e) = x$$

Hence, $\varphi(e)$ is an identity in T. The proof is complete.

1.6 Non-Isomorphic Binary Structures

We examine several non-isomorphic binary structures.

Example 1.6.1.

1. $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ are not isomorphic.
2. (Added) $\langle \mathbb{Q}, \cdot \rangle$ and $\langle \mathbb{Z}, \cdot \rangle$ are not isomorphic.

Proof.

1. This is due to the fact that $\langle \mathbb{Q}, + \rangle$ is "divisible" by any positive integer n.

   "Divisible by 3" means that for any $y \in \mathbb{Q}$, there is an element $x \in \mathbb{Q}$ such that:

   $$x + x + x = y$$

   namely $x = \frac{y}{3}$. But $\langle \mathbb{Z}, + \rangle$ does not enjoy this property.

2. For the second statement, note that all nonzero elements in $\mathbb{Q}$ have an inverse, while that is not true for $\mathbb{Z}$.

Example 1.6.2.

$\langle \mathbb{R}, \cdot \rangle$ is not isomorphic to $\langle M_2(\mathbb{R}), * \rangle$, where $*$ is usual matrix multiplication.

Among other things, the first structure is commutative, while the second one is not commutative.

Example 1.6.3.

$\langle \mathbb{R}, \cdot \rangle$ and $\langle \mathbb{C}, \cdot \rangle$ are not isomorphic.

Chapter 2

Group and Subgroup

2.1 Group

From school level, students are well accustomed with the sets like $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and the binary operations in these sets of numbers, what we call $+$, $-$, $\times$, etc.

In layman's words, a binary operation on a set combines any two elements of the set to produce a new element of the set.

At this point, let us place the formal definition of a binary operation on a set.

Definition 2.1.1. A binary operation $*$ on a nonempty set G is a function from the Cartesian product $G \times G$ to the set G which assigns each ordered pair (x, y) of elements of G into an element of G. We always write:

$$*(x, y) = x * y \quad \forall x, y \in G$$

Let us consider the set $Z_n = \{0, 1, 2, \ldots, n-1\}$ of equivalence classes corresponding to the equivalence relation $\equiv \pmod{n}$ defined on the set of integers $\mathbb{Z}$. In this set, we can define two binary operations, namely addition (mod n) and multiplication (mod n).

One can cite innumerable examples of algebraic structures which satisfy associativity, existence of identity, and existence of inverse. Instead of considering them individually, here we consider an abstract algebraic structure G called a **group**.

At this point, let us place the formal definition of a group.

Definition 2.1.2. A nonempty set G equipped with a binary operation is said to be a **group** if the elements of G satisfy the following:

(i) **Associativity:** For any $a, b, c \in G$

$$a(bc) = (ab)c$$

(ii) **Existence of Identity:** There exists an element $e \in G$ (called the identity element)

such that,

$$ae = ea = a \quad \forall a \in G$$

(iii) **Existence of Inverse:** For each element $a \in G$, there exists an element $b \in G$ such that,

$$ab = ba = e$$

The element b is called the inverse of a and is denoted by a^{-1}.

2.2 Remarks

1. If, in addition to the above properties, the commutative property holds in G, i.e., for any $a, b \in G$,

   $$ab = ba$$

   then the group G is called an **abelian group**.

2. In the case of an *additive group* G, the identity element e is replaced by 0, the zero element of G, such that for any $a \in G$,

   $$a + 0 = 0 + a = a$$

3. The inverse of an element a in an additive group G is called the *negative* of a and is denoted by $-a$, satisfying:

   $$a + (-a) = (-a) + a = 0$$

4. Additive groups are always abelian, i.e., for an additive group G,

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

5. For an element $a \in G$, we can write $a, a \in G$; by the closure property, $aa = a^2 \in G$. Again, $a, a^2 \in G$ implies $aa^2 = a^3 \in G$. Continuing this process, one can see that for any $a \in G$, we always have:

   $$a^n \in G \quad \forall n \in \mathbb{N}$$

   Also, we define:

   $$a^0 = e \quad \forall a \in G$$

Furthermore, for $a \in G$, $a^{-1} \in G$ and hence,

$$a^{-1}a^{-1} = a^{-2} \in G$$

Continuing this process, we conclude that:

$$a^n \in G \quad \forall n = -1, -2, -3, \ldots$$

Finally, one can conclude that,

$$a^n \in G \quad \forall n \in \mathbb{Z}$$

By the same argument, for an additive group G, one can conclude that,

$$na \in G \quad \forall n \in \mathbb{Z}$$

where

$$na = \begin{cases} a + a + \cdots + a \quad (n \text{ times}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ (-a) + (-a) + \cdots + (-a) \quad (-n \text{ times}) & \text{if } n < 0 \end{cases}$$

2.3 A few basic results:

1. A group G consists of one and only one identity element.
2. In a group, both right and left cancellation laws hold good.
3. For each element a in a group G, there exists a unique element $b \in G$ such that

$$ab = ba = e$$

4. For an element $a \in G$, the inverse of a^{-1} is the element itself, i.e.,

$$(a^{-1})^{-1} = a \quad \forall a \in G$$

5. For any $a, b \in G$,

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

This property is sometimes called the **Socks-Shoes property** or **reversal law**.

6. For $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions in the group G.

Proof (1): If possible, suppose that G is a group with two identity elements, namely e and e'. Since both e and e' are identities of the group G, therefore for any $a \in G$,

$$ae = a \quad \text{and} \quad e'a = a$$

Putting $a = e'$, we get

$$e'e = e' \quad \text{and} \quad e'e = e$$

Thus,

$$e' = e$$

Hence, the identity element is unique.

Proof (2): Let G be a group and $a, b, c \in G$ such that

$$ab = cb \tag{1}$$

and

$$ab = ac \tag{2}$$

Post-multiplying both sides of (1) by b^{-1}, we get:

$$(ab)b^{-1} = (cb)b^{-1} \implies a(bb^{-1}) = c(bb^{-1}) \quad \text{[By associativity in } G\text{]}$$

$$ae = ce \implies a = c$$

Pre-multiplying both sides of (2) by a^{-1}, we get:

$$a^{-1}(ab) = a^{-1}(ac) \implies (a^{-1}a)b = (a^{-1}a)c \implies eb = ec \implies b = c$$

It follows that both the cancellation laws hold good in G.

Proof (3): Suppose G is a group with identity element e. For an element $a \in G$, suppose that there exist $b, b' \in G$ such that:

$$ab = ba = e \quad \text{and} \quad ab' = b'a = e$$

It follows that:

$$ab = e = ab' \implies ab = ab' \implies b = b' \quad \text{[By left cancellation law]}$$

It follows that the inverse of an element in a group is unique.

Proof (4): For an element a in a group G, from the definition of inverse, we have:

$$aa^{-1} = a^{-1}a = e$$

Taking $b = a^{-1}$, we get:

$$ab = ba = e \implies ba = ab = e$$

Thus, taking the inverse of b, we have:

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

This completes the proof.

Proof (5): For any $a, b \in G$, by closure property $ab \in G$ and hence $(ab)^{-1} \in G$ such that,

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

Now,

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) \quad \text{[By associativity in } G\text{]}$$

$$= a((bb^{-1})a^{-1}) = a(ea^{-1}) = e$$

By the same argument, one can show that:

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

It follows that:

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

This completes the proof.

Proof (6): Given that G is a group and $a, b \in G$. To show that the equations $ax = b$ and $ya = b$ have unique solutions in the group G.

Clearly, $a^{-1}b$, $ba^{-1} \in G$ and $a^{-1}b$ is a solution of the equation $ax = b$ since:

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

If possible, suppose that the equation $ax = b$ has two solutions $x_1, x_2 \in G$ such that:

$$ax_1 = b \quad \text{and} \quad ax_2 = b \implies ax_1 = ax_2$$

$$\implies x_1 = x_2 \quad \text{[By left cancellation law]}$$

It follows that the equation $ax = b$ has a unique solution in the group G.

By the same argument, one can see that ba^{-1} is a solution of the equation $ya = b$ in G, and the solution is unique.

Definition 2.3.1: The number of distinct elements of a group G is said to be the *order* of the group, denoted by $|G|$.

If the order of a group is not finite, we say that it is an *infinite group* or a group of infinite order.

For instance, the additive group of integers $\mathbb{Z}$ is an infinite group, while the group:

$$U(10) = \{1, 3, 7, 9\}$$

(the set of those numbers which are co-prime to 10) under multiplication modulo 10 is a

finite group of order 4.

In general, for any positive integer n, the order of the group $U(n)$ is given by $\varphi(n)$, where φ is Euler's totient function defined as:

$$\varphi(n) = \begin{cases} 1, & \text{if } n = 1 \\ m, & \text{if } n > 1 \end{cases}$$

where m is the number of positive integers relatively prime to n.

Definition 2.3.2. The order of an element a in a group G is the smallest positive integer n for which $a^n = e$ and it is denoted by $|a|$.

$$|a| = n \iff a^n = e \quad \text{and if} \quad a^m = e \quad \text{then} \quad n \leq m$$

Remark 2.3.3. One must note that in a group G, for an element a, if $a^n = e$, then we can conclude that $|a| \leq n$. To conclude $|a| = n$, we must prove that n is the least positive integer for which $a^n = e$.

Remark 2.3.4. The order of the identity element in a group is always considered to be 1.

Remark 2.3.5. In case of an additive group G and for an element $a \in G$:

$$|a| = n \iff n \text{ is the least positive integer such that } na = 0$$

Example 2.3.6: Order of Elements in $U(15)$

Determine the order of each element in the group $U(15)$ under multiplication modulo 15.

We know that:

$$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

For the element $2 \in U(15)$:

$$2\,(mod 15) = 2, \quad 2^2\,(mod 15) = 4, \quad 2^3\,(mod 15) = 8, \quad 2^4\,(mod 15) = 1$$

It follows that $|2| = 4$.

For the element $4 \in U(15)$:

$$4\,(mod 15) = 4, \quad 4^2\,(mod 15) = 1$$

It follows that $|4| = 2$.

For the element $7 \in U(15)$:

$$7\,(mod 15) = 7, \quad 7^2\,(mod 15) = 4, \quad 7^3\,(mod 15) = -2, \quad 7^4\,(mod 15) = 1$$

It follows that $|7| = 4$.

For the element $8 \in U(15)$:

$$8\,(mod 15) = 8, \quad 8^2\,(mod 15) = 4, \quad 8^3\,(mod 15) = 2, \quad 8^4\,(mod 15) = 1$$

It follows that $|8| = 4$.

For the element $11 \in U(15)$:

$$11\,(mod 15) = 11, \quad 11^2\,(mod 15) = 1$$

It follows that $|11| = 2$.

For the element $13 \in U(15)$: we have

$$13\,(mod 15) = -2, \quad 13^2\,(mod 15) = 4, \quad 13^3\,(mod 15) = -8, \quad 13^4\,(mod 15) = (-2)(-8)\,(mod 15) = 1$$

It follows that $|13| = 4$.

For the element $14 \in U(15)$: we have

$$14\,(mod 15) = -1, \quad 14^2\,(mod 15) = 1$$

It follows that $|14| = 2$.

Thus, for the elements in the group $U(15)$, the orders of the elements are given by:

$$|1| = 1, \quad |2| = 4, \quad |4| = 2, \quad |7| = 4, \quad |8| = 4, \quad |11| = 2, \quad |13| = 4, \quad |14| = 2$$

Remark 2.3.7. One can note that the order of each element of the group $U(15)$ divides the order of the group.

Example 2.3.8 Determine the order of each element in the additive group $\mathbb{Z}_{10} = \{0, 1, 2, \cdots, 9\}$ under addition $\mod 10$.

Remark 2.3.9. One will find $|1| = 10 = |9|$. This little information will help us in near future during our journey.

2.4 Subgroup

A nonempty subset H of a group G is said to be a *subgroup* of the group G if H is itself a group under the binary operation in the group G and we denote it by $H \leq G$.

Remark 2.4.1. In case of the identity element e of the group G and $H = \{e\}$, then $H \leq G$ what we call the *trivial subgroup* of the group G.

In case $H \leq G$ and $H \neq \{e\}$, we say that H is a *nontrivial subgroup* of the group G.

Remark 2.4.2. In case $H \leq G$ and $H \neq G$, then H is said to be a *proper subgroup* of the group G and we denote it by $H < G$.

As we know, the set of integers $\mathbb{Z}$ is an additive group and $\mathbb{Z}_n$ is also an additive group under addition $\mod n$. However, $\mathbb{Z}_n$ is not a subgroup of $\mathbb{Z}$. Please note that neither $\mathbb{Z}_n \subseteq \mathbb{Z}$ nor the binary operation in $\mathbb{Z}_n$ is the same as that in $\mathbb{Z}$.

One can easily verify that $H = \{1, -1, i, -i\}$ is a subgroup of the multiplicative group $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

Theorem 2.4.3.(One step subgroup test)
Suppose that H is a nonempty subset of a group G. If for any $a, b \in H$, $ab^{-1} \in H$ then $H \leq G$.

Proof. It is given that $H \neq \emptyset$; therefore, there exists $a \in H$. It follows that:

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

In other words, H contains the identity element e of the group G.

On the other hand, $e, a \in H \implies ea^{-1} = a^{-1} \in H$. It follows that H contains the inverse of each element in it.

For any $a, b \in H$, we have:

$$a, b \in H \implies a, b^{-1} \in H \quad \text{(Since } H \text{ contains the inverse of each element in it).}$$

Therefore,

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

It follows that H is closed under the binary operation in the group G.

Since the binary operation in H and G are the same, and the elements of G satisfy the associative property, the associative property in H is hereditary.

It follows that H is itself a group under the binary operation in G, as a result of which $H \leq G$.

Theorem 2.4.4. (Two Steps Subgroup Test)
Suppose that H is a nonempty subset of a group G. If for any $a, b \in H$, $ab \in H$ and $a^{-1} \in H$ whenever $a \in H$, then $H \leq G$.

Proof. It is given that H is a nonempty subset of the group G which is closed under the binary operation in the group G and the inverse of each element in H is again an element in H. We now have,

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

$$aa^{-1} = e \in H \quad \text{[By the closure property of } H\text{]}$$

Since the binary operation in H and G are the same and the elements of G satisfy the associative property, therefore, the associative property in H will be hereditary true.

It follows that H is itself a group under the binary operation in the group G, as a result of which $H \leq G$.

Theorem 2.4.5. (Finite Subgroup Test)
Suppose that H is a finite subset of a group G. Then H is a subgroup of G if H is closed under the binary operation of G.

Proof: As it is given that H is closed under the binary operation in the group G, for any $a\,(\neq e) \in H$, the sequence

$$a,\, a^2,\, a^3,\, \ldots \in H$$

Since H is finite, all the elements in this sequence cannot be distinct. Suppose that for some integers $i > j$, we have

$$a^i = a^j \implies a^{i-j} = e$$

Thus,

$$a \cdot a^{i-j-1} = e \implies a^{-1} = a^{i-j-1} \in H$$

Since $a \neq e$ and $a^{i-j} = e$, it follows that $i - j \geq 1$.

In the case $a = e$, since the identity element has its own inverse, clearly $e = a^{-1} \in H$.

Therefore, each element of H has its inverse in H. It follows that H is a subgroup of G, that is, $H \leq G$.

Theorem 2.4.6.
Let G be a group. Then for any $a \in G$,

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

is always a subgroup of the group G.

Proof:
Clearly, $a \in \langle a \rangle$ and therefore $\langle a \rangle$ is a nonempty subset of the group G.
For any $x, y \in \langle a \rangle$, there exist $m, n \in \mathbb{Z}$ such that $x = a^m$ and $y = a^n$.
Now, we have

$$xy^{-1} = a^m(a^n)^{-1} = a^{m-n} \in \langle a \rangle \quad (\text{since } m, n \in \mathbb{Z} \implies m - n \in \mathbb{Z})$$

It follows that $\langle a \rangle$ is a subgroup of the group G.

Remark 2.4.7. The subgroup $\langle a \rangle$ is said to be a cyclic subgroup of the group G generated by the element a and a is said to be a generator of the cyclic group $\langle a \rangle$.

Remark 2.4.8. For any $a^i, a^j \in \langle a \rangle$ we have

$$a^i a^j = a^{i+j} = a^{j+i} = a^j a^i.$$

It follows that a cyclic group $\langle a \rangle$ is always an abelian group.

Remark 2.4.9. One must note that a cyclic group may have more than one generator. For instance, let us consider the additive group $\mathbb{Z}_n$ under addition $\mod n$.
We know $1 \in \mathbb{Z}_n$ and:

$$n = 1 + 1 + \cdots + 1 \quad (n \text{ times})$$

Thus:

$$n + 1 \equiv 1 \pmod{n}, \quad n + 2 \equiv 2 \pmod{n}, \quad \text{and so on.}$$

It follows that:

$$\mathbb{Z}_n = \langle 1 \rangle.$$

On the other hand, consider $n - 1 \in \mathbb{Z}_n$. We now have:

$$2(n-1) \mod n = (n + n - 2) \mod n = n - 2,$$

$$3(n-1) \mod n = (n + n - 3) \mod n = n - 3,$$

$$\vdots$$

$$(n-1)(n-1) \mod n = (n^2 - 2n + 1) \mod n = 1,$$

$$n(n-1) \mod n = (n^2 - n) \mod n = 0.$$

It follows that:

$$\mathbb{Z}_n = \langle 1 \rangle = \langle n-1 \rangle.$$

Definition 2.4.10. The center $Z(G)$ of a group G is the subset of elements of the group G which commutes with all other elements of the group G.

$$Z(G) = \{a \in G \mid ax = xa, \ \forall x \in G\}$$

Remark 2.4.11. Since the identity element e commutes with all elements of the group G, therefore $e \in Z(G)$ and hence $Z(G)$ is a nonempty subset of the group G.

For any $a, b \in Z(G)$, we have

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab), \quad \forall x \in G$$

It follows that $Z(G)$ is closed under the binary operation in the group G.

Further, for any $a \in Z(G)$ and for any $x \in G$, we have

$$ax = xa \implies a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1} \quad \text{(Pre and post multiplying by } a^{-1})$$

$$(a^{-1}a)xa^{-1} = a^{-1}x(aa^{-1})$$

$$a^{-1}x = xa^{-1}$$

It follows that a^{-1} commutes with all elements of the group G and consequently $a^{-1} \in Z(G)$.

Hence, $Z(G) \leq G$.

Remark 2.4.12. A group G is abelian if and only if $Z(G) = G$.

Definition 2.4.13. For any fixed element $a \in G$, the centralizer of the element a is defined as the set of those elements of the group G which commutes with the element a, and it is denoted by $C(a)$, i.e.

$$C(a) = \{g \in G \mid ga = ag\}$$

Remark 2.4.14 From the definitions, it is clear that $Z(G) \subseteq C(a)$.

Further, the identity $e \in C(a)$ and hence $C(a)$ is a nonempty subset of the group G.

For any $g \in C(a)$, we have

$$ga = ag \implies g^{-1}(ga)g^{-1} = g^{-1}(ag)g^{-1} \quad \text{(Pre and post multiplying by } g^{-1})$$

$$g^{-1}a = ag^{-1}$$

It follows that the inverse of each element of $C(a)$ lies in $C(a)$.

For any $g, g' \in C(a)$, we have

$$(gg')a = g(g'a) = g(ag') = (ga)g' = a(gg')$$

It follows that $C(a)$ is closed under the binary operation in the group G.

Hence, $C(a) \leq G$. Further, one can conclude that

$$Z(G) \leq C(a) \leq G$$

***

Conclusion

In this dissertation, we have examined the basic building blocks of groups and subgroups, the foundation of abstract algebra. Starting with the concept of binary operations and their fundamental properties such as associativity, commutativity, and the existence of identity and inverse elements, we established a systematic study of group structures.

The study of groups reveals profound insights into algebraic structures where symmetry and operations under specific regulations play a central role. Using examples such as additive groups of integers, multiplicative groups of units under modular arithmetic, and cyclic groups, we illustrated the formation and key characteristics of groups. The conception of subgroups, whether trivial or non-trivial, facilitates further analysis by considering subsets that themselves retain the group structure.

Furthermore, we explored critical subgroup tests, including the one-step, two-step, and finite subgroup tests, which provide essential tools for identifying subgroups effectively. We also discussed central concepts such as cyclic groups, centers of groups, and centralizers, which help uncover the internal structure and symmetry within groups.

In summary, the study of groups and subgroups not only enhances our understanding of algebraic structures but also lays the groundwork for more advanced mathematical topics, such as rings, fields, and their applications in areas like cryptography, physics, and beyond. Throughout this dissertation, we have presented a comprehensive overview of these concepts, paving the way for further study and research in the exciting domain of abstract algebra.

***

Bibliography

[1] Vijay K Khanna,S K Bhambri *A Course in Abstract Algebra, Fourth Edition*, Vikas Publishing House PVT Limited, 2013.

[2] Satya Mandal, *University of Kansas,Lawrence KS 66045 USA*, January 22.