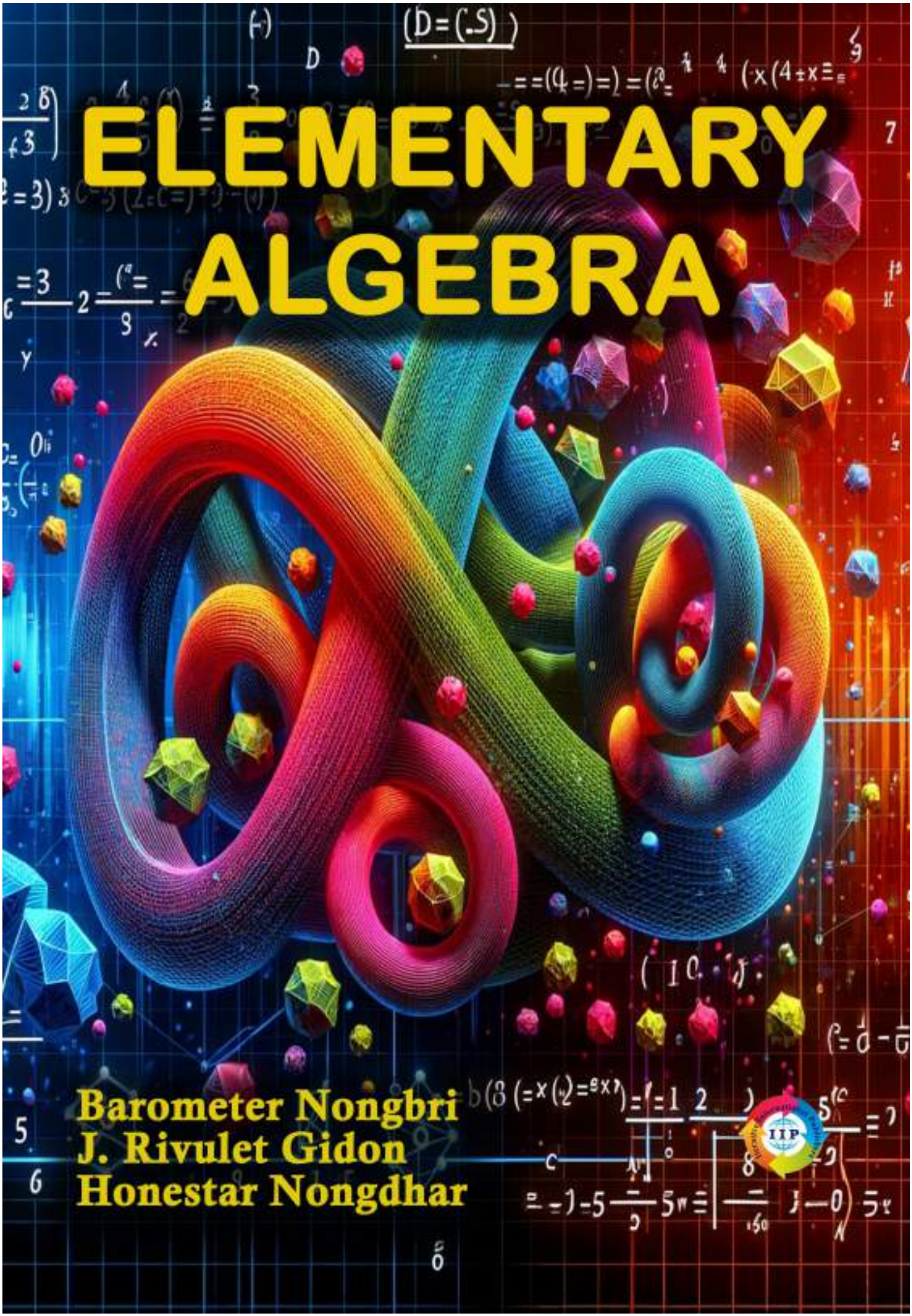
ELEMENTARY ALGEBRA



Barometer Nongbri
J. Rivulet Gidon
Honestar Nongdhar

Elementary Algebra

First Edition

Authors

Mr. Barometer Nongbri

Smt. J. Rivulet Gidon

Mr. Honestar Nongdhar

Title of the Book: Elementary Algebra

First Edition - 2024

Mr. Barometer Nongbri, Assistant Professor, Department of Mathematics, Shillong College, Shillong, India.

Smt. J. Rivulet Gidon, Assistant Professor, Department of Mathematics, Shillong College, Shillong, India.

Mr. Honestar Nongdhar, Assistant Professor, Department of Mathematics, Lady Keane College, Shillong, Meghalaya, India.

Disclaimer
The authors are solely responsible for the contents published in this book. The publishers don't take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the editors or publishers to avoid discrepancies in future.

ISBN: 978-93-6252-169-9

MRP Rs. 480/-

Publisher, Printed at & Distribution by:
Selfypage Developers Pvt Ltd.,
Pushpagiri Complex,
Beside SBI Housing Board,
K.M. Road Chikkamagaluru, Karnataka.
Tel.: +91-8861518868
E-mail:info@iipbooks.com

IMPRINT: I I P Iterative International Publishers

For Sales Enquiries:
Contact: +91- 8861511583
E-mail: sales@iipbooks.com

Preface

The book is designed to cover a certain portion of Advanced Algebra in the Under Graduate courses of different Indian Universities. This book contains a number of solved examples and exercises to give students a chance to work on their own. An attempt has been made to present the subject in a clear, lucid and intelligible manner.

-Mr. Barometer Nongbri

Acknowledgement

I would like to express my gratitude to all my colleagues, whose unwavering support and encouragement kept me motivated throughout the writing process. Their insightful feedback and constructive criticism were invaluable in shaping this book. I further could not leave mentioning how grateful I am to all my teachers at every level who have made me what I am now I have been during my study of the subject, influenced by the works of a number of authors including Joseph A. Gallian, I.N Herstein, J.B fraleigh, N. S. Gopalakrishnan etc. Their books have been immensely useful to our understanding of the subject. I feel deeply grateful to them all.

I take this opportunity to thank the publishers and the printers who did all they could to give the book the best form possible under time constraint situation.

I also express sincere thanks to co-author Smt. J. Rivulet Gidon and co-author Mr. Honester Nongdhar for their huge contributions.

-Mr. Barometer Nongbri

Contents

Chapter- 1

Revision of Operations on Numbers System

Introduction

In this chapter we shall take a quick look of some operations on real numbers without detailing the classification that is supposed to have been covered in lower standards .

Operations on real numbers include addition, subtraction, multiplication, and division. These operations follow certain rules that are fundamental to arithmetic:

#1.1: Let's now take a look at the usual properties followed by addition and multiplication in the set of real numbers

- **Commutative property:** The order of numbers can be changed without affecting the result.

  $a + b = b + a$

  $a \times b = b \times a$

- **Associative property:** The grouping of numbers can be changed without affecting the result.

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

  $(a \times b) \times c = a \times (b \times c)$

- **Distributive property:** Multiplication distributes over addition.

  $a \times (b + c) = a \times b + a \times c$ (left)

  $(a + b) \times c = a \times c + b \times c$ (right)

- **Identity elements:** There exist additive identity element "$'0'$ and multiplicative identity element $'1'$ with the property :

  Additive identity: $a + 0 = 0 + a = a$

  Multiplicative identity: $a \times 1 = 1 \times a = a$

- **Inverse elements:** Additive and multiplicative inverses exist for each number.

  Additive inverse: $a + (-a) = (-a) + a = 0$

  Multiplicative inverse (for non-zero numbers $'a'$): $a \times \frac{1}{a} = \frac{1}{a} \times a = 1$

- **Closure Property:**

  That $(a + b) \in R \ \forall \ a, b \in R$ and

  $ab \in R \ \forall \ a, b \in R$

#1.2: Cartisian Product

For any two sets A abd B, we defined the cartisian product or cross product as $A \times B = \{ (a, b) : a \in A, b \in B \}$ the cross product of A with itself is understood and $A \times A$ will also be denoted by A^2.

#1.3: Relation

Definition: A relation R from a set A to another set B is a rule that associates elements of A (not necessarily each elements of A) with elements of B.

If an element $a \in A$ is associated to an element $b \in B$, we say that $'a$ is related to b' and write $'aRb'$.

If $'aRb'$ we call an element $'b'$ an **image** of $'a'$ and $'a'$ is the **pre-image** of $'b'$.

The set A is called the **domain** and the set B is called the **co-domain** of R.

Eg. Let $A = \{ a, b, c, d \}$, $B = \{ 1, 2, 3, 4, 5 \}$. Let R be a relation that relates $a \ to \ 1, b \ to \ 2, c \ to \ 5$ i.e $aR1, bR2, cR5$.

This relation R can also be view as a set of ordered pairs i.e

$R = \{(a, 1), (b, 2), (c, 5) \}$ which is essentially a subset of $A \times B$.

In view of the above example , we can also define **a relation from a set A to another set B as a subset of $A \times B$.**

Range of a relation

Let R be a relation from a set A to a set B. The range of R is defined as the set of elements of B which has some pre-images in A.

Range$(R) = \{ y \in B : xRy \ for\ some\ x \in A \}$.

Equivalently , The range of R is defined as the set of all the first co-ordinates of R ,when R is viewed as a subset of $A \times B$.

Binary Relation: A relation R from a set A to itself is called a binary relation on A .

Type of Binary relations: Reflexive , Symmetric , Transitive and Equivalence

- Reflexive: A binary relation R on A is said tobe reflexive if $\forall\ a \in A \Rightarrow (a, a) \in R$

- Symmetric: A binary relation R on A is said tobe Symmetric if $(a, b) \in R \Rightarrow (b, a) \in R$

- Transitive: A binary relation R on A is said tobe transitive if $(a, b),\ (b, c) \in R \Rightarrow (a.c) \in R$

- A binary relation R on A is called an **Equivalence** relation if it is reflexive, symmetric, and transitive .

#1.4: Divisibility in the set of Integers

Another Peculiar operation is the **divisibility** in the set of integers (denoted by Z) and the set of natural numbers (denoted by N) which is of more interest later in this book .

We recall that if for three integers a, b, c satisfying $ab = c$ then $'a'\ and\ 'b'$ are called the **factors** of $'c'$ and c is called a **multiple** of a and b .

The above statement is also synonymous to saying that:
"a divides c" tobe denoted as "$a|c$" , "$b\ divides\ c$" tobe denoted as "$b|c$" keeping in mind that the divisor should not be "0" .

It is also tobe noted that given two integers a and c , we shall not always have $ab = c$ with $some$ integer b . We will briefly state below another concept namely – "**The division algorithm**" which is a fundamental concept in arithmetic that defines how to perform division of integers and obtain both a quotient and a remainder, skipping aside the details definition of divisor , dividend ,quotient and remainder.

The division algorithm: for any integer, n, and any positive integer, m, there exists unique integers q and r such that $n = mq + r$ where $0 \leq r < m$.

Eg. $10 = 8 \times 1 + 2$
Euclid's Lemma: If p is a prime and $p \mid ab$ then $p \mid a \; or \; p \mid b$.

#1.5: Arithmetic modulo n

We define what it means to take one integer m, modulo another integer, n.

Definition: Letting $n \geq 1$, $n \in N$,

"m (mod n)" is the smallest integer r where $0 \leq r < n$

such that $m = nq + r$ for some integer q.

i.e $\boldsymbol{m \; (\mathbf{mod}\; n) = r \Leftrightarrow m = nq + r}$, $\boldsymbol{0 \leq r < n}$

Notice that $\big(\boldsymbol{m \; (mod \; n)}\big)\boldsymbol{(mod \; n) = r \; (mod \; n) = r}$ as $0 \leq r < n$

$$= \boldsymbol{m \; (mod \; n)}$$

#1.6: Congruence Modulo n

For $n \geq 1$, $a, b \in Z$, we say that a is congruent to b modulo n (written as $a \equiv b \; (\text{mod } n)$) if $n|(a - b)$ or $n|(b - a)$

Some properties of **Congruence Modulo n**

(i) It can be seen that $n|(a - b) \Rightarrow \text{n}|ka - kb$

i.e $\boldsymbol{a \equiv b \; (\mathbf{mod}\; n) \Rightarrow ka \equiv kb \; (mod \; n)}$

(ii) Also we can see that $n|(a - b) \Rightarrow n|(a - b)^n$

and as $(a - b)^n = a^n - b^n + (\; a \; multiple \; of \; n)$

we have $n|(a-b) \Rightarrow n|a^n - b^n$

i.e $\boldsymbol{a \equiv b \ (\mathbf{mod}\ n) \Rightarrow a^n \equiv b^n \ (mod\ n)}$

(iii) If $x \equiv y\ (mod\ n)$ and $a \equiv b\ (mod\ n)$

then $n|(x-y)$ and $n|\ (a-b)$

$\Rightarrow n|(x+a)-(y+b)$

$\Rightarrow (x+a) \equiv (y+b)(mod\ n)$

(iv) Transitive property : If $a \equiv b\ (mod\ n\ )$ and $b \equiv c\ (mod\ n\ )$

Then $n|(a-b)$ and $n|(b-c)$

$\Rightarrow n\ \ (a-b+b-c)$ i.e $n|(a-c)$

$\Rightarrow\ \ a \equiv c\ (\ mod\ n)$

#1.7: Fermat's Little Theorem

If $\boldsymbol{p}$ is a prime number and $\boldsymbol{a}$ is an integer not divisible by $\boldsymbol{p}$ **then** $\boldsymbol{a^{p-1} \equiv 1\ mod\ p}$ this theorem can also be stated as

If $\boldsymbol{p}$ is a prime number and $\boldsymbol{a}$ is an integer not divisible by $\boldsymbol{p}$ then the remainder when a^{p-1} is divided by p is 1**.**

#1.8: Congruence classes Modulo $\boldsymbol{n}$

Let Z be the set of integers and n a positive integer .

We define a relation on Z as "a is related to b" if and only if $a \equiv b$ (mod n**).**

We leave to the reader to verify that this relation is an euivalence relation on Z**.**

Further , Let $[a]$ be the set of all integers that are congruent to a modulo n .

i.e $[a] = \{\, x \in Z :\ \ x \equiv a\ (mod\ n\ )\ \}$

Then the set of integers will give rise to the set of residue classes of the form $S = \ [o]\ , [1]\ , [2], \ldots \ldots . [n-1]. [n]\ , [n+1], \ldots.$

We shall show the equality of these sets in the theorem below.

Theorem: $[\boldsymbol{a}] = [\boldsymbol{b}] \Leftrightarrow \boldsymbol{a} \equiv \boldsymbol{b}\ (\boldsymbol{mod\ n})$

Suppose $[a] = [b]$

we have $a \equiv a\ (mod\ n) \Rightarrow\ \ a \in [a] \Rightarrow a \in [b]$ as $[a] = [b]$

But $a \in [b] \Rightarrow a \equiv b\ (\ mod\ n\ )$

Conversely , Suppose $a \equiv b\ (\ mod\ n\ )$

Let $x \in [a]$

$\Rightarrow x \equiv a(mod\ n)$

and since $a \equiv b\ (mod\ n)$

We have $x \equiv b\ (mod\ n)$

$\Rightarrow x \in [b]$

Showing that $[a] \subseteq [b]$

We can similarly show that $[b] \subseteq [a]$ so that $[a] = [b]$

Using this theorem we can deduce that for a fixed positive integer n , the residue classes modulo n are $[0], [1], [2], [3], \ldots \ldots [n-2], [n-1]$, any from the rest are equal to one of these .

#1.9: Addition modulo n

For a positive integer n **,** Addition modulo n , denoted as $(a +_n b)$, or "$(a + b) mod\ n$ " is a mathematical operation that calculates the remainder when the sum of two integers a and b is divided by n.

Given two integers a and a, the sum $(a + b)$ is calculated first in the usual way. Then, the result is reduced modulo n by taking the remainder of $(a + b)$ when divided by n.

i.e $(a +_n b) = (a + b)\ (mod\ n) =$ (least non-negetive integer when $(a + b)$ is divided by n .

Properties of modular addition

(1) Closure: For any integers a and b,

$(a + b) \bmod n$ is also an integer and

(2) (i) Distributive property

$$(\boldsymbol{a+b})(\mathbf{mod}\ \boldsymbol{n}) = \big(\boldsymbol{a}\ (\mathbf{mod}\ \boldsymbol{n}) + \boldsymbol{b}\ (\mathbf{mod}\ \boldsymbol{n})\big)\ (\mathbf{mod}\ \boldsymbol{n})$$

Proof: Let $a = q_1 n + r_1\ , b = q_2 n + r_2$ where $0 \le r_1, r_2 < n$

Then $a(mod\ n) = r_1\ ,\ b(mod\ n) = r_2$

R.H.S = $\big(a\ (\text{mod}\ n) + b\ (\text{mod}\ n)\big)\ (\text{mod}\ n) = (r_1 + r_2)\ (mod\ n)$

= (Least non-negetive integer when $(r_1 + r_2)$ is divided by n) .

L.H.S = $(a+b)(\text{mod}\ n) = \big((q_1 + q_2)n + (r_1 + r_2)\big)(mod\ n)$

= (Least non-negetive integer when $(q_1 + q_2)n + (r_1 + r_2)$ is divided by n)

= (Least non − negetive integer when $(r_1 + r_2)$ is divided by n) .

Thus $L.H.S = R.H.S$

(ii) $(\ \boldsymbol{a}(\boldsymbol{mod}\ \boldsymbol{n}) + \boldsymbol{b})\ (\ \boldsymbol{mod}\ \boldsymbol{n}) = (\boldsymbol{a+b})(\boldsymbol{mod}\ \boldsymbol{n})$

Proof: Let $a = q_1 n + r_1\ , b = q_2 n + r_2$ where $0 \le r_1, r_2 < n$

Then $a(mod\ n) = r_1\ ,\ b(mod\ n) = r_2$

Now $(\ a(mod\ n) + b)\ (\ mod\ n) = (r_1(mod\ n) + b)(mod\ n)$

$= (r_1 + b)\ (mod\ n)$ as $0 \le r_1 < n \Rightarrow r_1(mod\ n) = r_1$

$= \big(r_1(mod\ n) + b\ (mod\ n)\big)\ (mod\ n)$ using (i)

$= (r_1 + r_2)(mod\ n)$

And $(a+b)(mod\ n) = \big(a\ (mod\ n) + b(mod\ n)\big)\ (\ mod\ n)$ using (i)

$(r_1 + r_2)\ (\ mod\ n)$

Thus $(\ \boldsymbol{a}(\boldsymbol{mod}\ \boldsymbol{n}) + \boldsymbol{b})\ (\ \boldsymbol{mod}\ \boldsymbol{n}) = (\boldsymbol{a+b})(\boldsymbol{mod}\ \boldsymbol{n})$

(3) Associativity: For any integers a , b and c ,

$$(\boldsymbol{a}+_{\boldsymbol{n}}\boldsymbol{b})+_{\boldsymbol{n}}\boldsymbol{c} = \boldsymbol{a}+_{\boldsymbol{n}}(\boldsymbol{b}+_{\boldsymbol{n}}\boldsymbol{c})$$

or

$$\big((\boldsymbol{a+b})(\boldsymbol{mod}\ \boldsymbol{n}) + \boldsymbol{c}\big)\ (\boldsymbol{mod}\ \boldsymbol{n}) = \big(\ \boldsymbol{a} + (\ \boldsymbol{b} + \boldsymbol{c})(\boldsymbol{mod}\ \boldsymbol{n})\big)(\boldsymbol{mod}\ \boldsymbol{n})$$

Proof: Using the previous property ,

$$\boldsymbol{L.H.S} = \boldsymbol{R.H.S} = (\boldsymbol{a+b+c})(\boldsymbol{mod}\ \boldsymbol{n})$$

(4) Commutativity: $(a+_n b) = (b+_n a)$.
Proof is trivial .

(5) Identity Element: The identity element for addition modulo n is 0.
That is, $(a + 0)\ (mod\ n) = a\ (mod\ n)$

(6) Inverse Element: Every integer a modulo n has an inverse modulo n, denoted $-a$, such that $\big(a + (-a)\big)(mod\ n) = 0$

In a similar way we can define

#1.10: Multiplication modulo n

$(denoted\ by\ \ a \times_n b \quad or \quad ab(mod\ n)\ )$
$(a \times_n b) = r$ where r (least non-negetive integer when ab is divided by n and the following properties follows :

Properties of Multiplication Modulo n

(1) Closure: For any integers a and b,
$(ab)(\text{mod } n)$ is also an integer.

(2) Commutativity: $(a \times_n b) = (b \times_n a)$ or $ab\ (mod\ n) = ba\ (mod\ n)$

(3) Distributive property
$(ab)\ (\ mod\ n\ ) = \{\ \big(a\ (mod\ n)\big)\big(b\ (mod\ n)\big)\}\ (\ mod\ n)$

Proof: Let $a = m_1 n + r_1$, $b = m_2 n + r_2$ where $0 \le r_1, r_2 < n$

Therefore $a(mod\ n) = r_1$, $b\ (mod\ n) = r_2$

$R.H.S = r_1 r_2\ (mod\ n)$

$L.H.S = \big((\ m_1 m_2 n + m_1 r_2 + m_2 r_1)n + r_1 r_2\big)(mod\ n)$

$= \big((\ m_1 m_2 n + m_1 r_2 + m_2 r_1)n(mod\ n) + r_1 r_2\ (\ mod\ n)\big)(mod\ n)$

(using didstributive property for addition modulo)

$= (0 + r_1 r_2)\ (mod\ n) = r_1 r_2\ (mod\ n) = R.H.S$

(4) Associativity: For any integers a , b and c ,
$(\boldsymbol{a} \times_{\boldsymbol{n}} \boldsymbol{b}) \times_{\boldsymbol{n}} \boldsymbol{c} = \boldsymbol{a} \times_{\boldsymbol{n}} (\boldsymbol{b} \times_{\boldsymbol{n}} \boldsymbol{c})$

or

$$\left(\left(\boldsymbol{ab}\ (\boldsymbol{mod}\ \boldsymbol{n})\right) \times \boldsymbol{c}\right)\ (\boldsymbol{mod}\ \boldsymbol{n}) = \left(\boldsymbol{a} \times \left(\boldsymbol{bc}(\ \boldsymbol{mod}\ \boldsymbol{n})\right)\right)\ (\boldsymbol{mod}\ \boldsymbol{n})$$

Proof: Letting $\boldsymbol{a}\ (\boldsymbol{mod}\ \boldsymbol{n}) = \boldsymbol{r_1}$, $\boldsymbol{b}\ (\boldsymbol{mod}\ \boldsymbol{n}) = \boldsymbol{r_2}$, $\boldsymbol{c}\ (\boldsymbol{mod}\ \boldsymbol{n}) = \boldsymbol{r_3}$ and using the previous property we shall have

$$\boldsymbol{L.H.S} = \boldsymbol{R.H.S} = (\ \boldsymbol{r_1 r_2 r_3})(\boldsymbol{mod}\ \boldsymbol{n})$$

(5) Identity Element: The identity element for addition modulo n is 1. That is, $a \times_{\boldsymbol{n}} 1 = 1 \times_n a$

#1.11: Euler's Phi function

$(\phi(n)\colon\ positive\ integer\ n\ )$

Euler's phi function, denoted as $\phi(n)$, is a function that counts the number of integers up to $\boldsymbol{n}$ that are relatively prime to $\boldsymbol{n}$. In other words, $\phi(n)$ gives the count of integers $\boldsymbol{k}$ such that $1 \leq k \leq n$ and $gcd(k,n)$ = 1, where gcd denotes the greatest common divisor.

Some key properties of Euler's phi function include:

- If p is a prime number, then $\phi(p) = p - 1$.
- $\phi(p^k) = p^k - p^{\{k-1\}}$ for any prime p and integer $k \geq 1$.
- ϕ is multiplicative, meaning if $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m) \cdot \phi(n)$

#1.12: Euler's generalization of Fermat's Little Theorem

Euler's generalization of Fermat's Little Theorem extends the concept to any integer $\boldsymbol{a}$ coprime to $\boldsymbol{n}$, where $\boldsymbol{n}$ is not necessarily a prime number.

Euler's theorem states that

- If $\boldsymbol{a}$ and $\boldsymbol{n}$ are coprime integers, then $a^{\phi(n)} \equiv 1(mod\ n)$

Chapter- 2

Matrices and Determinant

Introduction

The theory of matrices is a fundamental area of mathematics that deals with the study of matrices, which are rectangular arrays of numbers (or elements) arranged in rows and columns. Matrices are extensively used in various branches of mathematics, as well as in physics, engineering, computer science, and economics, among other fields.

#2.1: Definition

A matrix is an arrangement of $'m \times n'$ numbers in m horizontal lines called **Rows** and n vertical lines called **columns** and enclosed by brackets or parenthesis.

A matrix having m rows and n columns is said tobe of **order** $m \times n$.
Matrices are denoted by capital letters.

An entry of a matrix lying in the i^{th} row and j^{th} column is denoted by $' a_{ij}'$.

#2.2: Representation of a matrix

A matrix of order $m \times n$ of the form

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \text{ will be denoted as } A = \left(a_{ij}\right)_{m\times n}$$

#2.3: Types of Matrices

1. **Row Matrix:** A row matrix has a single row and multiple columns. It is of order $1 \times n$, where n is the number of columns. **eg**. $A = [1 \quad 3 \quad 7 \quad 9]$
   Row Matrix are also called **Row Vector**.

2. **Column Matrix:** A column matrix has a single column and multiple rows. It is or order $m \times 1$, where m is the number of rows.
   Column Matrix are also called **Column Vectors**.

3. **Square Matrix:** A square matrix has an equal number of rows and columns. It is of order $n \times n$.

4. **Diagonal Matrix**: A diagonal matrix is a square matrix where all elements except those on the main diagonal (top-left to bottom-right) are zero. Equivalently, diagonal matrix is a matrix of the form

$A = (a_{ij})_{n\times n}$ where $a_{ij} = 0$ if $i \neq j$ **Eg.** $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 9 \end{pmatrix}$,

5. **Scalar Matrix:** A scalar matrix is a diagonal matrix where all elements except those on the main diagonal (top-left to bottom-right) are zero and all entries on the main diagonal are equal. Equivalently , a scalar matrix is a matrix of the form

$A = (a_{ij})_{n\times n}$ where $a_{ij} = 0$ if $i \neq j \; and \; a_{ii} = a_{jj}$

Eg. $A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

6. **Identity Matrix:** An identity matrix is a diagonal matrix where all elements except those on the main diagonal (top-left to bottom-right) are zero and all entries on the main diagonal are equal to 1.

Eg. $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

An identity matrix of order $n \times n$ will be denoted by I_n.

7. **Zero Matrix:** A zero matrix has all its elements as zero.

8. **Upper Triangular Matrix:** An upper triangular matrix has all its elements below the main diagonal equal to zero. Equivalently , upper triangular matrix is a matrix of the form

$A = (a_{ij})_{n\times n}$ where $a_{ij} = 0$ if $i > j$ **Eg**. $A = \begin{pmatrix} 1 & 3 & 1 \\ 0 & 4 & 2 \\ 0 & 0 & 6 \end{pmatrix}$

9. **Lower Triangular Matrix:** A lower triangular matrix has all its elements above the main diagonal equal to zero. Equivalently, a lower triangular matrix is a matrix of the form

$A = (a_{ij})_{n\times n}$ where $a_{ij} = 0$ if $i < j$ **Eg**. $A = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 4 & 0 \\ 6 & 3 & 6 \end{pmatrix}$

Equality of two matrices

Two matrices are said tobe equal if they are of same order and the corresponding entries are equal.

i.e if $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n}$ then $A = B \Leftrightarrow a_{ij} = b_{ij}\ \forall\ i,j = 1\ to\ n$

#2.4: Operations on Matrices

1. **Scalar Multiplication:** If $A = (a_{ij})_{m\times n}$ is a matrix and m a scalar , then mA is a matrix or order $m \times n$ given by $mA = (ma_{ij})_{m\times n}$

   In other words , if a matrix is multiplied by a scalar , all entries of the matrix is tobe multiplied by that scalar.

2. **Addition:** Given two matrices A and B of dimensions $m \times n$, the sum $A + B$ is also an $m \times n$ matrix where each element $(A + B)$ is obtained by adding the corresponding elements of A and B .

   i.e if $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n}$ then
   $(A + B) = C$ where $C = (c_{ij})_{m\times n}$ and $c_{ij} = a_{ij} + b_{ij}$

   It is easy to see that $(A + B) = (B + A)$ for any two matrices A , B that are conformable for addition.

   Subtraction of two matrices are similarly defined.

3. **Matrix Transposition:** Let $A = (a_{ij})_{m\times n}$ be a matrix . The transpose of A is the matrix of order $n \times m$, obtained by changing the rows of A into columns or vice versa and is denoted by $A'\ or\ A^t$.

   Thus $A' = (c_{ij})_{n\times m}$ where $c_{ij} = a_{ji}$.

   We leave to the readers to verify the property that
   - $(\boldsymbol{A \pm B})' = \boldsymbol{A' \pm B'}$
   - $(\boldsymbol{kA})' = \boldsymbol{kA'}$

Definition: A square matrix A is said tobe **symmetric** if $A' = A$ and skew-symmetric if $A' = -A$.

Note that a square matrix $A = (a_{ij})$ is symmetric if $a_{ij} = a_{ji}$ and skew symmetric if $a_{ij} = -a_{ji}$, $a_{ii} = 0$

Example: The matrix $A = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 3 & 4 \\ 2 & 4 & 7 \end{bmatrix}$ is symmetric.

and $A = \begin{bmatrix} 0 & 1 & -2 \\ -1 & 0 & -4 \\ 2 & 4 & 0 \end{bmatrix}$ is skew-symmetric.

Definition: The matrix obtained by replacing each element by its conjugate complex number of a given matrix A, is called the conjugate of A and is denoted by $\bar{A}$.

Example: If $A = \begin{bmatrix} 1+i & 1 \\ 3-2i & 5i \end{bmatrix}$ then $\bar{A} = \begin{bmatrix} 1-i & 1 \\ 3+2i & -5i \end{bmatrix}$

Definition: The transpose of a conjugate matrix A is called a tranjugate matrix of A and is denoted by A^*.

Example: If $A = \begin{bmatrix} 1+i & 1 \\ 3-2i & 5i \end{bmatrix}$ then $A^* = \begin{bmatrix} 1-i & 3+2i \\ 1 & -5i \end{bmatrix}$

Definition: A square matrix $A = [a_{ij}]$ is called a Hermitian matrix if $A^* = A$.

Thus $A = (a_{ij})$ is hermitian matrix if $a_{ij} = \bar{a}_{ji}$ $\forall$ i and j. and a_{ii} are real numbers .

Example: $A = \begin{bmatrix} 3 & 3-i & i \\ 3+i & 1 & 5i \\ -i & -5i & 0 \end{bmatrix}$ is Hermitian.

Definition: A square matrix $A = (a_{ij})$ is said to be a skew hermitian matrix if $A^* = -A$ Thus A is skew hermitian if $a_{ii} = -\overline{a_{ji}}$ $\forall$ i, j

and $a_{ii} = 0$ or a_{ii} is purely imaginary .

Example: A= $\begin{bmatrix} i & 2+i & -5+2i \\ -2+i & 0 & 3i \\ 5+2i & 3i & 0 \end{bmatrix}$ is skew-hermitian.

Definition: A square matrix A is called an ***orthogonal matrix***, if $A'A = AA' = I$
Definition: A square matrix A is called a ***unitary matrix*** if $AA^* = A^*A = \mathrm{I}$.

4. Matrix Multiplication: Two matrices A and B are conformable to form the product AB if the number of columns of A (the first matrix) is equal to the number of rows of B .

If $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{n\times p}$ then AB is a matrix of order $m \times p$ given by $AB = C$ where $C = (c_{ij})_{m\times p}$ and $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$

Example: If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$

Then $AB = \begin{pmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{pmatrix}$

Theorem: If A and B are two matrices where AB exists then $(AB)' = B'A'$.

Proof: Let $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{n\times p}$ so that
$A' = (r_{ij})_{n\times m}$, $B' = (s_{ij})_{p\times n}$

where $r_{ij} = a_{ji}$, $s_{ij} = b_{ji}$

Now $AB = (c_{ij})_{m\times p}$ and $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$

$\Rightarrow (AB)' = (x_{ij})_{p\times m}$ where $x_{ij} = c_{ji} = \sum_{k=1}^{n} a_{jk}b_{ki}$ ----------(1)

Also $(B'A') = (y_{ij})_{p\times m}$ where $y_{ij} = \sum_{k=1}^{n} s_{ik}r_{kj}$

But $s_{ik} = b_{ki}$ and $r_{kj} = a_{jk}$

Therefore ,
$y_{ij} = \sum_{k=1}^{n} s_{ik}r_{kj} = \sum_{k=1}^{n} b_{ki}a_{jk} = \sum_{k=1}^{n} a_{jk}b_{ki}$ ----------(2)

From (1) and (2) we conclude $(AB)' = B'A'$.

Theorem 2.01: Matrix multiplication is associative, i.e if A, B, C are three matrices where the products $(AB)C$ and $A(BC)$ exist, then $(AB)C = A(BC)$.

Proof

We take $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{n\times p}$, $C = (c_{ij})_{p\times r}$, $AB = (\alpha_{ij})_{m\times p}$, $BC = (\beta_{ij})_{n\times r}$, $(AB)C = (x_{ij})_{m\times r}$, $A(BC) = (y_{ij})_{m\times r}$

Then by definition we have $\alpha_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$, $\beta_{ij} = \sum_{(k=1)}^{p} b_{ik}c_{kj}$

Now $x_{ij} = \sum_{k=1}^{p} \alpha_{ik}c_{kj} = \sum_{k=1}^{p}(\sum_{s=1}^{n} a_{is}b_{sk})\, c_{kj} = \sum_{k=1}^{p}\sum_{s=1}^{n} a_{is}b_{sk}\, c_{kj}$

$$y_{ij} = \sum_{k=1}^{n} a_{ik}\beta_{kj} = \sum_{k=1}^{n} a_{ik}\left(\sum_{s=1}^{p} b_{ks}c_{sj}\right) = \sum_{k=1}^{n}\sum_{s=1}^{p} a_{ik}b_{ks}c_{sj}$$

$$= \sum_{s=1}^{p}\sum_{k=1}^{n} a_{ik}b_{ks}c_{sj} = x_{ij}$$

Showing that $(AB)C = A(BC)$.

5. **Matrix Inversion:** Let A be a square matrix of order n . Then A is said tobe invertible if there exists another square matrix B of same order such that $AB = BA = I_n$

   The matrix B is called inverse of A then A is the inverse of B and we write $A^{-1} = B$, $B^{-1} = A$.

Example: If $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ then $A^{-1} = \begin{pmatrix} -\frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix}$.

Verify that $AA^{-1} = A^{-1}A = I_2$

Theorem 2.02: (Uniqueness of Inverse): If A is invertible then the inverse is unique .

Proof: Suppose B and C are two inverses of A .

Then $AB = BA = I$ and $AC = CA = I$

Now $B = BI = B(AC) = (BA)C = IC = C$.

Theorem 2.03: If A and B are two invertible matrices of same order then (AB) is also invertible and $(AB)^{-1} = B^{-1}A^{-1}$.

Proof: We have $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$
$\Rightarrow \ (AB)^{-1} = B^{-1}A^{-1}$

Definition*:** Two matrices A and B are said to ***commute if $\boldsymbol{AB = BA}$.

If $\boldsymbol{AB = -BA}$, the matrices A and B are said to ***anti-commute.***

Positive Integral powers of a square matrix

Let A be a square matrix. Then we can write $A^0 = I, A^1 = A, A^2 = AA, A^3 = AAA$.

Similarly, $A^n = AA \ldots \ldots A$ (n −times), and $A^m A^k = A^{m+k}$; $(A^m)^n = A^{mn}$, where m, n and k are any positive integers.

Definition: A square matrix A is said to be **nilpotent** of index n if n is the least positive integer such that $A^n = 0$ (the zero matrix) .

Example: $A = \begin{bmatrix} 0 & 0 \\ 4 & 0 \end{bmatrix}$

$$\Rightarrow A^2 = \begin{bmatrix} 0 & 0 \\ 4 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 4 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

Therefore A is nilpotent of index 2.

Example : $A = \begin{bmatrix} 1 & 1 & 3 \\ 5 & 2 & 6 \\ -2 & -1 & -3 \end{bmatrix}$ is nilpotent of index 3 (verify)

Definition: A square matrix A is said **idempotent** if $A^2 = A$.

Example: Show that the matrix $\begin{bmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{bmatrix}$ is idempotent .

Ans : $A = \begin{bmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{bmatrix}$.

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

$$= \begin{bmatrix} 4+2-4 & -4-6+8 & -8-8+12 \\ -2-3+4 & 2+9-8 & 4+12+4-12 \\ 2+2-3 & -2+6-6 & -4-8+9 \end{bmatrix}$$

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

Therefore the given matrix is an idempotent matrix.

Definition*:** A square matrix ***A such that $A^2 = I$ is called an *Involutory matrix*.

Eg: $A = \begin{bmatrix} -5 & -8 & 0 \\ 3 & 5 & 0 \\ 1 & 2 & -1 \end{bmatrix}$ is involutory.

Example: Show that A is involutory if and only if $(I + A)(I - A) = 0$.

Solution: Let A be an involutory matrix. Then $A^2 = \text{I}$.
$\Rightarrow I - A^2 = 0$

$\Rightarrow I^2 - A^2 = 0$

$\Rightarrow (I + A)(I - A) = 0$

Conversely, if $(I + A)(I - A) = 0$

$\Rightarrow I^2 - IA + AI - A^2 = 0$

$\Rightarrow I - A + A - A^2 = 0$

$\Rightarrow I - A^2 = 0$

Thus, $A^2 = \text{I}$.

Example: If $AB = A$ and $BA = B$, show that A and B are idempotent.
Solution: Given, $AB = A$

$\Rightarrow A(BA) = A \ [\because BA = B]$

$\Rightarrow (AB)A = A$

$\Rightarrow AA = A \ [\because AB = A]$

$\Rightarrow A^2 = A$

$\Rightarrow A$ is idempotent.

Also, $BA = B$

$\Rightarrow B(AB) = B \ [\because AB = A]$

$\Rightarrow (BA)B = B$

$\Rightarrow BB = B \ [\because BA = B]$

$\Rightarrow B^2 = B$

$\Rightarrow B$ is idempotent.

Example: If B is an idempotent matrix, show that $A = I - B$ is also idempotent and that $AB = BA = 0$.

Solution: Since B is an idempotent matrix, $B^2 = B$.

Now, $A^2 = (I - B)^2 = (I - B)(I - B)$

$= I - IB - BI + B^2$

$= I - B - B + B^2 \ [\because IB = BI = B]$

$= I - B - B + B \ [\because B^2 = B.]$

$= I - B \quad [\because -B + B = 0.]$

$= A$

$\Rightarrow A^2 = A$, hence A is idempotent.

Now, $AB = (I - B)B = IB - BB = B - B^2 = B - B = 0.$

Similarly, $BA = B(I - B) = BI - BB = B - B^2 = B - B = 0.$

6. **Elementary Operations/Transformation:** Elementary operations on matrices are a set of three fundamental operations that can be performed without changing the fundamental properties of the matrix.

   The three elementary Rows operations on matrices are

   - **Row Interchang**e: Swap two rows of the matrix.
     The operation when an i^{th} row is interchanged with the i^{th} row will be denoted by
     $R_i \leftrightarrow R_j$

   - **Row Scaling:** Multiply all elements of a row say i^{th} row by a nonzero scalar k will be denoted by
     $R_i \rightarrow kR_i$

- **Row Replacement:** Replacing one row (say i^{th} row) of the matrix with the sum or difference of itself and a multiple of another row say j^{th} row is denoted by
  $R_i \to R_i \pm kR_j$.

The Elementary column operations are similarly defined.

- **Note:** If an elementary operation is applied to the product AB of two matrices. It is applied to the first matrix A only.

Method to find Inverse using elementary operations:

Given a square matrix A ,

We write $A = IA$ ……(1)

Apply a series of elementary operations both side of (1) (keeping in mind that in the right hand side , operations are applicable to the first matrix) until the left hand side becomes identity matrix.

i.e until equation (1) is of the form $I = BA$.

The matrix B is then the inverse of A .

The above steps is also same as these steps below:

Augment the matrix: Form an augmented matrix with the given matrix A on the left and the identity matrix I of the same size on the right. For example, if A is a 3×3 matrix, you form $[A \mid I_3]$.

Perform row operations: Apply a series of elementary row operations to transform the left part of the augmented matrix A into the identity matrix I. These operations are:

- Swapping two rows.
- Multiplying a row by a non-zero scalar.
- Adding or subtracting a multiple of one row to another row.

Achieve the form $[\boldsymbol{I} \mid \boldsymbol{B}]$: Once the left part of the augmented matrix is the identity matrix, the right part of the augmented matrix will be the inverse of A, denoted as A^{-1}.

Example: Find the inverse of the matrix

$$A = \begin{bmatrix} -1 & -3 & 3 & -1 \\ 1 & 1 & -1 & 0 \\ 2 & -5 & 2 & -3 \\ -1 & 1 & 0 & 1 \end{bmatrix}$$

Sol. Let $A = \mathrm{I}A$

$$\Rightarrow \begin{bmatrix} -1 & -3 & 3 & -1 \\ 1 & 1 & -1 & 0 \\ 2 & -5 & 2 & -3 \\ -1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} A$$

Applying $R_2 \to R_2 + R_1, R_3 \to R_3 + 2R_1, R_4 \to R_4 - R_1$, we get

$$\begin{bmatrix} -1 & -3 & 3 & -1 \\ 0 & -2 & 2 & -1 \\ 0 & -11 & 8 & -5 \\ 0 & 4 & -3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix} A$$

Applying $R_2 \to -\frac{1}{2}R_2$ we get

$$\begin{bmatrix} -1 & -3 & 3 & -1 \\ 0 & 1 & -1 & 1/2 \\ 0 & -11 & 8 & -5 \\ 0 & 4 & -3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 0 & 0 \\ 2 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix} A$$

Applying $R_3 \to R_3 + 11R_2, R_4 \to R_4 - 4R_2$ we get

$$\begin{bmatrix} -1 & -3 & 3 & -1 \\ 0 & 1 & -1 & 1/2 \\ 0 & 0 & -3 & 1/2 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1/2 & -1/2 & 0 & 0 \\ -7/2 & -11/2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix} A$$

Applying $R_3 \leftrightarrow R_4$ we get

$$\begin{bmatrix} -1 & -3 & 3 & -1 \\ 0 & 1 & -1 & 1/2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -3 & 1/2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1/2 & -1/2 & 0 & 0 \\ 1 & 2 & 0 & 1 \\ -\frac{7}{2} & -\frac{11}{2} & 1 & 0 \end{bmatrix} A$$

Applying $R_4 \to 2R_4$ we get

$$\begin{bmatrix} -1 & -3 & 3 & -1 \\ 0 & 1 & -1 & 1/2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -6 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1/2 & -1/2 & 0 & 0 \\ 1 & 2 & 0 & 1 \\ -7 & -11 & 2 & 0 \end{bmatrix}$$

Applying $R_4 \to R_4 + 6R_3$, we get

$$\begin{bmatrix} -1 & -3 & 3 & -1 \\ 0 & 1 & -1 & 1/2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1/2 & -1/2 & 0 & 0 \\ 1 & 2 & 0 & 1 \\ -1 & 1 & 2 & 6 \end{bmatrix} A$$

Applying $R_2 \to R_2 + R_3$ we get

$$\begin{bmatrix} -1 & -3 & 3 & -1 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1/2 & 3/2 & 0 & 1 \\ 1 & 2 & 0 & 1 \\ -1 & 1 & 2 & 6 \end{bmatrix} A$$

Applying $R_2 \to R_2 - \frac{1}{2}R_4$ we get

$$\begin{bmatrix} -1 & -3 & 3 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & -1 & -2 \\ 1 & 2 & 0 & 1 \\ -1 & 1 & 2 & 6 \end{bmatrix} A$$

Applying $R_1 \to R_1 + 3R_2$, we get

$$\begin{bmatrix} -1 & 0 & 3 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 3 & -3 & -6 \\ 1 & 1 & -1 & -2 \\ 1 & 2 & 0 & 1 \\ -1 & 1 & 2 & 6 \end{bmatrix} A$$

Applying $R_1 \to R_1 - 3R_3$, we obtain

$$\begin{bmatrix} -1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -3 & -3 & -9 \\ 1 & 1 & -1 & -2 \\ 1 & 2 & 0 & 1 \\ -1 & 1 & 2 & 6 \end{bmatrix} A$$

Applying $R_1 \to R_1 + R_4$

$$\begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -2 & -1 & -3 \\ 1 & 1 & -1 & -2 \\ 1 & 2 & 0 & 1 \\ -1 & 1 & 2 & 6 \end{bmatrix} A$$

Applying $R_1 \to (-1)R_1$ we get

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 1 & 3 \\ 1 & 1 & -1 & -2 \\ 1 & 2 & 0 & 1 \\ -1 & 1 & 2 & 6 \end{bmatrix} A$$

Therefore $A^{-1} = \begin{bmatrix} 0 & 2 & 1 & 3 \\ 1 & 1 & -1 & -2 \\ 1 & 2 & 0 & 1 \\ -1 & 1 & 2 & 6 \end{bmatrix}$

We show below a similar example using the second method mentioned.

Example : Let $A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}$. Calculate A^{-1}

***Ans*:** The augment the matrix with the identity matrix:

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

Divide row 2 by 2 : $R_2 = \frac{R_2}{2}$.

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

Subtract row 2 from row 1 : $R_1 = R_1 - R_2$.

$$\begin{bmatrix} 1 & 0 & -\frac{1}{2} & 1 & -\frac{1}{2} & 0 \\ 0 & 1 & 1 & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

Subtract row 2 from row 3 : $R_3 = R_3 - R_2$.

$$\begin{bmatrix} 1 & 0 & -\frac{1}{2} & 1 & -\frac{1}{2} & 0 \\ 0 & 1 & 1 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{3}{2} & 0 & -\frac{1}{2} & 1 \end{bmatrix}$$

Multiply row 3 by $\frac{2}{3}$: $R_3 = \frac{2R_3}{3}$.

$$\begin{bmatrix} 1 & 0 & -\frac{1}{2} & 1 & -\frac{1}{2} & 0 \\ 0 & 1 & 1_2 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 & 0 & -\frac{1}{3} & \frac{2}{3} \end{bmatrix}$$

Add row 3 multiplied by $\frac{1}{2}$ to row 1 : $R_1 = R_1 + \frac{R_3}{2}$.

$$\begin{bmatrix} 1 & 0 & 0 & 1 & -\frac{2}{3} & \frac{1}{3} \\ 0 & 1 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 & 0 & -\frac{1}{3} & \frac{2}{3} \end{bmatrix}$$

Subtract row 3 multiplied by $\frac{1}{2}$ from row 2 :

$R_2 = R_2 - \frac{R_3}{2}$.

$$\begin{bmatrix} 1 & 0 & 0 & 1 & -\frac{2}{3} & \frac{1}{3} \\ 0 & 1 & 0 & 0 & \frac{2}{3} & -\frac{1}{3} \\ 0 & 0 & 1 & 0 & -\frac{1}{3} & \frac{2}{3} \end{bmatrix}$$

Since we got identity matrix on the left . therefore on the right is the inverse matrix.

i.e $A^{-1} = \begin{bmatrix} 1 & -\frac{2}{3} & \frac{1}{3} \\ 0 & \frac{2}{3} & -\frac{1}{3} \\ 0 & -\frac{1}{3} & \frac{2}{3} \end{bmatrix}$

Determinant of Order 2

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a square matrix of order 2.

The determinant of A (denoted by $\det(A)$ or $|A|$ is defined as

$$|A| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

Minor: Let A be a square matrix . The minor of an entry a_{ij} (denoted by m_{ij}) is the determinant of a sub matrix obtained by deleting the row and column of A containing a_{ij} .

Co-factors: Let A be a square matrix . The co-factor of an entry a_{ij} (denoted by A_{ij}) is defined as $A_{ij} = (-a)^{i+j} m_{ij}$

Determinant of a square matrix: The determinant of a square matrix A is the sum of the products of each entries in any row (or column) with their corresponding co-factors.

Adjoint of a matrix *A*: The adjoint of A is obtained by first replacing each element of A by its cofactor and taking transpose . In other words , the adjhoint of A is the transpose of the matrix B of co-factors of the entries of A .

The adjoint of A is denoted by $adj(A)$

We show an example below with a 3×3 matrix

Let $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$

The cofactors of the entries of A are as follows:

$$\mathrm{A}_{11} = \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix}, A_{12} = -\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix}, A_{13} = \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

$$\mathrm{A}_{21} = -\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix}, A_{22} = \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix}, A_{23} = -\begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{vmatrix}$$

$$\mathrm{A}_{31} = \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}, A_{32} = -\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix}, A_{33} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

$B = \begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix}$ then Adj $(A) = B' = \begin{bmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{bmatrix}$

Proposition: If A is a square matrix and $|A| \neq 0$ then A^{-1} exists and

$$A^{-1} = \frac{adj(A)}{|A|}$$

Example: Calculate $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}^{-1}$ using the adjoint method .

Ans: We have

$$\begin{vmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{vmatrix} = (1)(-1)^{1+1}\begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix} + (0)(-1)^{2+1}\begin{vmatrix} 1 & 0 \\ 1 & 2 \end{vmatrix} +$$

$$(0)(-1)^{3+1}\begin{vmatrix} 1 & 0 \\ 2 & 1 \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix}$$

The determinant of a 2×2 matrix is $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$

$$\begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix} = (2) \cdot (2) - (1) \cdot (1) = 3 \quad \text{i.e} \quad \begin{vmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{vmatrix} = 3$$

The co-factors are given below

$A_{11} = (-1)^{1+1}\begin{vmatrix}2 & 1\\ 1 & 2\end{vmatrix} = 3$, $A_{12} = (-1)^{1+2}\begin{vmatrix}0 & 1\\ 0 & 2\end{vmatrix} = 0$, $A_{13} = (-1)^{1+3}\begin{vmatrix}0 & 2\\ 0 & 1\end{vmatrix} = 0$

$A_{21} = (-1)^{2+1}\begin{vmatrix}1 & 0\\ 1 & 2\end{vmatrix} = -2$, $A_{22} = (-1)^{2+2}\begin{vmatrix}1 & 0\\ 0 & 2\end{vmatrix} = 2$, $A_{23} = (-1)^{2+3}\begin{vmatrix}1 & 1\\ 0 & 1\end{vmatrix} = -1$

$A_{31} = (-1)^{3+1}\begin{vmatrix}1 & 0\\ 2 & 1\end{vmatrix} = 1$, $A_{32} = (-1)^{3+2}\begin{vmatrix}1 & 0\\ 0 & 1\end{vmatrix} = -1$, $A_{33} = (-1)^{3+3}\begin{vmatrix}1 & 1\\ 0 & 2\end{vmatrix} = 2$

Thus, the cofactor matrix is $A = \begin{bmatrix}3 & 0 & 0\\ -2 & 2 & -1\\ 1 & -1 & 2\end{bmatrix}$.

Therefore $Adj(A) = \begin{bmatrix}3 & -2 & 1\\ 0 & 2 & -1\\ 0 & -1 & 2\end{bmatrix}$

The inverse matrix is the adjoint matrix divided by the determinant.

Thus, the inverse matrix is $\begin{bmatrix}1 & -\frac{2}{3} & \frac{1}{3}\\ 0 & \frac{2}{3} & -\frac{1}{3}\\ 0 & -\frac{1}{3} & \frac{2}{3}\end{bmatrix}$.

Trace of a square matrix

Definition: Let A be a square matrix of order n. The sum of the elements of A lying along the principal diagonal is called the ***trace*** of A, written as **tr** A.

Thus, if $= [a_{ij}]_{n\times n}$, then

$$\text{tr A} = \sum_{i=1}^{n} a_{ii} = a_{11} + a_{22} + a_{33} + \cdots + a_{nn}.$$

Some properties of trace of a matrix

Let A and B be the two square matrices of order n and λ be a scalar. Then,

i) tr (λA) = λ tr A
ii) tr (A+B) = tr A + tr B
iii) tr (AB) = tr (BA)

Proof: Let $A = [a_{ij}]_{n\times n}$ and B = $[b_{ji}]_{n\times n}$

i) We have $\lambda A = \left[\lambda\, a_{ij}\right]_{n\times n}$

tr λA = $\sum_{i=1}^{n} \lambda a_{ii}$ = λ $\sum_{i=1}^{n} a_{ii}$ = λ tr A.

ii) A+B = $\left[a_{ij} + b_{ij}\right]_{n\times n}$. Then, tr (A+B) = $\sum_{i=1}^{n}(a_{ii} + b_{ii}) = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii}$ = tr A + tr **B**

iii) AB = $\left[c_{ij}\right]_{n\times n}$ and BA = $\left[d_{ij}\right]_{n\times n}$,where $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$ and $d_{ij} = \sum_{k=1}^{n} b_{ik}\, a_{kj}$

Now, tr (AB) = $\sum_{i=1}^{n} c_{ii}$

= $\sum_{i=1}^{n} (\sum_{k=1}^{n} a_{ik}b_{ki})$

= $\sum_{k=1}^{n} (\sum_{i=1}^{n} a_{ik}b_{ki})$

= $\sum_{k=1}^{n} (\sum_{i=1}^{n} b_{ki}a_{ik})$

= $\sum_{k=1}^{n} d_{kk}$

= $d_{11} + d_{22} + d_{33} + \cdots + d_{nn}$

= tr (BA)

Determinant Rank of a matrix: The rank of a matrix A is the order of the highest order submatrix of A whose determinant is non-zero.

The rank of A is denoted by $r(A)$ or rank(A) .

Result: (i) If A is a rectangular matrix of order $m \times n$ then $r(A) \leq m$, n .
(ii) $rank(A) = rank(A')$

Normal Form: A matrix of the form $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ or $[I_r \quad 0]$ or $\begin{bmatrix} I_r \\ 0 \end{bmatrix}$ is said tobe in normal form, where I_r is the identity matrix of order r .

Echelon Form: A matrix is in row echelon form if it satisfies the following conditions:

- The leading entry in any nonzero row is 1 called the leading 1.
- The leading 1 of any row lies to the right of the leading 1 of the row above it.

- Entries below the leading 1 are all 0's.
- All nonzero rows are above any rows of all zeros.

Example : $A = \begin{bmatrix} 1 & 2 & 4 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ is in echelon form .

Row Rank of a matrix: The row rank of a matrix is the number of non zero rows after reducing to echelon form.

Result: Rank of a matrix A is the order of the identity sub-matrix after reducing to normal form.

Result: Row rank = determinant rank.

Example: Reduce the matrix $A = \begin{bmatrix} 1 & 5 & 1 & 0 \\ 2 & 2 & 5 & 0 \\ 1 & 0 & 4 & 0 \\ 2 & 0 & 8 & 0 \end{bmatrix}$ to normal form and find its rank.

Solution

Subtract row 1 multiplied by 2 from row 2:

$R_2 = R_2 - 2R_1.$

$$\begin{bmatrix} 1 & 5 & 1 & 0 \\ 0 & -8 & 3 & 0 \\ 1 & 0 & 4 & 0 \\ 2 & 0 & 8 & 0 \end{bmatrix}$$

Subtract row 1 from row 3 : $R_3 = R_3 - R_1.$

$$\begin{bmatrix} 1 & 5 & 1 & 0 \\ 0 & -8 & 3 & 0 \\ 0 & -5 & 3 & 0 \\ 2 & 0 & 8 & 0 \end{bmatrix}$$

Subtract row 1 multiplied by 2 from row 4:

$R_4 = R_4 - 2R_1.$

$$\begin{bmatrix} 1 & 5 & 1 & 0 \\ 0 & -8 & 3 & 0 \\ 0 & -5 & 3 & 0 \\ 0 & -10 & 6 & 0 \end{bmatrix}$$

Divide row 2 by -8: $R_2 = -\frac{R_2}{8}$.

$$\begin{bmatrix} 1 & 5 & 1 & 0 \\ 0 & 1 & -\frac{3}{8} & 0 \\ 0 & -5 & 3 & 0 \\ 0 & -10 & 6 & 0 \end{bmatrix}$$

Subtract row 2 multiplied by 5 from row 1:

$R_1 = R_1 - 5R_2$.

$$\begin{bmatrix} 1 & 0 & \frac{23}{8} & 0 \\ 0 & 1 & -\frac{3}{8} & 0 \\ 0 & -5 & 3 & 0 \\ 0 & -10 & 6 & 0 \end{bmatrix}$$

Add row 2 multiplied by 5 to row 3: $R_3 = R_3 + 5R_2$.

$$\begin{bmatrix} 1 & 0 & \frac{23}{8} & 0 \\ 0 & 1 & -\frac{3}{8} & 0 \\ 0 & 0 & \frac{9}{8} & 0 \\ 0 & -10 & 6 & 0 \end{bmatrix}$$

Add row 2 multiplied by 10 to row 4:

$R_4 = R_4 + 10R_2$.

$$\begin{bmatrix} 1 & 0 & \frac{23}{8} & 0 \\ 0 & 1 & -\frac{3}{8} & 0 \\ 0 & 0 & \frac{9}{8} & 0 \\ 0 & 0 & \frac{9}{4} & 0 \end{bmatrix}$$

Multiply row 3 by $\frac{8}{9}$: $R_3 = \frac{8R_3}{9}$.

$$\begin{bmatrix} 1 & 0 & \frac{23}{8} & 0 \\ 0 & 1 & -\frac{3}{8} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{9}{4} & 0 \end{bmatrix}$$

Subtract row 3 multiplied by $\frac{23}{8}$ from row 1:

$R_1 = R_1 - \frac{23R_3}{8}$.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -\frac{3}{8} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{9}{4} & 0 \end{bmatrix}$$

Add row 3 multiplied by $\frac{3}{8}$ to row 2: $R_2 = R_2 + \frac{3R_3}{8}$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{9}{4} & 0 \end{bmatrix}$$

Subtract row 3 multiplied by $\frac{9}{4}$ from row 4:

$R_4 = R_4 - \frac{9R_3}{4}$.

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

Which is in normal form and its rank is 3.

Characateristic polynomial: The characteristic polynomial of a square matrix of order $n \times n$ the polynomial defined as $P(\lambda) = \det(A - \lambda I)$

Characteristic equation: The characteristic equation of a square matrix A whose characteristic polynomial is $p(\lambda)$ is the equation
$p(\lambda) = 0$ or $|A = \lambda I| = 0$

Characteristic Roots or Eigen Values: The roots of characteristic equation are called characteristic roots or eigen values.

Example: Find the characteristic polynomial and characteristic roots of the matrix

$$A = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 2 & 1 \\ -1 & 2 & 2 \end{pmatrix}$$

Solution: The characteristic polynomial is given by

$$p(\lambda) = \det(A - \lambda I)$$

In this example we have:

$$p(\lambda) = \det(A - \lambda I) = \det\left(\begin{bmatrix} 1 & 2 & 2 \\ 0 & 2 & 1 \\ -1 & 2 & 2 \end{bmatrix} - \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix}\right)$$

$$= \begin{vmatrix} 1-\lambda & 2 & 2 \\ 0 & 2-\lambda & 1 \\ -1 & 2 & 2-\lambda \end{vmatrix}$$

$$= (-\lambda + 1)(-\lambda + 2)(-\lambda + 2) + 2 \cdot 1 \cdot (-1) + 2 \cdot 0 \cdot 2 - (-\lambda + 1) \cdot 1 \cdot 2 - 0 \cdot 2 \cdot (-\lambda + 2) - (-1) \cdot (-\lambda + 2) \cdot 2$$

$$= -\lambda^3 + 5\lambda^2 - 8\lambda + 4 + (-2) + 0 - (-2\lambda + 2) - 0 - (2\lambda - 4)$$

$$= -\lambda^3 + 5\lambda^2 - 8\lambda + 4$$

$$= (\lambda - 1)(\lambda^2 - 4\lambda + 4)$$

The characteristics roots are: $1, 2, -2$

Eigen Vector: Let λ be an eigen value of a matrix A . A vector X (row or column) that satisfies the equation $AX = \lambda X$ or $(A - \lambda I)X = 0$ is called an eigen vector corresponding to the eigen value λ .

Example: Find the eigen values and eigen-vectors of matrix

$$A = \begin{bmatrix} 3 & 1 & 4 \\ 0 & 2 & 6 \\ 0 & 0 & 5 \end{bmatrix}$$

Sol. The characteristic equation is $|A - \lambda I| = 0$

$$\Rightarrow \begin{vmatrix} 3-\lambda & 1 & 4 \\ 0 & 2-\lambda & 6 \\ 0 & 0 & 5-\lambda \end{vmatrix} = (3-\lambda)\{(2-\lambda)(5-\lambda)\} - 0 + 0 = 0$$

Now, we consider the relation $(A - \lambda I)X = 0$

For $\lambda = 2$,

$$\begin{bmatrix} 3-2 & 1 & 4 \\ 0 & 2-2 & 6 \\ 0 & 0 & 5-2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = 0 \; X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 1 & 1 & 4 \\ 0 & 0 & 6 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = 0$$

$R_3 \to R_3 - \frac{1}{2} R_2$ on coefficient matrix

$$\begin{bmatrix} 1 & 1 & 4 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = 0$$

$\Rightarrow\ x_1 + x_2 + 4x_3 = 0$ and $x_3 = 0$

Let $x_2 = k$ then $x_1 + k + 0 = 0 \Rightarrow x_1 = -k$

$$\therefore\ X_1 = \begin{bmatrix} -k \\ k \\ 0 \end{bmatrix} = -k \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} \text{ or } \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$$

For $\lambda = 3$, from (i), we get

$$\begin{bmatrix} 0 & 1 & 4 \\ 0 & -1 & 6 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = 0$$

$R_2 \to R_2 + R_1$ on coefficient matrix

$$\begin{bmatrix} 0 & 1 & 4 \\ 0 & 0 & 10 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = 0$$

$R_3 \to R_3 - \frac{1}{5} R_2$

$$\begin{bmatrix} 0 & 1 & 4 \\ 0 & 0 & 10 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = 0$$

$\Rightarrow\quad x_2 + 4x_3 = 0$ and $10x_3 = 0 \Rightarrow x_3 = 0$
$\Rightarrow\quad x_2 + 0 = 0 \Rightarrow x_2 = 0$, let $x_1 = K$

$$\therefore\ X_2 = \begin{bmatrix} k \\ 0 \\ 0 \end{bmatrix} = k \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \text{ or } \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

Again, for $\lambda = 5$, we get

$$\begin{bmatrix} -2 & 1 & 4 \\ 0 & -3 & 6 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Rightarrow \begin{matrix} 2x_1 - x_2 - 4x_3 = 0 \\ 3x_2 - 6x_3 = 0 \end{matrix}$$

$x_3 = k$, then $3x_2 - 6k = 0$ and $2x_1 - 2k - 4k = 0 \Rightarrow x_1 = 3k$

$$\Rightarrow x_2 = 2k$$

$$\therefore X_3 = \begin{bmatrix} 3k \\ 2k \\ k \end{bmatrix} = k \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} \text{ or } \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}$$

Hence the eigen values are $\lambda = 2,3,5$

And eigen vectors are

$$X_1 = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}, X_2 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, X_3 = \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}$$

Cayley-Hamilton Theorem

Let A be an $n \times n$ square matrix, and let $p(\lambda)$ be its characteristic polynomial. The Cayley-Hamilton theorem asserts that if you substitute the matrix A into its own characteristic polynomial, the result is the zero matrix:
$p(A) = 0$

Inverse of a square matrix using by Cayley-Hamilton Theorem.

Example: Find the characteristic equation of the matrix $\begin{bmatrix} 2 & -1 & 1 \\ -1 & 2 & -1 \\ 1 & -2 & 2 \end{bmatrix}$ and also find A^{-1} by Cayley-Hamilton theorem.

Solution: The characteristic equation of A is

$$|A - \lambda I| = \begin{vmatrix} 2-\lambda & -1 & 1 \\ -1 & 2-\lambda & -1 \\ 1 & -2 & 2-\lambda \end{vmatrix} = 0$$

$$\Rightarrow (2-\lambda)[\lambda^2 - 4\lambda + 4 - 2] + [-2 + \lambda + 1] + [2 - 2 + \lambda] = 0$$

$$\Rightarrow \lambda^3 - 6\lambda^2 + 8\lambda - 3 = 0$$

By Cayley-Hamilton theorem $A^3 - 6A^2 + 8A - 3I = 0$.
Multiplying by A^{-1} on both sides, we get

$$A^2 - 6A + 8I - 3A^{-1} = 0$$

$$\Rightarrow A^{-1} = \frac{1}{3}(A^2 - 6A + 8I) \ldots\ldots\ldots\ldots (1)$$

Now $A^2 = A \cdot A = \begin{bmatrix} 2 & -1 & 1 \\ -1 & 2 & -1 \\ 1 & -2 & 2 \end{bmatrix}\begin{bmatrix} 2 & -1 & 1 \\ -1 & 2 & -1 \\ 1 & -2 & 2 \end{bmatrix} = \begin{bmatrix} 6 & -6 & 6 \\ -5 & 7 & -5 \\ 6 & -9 & 7 \end{bmatrix}$

$\therefore\ A^2 - 6A + 8I = \begin{bmatrix} 6 & -6 & 6 \\ -5 & 7 & -5 \\ 6 & -9 & 7 \end{bmatrix} - 6\begin{bmatrix} 2 & -1 & 1 \\ -1 & 2 & -1 \\ 1 & -2 & 2 \end{bmatrix} + \begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{bmatrix} = \begin{bmatrix} 2 & 0 & -1 \\ 1 & 3 & 1 \\ 0 & 3 & 3 \end{bmatrix}$

$(1)\ \Rightarrow\ A^{-1} = \frac{1}{3}\begin{bmatrix} 2 & 0 & -1 \\ 1 & 3 & 1 \\ 0 & 3 & 3 \end{bmatrix}$

Exercises:

1. Find the product AB of the matrices

$$A = \begin{bmatrix} 2 & 4 \\ 3 & 4 \\ 6 & 0 \end{bmatrix}\ ,\ B = \begin{bmatrix} 1 & 0 & 2 \\ 2 & 3 & 0 \\ 0 & 1 & 2 \end{bmatrix}$$

2. Verify that $(AB)' = B'A'$ for the matrices

$$A = \begin{bmatrix} 2 & 1 & -1 \\ 1 & 3 & 0 \\ 0 & 2 & 5 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 & 1 \\ -1 & 2 & 0 \\ 3 & 2 & -4 \end{bmatrix}$$

3. Example 3. Find the inverse of the following matrix employing elementary transformations. Also verify that $(AB)^{-1} = B^{-1}A^{-1}$

$$A = \begin{bmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{bmatrix}\ ,\ B = \begin{bmatrix} 3 & 2 & 4 \\ 2 & 0 & 4 \\ 1 & 1 & 1 \end{bmatrix}$$

4. Using Adjoint , find the inverse of the matrix $\begin{bmatrix} 1 & 2 & -2 \\ -1 & 3 & 0 \\ 0 & -2 & 1 \end{bmatrix}$.

6. Find the rank of

$A = \begin{bmatrix} 6 & 1 & 3 & 8 \\ 16 & 4 & 12 & 15 \\ 5 & 3 & 3 & 8 \\ 4 & 2 & 6 & -1 \end{bmatrix}$ using determint and echelon form and verify tha row rank is same as determinant rank .

7. Find the rank of the following matrix by reducing to normal form:

$$(i)\begin{bmatrix}1 & 2 & -1 & 3\\ 4 & 1 & 2 & 1\\ 3 & -1 & 1 & 2\\ 1 & 2 & 0 & 1\end{bmatrix}. \quad (ii)\begin{bmatrix}0 & 0 & 0 & 0 & 0\\ 0 & 1 & 2 & 3 & 4\\ 0 & 2 & 3 & 4 & 1\\ 0 & 3 & 4 & 1 & 2\end{bmatrix}.$$

8. Find the characteristic roots , eigen values and eigen vectors of the following matrices .

$$(i)\begin{bmatrix}3 & 1 & 4\\ 0 & 2 & 0\\ 0 & 0 & 5\end{bmatrix}. \quad (ii)\begin{bmatrix}1 & 1 & 3\\ 1 & 5 & 1\\ 3 & 1 & 1\end{bmatrix}. \quad (iii)\begin{bmatrix}-1 & 0 & 2\\ 0 & 1 & 2\\ 2 & 2 & 0\end{bmatrix}. \quad (iv)\begin{bmatrix}-9 & 4 & 4\\ -8 & 3 & 4\\ -16 & 8 & 7\end{bmatrix}.$$

Chapter- 3

Groups

Group introduction theory is a branch of abstract algebra that studies mathematical structures known as groups. Groups are fundamental objects in mathematics because they capture the essence of symmetry and can be used to model a wide range of physical, chemical, and mathematical phenomena.

Binary Operation:
Let G be a non empty set**.**
A function $*: G \times G \to G$ is called a binary operation on G.
If $a, b \in G$, we shall denote $*(a, b)$ by $(a * b)$.

Commutative Property: A binary operation $'*'$ on a set G is said tobe commutative if $*(a, b) = *(b, a)$ or $a * b = b * a$ for all $a, b \in G$.

Associative Property: A binary operation $'*'$ on a set G is said tobe associative if $*(a * b, c) = *(a, b * c)$ or $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.

Identity element: Let G be a non empty set and $*$ a binary operation on G .
An element $e \in G$ is called an identity element with respect to $*$ if $a * e = e * a = a \ \forall \ a \in G$.

Inverse of an element: Let G be a non empty set and $*$ a binary operation on G . An element $b \in G$ is called an inverse of another element $a \in G$ with respect to $*$ if $a * b = b * a = e$ (where e is an idenetity element) . Such an element b shall be denoted by a^{-1} .

Eg 1. On the set of integers Z, the usual addition $'+'$ is a function from $Z \times Z$ to Z and hence binary operation on Z with $'0'$ as identity elemenet and $'-a'$ as inverse of an element $a \in Z$.

Eg 2. On the set of integers R, the usual multiplication $'\cdot'$ is a function from $Z \times Z$ to Z and hence binary operation on R with $'1'$ as identity elemenet and $'\frac{1}{a}'$ as inverse of an element $a \in R$, $a \neq 0$.

Definition of Groups

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

The set G together with $'*'$ is called a group denoted by $\langle G, * \rangle$
if the following four conditions known as **group axioms** are satisfied:

- G is closed under $*$, i.e $a, b \in G \Rightarrow a * b \in G$.
- (This is actually implicit with the definition of a binary operation)
- (ii) $*$ is associative i.e $(a * b) * c = a * (b * c) \; \forall \; a, b, c \in G$.
- (iii) There exists an identity element $e \in G$ with respect to $*$.
- (iv) Each element $a \in G$ has inverse in G with respect to $*$.

If further, the binary operation $'*'$ satisfy the commutative property i.e $a * b = b * a$ for all $a, b \in G$, then G is called an **abelian group** or commutative group.

Note: For the sake of simplicity, we shall denote $'a * b'$ by $'ab'$ whenever $'*'$ is multiplication or the like and denote $'a * b'$ by $'a + b'$ when $'*'$ is addition.

Theorem 3.01: Let G be a group and $a, b \in G$. Then

(i) $e^{-1} = e$ i.e the identity element is its own inverse .
(ii) $(a^{-1})^{-1} = a$ i.e 'a' is the inverse of $'a^{-1}'$
(iii) $(ab)^{-1} = (b^{-1}a^{-1})$ i.e the inverse of $'ab'$ is $'b^{-1}a^{-1}'$

We shall skip the proof of (i) and (ii) as they are too obvious .

***Proof* (iii):** We have $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$ by associative law
$= aea^{-1} = aa^{-1} = e$ and
$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$

Thus $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$
By definition of inverse , we have $(ab)^{-1} = (b^{-1}a^{-1})$.

Theorem 3.02: If G is an abelian group then any subgroup of G is also abelian.

Proof: Let H be any subgroup of G
Let $a, b \in H$ then $a, b \in G$ as $H \subset G$
Therefore $ab = ba$ since G is abelian
Hence H is also abelian.

Theorem 3.03: A group G is Abelian if and only if $(ab)^2 = a^2 b^2$ for all $a, b \in G$.

Ans: Let G be abelian

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

Conversely, suppose $(ab)^2 = a^2 b^2$ for all $a, b \in G$ ------(1)

we have $(ab)^2 = (ab)(ab)$

and $(ab)^2 = a^2b^2$ by (1)

therefore $(ab)(ab) = a^2b^2$

Multiplying by a^{-1} from the left and by b^{-1} from the right we have

$a^{-1}(ab)(ab)b^{-1} = a^{-1}a^2b^2b^{-1}$

$\Rightarrow (a^{-1}a)(ba)(bb^{-1}) = (a^{-1}a)(ab)(bb^{-1})$

$\Rightarrow e(ba)e = e(ab)e$

or $ba = ab$ Hence G is abelian.

Eg 3. It is obvious to see that the sets Z, Q, R, C are abelian groups under usual addition and Q^*, R^*, C^* are abelian groups under usual multiplication. (Here Q^* is the set of non zero rational numbers, similarly R^*, C^*)

Eg 4. (**General Linear group** ($GL_2(R)$) Let G be the set of all 2×2 invertible real matrices. Then G is a group under matrix multiplication.

Proof

(i) G is closed since for any two invertible real matrices A, B, the product AB is also an invertible real matrix which hence is in G.

(ii) The associative property holds multiplication of matrices is associative .

(iii) An element $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is an identity element.

(iv) For any $A \in G$, A is invertible real matrix with its inverse A^{-1} is also a 2×2 real invertible matrix.

Thus G is a group. This group is denoted by $GL_2(R)$.

This group G is **non-abelian** as can be seen with the help of these elements below :

$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, $BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, $AB \neq BA$.

Eg 5. (**Special Linear group** $(\boldsymbol{SL_2(R)})$. Let G be the set of all 2×2 real matrices whose determinant is 1. Then G is a group under matrix multiplication .

Brief Justification

(i) For any two elements $A, B \in G$, AB is a 2×2 real matrix.
Also $|A| = |B| = 1$
$\Rightarrow |AB| = |A||B| = 1$
$\Rightarrow AB \in G$
i.e G is closed under matrix multiplication.

(ii) The associative property holds multiplication of matrices is associative .

(iii) An element $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is an identity element .

(iv) For any $A \in G$, since $|A| = 1 \neq 0$. Therefore A is an invertible 2×2 real matrix .

If A^{-1} is the inverse of A then A^{-1} is also a 2×2 real matrix .

Also $|A^{-1}| = \frac{1}{|A|} = 1$ Therefore $A^{-1} \in G$.

Therefore, every element of G has inverse in G .
Thus G is a group. This group is denoted by $\boldsymbol{SL_2(R)}$
This group G is **non-abelian** as can be seen with the help of these elements below :

$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, $BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, $AB \neq BA$.

Eg 6. Let n be a fixed positive integer and Let $Z_n = \{0, 1, 2, \ldots . (n-1)\}$. Z_n is an abelian group under **addition modulo** n denoted by $' +_n '$.

Proof

Recall that $(a +_n b) = r \Leftrightarrow (a + b) \equiv r \, mod \, n \;\; i.e \, nq + r \;\; : \;\; 0 \leq r < n \;\; , r \in Z$.

Thus (i) the closure property holds by definition of addition modulo n .

(ii) $'+_n'$ is associative (property modular addition)

(iii) For any $a \in Z_n$, Since $0 \leq a < n$, it is clear that when $(a + 0)$ is divided by n , the remainder is a . i.e $a+_n 0 = 0+_n a = a$ showing the existence of identity element $'0'$.

(iv) For $a \in Z_n \Rightarrow \ 0 \leq a < n \ \Rightarrow \ 0 \leq (n - a) < n$
and $(a + n - a) = n = (n - a + a)$
$\Rightarrow a+_n(n - a) = (n - a)+_n a = 0$
i.e $(n - a)$ is the inverse of $'a'$.

(v) We also have $(a+_n b) = r$
$\Leftrightarrow a + b = nq + r$ where $0 \leq r < n$
$\Leftrightarrow b + a = nq + r$ where $0 \leq r < n$
$\Leftrightarrow (b+_n a) = r$
i.e $a+_n b = b+_n a$

Hence Z_n is an abelian group.

Eg 7. For a fixed positive integer n , Consider the set G of equivalence class modulo n .

i.e $G = \{ \bar{0} , \bar{1} , \bar{2} , \ldots \ldots \ \overline{n-1} \}$ where $\bar{r}$ is a class of integers that leave remainder r when divided by n .

We define addition of these classes (tobe denoted here by $+_n$) as
$\bar{a}+_n\bar{b} = \overline{a + b} = \bar{r}$ where r is the remainder when $(a + b)$ is divided by n

Then G is an abelian group under this operation.

Justification

We first show that this addition is well- defined.

$If \ \ \bar{a} = \bar{x}$ and $\bar{b} = \bar{y}$

Then $a \equiv x \ (mod\, n)$ and $b \equiv y \ (mod\, n)$ **(see chapter 1, congruence modulo n)**

$\Rightarrow (a + b) \equiv (x + y)(mod\, n)$

$\Rightarrow \overline{a+b} = \overline{x+y}$ i.e $\bar{a}+_n\bar{b} = \bar{x}+_n\bar{y}$

(i) G is closed under $+_n$ Since For any $\bar{a},\ \bar{b} \in G$, if $\bar{a}+_n\bar{b} = \bar{r}$ then r is the remainder when $(a+b)$ is divided by n and as such r is an integer such that $0 \leq r < n$. $\Rightarrow \bar{r} \in G$.

(ii) $'+'_n$ is associative since $\left(\bar{a}+_n\bar{b}\right)+_n\bar{c} = \overline{a+b}+_n\bar{c} = \overline{a+b+c} = \overline{a+(b+c)} = \bar{a}+_n\overline{b+c} = \bar{a}+_n(\bar{b}+_n\bar{c})$.

(iii) $\bar{0} \in G$ is the identity element .

(iv) For $\bar{a} \in G$ we have $0 \leq a < n \Rightarrow\ 0 \leq (n-a) < n$

$\Rightarrow \overline{n-a} \in G$ and $\bar{a}+_n\overline{n-a} = \overline{a+n-a} = \bar{0} = \overline{n-a+a} = \overline{n-a}+_n\bar{a}$ showing that $\overline{n-a}$ is the inverse of $\bar{a}$.

(v) Also $\bar{a}+_n\bar{b} = \overline{a+b} = \overline{b+a} = \bar{b}+_n\bar{a}$

Hence G is an abelian group

Eg 8. Let $Z_n = \{\ 0,1,2,\ldots\ldots(n-1)\}$ and let $U_n = \{\ x \in Z_n : \gcd(x,n) = 1\ \}$.

Then U_n is a group under multiplication modulo n called The **group of units modolo** n .

***Proof* :** Let $a\ , b\ \in U_n\ , a \neq 1\ , b \neq 1$, Then $\gcd(a,n) = \gcd(b,n) = 1$

$\Rightarrow \gcd(ab\ , n\ ) = 1$
If $ab < n$ then remainder when ab is divided by n is ab itself .

$\Rightarrow a * b = ab \in\ U_n$

If $ab > n$

Then $ab = nq + r$ where $0 < r < n$

so that $a * b = r$

Also $\gcd(r,n) = 1$ otherwise if $\gcd(r,n) = d \neq 1$ then $d|r\ \ and\ d|n$

$\Rightarrow d|nq \Rightarrow d|(nq+r) \Rightarrow d|ab$ but $\gcd(ab,n) = 1$

Therefore $a * b = r \in U_n$

Showing that U_n is closed under multiplication mod n .
Associative property holds as multiplication modulo n is associative .
Clearly , the identity element is $1 \in U_n$.
To check the existence of inverse to each element ,

Let $m \in U_n$

Then $\gcd(m, n) = 1$

Therefore there exists integers x , y such that

$mx + ny = 1$ ……(1)

$\Rightarrow mx = 1 - ny$ (either $x > n$ or $x < n$)

In any case we can write

$x = ns + r \ : \ 1 \leq r < n$

Now $mr = m(x - ns) = mx - mns = 1 - ny - mns$

$\Rightarrow m * r = 1$

Also (1) shows that $\gcd(n, r) = 1$

This proves the existence of the inverse of m in U_n

Hence U_n is a group which is abelian as $*$ is commutative .

Eg 9 . The set $Z_p = \{1, 2, 3, \cdots, p - 1\}$ is a group under multiplication modulo p, p being a prime integer.

Ans: Let " $*$ " be multiplication modulo p

i.e $(a * b) = remainder \ when \ ab \ is \ divided \ by \ p$

Let $a, b \ \epsilon G$

As a, b are not divisible by p so ab is not divisible by p

Therefore, if r is a remainder when ab is divided by p then $r \ \epsilon G$
$\boldsymbol{i.e \ a * b \ \epsilon G}$ **so that** $\boldsymbol{G}$ **is closed under** $*$.

The associative property follows as $*$ is associative .

Clearly " 1" is the identity element.

$Let\ a\ \epsilon G$

Then $\gcd(a,p) = 1$

Therefore there exists integers m , n such that

$am + pn = 1$ *(consult number theory book*)

$\Rightarrow am = 1 - pn$ so that remainder when am is divided by p is 1

i.e $a * m = 1$

If $m\ \epsilon G$ then m is the inverse of a

If $m \notin G$.

Let $m = pk + r'$ where $0 < r' < p$ i.e $r'\ \epsilon G$

Now $ar' = a(m - pk) = am - apk = (1 - pn) - apk$

Therefore $a * r' = 1$

In this case r' is the inverse of a

Hence G is a group under $*$.

Eg. 10. Let n be a positive integer and Let $G = \{\, x \in C : x^n = 1 \,\}$.

Then G is an abelian group under usual multiplication .

Proof: (i) $a, b \in G \Rightarrow a^n = b^n = 1 \Rightarrow (ab)^n = a^n b^n = 1$

showing the closure property .

(ii) Associative property follows as $G \subset C$.

(iii) It is clear that 1 is the identity element .

(iv) If $a \in G$ then $a^n = 1 \Rightarrow \left(\frac{1}{a}\right)^n = 1 \Rightarrow \frac{1}{a} \in G$

and $a \cdot \frac{1}{a} = 1$

Therefore $\frac{1}{a}$ is the inverse of a .

(v) Commutative property follows as multiplication of complex numbers is commutative . Hence G is an abelian group .

Definition: A group G is called a finite group if it has a finite number of elements otherwise it is called an infinite group. The number of elements in G is denoted by $\#G$.

Group Tables for Finite Group

Let $G = \{ a_1 , a_2 , a_3 , \dots \dots a_n \}$ be a finite group under $' * '$ having $' n '$ elements with $a_1 = e$.

For $i , j = 1,2, \dots n$. We denote an element $(a_i * a_j)$ by m_{ij}
There will be n^2 such elements m_{ij} (not all are distinct) .

If we let an element $' m_{ij} '$ tobe an entry lying in the $i^{th}\ row$ and $j^{th}\ column$ of an $n \times n$ matrix . Then the group $G, *$ can be represented in a table form .

We show an example of a group table with a group having 4 elements after the next example .

Eg 11. The Klein four-group

Let $G = \{e, a , b , c \}$. We define $' * '$ on G as follows:

(i) $e * x = x * e = x \ \forall \ x \in G$
(ii) $x * x = e \ \forall \ x \in G$
(iii) $a * b = b * a = c \ , \ a * c = c * a = b , b * c = c * b = a$

As there are only four elements , it is easy to verify that G is an abelian group under $*$ with each element being its own inverse.
We can represent this group by a table as follows

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

The particular case of the Klein four group is the group $H = \{e, A, B, C \}$ where

$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} , B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} , C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

We leave to the readers to show that this is a group which follows the pattern of the Klein four group above .

Eg. 12. Let $G = \{ (\cos\theta + i\sin\theta): \ \theta \ \ is\ a\ rational\ number \}$. Show that G is an abelian group under multiplication .

Proof: $Let\ a, b \in G$
Then $a = \cos\theta + i\sin\theta$, $b = \cos\phi + i\sin\phi$ for some rational numbers θ , ϕ

Now $ab = (\cos\theta + i\sin\theta)(\cos\phi + i\sin\phi)$

$= (\cos\theta\cos\phi - \sin\theta\sin\phi) + i(sin\theta\cos\phi + \sin\phi cos\theta)$

$= \cos(\theta + \phi) + i\sin(\theta + \phi) \ \in \ G$

Therefore G is closed
Associative property holds since G is a subset of complex numbers and $multi[lication$ of complex numbers is associative.

The number $1 = \cos 0 + i\sin 0 \ \in G,$ therefore identity element exists in G .

Also for any $a = \cos\theta + i\sin\theta \ \in \ G$, we have θ is rational. Therefore $-\theta$ is also rational

Hence $a' = \cos(-\theta) + i\sin(-\theta) = \cos\theta - i\sin\theta \ \in \ G$

and $a\,a' = a'a = (\cos\theta - i\sin\theta)(\cos\theta + i\sin\theta) = \cos^2\theta + \sin^2\theta = 1$

Hence a' is the inverse of a .

Hence G is a group.

Clearly G is infinite and abelian.

Indices of Elements of a group

Let G be a group under $'*'$ and let $a \in G$. For any integer $n \geq 0$,

we define $(a * a * a \ldots\ldots\ n\ times) = a^n$.

If $'*'$ is addition then

$(a * a * a \ldots . n\ times) = (a + a + a \ldots . . n\ times\ ) = na$

Laws of indices

- **Product of Powers**: For any element g in a group G and any integers m and n

$$g^m * g^n = g^{m+n}$$

Proof **:** $g^m * g^n = (g * g * g \ldots . m\ times\ ) * (g * g * g \ldots . n\ times\ )$
$= (g * g * g \ldots \ldots \ldots . (m+n) times\ )$ using associativity
$= g^{m+n}$

- **Identity Law:** For any element g in a group G,
$g^0 = e$, where e is the identity element of the group.

Proof **:** $g^0 = g^{-1+1} = g^{-1} * g^1 = g^{-1} * g = e$

- **Power of a Power:** For any element $g$in a group G and any integers m and n ,

$$(g^m)^n = g^{mn}$$

The proof of this is purely counting the number times g has to occur and left to the readers.

- **Inverse of a Power:** For any element g in a group G and any integer n,

$$(g^n)^{-1} = g^{-n}$$

i.e g^{-n} is the inverse of g^n .
The proof follows from the previous property.

- **Distributive Law:** For any elements g and h in an abelian group G and any integer n ,
$(gh)^n = g^n h^n$.

Proof : Left to the reader.

These laws of indices can be translated in terms of addition in a usual way.

Cancellation Laws

Let G be a group under $*$ and $a , b , c \in G$. Then

(i) **Right Cancellation Laws** : $a * c = b * c \Rightarrow a = b$

(ii) **Left Cancellation Laws** : $a * b = a * c \Rightarrow b = c$

Proof (i) : As G is a group , $c \in G \Rightarrow c^{-1} \in G$

Now $a * c = b * c \Rightarrow (a * c) * c^{-1} = (b * c) * c^{-1}$

$\Rightarrow a * (c * c^{-1}) = b * (c * c^{-1})$ using associative property .

$\Rightarrow a * e = b * e \Rightarrow a = b$

Proof of (ii) is similar and left out .

Uniqueness of Identity: Let G be a group . The identity element in G is unique .

Proof: Suppose $e \ and \ e'$ are two identity elements .
Since e is an identity element,

we have $e' = e * e'$ -----(1)
Since e' is an identity element
we have $e = e * e'$ ---------(1)
(1) and (2) $\Rightarrow e = e'$

Uniqueness of Inverse: Let G be a group. The the inverse of any element $a \in G$ is unique.

Proof: Suppose $'b'$ and $'b''$ are two inverses of $'a'$.

Then we shall have $a * b = e = a * b'$
By cancellation law, we get $b = b'$ showing that $'a'$ has one and only one inverse .

Theorem 3.04: Let G be a group and $a, b \in G$.
The equations $a * x = b$ and $y * a = b$ have unique solution in G .

Proof: Since $a, b \in G$, $a^{-1} \in G$

Now $a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$
Showing that $x = (a^{-1} * b) \in G$ is a solution of $a * x = b$.
Suppose there is another solution x_0 where $a * x_0 = b$
By cancellation law we shall have

$a * x = a * x_0 \Rightarrow x = x_0$ showing that the solution of $a * x = b$ is unique .

The proof for $y * a = b$ is similar and left as exercise.

Order of group: The order of a finite group[G is the number of elements in G and is denoted by $o(G)$ or $|G|$ or $\#G$ whichever is convenient to use.

Order of Element: Let G be a group and $a \in G$. The order of an element $'a'$ is the least positive integer $'n'$ such that $a^n = e$ ($or\ na = e\ for\ additive\ group$) . If no such n exist , then $'a'$ is said to have infinite order.

Example of finite order elements

1. Let $G = \{e, a, b, c\}$ be the Klein four group.
We have $a \neq e$, $a^2 = e$
Therefore $o(a) = 2$
Similarly $o(b) = o(c) = 2$.

2. Let $G = Z_4 = \{0,1,2,3\}$. Under addition modulo 4 , $e = '0'$ is an identity element .
$o(1) = 4$ since $1 \neq e$, $1^2 = 2 \times 1 = 2 \neq e$, $1^3 = 3 \times 1 = 3 \neq e$ similarly $o(2) = 2$, $o(3) = 4$

Example: Let G be a group such that $o(a) = 2$ for each $a \in G$, $a \neq e$. Then G is abelian .

Alternatively , if G is a group such that $a^2 = e\ \forall\ a \in G$, then G is abelian .

Proof **:** Since $a^2 = e \Rightarrow a = a^{-1}$ for all $a \in G$ …….(1)
Let $x, y \in G$

Then $(xy) = (xy)^{-1}$ by (1)
$= y^{-1}x^{-1} = yx$.

Theorem 3.05: Let G be a group and $a \in G$. If $o(a) = m$ and $a^n = e$ then $m|n$.

Proof **:** Since $o(a) = m$

we have $a^m = e$ and $a^r \neq e$ for $0 < r < m$, $r \in N$. ……(1)

Let $n = mq + r$ where $0 \leq r < m$

Then $e = a^n = a^{mq+r} = a^{mq}a^r = (a^m)^q a^r = ea^r = a^r$

$\Rightarrow a^r = e$

$\Rightarrow r = 0$ otherwise it contradicts (1)

Hence $n = mq$ i.e $m|n$

Theorem 3.06: Let G be a group $a \in G$. Then $o(a) = o(a^{-1})$ finite or infinite.

***Proof* :** We first show that if $'a'$ is of infinite order then so is $'a^{-1}\ '$.

Otherwise , if $o(a^{-1}) = n$ for some $n \in N$ then $a^{-n} = e$.

Now $a^n = (a^{-n})^{-1} = e^{-1} = e$ which shows that $'a'$ must be of finite order .

If order of a is infinite then so is the order of $'a^{-1}\ '$ so that they may be treated as equal.

Supppose $'a'$ and $'a^{-1}\ '$ are of finite order.

Let $o(a) = m$ and $o(a^{-1}) = n$ so that $a^m = (a^{-1})^n = e$ ..(1)

Now $a^n = (a^{-n})^{-1} = e^{-1} = e$ and as $o(a) = m$

$\Rightarrow m|n$ ……(2)

Also $(a^{-1})^m = a^{-m} = (a^m)^{-1} = e^{-1} = e$ and as $o(a^{-1}) = n$

we have $n|m$ …….(3)

From (2) and (3) we deduce that $m = n$.

Cyclic Groups: A cyclic group is a type of group characterized by the property that all its elements can be generated by repeatedly applying the group operation to a single element, known as the generator of the group.

Definition: A group G is called a cyclic group if there exists an element $a \in G$ such that every element in G can be written as a^n for some integer n. The element $'a'$ is called a generator of the group.

Notation: A cyclic group generated by $'a'$ is usually denoted by $\langle a \rangle$.

Order: The order of a finite cyclic group G generated by $'a'$ is the smallest positive integer n such that $a^n = e$ (the identity element)

Note: If $G = \langle a \rangle$ (a cyclic group generated by $'a'$) is infinite then

$a^n = e \Leftrightarrow n = 0$

This is obvious for if $a^n = e$ and $n \neq 0$, n is finite , then G will be a finite cyclic groupof order n .

Theorem 3.07: Every infinite cyclic group has exactly two generator .

***Proof* :** Let G be an infinite cyclic group generated by $'a'$ i.e $G = \langle a \rangle$.
If $'b'$ is another generator then $G = \langle b \rangle$.

As both a and b are generators , there must exist integers m, n such that $a = b^m$, $b = a^n$

Now $a = b^m = (a^n)^m = a^{mn} \Rightarrow a^{mn-1} = e$

$\Rightarrow mn - 1 = 0$ and as m and n are integers

We have $mn = 1 \Rightarrow m = n = 1$ or $m = n = -1$

This show that $b = a$ or $b = a^{-1}$.

Theorem 3.08: Let G be a finite cyclic group of order n . Then every element $a \in G$ of order n generates G . (alternatively , if G is a finite group of order n and if there exists an element $a \in G$ such that $o(a) = n$ then G is cyclic)

***Proof* :** Let $a \in G$, $o(a) = n$

We look at the set $S = \{a, a^2, a^3, \ldots . a^{n-1}, a^n = e = a^0\}$

Then $S \subseteq G$. as $a \in G$.

We shall show that S has n elements .

We only have to show that all elements listed above are distinct .

Suppose If $a^r = a^s$ where $1 \leq r, s \leq n$, $r \neq s$

Then assuming $r > s$ *we have* $\boldsymbol{a^{r-s} = e}$ And since $1 < r, s \leq n$

we have $0 < r - s < n$ a contradiction to the order of a being n

Hence $a^r \neq a^s$ when $r \neq s$

Therefore all elements of S listed in (1) are distinct .

i.e S has n elements which is equal to number of elements of G

As $S \subseteq G$ we conclude $S = G$

Since S is generated by "a" , hence so is G .

Examples

1. The set Z of integers under addition, is an infinite cyclic group with 1 (or -1) as a generator.
2. The multiplicative group of four non-zero complex numbers $\{1, -1, i, -i\}$ is a cyclic group of order 4 generated by $'i'$.

Theorem 3.09: Every cyclic group is abelian.

Proof: Let G be a cyclic group generated by $'a'$.

Let $x, y \in G$. Then $x = a^m$, $y = a^n$ for some integers m , n .

Now $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$.

Theorem 3.10: Every group of prime order is cyclic and hence abelian.
Ans: Let G be a group with $o(G) = p$ where p is a prime .

Let $a \epsilon G$ where $a \neq e$.

If $o(a) = m$ $i.e$ $a^m = e$, $a^r \neq e$ for $0 < r < m$

Consider the cyclic subgroup $H = \{a, a^2, a^3, \ldots\ldots a^{m-1}, a^m = e\}$

If $a^i = a^j$ $where$ $1 \leq i, j \leq m$

Then If $i > j$ we have $a^{i-j} = e$ since $i - j < m$

therefore $i - j = 0$

i.e $a^i = a^j \Rightarrow i = j$

Hence all elements of H listed above are distinct .
Therefore $o(H) = m$

Theorem 3.11: Every group of order 4 is abelian.

proof: Case I- If there exists an element $a \epsilon G$ whose order is 4, then G is cyclic .

Case II- Suppose there does not exists any element of order 4.

Let a be any non identity element of G,

Since $o(a)|4$ therefore $o(a) = 1$ or 2 or 4

Since $a \neq e$ we have $o(a) \neq 1$

also $o(a) \neq 4$ by our assumption .

Hence $o(a) = 2$

Thus $a \in G \Rightarrow a^2 = e$

Also $e^2 = e$

Hence $a^2 = e$ for every element $a \in G$
$\Rightarrow a = a^{-1}$ i.e every element is its own inverse . Hence G is abelian

The Quarternion Group Q_8:

Let $G = \{e, -e, \hat{\imath}, -\hat{\imath}, \hat{\jmath}, -\hat{\jmath}, \hat{k}, -\hat{k}\}$

where $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\hat{\imath} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\hat{\jmath} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\hat{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $i^2 = -1$.

Under simplification by matrix multiplication we have
$ex = xe = x$ for each $x \in G$ So that $'e'$ is an edentity element .

and $\hat{\imath}\hat{\jmath} = -\hat{\jmath}\hat{\imath} = \hat{k}$, $\hat{\jmath}\hat{k} = -\hat{k}\hat{\jmath} = \hat{\imath}$, $\hat{k}\hat{\imath} = -\hat{\imath}\hat{k} = \hat{\jmath}$ …… **(1)**
Showing the closure property.

Again by simplification we have

$$\hat{\imath}(-\hat{\imath}) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} -i^2 & 0 \\ 0 & -i^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e = (-\hat{\jmath})\hat{\imath}$$

$$\hat{\jmath}(-\hat{\jmath}) = (-\hat{\jmath})\hat{\jmath} = \hat{k}(-\hat{k}) = (-\hat{k})\hat{k} = e$$

This proves the existence of inverse of each element in G with $-x$ being the inverse of any $x \in G$.

As multiplication of matrices is associative, The set G becomes a group called **The Quarternion Group Q_8 .**

Again by computation we get

$\hat{\imath}^2 = \hat{\jmath}^2 = (\hat{k})^2 = -e$, $\hat{\imath}^3 = -\hat{\imath}$, $\hat{\jmath}^3 = -\hat{\jmath}$, $\hat{k}^3 = -\hat{k}$, $\hat{\imath}^4 = \hat{\jmath}^4 = (\hat{k})^4 = e$ **…..** **(2)**

The last relation show that each element (other than e) are of **order** 4 .

Taking $x = \hat{\imath}$, $y = \hat{\jmath}$, and suing (1) we have

$G = \{ e, x^2, x, x^3, y, x^2y, xy, yx \}$ which (upon using (1) and (2)) can be represented by $G = \langle x, y \mid x^4 = y^4 = e,\ x^2 = y^2,\ xy = y^{-1}x \rangle$

Exercise

1. Let $S = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in R,\ a \neq 0 \}$. Show that S is an abelian group under matrix multiplication .

2. Let $S = \{1, \omega, \omega^2 : \omega^3 = 1 \}$. Show that S is a group under usual multiplication .

3. Show that the set $M_n(R)$ of $n \times n$ real matrices form a group under addition of matrices .

4. Let $G = R^2 = R \times R$. For two elements $(a, b), (x, y) \in G$ define $\oplus$ by $(a, b) \oplus (x, y) = (a + x, b + y)$. Show that G is a group under $\oplus$.

5. Let G be a group and $a, b \in G$. Show that the equation $y * a = b$ have unique solution in G .

6. Let G be the set of all real valued continuous function on $[0,1]$. For two functions $f, g \in G$, define point wise addition of these functions as $(f + g) = h$ where $h(x) = f(x) + g(x)\ \forall\ x \in [0,1]$. Show that G is a group under this addition.

7. Let G be the set of all bijective functions from $[0,1]$ to itself . Show that G is a group under the composition of functions.

8. Prove that every group of order 4 is abelian.
   ***Hint*:** either G is cyclic or any non identity element is its own inverse.
   $((ab) = (ab)^{-1} = b^{-1}a^{-1} = ba$

9. Give an example of a non abelian group which has an abelian subgroup.
   Hint: Scalar matrices of same order commute with each other.

10. If G is of order m and $a \in G$ then $a^m = e$.

11. If in the group G, $a^5 = e$, $aba^{-1} = b^2$ for some $a, b \in G$, $ind\ o(b)$.

Chapter- 4

Permutations and Symmetries

Permutation: Let S be a non empty set . A bijective (one -one and onto) function $\sigma: S \to S$ is called a permutation on S . A **permutation group** of a set S is a set of permutations of S that forms a group under function composition.
Also if σ is a permutation on S , we shall write σ^2 for $(\sigma \circ \sigma)$ and so on.

In this chapter, we shall be concentrating on some features of permutation groups of a a finite set S having a certain number of elements .

The Symmetric Group S_n

Let S be the set of n symbols . For simplicity we take $S = \{1,2,3, \ldots\ldots\ldots n\}$
Let S_n be the set of all bijective functions permutations on S .
The fact that

(i) Compostion of bijective functions is a bijective function .
(ii) Composition of functions is associative .
(iii) The identity function $I(x) = x \ \forall\, x \in S$ is bijective .
(iv) Inverse function of a bijective function exists and is itself bijective.

Make S_n into a group under composition of functions (or multiplication of permutations) called the **symmetric group of degree n** . Also S_n has $n!$ elements .

Two lines representation of permutations

Consider the set $S = \{1,2,3,4, \ldots . \ n\}$ having n elements.
Let S_n be the set of all permutations on S . If $\sigma \in S_n$ then σ can be represented in a matrix of order $2 \times n$ where the first row consists of elements of S and the second consists of images under σ.

i.e $\sigma = \begin{pmatrix} 1 & 2 & \ldots\ldots & n \\ \sigma(1) & \sigma(2) & \ldots\ldots & \sigma(n) \end{pmatrix}$

Cyclic Permutation / Cycle

Let $S = \{x_1, x_2, \dots\dots\dots, x_n\}$ be the set of n symbols and $f: S \to S$ be a permutation on S.

Then f is called an n- cycle if $f(x_i) = x_{i+1}$, $f(x_n) = x_1$. (each x_i are distinct)

i.e $f = \begin{pmatrix} x_1 & x_2 \dots\dots\dots & x_n \\ x_2 & x_3 \dots\dots\dots & x_1 \end{pmatrix}$

Such permutation shall be denoted by $f = (x_1\ x_2\ x_3\ \dots\dots\ x_n)$

It should be noted that

$$(\boldsymbol{x_1\ x_2\ x_3 \dots\dots x_n}) = (\boldsymbol{x_2\ x_3\ x_4 \dots\dots x_n\ x_1}) = (\boldsymbol{x_3\ x_4\ \dots\dots x_n\ x_1\ x_2})$$

Inverse of a cycle

If $\sigma = (x_1\ x_2\ x_3 \dots\dots x_n)$ then $\sigma^{-1} = (x_1, x_n, x_{n-1} \dots\dots x_3\ x_2)$
This can be seen by directly checking all the images and inverse images.

Fixed element of a permutation

An element which has itself as an image under a permutation is called a fixed element.

Eg.1. In S_3, in the permutation $\phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, an element 1 is the fixed element.

Note : Fixed element can be omitted in permutation representation

Eg. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} = (2\ \ 3\ ) = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\boldsymbol{Def^n}$: The length of a cyclic permutation is the number of elements permutes by the permutation . If $\sigma = (x_1\ \ x_2\ x_3\ \dots\dots\ \ x_n)$ then σ is a cycle of length n .

$\boldsymbol{Def^n}$: A cycle of length 2 is called a transposition.
A transposition is always of the form $\sigma = (a\ b)$ which is its own inverse .

i.e $\sigma^{-1} = (a\ b)$

$\boldsymbol{Def^n}$: Two cycles are said tobe disjoint if the set of elements permute by the two cycles permutations are disjoint .

Eg. Let $f = (x_1, x_2, \ldots \ldots x_r)$, $g = (y_1, y_2, \ldots . y_s)$ be two cyclic permutations on a non-empty set S . Then f and g are said tobe **disjoint** if

$\{x_1, x_2, \ldots \ldots . x_r\} \cap \{y_1, y_2, \ldots . y_s\} = \phi$ (ϕ is an empty set .)

Composition of two permutations: **Quick Simplification**

If f and g are two permutations, to simplify $(f \circ g)$, (keep in mind that $(f \circ g)(x) = f\big(g(x)\big)$)

We demonstrate this with the help of a concrete example below.

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ be two permutations on $S = \{1,2,3,4\}$

To calculate $(f \circ g$, we first list all elements of the set in the first row, keeping the second row unoccupied.

(1 2 3 4)

Next To find the image of $'1'$ under $(f \circ g)$, we first find the image of $'1'$ under g which is $'3'$ then find the image of $'3'$ under f which is $'1'$.
We can proceed this way to each elements of the set to get

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 \\ 4 & 2 & 3 \end{pmatrix} = (2 \quad 4 \quad 3)$$

The Symmetric Group of degree 3 : S_3

Let S={1,2,3 }

Let $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\phi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)$, $\phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$,

$\phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$, $\chi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$, $\omega = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2)$

be the six permutations on S.

It is clear that e is the identity element of S_3

We have , $\phi_3^2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = e$

Similarly $\phi_1^2 = {\phi_2}^2 = e = {\phi_3}^2$ ..... (1)

$\chi^2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \omega$ ..... (2)

Similarly $\omega^2 = \chi$ ..... (3)

and $\chi^3 = \chi\chi\chi = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = e$

Similarly $\omega^3 = e = \chi^3$ ..... (4)

Also we can see that
$\chi\omega = (1,2,3)(1,3,2) = e = (1,3,2)(1,2,3) = \omega\chi$ ..... (5)

Equation (1) shows that $\boldsymbol{\phi_1}$, $\boldsymbol{\phi_2}$, $\boldsymbol{\phi_3}$ each are their own inverse (since $a^2 = e \Rightarrow aa = e \Rightarrow a = a^{-1}$)

Equation (4) shows that $\boldsymbol{\chi}$ and $\boldsymbol{\omega}$ are inverse to each other .

Also equation (1) shows that $\boldsymbol{\phi_1}$, $\boldsymbol{\phi_2}$, $\boldsymbol{\phi_3}$ are each of order 2 and equation (2) shows that χ and ω are of order 3**.**

Of course $\boldsymbol{e}$ is of order 1 being the identity element.

By calculation we also have

$\phi_1\phi_2 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \chi$

$\phi_2\phi_1 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \omega$

$\phi_2\phi_3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \chi$

$$\phi_3\phi_2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \omega$$

$$\phi_1\phi_3 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \omega$$

$$\phi_3\phi_1 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \chi$$

The above two equations show that S_3 is non-abelian (The smallest non-abelian group in the sense that any group of lower order) are always abelian .

We present below the group table of S_3

$\circ$	$\boldsymbol{e}$	$\boldsymbol{\phi_1}$	$\boldsymbol{\phi_2}$	$\boldsymbol{\phi_3}$	$\boldsymbol{\chi}$	$\boldsymbol{\omega}$
$\boldsymbol{e}$	e	ϕ_1	ϕ_2	ϕ_3	χ	ω
$\boldsymbol{\phi_1}$	ϕ_1	e	χ	ω	ϕ_2	ϕ_3
$\boldsymbol{\phi_2}$	ϕ_2	ω	e	χ	ϕ_3	ϕ_1
$\boldsymbol{\phi_3}$	ϕ_3	χ	ω	e	ϕ_1	ϕ_2
$\boldsymbol{\chi}$	χ	ϕ_3	ϕ_1	ϕ_2	ω	e
$\boldsymbol{\omega}$	ω	ϕ_2	ϕ_3	ϕ_1	e	χ

Theorem 4.01: Disjoint Cycles Commute with each other.

***Proof* :** Let f and g be two disjoint cycles on a non empty set S .

Let A be the set of elements of S permutes by f and

Let B be the set of elements of S permutes by G .

As f and g are disjoint , we have $A \cap B = \phi$ (an empty set)

Also $f(x) = x$ if $x \notin A$ and $g(x) = x$ if $x \notin B$.

To show that $f \circ g = g \circ f$, we take any element $x \in S$ and show that

$(f \circ g)(x) = (g \circ f)(x)$

Let $x \in S$

Case (i): $x \notin A$, $x \notin B$

In this case $(f \circ g)(x) = f\big(g(x)\big) = f(x) = x$ and $(g \circ f)(x) = g\big(f(x)\big) = g(x) = x$

Case (ii): $x \in A$

If $x \in A$ then $f(x) \in A$ and $x \notin B \Rightarrow g(x) = x$

Now $(f \circ g)(x) = f\big(g(x)\big) = f(x)$ and $(g \circ f)(x) = g\big(f(x)\big) = f(x)$ as $f(x) \in A$ and g do nothing to elements of A .

Case (iii): $x \in B$

If $x \in B$ then $g(x) \in B$ and $x \notin A \Rightarrow f(x) = x$
Now $(f \circ g)(x) = f\big(g(x)\big) = g(x)$ as $g(x) \in B$ and f do nothing to elements of B . and $(g \circ f)(x) = g\big(f(x)\big) = g(x)$

Thus in each case we have , $(f \circ g)(x) = (g \circ f)(x)$
Therefore $f \circ g = g \circ f$

Definition: Let $x \in \{1,2,\dots,n\}$ and $\sigma \in S_n$. The orbit of x under σ, written orb (x), is orb $(x) = \{\sigma^m(x) : m \in \mathbb{Z}\}$

It should be seen that orb (x) is a finite set because it is a subset of $\{1,\dots,n\}$.

Proposition 1: Let $x \in \{1,\dots,n\}$ and $\sigma \in S_n$. Then there is a whole number $r > 0$ such that $\sigma^r(x) = x$.

Proof: The elements $\sigma^m(x)$ for $m = 0,1,2,\dots$ can't all be different, so there must exist $i < j$ such that $\sigma^i(x) = \sigma^j(x)$. Then $\sigma^{-i}\sigma^i(x) = \sigma^{-i}\sigma^j(x)$, so $x = \sigma^{j-i}(x)$ and we can take $r = j - i$.

Theorem 4.02: Let σ be a permutation of X. If k is the smallest strictly positive integer such that $\sigma^k(x) = x$, then the elements of $S = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{k-1}(x)\}$ are all distinct. Furthermore , $\sigma^m(x) = x$ for any multiple m of k and $\sigma^n(x) \in S$ for any integer n .

***Proof* :** Suppose $\sigma^r(x) = \sigma^s(x)$, where $0 \le r \le s < k$. Apply σ^{-r} to both sides to get

$x = \sigma^{s-r}(x)$. But $0 \le s - r < k$, so by the the assumption on k,

we have $s - r = 0$ or $s = r$. ***This proves the first part.***

That $\sigma^m(x) = x$ for any multiple m of k is obvious.

To show that $\sigma^n(x) \in S$, we take $n = kq + r$ where $0 \leq r < k$

Therefore $\sigma^n(x) = \sigma^{r+kq}(x) = \sigma^r\left(\sigma^{kq}(x)\right) = \sigma^r(x) \in S$

Theorem 4.03: Every permutation on a finite set can be written as a cycle or as a product of disjoint cycles and the cycles that appear in any such expression of a given permutation are the same, up to order.

Proof **:** Let σ be a permutation and let S be the set of elements permutes by σ. We assume that S has n elements.

Choose any element x_1 of S.

After it, write $\sigma(x_1)$. After that, write $\sigma(\sigma(x_1)) = \sigma^2(x_1)$, and continue until $\sigma^k(x_1) = x_1$.

The last element written is $\sigma^{k-1}(x_1)$. Write the result as a k-cycle:

$\sigma_1 = (x_1 \quad \sigma(x_1) \quad \sigma^2(x_1) \ldots\ldots\ldots \quad \sigma^{k-1}(x_1))$

After this, choose an element $x_2 \in$ S that is not in

$S_1 = \{x_1, \quad \sigma(x_1), \quad \sigma^2(x_1), \ldots\ldots\ldots \quad \sigma^{k-1}(x_1)\}$ and repeat.

Write the corresponding cycle $\sigma_2 = (x_2 \quad \sigma(x_2) \quad \sigma^2(x_2) \ldots\ldots\ldots \quad \sigma^{p-1}(x_2))$ after the one previously written.

We now show that σ_1 and σ_2 are disjoint.

i.e $S_1 = \{x_1, \quad \sigma(x_1), \quad \sigma^2(x_1), \ldots\ldots\ldots \quad \sigma^{k-1}(x_1)$ and $S_2 = \{x_2, \quad \sigma(x_2), \quad \sigma^2(x_2), \ldots\ldots\ldots \quad \sigma^{p-1}(x_2)\}$ are disjoint .

We already have $x_2 \notin S_1$ **……** **(1)**

We first show that $x_1 \notin S_2$.

If $x_1 \in S_2$ Then $x_1 = \sigma^t(x_2) : 1 \leq t \leq p$

Now $x_2 = \sigma^p(x_2) = \sigma^{p-t}\left(\sigma^t(x_2)\right) = \sigma^{p-t}(x_1) \in S_1$ using the previous theorem.

This contradicts that $x_2 \notin S_1$

Hence $x_1 \notin S_2$ …….. **(2)**

We now show that S_1 and S_2 have no common elements.

Any element of S_1 is of the form $\sigma^i(x_1)$ and any element of S_2 is of the form $\sigma^j(x_2)$.

If $\sigma^i(x_1) = \sigma^j(x_2)$ ……..(2)

Then (i) $i = j \Rightarrow x_1 = x_2$ which contradicts both (1) and (2)

(ii) $i < j \Rightarrow x_1 = \sigma^{j-i}(x_2) \in S_2$ which contradicts (2)

(iii) $i > j \Rightarrow x_2 = \sigma^{i-j}(x_1) \in S_1$ which contradicts (1)

Hence $\sigma^i(x_1) \neq \sigma^j(x_2)$

i.e S_1 and S_2 are disjoint.

We Continue choosing previously unused elements and writing out the cycles they traverse until every element of S has been taken to get a series of cycles $\sigma_1, \sigma_2, \sigma_3 \ldots \ldots \sigma_m$.

To show that

$\sigma = \sigma_1\sigma_2\,\sigma_3 \ldots \ldots \sigma_m$.

We note that each σ_i in the R.H.S are disjoint and that each $x \in S$ have been taken in the above process . Also since σ_i are defined interms of σ , this established that

$\sigma = \sigma_1\sigma_2\,\sigma_3 \ldots \ldots \sigma_m$.

To prove the **uniqueness of such decomposition**.

Suppose $\sigma_1\sigma_2\,\sigma_3 \ldots \ldots \sigma_m = \tau_1\tau_2 \ldots \ldots \tau_p$. …….. **(3)**

We shall show that σ_1 is equal to one and only one $\tau's$.

It is clear that there exist t : $1 \leq t \leq p$ and σ_1 and τ_t are not disjoint .

We let $\sigma_1 = (x_1, x_2 \ldots\ldots)$ where $x_2 = \sigma(x_1) \ldots$

Since any element of a cycle can be moved up to the initial position if need be and σ_1 and τ_t are not disjoint .

Then there exists y_1 where $\tau_t = (y_1, y_2 \ldots\ldots)$ and $x_1 = y_1$.

But $y_2 = \sigma(y_1) = \sigma(x_1) = x_2$

Continuing this way we can deduce that $\sigma_1 = \tau_t$.

and since each τ_s are disjoint , can only have one $'t'$ where $\sigma_1 = \tau_t$.

We can proceed in the same way to establish the correspondence between the remaining $\sigma_{,s}$ with the remaining $\tau's$.

Theorem 4.04: The order of a permutation of a finite set written in as a product of disjoint cycles is the least common multiple of the lengths of the cycles**.**

Proof. Let σ be a permutation and let $\sigma = \tau_1\tau_2 \ldots \tau_l$ be the decomposition of σ into disjoint cycles of lengths of length $k_1, k_2, \ldots, k_l$.

Let the order of σ be k .
As $\tau_1, \tau_2, \ldots, \tau_l$ are disjoint, it follows that

$\sigma^k = \tau_1^k\tau_2^k \ldots \tau_l^k$

But the RHS is equal to the identity, if and only if each individual term is equal to the identity.

It follows that $\tau_i^k = e$ and as $o(\tau_i) = k_i$

We have k_i divides k. Thus the least common multiple, m of $k_1, k_2, \ldots, k_l$ divides k.

But $\sigma^m = \tau_1^m\tau_2^m\tau_3^m \ldots \tau_l^m = e$ and $o(\sigma) = k$, Thus k divides m and so $k = m$.

Eg: (a) If $\sigma = (1\ 2\ )$ then order of σ is 2
(b) If $\psi = (1\ 2\ )(\ 3\ 4\ 5\ )$ then Order of ψ , $o(\psi) = \text{LCM}(2,3) = 6$

Theorem 4.05: Every permutation in $S_n, n > 1$, is a product of 2-cycles.

Proof: First, note that the identity can be expressed as $(1\ 2)(1\ 2)$, and so it is a product of 2-cycles. We know that every permutation can be written in the form

$\sigma = \tau_1\tau_2 \ldots \tau_k$ **.....** **(1)**

Suppose $\tau_r = (a_1\ a_2\ a_3 \quad a_r)$

It is easy to verify that $\tau_r = (a_1\ a_r)(a_1\ a_{r-1}) \ldots \ldots (a_1\ a_2)$

Proceeding this to each r in (1) completes the proof for the first part .

Theorem 4.06: A cycle of length k can be written as a product of $(k-1)$ transpositions.

i.e a cycle of even length is odd and a cycle of odd length is even .

Proof: Suppose $\tau_r = (a_1\ a_2\ a_3 \quad a_r)$

It is easy to verify that $\tau_r = (a_1\ a_r)(a_1\ a_{r-1}) \ldots \ldots (a_1\ a_2)$

Theorem 4.07: If $\sigma = \tau_1\tau_2 \ldots \tau_k$ where τ_r are transposition, then $\sigma^{-1} = \tau_k\tau_{k-1} \ldots . \tau_2\tau_1$.

The proof follows by direct computation since transposition is inverse to itself.

Definition: Even and Odd Permutations

A permutation that can be expressed as a product of an even number of 2-cycles is called an even permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an odd permutation.

Lemma: The identity permutation is even and not odd.
The proof of this is beyond the scope of this book. Consult advanced algebra books.

Theorem 4.08: Every permutation in S_n $(n > 1)$ is either even or odd, but not both.

Proof : Let σ be a permutation in S_n.
Let $\sigma = \sigma_1\sigma_2 \ldots . . \sigma_m = \tau_1\tau_2 \ldots . . \tau_k$

where σ_r , τ_r are transposition .

Suppose one of m *or* k is even and the other is odd .

By the previous theorem , we have $\sigma^{-1} = \sigma_m \sigma_{m-1} \ldots\ldots \sigma_2 \sigma_1$

$\Rightarrow I = \sigma^{-1}\sigma = \sigma_m \sigma_{m-1} \ldots\ldots \sigma_2 \sigma_1 \ \tau_1 \tau_2 \ldots\ldots \tau_k$ an odd permutation.

This is not possible using the above Lemma.

Hence both m and k must be even or odd.

Theorem 4.09: Let $\sigma , \tau \in S_n$. Then

(i) $\sigma\tau$ is even if σ and τ are both even or both odd.
(ii) $\sigma\tau$ is odd if one of σ and τ is even and the other is odd .

Proof: Let $\sigma = \sigma_1 \sigma_2 \ldots\ldots \sigma_m$ and $\tau = \tau_1 \tau_2 \ldots\ldots \tau_k$
where σ is expressded as the product of m transpositions and τ is expressded as the product of k transpositions .

Then $\sigma\tau = \sigma_1 \sigma_2 \ldots\ldots \sigma_m \tau_1 \tau_2 \ldots\ldots \tau_k$ is the product of $(m + k)$ transpositions which is even if m and k are both even or odd. and $(m + k)$ is odd if one of m and k is even and the other is odd

Theorem 4.10: The inverse of an even permutation is an even permutation.

***Proof* :** If P be an even permutation and P^{-1} be its inverse, then $PP^{-1} = I$, the identity permutation.

But P and I are even so P^{-1} is also even.

Theorem 4.11: The inverse of an odd permutation is an odd permutation.
Proof-: If P be an odd permutation and P^{-1} be its inverse, then $PP^{-1} = I$, the identity permutation.

But P is odd and I is even.

so P^{-1} is also odd.

The Alternating group- A_n: The set of even permutations in S_n is a group , called the Alternating group of degree n and is denoted by A_n.

***Proof* :** If $\sigma , \tau \in A_n$ then σ , τ are even permutations.

$\Rightarrow \tau^{-1}$ is also an even permutation.

$\Rightarrow \sigma\tau^{-1}$ is an even permutation (product of even permutations is even)

$\Rightarrow \sigma\tau^{-1} \in A_n$

Hence A_n is a group.

Example: The Alternating group of degree 3, A_3.

We know that an identity element and a cycle of odd length is even .

Thus $A_3 = \{ e, \ \chi = (1\ 2\ 3), \ \omega = (1\ 3\ 2) \}$

Introduction to symmetries

Symmetry in mathematics refers to a situation where a shape or object remains invariant under certain transformations, such as rotation, reflection, translation, or scaling.

We state below three types of symmetries that are of interest in pages to follow.

Reflective Symmetry (Mirror Symmetry): Reflective symmetry occurs when an object can be divided into two parts that are mirror images of each other. The dividing line or plane is called the line or plane of symmetry.

For example, in a circle , any diameter will divide the circle into two halves, one of which is the mirror image of the other.

Another example, a square has four lines of symmetry namely the two diagonals and the two lines bisecting the opposite sides.

Rotational Symmetry: An object has rotational symmetry if it can be rotated (less than 360 degrees) around a central point and still look the same.

Example: A regular pentagon has rotational symmetry of order 5, as it looks the same after rotations of 72°, 144°, 216°, and 288°.

Translational Symmetry: An object has translational symmetry if it can be shifted (translated) by a certain distance in a certain direction and still look the same.

Footprints are a great example of translational symmetry because they are asymmetrical figures that repeat in different locations. The symmetry occurs

because one footstep is identical to another while positioned at different spots from the previous ones. Remember that symmetry does not have to be on the figure or object itself.

Symmetries of the square

The symmetries of a square Rotation and reflection transformation. Consider the square ADCD and the 8 transformations given below:

Rotations

1. **Identity rotation (0°):** This leaves the square unchanged.
2. **90° rotation:** Rotates the square 90 degrees counter - clockwise.
3. **180° rotation:** Rotates the square 180 degrees counter - clockwise.
4. **270° rotation:** Rotates the square 270 degrees counter - clockwise .

Reflections

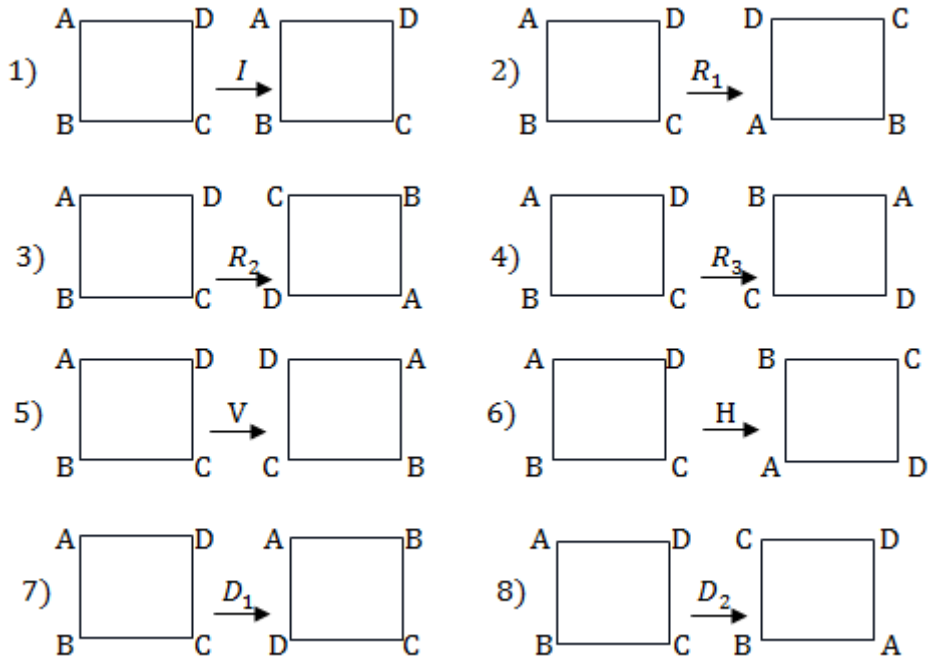
5. **Reflection over a vertical line:** This line goes through the midpoints of the left and right sides of the square.
6. **Reflection over a horizontal line:** This line goes through the midpoints of the top and bottom sides of the square.
7. **Reflection over the main diagonal:** This diagonal goes from the top-left corner to the bottom-right corner.

Reflection over the second diagonal: This diagonal goes from the top-right corner to the bottom-left corner.

We shall denoted the above transformations as follows:

(1) Identity rotation- I
(2) 90° rotation - R_1
(3) 180° rotation - R_2
(4) 270° rotation – R_3
(5) Reflection over a vertical line – V
(6) Reflection over a horizontal line - H
(7) Reflection over the main diagonal-D_1
(8) Reflection over the second diagonal - D_2

The effect of these transformations on a square is given below.

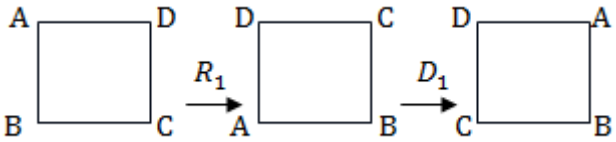


We can view these 8 motions as functions on the orientations of the square region to itself .

We now show a few examples that the combination of two of these actions is equivalent to one of the 8 actions .

We shall (in a natural way of functions composition) view an action g followed by an action f as $(f \circ g)$.

(i) If we "rotate the square anti-clockwise by 90° "and follow by" reflection over the main diagonal" we are actually applying the composition $(D_1 \circ R_1)$ on the square . We show below the final effect of the combination of these two actions:



We can see that these two actions combine, result the same as R_3 which is the rotation of $270°$. We leave to the readers to verify that any such combinations results to one of the 8 mentioned actions.

We also note that if we rotate the square $90°$ and then rotate again $270°$ and vice versa (both anti-clockwise) , the square will be in the original position.

i.e $(R_3 \circ R_1) = (R_1 \circ R_3) = I$ This shows that $R_1$and R_3 are inverse to each other.

We leave to the readers to verify that each of the above functions possesses inverses.

Also since $(f \circ g)$ is the result when $'g\ acts\ first"$ and $"f\ second"$, the associative property for the above functions is clearly satisfy .

With all the above discussion then we can now conclude that the set $D_4 = \{ I , R_1 , R_2 , R_3, V , H, D_1, D_2 \}$ forms a group under composition of functions . This group is called the **Dihedral group of order 8** and is denoted by D_4 .

It is tobe noted that the notation $'D_4'$ is abbreviated to " the dihedral group originated from the square which has 4 equal sides "

Dihedral group: With the above discussion about the the symmetries of a square**,** we can generalize to the symmetries of any regular $n-$gon like equilateral triangles, regular pentagon , regular hexagon and so on . The symmetries on these figures will form a group under composition of functions . For symmetries of a regular n-gon, we shall call the group, " The Dihedral group D_n"of order $2n$.

Exercise:

1. Write the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ in cycle notation.

2. Write the following cycles as the product of disjoint cycles.
   (i) (1 2 4 3 5)(4 5 6) (ii) (1 3 2 5 6)(2 3)(4 6 5 1 2)

3. Verify that composition of permutations is associative by showing $(\sigma\tau)\rho = \sigma(\tau\rho)$ for some permutations σ, τ, and ρ.

4. Find the inverse of the permutation $\sigma = (135)(24)$.
   Verify that $\sigma \cdot \sigma^{-1} = \mathrm{id}$.

5. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$

(i) Compute $\sigma\tau$, $\tau\sigma$, σ^{-1} , τ^{-1}
(ii) Express σ , τ as cycles or product of didsjoint cycles.

6. Let $\sigma = (1\ 3\ 2\ 5\ 7\ 6\ 4)$. Find σ^{-1} . Express σ and σ^{-1} as the product of transpositions.

7. Find the order of the following cycles.
(i) $(1\ 2)(1\ 3\ 4)(1\ 5\ 2)$ (ii) $(1\ 2\ 4)(3\ 5\ 7\ 8\ 6\ 9)$ (iii) $(a_1\ a_2\ a_3\ a_4)$

8. Determine whether the following permutations are even or odd .
(i) $(1\ 2\ 4\ 3)(3\ 5\ 2\ 1)$ (ii) $(1\ 3\ 2\ 5\ 6\ 4)$ (iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$

9. Construct the group table for
(a) The Dihedral group D_3 . (b) The Dihedral group D_4.

Also find all subgroups of both the groups.

10.1Prove or disprove the statements below.
(a) The Dihedral group D_3 is abelian.
(b) The Dihedral group D_4 is abelian

Chapter- 5

Subgroups and Cosets

Introduction

In mathematics, particularly in group theory, a subgroup is a subset of a group that is itself a group under the same operation or simply saying , " a subgroup is a group within a group. To qualify as a subgroup, a subset must satisfy the group axioms (closure, associativity, identity, and invertibility). We shall start the chapter with the formal definition of a subgroup .

Definition: A subset H of a group G which is itself a group under the operation of G, is called a subgroup of G . If H is a subgroup of G we shall denote as $H \leq G$.

Example: Consider the group Z of integers under addition and let $2Z$ be the set of even integers (which is obviously a subset of Z).

In $2Z$, the closure property under $'+'$is satisfied as the sum of even integers is even.

The associative property inherits from the whole set Z .

An element $'0'$ being even , is in $2Z$.

Fininally , that the negative of any even integer is an even integer , proves the existence of inverse.

These lines above shows that $2Z$ is a group by itself which is of course abelian.

As $2Z$ is a subset of Z , it is called a subgroup of Z .

Instead of verifying all the group axioms, it would be better if a fewer conditions is verified if those conditions are strong enough tobe equivalent to all the four group axioms.

We shall state below the theorem that would allow us to quickly determine if a subset is or is not a subgroup.

Theorem 5.01: (Subgroup Test) - A subset H of a group G is a subgroup of G if and only if

$a, b \in H \Rightarrow ab^{-1} \in H$.(in additive notation we write $a , b \in H \Rightarrow (a - b) \in H$)

***Proof* :** Let H be a subgroup of G . By existence of inverse . .

If $a , b \in H$ then $b^{-1} \in H$

$\Rightarrow$ $ab^{-1} \in H$ by closure property

Conversely,
Suppose $a, b \in H \Rightarrow ab^{-1}$ ---------- (1)

Let $a \in H$.

Then $aa^{-1} \in H$ by assumption.

$\Rightarrow e \in H$ i.e the identity element exists in H …… (2)

Let $a \in H$, Now $e , a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H$

Therefore each element of H has inverse in H . …… (3)

Associative property holds in H as $H \subseteq G$.

Finally , for $a , b \in H$ we have $b^{-1} \in H$ by (3)

and $a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H$ by assumption (1)
$\Rightarrow ab \in H$ so that H is closed .

Hence H is a group , a subgroup of G . This completes the proof.

The next theorem is called the two step subgroup test is equivalent to the above theorem.

Theorem 5.03: (two step subgroup test) : A subset H of a group G is a subgroup of G if and only if (i) $a, b \in H \Rightarrow ab \in H$ (closure property). and (ii) $a \in H \Rightarrow a^{-1} \in H$ (existence of inverse in H)

Proof: To prove this theorem , we shall show that it is equivalent to the previous theorem .

i.e one theorem implies the other .

We take " $a , b \in H \Rightarrow ab^{-1} \in H$ " as the first statement P_1 and
(i) $a, b \in H \Rightarrow ab \in H$.
(ii) $a \in H \Rightarrow a^{-1} \in H$ " as the second statement P_2.

Now Let $a , b \in H \Rightarrow ab^{-1} \in H$ ……..(1).

To prove that the conditions in this theorem are satisfied ,

we take $a , b \in H$

$\Rightarrow a , a \in H \Rightarrow aa^{-1} = e \in H$ by assumption (1)

Now $e , a \in H \Rightarrow ea^{-1} = a^{-1} \in H$. this proves condition (ii) of the second statement .

Also $b \in H \Rightarrow b^{-1} \in H$

and $a , b^{-1} \in H \Rightarrow a(b^{-1})^{-1} = ab \in H$. This proves condition (i) of the second statement .

Thus $P_1 \Rightarrow P_2$

We now assume that (i) $a, b \in H \Rightarrow ab \in H$. (ii) $a \in H \Rightarrow a^{-1} \in H$.

Let $a , b \in H$

Then $b^{-1} \in H$ by (ii)

and $a, b^{-1} \in H \Rightarrow ab^{-1} \in H$ by (i)

i.e $a, b \in H \Rightarrow ab^{-1} \in H$.

This proves that $P_2 \Rightarrow P_1$

Hence the two theorems are equivalent.

One can also prove this theorem without showing its equivalence to the previous theorem.

Finite Subgroup Test

Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

Proof **:** We already have $a, b \in H \Rightarrow ab \in H$.

As H is not empty , we take any element $a \in H$.

If $a = e$ then $a^{-1} = e \in H$.

If $a \neq e$

Consider the set $S = \{ a, a^2, a^3 \ldots \ldots a^n \ldots \}$.

By the closure of H , we have $S \subseteq H$.

Hence , elements of S cannot all be different .

Let $a^i = a^j$ (assume wlog $i > i$)

$\Rightarrow a^{i-j} = e$.

As $a \neq e$, $i - j > 1$ $(i - j - 1) \geq 1$

and $e = a^{i-i} = aa^{i-j-1}$

$\Rightarrow a^{-1} = a^{i-j-1}$. Also $(i - j - 1) \geq 1 \Rightarrow a^{i-j-1} \in H$

i.e $a^{-1} \in H$.

Hence H is a subgroup of G .

Proposition: If $m \in Z$ then mZ the set of multiples of m is always a subgroup of Z under $'+'$.

Proof: If $x, y \in mZ$ then $x = mp$, $y = mq$ for some integer p, q .

Now $(x - y) = (mp - mq) = m(p - q) \in mZ$

Thus mZ is a subgroup of Z.

Theorem 5.04: Any subgroup of $\langle Z, + \rangle$ is of the form mZ where $m \in Z$.

Proof **:** Let H be a subgroup of Z .

Let m be the least positive integer in H .

Let x be any element of H.

By division algorithm we have $x = mq + r$ where $0 \leq r < m$

Now $x, m \in H \Rightarrow x, mq \in H \Rightarrow (mq - x) \in H$

$\Rightarrow r \in H$.

By the condition for m and r , we must have $r = 0$ so that $x = mq$.

As $'x'$ is an arbitrary element of H , we conclude that every element of H is a multiple of $'m'$.

i.e $H = mZ$.

Theorem 5.05: If H and K are subgroups of a group G then $H \cap K$ is a subgroup of G .

Proof : Let $a, b \in H \cap K$

$\Rightarrow a, b \in H$ and $a, b \in K$

$\Rightarrow b^{-1} \in H$ and $b^{-1} \in K$

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

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

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

Example: The union of two subgroups may not be a subgroup of a group G .

Consider the group Z under $+$

Then $2Z$, $3Z$ are subgroup of Z .

Now $2 \in 2Z, 3 \in 3Z \Rightarrow 2, 3 \in 2Z \cup 3Z$

But $(2 + 3) = 5 \notin 2Z \cup 3Z$ as 5 is neither a multiple of 2 nor 3 .

Thus $2Z \cup 3Z$ is not closed under $'+'$ and hence not a subgroup .

Theorem5.06: Every subgroup of a cyclic group is cyclic.

Proof **:** Ans **:** Let $G = (a)$ be a cyclic group generated by $'a'$
Let H be a subgroup of G

Let m be the smallest positive integer such that $a^m \in H$

i.e $a^m \in H$ and $a^r \notin H$ for $0 < r < m$ ……..(1)

Let $b = a^m$.

We shall show that "b" generates H

Let $x \in H$ be any element .

$\Rightarrow x \in G$

$\Rightarrow x = a^n$ for some positive integer n

As $x \in H$

we have $n > m$

$\Rightarrow n = mq + r$ where $0 \leq r < m$

Now $a^n = a^{mq+r} = a^{mq}a^2 = (a^m)^q\, a^r$

$\Rightarrow a^r = a^n(a^{mq})^{-1}$

As $a^m \in H \Rightarrow a^{mq} \in H \Rightarrow (a^{mq})^{-1} \in H$

Also $a^n \in H$

Therefore $a^r = a^n\,(a^{mq})^{-1} = \in H$

As $0 \leq r < m$ using (1)

we must have $r = 0$

So that $n = mq$ Therefore $x = a^n = a^{mq} = (a^m)^q = b^q$

Showing that x is a power of b

As x is any element of H

Therefore H is generated by b

i.e H is cyclic .

Theorem 5.07: Let G be a group and $a \in G$. Then the set $\langle a\rangle = \{\, a^n : n \in Z \,\}$ is a subgroup of G . (***This is a cyclic subgroup generated by*** $'a'$)

Proof : If $x, y \in \langle a\rangle$ then $x = a^m$, $y = a^n$ for some $m, n \in Z$.

$xy^{-1} = a^m(a^n)^{-1} = a^{m-n} \in \langle a\rangle$

Thus $\langle a\rangle$ is a subgroup of G .

Example: Let $G = Z_6$. We shall examine the subgroups of Z_6 generated by each non identity element under addition mod 6.

We have $1 \times 1 = 1, 2 \times 1 = 2, 3 \times 1 = 3, 4 \times 1 = 4, 5 \times 1 = 5, 6 \times 1 = 6 \equiv 0$

$\Rightarrow \langle 1 \rangle = \{0,1,2,3,4,5\} = Z_6$

$1 \times 2 = 2, 2 \times 2 = 4, 3 \times 2 = 6 \equiv 0$

Thus $\langle 2 \rangle = \{0, 2, 4\}$

$1 \times 3 = 3, 2 \times 3 = 6 \equiv 0$

$\Rightarrow \langle 3 \rangle = \{0, 3\}$

$1 \times 4 = 4, 2 \times 4 = 8 \equiv 2, 3 \times 4 = 12 \equiv 0$

$\Rightarrow \langle 4 \rangle = \{0, 2, 4\}$

$1 \times 5 = 5, 2 \times 5 = 10 \equiv 4, 3 \times 5 = 15 \equiv 3, 4 \times 5 = 20 \equiv 2$

$5 \times 5 = 25 \equiv 1, 6 \times 5 = 30 \equiv 0$

$\Rightarrow \langle 5 \rangle = \{0,1,2,3,4,5\} = Z_6$.

Example: Consider the group $U_8 = \{1,3,5,7\}$ under multiplication mod 8. We have $3^2 = 9 \equiv 1 \, mod \, 8$

$5^2 = 25 \equiv 1 \, mod \, 8$

$7^2 = 49 \equiv 1 \, mod \, 8$

So that each elements are their own inverse.

Also $\langle 3 \rangle = \{1, 3\}, \langle 5 \rangle = \{1, 5\}, \langle 8 \rangle = \{1, 8\}$

Definition: Let G be a group. The center, Z(G), of G is the subset of elements in G that commute with every element of G.

i.e $Z(G) = \{a \in G \;\; ax = xa \;\; \forall \;\; x \; in \; G\}$.

Theorem: The center of a group G is a subgroup of G.

Proof: Let $Z(G)$ be the center of G.

Let $a, b \in Z(G)$

We have $by = yb \;\; \forall \;\; y \in G$

$\Rightarrow yb^{-1} = b^{-1}y \;\; \forall \; y \in G$

$\Rightarrow b^{-1} \in Z(G)$

Now , $(ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$

$=. (ab^{-1}) \in Z(G)$

Hence $Z(G)$ is a subgroup of G .

Definition: Centralizer of an element in G.
Let G be a group and $a \in$ G. The centralizer of a in G is the set $C(a)$ of all elements in Gthat commute with $'a'$.
i.e $C(a) = \{ x \in G \ : \ ax = xa \ \}$

Theorem 5.08: The centralizer of an element of a group G is a subgroup of G .

Proof: Let $a \in G$.

We have $C(a) = \{x \epsilon G \ : xa = ax\}$.

Let $x, y \ \epsilon \ C(a)$

Therefore $xa = ax \ and \ ya = ay$

Also $ay = ya \Rightarrow ayy^{-1} = yay^{-1}$

$\Rightarrow a = yay^{-1}$

$\Rightarrow y^{-1}a = y^{-1}yay^{-1}$

$\Rightarrow y^{-1}a = ay^{-1}$

Now $(xy^{-1})a = x(y^{-1}a) = x(ay^{-1}) = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1})$

This shows that $xy^{-1} \ \epsilon \ C(a)$

Hence $C(a)$ is a subgroup of G

Cauchy's Theorem for Abelian Groups
Let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p.

Cosets

Introduction

Cosets are fundamental constructs in group theory that allow us to partition a group into distinct subsets based on the subgroup structure. Let's delve into the details:

Coset of a Subgroup: Let G be a group and H a subgroup of G.

For any element $g \in G$, the **left coset** of H containing g is defined as:
$gH = \{gh: h \in H\}$ (in additive notation is written $g + H = \{ g + h : h \in H \}$)

This set consists of all elements obtained by multiplying/adding g on the left by elements of H.

Similarly, the **right coset** of H containing g is:
$Hg = \{hg \mid h \in H\}$ (in additive notation is written $H + g = \{ h + g : h \in H \}$ which consists of all elements obtained by multiplying/adding g on the right by elements of H.

Note: $He = H$ for an identity element $'e'$.

Note: As $e \in H$, for any $g \in G$, $g = ge \in gH$ and $g = eg \in Hg$.

Example: Consider the group Z_4 under addition mod 4 and its subgroup $H = \langle 2 \rangle = \{0,2\}$.

For an element $3 \in Z_4$, the left and right cosets of H containing 3 are
$3 + \langle 2 \rangle = \{ 3 + 0 , 3 + 2\} = \{3 , 5 \}$
and $\langle 2 \rangle + 3 = \{ 0 + 3 , 2 + 3 \} = \{ 3 , 5 \}$

Example: Consider the subgroup $2Z$ of even integers . For an element $1 \in Z$, the left and right cosets of $2Z$ containing $'1'$ are

$1 + 2Z = \{1 + 2m: m \in Z \}$
and $2Z + 1 = \{ 2m + 1 : m \in Z \}$ which is the set of odd integers .

Example: Consider the group $U_8 = \{1,3,5,7 \}$ and a subgroup $H = \langle 7 \rangle = \{ 1,7\}$

For $a = 3$, $Ha = \{1 * 3\ ,\ 7 * 3\} = \{3, 5\}$ (here $*$ is multiplication modulo 8)

For $a = 5$, $Ha = \{1 * 5, 7 * 5\} = \{5, 3\}$

For $a = 7$, since $7 \in H$, $Ha = H$

This can be verified also as

$Ha = \{1 * 7, 7 * 7\} = \{7, 1\} = H$

We shall later show that cosets partition the group G and that any two cosets have the same number of elements finite or infinite.

Definition: Let H be a subgroup of G. The number of distinct left (or right) cosets of H in G is called the **index** of H in G written as $|G: H|$.

Theorem 5.09: Let G be a group and H be a finite subgroup of G . Then any two right (or left) cosets of H in G have the same number of elements as H .

Proof: Let $H = \{h_1, h_2,\ h_3, \ldots \ldots h_n\}$ where each $g_i\ are\ distinct$ for $1 \leq i \leq n$ and $g \in G$.

Then $Hg = \{h_1 g\ , h_2 g\ ,\ h_3 g\ \ , \ldots \ldots h_n g\}$
These elements of Hg are distinct, otherwise $h_i g = h_j g$ with $i \neq j\ , by\ cancellation\ law$ we shall have $h_i = h_j$ which is not true as each h_i are distinct.
It is now clear that Hg and H have the same number of elements.

Theorem 5.10: Let G be a group and H a subgroup of G . For $a, b \in G$, $Ha = Hb \Leftrightarrow ab^{-1} \in G$.

Proof **:** If $Ha = Hb$

then $a \in Ha = Hb \Rightarrow a \in Hb$

so $a = hb$ for some$h \in H$.

$\Rightarrow ab^{-1} = h \in H$.

Conversely: If $ab^{-1} \in H$
Let $x \in Ha$, then $x = ha$ for some $h \in H$.

Now $x = ha = hab^{-1}b = h_1 b \in Hb$ where $h_1 = hab^{-1}$

$\therefore Ha \subseteq Hb$

Also $ab^{-1} \in H \Rightarrow \ (ab^{-1})^{-1} = ba^{-1} \in H$ as H is a subgroup .

Let $y \in Hb$, then $y = hb$ for some $h \in H$

Now $y = hb = hba^{-1}a = h_2 a \in Ha$ where $h_2 = bba^{-1}$

$\therefore Hb \subseteq Ha$

Hence $Ha = Hb$.

Theorem 5.11: Let G be a group and H a subgroup of G. Then any two right (or left) cosets are either identical or disjoint.

***Proof* :** Let Ha , Hb be two right cosets.

If $Ha \cap Hb = \phi$ the empty set , then the proof completed.

Suppose $Ha \cap Hb \neq \phi$

Let $x \in Ha \cap Hb$

Then $x \in Ha \Rightarrow x = ha$ and $x \in Hb \Rightarrow h_1 b$ where $h , h_1 \in H$.

Now $x = ha = h_1 b \Rightarrow ab^{-1} = h^{-1}h_1 \in H$

By previous theorem , $Ha = Hb$.

Theorem 5.12: Let G be a group and H a subgroup of G . Then any element $x \in G$ is in one and only one right (or left) coset of H in G . Also $G = \cup Hg$ where Hg runs over all distinct right cosets of H in G.

***Proof* :** Let $x \in G$. Then $x = ex \in Hx$

Suppose $x \in Ha$ for some right coset Ha , then $Ha \cap Hx \neq \phi$

$\Rightarrow Ha = Hx$

Hence x is and only is in Hx .

For the second part , that $\cup Hg \subseteq G$ is obvious.

Also $x \in G \Rightarrow x = ex \in Hx , \Rightarrow x \in \cup Hg$

Therefore $G = \cup Hg$.

Corollary: If G is a finite group and H a subgroup of G then $o(G) = |G:H| \times o(H)$

Lagrange's Theorem on Finite groups: Let G be a finite group and H a subgroup of G. Then the order of G is divisible by the order of H . or $o(H)|o(G)$.

Proof: Let the index of H in G be r , $o(G) = n$, $o(H) = m$
Let $Hg_1, Hg_2, Hg_3, \ldots\ldots Hg_r$ be the collection of all distinct right cosets of H .

Since any element $x \in G$ is in one and only one coset Hg_i

We have $G = \cup_{i=1}^{r} Hg_i$

As each Hg_i are distinct , they are disjoint .

Also Each cosets have the same number of elements as H .

Hence $n = o(G) = o(\cup_{i-1}^{r} Hg_i) = \sum_{i=1}^{r} o(Hg_i) = mr$

$\Rightarrow m|n$

Some of the applications of Lagrange's Theorem are given below:

Determining Possible Subgroup Orders

Lagrange's Theorem helps in identifying possible orders of subgroups of a given finite group.

For example, if a group G is of order 12, then its subgroups must have orders that are divisors of 12, i.e., 1, 2, 3, 4, 6, or 12.

Proving Non-existence of Certain Subgroups

Lagrange's Theorem can be used to show that certain subgroups do not exist. For instance, a group of order 12 cannot have a subgroup of order 5, since 5 is not a divisor of 12.

Cosets and Index of Subgroups

The theorem is used to understand cosets and the index of subgroups. The index of a subgroup H in G is given by $\frac{|G|}{|H|}$ This is always an integer due to Lagrange's Theorem.

Understanding Cyclic Groups

Lagrange's Theorem helps in analyzing the structure of cyclic groups. If G is a cyclic group of order n, then for any divisor d of n, there exists a unique subgroup of G of order d.

Example: Consider the symmetric group S_3, which is the group of all permutations of three elements. S_3 is of order 6. The possible orders of subgroups of S_3, according to Lagrange's Theorem, are the divisors of 6 which are 1, 2, 3, and 6.

- The trivial subgroup has order 1.
- The subgroups of order 2 are generated by single transpositions namely $(1\ 2)$, $(1\ 3)$, $(2\ 3)$ which are
  $H_1 = \{e, (2\ 3)\}$, $H_2 = \{e, (1\ 3)\}$, $H_3 = \{e, (1\ 2)\}$
- The subgroups of order 3 are cyclic subgroups generated by a 3-cycle $(1\ 2\ 3)$ or $(1\ 3\ 2)$
  i.e $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$
  The whole group S_3 itself is the subgroup of order 6.
- By Lagrange's Theorem, S_3 cannot have subgroups of any other orders.
- Using Lagrange's Theorem , we can determine the index of each of the above subgroups Index of $H_1\ in\ S_3 = \frac{o(G)}{o(H_1)} = 3$, Index of $H_2\ in\ S_3 = 3$, Index of $H_3\ in\ S_3 = 3$ Index of $H\ in\ S_3 = 2$

Exercise

1. Find all cyclic subgroups of Z_3 , Z_4, Z_5

2. Find all cyclic subgroups of D_4 .

3. Find the cosets of each of the subgroups $\{e, (1\ 2)\}$,$\{e, (1\ 3)\}$,$\{e, (2\ 3)\}$ of S_3 .

4. Prove that if a is the only element of order 2 in a group, then a lies in the center of the group.

5. Let $'a'$ be an element of a group and $a^{32} = e$. Find all possible orders of $'a'$.

6. Let $'a'$ be a group element and order of $'a'$ is infinite . prove that $a^n = a^m \Leftrightarrow n = m$.

7. Let $U(14)$ be a group of units integers modulo 14. Show that $U(14)$ is cyclic and find all its generator.

8. Let *a* be a group element of order *n*, and suppose that *d* is a positive divisor of *n*. Prove that $|ad| = \frac{n}{d}$.

9. Examine whether the following subsets are subgroup of C (the complex numbers .

   (i) $S = \{ a + ib : \ a, b \in R \ , ab \geq 0 \ \}$
   (ii) $S = \{ a + ib : \ a, b \in R \ , ab \leq 0 \ \}$

10. Prove that the set of Guassian integers$\{ a + ib : \ a, b \in Z \}$ is a group under usual addition of complex number . Is it a group under multiplication ?

Chapter- 6

Normal Subgroups and Direct Products

In group theory, a normal subgroup (or invariant subgroup) is a subgroup that is invariant under conjugation by members of the group. Before defining normal subgroups, we first introduce the definition of conjugate elements of a group.

Conjugate elements of a group

Two elements a and b in a group G are said to be **conjugate** if there exists an element g in G such that $b = gag^{-1}$. In other words, b is the result of conjugating a by g.

Conjugacy Class

The set of all elements in G that are conjugate to a given element a forms the **conjugacy class** of a. The conjugacy class of a in G is denoted by $Cl(a)$

$Cl(a) = \{ x \in G : x = gag^{-1}$ for some g in $G \}$

Definition: A subgroup N of a group G is called a **normal subgroup** if $gng^{-1} \in N \quad \forall n \in N \ , \ \forall g \in G$

If N is normal in G we write $N \trianglelefteq G$ or $N \triangleleft G$.

Example: Consider the group $G = \{ \pm 1 , \pm i \}$ and a subgroup $N = \{\pm 1 \}$ under usual multiplication.

It is easy to verify that $gng^{-1} \in N$ for each $n \in N , g \in G$ so that $N \triangleleft G$.

Example: Let G be a group . The centre $Z(G)$ of a group G is a normal subgroup of G.

Proof: Let $a , b \in Z(G)$

Therefore $ay = ya \ , \ by = yb \ \forall \ y \in \ G$

And $by = yb \Rightarrow yb^{-1} = b^{-1}y$

Now $(ab^{-1})y = a(b^{-1}y) = a(yb^{-1}) = (ay)b^{-1} = (ya)b^{-1} = y(ab^{-1})$

Thus ab^{-1} commutes with any element $y \in G$

ie. $a, b \in Z(G) \Rightarrow ab^{-1} \in Z(G)$ so that $Z(G)$ is a subgroup of G.

Let $g \in G$, $a \in Z(G)$. Then $ag = ga$, $ag^{-1} = g^{-1}a$

we have $(gag^{-1})y = (gg^{-1}a)y = ay = ya = y(gg^{-1}a) = y(gag^{-1})$

$\Rightarrow gag^{-1} \in Z(G)$ for any $a \in Z(G), g \in G$

proving that $Z(G)$ is a normal subgroup of G

Theorem 6.01: Every subgroup of an abelian group is normal.

Proof **:** Let G be an abelian group , H a subgroup of G .

For any $g \in G$, $h \in H$ we always have

$ghg^{-1} = gg^{-1}h = h \in H$

Theorem 6.02: A subgroup N of a group G is normal if and only if $gNg^{-1} = N \; \forall \; g\epsilon \; G$(here $gNg^{-1} = \{gng^{-1} : n\epsilon N\}$)

Proof: Suppose $gNg^{-1} = N \; \forall \; g\epsilon \; G$

we have $gng^{-1}\epsilon \; gNg^{-1} = N$

Hence $gng^{-1}\epsilon \; N$ therefore N is normal in G

Conversely if N is normal .

We have $gng^{-1}\epsilon gNg^{-1}$

Also $gng^{-1}\epsilon \; N$ as N is normal

$\Rightarrow gNg^{-1} \subseteq N$ ... ... (1)

Now , Let $n \; \epsilon \; N$

then $n = g(g^{-1}ng)g^{-1} = gn_1g^{-1}\epsilon \; gNg^{-1}$ .....(2) { where $n_1 = g^{-1}ng = g_1ng_1^{-1} \; \epsilon \; N$ as N is normal

From (1) and (2) we have $gNg^{-1} = N$

Theorem 6.03: A subgroup N is normal in G if and only if $every\ left\ coset\ of\ N$ in G is a right coset.

Proof : Suppose N is normal in G

Let gN be any left coset of N in G

Since N is normal , we have $gNg^{-1} = N$ (using previous theorem)

$\Rightarrow (gNg^{-1})g = Ng$ or $gN = Ng$ showing that the left coset gN is also the right coset Ng

Conversely Suppose every left coset of N in G is a right coset

Then for $g\epsilon G$, gN being the left coset must also be the right coset .

(which right coset ?)

Now $g = ge \epsilon gN$ and $g = eg \epsilon Ng$ $\{e \epsilon N$

Thus gN and Ng have a common element , hence must be identical

Therefore $gN = Ng$

$\Rightarrow gNg^{-1} = Ngg^{-1} = N$

Hence N is normal. (using previous theorem)

Theorem 6.04: A subgroup N of G is normal in G if and only if the product of two right cosets (or left cosets) is again a right coset (or left coset)

Proof: Let N be normal in G

Let $Na,\ Nb$ be two right cosets of N

Now , $NaNb = N(aN)b = N(Na)b$ $\{Na = aN$ as N is normal

$= NNab = Nab$

Conversely : suppose that the product of any two right cosets of N is again a right coset of N.

Then $NaNb$ is a right coset of N. (note here we cannot claim yet that $NaNb = Nab$)

Also $ab = (ea)(eb) \epsilon NaNa$ and $ab = e(ab)\epsilon Nab$

Thus $NaNb$ and Nab are two right cosets having common elements

Therefore $NaNb = Nab$

Now Let $g\epsilon G$ and $n\epsilon N$

Then $gng^{-1} = (eg)(ng^{-1})\, \epsilon NgNg^{-1} = Ngg^{-1} = Ne = N$
i.e $gng^{-1}\epsilon N$, therefore N is normal

Example: Recall the symmetric group S_3 of degree . We present again below its table

$\circ$	$\boldsymbol{e}$	$\boldsymbol{\phi_1}$	$\boldsymbol{\phi_2}$	$\boldsymbol{\phi_3}$	$\boldsymbol{\chi}$	$\boldsymbol{\omega}$
$\boldsymbol{e}$	e	ϕ_1	ϕ_2	ϕ_3	χ	ω
$\boldsymbol{\phi_1}$	ϕ_1	e	χ	ω	ϕ_2	ϕ_3
$\boldsymbol{\phi_2}$	ϕ_2	ω	e	χ	ϕ_3	ϕ_1
$\boldsymbol{\phi_3}$	ϕ_3	χ	ω	e	ϕ_1	ϕ_2
$\boldsymbol{\chi}$	χ	ϕ_3	ϕ_1	ϕ_2	ω	e
$\boldsymbol{\omega}$	ω	ϕ_2	ϕ_3	ϕ_1	e	χ

Consider the subgroup $H = \{e, \chi, \omega\}$

We shall calculate ghg^{-1} for each $g \in S_3$, $h \in H$

For $g = e, \chi, \omega$ it is clear that $ghg^{-1} \in H$ for any $h \in H$ as e, χ, ω

are elements of H

For $g = \phi_1, \phi_2, \phi_3$

We have $\phi_3\chi{\phi_3}^{-1} = (\phi_3\chi)\phi_3 = \phi_1\phi_3 = \omega$

$\phi_3\omega{\phi_3}^{-1} = (\phi_3\omega)\phi_3 = \phi_2\phi_3 = \chi$

$\phi_2\chi{\phi_2}^{-1} = (\phi_2\chi)\phi_2 = \phi_3\phi_2 = \omega$

$\phi_2\omega{\phi_2}^{-1} = (\phi_2\omega)\phi_2 = \phi_1\phi_2 = \chi$

$\phi_1\chi{\phi_1}^{-1} = (\phi_1\chi)\phi_1 = \phi_2\phi_1 = \omega$

$\phi_1\omega{\phi_1}^{-1} = (\phi_1\omega)\phi_1 = \phi_3\phi_1 = \chi$

Thus we have seen that $ghg^{-1} \in H \; for\; any \; g \in S_3$, $h \in H$
Therefore $H = \{e , \chi , \omega\}$ is a **Normal subgroup** of S_3
We state and prove below another useful theorem that can sometimes determine whether a subgroup is normal .

Theorem 6.05: If G is a group and H a subgroup of index 2 in G, prove that H is a normal subgroup of G.

Proof **:** Since H is of index 2 , there are only two distinct left cosets and only two distinct right cosets.

Let H and Ha be the right cosets , H and aH be the left cosets

Then $G = H \cup aH$ and $H \cap aH = \emptyset$

$\Rightarrow aH = G - H$ ---------- (1)

Similarly , $Ha = G - H$ --------- (2)

Therefore $aH = Ha$ showing that H is normal.

Example: Prove that if K is a subgroup of a group G such that $g^2 \in K$, $\forall\ g \in G$,
then K is normal in G.

Solution: Let $g \in G$

$\Rightarrow g^{-1} \in G$

$\Rightarrow (g^{-1})^2 = g^{-2} \in K$ using given condition .

Let $k \in K$

$\Rightarrow k^{-1} \in K$

$\Rightarrow k^{-1}g^{-2} \in K$

Also $(gk) \in G \Rightarrow (gk)^2 \in K \ \forall\ g \in G$

Now $(gk)^2\ (k^{-1}g^{-2}) \in K$

$\Rightarrow (gkgkk^{-1}g^{-2}) \in K$

$\Rightarrow gkg^{-1} \in K$.

Hence K is normal in G

Using this theorem in the previous example for $H = \{e, \chi, \omega\}$,

we have $o(H) = 3$, $o(S_3) = 6$

Therefore H is of index $\frac{6}{3} = 2$ in S_3 and as such , H is normal .

Theorem 6.06: The intersection of any two normal subgroups of a group G is a normal subgroup of G.

***Proof* :** Let G be a group
Let H , K be two normal subgroups of G

Let $a , b \in H \cap K$

$\Rightarrow a, b \in H$ and $a , b \in K$

As H and K are subgroups we have

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

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

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

Let $g \in G$, $n \in H \cap K$

$\Rightarrow n \in H$ and $n \in K$

As H and K are normal in G we have

$gng^{-1} \in H$ and $gng^{-1} \in K$

$\Rightarrow gng^{-1} \in H \cap K$. Thus $H \cap K$ is normal in G

Normalizer : Let G be a group and H a subgroup of G . The normalizer of H denoted by $N(H)$ is the set $N(H) = \{ g \in G \mid gHg^{-1} = H \}$.

Proposition: The normalizer of a subgroup of G is a subgroup of G .

Proof: Let H be a subgroup of G .

We have $N(H) = \{ g \in G \mid gHg^{-1} = H \}$

Let $x , y \in N(H)$

Then $xHx^{-1} = H$, $yHy^{-1} = H \Rightarrow y^{-1}Hy = H$

Now $(xy^{-1})H(xy^{-1})^{-1} = (xy^{-1})H(yx^{-1}) = x(y^{-1}Hy)x^{-1} = xHx^{-1} = H$

$\Rightarrow xy^{-1} \in N(H)$

Hence $N(H)$ is a subgroup of G .

Note: From the definition of the normalizer , it is clear that H is always a normal subgroup of $N(H)$.

Also If H is normal in G then $N(H) = G$.

Multiplication/Addition of cosets of normal subgroups

Let G be a group and N a normal subgroup of G . For two cosets Na, Nb of N we define the multiplication as $(Na)(Nb) = Nab$

We first show that this multiplication of cosets of N is **well- defined**
namely – if $Na = Nx \;\; and \;\; Nb = Ny$ then $NaNb = NxNy$
To prove this ,

We have $Na = Nx \Rightarrow ax^{-1} \epsilon\, N \Rightarrow ax^{-1} = n_1 \epsilon N \Rightarrow a = n_1 x$

Similarly $Nb = Ny \Rightarrow b = n_2 y$ for $n_2 \epsilon N$

Now $NaNb = N(n_1 x)N(n_2 y) = (Nn_1)x(Nn_2)y = NxNy$ as $n_1 , n_2 \epsilon\, N$

We can translate the above definition to addition as
$(N + a) + (N + b) = N + (a + b)$
with these definitions , we an proceed to the next topic .

Factor Group/Quotient Group

Definition: Let G be a group and N be a normal subgroup of G . Let $\frac{G}{N}$ be the collection of all distinct right (or Left) cosets of N in G .

i.e $\frac{G}{N} = \{Ng : g \epsilon G \}$ or $\frac{G}{N} = \{N + g : g \epsilon G \}$ for an additive group G

Then $\frac{G}{N}$ is a group under cosets multiplication . This group is called a **quotient group** or **Factor group** of G by N .

Proof: * Let Na, Nb be two rights cosets of N . As N is normal , we have $NaNb = Nab$ is aslo a right coset of N .

i.e $Na \,,\; Nb \,\epsilon \frac{G}{N} \Rightarrow\; NaNb = Nab \,\epsilon\, \frac{G}{N}$. So the closure property holds .

* If $Na,\ Nb\ , Nc\ \epsilon \frac{G}{N}$ then $(NaNb)Nc = NabNc = Nabc = (Na)(Nbc) = (Na)(NbNc)$
Therefore the associative property holds .

*We have $e\epsilon\ G \Rightarrow\ \ Ne = N\ \epsilon \frac{G}{N}$

and $(N)(Na) = NeNa = Nea = Na = Nae = NaNe = (Na)(N)$

Therefore $\boldsymbol{N = Ne}$ is the identity element .

Lastly , if $a\epsilon G$ then $a^{-1}\epsilon G$

therefore $Na\ \epsilon \frac{G}{N} \Rightarrow Na^{-1}\ \epsilon \frac{G}{N}$

and $NaNa^{-1} = Naa^{-1} = Ne = N = Na^{-1}a = Na^{-1}Na$

showing that $\boldsymbol{Na^{-1}}$ is the inverse of Na in $\frac{G}{N}$

Hence $\frac{G}{N}$ is a group .

Theorem 6.07: If G is a finite group and N is a normal subgroup of G then
$o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}$.

***Proof* :** Let n be the order of G and m be the order of N.

Let p be the index of $N\ in\ G$. (index of N is the number of distinct right cosets of N in G) then $o\left(\frac{G}{N}\right) = p$.

Also we know that if $Ng_1\ ,\ Ng_2\ ,\ Ng_3\ ,\ \cdots Ng_i\ ,\cdots Ng_p$ are the p distinct right cosets of N in G then $G = Ng_1 \cup Ng_2 \cup Ng_3\ \cup\ \cdots \cup Ng_i \cup \cdots \cup Ng_p$ so that $n = o(G) = o(Ng_1) + o(Ng_2) + o(\ Ng_3) +\ \cdots + o(Ng_i) +\ \cdots + o(Ng_p)$ as each Ng_i are disjoint .

Since $o(N) = m$ therefore $o(Ng) = m$

from above we have $n = mp$ or $p = \frac{n}{m}$ ie $o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}$

Example: Examine the elements of a group $\frac{Z}{4Z}$ where Z is the set of integers and $4Z$ is the set of all integers which are multiple of 4. (or $4Z = \{4x: x \epsilon Z\ \}$

***Ans*:** We first note that Z is a group under $+$.

Hence any element in $\frac{Z}{4Z}$ is of the form $4Z + z$ where $z \epsilon Z$.

Now $z\ \epsilon Z \Rightarrow\ z = 4k\ or\ 4k+1\ \ or\ \ 4k+2\ \ or\ \ 4k+3$

Thus $4Z + z = 4Z + 4k = 4Z$ as $4k\ \epsilon\ 4Z$

or $4Z + z = 4Z + (4k+1) = (4Z + 4k) + 1 = 4Z + 1$

or $4Z + z = 4Z + (4k+2) = 4Z + 2$

or $4Z + z = 4Z + (4k+3) = 4Z + 3$

Hence $\frac{Z}{4Z}$ has four elements i. e $\frac{Z}{4Z} = \{4Z\ ,\ 4Z+1,\ 4Z+2\ , 4Z+3\ \}$

As seen above we can generalize the statement as

If m is any positive integer, then $\frac{Z}{mZ}$ has m elements namely $mZ,\ mZ+1\ ,\ mZ+2\ , \cdots\cdots\ ,\ mZ+(m-1)$.

Product/Sum of Two Subgroups

Let H, K be two subgroups of G. The product of H and K is a set define as $HK = \{hk: h \epsilon H\ \ , k \epsilon\ K\ \}$

The Sum is defined as $H + K = \{h + k: h \epsilon H\ \ , k \epsilon\ K\ \}$

Note that HK is a subset of G

Result: Let H be a subgroup of G. Then $HH = H$ (or $H + H = H$ for additive group)

Proof: $h \epsilon H \Rightarrow h = eh \epsilon HH \Rightarrow H \subseteq HH$ And $x \epsilon HH \Rightarrow x = h_1 h_2 \epsilon H$ for $h_1\ , h_2\ \epsilon\ H$ and H is closed.

Theorem 6.08: If H and K are two subgroups of G then HK is a subgroup of G if and only if $HK = KH$

Proof: Suppose HK is a subgroup of G.

To show that $\boldsymbol{KH = HK}$

Let $\boldsymbol{x \epsilon\ KH}$.

Therefore $x = kh$ for some $h \epsilon H$ and $k \epsilon K$

Now $k = ek \in HK$ and $h = he \in HK$

Since HK is closed being a subgroup

we have $x = kh \in HK$.

Thus , $KH \subseteq HK$.

Now let $\boldsymbol{y \epsilon\ HK}$

As HK is a subgroup , we have $y^{-1} \epsilon HK$

Let $y^{-1} = hk : h \epsilon H , k \epsilon K$

Now $y = (y^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \epsilon KH$

This shows that $HK \subseteq KH$.

Hence if HK is a subgroup of G, then. $HK = KH$

Conversely suppose $HK = KH$. We will show that HK is a subgroup of G .

Let $a, b \in HK$; say $a = h_1k_1$ and $b = h_2k_2$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

Now $ab^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1k_3h_2^{-1}$ {**where $\boldsymbol{k_3 = k_1k_2^{-1} \epsilon K}$**

Also $k_3h_2^{-1} \epsilon KH = HK \Rightarrow k_3h_2^{-1} \epsilon HK$

$\Rightarrow k_3h_2^{-1} = h_3k$ where $h_3 \epsilon H$, $k \epsilon K$

Therefore $ab^{-1} = h_1k_3h_2^{-1} = h_1h_3k = hk \epsilon HK$ { $h = h_1h_3 \epsilon H$

Hence HK is a subgroup of G

Theorem 6.09: Let H be a normal subgroup of a group G and K be any subgroup of *G*.

Then $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G.

***Proof*:** If $x, y \in HK$ then $x = hk, y = h_1k_1$ *where* $h, h_1 \in H$, $k, k_1 \in K$
Now $xy^{-1} = (hk)(k_1^{-1}h_1^{-1}) = h(kk_1^{-1})h_1^{-1} = h(k_2h_2)$ where $k_2 = kk_1^{-1} \in K$ and $h_2 = h_1^{-1} \in H$

$= h(k_2h_2k_2^{-1})k_2$

$= h_3k_2 \in HK$

where $k_2h_2k_2^{-1} \in H$ as H is normal and $h_3 = h(k_2h_2k_2^{-1})$

Hence HK is a subgroup of G.

Internal Direct product: Let G be a group, H, K be normal subgroups of G. We say that G is the internal direct product of H and K if $G = HK$ and $H \cap K = \{e\}$.

If G is the internal direct product of H *and* K we shall write $G = H \otimes K$

Example: Consider the Klein's 4- group $G = \{e, a, b, c\}$ and the two subgroups $H = \{e, a\}$, $K = \{e, b\}$. Being an abelian group, both these subgroups are normal and $H \cap K = \{e\}$ Also we have, $e = ee$, $a = ae$, $b = eb$, $c = ab$
i.e $G = HK$

External Direct Product

Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The *external direct product* of $G_1, G_2, \ldots, G_n$ denoted by $G_1 \times G_2 \ldots\ldots\times G_n$, is the set of all *n*-tuples for which the i^{th} component is an element of G_i and the operation is componentwise.

In symbols, $G_1 \times G_2 \ldots\ldots\times G_n = \{(x_1, x_2, x_3, \ldots\ldots x_n) : x_i \in G_i\}$

Theorem 6.10: Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The external direct product $G_1 \times G_2 \ldots\ldots\times G_n$ is a group under the operation of each G_i componentwise with $(e_1, e_2, \ldots. e_n)$ as identity element (where e_i is the identity element in G_i) and $(a_1^{-1}, a_2^{-1}, \ldots\ldots a_n^{-1})$ as the inverse of $(a_1, a_2, \ldots\ldots a_n)$ *As the proof is straight forward , we leave this as an exercise .*

Proposition: Let $G = G_1 \times G_2 \ldots\ldots\times G_n$ be the external direct product of n finite groups. The order of G is the product of the orders of each G_i.

i.e $|G| = |G_1||G_2| \ldots\ldots |G_n|$

The proof is not required as it is a direct counting of elements in the product of sets.

Example: The set $R \times R = \{ (x, y) : x , y \} \in R \ \}$ is the direct product or R with itself .

We can easily verify that this is a group under componentwise addition.

Example: The set $R' \times R' = \{ (x, y) \mid x, y \in R' \}$ where R' is the set of non zero real numbers , is a group under componentwise multiplication.

Example: The set $G = Z_2 \times Z_3 = \{(0,0), (0,1) , (0,2) , (1,0) , (1,1) , (1,2) \}$ under the componentwise operation (addition mod 2 for the first coordinates and addition mod 3 for the second) is a group. We have $(0 , 0)$ as the identity element. $(0 , 1) \times (0 ,2) = (0,0)$ etc ..

Example: The groups $Z_2 \times Z_8$, $Z_4 \times Z_4$, Z_{16} are each or order 16 .

Order of an Element in a Direct Product

Let $G = G_1 \times G_2 \ldots\ldots\ldots \times G_n$ be the external direct product of a finite number of finite groups . If $g = (g_1, g_2, \ldots . g_n) \in G$ then the order of $'g'$ is the least common multiple of the orders of the components.

i.e $|g| = lcm \ (|g_1|, \ |g_2|, \ldots\ldots |g_n|)$

***Proof* :** Let e_i be the identity element of G_i so that $e = (e_1, e_2 , \ldots e_n)$ is the identity element of G .

For each $i = 1,2 \ldots n$. Let m_i be the order of g_i and

let $m = lcm \{ m_1 , m_2, \ldots . m_n\}$

As m is a multiple of each m_i , it is clear that

$g^m = (g_1, g_2, \ldots . g_n)^m = (g_1^m , g_2^m , \ldots . g_n^m) = (e_1, e_2 , \ldots e_n) = e$

Next we need to show that $g^{m_0} \neq e$ for $0 < m_0 < m$

Suppose $g^{m_0} = e$ and $0 < m_0 < m$

Then $g_i^{m_0} = e_i$ for each $i = 1.2 \ldots\ldots n$

Since m is the lcm of the $g_i's$ and $0 < m_0 < m$, therefore . there is atleast one $'i'$ where

m_0 is not divisible by m_i .

so that $m_0 = m_i q + r$ with $0 < r < m_i$

Now $g_{i_0}^{m} = e_i \Rightarrow g_i^{m_i q + r} = e_i \Rightarrow g_i^{m_i q} g_i^r = e_i \Rightarrow g_i^r = e_i$

This is a contradiction as g_i is of oder m_i and $0 < r < m_i$

Hence $g_0^m \neq e$ for any $m_0 \in Z$ where $0 < m_0 < m$

Therefore $|g| = m = lcm$ of the orders of $g_i's$

Example: Let $G = Z_4 \times Z_6 \times Z_8$
Let $g = (2,4,6)$

We have $2 \in Z_4$ and $|2| = 2$ since $2 \times 2 = 4 \equiv 0\ mod\ 4$

Similarly $4 \in Z_6$, $|4| = 3$ and $6 \in Z_8$, $|6| = 4$

$lcm\ \{2,3,4\} = 12$

Therefore $|g| = 12$

Example: Let $G = V \times Z_4 \times S_3$ where V is the Klein's 4-group .

Let $g = (a, 2, \omega)$ where $\omega = (1\ 3\ 2)$

We have $|a| = 2$, $|2| = 2$, $|\omega| = 3$

Therefore $|g| = lcm\ \{2,2,3\} = 6$

Example: Let $G = Z_2 \times Z_4$

Then $G = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)\}$

It is easy to see that

$|(0,0)| = 1$, $|(0,1)| = 4$, $|(0,2)| = 2$, $|(0,3)| = 4$

$|(1,0)| = 2$, $|(1,1)| = 4$, $|(1,2)| = 2$, $|(1,3)| = 4$

Since G is of order 8 and non of its elements are of order 8 , therefore G is not cyclic. We demonstrate below a similar example but cyclic.

Example: Let $G = Z_3 \times Z_4$
Then

$G = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3), (2,0), (2,1), (2,2), (2,3)\}$

We have $|(0,0)| = 1$, $|(0,1)| = 4$, $|(0,2)| = 2$, $|(0,3)| = 4$

$|(1,0)| = 3$, $|(1,1)| = 12$, $|(1,2)| = 6$, $|(1,3)| = 12$

$|(2,0)| = 3$, $|(2,1)| = 12$, $|(2,2)| = 6$, $|(2,3)| = 12$

Since G is of order 12 and there are many (at least one) elements of order 12 .Hence G is cyclic.

We present below a theorem that state the condition under which the external direct product of two groups is cyclic , the product for any finite number of groups can then just be generalized by induction.

Theorem 6.11: Let H and K be finite cyclic groups. Then $H \times K$ is cyclic if and only if $|H|$ and $|K|$ are relatively prime.

Proof : Let $|H| = m$, $|K| = n$ and let $H = \langle h \rangle$, $K = \langle k \rangle$
i.e h and k are generators of H and K respectively .

and $|h| = m$, $|k| = n$

Assume that $H \times K$ is cyclic .

It is clear that (h, k) generates $H \times K$.

Since $|H \times K| = mn$, we must have $|(h, k)| = mn$

Also $|(h, k)| = lcm\{m, n\} = \frac{mn}{\gcd\{m,n\}}$

Thus we have $mn = \frac{mn}{\gcd\{m,n\}}$

$\Rightarrow \gcd\{m, n\} = 1$ i.e m and n are relatively prime .

Conversely , assume that m and n are relatively prime.

Then $|(h, k)| = lcm\{m, n\} = mn$

Since $|H \times K| = mn$

We conclude that $H \times K$ is cyclic .

We continue below from the previous example above to verify that if $H = \langle h \rangle$, $K = \langle k \rangle$ then (h, k) is a generator of $H \times K$.

Example : Let $G = Z_3 \times Z_4$

$= \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3), (2,0), (2,1), (2,2), (2,3)\}$
Here $Z_3 = \langle 1 \rangle$, $Z_4 = \langle 1 \rangle$

To verify that $(1,1)$ is indeed the generator, you can check its order in $\mathbb{Z}_3 \times \mathbb{Z}_4$:
$(1,1)^1 = (1,1)$

$(1,1)^2 = (2,2)$

$(1,1)^3 = (0,3)$

$(1,1)^4 = (1,0)$

$(1,1)^5 = (2,1)$

$(1,1)^6 = (0,2)$

$(1,1)^7 = (1,3)$

$(1,1)^8 = (2,0)$

$(1,1)^9 = (0,1)$

$(1,1)^{10} = (1,2)$

$(1,1)^{11} = (2,3)$

$(1,1)^{12} = (0,0)$
Which clearly show that all elements of $Z_3 \times Z_4$ are generated by $(1,1)$

Exercises

1. Verify that the subgroups H_1, H_2, H_3 of order 2 are not normal subgroups of the symmetric group S_3 .

2. Determine all normal subgroups of the cyclic group $\frac{Z}{12Z}$.

3. Let $H = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in R , ad \neq 0 \right\}$. Show that H is a subgroup of $GL(2, R)$.
   Is H normal . Conclude the result for $K = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in R , ad \neq 0 \right\}$.

4. Let H be a subgroup of a group G . Show that the normalizer N(H) of H is the largest subgroup of G where H is normal.

5. Show that the commutator subgroup of a group G is normal in G.

6. For two subgroups H and K of an abelian group G , show that $HK = \{hk \mid h \in H \ , k \in K \}$ is a subgroup of G .

7. Give an example of a group G and two subgroups H and K where HK is not a subgroup .

8. If G is a finite group and H , K are subgroups of G, then $|HK| = \frac{|H||K|}{|H \cap K|}$

9. Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. Prove that t he external direct product $G_1 \times G_2 \ldots \ldots \ldots \times G_n$ is a group under the operation of each G_i componentwise .

10. Suppose H is the only subgroup of order $o(H)$ in the finite group G. Prove that H is a normal subgroup of G.

Chapter- 7

Group Homomorphism

Introduction

In this chapter, we shall be discussing about some type of functions from a group to another, that satisfy certain conditions and preserve some of the group features. We assume that readers are aware of basic definition and features of functions.

Definition: A mapping ϕ from a group $\langle G,* \rangle$ into a group $\langle G',*' \rangle$ called a homomorphism if for all $a, b \in G$ we have $\phi(a * b) = \phi(a) *' \phi(b)$

We shall omit the notation for $*$ and $*'$ and write $\phi(ab) = \phi(a)\phi(b)$ but it must be understood that product $a, b \in G$ so the operation between a and b is the operation on Gwhile the operation between $\phi(a)\ and\ \phi(b)$ is the operation in G'.

Definition: Two groups G and G' are said tobe homomorphic if there exists a homomorphism between them .

Definition: Let G, G' be two groups $x \in G, y \in G'$, $H \leq G$, $K \leq G'$. Then

(i) The image of $'x'$ under f is an element $y = f(x) \in G'$.
(ii) The image of H under f is the set $f(H) = \{ y \in G' \mid y = f(x)$ for some $x \in H \}$.
(iii) The inverse image of $'y'$ under f is the set
$f^{-1}(y) = \{ x \in G \mid f(x) = y \}$
(iv) The inverse image of K under f is the set
$f^{-1}(K) = \{ x \in G \mid f(x) \in K \}$

Note: Let A, B , C be three groups and $f: A \to B$, $g: B \to C$ be homomorphisms.

Then the composition $(g \circ f): A \to C$ is a homomorphism

Proof: Let $x, y \in A$

$$(g \circ f)(xy) = g\big(f(xy)\big) = g\big(f(x)f(y)\big) = g\big(f(x)\big)\ g\big(f(y)\big)$$
$$= (\boldsymbol{g \circ f})(\boldsymbol{x})\ (\boldsymbol{g \circ f})(\boldsymbol{y})$$

Therefore $(f \circ g)$ is a homomorphism.

Eg 1: Let G and G' be two groups with identity elements $e \; and \; e'$ respectively.

The two functions $f: G \to G'$ where $f(x) = e' \; \forall \; x \in G$ and $I: G \to G$ given by $I(x) = x \; \forall \; x \epsilon \; G$ are homomorphisms called trivial homomorphism

Proof: For $a, b \epsilon G$ we have $f(a) = e'$, $f(b) = e'$, $f(ab) = e'$
Therefore $f(ab) = e' = e' \cdot e' = f(a) \cdot f(b)$

Eg 2: let G be a group of all real numbers under addition and let G' be a group of non zero real numbers under multiplication . Show that the map $\phi: G \to G'$ defined by $\phi(x) = 2^x$ is a homomorphism .

Proof: We have $\phi(a + b) = 2^{a+b} = 2^a \cdot 2^b = \phi(a) \cdot \phi(b)$

Eg 3: Let *G* be the group of integers under addition. A function $f: G \to G$ given by $f(x) = 2x$ is a homomorphism.

Proof: We have $f(a + b) = 2(a + b) = 2a + 2b = f(a) + f(b)$

Eg 3: Let G be a group of all 2×2 invertible real matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ under matrix multiplication and G' a group of all non-zero real numbers under multiplication . A map $f: G \to G'$ define by $f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \left|\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right|$ is a homomorphism .

Proof : For $A, B \in G$

$f(AB) = |AB| = |A||B| = f(A)f(B)$

Lemma: Let G be a group and N a normal subgroup of G .
A map $f: G \to \frac{G}{N}$ given by $f(x) = Nx$ is a homomorphism of G onto $\frac{G}{N}$.

Proof: If $X \epsilon \frac{G}{N}$ then $X = Nx$ where $x \epsilon G$

i.e $x = f(x)$ so that f is onto .

Also $If \; a, b \epsilon G$ we have $f(ab) = Nab = NaNb = f(a)f(b)$

Therefore f is a homomorphism of G onto $\frac{G}{N}$

Theorem7.01 (Identity Preservation) : Let ϕ be a homomorphism of G into G'. Then $\phi(e) = e'$ where e, e' are the identity elements of G and G' respectively

***Proof* :** We have $\phi(e)\phi(e) = \phi(ee) = \phi(e) = \phi(e)e'$

By left cancellation law we have $\phi(e) = e'$

Theorem 7.02: (Inverse Preservation) : Let ϕ be a homomorphism of G into G' . Then $\phi(a^{-1}) = \big(\phi(a)\big)^{-1}$ for any $a \in G$

***Proof* :** For $a \in G$

We have $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e'$

Multiplying by $\big(\phi(a)\big)^{-1}$ from the left we have

$$\phi(a^{-1}) = \big(\phi(a)\big)^{-1}$$

Theorem 7.03: Let ϕ be a homomorphism of G into G' and let $g \in G$. If g is of finite order then the order of $\phi(g)$ divides the prder of g .

i.e $o\big(\phi(g)\big) \mid o(g)$

***Proof* :** Let $o(g) = n$
Now $\big(\phi(g)\big)^n = \phi(g^n) = \phi(e) = e$
$\Rightarrow o\big(\phi(g)\big) \mid n$

Definition: If ϕ is a homomorphism of G into G', the *kernel of* ϕ is defined by $Ker(\phi) = \{x \in G : \phi(x) = e'\}$ where e' is the identity element of G'. **(Note :** the kernel is never empty as the identity element is in the kernel)

Example: For a map $f: G \to G'$ define by $f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \left|\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right|$ where G is the set of invertible 2×2 real matrices and G' the set of non zero real numbers, the kernel is given by $K = \{ A \in G : |A| = 1 \}$

Theorem 7.04: Let ϕ be a homomorphism of G into G' with kernel K. Then K is a normal subgroup of G.

Proof: Let $a, b \in G$

Then $\phi(a) = \phi(b) = e'$

$\Rightarrow \phi(b^{-1}) = \big(\phi(b)\big)^{-1} = e'^{-1} = e'$

Now $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = e'e' = e'$

$\Rightarrow ab^{-1} \epsilon K$

Therefore K is a subgroup of G

Let $k \epsilon K$ and $g \epsilon G$

Then $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e'\phi(g^{-1}) = \phi(g)\big(\phi(g)\big)^{-1} = e'$

Therefore $gkg^{-1} \epsilon K$

Hence K is normal in G

Theorem 7.05: Let $\phi: G \to G'$ be an onto homomorphism with kernel K and $y \epsilon G'$. The set of all inverse image of y in G is given by $Kx_0 = \{kx_0 : k \epsilon K\}$ where x_0 is any particular inverse image of y i.e $\phi(x_0) = y$.

Proof

Let $a \epsilon \phi^{-1}(y)$ then $\phi(a) = y$

Now $a = (ax_0^{-1})x_0$

and $\phi(ax_0^{-1}) = \phi(a)\phi(x_0^{-1}) = \phi(a)(\phi(x_0)^{-1}) = yy^{-1} = e'$

$\Rightarrow ax_0^{-1} \epsilon K$

Hence $a = (ax_0^{-1})x_0 \epsilon Kx_0$

Therefore $\phi^{-1}(y) \subseteq Kx_0$

Conversely, let $b \epsilon Kx_0$ then $b = kx_0 : k \epsilon K$

Now $\phi(b) = \phi(kx_0) = \phi(k)\phi(x_0) = e'y = y$ as

$k \epsilon K, \phi(k) = e'$

$\Rightarrow b \epsilon \phi^{-1}(y)$

$\Rightarrow Kx_0 \subseteq \phi^{-1}(y)$

hence $Kx_0 = \phi^{-1}(y)$

Isomorphism

Definition: A homomorphism $\phi : G \to G'$ is called an isomorphism if ϕ is one-one and onto .

Definition: Two groups G and G' are said tobe isomorphic if there exists an isomorphism between them . If G and G' are isomorphic , we write $\boldsymbol{G \cong G'}$.

Theorem 7.06: An onto homomorphism $\phi : G \to G'$ with kernel K is an isomorphism if and only if $K = \{e\}$.

Alternatively , a homomorphism $\phi : G \to G'$ with kernel K *is* one-one if and only if $K = \{e\}$

***Proof* :** Let ϕ be an isomorphism . Therefore ϕ is 1-1 .

Let $x \in K$. Then $\phi(x) = e'$. Also $\phi(e) = e'$

As ϕ is 1-1 we have $x = e$ i.e $K = \{e\}$.

Conversely , Let $K = \{e\}$
Let x_1 , $x_2 \in G$ such that $\phi(x_1) = \phi(x_2)$

now $\phi(x_1) = \phi(x_2) \Rightarrow \phi(x_1)(\phi(x_2)^{-1}) = e' \Rightarrow \phi(x_1)\phi(x_2^{-1}) = e'$

$\Rightarrow \phi(x_1 x_2^{-1}) = e' \Rightarrow x_1 x_2^{-1} \in K = \{e\}$

$\Rightarrow x_1 x_2^{-1} = e \Rightarrow x_1 = x_2$

Hence ϕ is one-one .

Cayley's Theorem: Every group is isomorphic to a group of permutations.

Proof : Let G be a group .

For $g \in G$, let $T_g : G \to G$ be a map defined by $T_g(x) = gx \ \forall x \in G$

If $T_g(x_1) = T_g(x_2)$ for $x_1 , x_2 \in G$

Then $gx_1 = gx_2 \Rightarrow x_1 = x_2$, so T_g is one-one .

For any $x \in G$, we have $y = g^{-1}x \in G$ and $T_g(y) = gy = g(g^{-1}x) = x$

showing that T_g is onto and so a permutation on G .

Also $T_{ab}(x) = (ab)x$ and $(T_a \circ T_b)(x) = T_a\big(T_b(x)\big) = T_a(bx) = a(bx) = (ab)x$

$\Rightarrow T_{ab} = T_a T_b$ ……..(1)

Now let $G' = \{ T_g : g \in G \}$

Define $f : G \to G'$ by $f(g) = T_g$

We have , $f(a) = f(b) \Rightarrow T_a = T_b \Rightarrow T_a(e) = T_b(e) \Rightarrow a = b$

So , f is one-one .

f is clearly onto since $T_y \in G' \Rightarrow y \in G \Rightarrow f(y) = T_y$

Finally ,for $a , b \in G$ we have $f(ab) = T_{ab} = T_a T_b = f(a)f(b)$

This completes the proof that f is an isomorphism .

So G is isomorphic to G' .

** **Let A , B , C be three groups and $f: A \to B$, $g: B \to C$ be isomorphisms.**

Then the composition $(g \circ f): A \to C$ is a isomorphism.

Proof: The composition of two homomorphisms is a homomorphism therefore $(f \circ g)$ is a homomorphism. Also the composition of bijective functions is a bijective functions , Therefore $(f \circ g)$ is 1-1 and onto Hence $(f \circ g)$ is an isomorphism

Theorem 7.06: Let $f: G \to G'$ be an isomorphism . Then $f^{-1} : G' \to G$ is also an isomorphism.

proof: Let $y , z \in G'$

Since f is an isomorphism so onto , therefore there exist $a , b \in G$ such that

$f(a) = y , f(b) = z$

Now

$f^{-1}(yz) = f^{-1}\big(f(a)f(b)\big) = f^{-1}\big(f(ab)\big) = ab = f^{-1}\big(f(a)\big)\ f^{-1}\big(f(b)\big) = f^{-1}(y)\ f^{-1}(z)$

Therefore f^{-1} is a homomorphism

Also we know that the inverse of a bijective function is bijective , therefore f^{-1} is an isomorphism .

Theorem 7.07: If $\phi: G - G'$ be an isomorphism , then

(i) $\phi(e) = e'$. (Isomorphism preserves identity).

(ii) $\phi(a^n) = \big(\phi(a)\big)^n$

(iii) If $a \in G$ is of finite order then $o(a) = o\big(\phi(a)\big)$

Proof (i) and (ii) : ϕ is a homomorphism and so $\phi(e) = e'$, $\phi\,(a^n) = \big(\phi(a)\big)^n$.

Proof (iii) : Let $o(a) = m$, $o\big(\phi(a)\big) = n$

Then $e' = \big(\phi(a)\big)^n = \phi(a^n) = \phi(e)$

As ϕ is 1-1 we have , $a^n = e$. Since $a(a) = m$

Therefore $m|n$

Also $\big(\phi(a)\big)^m = \phi(a^m) = \phi(e) = e'$

Since $o\big(\phi(a)\big) = n$ we have $n|m$

Hence $m = n$.

Theorem 7.08: If $\phi : G \to G'$ is an isomorphism then $G = \langle a\rangle \Leftrightarrow \mathrm{G}' = \langle\phi(a)\rangle$

To prove $G = \langle a\rangle \Rightarrow \mathrm{G}' = \langle\phi(a)\rangle$

Let $y \in G'$. Then $y = \phi(a)$: $x \in G$.

But $x = a^m$ for some m .

$\Rightarrow y = \phi(a^m) = \big(\phi(a)\big)^m$

$\Rightarrow \mathrm{G}' = \langle\phi(a)\rangle$

Conversely to prove $\mathrm{G}' = \langle\phi(a)\rangle \Rightarrow G = \langle a\rangle$

$x \in G \Rightarrow \phi(x) \in G' \;\Rightarrow\; \phi(x) = \big(\phi(a)\big)^n$ for some n .

$\Rightarrow \phi(x) = \phi(a^n) \Rightarrow x = a^n$ as ϕ is one -one .
$\Rightarrow G = \langle a \rangle$

Theorem 7.09: Let $\phi : G \to G'$ be an isomorphism , $a \in G$. For a fixed integer m , if the equation $x^m = a$ has a solution in G then the equation $x^m = \phi(a)$ has the same number of solutions in G' as $x^m = a$.

Proof: If $x_0 \in G$ is a solution of $x^m = a$ then $\big(\phi(x_0)\big)^m = \phi(x_0^m) = \phi(a)$
Therefore $\phi(x_0)$ is a solution of $x^m = \phi(a)$.

Theorem 7.10: (Isomorphism preserves commutativity).

If G and G' are isomorphic then G is abelian if and only if G' is abelian .

***Proof* :** $\phi: G \to G'$ be an isomorphism .

Let G be abelian .

Let $y, z \in G'$. As ϕ is onto , $y = \phi(a)$, $z = \phi(b)$, a , $b \in G$

$xy = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = yx$

$\Rightarrow$ G' is abelian .

Conversely , let G' be abelian .

We have $\phi(ab) = \phi(a)\phi(b) = \phi(b)\phi(a) = \phi(ba)$

As ϕ is one-one we have $ab = ba$

Hence G is abelian .

Theorem 7.11: (isomorphism preserves cyclicity) .

If G and G' are isomorphic then G is cyclic if and only if G' is cyclic .

Proof : $\phi: G \to G'$ be an isomorphism .

Let $G = \langle a \rangle$ be cyclic generated by $'a'$

Let $y \in G'$. By onto of ϕ , $y = \phi(x) :\ x \in G$.

But $x = a^n$ for some integer n .

Therefore , $y = \phi(x) = \phi(a^n) = \big(\phi(a)\big)^n$

Thus G' is cyclic generated by $\phi(a)$.

Conversely , let $G' = \langle b \rangle$ be cyclic generated by $'b'$.

Since $b \in G'$, by onto of ϕ , $b = \phi(a)$ for $a \in G$.

Let $g \in G$. Then $\phi(g) \in G' \Rightarrow \phi(g) = b^m$

$= \big(\phi(a)\big)^m = \phi(a^m)$ for some integer m

As ϕ *is* $1-1$ we have $g = a^m$ showing that G is cyclic generated by $'a'$.

This theorem can also be stated as

Theorem 7.12: (isomorphism preserves subgroups) .

If $\phi : G \to G'$ be an isomorphism and $A \leq G$, $B \leq G'$ then

$\phi(A)$ is a subgroup of G' and $\phi^{-1}(B)$ is a subgroup of G .

Proof **:** We shall prove the first part only namely that $\phi(A)$ is a subgroup .
The second follows by considering ϕ^{-1} being an isomorphism from $G' \to G$.

Let $y, z \in \phi(A)$

$\Rightarrow y = \phi(a),\ z = \phi(b) \ : \ a, b \in A$

$\Rightarrow z^{-1} = \big(\phi(b)\big)^{-1} = \phi(b^{-1})$

Now $yz^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(A)$ as $ab^{-1} \in A$.

This proves that $\phi(A)$ is a subgroup of G' .

Theorem 7.13: (isomorphism preserves the center) .
If $\phi : G \to G'$ be an isomorphism and $Z(G), Z(G')$ be the centers of G and G' respectively . then $\phi\big(Z(G)\big) = Z(G')$.

Proof: let $z \in \phi\big(Z(G)\big) \Rightarrow z = \phi(x) : \ x \in Z(G)$

Let $y \in G' \Rightarrow y = \phi(a) : a \in G$ since ϕ is onto .

Now , $yz = \phi(a)\phi(x) = \phi(ax) = \phi(xa) = \phi(x)\phi(a) = zy$

$\Rightarrow z \in Z(G')$

Therefore $\phi\big(Z(G)\big) \subseteq Z(G')$

Conversely , Let $y \in Z(G')$

$\Rightarrow \ y = \phi(a) \ : \ a \in G$

Let $x \in G$

Then $\phi(xa) = \phi(x)\phi(a) = \phi(a)\phi(x)$ as $\phi(a) = y \in Z(G')$

$= \phi(ax)$

As ϕ is one-one , we have , $xa = ax$

$\Rightarrow a \in Z(G)$

$\Rightarrow y = \phi(a) \in \phi\left(Z(G)\right)$

$\Rightarrow Z(G') \subseteq \phi\left(Z(G)\right)$

Therefore $\phi\left(Z(G)\right) = Z(G')$

Classification of groups of order 3

Let G be a group of order 3 . G is cyclic as 3 is a prime ,

Hence $G = \langle a \rangle = \{ e, a , a^2 \}$

Consider a map $f : G \to Z_3$ where $Z_3 = \{0,1,2\}$ is a group of integers mod 3 .

defined by $f(a^r) = r$ ($note\ f(e) = f(a^0) = 0$

We have so define f tobe an isomorphism (verify) .

Hence G is isomorphic to Z_3 .

As this G is the only form of group of order 3 , we conclude that

" Every group of order 3 is isomorphic to Z_3 "

In other words , there is only one group (upto isomorphism) of order 3 .

Classification of groups of order 4

Let G be a group of order 4 . Then G is abelian .

For any $x \in G$, $x \neq e$, we shall always have $o(x) | 4$

Therefore , $o(x) = 2$ or $o(x) = 4$

Case I: If $o(x) = 4$ then G is cyclic .

Let $G = \langle a \rangle = \{ e , a , a^2, a^3\}$

As above , Define a map $f : G \to Z_4$ by $f(a^r) = r$

This is an isomorphism , so that cyclic groups of order 4 are isomorphic to Z_4.

Case II: If $o(x) = 2 \ \forall \ x \in G \ , x \neq e$

In this case , G will be of the form

$G = \{ e, a, b , c \}$ which is the Klein's 4 group .

We define $f ; G \to Z_2 \times Z_2$ by

$f(e) = (0,0)$, $f(a) = (1,0)$, $f(b) = (0,1)$, $f(c) = (1,1)$

By computation, we have , $f(ab) = f(c) = (1,1) = (1,0) + (0,1) = f(a) + f(b)$ and etc .. .so that f is a homomorphism . It is clear that f is 1-1 and onto.

Hence G is isomorphic to $Z_2 \times Z_2$

In other words , there are two groups (upto isomorphism) of order 4 namely Z_4 and $Z_2 \times Z_2$.

****Automorphism is an isomorphism from a group onto itself**

Theorem/definition 7.14: Let G be a group and $g \in G$ be a fixed element .A map $T_g : G \to G$ defined by $T_g(x) = gxg^{-1}$ is an isomorphism called an **Inner automorphism**.

Proof: Let $a , b \in G$

We have $T_g(ab) = g(ab)g^{-1} = (ga)(bg^{-1}) = (gag^{-1}g)(bg^{-1})$

$= (gag^{-1})(gbg^{-1}) = T_g(a)T_g(b)$ therefore T_g is a homomorphism

$T_g(x) = T_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow x = y$ by cancellation law

Therefore T_g is one-one .
Let $y \in G$, since $g \in G$ we have $g^{-1}yg \in G$
and $T_g(g^{-1}yg) = g(g^{-1}yg)g^{-1} = y$ showing that T_g is onto
Hence T_g is an isomorphism .

The group of automorphisms on G : $A(G)$

Let G be a group . Let $A(G)$ be the collection of all automorphisms on G .

i.e $A(G) = \{f \mid f: G \to G$ is an isomorphism $\}$
Then $A(G)$ is a group under composition of functions

***Proof* :**
The composition of automorphisms is an automorphism (closure property)
The identity function $I: G - G$, $I(x) = x \; \forall \; x \in G$ is an identity function we know that composition of functions is associative. Also the inverse of an automorphism is an automorphism
$\therefore A(G)$ is a group .

7.15: Fundamental Homomorphism theorem(First Isomorphism theorem)

Let $\phi: G - G'$ be an onto group homomorphism with kernel K .

Then $\frac{G}{K}$ is isomorphic to G'. $\left(\frac{G}{K} \cong G'\right)$.

Proof : As $\phi: G \to G'$ is onto , every element of G' has pre-image .
i.e $every$ element of G' are of the form $\phi(x): \; x \epsilon \; G$
We define a function $\psi: \frac{G}{K} \to G'$ as $\psi(Kx) = \phi(x)$

We first have to show that ψ is well-defined
We have $Kx_1 = Kx_2 \; \epsilon \; \frac{G}{K}$
$\Rightarrow x_1 x_2^{-1} \epsilon \; K$
$\Rightarrow \phi(x_1 x_2^{-1}) = e'$
$\Rightarrow \phi(x_1)\phi(x_2^{-1}) = e'$
$\Rightarrow \phi(x_1)\left(\phi(x_2)\right)^{-1} = e'$
$\Rightarrow \phi(x_1) = \phi(x_2)$
$\Rightarrow \psi(Kx_1) = \psi(Kx_2)$
Hence ψ is well-defined

To Show that ψ is ahomomorphism

We have $\psi(Kx_1 Kx_2) = \psi(Kx_1 x_2)$ as K is normal

$= \phi(x_1x_2) = \phi(x_1)\phi(x_2)$ as ϕ is a homomorphism

$= \psi(Kx_1)\psi(kx_2)$

Hence ψ is a homomorphism .

To Show that ψ is one-one

Let Kx_1 , Kx_2 ϵ $\frac{G}{K}$ such That $\psi(Kx_1) = \psi(Kx_2)$

Now $\psi(Kx_1) = \psi(Kx_2) \Rightarrow \phi(x_1) = \phi(x_2)$

$\Rightarrow \phi(x_1)\big(\phi(x_2)\big)^{-1} = e'$

$\Rightarrow \phi(x_1)\phi(x_2^{-1}) = e' \Rightarrow \phi(x_1x_2^{-1}) = e'$ as ϕ is a homomorphism .

$\Rightarrow x_1x_2^{-1}\, \epsilon\, K$

$\Rightarrow Kx_1 = Kx_2$ so that ψ is one-one

Hence ψ is an isomorphism .

i.e $\frac{G}{K} \cong G'$

…….

For an alternative statement :
We know that if $\phi: G \to G'$ is a function , then $\phi: G \to \phi(G)$ is always onto . Replacing G' by $\phi(G)$ above , we have the full proof .

7.16: Second Isomorphism theorem

Let N be a normal subgroup of G and K be a subgroup of G . Then

(i). $KN = NK \leq G$ (here $\leq$ stands for subgroup)

(ii). $N \lhd KN$

(iii). $(N \cap K) \lhd K$

(iv). $\frac{K}{N \cap K} \cong \frac{NK}{N}$

Proof : (i)

Let $x \epsilon KN$

Then $x = kn :\ k\epsilon K\ ,\ n\epsilon N$

Now $x = kn = (kn)e = (kn)(k^{-1}k) = (knk^{-1})k$

As $K \subseteq G$ therefore

$k \epsilon K \Rightarrow\ k \epsilon\ G$

Hence $knk^{-1} \epsilon\ N$ as N is normal

I.e $knk^{-1} = n' \epsilon N$

Therefore $x = (knk^{-1})k = n'k \epsilon NK$

Hence $KN \subseteq\ NK$

In a similar way we can show that $NK \subseteq KN$

So that $NK = KN$

Now let $a, b \epsilon KN$

Therefore $a = k_1 n_1\ ,\ b = k_2 n_2\ :\ k_1, k_2\ \epsilon K\ ,\ n_1\ ,\ n_2 \epsilon\ N$

$(ab^{-1}) = (k_1 n_1)(k_2 n_2)^{-1} = (k_1 n_1)(n_2^{-1} k_2^{-1}) = k_1 (n_1 n_2^{-1}) k_2^{-1}$

$= k_1 n_3 k_2^{-1}$ (where $n_3 = n_1 n_2^{-1} \epsilon\ N$)

$= (k_1 k_2^{-1})(k_2 n_3 k_2^{-1})$

$= kn\ \epsilon\ KN$ (where $k = k_1 k_2^{-1}\ \epsilon K\ ,\ n = k_2 n_3 k_2^{-1} \epsilon\ N$ as N is normal)

i.e $ab^{-1}\ \epsilon\ KN\ for\ any\ a\ ,\ b\ \epsilon KN$

Hence KN is a subgroup of G

Proof of (ii)

To show that N is normal in KN we only have to show that N is a subset of KN

We have $n \epsilon N \Rightarrow\ n = en :\ e \epsilon K\ ,\ n \epsilon N$

$\Rightarrow n\epsilon\ KN$

Therefore $N \subseteq\ KN$

Proof of (iii)

We have $N \cap K\ \subseteq\ K$ always

Also , intersection of subgroups is subgroup .

Let $k\ \epsilon K$ and $a \epsilon N \cap K$

$\Rightarrow k \epsilon G\ ,\ a \epsilon N$ and $a \epsilon K$

Now $kak^{-1} \epsilon\ N$ as N is normal

Also $kak^{-1} \epsilon K$ *as* both k , $a \epsilon K$

Hence $kak^{-1} \epsilon N \cap K$

Therefore $N \cap K$ is normal in K .

Proof of (iv)

Any element of $\frac{NK}{N}$ are of the form $Ny : y \epsilon NK$

Now $y \epsilon NK \Rightarrow y = nk : n \epsilon N , k \epsilon K$

Therefore $Ny = N(nk) = (Nn)k = Nk$

We now define a map $\phi: K \to \frac{NK}{N}$

as $\phi(k) = Nk$

We first have to show that ϕ is well defined

$k_1 = k_2 \epsilon K \Rightarrow k_1 k_2^{-1} = e' \epsilon N \Rightarrow Nk_1 = Nk_2 \Rightarrow \phi(k_1) = \phi(k_2)$

Therefore ϕ is well defined

We next show that ϕ is a homomorphism

Let k_1 , $k_2 \epsilon K$

Then $\phi(k_1 k_2) = Nk_1 k_2 = (Nk_1)(Nk_2) = \phi(k_1)\phi(k_1)$

Therefore ϕ is a homomorphism .

Again if $Ny \epsilon \frac{NK}{N}$ where $y \epsilon NK$

Then $Ny = N(nk) = (Nn)k = Nk$ where $n \epsilon N , k \epsilon K$

$= \phi(k)$

Therefore ϕ is onto.

To find the kernel of ϕ . (note that identity element of $\frac{NK}{N}$ *is* N *therefore*

Kernel of $\phi = \{ k \epsilon K : \phi(k) = N \}$)

Now $k \epsilon Ker(\phi)$

$\Leftrightarrow \phi(k) = N$

$\Leftrightarrow Nk = N$

$\Leftrightarrow k \in N$

$\Leftrightarrow k \in N \cap K$ as $k \in K$

hence $Ker(\phi) = N \cap K$

Using The first isomorphism theorem,

we have $\frac{K}{N \cap K} \cong \frac{KN}{N}$

(Note: Statement (iv) can be written as $\frac{\boldsymbol{K}}{\boldsymbol{N} \cap \boldsymbol{K}} \cong \frac{\boldsymbol{KN}}{\boldsymbol{N}}$

Notice that $KN = NK$ and so any element of $\frac{KN}{N}$ is of the form

Ny: $y \in KN$

Now $y \in KN \Rightarrow y \in NK \Rightarrow y = nk$ as before)

7.17: Third Isomorphism theorem

Let N and K be normal subgroups of G and N be normal in K .

Then $\frac{K}{N}$ is normal in $\frac{G}{N}$ and $\frac{G}{K} \cong \frac{\left(\frac{G}{N}\right)}{\left(\frac{K}{N}\right)}$

***Proof* :** we have $K \subseteq G \Rightarrow \frac{K}{N} \subseteq \frac{G}{N}$

Let $a = Nk_1, b = Nk_2 \in \frac{K}{N}$ where $k_1 , k_2 \in K$

Then $ab^{-1} = (Nk_1)(Nk_2^{-1}) = N(k_1k_2^{-1}) \in \frac{K}{N}$

Therefore $\frac{K}{N}$ is a subgroup of $\frac{G}{N}$

We now define a function $\phi: \frac{G}{N} \to \frac{G}{K}$ by

$\phi(Ng) = Kg$

We first show that ϕ is well defined .
Let $Ng_1 = Ng_2$

$\Rightarrow g_1g_2^{-1} \in N$

$\Rightarrow g_1 g_2^{-1} \ \epsilon \ K$ as $N \subseteq K$

$\Rightarrow Kg_1 = Kg_2 \Rightarrow \phi(Ng_1) = \phi(Ng_2)$

Therefore ϕ is well defined

we shall show that ϕ is a homomorphism .

We have $\phi(NaNb) = \phi(Nab) = Kab = KaKb = \phi(Na)\phi(Nb)$

Therefore ϕ is a homomorphism .

Again every element of $\frac{G}{K}$ is of the form $Kg \ : \ g \epsilon G$

and $Kg = \phi(Ng) : Ng \ \epsilon \frac{G}{N}$ so that ϕ is onto

We proceed to find the Kernel of ϕ

We have $Ker(\phi) = \{ Nx \ \epsilon \ \frac{G}{N} : \ \phi(Nx) = K\}$ K is the identity element in $\frac{G}{K}$

Now $Nx \ \epsilon \ Ker(\phi)$

$\Leftrightarrow \phi(Nx) = K \ \Leftrightarrow Kx = K \Leftrightarrow x \epsilon K \Leftrightarrow Nx \epsilon \frac{K}{N}$

Thus $Ker(\phi) = \frac{K}{N}$

Using The first isomorphism theorem ,

we have $\frac{\left(\frac{G}{N}\right)}{Ker(\phi)} \cong \frac{G}{K}$ or $\frac{\left(\frac{G}{N}\right)}{\left(\frac{K}{N}\right)} \cong \frac{G}{K}$

Exercise

1. Let G be a group of all positive real numbers under multiplication and G' a group of all real numbers under addition . The map $f: G \to G'$ given by $f(x) = \log_{10} x$ is a homomorphism .

2. Show that The map $f: R \to R'$ given by $f(x) = e^x$ is a homomorphism where R' is the set of positive real numbers excluding $'0'$.

3. Show that $I(G)$ the set of all inner automorphism on G is normal subgroups of $A(G)$

4. Let R' be the group of positive real numbers under multiplication. Show that the mapping $f(x) = \sqrt{x}$ is an automorphism of R'.

5. If a group G is isomorphic to H, prove that $Aut(G)$ is isomorphic to $Aut(H)$.

6. Let $U(16)$ be the group of units modulo 16. Show that $\phi: U(16) \to U(16)$, $\phi(x) = x^3$ is an automorphism .

7. Let ϕ and ψ be two isomorphism from a cyclic group $G = \langle a \rangle$ to another cyclic group G' . If $\phi(a) = \psi(a)$, show that $\phi(x) = \psi(x)$ $\forall$ $x \in G$

Chapter- 8

Rings

In this chapter, we will introduce another algebraic system different from group which is a two-operational system called ring.

8.1Definition: Let R be a non – empty set on which two operations denoted by + and are defined, satisfying the following properties:

i) $a + b \in R \ \forall \ a, b \in R$
ii) $a + b = b + a \ \forall \ a, b \in R$
iii) $(a + b) + c = a + (b + c) \ \forall \ a, b, c \in R$
iv) There is an element 0 in R such that $a + 0 = 0 + a = a \ \forall a \in R$
v) $\forall a \in R$, there exist $-a \in R$ such that $a + (-a) = 0 = (-a) + a$
vi) $a.b \in R, \forall a, b \in R$
vii) $a.(b.c) = (a.b).c \ \forall \ a, b, c \in R$
viii) $a.(b + c) = a.b + a.$ and $(a + b).c = a.c + b.c \ \forall \ a, b, c \in R$

[Left and right distributive laws of multiplication over addition]

Then, $(R; +, .)$ is called an ***associative ring.***

A ring $(R; +, .)$ such that $a.b = b.a \ \forall \ a, b \in R$ is called a ***Commutative ring.***

A ring $(R; +, .)$ where there exist $1 \in R$ such that $a.1 = 1.a = a, \ \forall a \in R$ is called a ***ring with unity***.

8.1.1 *Examples of rings*

1. $R = (\mathbb{Z}; +, .)$, the set of integers is a commutative ring with a unit element.
2. $R = (2\mathbb{Z}; +, .)$, the set of even integers is a commutative ring without unity.
3. $R = (\mathbb{Q}; +, .)$, the set of rational numbers is a commutative ring with unity.
4. $R = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$, the set of integers modulo 7 is a commutative ring with unit element.

8.1.2 *Types of rings*

Definition: Let R be a ring, $a \in R,\ a \neq 0$ is said to be a ***zero divisor*** if there exist $b \in R$, $b \neq 0$ such that $a \,.\, b = 0$.

In $(R = \mathbb{Z}_6\ ;\ +_6\ ,\cdot_6) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$, $\bar{2}$ and $\bar{3}$ are zero divisors in $\mathbb{Z}_6$.

Definition: A commutative ring R is said to be an ***Integral domain*** if R has no zero divisors.

1. $(\mathbb{Z};\ +\ ,\ .\ )$ is an integral domain.
2. $(\mathbb{Z}_m\ ;\ +_m\ ,\cdot_m\ )$ is not an integral domain when m is composite.

Definition: If the non – zero elements of a ring R form a multiplicative group, then R is said to be a ***division ring.***

Definition: A commutative division ring is called a ***field.***

Definition: A non – commutative division ring is called a ***skew – field.***

8.1.3 *Examples*

1. $(\mathbb{Z};\ +\ ,\ .\ )$ is not a division ring.
2. $(\mathbb{R};\ +\ ,\ .\ )$ is a field.
3. $(\mathbb{Q};\ +\ ,\ .\ )$ is a field .
4. $(\mathbb{C};\ +\ ,\ .\ )$ is a field.
5. $\left(\mathbb{Z}_p\ ;\ +_p\ ,\cdot_p\right)$, p a prime, is a field. This is an example of a finite field.
6. Consider the set $C = \mathbb{R} \times \mathbb{R} = \{\ (\alpha\ ,\beta)\ ;\ \alpha\ ,\beta\ \in \mathbb{R}\}$
   We define,

   $(\ \alpha\ ,\beta)\ =\ (\gamma, \delta)$ if and only if $\alpha\ =\ \gamma$ and $\beta\ =\ \delta$

   and $(\alpha\ ,\ \beta\ ) + (\ \gamma\ ,\ \delta\ ) = (\ \alpha + \gamma\ ,\ \beta + \delta\ )$ as addition in C .

   Then (0,0) is the identity element and for $(\ \alpha\ ,\beta)\ \in\ C, (-\alpha\ ,-\beta)\ \in C$ is the inverse.

Thus, with respect to addition defined above, C is an abelian group.

Now, define a multiplication '.' as follows:

$$(\ \alpha\ ,\beta)\ .\ (\ \gamma, \delta)\ =\ (\ \alpha\gamma\ -\ \beta\delta, \alpha\delta\ +\ \beta\gamma)$$

The element $(1, 0)$ is the unit element.

If $(\alpha, \beta) \neq (0,0)$, then $\alpha^2 + \beta^2 \neq o$ and the element $\left(\frac{\alpha}{\alpha^2+\beta^2}, \frac{-\beta}{\alpha^2+\beta^2}\right)$ is the multiplicative inverse of (α, β).

Thus $C - (0,0)$ is a commutative group with respect to multiplication.

Hence, $(C, +, .)$ is a field called ***the field of complex numbers.***

The real quaternions

Put $Q = \{(a, b, c, d) \mid a, b, c, d \in \mathbb{R}\}$

In $Q, (a, b, c, d) = (e, f, g, h)$ iff $a = e, b = f, c = g, d = h$.

Define an addition by,

$(a, b, c, d) + (e, f, g, h) = (a + e, b + f, c + g, d + h)$

Then $(0,0,0,0) \in Q$ is the identity.

For $(a, b, c, d) \in Q, (-a, -b, -c, -d) \in Q$ is the additive inverse.

Thus, with respect to this addition, Q is an abolian group.

Define a multiplication as follows:

Consider the elements of Q as symbols of the form $a + ib + jc + k d = (a, b, c, d)$ where i, j, k are such that $i^2 = j^2 = k^2 = 1$ and $ij = k, jk = i, ki = j, ij = -ji, jk = -kj, ki = -ik$.

This multiplication is not commutative.
This unit element is $(1,0,0,0)$.

If $(a, b, c, d) \neq (0,0,0,0)$, then $a^2 + b^2 + c^2 + d^2 \neq 0$ and its inverse is

$$\left(\frac{a}{a^2+b^2+c^2+d^2}, \frac{-b}{a^2+b^2+c^2+d^2}, \frac{-c}{a^2+b^2+c^2+d^2}, \frac{-d}{a^2+b^2+c^2+d^2}\right).$$

Therefore, $Q - (0,0,0,0)$ is a multiplicative non – commutative group and hence $(Q, +, .)$ is a skew – field called the "***Real quaternions***".

Lemma 8.1.4*: *If R is a ring, then for all $a, b \in R$,

i) $a.0 = 0.a = 0$
ii) $(-a).b = a.(-b) = -(a.b)$
iii) $(-a).(-b) = a.b$

If R has a unit element, then

iv) $(-1).a = -a$
v) $(-1).(-1) = 1$

Proof: i) If $\in R$, $a.0 = a.(0+0) = a.0 + a.0$

Since R is a group under addition, we get $a.0 = 0$.

ii) We see that $(a.b + (-a).b) = (a + (-a)).b$
$= 0.b$
$= 0$

$\Rightarrow (-a).b = -(a.b)$

Similarly, $a.(-b) = -(a.b)$

i) $(-a).(-b) = -(a.(-b))$ $(by\ (ii))$

$= -(-(a.b))$ $(by\ ii))$

$= a.b$

ii) $a + (-1).a = 1.a + (-1).a = \big(1 + (-1)\big).a = 0.a = 0$

$\Rightarrow (-1).a = -a.$

iii) Put $a = -1$ in (iv) we get,

$(-1).(-1) = -(-1) = 1.$

Lemma 8.1.5**:** *A finite integral domain is a field.*

Proof: Let $D = \{x_1, x_2, \ldots\ldots, x_n\}$ be a finite integral domain and let $x_1, x_2, \ldots\ldots, x_n$ be all its distinct elements.

Let $a \in D, a \neq 0$.

Consider the set $\{ax_1, ax_2, \ldots\ldots, ax_n\}$.

We claim that all these elements are distinct.

For if $ax_i = ax_j$

$\Rightarrow ax_i - ax_j = 0$

$\Rightarrow a(x_i - x_j) = 0$

But $a \neq 0$, and D is an integral domain,

So, $x_i - x_j = 0$ giving $x_i = x_j$.

Hence the elements of $\{ ax_1 , ax_2 , \ldots\ldots , ax_n \}$ are all distinct and so,

$$D = \{ ax_1 , ax_2 , \ldots\ldots , ax_n \}$$

i.e, every element of D can be expressed as ax_i for some $x_i \in D$.

In particular, $a = ax_{i0}$

We now claim that x_{i0} is the unit element of D.

Let $y \in D$. Then $y = ax_i$ for some i,

$$\therefore yx_{i0} = (ax_i)x_{i0}$$

$$= (x_i a)x_{i0}$$

$$= x_i(ax_{i0})$$

$$= x_i a$$

$$= ax_i$$

$$= y$$

Hence, x_{i0} is the unit element.

Let us denote $x_{i0} = 1$.

We can write $1 = ax_j$ for some j

$\Rightarrow x_j$ is the universe of a , since $a \neq o$ was an arbitrary element of D

Therefore, every non – zero element has an inverse.

Hence, D is a field.

Corollary: *$\mathbb{Z}_p$, p a prime, is a field.*

***Proof*:** Since $\mathbb{Z}_p$ is finite, by the above lemma it is enough to prove that $\mathbb{Z}_p$ is an integral domain.

Let $\bar{a}, \bar{b} \in \mathbb{Z}_p$ such that

$\bar{a} \cdot \bar{b} = 0$ and $\bar{a} \neq 0$

$\Rightarrow p \mid ab$

$\Rightarrow p \mid a \text{ or } p \mid b$

Since $\bar{a} \neq 0$, $p \nmid a$, and hence $p \mid b$

$\Rightarrow \bar{b} = 0$

Thus, $\mathbb{Z}_p$ is an integral domain and hence a field.

Problems

1. Prove that any field is an integral domain.
   Proof: Let F be a field. Let $a, b \in F$ be such that $a \neq 0$ and $a.b = 0$. Now, $a \neq 0$ and $a \in F$ implies that a^{-1} exist since F is a field. So,
   $a.b = 0$
   $\Rightarrow a^{-1}(a.b) = 0$
   $\Rightarrow (a^{-1}a)b = 0$
   $\Rightarrow \quad b = 0$
   $\Rightarrow F$ is an integral domain.

2. The set M of 2×2 matrices over the field of real numbers is a ring with respect to matrix addition and multiplication. Does this ring possess zero divisors? Justify your answer.

   Solution: The null matrix $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the zero element of this ring.

   Now $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ are two non-zero elements of this ring. i.e., $A \neq 0, B \neq 0$. We have

   $$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O.$$

   Thus the product of two non-zero elements of the ring is equal to the zero element of the ring. Therefore M is a ring with zero divisors.

3. Define integral domain. Prove that $\mathbb{Z}_n = \{0,1,2,\ldots,(n-1)\}$ w.r.t addition and multiplication modulo n is not an integral domain if n is not a prime.

Solution: Taking n=4, we have $\mathbb{Z}_4 = \{0,1,2,3\}$.

We see that 2.2=0 but 2≠0. Hence $\mathbb{Z}_4$ is not an integral domain.

4. Show that the set $\mathbb{Z}[i]$ of Gaussian integers (i.e. the set of complex numbers a+ib, where a and b are integers) forms a ring under ordinary addition and multiplication of complex numbers. Is it an integral domain? Is it a field? Justify your answer in each case.

Solution: Let $\mathbb{Z}$ [i] = {a + ib | a, b ∈ $\mathbb{Z}$, i^2 = -1} – the set of complex numbers a + ib where a and b are integers.

(a) Let a+ib, c+id be two elements in $\mathbb{Z}$ [i].

Then (a + ib)+(c+id)= (a+c)+i(b+d)

and (a + ib) (c+id) = (ac - bd) + i(ad + bc) , which are again members of $\mathbb{Z}$ [i].

Thus, $\mathbb{Z}$ [i] is closed with respect to addition and multiplication of complex numbers.

Further, in complex numbers both addition and multiplication are associative as well as commutative compositions. Also multiplication distributes with respect to addition.

The Gaussian integer 0+i0 is the additive identity.
The additive inverse of a+ib is (-a)+i(-b).
The Gaussian integer 1+i0 is the multiplicative identity.

Therefore the set of Gaussian integers is a commutative ring with unity for the given composition.

(b) $\mathbb{Z}$ [i] is an integral domain

Let x, y ∈ $\mathbb{Z}$ [i], x, y ≠ 0 , x = a + ib , y = c + id

Let xy = 0

⇒ (a + ib) (c+id) = 0

⇒ (ac - bd) + (ad + bc) i = 0

⇨ ac – bd = 0 and ad + bc = 0

⇨ ac=bd and ad=-bc

⇨ $adc = -bc^2$

⇨ $bd^2 = -bc^2$

⇨ $d^2 = -c^2$

⇨ d = 0 = c and consequently a=0,b=0

which is a contradiction since x and y ≠ 0.

∴ the product of two non-zero member of ℤ [i] cannot be zero.

Hence, ℤ [i] is an I.D.

(c) ℤ [i] is not a field since 2=2+0i does not possess an inverse.

For if 2(a+ib)=1, this implies that 2a=1 and a=1/2, which is not an integer.

8.2 Subring

Definition: Let $\{R, +, .\}$ be a ring. A non – empty subset S of R is called a ***subring*** of R if $\{S, +, .\}$ is a ring.

If R is any ring, then $\{0\}$ and R are always subrings of R. These are known as ***improper subrings*** of R.

Other subrings, if any, of R are called ***proper subrings*** of R.

***Theorem* 8.2.1:** *The necessary and sufficient conditions for a non – empty subset S of a ring R to be a subring of R are*

i) $a, b \in S \Rightarrow a - b \in S$
ii) $a, b \in S \Rightarrow ab \in S$

***Proof*:** The condition is necessary:

Let $(S, +, .)$ be a subring of $(R, +, .)$

Since S is a group with respect to addition, therefore $b \in S \Rightarrow -b \in S$.

Let $a, b \in S$. Then $a, -b \in S$ and so $a + (-b) \in S$

i.e $a - b \in S$, since S is closed under $+$.

Also, S is closed with respect to multiplication.

So, $a, b \in S \Rightarrow ab \in S$.

The condition is sufficient:

Suppose S is a non – empty subset of R such that i) and ii) are satisfied.

From i) $a, a \in S \Rightarrow a - a \in S$

i.e, $0 \in S$.

Now, since $0 \in S, a \in S$,

$\Rightarrow 0 - a \in S$

$\Rightarrow -a \in S$

i.e , each element of S possesses additive inverse .

Again, $a \in S, b \in S \Rightarrow a \in S, -b \in S$

So $a - (-b) \in S$ (by (i))

i.e $a + b \in S$

$\therefore S$ is closed with respect to addition.

Let $, b, c \in S$. Then $ab \in S$ (by (ii))

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

$a\,(b + c) = ab + ac$

$(b + c)\,a = ba + ca$

are true since $S \subseteq R$.

Hence S is a ring and so S is a subring of R.

***Theorem* 8.2.2:** *The intersection of two subrings of a ring R is a subring of R.*

Proof: Let A and B be two subrings of a ring R.

Clearly, $A \cap B$ is non – empty, since $0 \in A \cap B$.

Let $a, b \in A \cap B$.

Then $a, b \in A$ and $a, b \in B$.

Since A and B are subrings of R, $a - b \in A, ab \in A$ and $a - b \in B, ab \in$ B.

So, $a - b \in A \cap B$ and $ab \in A \cap B$.

Hence, $A \cap B$ is a subring of R.

Remark: *The union of two subrings of R need not be a subring of R.*

Definition: Let R be a ring. The ***centre of a ring*** R, denoted by $\boldsymbol{Z}(\boldsymbol{R})$, is defined as $Z(R) = \{a \in R : xa = ax \; for \; all \; x \in R\}$

***Theorem* 8.2.3:** *The centre of a ring R is a subring of R.*

***Proof*:** Since $0x = x0 \; \forall \, x \in R$, therefore $0 \in Z(R)$ is non – empty.

Let $a, b \in Z(R)$. Then

$xa = ax$ and $xb = bx \; \forall \; x \in R$

Now, $(a - b)\, x = ax - bx = xa - xb = x\,(a - b)$

Thus $(a - b)\, x = x\,(a - b) \; \forall \, x \in R$ implying that $a - b \in Z(R)$

Also, $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$

Hence, $(ab)x = x(ab) \; \forall \; x \in R$ implying that $ab \in Z(R)$.

Hence, $Z(R)$ is a subring of R.

Definition: Let S be a subset of a ring R. Then the smallest subring of R containing S is called the ***subring generated*** *by* S.

Definition: An integral domain D is said to be of ***characteristic 0*** if $ma = 0, a \neq 0 \in D, m$ is an integer, then $m = 0$.

Definition: An integral domain D is said to be of ***finite characteristic*** if there exist a positive integer m such that $ma = 0 \; \forall \; a \in D$.

The least such m is said to be the ***characteristic*** of D.

***Lemma* 8.2.4:** *The characteristic of a finite field is finite.*

***Proof*:** Let F be a finite field.

Let $o(F) = m, \; m > 0$

Then, $\underbrace{a + a + \cdots + a}_{m-times} = 0 \; \forall a \in F$

$\Rightarrow ma = 0$

$\Rightarrow F$ is of finite characteristic.

***Lemma* 8.2.5:** *If an integral domain is of finite characteristic, then its characteristic is prime.*

***Proof*:** Let D be an integral domain of finite characteristic p.

Suppose p is not prime. Then

$p = p_1 p_2$, where $p_1 \neq 1,\ p_2 \neq 0$ and $p_1 < p,\ p_2 < p$.
Let $a \neq 0, a \in D$.

Since D is an integral domain, $a^2 \neq 0$ and since p is the characteristic of D we have

$$0 = pa^2 = p_1 p_2 a^2$$

$$= p_1 \left(\underbrace{a^2 + a^2 + \cdots + a^2}_{p_2\ times} \right)$$

$$= (p_1 a) \left(\underbrace{a + a + \cdots + a}_{p_2\ times} \right)$$

$$= (p_1 a)(p_2 a)$$

As D is an integral domain, either $p_1 a = 0$ or $p_2 a = 0$, which is not possible as $p_1 < p,\ p_2 < p$.

Hence, p is a prime.

***Lemma* 8.2.6:** *In an integral domain, the left and right cancellation laws hold good.*

***Proof*:** Let D be an integral domain

Suppose $xa = xb,\ x \neq 0$

$\Rightarrow xa - xb = 0$

$\Rightarrow x(a - b) = 0$

$\Rightarrow a - b = 0$

$\Rightarrow a = b$

Hence, left and right cancellation laws hold good.

Definition: An element $'a'$ in a ring R is called ***idempotent,*** if $a^2 = a$.

Definition: An element $'a'$ in a ring R is called ***nilpotent*** if $a^n = 0$ for some positive integer n.

Remark: *If R is a ring with unity* 1, *then* 0 *and* 1 *are idempotent elements of* R. *Further* 0 *is always nilpotent.*

The element $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ in a 2×2 matrix ring is nilpotent.

Problems

1. If R is a ring such that $x^2 = x \; \forall \; x \in R$, prove that
   i) $x + x = 0 \; \forall \; x \in R \; i.e.,$ each element of R is its own inverse.
   ii) $x + y = 0 \Rightarrow x = y$
   iii) R is a commutative ring.

   Proof:
   i) Let $x \in R$, then

$$(-x)\,(-x) = (-x)^2 = -x$$

$$\text{and } (-x)(-x) = x^2 = x$$

$$\Rightarrow x = -x \quad \ldots(*)$$

   Hence, $x + x = 0 \; \forall \; x \in R$.

   ii) From i) we have $x + x = 0$

   Therefore, $x + y = 0 \Rightarrow x + y = x + x$

   $\Rightarrow y = x$, by left cancellation law for addition in R.

   iii) Let $a, b \in R$. Then

$$(a+b)^2 = a + b$$

$$\text{and} \quad (a+b)^2 = (a+b)(a+b)$$

$$= a^2 + ab + ba + b^2$$

$$\Rightarrow a + b = a + ab + ba + b$$

$$\Rightarrow ab + ba = 0$$

$$\Rightarrow ab = -ba = ba \quad (by\ (*))$$

Hence, R is commutative.

Definition: A ring R is called a ***Boolean Ring*** if all of its elements are idempotent i.e., if

$x^2 = x \forall x \in R.$

2. Prove that the only idempotent elements in an integral domain R with unity are 0 and 1. What happen if R is not an integral domain?

Solution: Let D be an integral domain.

Let $x \in D$ be idempotent.
i.e., $x^2 = x$

$\Rightarrow x^2 - x = 0$

$\Rightarrow x(x-1) = 0$

$\Rightarrow x = 0\ or\ x = 1$

Hence, the only idempotent elements in an integral domain R with unity are 0 and 1.

Let $R = \mathbb{Z}_{10}$, then R is not an integral domain and we see that $\bar{5}$, $\bar{6}$ are idempotent elements.

3. If R is an integral domain, then prove that R does not possess any non – zero nilpotent elements.

Solution: Let $a \neq 0 \in R$. Then

$a^n = 0 \Rightarrow aa^{n-1} = 0 \Rightarrow a^{n-1} = 0$

Continuing in this manner we get $a = 0$ which is a contradiction.

Thus, R does not possess any non – zero nilpotent elements.

8.3 Ideals

Definition: A non- empty subset S of a ring R is called a ***left ideal*** of R if

i) $a, b \in S$ implies $a - b \in S$
ii) $a \in S$ and $r \in R$ implies $ra \in S$

Definition: A non – empty subset S of a ring R is called a ***right ideal*** of R if

i) $a, b \in S$ implies $a - b \in S$
ii) $a \in S$ and $r \in R$ implies $ar \in S$

Definition: A non – empty subset S of a ring R is called an ***ideal*** or a ***two-sided ideal*** of R if

i) $a, b \in S$ implies $a - b \in S$
ii) $a \in S$ and $r \in R$ implies $ra \in S$ and $ar \in S$.

Remarks:

1) *In a commutative ring, every left ideal or right ideal is a two –sided ideal.*
2) *Since each ideal S of a ring R is a subgroup of the additive group $(R, +), 0 \in S$.*

***Example*:** If $R = \mathbb{Z}$ be a ring of integers and n be any integer, then $(n) = \{nx : x \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.

***Proof*:** Let , $b \in (n)$. Then $a = nx,\ b = ny$ for some integers x and y.

Now $a - b = nx - ny = n(x - y) \in (n)$

Let $r \in R = \mathbb{Z}$. Then $ra = r(nx) = rnx = n(rx)$

$\therefore ra = ar \in (n)$

Hence (n) is an ideal of $\mathbb{Z}$.

***Theorem* 8.3.1:** *Every ideal of a ring R is a subring of R.*

***Note*:** The converse of this theorem is not true.
Example: $R = \mathbb{Q}, S = \mathbb{Z}$

***Theorem* 8.3.2:** *The intersection of two ideals of a ring R is an ideal of R.*

Remark: *The union of two ideals of a ring R need not be an ideal of R.*

***Theorem* 8.3.3:** *If A and B are two ideals of a ring R, then,*

$$A + B = \{a + b : a \in A, b \in B\} \text{ is an ideal of } R.$$

***Proof*:** Let $a_1 + b_1,\ a_2 + b_2 \in A + B$.
Then, $a_1, a_2 \in A$ and $b_1, b_2 \in B$.
Since A and B are ideals of R, therefore they are subgroups of $(R, +)$
Therefore, $a_1, a_2 \in A \implies a_1 - a_2 \in A$
and $b_1, b_2 \in B \implies b_1 - b_2 \in B$
Consequently, $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in A + B$

Hence, $A + B$ is a subgroup of $(R, +)$.
Now let $r \in R$ and $a + b \in A + B$
Then $a \in A,\ b \in B$ and we have $r(a + b) = ra + rb \in A + B$.
Thus $A + B$ is an ideal of R.

Lemma* 8.3.4:Let R be a commutative ring with unity, whose only ideals are* (0) *and R itself. Then R is a field.*

***Proof*:** Let $x \in R,\ x \neq 0$.

Consider the set $Rx = \{rx | r \in R\}$

Clearly, $0 = 0x \in Rx$. So Rx is non – empty.

Let $r_1x, r_2x \in Rx$. Then

$r_1x - r_2x = (r_1 - r_2)x \in Rx$.

Also, if $rx \in Rx$ *and* $s \in R$, then

$s(rx) = (sr)x \in Rx$

And

$(rx)s = r(xs) = r(sx) = (rs)x \in Rx$

Hence Rx is an ideal of R.

Since the only ideals of R are (0) and R, we must have $Rx = (0)$ or $Rx = R$.

But $Rx = (0)$ is not possible since $1 \in R$ and $x \neq 0, 1.x = x \neq 0 \in Rx$.
Thus, we must have $Rx = R$.

i.e, every element of R can be written as rx for some $r \in R$.

In particular, $1 \in R$, can be written $r_0 x = 1$.

i.e, r_0 is the multiplicative inverse of x.

Since $x \neq 0$ was arbitrary, this means that every non – zero element of R has a multiplicative inverse.

Therefore, R is a field.

Problems

1. If R is a commutative ring and $a \in R$, then prove that the set $Ra = \{ra : r \in R\}$ is an ideal of R.

Solution: Let $r_1 a, r_2 a \in Ra$. Then

$$r_1 a - r_2 a = (r_1 - r_2)a \in Ra$$

Also if $r \in R, then\ r(r_1 a) = (rr_1)a \in Ra$

And $(r_1 a)r = r_1(ar) = r_1(ra) = (r_1 r)a \in Ra$

Thus Ra is an ideal of R.

2. Let R be a commutative ring, $a \in R, a \neq 0$. Let I= $\{x \in R | \ xa = 0\}$. Prove that I is an ideal of R. Give an example of R and $a \in R$ such that I$\neq \{0\}$.

Solution:

(a) I is a subgroup

Let $x, y \in I, a \in R, a \neq 0$.

Now,

$$\begin{aligned}(x - y)a &= xa - ya \\ &= 0 - 0 = 0 \\ &\Rightarrow x - y \in I.\end{aligned}$$

(b) I is a ideal

Let $r \in R, x \in I$. Then

$$(rx)a = r(xa) = r.0 = 0$$

$$\Rightarrow rx \in I$$

Thus I is an ideal of R.

Take $R = \mathbb{Z}_6, a = \bar{2}, I = \{\bar{0}, \bar{3}\}$.

8.4 Ring Homomorphism

Definition: Let R and R' be rings. A map $\emptyset: R \to R'$ is said to be a ***ring homomorphism*** if

$$\emptyset(a+b) = \emptyset(a) + \emptyset(b);\ \forall\ a, b \in R$$

$$\emptyset(ab) = \emptyset(a)\emptyset(b);\ \ \forall\ a, b\ \in\ R$$

8.4.1 Examples of ring homomorphism

i) $\emptyset: \mathbb{R} \to \mathbb{R}$
$\emptyset(x) = x$ is a ring homomorphism.

ii) $\emptyset: \mathbb{R} \to \mathbb{R}$
$\emptyset(x) = 0$ is a ring homomorphism.

iii) $\emptyset: \mathbb{Z} \to \mathbb{Z}$
$\emptyset(x) = 2x$ is not a ring homomorphism.

***Lemma* 8.4.2:** *Let $\emptyset: R \to R'$ be a ring homomorphism. Then,*

i) $\emptyset(0) = 0$
ii) $\emptyset(-a) = -\emptyset(a)\ \forall a \in R.$

***Proof*:** Let $a \in R$. Then

i) $\emptyset(a) = \emptyset\,(a+0) = \emptyset(a) + \emptyset(0)$
Thus, $\emptyset(0)$ is the zero of R'.

ii) $\emptyset(a) + \emptyset(-a) = \emptyset(a + (-a)) = \emptyset(0) = 0$
$\Longrightarrow \emptyset(-a) = -\emptyset(a).$

Definition: Let $\emptyset: R \to R'$ be a ring homomorphism. Then the set $\{x \in R \mid \emptyset(x) = 0\}$ is called the ***kernel of*** $\emptyset$ and is denoted by $\boldsymbol{ker}\emptyset$ or $\emptyset^{-1}(\mathbf{0})$.

***Lemma* 8.4.3:** *If $\emptyset$ is a homomorphism of R into R' with kernel $ker\emptyset$, then*

1. *$ker\emptyset$ is a subgroup of R under $+$.*
2. *If $x \in ker\emptyset$ and $r \in R$, then both xr and rx are in $ker\emptyset$.*

Proof: 1. If $a, b\ \in ker\emptyset$, then $\emptyset(a) = 0, \emptyset(b) = 0$
Thus, $\emptyset(a-b) = \emptyset(a) - \emptyset(b) = 0$

$\Rightarrow \quad a - b \in ker\emptyset$

Also $\emptyset(-a) = -\emptyset(a) = 0 \Rightarrow -a \in ker\emptyset$.

2. Let $x \in ker\emptyset$ and $r \in R$. Then

$$\begin{aligned}\emptyset(xr) &= \emptyset(x).\emptyset(r)\\ &= 0.\emptyset(r)\\ &= 0\end{aligned}$$

$\Rightarrow xr \in ker\emptyset$.

Similarly, $rx \in ker\emptyset$.

Definition: A homomorphism of R into R' is said to be an ***isomorphism*** if it is a one-to-one mapping.

Definition: Two rings are said to be ***isomorphic*** if there is an isomorphism of one onto the other.

***Lemma* 8.4.4:** The homomorphism $\emptyset$ of R into R' is an isomorphism iff $ker\emptyset = (0)$.

Proof: Let $\emptyset: R \to R'$ be a homomorphism.

Let $0, 0'$ be the zero elements of R and R' respectively.

We know that $ker\emptyset = \{x \in R: \emptyset(x) = 0'\}$ is an ideal of R.

Suppose $\emptyset$ is an isomorphism of R into R'. Then $\emptyset$ is one-one.

Let $a \in ker\emptyset$. Then $\emptyset(a) = 0'$.

$$\Rightarrow \emptyset(a) = \emptyset(0)$$
$$\Rightarrow a = 0$$

Since a was arbitrary, hence $ker\emptyset = (0)$.

Conversely, suppose $ker\emptyset = (0)$.

Let $a, b \in R$ such that $\emptyset(a) = \emptyset(b)$

$$\Rightarrow \emptyset(a) - \emptyset(b) = 0'$$
$$\Rightarrow \emptyset(a - b) = 0'$$

$$\Rightarrow a - b \in ker\emptyset$$

$$\Rightarrow a - b = 0$$

$$\Rightarrow a = b$$

Hence, $\emptyset$ is one-one and therefore $\emptyset$ is an isomorphism of R into R'.

Problems

1. If f is a homomorphism of a ring R into a ring $R'$with Kernel S, then prove that S is an ideal of R.

   Solution: Given $f : R \rightarrow R'$ is a homomorphism with *Ker f=S*.
   To prove: *S* is an ideal of *R*.
   Let $a, b \in S$. Then *f(a)=0, f(b)=0*.
   Now f$(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b) = 0 - 0 = 0$
   $Thus\ a - b \in S$.
   Also if $r \in R, a \in S, then\ f(ra) = f(r)f(a) = f(r).0 = 0,$ implying $ra \in S$ and $f(ar) = f(a)f(r) = 0.f(r) = 0,$ implying $ar \in S$ Thus *S* is an ideal of R.

2. Prove that any non-zero ring homomorphism from $\mathbb{Z}\ to\ \mathbb{Z}$ is identity.

Solution: Let f: $\mathbb{Z} \rightarrow \mathbb{Z}$ be a non-zero ring homomorphism. Since a ring homomorphism takes 0 to 0 and 1 to 1, we have f(0)=0 and f(1)=1.

Let m ϵ $\mathbb{Z}$.

Case I: m is positive. Then

f(m) =f(1+1+…+1)

=f(1)+f(1)+…+f(1) (m-times)

= 1+1+…+1 (m-times)

=m

Case II: m is negative. Then m=-n, where n is positive.

Now, f(m) = f(-n)

= -f(n) , since f is a ring homomorphism

= - n

= m

Therefore any non-zero ring homomorphism from $\mathbb{Z}\ to\ \mathbb{Z}$ is identity.

8.5 Quotient Ring

Let R be a ring and I an ideal of R.

Let R/I denote the set of all distinct cosets of I in R.

i.e., $\frac{R}{I} = \{a + I: a \in R\}$

For $r_1 + I,\ r_2 + I \in R/I$, we define

i) addition by $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$

and ii) multiplication by $(r_1 + I)(r_2 + I) = r_1 r_2 + I$.

***Theorem* 8.5.1**: *With respect to these operations defined above, R/I is a ring called the **quotient ring** of R by I.*

***Proof*:** a) The operations are well defined.

Let $X, Y \in R/I$. Let $X = a_1 + I = a_2 + I$, be two representations of X.

$$\Rightarrow a_1 - a_2 \in I.$$

Put $a_1 - a_2 = u_1 \Rightarrow a_1 = a_2 + u_1$.

Let $Y = b_1 + I = b_2 + I$, be two representations of Y.

$$\Rightarrow b_1 - b_2 \in I.$$

Put $b_1 - b_2 = u_2 \Rightarrow b_1 = b_2 + u_2$.

Addition: $X + Y = (a_1 + I) + (b_1 + I)$

$= (a_1 + b_1) + \mathrm{I}$

$= (a_2 + u_1) + (b_2 + u_2) + I$

$= (a_2 + b_2) + (u_1 + u_2) + I$

$= (a_2 + b_2) + I$

$$= (a_2 + \mathrm{I}) + (b_2 + I\,)$$

Thus addition in R/I is well defined.

Multiplication:

$$\begin{aligned} XY &= (a_1 + I)(b_1 + I\,) \\ &= a_1 b_1 + \mathrm{I} \\ &= (a_2 + u_1)(b_2 + u_2\,) + I \\ &= (a_2 b_2 + a_2 u_2 + u_1 b_2 + u_1 u_2) + I \\ &= a_2 b_2 + I \\ &= (a_2 + \mathrm{I})(b_2 + I\,) \end{aligned}$$

Hence multiplication in R/I is also well defined.

b) Closure property: By the definition of operations in R/I, it is closed w.r.t both addition and multiplication.

c) Associativity in R/I: We have

$$(a + \mathrm{I}) + [(b + I) + (c + I)] = (a + \mathrm{I}) + [(b + c) + I]$$
$$= [a + (b + c)] + I = [(a + b) + c] + I$$
$$= [(a + b) + I] + (c + I) = [(a + I) + (b + I)] + (c + I).$$

d) Commutativity in R/I: We have

$$(a + \mathrm{I}) + (b + I) = (a + b) + I = (b + a) + I = (b + \mathrm{I}) + (a + I).$$

e) Existence of additive identity: We have $I = 0 + I \in R/I$ and if $a + \mathrm{I} \in R/I$, then

$$(0 + \mathrm{I}) + (a + I) = (0 + a) + I = a + I.$$

Therefore, I is the additive identity.

f) Existence of additive inverse: Let $a + I \in R/I$, then its additive inverse is $-a + I$.

g) Associativity of multiplication: We have

$$(a + \mathrm{I})[(b + I)(c + I)] = (a + \mathrm{I})[(bc) + I] = a(bc) + I = (ab)c + I$$

$$= [(ab) + I](c + I) = [(a + I)(b + I)](c + I).$$

h) Distributive Law: We have

$$(a + \mathrm{I})[(b + I) + (c + I)] = (a + \mathrm{I})[(b + c) + I] = a(b + c) + I$$

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

Similarly, $[(b + I) + (c + I)](a + \mathrm{I}) = (b + I)(a + I) + (c + I)(a + I)$

Hence R/I is a ring with respect to two compositions.

***Proposition* 8.5.2:** The map $\phi : R \to R/I$ given by $\phi(r) = r + I$ is a ring homomorphism with $ker\phi = I$.

This mapping ϕ is called the ***projection mapping***

Proof: Let $r_1, r_2 \in R$. Then

$$\phi(r_1 + r_2) = (r_1 + r_2) + I$$
$$= (r_1 + I) + (r_2 + I)$$
$$= \phi(r_1) + \phi(r_2)$$

And $\phi(r_1\, r_2) = r_1\, r_2 + I$
$$= (r_1 + I)\,(r_2 + I)$$
$$= \phi(r_1)\,\phi(r_2)$$

$\ker \phi = \{x \in R : \phi(x) = 0 + I\}$
$= \{x \in R : x + I = I\}$
$= \{x \in R : x \in I\}$
$= I$

Theorem 8.5.3: ***Fundamental theorem of ring homomorphism***

If $\phi : R \to R'$ is an onto homomorphism of rings, with kernel I, then $R/I \cong R'$.

***Proof*:** Define $\Psi: R/I \to R'$ by $\Psi\ (r\ +\ I)\ =\ \phi(r)\ \forall\ r\ \in R$

a) This map is well defined.
Let $r_1 + I, r_2 + I \in R/I$ be such that

$$\begin{aligned} & r_1 + I = r_2 + I \\ \Rightarrow\ & r_1 - r_2 \in I \\ \Rightarrow\ & \phi(r_1 - r_2) = 0 \\ \Rightarrow\ & \phi(r_1) - \phi(r_2) = 0 \\ \Rightarrow\ & \phi(r_1) = \phi(r_2) \\ \Rightarrow\ & \Psi\ (r_1 + I) = \Psi\ (r_2 + I) \end{aligned}$$

$\therefore \Psi$ is well defined.

b) Ψ is a homomorphism:

$$\begin{aligned} \Psi\ [(r_1 + I) + (r_2 + I)] &= \Psi[(r_1 + r_2) + I] \\ &= \phi(r_1 + r_2) \\ &= \phi(r_1) + \phi(r_2) \\ &= \Psi\ (r_1 + I) + \Psi\ (r_2 + I) \end{aligned}$$

And

$$\begin{aligned} \Psi\ [(r_1 + I)(r_2 + I)] &= \Psi[r_1 r_2 + I] \\ &= \phi(r_1 r_2) \\ &= \phi(r_1)\phi(r_2) \\ &= \Psi\ (r_1 + I)\Psi\ (r_2 + I) \end{aligned}$$

c) Ψ is onto: For any $r' \in R'$, $\quad r \in R$ such that $\phi(r) = r'$.

$$\Rightarrow \Psi\ (r\ +\ I)\ =\ \phi(r)\ =\ r'$$

d) Ψ is one-one for if

$$\begin{aligned} & \Psi\ (r_1 + I) = \Psi\ (r_2 + I) \\ \Rightarrow\ & \phi(r_1) = \phi(r_2) \\ \Rightarrow\ & \phi(r_1) - \phi(r_2) = 0 \end{aligned}$$

$$\Rightarrow \phi(r_1 - r_2) = 0$$

$$\Rightarrow r_1 - r_2 \in I$$

$$\Rightarrow r_1 + I = r_2 + I$$

$\therefore \Psi$ is an isomorphism
Hence, $R/I \cong R'$.

***Proposition* 8.5.4:** (**Relation between ideals of R and ideals of R/I**)

Let I be an ideal in a ring R and let

$$\phi : R \to R/I$$

be the projection mapping.

i.e., $\phi(r) = r + I \ \forall r \in R.$

Then any $J \supset I$ *is an ideal in R if and only if* $\phi(J) = J/I$ *is an ideal in* R/I.

***Proof*:** Let $J \supset I$ be an ideal in R and $\phi(J) = J/I$.
Clearly J/I is a subgroup of R/I.

Now let $a + I \in J/I$ with $a \in J$ and $+I \in R/I$.

Then, $(x + I)(a + I) = xa + I \in J/I$ *as* $xa \in J$.

Similarly, $(a + I)(x + I) = ax + I \in J/I$ *a* $x \in J$.

Thus, J/I is an ideal in R/I.

Conversely, assume that $J/I = \{a + I / a \in J\}$ is an ideal in R/I. Then,

$J = \phi^{-1}(J/I)$ is an abelian subgroup of R.

Also, for any $x \in R, a \in J$,

$(x + I)(a + I) = xa + I \in J/I$ [$\because (a + I) \in J/I$ and J/I is an ideal of R/I]

Showing that $xa \in J$.
Similarly, $ax \in J$.
Hence, J is an ideal of R.

8.6 Prime and Maximal Ideals

Throughout this section, R is a Commutative ring with 1.

Definition: An ideal P in a ring R is said to be a ***prime ideal*** if whenever $ab \in P$, then either $a \in P \text{ or } b \in P, P \neq R$.

8.6.1 Examples

1. Let $R = \mathbb{Z}$ and $P = p\mathbb{Z}$ where p is a prime.

   Then, P is a prime ideal because if $ab \in P$ then,

   $ab = pk$ for some $k \in \mathbb{Z}$.

   $\Rightarrow p \mid ab$

   $\Rightarrow p \mid a \text{ or } p \mid b$ ($\because p$ is a prime)

   $\Rightarrow a \in p\mathbb{Z} \text{ or } b \in p\mathbb{Z}$

   Hence, $P = p\mathbb{Z}$ is a prime ideal.

2. Let R be an integral domain. Then $P = \{0\}$ is a prime ideal in R for if $ab \in P = \{0\}$, then $ab = 0$.
   This implies that $a = 0$ or $b = 0$

   i.e., $a \in P$ or $b \in P$.

   Hence, P is a prime ideal.

***Proposition* 8.6.2:** *An ideal P in R is a prime ideal if and only if R/P is an integral domain.*

***Proof*:** Suppose P is a prime ideal of R

Let $\bar{a} = a + P, \ \bar{b} = b + P \in R/P$ be such that $\bar{a}\,\bar{b} = 0$

i.e., $(a + P)(b + P) = 0 + P$

$\Rightarrow ab + P = P$

$\Rightarrow ab \in P$

$\Rightarrow a \in P$ or $b \in P$ ($\because P$ is a prime ideal)

$\Rightarrow a + P = P$ or $b + P = P$

i.e., $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$

Hence, R/P is an integral domain.

Conversely, let R/P be an integral domain and let $ab \in P$. Then,

$$ab + P = P$$
$$\Rightarrow (a + P)(b + P) = P$$
$$\text{i.e.,} \quad \bar{a}\,\bar{b} = 0.$$

Since, R/P is an integral domain we must have

$\bar{a} = 0$ or $\bar{b} = 0$
i.e., $a + P = P$ or $b + P = P$
i.e., $a \in P$ or $b \in P$, showing that P is a prime ideal.

Definition*:** An ideal M in a ring R is said to be ***maximal if M ≠ R, and if for any ideal I of R such that M ⊂ I ⊂ R, we have

I = M or I = R.

8.6.3 Examples

1. Let $R = \mathbb{Z}$ and $M = p\mathbb{Z}$ where p is a prime. Then, M is a maximal ideal of R.

   Let $I = m\mathbb{Z}$ be any ideal containing M.

   i.e., $p\mathbb{Z} = M \subset I \subset R$

   Now, $p \in M \Rightarrow p \in I = m\mathbb{Z}$

   $\Rightarrow p = mk$ for some $k \in \mathbb{Z}$

   $\Rightarrow m|p$

   $\Rightarrow m = 1$ or $m = p$ ($\because p$ is a prime)

   If $m = 1$, then $I = R$

   If $m = p$, then $I = M$

   Showing that M is a maximal ideal of R.

2. If R is a field, then $M = \{0\}$ is a maximal ideal in R because the only ideals in R are $\{0\}$ and R.

Hence, no ideal of R except R properly contains $\{0\}$.

***Proposition* 8.6.4:** *Let R be commutative ring with 1. An ideal M is a maximal ideal if and only if R/M is a field.*

***Proof*:** Let M be a maximal ideal.

To show: R/M is a field.

Let J/M be any ideal of R/M, where J is an ideal of R containing M.

i.e., $M \subset J \subset R$.

Since M is a maximal ideal, $J = M$ or $J = R$.

i.e., $J/M = \{0\}$ or $J/M = R/M$

Hence, R/M is a field.

Conversely, let R/M be a field.

To show that M is a maximal ideal.

Since, R/M is a field, the only ideals of R/M are $\{\bar{0}\}$ and R/M itself.

Let $M \subset J$ be any ideal.

Then, J/M is an ideal R/M.

$\Rightarrow J/M = R/M$ or $J/M = \{\bar{0}\}$.

i.e., $J = R$ or $J = M$.

Hence, M is a maximal ideal.

Corollary: If R is a commutative ring with 1, every maximal ideal in R is a prime ideal.

***Proof*:** Let M be a maximal ideal in R.
Then R/M is a field. (***Proposition* 8.6.4**)
$\Rightarrow R/M$ is an integral domain
$\Rightarrow M$ is a prime ideal. (***Proposition* 8.6.2**)

Note: The converse is not true:
For example in $R = \mathbb{Z}$, $I = \{0\}$ is a prime ideal which is not a maximal ideal.

Corollary: If R is a finite commutative ring, then every prime ideal of R is a maximal ideal.

***Proof*:** If P is a prime ideal of R, then

R/P is an integral domain which is finite

$\Rightarrow R/P$ is a field (since R is finite, so is R/P)

$\Rightarrow P$ is a maximal ideal.

Problems

1. Consider the ring of integers $\mathbb{Z}$. In this ring $5\mathbb{Z} = \{5k: k \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. How many distinct cosets are there in the quotient ring $\mathbb{Z}/5\mathbb{Z}$? Is this quotient ring a field? Justify your answer.

   Solution: We have

$$0 + 5\mathbb{Z} = 5\mathbb{Z} = \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}$$

$$1 + 5\mathbb{Z} = \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\}$$

$$2 + 5\mathbb{Z} = \{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\}$$

$$3 + 5\mathbb{Z} = \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\}$$

$$4 + 5\mathbb{Z} = \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\}$$

   Also, $$5 + 5\mathbb{Z} = \{\dots, -10, -5, 0, 5, 10, 15, 20, \dots\} = 5\mathbb{Z}$$

$$6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}$$

$$7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}$$

   and so on. Thus the quotient ring $\mathbb{Z}/5\mathbb{Z}$ has five distinct cosets.

   i.e., $\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z} = 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$

   i.e., $\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5$

   Since $\mathbb{Z}_5$ is a field, the quotient ring $\mathbb{Z}/5\mathbb{Z}$ is also a field.

2. Define maximal ideal of a ring R. Is $\{0\}$ in the ring if integers $\mathbb{Z}$ a maximal ideal? Justify your answer.

   Solution: $\{0\}$ is not a maximal ideal in the ring of integers $\mathbb{Z}$ since

$$\{0\} \subset \{\dots \dots, -4, -2, 0, 2, 4, \dots \dots\} \subset \mathbb{Z}$$

3. Let R be a ring with a unit element such that $a^2 = a$, for all $a \in R$. Prove that every prime ideal of R is maximal.

   Solution: Let I be a prime ideal of a ring R with unit element 1. Then $\frac{R}{I}$ is an integral domain.

We need to show that I is a maximal ideal.

i.e., we need to show that $\frac{R}{I}$ is a field.

Let $\bar{a} = a + I$ be a nonzero element of $\frac{R}{I}$, where $a \in R$.

In the ring R, $a^2 = a$, for all $a \in R$.

$$\Rightarrow \bar{a}^2 = (a + I)(a + I) = a^2 + I = a + I = \bar{a}.$$
$$\Rightarrow \bar{a}^2 - \bar{a} = 0.$$
$$\Rightarrow \bar{a}(\bar{a} - \bar{1}) = 0.$$

But $\bar{a} = a + I$ is a nonzero element of $\frac{R}{I}$ and $\frac{R}{I}$ is an integral domain. Thus

$$\bar{a} - \bar{1} = 0$$
$$\Rightarrow \bar{a} = \bar{1}$$

Therefore $\frac{R}{I}$ is an integral domain with two elements, $\bar{0}\ and\ \bar{1}$.

Since a finite integral domain is a field we obtain that $\frac{R}{I}$ is a field.

Hence *I* is a maximal ideal.

8.7 *Divisibility (in an integral domains with 1)*

Definition: Let D be an integral domain with identity element 1. An element $a \neq 0,\ a \in D$ is called ***regular element (or a unit)*** in D if there exists an element $b \in D$ such that ab=1.

8.7.1 Examples

1. If $D = \mathbb{Z}$, then the only units are ± 1.

2. If F is a field, then every non-zero element is a unit. In particular, the units of $\mathbb{Q} = \mathbb{Q} - \{0\}$.

3. In $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$, the units are $\bar{1}$ and $\bar{5}$.

4. Let us consider the set $D = \mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}\, b : a, b \in \mathbb{Z}\}$.

   Define a norm on $\mathbb{Z}[\sqrt{-5}]$ by $N[a + \sqrt{-5}b] = a^2 + 5b^2$. Then,

i) $N[a + \sqrt{-5}b = 0 \Leftrightarrow a = 0$ and $b = 0$.

ii) For $x, y \in \mathbb{Z}[\sqrt{-5}]$, $N(xy) = N(x).N(y)$

iii) $\mathbb{Z}[\sqrt{-5}]$ is an integral domain.

iv) All the units of $\mathbb{Z}[\sqrt{-5}]$ are those of $x \in \mathbb{Z}[\sqrt{-5}]$ such that $N(x) = 1$ i.e., the units are ± 1.

***Proof*:**

i) Trivially true.

ii) Suppose $x = a + \sqrt{-5}b$ and $y = c + \sqrt{-5}d \in \mathbb{Z}[\sqrt{-5}]$. Then,

$$xy = (a + \sqrt{-5}b)(c + \sqrt{-5}d)$$
$$= (ac - 5bd) + (ad + bc)\sqrt{-5}$$

Thus, $N(xy) = (ac - 5bd)^2 + 5(ad + bc)^2$

$$= (a^2c^2 - 10abcd + 25b^2d^2) + 5[a^2d^2 + 2abcd + b^2c^2]$$

$$= a^2c^2 + 25b^2d^2 + 5a^2d^2 + 5b^2c^2$$

$$= (a^2 + 5b^2)(c^2 + 5d^2)$$

$$= N(x).N(y)$$

iii) Let $x, y \in \mathbb{Z}[\sqrt{-5}]$ be such that $xy = 0$

iv)

$$\Rightarrow N(xy) = 0$$

$$\Rightarrow N(x)N(y) = 0$$

$\Rightarrow$ Either $N(x) = 0$ or $N(y) = 0$

$\Rightarrow$ Either $x = 0$ or $y = 0$.

Hence, $\mathbb{Z}[\sqrt{-5}]$ is an integral domain.

v) Let $x = a + \sqrt{-5}b$ be a unit. Then there exist $y = c + \sqrt{-5}d \in \mathbb{Z}[\sqrt{-5}]$ such that

$$xy = yx = 1$$

$$\Rightarrow N(xy) = N(1)$$

$$\Rightarrow N(x)N(y) = 1$$

This means that $N(x)$ divides 1.

But, $N(x) = a^2 + 5b^2$ will divide 1 only if $N(x) = 1$ which is possible only if $b = 0$ and $a = \pm 1$.
i.e., the units are ± 1.

Definition: Let D be an integral domain with unit element. If $a \neq 0$ and b are in D then a is said to ***divide*** b if there exists $c \in D$ such that $b = ac$. If this happen we say that a and c are factors of b.

We shall use the symbol $\boldsymbol{a/b}$ to represent the fact that *a* divides *b* and $\boldsymbol{a \nmid b}$ to mean that *a* does not divide *b.*

Remarks

i. If a / b and $b /$ c then $a /$ c.
ii. If a / b and a / c then $a / (b \pm c)$.
iii. If a / b then a / bx for all $x \epsilon D$.
iv. If a / b and a / c then $a /(\alpha b \pm \beta c); \alpha, \beta \in D$.

8.7.2 Examples

1. In $= \mathbb{Z}$, the ring of integers, 3 divides 15.

2. In $R = \mathbb{Z} + i\mathbb{Z} = \{a + ib |\ a, b\ \in \mathbb{Z}\}, (1 + 3i)\ divides\ 10\ because$
$$10 = (1 + 3i)(1 - 3i).$$

Definition: Let D be an integral domain with unit element. Two elements $a, b \in D; a \neq 0, b \neq 0,$ are said to be ***associates*** if $b = ua$ for some unit u in D.

8.7.3 Examples

1. In $= \mathbb{Z}$, associates of m are m and $-m$.

2.In $R = \mathbb{Z} + i\mathbb{Z} = \{a + ib |\ a, b\ \in \mathbb{Z}\}, a = 1 + i\sqrt{2}$ and $b = \sqrt{2} - i$ are associates because $b = (-i)a$ and –i is a unit in R.

Definition*:** An element $a \in D$ is called an ***irreducible element if (i) a is not a unit, and (ii) the only divisors of a are units and associates of a.

For example, 1 – i is an irreducible element of $\mathbb{Z}$ [i].

Solution: Clearly 1 – i is a non-zero and non-unit element of $\mathbb{Z}$ [i].
Let 1 – i = (a + ib) (c + di) ----- (I) where a, b, c, d $\in \mathbb{Z}$

Taking conjugate on both sides, we get

$1 + i = (a - ib)(c - id)$ ----- (II)

Multiplying (I) and (II) we get

$2 = (a^2 + b^2)(c^2 + d^2)$

Case I: $a^2 + b^2 = 1$ and $c^2 + d^2 = 2$

⇨ $(a + ib)(a - ib) = 1$

⇨ $a + ib$ is a unit

Case II: $a^2 + b^2 = 2, c^2 + d^2 = 1$

$\Rightarrow (c + id)(c - id) = 1$

$\Rightarrow c + id$ is a unit.

Hence $1 - i$ is an irreducible element of $\mathbb{Z}[i]$.

Definition*:** Let D be an integral domain with unit element and let $a \neq 0, a \in D$. Then a is said to be a ***prime element of D if whenever $a = ub$, where u, b are in D, then one of u or b is a unit in D.

***Theorem* 8.7.4:** *Let R be an integral domain with unity. Show that every prime element of R is irreducible. However, the converse need not be true.*

***Proof*:** Let p be a prime element of R.
Then $p \neq 0, p$ is not a unit.

To show: p is irreducible.
Let $p = ab$, where $a, b \in R$.

We shall prove that either a or b is a unit.
Now, $p = 1.p = ab$

⇨ $p \mid ab$

⇨ Either $p|a$ or $p|b$ (since p is prime)

If $p|a \Rightarrow a = pr$ for some $r \in R$
So, $p = ab$

⇨ p = (pr)b

⇨ p(1 - rb) = 0

⇨ 1 – rb = 0, as p≠ 0

⇨ rb = 1

⇨ b|1

i.e., b is a unit.
Similarly, if p|b, then we can show that a is a unit.
Hence, p is irreducible.
However, the converse need not be true. i.e., an irreducible element in an integral domain may not be prime.
Example:3 is an irreducible element of $\mathbb{Z}[\sqrt{-5}]$, but not a prime element of $\mathbb{Z}[\sqrt{-5}]$.

Problems

1. Prove that 3 is not a prime element in $\mathbb{Z}\left[\sqrt{-5}\right]$.

Solution: We know that $\mathbb{Z}\left[\sqrt{-5}\right]$is an integral domain with unity.

Now, $\left(2+\sqrt{5}i\right)\left(2-\sqrt{5}i\right)=9$.

So, 3 divides $\left(2+\sqrt{5}i\right)\left(2-\sqrt{5}i\right)$.

But 3 does not divide $\left(2+\sqrt{5}i\right)$ and $\left(2-\sqrt{5}i\right)$ for if 3 divides $\left(2+\sqrt{5}i\right)$, then $\left(2+\sqrt{5}i\right)=3\left(a+b\sqrt{5}i\right)$ for some $a,b\in\mathbb{Z}$.

$=> 3a=2, a\in\mathbb{Z}$, which is not possible.

Similarly, 3 does not divide $\left(2-\sqrt{5}i\right)$.

Hence, 3 is not a prime element in $\mathbb{Z}\left[\sqrt{-5}\right]$.

2. Find an associate of a non-zero element in $\mathbb{Z}$.

Solution: We know that 1 and -1 are the only units in the set of integers.

Now, if $a\in\mathbb{Z}, a\neq 0$. Then,

$$a=a.1\ and\ a=(-a).(-1)$$

Hence, associates of a are a and $-a$.

3. Define the term 'associates' in a Euclidean domain. In $\mathbb{Z}_5$, are 2 and 3 associates?

Solution: Let *E* be a Euclidean domain. Two elements $a, b \in E\ ;\ a \neq 0, b \neq 0$, are said to be ***associates*** if *b* = *ua* for some unit *u* in *E*.

Addition modulo 5					
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication modulo 5					
	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

From the above table we see that units in $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ are $\bar{1}, \bar{2}, \bar{3}, \bar{4}$.
Now, 2=4.3and 3=4.2.
Hence 2 and 3 are associates.

8.8 *Euclidean Domain and Principal Ideal Domain*

Definition*:** An integral domain *D* is said to be a ***Euclidean ring/ domain if for every $a \neq 0$ in *D* there is defined a nonnegative integer *d(a)* such that

1. For all *a*, b ∈ *R*, both nonzero, $d(a) \leq d(ab)$.

2. For any *a*, *b* ∈ *R*, both nonzero, there exist *t*, *r* ∈ *R* such that *a* = *tb* + *r* where either *r* = 0 or d(r) < *d(b)*.

For example, $D = \mathbb{Z}$, the ring of integers is a Euclidean domain if $d(a) = |a|$.

Definition: Let *R* be a ring. An ideal *A* of *R* is said to be a ***principal ideal*** if there exist $a_0 \in R$ such that $= \{xa_0 \,/\, x \in R\}$. Then a_0 is said to be the generator of *A* and we write $A = (a_0)$.

Example: In $R = \mathbb{Z}$, the ring of integers, every ideal of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ which are principal ideals generated by m or $-m$.

Definition: An integral domain *D* with unit element is said to be a *principal ideal domain (PID)* if every ideal *A* in *D* is a principal ideal. ie., if every ideal *A* in *D* is of the form *A* = (a) for some $a \in R$.

Theorem 8.8.1: *Every Euclidean domain is a PID.*

***Proof*:** We have to show that

(i) Every ideal of a Euclidean domain is a principal ideal.

(ii) $1 \in E$, i.e., E possess a unit element.

(i) Let E be a Euclidean domain and let A be any ideal of E.

If A = (0), then A is a principal ideal.

Let $A \neq (0)$. Let $a_0 \in A$, $a_0 \neq 0$ be such that $d(a_0)$ is minimal in A. This is possible because d(a) is non negative.

Now, let $0 \neq a$ be another element of A. By the division algorithm in E,

$a = t\,a_0 + r$ where $r = 0$ or $d(r) < d(a_0)$

Now, $r = a - ta_o \in A$, since A is an ideal.

Hence $d(r) \not< d(a_0)$ because $d(a_0)$ is minimal in A.

This show that r=0 , $a = t\,a_0$.

Therefore every element of A is a multiple of a_0 and so A is a principal ideal.

(ii) Since every ideal of E is a P.I, $E = (x_0)$ for some $x_0 \in E$.
Now, $x_0 \in E \Rightarrow x_0 = cx_0$ for some $c \in E$
Let $x \in E$, then $x = yx_0$ for some $y \in E$
$\therefore \quad xc = (yx_0)c = y(cx_0) = yx_0 = x$
Showing that c is the unit element in E.
Hence, every Euclidean domain is a PID.

Lemma 8.8.2: *Let E be a Euclidean Domain and A an ideal of E. if $a \neq 0$, $a \in A$ be such that d (a) is minimal in A, then A = (a).*

Proof: Let $x \in A$ be arbitrary. Then by division algorithm in E , $\exists\ t, r \in E$ such that

$x = ta + r$ where $r = o$ or $d(r) < d(a)$.

Now, $r = x - ta \in A$, as A is an ideal.
$\therefore d(r) \lneq d(a)$ as $d(a)$ is minimal in A.
Thus, $r=0$, implying that $x=ta$.
Hence, $A = (a)$.

Theorem 8.8.3: *In a Euclidean domain E, a g. c. d of any two elements a and b exists and it is of the form $\lambda a + \mu b$ for some $\lambda, \mu \in E$.*

Proof: Consider the set $A = \{ ra + sb \mid r, s \in E \}$

Claim 1: A is an ideal of E.

Let $r_1a + s_1b$, $r_2a + s_2b \in A$, Then

$(r_1a + s_1b_1) - (r_2a + s_2b) = (r_1 + r_2)\, a + (s_1 - s_2)\, b \in A$

Hence A is a sub group of E.

Now, let x ∈ E, then

$x(r_1a + s_1b) = xr_1a + xs_1b \in A$

∴ A is an ideal of E.

We know that a Euclidean Domain is a PID. Thus every ideal of E is a principal ideal.

Hence ∃ d ∈ A such that A = (d)

Claim 2: d is a g.c. d of a and b

Since 1 ∈ E and a = 1.a +0.b ∈ A

b = 0.a + 1.b ∈ A

i.e., a, b ∈ A

Hence ∃ x ∈ E such that a = xd ⇒ d|a

And ∃ y ∈ E such that b = yd ⇒ d|b

Thus, d|a and d|b.

Further d ∈ A ⇒ d= λa + μd for λ, μ ∈ E

Suppose ∃ some c ∈ E s.t c|a and c|b, then

c|λa and c|μb ⇒ c|λa + μb⇒c|d

∴ d is the g.c.d of a and b.

8.8.4 A particular Euclidean Ring*:* Gaussian Integers

Let $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z},\ i^2 = -1\}$ – the set of complex numbers a + ib where a and b are integers.

(d) Define $d(a + ib) = a^2 + b^2$

Note: (i) If $a + ib \neq 0, d(a + ib) > 0$
i.e., if $x \in \mathbb{Z}[i], d(x) = 0$ if $x = 0$.
(ii) $d(x) \geq 0$
(iii) $d(xy) = d(x).d(y)$

Let $x = a + ib$ and $y = c + id \in \mathbb{Z}[i]$. Then,

$$xy = (a + ib)(c + id)$$

$$= (ac - bd) + (ad + bc)i$$

Thus, $d(xy) = (ac - bd)^2 + (ad + bc)^2$

$$= (a^2c^2 - 2abcd + b^2d^2)$$

$$+ [a^2d^2 + 2abcd + b^2c^2]$$

$$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$$

$$= (a^2 + b^2)(c^2 + d^2)$$

$$= d(x).d(y)$$

(e) $\mathbb{Z}[i]$ is an integral domain.

Let $x, y \in \mathbb{Z}[i]$ be such that $xy = 0$

$$\Rightarrow d(xy) = 0$$

$$\Rightarrow d(x)d(y) = 0$$

$\Rightarrow$ Either $d(x) = 0$ or $d(y) = 0$

$\Rightarrow$ Either $x = 0$ or $y = 0$.

Hence, $\mathbb{Z}[i]$is an integral domain.

Note: i) The units of $\mathbb{Z}[i]$ are $1, -1, i, -i$, i.e., they are precisely those $x \in \mathbb{Z}[i]$such that

$$d(x) = 1$$

ii) 5 is a prime in $\mathbb{Z}$ but in $\mathbb{Z}[i]$,

$$5 = (1 + 2i)(1 - 2i) = (2 + i)(2 - i)$$

iii)$\mathbb{Z}[i]$ **is a Euclidean Domain**.

***Proof*:**

1) $d(x) \geq 0$
2) $d(x) \leq d(xy),\ x, y \neq 0$
   For $d(x) \leq d(x)d(y)$
   $= d(xy)$
3) The division algorithm:
   Given $x, y \in \mathbb{Z}[i]$, there exist $t, r \in \mathbb{Z}[i]$, such that
   $y = tx + r$ where either $r = 0$ or $d(r) < d(x)$

***Proof*:** We shall first of all prove this for the case when x is an integer.
Let $y = a + ib$ where $a, b \in \mathbb{Z}$.

Using the division algorithm in the Euclidean domain of integers to get

$a = v_1 x + u_1$ where either $u_1 = 0$ or $d(u_1) < \frac{x^2}{2}$.

Similarly, b $= v_2 x + u_2$ where either $u_2 = 0$ or $d(u_2) < \frac{x^2}{2}$.

Thus, $y = a + ib = (v_1 x + u_1) + i(v_2 x + u_2) = (v_1 + iv_2)x + (u_1 + iu_2)$

where either $u_1 + iu_2 = 0$ or $d(u_1 + iu_2) = {u_1}^2 + {u_2}^2$

$$< \frac{x^2}{2} + \frac{x^2}{2}$$

$$= x^2$$

$$= d(x)$$

Hence, $d(u_1 + iu_2) < d(x)$.

Now let x be any arbitrary element of $\mathbb{Z}[i]$ and let $\bar{x}$ be its complex conjugate.

Then $x\bar{x} \in \mathbb{Z}$, and applying what we have proved to $y\bar{x}$ and $x\bar{x}$, we get

$y\bar{x} = tx\bar{x} + r$ where either $r = 0$ or $d(r) < d(x\bar{x})$

i.e., $d(y\bar{x} - tx\bar{x}) < d(x\bar{x})$

i.e., $d(y - tx)d(\bar{x}) < d(x)d(\bar{x})$

i.e., $d(y - tx) < d(x)$

Putting $y - tx = r_1$, we get $y = tx + r$ where either $r_1 = 0$ or $d(r_1) < d(x)$

Hence, $\mathbb{Z}[i]$ is a Euclidean domain.

Definition: Let R be an integral domain with 1 and let a, b $\in R$. Then an element $d \in R$ is said to be a ***greatest common divisor (gcd)*** of a and b if
1. $d \mid a$ and $d \mid b$.

2. Whenever $c \mid a$ and $c \mid b$ for some $c \in R$,then $c \mid d$.

We shall use the notation $d = (a,$ b) to denote that d is a greatest common divisor of a and b.
Example: In $R = \mathbb{Z}$, gcd of $a = 10$ and $b = -25$ is 5.

***Lemma* 8.8.5:** If a, b ∈ E such that a|b and b|a, then a and b are associates.

Proof: a|b ⇒ b = xa, for some x ∈ E
b|a⇒ a = yb, for some y ∈ E

Now, a = yb ⇒ a = y (xa) ⇒ a (1 – yx) = 0
⇨ yx = 1 (∵ a ≠ 0)
⇨ x and y are units

Hence, a and b are associates.

***Lemma* 8.8.6:** Let d = (a,b) and let d_1 be an associate of d. Then d_1 is also a g. c d of a and b.

Proof: $d_1 \sim d \Rightarrow d = ud_1$ where u is a unit.

⇒ $d_1|d$ and $d|a \Rightarrow d_1|a$.
Also, $d|b \Rightarrow d_1|b$.
Now, let $c|a$, $c|b \Rightarrow c|d$ and $d|d_1$. so $c|d_1$
∴ d_1 is a. g. c. d. of a and b.

***Lemma* 8.8.7:** A unit is an associate of 1.
Proof: Let x be a unit. Then ∃ y (which is also a unit) such that
xy = 1
⇒x = $y^{-1}1$
⇒x ~ 1

***Lemma* 8.8.8:** Let $a \neq 0$, $a \in E$, a Euclidean domain. If $b \in E$, b not a unit, then $d(a) < d(ab)$.

Proof: Let $A = \{ax \mid x \in E\}$. Then by the first condition of a Euclidean domain,

$d(a) \leq d(ax)$ for any $x \in E$

Hence, d(a) is minimal in A.

If, $d(a) = d(ab)$, then d(ab) is also minimal in A and so $A = (ab)$

Also, $a \in A \Rightarrow a = aby$ for some $y \in E$

$\Rightarrow a(1 - by) = 0$
$\Rightarrow by = 1$ (as E is an I.D)
$\Rightarrow$ b is a unit , which is a contradiction

$\therefore d(a) \neq d(ab)$
$\Rightarrow d(a) < d(ab)$

***Lemma* 8.8.9:** Let $a \neq 0$, $a \in E$, a Euclidean domain. Then a is a unit if and only if $d(a) = d(1)$.

Proof: Let a be a unit, then a^{-1} exist and $aa^{-1} = 1$
Now, $d(1) \leq d(1.a) = d(a)$

and $d(a) \leq d(a.a^{-1}) = d(1)$

$\therefore$ $d(a) = d(1)$

Conversely; Let , $d(a) = d(1)$
If a is not a unit, then $d(a) < d(1.a)$
But, $d(a) = d(1)$
$\therefore$ a is a unit.

Definition: Let *E* be a Euclidean domain, then *a* and *b* are said to be *relatively prime* if their greatest common divisor is a unit of *E.*

Note: i) An associate of a g.c.d is again a g. c. d.
ii) A unit is an associate of 1.

***Lemma* 8.8.10:** If $a|bc$ and $(a,b) = 1$, then $a|c$.

Proof: $(a,b) = 1$
$\Rightarrow \lambda a + \mu b = 1$
$\Rightarrow \lambda ac + \mu bc = c$

Now, a|λac and a|μbc
∴ a|c.

***Theorem* 8.8.11:** *In a P.I.D, an element is prime if and only if it is irreducible.*

***Proof*:** Let R be a P.I.D. Since R is an integral domain, every prime element of R is irreducible.

Conversely, let p be any irreducible element of R. Then $p \neq 0$ and p is not a unit.

To prove: p is a prime.

Let $p|ab$, where $a, b \in R$

Let $p \nmid a$. Since (p) and (b) are ideals of R, so $(p) + (b)$ is also an ideal of R.

But R is a P.I.D, $(p) + (b) = (d)$ …… (1)

or some d $\in R$

From (1), $(p) \subseteq (d) \Rightarrow p \in (d) \Rightarrow p = dx$ …… (2)

for some $x \in R$.

Since p is irreducible, either d or x is a unit.

Suppose d is a unit, then $d^{-1} \in R$ and $dd^{-1} = 1 \Rightarrow 1 \in$ (d).

$\Rightarrow 1 \in (p) + (b) \Rightarrow 1 = pr + bs$ for some $r, s \in R$

$\Rightarrow a = a.1 = apr + abs$ …… (3)

Now, $p|p \Rightarrow p|apr$ and $p|ab \Rightarrow p|abs$

Then, $p|(apr + abs)$ and so, $p|a$ (by (3)), which is contrary to our assumption. So d cannot be a unit.

It follows that x is a unit, i.e, $x^{-1} \in R$.

From (2) we get $d = px^{-1}$

Let $\alpha \in (d)$. Then $\alpha = dy$ for some y $\in R$.

$$\Rightarrow \alpha = (px^{-1})y = p(x^{-1}y), \qquad x^{-1}, y \in R$$
$$\Rightarrow \alpha \in (p)\ \forall \alpha \in (d)$$
$$\Rightarrow (d) \subseteq (p)$$
$$\therefore (d) = (p).$$

$\therefore$ (1) gives $(p) + (b) = (p)$

$\Rightarrow (b) \subseteq (p)$

$\Rightarrow b \in (p)$

$\Rightarrow b = pt$, for some t $\in R$

$\Rightarrow p|b$

Hence, p is a prime.

***Theorem* 8.8.12:** *Let R be a Euclidean domain. Then every element in R is either a unit or can be written as the product of finite number of prime elements of R.*

***Proof*:** Let R be a Euclidean domain.
Let $a \in R$. We will prove the theorem by induction on $d(a)$.
If $d(a) = d(1)$, then a is a unit and so the theorem is true for a when $d(a) = d(1)$.

Now, we assume that the theorem is true for all $b \in R$ such that $d(b) < d(a)$. We shall prove the theorem for a.

If a is a prime element, we have nothing to prove.

Suppose a is not a prime element. Then $a = b.c$ where neither b nor c is a unit. Now,

$$d(b) < d(b.c), \text{since } c \text{ is not a unit}$$
$$= d(a).$$

Also,

$$d(c) < d(b.c) = d(a) \text{ as } b \text{ is not a unit}$$

By induction hypothesis, the theorem is true for b and c.

Hence, $b = p_1.p_2.p_3 \ldots . p_n$ where $p_1, p_2, p_3, \ldots, p_n$ are prime elements and n is finite.

Similarly, $c = p_1'.p_2'.p_3' \ldots . p_m'$ where $p_1', p_2', p_3', \ldots, p_m'$ are prime elements and m is finite.

Therefore, $a = b.c = (p_1.p_2.p_3 \ldots . p_n)(p_1'.p_2'.p_3' \ldots . p_m')$.

Hence a is expressible as a product of finite number of prime elements.

Lemma 8.8.13: Let $\pi \in R$, a Euclidean domain, be a prime element. If π/ab then π/a or π/b.

***Proof*:** If $\pi \nmid a \Rightarrow (\pi, a) = 1 \Rightarrow \pi/b$. (Using ***Lemma* 8.8.10**)

Theorem 8.8.14: (Unique Factorization Theorem)

Let R be a Euclidean domain and $a \neq 0$, a non-unit element of R.

Suppose $a = p_1.p_2.p_3 \ldots . p_m = q_1.q_2.q_3 \ldots . q_n$, where $p_i's$ and $q_j's$ are prime elements of R. Then, $m = n$ and each $p_i, 1 \leq i \leq m$ is an associate of some $q_j, 1 \leq j \leq n$ and conversely each $q_k$is an associate of some p_r.

***Proof*:** We have $p_1.p_2.p_3 \ldots . p_m = q_1.q_2.q_3 \ldots . q_n$.

Now $p_1 | \, p_1.p_2.p_3 \ldots . p_m \Rightarrow p_1 | q_1.q_2.q_3 \ldots . q_n$

$$\Rightarrow p_1 | q_j \text{ for some } 1 \leq j \leq n \quad (\text{ by } \textbf{\textit{Lemma}}\ \textbf{8.8.13})$$

$$\Rightarrow q_j = x_1 p_1, \text{ where } x_1 \text{ is a unit.}$$

Thus,

$$p_1.p_2.p_3 \ldots . p_m = x_1 p_1.q_1.q_2 \ldots q_{j-1}.q_{j+1} \ldots . q_n$$

$$\Rightarrow p_2.p_3 \ldots . p_m = x_1.q_1.q_2 \ldots q_{j-1}.q_{j+1} \ldots . q_n$$

We can proceed as above for p_2 and then with p_3 and so on till we finally have 1 on the LHS and a product of possibly some $q_j's$.

$$\Rightarrow m \leq n.$$

If we do these steps with $q_j's$ we would similarly obtain that $n \leq m$.
Therefore, $m = n$.

We also have shown that each $p_i, 1 \leq i \leq m,$ is an associate of some $q_j, 1 \leq j \leq n,$ and vice versa.

Problems

1. Prove that every field is a Euclidean ring.

   Solution: Let *F* be a field.
   We take $d(a) = 1, \forall\, a \neq 0 \in F$.

   Let $a, b \in F; a \neq 0, b \neq 0$ .Then $ab \neq 0$, since every field is an integral domain. Consequently, $d(a) = 1$ and $d(ab) = 1$.

   This implies that $d(a) = d(ab)$.

   Also $b \neq 0 \in F \Rightarrow b^{-1} \in F$ and so $a = (ab^{-1})b + 0 = tb + r$,

   where $t = ab^{-1} \in F$ and $r = 0 \in F$.

   Hence *F* is a Euclidean domain.

8.9 Unique Factorization Domain (U.F.D)

Definition: An integral domain *D* with unit element is said to be a *unique factorisation domain (U.F.D)* if

i) Every non-zero element of *D* is either a unit or can be expressed as a product of a finite number of prime elements.
ii) This factorisation is unique up to order and associates.

Examples: 1. $R = \mathbb{Z}$ is a U.F.D.

2. Every field F is a U.F.D.

Theorem* 8.9.1:Every Euclidean domain is a unique factorisation domain.*
Proof: Follows from Theorems **8.8.12 & 8.8.14.**

***Theorem* 8.9.2:** *An ideal $A = (a_0)$ of a Euclidean domain R is maximal if and only if a_0 is a prime element.*

***Proof*:** We shall prove that $A = (a_0)$ is not maximal if a_0 is not prime and that $A = (a_0)$ is maximal if a_0 is prime.

Suppose a_0 is not prime. Let $a_0 = b.c$, where neither b nor c is a unit.

Put $B = (b)$. Then $a_0 \in B \Rightarrow A \subseteq B \subseteq R$.

If $B = A$

$$\Rightarrow b \in A \Rightarrow b = a_0 r \text{ for some } r \in R$$

$$\Rightarrow b = bcr$$
$$\Rightarrow b(1 - cr) = 0$$
$$\Rightarrow cr = 1$$
$$\Rightarrow c \text{ is a unit, which is a contradiction.}$$

If $B = R$, then every element of R is generated by b.

Now $1 \in R$, therefore there exist $x \in R$ such that $1 = bx$.

$\Rightarrow b$ is a unit, which is a contradiction.

Thus, $A = (a_0)$ is not maximal in R.

We now assume that a_0 is prime.

Let U be an ideal of R such that

$$A \subseteq U \subseteq R.$$

Since a Euclidean domain is a PID, $U = (u_0)$ for some $u_0 \in U$.

So $a_0 \in A \subseteq U \Rightarrow a_0 = u_0 x$ for some $x \in R$.

Since a_0 is prime, either x is a unit or u_0 is a unit.

If u_0 is a unit, then $U = R$.

If x is a unit, then x^{-1}exists and we have

$$a_0 x^{-1} = u_0$$
$$\Rightarrow u_0 \in A$$
$$\Rightarrow U \subseteq A$$
$$\therefore \quad A = U.$$

Hence A is maximal in R.

8.10 Polynomial Rings over commutative Rings

Definition: Let R be a commutative ring. Then the symbol

$p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_n x^n$; $a_0, a_1 \ldots a_n \in R$ is called a ***polynomial*** in x over R.

We denote the set of all such symbols by R [x].

Definition: In R [x], p (x) = $a_0 + a_1x + \ldots + a_n x^n$ and q(x) = $b_0 + b_1 + b_1x + \ldots + b_mx^m$ are said to be ***equal*** if n= m and $a_i = b_i$ for all i.

Definition: Addition in R [x]

Let p(x) = $a_0 + a_1x + \ldots + a_n x^n$; q(x) = $b_0 + b_1 + b_1x + \ldots + b_mx^m$ be elements in R[x]. Then p(x) + q(x) = c(x) ∈ R[x], where c[x] = $c_0 + c_1x + \ldots + c_ix^i + \ldots$ and $c_i = a_i + b_i$ for all i.

Definition: Multiplication in R[x]

Let p(x) = $a_0 + a_1x + \ldots + a_n x^n$ and q(x) = $b_0 + b_1 + b_1x + \ldots + b_mx^m$ be elements of R[x]. Then

p(x) q(x) = $c_0 + c_1x + c_2x^2 + \ldots\ldots \in R[x]$
Where,

$c_j = a_0 b_j + a_1 b_{j-1} + a_2 b_{j-2} + \ldots + a_jb_0$.

Theorem 8.10.1: *With the addition and multiplication defined above, R[x] is a commutative ring*.

Note: If, 1 ∈ R , then R[x] also has the identity element.
R[x] is called the ***ring of polynomials*** in x over R.

Definition: Degree of a Polynomial

Let p(x) = $a_0 + a_1x + \ldots + a_n x^n \in R[x]$ such that $a_n \neq 0$.

Then n is said to be the ***degree*** of p(x) and we denote degree {p(x)} = n.

Note: i) We do not define the degree of the zero polynomial.
ii) A polynomial of the form p(x) = c ∈ R is called a ***constant polynomial*** and deg (p(x)) = 0

Hence, for any p(x) ∈ R [x], deg (p(x)) ≥ 0.

***Lemma* 8.10.2:** *Let R be an integral domain. The degree of the product of two polynomials in R[x] is equal to the sum of their degrees*.

Proof: Let p(x) = $a_0 + a_1x + \ldots + a_n x^n$, $a_n \neq 0$

And $q(x) = b_0 + b_1x + \dots + b_mx^m$, $b_m \neq 0$ be elements of R[x].

Then, degree (p(x)) = n and degree (q(x)) = m

$p(x)\, q(x) = C_0 + C_1x + \dots + C_jx^j + \dots$

where $C_j = a_0b_j + a_1b_{j-1} + \dots + a_jb_0$

We see that $C_{m+n} = a_n\, b_m \neq 0$, since $a_n \neq 0$, $b_m \neq 0$ and R is an I.D

If $j > m + n$, $C_j = \sum_{l+k=j} a_l\, b_k$; then $l + k > m + n$

⇨ Either $l > n$ or $k > m$

If $l > n$, $a_l = 0$ and if $k > m$, $b_k = 0$

∴ each $a_l\, b_k = 0$

⇨ $C_j = 0$ if $j > m + n$

Hence, deg (p(x) q(x)) = deg p(x) + deg q(x).

***Lemma* 8.10.3:** *If $p(x) \neq 0$, $q(x) \neq 0 \in R[x]$, then deg (p(x)) ≤ deg (p(x).q(x)).*

***Lemma* 8.10.4:** *If R is an I.D, then R[x] is also an I.D.*

***Proof*:** Let p(x) and q(x) ∈ R[x], $p(x) \neq 0$, $q(x) \neq 0$

Let deg (p(x)) = m , deg (q(x)) = n

Let $p(x) = a_0 + a_1x + \dots + a_mx^m$ and $q(x) = b_0 + b_1x + \dots + b_nx^n$;

$a_m \neq 0$, $b_n \neq 0$

Since R is an I.D , $a_m\, b_n \neq 0$

Then, $p(x)\, q(x) = C_0 + C_1x + C_2x^2 + \dots + C_{m+n}x^{m+n}$

and $C_{m+n} = a_mb_n \neq 0$

Hence $p(x)\, q(x) \neq 0$

∴ R[x] is an integral domain.

Corollary: If F is a field , F[x] is an I.D.

***Lemma* 8.10.5:** *Let F be a field. Then for any two non-zero polynomials p(x), q(x) in F[x] there exist polynomials t(x), r(x) such that*
p(x) = t(x) q(x) + r(x)

where either r(x) = 0 or deg (r(x)) < deg (q(x))

Proof: If deg (q(x)) > deg (p(x)), put t(x) = 0 and r(x) = p(x) and the lemma is proved. Suppose deg (q(x)) ≤ deg (p(x))

We shall prove the lemma by induction on deg (p(x)).

Let $p(x) = a_0 + a_1x + \dots + a_mx^m \in F(x)$, $a_m \neq 0 \in F$

$q(x) = b_0 + b_1x + \dots + b_nx^n \in F(x)$, $b_n \neq 0 \in F$

Then deg (p(x)) = m , deg (q(x)) = n and m ≥ n.

If m = 0, then n = 0. ∴ $p(x) = a_0$ and $q(x) = b_0$

and we can write $a_0 = a_0 (b^{-1}b_0) = a_0b^{-1}b_0$

i.e, $p(x) = t(x)\, q(x) + r(x)$

where ` $t(x) = a_0b_0^{-1}$ and r(x) = 0

Thus the result is true for m = 0.

Suppose that the lemma is true for all non-zero polynomials in F(x) of degree less than m.

Let $p_1(x) = p(x) - \frac{a_m}{b_n} x^{m-n}\, q(x)$

i.e., $p_1(x) = (a_0 + a_1x + \dots + a_mx^m) – a_mb_n^{-1}x^{m-n} (b_0 + b_1x + \dots + b_nx^n)$

$= (a_0 + a_1x + \dots + a_mx^m) – (a_mb_n^{-1}b_0\, x^{m-n} + \dots + a_mx_m)$

It follow that deg $(p_1(x)) \leq m – 1 < m = \deg (p(x))$

Thus, by induction hypothesis, there exist polynomials t(x) and r(x) in F(x) such that

$p_1(x) = t_1(x)q(x) + r(x)$

where either r(x) = 0 or deg (r(x)) < deg (q(x))

i.e., $p(x) - \frac{a_m}{b_n} x^{m-n}\, q(x) = t_1(x)q(x) + r(x)$

i.e., $p(x) = \left(\frac{a_m}{b_n} x^{m-n} - t_1(x)\right) q(x) + r(x)$

$= t(x)\, q(x) + r(x)$

where either $r(x)=0$ or $\deg(r(x)) < \deg(q(x))$

***Theorem* 8.10.6:** *Let F be a field. Then F[x] is a Euclidean Domain.*

Proof: Since every field is an integral domain, F is an integral domain and so F[x] is an integral domain.

Further, for any two non-zero polynomials p(x), q(x) in F[x], we have $\deg(p(x)\, q(x)) = \deg p(x) + \deg q(x) \geq \deg(p(x))$.

Thus, $\deg(p(x)) \leq \deg(p(x).q(x))$ …… (1)

We define the Euclidean valuation d on F[x] as follows:

$d(p(x)) = \deg(p(x))$, for all $p(x) \neq 0 \in F[x]$. …….(2)

Then d is a non-negative integer.

Lemma 8.10.5, for any two non-zero polynomials p(x), q(x) in F[x] there exist polynomials t(x), r(x) such that

$p(x) = t(x)\, q(x) + r(x)$

where either $r(x) = 0$ or $\deg(r(x)) < \deg(q(x))$.

Hence, F[x] is a Euclidean domain.

***Theorem* 8.10.7:** *Let F be a field. Then F[x] is a principal ideal domain.*

Proof: Since F is a field, F[x] is a Euclidean domain.
Further, every Euclidean domain is a PID.
Hence, F[x] is a PID.

8.10.8 Roots of a Polynomial

Let $f(x)$ be a polynomial over any ring R. An element $\alpha \in R$, such that $f(\alpha) = 0$, is called a ***root*** of $f(x) = 0$.

Definition: A polynomial $f(x) \in F(x)$ is said to be ***irreducible*** if for every factorization

$f(x) = g(x).h(x)$, either $g(x)$ or $h(x)$ is a unit in $F(x)$.

Units in F(x) are all non-zero polynomials of degree '0'

i.e., all constant polynomials.

***Note*:** The field over which the polynomials are constructed plays a vital role in irreducibility.

For example, $f(x) = x^2 + 1 \in \mathbb{R}(x)$ is irreducible

$f(x) = x^2 + 1 \in \mathbb{C}[x]$

$= (x-i)(x+i)$ is reducible

Remarks

1) F[x] is a P.I.D

   i.e,. every ideal of F[x] is of the form $\langle p(x) \rangle$

2) All the units in F[x] are non- zero elements of F.

3) Any two non- zero polynomials f(x) and g(x) $\in$ F[x] have a g.c.d and it can be written as $\lambda(x).f(x) + \mu(x).g(x)$ where $\lambda(x), \mu(x) \in F[x]$

4) The ideal $A = \langle p(x) \rangle$ in F[x] is a maximal ideal if and only if p(x) is an irreducible element of F[x].

   Proof:(a) we shall prove that A is not maximal if p(x) is not irreducible.
   Let p(x) = f(x).g(x) where neither f(x) nor g(x) is a constant.
   Put $B = \langle f(x) \rangle$. Then, $p(x) \in B$
   ⇨ $A \subseteq B \subseteq F[x]$

   If A = B, then $f(x) \in A$

   ⇨ f(x) = p(x) h(x) for some $h(x) \in F[x]$

   ⇨ f(x) = f(x) g(x) h(x)

   ⇨ f(x) (1 – g(x) h(x))= 0

   ⇨ g(x) h(x) = 1 ($\because$ F[x] is an I.D)

   ⇨ g(x) is a constant, which is not possible.

If B = F[x] , then 1 ∈ B.

⇨ 1 = f(x) q(x) for some q(x) ∈ F[x]

⇨ f(x) is a constant, which is not possible.

Hence A is not maximal.

b) We shall prove that A is a maximal if p(x) is irreducible.

If possible, let A ⊆ C ⊆ F[x]

Since F[x] is a P.I.D, there exists c(x) ∈ C such that C = <c(x)>

Now, A ⊆ C ⇒ p(x) ∈ C ⇒ p(x) = c(x) b(x) for some b(x) ∈ F[x]

But p(x) is irreducible.

⇨ Either c(x) or b(x) is a constant.

If c(x) is a constant, then C = F[x]

If b(x) is a constant, then c(x) = p (x)(b(x))$^{-1}$ ∈ A

⇨ C ⊆ A

∴ A = C

i.e., A is not maximal.

8.10.9: *Factorisation of Polynomials*

(***Eisenstein's Criterion***)**:** *Let R be a UFD and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$, $n \geq 1$. If there exist an irreducible element $p \in R$ such that $p/a_0,\ p/a_1, \ldots, p/a_{n-1}, p \nmid a_n, p^2 \nmid a_0$, then f(x) is irreducible.*

For example: If $f(x) = 25x^5 - 9x^4 + 3x^2 - 12$, we have $a_5 = 25, a_4 = -9, a_3 = 0, a_2 = 3, a_1 = 0, a_0 = -12$

Taking $p = 3$ we see that

$$p/a_0,\ p/a_1, p/a_2, p/a_3, p/a_4, p \nmid a_5, p^2 \nmid a_0.$$

Hence by Eisenstein Theorem, f(x) is irreducible.

***Remark*:** *A polynomial f(x) ∈ F[x] is reducible iff f(x) has a zero in F.*

For example, f(x) = $x^2 + 1$ has no root in $\mathbb{R}$ but has a root in $\mathbb{C}$.

Problems

1. Prove that

   (i) $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$
   (ii) $x^2 + 1$ is irreducible over $\mathbb{Z}_7$
   (iii) $x^3 - 9$ is reducible over $\mathbb{Z}_{11}$

   Solution:

   (i) Left to the readers.
   (ii) Here, $\mathbb{Z}_7 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6} \}$

   $f(\bar{3}) = \bar{3}^2 + 1 = \bar{3}$,

   $f(\bar{4}) = \bar{4}^2 + 1 = \bar{3}$,

   $f(\bar{5}) = \bar{5}^2 + 1 = \bar{5}$,

   $f(\bar{6}) = \bar{6}^2 + 1 = \bar{2}$

   We see that $x^2 + 1$ has no zero in $\mathbb{Z}_7$. So it is irreducible in $\mathbb{Z}_7$.

   (iii) We have $f(x)=x^3 - 9 = (\bar{x} - \bar{4})(x^2 + \bar{4}x + \bar{5})$

   and $f(\bar{4}) = \bar{4}^3 - 9 = 64 - 9 = 55 = \bar{0}$

   $\therefore$ $\bar{4}$ is a zero of $x^3 - 9$

   i.e, $(x - \bar{4})$ is a factor of $x^3 - 9$.

2. Prove that $\frac{\mathbb{Z}_5[x]}{\langle x^3+x^2+1 \rangle}$ is a field.

Solution: Since $x^3 + x^2 + 1$ is irreducible in $\mathbb{Z}_5[x]$, the ideal $\langle x^3 + x^2 + 1 \rangle$ is maximal and hence $\frac{\mathbb{Z}_5[x]}{\langle x^3+x^2+1 \rangle}$ is a field.

3. How many elements are there in $\frac{\mathbb{Z}_5[x]}{\langle x^3+x^2+1 \rangle}$? Justify.

Solution: We have $\frac{\mathbb{Z}_5[x]}{\langle x^3+x^2+1 \rangle} = \{f(x) + \langle x^3 + x^2 + 1 \rangle; f(x) \in \mathbb{Z}_5[x]\}$.

By Division algorithm in $\mathbb{Z}_5[x]$, there exists $t(x), r(x) \in \mathbb{Z}_5[x]$ such that

$f(x) = t(x)(x^3 + x^2 + 1) + r(x)$, where

$r(x) = 0 \; or \deg r(x) < \deg(x^3 + x^2 + 1) = 3.$

We may take $r(x) = \alpha x^2 + \beta x + \gamma \in \mathbb{Z}_5[x]$.

Since $t(x)(x^3 + x^2 + 1) \in \langle x^3 + x^2 + 1 \rangle, therefore$

$f(x) + \langle x^3 + x^2 + 1 \rangle = r(x) + \langle x^3 + x^2 + 1 \rangle$

$\Rightarrow f(x) + \langle x^3 + x^2 + 1 \rangle = \alpha x^2 + \beta x + \gamma + \langle x^3 + x^2 + 1 \rangle \ldots \ldots (1)$

In the above expression, α, $\beta, \gamma \in \mathbb{Z}_5$ and order of $\mathbb{Z}_5 = 5$. Consequently, each of α, β, γ can be selected in 5 ways. Hence by (1), the number of elements of the field $\frac{\mathbb{Z}_5[x]}{\langle x^3+x^2+1 \rangle}$ is $5^3 = 125$.

4. Show that < x+2 > is a maximal ideal of $\mathbb{Q}$ [x] and hence $\frac{\mathbb{Q}[x]}{<x+2>}$ is a field.

Solution: < x+2 > = {(x + 2) f(x): f(x) ∈ $\mathbb{Q}$ [x]}

Let x + 2 = f(x) g(x) ; f(x), g(x) ∈ $\mathbb{Q}$ [x]

Then deg (f(x)) + deg (g(x)) = 1 (∵$\mathbb{Q}$ [x] is an I.D)

Case I: deg f(x) = 0 and deg g(x) = 1

Let f(x) = a_0 , g(x) = $b_0 + b_1x$, so that f(x) g(x) = $a_0b_0 + a_0b_1x$

⇨ $a_0b_1 = 1 \Rightarrow a_0|1 \Rightarrow$ f(x) = a_0 is a unit.

So, x + 2 is irreducible.

Case II: deg (f(x)) = 1 and deg (g(x)) = 0, then g (x) is a unit.

Hence < x+2 > is maximal.

Since $\mathbb{Q}$ [x] is a commutative ring with unity, $\frac{\mathbb{Q}[x]}{<x+2>}$ is a field.

Unsolved Problems

1. Prove that any finite integral domain is a field.

2. If R is a ring such that $a^2 = a$, for all $a \in R$, prove that $a + a = 0$, for all $a \in R$.

3. Define maximal ideal of a ring R. Is $\{0\}$ in the ring if integers $\mathbb{Z}$ a maximal ideal? Justify your answer.

4. Prove that a field has only two ideals 0 and itself.

5. Show that $\mathbb{Z}_p = \{0,1,2,\ldots.,p-1\}$ modulo p is a field if and only if p is a prime.

6. Determine all the ideals in $\mathbb{Z}_6$.

7. Define units. Determine the number of units in the ring of integers.

8. Let F be an integral domain and F_1 *and* F_2 be subrings of F. Show that $F_1 \cap F_2$ is an integral domain.

9. Let R be an integral domain and $a, b \in$R. When do we say the following?

   i) a and b are associates in R
   ii) a is an irreducible element in R
   iii) a is a prime element in R

10. Show that the polynomial $x^2 + x + 4$ is irreducible over F, the field of integers modulo 11.

11. Prove that $2+\sqrt{-5}$ is an irreducible element but not a prime element in $\mathbb{Z}[\sqrt{-5}]$.

12. Let Rbe a commutative ring with unity. Prove that an ideal M of R is maximal if and only if $\frac{R}{M}$ is a field.

13. Show that a non-zero commutative ring with unity is a field if it has no proper ideal.

14. Let A and B be two ideals of a ring R, prove that $\frac{A+B}{A} \cong \frac{B}{A \cap B}$.

15. Show that a commutative ring R is an integral domain if and only if for all $a, b, c \in R, a \neq 0, ab = ac \Rightarrow b = c$.

16. Prove that in a principal ideal domain, every non-zero prime ideal is maximal.

17. Let R be a commutative ring with unity. When are the elements $a, b \in R$ called associates? If R be an integral domain with unity and $a, b \in R$ be non-zero elements such that $a|b$ and $b|a$, prove that a and b are associates.

18. Show that every field is an integral domain. Is the converse true? Justify your answer.

19. Define prime ideal and maximal ideal in a commutative ring R. Prove that an ideal P of R is a prime ideal if and only if $\frac{R}{P}$ is an integral domain.

20. Prove that every Euclidean domain is a principal ideal domain.

21. Show that in a unique factorization domain

    i. $a|c, b|c \; and \; (a, b) = 1 \Rightarrow ab|c$
    ii. $(a, c) = (b, c) = 1 \Rightarrow (ab, c) = 1$
    iii. Any two elements have a greatest common divisor.

22. Prove that every field is a Euclidean ring.

23. What do you mean by a prime element p of a commutative domain R with unity? Show that in a principal ideal domain, an element is prime if it is irreducible.

24. Prove that in the ring of integers $\mathbb{Z}$, if p is a prime number, then the ideal $p\mathbb{Z}$ consisting all multiples of p is a maximal ideal.

25. Prove that the principal ideal (a_0) of a Euclidean ring R is a maximal ideal of $R \iff$ the element a_0 is a prime element of R.

26. Let F be a field. Prove that if f (x) and g(x) are two non-zero elements of F [x], then

    deg (f(x) g(x)) =deg (f(x)) +deg (g(x))

Give an example of two non-zero polynomials u (x) and v (x) in $\mathbb{Z}_4$[x] such that
deg (u (x) · v(x)) ≠ deg (u(x)) +deg (v(x))

[Here deg (f (x)) denotes the degree of the polynomial f(x) and $\mathbb{Z}_4$ denotes the ring of integers modulo 4]

27. Let R be an integral domain, a and b be non-zero elements of R. Prove that a is an associate of b <=> the principal ideals (a) and (b) are equal.

28. Show that any non-zero ring homomorphism from a field F to a ring R is one-one.

29. Show that the only field isomorphism $f: \mathbb{Q} \to \mathbb{Q}$ ($\mathbb{Q}$ is the field of rational numbers) is the identity mapping on $\mathbb{Q}$.

30. Prove that if F is a field, then the ideal A=(p(x)) is a maximal ideal of F[x] ⇔ p(x) is an irreducible polynomial over F.

31. Let p be a prime number. Determine all the ideals of $\mathbb{Z}_p$, the ring of integers modulo p.

32. Show that the only units in $\mathbb{Z}[x]$ are 1 and -1.

33. Show that every ring R without identity element can be embedded in some ring with identity.

34. If I be an ideal generated by x^2+1 in $\mathbb{R}[x]$, show that

    i. $\mathbb{R}[x]/I$ is a field;
    ii. $\mathbb{R}[x]/I \cong \mathbb{C}$, the field of complex numbers.

35. Determine the irreducible elements of $\mathbb{Z}$.

36. Show that x^2+1 is a prime element of $\mathbb{R}[x]$.

37. If $f: R \to S$ is a ring homomorphism and I is an ideal of R, then is it necessarily true that $f(I)$ is an ideal of S? Answer with justification.

38. Let $f: \mathbb{Z} \to F$ be a ring homomorphism form the ring of integers $\mathbb{Z}$ onto a field F. Show that F is a finite field and the number of elements in F is a prime.

39. Is x^2+1 an irreducible element of $\mathbb{Z}[x]$? Justify. Show that $\phi: \mathbb{Z}[x] \to \mathbb{Z}[i]$ such that $\phi(f(x)) = f(i)$ is an onto ring homomorphism whose kernel is the principal ideal generated by x^2+1. (Here $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$ and $i^2 = 1$.

40. Consider the ring homomorphism $\phi: \mathbb{R}[x] \to \mathbb{C}$ such that $\phi(f(x)) = f(i)$. Show that ∃ a prime element $f(x) \in \mathbb{R}[x]$ such that $\phi(f(x))$ is not a prime element of $\mathbb{C}$.

41. Prove that if $f: R \to R'$ is an onto ring homomorphism, then f induces a ring isomorphism between $R/\ker(f)$ and R'.

42. If R is a finite commutative ring with unity element, prove that every prime ideal of R is a maximal ideal of R.

43. Show that the polynomial $x^2 - 3$ is irreducible over the field of rational numbers.

44. Prove that every prime element in an integral domain with unit element is irreducible.

45. Define integral domain. Prove that $\mathbb{Z}_n = \{0,1,2, \dots, (n-1)\}$ w.r.t addition and multiplication modulo n is not an integral domain if n is not a prime.

46. Define an ideal of a ring. Prove that $\mathbb{Z} = 98\mathbb{Z} + 99\mathbb{Z}$.

47. What is a principal ideal domain (PID)? Is $\mathbb{Z}$ [x] a PID? Justify.

48. Prove that the polynomial $x^3 + x^2 + 1$ is irreducible in $\mathbb{Z}_5[x]$.

References

[1] Joseph A. Gallian, Contemporary Abstract Algebra
[2] I.N Herstein , Topics in Algebra
[3] J.B fraleigh , Abstract Algebra
[4] N. S. Gopalakrishnan , University Algebra

ABOUT AUTHORS

Mr. Barometer Nongbri, is the Assistant Professor of Mathematics Department, Shillong College, Shillong, Meghalaya, India. He has taught various topics of Mathematics in the Undergraduate Course for the past 16 years. Email ID: baronongbri@gmail.com

Smt. J. Rivulet Gidon, is the Assistant Professor of Mathematics Department, Shillong College, Shillong, Meghalaya, India. He has taught various topics of Mathematics in the Undergraduate Course for the past 16 years. Email ID: rivuletgidon@gmail.com

Mr. Honestar Nongdhar, is the Assistant Professor of Mathematics Department, Lady Keane College, Shillong, Meghalaya, India. He has taught various topics of Mathematics in the Undergraduate Course for the past 13 years. Email : honestnongdhar@gmail.com

ISBN: 978-93-6252-169-9

9 789362 521699

MRP RS. 480/-

Selfypage Developers Pvt Ltd