B.A. 2nd Year
MATHEMATICS

Course Code: MATH202TH
Course Credit:06(DSC)

Algebra

UNITS: 1 to 20

Dr. Aarti Manglesh

Centre for Distance and Online Education (CDOE)
Himachal Pradesh University,
Summer Hill, Shimla - 171005

SYLLABUS

Course Code	MATH202TH
Credits= 6	L-5, T-1, P-0
Name of the Course	Algebra
Type of the Course	Core Course
Continuous Comprehensive Assessment: Based on Assignment	Max. Marks:30
End Semester Examination	Max Marks: 70
	Maximum Times: 3 hrs.

Instructions

Instructions for paper setter: The question paper will consist of two Sections A & B of 70 marks. Section A will be Compulsory and will contain 8 questions of 16 marks (each of 2 marks) of short answer type having two questions from each Unit of the syllabus. Section B of the question paper shall have four Units I, II, III, and IV. Two questions will be set from each unit of the syllabus and the candidates are required to attempt one question from each of these units. Each question in Units I, II, III and IV shall be of 13.5 markseach.

Instructions for Candidates: Candidates are required to attempt five questions in all. Section A is Compulsory and from Section B they are required to attempt one question from each of the Units I, II, III and IV of the question paper.

Core 2.2 : Algebra

Unit-I

Definition and examples of groups, examples of abelian and non-abelian groups, the group Zn of integers under addition modulo and the group U(n) of units under multiplication modul on. Cyclic groups from number systems, complex roots of unity.

Unit-II

Sub groups, cyclic subgroups, the concept of a subgroup generated by a subset and the commutator subgroup of group, examples of subgroups including the center of a group. Cosets, Index of subgroup, Lagrange's theorem, order of an element.

Unit-III

Normal subgroups: their definition, examples, and characterizations, Quotient groups Fundamental theorem of Homomorphism.

Unit-IV

Definition and examples of rings, examples of commutative and non-commutative rings: rings from number systems, Zn the ring of integers modul on. Rings of matrices, polynomial rings. Subrings and ideals, Definition of Integral domains and fields.

Books Recommended

1. John B. Fraleigh, A First Course in Abstract Algebra, 7th Ed., Pearson, 2002.
2. M. Artin, Abstract Algebra, 2nd Ed., Pearson, 2011.
3. Joseph A Gallian, Contemporary Abstract Algebra, 4" Ed., Narosa, 1999.
4. George E Andrews, Number Theory, Hindustan Publishing Corporation, 1984.

CONTENTS

Unit - 1

Some Basic Concepts

Structure

1.1 Introduction

Dear student, in this unit we will study about some of basic concepts which will be useful throughout the course of Algebra. We are families with all these topic, we will only summarize them. In this unit we will discuss about logics, set, function, binary operation.

1.2 Learning Objectives:

After studying this unit students will be able to

1. define mathematical logic and toutologies.
2. solve questions based on logic.
3. define set and basic operations on sets.
4. define function and solve questions based on them.
5. define binary operation and solve question based on them.

1.3 Mathematical Logic

In order to express our idea we use sentences. In mathematics we only deal with sentences which are either true or false but not both. Such sentences are of greater importance and a new term comes into existence i.e.

Statement

A sentence which is either true or false but not both is known as statement for example,

(1) Shimla is capital of Himachal Pradesh. This is a true sentences, so it is a statement.

(2) 9 is smaller than 7, this is a false sentence, so it is a statement.

(3) How are you? This is not a statement because it is neither true nor false.

The statements are mathematically denoted by small letters p, q, r, s etc. If p is a statement then we use 'T' for true statement and 'F' for false statement. 'T' and 'F' are known as truth values of the statement.

Some symbols and Notations

Following symbols are useful to express our ideas in mathematical form.

1. **The Symbol** $\forall$ **:** This symbol stand for "for all" or 'For every'. It is known as universal quantities.

   for example$\forall$ real number x, we have $x^4 \geq 0$.

2. **The Symbol** $\exists$ **:** This symbol is used for "there exists". It is known as existential quantities.

3. **The Symbol I. :**This symbol is used for "such that". Sometime ':' or 's.t.' are also useed for such that.

4. **The Symbol** $\forall$ **:** (Disjunction) : when two or more statement joined by the word 'or', the compound statement is formed which is known as disjunction. The symbol 'V' is a connective which represents or.

   So, p v q is statement which is read as 'p or q'

   The statement p v q is true if

   1. either p or q is true
   2. both p and q are true

   The statement p v q is false

   1. both p and q are false

5. The Symbol Λ or conjunction : When two or more statements are joined by word "and ". Then the compound statement so formed is known as a conjunction. The symbol 'Λ' is used for conjunction. So p Λ q is a statement which is read as 'p and q'

   The statement p Λ q is true iff

1. both p and q are true

The statement p Λ q is false if

1. p is false or q is false
2. both p and q are false

6. The Symbol $\Rightarrow$if p and q are two statement such that the truth of p implies that of q then we write p $\Rightarrow$ q , this is one way implication and we read it as 'p implies q'. For example

$x = 2 \Rightarrow x2 = 4$

The statement p $\Rightarrow$ q is false if

1. p is true and q is false

or we can say a true statement can imply only a true statement while a false statement can imply a true or false statement.

7. The symbol $\Leftrightarrow$: The symbol $\Leftrightarrow$ is used for "if and only if" or "implies and is implied by". We also use 'iff' for this symbol. if the truth of the statement p implies that of q and also the truth of q implies that of p, then we write p$\Leftrightarrow$q, this is both way implication.

For example $x + 3 = 10 \Leftrightarrow x = 7$

The statement p $\Leftrightarrow$ q is true only when p and q are either both true or both false.

The statement p$\Leftrightarrow$q is false when one of the statement is true and other is false.

8. **The symbol ~ or negation :-** opposite of a statement is known as negation of statement. The symbol '~' is used for negation. For example p is a statement 'x is 10' then '~p' is a statement "x is not 10".

Negation of true statement is false and negation of false statement is true.

Tautologies : A statement is a tautologies if it is always true.

Self Check Exercise - 1

Q. 1 Show that the statement (pΛq) $\Rightarrow$ p is a tautology.

Q. 2 Show that the statement ~ (pΛq) $\Leftrightarrow$ (U p V ~ q) is a tautology.

1.4 Set

In day today life, we talked about thegroup of objects of a specifictype, such as, numbers on a dics, a handball team, girlsof height 5 feets in a school etc. In mathematics, we also come across collection, such as, collection of natural number, collection of prime numbers, collection of real number, collection of rational numbers number etc. Some other examples of such collections are,natural numbers greater than 10, the set of consonents, the root of quadratice equation x^2-5x+6 = 0. In all of the preceding examples, we highlighted that each is clearly defined set of items in which we can determine with certainty whether a particular item is a

member of the set or not.. For instance, 1, 2, 3, 4,….9are not the elements of the set of natural numbers more than 10 but 11, 12, 13, 14,….. belong to this collection.

In mathematics, some other common examples of the sets that are used more frequently are :

N : the set of all natural numbers.

W : the set of whole numbers.

Z : the set of integers.

Q : the set of all rational numbers.

R : the set of real numbers.

Z+ : the set of positive integers.

Q+ : the set of positive rational numbers.

R+ : the set of positive real numbers.

Definition :

“A set is a clearly defined group of items.” We use the synonymous words objects, elements and members while defining a set. Capital letters are mainly used to indicate setslike R, S, T, etc whereas small alphabets of English indicates the elemnentof the set like a, b, c, etc. If 'a' is a member of the set 'A', then "a belongs to A" and mathematically we write it as a $\in$A, where '$\in$' is a greek symbol known as epsilon having meaning 'belongs to'. Also if b is not a member of the set A we write it as b $\notin$ A, means "b does not belongs to A".

Representation of Set

Set is mainly written by two methods::

1. Tabular or Roster method
2. Set-builder method

Tabular or Roster method:

In tabular method, we make list of all the elements of the set andandseprate them by commas, also braces { } are used to write the members of the set. The set of all odd integers greater than zero and less than 10, in tabular method is written as {1, 3, 5, 7, 9}. Also the set of all vowels in English alphabet is {a, e, i, o, u} is another example of a set in tabular method. While writtingthe set intabular method we should not write the repeated element i.e. every element is unique. Also the order in which elenents are written does not matter which means we can place element in any position.

For example, the set of letter forming the word 'MATHEMATICS' is {M, A, T, H, E, M, A, T, I, C, S}. If can we written as {S, C, I, E, M, A, T, H}, where the sequence of elements has no meaning

Set-Builder method

In set-builder method, every member of the set has a single common feature which is not satisfed by any member outside the set. For example, in the set {2, 3, 5, 7, 11}, all members are prime number less than 13, and no other number less than 13has this property. So in set-builder methodwe can write it as, X = {a :a is prime number less than 13}. Here we use a (small letter) formember of the set, then we place symbol of colon ":" after that we write that property which is satisfied by all the members of the set and then use braces for whole statement. Mathematically we read it as, "A is a set of all a such that a is a is prime number less than 13" Here "set of all" is given mathematically by the braces { }, and ' such that' is shown mathematically by colon ':'.

Consider a set X= {1, 4, 9, 16, 25, ...} in tabularmethod, in set-builder method it can be written as X = {a : a is the square of a natural number}.

To clarify what we have just said, consider the following examples :

Example 1 : Write the set R = $\left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}\right\}$ in the set-builder form.

Solution : We observe that each member of the set has the numerator one less than the denominator. Also, the numerator begin from 1 but less than 6.

Hence, in the set-builder form is it is written as

R = { a : a = $\frac{n}{n+1}$, where n is a natural number such that 1 $\leq$ n $\leq$6}

Example 2 : Write the roster form of X = {a : a is a letter of the word principal }.

Solution :X= {P, R, I, N, C, A, L} is a roster form of given set X.

Example 3 : Write the solution set of equation $x^2+x-2 = 0$ in roster form.

Solution : On factorization we can write this equation as (x-1) (x+2) = 0 so x = 1, -2. Therefore, the set of solutionof given equation in roster form is {1, -2}.

Now, you can try the following exercises -2

Self Check Exercise - 2

Q. 1 Write the following sets in the set-builder form.

(1) {3, 6, 9, 12 } (2) {2, 4, 8, 16, 32}

(3) {5, 25, 125, 625} (4) {2, 4, 6, ...}

(5) {1, 4, 9, ... 100}

Q. 2 Write in the roster form

(1) X = {a :a is an integer and -3 $\leq$a< 7}

(2) Y = {y :y is a natural number smaller than 6}

(3) Z = {z :z is a two-digit natural number such that sum of its digits is 8}

(4) D = {The set of letters in 'school' word}

(5) X = {b :b is a prime divisor of 50}.

Types of the Set

The Null Set

"A set which does not contain any element is called the empty set or the null set or the void set. We represent the empty set by the symbol ϕ or { }."

For example, X = {a :a is prime number bigger than 2 and divisible by 2 }. Then the set X is an empty set because 2 is the only even prime number.

Also, Y = {b :b^2 = 4, b is odd}, Here the set Y is empty because the equation b^2 = 4 is not satisfied for any odd value of b.

Finite And Infinite Sets

"A set which is empty or consists of a definite number of elements is called finite set otherwise the set is called infinite set."

For example, let W be the set of days of the week. The W is a finite set. As a week has seven days, this set has 7 members. Mathematically we write it as n(W)=7.Also, the set of natural numbers, the set of even numbers, the set of integers, set of red numbers etc are all the examples of infinite set.

Equal Set

"Two sets A and B are said to be equal if they have exactly the same elements and we write A = B. If two sets are not equal then we write A $\neq$ B i.e. set A is not equal to set B."

For example, A = {1, 2, 3, 4} and B = {4, 3, 2, 1}

Then the set A = B.

Also, A = {x : x - 5 = 0} and B = {x : x is an integral positive root of equation x^2-2x-15 = 0}.

Since the roots of equation x2-2x-15 = 9 are x = 5 and x = -3 and the integral positive root is x-5 = 0. Which is same as the given set A. So the set A = B.

Also the set A = {1, 2, 3} and B = {2, 1, 3, 2, 3} are equal since each element of set A is in B and vide-versa. So a set does not change of one or more elements of the set are repeated.

Subset

"A set A is said to be a subset of a set B if every element of A is also an element of B. If A is a subset of B then we write it as A < B." The symbol '<' stands for 'is a subset of' or is 'contained in'

Also we can write A < B if a $\in$A$\Rightarrow$a$\in$ B, means "A is a subset of B of a is an element of A implies that a is also an element of B."

In order to be a subset of B, A must have all of its elements in B. It is possible that not all of the elements in B are in A. If all elements of B are also in A, then B < A. then A and B are the same set, we have A<B & B<A $\Leftrightarrow$A=B

Hence, every set A is a subset of itself, i.e. A < A. Also empty set ϕ has not element, so ϕ is a subset of every set.

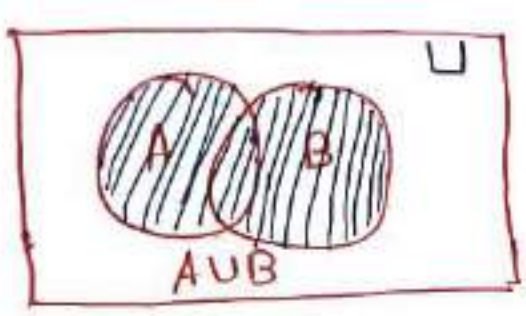
Some example of subset are

1. The set R of real numbers contains all the rational numbers, hence Q < R.
2. If X is the set of all divisions of 56 and Y is the set of all prime divisors of 56 than X = {1, 2, 4, 7, 8, 14, 28, 56} and Y = {1, 2, 7} so B < A.

Operations on Set

Union of Sets :

"Let A and B be any two sets. The union of A and B is the set which consists of all the elements of A and all the elements of B, the common elements being taken only once. The symbol 'U' is used to denote the union of two sets." Mathematically we write AUB and read it as 'A union B'.



Shaded portion of the diagram shows AUB i.e. A union B.

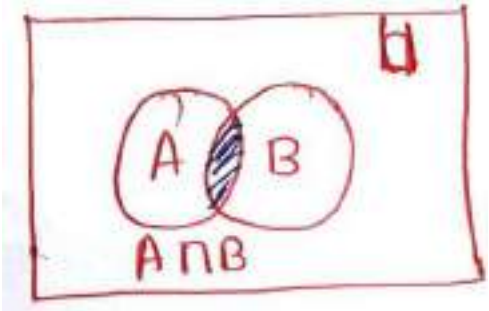
"So, union of two sets A and B is the set C which consists of all those elements which are either in A or in B (including those which are in both)."

$A \cup B = \{x : x \in A \text{ or } x \in B\}$

Intersection of Sets :

"The intersection of sets A and B is the set of all elements which are common to both A and B. The symbol '∩' is used to denote the intersection. So, intersection of two sets A and B is a set c which contains all those elements which belongs to both A and B." Mathematically

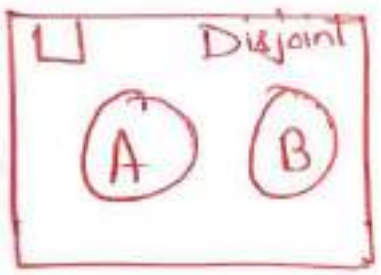
$A \cap B = \{x : x < A \text{ and } x \in B\}$



Shaded portion of the diagram show A∩B i.e. A intersection B

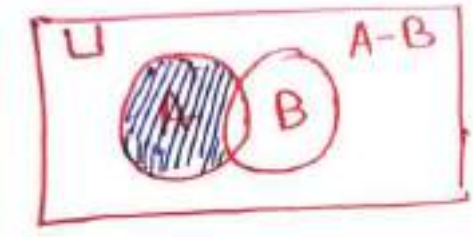
Disjoint Sets

If the intersection two set is empty means there is no common element in sets A and B then the sets are called disjoint sets. Mathematically for disjoint set $A \cap B = \phi$



Difference of Sets

The difference of the sets A and B in this order, is the set of elements which belongs to A but not to B. Symbolically, we write A-B and read it as 'A minus B' mathematically $A-B = \{x : x \in A \text{ and } x \notin B\}$



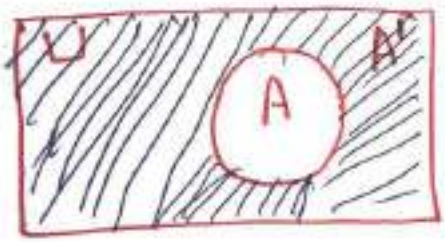
Shaded region shows the difference of Set A and B.

Complement of a set

let U be the universal set and A is a subset of U, then the complement of A is the set of all elements of U which are not the elements of A. Symbolically we write A^1 or A^c to denote complement of A with respect to U. Mathematically

$A^1 = A^c = \{x : x \in U \text{ and } x \notin A\}$

So $A^1 = U - A$



Shaded portion of the diagram shows A^1 or A^c.

To clarify all above topics, consider the following examples.

Example 4 : Let U = {1, 2, 3, 4, 5, 6, 7, 8, 9}, A = {1, 2, 3, 4} B = {2, 4, 6, 8} and C = {3, 4, 5, 6}. Find A', B', (AUC)', (AUB), (A'), (B-C)'

Solution: A' = Ac = {6, 6, 7, 8, 9}

B' = Bc = {1, 3, 5, 7, 9}

AUC = {1, 2, 3, 4, 5, 6}

(AUC)' = {7, 8, 9}

AUB = {1, 2, 3, 4, 6, 8}

(AUB)' = {5, 7, 9}

(A')' = {1, 2, 3, 4}

B - C = {2, 8}

(B-C)' = (1, 3, 4, 5, 6, 7, 9)

Example 5: Show that the set of letters needed to spell "CATARACT" and the set of letters needed to spell "TRACT" are equal.

Solution: Let X be the set of letters in "CATARACT" then

X = {CATR}

Let Y be the set of letters in 'TRACT' then

Y = {TRAC}

Since all the members of the set X and Y are same so X = Y.

Example 6: Let U = {1, 2, 3, 4, 5, 6}, A = {2, 3} and B = {3, 4, 5}

Find A', B', A' ∩ B', AUB and hence show that (AUB)' = A'∩B'

Solution: For the given set A, A' = {1, 4, 5, 6}

and for the set B, B' = {1, 2, 6}

Now A'∩ B' = {1, 6} (1)

AUB = {2, 3, 4, 5}

Now (AUB)' = {1, 6} (2)

∴ Using (1) and (2)

(AUB)' = A' ∩ B' = {1, 6}

Example 7: Let U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10} and A = {1, 3, 5, 7, 9}

Find A' and show that (A') = A

Solution: Given A = {1, 3, 5, 7, 9}

then A' = {2, 4, 6, 8, 10}

Now, (A') = {1, 3, 5, 7, 9} = A

Cartesian Product of Two Sets

Consider two sets A and B. Let a $\in$A and b $\in$B. Then (a, b) denotes the ordered pair. The object a is called first co-ordinate of ordered pair (a, b) and the object b is known as its second co-ordinate.

Definition:

"If A and B are sets, the set of all distinct ordered pairs whose first co-ordinate is an element of A and whose second coordinate is an element of B is called the Cartesian product of A and B and is denoted by A×B"

Mathematically

$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.

For Example: Let A = {a, b, c} and B = {p, q} then A×B = {(a, p), (a, q), (b, p), (b, q) (c, p), (c, q)}

Similarly B×A = {(p, a) (p, b), (p, c), (q, a), (q, b), (q, c)}.

For here we can see that A×B ≠B× A

Self Check Exercise - 2

Q.3 If A = {1, 2, 3, 4, 5, 6, 7, 8, 9}

B = {2, 3, 4, 5}

C = {2, 4, 6, 8}

D = {4, 5, 6, 7}

Find BUC, B∩D and verify that (BUC) U (AUD) = A.

1.5 Functions:

Let A = {a, b, c} and B = {x, y, z, t}. Let a is associated to x, b is associated to y and c is associated to z, by virtue of some rule we assign to each element of A, a unique element of B. Then the set $\{(a, x), (a, y), (b, z)\}$ of such assignment is called function from A to B. If we denotes. This function by f, then we write f : A→B and read if as f is mapping or f is a function from A to B.

Definition:

"Let A and B be two given non empty sets. Let a cossespondance 'f' which associates to each member of A a unique member of B." Then This mapping is written as

f : A $\rightarrow$ B.

Range And Domain of Function:

"Let f is a function from A to B i.e. $f : A \to B$, then the set A is called domain of function f and the set B is called co-domain of function f." Range of f consist of those elements of B which are images of at least one element in A.

Mathematically, We denote range of $f : A \to B$ by $f(A)$

So $f(A) = \{f(x); x \in A\}$ also $f(A) \subseteq B$.

Transformations OR Operators:-

If $f : A \to B$ i.e. if the domain and codain of a function is same, then we call f as an operator or transformation of A.

Equality of two functions: Two functions f and q of $A \to B$ are said to be equal iff $f(c) = g(x)$ $\forall$ $x \in A$ and then we write $f = g$.

If mappings, $f \neq g$, from A to B. then $\exists$ at least one element $x \in A$ such that $f(x) \neq g(x)$.

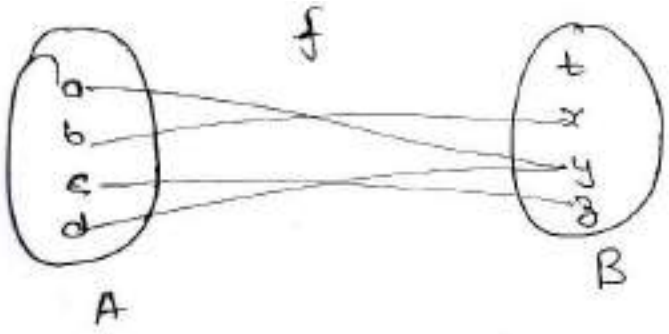
Diagrammatic Representation of a function:

Let $f : A \to B$ where

A = {a, b, c, d}

B = {t, x, y, z}

defined as $f(a) = y$, $f(b) = x$, $f(c) = z$, $f(d) = y$. then, diagrammatically.



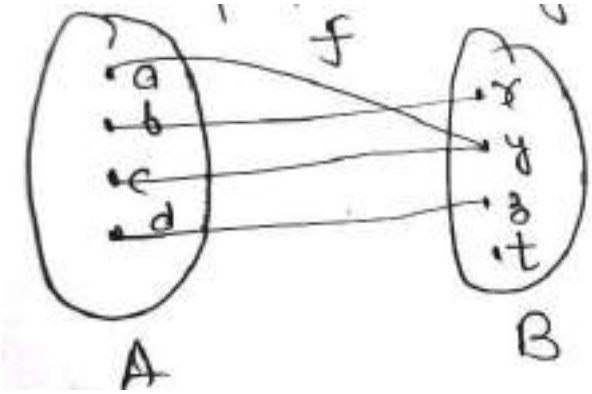
Then from definition of function, we have

1. every element of A is joined to some element in B
2. an element in A cannot be joined to two or more distinct elements in B. (unique image)
3. two or more element in A may be joined to same element in B. (two elements can have same image)
4. There are some element in B which are not joined to any element of A.

Types of Functions:-

Into Function:-

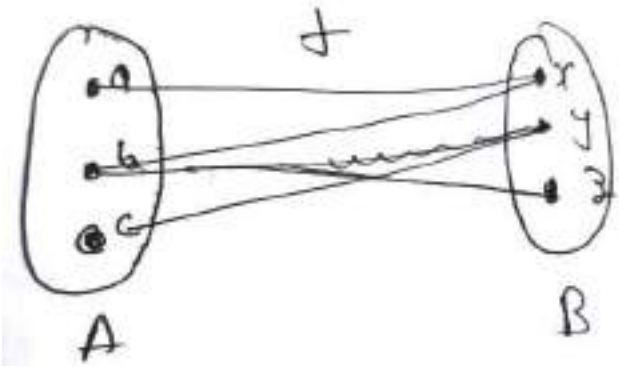
"If the function or mapping $f : A \to B$ is such that there is at least one element in B which is not the f -image of any element in A. Then we say that f is a mapping or function A 'into' B." Diagrammatic representation of into function.



Here the range of F is a proper sub set of the co-domain of f i.e. f (A) CB, So in 'into' mapping at least one member of the co-domain B is left converged by the f -images of the domain A.

Onto Function:

"A mapping or function $f : A \to B$ is such that each element in B is the f image of at least one element in A, then the mapping is known as 'onto' mapping or function."



Here the range of f is same as the co-domain of f i.e. f (A) = B. So in 'onto' mapping the co-domain B is completely covered by the f -images of the domain A.

One-One Function

"A mapping or function $f : A \to B$ is said to be one-one if different elements in A have different f -images in B," i.e. if

$f(x) - f(x') \Rightarrow x = x'$

In one-one function an element in B has only one pre-image in A.

Many-one Function

"A function $f : A \to B$ is said to be many-one if two (or more than two) distinct elements in A have the same f-image in B" i.e.

$f(x) = f(x')\ x \neq x'$

In many-one function some element in B have more than one pre-image in A.

One-One On To Function

"If $f : A \to B$ is one-one and onto B, then f is called a one to one correspondence between A and B."

A mapping which is one-one and onto is a bijection mapping.

Identity Function:

"Let A be a non empty set. Let the function $f : A \to A$ be defined as $f(x) = x\ \forall x \in A$, that is each element of A be mapped on itself. Then f is called the identity function or identity transformation on A."

Identity function is always one-one and onto.

Constant Function

"A function $f : A \to B$ is called a constant function if the same element $b \in B$ is assigned to each element of A." or we can say $f : A \to B$ is a constant function if $f(A)$ = range of f = b (only one element)

Inverse Image of An Element):-

"Let f be a function of A to B i.e. $f : A \to B$ and let $b \in B$. then the inverse image of the element b under f denoted by $f'(b)$, and it consists of others elements in A which have b as their f-image"

Mathematically, if $f : A \to B$

then $f'(b) = \{x: x \in A \text{ and } f(x) = b\}$.

f' is read as "f inverse" also. f' (b) is always a subset of A.

Inverse Function:

"If f : A $\rightarrow$ B is a one-one and onto function then f ': B $\rightarrow$ A is known as inverse function of the function f, which associates to each element b $\in$B the element a $\in$A, such that f (a) = b."

- only one-one onto function can have inverse function.
- If f : A $\rightarrow$ B is one-one and onto then f ': B $\rightarrow$ A is also one-one and onto
- The inverse function of a function is unique.

Self Check Exercise - 3

Q.1 Let A = {-2, -1, 0, 1, 2} and f : A $\rightarrow$ R is defined by f (x) = x^2 + 1. Find the range of f.

Q.2 Find the range of f (x) = x^3, f (x) = sin x, f (x) = x^2 + 1.

Q.3 Let f : Q $\rightarrow$Q defined as f (x) = 2x + 3, x $\in$ Q set of rational numbers. Show that f is one-one and onto. Also drive the formula for inverse function.

1.6 Binary Operations

In earlier classes, we studied various operations like addition, subtraction, multiplication and division of numbers along with union intersection of sets, and composition of function etc. In all these operations any two elements of given set are operated to get a unique element of the same set. Consider the operation of addition of natural number. When the addition '+' operates on any two natural numbers a, and b, it gives a unique natural number a+b. Or we can say that operation of addition '+' associates every ordered pair (a, b) of natural numbers a and b to a unique natural number a+b.

Definition:

"A binary operation '*' : A$\times$A$\rightarrow$A is called a binary operation on the set A.

If a set A is closed with respect to the composition '*' then we say that '*' is a binary operation on the set A."

For example:-

1. Addition is a binary operation on the set of natured number
2. Addition is binary operation on the set of even natural number.
3. Addition is not a binary operation on the set of odd natural number. $\therefore$ 3.5 $\in$ odd natural number but 3 + 5 = even number.
4. Subtraction is not a binary operation n the set of natural number.

Types of Binary Operations

1. **Commutative Operation:-** A binary operation '*' or a set A is called commutative if

   $a * b = b * a \quad \forall \quad a, b \in A$

2. **Associative Operation:-** A binary operation '*' on a set A is called associative if

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

3. **Distributive Operations:-** Let A be a set on which two binary operations '*' and '0" are defined. Then a * (b 0 c) = (a * b) 0 (a * c) is fifth distributive (b 0 c) * a = (b * a) 0 (c * a) is right distributive w.r.t. 0.

Identity And Inverse Element of Binary Operation

Let * : $A \times A \rightarrow A$ be a binary operation on A. then an element $e \in A$ is called an identity element for operation * if

$e * a = a \forall e \quad \forall \quad a \in A.$

Also an element a of the set A has inverse or is inversible for a binary operation * with identity e if $\exists$ $b \in A$ such that

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

Then b is the inverse of a and is written as a'.

Self Check Exercise - 4

Q.1 What is additive identity for set of real number.

Q.2 What is multiplicative identity for set of natural number.

1.7 Summary

Dear students in this unit we studied that

1. A sentence which is either true or false but not both is a statement.
2. A statement which is always true a tautology.
3. A well defined collection of objects is a set.
4. Set can be presented in roster or set builder form.
5. If $f : A \rightarrow B$ be a mapping or function then A is domain and B is co-domain of f.
6. If $f : A \rightarrow B$ then $f(A)$ = range of $f = \{f(x) : x \in A\}$.
7. one-one-onto function is a bijective function.
8. one-one-onto function only can have inverses function.
9. Inverse function if exists then it is unique.

10. If a set is closed with respect to composition '*' then '*' is a binary operation.

1.8 Glossary

- **Power Set:-** It is the set of all subset of S, where S is any set.
- **Relation:-** A Relation R is the subset of the Cartesian product of the two non-empty set $A \times B$.
- **Groupaid:-** It is the set having one binary operations satisfying only closure.

1.9 Answers to Self Check Exercises

Self Check Exercise - 1

Q.1

p	q	$p \wedge q$	$p \wedge q \Rightarrow p$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

Q.2

p	q	$p \wedge q$	$\vee (p \wedge q)$	$\vee p$	$\vee q$	$\vee p \vee q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	T	T
F	F	F	T	T	T	T

Self Check Exercise - 2

Q.1

1. $A = \{x : x \text{ is a multiple of } 3\}$
2. $A = \{2^n; n = 1, 2, 3, 4, 5\}$
3. $A = \{2^n, n^n \leq 5, n \in N\}$
4. $A = \{x ; x \text{ is an even integer } \geq 2\}$
5. $A = \{x^2; x \in N\ x \leq 10\}$

Q.2

1. $X = \{-3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
2. $Y = \{1, 2, 3, 4, 5\}$
3. $Z = \{17, 80, 44, 62, 26, 35, 53, 71\}$
4. $D = \{S, C, H, O, L\}$
5. $X = \{2, 5,\}$

Q.3

$B \cup C = \{2, 3, 4, 5, 6, 8\}$

$B \cap D = \{4, 5\}$

$A \cup O = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Self Check Exercise - 3

Q.1 f (A) = {5, 2, 1}

Q.2 R, [-1, 1], [1, ∞]

Q.3 Use definition of one-one and onto to prove this. Also f^{-1} (y) = $\frac{y-3}{2}$, y $\in$ Q is the formula for defining the inverse function f ' $\rightarrow$ Q $\rightarrow$Q.

1.10 References/Suggested Readings

1. Vijay k. Khanna and S.K. Bhaimbri, A course in Abstract Algebra.
2. Joseph A. Gallian, Contemporary Abstract Algebra.
3. Frank Ayres Jr. Modern Algebra, Schaum's outline Series.
4. A.R. Vasistha, Modern Algebra, Krishna Prakashan Media.

1.11 Terminal Questions

Q.1 X = $\left[-\pi/2, \pi/2\right]$ and

Y = {Y : Y $\in$ R and -1 < y < 1} Y = [-1, 1]

show that the function f : X $\rightarrow$ Y defined by f (x) = sin x, x $\in$x, is one-one and onto Also find the inverse map f ': Y $\rightarrow$ X.

Q.2 Let C be the set of complex number. Prove that f : C $\rightarrow$ R given by f (z) = |z|, z $\in$ C is neither one-one nor onto.

Q.3 Define binary operation. Show that the relation * given by a*b = a^b is a binary operation on the set of natural numbers. Also check for associative nature.

*****

Unit - 2

Group

Structure

2.1 Introduction

Dear student, in unit 1we revised the basic concepts of sets and binary operations. Here we shall study an algebraic system with a binary operation defined on its elements, which satisfies certain postulates, called group.

The term group was used by Galois around 1830 to describe sets of one to-one functions on finite sets that could be grouped together to form a set closed under composition. As is the case with most fundamental concepts in mathematics, the modern definition of a group that follows is the outcome of a long evolutionary process. Although this definition was given by both Heinrich weber and wather von Dyck in 1882, it did not gain universal acceptance until the 20th century.

Groups have widespread applications in various branches of mathematics, including algebra, number theory, geometry, physics and chemistry. They provide a framework for studying symmetry, transformations and abstract algebraic structures. The study of groups, known as group theory, is a rich and important area of mathematics with numberous applications and connections to other fields.

2.2 Objectives Learning

After studying this unit, students will be able to

- Understand Grouoid, semigroup and monoid

- Understand the Group.
- Define and prove different properties of group
- Solve questions related to group.

2.3 Groupoid, Semi Group And Monoid

Groupoid

A non-empty set G together with a binary operation '*' defined on it is called a groupoid if it satisfies the closure property only

$a*b \in G \ \forall \ a, b \in G$

Semigroup

A non-empty set G together with a binary operation '*' defined on it is called a semigroup if it satisfies, closure property and associative property i.e.

1. $a*b \in G, \forall \ a, b \in G$
2. $a*(b*c) = (a*b)*c, \forall \ a, b, c \in G.$

Monoid

A non empty set G together with a binary operation '' defined on it is called a monoid if it satisfies following properties

1. $a*b \in G \ \forall \ a, b \in G$
2. $a*(b * c) = (a * b) * c \ \forall \ a, b, c \in G$
3. $\exists$ an element $e \in G$ such that

   $a * e = a = e * a \ \forall a \in G.$

Here 'e' is known as identity element of G with respect to binary operation '*'.

In order to understand more about semi group and monold let us take following examples.

Example 1: Show that the set of all natural numbers form a semi-group under the composition of addition.

Solution: Let N = {1, 2, 3, 4, ...} be the set of natural numbers.

(i) Closure Property : Since $n + m \in N$

$\therefore$ N is closed under addition.

(ii) Associative Property : Since

$(n + m) + p = n + (m + p), \forall \ n, m \ p \in N.$

$\therefore$ Associative property hold in N under addition.

Hence N is semi-group under addition.

Note: (N, +) is not a monoid, as (n, +) do not have identity (zero) element.

Example 2: Show that the set G = $\{\begin{bmatrix} x & y \\ x & y \end{bmatrix}$: x, y $\in$ R, s.t. x + y $\neq$ 0} form a semi-group under the operation of matrix multiplication.

Solution: The G satisfies the following under multiplication of matrices.

(i) **Closure Property :** Let A = $\begin{bmatrix} x_1 & y_1 \\ x_1 & y_1 \end{bmatrix}$, B = $\begin{bmatrix} x_2 & y_2 \\ x_2 & y_2 \end{bmatrix}$ be any two elements of G, where $x_1 + y_1 \neq 0$ and $x_2 + y_2 \neq 0$.

$\Rightarrow$ $(x_1 + y_1)(x_2 + y_2) = x_1 x_2 + y_1 x_2 + x_1 x_2 + y_1 y_2 \neq 0$

$\therefore$ $AB = \begin{bmatrix} x_1 & y_1 \\ x_1 & y_1 \end{bmatrix}\begin{bmatrix} x_2 & y_2 \\ x_2 & y_2 \end{bmatrix}$

$= \begin{bmatrix} x_1x_2 + y_1x_2 & x_1y_2 + y_1y_2 \\ x_1x_2 + y_1x_2 & x_1y_2 + y_1y_2 \end{bmatrix} \in G$

for $x_1 x_2 + y_1 x_2 + x_1 y_2 + y_1 y_2 \neq 0$.

$\therefore$ G is closed under multiplication.

(ii) **Associative Property :** Since matrix multiplication is associative.

$\therefore$ Associative property hold in G also.

Hence G form a semi-group under multiplication.

Note: The above set do not form a monoid under multiplication. Since it has no identity element.

Proof: Let E = $\begin{bmatrix} a & b \\ a & b \end{bmatrix}$ be the element of G such that

$AE = A = EA, \forall = \begin{bmatrix} x & y \\ x & y \end{bmatrix} \in G$, where $x + y \neq 0$.

i.e. $\begin{bmatrix} x & y \\ x & y \end{bmatrix}\begin{bmatrix} a & b \\ a & b \end{bmatrix} = \begin{bmatrix} x & y \\ x & y \end{bmatrix} = \begin{bmatrix} a & b \\ a & b \end{bmatrix}\begin{bmatrix} x & y \\ x & y \end{bmatrix}$

i.e. $\begin{bmatrix} xa + ya & xb + yb \\ xa + ya & xb + yb \end{bmatrix} = \begin{bmatrix} x & y \\ x & y \end{bmatrix} = \begin{bmatrix} ax + bx & ay + by \\ ax + bx & ay + by \end{bmatrix}$

Taking first two, we get

$(x + y)\, a = x \quad \Rightarrow \quad a = \frac{x}{x+y}$

(x + y) b = y $\Rightarrow$ b = $\frac{y}{x+y}$

Also, taking, last two, we get

(a + b) x = x $\Rightarrow$ (a + b - 1) x = 0

(a + b) y = y $\Rightarrow$ (a + b - 1) y = 0. on adding we get

(a + b - 1) (x + y) = 0, but x + y $\neq$ 0

$\Rightarrow$ a + b - 1 = 0

$\Rightarrow$ a + b = 1

Thus, the element E in G is not unique.

Hence the identity element in G donot exist.

Example 3: Show that the set of natural numbers form a monoid under the composition of multiplication.

Solution: Let N = {1, 2, 3, 4, ...} be the set of natural numbers.

(i) **Closure Property :** Since m n $\in$N, $\forall$ m, n $\in$N

$\therefore$ N is closed under multiplication.

(ii) **Associative Property :** Since (m n) p = m (n p), $\forall$ m, n, p $\in$ N

$\therefore$ N is associative under multiplication.

(iii) **Existence of identity :** There exist 1 $\in$ N such that

m . 1 = m = 1.m, $\forall$ m $\in$ N, then

1 is the identity element of N under multiplication.

Hence (N, .) form a monoid.

Example 4: Let X be any non-empty set, let P(X) denote the power set of X. Then show that

(a) P(X) form a monoid under the operation $\cap$, intersection of sets.

(b) P(X) form a monoid under the operation U, union of sets.

Solution: (a) (i) **Closure Property:** For any elements A, B $\in$ P(X).

$\Rightarrow$ A, B are subsets of X $\therefore$ A $\cap$ B is also subset of X.

i.e. A $\cap$ B $\in$ P(X)

$\therefore$ Closure property hold in P(X)

(ii) **Associative Property :** Since associative law hold under intersection of sets.

$\therefore$ In particular, it hold in P(X) also

i.e. $(A \cap B) \cap C = A \cap (B \cap C), \forall, A, B, C \in P(X)$.

(iii) **Existence of identity :** There exist an element $X \in P(X)$ such that

$A \cap X = A, \forall A \in P(X)$

$\therefore$ X is the identity element of P(X).

Hence, $(P(X), \cap)$ is a monoid.

(b) (i) Closure Property: For any element $A, B \in P(X)$

$\Rightarrow$ A, B are subsets of X $\quad\therefore\quad$ AU B is also subset of X

i.e. $A \cup B \in P(X)$

$\therefore$ Closure property hold in P(X).

(ii) Associative Property : Since associative law hold under union of sets

$\therefore$ in particular, it hold in P(X) also.

(iii) Existence of identity : There exist an element $\phi \in P(X)$ such that

$A \cup \phi = A, \forall A \in P(X)$

Hence, (P(X), U) is a monoid.

Example 5: Let M(X) be the set of all mapping of a non-empty set X into itself, then show that M(X) form a monoid under the composition of composite of mapping.

Solution: Let $M(X) = \{ f \mid f : X \to X$ is a mapping$\}$

(i) Closure Property : Let $f, g \in M(X)$ be any two elements, then

f o g : $X \to X$ is also mapping.

$\therefore$ f o $g \in M(X) \forall f, g \in M(X)$.

$\therefore$ M(X) is closed under the composite of mapping.

$h \in M(X)$ be any elements. Then

$((f$ o g) oh) (x) = (f o g) (h(x)) = f (g (h(x))) and

f o(g o h)) (x) = f ((g o h) (x)) = f (g (h(x)))

$\therefore$ ((f o g) o h)) (x) = f ((g o h) (x)) = f (g (h (x)))

$\Rightarrow$ (f o g) o h = f o (g o h) $\forall f, g, h \in M(X)$

$\therefore$ Associative law hold in M(X).

(iii) **Existence of identity :** There exist an element i : X $\to$X defined by i (x) = x, $\forall$ x $\in$X such that

f o i = f = i of $\forall$ $f \in$ M(X)

i is called the identity element of M(X) under composite of mapping.

Hence M(X) form a moniod.

Example 6: Let $M_2(I)$ be the set of all 2 $\times$ 2 matrices over the set of integers. Show that the set $M_2(I)$ form a monoid under the composition of multiplication of matrices.

Solution: Let $M_2(I) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix}$: where a, b, c, d $\in$ I$\}$

(i) **Closure Property :** Let A = $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, B = $\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ be any two elements of $M_2(I)$, where $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in$ I

Now AB = $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$

Clearly, AB $\in M_2(I)$ $\forall$ A, B $\in M_2(I)$

$\therefore$ $M_2(I)$ is closed under multiplication.

(ii) **Associative Property :** Since multiplication of matrices is associative.

$\therefore$ in particular, associative law hold in $M_2(I)$ also

i.e. (AB) C = A (BC) $\forall$ A, B, C $\in M_2(I)$

Self Check Exercises - 1

Q.1 Show that (n, +), (N, .), (Z, +) and (R, +) are semi groups.

2.4 Group - Definition

A non-empty set 'G' togather with a binary operation '$*$' on

G is sais to form a group if it satisfies following postulates:

1. Closure Property: for all a, b, in G,

   a $*$ b $\in$ G, $\forall$ a, b $\in$ G.

2. Associative Property: For all a, b, c in G,

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

3. Existence of identity: For all a $\in$ G, $\exists$ an element e $\in$ G, such that, a $*$ e = e $*$ a = a $\forall$a$\in$ G.

Here e $\in$ G is called Identity element of G.

4. Existence of Inverse: For all a $\in$ G, $\exists$ a' $\in$ G (depending upon a), such that, a $*$a' = a' $*$ a = e.

   Here 'a', is called an inverse of 'a', we write a' = a^{-1}.

The algebraic structure $\langle G,* \rangle$ satisfying above properties is called a group.

Note: A group is always a group paid or semi group or monoid, but the converse is not true.

Finite and Infinite Groups

If the set G in the group $\langle G,* \rangle$ is a finite set, then it is called a finite group otherwise it is called an infinite group.

$\therefore$ Order of a Group

The order of a finite group < G, $*$> is defined as the number of distinct elements in G. It is denoted by 0(G) of |G|. If a group G has n elements, then o(G) = n.

Remark: The order of an infinite group is not defined or we say that the order is infinite.

Abelian and Non-abelian Group

A group <G, *> is called an abelian group or commutative group

iff a $\neq$ b = b $*$ a, $\forall$ a, b $\in$ G.

If a $*$ b $\neq$b$*$a, $\forall$ a, b $\in$ G, then the group <G, $*$> is called a non-abelian group.

Some Illustrative Examples of Groups

Example 1: Let Z be the set of all integers and let * is the binary opration '+' then to prove that (Z, +) is a group.

Solution: Here the non empty set is Z and the binary operation is ordinary addition. In order to prove that (Z, +) is a group, we have to prove all the four axioms of the group, as follows:

1. **Closure Property:-** Let us take two numbers from the set of integers and apply the operation of addition on them, the result and number will be the integer. For example, Let 2, 5 $\in$ Z and 2 + 5 = 7 $\in$ Z Hence it satisfies the closure property. So we can say $\forall$ a, b $\in$ Z, a +b $\in$Z (as sum of two integer is an integer).

2. **Associative Property:-** Just like closure property, if we take three intger and apply the operation of addition on then, we get the number which is an integer. For example, let 2, 5, 7 are three integers than

   2+ (5+7) = 2+ (12) = 14

   and

   (2 + 5) + 7 = 7 + 7 = 14

   So 2+(5 + 7) = (2 + 5) + 7 = 14

   Hence it satisfies the Associative Law.

Mathematically $\forall$ a, b, c $\in$ Z, a+ (b+c) = (a+b)+c.

3. **Existence of identity:** For the existence of identity in the set of integer under addition, we have to find an integer when added to an integer gives the same integer. As we know 0 is an integer and when we add 0 to any given integer we get the same integer. For example if we add 0 to 5, So '0' will act as identity element for 5. This '0' will act as identity element for the whole set of integer. So, mathematically we can write it as $\forall$ 0 $\in$ Z, $\exists$ 0 $\in$ Z, such that

   a + 0 = a = 0 + a.

   Here '0' is identity element for the set of integers.

4. **Existence of Inverse:-** For the existence of inverse, in the set of integer under addition, we have to find integer which when added, we have to find integer which when added to a given integer gives the identity element (which is zero in present case). As we know that set of integers contains negative, zero and positive numbers. When we add negative of an integer to itself we get zero which is identify element. As when we add (-5) to 5 i.e. 5+ (-5), we get '0' which is identity element, This is true for al integers. So, mathematically, we can write it as

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

Here (-a) is the additive inverse of a in Z.

Since all the four properties are satisfied for the set of integer under addition, So algebraic stature (z, +) forms a group.

Note: To prove (Z, +) is a commutative group or Abelian group.

Commutative Property:

When we add 2 and 5 we get 7 and also when we add 5 and 2 we get 7 i.e. 2+5 = 7 = 5+2, and this result holds for every integer, mean commutative law hold for the set of integers. Mathematically, we can write it as;

$\forall$ a, b $\in$ Z, a + b = b + a

As (Z, +) hold commutative Property, so (Z, +) is an abelian group.

Example 2: Let Q^+ be the set of +ve rational numbers. Define * on Q^+ as under: for a, b $\in$ Q+, a*b = $\frac{ab}{3}$, verify that (Q^+, $*$) is an abelian group.

Solution: To prove (Q+, $*$), an abelian group will will prove five properties as:

1. Closure Property:

Let a, b $\in$ Q^+, $\Rightarrow$ a b $\in$ Q^+ [because product of two positive rational numbers is a positive rational number]

$\Rightarrow$ $\frac{ab}{3} \in Q^+$ [$\because$ division of a positive rational number of 3 is a

positive rational number]

$\Rightarrow$ $a * b \in Q^+$

2. Associative Law:

$\forall a, b \in Q^+$

$$(a * b)*c = \left(\frac{ab}{3}\right) * c = \frac{\left(\frac{ab}{3}\right)c}{3} = \frac{(ab)c}{3.3} = \frac{abc}{a}$$

$\therefore$ $(a * b) * c = a * (b * c)$ $\forall$ a, b, c $\in Q^+$

Thus associative law holds.

3. Existence of Identity:

For each $a \in Q^+$, there must be an identity element $e \in Q^+$ such that

$a * e = a = e * a$

Now by defining $a * e = \frac{ae}{a} = a$

$\Rightarrow$ $ea = 3a$

$\Rightarrow$ $e = 3$

Thus $3 \in Q_+$ is the identity element

Now, $a * 3 = \frac{(a)(3)}{3} = a$

and $3 * a = \frac{3 \times a}{3} = a$

Thus $3*3 = a = 3 * a$

4. Existence of Inverse:

For each $a \in Q^+$, there must exists a number $a' \in Q^+$ such that

$a * a^1 = e = 0 = a * a$

Now, $a * a^1 = 3$

$\Rightarrow$ $\frac{aa^1}{3} = 3$

$\Rightarrow$ $a^1 = 9/a$

Now, $a * a^1 = a * \frac{9}{a} = \left(\frac{a.9/9}{3}\right) = \left(\frac{9}{3}\right) = 3 = e$

$\therefore \quad \frac{9}{a} \in Q^+$ is the inverse of $a \in Q^+$.

5. Commutative Law:

For each $a, b \in Q^+$,

$a * b = b * a$

$\therefore \quad a * b = \frac{ab}{3}$

and $b * a = \frac{ba}{3} = \frac{ab}{3} \quad \left[\because ab = ba \ \forall a, b \in Q^+\right]$

$\therefore \quad a * b = b * a \ \forall a, b \in Q^+$

Hence $(Q^+, *)$ is an abelian group.

Example 3: Show that the set S = {-1, 1} under the operation of usual multiplication of integers, is an abelian finite group.

Solution: We will prove all the five properties for both the elements of set S as follows:

Closure Property:

$1, -1 \in S$

$1 \times -1 = -1 \in S$, for $1, -1 \in S$

$-1 \times 1 = -1 \in S$, for $-1, 1 \in S$

$1 \times 1 = 1 \in S$, for $1, 1 \in S$

$-1 \times -1 = 1 \in S$, for $-1, -1 \in S$

Thus $\forall$ a, b $\in$ S $a \times b \in S$

Hence closure property satisfied.

Associative Law:

Since 1, -1 are integers and multiplication of integer is associative so

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

Thus associative property holds in S.

Existence of Identity:

Here we find the identity element for both the elements. Since $1\times1 = 1$ and $-1 \times 1 = -1$ So it satisfies the property $a*e = a = e*a$, where 'e' is identity element. Hence in this given set 'I' $\in$ act as identify element

Existence of Inverse:

Here we find the inverse of each element which also belongs to the set S. Since $1\times1 = 1$ and $-1\times-1 = 1$, which holds the property $a\times a^1 = e = a^1\times a$. So 1 is inverse of 1 and -1 is inverse of -1. Therefore every element of S has an inverse which belongs to S.

Commutative Property

$1\times-1 = -1$

Since $-1 \times 1 = -1 \ \forall\ 1, -1 \in S$

which holds the property $a \times b = b \times a$, which shows that S is a commutative under multiplication.

So, the given set S = {1, -1} is abedian group of finite order.

Example 4 : Show that the set C of all complex numbers forms on infinite abelian group under the addition of complex number.

Solution : Given C is the set of complex number, so

$C = \{x : x = a + ib, a, b \in R\}$

Closure Property

Let x_1 and $x_1 \in$ C then $x_1 = a_1 + ib_1$ and

$x_2 = a_2 + ib_2$ be any two complex numbers, where $a_{11}\ b_{11}\ a_{21}\ b_2 \in R$

Then $x_1+x_2 = (a_1 + ib_1)\ (a_2 + ib_2)$

$= (a_1 + a_2)\ (b_1+b_2)$

$\Rightarrow$ $x_1+x_2 \in$ C [$\because a_{11}\ b_{11}\ a_{21}\ b_2 \in R$ and $a_1 + a_2 \in R\ b_1+b_2 \in R$]

$\therefore$ C is closed under addition.

Associative Property

Let $z_1 = a_1 + ib_1$, $z_2 = a_2 + ib_2$, $z_3 = a_3 + ib_3$ be any three complex numbers, where a_1, a_2, a_3, b_1, b_2, $b_3 \in$ R.

Then $(x_1+x_2) + x_3 = (a_1 + ib_1) + (a_2 + ib_2) + (a_3 + ib_3)$

$= (a_1 + a_2) + i\ (b_1 + b_2) + (a_3 + ib_3)$

$= [(a_1 + a_2) + a_3] + i\ [(b_1 + b_2) + b_3]$

$= [a_1 + a_2 + a_3] + i\ [b_1 + b_2 + b_3]$

$= [a_1 + (a_2 + a_3)] + i\ [b_1 + (b_2 + b_3)]$

$= (a_1 + ib_1) + (a_2 + a_3) + i\ (b_2 + b_3)$

$\Rightarrow$ $(x_1+x_2) + x_3 = x_1+ (x_2 + x_3)$

Therefore addition is associative in C.

Existence of identity :

Since for all $x = a + ib \in C$ there exist

a complex number $0 = 0 + i- \in C$ such that

$x+0 = (a+ib) +(a+ib)$

$= (a+0) +i(b+0)$

$= a + ib$

$= x$

and $0+x = (a+i0) + (a+ib)$

$= (a+a) + i(0+b)$

$= a + ib$

$= x$

Hence $x+0 = x = 0+x$

Existence of inverse :

Since for all $x = a+ib \in c$, $a, b \in R$, there exist a complex number $-x = -a - ib \in c$, $-a, -b \in R$, such that, $x+(-x) = (a+ib) + (-a-ib)$

$= [a+(-a)] +i [b+(-b)]$

$0+i0$

$= 0$ [-identity of c]

also $-x+x = (-a-ib) + (a+ib)$

$= (-a-a) +i (-b+b)$

$= 0$ [identity of c]

Hence $x+(-x) = 0 = -x+x$

Therefore c has inverse element $-Z = -a-ib \in c$.

Commutative Property:

Since for all $x_1 = a_1+ib_1$ and $x_2 = a_2+ib_2$, $a_1, a_2, b_1, b_2 \in R$, we have

$x_1 + x_2 = (a_1+ib_1) + (a_2+ib_2)$

$= (a_1+a_2) + i (b_1+b_2)$

$= (a_2+a_1) + i (b_2+b_1)$

$= (a_2+ib_2) + (a_1+ib_1) = x_2+x_1$

Hence $x_1+x_2 = x_2+x_1$

Therefore, addition is commutative in C.

Hence C is an abelian group under usual addition.

Also as the set C of complex number is infinite set. So (C, +) is an infinite abelian group under addition.

Examples:- Let $Q*$ denotes the set of all rational numbers except 1, then show that $Q*$ forms an infinite abelian group under the operation $*$ defined by $a*b = a+b - ab \ \forall \ \alpha, \beta \in Q*$.

Solution: Given $Q*$ be the set of all rational numbers except 1, and the binary operation $*$ on $Q*$ is defined as:

$a*b = a+b - ab, a, b, \in Q*$

To prove $(Q*, *)$ is a abelian group we have to prove five properties as follows:

Closure Property: Let $a, b \in Q*$ be two elements of $Q*$ Here to prove $a*b \in Q*$, we will prove that $a+b - ab \in Q$ and $a+b-ab \neq 1$. $\forall$ a, b $\in$ Q*.

Let $a+b-ab = 1$

$a+b-ab-1 = 0$

$a(1-b) -1 (-1b) = 0$

$(a-1) (1-b) = 0$

$a-1 = 0$ or $1-b = 0$

$\Rightarrow$ $a = 1$, $b = 1$, which is not possible as $a, b \in Q*$. as $Q*$ is the set of all rational number except 1.

Hence $a+b-ab \neq 1$ and $a+b-ab \in Q$, therefore $a+b-ab \in Q*$

therefore $a, b \in Q*$

$a*b = a+b-ab \in Q*$.

Hence closure property satisfied.

Associative Property:

Let $a, b, c \in Q*$ be any three elements of $Q*$.

then $(a*b) *c = (a+b-ab) *c$

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

$= a+b+c-ab- [ac+bc-abc]$

$= a+b+c-ab-ac-bc+abc.$

Also $a*(b*c) = a * (b+c-bc)$

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

$= a+b+c-bc-ab-ac+abc$

= a+b+c-ab-ac-bc+abc

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

Thus associative property holds in $Q*$.

Existence of Identity:

Let $\exists e \in Q*$, where e is identity element such that

$e*a = a = a*e, \forall\ a \in Q*$

Now, $e*a = a = a*e-aa.$

$e*a = e+a-ea$ (using the defining of $*$)

$\Rightarrow$ $e-ea = 0$

$\Rightarrow$ $e(1-a) = 0$

$\Rightarrow$ $e = 0$ or $1-a = 0$

if $1-a = 0$

then $a = 1$, but as $a \in Q*$, set of all rational numbers except 1, so $a \neq 1$.

Therefore, $e = 0 \in Q*$

Now, $a*0 = a+0-a0$

$= 0$

$0*a = 0+a-0.a$

$= a$

Therefore, $e = 0 \in Q*$ works as identity element for Q*.

Existence of Inverse:

Let $a \in Q*$, be any element, Let $\exists\ Q^1 \in Q*$ such that $a*a^1 = e = a^1*a$.

Now, $a*a^1 = a+a^1 = a+a^1-a.a^1 = 0 = a^1+a-a^1a$ [$\because$ e = 0]

$\Rightarrow$ $a+a^1-aa^1 = 0$

$\Rightarrow$ $a+a^1(1-a) = 0$

$\Rightarrow$ $a^1(1-a) = -a$

$\Rightarrow$ $a^1 = \frac{-a}{1-a} = \frac{a}{a-1}$, $a-1 \neq 0$

Now $a*a^1 = a*\frac{a}{a-1} = a+\frac{a}{a-1} - a\times\frac{a}{a-1}$

$= \frac{a(a-1)+a-a^2}{a-1}$

$= \frac{a^2 - a + a - a^2}{a-1} = \frac{0}{a-1} = 0 = e$

Similarly $a^1 * a = e$

Hence $a * a^1 = e = a^1 * a$

$\therefore$ $a^1 = \frac{a}{a-1} \in Q^*$ works as inverse element of Q^*.

Commutative Law:

Let $a, b \in Q^*$ be any two elements then

a*b = a+b-ab

= b+a-ba

= b∗a.

$\therefore$ $a * b = b * a \quad \forall \quad a, b \in Q^*$

Also since Q^*, set of all rational numbers except 1, is an infinite set, so Q^* form an. infinite abelian group under the given binary composition.

Example 6: Show that the set of rational numbers does not form a group under multiplication.

Solution: Let Q be the set of all rational numbers.

Closure Property:

Let $a, b \in Q$

$\therefore$ $a = \frac{p_1}{q_1}$ and $b = \frac{p_2}{q_2}$ for some $p^1, p^2, q^1 q^2 \in Z$ and $q^1, q^2 \neq 0$

[By using definition of rational numbers]

then a. $b = \frac{p_1}{q_1} \cdot \frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2} \in Q$. [$\because$ set of integers is closed under multiplication.]

Also as $q_1 \neq 0 = q_2$, So $q_1 q_2 \neq 0$.

$\therefore$ Closures property hold for Q under multiplication.

Associative Property: Let $a_1\ b_1\ c \in Q$, such that $0 = \frac{p_1}{q_1}$, $b = \frac{p_2}{q_2}$ and

and $c = \frac{p_3}{q_3}$ for $p_1, b_2, b_3, 9_1, 9_2, 9_3 \in Z$ and $q_1, q_2, q_3 \neq 0$.

then (a. b). c = $\left(\frac{p_1}{q_1}.\frac{p_2}{q_2}\right).\frac{p_3}{q_3} = \frac{p_1p_2}{9_19_2}.\frac{p_3}{q_3} = \frac{p_1p_2p_3}{q_1q_2q_3}$

$= \frac{(p_1p_2).p_3}{(q_1q_2).q_3} = \frac{p(p_2p_3)}{9_1(q_2q_3)} = \frac{b_1}{9_1}.\frac{(p_2p_3)}{(q_2q_3)}$

Therefore, (a. b) . c = a. (b. c) [$\because$ set of integers is associative under multiplication.

Existence of identity:

For all a $\in$ Q, a = $\frac{p}{q}$, p, q $\in$ Z and q $\neq$ 0, there must exist some e $\in$ Q such that

a. e = a = e. a.

Since 1 $\in$ Q such that

a. 1 = a = 1. a

$\Rightarrow$ $\frac{p}{q}.1 = \frac{p}{q} = 1.\frac{p}{q}$

Hence 1 $\in$ Q, act here as identity element.

Existence of Inverse:

Since the set of rational number contain 0. and no element of Q satisfies

0. a^1 = 1 = a1 . 0

Hence 0 $\in$ Q has no multiplicative Inverse in Q.

Therefore (Q, .) is not a group.

Example 7: Prove that the set G = $\left\{\begin{bmatrix} x & y \\ x & y \end{bmatrix} : x, y \in R \, such \, that \, x + y \neq 0\right\}$ form. a semi group under the operation of matrix multiplication.

Solution: The given set is G = $\left\{\begin{bmatrix} x & y \\ x & y \end{bmatrix} : x, y \in R \, s.t. \, x + y \neq 0\right\}$

Closure Property:

Let A = $\begin{bmatrix} x_1 & y_1 \\ x_1 & y_1 \end{bmatrix}$, B = $\begin{bmatrix} x_2 & y_2 \\ x_2 & y_2 \end{bmatrix}$ be any two element of G where $x_1+y_1 \neq 0$. $x_2+y_2 \neq 0$

that $(x_1+y_1)(x_2+y_2) = x_1x_2 + y_1y_2 + x_1y_2 + x_2y_1 \neq 0$

Therefore A.B = $\begin{bmatrix} x_1 & y_1 \\ x_1 & y_1 \end{bmatrix}\begin{bmatrix} x_2 & y_2 \\ x_2 & y_2 \end{bmatrix}$

$= \begin{bmatrix} x_1x_2 + y_1y_2 & x_1y_2 + y_1y_2 \\ x_1x_2 + y_1y_2 & x_1y_2 + y_1y_2 \end{bmatrix} \in$ G, For $x_1x_2 + y_1y_2 + x_1y_2 + x_2y_1 \neq 0$

$\therefore$ G is closed under multiplication.

Associative Property:

Since matrix multiplication is associative.

Therefore Associative property holds in G also, as.

Let A1 = $\begin{bmatrix} x_1 & y_1 \\ x_1 & y_1 \end{bmatrix}$, B = $\begin{bmatrix} x_2 & y_2 \\ x_2 & y_2 \end{bmatrix}$, C = $\begin{bmatrix} x_3 & y_3 \\ x_3 & y_3 \end{bmatrix}$ be any three elements of G where $x_1+y_1 \neq 0$, $x_2+y_2 \neq 0$ and $x_3+y_3 \neq 0$.

Such that $(x_1+y_1)(x_2+y_2) \cdot (x_3+y_3) = (x_1x_2 + y_1y_2 + x_1y_2 + x_2y_1)(x_3+y_3)$

$= x_1x_2x_3 + y_1y_2y_3 + y_1y_2x_3 + x_1y_2x_3 + x_2y_1x_3 + x_1x_2y_3 + y_1y_2y_3$

$+ x_1y_2y_3 + x_2y_1y_3 \neq 0$

Now, (A.B).C = $\left(\begin{bmatrix} x_1 & y_1 \\ x_1 & y_1 \end{bmatrix}\begin{bmatrix} x_2 & y_2 \\ x_2 & y_2 \end{bmatrix}\right)\begin{bmatrix} x_3 & y_3 \\ x_3 & y_3 \end{bmatrix}$

$= \begin{bmatrix} x_1x_2 + y_1x_2 & x_1y_2 + y_1y_2 \\ x_1x_2 + y_1x_2 & x_1y_2 + y_1y_2 \end{bmatrix}\begin{bmatrix} x_3 & y_3 \\ x_3 & y_3 \end{bmatrix}$

$= \begin{bmatrix} x_1x_2x_3 + y_1x_2x_3 + x_1y_2x_3 + y_1y_2x_3 & x_1x_2x_3 + y_1x_2y_3 + x_1y_2y_3 + y_1y_2y_3 \\ x_1x_2x_3 + y_1x_2x_3 + x_1y_1x_3 + y_1y_2x_3 & x_1x_2x_3 + y_1x_2y_3 + x_1y_2y_3 + y_1y_2y_3 \end{bmatrix}$

Also A.(B.C) = $\begin{bmatrix} x_1 & y_1 \\ x_1 & y_1 \end{bmatrix}\left(\begin{bmatrix} x_2 & y_2 \\ x_2 & y_2 \end{bmatrix}\begin{bmatrix} x_3 & y_3 \\ x_3 & y_3 \end{bmatrix}\right)$

$= \begin{bmatrix} x_1 & y_1 \\ x_1 & y_1 \end{bmatrix}\begin{bmatrix} x_2x_3 + y_2x_3 & x_2y_3 + y_2y_3 \\ x_2x_3 + y_2x_3 & x_2y_3 + y_2y_3 \end{bmatrix}$

$= \begin{bmatrix} x_1x_2x_3 + x_1y_2x_3 + y_1x_2x_3 + y_1y_2x_3 & x_1x_2y_3 + x_1y_2y_3 + y_1x_2y_3 + y_1y_2y_3 \\ x_1x_2x_3 + x_1y_2x_3 + y_1x_2x_3 + y_1y_2x_3 & x_1x_2y_3 + x_1y_2y_3 + y_1x_2y_3 + y_1y_2y_3 \end{bmatrix}$

Therefore (AB) C = A. (BC)

Hence G forms a semi-group under multiplication.

Example 8: The set of all 2×2 matrices over the set of integers i.e. $M_2(I)$ forms a monoid under matrix multiplication.

Solution: Let $M_2(I) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : where\, a_1 b_1 c_1 d \in I \right\}$

Closure Property:

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ be any two elements

of $M_2(I)$, where $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2 \in I$.

Now, $AB = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$

As integer are closed under addition and multiplication. So $AB \in M_2(I)\ \forall\ A, B \in M_2(I)$

Hence $M_2(I)$ is closed under multiplication.

Associative Property:

Since multiplication of matrices is associative.

Therefore associative law hold in $M_2(I)$ also.

$\therefore$ $(AB)C = A(BC) \quad \forall \quad A_1B_1\, C \in M_2(I)$

Existence of Identity:

There exist an element $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M_2(I)$ such that

$AI = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a+0 & 0+b \\ c+0 & 0+d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$IA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+0 & b+0 \\ 0+c & 0+d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\therefore$ $AI = A = IA \quad \forall \quad A \in M_2(I)$

Here $I \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity element of $M_2(I)$ under multiplication.

Hence $M_2(I)$ Forms a monoid under multiplication

Example 9: Show that the set of all 2×2 non singular matrices over real forms on infinite non-abelian group under the composition of matrix multiplication.

Solution: Let G = $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right.$ where a_1 b_1 c_1 d, $\in$ R such

that ad - bc$\neq$ 0 and as matrix is non singular.

Closure Property:

Let A = $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, B = $\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ where

a_1, b_1, c_1, d_1, a_2, b_2, c_2, $d_2 \in$ R and $a_1d_1 - b_1c_1 \neq 0$ and $a_2d_2 - c_2b_2 \neq 0$

Then AB = $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} \in$ M.

as |AB| = |A| |B| $\neq$ 0.

Hence G is closed under multiplication.

Associative Property:

For A, B, C $\in$ M we have

(AB) C = A(BC) as metric multiplication is associative.

Existence of Identity:

For all A $\in$ M, there exist I $\in$ M such that

AI = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

AI = A = IA

So I = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ act as identity element of M.

Existence of Inverse:

Since for all A $\in$ M we have |A| $\neq$ 0.

Therefore A^{-1} exist in M such that

$AA^{-1} = I = A^{-1}A$.

So A^{-1} is the inverse of A.

Commutative Property:

Let A = $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ such that |A| $\neq$ 0

and B = $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ such that }B} $\neq 0$

then AB = $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0+1 & 1+0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

BA = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0+1 & 0+0 \\ 1+0 & 1+0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$

So that AB $\neq$ BA

Hence commutative does not holds

So G $\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix}, ab-cb \neq 0\right\}$ forms a non-abelian group under matrix multiplication.

Self Check Exercise - 2

Try the following exercises:

E 1. Show that (Z, -) is not a group, where Z is the set of integers.

E 2. Show that the set of all non zero rational numbers is commutative group form with operation $*$ defined by a$*$b = $\frac{ab}{2}$

E 3. Show that the set E of all even integers does not form a group under binary operation a$*$b = 2a+2b.

E 4. Show that the set R of real number form an infinite abelian group under usual addition of real number and also .

E 5. Show that usual multiplication of real number. It does not forms a group show that the set R$*$ of all non zero real numbers forms an infinite abelian group under usual multiplication of real number.

E 6. Show that set C of all complex number does not form a group under usual multiplication of complex number.

E 7. Let Q^* denotes the set of all rational number except - 1. Show that Q^* forms an infinite abelian group under the operation $*$ defined by a&b = a+b+ab, $\forall$ a, b $\in$ Q^*.

E 8. Show that the set of all non-zero rational numbers forms a group under multiplication.

E 9. The set C^* of all non-zero complex numbers forms an infinite abelian group under the operation of multiplication of complex number.

E 10. Does the set E of all even integers forms a group under usual addition?

E 11. Show that the set G of all m×nmatrias over Z forms an infinite abelian group under addition of matrix.

2.5 Elementary Properties of Group

Let $< G, *>$ be a group under the operation $*$. Then G has the following elementary properties.

Proof I. Uniqueness of identity element

The identity element of a group is unique.

Proof: If possible, suppose that e_1 - e_2 are two identity elements of a group.

$\therefore$ $e_1 * e_2 = e_2$ (Since e_1 is identity element) .....(1)

also $e_1 * e_2 = e_1$ (Since e_2 is identity element) ....(2)

Thus $e_1 = e_2$ [From (1) and (2)]

$\therefore$ the identity element of a group is unique.

Prop II. Uniqueness of inverse element

The inverse of each element of a group is unique.

Proof: Let e be the identity element of the group $(G, *)$ and $a \in G$ be an arbitrary element.

If possible, let $b_1, b_2 \in G$, be two inverses of a

$\therefore$ $a * b_1 = e = b_1 * a$ ($\because$ b_1 is inverse of a) ....(1)

and $a * b_2 = e = b_2 * a$ ($\because$ b_2 is inverse of a) ....(2)

Now $b_1 = b_1 * e$ (Since e is identity of G)

$= b_1 * (a * b_2)$ [$\because$ of (2)]

$= (b_1 * a) * b_2$ (By associatively in G)

$= e * b_2$ [$\because$ or (1)]

$= b_2$

$\therefore$ $b_1 = b_2$

Hence each element of a group has unique inverse.

Prop III. Cancellation laws hold in a group

For $a, b, c \in G$, we have

$a * b = a * c \Rightarrow b = c$ {Left cancellation law)

$b * a = c * a \Rightarrow b = c$ (Right cancellation law)

Proof: Let $a, b, c \in G$ so $a^{-1} \in G$ such that

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

Now suppose that $a * b = a * c$

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

$\Rightarrow$ $(a^{-1} * a) * b = (a^{-1} * a)\, c$, (By associative law in G.)

$\Rightarrow$ $e * b = e * c$

$\Rightarrow$ $b = c$

$\therefore$ $a * b = a * c \Rightarrow b = c$

Similarly, we can prove that

$b * a = c * a \Rightarrow b = c$.

Prop IV. For every $a \in G$, $(a^{-1})^{-1} = a$., where a^{-1} stands for inverse of a

Proof: $\forall\ a \in G \Rightarrow a^{-1} \in G$,

then $a\, a^{-1} = e = a^{-1}\, a$

$\Rightarrow$ inverse of a is a^{-1}

Again $a^{-1}\, a = e = a\, a^{-1}$

$\Rightarrow$ inverse of a^{-1} is a

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

Proof V. Reversal law for inverse of the product/Socks-Shoes Property

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

Proof. Since $a, b \in G$ $\therefore$ $a * b \in G$

$\Rightarrow$ $c \in G$ where $c = a * b$ ....(1)

Also $b, a \in G \Rightarrow b^{-1}, a^{-1} \in G \Rightarrow b^{-1} * a^{-1} \in G$

$\Rightarrow$ $d \in G$ where $d = b^{-1} * a^{-1}$. .....(2)

Consider $c * d = (a * b) * d$ [$\because$ of (1)]

$= a * (b * d)$ (Associative law in G)

$= a * (b * (b^{-1} * a^{-1}))$ [$\because$ of (2)]

$= a * ((b * b^{-1}) * a^{-1})$, (By associatively in G)

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

$\therefore$ $c * d = e$.

Now consider $d * c = (b^{-1} * a^{-1}) * c$ [$\because$ of (2)]

$= b^{-1} * (a^{-1} * c)$ (Associative law in G)

$= b^{-1} * (a^{-1} * (a * b))$ [$\because$ of (2)]

$= b^{-1} * ((a^{-1} * a) * b)$ (Associative law in G)

$= b^{-1} * (e * b) = b^{-1} * b = e$

$\therefore \quad d * c = e$

$\therefore \quad c * d = e = d * c$

$\Rightarrow \quad c^{-1} = d$

$\Rightarrow \quad (a + b)^{-1} = b^{-1} * a^{-1}$.

Prop VI. If a, b $\in$ G be any elements. Then the equations $a * x = b$ and $y * a = b$ have unique solution in G.

Proof. We first prove that the equation $a * x = b$ has a solution in G.

Since $a \in G$, so $\exists\ a^{-1} \in G$ such that

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

Since $a^{-1}, b \in G$ so $a^{-1} * b \in G$

Take $x = a^{-1} * b \quad \therefore \quad x \in G$

Now $a * x = a * (a^{-1} * b)$

$= (a * a^{-1}) * b$ (Associative law in G)

$= e * b$

$= b$

$\therefore$ the equation $a * x = b$ has a solution in G.

Uniqueness.

Let x_1, x_2 be two solutions of the equation $a * x = b$ in G.

$\therefore \quad a * x_1 = b \quad$ and $\quad a * x_2 = b$

$\Rightarrow \quad a * x_1 = a * x_2 \quad \Rightarrow \quad x_1 = x_2$ (By left cancellation law in a group).

Hence the equation $a * x = b$ has a unique solution in G.

Similarly, we can prove that the equation $y * a = b$ has a unique solution in G.

(Solution is $b * a^{-1}$)

Prop VII. Left identity and right identity are the same in a group

Let e and e' be the left identity and right identity in the group (G, $*$).

Then

$e * e' = e'$ (Here e is the left identity)

also $e * e' = e$ (Here e' is the right identity)

Thus $e' = e$.

Hence left identity and right identity in a group are same.

Prop VIII. Left inverse and right inverse of every element in a group is same

Let e be the identity of the group $(G, *)$ and let b and c be the left and right inverse of the element $a \in G$ respectively. Then

$b * a = e$ and $a * c = e$

Now $b = b * e$

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

$= e * c$

$= c.$

Hence the left inverse and the right inverse of every element in a group is same.

Theorem Based on Elementary Properties of Group.

Theorem I. Let G be a non-empty set together with a binary operation such that closure property and associative law hold in g. Then the existence of left identity and left inverse in G implies the existence of same right identity and same right inverse in G.

Proof. Let e be the left identity and a^{-1} be the left inverse of a in G.

i.e. $e * a = a, \forall a \in G$ and $a^{-1} * = e.$

We first show that left cancellation law holds in G.

i.e. if $a * b = a * c$ then $b = c$

Now $a * b = a * c$

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

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

$\Rightarrow$ $e * b = e * c$

$\Rightarrow$ $b = c.$

Next, we show that e is also the right identity in G.

i.e. $a * e = a, \quad \forall a \in G.$

Now $a^{-1} * (a * e) = (a^{-1} * a) * e$

$= e * e = e$

$= a^{-1} * a.$

$\therefore$ By left cancellation law, we have $a * e = a.$

Secondly, we show that a^{-1} is also the right inverse of a in G.

i.e. $a * a^{-1} = e.$

Now $a^{-1} * (a * a^{-1}) = (a^{-1} * a) * a^{-1}$

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

$\therefore$ By left cancellation law, we have $a * a^{-1} = e$.

Definition of a Group based on Left axioms

Let G be a non-empty set together with a binary operation $*$ defined on it, then the algebraic structure $\langle G, * \rangle$ is a group if it satisfies the following axioms.

(i) $a * b \in G, \forall\ a, b \in G$ (Closure Property)

(ii) $(a * b) * c = a * (b * c), \forall\ a, b, c \in G$ (Associative Property)

(iii) $\exists$ an element $e \in G$ such that

$e * a = a, \forall\ a \in G$ (Existence of left identity)

(iv) For all $a \in G$, $\exists$ an element $b \in G$ such that

$b * a = e$. (Existence of left inverse)

Definition of a Group based on Right axioms

Let G be a non-empty set together with a binary operation $*$ defined on it, then the algebraic structure $\langle G, * \rangle$ is a group if it satisfies the following axioms

(i) $a * b \in G, \forall\ a, b \in G$ (Closure Property)

(ii) $(a * b) * c = a * (b * c), \forall\ a, b, c \in G$ (Associative Property)

(iii) $\exists$ an element $e \in G$ such that

$a * e = a, \forall\ a \in G$ (Existence of right identity)

(iv) For all $a \in G$, $\exists$ an element $b \in G$ such that

$a * b = e$ (Existence of right inverse)

Note: If $\langle G, * \rangle$ be an algebraic system in which closure property, associative property holds. Then G need not be a group if left identity and right inverse exist in G (or right identity and left inverse exist in G).

For example : Let G be any set containing atleast two elements.

Define a binary operation $*$ on G by $a * b = b, \forall\ a, b \in G$.

Clearly, closure property, associative law holds in G.

Also the element $e \in G$ be the left identity in G for $e * a = a, \forall\ a \in G$.

Moreover, $a * e = e \Rightarrow$ e is the right inverse of a.

But $\langle G, * \rangle$ is not a group, for if a, b be two distinct elements of G then $a * b = b$ also $b * b = b$ so $a * b = b * b \Rightarrow a = b$ (by right cancellation law), a contradiction.

Theorem 2. A semi-group in which both the equations $a x = b$ and $y a = b$ have a unique solution, is a group. Prove it.

(It is also called a definition of a group)

Or

Let G be a set with binary operation which is associative. Assume that for all elements a and b in G, the equations a x = b and y a = b have unique solution in G, then prove that G is a group.

Proof. Let G be a semi-group under an operation denoted multiplicatively in which both the equations

$$a\,x = b \quad \ldots(1) \quad \text{and} \quad y\,a = b$$

have a unique solution.

To show that G be a group. For this we show that

(i) identity element exists in G. and

(ii) inverse of each element exists in G.

For (i) By condition (1). For any element $a \in G$, we have

$ax = a$, has a unique solution in G.

$\therefore$ $\exists$ an element $e \in G$ such that $a\,e = a$

Let $b \in G$ be any element of g. Then by condition (2)

$y\,a = b$ i.e. $b = y\,a$

Now $be = (ya)\,e = y\,(ae) = ya = b$

$\Rightarrow$ $b\,e = b$

$\therefore$ e is the right identity of G.

Similarly, by condition (2), for any element $a \in G$, we ahve

$y\,a = a$, has a unique solution in G.

$\therefore$ $\exists$ an element $f \in G$ such that $f\,a = a$ and $f\,b = b$

i.e. f is the left identity of G.

Now, $f\,e = f$ [$\because$ e is the right identity]

and $f\,e = e$ [$\because$ f is the left identity]

$\Rightarrow$ $e = f$

$\therefore$ e is the identity element in G.

For (ii) Let $a \in G$ be any element and e be the identity element of G. Then by condition (1) and (2) $\exists$ a', a'' $\in$ G such that

$aa' = e$ and $a''\,a = e$

Now $a' ' = a' ' e = a' ' (a\ a') = (a' ' a)\ a' = e\ a' = a'$

Thus inverse of each element in G exists and is unique.

Hence G is a group.

Note: If in a semi-group G only one of the equation has a solution. Then G may not be a group.

Theorem 3. Prove that any finite semi-group iff both the cancellation laws hold.

(It is also called a definition of a group, but for finite sets)

Proof: Let G be a semi-group under an operation denoted multiplicatively.

Let G be a group, then both the cancellation laws hold.

(already proved in 1.2 (III))

Conversely, let both the cancellation laws hold.

To prove G is a group

Since G is finite. Let $G = \{a_1, a_2, ..., a_n\}$ be different elements of G.

$\therefore$ $O(G) = n$.

$\forall\ a \in G$, consider $S = \{a_1a, a_2a, ..., a_na\}$

Due to closed property in G, $S \subseteq G$

Further all the elements of S are different.

For it, let $a_ia = a_ja$, $i \neq j$ i.e. $a_i \neq a_j \in G$.

Using Right cancellation law, we get.

$a_i = a_j$, which is absurd.

$\therefore$ all the elements of S are different.

$\therefore$ $O(S) = n = O(G) \Rightarrow S = G$

$\therefore$ $\forall\ a, b \in G$ but $G = S \Rightarrow b \in S$

let $b = a_1a$

i.e. a_1 is a solution of the equation $y\ a = b$, $\forall\ a, b \in G$.

Consider another set $T = \{aa_1, aa_2, ..., aa_n\}$.

$T \subseteq G$ and all the elements of T are different.

For it let $aa_i = aa_j$, $i \neq j$ i.e. $a_i \neq a_j \in G$.

Using left cancellation law, we get

$a_i = a_j$, which is absurd.

$\therefore$ all the elements of T are different

i.e. $O(T) = n = O(G) \Rightarrow T = G.$

$\forall\ a, b \in G, b \in G$ but $G = T \Rightarrow b \in T$

Let $b = aa_k$

$\therefore$ a_k is a solution of the equation $ax = b, \forall\ a, b \in G.$

Thus both the equation $a x = b$ and $y a = b\ \forall\ a, b \in G$ have solutions in G.

Hence G is a group.

Note: If one cancellation law holds, then the system may not be a group.

For example: Let G be any set containing at least two elements. Define a binary operation $*$ on G by $a * b = b, \forall\ a, b \in G.$

Clearly closed property and associative law holds

i.e. G is a semi group.

Here $\forall\ a, b, c \in G, a * b = b$ and $a * c = c.$

$\therefore$ $a * b = a * c \Rightarrow b = c$ i.e. left cancellation law holds.

But G is not a group under $*$.

Here right cancellation law does not hold.

Self Check Exercise = 3

Q.1 Give example of semi-group where cancellation Law may not hold.

Q.2 Give example of semi group, which are not group, but they satisfy cancellation law.

2.6 Summary

We conclude this unit by summarizing what we have covered in it:

1. Concept of groupsid, semi group and monoid.
2. Group set,
3. Finite and infinite groups
4. Abeliane and non-abelian groups
5. Examples of different types of groups.

2.7 Glossary

1. **Group:** A mathematical structure consisting of a set of elements and an operation that combines any two elements in the set, satisfying four properties : Closures, associatively, identity and invariability.
2. **Element:** An object that belongs to a group
3. **Operation:** A binary operation defined on the elements of a group.
4. **Closures:** A property of a group in which the result of performing the group operation on any two elements is always another element in the group.
5. **Associatively:** A property of a group in which the order of performing the group operation on three elements does not effect the final result.
6. **Identity Element:** An element of a group that, when combined with any other element, leaver the other element unchanged. It is denoted by the symbol e.
7. **Inverse Element:** For each element in a group, there exist another element such that their combination results in the identity element. The inverse of element 'a' is denoted by a'.
8. **Commutatively:** A property of a group in which the order of performing the group operation on two elements does not affect the final result. If a group satisfies this property, it is called an abelian group.

2.7 Answers to Self Check Exercise

Self Check Exercise - 2

Q.1 Does not hold associative property.

Q.2 Identity element is 2 and the inverse is $\frac{4}{a}$ for the element a.

Q.3 Does not hold associative property.

Q.4 Identity element is 0 and the inverse for on element a is -a. [For usual addition of real number] But for usual multiplication, for the element 0, there is no multiplicative inverse.

Q.5 Identity Element is 1 and the inverse of an element a is $\frac{1}{a}$.

Q.6 For the element $0 + i0 \in C$, there does not exists in inverse.

Q.7 Identity element is 0 and a' = $\frac{-a}{1+a}$ act as inverse for $a \in Q^*$.

Q.8 Identity element is 1, and for a = $\frac{Þ}{q}$, 0^1 = $\frac{q}{Þ}$ which act as inverse element.

Q.9 Here identity element is $1 + i\,0 = 1 \in C^*$.

and for Z = a + ib$\in$ C^*, $\frac{1}{Z} = \frac{a}{a^2+b^2} + i\left(\frac{-b}{a^2+b^2}\right)$ will act at inverse of Z.

Q.10 Yes.

Self Check Exercise - 3

Q.1 S = Set of 2×2 metrics over integers.

Then S is a semi group under multiplication

If A = $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, B = $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ and C = $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ then AB = Ac But B $\neq$ C.

Q.2 Set of natural number is a semi group under multiplication which hold both celellation law but is not a group.

2.7 References/Suggested Readings

1. Vijay k. Khanna and S.K. Bhaimbri, A course in Abstract Algebra.
2. Joseph A. Gallian, Contemporary Abstract Algebra.
3. Frank Ayres Jr. Modern Algebra, Schaum's outline Series.
4. A.R. Vasistha, Modern Algebra, Krishna Prakashan Media.

2.10 Terminal Questions

1. Show that the set of all natural numbers form a semi group under addition.
2. Show that the set of all natural number form a monoid under multiplication
3. Show that the set of positive integers does not form a group under addition and multiplication.
4. Check whether the set O of all odd integers Forms a group under addition.
5. Prove that the set of complex number Z, such that |Z| = 1, forms a group under multiplication of complex numbers.
6. Show that the set of all rational numbers of the form $\frac{p}{2q}$ is a group under addition.
7. Show that the set G = $\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix}, where\, a,b,c,d \in R\, s.t. ad-bc \neq 1\right\}$ forms a non-abelian group.

*****

Unit - 3

Some Special Group

Structure

3.1 Introduction

Dear student, in this unit we will studied about some special types of groups, like group of integers under addition modulo n, the group of units under multiplication modulo n the group of complex root of unit. These groups has several practical applications in various field like cryptography, computer graphics and image processing, network addressing, game development and simulation. The group of root of unity has its application in signal processing and polynomial inter potation etc.

But before studying about these group, we will study about the composition table and know how we can use this table, to prove given set is a group under certain binary operation.

3.2 Objectives Learning

After studying this unit, students will be able to

- understand the concept of composition table
- understand to write composition table for a given set under defined binary operation.

- able to understand the group of addition modulo n and multiplication modulo n.
- solve the question relate to groups of addition modulo n and multiplication modulo n.
- understand group of complex root of unity and solve questions related to its.

3.3 The Composition Table

A binary operation on finite set can be completely described by means of a table known as a composition table. A composition table provides a systematic way of listing all possible combinations of the group's elements on applying the group operation on them. It is a square array which indicates all the possible product in the system.

Composition table is also known as Cayley table, which is named after the 19th century British Mathematician Arthur Cayley. While writing the composition table, we write the elements of a finite set S in the top horizontal row and the left vertical column in the same order, and apply the rule.

$(ij)^{th}$ entry in table = (i^{th} entry on the left) . (j^{th} entry on the top).

To understand and write a composition table let us take a simple set S = {1, -1} under ordinary multiplication.

Multiplication	x	1	-1	Elements of given set
Elements of given set	1	1×1=1	1×-1=1	
	-1	-1×1 = -1	-1×-1 = 1	

We can check closure property, commutative property, identity element and inverse element by using the composition table, as

1. **Closure property :** If all the entries of the table are elements of the given set and each element of S appears once and only once in each row and in each column, then the set S is closed under the given binary operation.
2. **Commutative property :** If the entries in the table are symmetric with respect to the diagonal (which starts at the upper left corner of the table and terminates at the lower right corner) then the given set S is commutative with respect to given binary operation.
3. **Existence of Identity Element :** If any row is same as the first row in the composition table then the extrem left element in the 2nd row is the left identity of S. Similarly, if any column is same as the first column. Then the element at the top of 2nd column is the right identity of S.
4. **Existence of inverse :** If each row except the topmost row or each column except the left most column contains the identity element then every element of S is invertible with respect to the binary operation. To find the inverse of an

element, we consider that row (or column) in which the element is present and determine the position of identity element 'e' in that row (or column). The corresponding Column (or row) in which e appear act as inverse of that particular element.

To clarify what we have just said, consider the following examples :

Example 1 : The set G = {1, w, w^2} i.e. three roots of unity form a finite abelion group with respect to multiplication by using composition table.

Solution : Here the given set is G = {1, w, w^2} and the binary operation is multiplication

also $w^3 = 1$.

Write all elements of the set in row and column and given operation (x) on the corner and multiply the elements of column with row element one by one and write it in the row, as follow :

x	1	w	w^2
1	$1\times1=1$	$1\times w=w$	$1\times w^2=w^2$
w	$w\times1=w$	$w\times w=w^2$	$w\times w^2=w^3$
w^2	$w^2\times1=w^2$	$w^2\times w=w^3$	$w^2\times w^2=w^4$

Using the property $w^3=1$, $w^4=w^3.w=w$, above table can be written as

x	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

(1) **Closure Property:** Since all the elements in the composition table are elements of the set G, so G is closed under multiplication.

(2) **Associative Property:** Since element of, G are complex numbers and multiplication of complex numbers is associative, so multiplication is associative in G also.

(3) **Existence of Identity:** Since 2nd row is same as I^{st} row. Therefore 1 (extreme left element in 2^{nd} row) is the left identity element of G. Also 2^{nd} column is same as I^{st} column. Therefore 1 is the right identity element of G.

(4) **Existence of Inverse:** Here each raw (Column) of the composition table contains identity element '1' once and only once.

x	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

From the table inverse of 1 is 1, inverse of w is w^2 and inverse of w^2 is w. as $1\times1=e$, $w\times w^2=1=e$, and $w^2\times w = 1$ Hence every element of G has its inverse in G.

(5) **Commutative Property:** Since the entries in the composition table are symmetrical about the principal diagonal so the commutative property holds.

As G is a finite set. So G is a finite abelian group under multiplication.

Example 2: Prove that four roots of unity form a finite abelian group under multiplication using composition table.

Solution: The set of four roots of unity is G = $\{1,-1,i-i\}$, here the binary operation is multiplication. So the composition table, after using the property $i^2 = -1$, $-1^2 = 1$

x	1	-1	i	-i
1	$\boxed{1}$	-1	i	-i
-1	-1	$\boxed{1}$	-i	i
i	i	-i	$i^2=1$	$-i^2=\boxed{1}$
-i	-i	i	$\boxed{1}$	-1

Closure Property:

Since all the element in the composition table are elements of the set G, So G is closed under multiplication.

Associative Property:

Since element of G are complex number and multiplication of complex numbers is associative. So multiplication is associative in G also.

(3) **Existence of Identity:** Since 2^{nd} row is same as I^{st} row, and 2^{nd} column is same as I^{st} column, so 1 is the identity element of the given set G.

(4) **Existence of Inverse:** Since each row (column) of the composition table contain identity element once and only once.

Therefore inverse of 1 is 1, inverse of -1 is -1, inverse of i is -i and inverse of -i is i, as

$1 \times 1 = 1 = e$

$-1 \times -1 = 1 = e$

$i \times -i = -i^2 = -(-1) = 1 = e$

$-i \times i = -i^2 = -(-1) = 1 = e$

So each element of G has its inverse in G.

(5) **Commutative Property:** Since the entries in the composition table are symmetrical about the principal diagonal, so commutative property holds.

Hence G = $\{1, -1, i - i\}$ four roots of unity, a finite set, is a finite abelian group under multiplication.

Self Check Exercise - 1

Q.1 Consider the binary operation $*$ and 0 defined by the following tables on set S = $\{a, b, c, d\}$ forms a group?

(i)

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

(ii)

0	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Check that both binary operation are commutative.

Q.2 Let a set G $\{e,a,b,c\}$ under the composition defined as below by the composition table.

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

Is G is a group? If it is, whether abelian or not? $*$ G = $\{e,a,b,c\}$ is known as Klein's four group.

3.4 Group of Integers under Addition Modulo n (Zn).

The group of integers under addition modulo n is a mathematical structure that consists of positive integers modulo n under addition ($\oplus_n$). Before studying about this group, let us study about addition modulo n.

Addition Modulo n

Let n be a positive integer greater than 1 and a, b $\in$ Z_n, where Zn = $\{0,1i\,2,3.....,(n-1)\}$. Then we define addition modulo n i.e. $\oplus_n$ as follows:

a $\oplus_n$ b = least non negative remainder when a+b is divided by n.

For example,

1. 11 $\oplus_7$ 9 = (Least non-negative remainder when 11+9=20 is divided by 7) = 6
2. 8 $\oplus_5$ 7 = (Least non-negative remainder when 8+7=15 is divided by 5) = 0, as 15 is divided by 5 and remainder is zero.
3. 8 $\oplus_{10}$ 6 = (Least non-negative remainder when 8+6=14 is divided by 10) = 4.

Note: When a and b are integers such that a-b is divisible by n (a fixed positive integer), then we write it as a $\equiv$ b (mod n) and read it as a is congruent to b modulo n.

For example,

17 $\equiv$ 2 (mod 5), as 17-2 = 15, and 15 is divisible by 5.

16 $\equiv$ 1 (mod 3), as 16-1 = 15, 15 is divisible by 3

20 $\equiv$ 0 (mod 4), as 20-0 = 20 is divisible by 4, addition modulo n.

Now, we will study about group of integers under addition modul n. If a set -

$Z_n = \{0,1,2,.....,(n-1)\}$ n > 1, n $\in$ Z forms a finite abelian group under the composition of addition modulo n, then it is known as group of integers under addition modulo n, or additive group of integers modulo n.

Example 1: Show that $Z_n = \{0,1,2,.....,(n-1)\}$, n be a positive integer greater than 1, forms a finite abelian group under the composition of addition modulo n.

Solution: Given $Z_n = \{0,1,2,3,.....,n-1\}$, n > 1, n $\in$ Z. Also the composition defined here is addition modulo n.

$\therefore$ $\forall$ a, b $\in$]$_n$, a $\oplus_n$ b = least non-negative remainder 'r', when a+b is divided by n.

i.e. a $\oplus_n$ b = r $\Rightarrow$ a+b-r is divisible by n

$\Rightarrow$ a+b$\equiv$ r (mod n)

In order to prove above set Z_n is a group under addition modulo n, we have to satisfy properties of group, as follows:

(1) Closure Property:

$\forall$ a, b $\in$ Zn, 0 $\leq$ a, b < n

a+b$\equiv$ r (mod n) where 0 $\leq$ r < n.

As r $\in$ Z_n, therefore the closure property holds.

(2) Associative property:

$\forall$ a, b, c $\in$]$_n$, the least non-negative remainder remains the same if

(a+b)+c or a+(b+c) are divided by n as addition of positive integers is associative.

$\therefore$ a$\oplus$($_n$b+$_n$c) = (a$\oplus_n$b) $\oplus_n$ c

Thus associative property holds in Z_n.

(3) Existence of Identity:

$\forall$ a $\in$ Z_n, 0 < a < n, we have 0 $\in$ Z_n such that a $\oplus_n$ 0 = the least non negative remainder when (a+0) is divided by n = a

$\therefore$ a $\oplus_n$ 0 = a = 0 $\oplus_n$ a

Hence 0 $\in$ Z_n is the identity element.

(4) Existence of Inverse:

For 0 $\in$ Z_n, 0 $\oplus$n 0 = 0, so 0 is inverse of 0.

Also $\forall$ a $\in$ Z_n, a $\neq$ 0, n-a $\in$ Z_n such that

$a + (n-a) \equiv 0 \pmod{n}$

and $(n-a) + a \equiv 0 \pmod{n}$

i.e. $a \oplus_n (n-a) = 0 = (n-a) \oplus_n a$

Thus n-a act as inverse of a.

(5) Commutative Property:

$\forall\ a, b \in Z_n$,

$a \oplus_n b = b \oplus_n a$, the least positive remainder remains the same as a+b or b+a is divided by n. So commutative property holds.

As the set Z_n is finite. So Zn is a finite abelian group under addition modulo n. This group is known as additive group of integers modulo n.

In the above example, we studies how to prove Z_n. to be a group by using the definition of group, under addition modulo n. Now, we will do the same task by using the composition table, in the next examples.

Example 2: Show that the set $Z_5 \{0,1,2,3,4\}$ is a finite abelian group of order 5 under addition modulo 5.

Solution: Here the given set is $Z_5 = \{0,1,2,3,4\}$ and the binary operation is addition modulo 5 i.e.

$a \oplus_5 b$ = Least non-negative remainder when a+b is divided by 5.

$\therefore$ $0 \oplus_5 b$ = (remainder when 0+1=1 is divided by 5) $1 +_5 2$ = (remainder when 1+2=3 is divided by 5) and so n. Therefore the composition table is as follows:

$+_5$	0	1	2	3	4
0	$\frac{0+0}{5}=0$ 0	$\frac{0+1}{5}$ 1	$\frac{0+2}{5}$ 2	$\frac{0+3}{5}$ 3	$\frac{0+4}{5}$ 4
0	$\frac{0+0}{5}$ 1	$\frac{1+1}{5}$ 2	$\frac{1+2}{5}$ 3	$\frac{1+3}{5}$ 4	$\frac{1+4}{5}=\frac{5}{5}$ 0
2	$\frac{2+0}{5}$ 2	$\frac{2+1}{5}$ 3	$\frac{2+2}{5}$ 4	$\frac{2+3}{5}=\frac{5}{5}$ 0	$\frac{2+4}{5}=\frac{6}{5}$ 1

3	$\frac{3+0}{5}$ 3	$\frac{3+1}{5}$ 4	$\frac{3+2}{5}=\frac{5}{5}$ 0	$\frac{3+3}{5}=\frac{6}{5}$ 1	$\frac{3+4}{5}=\frac{7}{5}$ 2
4	$\frac{4+0}{5}$ 4	$\frac{4+1}{5}$ 0	$\frac{4+2}{5}=\frac{6}{5}$ 1	$\frac{4+3}{5}=\frac{7}{5}$ 2	$\frac{4+4}{5}=\frac{8}{5}$ 3

i.e.

$+_5$	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

We observe following points from the composition table.

(1) Closure Property:

Since all the elements in the composition table are element of Z_5, So Z_5 is closed under addition modulo 5.

(2) Associative Property:

Let 1, 3, 4 $\in Z_5$

then $(1 +_5 3) +_5 4 = 4 +_5 4 = 3$ {Least positive remainder when 8 is divided by 5}

and $1 +_5 (3 +_5 4) = 1 +_5 7 = 3$

Hence $(1 +_5 3) +_5 4 = 1 +_5 (3 +5 4)$

Similarly, it can be verified for other elements of Z_5 also.

So Addition modulo 5 is associative on Z_5.

(3) Existence of Identity:

Let a $\in Z_5$ be any element Also 0 $\in Z_5$, such that $a +_5 0 = a = 0 +_5 9$, Hence 0 is identity element of Z_5.

(4) Existence of Inverse:

Each row and column consist of the identity element 0. so, every element of Z_5 is invertible.

Also $0 +_5 0 = 0 \Rightarrow$ 0 is inverse of itself

$1 +_5 4 = 0 \Rightarrow$ 4 is inverse of 1

$2 +_5 3 = 0 \Rightarrow$ 3 is inverse of 2

$3 +_5 2 = 0 \Rightarrow$ 2 is inverse of 3

$4 +_5 1 = 0 \Rightarrow$ 1 is inverse of 4

(5) Commutative Property:

Since the composition table is symmetrical with respect to the principal diagonal.

Therefore, $+_5$ is a commutative binary operation on Z_5. As Z_5 has finite number of elements Hence order of Z_5 is 5.

Hence $Z_5 = \{0,1,2,3,4\}$ is a finite abelian group of order 5 under addition modulo 5.

Example 3: Show that the set G = $\{0,1,2,3,4,5\}$ is a finite abelian group of order 6 under addition modulo 6.

Solution: The given set is G = $\{0,1,2,3,4,5\}$ and the binary operation here is addition modulo 6. i.e. $a +_6 b = a+b \pmod 6$ = Remainder when a+b is divided by 6.

The composition table of G = $\{0,1,2,3,4,5\}$ under addition modulo 6 is

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(1) Closure Property: Since all the elements in the composition table are element of Z, So G is closed under the composition of addition modulo 6.

(2) **Associative Property:**Associative property can be cheeked by using any three elements of the set G

Let 1, 2, 3$\in$G

then $(1 +_6 2) +_6 3 = 3 +_6 3 = 0$ {Remainder when 6 is divided by 6}

again $1 +_6 (2 +_6 3) = 1 +_6 5 = 0$

So Associative property holds in G

(3) **Existence of Identity:** Let a $\in$G be any element, also 0 $\in$G, then $a +_6 0 = a = 0 +_6 a$

$\therefore$ 0 is the identity element of the group.

(4) **Existence of Inverse:**From the composition table, we find that each row and column consists of the identity element 0. So, every element of G is invertible.

Also $0 +_6 0 = 0 \Rightarrow$ 0 is inverse of 0

$1 +_6 5 = 0 \Rightarrow$ 5 is inverse of 1

$2 +_6 4 = 0 \Rightarrow$ 4 is inverse of 2

$3 +_6 3 = 0 \Rightarrow$ 3 is inverse of 3

$4 +_6 2 = 0 \Rightarrow$ 2 is inverse of 4

$5 +_6 1 = 0 \Rightarrow$ 7 is inverse of 5

(5) **Commutative Property:** Since the composition table is symmetrical with respect to the principal diagonal.

Therefore, $+_6$ is a commutative binary operation on G. Since G is a finite set satisfying commutative property. Hence G is a finite abelian group under addition modulo 6.

Self Check Exercise - 2

Q.1 Show that the set G = $\{0,1,2,3,4,5,6\}$ is a finite abelian group of order 6 under the composition of addition modulo 7.

Q.2 Show that the set G = $\{0,1,2,3\}$ forms a group 6 under addition modulo 4.

3.5 The Group of Units under Multiplication Modulo n. (U_n)

The group Zn consists of the elements $\{0,1,2,3,.....,(n-1)\}$ with addition modulo n as the operation. When we multiply the element of Z_n, we did not get a group, as the element 0 does not have a multiplicative inverse. However, if we take only that elements of Z_n, which have multiplicative inverse, called units, we get a group under multiplication modulo n (X_n) It is denoted by U_n and is called group of units in Z_n. Before studying about this group, Let us study about multiplication modulo n.

Multiplication Modulo n

Let n be a positive integer greater than 1 and a, b $\in$ Z_n where Z_n = $\{0,1,2,3,.....,(n-1)\}$ then, we define multiplication modulo n i.e. X_n as follows:

a $\times_n$ b = Least non-negative remainder when ab is divided by n.

For example:

1. 4 $\times_5$ 3 = Least non-negative remainder when 4×3 = 12 is divided by 5 = 2
2. 4 $\times_8$ 6 = Least not-negative remainder when 4×6 = 24 is divided by 8 = 0
3. 7 $\times_{12}$ 8 = Least non-negative remainder when 7×8 = 56 is divided by 12 = 8

As we said earlier that the set U_n consists of only those elements of Z_n which have multiplicative inverse. An integer 'a' has a multiplicative inverse modulo n if and only if a and n are co-prime or relative prime.

For n = 10

Zn = $\{0,1,2,3,4,5,6,7,8,9)\}$

But for U_n we have to select only those element of Z_n which has multiplicative inverse and only those element has multiplicative inverse which are co-prime to 10 and those elements are 1, 3, 5, 7, 9

Therefore for n = 10

U_n = $\{1,3,7,9\}$

Now, to prove that set U_n forms a group.

Example 1: Prove that U_n = $\{x \in Z;(x,n)=1,1 \le x \le h\}$ is a group under multiplication modulo n.

Solution:

Closure Property:

Let a, b $\in$ U_n and the binary operation is multiplication modulo n. i.e. a $\times_n$ b = r i.e least non-negative remainder when ab is divided by n.

Mathematically ab = (q) n+r, 0 ≤ r ≤ n-1.

as a, b $\in$ U_n so (a, n) = 1 and (b, n) = 1

[∵ a and b are co-prime to n.

So gcd of a and n will be 1 and bond n]

As a $\times_n$ b = r, to prove r $\in$ U_n, we have to prove

(1) r ≠ 0

(2) (r, n) = 1

Let r = 0 $\Rightarrow$ ab = an $\Rightarrow$ n/ab $\left[\because a/b.c,(a,b)=d \Rightarrow \frac{a}{d}/c\right]$

and (n.a) = 1 $\Rightarrow$ $\frac{n}{1}$|b $\Rightarrow$ n/b $\Rightarrow$ (b, n) $\neq$ 1 which is a contradiction as b $\in$ Un and (b, n) = 1.

So $r \neq 0$

(2) Now, to prove (r, n) = 1

If (r, n) $\neq$ 1 $\left[(a,b)\neq 1, \exists\ prime\ Þ\ such\ that\ Þ/a\ and\ Þ/b\right]$

$\exists$ prime no Þs.t.Þ/r and Þ/n

Now, Þ/n $\Rightarrow$ Þ/qn

and Þ/r $\Rightarrow$

$\Rightarrow$ Þ/qn+r $\Rightarrow$ Þ/ab

$\Rightarrow$ either Þ/a or Þ/b

If Þ/n and Þ/a $\Rightarrow$ Þ = 1 which is a contradiction

again Þ/n and Þ/b $\Rightarrow$ Þ = 1 which is a contradiction

$\therefore$ (r, n) = 1, $r \neq 0$

Hence r$\in$ U(n)

$\therefore$ Closure property is satisfied under multiplication modulo n.

(2) Associative Property:

$\forall$ a, b, c $\in U_n$

The least non-negative remainder remains the same if (ab) c or a(bc) is divided by n.

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

Thus associatively holds in U_n.

(3) Existence of Identity:

Since for a $\in U_n$.

$a \times_n 1 = 1 \times_n a = a$ and 1 $\in U_n$ as

a.1 and 1.a leaves the same remainder when divided by n.

So 1 $\in$ Un act as identity element of U_n.

(4) Existence of Inverse:

Let a $\in U_n$ so (a, n) = 1

$\exists$ integer l, m $\in$ Z such that [$\because$ (a, b) = 1, $\exists$ l, m$\in$Z such that l(a) + m(b) = 1]

la + mn = 1

l = q(n) + r, $0 \leq r \leq n-1$

We claim that r is the inverse of a we have to prove.

(1) $a \times_n r = 1$

(2) $r \in U_n \Rightarrow r \neq 0$ and (r, n) = 1

(qn + r) a + mn = 1

qna + mn + ra = 1

$$\frac{n.(qa+m)+ar=1}{ar=(-qa-m)^{n+1}}$$

$\Rightarrow$ $a \times_n r = 1$

Now to prove $r \in U_n$, $r \neq 0$

Let r = 0

(qa + m) n + 0 = 1

(qa + m) n = 1, which is not possible for $n \geq 2$

$\Rightarrow$ $r \neq 0$

Now to prove (r, n) = 1

Let (r, n) = d

$\Rightarrow$ d/r and d/n

$\Rightarrow$ d/ar and d/(qa+m) n

$\Rightarrow$ d/ar + (qa+m) n

$\Rightarrow$ d/1 and 1/d

$\Rightarrow$ d = 1

$\therefore$ (r, n) = 1

as $r \neq 0$ and (r, n) = 1 $\therefore$

Therefore $a \times_n r = 1$

$\therefore$ $a-1 = r \in U_n$.

(5) Commutative Property: $\forall$ a, b $\in U_n$, the least non-negative remained remains the same if ab or ba is divided by n.

i.e. $a \times n\ b = b \times_n a$

Thus commutative property holds in U_n.

Thus U_n is an abelian group. Under multiplication modulo n. This completer the result.

Now we will prove the group U_n be an abelian group using composition table.

Example 2: Prove that group of unit U_{10} forms a group under multiplication modulo 10 using composition table.

Solution: Since the elements of U_{10} will be the elements of $Z_n = \{0,1,2,3,4,5,6,7,8,9\}$ which are co-prime to 10.

$\therefore$ $U_n = \{1,3,7,9\}$

To prove $U_{10} = \{1,3,7,9\}$ is a group under multiplication modulo 10

i.e. $a \times_{10} b$ = least non negative remainder when ab is divided by 10

$3 \times_{10} 7$ = Least non negative remainder when $3 \times 7 = 21$ is divided by 10 = 1

$9 \times_{10} 7$ = Least non negative remainder when $9 \times 7 = 63$ is divided by 10 = 13

The composition table is:

$+_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(1) **Closure Property:** Since all the elements in composition table are element of U10, so U10 is closed under multiplication modulo 10.

(2) **Associative Property:** Since the least non-negative remainder remains the same if (ab)c or a(bc) is divided by n.

$\therefore$ $(a \times_{10} b) \times_{10} c = a \times_{10} (b \times_{10} c)$

So associativity holds in U_{10}.

(3) **Existence of identity:** For any $a \in U_{10} \exists\ 1 \in U_{10}$ such that $a \times_{10} 1 = a = 1 \times_{10} a$, Hence 1 is the identity element of U_{10}.

(4) **Existence of Inverse:** Since each row and column consist of identity element 1 once and only once, so every element of U_{10} is invertible.

Also $1 \times_{10} 1 = 1$ 1 is inverse of 1

$3 \times_{10} 7 = 1$ $\Rightarrow$ 7 is inverse of 3

$7 \times_{10} 3 = 1 \quad \Rightarrow \quad$ 3 is inverse of 7

$9 \times_{10} 9 = 1 \quad \Rightarrow \quad$ 9 is inverse of 9

(5) **Commutative Property**: Since the composition table is symmetrical with respect to the principal diagonal.

Therefore X_{10} is a commutative binary operation on U_{10}.

Since U_{10} has 4 elements, so U_{10} is finite abelian group of order 4.

Example 3: Prove that U_6 forms a group under multiplication modulo 6 using composition table.

Solution: Since $U_6 = \{1, 5\}$, so the composition table will be.

$+_6$	1	5
1	1	5
5	5	1

$\because \quad 5 \times_6 5 =$ Least non negative

remainder when $5 \times 5 = 25$ is divided by $6 = 1$

(1) **Closure Property:** Since all the elements in the composition table are elements of U_6, so U6 is closed under multiplication modulo 6

(2) **Associative Property:** Since the least non-negative remainder remarks the same if (ab) c or a (bc) divided by 6.

$\therefore \quad (a \times_6 b) \times_6 c = a \times_6 (b \times_6 c)$

So associativity holds in U_6

(3) **Existence of Identity**: For $a \in U_6 \exists\ 1 \in U_6$ such that $a \times_6 1 = a = 1 \times_6 a$. Hence 1 is the identity element of U_6

(4) **Existence of Inverse:** Since each row and column contains the identity element 1, so every element of U6 is invertible.

Also $1 \times_6 1 = 1$ so 1 is inverse of 1

$5 \times_6 5 = 1$ so 5 is inverse of 5

(5) **Commutative Property:** Since the composition table is symmetrical with respect to the principal diagonal. Therefore $\times_6$ is a commutative binary operation on U_6.

Since U6 has 2 element. Hence U_6 is a finite abelian group of order 2

Example 4: Show that the set G = $\{0,1,2,3,4,5,6\}$ is a finite abelian group of order 6 under the composition, multiplication modulo 7.

Solution: The composition table of G = $\{0,1,2,3,4,5,6\}$ under the operation multiplication modulo 7 i.e. a $\times_7$ b = least non negative remainder when ab is divided by 7

$+_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

1. **Closure Property:** Since all the elements in the composition table are elements of G. So G is closed under multiplication

2. **Associative Property:** Since the least non-negative remainder remains the same if (ab)c or a(bc) is divided by 7

   i.e. $(a \times_7 b) \times_7 c = a \times_7 (b \times_7 c)$

   So associatively holds in G

3. **Existence of Identity:** For all $a \in G$, $\exists\ 1 \in G$ such that $a \times_7 1 = a = 1 \times_7 a$. Hence 1 is the identity element of G

4. **Existence of Inverse:** Since each row and column contains the identity element 1, so every element of G is invertible.

   Also $1 \times_7 1 = 1 \Rightarrow$ 1 is inverse of 1

   $2 \times_7 4 = 1 \Rightarrow$ 4 is inverse of 2

   $3 \times_7 5 = 1 \Rightarrow$ 5 is inverse of 3

   $4 \times_7 2 = 1 \Rightarrow$ 2 is inverse of 4

   $5 \times_7 3 = 1 \Rightarrow$ 3 is inverse of 5

   $6 \times_7 6 = 1 \Rightarrow$ 6 is inverse of 6

5. **Commutative Property:** Since the composition table is symmetrical with respect tothe principal diagonal. Therefore, $\times_7$ is a commutative binary operation on G.

Since G has 6 element, so G is finite abelian group of order 6.

Note: Above result can be generalised as.

The set Jp= $\{1,2,3,.....(p-1)\}$ where Þ is a prime number, forms a finite abelian groupof order (Þ-1), under the composition of multiplication modulo Þ.

Self Check Exercise - 3

Q.1 Prove that group of units U_{12} forms a group under multiplication modulo 12 using composition table.

Q.2 Prove that G = $\{0,1,2,3,4,5,6,7,8,9,10\}$ forms a group under multiplication modulo 11

Q.3 Prove that U_{17} forms a group under multiplication modulo 17

Q.4 prove that U_{18} forms a group under multiplication modulo 18

Q.5 U_{11} is an abelian group under multiplication modulo 11.

3.6 Group of Complex

Roots of Unity

A complex number is just a pair z = (a, b) real numbers. We usually write this pair in the form z = a+ib. The number a is called real part of z, write b is called imaginary part of z, and we denote set of complex number by C. Also for every complex number z, we have i.z = z.1 = z./Addition and multiplication of complex number obeys commutative, distributive and associative laws and they also have additive and multiplicative identity.

Also $i^2 = -1$, for complex number. In polar form complex number z is written as

$z = r \cos\theta = r(\cos\theta + 1 \sin\theta) = re^{i\theta}$

If we multiply a complex number by itself repeatedly, then by De Moiner's Formula we have

$$\left[r(cox\theta + i\sin\theta\right]^n = r^n\left(cox\,n\theta + i\sin n\theta\right)$$

This formula can be use to find n^{th} root of any complex number. There are n-1 different n^{th} root of any complex number.

Primitive nth Root of Unity:

The primitive nth root of unity is the complex number w = $e\frac{2\pi i}{n}$. All other n^{th} roots of unity are powers of w. So the n nth root of unity are

$1 = w^0, w^1, w^2, ...w^{n-1}$.

Proof: Since,

$(1)^{\frac{1}{n}} = (1+i0)^{\frac{1}{n}} = (cox\,0 + i\sin 0)^{\frac{1}{n}}$

$= \left[cox(2k\pi+0) + i\,sin(2k\pi+0)\right]^{\frac{1}{n}}$ [$\because$ period of sin and cox is 2π]

$= \left[cox\,2k\pi + i\,sin\,2k\pi\right]^{\frac{1}{n}}$

$= cox\frac{2k\pi}{n} + \sin\frac{2k\pi}{n}, \left[k = 0,1,2,.....n-1\right]$

$(1)^{\frac{1}{n}} = e\frac{2\pi i}{n}$

k = 0 $= \text{cox } 0 + \text{i sin } 0 = 1 + \text{i } 0 = 1$ $\left(cox\frac{2k\pi}{n} + \sin\frac{2k\pi}{n}\right)^0 = w^0 = 1$

k = 1 $= cox\frac{2\pi}{n} + \sin\frac{2\pi}{n} = \text{w}$

k = 2 $= cox\frac{4\pi}{n} + i\sin\frac{4\pi}{n} = cox\,2\left(\frac{2\pi}{n}\right) + i\sin 2\left(\frac{2\pi}{n}\right)$

$= \left(cox\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)$ [By demoives Theorem]

$= \text{w}^2$

k = 3 = cox $\frac{6\pi}{n}$ + i sin $\frac{6\pi}{n}$ = cox $3\left(\frac{2\pi}{n}\right)$ + i sin $3\left(\frac{2\pi}{n}\right)$

$= \left[cox\left(\frac{2\pi}{n}\right) + i\,sin\,3\left(\frac{2\pi}{n}\right)\right]^3$

$= \text{w}^2$

k = n - 1 we get wn-1

k = n = $\left[cox\left(\frac{2\pi}{n}\right) + i\,sin\left(\frac{2\pi}{n}\right)\right]^n$ = (cox 2π + i sin 2π) = 1 + i0 = 1 = w^0

$\therefore$ G = $\{\text{w}^0, \text{w}^1, \text{w}^2, ...\text{w}^{n-1}\}$

$= \{1, \text{w}, \text{w}^2, ...\text{w}^{n-1}\}$

Therefore the set G = $\{\text{w}^0, \text{w}^1, \text{w}^2, ...\text{w}^{n-1}\}$ is the set of n^{th} root of unity.

Example 1: Prove that the set G = {1, w, w^2, ...w^{n-1}}, set of nth root of unity is a finite abelian group w.r.t. multiplication.

Solution: Since the given set is G = {1, w, w^2, ...w^{n-1}} This set has n element so set is finite set of order n.

Closure Property:

Let w^i, w^j, $0 \leq i, j \leq n-1 \in G$

Now $w^i.w^j = w^{i+j}$

Three cases are there

case i, when i+j<n

then wi, wj$\in$ G are as G = {1, w, w^2, ...w^{n-1}}

Case ii; when i + j = n

then w^i, $w^j = w^{i+j} = w^n$

$$= \left[cox\frac{2\pi}{n} + i\,sin\frac{2\pi}{n} \right]^n$$

$= \cos 2\pi + i \sin 2\pi$

$= 1 + i\,0$

$= 1 \in G$

Case (iii) when i+j> n

then i+j = nq+t, 0 < + < n-1

$\therefore$ $w^j.\ w^j = w^{i+j} = w^{nq+t} = w^{nq}.w^t$

$= (w^n)^q.\ w^t$

$= 1^q.\ w^t$ as $w^n = 1$

$= 1.\ w^t$ as t < n-1

w^i, w^j $= w^t \in G$

Therefore for w^i, $w^j \in G$ $w^i.w^j \in G$.

So the set of n^{th} not of unity is closed under multiplication.

Associative Property:

Since multiplication is associative in complex number, so Associative property holds in G, as G is a set of complex number.

Existence of identity:

Since $1 \in G$ works as identity element for the set G.

$\therefore$ $1.\ rw^i = rw^j = w^i, i$ $w^i \in G$

Existence of Inverse:

Since $rw^j \in G \exists w^{n-1} \in G$ such that $w^i, w^{n-i} = w^{n-i}, w^i = w^{n-i+i} = w^n = 1 \in G$ so for $w^i \in G$ w^{n-i} works as inverse element so every element of a has a inverse element.

Commutative Property:

Since complex number holds mutative property under multiplication, so the set G also obeys commutative property.

Hence the set G = $\{w^0, w^1, w^2, ...w^{n-1}\}$ form a finite abelian group under multiplication.

Self Check Exercise - 4

Q.1 Show that the set G = $\{w^0, w^1, w^2, w^3, w^4, w^5\}$ 6^{th} root of unity form an abelian group.

Q.2 Show that the set of cube root of unity forms a group under multiplication, also check the property of commutatively.

Note: Properties of nth root of unity

1. n^{th} root of unity form a GP with common ratio $e^{\frac{i2\pi}{n}}$.
2. Sum of n^{th} root of unity is always 0.
3. Sum of n^{th} power of nth root of unity is zero, if p is a multiple of n.
4. Sum of p^{th} power of nth root of unity is zero if p is not a multiple of n.

3.7 Summary

We conclude this unit by summarizing what we have studied in it:

1. Group of addition modulo n.
2. Group of addition modulo n.
3. Group of units under multiplication modulo n.
4. Group of complex root of unity.
5. Questions related to these special types of group.

3.8 Glossary:

- **Composition Table :-** A composition table is a square matrix that describes the group operation for a finite group.
- **n^{th} Roots of Unity:-** The nth roots of unity refer to the solution of the equation $z^n = 1$. In the complex number system, where n is a positive integer.
- **Addition under Modulonn:-** It involves performing the usual arithmetic addition operation but then taking the remainder when divide by n.

3.9 Answer to Self Check Exercise

Self Check Exercise - 1

Q.1 Yes

Q.2 Yes

Self Check Exercise - 2

Q.1 Solve it same as in example 3.

Q.2 Solve it same as in example 3.

Self Check Exercise - 3

Q.1 Solve it same as in example 4.

Q.2 Solve it same as in example 4.

Q.3 Solve it same as in example 4.

Q.4 Solve it same as in example 4.

Q.5 Solve it same as in example 4.

Self Check Exercise - 4

Q.1 Solve it same as in example 1

Q.2 Solve it same as in example 2

3.10 References/Suggested Reading

1. Vijak k. Khanna and S.K. Bhambri, A course in Abstract Algebra, 5th Edition
2. Joseph A. Gallian, Contemporary Abstract Algebra, 8th Edition.
3. Frank Ayrer Jr, Modern Algebra, Schaum's Outline Series.
4. A.R. Vasistha, Modern Algebra, Krishna Prakashan Media.

3.11 Terminal Questions

1. Let G = $\{1, 2\}$ and define $*$ on G by a$*$b = |a-b|. Is the given set under given binary operation is a group or not.

*****

Unit - 4

Some Special Groups-II

Structure

4.1 Introduction

Dear student, in this unit we will study about some more types of groups known as permutation group and dihedral group. We will try to write the elements of these group and will discuss some of their properties.

4.2 Learning Objectives:

After studying this unit, students will be able to

1. define permutation group
2. prove and apply properties on permutation group
3. define dihedral group
4. prove and apply properties on dihedral group

4.3 Permutation Group

Permutation group are control to study of geometric symmetries and to Galoir theory and to the study of finding solutions of polynomial equations. Permutation groups also gives us an example of non abelian group. Before defining permutation group, we first read about the symmetries of an equilateral triangle Δ ABC. The symmetries actually consists of permutations of the three vertices. These three vertices have the following six permutations.

$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$ $\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$ $\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$

$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$ $\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$ $\begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$

Here a permutation of the set S = $\{A, B, C\}$ is a one-to-one and onto map π : S $\rightarrow$S.

Here $\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$ denotes the permutation that send A to B, B to C and C to A.

* The symmetry of a triangle also form a group

Permutation of Degree n :

Let S be a set having n elements. Then a one-one mapping of S onto itself is called a permutation of degree n.

Degree of the Permutation:

The number of elements in the finite set S is known as the degree of the permutation.

For Example:-

Let S_n = $\left[f(a_1), f(a_2) ..... f(a_n) \right]$

This can be written as

$$\begin{pmatrix} a_1 & a_2 & \_\_\_\_\_ & a_n \\ b_1 & b_2 & \_\_\_\_\_ & b_n \end{pmatrix}$$

Here the first line we write the element of S_n and in second line we write the image of that element of S_n. Two permutations f and g of degree n are said to be equal if we have f (a) = g(a) $\forall$ a $\in$ S.

For example:

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

and g = $\begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

are two permutations of degree 4. In this case, in

f replace 1 $\rightarrow$ 2 2 $\rightarrow$ 3 3 $\rightarrow$ 4 and 4 $\rightarrow$ 1

and g replace 1$\rightarrow$ 2 2 $\rightarrow$ 3 3 $\rightarrow$ 4 and 4 $\rightarrow$ 1

i.e. in both f and g replacement is same

so $f = g$

Note: If S is a finite set having n distinct elements then we have n! distinct permutations of the elements of S.

Symmetric Set of Permutation of Degree n:

The set consisting of all permutation forms a symmetric set of permutation. If S_n be the set consisting of all permutations of degree n, then the set S_n is called the symmetric set of permutation of degree n.

Example 1: S_2 be the set consisting of all permutation of degree 2 and having 2! element.

$$S_2 = \left\{\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\right\}$$

Similarly $S_3 = \left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right\}$ having 6 elements

Similarly S_4, S_5 etc.

Identity Permutation:

If I is permutation of degree n such that I replaces each element by the element itself, then I is called identity permutation of degree n.

For example : $\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}$ are identity permutation of 2, 3 and 4 degree.

Product of two Permutations

If $f = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$ and $g = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$

then $f\,g = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$

Since in f, $1 \to 1$ and in g $1 \to 2$ so in f g we have $1 \to 2$

Similarly in f, $2 \to 3$ and in g $3 \to 1$ so in f g $2 \to 1$

and in f $3 \to 2$ and in g $2 \to 3$ so in f g $3 \to 3$

$$\therefore \quad f\,g = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

Similarly If $= \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$

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

So we can say that in general f g $\neq$g f .

Cycuc Permutation:

A permutation f on a set S is called a cyclic permutation of Length x. If for x_1, x_2, ... $x_n \in$ S such that f (x_t) = x_1 and leaves all other elements of S fixed.

For Example: If f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 5 & 6 \end{pmatrix}$ be a permutation of degree 6 such that f (1) = 3, f (3) = 4 f (4) = 1 f (2) = 2 f (5) = 5 f (6) = 6

Then f = (1 3 4) is a cyclic permutation of degree of length 3. Here the element whose image is the element itself is called an invariant element.

For Example: In f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 8 & 9 \end{pmatrix}$

f (1) = 2, f (2) = 3, f (3) = 4 f (4) = 5 and f (5) = 1

then f = (1 2 3 4 5) is a cyclic permutation of length 5.

Example: (1, 2, 4, 5, 3) on the set (1, 2, 3, 4, 5, 6, 7, 8, 9)

Means: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 1 & 5 & 3 & 6 & 7 & 8 & 9 \end{pmatrix}$ Here the elements 6, 7, 8, 9 remains as it is and the remaining changes as $1 \to 2$, $2 \to 4$, $4 \to 5$, $5 \to 3$, $3 \to 1$

Remarks:

1. Every permutation can be written as product of two cycles
2. A 2 - cycle permutation is called transposition
3. If a permutation can be written as product of even number of permutation then it is called even permutation

   $(1 \quad 2 \quad 3)$ = $(1 \quad 2)(1 \quad 3)$, So $(1 \quad 2 \quad 3)$ is even permutation.
4. If a permutation cannot be written as a product of even number of permutation is called odd permutation $(1 \quad 2 \quad 3 \quad 4)$ = $(1 \quad 2)(1 \quad 3)(1 \quad 4)$ is odd permutation
5. Product of two even permutation is even permutation
6. Product of an odd and an even permutation is permutation.
7. Product of two odd permutation is even permutation.

The set S_3 can be written as

$S_3 = \{I, (1\ \ 2), (1\ \ 3), (2\ \ 3), (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$

Self Check Exercises - 1

Q.1 Write all the elements of the permutation group on symmetric group S4 for (1, 2, 3, 4)

Q.2 If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ and g = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

Show that permutation multiplication is not commutative

Q.3 Write the cycle of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix}$

Write the cycle of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix}$

Example: the symmetric group of n elements S_n is a group with n! elements where the binary operation is the composition of maps.

Here binary operation is composition of map i.e. I : R $\rightarrow$R : I (x) = x is in 5.

Solution:Closur Property: Since let f , g $\in$ S then f 0 g also belongs to S. So composition of map is closed in S.

So composition of map is a binary operation on the set S_n.

Associative Property:

The binary operation is associative so, composition of map is associative on the set S_n.

Existence of Identity:

Since, I_x is the identity map, is the identity of S_n as

f 0 I_x = I_x 0 f = f $\forall$ f $\in$ S_n.

Existence of Inverse:

Also we know that if a function is one-one and onto i.e. f : X $\rightarrow$X then $\exists$g : X $\rightarrow$X sit. f 0 g = g 0 f = Ix So g will act as inverse of f .

Hence S_n, the permutation group or symmetric group on n elements forms a group under the binary operation of composition of map.

Inverse of a Permutation:

The two row representation of inverse of a permutation in S_n is obtained by interchanging the row 0 of the 2 row representation of given permutation.

For Example: If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ then f^{-1} is obtained by interchanging the rows.

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

Example: Find the inverse of $f = (1 \quad 2 \quad 3)$

Solution: Since $f = (1 \quad 2 \quad 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

So $f^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (2 \quad 3 \quad 1)$

Self Check Exercise - 1

Q.5 If f is a cycle $(1 \quad 3)$ in S_5, write f^{-1} in the 2-row format. Also cheek if f^{-1} is a cycle or not

Q.6 Write inverse of $(1 \quad 2)$ and $(2 \quad 4 \quad 5)$ in S_5

Example: Write the composition table of S_2

Solution: Since $S_2 = \{I, (1, 2)\}$

0	I	(1, 2)
I	I	(1, 2)
(1, 2)	(1, 2)	I

$\left[\because \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \right]$

Self Check Exercises - 1

Q.7 Write the composition table of S_3 and prove that S_3 forms a group under composition of map.

The Alternating Group:

The set of all even permutation of S_n row, is called alternating group A_n for n elements.

- The alternating group A_n is a sub group of S_n.

- The number of even permutation in S_n is equal to number of odd permutation, hence order of An is $\frac{n1}{2}$

Self Check Exercise - 1

Q.8 Write the alternating group A_4 of S_4.

4.4 Dihedral Group

A dihedral Group is a group of symmetries of regular polygon with n sides, where n is positive integers. The dihedral group of order 2_n, denoted by D_n is the group of all possible rotations and reflections of the regular polygon. The group D_n consists of 2_n elements, which can be depicted as follows:

- n rotations denoted by R0, $\frac{R360}{n}$, $\frac{R_2(360)}{n}$, ... $\frac{R(n-1)360}{n}$ where R $\frac{i360}{n}$ represents a rotations of $\left(\frac{360i}{n}\right)$ clockwise about the center of polygon.
- n reflections denoted by F_0, F_1, F_1, ..., F(n-1) where F_i represent a reflections across a line passing through the center of the polygon and one of the vertices.
- The group operation in D_n, is the composition of symmetries
- D_1 and D_2 are only abelian dihedral groups otherwise D_n s non abelian for n $\geq$ 3.
- Alternatively, the dihedral group D_n is defined by

Dn = $\left\{r^i s^j; r^n = e, s^2 = e, srs^{-1} = r^{-1}, i = 0, 2...., n-1, j = 12\right\}$

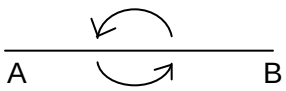
Some Dihedral Groups:

Example 1:

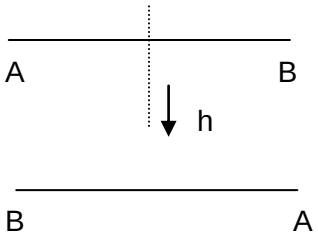
1. D1 = |D1| = 2 i.e. (1 rotation + 1 reflection) = $\left\{r^i s^j; r^1 = 1, s^2 = 1, srs^{-1} = r; i = i, j = 1, 2\right\}$

(1) Ration $\left(\frac{360i}{n} = \frac{360i}{1} = 360\,i; i = 0\right)$ (1) Reflection

(1)



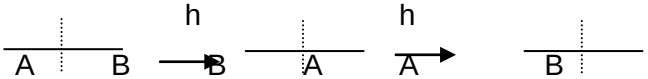
(2)



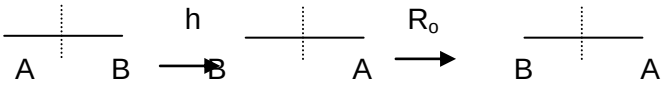
Composition Table:-

$*$	R_0	h
R_0	R_0	h
h	h	R_0

Here h.h $\Rightarrow$



11y R_o h $\Rightarrow$



Example 2:

1. D_2 = |D2| = 4 = (2 rotations + 2 reflections)

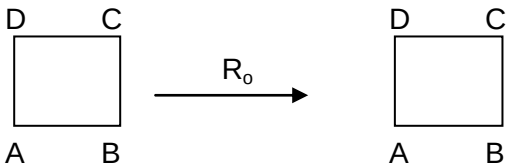
   $D_2 = \left\{r^i s^j; r^2 = 1, s^2 = 1, srs^{-1} = r^{-1}, i = 1,2,\ j = 1,2\right\}$

   $= \{e, r, s, r, s\}$

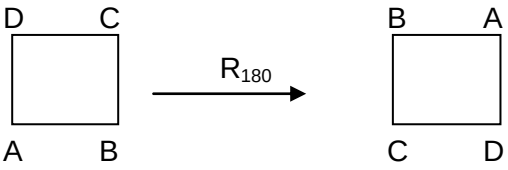
   Alternatively $D_2 = \{R_0, Riso, h, v\}$. Explained below:

2. Rotations $\left(\frac{360i}{n} = \frac{360i}{2} = 180\,i; i = 0,1\right)$

   (1)

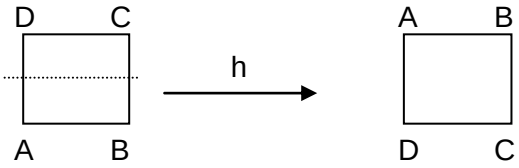


(2)

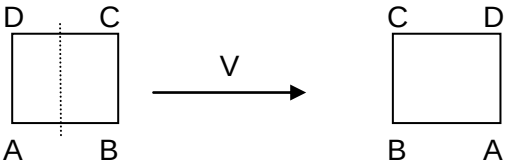


(2) Reflections

(3)

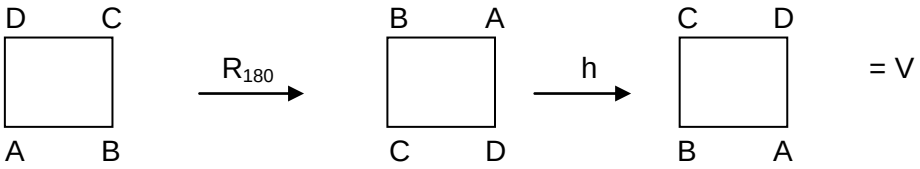


(4)

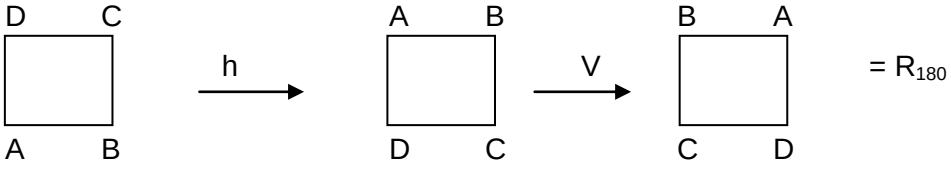


Production of terms :

- h.R180 ⇒



- V h ⇒



Thus, Composition table is given by

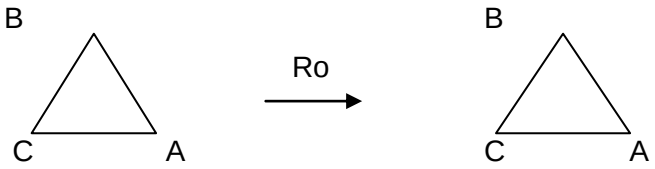
*	R_0	R_{180}	h	v
R_0	R_0	R_{180}	h	v
R_{180}	R_{180}	R0	v	h
h	h	v	R_0	R_{180}
v	v	h	R_{180}	R_0

Example 3:

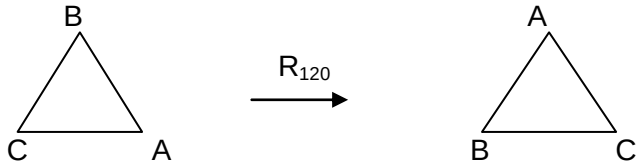
Construction of D_3: (3 rotation + 3 reflection) = $\left\{r^i s^j; r^2 = 1, r^3 = 1, srs^{-1} = r^{-1}, i = 1,2,3;\ j = 1,2\right\}$

= B {e, r, r^2, s, r s, r^2 x}

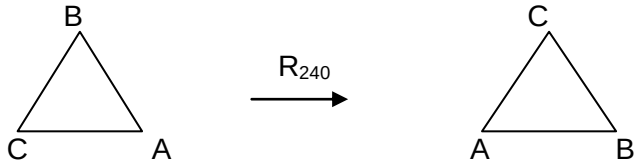
(1)



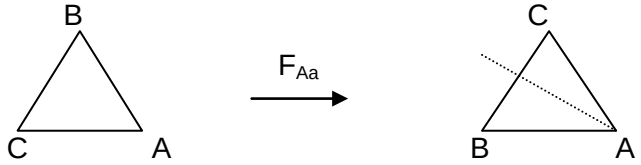
(2)



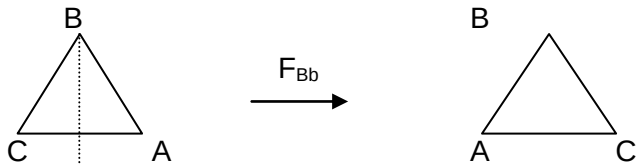
(3)



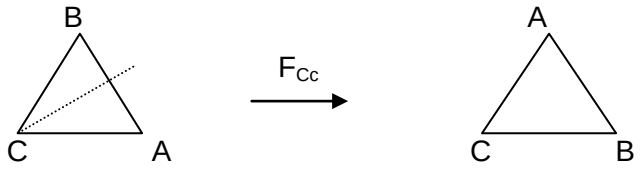
(4)



(5)



(6)



Alternatively thus, $D_3 = \{R_0, R_{120}, R_{240}, F_{Aa}, F_{Bb}, F_{Cc}\}$

Now, composition table is given by

0	R_0	R_{120}	R_{240}	F_{Aa}	F_{Bb}	F_{Cc}
R_0	R_0	R_{120}	R_{240}	F_{Aa}	F_{Bb}	F_{Cc}
R_{120}	R_{120}	R_{240}	R_0	F_{Cc}	F_{Aa}	F_{Bb}
R_{240}	R_{240}	R_0	R_{120}	F_{Bb}	F_{Cc}	F_{Aa}
F_{Aa}	F_{Aa}	F_{Cc}	F_{Bb}	R_0	R_{240}	R_{120}
F_{Bb}	F_{Bb}	F_{Aa}	F_{Cc}	R_{120}	R_0	R_{240}
F_{Cc}	F_{Cc}	F_{Bb}	F_{Aa}	R_{240}	R_{120}	R_0

It can be calculated as:

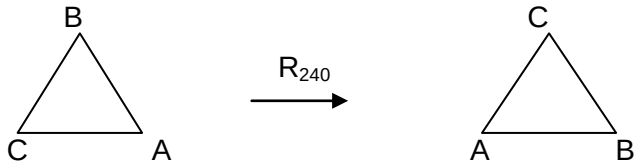
$F_{Aa}\ R_{140}$ $\Rightarrow$ (1) 1st apply R_{240}

(2) Then apply F_{Aa}

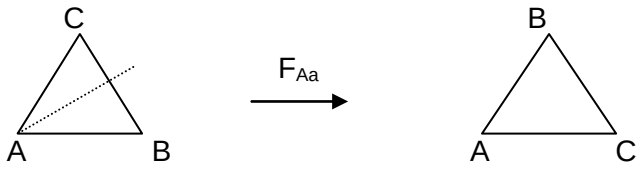
Ultimatimaely

SimilarlyF_{Bb}. F_{Aa} $\Rightarrow$

(1) 1st apply R_{240}

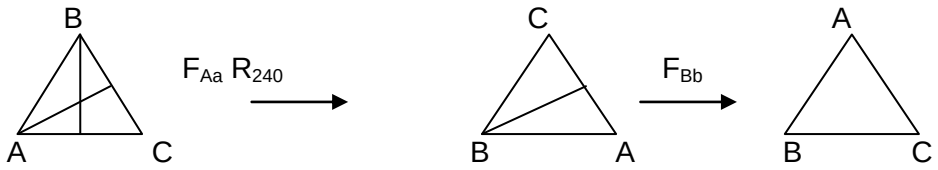


(2) Then apply F_{AQ}



Ultimalimatety

SimilarlyFBb. FAa⇒



Example 4:

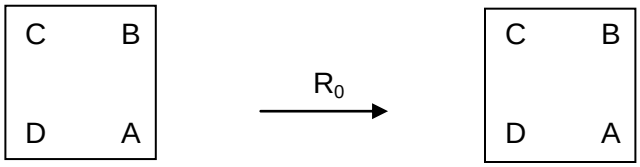
$D_4 : \{r^i s^j \mid r^4 = 1, s^2 = 1, srs = r^{-1}, i = 1,2,3;\ j = 1,2\}$ = $\{e, r, r^2, r^3, s, r, s, r^2 s, r^3 s\}$

$|D_4|$ = 8 i.e. 4 rotations + 4 reflections

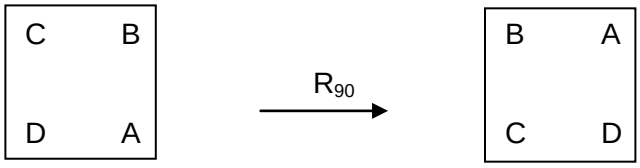
Construction of D_4 :

4. Rotations $\left\{ i.e. \frac{360\,i}{4} = 90i; i = 0,1,2,3 \right\}$

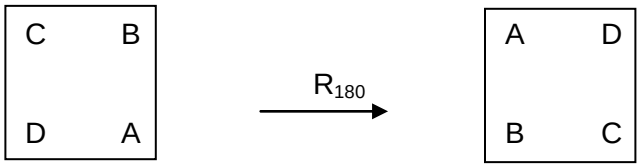
(1)



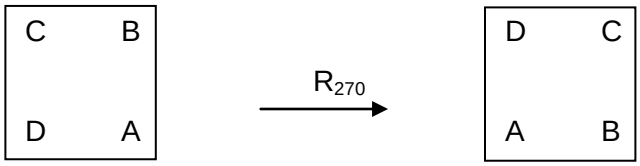
(2)



(3)

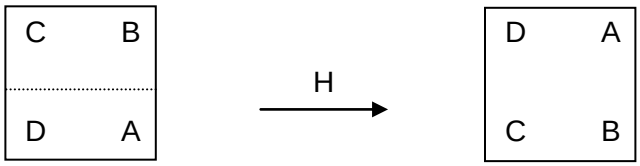


(4)

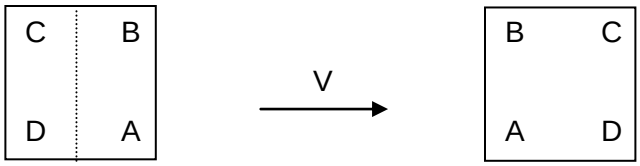


4 Reflections

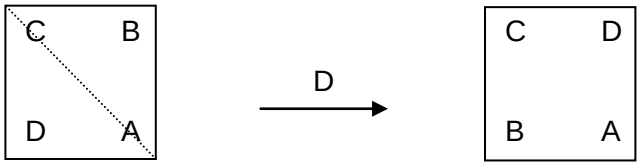
(5)



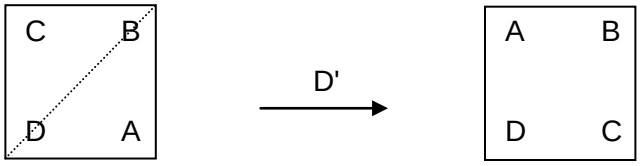
(6)



(7)



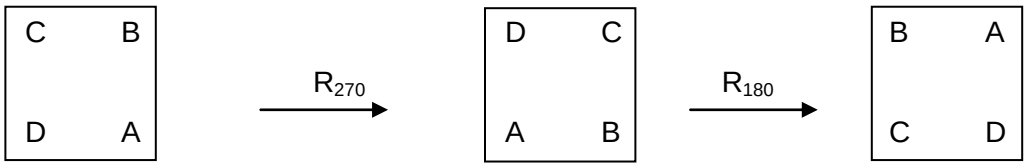
(8)



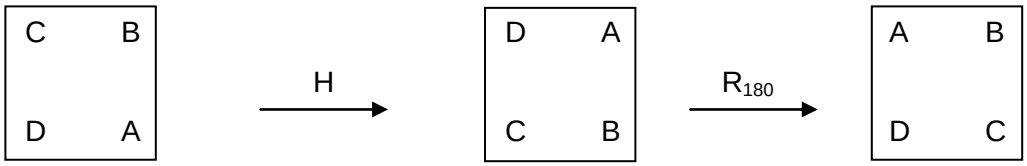
Therefore $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D^1\}$

Product of Elements:

Here, R_{180}. R_{270}



Rao . H



H. R_{90} = D Similarly, we can find product of other elements.

Composition Table:

0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D^1
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D^1
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D^1	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D^1	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D^1	V	H
H	H	D	V	D^1	R_0	R_{180}	R_{90}	R_{270}
V	V	D^1	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D^1	H	R_{90}	R_{270}	R_0	R_{180}
D^1	D^1	H	D	V	R_{270}	R_{90}	R_{180}	R_0

Example 5:

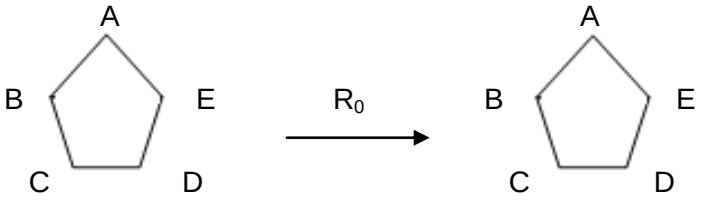
(5) $D_5 = \left\{ r^i s^j \mid r^5 = 1, s^2 = 1, srs = r^{-1}, i = 1,2,3,4; j = 1,2 \right\} = \left\{ e, r, r^2, r^3, r^4 s, r, s, r^2 s, r^3 s, r^4 s \right\}$

$|D_5| = 10$ i.e. 5 rotations + 5 reflections

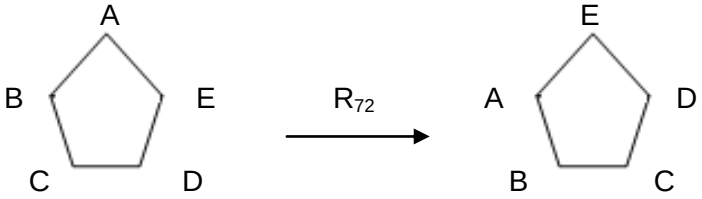
Construction of D_5 :

5 Rotations $\left\{ i.e. \frac{360\,i}{n} = \frac{360\,i}{5} = 72i; i = 0,1,2,3,4 \right\}$

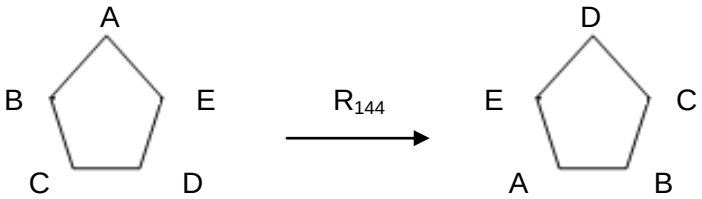
(1)


A
B
E
C
D
R_0
A
B
E
C
D

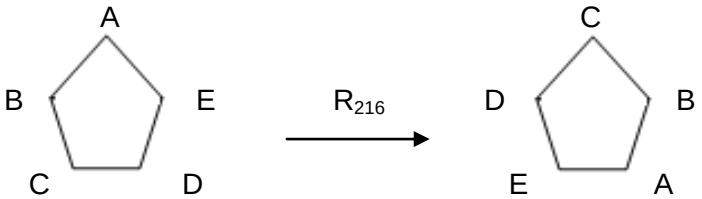
(2)


A
B
E
C
D
R_{72}
E
A
D
B
C

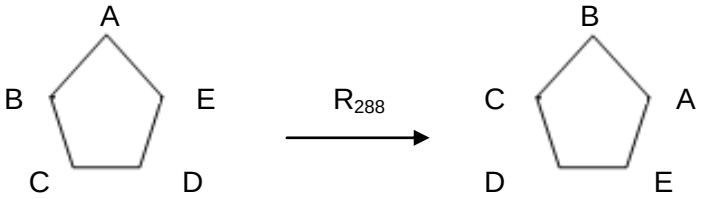
(3)


A
B
E
C
D
R_{144}
D
E
C
A
B

(4)

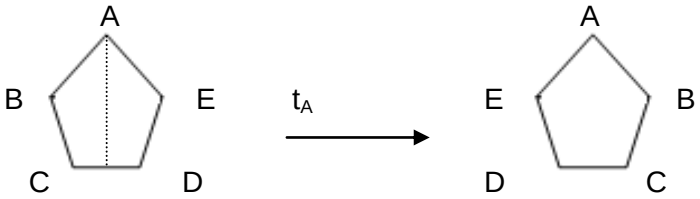

A
B
E
C
D
R_{216}
C
D
B
E
A

(5)

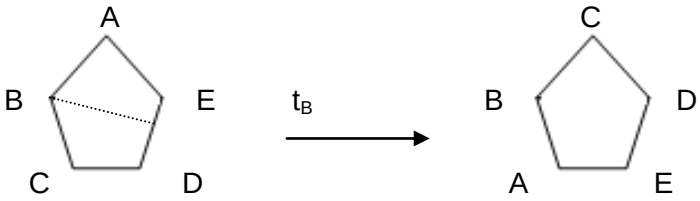

A
B
E
C
D
R_{288}
B
C
A
D
E

5 Reflections

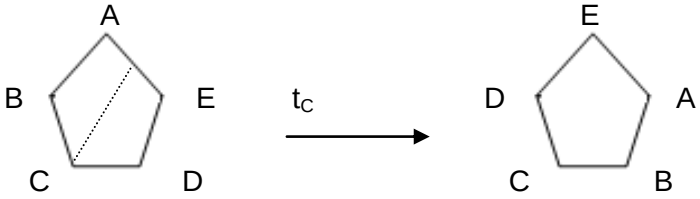
(6)



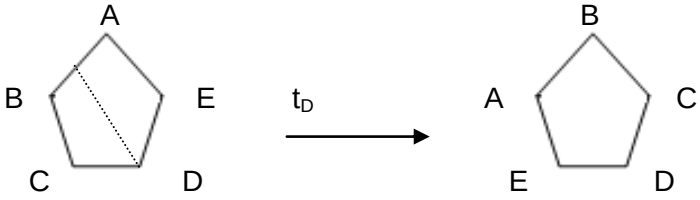
(7)



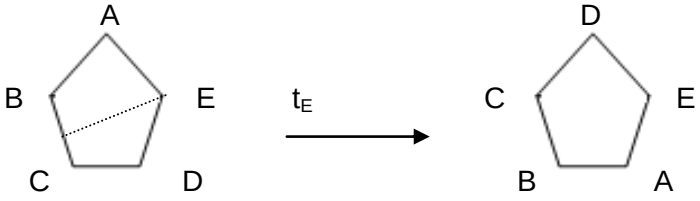
(8)



(9)



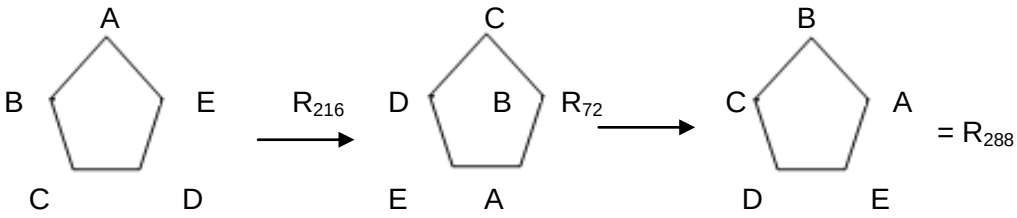
(10)



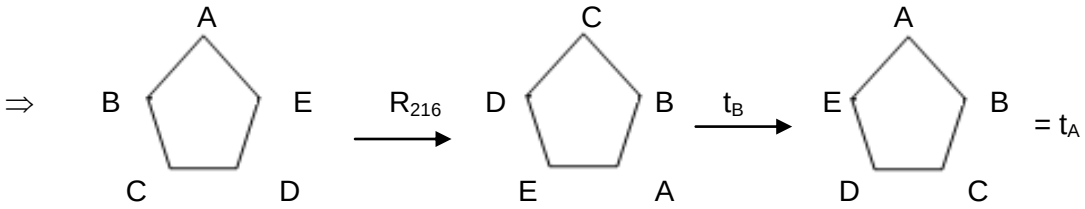
$\therefore$ $D_5 = \{R_0, R_{72}, R_{144}, R_{216}, R_{288}, t_A, t_B, t_c, t_D, t_E\}$

Product of elements:

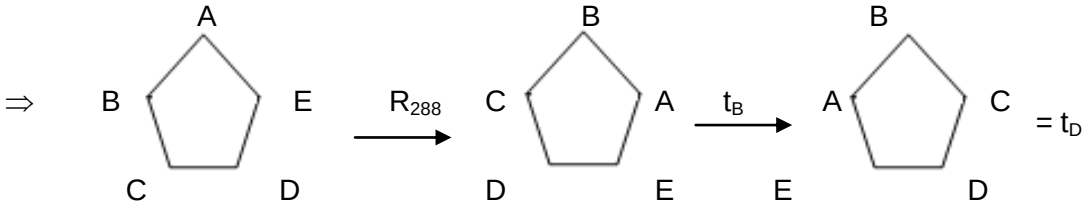
Here R_{27}. R_{216}

- 

- t_B . R_{216}



- t_B . R_{288}



Similarly,We can find product of other dements

Composition Table:

0	R_0	R_{72}	R_{144}	R_{216}	R_{288}	t_A	t_B	t_C	t_D	t_E
R_0	R_0	R_{72}	R_{144}	R_{216}	R_{288}	t_A	t_B	t_C	t_D	t_E
R_{72}	R_{72}	R_{144}	R_{216}	R_{288}	R_0	t_D	t_E	t_A	t_C	t_B
R_{144}	R_{144}	R_{216}	R_{288}	R_0	R_{72}	t_B	t_C	t_D	t_E	t_A
R_{216}	R_{216}	R_{288}	R_0	R_{72}	R_{144}	t_E	t_A	t_B	t_C	t_D

R_{288}	R_{288}	R_0	R_{72}	R_{144}	R_{216}	t_C	t_D	t_E	t_A	t_B
t_A	t_A	t_D	t_B	t_E	t_C	R_0	R_{144}	R_{188}	R_{72}	R_{216}
t_B	t_B	t_E	t_C	t_A	t_D	R_{216}	R_0	R_{144}	R_{288}	R_{72}
t_C	t_C	t_A	t_D	t_B	t_E	R_{72}	R_{216}	R_0	R_{144}	R_{288}
t_D	T_D	t_B	t_E	t_C	t_A	R_{288}	R_{72}	R_{216}	R_0	R_{144}
t_E	t_E	t_C	t_A	t_D	t_B	R_{144}	R_{288}	R_{72}	R_{216}	R_0

Similarly, we can form composition table for D_6, D_7, D_8 ..... by using group operation of composition of symmetries.

Self Check Exercise - 2

Q.1 Write the composition table for D_6

Q.2 Write the composition table for D_7

4.5 Summary:

In this unit, we studied that

1. Symmetric group of n elements Sn is a group with n! elements.
2. The set of all even permutation of Sn is called alternating group. An.
3. Dihedral group is a group of order 2n, of n rotation and n refection.
4. Dihedral group is defined as

   $D_n = \left\{ r^i s^j \mid r^n = e, s^2 = e, srs^{-1} = r^{-1}, i = 0,1,2.....n-1\ j = 1,2 \right\}$

5. D_1 and D_2 are only abelian dihedral group

4.6 Glossary:

- **Permutation Group:** A permutation group G on a set X is a subgroup of the symmetric group S_x, which is the group of all bijective mapping from X to itself under function composition.
- **Dihedral Group:** The dihedral group D_n is the group of symmetries of a regular n-gon. It consists of all rotations and reflections that preserve the geometric structure of n-gon.
- **Permutation:** A permutation of a set X is a rearrangement of its element. If X has n elements, there are n! permutations of X.

4.7 Answers to Self Check Exercise

Self Check Exercise - 1

Q.1 $S_4 = [i, (1,2), (13), (14), (2,3), (2,4), (3,4), (1,2,3)(1,3,2)(1,2,4), (1,4,2),$

$(1,3,4), (1,4,3), (2,3,4), (2,4,3), (12)(34)]$ (14, 23), (13) (24), (1, 2, 3 4),

Q.2 f g $= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ g f $= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$

Q.3 (1, 6, 2, 3, 5, 4)

Q.4 $(2, \quad 4, \quad 3)$

Q.5 $(1 \quad 3)$ in S_5

then $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$

$f^{-1} = \begin{pmatrix} 3 & 2 & 1 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} = f$

So f^{-1} is a cycle also

Q.6 f = (1, 2) $= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$

$f^{-1} = \begin{pmatrix} 2 & 1 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ = (1, 2)

$f = (2 \quad 4 \quad 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$

$f^{-1} = \begin{pmatrix} 1 & 4 & 3 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (2 \quad 5 \quad 4)$

Q.7

0	I	(12)	(13)	(23)	(123)	(132)
I	I	(12)	(13)	(23)	(123)	132
(12)	(12)	I	(32)	(123)	(23)	(13)

(3)	(13)	(123)	I	(132)	(12)	(23)
(23)	(23)	(132)	(123)	I	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(123)	I
(132)	(132)	(23)	(12)	(13)	I	(123)

Q.8 I, (12) (34), (13) (24), (14) (23), (123) (132) (124) (142) (134) (143) (234) (243)

Self Check Exercise - 2

Q.1 Do same as D_5

Q.2 Do same as D_5

4.8 References/Suggested Readings:-

1. Vijak. K. Khanna and S.K. Bhambri, A course in Abstract Algebra.
2. Joseph A Gallian, Contemporary Abstract Algebra.
3. Frank Ayrer Jr. Modern Algebra, Schaum's Outline Series.
4. A.R. Vasistha, Modern Algebra, Modern Algebra, kushan Prakashan Media.

4.9 Terminal Questions

Q.1 Write the alternating group of A_3 of S_3

Q.2 Write the dihedral group D_8.

*****

Unit - 5

Cyclic Group

Structure

5.1 Introduction

Dear student, in this unit you will studied about the order of an element of a group, idempotent element and about cyclic group. You will study how we can prove that a given group is cyclic by using various examples, along with their properties.

5.2 Learning Objectives:

After studying this unit, student will be able to

1. Define and find the order of an element of a group
2. Prove the theorem based on order of an element.
3. Define and prove, that a given group is cyclic
4. Find the generators of a cyclic group.

5.3 Order of an Element

Definition:

Let a be an element of a group G. If there exists a positive integer n such that $a^n = e$, (using the binary operation), then a is said to have finite order, and the smallest such positive integer 'n' with this property is known as the order of a and is denoted by O(a).

- Here a^n does not mean only n times multiple of a, but it means we apply the given binary operation n times on element 'a'.
- In case of additive notation, above definition becomes, if n a = e then o(a) = n. We apply n times the additive operation.
- If there does not exist a positive integer n such that $a^n = e$, then a is said to have infinite order or the order does not exist or the order of a is zero.
- In a group, order of identity element is always 1, i.e. 0(e) = 1 Let us try to clear the concept of order of an element of a group by examples:

Example 1: Find the order of each element of group G {i, w, w^2} cube root of unity under multiplication.

Solution: Since in this given group G (1, w, w^2}, 1 act as identity element under multiplication. Now we have to find a positive integer n such that $a^n = 1$, for all the elements of G. Also we know $w^3 = 1$.

Since, is identity element of G so 0(1) = 1

Now for w, Since$w \times w \times w = w^3 = 1$, so order of w is 3, i.e. 0(w) = 3

3, i.e. 0(w) = 3. [By definition]

Now taking the element w^2,

Since $w^2 \times w^2 \times w^2 = w^6 = (w^3)^2 = (w^2)^3 = 1$

So $0(w^2) = 3$.

Example 2: find the order of each element of the group of order four of G = {1, i, -1, -i} under multiplication.

Solution: To find the order of each element of G we have to find a positive integer k such $(element)^k$ = identity since 1 is identity element of this group.

0(1) = 1

Now, 0(i), Since $i \times i \times i \times i = i4 = (i2)^2 = (-1)2 = 1 =$ identity

i4 = 1

$\therefore$ 0(i) = 4

Now 0(-1), Since $-1 \times -1 = 1$ = identity

$(-1)^2 = 1$

$\therefore$ 0(-1) = 2

Now, 0(-i), since $-i \times -i \times i \times -i = (-i)4 = 1$ = identity

0 (-i) = 4

Example 3: Find the order of each element of the group {0, 1, 2, 3, 4} under addition modulo 5.

Solution: Given group is G = {0, 1, 2, 3, 4} and the binary operation is addition modulo 5 i.e.

$a +^5 b$ = Least non negative remainder when a+b is divided by 5.

Since 0 is identity element of the given group.

So 0(0) = 1

Now, 0(1), Since $1+_5 1+_5 1+_5 1+_5 1 = 0$ [we apply the operation addition modulo 5, five time on 1 so that the remainder is zero that is identity element of group.

$\therefore$ 0(1) = 5

Now, 0(2), Since $2+_5 2 = 4$, $2+_5 2+_5 2 = 1$, $2+_5 2+_5 2+_5 2+_5 2 = 0$ (Remainder is zero when 10 is divided by 5), we apply the operation 5 times on element 2 to get the identity element.

$\therefore$ 0(2) = 5

Now, 0(3), Since $3+_5 3 = 1$, $3+_5 3+_5 3 = 4$, $3+_5 3+_5 3+_5 3 = 2$

$3+_5 3+_5 3+_5 3+3 = 0$, we apply the operation addition modulo 5 five times on element to get 0 (identity element)

$\therefore$ 0(3) = 5

Now, 0(4), Since $4+_5 4,_5 4 = 2$, $4+_5 4+_5 4+_5 4 = 1$,

$4+_5 4+_5 4+_5 4+4 = 0$

$\therefore$ 0(4) = 5

Example 4: Find the order of each element of the group {1, 2, 3, 4, 5, 6} under multiplication modulo 7.

Solution: Since we know that 1 is identity element of the group under multiplication modulo 7. i.e.

$a\times_7 b$ = least non negative integer when ab is divided by 7.

As 1 is identity element, so 0(1) = 1

Now 0(2), Since $2\times_7 2 = 4$, $2\times_7 2\times_7 = 1$, which is identity element when 8 is divided by 7,

$\therefore$ 0(2) = 3

Now 0(3), Since $3+_7 3 = 2$, $3+_7 3+_7 3 = 6$, $3+_7 3+_7 3+_7 3 = 4$

$3+_7 3+_7 3+_7 3+_7 3 = 5$, $3+_7 3+_7 3+_7 3+_7 3+_7 3 = 1$, (which is identity

element when 729 is divided by 7)

$\therefore$ 0(3) = 6

Now, 0(4), $4+_7 4 = 2$, $4+_7 4+_7 4 = 1$, which is identity element

when 63 is divided by 7

Similarly 0(5) = 6 and 0(6) = 2.

Example 5: Consider the group Z_{10} with addition modulo 10. what is the order of the elements.

Solution: Let since Z10 = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}

Here a is identity $0(0) = 1$ $\because 0(e) = 1$

Now taking each element

0 $0(e) = 1 \Rightarrow 0(0) = 1$

1 $110 \equiv 0 \pmod{10}$ as $1+_{10}1+_{10}1+_{10}1+_{10}1+_{10}1+_{10}1+_{10}1+_{10}1+_{10}1 \equiv 0 \pmod{10}$

2 $2 \equiv 2 \pmod{10}$ $\because 0(2) = 5$

$2+2 = 4 \equiv 4 \pmod{10}$

$2+2+2 = 6 \equiv 6 \pmod{10}$

$2+2+2+2 = 8 \equiv 8 \pmod{10}$

$2+2+2+2+2 = 10 \equiv 0 \pmod{10}$

3 $3 \equiv 3 \pmod{10}$

$3+3 = 6 \equiv 6 \pmod{10}$

$3+3+3 = 9 \equiv 9 \pmod{10}$

$3+3+3+3 = 12 \equiv 2 \pmod{10}$

$3+3+3+3+3 = 15 \equiv 5 \pmod{10}$

$3+3+3+3+3+3 = 18 \equiv 8 \pmod{10}$

$3+3+3+3+3+3+3 = 21 \equiv 1 \pmod{10}$

$3+3+3+3+3+3+3+3 = 24 \equiv 4 \pmod{10}$

$3+3+3+3+3+3+3+3+3 = 27 \equiv 3 \pmod{10}$

$3+3+3+3+3+3+3+3+3+3 = 30 \equiv 0 \pmod{10}$

$\therefore 0(3) = 10$

4 $4 \equiv 4 \pmod{10}$

$4+4 = 8 \equiv 8 \pmod{10}$

$4+4+4 = 12 \equiv 2 \pmod{10}$

$4+4+4+4 = 16 \equiv 6 \pmod{10}$

$4+4+4+4+4 = 20 \equiv 0 \pmod{10}$

$0(4) = 5$

5 $5 \equiv 5 \pmod{10}$

$5+5 = 10 \equiv 0 \pmod{10}$

$0(5) = 2$

6 $6 \equiv 6 \pmod{10}$

$6+6 = 12 \equiv 2 \pmod{10}$

$6+6+6 = 18 \equiv 8 \pmod{10}$

$6+6+6+6 = 24 \equiv 4 \pmod{10}$

$6+6+6+6+6 = 30 \equiv 0 \pmod{10}$

$0(6) = 5$

Theorems Based On Order of Element

Theorem 1: In a finite group the order of every element exists.

Proof. Let G be a finite group of order n.

Let $a \in G$ be any element.

$\therefore$ By closure property in G, the collection $\{a, a^2, a^3, ...\}$ of powers of a are element of G.

But G is finite.

$\therefore$ the elements in the above collection cannot be all different.

Let $a^i = aj$, i, j are +ve integers; $i \neq j$, i> j (say) i.e. i - j is a positive integer.

Now $a^j \in G$ and G is a group. $\therefore$ $a^{-j} \in G$

$\Rightarrow$ $a^i a^{-j} = a^j . a^{-j}$ $\Rightarrow$ $a^{i-j} = a^0 = e$

$\Rightarrow$ a^{+ve} integer = e

By well ordering principle, let m be the smallest +ve integer, then

$a^m = e$

$\Rightarrow$ Order of a exists and O(a) = m.

But a is any element of G.

Thus the order of every element exists.

Theorem 2. If G is a finite group of order n then show that for any $a \in G$, $\exists$ some positive integer r, $1 \leq r \leq n$, such that $a^r = e$.

Proof: G is finite group of order n i.e. O(G) = n

Let $a \in G$ be any element.

By closure property $a^2, a^3, ...$ all belong to G.

Consider n+1 elements e, a, a^2 ....., a^n

[All these elements are in G]

But G contains only n elements.

$\Rightarrow$ at least two of these elements are equal

If any of a, a^2, ..., a^n equal e

then $a^r = e$ for $1 \leq r \leq n$ and r is +ve integer.

So our result is proved.

If each of a, a^2, ..., a^n is not equal to e,

then $a_i = a_j$ for some i, j, $1 \leq i \leq n$, $1 \leq j \leq n$.

Without any loss of generality, take i> j

then $a^i = a^j$

$\Rightarrow$ $a^i, a^{-j} = a^i a^{-j}$

$\Rightarrow$ $a^{i-j} = e$, $1 \leq i - j \leq n$

Put $i - j = r$

$\Rightarrow$ $a^r = e$ for $1 \leq r \leq n$ and r is +ve integer.

Theorem 3: Let G be a group and $a \in G$ be of order m. Prove that

(i) $a^0 = e, a, a2, ..., am-1$ are all different.

(ii) $\forall\ n \in I$, an is equal to some one from the above list.

Proof: Given O(a) = m where $a \in G$, a group.

$\Rightarrow$ am = e and m is the smallest positive integer.

Let if possible $a^i = a^j$, $0 < i, j < m$; $i \neq j$ and say $i > j$

Operating by a^{-j} ($\because a^j \in G$ and G is a group $\therefore a^{-j} \in G$)

$\Rightarrow$ $a^i, a^{-j} = a^j. a^{-j}$

$\Rightarrow$ $a^{i-j} = a^0 = e$, where $0 < i - j < m$.

which is a contradiction as m is the smallest integer such that $a^m = e$.

$\therefore$ Our supposition is wrong.

Hence all the elements $e, a, a^2, ..., a^{m-1}$ are different.

(ii) $\forall\ n \in I$, let $n = m q + r$ where $0 \leq r < m$

Consider $a^n = a^{mq+r} = a^{mq}. a^r$

$= (a^m)^q. a^r = e^q. a^r$ ($\because$ $O(a) = m \Rightarrow a^m = e$)

$= e.a^r = a^r$, $0 \leq r < m$

Hence $\forall\ n \in 1$, $a^n = a^r$, $0 < r < m$; which is some one from the above list.

Theorem 4: Let G be a finite group and let $a \in G$ be an element of order n. Then $a^m = e$ iff n is a divisor of m.

Proof: Firstly, let n be a divisor of m i.e. n|m, where O(a) = n.

$\therefore$ there exists a positive integer q such that

m = nq

Now $a^m = a^{nq} = (a^n)^q = e^q = e$. $\begin{bmatrix} \because & O(a) = n. \\ \therefore & an = e \end{bmatrix}$

Conversely let am = e, where O(a) = n.

By division algorithm theorem

$m = n\,q + r$, where $q, r \in 1$ and $0 \leq r < n$

$\therefore$ $e = a^m = a^{nq+r} = a^{nq} .a^r = (a^n)^q .a^r = e^q .a^r = a^r$

$\Rightarrow$ $a^r = e$, where $0 \leq r < n$

which is not possible, because $O(a) = n$ and n is the least positive integer such that $a^n = e$.

$\therefore$ Above result holds only if $r = 0$.

i.e. when $m = nq + 0 = nq$

i.e. when n is a divisor of m.

Theorem 5: Let G be a group and let $a \in G$ be order m. Then

$O(a^k) = \frac{m}{(m,k)}$, where k = 1, 2, ... m-1

Proof: Let $O(a^k) = t$. To show that $t = \frac{m}{(m,k)}$.

Now $a^{kt} = (a^k)^t - e$, but $O(a) = m$.

$\therefore$ m/kt [By Theorem 1.3.3]

$\Rightarrow$ d/m and d/k

Let $m = m_1 d$ and $k = 1d$, where $(m_1, k_1) = 1$

$\Rightarrow$ $\frac{m}{d} = m_1$, so we need to show $t = m_1$.

Now m/kt $\Rightarrow$ $m_1 d/k_1 dt$ $\Rightarrow$ $m_1/k_1 t$

but $(m_1, k_1) = 1$ $\Rightarrow$ m_1/t

Again $(a^k)^{m}_1 = a^{km}_1 = a^{k}_1{}^{dm}_1$

$= a^{k}_1{}^{m}$

$= (a^m)^{k}_1 = e^{k}_1 = e$

But $O(a^k) = t$

$\therefore$ t/m_1

So, from (1) and (2), we get

$t = m_1$

i.e. $O(a^k) = \frac{m}{d} = \frac{m}{(m,k)}$

Cor.1. If $O(a) = m$, then $O(a^k) = m$ iff $(m, k) = 1$

By above theorem,

$O(a^k) = \frac{m}{(m,k)}$

$\therefore$ $O(a^k) = m$ iff $\frac{m}{(m,k)} = 1$ i.e. iff (m, k) = 1

2. If O(a) = p, where p is a prime number, then

$O(a^k) = p$, for all k = 1, 2, ..., p - 1. ($\because$ (p, k) = 1)

Theorem 6: Let a, b and x be any elements of a group G. Then prove that

(i) $O(a^{-1}) = O(a)$

(ii) $(x^{-1}ax)^k = x^{-1}a^k x$, for all $k \in 1$

(iii) $O(a) = O(x^{-1} ax)$

(iv) $O(ab) = O(ba)$

Proof. (i) Let $O(a) = m$ and $O(a^{-1}) = n$

$\Rightarrow$ m, n are the least +ve integers such that

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

Now $(a^{-1})^m = a^{-m} = (a^m)^{-1} = e^{-1} = e$, but $O(a^{-1}) = n$

$\therefore$ n/m .....(1)

Again, $a^n = (a^{-n})^{-n} = [a^{-1})^n]^{-1} = e^{-1} = e$, but O(a) = m

$\therefore$ m/n .....(2)

From (1) and (2), we get

m = n

$\therefore$ $O(a^{-1}) = O(a)$.

(ii) We shall prove by induction that

$(x^{-1}ax)^k = x^{-1}a^k x$, for all $k \in I$

when k = 1, L.H.S. = $(x^{-1} ax)^1 = x^{-1} a^1 x$ = R.H.S.

$\therefore$ the result is true for n = 1.

Let the result holds for k = m, where m is a positive integer.

$\therefore$ $(x^{-1}ax)^m = x^{-1} a^m x$ is true.

Now $(x^{-1}ax)^{m+1} = (x^{-1} ax)^m (x^{-1} ax)$

$= x^{-1} a^m (x^{x-1}) ax$

$= x^{-1} a^m eax$

$= x^{-1} a^{m+1} x.$

$\therefore$ The result is true for k = m+1 also.

Hence the result is true for all positive integers.

Also when k = 0, then

L.H.S. $= (x^{-1} ax)^0 = e = x^{-1} ex$

$= x^{-1} a^0 x$ = R.H.S.

Now, let k = -m, where m is a positive integer.

$\therefore \quad (x^{-1}ax)^k = (x^{-1} ax)^{-m} = \{(x^{-1} ax)^m\}^{-1}$

$= \{x^{-1} a^m x)^{-1}$

$= x^{-1} a^{-m} (x^{-1})^{-1}$

[By Reversal law $(ab)^{-1} = b^{-1} a^{-1}$]

$= x^{-1}a^k x.$ $[\because (x^{-1})^{-1} = x]$

$\therefore$ The result is true for zero and negative integers also. Hence the result is proved for all integers.

(iii) Let $O(x^{-1} ax) = m$ and $O(a) = n$

Now $(x^{-1}ax)^n = x^{-1}$ an $x = x^{-1} ex = x^{-1} x = e$

But $O(x^{-1} ax) = m$

$\therefore$ m/n .....(1)

Again $\because \quad O(x^{-1} ax) = m$

$\Rightarrow \quad O(x^{-1} ax)^m = e$

$\Rightarrow \quad x^{-1} a^m x = e\, x^{-1} x$

$\Rightarrow \quad x^{-1} a^m x = x^{-1} e x$

$\Rightarrow \quad a^m = e$ [Using left and right cancellation laws]

But $O(a) = n$

$\therefore$ n/m ....(2)

From (1) and (2), we get

n = n.

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

(iv) From (iii) we have

$O(a) = O(x^{-1} a x), \forall\ a, x \in G$

Replacing a by a b and x by a, we get

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

= O(e b a) = O(b a)

Aliter: Since ab = eab = $(b^{-1} b)$ ab = b^{-1} (ba)b

$\therefore$ O(ab) = $O(b^{-1}$ (ba)b)

$\Rightarrow$ O(ab) = O(ba). [Using (iii)]

Remark: If a, b $\in$ G be elements of finite order or a group G, then O(ab) may not be finite and if it is finite even then it need not be equal to O(a) O(b)

To prove above thing, let us take the following examples.

Example 6: Let G = { f ; f : R $\to$R is one-one and onto function} be a group under the operation of composition of functions.

Let f_1, $f_2 \in$ G be two elements such that f_1(x) = -x and f_2 (x) = 1-x.

Then O(f_1) = 2 = O(f_2), but (f_1 f_2) does not exist.

Solution: For f_1^2(x) = f_1(f_1(x)) = f_1(-x) = (-x) = x $\Rightarrow$ O(f_1) = 2

and f_2^2 (x) = f_2 (f_2 (x)) = f_2 (1-x) = 1 - (1-x) = x

$\Rightarrow$ O(f_2) = 2

But f_1 f_2 (x) = f_1 f_2 (x)) = f_1(1-x) = - (1-x) = -1 + x

Also, (f_1 f_2)^n (x) $\neq$ x, $\forall$ n $\in$N.

$\therefore$ O(f_1 f_2) does not exist.

Example 7: Let G = $\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in R \, such \, that \, ad - bc \neq 0\right\}$

i.e. G is a group of all non-singular 2 $\times$ 2 matrices under the operation of multiplication of matrices.

Let A = $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and B = $\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ be two elements of G.

Prove that O(A) = O(B) = 2 but O(AB) does not exist.

Solution: Here $A^2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $\Rightarrow$ (A) = 2

$B^2 = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $\Rightarrow$ O(B) = 2

and $AB = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$

.....

.....

$(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}, \forall\ n \in N$

$\therefore$ O (AB) does not exist.

Theorem 8: If a, b be any two elements of a group G such that ab = ba and (O(a), O(b)) = 1. Then prove that

O(a b) = O(a) O(b).

Proof: Let O(a) = m and O(b) = n, where (m, n) = 1

Let O(ab) = k. To show that k = m n, where ab = ba.

Now $e = (ab)^{nk} = a^{nk}b^{nk} = a^{nk}.(b^n)^k$

$= a^{nk}.e^k = a^{nk}\,e = a^{nk}$

i.e. $a^{nk} = e$, but O(a) = m

$\Rightarrow$ m/n k, but (m, n) = 1

$\therefore$ m/k. .....(1)

Similarly, $e = (ab)^{mk} = a^{mk}b^{mk} = (a^m)^k b^{mr}$

$= e^k b^{mr} = eb^{mk} = b^{mk}$

i.e. $b^{mk} = e$, but O(b) = n

$\Rightarrow$ n/m k, but (m, n) = 1

$\therefore$ n/k

From (1) and (2), we get ....(2)

m/k and n/k $\Rightarrow$ [m, n] | k

But [m, n].(m, n) = mn ....(3)

$\Rightarrow$ [m, n] . 1 = mn

$\therefore$ From (3), we have

m n / k. ....(4)

Again $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n\,(b^n)^m = e^n e^m = ee = e$

but O (ab) = k

$\therefore$ k/mn

$\therefore$ from (4) and (5), we get .....(5)

$k = m\ n$

i.e. $O(ab) = O(a).O(b)$.

Self Check Exercise - 1

Q.1 Find the order of each element of the group {1, i, $\pm$j $\pm$k} under multiplication.

Q.2 find the order of each element of the group Z_n under addition modulo 7

Q.3 Find the order of each element of the group U_{10}.

Q.4 Show that the group Q-{0} i.e. non zero rational numbers under multiplication has only two element of finite order.

5.4 Idempotent Element:

In 0 group G an element a is called an idempotent element of $a*a = a$, where $*$ is a binary operation.

Let us take following examples:-

Example 1: Show that if G is a group then $a \in G$ is an idempotent if and only if a = e, the identity of a.

Solution: Given G is a group

Let $a \in G$ is idempotent

then by definition of idempotent

$a^2 = a$

$\Rightarrow$ $a.a = a.e$

$\Rightarrow$ $a = e$ (using cancellation law)

Conversely Let $a = e$

$a.a = a.e$

$= e.e. = e = a$

$\Rightarrow$ $a^2 = a$, So a is idempotent element.

Example 5: Continue

7. $7 \equiv 7 \pmod{10}$

$7+7 = 14 \equiv 4 \pmod{10}$

$7+7+7 = 21 \equiv 1 \pmod{10}$

$7+7+7+7 = 28 \equiv 8 \pmod{10}$

$7+7+7+7+7 = 35 \equiv 5 \pmod{10}$

$7+7+7+7+7+7 = 42 \equiv 2 \pmod{10}$

$7+7+7+7+7+7+7 = 49 \equiv 9 \pmod{10}$

$7+7+7+7+7+7+7+7 = 56 \equiv 6 \pmod{10}$

$7+7+7+7+7+7+7+7+7 = 63 \equiv 3 \pmod{10}$

$7+7+7+7+7+7+7+7+7+7 = 70 \equiv 0 \pmod{10}$

$\therefore \quad 0(7) = 10$

8. $8 \equiv 8 \pmod{10}$

$8+8 = 16 \equiv 6 \pmod{10}$

$8+8+8 = 24 \equiv 4 \pmod{10}$

$8+8+8+8 = 36 \equiv 6 \pmod{10}$

$8+8+8+8+8 = 40 \equiv 0 \pmod{10}$

$0(8) = 5$

9. $9 \equiv 9 \pmod{10}$

$9+9 = 18 \equiv 8 \pmod{10}$

$9+9+9 = 27 \equiv 7 \pmod{10}$

$9+9+9+9 = 36 \equiv 6 \pmod{10}$

$9+9+9+9+9 = 45 \equiv 5 \pmod{10}$

$9+9+9+9+9+9 = 54 \equiv 4 \pmod{10}$

$9+9+9+9+9+9+9 = 63 \equiv 3 \pmod{10}$

$9+9+9+9+9+9+9+9 = 72 \equiv 2 \pmod{10}$

$9+9+9+9+9+9+9+9+9 = 81 \equiv 1 \pmod{10}$

$9+9+9+9+9+9+9+9+9+9 = 90 \equiv 0 \pmod{10}$

$\therefore \quad 0(9) = 10$

Example 2: Let G be a group such that $a^2 = e$, for all $a \in G$, Show that G is abelian.

Or

Show that a group in which every element is its own inverse is an abelian group.

Or

If each element of a group, except the identity element, is of order 2, show that the group is abelian.

Solution: Let $a, b \in G$ be any two elements, where $a \neq e$, $b \neq e \Rightarrow a\,b \neq e$.

$\therefore \quad a^2 = e$ and $b^2 = e$ (or $O(a) = 2$, $O(b) = 2$)

$\Rightarrow$ $a^{-1} = a$ and $b^{-1} = b$ (i.e. every element is its own inverse)

Also $a, b \in G \Rightarrow ab \in G$ (By Closure Property)

$\therefore$ $(ab)^2 = e$ (or $O(ab) = 2$)

$\Rightarrow$ $(ab^{-1} = ab$

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

$\therefore$ $b^{-1} a^{-1} = ab$

$\Rightarrow$ $ba = ab$ [$\because$ $b^{-1} = b$ and $a^{-1} = a$]

$\therefore$ G is abelian group.

Example 3: If in a group G, $a^5 = e$ and $ab\,a^{-1} = b^2$ for all $a, b \in G$.

Prove that if $b \neq e$, then $O(b) = 31$

Solution: Now, $b^2 = aba^{-1}$ .....(1)

$\therefore$ $b^4 = (aba^{-1})^2$

$= ab^2\,a^{-1}$ [$\because$ $(x^{-1}ax)^k = x^{-1}a^kx$]

$= a(aba^{-1})a^{-1}$ [Using (1)]

$= a^2\,ba^{-2}$

$\therefore$ $b^8 = (a^2\,ba^{-2})^2$

$= a^2b^2\,a^{-2}$

$= a^2(aba^{-1})\,a^{-2}$ [Using (1)

$= a^3\,ba^{-3}$

$\therefore$ $b^{16} = (a^3\,ba^{-3})^2 = a^3\,b^2\,a^{-3}$

$= a^3(aba^{-1})a^{-3}$ [Using (1)]

$= a^4\,ba^{-4}$

Similarly, $b^{32} = a^2\,ba^{-5}$

$b^{32} = ebe^{-1} = b$ [$\because$ $a^5 = e$]

$\Rightarrow$ $b.b^{31} = be$

$\Rightarrow$ $b^{31} = e.$ [By left cancellation law]

$\therefore$ O(b) must divide 31. But 31 is a prime number.

$\therefore$ O(b) = 31

Example 4 : If G is an abelian group, then $(a\,b)^n = a^n\,b^n$, holds for all $a, b \in G$ and for all $n \in I$.

Solution : Given G is an abelian group.

Let $a, b \in G$. We shall prove the result $(a\,b)^n = a^n\,b^n$ by Mathematical Induction.

If n = 0, then $(a\ b)^0 = e = e\ e = a^0\ b^0$

$\therefore$ the result is true for n = 0

If n = 1, then $(a\ b)^1 = ab = a^1\ b^1$

$\therefore$ the result is true for n = 1

Suppose that the result is true for $n = k \geq 1$.

$\therefore$ $(ab)^k = a^k\ b^k$

Consider $(ab)^{k+1} = (ab)^k\ (ab) = (a^k\ b^k)\ (ab)$

$\Rightarrow$ $= \left(\left(a^k b^k a\right)\right)$ b, by associativety in G

$= \left(a^k \left(b^k a\right)\right)$ b, by associativity in G

$= \left(a^k \left(ab^k\right)\right)$ b, since G is abelian

$= \left(\left(a^k a\right) b^k\right)$ b, by associativity

$= \left(a^{k+1} b^k\right)$ b

$= a^{k+1}\ (b^k b)$ by associativity

$= a^{k+1}\ b^{k+1}$

$\therefore$ the result is true for n = k+1, if it is true for n = k.

But we have already proved the result for n = 1

$\therefore$ the result is true for every positive integer n.

When n is a negative integer

Let n = -m for some positive integer m.

Then $(ab)^n = (ab)^{-m}$

$= \left(\left(ab\right)^m\right)^{-1}$

$= (a^m\ b^m)^{-1}$, since m is a positive integer

$= (b^m\ a^m)^{-1}$, since G is abelian

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

$= a^n\ b^n$

Hence $(ab)^n = a^n\ b^n$, $\forall$ $n \in I$.

Example 5: If (G, +) is a group such that 2 a = 0 for all $a \in G$, then show G is an abelian group.

Solution: Let $a, b \in G$ be any two elements

Then $2a = 0 \Rightarrow a + a = 0 \Rightarrow a = -a$ ....(1)

and $2b = 0 \Rightarrow b + b = 0 \Rightarrow b = -b$ ....(2)

By closure property, $a + b \in G$

$\therefore$ $2(a+b) = 0$

$\Rightarrow$ $(a+b) + (a+b) = 0$

$\Rightarrow$ $a+b = -(a+b = - b - a$

$\Rightarrow$ $a+b = b+a$ [Using (1) and (2)]

Hence G is an abelian group

Self Check Exercise - 2

Q.1 Show that a group of even order has an element of order 2

Q.2 Show that in a group of even order the number of element whose order is 2 are add.

5.5 Cyclic Group

Definition:

A group G is called a cyclic group if there exist on element $a \in G$, such that every element of G can be expressed as a power of a Mathematically

$G = \{a^n, n \in Z\}$, when binary operation is multiplication

and

$G = \{na, n \in Z\}$ when binary operation is addition.

Such element is called generator of G and is written as G = <a>

Some Properties of a cyclic group

1. If G = <a> be a cyclic group of order n, then

   $G = \{e, a, a^2, ...a^{n-1}\}$ i.e. O(G) = O(a) = n.

2. If a is a generation of a cyclic group G then a^{-1} is also a generator of G i.e.

   for ang $x \in G$, we have $x = a^n$ also $x = (a^{-1})^{-n}$ where $n, -n \in Z$.

Example 1: Consider the group $Z_4 = \{0, 1, 2, 3\}$ under addition modulo 4 then 0(0) = 1, 0(1) = 4, 0(2), 0(3) = 4, is a cyclic group. To verify this statement, all we need to do prove that some element of Z_4 is a generator, here 1 is a generator of the group, as every element of $(Z +_4)$ can be expressed as a power of 1.

Remark: Any cyclic group can have more than one generator.

Example 2: $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is cyclic group under addition abvious modulo 8.

Since <1> is a generator of given group. Also

<3> = $\{3, 3+3 (\text{mod } 8), 3+3+3 (\text{mod } 8), 3+3+3+3 (\text{mod } 8),$

$3+3+3+3+3 (\text{mod } 8), 3+3+3+3+3+3 (\text{mod } 8)\}$

= {3, 6, 1, 4, 7, 2, 5, 0} (mod 8}

<3> = {0, 1, 2, 3, 4, 5, 6, 7} = Z_8

So <3> is a generator of Z_8:

Similarly, if we cheek ,<2> =

$\{2, 2+2 (\text{mod } 8), 2+2+2 (\text{mod } 8), 2+2+2+2 (\text{mod } 8)\}$

= {2, 4, 6, 0, 4} $\neq Z_8$, so <2> is not a generator of Z_8.

So Z_8 is a cyclic group

Example 3: $(Z_{12}, +_{12})$ is a cyclic group. Under addition modulo 12.

Again <1> is a obvious generator of the given group.

Here the element 5 is a generator, as

<5> = {1×5 (mod 12), 2×5 (mod 12),3×5 (mod 12), 4×5 (mod 12), (5×5) mod 12, (6×5) mod 12, (7×5) mod 12, (8×5) mod 12, (9×5) mod 12, (10×5) mod 12, (11×5) mod 12, (12×5) mod 12}

= {5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0}

= {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11} = Z_{12}

So $(Z_{12}, +_{12})$ is a cyclic group.

Example 4 : U_{10} = S {1, 3, 7, 9} is a cyclic group. Under multiplication modulo 10.

To prove U_{10} is cyclic, we have to prove one of its element is its generator.

Now, <3> = $\{3^0, 3^1, 3^2, 3^3\}$ mod 10

= {1, 3, 9, 7} = U_{10}. <3> is generator of U_{10}.

So U_{10} is a cyclic group.

Note : an integer K in Zn is a generator of Zn if and only if gcd (n1k) = 1

Example 5 : 1. Group of integers Z, under addition (Z, +) is cyclic, with generators <1>

and <-1>

2. Group of real number under addition is not a cycle group.

3. Group of rational number under addition is not cyclic.

Because, let q $\in$Q then <q> = {nq : n $\in$ z} But this gives us atmost integer multiple of q not every element of Q.

Some Theorems on Cyclic Group

Theorem 1 : A subgroup of a cyclic group is cyclic.

Proof : Let G = <a> and let H $\leq$ G.

If H = (e), then there is nothing to prove.

Let H $\neq$ (e) Members of H will be powers of a. Let m be the least +ve integer such that am $\in$ H.

We claim that $H = \langle a^m \rangle$

Let $x \in H$ be any element. Then

$x = a^k$ for some k.

By division algorithm, $k = mq + r$ where $0 \leq r < m$

$\Rightarrow$ $r = k - mq$

$\Rightarrow$ $a^r = a^k \cdot a^{-mq} = x.(a^m)^{-q} \in H$.

But m is the least +ve integer such that $a^m \in H$.

$\therefore$ $r = 0$

$\therefore$ $m = mq$

$\therefore$ $k = a^k = (a^m)^a$ i.e. any member of H is a power of a^m.

$\therefore$ H is cyclic and H = <am> i.e. H is generated by am.

Theorem 2. A cyclic group is abelian

Proof : Let G = <a>. If x, y $\in$ G be any elements, then $x = a^n$, $y = a^m$ for some integers m, n.

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

$= a^{m+n} = a^m . a^n$

$= y.x$

$\therefore$ $xy = xy \forall x, y \in G$.

$\therefore$ G is abelian.

Note. Clearly all non-abelian groups are non-cyclic.

Example : Give an example of an abelian group which is not cyclic.

Solution : Let (Q, +) be the group of rationals under addition.

This is clearly an abelian group. [$\because$ a + b = b _ a $\forall$a, b $\in$ Q]

Let if possible, the group of cyclic. Let $\frac{m}{n} \in$ Q be a generator of Q. Then any element of Q should be a multiple of $\frac{m}{n}$.

Now $\frac{1}{3n} \in$ Q and if $\frac{m}{n}$ is a generator, then we should be able to write.

$\frac{1}{3n}$ = k. $\frac{m}{n}$ for some k.

$\Rightarrow$ $\frac{1}{3}$ = km, which is not possible. [$\because$ k, m are integers. But $\frac{1}{3}$ is not]

Hence no element can act as generator of Q.

Theorem 3. Order of a cyclic group is equal to order of its generator.

Proof : Let G = <a> i.e. g be a cyclic group generator by a.

Case (i) O(a) is finite say n.

Then n is the least +ve integer such that $a^n = e$

Consider the elements

$a^0 = e, a, a^2, ... a^{n-1}$

These are all elements of G and are n in number.

Suppose any two of the above elements are equal say

$a^i = a^j$ with i> j

Then $a^i.a^{-j} = e \Rightarrow a^{i-j} = e$

But $0 < i - j \leq n - 1 < n$.

Then $\exists$s a +ve integer i - j such that $a^{i-j} = e$ and i - j < n.

Which is a contradiction to the fact that O(q) = n

There no two of the above n elements can be equal i.e. G contains at least n elements. We shall show that it does not contain any other element.

Let x $\in$ G be any element. since G is cyclic generated by a, $\therefore$ x will be some power of a.

$\therefore$ $x = a^m$

By division algorithm, we can write

$m = nq + r$ where $0 \leq r < n$

Now $a^m = a^{nq + r} = (a^n)^q . a^r$

$= e^q.a^r = a^r$

$\therefore$ $x = a^r$ where $0 \leq r < n$

i.e. x is one of $a^0 = e, a, a^2, ...a^{n-1}$

$\therefore$ g contains precisely n elements.

Hence $O(G) = n = O(a)$

Case (iii) O(a) is infinite.

In this case no two powers of a can be equal [$\because$ if $a^n = a^m$ (a > m)]

then $a^{n-m} = e$

i.e. it is possible to find a +ve integer n-m such that $a^{n-m} = e$

$\Rightarrow$ O(a) is finite.

Hence no two power of a can be equal.

Thus G would contain infinite number of elements.

Theorem 4. A group of prime order is cyclic and every element of G other than identity can be taken as its generator.

Proof : Let $O(G) = p$, a prime.

Take any $a \in G, a \neq e$

Let $H = [a^n : n \text{ is an integer}]$

Then H is a cyclic subgroup of G. $\therefore \frac{O(H)}{O(G)} \Rightarrow \frac{O(H)}{p}$

$\Rightarrow$ $O(H) = 1$ or p [$\because$ p is prime]

But $O(H) \neq 1$ [$\because$ $a \in H, a \neq e$]

$\therefore$ $O(H) = p$

$\Rightarrow$ $H = G$.

i.e. G is a cyclic group generated by a.

Since a was taken as any element (other than e) $\therefore$ any element of G can act as its generator.

Cor. A group of prime order is abelian.

Sol. A group of prime order is always cyclic.

Also a cyclic group is always abelian.

Hence a group of prime order is always abelian.

Let us understand above theorems through following examples.

Example 5 : Prove that group of order 3 must be cyclic.

Solution : Using the theorem that a group of prime order is cyclic. Hence a group of order 3 is cyclic.

Example 6 : Prove that the set K_4 = {e, a, b, ab} under the binary operation. On K_4 given by table.

.	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

is abelian but not cyclic. K4 is known as Klein-4-group.

Solution : From the given composition table. We find that it is symmetrical about main diagonal, So it is abelian.

Now, to prove that it is cyclic or not. To prove the given group is cycle we have to generate K_4 by any of its element.

From the table, you can see, <a> = {e, a} $\neq K_4$

Similarly<b> = {e, b} $\neq K_4$, <ab> = {e, ab} $\neq K_4$.

Therefore, K_4 cannot be generated by {e} {a}, {b} {a b}.

Thus K_4 is not cyclic.

Theorem 5 : An infinite cyclic group has precisely two generators.

Proof : Let G = <a> be an infinite cyclic group.

If a is a generator of G, then a^{-1} will also be a generator of G.

[$\because$ If $a^n = e$, then $(a^{-1})^n = (a^n)^{-1} = (e)^{-1} = e$]

Let if possible$b \neq a$, $b \neq a^{-1}$ be any other generator of G.

Since $b \in G$ and a is a generator of g.

$\therefore$ $b = a^n$ for some integer n.

Again $\because$ $a \in G$ and b is a generator of G.

$\therefore$ $a = b^m$ for some integer m.

$\therefore$ $a = b^m = (a^n)^m = a^{nm}$

$\Rightarrow$ $a^{nm-1} = e$

$\Rightarrow$ O(a) is finite and$\leq$ nm - 1

Since O(G) = O(a) is infinite.

$\therefore$ the above result is possible only if nm - 1 = 0

$\Rightarrow$ nm = 1

$\Rightarrow$ $m = \frac{1}{n}$

$\Rightarrow$ n = ± 1 [$\because$ m, n are integers]

i.e. $b = a$ or a^{-1}

Thus a and a^{-1} are precisely the generators of G.

Hence the result

Next we shall find the number of generators for a finite cyclic group.

For this first of all we shall define a function known as Euler's Function.

For any integer n, we define.

$\phi(1) = 1$ and for $n > 1$,

$\phi(n)$ = number of +ve integers less than n.

and relatively prime to n.[e.g. $\phi(6) =$, $\phi(10)$ - 4 etc.]

Following two results will be helpful to fine $\phi(n)$.

(i) If $p_1, p_2, ..., p_n$ are distinct prime factor of n(>1), then

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right).....\left(1-\frac{1}{p_k}\right)$$

(ii) If m, n are co-prime, then $\phi(mn) = \phi(m).\phi(n)$. [m, n $\geq$1]

Theorem 6 : Number of generators of a finite cyclic group of order n is $\phi(n)$.

Proof : Let G = <a> be a cyclic group of order n.

Then O(a) = O(b) = n.

We claim that am is a generator of G.

iff (m, n) = 1 i.e. m, n are relatively prime.

Let now am be a generator of G for some m.

Since $a \in G$

$\therefore$ $a = (a^m)^i$ for some $i = a^{mi}$

$\Rightarrow$ $a^{mi-1} = e$

$\Rightarrow$ $\frac{O(a)}{mi-1}$

$\Rightarrow$ $\frac{n}{mi-1}$

$\Rightarrow$ mi -1 = nj for some integer

$\Rightarrow$ mi - nj = 1

$\Rightarrow$ (m, n)

Conversely.

Let (m, n) = 1

Then $\exists$s integers x and y such that

mx + ny = 1

$\Rightarrow$ $a^{mx + ny} = a$

$\Rightarrow$ $a^{mx} . a^{ny} = a$

$\Rightarrow$ $a^{mx} . (a^n)^y = a$

$\Rightarrow$ $a^{mx} = a$

$\Rightarrow$ $a = (a^m)^n$

Since every elt. of G is a power of a and a itself is a power of a^m.

$\therefore$ am generates G.

Hence the result.

To understand above theorems, Let us take following examples.

Examples of Eluer'sϕ Function

Let n = 20, $4\times4 = 2^2\times5^1$ [Prime factors of n]

$$\phi(n) = 20\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$$

$$= 20\times\frac{1}{2}\times\frac{4}{5}$$

$\phi(n) = 8$

Example 7 : Find the number of generator of (Z8+8) and list than

Solution : Here n = 8

$n = 2\times2\times2 = 2^3$ [Prime factorization]

Now $\phi(8)$ $=8\left(1-\frac{1}{2}\right)$ definition of Euler's ϕ function

$$= 8\times\frac{1}{2}$$

$\phi(8)$ = 4

$\therefore$ There are 4 generators of Z_8

As $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Using the result, "an integer k in Zn is a generator of $Z_n$iffgcd (n, k) = 1"

To find the generators of Z8 we have to find the integer from the set Z_8 which are co prime to 8, and the elements are {1, 3, 5, 7}

Therefore the 4 generators of Z_8 are <1>, <3>, <5>, and <7>.

Note : Let G = <g> be of order n, and let d be positive divisor of n. Then the number of elements of G of order d is $\phi(d)$

Example 8 : How many elements of order 2 and 5 do Z_{50} under addition have? modulo 50.

Find the elements also.

Given $O(Z_{50}) = 50$

Since 2 and 5 are positive divisor of n.

then number of elements of G of order 2 is $\phi(2)$=

$$\phi(2) = 2\left(1-\frac{1}{2}\right)$$

$$\phi(2) = 2\times\frac{1}{2}=1$$

$$= 1$$

Hence in Z50 there is only 1 element of order 2.

And the element of order 2 is 25.

Similarly, the number of elements of G, of order 5 = $\phi(5)$

$$= 5 \times \left(1-\frac{1}{5}\right)$$

$$= 5 \times \frac{4}{5}$$

$$= 4$$

Hence in Z_{50}, there are 4 element having order 5.

and these elements are 10, 20, 30 and 40.

Self Check Exercise - 3

Q. 1 Show that $\{1, w, w^2\}$ terms a cyclic group under multiplication.

Q. 2 Show that {1, -1, -i, -i}, the group of fourth root of unity terms a cyclic

group under multiplication.

Q. 3 Show that a = {0, 1, 2, 3, 4, 5, +6} is a cyclic group.

Q. 4 Is the group (6z, +) is cyclic.

Q. 5 Find all the generators of Z_6, Z_8 and Z_{20} under addition modulo n and list them.

Q. 6 Find the generators of Z_{25} and Z_{256}.

5.6 Summary:

In this unit, we have discussed the following points

1. Order of an element
2. Cyclic group
3. Cyclic Abelian group
4. Abelian group that is not cyclic
5. Number of Generators of a Cyclic group
6. Number of elements in a cyclic group having order, which is a divisor of order of group.

5.7 Glossary:

- **Order of an element :** Let $a \in g$, where G is a group. If there exist least positive integer n s.t. $a^n = e$. The n is the orders of an element.
- **Idempotent element:** Let G be a group with binary operation '$*$'. If $a \in G$ and satisfy $a*a = a$. Then a is idempotent element of G.
- **Finite Cyclic Group:** Let G be a group. If $a \in G$, order of element a is equal to the order of the group. Then g is finite cyclic group.

5.8 Answers to Self Check Exercise

Self Check Exercise - 1

Q.1 O(1) = 1

O(-1) = 2

O(i) = 4

O(-i) = 4

Q. 2 O(0) = 1

O(1) = 7

O(2) = 7

O(3) = 7

O(4) = 7

O(5) = 7

O(6) = 7

Q.3 O(1) = 1

O(3) = 4

O(7) = 4

O(9) = 2

Q.4 Since 1 is the identity element and O(1) = 1 also (-1)2 = 1, so O(-1) = 2, so 1 and -1 are only two elements of finite orders.

Self Check Exercise - 2

Q. 1 Let G be a finite group of order 2n

Let $t = \{x \in G : x^2 = e\}$

and $S = \{x \in G : x^2 \pm e\}$

Then $T \neq \phi$ as $e \in T$

also $T \cap S = \phi$ and $TUS = G$

$\therefore O(G) = 0 (TUS)$

$= O(T) + O(S)$

When $G \neq \phi$, Let $x \in S$

$\Rightarrow$ $x\text{-}1 \in S$ [$\because x^2 \neq e$ and $x^{-1} \neq x$]

$\therefore$ O(S) is even

and when $S = \phi$, so G has an element of order 2

Let O(s) = 2k

$\therefore O(T) \geq 2$

$\therefore \exists$ at least are element $a \neq e \in T$ s.t. $a^2 = e$

$\therefore O(a) = 2$

Q. 2 As per as Question 1.

Self Check Exercise - 3

Q.1 Since $1 = w^3$, each element of G is an integral power of w. So $\{1, w, w^3\}$ is a cyclic group.

Q. 2 Since $1 = i^4$, $-1 = i^2$, $-i = i^3$

each element of {1, -1, i, -i} is an integral power of i so {1, -1, i, -i} is a cyclic group.

Q. 3 Do same as example 1.

Q. 4 Yes

Q. 5 $Z_6 \rightarrow$ <1> and <5>

$Z_8 \rightarrow$ <1>, <3>, <5> and <7>

$Z_{20} \rightarrow$ <1>, <3>, <7>, <9>, <11>, <13>, <17> and <19>

Z_{25} the generators are all non-zero element other than 5, 10, 15, 20.

Z_{256} the generators are all odd integers.

5.9 References/Suggested Readings:-

1. Vijak. K. Khanna and S.K. Bhambri, A course in Abstract Algebra.
2. Joseph A Gallian, Contemporary Abstract Algebra.
3. Frank Ayrer Jr. Modern Algebra, Schaum's Outline Series.
4. A.R. Vasistha, Modern Algebra, Modern Algebra, kushan Prakashan Media.

5.10 Terminal Questions

*****

Unit - 6

SUBGROUP

Structure

6.1 Introduction

Dear student, in previous units related to groups you have studies about the algebraic structures of integers, rational numbers, real number and complex numbers. You may have noticed that some groups ae contained within another large group under the same binary operation. For examples to get of integers under addition (z_1+) is contained in set of real under addition (R_1+). Here the thing to be noticed is that, it is not only the set of a group to be a subset of the other, but also that of the group operation on the subset be the induced operation that assigned the same element to each offered pair from that subset as is assigned by the group operation or whole set.

In this unit, you will such subject of a set under a binary operation, known as subgroup, along with their properties and theorems based on them. You will also study about the set operation (union and intersection) on and product subgroups.

6.2 Learning Objectives:

After studying this unit, you will be able to :

1. define and give examples of subgroups.
2. prove theorem based on subgroups.

3. check that the conditions for a subset of a given up to be a subgroup are satisfied or not.

4. prove and apply results related to set operations on subgroups.

6.3 Subgroup

Definition:

A non empty subset H of a group <G, $*$> is said to be a subgroup of G if <H, $*$) is itself a group. Here H is a group in itself under the same operation of G. If (H, $*$) is a subgroup of (G, $*$), we denote it mathematically as (H, $*$) or (H < G)

Also if H is not a subgroup of G, then we write (H, $*$) $\leq$ (G, $*$) or (H, G).

For Example:- (1) (Z, +) set of integers under addition is a subgroup of (Q, +), (R, +) and (C, +) i.e. set of rational number, set of real numbers and set of complex numbers under addition.

(2) G = {1, -1, i, -1} and H = {1, -1} where $i^2 = -1$ where G is a group under usual multiplication of complex number, Since H is a subset of G, we can easily prove that H is a subgroup of G, as it form a group under multiplication.

.	1	-1
1	1	-1
-1	-1	1

From composition table it can easily be verified that (H, .) is a group.

Proper Subgroup:

Let (G, $*$) be a group and (H, $*$) $\leq$ (G, $*$), is a Subgroup of G such that H $\leq$ G. Then H is called proper subgroup of G. Mathematically, H < G or H $\leq$ G or H < G, H $\neq$ G. H $\neq$ {e}

Improper or Trivial Subgroup:

Since every group has all east two subgroups i.e. {e} and G itself. These two subgroup are called trivial or improper subgroup.

Note: 1. If H is a subgroup of G and k is a subgroup of H then k is a subgroup of G

2. If H and k are subgroups of a group G and H $\leq$ K then H is a subgroup of K.

For more understanding of subgroups, let us take following examples.

Example 1: Show that the set <Q +, .> is a subgroup of <Q - {0}, .>

Solution: The set Q - {0} is the set of all non zero rational numbers forms a group under multiplication and Q^+, set of positive rational number. So Q+ < Q-{0}.

Also that set Q+ - the set of positive rational numbers.

Since rational numbers are closed under multiplication, obeys alsociative property under multiplication, 1 is its identity and for $p/q \in Q^+$, $q/p \in Q^+$ act act inverse element.

So Q^+ forms a group under multiplication

So $<Q^+, .>$ forms a subgroup of $<Q - \{0\}, .>$

Example 2: Show that the set n Z = {....., -3n, -2 n, -n, 0, n, 2 n, 3n,.....} of all integral multiplies of n, is a subgroup of the group Z of all integers under the operation of addition.

Solution: We know that Z, the set of integers forms a group under addition.

Now $n Z = \{n m : m \in Z\}$

Since $n, m \in Z \quad \Rightarrow \quad n m \in Z$

$\therefore \quad n Z \subseteq Z$.

We now show that nZ forms a group under addition.

Let $x, y \in n Z$ so that $x = n m_1$ and $y = nm_2$ for some $m_1, m_2 \in Z$.

$\therefore \quad x - y = nm_1 - nm_2 - n(m_1 - m_2) \in n Z$.

[Since $m_1 - m_2 \in Z$ for every m1, $m_2 \in Z$]

$\therefore$ The closure property holds in n Z.

The associative law holds in n Z since it holds in Z and $n Z \subseteq Z$.

Also $0 = n 0 \in n Z$ and $x + 0 = x = 0 + x, \quad \forall x \in n Z$.

$\therefore$ 0 is identity element of n Z.

Now for $x = n m \in n Z$ we have $y = n (-m) \in n Z$.

And $x + y = n m + n(-m) = nm - nm = 0 = y + x$.

$\therefore$ y is the inverse of x in n Z.

$\Rightarrow$ inverse of every element in nZ exists.

$\therefore$ n Z forms a group under addition.

Thus n Z is a subgroup of Z.

Example 3: Verify the following statement for being true or false.

1. The additive group of even integers is a subgroup of the additive group of all integers.
2. The set of all odd integers is not a subgroup of $<Z_1 +>$

(1) Let Z be the additive group of integers and

E be the set of all even integers of Z

Clearly $0 \in E \quad \therefore \quad$ E is non-empty subset of Z

Let $x, y \in E$ be any two elements.

$\therefore$ $x = 2n$, and $y = n_2$ for some $n_1, n_2 \in Z$

$\therefore$ $x - y = 2n_1 - 2n_2 = 2(n_1 - n_2) \in E$

$\therefore$ E is a subgroup of Z.

(2) Let O be set of odd integers

Then if we take $3, 5 \in O$

Then $3 + 5 \notin O$ ($\because$ $8 \in E$)

$\Rightarrow$ O is not a subgroup of <Z, +>.

Example 4: Let C* denote the group of all non-zero complex numbers.

Show that the set $S = \{z \in C^* \text{ s.t. } |z| = 1\}$ is a subgroup of C^*

Solution: Since $|\in C^*$ and $|1| = 1$, $\therefore$ $1 \in S$

i.e., S is non-empty subset of C*

Let $z_1, z_2 \in S$ be any two element $\Rightarrow$ $|z_1|$ = and $|z_2| = 1$

Now $|z_1 z_2| = \{z_1| \, |z_2| = 1 = 1$

$\Rightarrow$ $z_1 z_2 \in S$

$\therefore$ the closure property hold in S

The associative law holds in S since it holds in C* and $S \subseteq C^*$

Since $1.z = z = z.1$ for all $z \in C^*$

In particular $1.z = z = z.1$ for all $z \in S$

$\therefore$ 1 is the identity element of S

Since for every $z \in S \Rightarrow$ $z \in C^*$ $\therefore$ $\exists\, z' \in C^*$ s.t.

$zz' = 1 = z' z$ [$\because$ C* is a group]

But $|zz'| = |1| = |z'z|$

$\Rightarrow$ $|z| \, |z'| = 1 = |z'| \, |z|$

$\Rightarrow$ $1.|z') = 1 \Rightarrow |z'| = 1 \Rightarrow z' \in S$

$\therefore$ for every $z \in S$, $\exists\, z' \in S$ s.t.

$z\, z' = 1 = z' z$

$\therefore$ inverse of every elements of S exists in S

$\Rightarrow$ S is a group under multiplication.

Hence s is a subgroup of C*.

Example 5 : If x is any element of group G, then show that $\{x^n \mid n \in Z\}$ is a subgroup of G.

Solution : Let x be any element of group G

Take H = $\{x^n \mid n \in Z\}$

Clearly $H \neq \phi$ as $(x = x^1 \in H)$ and $H \subset G$

Now take .$\alpha, \beta \in H$. Then $\alpha = x^{k_1}$, $\beta = x^{k_2}$ for $k_1, k_2 \in Z$

$\Rightarrow \quad \alpha\beta^{-1} = (x^{k_1})(x^{k_2})^{-1}$

$= x^{k_1 - k_2}$ where $k_1 - k_2 \in Z$

$\in H$

$\Rightarrow$ h is a subgroup of G.

Example 6 : Is Q_0, the set of non-zero rational numbers, a subgroup of

$G = \{a + \sqrt{2}\ b \mid a, b \in Q \text{ and } a^2 + b^2 \neq 0\}$ a group under multiplication? Justify.

Solution : Let $a \in Q_0$. Then $a = a + \sqrt{2}\,(0) \in G$

$\Rightarrow \quad Q_0 \subset G$

and $Q_0 \neq \phi$ as $1 \in Q_0$ $\qquad (1 = 1 + \sqrt{2}\,(0))$

Now inverse of $x = a + \sqrt{2}\ b \in G$ is $= \frac{1}{x} = \frac{1}{a+\sqrt{2}\ b} = \frac{a-\sqrt{2}\ b}{a^2-2b^2}$

$$= \frac{a}{a^2-2b^2} \sqrt{2}\left(\frac{-b}{a^2-2b^2}\right)$$

$= a + \sqrt{2}\, d \in G$

For $x, y \in Q_0 \Rightarrow x y^{-1} = \frac{x}{y} \in Q_0$

(a, b are rationals $\Rightarrow \frac{a}{b}$ is rational)

$\therefore \quad Q_0$ is subgroup of G.

Example 7 : for positive integers m, n show that n Z is a subgroup of m Z if m | n.

Solution : We have m Z = {....., -2m, -m, 0, m, 2, m, ...}

Take H = n Z = p m Z $\qquad$ (Given m | n $\Rightarrow$n = p m for $p \in Z$)

= {....., -2 p m, -p m, 0, p m, 2 p m, ...}

where m and p are fixed integers

Clearly $H \subseteq$ m Z for p = 1

Let a, b $\in$ H $\Rightarrow \exists$ r, s $\in$ Z s. T. a = p m r, b = p m s

$\Rightarrow$ a - b = p m r - p m s = p m (r - s) $\in$ H (as r - s $\in$ Z)

$\therefore$ H_1 is a subgroup of m Z

= nZ.

Example 8 : Let G be group of 2 $\times$ 2 non singular matrices over R under multiplication.

Show W = $\left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \middle/ a\,d \neq 0\right\}$ is a subgroup of G.

Solution : Clearly W = $\left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \middle/ \begin{matrix} a\,d \neq 0 \\ a, bd \in R \end{matrix}\right\}$ is non empty

subset of group G = $\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle/ \begin{matrix} a, b, c, d \in R \\ \text{and } a\,d - b\,c \neq 0 \end{matrix}\right\}$ as $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in$ W

Let A = $\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}$ and B = $\begin{bmatrix} a_b & b_2 \\ 0 & d_2 \end{bmatrix} \in$ W

Now AB^{-1} = $\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \begin{bmatrix} \frac{1}{a_2} & -\frac{b_2}{a_2 d_2} \\ 0 & \frac{1}{d_2} \end{bmatrix}$ $\left(B-1 = \frac{1}{a_2 d_2}\begin{bmatrix} d_2 & -b_2 \\ 0 & a_2 \end{bmatrix}\right.$

$= \begin{bmatrix} \frac{a_1}{a_2} & -\frac{a_1 b_2}{a_2 d_2} + \frac{b_1}{d_2} \\ 0 & \frac{d_1}{d_2} \end{bmatrix} \in$ W $\left(\because \frac{a_1}{a_2} \times \frac{d_1}{d_2} = \frac{a_1 b_2}{a_2 d_2} \neq 0\right)$

$\Rightarrow$ W is a subgroup of G.

Example 9 : Show that SL (2, R) is a subgroup of the group GL (2, R) under the composition of multiplication of matrices.

Solution : Now SL (2, R) = $\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \text{ where } a,\ b,\ c,\ d\ \in R \text{ s. t. } a\ d\ -\ b\ c = 1\right\}$

is a non-empty subset of the group

GL (2, R) = $\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \text{ where } a,\ b,\ c,\ d\ \in R \text{ s. t. } a\ d\ -\ b\ c\ \neq 0\right\}$

as I = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in$ SL (2, R).

Moreover, SL (2, R) is a group under the operations of multiplication of matrices.

(Already Proved)

Hence SL (2, R) is a subgroup of GL (2, R).

Example 10 : If e is an identity element of a group G, then { e } is a subgroup of G.

Solution : Since e is the identity element of group G, therefore e $\in$ G.

Let H = { e }, then H $\subseteq$ G.

Since e e = e $\in$ H, therefore closure property holds in H.

Also (e e) e = e (e e) = e.

$\therefore$ Associatively to holds is H

Since e e = e = e e

$\therefore$ e is identity element of H and

e-1 = e $\in$ H.

$\therefore$ H itself is a group

$\therefore$ H is a subgroup of G

Remark : The subgroup G and { e } are called trivial or improper subgroups of G. Any subgroups of group G other then G and { e } is called proper subgroup of G.

Example 11. Show that the set of cube roots of unity H = {1, w, w2} and the set of fourth roots of unit K = {1, -1, i, -i} are subgroups of the group of twelfth roots of unity

G = $\left\{ \text{cis}\frac{2k\pi}{12} : \text{k} = 0, 1, 2, 3 ..., 11 \right\}$ under multiplication of complex numbers.

Solution : Clearly, H and K are non-empty subset of G. The composition table for H and K are given below:

Composition table for H

.	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

Composition table for K

.	1	-1	i	-i
1	1	-1	I	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

From the composition table, it is easy to see that H and K from groups and hence are subgroups of G.

Example 12 : Show that the set H {0, 3} and K = {0, 2, 4} are subgroups of the group G = {0, 1, 2, 3, 4, 5} under the operation addition modulo 6.

Solution : Clearly, H and K are non-empty subset of G. The composition table for H and K are given below:

Composition table for H

$+_6$	0	3
0	0	3
3	3	0

Composition table for K

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

From the composition table, it is easy to see that H and K from groups and hence are subgroups of G.

Properties of Subgroups

Just like group subgroups also have some properties which are related to their group these are :

Property I. The identity element of a subgroup is same as the identity element of the group.

Proof . Let H be a subgroup of a group G.

Let e and e' be the identity elements of G and H respectively

Let $a \in H$ be any element

$\therefore$ $a\,e' = a$ [$\because$ e' is the identity of H]

Also $\because$ $a \in H$ and $H \subseteq G \Rightarrow a \in G$

$\therefore$ $a\,e = a$ [$\because$ e is the identity of G]

$\therefore$ we have $a\,e = a\,e'$

$\Rightarrow$ $e = e'$. [by left cancellation law]

Hence the identity of a group and that of a subgroup is the same.

Property II. The inverse of any element of a subgroup is the same as the inverse of the element regarded as the element of the group.

Proof. Let e be the identity element of G and H.

Let $a \in H$ be any element.

Since $H \subseteq G$ $\therefore$ $a \in G$.

Let b be the inverse of a in H and c be the inverse of a in G.

$\therefore$ $b\,a = e$ and $c\,a = e$

$\Rightarrow$ $b\,a = c\,a$

$\Rightarrow$ $b = c$. [by right cancellation law]

Hence the inverse of any element of a subgroup is same as the inverse of the same element regarded as an element of the group.

Property III. The order of any element in a subgroup is the same as the order of the element regarded as the element of the group.

Proof. Let e be the identity element of G and H.

Let $a \in H$ such that $o(a) = n$

$\Rightarrow$ $a^n = e$ and $a^m \neq e$ for every $m < n$.

Also $a \in H \Rightarrow a \in G$ and so $a^n = e \in G \Rightarrow o(a) = n$ in G.

Hence order of any element in a subgroup is same as the order of the element regarded as the element of the group.

Property IV. Subgroup of an abelian group is abelian.

Proof. Let H be a subgroup of an abelian group G

$\therefore$ $H \subseteq G$.

Let $a, b \in H$ be any two elements

$\therefore$ $a, b \in G$ $\Rightarrow$ $a\,b = b\,a$ [$\because$ G is abelian]

$\therefore \quad \forall\ a, b \in H \quad$ we have $a\,b = b\,a$

Hence H is an abelien subgroup of G.

The converse of above result is false

i.e., A subgroup may be abelian even if G is not abelian.

Note : A non-abelian group may have abelian sub group.

To prove above properties let us take following examples.

Example 13 : Can an abelian group have non abelian subgroup?

Solution : No, Let G be a group which is abelian and let H be its subgroup. As commutative property holds in G so it will hold in H. Therefore, an abelian group always has an abelian subgroup.

Example 14 : Can a non abelian-group have an abelian subgroup?

Solution : Yes, the example for in abelian subgroup of a non abelian group is given as.

As the quaternion Group Q = {±1, ±i, ±j, ±k}, under multiplication is a non abelian group, but if we take the subset H {1, -1, i, -1} of Q. then by composition table for H is

.	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

From the table we conclude that (H, .) is a group.

We find that the element are symmetric about the main diagonal, Also H = {1, -1, i, -1} form an abelian group.

Hence a non abelian group can have an abelian sub group.

Self Check Exercise - 1

Q. 1 Prove that {1, -1} and {1, -1, i, -i} are abelian subgroups of non-abelian Quaternion group.

Q. 2 Prove that H = subset of Z consisting all multiple of n (n is any non zero) integer is a proper subgroup of Z under addition.

6.4 Theorems on Subgroups

Theorem 1. A non-empty subset H of a group G is a sub group of Giff

(1) $a, b \in H \Rightarrow a , b \in H$

(2) $a \in H \Rightarrow a^{-1} \in H$.

Proof . If H < G, then (1), (2) follows from definition [$\because$ H is a group]

Conversely : Let (1) and (2) be satisfied.

By (2) $a, b \in H \Rightarrow a^{-1} \in H$

By (1) $a \in H, a^{-1} \in H \Rightarrow a \cdot a^{-1} \in H \Rightarrow e \in H$ i.e. id. elt. exists in H.

Since Ass. law holds for all elts of G. $\therefore$ in particular in holds for all elts of H.

[$\because$ H is a subset of G]

$\therefore$ H is a group under the binary operation (product) in G.

$\therefore$ H is a subgroup of G.

Theorem 2 : The necessary and sufficient condition that H be a subgroup of G is that $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof. The condition is necessary

Let $H \leq G$. $\therefore$ H is a gp.

$\therefore$ $b \in H \Rightarrow b^{-1} \in H$

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

The condition is sufficient

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

Since Ass. law holds for G. $\therefore$ it holds for H [$\because$ $H \leq G$]

Again a, $a \in H \Rightarrow a \cdot a^{-1} \in H \Rightarrow e \in H$ $\therefore$ Id. elt. exists in H.

Again e, $a \in H \Rightarrow e \cdot a^{-1} \in H \Rightarrow a^{-1} \Rightarrow H$ $\therefore$ inverse exists in H.

Again a, $b^{-1} \in H \Rightarrow a (b^{-i})^{-1} \in H \Rightarrow ab \in H$

$\therefore$ closure property is satisfied $\therefore$ H is a gp. Hence $H \leq G$.

Definition . Any non-empty subset H of G is called a complex of the group G

if $a \in H, b \in H \Rightarrow a\, b \in H$, then the complex H is stable.

Note : In case of additive notation, above two theorems can be stated as :

Remark 1 A non empty subset H of a group G is a sub group of Giff $\forall$ $a, b \in H \Rightarrow a + b \in H$ and $\forall$ $a \in H \Rightarrow -a \in H$.

Remark 2 A non empty subset H of a group is a subgroup of G iff $a - b \in H$ $\forall$ a, b $\in$ H.

Theorem 3. A non-empty finite subset H of a group is a subgroup of G iff $a\, b \in H$, $\forall$ a, b $\in$ H.

Proof :Necessary Part. Let a non-empty finite subset H of a group G be its subgroup.

$\therefore$ H itself is a group

$\therefore$ $a\, b \in H$, $\forall$ a, b $\in$ H. (By closure property}

Sufficient Part. Suppose that H is a non-empty finite subset of a group G

such that $a\,b \in H, \forall\ a, b \in H$.

$\therefore$ The operation of multiplication is a binary operation on H.

Let $a, b\,c \in H \Rightarrow a, b\,c \in G$, since $H \subseteq G$.

$\Rightarrow$ $(a\,b)\,c = a\,(b\,c)$, Since G is a group.

$\therefore$ The associative law holds in H under multiplication.

Firstly we prove that cancellation laws hold in H.

Let $a, b, c \in H$, such that $a\,b = a\,c$.

Since $a \in H$, so $a \in G$.

$\therefore$ $a^{-1} \in G$ such that $a\,a^{-1} = e = a^{-1}\,a$

Now $a\,b = a\,c$

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

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

$\Rightarrow$ $e\,b = e\,c \quad \Rightarrow \quad b = c$

$\therefore$ $a\,b = a\,c \quad \Rightarrow \quad b = c$.

Similarly $b\,a = c\,a \quad \Rightarrow \quad b = c$.

$\therefore$ The cancellation laws hold in H.

$\therefore$ H is a non-empty finite set with an associative binary operation in H and the cancellation laws hold in H.

$\therefore$ H itself is a group. (already proved)

Thus H is a subgroup of G.

Notice that the above theorem holds only finite subsets of a group.

Remark : In case of additive notation, the above lemma can be stated as

A non-empty finite subset H of a group G is a subgroup iff

$a - b \in H, \quad \forall\ a, b \in H$.

Let use try some examples of subgroups based on above theorems :

Example 1. Show that SL (2, R) is a subgroup of the group GL (2, R).

Solution : Now SL (2, R) = $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in R \text{ s. t. } a\,d - b\,c = 1 \right\}$

and GL (2, R) = $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in R \text{ s. t. } a\,d - b\,c \neq 0 \right\}$

To show that SL(2, R) is a subgroup of GL (2, R)

Clearly, SL (2, R) is a non-empty subset of GL (2, R)

for, I = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in$ SL (2, R).

Let A, B $\in$ SL (2, R) $\Rightarrow$ |A| = 1, |B| = 1

Now | AB | = | A | | B | = 1.1 = 1

$\Rightarrow$ AB $\in$ SL (2, R)

Also for each A $\in$ SL (r, R), $\exists$ B (= adj A)

s.t. AB = I = BA

where | B | = | adj-A | = | A |$^{2-1}$ = | A | = 1 $\Rightarrow$ B $\in$SL(2, R).

B is the inverse of A i.e., B = A^{-1}.

Hence SL (2, R) is a subgroup of GL (2, R).

Example 2. G = $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,\ b,\ c,\ d\ \in \mathrm{Z} \right\}$ under addition.

Let H = $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a+b+c+d=0 \right\}$. Prove that H is a subgroup of G.

What if 0 is replaced by 1?

Solution : Clearly, H is a non-empty subset of G for $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in$ H,

Let A = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, B = $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ be any two elements of H,

where a + b + c + d = 0 and a' + b' + c' + d' = 0

Now A - B = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ - $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$

= $\begin{bmatrix} a-a' & b-b' \\ c-c' & d-d' \end{bmatrix}$

so (a - a') + (b - b') + (c - c') + (d - d')

= (a + b + c + d) - (a' + b' + c' + d')

= 0 - 0 = 0

A - B $\in$H, $\forall$ A - B $\in$ H.

Hence H is a subgroup of G.

Now, when 0 is replaced by 1, them

H $= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a+b+c+d=1 \right\}$ is not a subgroup of G.

for, A = $\begin{bmatrix} 1 & 3 \\ -5 & 2 \end{bmatrix}$, B = $\begin{bmatrix} 2 & 3 \\ 4 & -8 \end{bmatrix}$ be two elements of H.

But A - B = $\begin{bmatrix} +1 & 0 \\ -9 & 10 \end{bmatrix}$ is not an element of H.

as -1 - 9 + 0 + 10 $\neq$ 1 $\quad\quad$ $\therefore$ A - B $\notin$ H.

$\therefore$ $\quad$ H will not a subgroup of G.

Example 3. Let G. = GL (2, R)

and H = $\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : \text{a and b are non-zero integers} \right\}$

Prove or disprove that H is a subgroup of G under multiplication.

Solution : H is not a subgroup of G, for the inverse of the matrix A = $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ is

the matrix B = $\begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{bmatrix} \notin$H if a, b > 1.

Example 4. Show that subset H = {(1, b) : b $\in$ R} of the group

G = {(a, b) : where a, b $\in$ R, s.t. a $\neq$ 0} under the operation * defined by

(a, b)* (c, d) = (a c, b c + d) is a subgroup of G.

Solution : Clearly, H is a non-empty subset of G, for (1, 0) $\in$ H.

Let (1, b), (1, c) $\in$ H be any two elements, where b, c $\in$ R.

$\therefore$ $\quad$ (1, b)* (1, c) = (1.1, b.1 +c) = (1, b + c) $\in$ H.

Also, we know that the identity of the group G is (1, 0)

Let (x, y) be the inverse of the element (1, b)

$\therefore$ $\quad$ (x, y) * (1, b) = (1, 0)

$\Rightarrow$ $\quad$ (x.1, y.1 + b) (1, 0)

$\Rightarrow$ $x = 1, y + b = 0$

$\Rightarrow$ $x = 1, \quad y = -b$ i.e. $(1, -b)$ is the inverse of $(1, b)$

Clearly, $(1, -b) \in H$.

$\therefore$ Inverse of each element of H exists in H.

Example 5 : Show that the elements of finite order in a commutative group G from a subgroup of G.

Solution : Let G be commutative group and let

$H = \{a \in G : o(a) = \text{finite number}\}$

Clearly, $H \neq \phi$, for $e \in H$, as $o(e) = 1$; a finite number

Let $a, b \in H$ be any two elements.

$\therefore$ o (a) and o (b) are finite number Let $o(a) = m$, $o(b) = n$

$\therefore$ $a^m = e, b^n = e$.

Now $(a\,b)^{m\,n} = a^{m\,n}\, b^{m\,n} = (a^m)^n . (b^n)^m = e^n . e^m = e . e = e$

$\therefore$ o (a b) is also finite $\Rightarrow a\,b \in H$.

Also $o(a^{-1}) = o(a)$

i.e. if $a \in H$ then a^{-1} H.

Hence H is a subgroup of G.

Example 6. G is an abelian group having n elements $g_1, g_2, g_3, ...g_n$.

Show that $(g_1\, g_2.....g_n)^2 = e$, where e is identity of G.

Solution : Given $G = \{g_1, g_2, ..., g_n\}$ is an abelian group.

Since e, the identity element is in G

$\therefore$ some $g_1 = e$ for fixed l. ...(1)

Further every element of G is invertible.

i.e. $\forall g_j \in G, (j \neq l), \exists g_k \in G$ s.t. $g_j g_k = e$ ...(2)

Now consider

$(g_1\, g_2 .... g_n)^2 = (g_1\, g_2 .... g_n)\, (g_1\, g_2 .... g_n)$

Since G is abelian and also associative law holds

$\therefore$ using (1) and (2), we get

$(g_1\, g_2 .... g_n)^2 = e$.

Example 7 Let $H = \{7x \mid x \in Z\}$. Prove H is a subgroup of (Z, +)

Solution : Clearly H is non empty as $0 \in Z$ $(7 . 0 = 0)$

Take a, b $\in$ H be any two elements

Then a = 7 x and b = 7 y for some x, y $\in$ z

$\therefore$ a - b = 7 x - 7 y = 7 (x - y) $\in$ H (as x, y $\in$ Z $\Rightarrow$ x - y $\in$ Z)

$\Rightarrow$ a - b $\in$ H $\forall$ a, b $\in$ H

$\therefore$ H is a subgroup of Z.

Example 8 . Let G be an abelian group with identity e. Show that

H = {x $\in$G : x^2 = e} is a subgroup of G.

Solution : e^2 = e for e $\in$ G

$\therefore$ e $\in$H $\Rightarrow$H is non empty subset of G

Now let x, y $\in$ H be any two elements

$\therefore$ x^2 = e and y^2 = e $\Rightarrow$ x^{-1} = x and y^{-1} = y ...(1)

Now $(x\ y^{-1})^2$ = (x y^{-1}) (x y^{-1}) = x (y^{-1} x) y^{-1}

= x (y x^{-1}) y^{-1} (Using (1))

= x(x^{-1} y) y^{-1} ($\because$ y x^{-1} = x^{-1} y as G is abelian)

= (x x^{-1}) (y y^{-1})

= e e = e

$\therefore$ x y-1 $\in$ H $\forall$ x, y $\in$ H

$\Rightarrow$ H is a subgroup of G.

Example 9 . Let H be a subgroup of group g and a $\in$ G.

Show that a H a^{-1} = {a h a^{-1} : h $\in$ H} is a subgroup of G.

Solution : Since e = a e $a^{-1}$$\Rightarrow$ e $\in$ a H a^{-1}

$\therefore$ a H a^{-1} is a non empty subset of G

[$\because$ $\forall$ a h $a^{-1}$$\in$ a H a^{-1} where a, h $\in$G as H $\subseteq$ g and G is a group

$\therefore$ a h $a^{-1}$$\in$ G i.e. a H $a^{-1}$$\subseteq$ G]

Let x, y $\in$ a H a^{-1} be any two elements

Then x = a h_1 a^{-1} and y = a h_2 a^{-1} for some h_1, $h_2$$\in$ H

Now x y^{-1} = (a h_1 a^{-1}) (a h_2 a^{-1})$^{-1}$

= (a h_1 a^{-1}) (a h_2 a^{-1}) [$\because$ $(a^{-1})^{-1}$ = a]

= a h_1 (a^{-1} a) h_2 a^{-1}

= a h_1 $h_2^{-1}$$a^{-1}$ ($\because$ a^{-1} a = e]

= a h_3 a^{-1} where h_3 = h_1 $h_2^{-1}$$\in$H

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

$\therefore$ $a H a^{-1}$ is a subgroup of G.

Example 10. Show that the elements of a group G which commute with the square of given element 'a' form a subgroup H of G and which commute with 'a' itself form a subgroup of G.

Solution : Let a be any element of G

and $H = \{ x \in G \mid x a^2 = a^2 x\}$

1st Part

Now to show H is a subgroup of G

Let $x, y \in H \Rightarrow x a^2 = a^2 x$ and $y a^2 = a^2 y$

Here $y a^2 = a^2 y$

$\Rightarrow$ $a^2 y = y a^2$

$\Rightarrow$ $y = (a^2)^{-1} y a^2 \Rightarrow y^{-1} = (a^2)^{-1} y^{-1} (a^2)$ ....(1)

Now $(x y^{-1}) a^2 = x e y^{-1} a^2$ (e is identity of H)

$= x (a^2 (a^2)^{-1}) y^{-1} a^2)$

$= (x a^2) ((a^2)^{-1} y^{-1} a^2)$

$= (x a^2) y^{-1}$ [Using (1)]

$= (a^2 x) y^{-1} = a^2 (x y^{-1})$

$\Rightarrow$ $(x y^{-1})a^2 = a^2 (x y^{-1}) \Rightarrow x y^{-1} \in H$

$\therefore$ H is a subgroup of G.

IInd part

Let $H_1 = \{x \in G : x a = ax\}$

Now to show H_1 is a subgroup of G

Now for $x \in H_1$ we have $x a = a x, x \in G \Rightarrow a = x a x^{-1}$

$\Rightarrow$ $x^{-1} a = (x^{-1} x) a x^{-1}$

$\Rightarrow$ $x^{-1} a = a x^{-1}$ $(\because x^{-1} x = e, x^{-1} \in G$

$\Rightarrow$ $x^{-1} E H_1$

Further let $x, y \in H_1 \Rightarrow x a = a x, y a = a y; x, y \in G$

$\Rightarrow$ $(x y) a = x (y a) = x (a y) = (x a) y = (a x) y = a (x y)$

$\Rightarrow$ $(x y) a = a (x y) ; x y \in G$

$\therefore$ $x y \in H_1$

Hence H_1 is a subgroup of G.

Self Check Exercise - 2

Q. 1 Check whether or not $Z(\sqrt{3}) = a + b\sqrt{3}$, a, b $\in$ Z is a subgroup of R.

Q. 2 Check whether or not $Z\sqrt{6} = a + b\sqrt{6}$, a, b $\in$ Z is a subgroup of R.

Q. 3 Check whether or not {1, w^2, w^4, w^8} is a subgroup of 10th root of unity.

6.5 Set Operations on Subgroups

Dear students, in set operations on subgroup we will study about the operations of like union, intersection and product on subgroups of group. To study the effect of union, intersection and product on subgroup of group, Let us prove following theorems.

Intersection of two Subgroup

Theorem 1: Prove that the intersection of two subgroups of a group is again a subgroup of the group.

Proof. Let H and K be two sub groups of a group G.

$\therefore$ H and K are subset of G.

$\Rightarrow$ $H \cap K \subseteq g$.

Now let x, y $\in$ H $\cap$ K

$\therefore$ x, y $\in$ H and x, y $\in$ K

$\Rightarrow$ $x y^{-1} \in$ H and $x y^{-1} \in$K, since H, K are both subgroups of G.

$\Rightarrow$ x y-1 $\in$ H $\cap$ K

$\therefore$ x y-1 $\in$ H $\cap$K, $\forall$ x, y $\in$ H $\cap$ K

$\therefore$ H $\cap$ K is a subgroup of G.

Theorem 2. the intersection of an arbitrary collection of subgroups of a group is again a subgroup of the group.

Solution : Let G be the group and $\{H_\lambda \mid \lambda \in \wedge\}$ be a family of subgroups of G.

Take H = $\bigcap_{\lambda \in \wedge} H_\lambda$

Since H_λ is a subgroup of G, $\forall \lambda \in \wedge$

$\therefore$ $e \in H_\lambda \forall \lambda \in \wedge$

$\Rightarrow$ $e \in \bigcap_{\lambda \in \wedge} H_\lambda$

$\Rightarrow$ $e \in H \Rightarrow H \neq \phi$

Also as $H_\lambda \subseteq$ G, $\forall \lambda \in \wedge$

so $\bigcap_{\lambda\in\wedge} H_\lambda \subseteq G$

$\Rightarrow$ $H \subseteq g$

Now let a, b $\in$ H

$\Rightarrow$ a, b $\in \bigcap_{\lambda\in\wedge} H_\lambda$

$\Rightarrow$ a, b $\in H\lambda$, $\forall\lambda\in\wedge$

$\Rightarrow$ a $b^{-1}\in$ H $\forall\lambda\in\wedge$

($\because$ for each $\lambda\in\wedge$, Hλ is a subgroup of G)

$\Rightarrow$ a $b^{-1}\in \bigcap_{\lambda\in\wedge} H_\lambda$

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

$\Rightarrow$ H is itself is a group and H$\subseteq$ G

So H is a subgroup of G

* The union of any two subgroups of a group is not necessarily a subgroup of the group.

For example : (i) The sets H = {0, 3} and K = {0, 2, 4} are subgroups of the group G = {0, 1, 2, 3, 4, 5} under the operation addition modulo 6. But the union H U K = {0, 2, 3, 4} is not a subgroup of G, for 2, 3 $\in$ H U K, but 2 + 3 = 5 $\notin$ H U K.

(ii) The set n Z = {....., -3 n, -2 n, -n 0, 2 n, 3 n, ...} of integral multiple of n, is a subgroup of the group of integers under addition.

$\therefore$ 2 Z = {....., -6, -4, -2, 0, 2, 4, 6, ...}

and 3Z = { ...., -9, -6, 3, 0 3, 6, 9, ...} are subgroups of Z, under addition.

But 2Z U 3Z = {....., -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9, ...} is not a subgroup of Z, for 4, 3 $\in$ 2 Z U 3 Z but 4 + 3 = 7 $\notin$ 2 Z U 3Z.

(iii) The set H = {1, -1, i, -i} and K = {1, -1, j -j} are subgroups of the Quaternion group Q_8, but H U K = {1, -1, i - i, j, -j} is not a subgroup of the Q_8 for, i, j $\in$ H U K, but i, j = k $\notin$ H U K.

Union of Subgroups

Theorem 3. The union of two subgroups of a group is a subgroup iff one is contained in the other.

Proof.Necessary Part : Let H_1 and H_2 be two subgroups of a group G such that H_1 U H_2 is again a subgroup of G.

We shall prove that either $H_1\subseteq H_2$ or $H_2\subseteq H_1$.

If possible, suppose that $H_1\not\subseteq H_2$ or $H_2\not\subseteq H_1$.

Since $H_1\not\subseteq H_2$, so $\exists$ a $\in$ G such that a $\in H_1$ but a $\notin H_2$.

Again since $H_2 \not\subseteq H_1$, so $\exists\ b \in G$ such that $b \in H_2$ but $b \notin H_1$.

Since $a \in H_1$ and $H_1 \subseteq H_1 \cup H_2$ so $a \in H_1 \cup H_2$.

Similarly $b \in H_2$ and $H_2 \subseteq H_1 \cup H_2 \Rightarrow b \in H_1 \cup H_2$

$\therefore$ $a, b \in H_1 \cup H_2$

$\Rightarrow$ $a\,b^{-1} \in H_1 \cup H_2$, since $H_1 \cup H_2$ is a subgroup

$\Rightarrow$ $a\,b^{-1} \in H_1$ or $a\,b\text{-}1 \in H_2$.

First consider the case when $a\,b^{-1} \in H_1$.

Since $a \in H_1$ and H_1 is a subgroup $\therefore\ a^{-1} \in H_1$

$\therefore$ $a^{-1}(a\,b^{-1}) \in H_1$

$\Rightarrow$ $(a^{-1}a)b^{-1} \in H_1$

$\Rightarrow$ $e\,b^{-1} \in H_1$

$\Rightarrow$ $b^{-1} \in H_1$

$\Rightarrow$ $(b^{-1})^{-1} \in H_1$

i.e., $b \in H_1$, which is not true.

$\therefore$ This case is not possible.

Now consider the case $a\,b^{-1} \in H_2$

Since $b \in H_2$.

$\therefore$ $(a\,b^{-1})\,b \in H_2 \Rightarrow a\,(b^{-1}\,b) \in H_2$

i.e., $a\,e \in H_2 \Rightarrow a \in H_2$, which is again false.

$\therefore$ This case is also not possible

So both the cases are not possible. Therefore, out supposition is wrong.

$\therefore$ either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Sufficient Part : Suppose that either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

$\Rightarrow$ $H_1 \cup H_2 = H_2$ or $H_1 \cup H_2 = H_1$

$\Rightarrow$ $H_1 \cup H_2$ is a subgroup of G, since both H_1 and H_2 are subgroups of G.

Product of Two Subgroups

Definition :

Let H and K be two subgroups of a group G, then the set HK defined by $HK = \{h\,k : \text{for all } h \in H, k \in K\}$ is called the product of the subgroups H and K.

Remark : The product HK of two subgroups of a group G may or may not be a subgroup of G.

For example : Let H = {I, (12)} and K = {I, (13)} be two subgroups of the symmetric group S_3 on three elements 1, 2, 3.

But HK = {I, (12), (13), (12) (13)} = {I, (12), (13), (123)}

So, HK is not a subgroup of S3, for

(123) $\in$ HK and (123) (123) = (132) $\notin$ HK.

In fact here K H = {I, (12), (13), (132)}

i.e. HK $\neq$KH.

Theorems on Product of Two Subgroups

Theorem 4. If H and K are two subgroups of a group G, then HK is a subgroup of g iff HK = KH.

Proof .Necessary Part. Let H and K be two subgroups of a group G such that HK is also a subgroup of G.

We shall prove that HK = KH.

Let x $\in$ HK be arbitrary element.

$\therefore$ $x^{-1} \in$ HK, as HK is a subgroup of G.

$\Rightarrow$ x^{-1} = h k for some h $\in$H, k $\in$K

$\Rightarrow$ $(x^{-1})^{-1} = (h\ k)^{-1}$

$\Rightarrow$ $x = k^{-1}\ h^{-1}$

Since k $\in$K and K is a subgroups of G, so $k^{-1} \in$ K.

Similarly $h^{-1} \in$ H.

$\therefore$ $k^{-1}\ h^{-1} \in$ K H.

$\Rightarrow$ x $\in$ K H

$\therefore$ $\mathrm{H\ K} \subseteq \mathrm{K\ H}$.

Let now x $\in$ K H be arbitrary element

$\therefore$ x = k h for some k $\in$K and h $\in$H.

$\Rightarrow$ $x^{-1} = (k\ h)^{-1} = h^{-1}\ k^{-1} \in \mathrm{HK}$

$\Rightarrow$ $x^{-1} \in$ HK

$\Rightarrow$ $(x^{-1})^{-1} \in$ HK, as HK is a subgroup of G,

$\Rightarrow$ x $\in$ HK.

$\therefore$ KH $\subseteq$ HK

Thus HK = KH.

Sufficient Part. Suppose that H and K are two subgroups of a group G such that HK = KH.

We shall prove that HK is a subgroup of G.

Let $x, y \in HK$ be arbitrary elements.

$\therefore$ $x = h_1 k_1$ and $y = h_2 k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$

$\therefore$ $xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = (h_1 k_1)(k_2^{-1} h_2^{-1}) = h_1 (k_1(k_2^{-1} h_2^{-1}))$

$= h_1 ((k_1 k_2^{-1}) h_2^{-1})$. ...(1)

Now $(k_1 k_2^{-1}) h_2^{-1} \in KH$

$\Rightarrow$ $(k_1 k_2^{-1}) h_2^{-1} \in KH$, since $HK = KH$

$\Rightarrow$ $(k_1 k_2^{-1}) h_2^{-1} = h_3 k_3$ for some $h_3 \in H$ and $k_3 \in K$ ....(2)

$\therefore$ $x y^{-1} = h_1 (h_3 k_3)$ [From (1) and (2)]

$= (h_1 h_3) k_3 \in HK$

$\therefore$ $x y^{-1} \in HK$, $\forall\ x, y \in HK$.

$\therefore$ HK is a subgroup of G.

Note : (i) See another proof of the above theorem as 2.1.15.

(ii) HK = KH does not mean that each element of H commute with every element of K. It only mean that for each $h \in H$ and $k \in K$, $hk = k_1 h_1$, for some $h_1 \in H$ and $k_1 \in K$.

(iii) If the composition in G is addition, then we define

$H + K = \{h + k : \text{for } h \in H, k \in K\}$.

Cor. If G is an abelian group, then HK is also a subgroup of G, for HK = KH.

Remark : If H and K are two abelian subgroups of a group G, then HK need not be a subgroup of G.

Theorem 5. If H and K are finite subgroups of a group G, then

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

Proof. We known that

$HK = \{hk : h \in H, k \in K\}$.

Let $H \cap K = \{x_1, x_2, ..., x_n\}$ and suppose $O(H) = r$, $O(K) = s$

Now $hk = h x_i x_i^{-1} k = (h x_i) x_i^{-1} k) \in HK$, $\forall i = 1, 2, 3, ..., n$.

Since $h x_i \in H$, $x_i^{-1} k \in K$

Thus $hk = (h x_i)(x_i^{-1} k) \in HK$, $\forall i = 1, 2, 3, ..., n$.

i.e., hk can be written in atleastn different ways. We show that these are the only n ways that hk can be expressed as an element of HK.

If possible, let $hk = h_i k_1$ be another representation

$\Rightarrow$ $h^{-1} h_1 = k k_1^{-1} \in H \cap K$

$\Rightarrow$ $h^{-1} h_1 = x_i$ and $k k_1^{-1} = x_i$ for some $x_i \in H \cap K$

$\Rightarrow$ $h_1 = h x_i$ and $k_1 = x_i^{-1} k$.

Thus $h k = h_1 k_1 = (h x_i)(x_i^{-1} k)$.

Which is not a new representation.

Hence each h k can be written in exactly n different ways.

Also h can be chosen in r ways, k can be chosen in s ways.

$\therefore$ h k can be choosen in $\frac{rs}{n}$ different ways.

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

Note : There is another proof for this theorem in 2.2.8.

Cor. (i) If H and K are two subgroups of a group G such that G = HK and H ∩ K = {e}, then O (G) = O (H) O (K).

Proof . Since G = HK and H ∩ K = { e } i.e. O(H ∩ K) = 1

Therefore O (G) = O (HK) = $\frac{O(H).O(K)}{O(H \cap K)} = \frac{O(H).O(K)}{1}$

$\Rightarrow$ O (G) = O (H) . O (K).

(ii) If H and K are two subgroups of a group G such that O (H) > $\sqrt{O(G)}$ and O (K) > $\sqrt{O(G)}$, then O (H ∩ K) > 1.

Proof. Since H, K are subsets of G, $\therefore$ HK is also a subset of G.

$\therefore$ $O(G) \geq O(HK) = \frac{O(H)O(K)}{O(H \cap K)} > \frac{\sqrt{O(G)}\sqrt{O(G)}}{O(H \cap K)} = \frac{O(G)}{O(H \cap K)}$

$\Rightarrow$ O(H ∩ K) > 1.

Inverse of a Subset of a Group

Definition :

Let H be a subset of a group G, then the inverse of H is H^{-1} and is defined as

$H^{-1} = \{h^{-1} : \text{for all } h \in H\}$.

Remark : In case of additive notation the above concept transformed as Let H be a subset of a group G, then the inverse of H is H-1 and is defined as

$H^{-1} = \{-h : \text{for all } h \in H\}$.

Theorem 6. If H be a subgroup of a group G, then $H^{-1} = H$.

Proof. Let $h^{-1} \in H^{-1}$ be any element, where $h \in H$.

Since H is a subgroup of G $\therefore h^{-1} \in H$

Thus $h^{-1} \in H^{-1} \Rightarrow h^{-1} \in H$

$\therefore$ $H^{-1} \subseteq H$. ....(1)

Conversely,

Let $h \in H$ be any element of H

Since H is a subgroup of G $\therefore h^{-1} \in H$

$\Rightarrow$ $(h^{-1})^{-1} \in H^{-1}$ i.e., $h \in H^{-1}$

Thus $h \in H \Rightarrow h \in H^{-1} \therefore$ $H \subseteq H^{-1}$ ....(2)

From (1) and (2), we get $H = H^{-1}$

Remark : The converse of above theorem need not be true. i.e., if H is a subset of a group G such that H-1 = H, then H need not be a subgroup of G.

For example : (i) Let G be the group of square roots of unity, i.e., G = {-1, 1} under multiplication, let H = {-1} be a subset of G.

Here $H^{-1} = \{-1\} = H$, for $(-1)^{-1} = -1$.

But H is not a subgroup of G.

(ii) Let $G = \{(0, 1, 2, 3, 4, 5), +_6\}$ be a group under addition modulo 6.

Let H = {1, 3, 5} be a subset of G. then $H^{-1} = \{1, 3, 5\} = H$, for

$(1)^{-1} = 5$, $(3)^{-1} = 3$, $(5)^{-1} = 1$, but H is not a subgroup of G as $3 +_6 5 = 2 \notin H$.

Theorem 7 : A non-empty subset H of a group g is a subgroup, the HH = H.

Proof. Let $H_1 h_2 \in HH$ be any element, where $h_1, h_2 \in H$

Since H is a subgroup of G $\Rightarrow h_1 h_2 \in H$

Thus, $\forall h_1, h_2 \in HH$ $\Rightarrow h_1 h_2 \in H$

$\therefore$ $HH \subseteq H$. ...(1)

Conversely :

Let $h \in H$ be any element of H.

Now $h = h e \in HH$. ($\because e \in H$)

Thus $h \in H$ $\Rightarrow$ $h \in HH$

$\therefore$ $H \subseteq HH$. ...(2)

$\therefore$ from (1) and (2), we get

$HH = H$

Remark. : The converse of above theorem need not be true i.e., If H is a non-empty subset of a group G such that HH = H, then H need not be a subgroup of G.

For example : (i) Let G be the additive group of integers of H be the set of all non negative integers, then HH = H, but H is not a subgroup of G.

(ii) Let <Q - {0}, X > be the group of non-zero rational numbers under multiplication. Let H be the set of all odd integers. Then HH = H, but H is not a subgroup of G, as H has no multiplicative inverse of each elements.

Note. If H is a finite subset of a group g having the property that HH = H, then H is a subgroup of G.

Proof . The result follows immediately by applying Lemma 2.1.4.

Theorem 8 : A non-empty subset H of a group G is subgroup iff $HH^{-1} = H$.

Proof : The result follows immediately by applying Lemma 2.1.3 and

Theorem 2.1.11 and 2.1.12.

Theorem 9 : If H and K be any two subset of a group G, then

$(HK)^{-1} = K^{-1} H^{-1}$.

Proof : Let $(h k)^{-1}$ be any element of $(HK)^{-1}$, where $h \in H$, $k \in K$

$\therefore$ $(h k)^{-1} = k^{-1} h^{-1} \in K^{-1} H^{-1}$ [$\because$ $h^{-1} \in H^{-1}$ and $k^{-1} \in K^{-1}$]

Thus $(h k)^{-1} \in (HK)^{-1}$ $\Rightarrow (h k)^{-1} \in K^{-1} H^{-1}$

$\therefore$ $(HK)^{-1} \subseteq K^{-1} H^{-1}$ ...(1)

Conversely,

Let $k^{-1} h^{-1} \in K^{-1} H^{-1}$ be any element, where $k \in K$, $h \in H$.

$\therefore$ $k^{-1} h^{-1} = (h k)^{-1} \in (HK)^{-1}$

Thus $K^{-1} H^{-1} \in K^{-1} H^{-1}$ $\Rightarrow$ $k^{-1} h^{-1} \in (HK)^{-1}$

$\therefore$ $K^{-1} H^{-1} \subseteq (HK)^{-1}$ .... (2)

From (1) and (2), we get

$(HK)^{-1} = K^{-1} H^{-1}$

Note: we are having another proof of the theorem 2.1.8

Theorem 10: If H and K are two subgroups of a group G, then HK is a subgroup of G iff HK = KH.

Proof, Firstly, let HK = Kh. To show that HK is a subgroup of G

It is sufficient to show that $(HK)(HK)^{-1} = Hk$

we have $(HK)(HK)^{-1} = (HK)(K^{-1}H^{-1}) = H(KK^{-1}) H^{-1} = (HK)H^{-1}$

[$\because$ K is a subgroup of G $\quad\therefore\quad KK^{-1} = K$]

$= (KH)H^{-1}$

$= K(HH^{-1})$

$= KH$ [$\because$ H is a subgroup of G $\therefore HH^{-1} = H$]

$= HK.$

Thus HK is a subgroup of G.

Conversely:

Suppose HK is a subgroup of G. To show HK = KH.

Now $(HK)^{-1} = HK$ [$\because$ if H is a subgroup of G then $H^{-1} = H$]

$\Rightarrow \quad K^{-1}H^{-1} = HK \quad \Rightarrow \quad KH = HK$

Cor. If H, K are subgroups of an abelian group G, then HK is a subgroup of G.

Proof: Since H, K are subgroups of an abelian group G. Then HK = KH

$\therefore$ By above theorem HK is a subgroup of G.

Consider following examples for its better understanding.

Example 14. Let Z be the additive group of integers and for any positive integer n, let H_n denote the set of all multiplie of n. Show the following:

(i) H_n is a subgroup of Z.

(ii) For any two positive integers m, n, if j and k are their H.C.F and L.C.M respectively, then

$H_j = H_m + H_n$ and $H_k = H_m \cap H_n$.

Solution: (i) Now $H_n = n\,Z = \{....., -3\,n, -2\,n, -n, 0, n, 2\,n, 3\,n,.....\}$

Clearly H_n is a non-empty subset of Z, as $0 \in H_n$.

Let $a, b \in H_n$ be any two element then

$a = p_n$, $b = q_n$ for some $p, q \in Z$.

$\therefore \quad a - b = p_n - q_n = (p - q)\,n \in H_n$

$\therefore \quad a - b \in H_n, \quad \forall\ a, b \in H_n.$

Hence H_n is subgroup of Z.

(ii) Let HCF {m, n} = j and LCM {M, n} = k.

We show that $H_m + H_n = H_j$ and $H_m \cap H_n = H_k$.

Now by part (i) H_m, H_n, H_j are subgroups of Z.

Moreover, $H_m + H_n = H_n + H_m$ [$\because$ Z is abelian group]

$\Rightarrow$ $G_m + H_n$ is a subgroup of Z.

Let $x \in H_m + H_n \Rightarrow x = a_m + b_n$, for some $a, b \in Z$.

Since $j = HCF\{m, n\} \Rightarrow j/m$ and $//n \Rightarrow j/am + bn$

$\Rightarrow j/x \Rightarrow x \in H_j$

$\therefore H_m + H_n \subseteq H_j$.

Again, let $y \in H_j \Rightarrow y = t\,j = t\,(am + bn) = t\,am + t\,bn \in H_m + H_n$.

$\therefore H_j \subseteq H_m + H_n$.

Thus $H_j = H_m + H_n$.

Secondly, because $H_m H_n H_j$ are subgroups of Z.

Also intersection of two subgroups is a subgroup.

$\therefore$ $H_m \cap H_n$ is a subgroup of Z.

Let $x \in H_n \Rightarrow x \in H_m$ and $x \in H_n$

$\Rightarrow x = a\,m$ and $x = b\,x$ for some $a, b \in Z$.

Since $k = LCM\{M, n\} \Rightarrow m/k$ and n/k

$\Rightarrow am/ak$ and bn/bk

$\Rightarrow x/ak$ and x/bk

$\Rightarrow x/(ak, bk)$

$\Rightarrow x/k\,(a, b)$

$\Rightarrow x \in H_k$.

$\therefore H_m \cap H_n \subseteq H_k$

Again, let $y \in H_k \Rightarrow y = t\,k$, for some $t \in Z$

$y = t\,(mp)$ [$\because m/k \Rightarrow k = mp$ for some $p \in Z$]

$= m\,(tp)$

$\Rightarrow y \in Hm$.

Similarly $y \in H_n$, for $y = tk$ and n/k

$\Rightarrow k = nq$ for some $q \in Z$

$\therefore y \in H_m \cap H_n$.

$\therefore y = t\,(nq) = (tq)\,n \in H_n$

$\therefore H_k \subseteq H_m \cap H_n$.

Thus $H_k = H_m \cap H_n$.

Example 2: Let G be an abelian group, let n be a fixed positive integer. Let $G^n = \{g^n : g \in G\}$. Prove that G^n is a subgroup of G. Give an example showing that G^n need not be a subgroup of G when G is non-abelian.

Solution: Clearly $G^n \neq \phi$, for $e = e^n \in G^n$.

Now, let $x, y \in Gn$ be any two elements such that $x = g_1^n$, $y = g_2^n$,, where $g_1, g_2 \in G$.

Now $xy^{-1} = g_1^n (g_2^n)^{-1} = g_1^n g_2^{-n} = (g_1 g_2^{-1})^n \in G^n$.

$[\because g_1, g_2 \in G \Rightarrow g_1 g_2^{-1} \in G]$

Hence G^n is a subgroup of G.

Next, consider the group $S_3 = \{i, (12), (13), (23), (123), (132)\}$

Now $S_3^3 = \{g^3 : g \in S^3\} = (t^3, (12)^3, (13)^3, (23)^3, (123)^3, (132)^3\}$

$= \{i, (12), (13), (23)\}$.

But S_3^3 is not a subgroup of S_3, for $(12), (13) \in S\frac{3}{3}$ but

$(12)\,(13) = (123) \notin S_3^3$

Example 3: Let H be a sub-group of a group G. Prove the following:

(i) For any $x \in G$, $x^{-1}Hx = \{x^{-1}hx : \text{for all } h \in H\}$ is a subgroup of G.

(ii) $O(H) = O(x^{-1}Hx)$, if H is a finite subgroup of G.

Solution: (i) Since $e = x^{-1} ex \Rightarrow e \in x^{-1}Hx$

$\therefore$ $x^{-1} H x$ is a non-empty subset of G.

$[\because \forall\, x^{-1} h x \in x^{-1} H x$ where $x, h \in G$ as $H \subseteq G$ and G is a group

$\therefore x^{-1}hx \in G$ i.e. $x^{-1} H x \subseteq G]$

Let $a, b \in x^{-1} H x$ be any two elements.

Then $a = x^{-1} h_1 x$, $b = x^{-1} h_2 x$, for some $h_1, h_2 \in H$

Now $ab^{-1} = (x^{-1} h_1 x)(x^{-1} h_2 x)^{-1}$

$= (x^{-1} h_1 x)(x^{-1} h_2^{-1} x)$

$= x^{-1} h_1 (xx^{-1}) h_2^{-1} x$

$= x^{-1} h_1 h_2^{-1} x$ $[\because xx^{-1} = e]$

$= x^{-1} h_3 x$, where $h_3 = = h_1 h_2^{-1} \in H$

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

Thus $x^{-1} H x$ is a subgroup of G

(ii) Let $f : H \to x^{-1} H x$ be a map defined by $f(h) = x^{-1}hx, \forall h \in H$.

We show that f is one-one and onto map.

Clearly, for each $x^{-1}hx$

$\therefore$ f is onto.

Let $f(h_1) = f(h_2)$

Let $f(h_1) = f(h_2)$

$\Rightarrow$ $x^{-1} h_1 x = x^{-1} h_2 x$

$\Rightarrow$ $h_1 = h_2$ [By left and right cancellation law in G]

$\therefore$ f is one-one. Thus f is one-one onto.

$\Rightarrow$ $O(H) = O(x^{-1}Hx)$.

Example 4: Prove that if <H, $*$> is a sub-group of <G, $*$> and <K, $*$> is a subgroup of <H, $*$> is also a subgroup of <G, $*$>

Solution: Given K is a subgroup of H and H is a subgroup of G.

To show that K is also a subgroup of G.

Let a b $\in$ K be any elements.

$\Rightarrow$ a, b $\in$ G.

Also $b^{-1} \in K$ [$\because$ $K \subseteq H \subseteq G$]

$\Rightarrow$ $ab^{-1} \in G$

Thus K is a subgroup of G also.

Example 5: G be an abelian group, show that all elements of finite order in G form subgroup of G.

Solution: Let T = {a : a $\in$ G s.t. O (a) is finite}.

Clearly T $\neq \phi$, for e $\in$ T $\because$ O (e) = 1, a finite number.

Let a, b $\in$ T be any element s.t. O (a) = m and O (b) = n

i.e., $a^n = e = b^m$.

Now $(ab)^{mn} = a^{mn}b^{mn} = (a^n)^m . (b^m)^n = e^m . e^n = e^m . e^n = e.e = e$

$\therefore$ O (a b) is also finite $\Rightarrow$ a b $\in$ T.

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

$\therefore$ if a $\in$ T$\Rightarrow$ $a^{-1} \in$ T.

Hence T is a subgroup of G.

Note: The above group is known as the torsion subgroup of a group.

Example 6: Show that a group can never be expressed as the union of two of its proper subgroups.

Solution: Let G = H U K, where H and K are proper subgroups of G.

Clearly, $H \subseteq K$ and $K \subseteq H$.

$\therefore$ We can choose $a \in H$ s.t. $a \notin K$ and $b \notin K$ s.t. $b \notin H$.

Also then $a, b \in H \cup K$ and since H U K is a group $\Rightarrow$ $ab \in H \cup K$

$\Rightarrow$ $ab \in H$ or $ab \in K$

If $ab \in H$ then $a^{-1}(ab) \in H$ i.e., $b \in H$, a contradiction

and if $ab \in K$ then $(ab)b^{-1} \in K$ i.e., $a \in K$, a contradiction.

So our supposition is wrong.

Hence group cannot be expressed as union of two of its proper subgroup.

Example 7: Let G be the group of all 2×2 non-singular matrices over the reels.

Find the centre of G.

Solution: Here $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}; a,b,c,d \in R \, s.t. \, ad - bc \neq 0 \right\}$

Now by definition of C (G),

$C(G) = \{g \in G | gx = xg, \quad \forall x \in G\}$.

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C(G)$ be any element. Then it should commutate with all elements of G.

In particular it commutes with $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in G$.

$\Rightarrow$ $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\Rightarrow$ $\begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$

$\Rightarrow$ $b = c, a = d$.

Also $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\Rightarrow \quad \begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix} = \begin{bmatrix} a & b \\ a+c & b+d \end{bmatrix}$

$\Rightarrow$ a + b = a, b = c = 0 [using (1)]

Hence $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in$ C (G) is of the form $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$

Hence C (G) = $\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \neq 0 \in R \right\}$

Example 8: Find all the subgroups of S_3.

Solution: Since S_3 = {i, (12), (13), (23), (123), (132)}.

All the subgroups of S_3 are

H_1 = {i, (12)}, H_2 {i, (13)}, H_3 = {i, (23)}, and H_4 = {i, (123), (132}

Self Check Exercise - 3

Q.1 Show that (2Z)Z) = 6Z < Z

Q.2 Let H = {I, (1, 2, 3), (1, 3, 2), (1, 3, 2)} and K = {I, (1, 2)}

Check whether or not HK < S_3. If it is,

Find O(HK). Find O (H∩K)

6.6 Summary:

In this unit you studied about

1. Subgroup, its definition and various examples
2. Elementary properties of subgroup with their explanatory exaples.
3. Theorems based on subgroups
4. Set operations like Union, intersection and product of two subgroups along with the theorems and examples.

6.7 Glossary:

- **Abelian Group:**A group g is abelian of for all elements a, b $\in$ G, the following commutative properly holds.

  a∗b = b∗a, where '∗' is the binary operations associated with G.

- **Subgroup:**Let G be a group with operation '∗'. A non-empty subset H$\subseteq$G is called a subgroup of g if H itself is a group under the operation '∗'.

- **Non-Abelian Group:**A Group G with operation '∗' is called non-abelian group, there exist a, b $\in$ G. Such that a ∗ b ≠b∗ a.

6.8 Answers to Self Check Exercise

Self Check Exercise - 1

Q.1 Yes, {1, -1} and {1, -1, i, -1} are abelian subgroups of non abelian Quaternion group.

Q. 2 Yes, It is a proper subgroup of Z.

Self Check Exercise - 2

Q. 1 Yes, $Z\sqrt{3}$ is a subgroup of R

Q. 2 Yes, $Z\sqrt{6}$ is a subgroup of R.

Q. 3 No, it is not a subgroup of 10th root of unity.

.	1	w^2	w^4	w^8
1	1	w^2	w^4	w^8
w^2	w^2	w^4	w^6	w^{10}
w^4	w^4	w^6	w^8	w^{12}
w^8	w^8	w^{10}	w^{12}	w^{16}

Also $w^2 . w^4 = w^6$

[as $w^3 = 1$

$(w^3)^2 = 1$ as son on

Self Check Exercise - 3

Q.1 $2Z = 2m, m \in Z.$

$3Z = 3n, n \in Z.$

Now $(2Z)(3Z) = (2m)(3n)$

$= 6mm, m, n \in Z$

Again $6Z = 6z, z \in Z$

$= (2.1)(3.z)$

$= 2Z. 3z$

Thus $(2Z)(3z) = 6Z$

Thus product of two subgroups of Z is a subgroup of Z.

Q. 2 As O(H) = 3, O(K) =2, O(H∩K) = 1 as only I is common element

$O(HK) = \frac{O(H)O(K)}{O(H \bigcap K)} = \frac{3 \times 2}{1} = 6 = O(S_3)$.

Since order is same so [$HK \leq S_3$]

6.9 References/Suggested Readings:-

1. Vijak. K. Khanna and S.K. Bhambri, A course in Abstract Algebra.
2. Joseph A Gallian, Contemporary Abstract Algebra.
3. Frank Ayrer Jr. Modern Algebra, Schaum's Outline Series.
4. A.R. Vasistha, Modern Algebra, Modern Algebra, kushan Prakashan Media.

6.10 Terminal Questions

1. Let G be on abelian group with identity e show that

   H = { $x \in G : x^2 = e$} is a subgroup of G

2. Show that the elements of a group G which commute with the square of given element a from a subgroup H of G and which commute with a itself form a subgroup of G.

*****

Unit - 7

Cosets and Lagrange's Theorem

Structure

7.1 Introduction

Dear Students in this unit you will study about the equivalence relations defined or group, corresponding to each of its subgroups. You will also study the importance of the partitioning of a group into the equivalence classes, called Cosets. We will use the concept of Coset to prove a very important theorem known as Lagrange's theorem, which is named after a French Mathematician Lagranges. You will also study about the index of a subgroup.

7.2 Learning Objectives

After studying this unit, students shall be able to

1. Define and give examples of coset both left and right.
2. State and prove Lagerange's theorem.
3. Apply Lagrange's Theorems on mathematical questions.

Introduction

In group theory, a coset is subject of a group obtained by multiplying each element of a subgroup by a fixed element of the group. The cosets of a subgroup partition the group into distinct subsets or we can say the cosets are disjoint and their union is equal to the whole group. The number of Lay cosets is equal to right cosets, and this number is known as index of the subgroup.

Cosets Lays important role in defining other types of groups like quotient group.

7.3 COSETS

Dear students, we have already discussed about the product of two subgroups. Here we will study the case when one of the subgroup, for the product, is a single element. Here we take product of the subgroup of G i.e. H with an element of a group G.

Definition of Coset

Let H be a subgroup of a group G and let $a \in G$

1. Then the set $Ha = \{ha : h \in H\}$ is called a right coset of H in G determined by a.
2. The set $a H = \{ah : h \in H\}$ is called the left coset of H in G determined by a.

If the operation is addition, then above defining becomes. Let H be a subgroup of a group G and let $a \in G$

1. $H+a = \{h+a; h \in H$, is called a right coset of H in G determined by a
2. $a + H = \{a+h; h \in H$, is called left coset of H in G determined by a

Notes : 1 If H is a subgroup of a group G, Then H itself is a right as well as left coset of H of G determined. If e is identity element of the group G, Then he and eH are right and lay coset of H in G

Also $He = \{he : h \in H\} = \{h ; h \in H\} = H$

$eH = \{eh : h \in H\} = \{h : h \in H\} = H$

2. When G is an abelian group then there is no distinction between a left and right cosets.

Let us take following examples to more understanding

Example 1 What are the right cosets of uZ in (Z,+)

Solution : Here the group G is Z and the subgroup H is uZ and the operation is addition.

Since the elements of Z are $= \{-4, -3, -2, -1, 0, 1, 2, 3, 4.....\}$

$= 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, ...$

and H = uz $= \{-16, -12, -8, -4, 0, 4, 8, 12, 16, ...\}$

$= \{0_1, \pm 41, \pm 81, \pm 121, \pm 161, ...$

So to find the right cosets of uz in z we have to add element of z in H, Let us start from 0

$\therefore H+0 = \{h+0, h \in H\} = \{0+0, \pm 4+0, \pm 8+0, \pm 12+0,.....\}$

$= \{0, \pm 4, \pm 8, \pm 12, ...\} = H$

H+1 = {0+1, +4+1, -4+1, +8+1, -8+1, +12+1, -12+1, ...}

= {1, 5, -3, 9, -7, 12, -11}

= {......., -11, -7, -3, 1, 5, 9, 13,.....}

Now H-1 = {0-1, +4-1, -4-1, +8-1, -8-1, +12-1, -12-1, ...}

= {-1, 3, -5, 7, -9, 11, -13, ...}

= {......., -13, -9, -5, -1, 3, 7, 11,.....}

H+2 = {0+2, +4+2, -4+2, +8+2, -8+2, +12+2, -12+2, ...}

= {2, 6, -2, 10, -6, 14, -10, ...}

= {......., -10, -6, -2, 2, 6, 10, 14,.....}

H-2 = {0-2, +4-2, -4-2, +8-2, -8-2, +12-2, -12-2, ...}

= {-2, 2, -6, 6, -10, 10, -14, ...}

= {......, -14, -10, -6, -2, 2, 6, 10,.....}

H+3 = {0+3, +4+3, -4+3, +8+3, -8+3, +12+3, -12+3, ...}

= {3, 7, -1, 11, -5, 15, -9, ...}

= {......., -9, -5, -1, 3, 7, 11, 15,.....}

H-3 = {0-3, +4-3, -4-3, +8-3, -8-3, +12-3, -12-3, ...}

= {-3, 1, -7, 5, -11, 9, -15, ...}

= {......, -15, -11, -7, -3, 1, 5, 9,.....}

H+4 = {0+4, +4+4, -4+4, +8+4, -8+4, +12+4, -12+4, ...}

= {4, 8, 0, 12, -4, 16, -8, ...}

= {......., -8, -4, 0, 4, 8, 12, 16,.....} = H

H-4 = {0-4, +4-4, -4-4, +8-4, -8-4, +12-4, -12-4, ...}

= {-4, 0, -8, 4, -12, 8, -16, ...}

= {......, -16, -12, -8, -4, 0, 4, 8,.....} = H

H+5 = {0+5, 4+5, -4+5, 8+5, -8+5, 12+5, -12+5, ...}

= {5, 9, -1, 13, -3, 17, -7, ...}

= {......., -7, -3, 1, 5, 9, 13, 17,.....} = H+1

H-5 = {0-5, 4-5, -4-5, 8-5, -8-5, 12-5, -12-5, ...}

= {-5, -1, -9, 3, -13, 7, -17, ...}

= {......, -17, -13, -9, -5, -1, 3, 7,.....} = H-1

Also from above we find that

H+0 = H

H+1 = {....., -11, -7, -3, 1, 5, 9, 13,.....} = H-3

H+2 = {....., -13, -9, -5, -1, 3, 7, 11,.....} = H-2

H+3 = {....., -9, -5, -1, 3, 7, 11, 15,.....} = H-1

H+4 = {....., -8, -4, 0, 4, 8, 12, 16,.....} = H

H+5 = {....., -17, -13, -9, -5, -1, 3, 7,.....} = H-1

and so on,

Therefore, the distinct right cosets of H in G are

H, H+1, H+2, H+3

Note :- In above example $O \in H+x$, if and only if $x \in H$. Thus H+x is not a sub group of a unless $x \in H$. Here H+1, H+2 are not subgroups of G.

Example 2 Find the right cosets of the subgroup {1, -1} of the group {1, -1, i, -i} under multiplication.

Solution : Here of set G = {1, -1, i, -i} under operation of multiplication and the subgroup H = {1, -1}

Therefore, right coset of H in G are H.1, H.(-1), H.(i) and H. (-i)

Now, H.1 = {1.1), (-1.1)} = {1, -1} = H

H.(-1) = {1.-1), (-1.-1)} = {-1, 1} = {1, -1} = H

H.(i) = {(1.i), -1.i)} = {i, -i}

H.(-i) ={1.(-i), -1.(-i)} = {-i, i} = H(i)

$\therefore$ the distinct cosets of H in G are H and Hi

Example 3 : Find all left and right cosets for S_3 symmetric group on {1, 2, 3} of subgroup H = {I, (1, 2)}

Solution : Here G = S_3 = {I, (1 2), (1 3), (2, 3) (1 3 2)} and given H = {I_1 (1, 2)}

binary composition of symmetric group is composition of function

Now the left cosets of H in G = S_3 are

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

(1 2).H = $\left\{\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\begin{pmatrix}I & 2\\ I & 2\end{pmatrix},\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\right\} = \left\{\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix},\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}\right\}$ = {(1 2), I} = H

(1 3).H = $\left\{\begin{pmatrix}1 & 3\\ 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix},\begin{pmatrix}1 & 3\\ 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\right\}$

= {(1 3) , (1 3 2)} ∵ (1 2 (1 3) = (1 2 3)

(2 3).H = $\left\{\begin{pmatrix}2 & 3\\3 & 2\end{pmatrix}\begin{pmatrix}1 & 2\\1 & 2\end{pmatrix},\begin{pmatrix}2 & 3\\3 & 2\end{pmatrix}\begin{pmatrix}1 & 2\\2 & 1\end{pmatrix}\right\}$

= {(2 3) , (1 2 3)} ∵ (1 2 3) = (2 3) (1 2)

(1 2 3). H = $\left\{\begin{pmatrix}1 & 2 & 3\end{pmatrix}I,\begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\2 & 1\end{pmatrix}\right\}$

= $\left\{\begin{pmatrix}1 & 2 & 3\end{pmatrix},\begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}\right\}$

= {(1 2 3), (2 3)} = (2 3). H

(1 3 2).H = $\left\{\begin{pmatrix}1 & 2 & 3\end{pmatrix}.I,\begin{pmatrix}1 & 3 & 2\\3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\2 & 1\end{pmatrix}\right\}$

= $\left\{\begin{pmatrix}1 & 2 & 3\end{pmatrix},\begin{pmatrix}1 & 3 & 2\\3 & 1 & 2\end{pmatrix}\right\}$

= {(1 2 3), (1 3)} = (1 3). H

Therefore the distinct left cosets of H in S_3 are.

H, (13)H and (23).H

Now right cosets of H in $S_3$are :

H.I = {I.I., (1.2) I}

= {I, (1, 2) = H

H.(1 2) = {I.(1 2), (1 2). (1 2)}

= $\left\{\begin{pmatrix}1 & 2\end{pmatrix},\begin{pmatrix}1 & 2\\1 & 2\end{pmatrix}\right\}$ = {1, 2), I}

H.(1 3) = {I. (1 3), (1 2). (1 3)}

={(1 3), (1 2 3)}

H.(2 3) = {I. (2 3), (1 2). (2 3)}

={(2 3), (1 2 3)}

H.(1 2 3) = {I.(1 2 3), (1 2).(1 2 3)}

= $\left\{\begin{pmatrix}1 & 2 & 3\end{pmatrix},\begin{pmatrix}1 & 2\\2 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}\right\}$

$$= \left\{ \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

= {(1 2 3), (1 3)} = H.(1 3)

H. (1 3 2) = {I. (1 3 2), (1 2) (1 3 2)}

$$= \left\{ \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

= {(1 3 2) (2 3)} = H.23

Therefore distinct right cosets of H in S_3 are H, H.(1 3) and H (2 3)

Example 4 : Find the left cosets of the subgroup H = {1,-1, i,-1} of the group G = {$\pm 1, \pm i \pm k$} under multiplication.

Solution : The left coset of H in G are

1 H = {1.1, 1.-1, i.i, 1.-i} = { 1, -1, i, -i} = H

-1 H = {-1.1, -1.-1, -i.i, -1.-i} = {-1, 1, -i, i} = H

i H = {i.1, i.-1, i.i, i.-i} = {i, -i, 1, -1} = H $\quad \because i^2 = -1 \quad -i^2 = 1$

-i H = {-i.1, -i.-1, -i.i, -i.-i} = {-i, i, 1, -i} = H

j H = {j.1, j.-1, j.i, j.-i} = {j, -j, -k, k}

-j H = {-j.1, -j.-1, -j.i, -j.-i} = {-j, j, k, -k} = j H

k H = {k.1, k.-1, k.i, k.-i} = {k, -k, -j, j} = j H

-k H = {-k.1, -k.-1, -k.i, -k.-i} = {-k, k, j, -j} = j H

So the distinct left cosets of H in G are H and i H.

Self Check Exercises - 1

Q.1 Let <G, +> be additive group of integer and H be set of all integer multiple of 5. Find all right cosets of H in G.

Q. 2 Find all left and right cosets of H = {I, {1, 2, 3}} in S_3.

Q. 3 Let H = {1, -1} be a subgroup of G = {$\pm 1, \pm i, \pm j, \pm k$}. Find all its left and right cosets.

Q. 4 Let G be group of integers under addition and H be subgroup of G having even integers. Find all right cosets of H in G.

Q. 5 Let (G, +) be a additive group of integers and H be the set of all integral multiple of 3. Prove that H is a subgroup of G and find all the cosets of H in G.

7.4 Theorems on cosets

In this section we will discuss some important theorems based on cosets :

Theorem 1 (i) $H\alpha = H$ iff $\alpha \in H$.

(ii) $\alpha H = H$ iff $\alpha \in H$.

where H is a subgroup of G.

Proof (i) We prove that $H\alpha = H$ iff $\alpha \in H$.

Firstly, suppose that $H\alpha = H$. ...(1)

Since H is a subgroup of G, so $e \in H$, where e is the identity element of H

$\therefore e\alpha \in H\alpha \quad \Rightarrow \quad \alpha \in H\alpha$

$\Rightarrow \quad \alpha \in H$ (From (1)

$\therefore H\alpha = H \quad \Rightarrow \quad \alpha \in H.$

Conversely, suppose that $\alpha \in H$.

We shall prove that $H\alpha = H$.

Let $x \in H\alpha$ be an arbitrary element.

$\therefore \quad x = h\alpha$ for some $h \in H$

$\therefore \quad h, \alpha \in H$

$\Rightarrow \quad h\alpha \in H$, since H is a subgroup of G

$\Rightarrow \quad x \in H$

$\therefore \quad x \in H\alpha \quad \Rightarrow x \in H$

$\Rightarrow \quad H\alpha \subseteq H.$ ...(2)

Now let $x \in H$. Since α also belongs to H and H is a subgroup

$\therefore \quad x\alpha^{-1} \in H$

$\Rightarrow \quad (x\alpha^{-1})\alpha \in H\alpha$

$\Rightarrow \quad x(\alpha^{-1}\alpha) \in H\alpha$

$\Rightarrow \quad x \in H\alpha$

$\therefore \quad x \in H \quad \Rightarrow \quad x \in H\alpha$

$\Rightarrow \quad H \subseteq H\alpha.$ ...(3)

From (2) and (3), we get H a = H.

(ii) Its proof is similar to (i).

Theorem 2 (i) $H\alpha = Hb$ iff $\alpha b^{-1} \in H$.

(ii) $\alpha H = bH$ iff $\alpha^{-1} b \in H$.

Proof (i) We prove that $H\alpha = Hb$ iff $\alpha b^{-1} \in H$.

Firstly, let $H\alpha = Hb$

Since H is a subgroup of G, so $e \in H$,

$\therefore e\alpha \in H\alpha$ i.e., $\alpha \in H\alpha$

$\Rightarrow$ $\alpha \in Hb$, since $H\alpha = Hb$

$\Rightarrow$ $\alpha \in hb$ for some $h \in H$

$\Rightarrow$ $\alpha b^{-1} = (hb)^{-1} = h(bb)^{-1} = he = h \in H$

$\therefore$ $\alpha b^{-1} \in H$.

Conversely, let $\alpha b^{-1} \in H$.

We shall prove that $H\alpha = Hb$.

Since $\alpha b^{-1} \in H$, so $\alpha b^{-1} = h$ for some $h \in H$

$\Rightarrow$ $\alpha(b^{-1}b) = hb$

$\Rightarrow$ $\alpha e = hb$

$\Rightarrow$ $\alpha = hb$

$\therefore$ $H\alpha = H(hb)$

$= (Hh)b$

$= Hb$, since $h \in H$, so $Hh = H$.

(ii) Its proof is similar to that of (i).

Theorem 3 : Any two right (or left) cosets are either disjoint or identical.

Proof. Let H be a subgroup of a group G. Let $H\alpha$ and Hb be two right cosets of H in G, so that $a, b, \in G$.

We shall prove that either $H\alpha = Hb$ or $Ha \cap Hb = \phi$

If $H\alpha \cap Hb = \phi$, then we have noting to prove.

So, let $H\alpha \cap Hb \neq \phi$.

In this case we shall prove that $H\alpha = Hb$.

Since $H\alpha \cap Hb \neq \phi$, so $\exists$ at least one $x \in H\alpha \cap Hb$

$\therefore$ $x \in H\alpha$ and $x \in H\alpha \cap Hb$

$\Rightarrow$ $h_1^{-1}(h_1\alpha) = h_1^{-1}(h_1 b)$

$\Rightarrow$ $(h_1^{-1}h_1)\alpha = (h_1^{-1}h_1)b$

$\Rightarrow$ $e\alpha = h_3 b$, where $h_3 = h_1^{-1}h_2 \in H$.

$\Rightarrow$ $\alpha = h_3 b$

$\Rightarrow$ $H\alpha = H(h_3 b)$

$= (Hh_3)b$

= H b since $h_3 \in$ H, So H h_3 = H

$\therefore$ H α = H b.

$\therefore$ If H $\alpha \cap$ H $b \neq \phi$, then H α = H b.

So, either H $\alpha \cap$ H $b = \phi$, or H α = H b.

Theorem 4 The group G is equal to the union of all right cosets of H in G.

Proof. Let e, a, b, c, ...

$\therefore$ H e = H, H a, H b, H c, ... are all the right cosets of H in G

We shall prove that G = H U H a U H b U H c U .....

Let $x \in$ G be any element.

$\therefore$ H $x$is a right coset of H in G.

Since H is a subgroup of G, so $e \in$ G, where e is the identity element of G.

$\therefore$ $ex \in$ H x i.e., $x \in$ H x

$\Rightarrow$ $x \in$ H U a U H b U H c U.....U Hx U.....

$\therefore$ G $\subseteq$ H U a U H b U H c U..... ...(1)

Conversely, let H a be any right coset of H in G, where a $\in$ G.

Let $x \in$ H a

$\therefore$ x= ha for $h \in$H.

Since $h \in$H

$\therefore$ $h \in$ G also $a \in$ G

$\Rightarrow$ $ha \in$ G

$\Rightarrow$ $x \in$ G

$\therefore$ $x \in$ H a $\Rightarrow x \in$ G

$\Rightarrow$ H $a \subseteq$ G

$\therefore$ $\bigcup_{a \in G}$ H $a \subseteq$ G

$\Rightarrow$ H U a U H b U H c U.....$\subseteq$ G ....(2)

From (1) and (2), we get

$\therefore$ G = H U a U H b U H c U.....

Theorem 5. There is one to one correspondence between any two right cosets of H in G.

Proof. Let H a, H b be two right cosets of H in G, where a, $b \in$ G.

Define a map f : H $a \rightarrow$ H b by

$f(ha) = hb, \ \forall ha \in H\ a.$

f is one-one. Let x, y $\in$ H a such that $f(x) = f(y)$

Since x , y $\in$ H a

$\therefore$ $x = h_1 a$ and $y = h_2 a$ for some $h_1, h_2 \in$ H.

$\therefore$ $f(x) = f(y) \Rightarrow f(h_1 a) = f(h_2 a)$

$\Rightarrow h_1 b = h_2 b$

$\Rightarrow h_1 = h_2$

by the right cancellation law in the group G.

$\Rightarrow h_1 a = h_2 a$

$\Rightarrow x = y$

$\Rightarrow$ f is one-one

f is onto. Let y $\in$ H b

$\therefore$ y = h b for some h $\in$H

Take $x = ha.$

Since $h \in$H, so h a $\in$ H a

$\Rightarrow$ $x \in$ H a, where $x = ha \in$ H a

$\therefore$ $f(x) = f(ha) = h\ b = y$

$\therefore$ f is onto.

$\therefore$ f : H $a \rightarrow$ H b is one-one and onto.

$\therefore$ H a, H b are in one-one correspondence.

Cor, if H is a finite subgroup of G. Then O (H a) = O(H).

Proof. Since by property V above, there is one-one correspondence between any two right cosets of H in G. In particular there is one-one correspondence between H and H a.

O (H a) = O(H).

Theorem 6. There is one-one correspondence between the set of left cosets of H in G and the set of right cosets of H in G.

Proof. Let L and M be respectively the set of left cosets and right cosets of H and G.

$\therefore$ L = {aH :$a \in$ G} and M = {H a : $a \in$ G}

Define a map f: L $\rightarrow$ M by

$f(a\ H) = H\ a_{-1}, \ \forall a \in G.$

If $a \in$ G, then $a^{-1} \in$ G and hence H $a^{-1} \in$ M.

$\therefore$ f is a map from L to M.

We now prove that f is well defined

Let a, b $\in$ G such that a H = b H.

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

$\Leftrightarrow$ H $a^{-1}b$ = H

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

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

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

$\Leftrightarrow$ H $a^{-1}e$ = H b^{-1}

$\Leftrightarrow$ H a^{-1} = H b^{-1}

$\Leftrightarrow$ f(a H) = f (b H).

$\therefore$ f is well-defined.

The reverse steps shows that f is one-one.

We finally prove that f is oneto.

Let H a $\in$ M be arbitrarily .

$\therefore$ $a \in$ G. $\Rightarrow$ $a^{-1} \in$ G.

$\Rightarrow$ a^{-1} H $\in$ L, such that f(a^{-1} H) = H $(a^{-1})^{-1}$ = H a.

$\therefore$ f is onto.

$\therefore$ the mapping f : L $\rightarrow$ M is in one-one and onto.

$\Rightarrow$ The set of left cosets of H in G and the set of right cosets of H in G are in one-one correspondence.

Theorem 7 (H a)$^{-1}$ = a^{-1} H, where $a \in$ G.

Proof. Let $x \in$ (H a)-1

$\therefore$ x= y^{-1} for some y $\in$ H a.

Now, y $\in$ H $a \Rightarrow$ y = ha for some $h \in$ H.

$\therefore$ x= y^{-1} = (ha)$^{-1}$ = $a^{-1}h^{-1}$

Since $h \in$ H and H is a subgroup, $\therefore h^{-1} \in$ H.

$\therefore$ $a^{-1}h^{-1} \in a^{-1}$ H

$\Rightarrow$ $x \in a^{-1}$ H

$\therefore$ $x \in$ (H a)$^{-1} \Rightarrow x \in a^{-1}$H

$\Rightarrow$ (H a)$^{-1} \subseteq$ a^{-1} H. ...(1)

Now, let $x \in a^{-1}$ H.

$\therefore$ $x = a^{-1} h$ for some $h \in H$

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

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

Now $h \in H \Rightarrow h^{-1} \in H$, since H is a subgroup

$\Rightarrow$ $h^{-1} a \in H a$

$\Rightarrow$ $(h^{-1}a)^{-1} \in (H a)^{-1} \Rightarrow x \in (H a)^{-1}$

$\Rightarrow$ $x \in (a^{-1}H) \quad \Rightarrow x \in (H a)^{-1}$

$\Rightarrow$ $a^{-1} H \subseteq (H a)^{-1}$. ...(2)

From (1) and (2), we get

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

Note : For $n \in N$, the distinct right cosets of nz in z under addition are nz, nz+1, -nz+(n-1).

Similarly under addition distinct left cosets of nz in z are nz, H-nz, 2+nz, ...(n-1) + nz.

Using above not we can, say that the right cosets of 4z in z (as in example 1) are H, H+1, H+2, H+3. For Higher values of $n \in N$ the cosets becomes identical with these distinct cosets for example :

$4z + 57 = 4z + 1 = H+1$

$\because \quad 57 \equiv 1 \pmod 4$

again $4z - 26 = 4z + 2 = H + 2$

$\because -26 \equiv 2 \pmod 4$

also $4z + 96 = 4z+0 = H+0 = H$

$\because 96 \equiv 0 \pmod 4$

Example 1:- Prove that Union of two distinct right cosets of a group is equal to a group, liking example.

Solution : Since for H_2 {I, (12)} be a subgroup of a of S_3, Then the distinct light cosets of H in a are H, H(13) and H(23). then.

H U H (13) U H (23)

= H U {(13), (123)} U { (23), (132)}

= {I, (12)} U {(13), (123)} U {(23), (132)}

= {I, (12), (13), (23), (123), (132) } = S_3

Example 2:- To prove that the distinct right cosets of of group S_3 for H_2 {I, (12)} are disjoint.

Solution : Since H_1 H(13) and H(23) are distinct cosets of H in S_3

To prove these cosets are disjoint H(23)

$H \cap H (13) \cap H (23)$

= (I, 12) ∩ {(13), (123)} ∩ {(23), (132)}

= ϕ

Example 3:- Let H = {11 a2} be a subgroup of group a = {a, a2, a3, a4 = 1}. Find all the left cosets of H in a. Also show that union of all these cosets is equal to a and any two costs are either identical or disjoint.

Solution:- Given H = {1, a^2)} is a subgroup of G = {a, a^2, a^3, a^4 = 1} How Lest cosets of H in a are

aH = a {1, a^2} = {a1, a.a^2} = {a. a^3}

a^2H = a^2 {1, a^2} = {a^2.1, a^2.a^2} = {a^2, a^4 = 1} = {a^2, 1} = H

a^3 H = a^3 {1, a^2} = {a^3.1, a^3.a^2} = {a^3, a^5} = {a^3, a^4.a} = { a^3, a} = aH

a^4 H2 IH = 1. {ϕ, a^2} = {1, a^2} = H.

$\therefore$ The distinct left cosets of H in a are H and aH.

To prove any two cosets are disjoint

Since H and aH are to distinct cosets, to prove they are disjoint, prove there intersicsetions is empty i.e.

H ∩ a H = {1, a^2} ∩ { a, a^3} = ϕ

To show Union of all cosets of H in G is equal to G

As H and H are two distinct cosets of H in G so liking union i.e. HUAH = {1, a^2} U { a,a^3} = { 1, a, a^2, a^3} = G.

Hence Proved

Example4 :- Prove that union of all distinct right cosets of 4Z in Z are gives Z and any two cosets are either identical or disjoint.

Solution :- For example 1, we know that distinct right cosets of 4Z in Z are H1 H+1, H+2 and H+3. To prove, two distinct cosets are disjoint, Let us take H and H+1, to prove H ∩ H + 1 = ϕ

Since H = {0, ± 4, ± 8 ± 12, ± 16, + ...}

H + 1 = {-11, -7, -3, 1, 5, 9, 13 .....}

H ∩ H + 1 = { --, -8, -4, 0, 4, 8, --} ∩ {....., -11, -7, -3, 1, 5, 9 .....} = ϕ

Similarly we can prove it for others also.

Now to prove that Union of all distinct coset of H in G gives

G i.e. H U H + 1 U H + 2 U H + 3 = Z

Let = {-8, -4, 0, 4, 8 ....} U {.....m -11, -7, -3, 1, 5, 9, 13 ---.}

U { ----, -10, -6, -2, 2, 6, 10, 14 -----}

U { --- -9, -5, -1, 3, 7, 11, 15, ---}

= {- - - , -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 7, 8}

= {0, ± 1, ± 2, ± 3, ±, 4, ± 5, ± 6, ± 7, ± 8 ----} = Z

Hence HUH + 1 U H + 2 U H + 3 = Z (set of inegers).

Self CheckExercises - 2

Q.1 Prove that subgroup H = {i, -i} of G = { ± 1, + i, ± j > ± k} has disjoint cosets and their union gives the set G.

Q.2 Prove that left coset of the subgroup H = {1, -1, *i*, -1} of G = {± 1, ± j, ± k } are disjoint and their Union gives the set G.

7.5 Index of A Subgroup :

Let H is a subgroup of a then the number of distinct let or distinct right costs is called the index of H in G. It is denoted by [a : H] or *i*a (H).

Note : The index of every subgroup of finite group is a divisor of the order of group. If k is index of H in G and n is order of finite group then n = mk. or k/n.

n = m k where m $\in$ Z.

order of G = order of H X index of H in G

or index of H in G = $\frac{order\ of\ a}{order of\ H} = \frac{0(a)}{0(H)}$

2. If the group G is an infinite group, then the quotient $\frac{0(a)}{0(H)}$ does not make sense. Infinite group may have subgroup of finite of infinite india.

For, **Example :- 1** [R : Z] = ∞ as the group G = R is infinite also the subgroup H is infinite.

2. Let H = { i, -i, 1, -1} be a finite subgroup of C complex numbers, as c is infinite, then [C : H] = infinite.

To have more Understanding of index of a subgroup of G, Let us take following examples, here we take previously solved question of cosets.

Examples 1. Find $|Z:4Z|$ i.e. index of 4Z in Z.

Solution : Here the group is Z and subgroup is 4Z Since the distinct cosets of 4Z in Z are,

H_1 H+1_1, H+2_1 H+3 = 4

So $|Z:4Z|$ = 4.

Example 2 Find the index of H = {11 - 1} in G = {1, - i, i, - i}

Solution Since the no of distinct coset of H in G are 2 therefore, index of H in G is 2 [From Example 2.]

Example 3 Find the index of H = {I, (1,2)} in S3.

Solution Since the distinct number of cosets of H in G are 3, therefore index of H in G is 3.

[From example 3.]

Example 4 Find the index of H = {1, -1, i, -i} of group

G = {± 1, ± i, ± j, ± k}.

Solution Since the distinct number of cosets of H in G are H and iH, only 2. So index of H in G is 2. [From example 4]

Self check exercise

Q.1 Find $|Z:5Z|$ 5

Q.2 Find $|4Z:12Z| = 3$

Q.3 Find $|S_3:<(12)>|$ 3

Q.4 Find $|Z_{12}:<4>| = 4$

Q.5 Find $|D_4:<t>| = 4$

7.6 Lagrange's Theorem

Lagrange's Theorem is a fundamental result in group Theory. This Theorem provides a relationship between the order of a finite group and order of its subgroups. Lagrange's Theorem provides a useful tool for studying to studying the structures and properties of finite group as well as for determining certain properties of subgroups within those group. Lagrange's theoreum has application in various are as of mathematics including number theory, ayptogrophy and combinations.

Statement of Lagdage'sTheorem : The order of each subgroup of a finite group is divisor of the order of group.

Proof : Let a be a group of finite order n

Let H be a subgroup of a and let 0(H) = m

Let order h_1, n_2 ----- h_m be m distinct members of H

If H - G, then there is nothing to prove.

But if H ≠ G,

Let a ∈ G. Then Ha is a right coset of H in G and by the definition of coset

Ha = {h_1a, h_2a, ... h_ma}

Ha has m distinct members,

If any two entries of W a are equal, then

hia - hj a with i ± j

hi = hj [using cancelation law]

which is a contradiction, as hi, h_2 ..... h_m are m distinct members of H

Since, any two distinct right coosets of H in G are disjoint, i.e. they have no element in common. Since [Theorem 3 of cosets] G is finite group, the number of distinct right cosets of H in G will be finite, Let it be equal to k.

Using, the result of theorem, i.e. the group G is equal to the union of all right cosets of H in G. [Theorem 4 of coset So the union os k distinct right cosets of H in G is equal to G, Therefore as Ha_1, Ha_2, Ha_3 ..... Ha_k are ok distinct right cosets of H in G then.

G = H U Ha_1U Ha_2 ..... U Ha_k

= No of elements in G = Numbers of elements in Ha_1

+ Number of element in Ha_2

+ ..... + Number of elements in Ha_k

As two distinct right cosets are mutually disjoint i.e. they have no common element. [Theorem 5 of coset as O(Ha) = O(H).

∴ No of element in G = mk {where m is order of H

= n = km

O(G) = k O(H)

=) O(H)| O(G)

∴ O(H) is a divisor of O(G)

Hence the proof of the theorem

Remarks 1. Lagrange's theorem immediately limits the possibilities of the subgroups of any given finite group. For example let G be a group of order 25, Alon it can only have subgroup of orders which are divisor of 25 i.e. 1, 5 & 25. It cannot have subgroup of order 2, 3, 10, 12 as non of these are divisor of 25.

To have more understanding of Lagrange's theorem Let us take following examples.

Example 1. What are the posible order of a subgroup of a group of order 30. Also list the corresponding no of cosets.

Solution : Since given a is a group of order 30. By using Lagrange's theorem, the possible order of its subgroup will be a divisor of 30, i.e. 1, 2, 3, 5, 6, 1, 15 and 30.

Also in order to find the number of cosets, we will use the result of index of a group i.e.

$$|G:H| = \frac{o(G)}{o(H)}$$

So index of a subgroup of are.

Index of subgroup of order 1 - = $\frac{30}{1}$ = 30

Index of subgroup of order 2 = $\frac{30}{2}$ = 15

Index of subgroup of order 3 = $\frac{30}{3}$ = 10

Index of subgroup of order 5 = $\frac{30}{5}$ = 6

Index of subgroup of order 6 = $\frac{30}{6}$ = 5

Index of subgroup of order 10 = $30/10$ = 3

Index of subgroup of order 15 = $30/15$ = 2

Index of subgroup of order 30 = $30/30$ = 1

Remark 2 Lagrange's Theorem cannot be generalised to infinite group since o(H)|o(G) is meaningful only for finite group. But an infinite group can have finite subgroup and infinite group can have a subgroup of finite index. As in example 1, (Z, +) is an infinite group but its subgroup H = 4Z, has finite number of cosets hamly H, H+1, H+2, H+3.

Example 2 : Let G be a group of order 300. H is a proper subgroup of G and K is a proper subgroup of H. If O(k) = 30 what are possible order of H? What would be the corresponding indices of H in G be.

Solution - Given O(G) = 300 & O(k) = 30,

H is proper subgroup of G $\Rightarrow$O(H) ≠ O(G)

K is proper subgroup of H $\Rightarrow$ O(k) ≠ O(H)

$\Rightarrow$ O(H) ≠ 30.

Since given K $\leq$ H $\leq$ G, So the possible subgroups of G should be a divisor of G, but K is subgroup of H of order 30. So order of H must be greater than 30, So the divisors of 300 which are greater than 30 are, 60 & 150

So possible order of H is either 60 or 150

$\therefore$ Index of subgroup of order 60 in G = $\frac{O(G)}{O(H)} = \frac{300}{60}$ = 50

and Index of Subgroup of order 150 in G = $\frac{O(G)}{O(H)} = \frac{300}{100}$ = 2

Example 3 - If H and k are subgroups of group G of order 12 and 35 respectively then find H ∩ k.

Solution Given $H \leq G$ and $k \leq G$

$o(H) = 12$ and $o(k) = 35$

Also $H \cap k \leq H$ and $H \cap k \leq k$

$\therefore$ $o(H \cap k)$ must be a factor of 12 and 35

Since 12 and 35 are co prime i.e. (12, 35) = 1

Hence $o(H \cap k) = 1$, So $H \cap k = e$.

Example 4. Find the possible order of subgroups of S_4, D_{10}, Q_8

Solution.

1. Since S_4 is a symmetric group of order 4!

   So $O(s_4) = 4! = 24$

   So possible order of the subgroups will be the divisor of 24, which are = 1, 2, 3, 4, 6, 8, 12, 24

2. Since D10 is a Dihedreal group of order 10 = 20 so $O(D_{10}) = 10 = 10$

   So posssible order of its subgroups will be its divisor of 10, which are = 1, 2, 5, 10,

3. Since Q_8 is a group of order 5

   $O(Q_8) = 8$

So possible order of its subgroups will be a divisor of 8, which are = 1, 2, 4, 8

In above example of we wish to find nontrivial proper subgroups then subgroup of order 1 and subgroups of order equal to order of group will be removed from the possible collection.

Converse of Lagrange's Theorem : If a is a finite group and m/ocg) then G has a subgroup of order m. The corvese of this theorem is not always true.

For example, Let G be a group under addition modulo 6

i.e. G = {0, 1, 2, 3, 4, 5}

o(G) = 6

Then the possible order of subgroup of G will be, = 1, 2, 3, 6

Let H = {0, 4}, o(H) = 2

and (O(H) |O(G) i.e. 2|6

But H = {0, 4} to be a subgroup it must be a subset of G under some binary operation

taking the element 4, $4+4 = 8 \equiv 2 (\text{mod } 6)$

but $2 \notin H$, so H is not a subgroup of G. Although O(H)| O(G).

Examples - What is the least order of a non-abelian group Prove that all proper subgroup of a group of order 8 must be abelian.

Solution : As we know that a group of order lesss than or equal to 4 are abelian. Also a group of prime order is also abelian. So the group of order 1, 2, 3, 4, 5 are all abelian So the least order of a non abelian group is 6.

Let G be a group of order 8 i.e. o(9) = 8

Subgroup of G will have the order 1, 2, 4, 8, but proper subgroup of G will have order 2 and 4 only. The group of order 2 and 4 are abelian. Since a subgroup is also a group, So all proper subgroup of a group of order 8 are abelian.

Theorem. 1 If H and K are finite subgroups of a group G, then

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

Proof : Since H and K are finite subgroups of a group G

$\therefore$ $D = H \cap K$ is also a finite subgroup of a group G.

Also $D = H \cap K \subseteq K$.

$\therefore$ D is a subgroup of a finite group K.

$\therefore$ The number of distinct right cosets of D in K is also finite.

Let α_1, α_2 .....$a_t \in K$ such that $D\alpha_1, D\alpha_2$,....., $D\alpha_t$ are the distinct and hence pairwise disjoint and right cosets of D and K.

Here, ℓ = The number of distinct right cosets of D in K.

= The index of D in K = $\frac{O(K)}{O(D)}$

$\therefore$ $\ell = \frac{O(K)}{O(D)}$

From (1), we get, $HK = H(D\alpha_1 \ D\alpha_2 \ \ldots\ldots D\alpha_\ell)$

$\Rightarrow$ $HK = H\left(\bigcup_{i=1}^{\ell} D\alpha_i\right) = \bigcup_{i=1}^{\ell} H(D\alpha_i) = \bigcup_{i=1}^{\ell} (HD)\alpha_i$

$= \bigcup_{i=1}^{\ell} H\alpha_i$, since D is subgroup of H, so HD = H.

$\therefore$ $HK = H\alpha_1 \cup H\alpha_2 \cup \ldots\ldots \cup H\alpha_t$

Now we prove that no two of $H\alpha_1 \cup H\alpha_2$ .....$H\alpha_t$are equal.

Let $H\alpha_i = H\alpha_j$ for some $1 < i, j < \ell$.

$\Rightarrow$ $\alpha_i\alpha_j^{-1} \in H$

Also $\alpha_i, \alpha_j \in K$

$\therefore$ $\alpha_i\, \alpha_j^{-1} \in K$

$\therefore$ $\alpha_\iota \alpha_j^{-1} \in K$

$\therefore$ $\alpha_\iota \alpha_j^{-1} \in H \cap K$

$\Rightarrow$ $\alpha_\iota \alpha_j^{-1} \in D$

$\Rightarrow$ $D\alpha_\iota = D\alpha_j$

Since $D\ \alpha_1, H\alpha_2, ..., D\alpha_\tau$ at are distinct

$\therefore$ $H\alpha_1, H\alpha_2, ..., H\alpha_\tau$ are distinct.

$\Rightarrow$ $H\alpha_1, H\alpha_2, ..., H\alpha_\tau$ are mutually disjoint. .....(4)

From (3) and (4), we get

$O(HK) = O(H\alpha_1) + O(H\alpha_2) + ... + O(H\alpha_t)$

$$= \frac{O(H)+O(H)+.....+O(H)}{\ell\ times}$$

Since H is a subgroup of a finite group G, so order of each right coset of H in G is equal to order of H.

$\therefore$ $O(HK) = l.\ O(H) = \frac{O(K)}{O(D)}.\ O(H)$ (From (2))

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

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

Theorem 2. Let G be a finite group and $\alpha \in$ G. then $O(\alpha) \mid O(G)$ i.e., the order of an element of a group is a divisor of the order of the group.

Proof. Let G be a finite group of order n Let $\alpha \in$ G and let $O(\alpha) = m$.

To prove that *m* is a divisor of *n*.

Let H = { ....., $\alpha^{-3}, \alpha^{-2}, \alpha^{-1}, \alpha^0, \alpha^1, \alpha^2, \alpha^3$, ...} be the subset of G consisting of all integral powers of α.

Then we know that H is a subgroup of G. We shall show that H contains only m distinct elements and that they are $\alpha, \alpha 2, \alpha 3, ..., \alpha\mu = \varepsilon = \alpha 0$.

Let $1 \leq r \leq m$, $1 \leq s \leq$ and $r > s$.

Then $\alpha^r = \alpha^s$

$\Rightarrow$ $\alpha^r \alpha^{-s} = \alpha^s \alpha^{-s}$ $\Rightarrow$ $\alpha^{r-s} = \alpha^0$ $\Rightarrow$ $\alpha^{r-s} = e$.

Thus there exists a positive integer r- s less than m such that $\alpha^m = e$. But *m* is the least positive integer such that $\alpha^m = e$. Therefore $\alpha^r \neq \alpha^s$. Thus $\alpha, \alpha^2, \alpha^3, ..., \alpha^m = \alpha^0 = e$ are all distinct elements of H.

Now suppose at is any element of H, where t is any integer. By division algorithm, we have t = m p + q, where p and q are some integers and $0 \leq q < m$.

We have $\alpha^t = \alpha^{mp+q} = \alpha^{mp}\alpha^q = (a^m)^p\alpha^q = e^p\alpha^q = \alpha^q$.

Since $0 \leq q < m$, therefore a^q is one of the m elements $\alpha, \alpha^2, ..., \alpha^m = \alpha^0$

Hence H has only m distinct elements. Thus order of H is m. By Lagrange's Theorem *m* is a divisor of *n*.

Cor. If G is a finite group of order n and $\alpha \in G$, then $\alpha^{O(G)} = e$ i.e. $\alpha^n = e$.

Proof. Let $O(\alpha) = m$, then by above Theorem 2.2.9

$\therefore$ $O(\alpha) \mid O(G) \Rightarrow m \mid n$.

Let $n = m\,k$, for some $k \in I$.

$\therefore$ $n = m\,k$, for some $k \in I$.

$\therefore$ $\alpha^n = \alpha^{m\,k} = (\alpha^m)^k = e^k = e. \quad \Rightarrow \quad \alpha^{O(G)} = e.$

Definition :Euler's Function ϕ

For any positive integer n, $\phi(n)$ is defined as follows :

$\phi(1) = 1$, and for $n > 1$ we have

$\phi(n)$ = The number of positive integers less than *n* and relatively prime to *n*.

If n = 6, then the positive integers less than 6 and relatively prime to 6 are 5 and 1

$\therefore$ $\phi(6) = 2$.

If p is a prime number, then all of 1, 2, ..., p - 1 are coprime with p.

$\therefore$ $\phi(p) = p - 1$, if p is a prime number

If *n* is any positive integer (n > 1), then we know

$n = p_1^{\alpha 1}\, p_2^{\alpha 2} ..... p_k^{\alpha k}$ where $p_1, p_2, ... p_k$ are distinct primes and $\alpha_i \in N$, then

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right).....\left(1-\frac{1}{p_k}\right)$$

Now $r_i^{\phi(n)} \equiv 1 \pmod n$

[$\because$ $r_1 \in G \Rightarrow r_1^{O(G)} = i$ in $G \Rightarrow r_1^{\phi(n)} - 1$ in $G \Rightarrow n \mid r_1^{\phi(a)} - 1$]

Hence $\alpha^{\phi(n)} \equiv 1 \pmod n$

so theorem is proved.

Theorem 3. Fermat's theorem

If p is a prime integer and α is any integer, then $\alpha^p \equiv \alpha \pmod p$.

Proof. Case I. $(\alpha, p) = 1$.

If $(\alpha, p) = 1$, then by Euler's theorem,

$\alpha\phi(p) \equiv 1 \pmod{p}$

$\Rightarrow \quad \alpha^{p-1} \equiv 1 \pmod{p}$, since p is prime number $\phi(p) = p - 1$.

$p \mid \alpha^{p-t} - 1$

$\Rightarrow \quad \alpha^{p-1} - 1 = k\,p$ for some integer k.

Multiplying throughout by α, we get

$\alpha^{p-1}\alpha - \alpha = \alpha\, k\, p$

$\Rightarrow \quad \alpha^{p} - \alpha = \alpha = \alpha\, k\, p$

$\Rightarrow$ p divides $\alpha p - \alpha$

$\Rightarrow \quad \alpha^{p} \equiv \alpha \pmod{p}$.

$\Rightarrow$ This complete the theorem in this case.

Case 2. $(\alpha, p) > 1$

Since p is *a* prime number, therefore the only divisors of p are 1 and p.

If $(\alpha, p) = d$, then $d \mid p$ and $d > 1$.

$\therefore \quad d = p$.

$\therefore \quad (\alpha, p) = p$

$\Rightarrow \quad p \mid \alpha$ also $\alpha \mid \alpha^{p}$

$\therefore \quad p \mid \alpha^{p}$ also $p \mid \alpha$

$\Rightarrow \quad p \mid d^{p} - \alpha$

$\Rightarrow \quad \alpha^{p} \equiv \alpha \pmod{p}$.

$\Rightarrow$ This complete the theorem in this case.

Let use try to apply these theorem on some examples.

Example : Find the remainder when 6^{41} is divided by 55.

Here n = 55 and a is 6

Solution : Since prime fectasiation of 55 is 55 = 5x11 where

5 and 11 both are prime.

So $\phi(55) = \phi(5)\,\phi(11)$ Using $\phi(mn) = \phi(m)\,\phi(n)$

$= 5x \left(1 - \frac{1}{5}\right) 11 \left(1 - \frac{1}{11}\right)$ Using the definition of ϕ function

$= 4 \times 10$

ϕ (55) = 40

Theorem 4 : Theorem (Euler's)

If n is a positive integer and a is any integer such that (a, n) = 1, n> 1

Prove $a^{\phi(n)} \equiv 1 (\text{mod } n)$

Proof : Consider G = {r | $r \in$ Z; (r, n) = 1, 1 $\leq r < n$]

G is a group under multiplication modulo n with identity element 1.

$\therefore$ O(G) = $\phi(n)$ (by definition of Euler's function $\phi(n)$)

When n = 1, then ϕ(n) = ϕ (1) = 1

$\therefore$ $a^{\phi(n)} = a^1 \equiv 1 (\text{mod } 1)$ ($\because 1 \mid a-1$)

When n > 1, then

$a = nq_1 + r_1$ for some integers q_1 and r_1, where $0 \leq r_1 < n$

If $r_1 = 0$, then $a = nq_1$

$\Rightarrow n$ divides a

$\Rightarrow (a, n) = n$

$\Rightarrow (a, n) > 1$ ($\because n > 1$)

which contradicts given

$\therefore r_1 \neq 0$ i.e. $1 \leq r_1 < n$

Let (r_1, n) = m

$\Rightarrow$ $m \mid r_1$ and $m \mid n$

$\Rightarrow$ $m \mid a - nq_1$ and $m \mid nq_1$

$\Rightarrow$ $m \mid a - nq_1 + nq_1$ and $m \mid n$

$\Rightarrow$ $m \mid a$ and $m \mid n$

$\Rightarrow$ $m \mid (a,n)$ $\Rightarrow m \mid 1 \Rightarrow m = 1$

$\therefore$ (r_1, n) = 1 and $1 \leq r_1 < n$

$\Rightarrow$ $r_1 \in G$

And $a = nq_1 + r_1$ $\Rightarrow a \equiv r_1 (\text{mod } n)$

$\Rightarrow a^{\phi(n)} \equiv r_1^{\phi(n)} (\text{mod } n)$

So here n is 55

and ϕ(55) = 40

Applying Euler's theorem i.e. $a^{\phi(n)} \equiv 1 (\text{mod } n)$

$6^{40} \equiv 1 (\text{mod } 55)$

$6^{40}.6 \equiv 6 (\text{mod } 55)$

$6^{41} \equiv 6 (\text{mod } 55)$

$\because$ or dividing 6^{41} by 55 we get remainder 6

Example 6 What is the remainder obtained on dividing 3^{47} by 23.

Solution : Here n = 33, a = 3, as n = 33 is prime, so $\phi(n) = n\left(-1 = \frac{1}{n}\right) = 22$

Applying $a^{d(n)} \equiv 1 (\text{mod } n)$

$3^{22} \equiv 1 (\text{mod } 23)$

$(3^{22})^2 \equiv (1)^2 (\text{mod } 23)$

$3^{44} \equiv 1 (\text{mod } 23)$

$3^{44}.3 \equiv 1.3 (\text{mod } 23)$

$\Rightarrow 3^{45} \equiv 3 (\text{mod } 23)$

$= 3^{45}.3^2 \equiv 9.3 (\text{mod } 23)$

$\Rightarrow 3^{47} \equiv 27 (\text{mod } 23)$

but as $27 \equiv 4 (\text{mod } 23)$

$\Rightarrow 3^{47} \equiv 4 (\text{mod } 23)$

Hence when we divide 3^{47} by 23 we get remainder 4.

Example 7. Use Fermat's theorem to determine the remainder when 8^{103} is divided by 103.

Solution. By Fermat's Theorems $a^p \equiv a (\text{mod } p)$

Here p = 103 which is a prime, and a = 8

So $8^{103} \equiv 8 (\text{mod } 103)$

So remainder is 8 when 8^{103} is divided by 103.

Self Check Exercises-4

Q 1. Let G be a group. H and K be finite subgroup G such that O(H) and O(K) are relatively prime. Show that $H \cap K = \{e\}$.

Q. 2. What is remainder when 1318 is divided by 19.

Q. 3 What is remainder when 1332 is divided by 15.

Q. 4 What is remainder when 192200002 is divided by 23.

Q. 5 How many numbers from 1 to 300 can neither be divisible by 2 nor by 3 or nor by

5.

7.7 Summary

In this unit we have studies the following :

1. The difinition and examples of cosets of a subgroup of a group
2. Two left (right) cosets of a subgroup are disjoint.
3. The group G is equal to the union of all of its cosets.
4. There is one one correspondence b/w and left(right) cosets
5. There is one one correspondence b/w the set of left and right cosets of H in G.
6. From Lagrange's theorem, we learn that order of a subgroup divides the order of a group.
7. The index of a subgroup of a group, also index of a subgroup, divides the order of a group.
8. Euler's and Fermat theorem.
9. Application of Euler's and Fermat's theorem.

7.8 Glossary

- **Coset :** A coset is a subset of a group obtained by multiplying each element of a subgroup by a fixed element of the group.
- **Index of a subgroup :** Let H is a subgroup of G then the number of distinct left or distinct right cosets is called the index of H in G.
- **Converse of Lagrange's Theorem :** Let G is a finite group and m/O(G) the G has a subgroup of order m.

7.9 Answer to Self Check exercises

Self Check Exercise-1

Q. 1 The right cosets will be H, H+1, H+2, H+3, H+4.

Q. 2 Left cosets are H, (13) H, (23) H.

Right cosets are H, H(13), H(23).

Q. 3 Right cosets are

Q. 4 The distinct cosets are H & H+1

Q. 5 The distinct Cosets are H, H+1, H+2

Self Check Exercise-2

Q. 1 By using answer to self check exercise 3

Q. 2 Use the example 4 the prove this.

Self Check Exercise-3

Q. 1 5

Q. 2 3

Q. 3 3

Q. 4 4

Q. 5 4

Self Check Exercise-4

Q. 1 As $H \cap K \leq K$ and $H \cap K \leq H$ $O(H) = m_1$ $O(K) = n$.

$O(H \cap K) = (m, n)$

Q. 2 1

Q. 3 1

Q. 4 16

Q. 5 80

7.10 References/Suggested readings

1. Vijak K Khanna and S.K. Bhambri, A course in Abstract algebra 5th edition.
2. Joseph A. Gallian, Contemporary Abstract Algebra.
3. Frank Ayrer Jr Modern Algebra, Schaum's outline series.
4. A.R. Vasijiha, Modern Algebra, Krishna Prakason Media.

7.11 Terminal Questions

Q. 1 Use Fermat's theorem to determine the remainder 5^{103} is divided by 103.

Q. 2 Let Z be additive group of integers and H_n i.e. the subgroup of multiples of a fixed integers $n > 1$. What is the index of H_n in Z. Write all the cosets of H_n in Z.

Unit - 8

Normal Subgroup

Structure

8.1 Introduction

Dear students in this unit you will learn about one special type of subgroup known as normal subgroup. These subgroups are directly related to coset of a subgrup of a group. If H is a subgroup of a group G, then the left coset aH of H in G may not be equal to the corresponding right coset Ha. In this unit you will study a particular class of subgroups H for which each left coset of H in G is equal to the corresponding right coset of H in G. Such subgroup give size to normal subgroup. You will also study properties of normal subgroup as well as & due theorem based or normal subgroup.

8.2 Learning Objectives

After studying this unit, students will be able to

1. define normal subgroup with examples.
2. prove a given subgroup is normal or not using properties of normal subgroup.
3. state and prove thesens based on normal subgroup.
4. Apply the properties of normal subgroups.

8.3 Normal Subgroup

Definition : A subgroup H of a group G is called normal subgroup of G of every left coset of H in G is equal to the corresponding right coset of H in G i.e. aH = Ha $\forall$ a $\in$ G For additive composition, above definition becomes, if a + H = H + a $\forall a \in$ G then H is called normal subgroup of G.

Normal subgroup is also known as invariant subgroups or say conjugate subgroups.

Notes : 1 If H is a normal subgroup of G, then mathematically we write it as H Δ G.

2. When G is a abelian group. Then every subgroup H of G is a normal subgroup.

3. The subgroups Se f and G of any group G are always normal subgroups of G. These are called trivial normal subgroups of G.

Example 1 : Consider 4Z is a subgroup of (Z, +) then write its left and right cosets and check 4Z is a normal subgroup of (Z, +)

Solution : Considering the example of unit 7, where we have find the right cosets of 4Z in (Z, +). From here, we known that H, H+1, H+2, H+3 are right cosets of 4Z in (Z, +).

Let us find left cosets of 4Z in (Z, +) [in the same line as in example of unit 7]

0th = {0, ±4, 8±, ±12, ±16.....} = H

1+H = {....., -11, -7, -3, 1, 5, 9, 13,.....}

2+H = {....., -13, -9, -5, -1, 3, 7, 11,.....}

3+H = {....., -9, -5, -1, 3, 7, 11, 15,.....}

H = H

Since 1+H = H+1

2+H = H+2

3+H = H+3

Thus every left coset of 4Z is a right coset of 4Z in (Z, +).

Hence 4Z is a normal subgroup of (Z, +)

Example 2 : Show that H = {-1, 1} is a normal subgroup of quaternion group

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

Solution : Cosets of H in Q_8 are

H.1 = { (-1).1, 1.1} = {-1, 1} = 1.H

H.(-1) = { (-1)x(-1), (-1).1} = {1, -1} = (-1).H

H.(+i) = { (-1)x(i), (-1)xi} = {-i, i} = i.H

H.(-i) = { (-1)x-i, 1x-i} = {i, -i} = -i.H

H.(j) = { -1xj, 1xj} = {-j, j} = j.H

H.(-j) = {-1x-j, 1x-j} = {-j, -j} = -j.H

H.(k) = { -1xk, 1xk} = {-k, k} = k.H

H.(-k) = {-1x-k, 1x-k} = {k, -k} = -k.H

Here Ha = aH = {-a, a} $\forall$ a $\in$ G.

Hence H {-1, 1} is normal subgroup of Q_8.

Example 3 : Let G = S_3 the symmetric group on these numbers 1, 2, 3. Show that the subgroup H {II, (1 2 3), (1 3 2) is a normal subgroup of G.

Solution : Here G = S_3 = {I, (1 2), (1 3), (2 3), (1 2 3) (1 3 2)}

Also H {I, (1 2 3) (1 3 2)}

Now,

I H = {I.I, I(1 2 3), I(1 3 2)} = {I, (1 2 3), (1 3 2} = HI

(1 2) H = $\left\{\begin{pmatrix}1&2\\2&1\end{pmatrix}I,\begin{pmatrix}1&2\\2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2\\2&1\end{pmatrix}\begin{pmatrix}1&3&2\\3&2&1\end{pmatrix}\right\}$

= $\left\{\begin{pmatrix}1&2\\2&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right\}$

= {(1 2), (1 3), (2 3)}

Now H (1 2) = $\left\{I\begin{pmatrix}1&2\\2&1\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2\\2&1\end{pmatrix},\begin{pmatrix}1&3&2\\3&2&1\end{pmatrix}\begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}$

= $\left\{\begin{pmatrix}1&2\\2&1\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&3&2\\3&1&2\end{pmatrix}\right\}$

= {1 2, (2 3), (1 3)}

$\therefore$ (1 2) H = H(1 2)

Now, (1 3) H = $\left\{\begin{pmatrix}1&3\\3&1\end{pmatrix}I,\begin{pmatrix}1&3\\3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&3\\3&1\end{pmatrix}\begin{pmatrix}1&3&2\\3&2&1\end{pmatrix}\right\}$

= $\left\{\begin{pmatrix}1&3\\3&1\end{pmatrix},\begin{pmatrix}1&3&2\\1&2&3\end{pmatrix}\begin{pmatrix}1&3&2\\2&3&1\end{pmatrix}\right\}$

= {(1 3), (2 3), (1 2)}

Now

H(1 3) = $\left\{ I\begin{pmatrix}1 & 3\\ 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 3\\ 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 3\\ 3 & 1\end{pmatrix}\right\}$

$= \left\{\begin{pmatrix}1 & 3\\ 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\\ 1 & 2 & 3\end{pmatrix}\right\}$

= {(1 3), (1 2), (3 2)}

Therefore H (1 3) = (1 3) H

Again (2 3) H = $\left\{\begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix} I, \begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix}\begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\right\}$

$= \left\{\begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix}, \begin{pmatrix}2 & 3 & 1\\ 1 & 3 & 2\end{pmatrix}\begin{pmatrix}2 & 3 & 1\\ 2 & 1 & 3\end{pmatrix}\right\}$

= {(2 3), (2 1), (3 1)}

Now H(2 3) = $\left\{ I\begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix}\right\}$

$= \left\{\begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\\ 2 & 3 & 1\end{pmatrix}\right\}$

= (2 3), (1 3) (1 2)}

Therefore H (2 3) = 2 3 H.

Also (1 2 3) H = $\left\{\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} I, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\right\}$

$= \left\{\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}\right\}$

= {(1 2 3), (1 3 2), I}

={I, (1 2 3) (1 3 2)} = H

Now H (1 2 3) = $\left\{ I\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\right\}$

$= \left\{\begin{pmatrix}1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\\ 1 & 3 & 2\end{pmatrix}\right\}$

= {1 2 3), (1 3 2) (I)}

= H

Therefore, H(1 2 3) = (1 2 3) H

Again (1 3 2)H = {(1 3 2) I, (1 3 2) (1 2 3), (1 3 2) (1 3 2)}

$$= \left\{(1\ \ 3\ \ 2), \begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\right\}$$

$$= \left\{(1\ \ 3\ \ 2), \begin{pmatrix}1 & 3 & 2\\ 1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\\ 2 & 1 & 3\end{pmatrix}\right\}$$

= {(1 3 2), I, (1 2 3)}

= H

H (1 3 2) = {(1 3 2), (1 2 3) (1 3 2), (1 3 2) (1 3 2)}

$$= \left\{(1\ \ 3\ \ 2), \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\right\}$$

$$= \left\{(1\ \ 3\ \ 2), \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\\ 2 & 1 & 3\end{pmatrix}\right\}$$

= {(1 3 2), I, (1 2 3)}

= H

H(1 3 2) = (1 3 2) H.

Hence $\forall$ a $\in$ S_3, Ha = aH

$\therefore$ H = {I, (1 2 3), (1 3 2)} is a normal subgroup of S_3

Example 4 : Show that H = {I, (1 2)} is not a normal subgroup of S_3.

Solution : Since S_3 = {I, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)}

H = {I, (1 2)}

Now, HI = IH

(1 2) H = {(1 2) I, (1 2) (1 2)}

$$= \left\{(1\ \ 2), \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\right\}$$

$$= \left\{(1\ \ 2), \begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}\right\}$$

= {(1 2), I}

= H

$H(1\ 2) = \{I(1\ 2), (1\ 2)(1\ 2)\}$

$= \{(1\ 2)\ I\} = H$

$\therefore \quad H(1\ 2) = (1\ 2)\ H$

Now $(1\ 3)H = \{(1\ 3)\ I, (1\ 3)(1\ 2)\}$

$$= \left\{(1\ \ 3), \begin{pmatrix}1 & 3\\ 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\right\}$$

$$= \left\{(1\ \ 3), \begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}\right\}$$

$= \{(1\ 3)(1\ 3\ 2)\}$

Now $H(1\ 3) = \{I(1\ 3), (1\ 2)(1\ 3)\}$

$$= \left\{(1\ \ 3), \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\begin{pmatrix}1 & 3\\ 3 & 1\end{pmatrix}\right\}$$

$$= \left\{(1\ \ 3), \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\right\}$$

$= \{(1\ 3), (1\ 2\ 3)\}$

Since $(1\ 3)\ H \neq H\ (1\ 3)$

So $H = \{I, (1\ 2)\}$ is not a normal subgroup of S_3.

Self Check Exercises-1

Q. 1 Check whether or not $H = \{I, (1\ 2), (3\ 4)$ is a normal subgroup of S_4.

Q. 2 Check whether or not $H = \{1, -1, i, -i\}$ is a normal subgroup of Q_8.

8.4 Theorems BASDED on Normal Subgroups

Theorem 1 : A subgroup H of group G is a normal subgroup of G iff $ghg^{-1} \in H$ for every $h \in H, g \in G$.

Proof : Let H be a normal subgroup of G, to prove $ghg^{-1} \in H$. As H is a normal subgroup of G, then by definition of normal subgroup of G.

$gH = Hg\ \forall g \in G$

Let $h \in H$ and $g \in G$ be any element.

$\Rightarrow gh \in Hg$

Therefore $gh = h.g$ for some $h_1 \in H$

$\Rightarrow ghg^{-1} = h_1$

$\Rightarrow ghg^{-1} \in H$ $[\because h_1 \in H]$

Conversely : Let H is a subgroup of G such that $ghg^{-1} \in H$, $h \in H \forall g \in G$ to prove H is normal subgroup of G i.e. $aH = Ha \ \forall a \in G$.

Let $a \in G$ be any element, then $aha^{-1} \in H \ \forall \ h \in H$

Let $ah \in aH$ be any element. Then

$ah = aha^{-1}a = (ah^{-1})\ a \in Ha$ $[\because aha^{-1} \in H]$

$\Rightarrow ah \in Ha$

$\therefore aH \leq Ha.$ ...(1)

Again, Let $b = a^{-1}$ be any element of G

Then again using given hypothesis $bhb^{-1} \in H$

But $bhb^{-1} = a^{-1}h(a^{-1})^{-1} = a^{-1}\ ha \in H$

Let $ha \in Ha$ be any element Then

$ha = (aa^{-1})ha = (aa^{-1}h)a = a(a^{-1}ha) \in aH.$

$\Rightarrow ha \in aH$

$Ha \leq aH$ ...(2)

From (1) and (2), we have

$aH = Ha \ \forall \ a \in G$

Hence H is a normal subgroup of G.

Theorem 2 : Let H be a subgroup of a group G. Then the following statements are equivalent.

(i) $g\ h\ g^{-1} \in H,$ $\forall\ g \in G.\ h \in H.$

(ii) $g\ H\ g^{-1} \in H,$ $\forall\ g \in G$

(iii) $g\ H = H\ g$ $\forall g \in G.$

Proof : (i) $\Rightarrow$ (ii) Since $g\ h\ g^{-1} \in H,$ $\forall\ g \in G.\ h \in H.$

Let $g\ h\ g^{-1} = h_1$ for some $h_1 \in H$

$\Rightarrow$ $g\ H\ g^{-1} = H,$ $\forall\ g \in G$

(ii) $\Rightarrow$ (iii) Let $g\ H\ g^{-1} = H,$ $\forall\ g \in G$

$\Rightarrow$ $(g\ H\ g^{-1})g = H\ g$

$\Rightarrow$ $gH(gg^{-1}) = H\ g$

$\Rightarrow$ $g\ H\ e = H\ g$ $(\because H\ e = H)$

$\Rightarrow$ $g\ H = H\ g.$

(iii) $\Rightarrow$ (i) Let $g\ H = H\ g$ $\forall g \in G$

$\Rightarrow g\,h = h_1\,g$ for some $h, h_1 \in H$

$\Rightarrow g\,h\,g^{-1} = h_1 \in H$

$\Rightarrow g\,h\,g^{-1} \in H, \ \forall\ g \in G, h \in H$

Hence (1) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i)

Hence the given statements are equivalent.

Theorem 3 : A subgroup H of a group G is a normal subgroup of G iff the product of two right cosets of H in G is again a right coset of H in G.

Or

Prove that a subgroup H of a group G is normal

iff $Ha\ Hb = H\,ab\ \forall\ a, b \in G$

(the composition is denoted multiplicatively)

Sol. Let H be a normal subgroup of G and

Let H a, H b be two right cosets of H in G. Then

$(H\,a\,(H\,b) = H\,(a\,(H\,b))$

$= H((a\,H)\,b)$

$= H\,(H\,a)\,b$, since H is a normal subgroup of G so

$a\,H = H\,a$

$= H\,(H\,(a\,b))$

$= (H\,H)\,a\,b$

$= H\,a\,b$, since H is a subgroup of G so $HH = H$

$\therefore$ $(H\,a)\,(H\,b) = H\,a\,b$.

$\therefore$ $a, b \in G \Rightarrow a\,b \in G$

$\therefore$ H a b is a right coset of H in G.

Thus the product of two right cosets of H in G is again a right coset of H in G.

Conversely, suppose H is a subgroup of a group G such that the product of two right cosets of H in G is again a right coset of H in G.

To show that H is a normal subgroup of G.

Let $g \in G$ be any element.

$\therefore\ g^{-1} \in G$, since G is a group.

$\therefore$ H g, $H\,g^{-1}$ be two right cosets of H in G.

$\therefore$ $(H\,g)\,(H\,g^{-1})$ is again a right cosets of H in G.

Since H is a subgroup of G, therefore $e \in H$, where e is the identity element of G.

Since e $\in$ H.

$\therefore$ (e g) (e g^{-1}) $\in$ (H g) (H g^{-1})

$\Rightarrow$ g $g^{-1} \in$ (H g) (H g^{-1})

$\Rightarrow$ e $\in$ (H g) (H g^{-1})

Also H is a right coset of H in G and e $\in$ H.

$\therefore$ (H g) (H g^{-1}) and H are two right cosets of H, each containing e.

$\therefore$ (H g) (H g^{-1}) $\cap$ H $\neq \phi$.

Since the two right cosets of H in G are either disjoint or identical.

$\Rightarrow$ (H g) (Hg^{-1}) = H.

Let h $\in$H be any element.

$\therefore$ (h g) (h g^{-1}) $\in$ (H g) (H g^{-1})

$\Rightarrow$ (h g) (h g^{-1}) $\in$ H, since (Hg) (Hg^{-1}) = H.

$\Rightarrow$ h (g h g^{-1}) $\in$ H.

$\Rightarrow$ g h $g^{-1} \in$ h^{-1} H.

$\because$ h $\in$H and H is a subgroup $\Rightarrow$ $h^{-1} \in$ H $\Rightarrow$ h^{-1} H = H

$\therefore$ g h $g^{-1} \in$ H.

This is true $\forall$ g $\in$G and h $\in$H.

Hence H is a normal subgroup of G.

Theorem.4 Let H am nd K be two subgroups of a group G. Then

(i) if H is a normal subgroup of G, then HK = KH is a subgroup of G.

(ii) if H and K both are normal subgroups, then HK = KH is a normal subgroup of G.

Proof. (i) Given H is a normal subgroup of G. To show that HK = KH is a subgroup of G.

Let b $\in$ K be any element. Then H b = bH [$\because$ H Δ G]

$\Rightarrow$ H b = bH $\in$ KH, $\forall$ b $\in$ K

$\Rightarrow$ H K $\subseteq$ KH.

Similarly, b H = H b $\in$ HK i.e. b H $\in$ HK, $\forall$ b $\in$ K

$\Rightarrow$ KH $\subseteq$ HK. .....(2)

$\therefore$ from (1) and (2), we get HK = KH.

$\therefore$ By Theorem 2.1.8, HK (= KH) is a subgroup of G.

(ii) Let H and K be both normal subgroups of G.

$\therefore$ By (i) HK = KH is a subgroup of G. To show that H is a normal subgroup of G.

Let $g \in G$ be any element. Then

$g(HK)g^{-1} = gHg^{-1}gKg^{-1} = (gHg^{-1})(gKg^{-1}) \subseteq HK$.

[$\because$ H, K are normal subgroup $\therefore$ $gHg^{-1} \subseteq H$, $gKg^{-1} \subseteq K$]

Hence HK is a normal subgroup of G.

Theorem 5. Every subgroup of abelian group is normal.

Proof: Let H be a subgroup of an abelian group G.

$\therefore$ $gx = xg$ $\forall\, x \in G$, $\forall\, g \in G$ [as G is abelian]

In particular $gh - hg$ $\forall\ h \in H, g \in G$

$\Rightarrow$ $ghg^{-1} = hgg^{-1} = he = h$

$\Rightarrow$ $ghg^{-1} = h \in H$

$\Rightarrow$ $ghg^{-1} \in H$ $\forall\, h \in H dg \in G$

Hence by definition of normal subgroup H is normal subgroup of G.

The converse of above is not true. There are non commutative groups whose subgroups are normal.

Example: Since Q8 is a non commutative group but its subgroup $H_2\{-1,1\}$ is a normal subgroup (as proved in example 2).

Let us consider some question to when we can use those theorems.

Example 1: Show that the set H2 $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d,E,R,S\ ad-bc=1\right\}$ is a normal subgroup of the group or

$$G = \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : a,b,c,d,E,R,S\ t\ ad-bc \neq 0\right\}$$

Solution: To Prove H is a normal subgroup of G firstly we have to show that H is non empty set and subgroup then of G. We apply the theorem 1.

Since $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ be the identity element as

$|I| = I$

$\Rightarrow$ $I \in H$

$\therefore$ H is non empty subset of G.

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in H$ s.+. $a_1d_1 - c_1b_1 = 1 = |\Delta|$

and B = $\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in$ H s.+. $a_2d_2 - b_2 c_2 = 1 = |B|$

Also $|A| = 1 \neq 0$, so A^{-1} exists.

So $A A^{-1} = I$

$|A A^{-1}| = |I|$

$\Rightarrow \quad |A|\,|A^{-1}| = 1$

$= \quad ||A^{-1}| = 1$

$\Rightarrow \quad |A^{-1}| = 1$

as $|A^{-1}| = 1$ so $A^{-1} \in$ H.

Also $|AB| = |A|\,|B| = 1.1$

$\Rightarrow \quad |AB| = 1$

As $|AB| = 1$ so AB $\in$ H

as A B $\in$ H and $A^{-1} \in$ H so H is a subgroup of a Now to prove, H is a normal subgroup of G.

Let $A \in H\ \alpha\nu\delta\ B \in G$ be any elements

Since A $\in$ H $\Rightarrow |A| = 1$

and B $\in$ G $\Rightarrow |B| \neq 0$

as $|B| \neq 0$, so B^{-1} exists.

Now $|BAB^{-1}| = |B|\,|A|\,B^{-1}| = |B|.1.\frac{1}{|B|} = 1$

$\Rightarrow \quad BAB^{-1}| = 1$

$\Rightarrow \quad BAB^{-1} \Leftarrow$ H $\quad \forall$ A $\in$ H B E G

Hence H is a normal subgroup of G.

Question 2. Let G denotes the group of all non-singular upper triangular 2x2 matrices with real entries i.e. G = $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d,E,R, and\ ad \neq 0\right\}$ show that H = $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ 1 b $\in$ R is a normal subgroup of G.

Solution: Given G = $\left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a,b,c,d,E,R, ad \neq 0\right\}$

and H = $\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}, b, E, R\right\}$

So H is a subset of G.

Now, to prove H is a subgroup of G.

Let A, B $\in$ H s.t A = $\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}$, B E R and B = $\frac{-1}{d}+\frac{ab}{d}$, C E R

be two elements of H.

Then AB = $\begin{pmatrix}1 & c+b\\ 0 & 1\end{pmatrix}$, as b + c E $\in$ R so AB $\in$H

Also As |A| $\neq$ 0, so A^{-1} exists.

So, H is a subgroup of G.

Now to prove H is a normal subgroup of G.

Let A $\in$ H and B $\in$ G

$\therefore$ A = $\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}$ b $\in$ R and B = $\begin{pmatrix}a & b\\ 0 & a\end{pmatrix}$, a, b, d, $\in$, R, ad $\neq$ 0

As |B| $\neq$ 0 So B^{-1} exists.

So $B^{-1} = \frac{Adj\, B}{|B|} = \begin{pmatrix}d & -b\\ 0 & a\end{pmatrix} = \begin{bmatrix}\frac{1}{a} & -b/ad\\ 0 & 1/d\end{bmatrix}$

Then $B A B^{-1} = \begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\begin{bmatrix}\frac{1}{a} & -b/ad\\ 0 & 1/d\end{bmatrix}$

$= \begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\begin{bmatrix}\frac{1}{a} & -b/ad + b/d\\ 0 & 1/d\end{bmatrix}$

$= \begin{bmatrix}1 & \frac{-ab}{ad}+\frac{ba}{d}\\ 0 & 1\end{bmatrix}$

$= \begin{bmatrix} 1 & -b/a + a\,b/d \\ 0 & 1 \end{bmatrix}$ as, a, b, c, $\in$ R So $\frac{-1}{d} + \frac{ab}{d} \in$ R

$BAD^{-1} \in H$

Hence H is a normal subgroup of G.

Self Check Exercise - 2

Q. 1 Show that Z (G), contra of a group is a normal subgroup of G.

Q. 2 Let H be normal subgroup of group G. If $x^2 \in H$, $\forall\ x \in G$ then prove that H is normal subgroup of G.

8.5 Properties of Normal Subgroup

Property :- Section of two normal subgroups is a normal subgroup.

Proof :- Let M and N be two normal subgroups of G So, M and N are subgroup of G

$\Rightarrow$ $M \cap N$ is also a subgroup of G.

Let $h \in M \cap N$ and $g \in G$

$\Rightarrow$ $h \in M$ and $h \in N$ and $g \in G$

Since M and N are normal subgroups of G

$\Rightarrow$ $ghg^{-1} \in M$ and $ghg^{-1} \in N$ [by theorem]

$\Rightarrow$ $ghg^{-1} \in M \cap N\ \forall\ g \in G$ and $h \in M \cap N$

$\Rightarrow$ $M \cap N$ is a normal subgroup of G.

Property 2. A normal subgroup H of a group G and K is a subgroup of a such that $H \subseteq G$. Then H is also a normal subgroup of K.

Proof : Given H is a normal subgroup of G

$\Rightarrow$ H is a subgroup of G

Also K is a subgroup of G and $H \subseteq K$.

$\Rightarrow$ H is also a subgroup of K.

To prove H is a normal subgroup of K

Let $X \in K$ $\Rightarrow$ $x \in G$ [$\because$ $K \subseteq G$

Since H is a normal subgroup of G

$\Rightarrow$ $Hx = xH$

So $Hx = xH$, $x \in K$

so H is also a normal subgroup of K.

Property 3. A non empty subset H of a group G is normal subgroup of G (ga(gb)-1 $\in$H & a, b $\in$H adg$\in$G.

Proof : Let H is normal subgroup of G

to prove (ga) $(gb)^{-1} \in H$.

Let H is normal subgroup of G.

Let a, b $\in$ H and g $\in$G

then $(ga)(gb)^{-1} = ga(b^{-1}g^{-1})$

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

$\because a_1 b \in H, b^7 \in H$

$ab^{-1} \in H$ *as* H *is subgroup of* a

$g(ab^{-1})g^{-1} \in H \because H$ *is normal subgroup of* G.

Conversely: Let $(g\ a)^{-1}$ (g B) $\in$ H $\forall$ a_1 b $\in$ H_1 g $\in$G

to prove H is normal subgroup

H is subgroup of G

Let a_1 b $\in$ H_1then

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

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

$= (ea)\ (eb)^{-1}$ $\because e^{-1} = e$

$\in$ H by given of g $\in$G

(g a) $(e\ b)^{-1} \in$ H

and e $\in$ G is identity of G

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

So H is subgroup of G.

H is normal subgroup of G

Let h $\in$H and g $\in$G. Also e, identity element of G

$\Rightarrow$ e $\in$ H

Given $(gh)\ (ge)^{-1} \in$ H

$\Rightarrow$ $gh\ (eg^{-1}) \in$ H [$\because$ $(ge)^{-1} = e\ g$

$\Rightarrow$ $g\ (he)g^{-1} \in$ H and $e^{-1} = e$

$\Rightarrow$ $g\ h\ g^{-1} \in$ H $\because$ he - h

$\Rightarrow$ H is a normal subgroup of G.

Property 4. If H is the only subgroup of order n in a group G, then H is normal subgroup.

Proof: Let $g \in G$ be any element. Then gHg^{-1} is a subgroup of G.

Also $|H| = |ghg^{-1}|$

Also $|ghg^{-1} = n$, but H is only subgroup of order n

$\therefore$ $gHg^{-1} = H|$

Hence H is a normal subgroup of G.

Property 5. If H is a subgroup of G of index 2 in G. Then H is normal subgroup of G.

Proof: Let H be a subgroup of G such that [G : H] = 2

$\therefore$ The number of distinct left (or right) cosets of H in G is 2.

To prove H is normal subgroup of G.

Case I When $x \in H$

Since $x \in H$ so $x H = H = H x$

$\Rightarrow$ $x H = H x$

Case II : When $x \notin H$

$x H \neq H$ and $H x \neq H$

Given [G : H] = 2

So $H \cup x H = G = x H \cup H$ [Union of all coset is group itself].

$\Rightarrow$ $x H = H x$

Combining both of cases we find that

$x H = H x$ & $x \in G$.

$\therefore$ H is normal subgroup of G.

Using above property let us do some question

Question:- Given an example of non-abelian group in which all subgroups are normal

Solution: The Question group $G = \{\pm i, \pm J, \pm K, \pm 1\}$

O (G) = 8

Let H be a subgroup of G. Then by Lagrange's theorem O(H) | O(G).

$\therefore$ Subgroup of G must have order same as divisor of 8 and divisor of 8

are 1, 2, 4, 8

$\therefore \quad O(H) = 1, 2, 4, 8$

If O(H) = 1 then H = {e}

If O(H) = 8, then H = G

Since {e} and G are leivial subgroup of G.

Alsolivial subgroups are livial normal subgroup of G.

Now of O(H) = 4 then index of G in H [G : H] = $\frac{O(G)}{O(H)} = \frac{8}{4}$ = 2

So if index of G in H i.e. [G : H] = 2, So by property 5, the subgroup is normal.

Again if O(H) = 2 then H = $\{1_1 - 1\}$

In this case x H = H x $\forall$ x $\in$ G

$\therefore$ All subgroups of this group are normal

Question 2. Show that the set 3z from a normal subgroup of the group of integer under addition.

Solution: Give (Z, +) is a group of integer under addition.

Now 3Z = {3n ; n $\in$ z}

Let x, y $\in$ 3Z, then

$x = 3n_1$, $y = 3n_2$ for $n_1, n_2 \in Z$

Now $x - y = 3n_1 - 3n_2$

$= 3 (n_1 - n_2)$

$\in 3Z$ [$\because$ $n_1, n_2 \in Z$ so $n_1 - n_2 \in Z$]

So 3Z is a subgroup of Z.

To prove 3Z is normal subgroup

Let $g \in Z$ and $h \in 3Z$-

$\Rightarrow$ $g \in Z$ and h = 3n, $n \in Z$

then g + h + (g) = g + 3n - g

= 3n

$\Rightarrow$ g + h - g $\in$ 3Z

Hence 3Z is a normal subgroup of Z.

Self Check Exercises-3

Q. 1 Prove that the intersection of any collection of normal subgroup is itself normal subgroup.

Q. 2 Show that the set 5Z forms a normal subgroup of the group of integers under addition.

8.6 Summary

Dear students, in this unit, we studied that

(1) If every left coset of H in G is equal to corresponding right coset of H in G i.e. aH = Ha, $a \in a$, than H is normal subgroup of G.

(2) If G is abelion group. Then every subgroup's normal subgroup.

(3) If $n \in G$. where H is subgroup of G then of $ghg^{-1} \in H$ then H is normal subgroup of G

(4) H is a normal subgroup of G. H HaHb = Hab $\forall$ a,b$\in$ G.

(5) Intersection of two normal subgroup is a normal subgroup.

(6) If H is a subgroup of G of index 2, then H is normal subgroup of G.

8.7 Glossary

- **Normal Subgroup:-** Let G be a group. A Subgroup H of G is said to be a normal Subgroup of G if aH = Ha for all $a \in G$.
- **Right Coset:-** A night coset of a subgroup H in a group G is a set of elements obtained by multiplying every element of H by a fixed element of from G on the right side.
- **Intersection of Subset:-** $N_1 \cap N_2 = (x \in G/n \in N$, and $n \in N_2)$, where N_1 and N_2 be the subset of Group G.

8.8 Answers to Self Check Exercise

Self Check Exercises-1

Q. 1 Apply definition of normal subgroup same as in question 4.

Q. 2 Apply definition of normal subgroup same as in question 2.

Self Check Exercises-2

Q. 1 Prove theorem 1 for Z(a), i.e. $ghg^{-1} \in Z(a)$ for $x \in G$ and $H \in H$

Q. 2 Prove $ghg^{-1} \in H$, $n \in H$ and $g \in G$.

Self Check Exercises-3

Q. 1 Generaliz the result of property 1.

Q. 2 Same as question 2.

8.9 References/Suggested Readings

1. Vijay k Khanna and S.K. Bhambri, A coures in Abstract Argebra
2. Joseph A. Gallian, Contemporary Abstract Argeora.
3. Fronk Ayers Is. Modern Algebra, Schaum's outline series.
4. A.R. Vasistha, Modern Argebra, KeishnaPrakaslal Media.

8.10 Terminal Questions

1. Let T denotes the group of all non- singular upper triangular 3x3 matrices with real entries. Show that H = $\left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, a, B, C \in R \right\}$ is a normal subgroup of G.

2. A cyclic subgroup T of a group G is normal in G then every subgroup of T is also normal in G.

*****

Unit - 9

Quotient Group

Structure

9.1 Introduction

Dear Students student in previous unit we studied about normal subgroup of a group. Normal Subgroup have some special significance because when a Subgroup H of G is normal, then the set of left (right) cosets of H in G is itself form a group. And from here we get another type of group which is known as Quotient group of G by H We can information about a group by studying one of its quotient group. So in this unit we will study about quotient group along with some properties and theorem related to quotient group.

9.2 Learning Objectives

After studying this unit students will be able to

(1) define a quotient group

(2) Find quotient group of a given group.

(3) Prove and apply the theorems based on quotient group.

9.3 Quotient Group

Definition : If G is a group and H is a normal subgroup of G, then the set G/H of all cosets of H in G is a group with respect to the multiplication of cosets i.e. (Ha) (Hb) = Hab

This group is known as quotient group or factor group of G by H.

Note 1:- Under addition of coset, the composition is defined as

(H + a) + (H + b) = H + (a + b)

Note 2:- The identity element of quotient group G/H is H

Note 3:- If H is normal subgroup of tinit group G than G/H forms a group of order $\frac{O(G)}{O(H)}$.

Let us try to understand more about quotient group by solving some questions about this group.

Question 1: Let Z be the additive group of integers Let H = 4Z be additive group of integer multiple of 4. Show that H is a normal subgroup of Z. Also write the elements of Z/H. Also write the composition table for Z/H.

Solution:- Given Z be additive group of integers and H = 4Z

To show H is a normal subgroup of Z under addition.

Let $g \in Z$, $h \in H \Rightarrow h = 4n$, $n \in Z$

then g + h + (-g) = g + 4n - g

= 4n

$\Rightarrow$ $g + h + (-g) = 4n \in H$.

Hence 4z is a normal subgroup of Z.

In order to write the elements of Z/H or Z/4H, we have to write the set of all cosets of 4H in G.

Since from (question of unit 7) we know that only distinct cosets of 4z in a all.

H, H + 1, H + 2, H + 3.

So elements of Z/H = Z/4H = {H, H+1, H+2, H+3}

Composition table for Z/H or H/4H, Here H is identity for Z/H

+	H	H+1	H+2	H+3
H	H	H+1	H+2	H+3
H+1	H+1	H+2	H+3	H
H+2	H+2	H+3	H	H+1
H+3	H+3	H	H+1	H+2

Question 2: Let G = {-1, 1, -i, i} be a group and H = {-1, 1} subset. Show that H is normal subgroup of G. Find the elements of G/H and prepare the composition table.

Solution: Given G = {-1, 1, -i, i}

and H = {-1, 1}

Since $H \subseteq G$ and H is itself a group

So H is a subgroup of G

Since [G : H] = Index of G in H = $\frac{O(a)}{O(H)}$

$= \frac{4}{2}$

Since index of G in H is 2, So he Subgroup is a normal subgroup of a

[Property of normal subgroup]

So, H is a normal subgroup of G.

Now, to find all the coset of H in G.

Since we known that (From question 2 of unit 7)

all cosets of H in G are H and Hi

So elements G/H = {H, Hi}

Composition table of element of G/H

.	H	Hi
H	H	Hi
Hi	Hi	H

Self Check Exercises-1

Q. 1 Find all the elements of Z/H, where Z is a additive group of integers and H = 3Z.

Q. 2 Find all the elements of Z/H, where Z is a Symmetric group on {1,2,3} and H = {I, (1, 2)}.

9.4 Theorem on Quotient Group

Theorem 1. If H is a subgroup of an abelian group G, then the group G/H of all right cosets of H in G forms on abelian group under the composition defined by Ha.Hb = Hab.

Proof: Given H is a subgroup of an abelian group G. Since a subgroup of an abelian group is normal. So H is a normal subgroup.

Now to prove G/H is an ablian group under the composition Ha.Hb = Hab.

(1) ClosursProperty : Let a, b $\in$ G, then ab$\in$G

$\therefore$ Hab $\in$ G/H

$\Rightarrow$ Ha.Hb$\in$ G/H

$\therefore$ Clasues property holds.

(2) Associative Property: (Ha . Hb). Hc = (Hab) . HC

= H (ab)C

= Ha (bc)

= Ha (Hbc)

= Ha (Hb) (Hc)

= Ha (Hb Hc)

$\Rightarrow$ (Ha . Hb) .Hc

So, Associative property good.

(3) Existence of identity:-

Let e be the identity of G

then $He \in G/H$

Now (Ha).(He) = H(ae)

= Ha

= H(ea)

= (He) (Ha)

$\therefore$ He = H is identity of G/H.

(4) Existence of inverse: for $H a \in G/H$, We have $a \in G$

$\therefore$ $a^{-1} \in G$

$\Rightarrow$ $Ha^{-1} \in G/H$

Now, (Ha) (Ha^{-1}) $= H (aa^{-1})$

$= He$

$= Ho$

$= He$

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

$= (Ha^{-1})(Ha)$

$\therefore$ $(Ha)^{-1} = Ha^{-1} \in G/H$

$\therefore$ Ha^{-1} is the inverse of Ha in G/H

(5) Commutative Property : Let $Ha, Hb \in G/H$, $a, b \in G$.

Now (Ha) (HG) = Hab

= Hba

= (Hb) (Ha)

$\Rightarrow$ (Ha) (Hb) = H (b) (Ha)

$\Rightarrow$ G/H is on abelian group.

Converse may not be true i.e.

An example of non abelian group G and a normal subgroup H of G such that quotient group G/H is abelian

The group G = {± 1, ± i, ± j, ± k} is non abelian group of unit quaternion under multiplication defined as i2 = j2 = k2 = -1, jj = k = -ji, jk = i = -ki, ki = j = -ik

Let H = {1, -1, -i, -i} be a subgroup of G.

Then [G : H] = $\frac{O(G)}{O(H)}$

= $\frac{8}{4}$

= 2

$\Rightarrow$ [G : H] = 2

Since H is a subgroup of G of index 2 Hence it is a normal subgroup of G.

Then the quotient group G/H gives the set of all left right coset of H in G. then

G/H = {H, iH}

O (G/H) = 2

Since O(G/H) = 2, a prime number

Since a group of prime order is an abelian group

Hence G/H is aabelien quotient group of non abelian group.

Theorem 2. Let H be a normal subgroup of a group G. Show that quotient group G/H is abelian it and only if for all x,y$\in$G, xy $x^{-1}y^{-1}\in$N.

Proof : Let H be a normal subgroup of G such that G/H is abelian. To prove, for all x,y$\in$g, $xyx^{-1}y^{-1}\in$H

Now Hxy $x^{-1}y^{-1}$ = Hx Hy $Hx^{-1}Hy^{-1}$ [by defining of quotient Hab=HaHb group)

= HxHy $(Hx)^{-1}$ $(Hy)^{-1}$ $\because$ $(Hx)^{-1} = (Hx)^{-1}$

= Hx $(Hx)^{-1}$ (Hy) $(Hy)^{-1}$[$\because$ G/H is an abelian group]

= H H [$\because$ H is identity of G/H

= H

$\therefore$ $Hxyx^{-1}y^{-1}$ = H

$\Rightarrow$ $xyx^{-1}y^{-1}\in$H x, y $\in$ G

Conversely: Let for all x, $y \in G$, $xyx^{-1}y^{-1} \in H$

To prove G/H is an abelian group

Since given $xyx^{-1}y^{-1} \in H$

$\Rightarrow$ $Hxyx^{-1}y^{-1} = H$

$\Rightarrow$ $xHy\ Hx^{-1}Hy^{-1} \in H$

$\Rightarrow$ $Hx\ Hx^{-1}Hy\ Hy^{-1} = H$

$\Rightarrow$ $Hx\ (Hx)^{-1}\ (Hy)\ (Hy)^{-1} = H$

$\Rightarrow$ $(Hx)\ (Hy)\ (Hx)^{-1} = H\ (Hy)$

$\Rightarrow$ $(Hx)\ Hy = Hy\ Hx.$

$\Rightarrow$ $Hx\ Hy = Hy\ Hx$

$\Rightarrow$ G/H is abelian group

Theorem 3: Every quotient group of a cyclic group is cyclic.

Proof: Let G = G = <a> be a cyclic group generated by an element a.

$\Rightarrow$ G is an abelian group

$\Rightarrow$ Every subgroup of G is is normal subgroup

Let H be a subgroup of G, which is normal, such that G/H is quotient group of G.

To prove G/H is a cyclic group generated by Ha.

Let $Hx \in G/H$ be an arbitrary element where $x \in G$.

But $G = \langle a \rangle$

So $x = a^n$ for some integer n.

$\therefore$ $Hx = Han = \underbrace{Ha.a. \ldots\ldots\ldots a,}_{\text{n times}}$ $\because$ G/H is quotient group.

$= \underbrace{Ha\ Ha.\ Ha. \ldots\ldots\ldots Ha}_{\text{n time}}$

$= (Ha)^n$

$\Rightarrow$ $Hx = (Ha)^n, \quad \forall\ Hx \in G/H$

$\Rightarrow$ G/H is a cyclic group generated by Ha.

Hence every quotient group of a cyclic group is cyclic.

Remark : The converse of above theorem may not between, i.e. quotient group may be cyclic even if the group may not be cyclic.

Theorem 4. If G is a group such that G/Z (a) is cyclic, where Z(a) is the contra of G. Then G is abelian.

Proof: Given Z(G) is the centre of G

Let $H = Z(a) = \{g \in G ; x = xg \ \forall \ x \in G\}$

Let G/H = <gH> be a cyclic group

Let $a,b \in G$ be any two elements

$\Rightarrow$ $aH, bH \in G/H$ by defining of quotient group

Therefore $aH = (gH)^m$ and $bH = (gw)^n$, for, $m, n \in Z$ [by defining of cyclic group]

$\Rightarrow$ $aH = g^mH$ and $bH = g^nH$

$\Rightarrow$ $a^{-1}g^m \in H$ and $b^{-1}g^n \in H$

$\Rightarrow$ $g^{-m}a \in H$ and $g^{-n} b \in H$

Let $g^{-m}a = n_1$, $g^{-n} b = h_2$ for $h_1, h_2 \in H$

$\Rightarrow$ $a = g^m n_1$ and $b = g^n h_2$

Now $ab = g^m h_1 . g^n h_2 = g^m (h_1 g^n) h_2$

$= g^m (g^n h_1) h_2$

$= g^{m+n} h_1 h_2$

$\Rightarrow$ $ab = g^m g^n h_1 h_2 = g^{m+n} h_1 h_2$

Now $ba = (g^n h_2) (g^m b_1) = g^n (h_2 g^m) h_1$

$= g^n (g^m h_2) h_1$

$= g^{n+m} h_2 h_2$

$ba = g^{m+n} h_1 h_2$

$\Rightarrow$ $ab = ba$

Hence G is abelian

Self Check Exercises-2

Q. 1 Give an example of a group G and a normal subgroup H such that G/H is cyclic but G may not be cyclic

Q. 2 Let H_1 and H_2 be two normal subgroups of a group G. Prove that G/H1 = G/H2 if and only if $H_1 = H_2$.

9.5 Summary

Dear Students in this unit we studied that

(1) The set of all cosets of H in G is known as quotient group

(2) Identity element of a quotient group G/H is H.

(3) If H is a subgroup of an abelian group G then the quotient group G/H is also abelian.

(4) If H is a normal subgroup of a group G then quotient group G/H is abelian it $xyx^{-1}y^{-1} \in H$.

(5) Every quotient group of a cyclic group is cyclic

9.6 Glossary

- **Quotient group :**A Quotient group G/N is formed by dividing a group G by normal subgroup N, where elements are cosets of N in G with a defined group operation based on coset multiplication.
- **Cyclic group :** A group G is cyclic if there exists an element of g in G such that every element of G can be expressed as a power g^n for some integer n.

9.7 Answers to Self Check Exercise

Self Check Exercises-1

Q. 1 Do same as question 1

Q. 2 Z/H = {H, H. (13), H. (2, 3)}

Self Check Exercises-2

Q. 1 Taking G = {±1, ±i, ±j, ±k} and H = {1, -1, i, -i} Here G/H is cyclic but G is not cyclic

Q. 2 If $N_1 = N_2$ than nothing to prove.

Inversely of $G/N_1 = G/N_2$ to prove $N_1 = N_2$ we can prove this by using the concept that two cosets in G are either disjoint or identical.

9.8 References/ Suggested Readings

1. Vijay K. Khanna and S.K. Bhambri, A course in Abstract algebra.
2. Joseph A. Gallian, Contemporary Abstract Algebra.
3. Frank Ayrer Jr., Modern Algebra, Schaum's Outline Series.
4. A. R. Vasistha, Modern Algebra, KeishnaPrakasham Media.

9.9 Terminal Questions

Q. 1 If H, K are normal subgroups of a group G and HCK, then show that K/H is a normal subgroup of G/H.

Q. 2 Give an example of verify that if the quatient group G/H is abelian then G may not be abelian.

*****

Unit - 10

Special Subgroups

Structure

10.1 Introduction

Dear student in this unit we will study about some special type of subgroup on the basis of their formulation. In this unit we will study about subgroup which is generated by a subset of a group along with its pro property. Also, commutator subgroup will be discussed, which is an other form of a subgroup.

10.2 Learning Objectives

After studying this unit, students will be able to

(1) define subgroups generated by subset of a group.

(2) solve question based on subgroup generated by subset of a group.

(3) define commutator subgroup.

(4) solve question based on commutator susbgroup.

10.3 Subgroup Generated by Subset of a Group

Definition : A subgroup N of a group G is said to be generated by a non empty subset S of G of H is the smallest subgroup of a containing S.

The smallest subgroup of G containing S is called subgroup generated by S and is denoted by {s} = H

Theorem 1 : If S is any subset of a group G, then smallest subgroup of G containing S exists and is unique.

Proof : Let F B the family of all sub groups of a which contain S.

F = {H : H is a subgroup of G containing S}

The family F is not empty since atleast G belong to this family.

[$\because$ G is itself a subgroup of G]

Let K be the intersection of the family F.

i.e. K = $\bigcap_{H \in F} H$

Since auditory intersection of subgroups is a subgroup, so k is a subgroup of G.

Also $S \subseteq H \ \forall H \in F$

$\therefore \quad S \subseteq \bigcap_{H \in F} H = K$

Therefore K is a subgroup of G containing S.

Now let H be any subgroup of G containing S

$\therefore \quad H \in F$

$\Rightarrow \bigcap_{H \in F} H \subseteq H$

$\Rightarrow K \subseteq H$

Therefore, K is the smallest subgroup of G containing S.

$\Rightarrow$ K is a subgroup of G generated by S and is equal to intersection of all subgroups of G containing S.

Uniqueness

Let K_1 and K_2 be two smallest subgroups of G containing S.

Then we have $K_1 \subseteq K_2$ and $K_2 \subseteq K_1$

$\therefore K_1 = K_2$

Theorem 2 : Let S is a subset of a group G. Then the set of elements of G expressible as products of positive and negative integral powers of finite number of elements of S is the smallest subgroup of G containing M.

Proof : Let H be the set of those elements of G which can be expressed as product of positive and negative integral powers of finite number of elements of S. Let a, b $\in$ G then clearly $ab^{-1} \in H$.

so, by critical of a subgroup H is a subgroup of G. clearly $S \subseteq H$.

Also of K is any subgroup of G containing S, then definitely H must contained in K.

Hence H is the smallest subgroup of G containing S.

Let us take following examples to have more understanding of subgroup generated by a subset of a group.

Question 1 : G = {I, w, w^2} is a subgroup generated by s = {w}

Solution : Given G = {I, w, w^2} be the group of cube root of unity.

Let S = {w} is a non empty subset of G.

Let H be a subgroup of G generated by S.

$\Rightarrow S \subseteq H$

$\Rightarrow w \in H$

$\therefore w^2 = w.w. \in H$ $\quad\quad$ $\because$ H is a subgroup of G.

$w^3 = w.w.w = 1 \in H$

Therefore, H contains all elements of G.

$\therefore \quad G \subseteq H$ and $H \subseteq G$

$\Rightarrow \quad G = H$

$G = \langle S \rangle$

Question 2 : Let {±1, ±i, ±j, ±k} be the group of quaternions and S = {i, j}. Then show that G is a subgroup generated by S.

Solution : Given G = {±i, ±j, ±k, ±1} and

S = {i, j}

The $S \subseteq G$

Let H = <S> be subgroup of G generated by S.

$\therefore \quad S \subseteq G$

$\Rightarrow \quad i, j \in H$

So, $i^2 = i.i = -1 \in H$,

$i \in H$, $i^3 = i.i.i = -i \in H$

Similarly $j \in H \Rightarrow -j \in H$

also $K = i\,j \in H$

$\therefore K^3 \in H \Rightarrow K^2.K \in H \Rightarrow -K \in H$

$\therefore$ H contains all elements of G.

$\Rightarrow G \subseteq H$

also $H \subseteq G$

$\Rightarrow G = H = \langle S \rangle$

Self check Exercise-1

Q. 1 In the group (Z, +) the subgroup generated by 2 and 7 is?

10.4 Commutator Subgroup

Definition : Let G be a group consider the set

$S = \{a\ b, a^{-1}\ b^{-1}; a, b \in G\}$ and $K = \{S_1, S_2.....S_n, S_i \in S,\}$

m is arbitrary. Then k is known as the commutator subgroup of group G.

- If $a, b \in G$, G is a group then $a\ b\ a^{-1}\ b^{-1}$ is called a commutator of a, and b in G.
- If S denotes the set of all commutors in G and G1 denotes the subgroup of G generated by S. Then G1 is called commutator subgroup of G or devided subgroup of G.

Theorem 1 : A group G is abelian if and only of the commutator subgroup of G is the Trivial group.

Proof : Let G be an abelian group

$\Rightarrow \forall\ a, b, \in G, a\ b = b\ a$

$\Rightarrow a\ b\ b^{-1}\ a^{-1} = e$

Therefore commutator subgroup whose elements will be the finite product of e's is the trivial group.

Conversely : Let the commutator subgroup be the trivial group. Then for any $e \in G, b \in G$

$\Rightarrow$ $a\ b\ a^{-1}\ b^{-1} \in \{e\}$

$\Rightarrow$ $a\ b\ a^{-1}\ b^{-1} = e$

$\Rightarrow$ $a\ b = b\ a$ $\forall a, b \in G$

$\Rightarrow$ G is abelian.

Theorem 2 : The commutator subgroup G^1 of G is a normal subgroup of G.

Proof : Let $a \in G^1$ and $x \in G$ be any element

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

Now $x\ a\ x^{-1}\ a^{-1} \in G^1$ and $a \in G^1$ is a subgroup of G

$\Rightarrow (x\ a\ x^{-1}\ a^{-1})\ a \in G^1$

$\Rightarrow x\ a\ x^{-1} \in G^1 \forall\ a \in G^1, x \in G$

So G^1 is a normal subgroup. [by dyiningof normal subgroup.]

Theorem 3 : Let G^1 be the commutator subgroup of G. Then G^1 is the smallest normal subgroup of G such that G/G^1 is abelian. Also of H be any normal subgroup of G then G/H is abelian $H\ G^1 \subseteq H$.

Proof : To prove G/G^1 is abelian group.

Let $a\ G^1$, $b\ G^1$ be any two element of G/G1, where $a, b \in G$

Now $a\ b\ a^{-1}\ b^{-1} \in G^1$

$\Rightarrow$ $(a\ b)(a\ b)^{-1} \in G^1$

$\Rightarrow$ $(a\ b)\ G^1 = b\ a\ G^1$ [$\because$ $a\ H = b\ H$ iff $ab^{-1} \in H$]

$\Rightarrow$ $(a\ G^1)\ (b\ G^1) = (b\ G^1)\ (a\ G^1)$ [$\because$ G^1 is normal subgroup)

$\Rightarrow$ G/G^1 is abelian group.

Now, to show G^1 is the smallest normal subgroup of G such that G/N is abelian.

Let $a, b \in G$ be any element

Then $\forall$ $a\ H, b\ H \in G/H$, since G/H is abelian

$\therefore$ $(a\ H)\ (b\ H) = (b\ H)\ (a\ H)$

$\Rightarrow$ $(a\ b)H = (b\ a)\ H$ [$\because$ H is normal in G]

$\Rightarrow$ $a\ b\ (b\ a)^{-1} \in N$

$\Rightarrow$ $a\ b\ a^{-1}b^{-1} \in N$

i.e. H contains all the commutators of G.

i.e. $H \geq G^1$ i.e. $G^1 \leq H$.

Hence G^1 is the smallest normal subgroup of G such that G/G^1 is abelian.

Also if H is normal subgroup of G such that G/H is abelian then $G^1 \subseteq H$.

Conversely, let $G^1 \subseteq H$ then $a\ b\ a^{-1}b^{-1} \in H$ $\forall$ $a_1\ b \in G$

[by definition of commutator]

$\Rightarrow$ $a\ b\ (b\ a)^{-1} \in H$

$\Rightarrow$ $a\ b\ H = b\ a\ H$

$\Rightarrow$ $a\ H\ b\ H = b\ H\ aH$

$\Rightarrow$ G/H is abelian

Hence the proof.

Self check Exercise-2

Q. 1 If G has not proper normal subgroup then $G = G^1$.

10.5 Summary

In this unit we studied that the

1. The smallest subgroup of a containing non empty subset S is known as subgroup generated by a subset of a group.
2. Subgroup generated by a smallest is equal to interaction of all subgroups of G containing S.
3. If $a, b \in G$ then a b a-1b-1 is called a commutator of a, b in G.

4. A group is abelian iff the commutator subgroup is the bivial group.

5. Commutator subgroup is a normal subgroup.

10.6 Glossary

- **Commutator element :** Let G be a group. The commutator element [g, h] of g and h in G is defined as $[g, h] = ghg^{-1}h^{-1}$.
- **Commutator subgroup :** The commutator subgroup consists of all elements of the forms $ghg^{-1}h^{-1}$ for $g, h \in G$.

10.7 Answer to self check exercise

Self Check Exercise - 1

Q. 1 Z

Self Check Exercise - 2

Q. 1 The only normal subgroup of group G are {e} and G which are trivial subgroup.

Gives $G^1 = \{e\}$ so $G^1 = G$ only.

10.8 References/ Suggested Readings

1. Vijay K. Khanna and S.K. Bhambri, A course in Abstract algebra.
2. Joseph A. Gallian, Contemporary Abstract Algebra.
3. Frank Ayrer Jr., Modern Algebra, Schaum's Outline Series.
4. A. R. Vasistha, Modern Algebra, KeishnaPrakasham Media.

10.9 Terminal Questions

Q. 1 Find the commutator subgroup of $G = \{\pm 1, \pm i, \pm k, \pm j\}$

Q. 2 Find the commutator subgroup of S_3.

Q. 3 Find the commutator subgroup of D_4.

*****

Unit - 11

Homomorphism and Isomorphism of Group

Structure

11.1 Introduction

Dear students, till yet we have not discussed about functions from one group to another group. In this unit we will discuss we will discuss various properties of function like preservation of composion, one and onto between group. On the basis of these properties we will define homomorphism, isomorphism and automorphism of groups.

11.2 Learning Objectives

After studying this unit, students will be able to

1. define homomorphism in group.
2. verify whether a function between groups is a homomorphism or not.
3. obtain the Kernal and image of any homomorphism of group.
4. define isomorphism in group
5. verify whether a function between groups is an isomorphism or not.
6. define automorphism in group.
7. verify whether a function between group is an automorphism or not.

11.3 Homomorphism

The functions between groups, which preserve the algebraic structure of their domain group, are known as group homomorphism. The term homomorphism is first introduced by mathematician Klein in 1893. The term homomorphism is divided term greek word 'homo' and 'morph', which togather means 'same shape'. A homomorphism is a mathematical tool for briefly expressing precise structural correspondences. It is a function between groups satisfying a few natural properties.

Domain Group : The group from which a function is originated is known as domain group.

Co domain Group : The group into which the function maps is known as co domain group.

Definition : Let G and G^1 be any two group with binary operation * and $*^1$ respectively. Then a mapping $f : G \Rightarrow G^1$ is said to be homomorphism if

$\forall$ a, b $\in$ G, f (a * b) = f (a) $*^1 f$ (b)

Homomorphic Image : Let G and G^1 be two group with mapping $f : G \Rightarrow G^1$, then group G^1 is called homomorphic image of the group G, if f is homomorphism and onto.

Let us try to save some questions to have better understanding of homomorphism.

Example 1 : Let G = {1, -1, i, -i} be a group under multiplication and I = group of all integers under addition. Then prove that $f : I \rightarrow G$ is a homomorphism where $f(n) = i^n \forall n \in I$.

Solution : Here domain group is I and its binary operation is addition whereas co domain group is G and m binary operation is multiplication.

Also given $f(n) = i^n \forall n \in I$

Let m, n $\in$ I, then

$f(m) = i^m$ and $f(n) = i^n$

Now $f(m+n) = i^{m+n}$

$= i^m . i^n$

$= f(m) . f(n)$

$\Rightarrow \quad f(m+n) = f(m).f(n)$

Hence f: I $\rightarrow$ G is a homomorphism.

Example 2 : Let G = {a, a^2, a^3, ... d^2} is a cyclic group under multiplication and its subgroup G^1 = {a^2, a^4, a^6 .....a^{12}} where $f(a^n) = a^{2n}$. Prove that f is homomorphism.

Solution : Here G is a group under multiplication and G^1 is the subgroup, so the binary operation on G1 will be multiplication.

Now let an and am be two elements of G, such that $f(a^n) = a^{2n}$ and $f(a^m) = a^{2m}$

Then f(an am) = $f(a^{n+m})$ [base is same so power can be added]

$= a^{2(n+m)}$ [$\because f(a^n) = a^{2n}$

$= a^{2m+2m}$

$= a^{2n}.a^{2m}$

$= f(a^n).f(a^m)$

$\Rightarrow \quad f(a^n.a^m) = f(a^n).f(a^m)$

Example 3 : Let Z be the group of all integers under addition and E be the group of even integers under addition.

Then show that the mapping $f : Z \rightarrow E$ defined by $f(x) = 2x$ is a homomorphism.

Solution : Given Z and E are group of all integers and group of integers, under addition respectively.

Let $x, y \in Z$ such that

$f(x) = 2x$ and $f(y) = 2y$

Now $f(x+y) = 2(x+y)$

$= 2x + 2y$

$= f(x) + f(y)$

$\Rightarrow f(x+y) = f(x) + f(y)$

Hence f is a homomorphism.

Endomorphism : A homomorphism from G to G is called an endomorphism.

Self Check Exercise - 1

Q. 1 Let Z be the group of all integer under addition and $G = \{2n, n \in Z\}$ be a group under multiplication then $f : Z \rightarrow G$ such that $f(n) = 2n \ \forall \ n \in Z$

Show that f is homomorphism.

Q. 2 Let Z be the group of integers under addition and G = {-1, 1} be the group under multiplication. Show that the mapping $f : Z \rightarrow G$ defined by

$$f(n) \begin{cases} 1 & \text{if n is even} \\ -1 & \text{if n is odd} \end{cases}, n \in Z$$

is a homomorphism.

11.4 Isomorphism and Isomorphic Group

Let G and G^1 be two groups. Let we are intersected to map from G to G^1 that relate group structure of f: $G \rightarrow G^1$. G to the group structure of G^1. An isomorphism is an example of structure relationship. If we known all about group G and known that f is isomorphism, we immediately know all about group structure of G^1, as it is structurally just a copy of G.

The term isomorphism is derived from Greek word isos and morph means equal term or shape.

Isomorphism : Let G and G^1 be any two groups with binary operation * and $*^1$ respectively. Then a mapping $f : G \to G^1$ is said to be isomorphism if

1. f is homomorphism
2. f is one-one i.e. distinct elements in G have distinct f-images in G^1
3. f is onto i.e. for every y, there is a x such that $f(x) = y$.

Isomorphic Group : Two groups G and G^1 are called isomorphic group if there exists a mapping $f : G \to G1$ such that f is homomorphism, one-one and onto.

If G is isomorphic to G1 then we write $G \cong G^1$

Let us by following question on isomorphic to have more understanding of this.

Question 1 : Let be the group of all real numbers under addition and R^+ is the multiplicative group of positive real numbers. Prove that the mapping $f : R \to R^+$ defined by $f(x) = e^x$ is an isomorphism.

Solution : In order to show that given mapping is isomorphism we have to show that mapping is homomorphism and one to one and onto.

***f* is homomorphism**

Let $x_1, x_2 \in R$ such that

$f(x_1) = e^{x1}$ and $f(x_2) = e^{x2}$

Now $f(x_1+x_2) = e^{x1+x2}$

$= e^{x1}. e^{x2}$

$= f(x_1) .f(x_2)$

$\Rightarrow$ $f(x_1+x_2) = f(x_1) .f(x_2)$

Hence f is homomorphism

***f* is one-one :**

Let $x_1, x_2 \in R$. Then

$\Rightarrow$ $f(x_1) = \Rightarrow f(x_2)$

$\Rightarrow$ $e^{x1} = e^{x2}$

$\Rightarrow$ taking log both side

$\Rightarrow$ $\log e^{x1} = \log e^{x2}$

$\Rightarrow$ $x_1 \log e = x_2 \log e$

$\Rightarrow$ $x_1 = x_2$

***f* is onto**

Let $y \in R+$ i.e. y is any positive real number.

Then log y is real number $\Rightarrow \log y \in R$

Now $f(\log y) = e^{\log y} = y$

Thus $y \in R^+ = 7 \exists \log y \in R$ such that $f(\log y) = y$.

So each element of R-1 is the f-image of some element of R. Thus f is onto.

Since $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ means two elements in R have the same f-image in R^+ only if they are equal. Consequently distinct elements in R have distinct f-image in R+. Therefore f is one-one and onto.

Since f is homomorphism and one-one and onto. Hence f is an isomorphism.

Question 2 : The additive group of integers Z and additive group of integral multiple of 5 under map $f : Z \rightarrow 5Z$ defined by $f(n) = 5n \forall n \in Z$ is an isomorphism.

Solution : Given map is $f : Z \rightarrow 5Z$ defined by

$f(n) = 5n \forall n \in Z$

f is isomorphism.

Let $n, m \in Z$ such that

$f(n) = 5n$ and $f(m) = 5m$.

Then $f(m+n) = 5(m+n)$

$= 5m + 5n$

$= f(n) + f(n)$

$\Rightarrow f(m+n) = f(m) + f(n)$

$\Rightarrow f$ is homomorphism

f is one-one :

Let $m, n \in Z$ then

$f(m) = f(n)$

$\Rightarrow 5m = 5n$

$\Rightarrow m = n$

So, f is one-one

f is onto

Let $y \in 5Z$

$\therefore y = 5n, n \in Z$

Since $n \in Z$, so $f(n) = 5n = y$

Thus each element of 5 z is a f-image of same element of Z. Thus f is onto.

Since f is homomorphism, one-one and onto. Hence f is an isomorphism.

Question 3 : Let G be the group of ordered pair of real number under operation (a, b) + (c, d) = (a+c, b+d) $\forall$ (a, b)(c, d) $\in$ G. Let R be the group of real number under addition let f : G $\rightarrow$ R defined by f(a, b) = a $\forall$ (a, b) $\in$ G. Check that f is an isomorphism or not.

Solution : Given G is an group of order pair of real number under addition and R is group of real number under addition.

To show f : G $\rightarrow$ G is an isomorphism we have to prove

1. f is homomorphism
2. f is one-one
3. f is onto

f is homomorphism

Let (a, b) (c, d) $\in$ G then

f(a, b) = a and f(c, d) = c

Now f [(a, b) + (G d)] = f (a + c, b + d) [by defining of G

= a + c [by dying f (a, b) = a

= f (a, b) + f (G d)

$\Rightarrow$ f [(a, b) + (, d) = f (a, b) + f (c, d)

So f is homomorphism.

f is one-one:-

Let (a, b), (c, d) $\in$ G Then

= f (a, b) = f (c, d)

= a = c, but a and c are distinct

so a $\neq$c

Let x = (1, 2) and y (1, 3)

f (1, 2) = f (1, 3)

1 = 1

But (1, 2)$\neq$ (1, 3)

Since different element has same image. So f is not one-one. So f is not isomorphism.

Epimorphism:- A homomorphism which is onto is called epimorphism.

Example 4:-Let C and R be the group of complex number and real number under addition. Then the map f : c $\rightarrow$ R defined by $\rightarrow$(x + iy) = x$\forall$x$f$iy$\in$C. Prove that f is epimorphism, not isomorphism.

Solution:-Since C and R be the group of complex and real number under addition respectively.

Given f: C $\rightarrow$ R such that + (x + iy) = x.

To prove f is epimorphism, we have to prove f is homomorphism and f is onto.

f is homomorphism :- Let $3_1, 3_2 \in \subset$

$f(3_1) = f(a + ib) = a$ and $f(3_2) = f(c + id) = \subset$

Now $3_1 + 3_2 = (a + ib) + (c + id)$

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

$\therefore$ $f(3_1 + 3_2) = f[(a + c) + i(b + d)]$

$= a + c$

$= f(a + ib) + f(c + id)$

$= f(3_1) + f(3_2)$

$\Rightarrow$ $f(3_1 + 3_2) = f(3_1) + (3_2)$

$\therefore$ f is homomorphism.

f is not one - one

Let $3_1 = 1 + 2i$

$3_2 = 1\ 3i$

$3_1, 3_2 \in \subset$

then $f(3_1) = f(H_2i) = 1$

$f(3_2) = f(1 + 3i) = 1$

$\Rightarrow$ $f(3_1) = f(3_2)$

but $3_1 \neq 3_2$

So, f is not one - one.

f is onto :-

Let $r \in R$

Then $r = r + io \in C$

so $f(r + io) = r$ [by defining of f]

So every element of co domain is animage of same element of domain. So f is onto.

Since f is homomorphism, and onto but not one-one Question So f is epimorphism but not isomorphism

Question 5:-Let Z and E be group of integers and even integers under addition respectively. The mapping $f : Z \rightarrow E$ defined by $f(x) = 2x\ \forall\ x \in Z$ isomorphism or not.

Solution : f is homomorphism [Check question 3]

To prove f is onto

Let $y \in E$ be any element

Then $y = 2x, x \in Z$ by defining $f : Z \to E$ $f(x) = 2x$

$\therefore$ $f(x) = 2x = y$

Since every element of codomain is an image of some element of domain. So f is onto.

Hence f is epimorphism.

Hence f is epimorphism.

To prove f is one-one

Let x_1 $y \in Z$ such that $f(x) = 2x$ and $f(y) = 2y$

$f(x) = f(y)$

$\Rightarrow$ $2x = 2y$

$\Rightarrow$ $x = y$

$\therefore$ f is one - one

So f is isomorphism.

Question 6:- Show that additive group of complex number $a + ib$, $a, b \in z$ is isomorphic to multiplicative group of rational numbers, $\{2^a 3^b, a, b \in Z\}$

Solution:- Let $G = \{a + i b ; a, b \in Z\}$ be the additive group of complex numbers.

and $G^1 = \{2^a 3^b, a, b \in Z\}$ be the multiplicative group of rational number.

Let $f : G \to G \to$ by is defined by

$f(a + i b) = 2^a 3^b \forall$ $a + i b \in G, a, b \in I$

To prove G is isomorphic to G^1 we have to show

(1) f is homomorphism

(2) f is one one

(3) f is onto

(1) f is homomorphism:- Let $x, y \in G$ be any two element then $x = a + ib$, $y = c + id$, $a, b, c, d \in Z$

Then $f(a + ib) = 2a\ 3a = f(x)$

and $f(c + id) = 2c\ 3d = f(y)$

Now $f(x + y)$

$\Rightarrow$ $f[(a+ib) + (c + id)] = f[(a+c) + i(b+d)]$

$= 2^{a+c} 3^{b+d}$

$= 2^a 2^c 3^b 3^d$

$= (2^a . 3^b)(2^c . 3^d)$

$= f(a + i b)\ f(c + i d)$

$= f(x)\, f(y)$

$= f(x + y) = f(x)\, f(y)$

So f is homomorphism.

2. f is one - one:-

Let $x, y \in G$ such that

$f(x) = f(y)$

$\Rightarrow$ $f(a + ib) = f(b + id)$

$\Rightarrow$ $2^a 3^b = 2^c \cdot 3^d$

$\Rightarrow$ $\frac{2^a 3^b}{2^c 3^d} = 1$

$\Rightarrow$ $2^{a-c} 3^{b-d} = 1 = 2^0 3^0$ [$\because$ anything raise to power 0 is 1]

$\Rightarrow$ $a - c = 0$ and $b - d = 0$

$\Rightarrow$ $a = c$ and $b = d$

$\Rightarrow$ $a + ib = c + id$

$\Rightarrow$ $x = y$

So f is one - one.

3. f is onto:-

Let $y \in G^1$ be any element, then f a, $b \in Z$ such that

$y = 2^a 3^b$

Thus corresponding to every $y \in G^1$, f $a + ib \in G$ such

that $f(a + ib) = 2^a 3^b$

$\therefore$ f is onto

Since f is homomorphism, one-one and onto

So f is isomorphism

and G is isomorphic to G^1.

Automorphism: A homomorphism from $G \to G$ which is one-one and onto is known as automorphism. How note that domain and codomain groups are same.

Question 7. Let R^+ be the multiplicative group of stoutly position real numbers. Prove that the mapping f $R^+ \to R^+$ defined by $f(x) = x^2 \forall\ x \in R^+$ is automorphism.

Solution: Given f + $R^+ \to R^+$

defined as $f((x) = x^2 \forall\ x \in R^+$

To show f is automorphism, we have to show

1. f is homomorphism or endomorphism
2. f is one = one
3. f is onto

f is homornorphism/endomorphism

Let x, y $\in$ R^+ such that f((x) = x^2, f(y) = y^2

Now, f(xy) = $(xy)^2$

= x^2 y^2

= f(x). f(y)

$\Rightarrow$ f(xy) = f(x). f(y)

So f is homomorphism.

f is one-one:-

Let x, y $\in$ R^+ then f(x) = x^2 and f(y) = y^2

such that f(x) = f(y)

$\Rightarrow$ $x^2 = y^2$

$\Rightarrow$ x = y

$\Rightarrow$ f is one-one

f is onto :-

Let for any x $\in$ R+ $\exists$ $\sqrt{x} \in$ R+ such that

$\Rightarrow$ $f\left(\sqrt{x}\right) = \left(\sqrt{x}\right)^2 = x$

$\Rightarrow$ $f\left(\sqrt{x}\right) = x$

So f is onto.

Since f : $R^+ \rightarrow$ R^+, is homomorphism, one-one and onto So, f is auto morphism i.e. isomorphism of R^+ onto itself.

Question 8:- Show that the mapping ϕ : $\leftrightarrow$ c given by (x + iy) = x = iy, is an automorphism. Here c is the additive group of complex number.

Solution:- Given f : $\leftrightarrow$ c defined by ϕ (x + iy) = x - iy

f is homomorphism = Let 3_1, $3_2 \in \subset$ here

3_1 = a + iy and 3_2 = c + id

then $f(3_1)$ = a = ib and $f(3_2)$ = c - id

Now f (3_1 + 3_2) = $f\left[\left(a+ib\right)+ f\ (c+id)\right]$

$= f\left[(a+c)+i(b+d)\right]$

$= (a + c) - i (b + d)$

$= (a - ib) + (c - id)$

$= f(3_1) + f(3_2)$

$\Rightarrow \quad f(3_1 + 3_2) = f(3_1) + f(3_2)$

$\Rightarrow \quad f$ is homomorphism

f is one-one:-

Let $3_1, 3_2, \in$ c such that

$f(3_1) = f(3_2)$

a - ib = c - id

Using equality of complex numbers

a = c, b = d

$\Rightarrow$ a = ib = c + id

$\Rightarrow \quad 3_1 = 3_2$

So f is one - one

f is onto :

Let $3 \in$ c $\quad \Rightarrow \quad$ a + ib$\in$ c, then a - ib$\in$ c

such that f (a + ib) = a - ib

$\Rightarrow \quad f$ is onto

So f is automorphism.

Self Check Exercise - 2

Q. 1 Let R^+ be multiplicative group of all positive real numbers and R be additive group of all real numbers. Then show that the mapping $f : R^+ \to R$ defined by $f(x) = \log x \forall\ x \in R^+$ is an isomorphism.

Q. 2 Prove that multiplicative group of all matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, a, b, c, d are real number not both equal to zero, is isomorphic to group of non zero complex number a + ib, a, b $\in$ R, $a^2 + b^2 \neq 0$ under multiplication.

Q.3 Prove that a group is abelian the mapping $f : G \to G^1$ defined by $f(x) = x^{-1}$ is an automorphism.

Q.4 Prove that if for a group $f : G \to G$ is given by $f(x) = x^3$, $x \in G$ is an isomorphism, then G is abelian.

11.5 Kernel of Homomorphism :

Let G and G1 be two groups and $f : G \to G^1$ be a homomorphism. Then kernel of f is defined as

Kernel to $f = \{x \in G : f(x) = e^1\}$ where e1 is identity element of G^1

Kernal of f is denoted by Ker$f$

Image of Homomorphism:- A group G1 is called homomorphic image of a group G is there exists a mapping $f : G \to G1$ such that f is homomorphism and onto.

Let us try to find kerpel of homomorphism for some functions as given below:

Question 1: Find Kernel of f, for $f : 2 \to G$ defined by $f(n) = 2^n$, $n \in Z$, where is the group of integer under addition and $G = 2^n$, $n \in Z$, is a group under multiplication.

Solution:- First to show that $f : Z \to G$ is f is homomorphism

Let $m, n \in Z$

Such that $f(m) = 2^m$ and $f(n) = 2^n$

Now $f(m + n) = 2^{m+n}$

$= 2^m . 2^n$

$= f(m) . f(n)$

$\Rightarrow$ $f(m+n) = f(m) . f(n)$

So f is homomorphism.

Since $f : Z \to G$

Since G = n, is a group under multiplication, $n \in Z$

Since $2^o = I \in G$ will act as identity element of group G

Now using the defining of karnel of homomorphism

Ker $f = \{n \in Z : f(n) = 1\}$

$= \{n \in Z, f(n) = 2^n = 1 = 2^o\}$

$= \{n \in z ; n = 0\}$

$= \{0\}$

$\therefore$ Ker $f = \{0\}$

Question 2: Given $f : Z \to \in$ defied by $f(x) = 2x \ \forall \ x \in Z$ is homomorphism. Find kernal of f. Here Z is set of integers and E is set of even integer under addition.

Solution:- Given $f : Z \to E$ is a homomorphism.

To find kernel of f. By definition of kernel of homomorphism, the identity element of E i.e. set of even integer under addition is 0.

So Ker $f = \{x \in Z : f(x) = 0\}$

$= \{x \in Z : 2x = 0\}$

$= \{x \in Z : x = 0\}$

Ker $f = \{x\}$

Self Check Exercise - 3

Q. 1 Find Kernel of f for all the questions done in the section of homomorphism and isomorphism.

11.6 Summary

Dear Students in this unit, we studied that

1. If $f : G \to G^1$, and this mapping preserver the Compositions in G and G1 then f is homomorphism.
2. If $f : G \to G$, then the homomorphism from G to G is known as endomorphism
3. If $f : G \to G^1$, then the homomorphism which is one-one then it is known as monomorphism
4. If $f : G \to G^1$, then the homomorphism which is onto is known as opimorphism.
5. If $f : G \to G^1$, then the homomorphism which is one-one and onto is known as isomorphism.
6. If $f : G \to G$, then the homomorphism which is one-one and onto is known as automorphism.
7. If $f : G \to G^1$, is the homomorphism then Ker $f = \{x \in G : f(x) = e^1\}$ where e^1 is identity element of group G^1.

11.7 Answers to Self Check Exercises

Self Check Exercise -1

Q. 1 $f : Z \to G$

then for $n_1, n_2 \leftarrow Z$

$f(n_1 + n_2) = f(n_1).\ f(n_2)$

Q.2 Prove $f(n_1 + n_2) = f(n_1)\ f(n_2)$, $n_1, n_2 \in Z$

for there different cases

1. when n_1, n_2 are even
2. when n_1, n_2 are odd
3. when one of n_1, n_2 is even and other is add.

Self Check Exercise - 2

Q. 1 Show that f is homomorphism, one-one and onto

Q. 2 Cheek the properties of homomorphism, one-one and onto.

Q.3 To prove f is automorphism how that f is homomorphism, one-one and onto from G to G i.e. fro in same group G.

Q.4 Show that f is homomorphism, one-one and onto.

Self Check Exercise 3

Q. 1 Ker f = {4}

Q. 3 Ker f = {0}

Q. 4 Ker f {0}

Q. 2 Ker f {0}

Q.3 Ker f = {(o, b) : (b $\in$ R}

11.8 Glossary

- **Domain Group:** The group from which a function is originated is known as domain group.
- **Epimorplism:** A homomorphism which is onto is called epimorplism.
- **Kernal of homomorplism:** Let f : G - G^1 be a homomorplism. The Kernal of f = {x $\in$G : F(n) = e^1} where e^1 is identity of G^1.

11.9 References/Suggested Reading

1. Vijay K. Khanna and S.K. Bhambari, A course in Abstract Algebra
2. Joseph A Gallian, Contemporary Abstract Algebra
3. Flank Ayers Jr. Modern Algebra, Schaunis outline Series
4. A.R. Varistha, Modern Algebra, Krishna Perkashan Media.

11.10 Terminal Questions

Q.1 If G is the multiplicative group of nxnnon singular real matrices and R^+ be the multiplicative group of non zero real numbers, then show that the mapping f : G $\rightarrow$ R^+ defined by f(A) = |A|, $\forall \in$ G is a homomorphism, onto. Also find ker$f$.

Q.2 Prove that every cyclic group of order n is isomorphic to the group of n^{th}root of unity under multiplication.

****

Unit - 12

Theorems On Homomorphism

Structure

12.1 Introduction

Dear Students, though on isomorphism is a special case of homomorphism. Yet oath the concepts have totally different roles. Homomorphism act as investigative tool in group theory. We may understand the cocept homomorphism by wing this analogy between homomorphism and photography. A photograph of a person cannot tell us about the person's exact height, weight or age. But from photograph we are able to decide that a person is tall or short, heavy or thin, old or young, male or female. In the same way homomorphic image of a group gives us some information about the group. By several homomorphic images of a group we can know more about the group. So dear student in this unit we shall prove some results about relation between homomorphism and different types group in the form of some theorem.

12.2 Learning Objectives

After studying this unit student will be able to

(1) Prove some basic theorems on homomorphism

(2) State and prove first theorem on homomorphism

(3) Apply theorems of homomorphism in group

12.3 Theorems on Homomorphism

Theorem 1:- Let f is homomorphism of G into G^1. $f : G \to G^1$ is a homomorphism then $f(e) = e^1$ when e and e^1 are identity elements of G and G^1 respectively. Or, then f caries the identity of G into identity of G^1

Given f G $\to$ G^1

Proof:- Let g $\in$G

then f (g) $\in G^1$

As e^1 is identity element of group G^1i e $e^1 \in G^1$ Since G^1 is a group, so closed under multiplication.

So f (g). $e^1 = f$ (g)

$= f$ (ge) [as e is identity of group G]

$\Rightarrow$ f (g). $e^1 = f$ (ge)

Since f is a homomorphism

f (g) . $c^1 = f$ (ge) = f (g). f (e)

Since G^1 is a group, So Cancellation law holds

$\Rightarrow$ $e^1 = f$ (e)

$\Rightarrow$ f (e) = e^1

Theorem 2 : If f is a homomorphism of G into G^1 i.e. $f : G \rightarrow G^1$ ten F $(g^{-1}) = [f (g)]^{-1} \forall$ g $\in$G

Proof : Given $f : G \rightarrow G^1$ is a homomorphism

Let g $\in$G, Since G is a group, So every element has a inverse. Let inverse of of is sg-1.

So G, $g^{-1} \in$ G

Since f is a homomorphism

f (g) .f $(g^{-1}) = f$ $(g\, g^{-1})$

$= f$ (e)

$= e^1$ [Using theorem 1]

Also f (g^{-1}) f (g) = f $(g^{-1}g)$

$= f$ (e)

$= e^1$

$\Rightarrow$ f (g) .f $(g^{-1}) = e^1 = f$ (g^{-1}) .f (g)

$\Rightarrow$ $[f (g)]^{-1} = f$ (g^{-1}) $\left[\begin{array}{l} a.b = e \\ then\, b = a^{-1} \end{array}\right]$

Hence proved

Theorem 3:- Let f is a homomorphism of G into G^1 i.e. $f : G \rightarrow G^1$ with Kernel K, then Kernel f is normal subgroup of G.

Proof : Given $f : G \rightarrow G^1$ is a homomorphism with key = Kunel$f$ = {x $\in$ G ; f (x) = e^1}

Since G and G1 are group; Let e and e^1 be identity elements of G and G^1.

We have to show that Ker f = k is normal subgroup of G. We first prove that k is a subgroup of G and then will prove k is a normal subgroup of G.

K is a subgroup of G:-

Since e is identity of G and by theorem 1,

f (e) = e^1, e $\in$ G.

So k $\neq \phi$.

Let x, y $\in$ k be any two elements.

So by definition of k, f f (x) = e^1

f (y) = e^1

Since y $\in$ k

Now f (y^{-1}) = [f (y)]$^{-1}$

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

$\Rightarrow$ f (y^{-1}) = e^1

$\Rightarrow$ $y^{-1} \in$ k

f (xy^{-1}) = f(x) f (y^{-1}) [$\because$ f is homomorphism]

= f (x) [f (y)]$^{-1}$ [Using theorem 2]

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

= e^1e^1

= e^1

f (xy^{-1}) = e^1

$\Rightarrow$ xy-1 $\in$K $\forall$ x, y $\in$ k

Hence k is a normal subgroup of G.

K is normal subgroup of G

Let g $\in$G and, x $\in$ k be any element

f since x $\in$ k $\Rightarrow f$ (x) = e^1

So f ($g x g^{-1}$) = f (g) f (x) f (g^{-1}) [$\because$ f is homomorphism]

= f (g) e^1 [f (a)]$^{-1}$ [$\because$ f (g^{-1}) = [f (g)]$^{-1}$

= f (g) [f (g)]$^{-1}$

= e^1

$\Rightarrow$ f ($g x g^{-1}$) = e^1

$\Rightarrow$ $g x g^{-1} \in$ k

They $g \times g^{-1} \in k$ when $g \in G$ and $x \in k$

Hence $k = \ker f$ is normal subgroup of G.

Theorem 4: The homomorphism $f : G \to G^1$ is an isomorphism if and only if $\ker f = \{e\}$ i.e. $\ker f$ consist only identity element of G.

Proof:- Given $f : G \to G1$ is a homomorphism of G to G^1. Let e and e1 be identity element of G and G^1 respectively. Also let kernel f is given by k. Let f is an isomorphism to prove $\ker f = \{e\}$ Since f is an isomorphism, so f is one-one, onto homomorphism.

Let $a \in \ker f$

then by definition of $\ker f$, $f(a) = e^1$

$\Rightarrow$ $f(a) = e^1 = f(e)$ [$\because$ Theorem 2 $f(e) = e^1$]

$\Rightarrow$ $a = e$

Thus $a \in \ker f \Rightarrow a = e$

So e is the only element of G which belongs to $\ker f$.

Thus $\ker f = \{e\}$

Conversely:- If $\ker f = \{e\}$ then to show f is isomorphism of G to G^1 it is sufficient to prove f is one-one.

Let $a, b \in G$, then $f(a) = f(b)$

$\Rightarrow$ $f(c)\,[f(b)]^{-1}$

$\Rightarrow$ $f(a)\, f(b^{-1}) = e^1$ [$\because$ $[f(b^{-1})] = [f(b)^{-1}]$ and $f(b).\,[f(b)]^{-1} = e$

$\Rightarrow$ $f(a\, b^{-1}) = e^1$ [$\because$ f is homomorphism]

$\Rightarrow$ $ab^{-1} \in \ker f$ [by defining of $\ker f$]

$\Rightarrow$ $ab^{-1} = e$ $\because \ker f = \{e\}$

$\Rightarrow$ $ab^{-1}\, b = eb$

$\Rightarrow$ $a = b$

$\Rightarrow$ f is one - one

Hence f is isomorphism of G into G^1.

Theorem 5: Let H be a normal subgroup of a group G. Also let $f : G \to G/H$ be a map defined by $f(x) = Hx \forall\, x \in G$. Then f is a homorphism of G onto G/H with H as kernel of f.

Proof: Given the mapping $f : G \to G/H$ is defined by $f(x) = H\,x \;\forall x \in G$.

$\Rightarrow$ H x is any element of G/H, for $x \in G$.

So the mapping is onto.

f is Homomorphism $G \to G/H$

Let a, b $\in$ G Then, f(a) = Ha and f(b) = Hb

f (ab) = Hab [by defining f (x) = Hx

= (Ha) (Ha) [$\because$ H is normal]

= f (a) f (b)

$\Rightarrow$ f (a b) = f (a) f (b)

$\therefore$ f is homomorphism of G onto G/H.

So every quotient group of a group is a homomorphic image of that group.

Now to prove ker$f$ = H

Let ker$f$ be the kernel of homomorphism f. Also we know that identy element of quotient group G/H is the coset of H

So ker$f$ = {y $\in$G ; f (y) = H}

= {y $\in$G ; H y = H}

= { y$\in$ G, y $\in$ H}

= H [$\because$ H is subgroup of G.]

So Ker f = H

Hence proved

Theorem 6 : Every homomorphic image of a group is isomorphic to some quotient group of G.

This is also known as fundamental theorem on Homomorphism.

Let G and G^1 be two group and f : G $\rightarrow$ G^1 is homomorphism G onto G^1. If H is the kernel of f. Then G/H $\cong$ G^1.

Proof : Since H is kernel of f, and kernal of f is a normal subgroup. So H is a normal subgroup of a group G.

So, G/H = {Ha ; a $\in$ G} is a quotient group under the composition, (Ha) (Hb) = Hab $\forall$ Ha, Hb $\in$ G/H [by defining composition, (Ha) (Hb) = Hab $\forall$ Ha, Hb $\in$ G/H [by defining]

Let us define a map f : G G/H by

f (a) = Ha ; a $\in$ G

To prove f is homomorphism and onto

***f* is homomorphism :**

Let a, b $\in$ G such that f (a) = Ha, f(b) = H (b)

$\Rightarrow$ ab $\in$ G [$\because$ G is a group]

Now f (ab) = Hab

= (Ha) (Hb) [$\because$ H is normal Subgroup of G]

$= f(a)\, f(b)$

$\Rightarrow \quad f(ab) = f(a)\, f(b)$

So, f is homomorphism

f is onto :

Let $X \in G/H$ be any element

$X = Ha$; for some $a \in G$ such that

$f(a) = Ha = X$

$\therefore \quad f$ is onto.

So, $f : G \to G/H$ is homomorphism and onto.

$\Rightarrow \quad G/H$ is homomorphic image of G.

Conversely: Let group G^1 is the homomorphic image of G. So, there exist a map $f : G \to G^1$ such that f is homomorphism and onto.

Let $H = \ker f$

$\Rightarrow \quad H$ is normal subgroup of G.

$\therefore \quad G/H$ forms a quotient group.

Let $f : G/H \to G^1$ by

$\phi(Ha) = f(a), \forall\ Ha \in G/H$

If $Ha \in G/H^1$ then $a \in G$ [by defining of Quotient group]

$\therefore \quad f(a) \in G^1$

$\Rightarrow \quad f(Ha) \in G^1$ [$\because f : G \to G^1$]

To show ϕ is well defined homomorphism, one one and onto.

ϕ is well defined :

Let $Ha, Hb \in G/H$ and onto.

$Ha = Hb$

$\Rightarrow \quad ab^{-1} \in H$, here H is the Kernel of F.

$\Rightarrow \quad f(an^{-1}) = e^1$ {e^1 is identity element of G^1}

$\Rightarrow \quad f(a)\, f(b^{-1}) = e^1$ [$\because f$ is homomorphism]

$\Rightarrow \quad f(a)\, [f(b)]^{-1} = e^1$ [$\because f(a^{-1}) = [f(a)]^{-1}$ [by theorem 2]

$\Rightarrow \quad f(a)\, [f(b)]^{-1} f(b) = e^1 \quad f(b)$ [multiplying both side by $f(b)$

$\Rightarrow \quad f(a) = f(b)$ [$\because f(b^{-1})]\, f(b) = e$ and $e^1 f(b) = f(b)$]

$\Rightarrow \quad \phi(Ha) = \phi(Hb)$

So ϕ is well defined

ϕ is homomorphism

Let Ha, Hb $\in$ G/H, a, b $\in$ G

Now ϕ (Ha.Hb) $= \phi$ (H ab)

$= f$ (ab)

$= f$(a) f (b) [$\because f$ is homomorphism]

$= \phi$ (Ha) .ϕ (Hb)

$\Rightarrow$ ϕ(Ha.Hb) $= \phi$ (Ha) . ϕ (Hb)

$\therefore$ ϕ is homomorphism of G/H into G^1

ϕ is one-one

Let Ha, Hb $\in$ G/H such that

ϕ (Ha) $= \phi$ (Hb)

$\Rightarrow$ f(a) $= f$ (b)

$\Rightarrow$ f(a) $[f(b)]^{-1} = f(b)\,[f(b)]^{-1}$ [multiplying both side by $[f(b)]^{-1}$

$\Rightarrow$ $f(a)\,f(b^{-1}) = e^1$ [$\because$ $[f(b)]^{-1} f(b^{-1})$ and $f(b)\,(f(b))^{-1} = e^1$]

$\Rightarrow$ $f(ab^{-1}) = e^1$ [$\because f$ is homomorphism]

$\Rightarrow$ $ab^{-1} \in$ Ker f [by defining of Ker f]

$\Rightarrow$ $ab^{-1} \in$ H [$\because$ H = Ker f]

$\Rightarrow$ Ha = Hb [$\because$ H is normal subgroup of G]

$\Rightarrow$ ϕ is one - one.

Some Results Related to Homomorphism

If f G $\rightarrow G^1$ be a homomorphism. Then

1. For any subgroup H of G, f(H) is a subgroup of G^1.
2. For any subgroup K^1 of G^1; f^{-1} (K^1) is a subgroup of G containing Ker f and $f^{-1}(K^1)$ is normal in G whenever K^1 is normal in G^1.
3. If f is onto, then for any normal subgroup K of G, f(K) is normal subgroup of G^1.

Let us do some questions related to these theorems for their application part.

Question 1 : Let f and g be homomorphism from G to G^1.

Show that H = {x $\in$ G; f(x) = g(x)} is a subgroup of G.

Solution : Given f. g are homomorphism from G to G^1

Let e and e^1 be the identity element of G and G^1 respectively, then

$f(e) = g(e) = e^1$ [$\because f : g \to G^1$ and $g : G \to G^1$]

$\Rightarrow$ $e \in H$ by using defining of H.

$\Rightarrow$ $H \neq \phi$

H is non empty set.

To show, H is a subgroup of G, we have to prove $xy^{-1} \in H$ for $x, y \in H$.

So let $x, y \in H$ be any two elements.

So by defining of H, $f(x) = g(x)$ and $f(y) = g(y)$

Now $f(xy^{-1}) = f(x)\, f(y^{-1})$ [$\because f$ is homomorphism]

$= f(x)\, [f(y)]^{-1}$ [$\because f(y^{-1}) = [f(y)]^{-1}$ as f is homomorphism]

$= g(x)\, [g(y)]^{-1}$ [$\because$ g is homomorphism so $g(y^{-1}) = [g(y)]^{-1}$]

$= g(xy\text{-}1)$ [$\because$ g is homomorphism]

$\Rightarrow$ $f(xy^{-1}) = g(xy^{-1})$.

so for, $x, y \in H$, $f(xy^{-1}) = g(xy^{-1})$

$\Rightarrow$ $xy^{-1} \in H$

Hence H is a subgroup of G.

Question 2 : Find all subgroups of Z/21Z

Solution : Let K be a subgroup of Z/21Z

Then K = H/21Z, for some subgroup H of Z

satisfying $21Z \subseteq H$.

As H is a subgroup of Z, such that $21Z \subseteq H$, then

H/21Z is a subgroup of Z/21Z.

In order to find all subgroup of Z that contain 21Z, we have to find positive divisor of 21

Since, 1, 3, 7, 21 are only positive divisor of 21

So Z, 3Z, 7Z and 21Z are only subgroup of Z that contain 21Z

Hence Z/21Z, 3/21Z, 7Z/21Z and 21Z/21Z {e} are the only subgroup of Z/21Z.

Question 3 : Show that the group $6Z/30Z \cong Z_5$ where

$Z_5 = \{[0], [1], [2], [3], [4], +_5\}$ bea additive group of residue classes module 5.

Solution : Let $f : 6Z \to Z_5$ be a mapping defined as $f(6Z) = [n]\ \forall\ n \in Z$

To show f is homomorphism and onto

f is homomorphism

Let $m, n \leftarrow Z$, then $6m, 6n \in 6Z$

So, $f(6m + 6n)$ $= f\ (6(m+n))$

$= [m + n]$

$= [m] + [n$

$= f(6m) + f(6n)$

$\Rightarrow$ f is homomorphism

f is onto

For $[n] \in Z_5$, $n \in Z$

$\Rightarrow$ $6n \in 6Z$ such that $f(6n) = [n]$

$\Rightarrow$ f is onto

Using fundamental theorem of homomorphism

$6Z/\text{Ker } f \cong Z_5$.

Now, to show Ker $f = 30Z$

Since [0] is identity element of Z_5

Since Ker f $= \{6n \in 6Z, f(6Z) = [0]\}$

$= \{6n \in 6Z, [n] = [0]\}$

$= \{6n \in 6Z;$ n is a multiple of 5$\}$

$= \{6n \in 6Z, n = SK, K \in Z\}$

$= \{6.5\ K \in 6Z\}$

$= \{30\ Z\}$

Ker $f = 30Z$

Hence $6Z/30Z \cong Z_5$.

Self Check Exercise-1

Q. 1 Find all the subgroups of Z/24Z.

Q. 2 Show that the group $4Z/12Z \cong Z_3$.

Q. 3 Show that $GL(2_1R)\ /SL(2_1R) \cong R$.

12.4 Summary

Dear Students in this unit, we studied that

1. If $f : G \to G^1$ is homomorphism, then f carries the identity of G into identity of G1.
2. If $f : G \to G^1$, is homomorphism, then $f(g^{-1}) = [f(g)]^{-1}$.
3. If $f : G \to G^1$, is homomorphism, then Ker f is normal subgroup of G.

4. If $f : G \to G^1$, is homomorphism is isomorphism iff $\ker f = \{e\}$'

5. Every homomorphic image of a group is isomorphic to same quotient group of G.

12.5 Answers to Self Check Exercises

Self Check Exercise -1

Q. 1 Z/24Z, 2Z/24Z, 3Z/24Z, 4Z/24Z, 6Z/24Z, 8Z/24Z, 12Z/24Z, 24Z/24Z

Q.2 Same as Question 3.

Q. 3 Same as Question 3.

12.6 Glossary

- **Homomorphism :** Let G and G^1 be the two group with binary operation * and $*^1$ respectively. Then a mapping $f : G \to G^1$ is said to be homomorphism is $\forall$ a, b $\in$ G, $f(a*b) = f(a)*^1 f(b)$.
- **Isomorphism :** A mapping $f : G - G^1$ is said to be isomorphism, is f is homomorphism and f is one-one and onto also.

12.7 References/Suggested Reading

1. Vijay K. Khanna and S.K. Bhambari, A course in Abstract Algebra
2. Joseph A Gallian, Contemporary Abstract Algebra
3. Flank Ayers Jr. Modern Algebra, Schaunis outline Series
4. A.R. Varistha, Modern Algebra, Krishna Perkashan Media.

12.8 Terminal Questions

Q.1 Prove that every group is isomorphic to a permutation group.

Q.2 Any infinite cyclic group is isomorphic to additive group of integers.

****

Unit - 13

Ring

Structure

13.1 Introduction

Dear student, in previous unit we studies about group which is an algebraic structure equipped with one binary operation. Here in this unit we shall study ring, which is again an algebraic structure equipped with two binary operations. In this unit we will study the definition of ring along with same examples and will prove some theorems base on ring.

13.2 Learning Objectives

After studying this unit, students will be able to

1. define ring
2. give examples of ring.
3. can prove a given algebraic structure with defined binary operation is a ring
4. prove the theorem base on ring.

13.3 Definition of Ring

Let R be a non-empty set in which there are defined two binary operations called addition and multiplication, denoted by '+' and '.' respectively, then the algebraic structure (R1 + .) is called a ring if the following axioms are satisfied :

Axioms of additions

1. **Closure property :** $\forall$ a, b $\in$ R, a + b $\in$ R.

2. **Associative property :** $\forall$ a, b, c $\in$ R, a +(b+c) = (a+b)+c

3. **Existence of additive identity :** $\forall$ a $\in$ R, $\exists$ and element O$\in$R such that a + 0 = a = 0+a.

4. **Existence of additive inverse :** $\forall$ a $\in$ R, $\exists$ - a$\in$R such that a+(-a) + a.

5. **Commutative under addition :** $\forall$ a, b $\in$ R, a + b = b+a.

Axioms of Multiplication

6. **Closure Property :** $\forall$ a, b $\in$ R, a.b$\in$ R

7. **Associative Property :** $\forall$ a, b, c $\in$ R, a(bc) = (ab) c

Axiom of distributivity

Multiplication is distributive with respect to addition i.e. $\forall$ a, b, c $\in$ R

a.(b+c) =a.b + a.c Left distributive law

and

(b+c).a = b.a + c.a Right distributive law

So any algebraic structure with two binary operation satisfies above properties is known as a ring.

Note

1. From the definition, it is clear that a ring is cumulative or abelian group under addition and semi group under multiplication which satisfies distributive property.
2. The element O $\in$ R is the additive identity. It is known as zero element of φ the ring. As identity element is unique, So every ring has a unique zero element.

Ring with Unity : If a ring possesses multiplicative identity. They it is known as ring with unity. Mathematically, if in a ring R_1 there exists an element denoted by 1 such that $\forall a \varepsilon R$, a.1 = 1.a = a, then R is called a ring with unity. The element IεR, is called the unit element of the ring.

Commutative Ring : If in a ring R, the multiplication composition is also commutative i.e. $\forall$ a, b $\in$ R a. b = b. a then R is called a commutative ring.

To have more understand of ring let us take following examples:

Example: The set I of all intergers is a ring with respect to addition and multiplication of integers. This ring is known as ring of integers.

Solution: Axions of addition

(1) Closure Property:-

$\forall$ a, b $\in$ I, a + b $\in$ I, as sum of two integers is an integer.

(2) Associative Property:-

Associative property holds in integers, so if $\forall$ a, c $\in$ I a + (b + c) = (a + b) + c.

(3) Existence of additive identity:-

Since $0 \in I$, so $\forall a \in I$

$a + 0 = 0 + a = a$. So, 0 is additive identity

(4) Existence of additive inverse:-

$\forall \in I$, there exist $-a \in I$, such that

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

So, -a is additive inverse of a.

(5) Commutative property:-

Commutative property holds in integers. So $\forall\ a, b \in I\ a + b = b + a$.

So I is an abelian group.

Axioms of multiplication

(6) Closure Property under multiplication:-

Since product of two integer is again an integer so $\forall a, b \in I, ab \in I$

So, set of integer is closed under multiplication.

(7) Associative property:-

Associative law holds in integer under multiplication so $\forall\ a, b, c \in I$, $a(bc) = (ab)c$.

Axioms of distributivity

(8) Since multiplication of interger is distributive with respect to addition of integers, so $\forall\ a, b, c \in I$

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

and $(b + c) a = ba + ca$.

So the set of integer I is a ring under addition and multiplication.

Remark: The set I is a commutative ring with Unity.

Since $1 \in I$, so $\forall a \in I$ $a.1 = a$, so 1 act as multiplicative identity. So the set I is ring with Unity.

Again multiplication is commutative in integers i.e. $\forall\ a, b \in I$

$a.b = b.a$.

So, the set I is a commutative ring with unity.

Example 2: Let the set] [i], set of all complex number a + ib, where a and b are integer. Then show that the set] [i] is a ring under addition and multiplication of complex number.

This ring is known as ring of Gaussian integers.

Solution: Give][i] = {a + ib ; a.b$\in$ I}

Since element of][i] are complex number, so all properties of complex numbers are two for the set][i].

Axioms Under Addition

(1) Closure Property:-

Let x, y $\in$][i], such that

x = a + ib

y = c + id, a, b, c, d $\in$ I

Then x + y = (a + ib) + (c + id)

= (a + c) + i(b + d)

$\in$][i] [$\therefore$ a + c $\in$ I, b + d $\in$ I

Hence][i] is closed under addition.

(2) Associative Property:-

Let x, y, z $\in$][i] such that

x = a + ib

y = c + id

z = c + if, a, b, c, d, e, f $\in$ I

Then (x + y) + z = $\left[\left(a+ib\right)+\left(c+id\right)\right]+\left(e+if\right)$

= $\left[\left(a+c\right)+\left(b+d\right)\right]+\left(e+if\right)$

= (a + c + e) + I (b + d + f).

as addition is associative for integers, so

$=\left[a+\left(c+e\right)\right]+i\left[b+\left(d+s\right)\right]$

$=\left(a+ib\right)+\left[\left(c+e\right)+i\left(d+f\right)\right]$

$=\left(a+ib\right)+\left[\left(c+id\right)+\left(e+if\right)\right]$

= x + (y + z)

Hence (x + y) + z = x + (y + z)

So Associativity holds in][i]

(3) Existence of additive identity:-

Let $x = a + ib \in][i]$, $a, b \in I$.

we know that $0 \in I$, so $0 + i0 \in][i]$ such that

$x + 0 = (a + ib) + (0 + i0) = (a + 0) + I (b + 0)$

$= a + ib$

$= x$

$= 0 + x$

Hence $0 + i0$ is the additive identity of $][i]$.

(4) Existence of additive inverse:

Let $x = a + ib \in][i]$, $a, b \in I$, then $-a, -b \in I$ such that $xa + ib + \left[-a + i(-b)\right] = \left[a + (-a)\right] + i\left[b + (-b)\right]$

$= 0 + i0$

$= 0$

$= \left[-a + i(-b)\right] + \left[a + ib\right]$

(5) Commutative under addition

Let $x, y \in][i]$ such that

$x = a + ib$

$y = c + id$, $a, b, c, d \in I$

Then $x + y = (a + ib) + (c + id)$

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

$= (0 + a) + I (d + b)$ [$\therefore$ addition is commutative for integers]

$= (c + id) + (a + ib)$

$= y + x$

So $x + y = y + x$

Hence $][i]$ is commutative under addition

Hence $-a + I (-b)$ is the additive inverse of $a + ib = x$.

Axioms under multiplication

(6) Closure Property:-

Let $x, y \in][i]$ such that

x = a + ib

y = c + ib, a, b, c, d $\in$ I.

Then x.y = (a + ib) (c + id)

= ac + ibc + iad + i^2bd

= ac – bd + I (bc + ad) [$\therefore$ i^2 = -1]

= (ac – bd) + I (bc + ad)

as a, b, c, d are integers so ac – bd $\in$I and bc + ad $\in$I

sox.y = (ac – bd) + I (bc + ad) $\in$][i]

So][i] us kissed under multiplication.

(7) Associative Property:-

Let x, y, z $\in$][i] such that

x = a + ib

y = c + id

z = e + if

then x.(y.3) = (a + ib). $\left[\left(c+id\right).\left(e+if\right)\right]$

= (a + ib). [ce + ide + ief + i^2df]

= (a + ib). $\left[\left(ce-df\right)+i\left(de+cf\right)\right]$ [$\therefore$ i^2 =-1]

= a(ce – df) + I a(de + cf) + ib (ce – df)

+ ib . I (de + cf)

= (ace – adf) + I (ade + acf) + I (bce – bdf)

- bde – bcf

x. (y.z) = (ace – adf – bde – bcf) + I (ade + acf + bce – bdf)

Now (x.y)z = $\left[\left(a+ib\right).\left(c+id\right)\right]\left(e+if\right)$

= [ac + ibc + iad + i^2bd] (e + if)

= [ac – bd + I (bc + ad)] (e + if)

= ace – bde + I (bce + ade) + I (acf – baf) +i^2 (bcf + adf)

$\Rightarrow$ (x.y).z = (ace – bde – bcf -adf) + I (bce + ade + acf – bdf)

So x.(y.z) = (x.y).z

So associativity holds in][i]

(8) Distributive Property:-

Let x, y, z $\in$ such that

x = a + ib

y = c + id

z = e + if , a, b, c, d, e, f, $\in$ I

Then x.(y+z) = (a + ib) .$\left[\left(c+e\right)+i\left(e+if\right)\right]$

= (a + ib) - $\left[\left(c+e\right)+i\left(d+f\right)\right]$

= a (c + e) + I a (d + f) + ib (c + e) + i^2b (d + f)

= ac + ac – bd – bf + I (ad + af + bc + be)

x.(y + z) = $\left[\left(ac-bd\right)+\left(ae-bf\right)\right]+i\left[\left(ad+bc\right)+\left(af+bc\right)\right]$

Now x.y + x.z = (a + ib) (c + id) + (a + ib) (e + if)

= ac + iad + ibc + i^2bd + ac + iaf + ibe + i^2bf

= (ac – bd) +I (ad + bc) + (ae – bf) + I (af + bc)

x.y + x.z = $\left[\left(ac-bd\right)+\left(ac-bf\right)\right]+i\left[\left(ad+bc\right)+\left(af+be\right)\right]$

Hence x(y + z) = x.y + x.z

Hence][i] is a ring.

Example 3: Prove that the set G = $a+\sqrt{2b}$, a, b $\in$ Q where Q is the set of rational number, is a ring.

Solution: Properties | axioms under addition.

(1) Closure Property: Let x, y $\in$ G such that

x = $a+b\sqrt{2}$, y = $c+d\sqrt{2}$, where a, b, c, d $\in$ Q.

Now x + y = $\left(a+b\sqrt{2}\right)$ + $\left(c+d\sqrt{2}\right)$

= (a + c) + (b + d)$\sqrt{2}$

as set of rational number is closed under addition

so x + y = (a + c) + (b + d)$\sqrt{2}$ $\in$ G $\forall$ x, y $\in$ G.

Hence G is closed under addition.

(2) Associative Property:

Since the set of rational number is associative under addition and G is a subset of Q,

So G = $\left\{a+b\sqrt{2}, a,b \in Q\right\}$ is associative under addition.

(3) Existence of identity:

Sin θ 0 $\in$ G, as

0 = $0+0\sqrt{2}$

then for x $\in$ G, x + 0 = $a+b\sqrt{2}$ +0 = $a+b\sqrt{2}$ = x.

Similarly 0 + x = x

So, 0 is additive identity of G

(4) Existence of inverse:

Let x = $a+b\sqrt{2}$, a, b $\in$ Q

then -a, - b $\in$ Q.

How – x = -a + (-b)$\sqrt{2}$ $\in$G

Such that x + (-x) = $a+b\sqrt{2}$ + (-a) + (-b)$\sqrt{2}$

= (a + (-a) + (b + (-b)$\sqrt{2}$)

= 0 + $0\sqrt{2}$

= 0

Similarly (-x) + x = 0

So -x is inverse of x.

(5) Commutative Property:

Let x = $a+b\sqrt{2}$, y = $c+d\sqrt{2} \in$ G

then x + y = $\left(a+b\sqrt{2}\right)$ + $\left(c+d\sqrt{2}\right)$

= (a + c) + (b + d)$\sqrt{2}$

= (c + a) + (d + b)$\sqrt{2}$ [as rational number holds commutative property

= + $\left(c+d\sqrt{2}\right)$+$\left(a+b\sqrt{2}\right)$

= y + x

Thus commutative property holds in G.

Axioms under multiplication

(6) Closure Property

Let x, y $\in$ G

x = $a+b\sqrt{2}$ and y = $c+d\sqrt{2}$, a, b, c, d $\in$ Q

then x.y = $\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right)$

= ac + bc$\sqrt{2}$ + ad$\sqrt{2}$ + 2bd

xy = (ac + 2bd) + (bc + ad)$\sqrt{2}$

as a, b, c, d $\in$ Q then ac + 2bd $\in$ Q and bc + ad $\in$ Q

Hence x y $\in$ G

Hence G is closed under multiplication.

(7) Associative Property:

Let x, y, z $\in$ G, such that

x = $a+b\sqrt{2}$, y = $c+d\sqrt{2}$, z = $e+f\sqrt{2}$

where a, b, c, d, e, f $\in$ Q

Since set of rational number is associative under multiplication so that G as

(xy) z = $\left\{\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right)\right\}\left(e+f\sqrt{2}\right)$

= $\left\{\left(ac+2bd\right)+\left(bc+ad\right)\sqrt{2}\right\}\left(e+f\sqrt{2}\right)$

= ace + 2bde + (bce + ade)$\sqrt{2}$

+2 (bcf + adf)

= (ace + 2bde + 2bcf + 2adf) + $\sqrt{2}$ (bce + ade + acf + 2bdf)

Now, x(yz) = $\left(a+b\sqrt{2}\right)\left\{\left(c+d\sqrt{2}\right)\left(e+f\sqrt{2}\right)\right\}$

= $\left(a+b\sqrt{2}\right)$ {ce + de$\sqrt{2}$ + cf$\sqrt{2}$ +2df}

= $\left(a+b\sqrt{2}\right)$ {ce + de$\sqrt{2}$ +cf$\sqrt{2}$ +2df}

= $\left(a+b\sqrt{2}\right)\left\{\left(ce+2df\right)+\left(d+cf\right)\sqrt{2}\right\}$

= ace + 2dfa + (ade + acf)$\sqrt{2}$ + (ceb + 2dfb)$\sqrt{2}$

+2(deb + cbf)

= (ace + 2dfa + 2deb + 2cbf) $\sqrt{2}$ (ade + acf + ceb + 2dfb)

= (ace + 2bde + 2bcf + 2adf) $\sqrt{2}$ (bce + ade + acf + 2bdf)

Hence (xy)z = x(yz)

Hence multiplication is associative in G.

(8) Distributive Property

Let x, y.z$\in$ G such that x = x = $a+b\sqrt{2}$, y = $c+d\sqrt{2}$, z = $e+f\sqrt{2}$

where a, b, c, d, e, f $\in$ Q

Then x. (y + z) = $\left(a+b\sqrt{2}\right).\left[\left(c+d\sqrt{2}\right)+\left(e+f\sqrt{2}\right)\right]$

= $\left(a+b\sqrt{2}\right)\left[(c+e)+(d+f)\sqrt{2}\right]$

= (ac + ae) + (ad + af) $\sqrt{2}$ + (bc + be) $\sqrt{2}$

+ 2 (bd + bf)

= (ac + ae) + (ad + af) $\sqrt{2}$ + (bc + be) $\sqrt{2}$

+2 (bd + bf)

= (ac + ac + 2bd + 2bf) + (ad + af + bc + be) $\sqrt{2}$

Now, xy + xz = $\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right)+\left(a+b\sqrt{2}\right)\left(e+f\sqrt{2}\right)$

= ac + ad $\sqrt{2}$ + 2bd + bc $\sqrt{2}$ + ac + af $\sqrt{2}$ + bc $\sqrt{2}$ + 2bf

= (ac + ac + 2bd + 2bf) + (ad + bc + af + be) $\sqrt{2}$

Hence x.(y + z) = xy + xz.

Similarly we can prove (y + z) . x = yx + zx.

Hence G Hidds distributive property.

So, G is a ring.

Example 7: Show that set of rational number Q is a ring under the composition defined as

a $\oplus$ b = a + b – 1 and a $\odot$ b = a + b – ab $\forall$ a, b $\in$ Q

Solution: Axions under addition

(1) Closure Property

Let a, b $\in$ Q then a $\oplus$ b = a + b – 1 $\in$ Q.

Hence a $\oplus$ b is closed under addition.

(2) Associative Property:

Let $a, b, c \in Q$

then $(a \oplus b) \oplus c = (a + b - 1) \oplus c$

$= a + b - 1 + c - 1$

$= a + b + c - 2$

and $a \oplus (b \oplus c) = a \oplus (b + c - 1)$

$= a + b + c - 1 - 1$

$= a + b + c - 2$

$\therefore \quad (a \oplus b) \oplus c = a \oplus (b \oplus c)$

So Associative property holds under addition.

(3) Existence of identity:

Let $a \in Q$ then we to find on element e

such that $a \oplus e = a = c \oplus a$

Since $a \oplus e = a + e - 1$

if we take $e = 1$, then $a + e - 1 = a$, so that $a \oplus e = a$

Hence, here $1 = e$ will act as identity element as $1 \in Q$.

(4) Existence of inverse:

Let $a \in Q$ than we have to find on element $b \in Q$

such that $a \oplus b = e = 1\ b \oplus a$

$= a + b - 1 = 1$

$= b = 1 + 1 - a$

$b = 2 - a \in Q$

Hence $\forall\ a \in Q\ \exists\ b = 2\text{-}a$ which act as identity element for a such that

$a \oplus b = b \oplus a$.

(5) Commutative Property:

$\forall\ a, b \in Q, a \oplus b = a + b - 1$

and $b \oplus a = b + a - 1$

$= a + b - 1$

Hence $a \oplus b = b \oplus a$

Hence commutative property holds.

Axions of multiplication

(6) Closure Property:

$\forall$ a, b $\in$ Q, a Θ b = a + b – ab

as a, b $\in$ Q, a + b, ab $\in$ Q and a + b – a b $\in$ Q

So Q is closed under multiplication.

(7) Associative Property:

$\forall$ a, b, c $\in$ Q

a Θ (b Θ c) = a Θ (b + c – bc)

= a + b + c – bc – a(b + c – bc)

= a + b + c – bc – ab – ac + abc

a Θ (bΘ c) = a + b + c – bc – ab – ac + abc.

How (a Θ b) Θ c = (a + b – ab) Θ c

= a + b – ab + c – (a + b – ab) c

= a + b – ab + c – ac – bc + abc

(a Θ b) Θ c = a + b + c – ab – ac – bc + abc.

Hence aΘ (bΘ c) = (aΘ b) Θ c

So associative property holds

(8) Distributive property

For all a, b, $\in$Q

aΘ (b $\oplus$ c) = aΘ (b + c - 1) by using the defining of a $\oplus$ b

= a + b + c – 1 – a(b + c – 1) using the defining of a Θ b

= a + b + c – 1 – ab – ac + a

aΘ (b $\oplus$ c) = 2a + b + c – ab – ac – 1

Now, (a Θ b) $\oplus$ (a Θ c) = (a + b – ab) $\oplus$ (a + c – ac)

= a + b – ab + a + c – ac – 1

(a Θ b) + (a Θ c) = 2a + b + c – ab – ac – 1

So we get aΘ (b $\oplus$ c) = (a Θ b) $\oplus$ (a Θ c)

Similarly (a $\oplus$ c) Θ a = (b Θ a) $\oplus$ (c Θ a)

Hence the given set of ration number under given defined operation forms a ring.

Self Check Exercise – 1

Q.1 Prove that set Q, set of rational numbers is a commutative ring under addition and multiplication, with unit element.

Q.2 Prove that the set R_1 set of real number is a comitative ring with unity.

Q.3 The set c, of complex numbers is a commutative ring with Unity, prove this statement.

Q.4 The set 2z, of even integers is a commutative ring without unity.

13.4 Properties of Ring

Theorem 1: Rules of multiplication

Let a, b, and c belongs to a ring R then

1. $ao = oa = 0$
2. $(-a)(-b) = ab$
3. $(-a)(-b) = ab$
4. $a(b - c) = ab - ac$
5. $(b - c)a = ba - ca$

If R has a unity element 1 then

6. $(-1)a = -a$
7. $(-1)(-1) = 1$

Proof: 1. Since R is a ring, so distributive property holds, also R is a group under addition with o as additive identity. So we can write

$a.o + a.o = a(o + o) = a.o + = a.o + o$

$\Rightarrow$ $a.o + a.o = a.o = a.o + o$

using Cancellation Law we get

$a.o = 0$

Similarly we can get $o.a = 0$

2. Taking $a(-b) + ab = a(-b + b)$ [using distributive properly]

$= a.o$

$a(-b) + ab = 0$

$\Rightarrow$ $a(-b) = -(ab)$

Similarly we can prove $(-a)b = -(ab)$

3. Taking $(-a)(-b) = -(-a)b$ [using 2]

$= -(-ab)$ [using 2]

$= ab$ [minus times mitrus equation plus]

So $(-a)(-b) = ab$

4. Taking $a(b - c) = a[b + (-c)]$

$= ab + a(-c)$ [using distributive property]

$= ab - ac$ [using 2]

Hence $a(b - c) = ab - ac$

5. Taking $(b - c)a = [b + (-c)]a$

$= ba + (-c)a$ [using distributive property)

$= ba - ca$ [using 2)

So $(b - c)a = ba - ca$

If R is a ring with unity i.e. 1 is multiplicative identity of R then $1.x = x = x.1$

6. $(-1)a = 1(1a)$ [using 2

$= -a$ [$\therefore$ 1 is multiplicative identity of R]

$(-1)a = -a$

7. $(-1)(-1) = -(-1)1$ [using 2 and using is unity of R]

$= -(-1)$

$= 1$

So $(-1)(-1) = 1$

Theorem 2: If the ring R has a multiplicative identity then it is unique.

Theorem 3: If a ring has a multiplicative obverse then it is also unique.

Let try some more examples of ring.

Example 1: Let R be a ring such that $x^2 = x \ \forall x \in R$ then prove that

1. $x + x = 0 \quad \forall x \in R$
2. $x + y = 0 \Rightarrow x = y$
3. $xy = yx \forall x\, y \in R$

Solution: 1. Given $\forall x \in R, x^2 = x$

Since R is a ring, So R is closed under addition

So $\forall x \in R, x + x \in R$

Now $(x + x)^2 = x + x$ [$\therefore$ given $x^2 = x$]

$\Rightarrow \quad (x + x)(x + x) = x + x$

$\Rightarrow \quad (x + x)x + (x + x)x = x + x$

$\Rightarrow$ $(x^2 + x^2) + (x^2 + x^2) = x + x$

$\Rightarrow$ $(x + x) + (x + x) = (x + x)$

Since R is a ring so it has o as additive identity

So $x + o = x$, using this, we get

$(x + x) + (x + x) = (x + x) + 0$

using left Cancellation Law,

$x + x = 0$

So $\forall\ x \in R \qquad x + y = 0$

2. Given $\forall\ x \in R \qquad x + y = 0$

$\Rightarrow$ $x + y = x + x$ [using 1]

using by Cancellation Law, we get

$\Rightarrow$ $y = x$

$\Rightarrow$ $x = y$

So if R is a ring with $x^2 = x$ then $x + y = 0 \Rightarrow x = y$

3. Let $xy \in R$, as R is a ring so $x + y \in R$

Now $(x + y)^2 = x + y \qquad [\because x^2 = x$ given]

$\Rightarrow$ $x2 + xy + yx + y2 = x + y$

$\Rightarrow$ $(x2 + y2) + (xy + yx) = x + y$ [using commutative property]

$\Rightarrow$ $(x + y) + (xy + yx) = x + y$

Since R is a ring so having as additive identity.

$\Rightarrow$ $(x + y) + (xy + yx) = (x + y) + 0$

using left cancellation law

$xy + yx = 0$

$xy = yx.$ [using 2 i.e. $x + y = 0 \Rightarrow x = y$]

Hence R is a commutative ring.

Self Check Exercise – 2

Q.1 Let R be a ring and a, b, c, d $\in$ R then prove that

1. $(a + b)\ (c + d) = ac + bc + ad + bd$
2. $(a – b)\ (c – d) = ac – bc – ad + bd$

3. $(a + b)^2 = a^2 + ab + ba + b^2$

4. $(a – b)^2 = a^2 – ab – ba + b^2$

5. $(a + b)(a – b) = a^2 – ab + ba – b^2$

Q.2 If R is a system satisfying all the conditions for a ring with unit element with the possible exception $x + y = y + x \ \forall x_1 \ y \in R$. Then prove that the axiom $x + y = y + x$ also holds in R.

13.5 Summary

In this unit we studied about

1. ring and its properties, along with some examples.
2. a ring is an abelian group and a semi group which satisfies distributive law.
3. multiplicative identity i.e. unity element and multiplicative inverse of group is unique.

13.5 Glossary

- **Ring with Unity:** If a ring possesses multiplicative identity. Then it is ring with unity.
- **Commutative Ring**: In a RingR, the multiplication composition is also commutative, i.e.$\forall$ a b $\in$ R $\Rightarrow$a.b = b.a

13.7 Answer to Self Check Exercises

Self Check Exercise – 1

Q.1 Do the same as in example 1

Q.2 Do the same as in example 1

Q.3 Do the same as in example 1

Q.4 Do the same as in example 1.

Self Check Exercise – 2

Q.1 Use distributive properties to prove there.

Q.2 Using the fact that 1 is unity of ling i.e. multiplicative identity and using distributive law.

13.8 Suggested Readings/References

1. Vijay K. Khanna and S.k. Bhambri, A course in Abstract Algebra. 5th Edition.
2. Jaseph A. Gallian, contemporary Abstract Algebra, 8th Edition.
3. Frank Ayres Jr, Modern Algebra, Schqum's outline series.
4. A.R. Vasistha, Madren Algebra, Krishna Prakashan Media.

13.9 Terminal Questions

1. Prove that the set R = $\{(a_1 b) \mid a_1 b \in R\}$ is a comitative ring under addition and multiplication of ordered pairs defined as

   $(a_1b) + (c_1d)) = (a + c, b+ d)$

   $(a_1b)\ (c_1d) = (ac, bd)\ \forall\ (a_1\ b), (c_1d) \in R.$

2. Prove that the set R = $\{(a_1 b) \mid a_1 b \in R\}$ is a ring under the addition and multiplication of orders paris defined as

   $(a_1b) + (c_1d) = (a + c, b + d)$

   $(a_1b) - (c_1d) = (a \in - bd, bc + ad)\ \forall (a_1b)\ (c_1d) \in R$

3. Prove that the set G of all real valued functions of x defined on $[0_1 1]$ is a ring under the addition and multiplication defined as below:

   $(f + g)\ (x) = f(x) + g(x)\ \forall\ x \in [0_1 1]$

   $(fg)\ (x) = f(x) + g(x)\ \forall\ x \in [0_1 1]$, where $f_1\ g \in G$.

4. Prove that <R, + ,.> is a commutative ring, under usual addition and multiplication defined by $a \times b = a.b + b.a$

5. Show that the set of real number R is a ring under the composition $\oplus$ and Θ defined by $a \oplus b = a + b + 1$ and $a\ \Theta\ b = a + b + ab\ \forall\ a_1\ b \in R$

Unit - 14

Some Special Rings

Structure

14.1 Introduction

Dear student, in this unit we will study about some special types of ring, like ring of matrices where the element of ring is matrix and ring of integer modulo n. In this unit we will try prove that set of matrix and set of integer modulo n forms a ring and solve same examples related to ring of mortices and ring of integer modulo n.

14.2 Learning Objectives:

After studying this unit, students will be able to

1. define ring of matrices
2. Solve question related to ring of matrices
3. define ring of integer modulo n.
4. Solve numerical related to ring of integer modulo n.

14.3 Ring of Matrices:

Definition: The set M of all $n \times n$ matrices over real/ratind/complex/integer is a non commutative ring with unity under addition and multiplication of matrices. This ring is known as ring of matrices.

Examples: Prove that the set M of all n×n matrices over real is or non-commutative ring with unity under addition and multiplication of matrices.

Solution: Let M be the set of n×n matrices. Let A, B, C be any element of M. So A, B, C be square matrices of order n over reals, such that

$A = \left[a_{ij}\right]_{n\times n}$; $B = \left[b_{ij}\right]_{n\times n}$, $C = \left[c_{ij}\right]_{n\times n}$,

aij, bij, cij∈ R, ≤ I ≤ n, ≤j≤n.

Properties under addition

1. Closuer Property:

Let A,B∈M, then $A + B = \left[a_{ij}\right]_{n\times n} + \left[b_{ij}\right]_{n\times n}$

$= a_{ij} + b_{ij}\left[a_{ij} + b_{ij}\right]_{n\times n}$

as a_{ij}, b_{ij}∈R, so $a_{ij} + b_{ij}$∈ R

A + B ∈ M.

Hence addition is closed for the set M.

2. Associative Properties

For A,B∈M, we have

$A + (B + C) = \left[a_{ij}\right]_{n\times n} + \left[b_{ij}\right]_{n\times n} + \left[c_{ij}\right]_{n\times n}$,

$= \left[a_{ij}\right]_{n\times n} + \left[b_{ij} + c_{ij}\right]_{n\times n}$

$= \left[a_{ij} + \left(b_{ij} + c_{ij}\right)\right]_{n\times n}$

$= \left[\left(aij + bij\right) + \left(cij\right)\right]_{n\times n}$ $\left[\therefore Associativepropertyholdinreals\right]$

= (A + B) + C

∴ A + (B + C) = (A + B) + C

3. Existence of identity:-

For A∈M, ∃ O∈M,

$O = [o]_{n\times n}$such that

$A + O = [aij]_{n\times n} + [O]_{n\times n}$

$= [aij + O]_{n\times n}$

= A

Similarly O + A = A

Hence $A + O = A = O + A$,

So $O = [O]_{ij}$ is the additive identity of the set M.

(4) Existance of inverse:-

Let $A = [aij]_{n\times n}, aij \in R$ then

$-A = [-aij]_{n\times n}$, $-aij \in R$ such that

$A + (-A) = [aij]_{n\times n} + [-aij]_{n\times n}$

$= \left[aij + (-aij)\right]_{n\times n}$

$= [O]_{n\times n}$

$= O$

$A + (-A) = O$

Similarly $(-A) + A = O$

Hence $A + (-A) = (-A) + A = O$

So, $(-A)$ is the additive inverse of $A \in M$.

(5) Commutative Property:-

Let $A, B \in M$ such that $A = [aij]_{n\times n}$, $B = [bij]_{n\times n}$, $aij, bij \in R$

Then $A + B = [aij]_{n\times n} + [bij]_{n\times n}$

$= [aij + bij]_{n\times n}$

$= [bij + aij]_{n\times n}$ $\quad \left[\because addition of real number is commutative\right]$

$= [bij]_{n\times n} + [aij]_{n\times n}$

$\Rightarrow$ $A + B = B + A$

Hence Commutative Property hold in the set M.

Axioms under Multiplication

(6) Closure property:-

Let $A, B \in M$ such that

$A = [aij]_{n\times n}$, $B = [bjjk]_{n\times n}$

Then $AB = [aij]_{n\times n}\,[ajj]_{n\times n}$

$= [cik]_{n\times n}$

$= \sum_{j=1}^{n} aij\, bjk \in R$

Hence $AB \in M$

So the set of all n×nmatri as is closed under multiplication.

(7) Associative Property:-

Let A, B, C $\in$ M where A = $[aij]_{n\times n}$

B = $[Bjk]_{n\times n}$, c = $[ckp]_{n\times n}$, aij, bjjk, ckp$\in$R, be three elements of M.

Let AB = $[aij]_{n\times n}$ $[bjk]_{n\times n}$

$$= \sum_{j=1}^{n} aij\, bjk$$

$= [d_{ik}]_{n\times n}$

and BC = $[b_{jk}]_{n\times n}$ $[c_{kp}]_{n\times n}$

$$= \sum_{k=1}^{n} b_{jk} c_{kp}$$

$= [e_{jp}]_{n\times n}$

Now, to prove (AB)C = A (BC)

We will prove this by taking an arbitrary element of both side, as we know that two matrias are equal if the order of matrices is same and Corresponding element is also equal or same.

i.e. $(I,p)^{th}$ element of (AB)C = $(I,p)^{th}$ element of A(BC)

Taking $(I,p)^{th}$ element of (AB)C = (ith row of AB) (p^{th} column of C).

$$= \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) \left(\sum_{k=1}^{n} c_{kp} \right)$$

$$= \sum_{k=1}^{n} \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) c_{kp}$$

$$= \sum_{k=1}^{n} \sum_{j=1}^{n} a_{ij} b_{jk}\, c_{kp}$$

Now, $(I,p)^{th}$ element of A(BC) = (i^{th} row of a) (p^{th}column of BC)

$$= \sum_{j=1}^{n} \left(a_{ij} \right) \cdot \left(\sum_{k=1}^{n} b_{jk} c_{kp} \right)$$

$$= \sum_{j=1}^{n} \left(\sum_{k=1}^{n} b_{jk} c_{kp} \right) a_{ij}$$

$$= \sum_{j=1}^{n}\sum_{k=1}^{n} b_{jk}c_{kp}\, a_{ij}$$

$$= \sum_{k=1}^{n}\sum_{j=1}^{n} a_{ij}b_{jk}c_{kp}$$

Hence A (BC) = (AB) C

So Associative property holds in M.

(8) Distributive Property:-

Let $A = [a_{ij}]_{n\times n}$, $B = [B_{jk}]_{n\times n}$

and $c = [c_{jk})_{n\times n}$ be three elements of M then.

To prove A – (B +C) = AB + AC

Taking $B + C = [B_{jk}]_{n\times n} + [c_{jk})_{n\times n}$

$B + C = [b_{jk} + C_{jk}]_{n\times n}$

Therefore (I, k) element of $A(B + C) = \sum_{k=1}^{n} a_{ij}\left(b_{jk}c_{jk}\right)$

$$= \sum_{k=1}^{n}\left(a_{ij}b_{jk} + a_{ij}c_{jk}\right)$$

$$= \sum_{k=1}^{n} a_{ij}b_{jk} + \sum_{k=1}^{n} a_{ij}c_{jk}$$

= $(I, k)^{th}$ element of AB + $(ik)^{th}$ element of AC

= $(I, k)^{th}$element of (AB + AC)

Hence A(B + C) = AB + AC

Hence distributive property holds in M.

Hence the set of matrices of order n ×n form a ring under usual matrix multiplication and addition.

Non-Commutative ring:-

Now, to prove set of matrices is a non-commutative ring since we know that matrix multiplication is not commutative in general. So ring of matrices is non commutative ring.

Ring with Unity

Since we know that in the set of matrices we have identity matrix $I_{n\times n}$ such that $\forall A\in M$, $I\in M$, AI = IA = A

So identity matrix I act as multiplicative identity or unity for this ring.

So ring of matrices is a non commutative ring with unity.

Let us try to solve some examples related to ring of matrices.

Example 2: Prove that the set of all matrices of the form $\begin{bmatrix} o & x \\ o & y \end{bmatrix}$; x,y$\in$R, with matrix addition and multiplication is a ring. Also check about the commutative property for this ring.

Solution: Given R = $\left\{ \begin{bmatrix} o & x \\ o & y \end{bmatrix}, x, y \in R \right\}$

Axioms under addition

(1) Closure Property:

Let A = $\begin{bmatrix} o & x_1 \\ o & y_1 \end{bmatrix}$, B = $\begin{bmatrix} o & x_2 \\ o & y_2 \end{bmatrix}$, x_1, x_2, y_1 $y_2 \in$R be any two elements of R then

$$A + B = \begin{bmatrix} o & x_1 \\ o & y_1 \end{bmatrix} + \begin{bmatrix} o & x_2 \\ o & y_2 \end{bmatrix}$$

$$= \begin{bmatrix} o & x_1 + x_2 \\ o & y_1 + y_2 \end{bmatrix}$$

As x_1, x_2, y_1 y_2 are real so $x_1 + x_2 + y_1 + y_2$ are also real.

Hence $A + B \in R$

So R is closed under addition

(2) Associative Property:-

Let A = $\begin{bmatrix} o & x_1 \\ o & y_1 \end{bmatrix}$, B = $\begin{bmatrix} o & x_2 \\ o & y_2 \end{bmatrix}$, C = $\begin{bmatrix} o & x_3 \\ o & y_3 \end{bmatrix}$ be any three elements of R

where x_1, x_2, y_1, y_2, x_2, $y_3 \in$ R, then

$$(A + B) + C = \left[\begin{bmatrix} o & x_1 \\ o & y_1 \end{bmatrix} + \begin{bmatrix} o & x_2 \\ o & y_2 \end{bmatrix} \right] + \begin{bmatrix} o & x_3 \\ o & y_3 \end{bmatrix}$$

$$= \begin{bmatrix} o & x_1 + x_2 \\ o & y_1 + y_2 \end{bmatrix} + \begin{bmatrix} o & x_3 \\ o & y_3 \end{bmatrix}$$

$$= \begin{bmatrix} o & x_1 + x_2 + x_3 \\ o & y_1 + y_2 + y_3 \end{bmatrix}$$

Since x_1, x_2, x_3, y_1, y_2, $y_3 \in$ R and additions set of real numbers is associative under addition so

$$(A + B) + C = \begin{bmatrix} o & x_1 + (x_2 + x_3) \\ o & y_1 + (y_2 + y_3) \end{bmatrix}$$

$$= \begin{bmatrix} o & x_1 \\ o & y_1 \end{bmatrix} + \begin{bmatrix} o & x_2 + x_3 \\ o & y_2 + y_3 \end{bmatrix}$$

$$= \begin{bmatrix} o & x_1 \\ o & y_1 \end{bmatrix} + \left[\begin{bmatrix} o & x_2 \\ o & y_2 \end{bmatrix} + \begin{bmatrix} o & x_3 \\ o & y_3 \end{bmatrix} \right]$$

$= \Delta + (B + C)$

Hence (A + B) + C = A + (B + C)

So Associativity hold in given set.

3. Existence of identity

Let $A \in R$ such that $A = \begin{vmatrix} o & x \\ o & y \end{vmatrix}$, we know that in matrix

we have $O = \begin{vmatrix} o & o \\ o & o \end{vmatrix} \in R$ such that

$$A + O = \begin{vmatrix} o & x \\ o & y \end{vmatrix} + \begin{vmatrix} o & o \\ o & o \end{vmatrix}$$

$$= \begin{vmatrix} o & x \\ o & y \end{vmatrix}$$

$= A$

Similarly O + A = A

So $O = \begin{vmatrix} o & o \\ o & o \end{vmatrix}$ act as additive identity for $A \in R$.

4. Existence of inverse:-

For each $A = \begin{vmatrix} o & x \\ o & y \end{vmatrix}$, x, y $\in$R

we have $B = \begin{vmatrix} o & -x \\ o & -y \end{vmatrix}$, -x,-y$\in$R such that

$$A + B = \begin{vmatrix} o & x \\ o & y \end{vmatrix} + \begin{vmatrix} o & -x \\ o & -y \end{vmatrix}$$

$$= \begin{vmatrix} o & x+(-x) \\ o & y+(-y) \end{vmatrix}$$

$$= \begin{vmatrix} o & o \\ o & o \end{vmatrix} = \text{identity element}$$

So, $B = \begin{vmatrix} o & -x \\ o & -y \end{vmatrix}$ will act as inverse element for A.

5. Commutative Property:-

Let $A = \begin{vmatrix} o & x_1 \\ o & y_1 \end{vmatrix}$, $B = \begin{vmatrix} o & x_2 \\ o & y_2 \end{vmatrix}$, $x_1, y_1, x_1, y_2 \in R$

then $A + B = \begin{vmatrix} o & x_1 \\ o & y_1 \end{vmatrix} + \begin{vmatrix} o & x_2 \\ o & y_2 \end{vmatrix}$

$$= \begin{vmatrix} o & x_1+x_2 \\ o & y_1+y_2 \end{vmatrix}$$

$$= \begin{vmatrix} o & x_2+x_1 \\ o & y_2+y_1 \end{vmatrix} \qquad [\therefore \text{addition is dosed in real numbers}]$$

$$= \begin{vmatrix} o & x_2 \\ o & y_2 \end{vmatrix} + \begin{vmatrix} o & x_1 \\ o & y_1 \end{vmatrix}$$

So $A + B = B + A$

$\therefore$ Commutative property holds under addition.

Axioms under multiplication

6. Closure Property:

Let $A = \begin{vmatrix} o & x_1 \\ o & y_1 \end{vmatrix}$ and $B = \begin{vmatrix} o & x_2 \\ o & y_2 \end{vmatrix}$, $x_1, x_2, y_1, y_2 \in R$ then

$A.\ B = \begin{vmatrix} o & x_1 \\ o & y_1 \end{vmatrix} \begin{vmatrix} o & x_2 \\ o & y_2 \end{vmatrix}$

$$= \begin{bmatrix} 0+0 & 0+x_1y_2 \\ 0+0 & 0+y_1y_2 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & x_1y_2 \\ 0 & y_1y_2 \end{bmatrix}$$

as $x_1, x_2, y_1, y_2 \in R$ So $x_1, y_2, y_1, y_2 \in R$

So $AB \in R$

$\Rightarrow$ R is closed under multiplication.

7. Associative Property:

Let $A = \begin{vmatrix} o & x_1 \\ o & y_1 \end{vmatrix}$, $B = \begin{vmatrix} o & x_2 \\ o & y_2 \end{vmatrix}$, $C = \begin{vmatrix} o & x_3 \\ o & y_3 \end{vmatrix}$ be any three elements of R,

where $x_1, y_1, x_2, y_2, x^3, y^3 \in R$ then

Now (AB) C $= \left(\begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix} \begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix} \right) \begin{bmatrix} 0 & x_3 \\ 0 & y_3 \end{bmatrix}$

$$= \begin{bmatrix} 0 & x_1y_2 \\ 0 & y_1y_2 \end{bmatrix} \begin{bmatrix} 0 & x_3 \\ 0 & y_3 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & x_1y_2y_3 \\ 0 & y_1y_2y_3 \end{bmatrix}$$

as $x_1, x_2, x_3, y_1, y_2, y_3 \in R$ and $y_1\, y_2\, y_3 \in R$

So (AB) C $= \begin{bmatrix} 0 & x_1(y_2y_3) \\ 0 & y_1(y_2y_3) \end{bmatrix} \in R$

Now A(BC) $= \begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix} \left(\begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix} \begin{bmatrix} 0 & x_3 \\ 0 & y_3 \end{bmatrix} \right)$

$$= \begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix} \begin{bmatrix} 0 & x_2y_3 \\ 0 & y_2y_3 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & x_1y_2y_3 \\ 0 & y_1y_2y_3 \end{bmatrix}$$

So, we get (AB)C = A(BC)

Hence matrix multiplication is associative in R.

8. Distributive Property:-

Let A = $\begin{vmatrix} o & x_1 \\ o & y_1 \end{vmatrix}$, B = $\begin{vmatrix} o & x_2 \\ o & y_2 \end{vmatrix}$, C = $\begin{vmatrix} o & x_3 \\ o & y_3 \end{vmatrix}$ where $x_1, x_2, x_3, y_1, y_2, y_3$

are any three element of R.

$$A\,(B+C) = \begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix}\left(\begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix}+\begin{bmatrix} 0 & x_3 \\ 0 & y_3 \end{bmatrix}\right)$$

$$= \begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix}\begin{bmatrix} 0 & x_2+y_3 \\ 0 & y_2+y_3 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & x_1(y_2+y_3) \\ 0 & y_1(y_2+y_3) \end{bmatrix}$$

$$A\,(B+C) = \begin{bmatrix} 0 & x_1y_2+x_1+y_3 \\ 0 & y_1y_2+y_1+y_3 \end{bmatrix}$$

Now $AB + AC = \begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix}\begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix}+\begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix}\begin{bmatrix} 0 & x_3 \\ 0 & y_3 \end{bmatrix}$

$$= \begin{bmatrix} 0 & x_1y_2 \\ 0 & y_1y_2 \end{bmatrix} + \begin{bmatrix} 0 & x_1y_3 \\ 0 & y_1y_3 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & x_1y_2+x_1+y_3 \\ 0 & y_1y_2+y_1+y_3 \end{bmatrix}$$

So $A\,(B+C) = AB + AC$

Hence distributive property holds in R.

So, the set R = $\left\{\begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix}, x, y \in R\right\}$ is a ring.

To check the commutative property:

Let $A = \begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix}$, $x_1, x_2, y_1, y_2 \in R$

then AB = $\begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix}\begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix}$

$= \begin{bmatrix} 0 & x_1y_2 \\ 0 & y_1y_2 \end{bmatrix}$

Now BA = $\begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix}\begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix}$

$= \begin{bmatrix} 0 & x_2y_1 \\ 0 & y_2y_1 \end{bmatrix}$

Since AB ≠ BA, So the set R = $\left\{\begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix}, x, y \in R\right\}$ form a non commutative ring.

Self Check Exercise-1

Q.1 Let M be a set of all 2×2 matrices with their element as integers, then show that M is a ring under usual matrix addition and multiplication. Check the unity element of ring.

Q. 2 Let M be the set of all 2×2 matrices over rational then show that M is a ring with unity.

14.4 Ring of Integers Modulo n.

Definition:

The set Z_n = {0, 1, 2, ……. n-1} under addition modulo n and multiplication modula n form a ring which is commutative. This ring is known as ring of integedmodula. This is a finite ring.

Examples: Show that the set Z_n = {0, 1, 2, ……. n-1} form finite a commutative ring under addition modulo n and multiplication modulo n.

Solution: Given set is Z_n = {0, 1, 2, ……. n-1}, n > 1 for addition modulo n composition we have, for all a, b $\in Z_n$

a $\hat{+}_n$ b = Least non- negative remainder 'r' when a + b is divided by n. i.e. a + b = r (mod n) and for multiplication modulo n,

a $\times_n$ b = least non-negative remainder 'r' when a × b is divided by n. i.e. ab = r (mod n)

Now, to prove Z_n form a ring;

Axioms under Addition

1. Closure Property:-

Let a, b $\in$Zn then $\forall$a, b $\in Z_n$, a $\leq$ a, b $\leq$ n, then

$a +_n b$ = Least non-negative remainder 'r' when a + b is divided dy n

Since for r, 0 < r < n

$= r \in Z_n$

So, $a +_n b \in Z_n$.

So Z_n is closed under addition.

2. Associative Property:-

Let a, b, c, $\in Z_n$ then

$(a +_n b) +_n c$ = least non negative remainder when (a + b)+c is divided by n

= Least non negative remainder when a + (b + c) is divided by n.

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

So associative property hold in Z_n.

3. Existence of identity:-

$\forall a \in Z_n$, 0 $\leq$ a < n, when we add 0 i.e. a + o or o + a have the remainder a

when divided by n. So

$a +_n o = a = o +_n a$

So $O \in Z_n$ act as identity element of Z_n.

4. Existence of inverse:-

$O \in Z_n$then o is the inverse of itself. Also for all $O \in Z_n$, $a \neq o$, we have $n - a \in Z_n$such that

$a +_n (n - a) = O$

and $(n - a) +_n a = o$

Hence (n – a) is the inverse element of $a \in Z_n$

5. Commutative property:

Since the least non negative remain remains the same if we divide a + b by n or b + a by n. So commutativity holds in Z_n. Mathematically.

$a +_n b = b +_n a$.

Axioms Under Multiplication

Here composition is $a \times_n b$ = least non-ve remainder when ab is divided by n

6. Closure Property

For a, b $\in$ Zn i$\leq$r , b $\leq$ n

$a \times_n b$ = least non-ve remainder when ab is divided by n

= r, o < r < n

$a \times_n b \in Z_n$.

So Z_n is closed under multiplication.

7. Associative Property:

$\forall$ a, b, c $\in Z_n$, the least non negative remainder remains the same

if (ab)c or a(bc) is divided by n.

$\therefore$ $(a \times_n b) \times n\ c \equiv a \times_n (b \times_n c)$

So associativity holds in Z_n.

8. Distributive Property:-

$\forall$ a, b, c $\in Z_n$

$a \times_n(b \times_n c) = a \times_n (b + c)$ [$\therefore$ $b \times_n c \equiv b + c$ (modn)

= least non negative remainder when a (b + c)

= ab + ac is divided by n.

$= ab \times_n ac$

$= (a \times_n b) \times_n (a \times_n c)$ [$\therefore$ $ab \equiv a \times_n b$ (mod n) $ac \equiv a \times_n b$ (mod n)

Similarly $(b \times_n c) \times_n a = (b \times_n a) \times_n (c \times_n a)$

Hence distributive property holds.

So, Z_n is a ring.

To prove Z_n is a commutative ring.

Let a, b $\in$ Zn

then $a \times_n b$ = least non negative remainder when a.b is divided by n.

= Least non-negative remainder when b.a is divided by n

Hence $a \times_n b = b \times_n a$

So Z_n is a commutative ring.

Example 2: Show that the set Z_n = {1, 1, 2, 3, 4, 5} is a commutative ring with respect to addition modulo 6 and multiplication modulo 6..

Solution: Given Z_6 = {1, 1, 2, 3, 4, 5}

then addition modulo 6 is defined as if a, b $\in Z_6$.

then $a \times_6 b$ = least non negative remainder when a + b is divided by 6

In order to prove Z_6 is a ring, firstly to prove Z_6 is an abelian group under addition modulo 6. Hence the composition table is

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

From composition table, we can say that (using the concept of unit)

1. Z_6 is closed under addition
2. Z_6 holds associative property
3. 0 is additive identity of Z_6
4. every element of Z_6 has a inverse.

   inverse of 0 is 0

   inverse of 1 is 5

   inverse of 2 is 4

   inverse of 3 is 3

   inverse of 4 is 2

   inverse of 5 is 1

5. As the composition is symmetrical about the main diagonal. Hence it is commutative.

So Z_6 is an abelian group.

Now to prove Z_6 is a semi group under multiplication

$+_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3

4	0	4	2	0	4	2
5	0	5	4	3	2	1

7. Since the element of composition table are element of Z_6, so Z_6 is closed under multiplication modulo 6.

8. Since elements of Z_6 are real number and real numbers are associative under multiplication. So the least non negative remainder when $(a \times b) \times c$ is divided by n

   = the least non negative remainder when $a \times (b \times c)$ is divided by n

   Hence associative property hold in Z_6.

(8) Let us prove it by taking any three element of Z_6.

Since $1, 2, 3 \in Z_6$.

then $1 \times_6 (2 +_6 3) = 1 \times_6 5$

$= 5$

Also $(1 \times_6 2) +6 (1 \times_6 3) = 2 +_6 3$

$= 5$

$+_5$	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

From composition table, it is clear that

1. All the element of composition table are element of Z_5

   So Z_5 is closed under addition modulo 6.

2. The element of Z_5 are real numbers and associative property holds in real numbers. So the least non negative remainder when a + (b + c) is divided by 5

   = the least non negative remainder when (a + b) +c is divided by 5

   So associative property hold in Z_5

3. Here 0 is the additive identity of Z_5

4. Every element of Z_5 has its inverse as

inverse of 0 is 0

inverse of 1 is 4

inverse of 2 is 3

inverse of 3 is 2

inverse of 4 is 1

5. Since elements of composition table are symmetrical about the main diagonal. So Z_5 is commutative.

So $1 \times_6 (2 +_6 3) = (1 \times_6 2) +_6 (1 \times_6 3)$

Similarly we can prove it for every element of Z_6

Hence Z_6 holds distributive property

So $Z_6 = \{0, 1, 2, 3, 4, 5\}$ is a ring.

Now to prove Z_6 is a commutative ring.

Since from the composition table of Z_6 under multiplication modulo 6, it is clear that elements are symmetric about the main diagonal. Hence it is commutative under multiplication modulo 6.

Therefore Z_6 is a commutative ring under addition modulo 6 and multiplication modulo 6.

Example 3: Show that $Z_5 = \{0, 1, 2, 3, 4\}$ is a commutative ring under addition and multiplication modulo 5.

Solution: Since given $Z_5 = \{0, 1, 2, 3, 4\}$ and $+5$ and $\times_5$ is defined for $a, b \in Z_5$ as

$a +5 b$ = least non negative remainder when $a + b$ is divided by 5.

$a \times_5 b$ = least non negative remainder when $a \times b$ is divided by 5

To prove Z_5 is a ring, firstly to prove Z_5 is a commutative or abelian group. We will prove this by using composition table as.

Hence Z_5 is on abelian group.

Now to prove Z_5 is semi group under multiplication modulo 5. The composition table is

$+_5$	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

6. Since all the element of composition table are the element of Z_5, so Z_5 is closed under multiplication modulo 5.

7. Since the element of Z_5 are real numbers and real numbers are associative under multiplication. So

The least non negative remainer 'r' when (a.b)c is divided by n for a, b, c $\in Z_5$

= The least non negative remainder 'r' when a. (b.c) is divided by n.

So $(a \times_n b) \times_n c = a \times_n (b \times_n c)$

Hence Z_5 is associative under multiplication.

8. Distributive Property:-

Let us prove it by taking any three element of Z_5

Since 2, 3, 4 $\in Z_5$

then $2 \times_5 (3 +_5 5) = 2 \times_5 3$

$= 1$

Now, $2 \times_5 3 + 2 \times_5 5 = 1 + 0$

So $2 \times_5 (3 +_5 5) = 2 \times_5 3 + 2 \times_5 5 = 1$

Similarly we can prove this for other elements

Hence Z_5 is a ring under addition and multiplication modulo 5.

Now to prove Z_5 is commutative.

Since the elements of Z_5 are real numbers and real numbers are commutative under multiplication. So

The least non negative remainder when $a \times b$ is divided by n.

= the least non negative remainder when $b \times a$ is divided by n.

Hence Z_5 is a commutative ring.

Self Check Exercise – 2

Q.1 Prove that Z_7 is a commutative ring under addition and multiplication modulo 7.

Q.2 Prove that Z_9 is a commutative ring under addition and multiplication modulo 9.

14.5 Ring with or Without Zero Divisor

In the above section-2 we studied that set of all 2×2 matrices over real forms a ring. Let us consider two elements of such ring, M. i.e. $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

Here $A \neq 0$ and $B \neq 0$

But $AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

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

$= 0$

We, see that product of two non zero elements of the set of 2×2 matias, M is a zero element of M. i.e. additive identity of M.

$AB = 0, A \neq 0, B \neq 0$

So, a new term comes here i.e. zero Divisor

Zero Divisor

A non-zero element of the ring R is called a zero divisor or divisor of zero if there exists an element $\neq 0 \in R$ such that either ab = 0 or ba = 0.

So, from above example $AB = 0, A \neq 0, B \neq 0$

$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor of ring M, which is itself non zero.

Also $BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

So, in a ring R it is also possible that $AB = 0$ but $BA \neq 0$ for $A \neq 0, B \neq 0$.

Ring With Zero Divisor

If in a ring R there exist non-zero elements a and b such that ab = 0, then R is said to be a ring with zero divisor.

Ring Without Zero Divisor

If in a ring R, the product of two non zero elements of R is zero then either 0 = 0 or b = 0.

In this unit, we only discuss ring with zero divisor.

Let us take following examples to have more understanding of ring with zero divisor.

Example 16:- Set of 2×2 matrices with their elements are integers, under usual addition and multiplication of matrices, is a ring with zero divisor.

Solution: We can easily prove that set of 2×0 merrier, M is a ring (Ring of matrices).

Let us take matrix $A = \begin{bmatrix} 4 & 0 \\ 0 & 0 \end{bmatrix}_{2\times2}$ and $B = \begin{bmatrix} 0 & 0 \\ 0 & 5 \end{bmatrix}_{2\times2}$ be any two elements of

set of 2×2 matriar, M

Since A = $\begin{bmatrix} 4 & 0 \\ 0 & 0 \end{bmatrix} \neq 0$, non zero element of M

B = $\begin{bmatrix} 0 & 0 \\ 0 & 5 \end{bmatrix} \neq 0$ non zero element of M

Now, AB = $\begin{bmatrix} 4 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 5 \end{bmatrix}$

AB = $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Since AB = $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ = 0, but A $\neq$ 0 and B $\neq$ 0

So using the definition of ring with zero divisor, i.e. product of two non zero element is zero, the set of all 2×2 matrices is a ring with zero divisors.

Example 2: The set $Z_6 = \{0,1,2,3,4,5\}$ is ring with zero divisor under addition modulo 6 and multiplication modulo 6.

Solution: Since Z6 is a Commutative ring (Proved in ring of integer modulo n)

Since, 2, 3 $\in$ Z_6, are non zero elements of Z_6. Also 0 is the zero element or additive identity of Z_6

Taking $2 \times_6 3$ = Least non negative remainder when 2×3 is devided by 6

= 0

So $2 \times_6 3 = 0$

i.e. product of two non zero elements is equal to zero element of ring.

Again taking 3, 4 $\in$ Z_6

$3 \times_6 4$ = Least non negative remainder when 3×4 is divided by 6

= 0

$\Rightarrow$ $3 \times_6 4 = 6$

i.e. product of two non zero elements is equal to zero element of ring.

So, Z_6 is a ring with zero divisor

Self Check Exercise - 3

Q.1 Check Whether or not Z8 is a ring with zero divisor.

Q.2 Give an example of ring with zero divisor.

14.6 Summary

In this unit we studied about :

1. ring of matrias with examples
2. ring of integer modulo n with examples
3. ring with zero divisor with examples.

14.7 Glossary

- Non-Commutative Ring:- In a Ring R, it is said to be non-commutative ring, if the multiplication is not commutative. i.e. $\exists a, b \in R$ s.t $a.b \neq b.a$.
- Zero divisor :- A non-zero element of the Ring R is called zero divisor if there exist an element $b \neq 0 \in R$ such that either $ab = 0$ or $ba = 0$.
- Ring without zero divisor - If in a ring R, the product of two non-zero elements of R is zero, i.e. $ab = 0$, there either $a = 0$ or $b = 0$.

14.8 Answer to Self Check Exercises

Self Check Exercise - 1

Q.1 Can be solved on the same line as of example 2.

Q.2 Can be solved on the same line as of example 2

Self Check Exercise - 2

Q.1 Can be solved on the same line as of example 4

Q.2 Can be solved on the same line as of example 5

Self Check Exercise - 3

Q.1 as 2, 4, $\in Z_8$ and $2 \times_8 4$ = Least non negative remainder when 2×4 is divided by 8 = 0, Hence Z_8 is a ring with zero divisor.

Q.2 Z_9 is a ring with zero divisor.

14.9 References/Suggested Readings

1. Vijay K. Khanna, and S.K. Bhambri, A course in Abstract Algebra.
2. Joseph A. gallian, Contemporary Absteract Argebro.
3. Frank Ayres. Jr, Modern Argebra, Schaum's Outline Series.
4. A.R. Vasistha, Modern Algebra, Keishna Prakashan Media.

14.10 Terminal Questions

1. Give an example of a Commutative ring with unity.
2. Give an example of a non Commutative ring with unity.
3. Give an example of ring with zero divisor.

*****

Unit - 15

Integral Domains

Structure

15.1 Introduction

Dear student, in this unit we will study about some ring having certain charactersties like ring without zero divisor and integral domain. We will use some examples to have proper knowledge of these special types of ring.

15.2 Learning Objectives:-

After studying this unit, students will be able to

1. define ring without zero divisor
2. give examples and prove questions related to ring with zero divisor.
3. define integral domain
4. give example and prove questions related to ring with zero divisor.

15.3 Ring Without Zero Divisor

As in previous unit we have discussed about ring with zero divisor, here we will study about ring without zero divisor

As a ring without zero divisor is a ring when the product of ro two non zero element of R is zero. Mathematically, if $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Let us try following example to have more cleanly of ring without zero divisor.

Example 1:- The ring of integers is a ring without zero divisors.

Solution: As we know that set of integers from a ring also product of two non zero integers cannot be equal to zero integer. Hence ring of integers is a ring without zero divisor.

Example 2: The set of real number R is a ring without zero divisor

Solution: As again product of two non zero real numbers cannot be equal to zero

Example 3: Show that ring $Z_5 = \{0,1,2,3,4\}$ is a ring without zero divisor.

Solution: Since Z_5 is a ring.

As $Z_5 = \{0,1,2,3,4\}$

In order to prove Z_5 is a ring without zero divisor

we have to check that ab = 0 $\Rightarrow$ a = 0 or b = 0.

So, taking the non zero elements of Z_5

$1 \times_5 2$ = Least non negative remainder when 1×2 is divided by 5 = 2

$1 \times_5 3$ = Least non negative remainder when 1×3 is divided by 5 = 3

$1 \times_5 4$ = Least non negative remainder when 1×4 is divided by 5 = 4

$2 \times_5 3$ = Least non negative remainder when 2×3 is divided by 5 = 1

$2 \times_5 4$ = Least non negative remainder when 2×4 is divided by 5 = 3

$3 \times_5 4$ = Least non negative remainder when 1×4 is divided by 5 = 2

So there are no such non zero element in Z_5 such that There product is zero element of Z_5.

Hence Z_5 is a ring without zero divisor

Example 4: Show that the ring Z_1 is a ring without zero divisor

Solution: Since $Z_1 = \{0,1,2,3,4,5,6\}$, how we have to check that is there any non zero element in Z_1 such that there product is zero. So

$1 \times_7 2 = 2$

$1 \times_7 3 = 3$

$1 \times_7 4 = 4$

$1 \times_7 5 = 5$

$1 \times_7 6 = 6$

$2 \times_7 3 = 6$

$2 \times_7 4 = 1$

$2 \times_7 5 = 3$

$2 \times_7 6 = 5$

$3 \times_7 4 = 5$

$3 \times_7 5 = 1$

$3 \times_7 6 = 4$

$4 \times_7 5 = 6$

$4 \times_7 6 = 3$

$5 \times_7 6 = 2$

So there are no such non zero elements in Z_1 such that there product is zero

Hence Z_7 is a ring without zero divisor

Self Check Exercise - 1

Q.1 Show that Z11 is a ring without zero divisor

Q.2 Show that Z13 is a ring without zero divisor

Q.3 Show that ring of rational and complex number are ring without zero divisor.

15.4 Cancellation Laws in Ring

If R is a ring, then R is an abelian group under addition and semi group under multiplication, with which obeys distributive property. As R is an abelian group under addition, so by the properties of group, Cencellation Law holds in ring also for addition. For multiplication Composition, Cencellation Law for ring holds only if.

$A \neq 0$, $ab = ac \Rightarrow b = c$, left Cencellation Law

and $a \neq 0$, $ba = ca \Rightarrow b = c$, right Cencellation Law.

Theorem 1 - A ring R is without zero divisor if and only if the cencellation laws holds in R, or

R is without zero divisor $\Leftrightarrow$ Cencellation Laws holds in R.

Proof:- Let R is without zero divisor to prove Cencellation Law holds in R.

Since R is without zero divisor. Let a, b, c be any three elements of

R such that $a \neq 0$, $ab = ac$

$\Rightarrow ab - ac = 0$

$\Rightarrow a(b - c) = 0$

as R is without zero divisor and $a \neq 0 \Rightarrow b - c = 0$

$\Rightarrow b = c$

Hence we have proved if $a \neq 0$, $ab = ac \quad \Rightarrow \quad b = c$

So left Cencellation Law holds.

Similarly we can prove right Cencellation Law,

Conversely:- If cencelletion Laws holds in ring then ring is without zero divisor.

Suppose that Cencellation Laws holds in ring R. If possible

Let ab = 0, $a \neq 0$, $b \neq 0$ in R, i.e. R is a ring with zero divisor

As Cencellation Law holds so, $a \neq 0$, ab = a.0 $\Rightarrow$ b = 0

Which is a contradiction,

Hence R is a ring without zero divisor

15.5 Intergral Domain (ID):-

A ring is known as integral domain if it is

1. commutative ring
2. has unit element
3. is without zero divisor

Example: The ring of integers is an integral domain

Solution: Since set of integers form a ring, which is Commutative.

Also $I \in I$, act as unit element. So ring of interger has unity.

Also if a, b are two integers such that ab = 0, then either a = 0 or b = 0.

So ring of integers is an intgeal domain.

Example 2: The algebraic structure (C, +, .), set of complex number under addition and multiplication of Complex number is an integral domain

Example 3: Set of rational number and set of real number under usual addition and multiplication are integral domain.

Example 4: Show that Z_5 is an integral domain.

Solution:- Since we have earlier proved that $Z_5 = \{0,1,2,3,4\}$ is a ring, which is commutative. Also we have proved that Z_5 is a ring without zero divisor (Example 3). Also $Z_5 = \{0,1,2,3,4\}$

Since $1 \in Z_5$ such that $\forall$ a, $\in Z_5$, $1 \times_5 a = a = a \times_5 1$, Hence 1 is unity of Z_5.

Since Z_5 is a Commutative ring, having unity element and is a ring without zero divisor

Hence Z_5 is an integral domain.

Example 5: Show that Z_6 is not an integral domain.

Solution: As $Z_6 = \{0,1,2,3,4,5\}$ is a Commutative ring (proved)

Also $\forall$ a, $\in Z_6$, $1 \in Z_6$, such that

$a \times_6 1 = 1 \times_6 a = a$

So $1 \in Z_6$ act as unity element of Z_6

So Z_6 is a Commutative ring with unity.

Again, 2, 3 $\in Z_6$, and $\neq$and are non zero elements of Z6

So $2 \times_6 3$ = Least non negative remainder when 2×3 is divided by 6

= 0

$\Rightarrow$ $2 \times_6 3 = 0$

Similarly, 3, 4 $\in$ Z6 and are non zero element of Z_6

So, $3 \times_6 4$ = Least non negative remainder when 3×4 is divided by 6

= 0

So $\Rightarrow 3 \times_6 4 = 0$

So, in Z_6, product of two non zero elements is zero. Hence Z_6 is a ring with zero divisor

Since Z_6 is a commutative sing with unity but is a ling with zero divisor

So Z_6 is not an integral domain

Example 6: Let R_1 and R_2 be integral domains. Is $R_1 \times R_2$ is an integral domain?

Solution: Since we know that

$R_1 \times R_2 \{(a,b) : a \in R_1, b \in R_2\}$

Since R_1 and R_2 are integral domains

$\Rightarrow$ R_1 and R_2 are rings

So $R_1 \times R_2$ is a ring.

Since (a, 0), (0, b) $\in R_1 \times R_2$ for $a \neq 0 \in R_1$ and $b \neq 0 \in R_2$

Also (a, 0) . (0, b) = (0, 0)

i.e. Product of two non zero element is zero. So $R_1 \times R_2$ is a ring with zero divisor. So $R_1 \times R_2$ is not an integral domain.

Self Check Exercise - 2

Q.1 Prove that ring of Gaussian integers $Z_{[1]} = \{a + ib, a, b \in z\}$ is an integral domain.

Q.2 The ring $Z_{[x]}$ of polynomials with integer coefficients is an integral domain

Q.3 The ring $z\sqrt{z} = \{a + b\sqrt{2}, a, b \in z\}$ is an integral domain.

Q.4 the ring Z_P of integrals modulo a prime p is an integral domain.

Q.5 The ring Z_B of integers modulo B is not an integral domain,

15.6 Summary:

Dear students in this unit, we studied about

1. The ring without zero divisor with their examples.
2. R is a ring without zero divisor iff Cancellation Law holds in R.
3. A commutative ring with unity, without zero divisor is known as integral domain.

15.7 Glossary:-

- **Integral domain:-** A commutative ring with unity is said to be integral domain if it has no zero divisor.
- **Ring with zero divisor:-** In a ring R, $\exists$

  non-zero element a and b such that ab = 0

  left Cancellation law + If. a, b, c $\in$ R, then

  $a \neq 0$, ab = ac $\Rightarrow$ b = c

15.8 Answers to Self Check Exercises

Self Check Exercise - 1

Q.1 Since in Z11 there is no any non zero elements such that their product is zero (As in example 4)

Q.2 In Z_{13} there is no non zero elements such that their product is zero (As in example 4)

Q.3 Since product of two non zero rational/Complex number cannot be equal zero. So ring of rational and Complex numbers are ring without zero divisor

Self Check Exercise - 2

Q.1 Since product of two Complex number cannot be equal to zero.

Q.2 Product of two non zero polynomial cannot be equal to zero polynomial

Q.3 Let x_1 y $\in z\sqrt{2}$ be any two non zero elements and such that x = $a_1 + b_1\sqrt{2}$, a_1, a_2, b_1, b_2 are integral. Which are non zero.

Since product of two non zerointegeu cannot be equal to zero.

Q.4 $Z_8 = \{0,1,2,3,4,5,6,7\}$

2, 4 $\in Z_8$, are non zero elements of Z_8

Also $2 \times_8 4$ = best non negative remainder when 2×4 is divided by 8

Product of two non zero element is zero

So Z_8 is have zero divisor

So Z_8 is not an integral domain.

15.9 Reference/Suggested Readings

1. Vijay K. Khanna and S.K. Bhambri, A course in Abstract Algebra,
2. Joseph A Gallian, Contemporary Abstract Algebra.
3. Frank Ayres Jr. Modern Algebra, Schaum's Outline Series.
4. A.R. Vasistha, Modern Algebra, Krishna Prakashan Media.

15.10 Terminal Questions

1. Let R_1 and R_2 be two rings. Show that $R_1 \times R_2$ is an integral domain iff one of R_1 or R_2 is an integral domain and the other contains only a zero elements

*****

Unit - 16

Division Ring And Field

Structure

16.1 Introduction

Dear student, in this unit we will study about one other characteristic of ring, i.e. inverse of an element or unit element. One the basis of unit or inverse of an element we can defined a division ring and fields. So division rings and fields are again some special types of ring.

16.2 Learning Objectives:

After studying this unit student will be able to

1. define unit element of a ring
2. find the unit or inverse of an element of ring.
3. Define division ring
4. solve question related to division ring.
5. define field
6. solve questions related to field.

16.3 Unit Element

Since a ring is a abelian group, so inverse of each element exist under addition. But, under multiplication we have to check either verse of element exists or not. So for inverse of element under multiplication the term unit is defined.

Definition

Let R be a ring with unity. Then an element $a \in R$ is said to be unit or inversibly if there exists $b \in R$ such that ab = 1 - ba. In this case we can also write $b = a^{-1}$.

Let us try following examples to have understanding of unit element.

Example 1: Find the unit elements or inversible element of the ring of all integers.

Solution: The elements of ring of integers are $\{.....-3,-2,-1,0,1,2,3.....\}$ we can easily check that 1 is unity or multiplicative identity of ring of integers. Also, in the ring of integers only two elements are there which are inversible or having unit. These elements are 1 and -1

as $1 \times 1 = 1$

$-1 \times -1 = 1$

Let $3 \in Z$ then $3\text{-}1 = 1/3 \notin Z$ is not an integer

So 1 and -1 are only unit elements of ring of all integers.

Example 2: Find the units of Z_7, which is commutative ring with unity.

Solution: Since $Z_7 = \{0,1,2,3,4,5,6\}$. We will find the inversible element of units of Z_7 using composition table.

Since composition table of Z_7 is as

X_{-1}	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Since 1 is multiplicative identity. Using cermposition table, we can write

$1 \times_7 1 = 1$

$2 \times_7 4$ = Least non negative remainder when 2×4 is divided by 7 = 0

$\therefore$ 4 is inverse of 2

$\therefore$ 2 is a unit or inversible element.

Similarly we can write

$3 \times_7 5 = 1$

$4 \times_7 2 = 1$

$5 \times_7 3 = 1$

$6 \times_7 6 = 1$

Hence 1, 2, 3, 4, 5, 6 are units of Z_7 or we can say inverse of there element exists.

Example 3: Write the units of ring of all n×n matrices with elements as real numbers.

Solution: Since the inverse of a matrix exist if it is non singular i.e. its determinant is non zero. Hence all n×n matrices with element as real number, which are non singular are inversible elements or unit of ring of all n×nmatricer.

Example 4: Find unit elements of Commutative ring with unity Z_8.

Solution: Since $Z_8 = \{0,1,2,3,4,5,6,7\}$

The composition table of Z_8 under multiplication is

X_{-8}	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Since 1 is identity element under multiplication. So from the table we find that

$1 \times_8 1 = 1$

$3 \times_8 3$ = Least non negative integer when $3 \times 3 = 9$ is divided by 8 = 1

$5 \times_8 5$ = Least non negative integer when $5 \times 5 = 25$ is divided by 8 = 1

$7 \times_8 7$ = Least non negative integer when $7 \times 7 = 49$ is divided by 8 = 1

So in Z_8, 1, 3, 5, 7 are unit or inversible element.

as, 2, 4, 6 does not multiplicative inverse so 2, 4, 6 are not units in Z_8.

Example 5: Find units of Z_6.

Solution: $Z_6 = \{0,1,2,3,4,5\}$

The composition table of Z_6 is.

X_{-6}	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

From composition table we can say that only 1 and 5

are inversible elements as $1 \times_6 1 = 1$ and $5 \times_6 5 = 1$

So only units of Z6 are 1 and 5

Example 6: Find units of Z[1].

Solution: Let $a+ib \in Z[i]$., $a, b \in Z$

Let a+ib is a unit. Then

$(a + ib)^{-1} = \dfrac{1}{a+ib}$

$= \dfrac{1}{a+ib} \times \dfrac{a-ib}{a-ib}$

$= \dfrac{a-ib}{(a+ib)(a-ib)}$

$= \dfrac{a-ib}{a^2+b^2}$ $\quad \because (a+b)(a-b) = a^2 - b^2$

$= \dfrac{a}{a^2+b^2} + i\left(\dfrac{-b}{a^2+b^2}\right)$

Now, (a + ib)-1 $\in$ Z [i] iff $\frac{a}{a^2+b^2}$ and $\frac{-b}{a^2+b^2}$ are integers

i.e. $a^2 + b^2 = 1$

Putting b = 0, $a^2 = 1 \Rightarrow a \pm 1$

Now putting values of a and b in a + ib

When b = 0, a = $\pm$ 1 so unit is $\pm$ 1 $\pm$ 0 = $\pm$ 1

When a = 0, b = $\pm$ 1, so unit is 0 $\pm$i = $\pm$i

So units of Z[i] are +11 -11 i, -i

Example 7: Check that -7 + $4\sqrt{3}$ is a unit in $Z\sqrt{3}$

Solution: Since $Z\sqrt{3} = \left\{a+b\sqrt{3}, a, b \in z\right\}$

Let -7 + $4\sqrt{3}$ is a unit in $Z\sqrt{3}$

Using definition, i.e. a $\in$ R is a unit. If $\exists$ b $\in$ R such that a.b = 1 then a^{-1} exists.

Since -7 + $4\sqrt{3}$ is a unit so $\left(-7+4\sqrt{3}\right)^{-1}$ exists.

So. $\left(-7+4\sqrt{3}\right)^{-1} = \frac{1}{-7+4\sqrt{3}}$

$= \frac{1}{-7+4\sqrt{3}} \times \frac{-7-4\sqrt{3}}{-7-4\sqrt{3}}$

$= \frac{-7-4\sqrt{3}}{\left(-7\right)^2-\left(4\sqrt{3}\right)^2}$

$= \frac{-7-4\sqrt{3}}{49-48}$

$= \frac{-7-4\sqrt{3}}{1}$

$-7-4\sqrt{3} \leftarrow Z\sqrt{3}$

So $-7+4\sqrt{3}$ is a unit in $Z\sqrt{3}$.

Example 8: find the units of $Z\sqrt{-2} = \left\{a+i\sqrt{2}b; a, b \in z\right\}$ under usual addition and multiplication.

Solution: Let $a+i\sqrt{2}b; a,b \in z$ is a unit element of $Z\left(\sqrt{-2}\right)$

Then $\left(a+i\sqrt{2}b\right)^{-1} = \frac{1}{a+i\sqrt{2}b}$

$= \frac{1}{a+i\sqrt{2}b} \times \frac{a-i\sqrt{2}b}{a-i\sqrt{2}b}$ on

$= \frac{a-i\sqrt{2}b}{a^2-\left(i\sqrt{2}b\right)^2}$ $\because$ (a + b) (a - b) = $a^2 - b^2$

$= \frac{a-i\sqrt{2}b}{a^2-\left(-2b^2\right)}$ $\because$ $i^2 = -1$

$= \frac{a-i\sqrt{2}b}{a^2+-2b^2}$

$= \frac{a}{a^2+2b^2} + \frac{i\sqrt{2}(-b)}{a^2+2b^2}$

$= \frac{a}{a^2+2b^2} + i\sqrt{2}\left(\frac{(-b)}{a^2+2b^2}\right)$

Now, $\left(a+i\sqrt{2}b\right)^{-1} \in Z\sqrt{-2}$ iff $\frac{a}{a^2+2b^2}$ and $\frac{-b}{a^2+2b^2}$ are integers.

i.e. a2 + 2b2 = 1

This is possible only if b = 0 and $a^2 = 1$

$\therefore$ a = $\pm$ 1

So, 1 and -1 are the only units of $Z\sqrt{-2}$

Self Check Exercise - 1

Q.1 Find the unit in Z12

Q.2 Find the units of ring R = $\left\{a+b\sqrt{-3}, a,b \in Z.\right\}$

Q.3 Check that $-7+4\sqrt{3}$, $2-\sqrt{3}$, $5+3\sqrt{3}$, $-3+2\sqrt{3}$ is a unit in $Z\sqrt{3}$ or not.

Q.4 Check that $1+\sqrt{2}$ is a unit of $Z\sqrt{2}$ or not.

16.4 Division Ring or Skew Field

Definition:- A ring R with atleast two elements is called a division ring or a skew field if it

1. has unity
2. is such that each non zero element possesses multiplicative inverse.

Here it is interstingti note that a ring is an abelian group under addition holding distributive property along with semi group under multiplication. So a ring under multiplication is

(1) Closed under multiplication

(2) Associatively holds

For division ring (3) has unity i.e. multiplicative identity exists

(4) non zero element has inverse.

So looking on above condition we can say, if R is a division ring, then the set of all non zero elements of R from a group under multiplication.

Example 1: The ring Q, ring of rational number is a division ring.

Solution: Since 1 $\in$Q will act as unity of the ring i.e. multiplicative in identity and $\forall$ x = p/q $\in$Q. $\exists$ y = q/p such that xy = 1 = yx i.e. every non zero element has its inverse. So the ring Q is a division ring.

Example 2: The ring R, ring of real number is a division ring.

Solution: Ring of real number has unity. Also $\forall$ a $\in$ R, $\exists \frac{1}{a} \in$ R such that a. $\frac{1}{a}$ = $\frac{1}{a}$ .a = 1

So every non zero element has its inverse. So ring of real number is a division ring.

Example 3: The ring C, ring of complex number is a division ring.

Solution: Ring of complex number has 1+0 i$\in$ C, which act as multiplicative identity i.e. unity of the ring.

Also, if a + i b $\in$ C, a, b $\in$ R, then $\frac{1}{a+ib} \in$ C

Such that (a + ib). $\frac{1}{a+ib}$ = 1 = $\frac{1}{(a+ib)}$. $(a+ib)$

Elence ring of complex number is a division ring.

Self Check Exercise - 2

Q.1 Check that (z, + i) is a division ring or not.

16.5 Field

Definition:- A ring R with at least two element is called a field if,

(1) has unity

(2) every non zero element has its multiplicative inverse.

(3) it commutative.

We can see that division ring has (1) and (2) property.

So we can say that commutative division ring is a field. Let us try following examples based on division ring.

Example 1: The set of real numbers is a field.

Solution:- As we have proved in example 10, that the set of real number is a division ring. Also real number are commutative under multiplication. So the set of real number form a field.

Example 2: The set of rational number is a field.

Solution: Since set of rational number is a division ring (Example 9) Also rational numbers are commutative under multiplication. So the set of rational numbers form a field.

Example 3: The set of complex number is a field.

Solution: As set of complex number is a division ring (Example 11) Also complex number are commutative under multiplication. So the set of complex number form a field.

Note:- (1) Set of natural number is not a field as N = $\{1, 2, ...\}$ so it does not has additive identity.

(2) Set of integers is not a field. As Z = $\{-3, -4-1, 0, 1, 2, 3.....\}$

Let a = 2 $\in$ Z, we can not find an element b $\in$ Z such that a. b = b - a = 1

i.e. all non zero elements has no multiplicative inverse so set of integer is not a field.

Theorem 1: Every field is an integral domain.

Proof:- Let F is a field. Then F is a commutative ring with unity and all non zero element have inverse. To prove every field is an integral domain, we have to prove that field has no zero divisors or field is without zero divisor.

Let a, b be any two element of field F, with $a \neq 0$ such that ab = 0

Since $a \neq 0$ so a^{-1} exist as F is a field.

Also we have ab = 0

$\Rightarrow$ $a^{-1}(ab) = a^{-1}(0)$

$\Rightarrow$ $(a^{-1}a)b = 0$

$\Rightarrow$ $1 . b = 0$ [$\because$ $a^{-1} a = 1$]

$\Rightarrow$ b = 0 [1. b = b]

Similarly if $b \neq 0$, such that ab = 0

as ab = 0

$\Rightarrow$ $(ab)\, b^{-1} = 0\, b^{-1}$

$\Rightarrow$ $a(bb^{-1}) = 0$

$\Rightarrow$ a. 1 = 0

$\Rightarrow$ a = 0

Thus if F is a field, then for a, $b \in F$, ab = 0 $\Rightarrow$ a = 0 or b = 0.

Hence F has no zero divisor or F is without zero divisor. So F is an integral domain.

The converse of this theorem is not true. i.e. every integral domain is not a field. We will prove this statement in next example.

Example 4: Show that Ring of integers is an integral domain but it is not a field.

Solution: Since ring of integer is an integral domain as product of two non zero integer cannot be equal to zero. So ring of integer is an integral domain.

But, ring of integer has unity and is commutative under multiplication but every integer other than 1 and -1 does not have multiplication inverse. So ring of integers is not a field

Note:- (1) For a field F, unity and zero are distinct elements $1 \neq 0$

(2) A field has no zero divisor. Therefore in a field the product of two non zero element will again be a non zero element.

A division ring has no zero divisor.

Finite/Infinite Ring

The number of elements in a ring is called order of ring. If number of element on order of ring is finite then it is known as finite ring otherwise it is called an infinite ring.

Theorem 2: Every finite integral domain is a field.

OR

A finite Commutative ring without zero divisor is a field.

Proof:- Let R be a finite integral domain

Then by definition of integral domain, R is a finite commutative ring without zero divisors.

First two show that R has unit element.

Let R = $\{a_1, a_2, ...a_n\}$ be distinct elements of R.

Let $a \in R$ be any non zero element.

Then by using closures property under multiplication, the elements aa_1, aa_2, ... aa_n are in R.

Now to prove that these elements are distinct,

Let aai = aaj where $1 \leq i, j \leq n$

$\Rightarrow$ $aa_i - aa_j = 0$

$\Rightarrow$ $a(a_i - a_j) = 0$

Since R is an integral domain, so product of two elements is equal to zero even when elements are non zero i.e.

$a \neq 0$ (given), $(a_i - a_j) = 0$

$\Rightarrow$ $a_i - a_j = 0$

$\Rightarrow$ $a_i = a_j$

$\Rightarrow$ $i = j$

Hence the elements $aa_1, aa_2, \ldots\ldots\ldots aa_n$ are all distinct and are n in number.

Since we initially taken R = $\{a_1, a_2, \ldots\ldots a_n\}$ and R has also n elements of the form

R = $\{aa_1, aa_2, \ldots\ldots aa_n\}$, where $a \in R$ so $\exists a_k$ $(1 < k < n)$ such that

$a = aa_k$, (1) as R has only n distinct element.

Let $ai \in R$ $\{1 \leq i \leq n\}$ be any element.

$\therefore$ ai = aaj for same j, i< j < n 2

Now $a_k ai = a_k(aa_j)$ using 2

$= (a_k a)a_j$ (using associative property)

$= (aa_k)a_j$ (using commutative property)

$= aa_j$ using (1) i.e. $aa_k = a$

$= a_i$ using (2)

as R is commutative so, $a_k a_i = a_i a_k = a_i$ $\forall a_i \in R$

Hence a_k is the unit element of R

Since the unit element of ring is unique and we denoted it by 1.

Now $1 \in R = \{aa_1, aa_2, \ldots\ldots aa_n\}$ therefore $\exists$ a_l, $1 \leq l \leq n$ such

that $1 = aa_l = a_l a$,

Which shows that a is invertible with respect to multiplication.

Thus every non zero element of R is invertible with respect to multiplication. Hence R is a filed.

Theorem 3: the ring $Z_þ$ of integers modulo a prime þ is a field iff þ is a prime.

Proof: Let Z_p be a field, to show þ is a prime.

Let þ is not a prime.

Then $\exists$ a, b such that þ = ab where 1 < a, < b < þ. By definition of composting of multiplication modulo þ a $\times_{þ}$ b = least non negative remainder when a×b is divided by þ

= 0 as ab = þ

$\Rightarrow$ a $\times_{þ}$ b = 0

as a $\neq$ 0, b $\neq$ 0, so Z_p as zero divisor

$\Rightarrow$ Zp is not an integral domain

Which leads to a contradiction because we suppose Z_p is a field So Z_p is an integral domain.

Hence our supposition is wrong that þ is a not a prime

Hence þ is a prime.

Coveristy :- Let þ is a prime, to prove Z_p is a field.

Let a, b $\in Z_p$ such that

a $\times_{þ}$ b = 0

$\Rightarrow$ ab is a multiple of þ

$\Rightarrow$ þ /a or þ/b $\because$ þ is a prime.

$\Rightarrow$ a = 0 or þ = 0

So a $\times_{þ}$ b = 0 if a = 0 or b = 0

i.e. Z_p ring without zero divisor

So Z_p is integral domain.

AlsoZ_p = $\{0,1,2,.....\rho-1\}$ has finite number of element and finite integral domain is field.

Hence Z_p is a field.

To have more understanding of field let us take following examples.

Example 4: Show that the set G = $\{0,1,2,3,4\}$ Forms a field with respect to addition and multiplication modulo 5.

Solution: Since G = $\{0,1,2,3,4\}$

Here Composition of addition and multiplication are defined as a $+_5$ b = Least non negative remainder when a+b is divided by 5.

and

a $\times_5$ b = Least non negative remainder when a×b is divided by 5.

Now, Composition table under $+_5$ is

X_{-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

Axioms under addition:-

1. **Closure properties:-** Since all entries (in each column) are the element of G. So G is closed under addition.
2. **Associative property:-** Since the element of G are integers, so the least non negative remainder remains the same if (x+y)+z or x+(y+z) is divided by 5

   So Associative property holds.
3. **Existence of identity:-** Here 0 is the identity element of G as $\forall\ x \in G \quad x +_5 0 = x = 0 +_5 x$.
4. **Existence of inverse:-** Here 0 is inverse of itself.

   Inverse of 1 is 4, inverse of 2 is 3, inverse of 3 is 2 Hence every element has its additive inverse.
5. **Commutative Property:-** Since element of composition table are symmetrical about main diagonal. Hence G is commutative.

Hence G is an abelian group under addition.

Axioms under multiplication

Composition table for X_5

X_{-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

Closure Property

As the element of composition table are element G. Hence G is closed under multiplication

Associative Property:

As integers are associative under multiplication.

So the least non-negative remainder when $a(b\times c)$ is divided by 5

= the least non-negative remainder when $(a\times b)\times c$ is divided by 5

Hence associative property holds in G.

Existence of identity:-

Since $1 \in G$ and $\forall\ a \in G$

$a \times_5 1 = a = 1 \times_j a$. Hence 1 will act as identity element of G.

Existence of inverse:-

From composition table it is easily seen that inverse of 1 is 1, is

inverse of 2 is 3

inverse of 3 is 2

inverse of 4 is 4

Here we have to check the inverse of only non zeroelernt.

Commutative Property

Since integers are commutative under multiplication. So

The least non negative remainder when $a\times b$ is divided by 5

= The least non negative remainder when $b\times a$ is divided by 5

Hence commutative property holds in G.

Distributive Law

Since 'X_5' is distributive in R with respect to '$+_5$'. If a, b, c are any elements of R then

$a \times_5 (b +_5 c) = (a \times_6 6) +_6 (a \times_6 c)$

as the least non-negative remainder when $a\times(b+c)$ is divided by 5

= the least non negative remainder when $(a\times b)+(b\times c)$ is divided by 5.

Hence G $\{0,1,2,3,4\}$ is a field.

Example 5: Find the root of $x^2 + 3x - 4$ in Z_1 Z_6 and Z_4.

Solution: Let $f(x) = x^2 + 3x - 4$

$= x^2 + 4x - x - 4$

$= x(x + 4) -1 (x + 4)$

$\Rightarrow \quad f(x) = (x + 4)(x - 1)$

(1) To find root of $f(x) = x^3 + 3x - 4 = (x + 4)(x - 1)$ in Z

$(x + 4)(x - 1) = 0$

$\Rightarrow \quad x = -4, 1$ in Z

(2) The roots of $x_2 + 3x - 4$ in Z_6

Since $Z_6 = \{0,1,2,3,4,5,6\}$

So $f(x) = 0$ in Z_6iff $(x + 4)(x - 1) = 0$ in Z_6

taking values of x from Z_6, we get

$x = 0, (0 + 4)(0 - 1) = - 4$

when, $x = 1, (1 + 4)(1 - 1) = 0 \equiv 0 \pmod 6$

$x = 2, (2 + 4)(2 - 1) = 6 \equiv 0 \pmod 6$

$x = 3, (3 + 4)(3 - 1) = 4 \equiv 2 \pmod 6$

$x = 4, (4 + 4)(4 - 1) = 12 \equiv 0 \pmod 6$

$x = 5 (5 + 4)(5 - 1) = 36 \equiv 0 \pmod 6$

So only $x = 1, 2, 4, 5$ satisfies the condition $(x + 4)(x - 1) \equiv o \pmod 6$

So roots in Z_6 are 1, 2, 4 and 5

(3) The roots of $x^2 + 3x - 4$ in Z_4

Since $Z_4 = \{0,1,2,3\}$

So $f(x) = 0$ in Z_4iff $(x + 4)(x - 1) = 0$ in Z_4

Considering the same as above, $x = 1, 2$ are the roots of $x^2 + 3x - 4$ in Z_4.

Example 6: Solve the equation $f(x) = x^2 - 5x + 6 = 0$ in the ring Z_{12}.

Solution: Since $Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

Given, $f(x) = x^2 - 5x + 6$

$= x^2 - 3x - 2x + 6$

$= x(x - 3) - 2(x - 3)$

$= (x - 3)(x -2)$

So the roots of f (x are given by $(x - 3)(x - 2) = 0$

Taking the value of x from Z12, we get

When x = 1, (1 - 3) (1 - 2) = 2 $\equiv$ 0 (mod 12)

When x = 2, (2 - 3) (2- 2) = 0 $\equiv$ 0 (mod 12)

When x = 3, (3 - 3) (3 - 2) = 0 $\equiv$ 0 (mod 12)

When x = 4, (4 - 3) (4 - 2) = 2 $\equiv$ 2 (mod 12)

When x = 5, (5 - 3) (5 - 2) = 6 $\equiv$ 6 (mod 12)

When x = 6, (6 - 3) (6 - 2) = 12 $\equiv$ (0 mod 12)

When x = 7, (7 - 3) (7 - 2) = 20 $\equiv$ 8 (mod 12)

When x = 8, (8 - 3) (8 - 2) = 30 $\equiv$ 6 (mod 12)

When x = 9, (9 - 3) (9 - 2) = 42 $\equiv$ 6 (mod 12)

When x = 10, (10 - 3) (10 - 2) = 56 $\equiv$ 8 (mod 12)

When x = 11, (11 - 3) (11 - 2) = 72 $\equiv$ 0 (mod 12)

So only, x = 2, 3, 6 and 11 satisfies the condition (x - 3) (x - 2) = 0 in Z_{12}

So the root of f (x) = x^2 - 5x + 6 = 0 are 2, 3, 6 and 11.

Self Check Exercise - 3

Q.1 Prove that Z7 is a field

Q.2 Prove that Z8 is not a field.

16.6 Summary:

In this unit we studied about

1. the unit element of ring which is also known as inversible element of ring.
2. the division ring which is a ring having multiplicative identity and all non zero elements have their inverse under multiplication.
3. the field which is a commutative division ring.

To Summarized all

Under addition

1. Closures property
2. Associative property
3. Existence of Identity
4. Existence of inverse
5. Commutative under addition under multiplication
6. Closure property
7. Associative property

8. Distributive property

9. Existence of identity

10. Existence of inverse of all non zero element

11. Commutative under multiplication

16.7 Glossary:-

- **Unit element:-** Let R be the ring with unity. Then an element a $\in$ R is said to be unit if $\exists$ b$\in$R such that ab = 1 = ba.
- **Division Ring:-** A rring R with unity is said to be division ring such that each non zero element possesses multiplicative inverse.

16.8 Answers to Self Check Exercises

Self Check Exercise - 1

Q.1 $\{1,5,7,11\}$ are units of Z12

Q.2 1 and -1

Q.3 -7 + $4\sqrt{3}$, $2-\sqrt{3}$ are units only

Q.4 Yes

Self Check Exercise-3

Q.1 As Z7 is a finite integral domain, so is a field.

Q.2 As every all non zero element does not have inverse. So not a field.

16.9 References/Suggested Readings

1. Vijay k. Khanna, and S.K. Bhambri, A course in Abstract Algebra
2. Joseph A. Gallian, Contemporary Abstract Algebra.
3. Frank Ayrer Jr, Modern Algebra, Schaumn's Outline Series
4. A.R. Vasistha, Modern Algebra, Krishna Prakashan Media.

16.10 Terminal Questions

1. Give an example of a division ring which is not a field
2. Prove that $a\sqrt{2} = \left\{a+\sqrt{2}b, a, b \in Q\right\}$ where Q is set of rational, is a field under usual addition and multiplication
3. Show that the set of rational Q is a field under the compositions $\oplus$ and (.) defined as

   a $\oplus$ b = a + b - 1 and a (.) b = a + b - ab $\forall$ a, b $\in$ Q.

*****

Unit - 17

Properties of Ring Element

Structure

17.1 Introduction

Dear student, in this unit we will study about some properties of ring element such as idempotent element and nilpotent element, on the basis of which we will define a special type of ring i.e. Boolean ring. We will also study about the characteristic of ring and do some examples to find characteristic of ring.

17.2 Learning Objectives:-

After studying this unit student will be able to

1. define idempotent and nilpotent element of ring
2. define Boolean ring with its properties
3. do prove a given ring is Boolean or not.
4. define and find the characteristic of ring.

17.3 Idempotent Element of a Ring

Definition:- An element x in a ring R is said to be idempotent if $x^2 = x$.

Example 1: Prove that $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is an idempotent element of $M_3(R)$, the ring of real matrices of order 3×3.

Solution: Since we know that an element is said to be idempotent element if $x^2 = x$ for $x \in R$.

So we have to prove that $A^2 = A$ for $A \in M_3(R)$.

Given $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

how, $A^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

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

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

$= A$

Hence A is an idempotent element of $M_3(R)$

Self Check Exercise-1

Q. 1 Prove that $A = \begin{bmatrix} 2 & -2 & -4 \\ -1 & -3 & 4 \\ 1 & -2 & -3 \end{bmatrix}$ is on idempotent dement of M_3R.

17.4 Nilpotent Element

An element x in a ring R is called nilpotent element if $x^n = 0$, for some positive integer n. The smallest positive integer satisfying $x^n = 0$ is called degree of nilpotency of the element x.

Example 1 : Prove that $A = \begin{bmatrix} 1 & 1 & 3 \\ 5 & 2 & 6 \\ -2 & -1 & -3 \end{bmatrix}$ is a nilpotent element of $m_3(R)$, the right of real matrices of order 3x3.

Solution : since we know that an element of a ring is nilpotent of $x^n = 0$. So we have to find that power of A for which $A^n = 0$

Given $A = \begin{bmatrix} 1 & 1 & 3 \\ 5 & 2 & 6 \\ -2 & -1 & -3 \end{bmatrix}$

$$A^2 = \begin{bmatrix} 1 & 1 & 3 \\ 5 & 2 & 6 \\ -2 & -1 & -3 \end{bmatrix}\begin{bmatrix} 1 & 1 & 3 \\ 5 & 2 & 6 \\ -2 & -1 & -3 \end{bmatrix}$$

$$= \begin{bmatrix} 1+5-6 & 1+2-3 & 3+6-9 \\ 5+10-12 & 5+4-6 & 15+12-18 \\ -2-5+6 & -2-2+3 & 1-6-1+9 \end{bmatrix}$$

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

$$\text{Now } A^3 = \begin{bmatrix} 0 & 0 & 0 \\ 3 & 3 & 9 \\ -1 & -1 & -3 \end{bmatrix}\begin{bmatrix} 1 & 1 & 3 \\ 5 & 2 & 6 \\ -2 & -1 & -3 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 \\ 3+16-18 & 3+6-9 & 9+18-27 \\ -1-5+6 & -1-2+3 & -3-6+9 \end{bmatrix}$$

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

Since $A^3 = 0$

So, A is nilpotent element of $M_3(R)$ and the degree of nilpotency is 3.

Theorem 1 : The sum of two nilpotent element of a commutative ring is also nilpotent.

Proof : Let R be a commutative ring and a, b $\in$ R be two nilpotent elements of ring such that $a^m = 0$ and $b^n = 0$ for some positive integers m and n.

Now $(a+b)^{m+n} = a^{m+n} + {}^{m+n}C_1\, a^{m+n+1} b + \ldots + {}^{m+n}C_n\, a^{m+r} b^n \ldots\ldots {}^{m+n}C_{n+1}\, a^{n-1} b^{n+1} + \text{----} + b^{m+n}$

using Binomial expensin

$$= a^m \left\{ a^n + {}^{m+n}C_1\, a^{n-1} b + --- {}^{m+n}C_r\, b^n b \right\} +$$

$$b^n \left\{ a^n + {}^{m+n}C_{n+1}\, a^{n-1} b + --- b^n \right\}$$

as $a^m = 0$ and $b^n = 0$, so

$(a+b)^{m+n} = 0 + 0$

$= 0$

Hence sum two nilpotent element of a commutative ring is also nilpotent.

Theorem 2 : Show that in a ring R, a non zero idempotent cannot be nilpotent.

Solution : Let x$\in$ R be a non zero idempotent element then by definition of idempotent $x^2 = x$.

If x is also nilpotent element then there exists an integer $n \geq 1$ such that

$x^n = 0$ (1)

But since $x^2 = x$, so

$x^3 = x.x^2$

$= x.x$

$= x^2$

$\Rightarrow$ $x^3 = x$

$x^4 = x^2.x^2$

$= x.x$

$= x^2$

$\Rightarrow$ $x^4 = x$

similarly$x^n = x$ (2)

So from (1) and (2) x = 0, which is a contradiction that x is a non zero element of ring R.

Hence, a non zero idempotent cannot be nilpotent.

Theorem 3 : Prove that a ring R has no zero nilpotent elements if and only if the solution of the equation $x^2 = 0$ in R.

Solution : Let R has non zero nilpotent element then by definition

$x^n = 0$

So the equation $x^2 = 0$ has only one solution i.e. x = 0 in R

Conversely :

Let $x^2 = 0 \Rightarrow x = 0$ in R

If possible, let a be a nilpotent element in R.

$\therefore \exists$a least positive integer n such that $a^n = 0$

If $n \leq 2$ then a = 0

Let n > 2, then n must be odd, for otherwise by hypotheses $a^{n/2} = 0$, which contradict the condition that n is minimal.

Let n = 2m+1. Then m > 0 and m+1<n

Now $(a^{m+1})^2 = a^{2m+2}$

$= a^{2m+1} . a$

$= a^n . a$

$= a .a$ $\quad \because a^n = 0$

$= 0$

$\Rightarrow a^{m+1} = 0$, which again contradict the condition that n is minimal.

Hence $x^n = 0$, for n the least position integer which completes the proof.

Example 2 : Show that in an integral domain R with unit y the only idemponents are zero and unity.

Solution : Let $a \in R$ be an idempotent element of R

Then by definition $a^2 = a$

$\Rightarrow \quad a^2-a =0$

$\Rightarrow \quad a(a-1) = 0$

$\Rightarrow \quad a = 0$ or $a = 1$

Because R is an integral domain i.e. a ring without zero divisor. So product of two element is zero only if one of them is zero.

Example 3 : If a is a nilpotent element of the competative ring R, then prove that

1. ar is nilpotent $\forall$ r $\in$R
2. a is either zero or a zero divisor
3. 1+a is unit in P

4. u+a is a unit in R where $u \in$ R is a unit.

Solution : (1) Given a is nilpotent element in a computative ring R. so

$a^m = 0$, where m is least positive integer > 1

To prove ar is nilpotent, $r \in R$.

$(ar)^m = a^m r^m$

$= 0.r^m$

$= 0$

$\Rightarrow$ $(ar)^m = 0$

Hence ar is nilpotent.

(2) If $m = 1$, $a^1 = 0 \Rightarrow a = 0$, a is zero itself.

if $m > 1$ then $a^m = 0$

$\Rightarrow a\, a^{m-1} = 0$

$\Rightarrow$ a is a zero divisor. as $a \neq 0$ so $a^{m-1} \neq 0$

(3) Let $b = 1 - a + a^2 ---- +(-1)^{m-1} a^{m-1}$

then $(1+a)b = (1+a)\,[1-a+a^2 ----- +(-1)^{m-1} a^{m-1}]$

$= 1 - a + a^2 ---- +(-1)^{m-1} a^{m-1} + a - a^2 + a^3 ---- +(-1)^{m-1} a^m$

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

$= 1 - (-1)^{m-1} 0$ [$\because$ $a^m = 0$

$= 1 - 0$

$= 1$

$(1+a)\, b = 1$

So 1+a is unit.

(4) Let $u \in R$ is a unit,

then $u^{-1} \in R$ and $uu^{-1} = 1\ u^{-1}u$ [by definition of unit

$\therefore$ $u^{-1}a$ is nilpotent in R [using (1)

$\Rightarrow (1+u^{-1}a)$ is a unit in R [using (3)

$= u(1+u^{-1}a)$ is a unit R. [using 3

= u + a is a unit in R

Hence proved.

Self Check Exercise - 2

Q. 1 Show that $A = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is a nilpotent element of $m_3(R)$.

17.5 Characteristic of A Ring

Definition

If in a ring R, $\exists$ a positive integer m such that $ma = 0 \ \forall \ a \in R$, then R is called a ring of finite characteristic and if n is the least positive integer for which $na = 0 \ \forall \ a \in R$, then n is called characteristic of a ring R.

Here na= a + a + -------- + 0

n times

Note : If no such positive integer exists then the ring R is said to be a ring of characteristic zero. the characteristic of a ring is denoted by char R.

Example 1 : Set of integer has Characteristic zero

Solution : There is no positive integer, which when multiplied by each element of set of integer becomes zero. So characteristic of Z set of integer is zero.

Example 2 : Set of rational Q, set of real R and set of complex numbers C all have characteristic zero.

Example 3 : Show that characteristic of Z_2 is 2

Solution : Since $Z_2 = \{0, 1\}$

Since Z_2 is a ring, so $(Z_2 +2)$ is a group under addition, Then for any $a \in Z_2$ if we have

na = a + a + a -------- a = 0

n times

Then n is characteristic of Z_2

Since $0 \in Z_2$ and $0 +_2 0 \equiv 0 \bmod 2$

$1 \in Z_2$ and $1 +_2 1 \equiv 0 \bmod 2$

So , Z_2 has characteristic 2

Example 4 : Find the Characteristic of Z_4

Solution : Since $Z_4 = \{0, 1, 2, 3,\}$

Since $0 \in Z_4$, $0 +_4 0 +_4 Q +_4 0_4 \equiv 0 \pmod 4$

$1 \in Z_4$, $1 +_4 1 +_4 1 +_4 1 \equiv 0 \pmod 4$

$2 \in Z_4$, $2 +_4 2 +_4 2 +_4 2 \equiv 0 \pmod 4$

$3 \in Z_4$, $3 +_4 3 +_4 3 +_4 3 \equiv 0 \pmod 4$

Hence Char $(Z_4) = 4$

Remark

Char $Z_n = n$.

Theorem : The characteristic of an integral domain is either zero or a prime number.

Proof : Let R be an integral domain.

If characteristic of R is zero, then there is nothing to prove.

Suppose R has a finite characteristic

Then there exists a positive integer m such that

$ma = 0 \forall a \in R$.

Let p be such least positive integer, then char (R) = p.

To prove p is a prime.

Let p is not a prime, then $p = p_1p_2$, $p_1 \neq 1$, $p_2 \neq 1$

and $p_1 < p$, $p_2 < p$.

Now $pa = 0 \forall a \in R$

$\Rightarrow (p_1p_2)a = 0 \forall a \in R$

$\Rightarrow (p_1p_2)ab = 0 \forall a,b \in R$

$\Rightarrow ab + ab +$ ---------- $+ ab = 0 \forall a, b \in R$

---------- p_1p_2 times ----------

$\Rightarrow \{a + a +$ -------- $+a\} \{b + b +$ ------- $+ b\} = 0$

$p_1$times $p_2$times

$\Rightarrow p_1a \,.\, p_2b = 0$

$\Rightarrow$ either $p_1a = 0$ or $p_2b = 0$ $\because$ R is an integral

domain i.e. ring without zero divisor

Also $p_1 < p$ and $p_2 < p$, and p is least positive integer such that $pa = 0$

Hence this a contradisticion.

Hence p must be a prime

Theorem 2 : Let R be ring with identity 1. If is an element of finite order in the group $(R_1 +)$ then the order of 1 is the characteristic of R. If 1 is infinite order then characteristic of ring is zero.

Proof : Suppose the order of 1 is n. Then n is least positive integer such that n.1 = 0

n.1 = 1+1+ ------- +1 (n times) = 0

Now Let $a \in R$, then

na = a + a+ ------ + a (n times)

= 1.a +1.a + -----+1.a

= (1+1+1 ------- +1)a

= 0. a $\because$ n.1 = 0

na = 0

Thus na = 0 $\forall$ a $\in$ R

Hence the characteristic of the ring is n.

If 1 is of infinite order then there, is no positive integer n such that n.1 = 0.

Hence Characteristic of the ring is zero.

Example 5 : If r is a ring in which x2 = x $\forall x \in$ R, Prove that R is commutative ring of characteristic 2

Solution : R is a ring so (R1+) is an abelian group.

Let x $\in$ R then -x $\in$ R

Now given $x^2 = x$

so $x^2 = (-x)^2 = -x$

$\Rightarrow$ x = -x

$\Rightarrow$ x + x = 0

2x = 0 $\forall$ x $\in$ R

Therefore, char (R) = 2 (1) [by definite of characteristic of R

Now $\forall x, y \in R$, x + y $\in$ R $\because$ (R+) is ring so closed under addition

$x + y = (x+y)^2$ $\because$ given x $\in$ R $x^2 = x$

$= (x+y)(x+y)$

$= x^2 + xy + yx + y^2$

x+y $= x + xy + yx + y$ $\because$ $x^2 = x, y^2 = y$

using cancellation Law under addition, we get

xy + yx = 0 (2)

Since x, y $\in$ R $\Rightarrow$xy$\in$ R [$\because$ R is a ring, so closed under multiplication]

Since char (R) = 2 [using (1)]

So 2(xy) = 0

xy + xy = 0 (3)

From (2) and (3) we get

xy + yx = xy + xy

using left cancellation law

$yx = xy \qquad \forall\ x, y \in R$

Hence R is a commutative ring.

Example 6: Let a, b be elements of commutative ring R of characteristic two, show that $(a+b)_2 = a_2 + b_2 = (a-b)_2$

Solution: Let R be a commutative ring of characteristic 2 let $a, b \in R$

then $(a+b)^2 = (a^2+b)\ (a+b)$

$= a(a + b) + b\ (a + b)$

$= aa + ab + ba + bb$

$= a^2 + ab + ba + b^2$

$= a^2 + 2ab + b^2 \qquad \because$ ab = ba, R is commutative

$\Rightarrow \quad (a+b)^2 = a^2 + b^2 \qquad \begin{bmatrix} \because a, b \in R, ab \in R \text{ and } Charcr) = 2 \\ so\ 2(ab) = 0 \end{bmatrix}$

Again, $(a-b)^2 = (a-b)\ (a-b)$

$= a(a-b) - b\ (a-b)$

$= aa - ab - ba + bb$

$= a^2 - ab - ab + b^2 \qquad [\because$ Char R = 2 so 2 (ab) = 2]

$\Rightarrow \quad (a-b)^2 = a^2 + b^2$

Hence $(a+b)^2 = a^2 + b^2 = (a-b)^2$

Example 7: Let R be a ring of characterstic n. Let M be a ring of all 2×2 matrices over R, then show that char (M) = n

Solution: Since R be a ring of char (R) = n

then by definition, if $x \in R$ then $nx = 0\ \forall\ x \in R$

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be any matrix in M, where $a, b, c, d \in R$

Since a, b, c, $d \in R$ and R be ring of characteristic n

so na = nb = nc = nd = 0

Now, $nA = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \ldots\ldots\ldots\ldots\ldots + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ [n times]

$= \begin{bmatrix} na & nb \\ nc & nd \end{bmatrix}$

$= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $\because$ na = nb = nc = nd = 0

$\Rightarrow$ nA = 0 $\forall$ A $\in$ M

So Char (M) = n.

Example 8: Let R be an integral domain. Let a$\in$ R - {0} be such that na = 0 for some positive integer n. Show that R is of a finite characteristic

Solution: Let a $\in$ R - {0} be such that na = 0 (given)

Let x $\in$ R, then

(na) x = 0

$\Rightarrow$ (a + a + ... + a) x = 0

..... n times

= (ax + ax + ... ax) n times = 0

= a (x + x + ... + x) = 0 $\forall$ x $\in$ R

As R is an inlegral domain, so does not have zero divisor, also a $\neq$ 0 so

= x + x + ... + x = 0

n times

= nx = 0 $\forall$ x $\in$ R

$\therefore$ Characteristic of R is finite = n

Self Check Exercise - 3

Q.1 Find the char (Z_6)

Q.2 Let R be a commutative ring with characteristic þ, þ$\in$ P then show that $(a+b)^{þ} = a^{þ} + b^{þ}$, a, b $\in$ R.

17.6 Boolean Ring:-

Definition:

A ring R is called a Boolean ring if every element of R is idempotent

i.e. for all x $\in$ R, $x^2 = x$.

Examples 1: The ring $(Z_2, +_2, \times_2)$ is a Boolean ring.

Solution: Since $Z_2 = \{0, 1\}$

Z_2 has only two element, we can easily prove that Z_2 is a ring.

Now to prove $x^2 = x$ for 0 and 1

as $0^2 = 0$, and $1^2 = 1$

Since both the elements of Z_2 are idempotent, So $(Z_2, +_2, \times_2)$ is a Boolean ring.

Example 2: Show that $(Z_3, +_3, \times_3)$ is not a Boolean ring

Solution: Since $Z_3 = \{0, 1, 2\}$

we can easily prove that Z_3 is a ring.

Now to check $\forall\ x \in Z_3$, $x^2 = x$

as $0^2 = 0$, $1^2 = 1$ but $2^2 = 4$

Since 2 is not an idempotent element of Z_3.

So Z_3 is not a Boolean ring.

Example 3: Show that characteristic of a Boolean ring is 2.

Solution: Let R be a Boolean ring.

then by definition $\forall\ x \in R$ x2 = x

If $x \in R$ then $-x \in R$

Also $x = x^2 = (-x)^2 = -x$

$\Rightarrow$ $x = -x$.

$\Rightarrow$ $x + x = 0$

$\Rightarrow$ $2x = 0$

$\Rightarrow$ char (R) = 0, as $x \in R$.

Theorem 1: Let R be a Boolean ring. Then

1. $2x = 0$ $\forall\ x \in R$
2. $xy = yx$ $\forall\ x, y \in R$

Proof: (1) Let $x \in R$, as R is a ring, $-x \in R$

Now $x = x^2$ R is Boolean ring

$= (-x)^2$

$= -x$

$\Rightarrow$ $x + x = 0$

$= 2x = 0$ $\forall\ x \in R$.

(2) Let $x, y \in R$ then

$x + y = (x + y)^2$

$= (x + y)(x + y)$

$= x(x + y) + y(x + y)$

$= x^2 + xy + yx + y^2$ $\left[\because R \text{ is Boolean ring } x, y \in R \Rightarrow x^2 = x, y^2 = y\right]$

$\Rightarrow$ $x + y = x + xy + yx + y$

using cancellation law under addition

$xy + yx = 0$ (1)

as $x, y \in R \Rightarrow x y \in R$ then using (1)

$2 (xy) = 0$

$\Rightarrow$ $xy + xy = 0$ (2)

From (1) and (2)

$xy + yx = xy + xy$

using cancellation law, we have

$\Rightarrow$ $yx = xy, \forall x, y \in R$

Hence Booleans ring is commutative

The converse of this is not true.

Self Check Exercise - 4

Q.1 Give an example of commutative ring which is not Boolean.

17.7 Summary:-

In this unit, we studied that

1. an element of a ring is called idempotent if $x^2 = x$
2. an element of a ring is called nilpotent if $x^n = 0$ for some least positive integer n
3. If for $x \in R$, R is a ring and $nx = 0$ then char (R) = n
4. In Boolean ring, $\forall x \in R$, $x^2 = x$ i.e. each element of Boolean ring is idempotent.

17.8 Glossary

- **Nilpotent element:-** An element $x \in R$ is called nilpotent if $x^n = 0$ for some positive integer n.
- **Idempotent element:-** An element $x \in R$ is called idempotent, if $x^2 = x$.
- **Boolean ring:-** A Ring R is called Boolean ring if every element

17.9 Answers to Self Check Exercises

Self Check Exercise - 1

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

Self Check Exercise - 2

Q. 1 $A^2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = 0$

Self Check Exercise - 3

Q.1 Char $(Z_6) = 6$

Q.2 defining of characteristic of ring to prove this.

Self Check Exercise - 4

Q.1 Ring of integers is a commutative ring. But all elements of ring of integers not satisfies the property $x^2 = x$. So it is not a Boolean ring.

17.10 References/Suggested Reading

1. Vijak. . Khanna, and S.K. Bhambri, A course in Abstract Algebra.
2. Joseph A Gallian, Contemporary Abstract Algebra.
3. Frank Ayres Jr. Modren Algebra, Schaum's Outline Series
4. A.R. Vasistha, Modern Algebra, Krishna Prakashna Media.

17.11 Terminal Questions

1. Show that the characteristic of M2 (Z3) is 3.
2. Give an example of infinite ring of non zero characteristic

*****

Unit - 18

Subring

Structure

18.1 Introduction

Dear student, in this unit we will study about the subring. We will prove certain sets to be a subring. We will study about the intersection and union operation applied on subring and their results. We will also discuss about the subring generated by a subset of a ring.

18.2 Learning Objectives:

After studying this unit, students will be able to

1. define and give examples of subrings
2. prove a given set a subring
3. apply set operations on subring
4. solve theorem based on subring.

18.3 Subring:-

Definition:

Let R be a ring. A non empty subset of S of the set R is said to be a subring of R if S is closed with respect to the operation of addition and multiplication in R and S itself is a ring for

these operation. or a non empty subset S of ring $\langle R,+,.\rangle$ is called a subring of R if $\langle S,+,.\rangle$ is a ring itself.

Trivial Subrings:

If R is a ring then {0} and R alway subring of R. These are called trivial subrings of R.

Over Ring

If S is subring of R, then R is called an over ring of S.

Let us taken following examples to understand more about subring.

Example 1: 2Z is a subring of Z

Solution: Since Z = $\{.....-4,-3,-7,-1,0,1,2,3,4.....\}$ is the set of integers. In the unit of ring we had already prove that Z is a ring

Now 2Z = $\{.....-8,-6,-4,-2,0,2,4,6,8.....\}$

Axioms under addition

1. Closure property:

   Since Z si closed under addition. So 2Z is also closed under addition

2. Associative property:

   Since Z is associative under addition so that 2z.

3. Existence of identity:-

   Since $0 \in 2Z$, So 0 is identity element under addition for the subset 2Z of Z.

4. Existence of Inverse:-

   Since for all $x \in 2Z \exists -x \in 2Z$ such that x + (-x) = 0 = (-x) +x.

   So -x act as inverse element of each $x \in 2Z$

5. Commutative Property:-

   Since integers are commutative under addition. So 2Z is also commutative under addition i.e. $x, y \in 2Z$ x+y = y + x.

6. Closure property:-

   Since Z is closed under multiplication so as 2Z.

7. Associative property:

   Since Z is associative under multiplication so as 2Z.

8. Distributive Property:

   Since Z, set of integers holds distributive property so as 2z, will hold this property too.

Example 2: Z is a subring of Q

Example 3: Q is a subring of R

Example 4: R is a subring of C.

Criteria For a Subset of a Ring to Be a Subring

Theorem 1: Let R be a ring and S be a non empty subset of R. Then necessary and sufficient condition that S is a subring of R is

$\forall$ a, b $\in$ S $\Rightarrow$ a - b, a b $\in$ S.

Proof: Let S be a subring of R. Then $\langle S, + \rangle$ is on abelian sub group under addition of $\langle R, + \rangle$.

Since $\langle S, + \rangle$ is a sub group

So, let a, b $\in$ S

$\Rightarrow$ a - b $\in$ s $\forall$ a b $\in$ S (by definition of sub group)

Also as s is a subring of R. So S is closed under multiplication. So if a, b $\in$ S then a b $\in$ S

Hence if s is a subring of R then a - b, a b $\in$ S $\forall$ a b $\in$ S

Conversely:

Let a, b $\in$ S then a - b, a b $\in$ S

To prove S is subring of R.

$\Rightarrow$ $\langle S, + \rangle$ forms a subgroup of $\langle R, + \rangle$

also, a, b $\in$ R, a + b = b + a, this also holds in S

So $\langle S, + \rangle$ is abelian subgroup of $\langle R, + \rangle$

Since multiplicative associativity and distributive holds automatically in S.

So S is a ring itsey

$\Rightarrow$ S is a subring of R.

Example 5: Show that the set of matrices $\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$, x, y, z $\in$Z is a subring of ring of 2×2 matrices over integers.

Solution: Given R is a ring of 2×2 matrices over integers.

Let S = $\left\{ \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}, x, y, z \in z \right\}$ be a subset of R.

Now Let A = $\left\{ \begin{bmatrix} x_1 & y_1 \\ 0 & z_1 \end{bmatrix}, x_1, y_1, z_1 \in z \right\}$

and B = $\begin{bmatrix} x_2 & y_2 \\ 0 & z_2 \end{bmatrix}, x_2, y_2, z_2 \in z$

Now A - b = $\begin{bmatrix} x_1 & y_1 \\ 0 & z_1 \end{bmatrix}$ - $\begin{bmatrix} x_2 & y_2 \\ 0 & z_2 \end{bmatrix}$

$\Rightarrow$ A - B = $\begin{bmatrix} x_1 - x_2 & y_1 - y_2 \\ 0 & z_1 - z_2 \end{bmatrix}$

as $x_1, x_2, y_1, y_2, z_1, z_2 \in$ Z so $x_1 - x_2, y_1 - y_2, z_1 - z_2 \in$ Z

So A - B $\in$ S

Now AB = $\begin{bmatrix} x_1 & y_1 \\ 0 & z_1 \end{bmatrix}\begin{bmatrix} x_2 & y_2 \\ 0 & z_2 \end{bmatrix}$

AB = $\begin{bmatrix} x_1x_2 & x_1y_2 + y_1z_2 \\ 0 & z_1 - z_2 \end{bmatrix}$

As $x_1, x_2, y_1, y_2, z_1, z_2 \in$ Z so x_1x_2, $x_1y_2 + y_1z_2$, $z_1z_2 \in$ Z

So that A B $\in$ S

then S = $\left\{\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}, x, y, z \in z\right\}$ is a subring of 2×2 matrices over integers.

Example 6: Let R be a ring of 3×3 matrices over real. Show that

S = $\left\{\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix} : x \in R\right\}$ is a subring of R.

Solution: Given S = $\left\{\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix} : x \in R\right\}$

Since 0 $\in$R so $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in S$

So S is non empty sub set of R.

Let A = $\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix}$ B = $\begin{bmatrix} y & y & y \\ y & y & y \\ y & y & y \end{bmatrix}$ be any two elements of S, x, y $\in$ R

then A - B = $\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix}$ - $\begin{bmatrix} y & y & y \\ y & y & y \\ y & y & y \end{bmatrix}$

A - B = $\begin{bmatrix} x-y & x-y & x-y \\ x-y & x-y & x-y \\ x-y & x-y & x-y \end{bmatrix}$

As x, y $\in$ R so that x - y $\in$ R.

Hence A - B $\in$ S.

Now AB = $\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix}\begin{bmatrix} y & y & y \\ y & y & y \\ y & y & y \end{bmatrix}$

= $\begin{bmatrix} xy+xy+xy & xy+xy+xy & xy+xy+xy \\ xy+xy+xy & xy+xy+xy & xy+xy+xy \\ xy+xy+xy & xy+xy+xy & xy+xy+xy \end{bmatrix}$

AB = $\begin{bmatrix} 3xy & 3xy & 3xy \\ 3xy & 3xy & 3xy \\ 3xy & 3xy & 3xy \end{bmatrix}$

As x, y $\in$ R $\Rightarrow$ x y $\in$ R So 3 x y $\in$ R

Hence A B $\in$ S

Therefore S is a sub ring of ring of 3×3 matricere

Example 7: Check T = $\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix}$, a, b $\in$ R is a subring of $M_2(R)$

Solution : Given T = $\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix}$, a, b $\in$ R

Let A = $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ for a = 1, b = 0 $\in$ T

and $B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ for a = 0, b = 1 $\in$ T

Then A - B = $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

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

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

Since 0_1 1_1 -1 $\in$ R

So A - B $\in$ $M_2(R)$

Now AB = $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

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

$= \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \notin$ T

AB $\notin$ T

So T = $\left\{\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix}\right.$ is not a subring of $M_2(R)$

Example 8 : If S is a subring of a ring R then S is commutative of R is commutative ring.

Solution : Given S is subring of commutative ring R.

To prove S is commutative

Let a, b $\in$ S

As S $\in$ R

so a, b$\in$ R

as R is commutative

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

So, a, b $\in$ S ab = ba

Hence S is commutative subring of R which is itself commutative.

Theorem 2 : The subring $\leq$ is without zero divisor if R is without zero divisor.

A subring of on integral domain is an integral domain

Solution : Let S is a subring of R and R is an integral domain i.e. a, b $\in$ R a $\neq$ 0, ab = 0

To prove S is an integral domain

Let a, b $\in$ S and S $\leq$ R

so a, b $\in$ R

as R is an integral domain

so ab = 0

$\Rightarrow$ either a = 0 or b = 0

since a $\neq$ 0, so b = 0

so S is a subring without zero divisor.

Hence a subring of integral domain is an integral domain.

Note :

Ring and subring may have same or different multiplicative identities. For example.

Example 1 : The subring Z of Q.

Solution : Here the identity element is same that is 1.

Example 2 :nZ, n $\neq$1, -1, is a subring of Z.

Solution : Here the ring Z has identity 1 but subring has no identity.

Example 3 : $R_1 = \left\{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, a \in R\right\}$ is a subring of $R_2 = \left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, b \in R\right\}$

Solution : Here the ring has no identity whereas subring has identity $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

Example 4 : Zx{0} = {(a, 0 : a $\in$ Z} is a subring of ZxZ = {(a, b) : a, b $\in$ z}

Solution : The ring has identity (1, 1) whereas subring has identity (1, 0). So both ring and subring has different identity element.

Self Check Exercises

Q. 1 Check $S = \left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix}, a, b \in R\right\}$ is a subring or not of $M_2(R)$

Q. 2 Prove that $S = \left\{\begin{bmatrix} a & B \\ -\bar{B} & \bar{x} \end{bmatrix}\right.$, is a subring of $M_2(c)$, all 2x2 makices over complex.

Q. 3 Find the identity element of M3(R) and its subring S = $\left\{ \begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix}, x \in R \right\}$

18.4 Set operations of Subrings

Theorem 1 : Intersection of a family of subring of a ring R is also a subring of R.

Proof : Let R be a ring

Let S_1, S_2 ------- S_n be subring of R then

$\bigcap_{i=1}^{n} S_i \subset$ R obviously.

Since , O $\in$ each S_i

$\Rightarrow$ O $\in \bigcap_{i=\phi}^{n} S_i$

So $\bigcap_{i=1}^{n} S_i$ is non empty subset of R.

Now to prove $\bigcap_{i=1}^{n} S_i$ is a subring

Let x, y $\in \bigcap_{i=1}^{n} S_i$

$\Rightarrow$ x, y $\in$ each S_i

Since each S_i is a subring, So

x - y, xy$\in$ each si

$\Rightarrow$ x - y, xy$\in \bigcap_{i=1}^{n} S_i$

Hence $\bigcap_{i=1}^{n} S_i$ is a subring R.

Example 1 : Show by example that union of two subring need not be a ring.

Solution : Let 2z and 3z be the two subring of z

z = { ..... -3, -2, -1, 0, 1, 2, 3 ....}

then 2z = {.... -6, -4, -2, 0, 2, 4, 6, ...}

and

3z = {..... -9, -6, -3, 0, 3, 6, 9, ...}

Now 2z U 3z = {..... -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9 .....}

Since 21 3 $\in$ 2z U 3 z

But 2+3 = 5 $\notin$ 2z U 3 z

So not closed under addition

Hence union of two subring is not a ring.

Example 2 : Give an example to show that sum of two subring need not be a subring of R.

Solution : Let $M_2(Z)$ be a ring of all 2x2 matrices.

Let $R_1 = \left\{\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, a \in Z\right\}$

$R_2 = \left\{\begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix}, b \in Z\right\}$ be two subring of $M_2(Z)$

Now $R_1+R_2 = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix}$

$R_1+R_2 = \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix}$ 1

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

$AB = \begin{bmatrix} 4 & 0 \\ 0 & 6 \end{bmatrix} \notin R_1+R_2$

So R_1+R_2 is not closed under multiplication

Hence sum of two subring needs not be a subring.

Example 3 : Let R_1 and R_2 be two rings and S_1 and S_2 be two subrings of R_1 and R_2 respectively. Then S_1 x S_2 is a subring of R_1 x R_2.

Solution : Let a $\in$ S_1 and b $\in$ S_2

Then S_1 x S_2 = {(a, b); a$\in$ S_1, b $\in$ S_2}

As S_1 and S_2 are subrings

so a $\in$ S_1 and a $\in$ S_2

$\Rightarrow$ a $\in$ S_1 x S_2

$\Rightarrow$ S_1 x S_2 is non empty subset.

Let $x = (a_1, b_1)$ and $y = (a_2, b_2)$ be two elements of $S_1 \times S_2$

where $a_1, a_2 \in S_1, b_1, b_2 \in S_2$,

Then $x - y = (a_1, b_1) - (a_2, b_2)$

$x - y = (a_1 - a_2 , b_1 - b_2)$

Since S_1 and S_2 are ring so

$a_1 - a_2 \in S_1$ and $b_1 - b_2 \in S_2$

$x - y \in S_1 \times S_2$

Now $xy = (a_1, b_1)(a_2, b_2)$

$\Rightarrow xy = (a_1 a_2 , b_1 b_2)$

as $a_1, a_2 \in S_1 \Rightarrow a_1, a_2 \in S_1$

and $b_1, b_2 \in S_2$ So $b_1, b_2 \in S_2$

So $xy \in S_1 \times S_2$

Hence $S_1 \times S_2$ is a set ring of ring $R_1 \times R_2$

Self Check Exercise - 2

Q. 1 Intersection of two subrings of a ring R is a subring.

18.5 Centre of a Ring

Definition :

Let R be a ring. Then

$C(R) = \{a \in R, xa = ax \ \forall \ x \in R\}$ then C(R) is called the centre of the ring R.

Theorem 1 : The centre of a ring R is a subring of R.

Proof : Since $0 \in C(R)$

So $C(R) \neq \phi$, is non empty set.

Now to prove $a - b \in C(R)$ and $ab \in C(R)$

Let $a, b \in C(R)$

Then for all $x \in R$, $xa = ax$ and $xb = bx$ [by definition of centre of ring]

Now $xa - xb = ax = bx$

$\Rightarrow x(a - b) = (a - b) x$

$\Rightarrow (a - b) \in C(R)$

Again $xab = axb$ $\therefore x \in R$, and

$= abx$

$\Rightarrow x(ab) = (ab)x$

$\Rightarrow ab \in C(R)$

Since a-b, $ab \in C(R)$ so, c(R), centre of ring is a subring.

Note :

1. R is a commutative ring if and only if C(R) = R
2. C(R) is a commutative subring of R.

Theorem 2 : Let R be a division ring, then the centre C(R) of R is a field

Proof : Since a commutative division ring is a field.

We know C(r) is a commutative subring of R.

Now to prove C(R) is a divison ring

Given R is a division ring

$\Rightarrow$ R is a ring with unity

$\Rightarrow 1 \in R$

$\Rightarrow$ all non zero elements have inverse.

Also $1.x = x = x.1$ For all $x \in R$

Since C(R) is a subring of R

Let $x \in C(R)$, $x \neq 0$ be any element

So $x \in R$ as $C(R) \leq R$.

Since R is a division ring, so $x^{-1} \in R$.

Let $y \in R$ be any non zero element then $y^{-1} \in R$

Now $x^{-1}y = (y^{-1} x)^{-1}$

$= (xy^{-1})^{-1}$ $\because x \in C(R)$

$= yx^{-1}$

$\Rightarrow x^{-1}y = yx^{-1}$

$\Rightarrow$ x^{-1} commute of with non zero element of R

Also $x^{-1} . 0 = 0 = 0.x^{-1}$

$\Rightarrow x^{-1} \in C(R)$

Thus C(R) is a division ring also C(R) is commutative ring So C(R) is a field.

Self check Exercise - 3

Q. 1 Find centre of S, for E2.

18.6 Summary :

In this unit we studied that

1. A non empty subset S of set R is a subring if itself is a ring.
2. The necessary and sufficient condition that a non empty subset is a subring of R is $\forall$ a, b $\in$ S $\Rightarrow$ a - b, ab $\in$ S
3. Subring of a integral domain is an integral domain.
4. Ring and subring may have same or different identities.
5. Intersection of two subring is again a subring.
6. Union of two subring may or may not be a ring
7. Centre of ring is a commutative subring.
8. Centre of ring is a field.

18.7 Glossary :

- **Subring :** A non-empty subset S of Ring R is called subring if S is itself a Ring.
- **Over Ring :** If S is subring of R_1 then R is called an over ring of S.
- **Centre of Ring :** Let R be a ring, then

  C(R) = {a$\in$ R1 xa = ax $\forall$ x $\in$ R}

18.8 Answers to Self Check Exercises

Self Check exercise-1

Q. 1 Yes

Q. 2 Prove A - B, and AB $\in$ S where A, B are two elements of S.

Q. 3 Identity of R = $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

and identity of S = $\begin{bmatrix} 1/3 & 1/3 & 1/3 \\ 1/3 & 1/3 & 1/3 \\ 1/3 & 1/3 & 1/3 \end{bmatrix}$

Self Check Exercise - 2

Q. 1 Can be prove easily on the basis of theorem i.e. intersection of a family of subring of a ring is always a subring.

Self CheckExercise - 3

Q. 1 C(S) = $\left\{ \begin{bmatrix} x & 0 \\ 0 & \bar{x} \end{bmatrix}; \forall x \in C \right\}$

18.9 References/Suggested Readings

1. Vijay K Khanna and S.K. Bhambri, A course in Abstract Algebra.
2. Joseph A. Gallian, Contemporary Abstract Algebra.
3. Frank Ayres Jr, Modern Algebra, Schaum's outline series.
4. A.R. Vasistha, Modern Algebra, Krishna Prakashan Media.

18.10 Terminal Questions

1. Show that the set of matrices $\begin{bmatrix} x & 0 \\ y & z \end{bmatrix}$ where x, y z $\in$ I is a subring of the ring of 2x2 matrices over integers.
2. Let S. {[0], [2], [4], [6], [8]} where [n] denotes equivalence classes of n module 10. Prove that S is a subring of Z_{10} with the usual operations of Z_{10}. Also show that S has an identity which is different from Z_{10}.

Unit - 19

Ideal

Structure

19.1 Introduction

Dear students in this unit we will study about another property related to ring which finally gives us an idea of ideal. We will discuss about proper and improper ideal along with algebra of ideals i.e. addition, multiplication, union and intersection of ideal.

19.2 Learning Objectives:

After studying this unit students will be able to

1. define ideal of a ring, left and right ideal or two sided ideal of a ring.
2. define distinguish and find proper and improper ideal of a ring.
3. prove theorem based on algebra of ideal and able to do question related to algebra of ideal.

19.3 Left and Right Ideal

Definition:

Left Ideal : A non empty subset I of a ring R is called a left ideal of R if

(1) For all $a, b \in I \Rightarrow a - b \in I$

(2) For all $a \in I$, $r \in R \Rightarrow r\,a \in I$

Right Ideal

Similarly, A non empty subset I of a ring R is called a right ideal of R if

(1) For all $a, b \in I \Rightarrow a - b \in I$

(2) For all $a \in I$, $r \in R \Rightarrow a\,r \in I$

Two sided ideal or Ideal

An Ideal I is called a two sided ideal or simply an ideal of ring R if I is both left sided and right sided i.e.

(1) For all $a, b \in I \Rightarrow a - b \in I$

(2) For all $a \in I$, $r \in R \Rightarrow ar = ra \in I$

Note

When a ring is commutative then there is no difference between left and right ideal.

Theorem 1 : An ideal I of a ring R is a subring of R, but converse is not true.

Proof : Let I be ideal of ring R, to prove I is a subring of R.

Since I is ideal of ring R, then by definition of ideal

(1) For all $a, b \in I$, $a - b \in I$

(2) For all $a \in I$, $r \in R$,$ar \in I$

We can easily say that I is a subring of R (using the criterion of a subring)

Converse :

Converse of this theorem need not be true.

i.e. a subring may not be an ideal, to prove this we shall take example

The set of rational Q is a ring and the set of integers is a subring of Q i.e $Z \subseteq Q$

But Z is not an ideal because,

Let $3 \in Z$ and $\frac{1}{2} \in Q$

then $3.\frac{1}{2} = \frac{3}{2} \notin Z$

Hence Z is not an ideal of Q.

To have more understanding of ideal let us take following examples of ideal.

Example : Show that nZ is an ideal of the right Z.

Solution : Since Z = {..... -4, -3, -2, -1, 0, 1, 2, 3, 4, ...}

Since Z is a ring

AlsonZ = {..... -4n, -3n, -2n, -n, 0, n, 2n, 3n, 4n, ...}

To prove nZ is an ideal of Z.

Let a, b $\in$nZ, the a - b $\in$nZ

Let a = nx, b = ny

Then a - b = nx - ny

= n(x-y)

a-b $\in$ n Z

Again a $\in$nZ, z $\in$Z

Then nx.z = n(xz) $\in$nZ

$\therefore$ nZ is a right ideal of Z

Since Z is a commutative ring

$\therefore$ nZ is also a left ideal of Z

Hence nZ is an ideal of Z.

Proper and improper Ideal

For any ring R, {0} and R are ideal of R. These ideals are called improper ideal. Any ideal other that {0} and R of ring R is known as proper ideal.

Example 2 : Show that set of even integers is an ideal of ring Z.

Solution : Since Z = {..... -4, -3, -2, -1, 0, 1, 2, 3, 4, ...}

Now 2Z = set of even integers

= {..... -8, -6, -4, -2, 0, 2, 4, 6, 8, ...}

Since Z is a commutative ring, so we just prove 2Z is an right ideal.

To prove 2Z is an ideal

Let x = -4, y = 2 $\in$ 2Z

Then x - y = -4 - 2

= -6 $\in$ 2 Z

So $\forall$ x, y $\in$ 2Z, x - y $\in$ 2 Z

Again Let x = -4 $\in$ 2 Z and r = -3 $\in$ Z

then x.r = -4x-3

= +12

= 2.6

= even integer

So $\forall$ x $\in$ 2 Z, R $\in$ Z then xr$\in$ 2Z

Hence 2Z is an ideal of the ring Z.

Example 3 : Consider the ring $M_2(z)$. Let

$I = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}; a, b \in Z \right\}$ then prove that I is a left ideal of $M_2(Z)$ but not a right ideal.

Solution : Since we known that M2(Z) is a ring.

To prove $I = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}; a, b \in Z \right\}$ is an left ideal.

Let $x = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \in I$

$y = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} \in I$

and $r = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_2(Z)$. Then

$x - y = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} - \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$

$= \begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix}$

$\Rightarrow$ $x - y \in I$

$xr = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix}$

$= \begin{bmatrix} ax & ay \\ bx & by \end{bmatrix} \in M_2(Z)$

Again $rx = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$

$= \begin{bmatrix} xa+yb & 0 \\ za+wb & 0 \end{bmatrix}$

$\Rightarrow$ $rx \in I$

Since $rx \in I$, but $xr \notin I$, $xr \in M_2(z)$

So, I is left ideal out not right ideal.

Example 4 : Consider the ring $M_2(Z)$ and Let I = $\left\{\begin{bmatrix} a & c \\ b & d \end{bmatrix}; \text{a, b, c, d are even integres}\right\}$. Prove that I is an ideal of $M_2(Z)$.

Solution : Since we know that $M_2(Z)$ is a ring.

Given I = $\left\{\begin{bmatrix} a & c \\ b & d \end{bmatrix}; \text{a, b, c, d are even integres}\right\}$

Let x = $\begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}$, y = $\begin{bmatrix} 6 & 8 \\ 4 & 10 \end{bmatrix}$

Then x - y = $\begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}$ - $\begin{bmatrix} 6 & 8 \\ 4 & 10 \end{bmatrix}$

= $\begin{bmatrix} 2-6 & 4-8 \\ 6-4 & 8-10 \end{bmatrix}$

= $\begin{bmatrix} -4 & -8 \\ 2 & -2 \end{bmatrix}$

$\Rightarrow$ x - y $\in$ I where -4, -8, 2, -2 are even integers

Now x = $\begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}$ and r = $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \in M_2(Z)$

Then r x = $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}$

= $\begin{bmatrix} 2+12 & 4+16 \\ 6+24 & 12+32 \end{bmatrix}$

= $\begin{bmatrix} 14 & 20 \\ 30 & 44 \end{bmatrix}$

$\in$ I, as 14, 20, 30, 44 are all even integer.

Now xr = $\begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$

= $\begin{bmatrix} 2+12 & 4+16 \\ 6+24 & 12+32 \end{bmatrix}$

$= \begin{bmatrix} 14 & 20 \\ 30 & 44 \end{bmatrix}$

$\in I$

Since $\forall$ x, y $\in$I, x - y $\in$ I

and $\forall$ x $\in$ I and r $\in$ $M_2(Z)$ $\Rightarrow$xr = rx$\in$ I

Hence I is an ideal of M_2 (Z).

Example 5 : Let $M_2(Z)$ is a ring and I = $\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}; a \in Z \right\}$ be a subset of $M_2(Z)$ then show that I is a subring of $M_2(Z)$ but not an ideal.

Solution : Since we know that $M_2(Z)$ is a ring.

Let I = $\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}; a \in Z \right\}$

To prove I is an ideal or not.

Let x = $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, y = $\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$, 1, 2, $\in$ Z

Now x - y = $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$

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

$\Rightarrow$ x - y $\in$ I

Now xy = $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$

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

$\Rightarrow$ x - y $\in$ I

Since $\forall$ x, y $\in$I, x - y, xy$\in$ I

So, I is a subring.

Now, Let r = $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in M_2(Z)$

and $x = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

then $xr = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$

$= \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \in I$

and $rx = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

$= \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \notin I$

So I is not a ideal of M_2 (Z).

Self Check Exercise-1

Q. 1 Let $M_2(Z)$ be a ring then prove that $I = \left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, a, b \in Z\right\}$ is a right ideal of $M_2(Z)$ but not a left ideal.

Q. 2 If R is a commutative ring and $a \in R$ then show that $aR = \{ar.; r \in R\}$ is a two sided ideal.

Q. 3 Give an example to show that if the ring is not commutative then the ideal is not two sided ideal.

19.4 Left and Right Annihilator

Left Annihilator

Let R be a ring and S be a non empty subset of the ring R then

$ann_l (S) = \{x \in R; xS = 0\}$ is known as left annihilator of ring R.

Right Annihilator

Let R be a ring and S be a non empty subset of the ring R then

$ann_r (S) = \{x \in R; Sx = 0\}$ is known as right annihilator of ring R.

Let us try following examples to have more understanding of these terms:

Example 1 : Show that left and right annihilators of R and left and right ideal of ring R.

Solution : Since R is a ring. So $a \in R$

Also we know that if S be a non-empty subset of a ring R such that $ann_r(S) = \{x \in R : Sx = 0\}$ and $ann_r(S) = \{x \in R : xS = 0\}$ are known as right and left annihilators of R.

Since $0 \in R$ s.t.S.o $= 0 \in ann_r(S)$

$\therefore$ $ann_r(S) \neq 0$, is a non emptyset :

Let $x_1, x_2 \in ann_r(S)$ be any two elements.

$\therefore Sx_1 = 0$ and $Sx_2 = 0$

$\Rightarrow Sx_1 - Sx_2 = 0$

$\Rightarrow S(x_1 - x_2) = 0$

$\Rightarrow x_1 - x_2 \in ann_r(S)$

Again, if $r \in R$, be any element and $x \in ann_r(S)$.

Then $Sx = 0$

Now $S(xr)r = (Sx)r$

$= 0.r$

$= 0$

$\Rightarrow$ $xr \in ann_r(S)$

Hence $ann_r(S)$ is a right ideal of R.

Similarly we can prove that $ann_r(S)$ is left ideal of R.

Example 2 : If R is a ring and $a \in R$ be any fixed element of R. Let $x = \{x \in R : ax = 0\}$. Then prove that x is a right ideal of R or Left annihilator of a in R.

Solution : Since $0 \in R$

$\Rightarrow 0 = a.0$

$\Rightarrow 0 \in x$

$\Rightarrow$ x is a non empty set

Let x_1 and x_2 be any two elements of x then

$ax_1 = 0$ and $ax_2 = 0$

$\Rightarrow$ $ax_1 - ax_2 = 0$

$\Rightarrow$ $a(x_1 - x_2) = 0$

$\Rightarrow$ $x_1 - x_2 \in x$

Also, Let $x \in x$ and $y \in R$ be any element, then $ax = 0$

Now $a(xy) = (ax)\, y$

$= 0.y$

$= 0$

$\Rightarrow xy \in x, \forall\ x \in x$ and $y \in R$

$\therefore$ x is right ideal of R

Using the definition of left annihilator we can easily say that x is right annihilator of R.

Self Check Exercise - 2

Q. 1 Let R is a ring and $a \in R$ be any fixed element of R. Let $x^1 = \{x \in R : xa = 0\}$. Then prove that x^1 is a left ideal of R, then it is also a right annihilator of a in R.

19.5 Algebra of Ideals

Theorem 1 : Intersection of two left (or right) ideals of a ring is a left (or right) ideal.

Proof : Let I and J be any two left ideal of a ring R.

Since $0 \in I$ and $0 \in J$

$\Rightarrow 0 \in I \cap J$

So $I \cap J$ is a non empty set.

Let $x, y \in I \cap J$ be two elements, to prove $x - y \in I \cap J$

Then $x \in I$ and $x \in J$

also $y \in I$ and $y \in J$

Therefore taking $x \in I$, $y \in I$ and I is a left ideal of R

$\Rightarrow x - y \in I$

Similarly $x \in J$ and $y \in J$ and J is left ideal of R

$\Rightarrow x - y \in J$

Since $x - y \in I$ and $x - y \in J$

$\Rightarrow x - y \in I \cap J$

Again, Let $r \in R$ be any element and let $x \in I \cap J$

to prove $rxi \in I \cap J$

Since $x \in I \cap J$

$\Rightarrow x \in I$ and $x \in J$

Taking, $r \in R$ and $x \in I$ and I is left ideal of R

$\Rightarrow rx \in I$

Similarly taking $r \in R$ and $x \in J$ and J is left ideal of R

$\Rightarrow rx \in J$

As $rx \in I$ and $rx \in J$

$\Rightarrow rx \in I \cap J \ \ \forall\ r \in R$ and $x \in I \cap J$.

Hence $I \cap J$ is a left ideal of R

* Similarly we can prove the same for right ideal.

Theorem 2 : the intersection of a family of left (or right) ideals is also a left (or right) ideal.

Proof : Let $\{I_x; x \in \cap\}$ be collection of left ideals of R. Also each I_x is a subring of R.

Also, since we known that intersection of a family of subring of a ring R is a subring of R.

Let $I = \bigcap_{x \in \wedge} Ix$ is a subring of R

Let $x \in I$ and $r \in R$

Then $x \in I_x$ and hence $rx \in I_x$ for each $r \in \Lambda$

Since Ix is a left ideal of R.

Thus $r\ x \in I$

$\Rightarrow$ I is left ideal of R.

Example 1 : Is union of ideals is an ideal or not? Prove using example.

Solution : Union of ideals is not an ideal. Let us show this by taking this examples. Since we known that nZ are ideals of Z. Specifically let 2Z and 3Z are ideals of Z.

To prove 2Z U 3 Z is an ideal or not.

Since Z = {..... -4, -3, -2, -1, 0, 1, 2, 3, 4, ...}

2Z = {..... -6, -4, -2, 0, 2, 4, 6, ...}

3Z = {..... -9, -6, -3, 0, 3, 6, 9, ...}

So 2Z U 3Z = {..... -9, -6, -4, -2, 0, 2, 3, 4, 6, 9 .....}

Since $2, 3 \in 2Z \cup 3Z$

To prove 2Z U 3Z is an ideal, we have to prove for $x, y \in 2Z \cup 3Z$, $x - y \in 2Z \cup 3Z$

As $2, 3 \in 2Z \cup 3Z$

$\Rightarrow 2 - 3 = -1 \notin 2Z \cup 3Z$

Hence 2Z U 3Z is not an ideal.

Theorem 3 : Let I and J be two ideals of ring R, then IUJ is an ideal of R iff either $J \subseteq I$.

Proof : Let I and J be two ideals of ring R such that either $I \subseteq J$ or $J \subseteq I$, to prove $I \subseteq J$ is not ideal.

Since $I \subset J$

$\Rightarrow$ I U J = J and J is an ideal of ring R

Therefore I U J is an ideal of R.

Again $J \subset I$

$\Rightarrow$ I U J = I and I is an ideal of ring R.

So I U J is an ideal of R.

Conversely

Let I U J is an ideal r, then to prove either I $\subseteq$ J or J $\subseteq$ I.

Since I U J is an ideal of R.

Let a $\in$ I and b $\in$ J

Then a, b $\in$ I U J.

Since I U J is an ideal of R.

Then a - b$\in$ I U J.

So either a - b $\in$ I or a - b $\in$ J

If a - b $\in$ I and a $\in$ I and I is an ideal of R

Then a - (a - b) $\in$ I

$\Rightarrow$ b $\in$ I

So, hence, J $\subseteq$ I [By property of subset]

Again if a - b $\in$ J and b $\in$ J and J is an ideal of R

Then a + (a - b_ $\in$ J

$\Rightarrow$ a $\in$ J

As a $\in$ I $\Rightarrow$ a $\in$J

So I $\subseteq$ J [using the property of subset]

Hence proved.

Sum of two ideals

Let R be a ring and I and J be two ideal of R then sum of two ideals is defines as

I + J = { a + b; a $\in$ I, b $\in$ j }

Product of two ideals

Let R be a ring and I and J be two ideals of R, then product of two ideals is defined as

$$IJ = \left\{ \sum_{i=1}^{n} ai\ bi;\ ai \in I,\ bi \in J,\ n \in N \right\}$$

Theorem 4 : If I and J be any two ideals of a ring R then I + J is an ideal of R. Also prove that I + J = {I U J} is the smallest ideal of R containing I U J.

Proof : Since I and J be any two ideals of a ring R

So 0 $\in$ I and 0 $\in$ J

$\Rightarrow 0 = 0 + 0 \in I + J$

Therefore, I + J is a nom empty set.

Let x_1 $y \in I + J$ be any two elements of I + J such that

$x = a_1 + b_1$ and $y = a_2 + b_2$ where $a_1 a_2 \in I$ and $b_1, b_2 \in J$

Now $x - y = (a_1 + b_1) - (a_2 + b_2)$

$= (a_1 - a_2) + (b_1 - b_2)$

$\Rightarrow x - y \in I + J$ [Because $a_1, a_2 \in I$ and I is an ideal so $a_1 - a_2 \in I$, similarly $b_1, b_2 \in J$]

Now, let $r \in R$ be any element, then

$rx = r (a_1 + b_1)$

$= ra_1 + rb_1$ [$\because r \in R_1$ $a_1 \in I$ and I is an ideal, so ra, $\in I$ and $r \in R_1$ $b_1 \in J$, J is an ideal so $rb_1 \in J$]

Both the properties are satisfied

Hence I + J is an ideal of R.

Now, to prove I + J = {I U J} is the smallest ideal of R containing I U J.

Let $x \in I + J$ be an element

then $x = a + b$; $a \in I$ and $b \in J$

Also $a \in I$ and $b \in J$

so $a, b \in I \cup J$

$\Rightarrow a \in I, b \in J \Rightarrow a, b \in I \cup J$

then $a + b \in \{I \cup J\}$ is the smallest ideal of R containing IUJ

$\Rightarrow x \in \{IUJ\}$

Thus $x \in I + J$

$\Rightarrow x \in \{I + J\}$

So $I + J \subseteq \{I \cup J\}$.

Further, $\forall$ $a \in I$, and $0 \in J$ we can have

$a = a + 0 \in I + J$

$\Rightarrow I \subseteq I + J$

Similarly, $\forall$ $b \in J$ and $0 \in I$

$b = 0 + b \in I + J$

$J \subseteq I + J$

Since $I \subseteq I + J$ and $J \subseteq I + J$

$\Rightarrow I \cup J \subseteq I + J$

$\Rightarrow \{I \cup J\} \subseteq I + J$

Hence $1 + J = \{I \cup J\}$

Theorem 5 : If I and J be any two ideals of a ring R, then IJ is an ideal of R.

Moreover $IJ \subseteq I \cap J$.

Proof : Given I and J are ideals of R. So

$0 \in I$ and $0 \in J$

$\Rightarrow 0 = 0.0 \in IJ$

Hence IJ is non empty set.

Let $x, y \in IJ$ be any two elements, then

$x = \sum_{i=1}^{n} a_i\ b_i$ and $y = \sum_{i=1}^{n} c_i\ d_i$, $a_i, c_i \in I$ and $b_i, d_i \in J$

and m and n are positive integers, the

$x - y = \sum_{i=1}^{n} a_i\ b_i - \sum_{i=1}^{n} c_i\ d_i$

$= a_1b_1 + a_2b_2 + ... a_nb_n - (c_1 d_1 + d_2d_2 + ... -c_nd_m)$

$= \sum_{k=1}^{m+n} x_k y_k$

Where, $x_k = a_k$ and $y_k = b_k$ for k = 1, 2, ... n

and $x_{n+t} = -c_k$ and $y_{n+t} = d_t$ for t = 1, 2, 3, ...m

so $x - y = \sum_{k=1}^{m+n} x_k y_k$

$\in I J$

Now let r be any element of R, then

$rx = r \left(\sum_{i=1}^{n} a_i\ b_i \right)$

$= \sum_{i=1}^{n} (ra_i)\ b_i$

Since I is an ideal of R so $rai \in I$ and $b_i \in J$

So rx = $\sum_{i=1}^{n}(ra_i)\ b_i$

$\in$ IJ

Similarly x r = $\left(\sum_{i=1}^{n} a_i\ b_i\right) r$

= $\sum_{i=1}^{n} a_i\ (b_i r)$

Since J is an ideal of R so $b_i.r \in J$ and $a_i \in I$

So xr = $\sum_{i=1}^{n} a_i\ (b_i r)$

$\in$ IJ

Hence IJ is an ideal of R.

Now, to prove $IJ \subseteq I \cap J$

Let x 0 = $\sum_{i=1}^{n} a_i b_i$, be any element of IJ., where $a_i \in$ I and bi $\in$ J, n is a positive integer.

Since $b_i \in$ J and J is an ideal of R

$\Rightarrow b_1 \in$ R

Also I is ideal of R and $a_i \in$ I, $b_i \in$ R

So $a_i b_i \in$ I

Similarly Ji $\in$ I and I is an ideal of R

$\Rightarrow a_i \in$ R

Also J is an ideal of R, $b_i \in$ J, $a_i \in$ R

$\Rightarrow a_i b_i \in$ J

Since $a_i b_i \in$ I and $a_i\ b_i \in$ J

$\Rightarrow a_i b_i \in I \cap J$ for i = 1, 2, ...n.

$\Rightarrow$ x = $\sum_{i=1}^{n} a_i b_i \in I \cap J$

Hence x $\in$ I J

$\Rightarrow$ x $\in$ I $\cap$ J

Therefore I J $\subseteq$ I $\cap$ J

Hence the proof.

Theorem 6 :Modular Law : If A, B, C are ideal of a ring R such that $B \subseteq A$. Prove that

$A \cap (B+C) = B + (A \cap C) = (A \cap B) + (A \cap C)$

Solution : Let $x \in A \cap (B + C)$ be any element

Then $x \in A$ and $x \in B+C$

when $x \in B+C$

then $x = b + c$ for $b \in B$ and $c \in C$

Given $B \subseteq A$

$\Rightarrow b \in B$ the $b \in A$

Now, $x \in A$ and $b \in A$ and A is an ideal then

$\Rightarrow x - b \in A$

$\Rightarrow (b+c) - b = c$ $\quad \because \ x = b + c$

$\Rightarrow c \in A$

But initially $c \in c$

$\Rightarrow c \in a \cap c.$

Therefore $x = b + c \in B + (A \cap C)$

$\Rightarrow A \cap (B + C) \subseteq B + (A + C)$ (1)

Conversely

Let $y \in B + (A \cap C)$ be any element, then

$y = b + K$, where $b \in B$ and $k \in A \cap C \Rightarrow k \in A$ and $k \in C$

Now $b \in B$, and $k \in C$

$\Rightarrow b + k \in B + C$

$\Rightarrow y \in B + C$

Again, Since $b \in B$ and $B \subseteq A$

$\Rightarrow b \in A$ and also $k \in A$

$\Rightarrow b + k \in A$

$\Rightarrow y \in A$

Since $y \in B + c$ and $y \in A$ also

$\therefore \quad y \in A \cap (B + C)$

$\therefore \quad B + (A \cap C) \subseteq A \cap (B+C)$ (2)

From (1) and (2)

$A \cap (B+C) = B + (A \cap C)$. (3)

Also since $B \subseteq A \Rightarrow A \cap B = B$

using this in (3), we get

$A \cap (B+C) = B + (A \cap C) = (A \cap B) + (A \cap C)$

Hence proved.

Example 2 : Let Z is a ring of integer. 4 Z and 6Z are two if its ideal. Then find $4Z \cap 6Z$, $4Z + 6Z$ and $4Z.6Z$

Solution : Since Z = {..... -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, ...}

4Z = {..... -24, -20, -16, -12, -8, -4, 0, 4, 8, 12, 16, 20, 24, ...}

6Z = {..... -36, -30, -24, -18, -12, -6, 0, 6, 12, 18, 24, 30, 36, ...}

Since we know that if $x \in I \cap J$ then $x \in I$ and $x \in J$

So $4Z \cap 6Z$ contain only those elements which are in 4Z and in 6Z also.

Therefore $4Z \cap 6Z$ = { .....-24, -12, 0, 12, 24....}

= set of integer which are multiple of 12

= 12Z

Hence $4Z \cap 6Z = 12Z$.

(2) $4Z + 6Z$,

Since we know that if I and J are two ideals of R

then $I + J = \{a + b ; a \in I \text{ and } b \in J\}$

$\therefore$ $4Z + 6Z$ = { 0, $\pm$(4+6), $\pm$(8+12), $\pm$ (12+18), $\pm$ (16+24), $\pm$ (20+30), $\pm$ (24+36), ...}

= { 0, $\pm$10, $\pm$20, $\pm$ 30, $\pm$ 40, $\pm$ 50, $\pm$ 60, $\pm$ ....}

= set of integer which are multiple of 10

= 10Z

$\therefore$ $4Z + 6Z = 10Z$.

(3) If I and J are two ideals of R then IJ is also an ideal of R such that $IJ = \left\{ \sum_{i=1}^{n} a_i b_i \right.$,

$a_i \in I$, $b_i \in J$, So

4Z = { 0, $\pm$ 4, $\pm$ 8, $\pm$ 12, $\pm$ 16, $\pm$ 20, $\pm$ 24, $\pm$ 28,....}

6Z = { 0, $\pm$ 6, $\pm$ 12, $\pm$ 18, $\pm$ 24, $\pm$ 30, $\pm$ 36, $\pm$ 28,....}

$4Z.6Z = \{ 0, \pm 24, \pm 96, \pm 216, \pm 384, \pm 600, \pm 864, \pm ....\}$

= Set of integer which are multiple of 24.

$4Z.6Z = 24Z$.

We can generalised above result as.

Note : If $n, m \in Z$ and nZ and mZ are ideals of Z then $nZ \cap mZ = kZ$, where k is common multiple of n, m

$n = 1cm\ (n, m)$

$nZ + mZ = dZ$, where d is common division of m, n

$=gcd\ (m, n)$

Self Check Exercise - 3

Q. 1 Find $6Z \cap 6Z$, $6Z + 6Z$, $6Z.6Z$, where 6Z is an ideals of Z.

Q. 2 Find $8Z \cap 5Z$, $8Z + 5Z$, $8Z.5Z$, where 8Z and 5Z are ideals of Z.

Q. 3 Find $3Z \cap 5Z$, $3Z + 5Z$ and $3Z.5Z$, where 3Z and 5Z are ideals of Z.

19.6 Summary :

In this unit we studied about

1. In a non empty subset of a ring if $a, b \in I$ and $r \in R$ then $a - b \in I$ and $ra = ar \in I$ then I is known as ideal of ring R
2. An ideal of a ring is a subring but converse is not thru.
3. {0} and R are improper ideal of ring R, whereas any other ideal is known as proper ideal.
4. In a non empty subset S of a ring, for $x \in R$ if {xS = Sx = 0}, then this is known as annihilator of ring R.
5. Left and (right) annihilators of ring R are Left (or right) ideal of ring.
6. Intersection of two ideal is again an ideal.
7. Union of two ideals is need not be an ideal.
8. Union of two ideals will be an ideal iff either $I \subseteq J$ or $J \subseteq I$.
9. Sum and product of two ideals is an ideal.
10. Modular law hold in ideal i.e. if A, B, C are ideals of ring R and $B \subseteq A$ then

    $A \cap (B+C) = B + (A \cap C) = (A \cap B) + (A \cap C)$
11. If nZ and mZ are ideals of Z then

    $nZ + mZ = dz$, $d = gcd\ (m, n)$

$nZ \cap mZ = kz$, $k = \text{lcm}(m, n)$

19.7 Glossary :

- **Ideal :** An ideal is said to be ideal of Ring R if I is both left sided and right sided.
- **Improper Ideal :** {0} and R is ideal of R. These ideal's called improper ideal.
- **Left Annihilator :** Let S be the non-empty subset of Ring R then

  $ann_l(S) = \{x \in R; xS = 0\}$.

19.8 Answers to Self Check Exercises

Self Check exercise-1

Q. 1 Use definition of left and right ideal to prove this.

Q. 2 Given R is a commutative ring, So $r \in R$.

$xr = rx \forall x \in$ a R.

Q. 3 Consider the ring $M_2(Z) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, a, b, c ,d$\in$ Z

and let A = $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, a $\in$ Z

then AR = {Ar, r $\in$ R}

$= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$= \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$

Taking r = $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix} \in$ A R

Prove that $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$

Self Check Exercise - 2

Q. 1 Do same as example 2.

Self CheckExercise - 3

Q. 1 6Z, 6Z, 6Z

Q. 2 40Z, 13Z, 40 Z

Q. 3 15Z, 8Z, 15Z

19.9 References/Suggested Readings

1. Vijay K Khanna and S.K. Bhambri, A course in Abstract Algebra.
2. Joseph A. Gallian, Contemporary Abstract Algebra.
3. Frank Ayres Jr, Modern Algebra, Schaum's outline series.
4. A.R. Vasistha, Modern Algebra, Krishna Prakashan Media.

19.10 Terminal Questions

1. Let I = (a), J = (b) be two ideals of ring Z of integers, where a and b are positive integers. Determine

   I + J, I ∩J , IJ.

2. Prove that the set S of all matrices of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ with a, b $\in$ Z, forms a subring of ring $M_2(Z)$ Further prove that S is neither a left nor a right ideal of $M_2(Z)$

—

Unit - 20

Types of Ideal

Structure

20.1 Introduction

Dear students in this unit, we will study about the type of ideal, mainly about Principal ideal, Maximal ideal and Prime ideal. Also we will study the property and example related to these ideal.

20.2 Learning Objectives:

After studying this unit, students will be able to

1. define principal, maximal and prime ideal.
2. can prove property of types of ideals.
3. can solve questions related to types of ideals.

20.3 Principal Ideal

In group, we studied about the group generated by an element, similarly here we will study about ideal generated by a non empty subset and an the basis of this we will define principal ideal.

Ideal Generated by a Subset

Let R is a ring and I is an ideal of R. Let S be any subset of ring R. An ideal I of R is said to be generated by subset S if

(1) $S \subseteq I$

(2) for any other ideal J of R, $S \subseteq J \Rightarrow I \subseteq J$

In other words we can say that I is an ideal generated by a subset S of R if I is the smallest ideal among all the ideals of R which contain S. or I is the intersection of all ideals of R which contains S.

Mathematically, we writ an ideal I generated by S as

$I = \langle S \rangle = \{S\} = \cap \{J; J \text{ is ideals of R s.t. } J \supseteq S\}$

Using this definition we will define principal ideal.

Definition of Principal Ideal

An ideal of a ring which is generated by a single element of ring is called principal ideal of the ring. If I is principal ideal of the ring R generated by a. Then we write.

$I = \langle a \rangle$

Let us take following examples

Example 1 : Let Z be the ring show that nZ is a principal ideal.

Solution : Since Z = { ..... -4, -3, -2, -1, 0, 1, 2, 3, 4, ...} be the set of integers and we know. that Z form 0 ring under usual addition and multiplication.

The nZ = { ..... -4n, -3n, -2n, -n, 0, n, 2n, 3n, 4n, ...}

where $n \in Z$

$\therefore nZ = \langle n \rangle$ = generated by a single element of Z. Hence nZ is a principal ideal.

Example 2 : If R be a commutative ring with unit and $a \in R$ be any element then

$OR = Ra = [Or = ra ; r \in R\} = \langle a \rangle$ is a principal ideal.

Example 3 : For ring of integers Z = {0, $\pm$1, $\pm$2, $\pm$3, ...}

2Z = {0, $\pm$2, $\pm$4, $\pm$5, $\pm$8, ...} Since every element of 2Z is generated by a single element Z. Hence 2Z is principal ideal generated by 2 or <2>.

Now 3Z = {0, $\pm$3, $\pm$6, $\pm$9, ...}

Again, every element of 3Z is genered by a single element 3. Hence 3Z is principal ideal generated by 3 or <3>

Self Check Exercises-1

Q. 1 Prove that 5Z, 7Z are principal ideal of ring of integers Z.

20.4 Maximal Ideal

Definition

If R is a ring and S is a non zero ideal of R such that $S \neq R$ then S is called a maximal ideal of R, if there exists no proper ideal of R containing S.

Example 1 : Show that $2Z = \langle 2 \rangle$ is a maximal ideal of ring of integers Z.

Solution : Since $Z = Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$

and $2Z = \{0, \pm 2, \pm 4, \pm 5, \pm 8, ...\}$ is a non zero ideal of Z.

Since $2Z \neq Z$

Also there is no proper ideal of R which contains 2Z

Theorem 1 : $pZ = \langle p \rangle$ where p is a prime is a maximal ideal of ring of integer Z.

In the ring of integers Z, the ideal $\langle p \rangle$ is a maximal ideal iff p is prime number.

Proof : Let S be an ideal of ring of inters Z generated by a prime integer to prove $\langle p \rangle$ is a maximal ideal.

Since $S = \langle p \rangle = pZ$ given

Now Let T be an ideal of Z containing S and generated by some positive integer q then

Since $S \subseteq T$ and $p \in S$

$\Rightarrow p \in T$

So, there exists some $a \in z$ such that

$p = qa$

since p is a prime

$\Rightarrow$ either $q = I$ or $q = p$.

When $q = 1$, then $T = 1Z = Z$

When $q = p$, then $T = pZ = S$

Thus the ideal of Z generated by prime p is a maximal ideal.

Conversely :

Let S be a maximal ideal of Z generated by a positive integer p i.e. $S = pZ$.

To prove p is a prime.

Let, p is not a prime, then

$p = mn$ where $m \neq 1, n \neq 1$.

Let T be an ideal of Z generated by m. the we have

$S \subseteq T \subseteq Z$

But S is a maximal ideal

So either S = T or T = Z

Now if T = Z $\Rightarrow$ T is an ideal gerated by1

$\Rightarrow$ m = 1, which is acontracition.

Again if T = S

$\Rightarrow$pZ = mZ

m = pa for same a $\in$ Z.

$\Rightarrow$ mn = pan

p = pan

$\Rightarrow$ an =1 $\Rightarrow$ n =1 which is again a contraction.

Hence p must be a prime number.

Example 2 : Show that in a division ring R <0> is a maximal ideal.

Solution : Since <0>$\neq$ R as R is a ring, so i$\in$ R also 1 $\neq$ 0

Let J be any non zero ideal of R, then J xz non zero element x in J.

Also R is a division ring, so inverse of each element exists.

Therefore $x^{-1} \in$ R. Such that $xx^{-1} = 1$

Since J is ideal R so $xx^{-1} = 1 \in$ J

Hence J is an ideal of R which contain the unity element of R

$\therefore$ J = R

Hence <0> is a maximal ideal of R.

Example 3 : Let E = 2Z is the ring of even integer then show that <4> = 4Z is a maximal in E.

Solution : Since we known that

Z = {0, $\pm$1, $\pm$2, $\pm$3, $\pm$4, ...}

then 2Z = {0, $\pm$2, $\pm$4, $\pm$6, $\pm$8, $\pm$ 10, ...} is the ring of even integer.

4Z = {0, $\pm$4, $\pm$8, $\pm$12, $\pm$16, ...}

clearly 2 $\notin$ 4Z

Hence 2Z $\neq$ 4Z or <4> = E

Also now to prove there exists no other ideal of R containing <4>

Let J be any ideal of E such that <4> C J.

Let x $\in$ J such that x $\notin$<4> i.e. x is not a multiple of 4

Then $x = um + r$ where $r = 1$ or 2 or 3.

But if $r = 1$ or 3, then x will be an add integer but

$x \in J$ which is an ideal of E i.e. having even integer so only possibility is $r = 2$.

$\therefore x = um + 2$

$\Rightarrow 2 = x - 4m \in J$

so every integral multiple of 2 belongs to J

$\Rightarrow J = E$

So, there is no other ideal of R containing <4>

Hence <4> is a maximal ideal.

Example 4 : Find maximal ideal of Z_8

Solution : In order to find maximal ideal of Z_8 we first have to find all ideals of Z_8. We will use following theorem. Also ideal of Z_n, at the first place, are additive sub group of Z_n. Also, for each positive divisor d of an the set <n/d> is the unique subgroup of Z_n of order d, these are only subgroups of Z_n. Therefore, to find all ideals of Z_8 we just have to find all the divisor of 8.

Since $(Z_8, +1 X) = \{ 0, 1, 2, 3, 4, 5, 6, 7\}$

Since 1, 2, 4, 8 are only divisor of 8. Using x_8 we get

so $1/8 = <1> = \{ 0, 1, 2, 3, 4, 5, 6, 7\} = Z_8$

Now $2/8 = <2> = \{ 0, 2, 4, 6, 0, 2, 4, 6\}$

$= \{0, 2, 4, 6\}$

Now $4/8 = <4> = \{0, 4, 0, 4, 0, 4, 0, 4\}$

$= \{0, 4\}$

Now $8/8 = <8> = \{0, 0, 0, 0, 0, 0, 0, 0\}$

$= \{0\}$

Now, $<8> \subseteq <4> \subseteq <2> \subseteq <1> = Z_8$

Hence <2> is the only maximal ideal of Z_8.

Example 5 : Find maximal ideal of Z_{10}

Solution : First of find all ideal of Z_{10}.

Since $Z_{10} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Now to find the divisor of 10

Since, 1, 2, 5, 10 are only divisors of 10

So $1/10 = <1> Z_{10} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} = Z10$

$2/10 = <2> = \{0, 2, 4, 6, 8, 0, 2, 4, 6, 8\}$

$= \{0, 2, 4, 6, 8\}$

5/10 = <5> = {0, 5, 0, 5, 0, 5, 0, 5, 0, 5}

{0, 5}

and 10/10 = <10> = {0}

Since <10>$\subseteq$<5>$\subseteq$<1>

and <2>$\subseteq$<1>

Hence <2> and <5> are maximal ideal of Z_{10}.

Example 6: Find the maximal ideal of Z_{12}

Solution: Since Z_{12} = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}

the divisor of $Z_{12}$are, 1, 2, 3, 4, 6, 12

So, 1/12 = <1> = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11} = Z_{12}

2/12 = <2> = {0, 2, 4, 6, 8, 10, 0, 0, 4, 6, 8, 10}

= {0, 2, 4, 6, 8, 10}

3/12 = <3> = {0, 3, 6, 9, 0, 3, 6, 9, 0, 3, 6, 9}

= {0, 3, 6, 9}

4/12 = <4> = {0, 4, 8, 0, 4, 8, 0, 4, 8, 0, 4, 8}

= {0, 4, 8}

6/12 = <6> = {0, 6, 0, 6, 0, 6, 0, 6, 0, 6, 0, 6}

= {0, 6}

12/12 = <12> = {0}

Since <12>$\subseteq$<6>$\subseteq$<3>$\subseteq$<1> = Z12

<12>$\subseteq$<4>$\subseteq$<2>$\subseteq$<1> = Z12

Hence <2< and <3> are maximal ideal of Z12.

Self Check Exercise - 2

Q.1 Find the maximal ideal of Z_{36}

Q.2 Find the maximal ideal of Z_{52}

20.5 Prime Ideal

Definition:-

Let R be a commutative ring. An ideal P of R is called q prime ideal if for every a, b $\in$ R, a b $\in$ p then either a$\in$p or b$\in$p.

Example 1: Show that in an integral domain R, <0> is a prime ideal.

Solution: Let R be an integral domain.

Let $\forall$ a, b $\in$ R set a b $\in$<0> [definition of prime ideal]

$\Rightarrow$ ab = 0

Since R is an integral domain so

ab = 0 $\Rightarrow$ either a = 0 or b = 0

$\Rightarrow$ either a $\in$<0> or b $\in$<0>

Hence <0> is a prime ideal, in ab integral domain R.

Example 2: Show that in the ring of integral Z the ideal

<3> = 3Z = {3n ; n$\in$z} is a prime ideal.

Solution: Using definition of a prime ideal, if <3> is as prime ideal,

$\forall$ a, b $\in$ Z, a b $\in$<3>

$\Rightarrow$ ab = 3n, n $\in$ Z.

$\Rightarrow$ 3/ab

Since 3 is a prime number, so

$\Rightarrow$ either 3/9 or 3/b

$\Rightarrow$ either a = 3 m_1 or b = 3 m_2 for some m_1 $m_2\in$ Z.

$\Rightarrow$ either a $\in$<3> or b $\in$<3>

Hence $\forall$ a, b $\in$ Z, a b $\in$<3>$\Rightarrow$ either a $\in$<3> or b $\in$<3>

Hence <3> is a prime ideal of Z.

Example 3: Show that <4> = 4Z is not a prime ideal of 2Z.

Solution: Since 2Z = {0, $\pm$2, $\pm$4, $\pm$6, $\pm$8, ...}

4Z = {0, $\pm$4, $\pm$8, $\pm$12, $\pm$12, ...}

Since 4Z $\subset$ 2Z and 4Z $\neq$ 2Z, so 4Z is maximal ideal.

For prime ideal, $\forall$ a, b $\in$ 2Z, ab $\in$ 4Z either a $\in$ 4Z or b$\in$ 4Z

Since, 2, 2$\in$ 2Z, 2.2 $\in$ 4Z

$\Rightarrow$ but neither 2$\in$4Z nor 2$\in$4Z

Hence 4Z is not a prime ideal of 2Z.

Example 4: Let R = Z15, I = {0} is an ideal of Z15.

Check I = {0} is a prime ideal of Z15 or not.

Solution: Since (Z_{15}, +, .) is a ring

Z_{15} = {0, 1, 2, 3, ... 14}

As 3 $\in$ Z15, 5 $\in$ Z_{15}

Now $3_{15}.5 = 0 \in I$

But $3 \notin I$ and $5 \notin I$,

As I {0} contains only single element i.e. 0.

So I = {0} is not a prime ideal in Z_{15}.

Note:- No of prime ideal in Z_n - No of prime divisors of n.

Example 5: Find all prime ideal in Z_6.

Solution: Since Z6 = {0, 1, 2, 3, 4, 5}

Since $(Z_6, +_i)$ is a ring. Also no of prime ideal in Z_6.

= no of prime divisors of 6

= 2 [as 2, 3 are only prime divisor of 6]

Since divisors of 6 are 1, 2, 3, 6

So $I_1 = 1/6 = <1> = \{0, 1, 2, 3, 4, 5\} = Z_6$.

$I_2 = 2/6 = <2> = \{0, 2, 4, 0, 2, 4\}$

$= \{0, 2, 4\}$

$I_3 = 3/6 = <3> = \{0, 3, 0, 3, 0, 3\} = \{0, 3\}$

$I_4 = 6/6 = <6> = \{0\}$

Out of there four ideals two will be prime ideals of Z_6.

Now to find these prime ideal

Since $I_1 = Z_6$ so by definition $I_1 = <1>$ is not a prime ideal of Z_6.

$I_2 = <2> = \{0, 2, 4\}$

The remaining elements of Z_6 are, 1 3, 5 and their composition table under multiplication is

X_6	1	3	5
1	1	3	5
3	3	3	3
5	5	3	1

Since non of element of composition table belongs to I_2

Hence I_2 is for prime ideal.

$I_3 = <3> = \{0, 3\}$

The elements of Z_6 other than 0, 3 are 1, 2, 4, 5 and their composition table under multiplication is

X_6	1	2	4	5
1	1	2	4	5
2	2	4	2	4
4	4	2	4	2
5	5	4	2	1

Since non of element of composition table belongs to I_3

Hence I_3 is a prime ideal.

Now, $I_4 = <6> = \{0\}$

using definition, Let $2, 3 \in Z_6$

$2 \times_6 3 = 0 \in I_4$ or $3 \in I_4$

So I_4 is not a prime ideal.

Example 6: How many prime ideal in Z_{15}.?

Solution: No of prime ideal in Z_{15} = No of prime divisor of 15

$\therefore$ No of prime ideal in $Z_{15} = 2$

Since 3 and 5 are only prime divisor of 15. Hence <3> and <5> are prime ideal of Z_{15}

Since $Z_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$

Now $I_1 = <3>$

$= \{0, 3, 6, 9, 12, 0, 3, 6, 9, 12, 0, 3, 6, 9, 12\}$

$= \{0, 3, 6, 9, 12\}$

$I_2 = <5>$

$= \{0, 5, 10\}$

Example 7: Find prime ideal of Z_{12}

Solution: Since prime divisor of 1_2 are 2, and 3, so there are two prime ideal of Z_{12} and they are <2> and <3>

Let $I_1 = <2> = \{0, 4, 6, 8, 10\}$

$I_2 = <3> = \{0, 3, 6, 9\}$

Example 8: Is intersection of two prime ideal is a prime ideal? Prove by example.

Solution: Let $Z = 0, +1, \pm 2, \pm 3, ...\}$

$2Z = \{0, \pm 2, \pm 4, \pm 6, \pm .....\}$

$3Z = \{0, \pm 3, \pm 6, \pm 9, ...\}$

$2Z \cap 3Z = \{0, \pm 6, \pm 12, \pm 18, ...\}$

$2Z \cap 3Z = 6Z = <6>$

Also 6Z is not a prime ideal as, $2, 3 \in Z$

$2 \times 3 = 6 \in 6Z$

but $2 \notin 6Z$ and $3 \notin 6Z$

Hence by definition of prime ideal, 6Z is not a prime ideal in Z.

As 6Z is not a prime ideal. So intersection of two prime ideal may not be a prime ideal.

Now, Let us prove following theorems for prime ideals.

Theorem 1: In the ring of integers Z_1 the ideal $<m> = mZ = \{mn, n \in Z\}$ is a prime ideal iff m is prime number.

Proof:- Let <m> be a prime ideal, to show that m is prime

Let $a, b \in Z$ such that $ab \in <m>$

Since <m> is a prime ideal

$\Rightarrow$ either $a \in <m>$ or $b << m>$

$\Rightarrow$ either $a = m$ or $b = mn$

$\Rightarrow$ either m/a or m/b

$\therefore$ when na/ab, we have m/a or m/b

so m is a prime ideal.

Conversely:

Let m be a prime number to show <m> is a prime ideal.

Let $a, b \in Z$ such that $ab \in <m>$

$\Rightarrow$ $ab = mn$ for some $n \in Z$

$\Rightarrow$ m/ab, but m is a prime number

$\Rightarrow$ either m/a or m/b

$\Rightarrow$ either $a = mn_1$ or $b = mn_2$ where $n_1, n_2 \in Z$.

$\Rightarrow$ either $a \in <m>$ or $b \in <m>$

Hence <m> is a prime ideal.

Theorem 2: An ideal P of a commutative ring is prime if and only if R/P is an integral domain.

Proof: Let P be a prime ideal of R. To show R/P is on integral domain.

Let $\bar{a} = a+p$ and $\bar{b} = b+p$ where $a, b \in R$, be two elements of R/P such that

$\bar{a}\,\bar{b} = \bar{0}$

$\Rightarrow \quad \overline{ab} = \bar{0}$

$\Rightarrow$ ab + P = P

$\Rightarrow$ ab $\in$ P

Since P is a prime ideal

So either a $\in$ P or b $\in$ P

So either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$

Hence for $\bar{a}\,\bar{b} = \bar{0}$ either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$

So R/P has no zero divisor

Also R is a commutative ring with unity.

$\Rightarrow$ R/P is a commutative ring with unity T.

Hence R/P is an integral domain

Conversely:

Let R/P is an integral domain, o prove P is a prime ideal.

Let a, b $\in$ R such that a b $\in$ P

$\Rightarrow$ ab + P = P

$\Rightarrow \quad \overline{ab} = \bar{0}$

$\Rightarrow \quad \bar{a}\,\bar{b} = 0$

As R/P is an integral domain

$\Rightarrow$ either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$

$\Rightarrow$ either a $\in$ P or b $\in$ P

$\therefore$ P is a prime ideal.

Hence Proved.

Theorems 3: Let R be a commutative ring with unity. Then every maximal ideal of R is a prime ideal.

Proof: Let R be commutative ring with unity.

Let M be a maximal ideal of R

Then R/M is a field

$\Rightarrow$ R/M is an integral domain

Hence M is a prime ideal

Converse of this theorem is not true.

Example 9 : Give an example to show that maximal ideal need not be prime ideal for ring without unit.

Solution : Since 2Z is set of even integer is a ring, without unit.

and 4Z is a maximal ideal of 2Z. Put 4Z is not a prime ideal.

To prove this let 2, $6 \in 2Z$, so

$2x6 = 12 = 6$

$4.3 \in 4Z$

but $2 \notin 4Z$ and $6 \notin 4Z$

Hence by definition of prime ideal 4Z is not a prime ideal still it is a maximal ideal of 2Z.

Self Check Exercise-3

Q. 1 How many prime ideal Z = pq where p and q are distinct prime.

Q. 2 How many prime ideal in Z.

Q. 3 Show that 6Z is not prime ideal in Z.

20.6 Summary :

In this unit we studied

1. An ideal of a ring which is generated by a single element of ring is called principal ideal of that ring.
2. pZ = <p> where p is a prime, is a maximal ideal of ring.
3. A non zero ideal of R is known as maximal ideal if $S \neq R$ and if there exists no proper ideal of R containing S.
4. An ideal P of R is known as prime ideal if for every a, $b \in R$, $ab \in P$ then either $a \in P$ or $b \in P$.
5. Intersection of two prime ideal may or may not be prime ideal.
6. No of prime ideal in a ring Z_n is equal to number of prime divisor of n.
7. In ring of integer Z the ideal <m> is a prime ideal iff m is prime.
8. An ideal P of commutative ring is prime iff R/P is an integral domain.
9. Let R is a commutative ring with unity then every maximal ideal of R is a prime ideal.
10. A prime ideal may not be a maximal ideal.

20.7 Glossary :

- **Principal Ideal :** An ideal of Ring, which is generated by a single element of Ring is called principle Ideal of Ring.

- **Maximal Ideal :** If S is non-zero ideal of Ring R such that $S \neq R$ then S is called maximal ideal, if J no proper ideal of R containing S.
- **Prime Ideal :** A ring R with commutative. An ideal P of R is called a prime ideal if for every a, $b \in R$, $ab \in P_1$ then either $A \in P$ or $b \in P$.

20.8 Answers to Self Check Exercises

Self Check exercise-1

Q. 1 Same as example 3.

Self Check Exercise - 2

Q. 1 <2> and <3> are maximal ideal of Z_{36}.

Q. 2 <2> ,<13> are maximal ideal of Z_{52}.

Self CheckExercise - 3

Q. 1 Only two prime ideal<p> and <q>

Q. 2 Infinite prime ideal in Z that are <p> where p is a prime number

Q. 3 Since $2, 3 \in Z$

$2x3 = 6 \in 6Z$

but $2 \notin 6Z$ and $3 \notin 6Z$

So 6Z is not a prime ideal in 2

20.9 References/Suggested Readings

1. Vijay K Khanna and S.K. Bhambri, A course in Abstract Algebra.
2. Joseph A. Gallian, Contemporary Abstract Algebra.
3. Frank Ayres Jr, Modern Algebra, Schaum's outline series.
4. A.R. Vasistha, Modern Algebra, Krishna Prakashan Media.

20.10 Terminal Questions

1. Give an example of a ring in which a prime ideal is not a maximal ideal.
2. Prove that in a Boolean ring with identity every prime ideal is a maximal ideal.
3. Find all maximal and prime ideal of Z_{21}.