Basics of Group Theory

DR.E.GEETHA

ASSISTANT PROFESSOR OF MATHEMATICS

SCSVMV (DEEMED TO BE UNIVERSITY)

Outline

- **Aim**
- **Learning Outcomes**
- **Introduction**
- **History**
- **Semigroup**
- **Monoid**
- **Group**
- **Abelian Group**
- **Cancellation Laws**

AIM

- **Explicate the concept of binary operation and algebraic structures**
- **Explain about the semigroup, monoid and group by an example**
- **Explain about the abelian group**

Learning Outcomes

Students can be able to identify

- **Existence of binary operation**
- **About the algebraic structure**
- **About the existence of identity element and inverse element**

Introduction

- In mathematics and abstract algebra, group theory studies the algebraic structures known as groups.

- The concept of a group is central to abstract algebra, other well known algebraic structures, such as rings, fields and vector spaces, can all be seen as groups endowed with additional operations and axioms.

- Groups recur throughout mathematics, and the method of group theory have influenced many parts of algebra.

History

- The term group was coined by Galois around 1830 to described sets of functions on finite sets that could be grouped together to form a closed set.

- The modern definition of group given by both Heinrich Weber and Walter Von Dyck in 1882, it did not universal acceptance until the twentieth century.

Prerequisites

- **Set theory**
- **Relations**
- **Matrix Algebra**

Binary Operation

Let G be a set. A binary operation on G is a function that assigns each order pair of elements of G an element of G.

$$f : G \times G \rightarrow G$$

It is customary to denote binary operations by symbols such as +, -, x, /, etc.,

Remark:

o is a binary operation on G if and only if a o b $\in G$

Algebraic Structure:

A non empty set together with one or more than one binary operation is called algebraic structure.

Examples:

1. **(R, +, .) is an algebraic structure.**
2. **(N, +), (Z, +), (Q, +) are algebraic structures.**

Examples with one binary operation:

Let N be the set of all natural number.

i.e N={0,1,2,3....}

(i) Let us consider the operation addition (+) on N

Clearly for any two element a, b $\in$ N, a+b $\in$ N.

Therefore the addition '+' is a binary operation on the set N

{N,+} is called ***algebraic structure with one binary operation*** (+).

(ii) Let us consider the operation multiplication(x) on N

Clearly for any two element a, b $\in$ N, then a * b $\in$ N.

Therefore the '*' is a binary operation on the set N

{N,*} is viewed as ***algebraic structure with one binary operation***

Example with two binary operations:

(i) Let S={1, -1, 0} , then the operation addition (+) is not a binary operation on S.

Since 1+1=2 is $\notin$ S.

(ii) Let S={1,-1,0}, then the operation multiplication (x) is a binary operation on S

Since

X	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

Note:-

(i) From the above {N,+,x} can be viewed as algebraic structure with two binary operations (+,x).

(ii) A binary operation so called because it combines two elements.

Definition: Closure Property

Let {S,*, ⊕ } be an algebraic system, then for any two element a , b $\in$ S, a*b $\in$ S.

It is called closure property.

Example:-

Let {N, +, x} be an algebraic structure, where N is a natural number.

If a, b $\in$ N, then a + b $\in$ N

If a, b $\in$ N, then a x b $\in$ N

Definition: Associative Property

Let $\{S, *, \oplus\}$ be an algebraic system, then for any three element a , b and c $\in$ S, $(a*b)*c = a*(b*c)$. It is called associative property.

Example:-

Let {N, +, x} be an algebraic structure, where N is a natural number.

If a, b and c $\in$ N, then $(a + b) + c = a + (b + c)$

If a, b and c $\in$ N, then $(a \times b) \times c = a \times (b \times c)$

Definition: Commutative Property

Let $\{S, *, \oplus\}$ be an algebraic system,

For any two element a, b $\in$ S, a*b=b*a

xample:-

Let {Z, +, x} be an algebraic structure, where Z is set of all non negative integer.

) For any element a , b $\in$ Z, a+b=b+a, The set Z is commutative with respect to the binary

peration '+'.

) For any element a, b $\in$ Z, a x b = b x a, therefore the set Z is commutative with respect to

e binary operation 'x'.

Definition: Existence of Identity Element

Let {S,*, ⊕ } be an algebraic system, then for any element 'a' ∈ S, there exist an distinguished element 'e' in S such that a*e=e*a=a, then the element 'e' is called identity element of S with respect to the operation *

Example:-

Let {Z, +, x} be an algebraic structure, where Z is set of all non negative integer.

(i) For any element 'a' ∈ Z, a+0=0+a=a, therefore 0 is an identity element of Z with respect to the binary operation '+'. and '0' is also called additive identity of Z.

(ii) For any element 'a' ∈ Z, a x 1 = 1 x a=a, therefore 'a' is an identity element of Z with respect to the binary operation 'x'. and '1' is also called multiplicative identity of Z.

Definition: Existence of Inverse Element

Let {S,*,⊕} be an algebraic system, then for any element 'a' ∈ S, there exist an element a^{-1} in S such that $a*a^{-1} = a^{-1}*a = e$, where e is an identity element with respect to the operation (*). then the element a^{-1} is called inverse element of ' a' ∈ S under the operation(*).

Example:-

Let {R, +, x} be an algebraic structure, where R is set of all real numbers.

(i) For any element 'a' ∈ R, a+(-a)=(-a)+a=0, where '0' is an identity element of R with respect to the binary operation '+'. and '-a' is the additive inverse element of 'a' ∈ R.

(ii) For any element 'a' in R, $a \times a^{-1} = a^{-1} \times a = 1$, where '1' is an identity element of R with respect to the binary operation 'x'. and 'a^{-1}' is called multiplicative inverse 'a' ∈ R. but the element '0' ∈ R has no multiplicative inverse in R.

Definition: Distributive Property

Let {S,*,⊕} be an algebraic system. For any a, b and c ∈ S, a*(b⊕c)=(a*b)⊕(a*c), It is

alled distributive law. In this case the operation ' * ' is distributive over the operation ' ⊕'.

xample:-

Let {R, +, x} be an algebraic structure, where R is set of all real numbers.

The multiplication operation ' x ' is distributive over the addition operation ' + '

i.e For any a, b and c ∈ R , a*(b+c)=a*b+a*c.

Cancellation Laws

Let $\{S, *, \oplus\}$ be an algebraic system. For any a, b, c $\in$ S and a $\neq$ 0, then

(i) a*b=a*c=>b=c (Left Cancellation Law) and

(ii) b*a=c*a=>b=c (Right Cancellation Law)

Example:-

Let {R, +, x} be an algebraic structure, where R is set of all real numbers.

(i) Since for any a, b, c $\in$ R, then

a+b=c+b=>a=c (Right Cancellation Law)

b+a=b+c=>a=c (Left Cancellation Law)

i.e Cancellation property hold for a, b, c in R under addition operation.

Definition: Idempotent element

An element 'a' ∈ S is called an idempotent element with respect to the operation *, if a*a=a.

Example:-

Let {R, +, x} be an algebraic structure, where R is set of all real numbers.

(i) Since 0 + 0=0, where '0' ∈ R. Therefore '0' is an idempotent element under the addition operation (+).

(ii) Since 1 x 1=1, where '1' ∈ R. Therefore '1' is an idempotent element under the multiplication operation(*).

(iii) Since 0 x 0=0, where '0' ∈ R. Therefore '0' is an idempotent element under the addition operation(*).

Definition: Semigroup

If S is a nonempty set and * be a binary operation on S, then the algebraic system {S,*} is called semi group, if the operation * is associative. i.e for any a, b, c $\in$ S, (a*b)*c=a*(b*c).

Definition: Commutative Semigroup

A semi group {S,*} is said to be semi group, if the binary operation * satisfies the commutative property. i.e for all a, b $\in$ S, a*b=b*a.

Definition: Monoid

If a semi group {M,*} has an identity element with respect to the operation *, then {M,*} is called a monoid.

i.e for any element ' a ' $\in$ M, a * e = e * a = a, where 'e' is an identity element in M with respect to the binary operation *.

Example:

Let N be the set of positive integers, then the algebraic system {N,+} is a ***semi group***.

since the binary operation addition (+) on N satisfies associative property.

i.e for all a, b, c $\in$ N, (a+b)+c=a+(b+c)

Additionally for a, b $\in$ N a+b=b+a, therefore {N,+} is a ***commutative semi group***

Also for all a $\in$ N, 0 + a = a + 0 = a, where '0' is additive identity element , but it is not in N.

Hence {N,+} is ***not a monoid.***

Example:

Let I be the set of all integers, then the algebraic system {I,-} is ***not a semi group.***

Since the binary operation subtraction (-) on I does not satisfies the associative property.

For example consider the integers 12, -15, 2 in I

(12-(-15))-2=(12+15)-2=27-2=25,   But   12-((-15)-2)=12-(-17)=12+17=29, Both are not same.

Since {I,-} is not a semi group,

Hence {I,-} is ***not a Monoid***.

Example:

Let P(S) be the power set of s, then the algebraic system {P(S), U} is a ***semi group***

Since the binary operation union (U) on P(S) satisfies the associative property.

i.e for all S_1, S_2, $S_3 \in$ P(S), (S_1 U S_2) U S_3 = S_1 U (S_2 U S_3)

Additionally for all S_i, $S_j \in$ P(S), S_i U S_j = S_j U S_i, {P(S),U} is called a ***commutative semi group***.

Also for all $S_i \in$ P(S), S_i U {} ={} U S_i =S_i, where the element {} is an identity element in P(S).

Hence {P(S),U} is ***a monoid***.

Definition: Group

If G is a non empty set and * is a binary operation of G, then the algebraic system {G,*} is called a group if the following conditions are satisfied.

(i) For all a, b, c $\in$ G, (a*b)*c=a*(b*c) (Associative Property)

(ii) There exists an element e in G such that, a*e=e*a=a, for any a $\in$ G (Existence of Identity)

(iii) For every a $\in$ G, there exist a^{-1} in G such that $a*a^{-1}=a^{-1}*a=e$ (Existence of inverse)

Definition: Order of a Group

When G has finite number of element, the number of elements in G is called the order of G.

It is denoted by O(G) or |G|.

Definition: Commutative Group (or) Abelian Group

Let {G,*} be a group with binary operation *, G is said to be ***commutative group*** if for every a, b $\in$ G, a+b=b+a.

It is also called ***Abelian group.***

Example:

Let Z be the set of natural number ,

since (a+b)+c=a+(b+c) , for all a, b, c $\in$ Z.

The element '0' $\in$ Z is an additive identity

The element '-a' $\in$ Z is an additive inverse for all a $\in$ Z.

Therefore the algebraic system {Z,+} is ***a group.***

The order of the group is **O(Z)=** ∞

Since a+b=b+a, for all 'a' $\in$ Z. Therefore {Z,+} is a **commutative group.**

Example:

Let G={1,-1,i,-i}, then {G,x} is a algebraic structure

x	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 above Cayley's table , it is clear that the operation x is binary and satisfies the associative property.

The multiplicative identity is e=1

Since $1 \times e = e \times 1 = 1$, $-1 \times e = e \times (-1) = -1$, $i \times e = e \times i = i$, and $-i \times e = e \times (-i) = -i$

Every element has its inverse in G

since the element 1 is the inverse of 1, $1 \times 1 = 1 \times 1 = e$

the element -1 is the inverse of -1, $-1 \times -1 = -1 \times -1 = e$

the element i is the inverse of -i, -i x i = i x -i = e

the element -i is the inverse of i, i x -i = -i x i= e

Therefore the algebraic structure {G,x} is a **group**

Also the operation x is commutative in G, therefore {G,x} is a **abelian group.**

The order of the group O(G)=4.

Definition: Order of an element

If the element 'a' in G, where G is a group with identity 'e', then the least positive integer 'm' for which $a^m=e$ is called the order of the element 'a'.

It is denoted by O(a).

Examples:

(i) Let G={1, -1, i, -i} be a group, where e=1 is the multiplicative **identity** element.

Since $(1)^1=e$, $O(1)=1$,

$(-1)^2=e$, $O(-1)=2$

$(i)^4=e$, $O(i)=4$

$(-i)^4=e$, $O(-i)=4$

(ii) Let G={1, w, w^2} be a group , where $w^3=1$ and e=1 is the multiplicative **identity** element .

Since $(1)^1=1$, $O(1)=1$

$(w)^3=1$, $O(w)=3$

$(w^2)^3=1$, $O(w^2)=3$

i) Let Z be a set of natural numbers, i.e z={0,1,2,3...} be a group and e=0 is additive identity ement.

nce $(0)^1=0$, $O(0)=1$

$O(a)=\infty$ for all a in Z other than zero.

ote:-

If no such integer 'm' exists, then 'a' is of ***infinity order***

Properties of a group

The identity element of a group {G,*} is unique

roof:

We have to prove the identity element of a group {G,*} is unique,

Suppose if there are two identity element e_1, e_2 are in G, we have to prove $e_1=e_2$

Since e_1 is an identity element in G, therefore $a*e_1=e_1*a=a$ for all a in G

Clearly e_2 is an element of G, therefore $e_2*e_1=e_1*e_2=e_2$,-----(1)

Similarly e_2 is an identity element in G, therefore $a*e_2=e_2*a=a$ for all a in G

Clearly e_1 is an element of G, therefore $e_1*e_2=e_2*e_1=e_1$,-----(2)

From equations, (1) and (2), we have

(1)=> $e_1*e_2=e_2$

=> $e_1=e_2$ (Using equation (2) $e_1*e_2=e_1$)

Hence the proof.

Properties of a group

The inverse of each element of {G,*} is unique

roof:

We have to prove the inverse of each element of a group {G,*} is unique,

Suppose if there are two inverse element b and c for an element 'a' in G,

we have to prove b=c

Since 'b' is an inverse element of ' a' in G, therefore a*b=b*a=e ---(1), where 'e' is an identity element in G with respect to the operation *

Since 'c' is an inverse element of 'a' in G, therefore a*c=c*a=e---(2), where 'e' is an identity element in G with respect to the operation *

L.H.S=b=e*b (since a*e=e*a=a, e is identity element in G)

L.H.S=(c*a)*b (using the equation (2))

L.H.S=c*(a*b) (Using associative property of G)

L.H.S=c*e (using the equation (1))

L.H.S=c (since a*e=e*a=a, e is identity element in G)

Therefore L.H.S=R.H.S

Hence the proof.

Properties of a group

The cancellation laws are true in group.

roof:

Proof of left cancellation

Let a*b=a*c, we have to prove b=c

=> $a^{-1}*(a*b)=a^{-1}*(a*c)$ (multiply the element a^{-1} on left hands side and on both sides.

=> $(a^{-1}*a)*b=(a^{-1}*a)*c$ (using associative property of G)

=> e*b=e*c (for any a in G, $a^{-1}*a=a^{-1}*a=e$, where a^{-1} is inverse of 'a' and 'e' is identity element in G with respect to the operation *.)

=> b=c (since a*e=e*a=a, e is identity element in G)

Proof of right cancellation

Let b*a=c*a, we have to prove b=c

=> $(b*a)*a^{-1}=(c*a)*a^{-1}$ (multiply the element a^{-1} on right hands side and on both sides.

=> $b*(a*a^{-1})=c*(a*a^{-1})$ (using associative property of G)

=> b*e=c*e (for any a in G, $a^{-1}*a=a^{-1}*a=e$, where a^{-1} is inverse of 'a' and 'e' is identity element in G with respect to the operation *.)

=> b=c (since a*e=e*a=a, e is identity element in G)

Properties of a group

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

Proof:

We have to prove that $(a*b)^{-1}=b^{-1}*a^{-1}$, for all a , b in G

i.e we have to prove that $b^{-1}*a^{-1}$ is the inverse of $a*b$.

it is enough prove that $(a*b)*(b^{-1}*a^{-1})= (b^{-1}*a^{-1})*(a*b)=e$, where 'e' is the identity element

G with respect to the operation *.

Now $(a*b)*(b^{-1}*a^{-1})= a*(b*b^{-1})*a^{-1}$ (using associative property of G)

$(a*b)*(b^{-1}*a^{-1})= a*e*a^{-1}$ (for any b in G, $b^{-1}*b=b^{-1}*b=e$, where b^{-1} is inverse of

and 'e' is identity element in G with respect to the operation *.)

$(a*b)*(b^{-1}*a^{-1}) = a*a^{-1}$ (since a*e=e*a=a, where 'e' is identity element in G)

$(a*b)*(b^{-1}*a^{-1}) = e$ **---(1)** (for any a in G, $a^{-1}*a=a^{-1}*a=e$, where a^{-1} is inverse of 'a' and 'e' is

lentity element in G with respect to the operation *.)

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

$(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b$ (using associative property of G)

$(b^{-1}*a^{-1})*(a*b) = b^{-1}*e*b$ (for any a in G, $a^{-1}*a=a^{-1}*a=e$, where a^{-1} is inverse of 'a'

nd 'e' is identity element in G with respect to the operation *.)

$(b^{-1}*a^{-1})*(a*b) = b^{-1}*b$ (since b*e=e*b=b, where ' e ' is identity element in G)

$(b^{-1}*a^{-1})*(a*b)=e$---**(2)** (for any b in G, $b^{-1}*b=b^{-1}*b=e$, where b^{-1} is inverse of 'b' and 'e' is identity element in G with respect to the operation *.)

From equations (1) and (2), we have $(a*b)*(b^{-1}*a^{-1})=(b^{-1}*a^{-1})*(a*b)=e$

Thus $(b^{-1}*a^{-1})$ is the inverse of $(a*b)$

Hence we have proved $(a*b)^{-1}=b^{-1}*a^{-1}$

Multiple Choice Questions

1. A non empty set A is termed as an algebraic structure____________________
   a. With respect to binary operation *
   b. With respect to binary operation ?
   c. With respect to binary operation +
   d. With respect to binary operation -

Answer: a

2. An algebraic structure ____________________ is called a semigroup.
   a. (P, *)
   b. (Q, +, *)
   c. (P, +)
   d. (+, *)

Answer: a

3. Condition for monoid is _____________
    a. (a + e) = a
    b. (a * e) = (a + e)
    c. a = (a *(a + e))
    d. (a * e) = (e * a) = a

Answer: d

4. A monoid is called a group if _________________
    a. (a * a) = a = (a + c)
    b. (a * c) = (a + c)
    c. (a + c) = a
    d. (a * c) = (c * a) = e

Answer: d

5. A group (M, *) is said to be abelian if _______________
   a. (x + y) = (y + x)
   b. (x * y) = (y * x)
   c. (x + y) = x
   d. (y * x) = (x + y)

Answer: b

6. Matrix multiplication is a/an ______________ property
   a. Commutative
   b. Associative
   c. Additive
   d. Disjunctive

Answer: b

7. How many properties can be held by a group?

a. 2

b. 3

c. 4

d. 5

Answer: c

8. If a*b = a such that a * (b * c) = a * b = a and (a * b) * c = a * b = a then ____________

a. * is associative

b. * is commutative

c. * is closure

d. * is abelian

Answer: a

9. The set of rational numbers form an abelian group under ___________

a. Associative

b. Closure

c. Multiplication

d. Addition

Answer: c

10. ______ is the multiplicative identity of natural numbers

a. 0

b. -1

c. 1

d. 2

Answer: c

Assignment Questions

1. Let G = { 1, -1 }. Prove that G is a group under usual multiplication.
2. Show that M_2, the set of all 2 x 2 non – singular matrices over R is group under ususl matrix multiplication. Is it abelian?
3. Show that the set of all non- zero real numbers is an abelian group under the operation*defined by a * b = ab
4. Let S = Q x Q be the set of ordered pairs of rational numbers and given that (a, b) *(x, y) = (ax, ay+b).

   (i). Check (S, *) is a semigroup. Is it Commutative?

   (ii). Also find the identity and inverse element of S.
5. Show that the set G = {1, 2, 3, 4, 5} is not a monoid or semigroup or group under addition modulo 6.

Thank you