

1. 1

①

Algebraic structure:

G is a non-empty set and \star is a b-o on it, G together with the b-o is called an algebraic structure and is denoted by (G, \star) .

or

A non-empty set equipped with one or more b-o is called an algebraic structure.

Ex: $(\mathbb{N}, +)$, $(\mathbb{N}, +, \cdot)$, $(\mathbb{I}, +, \cdot, -, -)$ etc

is called an algebraic structure.

Ex: $(\mathbb{N}, +)$, $(\mathbb{N}, +, \cdot)$, $(\mathbb{I}, +, \cdot, -, -)$ etc

are algebraic structure.

Groupoid or quasi group:

An algebraic structure $(G, *)$ is said to be groupoid if it satisfied the closure property.

i.e $\forall a, b \in G \Rightarrow a * b \in G$.

Ex: $(\mathbb{N}, +)$, $(\mathbb{I}, +)$ etc are groupoid.



Ex: $(\mathbb{N}, +)$, (\mathbb{Z}^+, \cdot)

Semi group or Demi group:

If an algebraic structure $(G, *)$ satisfies the closure and associative properties then $(G, *)$ is called semi group.

Ex: $(I, ?)$, (I, \cdot) etc are semi-groups,
but $(I, -)$ is not a semi group because
it is closure but not associative.

$$\text{Q.E.D}$$

1, 2, 3

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

$$(1-2)-3 \neq 1-(2-3)$$

Monoid:

A semi-group (G, \ast) with an identity element w.r.t \ast is known as a monoid.

Ex: A semi group $(I, +)$ is a monoid and the identity is '0'.
 $a + 0 = a$ $2 + 0 = 2$
 $2 + 0 = 2$ $2 \times 1 = 2$

- A semi group (I, \cdot) is a monoid and the identity element is 1.

- A semi group $(N, +)$ is not monoid and the identity element is '0'.

Ex: A semi group $(\mathbb{Z}, +)$ is a monoid because it has an identity element '0'.
 $a + 0 = a$
 $2 + 0 = 2$
 $2 \times 1 = 2$

- A semi group (\mathbb{Z}, \cdot) is a monoid and the identity element is 1.
- A semi group $(\mathbb{N}, +)$ is not a monoid and the identity element is 0 because $a + b = \frac{a+b-ab}{2ab} \neq a$.

Group: A monoid $(G, *)$ with the inverse element

0 \notin N^{*}

$\xrightarrow{*}$

2ab

✓ Group: A monoid $(G, *)$ with the inverse element w.r.t $*$ is known as a group.

or
The algebraic structure $(G, *)$ is said to be a group. if the b-o $*$ on G satisfies the following properties:

① closure prop: $\forall a, b \in G, \Rightarrow a * b \in G$

properties:

① closure prop: $\forall a, b \in G, \Rightarrow a * b \in G$

② Associative prop: $\forall a, b, c \in G$
 $\Rightarrow (a * b) * c = a * (b * c)$

③ Existence of Identity:
 $\exists e \in G$ s.t $a * e = e * a = a \quad \forall a \in G$.

'e' is called the identity element in G.

$$(1 - 2) - 3$$

$$\begin{array}{r} e_1 - (e_2 - e_3) \\ e_1 + e_2 \\ \hline e_3 \end{array}$$

$71 - \frac{3}{4} = ?$

Existence of Inverse:
for each $a \in G$, $\exists b \in G$, s.t

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

'b' is inverse of a in G.

$$(G, *) \quad (3)$$

$2 \in G$

$$2 * \frac{1}{2} = 1$$

$$3 * \frac{1}{3} = 1$$

I;

$$2 + 3 = 3 + 2$$

$$a * b = b * a$$

$$2 - 3 \neq 3 - 2$$

Abelian or Commutative group:

Scanned with CamScanner

Abelian or commutative group:

I;
 $2+3 = 3+2$
 $a*b = b*a$
 $2-3 \neq 3-2$

A group $(G, *)$ which satisfies the commutative property is known as the abelian group.

Otherwise: It is known as non-abelian group.

Finite and Infinite group:

If the number of elements in the group G is finite then the group $(G, *)$ is called a finite group. An infinite group

finite and infinite group:

If the number of elements in the group $(G, *)$ is finite then the group $(G, *)$ is called a finite group, otherwise it is called an infinite group.

order of a group:

The number of elements in a finite group is called the order of the group. It is denoted by $o(G)$ or

infinite.

the order of the group

$|G|$

the order of infinite group is infinite.

Note 1: the order of identity

- ② $G = \{e\}$ (i.e. the set consisting of identity element e alone).
- is a group w.r.t given composition which is known as the smallest group.

problems:

① The algebraic structure $(\mathbb{Z}, +)$ where

$\mathbb{Z} = \{-\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

is an abelian group.

Note: (i) The set \mathbb{Z}^+ under $+$ is not a group.
There is no identity element for $+$ in \mathbb{Z}^+ .

(ii) The set of all non-negative integers (includes 0) under $+$ is not a group because there is no inverse of $a \in \mathbb{Z}$.

- New Doc 2020-05-22 08.21.53 (12).pdf - Adobe Reader
- File Edit View Document Tools Window Help
- 4 / 23 162% Find
- o) under $+$ is not a group.
 - is no inverse of $a \in \mathbb{Z}$.
 - ② The set I_E of all even integers is an abelian group w.r.t $+$.
 - Note: The set I_O of all odd integers is not a group w.r.t $+$ because the closure property is not satisfied.
 - The sets \mathbb{Q} , \mathbb{R} and \mathbb{C} of all rational, real and complex numbers are abelian groups.

as left the meeting

Note: The "group w.r.t $+^n$ " because the condition is not satisfied.

③ The sets \mathbb{Q} , \mathbb{R} and \mathbb{C} of all rational, real and complex numbers are abelian groups under " $+^n$ ".

④ $G = \text{The set of } m \times n \text{ matrices}$ is an abelian group w.r.t $b = 0 \in +^n$.
..... is an abelian group

- ③ The sets \mathbb{Q} , \mathbb{R} and \mathbb{C} of all numbers are abelian groups.
- and complex numbers under $+$
- ④ $G = \text{the set of } m \times n \text{ matrices}$ is an abelian group w.r.t $b - o \in \mathbb{F}^n$.
- ⑤ $H = \text{the set of vectors}$ is an abelian group w.r.t $b - o \in \mathbb{F}^n$.

6) The set $G = \{ -m, -2m, -m, 0, m, 2m, 3m, \dots \}$ (5)
of multiples of integers by fixed integer m is an
abelian group w.r.t $+$.

7) The set N under \times^n is not a group because
there is no inverse of $a \in N$.
. real and

- New Doc 2020-05-22 08.21.53 (12).pdf - Adobe Reader
- File Edit View Document Tools Window Help
- 5 / 23 162% Find
- Q
- The set \mathbb{N} under \times^n is not a group because there is no inverse of $a \in \mathbb{N}$.
- ⑧ The sets \mathbb{Q} , \mathbb{R} , \mathbb{C} of all rational, real and complex numbers are not groups w.r.t \times^n because the inverse of 0 is not defined.
- ⑨ The sets \mathbb{Q}^+ and \mathbb{R}^+ of all positive rational and real numbers are abelian groups under \times^n .
- ⑩ The sets \mathbb{Q}^* , \mathbb{R}^* and \mathbb{C}^* of all non-zero rational, real and complex numbers are abelian groups.

and real numbers

- (10) The sets \mathbb{Q}^* , \mathbb{R}^* and \mathbb{C}^* of all non-zero rational, real and complex numbers are abelian groups w.r.t \times^n .

- (11) In the set of all rational numbers x s.t $0 < x \leq 1$, a group w.r.t \times .
Sol: Let $G = \{x \mid x \text{ is a rational number and } 0 < x \leq 1\}$ because if $a \in G$ then it is not a group under \times^n because if $a \in G$ and $0 < a < 1$ then inverse of a^n is not

(ii) Is the set of all rational numbers x s.t.
 $0 < x \leq 1$, a group w.r.t \times .

Sol: Let $G = \{x \mid x \text{ is a rational number and } 0 < x \leq 1\}$
then it is not a group under \times because if $a \in G$
and $0 < a < 1$ then inverse of aa' is not
possible in G .

Ex: Let $a = \frac{1}{5} \in G$ then the inverse of $\frac{1}{5}$ is $5 \notin G$.

(12) The set of all the rational numbers forms an abelian group under the composition by $a+b = \frac{ab}{2}$.

Elementary properties of groups:

If G is a group with $b=0$

then the left and right cancellation laws hold in G

Elementary properties of groups:

If G is a group with $b = 0$

then the left and right cancellation laws hold in G

i.e. $\forall a, b, c \in G$ (i) $ab = ac$.

$$\Rightarrow b = c \quad (L \cdot C \cdot L)$$

and (ii) $ba = ca$.

$$\Rightarrow b = c \quad (R \cdot C \cdot L)$$

Proof: Given that

$$a + b = 0$$

Proof:

Given that

G is a group w.r.t \circ .

for each $a \in G$ $a^{-1} \in G$ s.t

$$a^{-1}a = a \cdot a^{-1} = e \text{ (where 'e' is identity)}$$

Now suppose $a \cdot b = a \cdot c$

Multiplying both sides a^{-1} on left.

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

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

(Associative Property)

Multiplying both sides a' on left.

$$a'(ab) = a'(ac)$$

$$\Rightarrow (a'a)b = (a'a)c$$

(Associative Property)

$$\Rightarrow ab = ac \quad (\text{Identity}).$$

Similarly

$$b \cdot a = c \cdot a \\ \Rightarrow b = c$$

Scanned with CamScanner

∴ $a = b$ i.e., a commutes with b or 't'hen the (\exists)

Note: If G is a group with b- \circ 't' then the (7)
left and right cancellation laws hold in G .

$$\text{i.e } a + b = a + c \Rightarrow b = c \text{ (L.C.L)}$$

$$\text{and } b + a = c + a \Rightarrow b = c \text{ (R.C.L)}$$

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

\Rightarrow If G is a group with b- \circ and a & b are elements
of G , then the linear eqns $ax = b$ and $ya = b$ have
unique soln. x and y in G .

i.e. $a+b = a+c \Rightarrow b=c$ (L.C.L)

and $b+a = c+a \Rightarrow b=c$ (R.C.L)

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

\Rightarrow If G is a group with b -op and a & b are elements of G , then the linear eqns $ax=b$ and $ya=b$ have unique soln x and y in G .

Proof :- Given that G is a group w.r.t b -op "•"

$\therefore a \in G \exists a^{-1} \in G$ s.t $a a^{-1} = a^{-1} a = e$.

where ' e ' is identity.

Proof: Given that G is a group.
 for each $a \in G \exists a^{-1} \in G$ s.t. $a a^{-1} = a^{-1} a = e$.
 where ' e ' is identity.

Now, we have —

$$ax = b$$

multiplying both sides a^{-1} on left

we get $a^{-1}(ax) = a^{-1}b$ (by associative prop.)

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

$$\Leftrightarrow ex = a^{-1}b$$

(by inverse)

$$\Rightarrow x = a^{-1}b$$

(by identity)

we get

$$\Leftrightarrow (a^{-1}a)x = a^{-1}b \cdot \text{("by")}$$

$$\Leftrightarrow ex = a^{-1}b \quad (\text{by inverse})$$

$$\Rightarrow x = a^{-1}b \cdot$$

(by identity)

$$\Rightarrow x = a^{-1}b \cdot$$

Now $a \in G$, $b \in G$, $\Rightarrow a^{-1} \in G$, $b \in G$.

$\Rightarrow a^{-1}b \in G$. in the left hand

Now substituting $a^{-1}b$ for x

side of the eqⁿ $ax = b$.

$$we have: a(a^{-1}b) = (a a^{-1})b = e b = b$$

$\therefore x = a^{-1}b$ is the solⁿ in G of the $ax = b$.

To show that the solⁿ is unique.

Now, if possible suppose that
 $x = x_1$ and $x = x_2$ are two solⁿ of the eqⁿ.

$$ax = b \text{ then } ax_1 = b, ax_2 = b$$

$$\therefore ax_1 = ax_2 \Rightarrow x_1 = x_2 \text{ (by l.c.l.)}$$

∴ The solⁿ is unique.

Similarly we prove that $ya = b$ has unique solⁿ.

+ and

Note: If G is a group with the $b = 0 +$ and a, b are two elements of G then the linear equations $a+x=b$ and $y+a=b$ have unique sol'n x and y in G .

Note [1]: cancellation laws hold in a group i.e.

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

$$(i) ab = ac \Rightarrow b = c \quad (\text{LCL})$$

$$(ii) ba = ca \Rightarrow b = c \quad (\text{RCL})$$

$$(ii) \quad ba = ca \Rightarrow b = c \quad (\text{Ans})$$

[2] In a semi group. the cancellation laws may or may not hold.

Ex: let 'S' be. the set of all 2×2 matrices with their elements as integers and ' $x^n = b - 0$ ' on 'S' then 'S' is a semi group but not satisfy the cancellations law because if

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

their elements.

then 'S' is a semi group but not satisfy the cancellation law because if

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

Scanned with CamScanner

then $A, B, C \in S$ and $AB = AC$ but $B \neq C$ ①

\therefore left cancellation law is not true in the semi group.

3

$(\mathbb{N}, +)$ is a semi group.

for $a, b, c \in \mathbb{N}$ $a+b = a+c$

and $b+a = c+a$.

$$\Rightarrow b=c$$

But $(\mathbb{N}, +)$ is not a group.

\therefore If a semi group even if cancellation laws hold
the semi group is not a group.

If a finite semi group (G, \cdot) satisfy the



the semi group is not a group.

4

A finite semi group (G, \cdot) satisfy the cancellation law is a group.

(or)

A finite set G with a binary operation \cdot is a group if \cdot is associative and cancellation

4

cancellation

law is a group

(or)

A finite set G with a binary operation \cdot is a group if \cdot is associative and cancellation laws hold in G .

uniqueness of identity in a group is unique.

The identity element in a given group. If possible.

Proof: Let (G, \cdot) be the given group. Suppose that e_1 & e_2 are two identity elements in G .

Since e_1 is an identity in G then

$$e_1 e_2 = e_2 = e_2 e_1. \quad \text{--- } \textcircled{1}$$

Since e_2 is identity in G then $e_1 e_2 = e_1 = e_2 e_1. \quad \text{--- } \textcircled{2}$

From $\textcircled{1}$ and $\textcircled{2}$, we have —

Suppose

Since e_1 is an identity in G then

$$e_1 e_2 = e_2 = e_2 e_1 \quad \text{--- } \textcircled{1}$$

Since e_2 is identity in G then $e_1 e_2 = e_1 = e_2 e_1 \quad \text{--- } \textcircled{2}$

From $\textcircled{1}$ and $\textcircled{2}$, we have —

$$e_1 = e_1 e_2 = e_2$$

$$\Rightarrow \boxed{e_1 = e_2}$$

Uniqueness of Inverse

Uniqueness of Inverse:
Inverse of each element of a group is unique.

Proof: Let (G, \cdot) be the given group.
Now suppose that $a \in G$ has two inverses a' and a'' .
Since a' is an inverse of a in G .
 $\therefore aa' = a'a = e \quad \text{--- (1)}$

Since a'' is an inverse of a in G .
 $\therefore aa'' = a''a = e \quad \text{--- (2)}$

Now suppose that — 44
 since a' is an inverse of a in G .

$$\therefore aa' = a'a = e \quad \text{--- } \textcircled{1}$$

since a'' is an inverse of a in G .

$$\therefore aa'' = a''a = e \quad \text{--- } \textcircled{2}$$

from $\textcircled{1}$ and $\textcircled{2}$, we have —

$$aa' = e = aa'' \quad \therefore aa' = aa'' \\ \therefore a' = a'' \quad (\text{By L.C.L})$$

Note:

The identity element is its own inverse II

$$\text{Since } ee = e \Rightarrow e^{-1} = e.$$

\Rightarrow If the inverse of a is a^{-1} then the inverse of

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

Proof: Let (G, \cdot) be the given group.

$\exists a \in G$ such that

Note :-

Since $ee = e \Rightarrow e^{-1} = e$.

\Rightarrow If the inverse of a is \bar{a} then inverse of
 \bar{a} is a i.e. $(\bar{a})^{-1} = a$.

Proof :- Let (G, \cdot) be the given group.

for each $a \in G$, $\exists \bar{a} \in G$ such that
 $a\bar{a} = \bar{a}a = e$.

Now $a\bar{a}^{-1} = e$
Multiplying both sides with $(\bar{a}')^{-1}$ on the right -

$$(a\bar{a}^{-1})(\bar{a}')^{-1} = e(\bar{a}')^{-1}$$

$$\Rightarrow a(\bar{a}'(\bar{a}')^{-1}) = (\bar{a}')^{-1} \quad [\text{by associative and } e \text{ is identity}]$$

$$\Rightarrow a(e) = (\bar{a}')^{-1} \quad [\because (\bar{a}')^{-1} \text{ is inverse of } \bar{a}']$$

$$\Rightarrow a = (\bar{a}')^{-1} \quad [\because e \text{ is identity}]$$

$$\Rightarrow a = (a^{-1})^{-1} \quad [\because e \text{ is identity}]$$

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

Note: If $(G, +)$ is a group and inverse of a is
 $-a$ then, inverse of $-a$ is a

$$\therefore -(-a) = a$$

Let (G, \cdot) be a group.

Prove that $(ab)^{-1} = b^{-1}a^{-1}$ for $a, b \in G$.

Proof: Given that (G, \cdot) is a group.

for each $a \in G$, $\exists a^{-1} \in G$ such that

$$aa^{-1} = a^{-1}a = e \text{ and}$$

for $b \in G$, $\exists b^{-1} \in G \Rightarrow ab \in G$

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

$$aa^{-1} = a^{-1}a = e \text{ and}$$

for $b \in G$, $\exists b^{-1} \in G \Rightarrow ab \in G$

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

Now we have $\xrightarrow{\hspace{1cm}}$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} \quad (\text{by Associativity})$$

$$= ae a^{-1} \quad \text{by inverse}$$

$$= aa^{-1} \quad \text{by identity}$$

$$= e \quad \text{by inverse}$$

$$\therefore (ab)(b^{-1}a^{-1})$$

Now, we have —

$$(b^{-1}a^{-1})(ab) = e \quad \text{--- } \textcircled{2}$$

from $\textcircled{1}$ and $\textcircled{2}$, we have —

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

\therefore The inverse of ab is $b^{-1}a^{-1}$.

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

Note:

① Let $(G, +)$ be a group then
 $-(a + b) = (-b) + (-a)$

(P3)

② Generalization —

$$(a_1, a_2, a_3, \dots, a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_2^{-1} a_1^{-1}$$

Def' of a group based upon left Axioms or Right Axioms:

The algebraic structure (G, \circ) is said to be group following

Defⁿ of a group based upon left Axioms and Right Axioms:

The algebraic structure (G, \circ) is said to be group if the binary operation \circ satisfies the following properties:

(i) Closure property:

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

(i) Closure $P \vdash \neg O$

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

(ii) Associative property:

$$(ab)c = a(bc) \quad \forall a, b, c \in G$$

(iii) Existence of left identity:

$\exists e \in G$ such that $ea = a \quad \forall a \in G$,

\therefore the element 'e' is called left identity

in 'G'

(iv) Existence of left inverse:

$\exists e \in G$ such that $ea = a \forall a \in G$,

\therefore the element 'e' is called left identity
in G .

(iv) Existence of left inverse:

for each $a \in G$, $\exists a' \in G$ such that

$$(aa') = e$$

\therefore the element a' is called the left inverse of a
in G .

Theorem:

... is also the right identity.



Theorem:

the left identity is also the right identity
if 'e' is the left identity then $a \cdot e = a + a \cdot e$

Proof: Let (G, \cdot) be the given group

and let e be the left identity $\cancel{e \cdot e = a}$

To prove that 'e' is also the right identity -

let $a \in G$ and e be the left identity then
'a' has the left inverse in G .



if 'e' is the left identity then $a \cdot e = a$

Proof: Let (G, \circ) be the given group.

and let e be the left identity $e \cdot a = a$

To prove that 'e' is also the right identity -

let $a \in G$ and e be the left identity then
 'a' has the left inverse in G .

$$\therefore a^{-1} \cdot a = e$$

1) (i) Associative

Let $a \in G$ and e be the identity element.
 a has the left inverse in G .

$$\therefore a^{-1}a = e.$$

Now we have $a^{-1}(ae) = (a^{-1}a) \cdot e$ (by Associative
 = $e \cdot e$ (by inverse)
 = e (by identity)
 i.e. e is left identity
 $= a^{-1}a$ ($\because a^{-1}a = e$)

i.e. e is left identity
 $= a^{-1}a$ ($\because a^{-1}a = e$)

$$\begin{aligned}\therefore a^{-1}(ae) &= a^{-1}a \\ \Rightarrow ae &= a \quad (\text{by LCL in 6})\end{aligned}$$

\therefore If e is the left identity then e is also right identity.

Theorem : The left inverse is also right inverse, i.e., if \tilde{a}^{-1} is the left inverse of a then also $a\tilde{a}^{-1} = e$.

15

Proof: Let (G, \cdot) be the given group.
 Let $a \in G$ and e be the left identity in G .
 Let $a \in G$ and e be the left inverse of a then $a^{-1}a = e$.
 To prove that $aa^{-1} = e$.
 Now, we have —

Let a be in S

To prove that $aa^{-1} = e$

Now, we have

$$\begin{aligned}a^{-1}(aa^{-1}) &= (a^{-1}a) a^{-1} \quad (\text{by Associative}) \\&= ea^{-1} \quad (\text{by inverse}) \\&= a^{-1} \quad (\because e \text{ is the left identity}) \\&= a^{-1}e \quad (\because e \text{ is also right identity})\end{aligned}$$

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

$$\Rightarrow aa^{-1} = e \quad (\text{by L(C)})$$

$$\therefore aa^{-1} = e$$

$a^T a = e$

$\therefore \text{If } a^T a = e \text{ then } a a^T = e.$

Note: we cannot assume that the existence of left identity and the existence of left right inverse or we cannot assume the existence of right identity and the existence of left inverse.



16 / 23

162%

Find

Problems:

- ① Show that the set

$$G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$
 is a group w.r.t. $+$.

- ② P.T. the set of all $m \times n$ matrices having their elements as integers is an infinite abelian group w.r.t $+$ of matrices.

- ③ show that the set of all $m \times n$ non-singular matrices having their elements as irrational numbers

③

Show that the set of all $m \times n$ non-singular matrices having their elements as rational (real or complex) numbers is an infinite non-abelian group w.r.t matrix multiplication.

Solⁿ: Let M be the set of all $m \times n$ non-singular matrices with their elements as rational numbers.

(i) closure Property:

If $|A| \neq 0$ then

singular matrices with their eigenvalues

(i) closure Property:

Let $A, B \in M$; $|A| \neq 0, |B| \neq 0$ then

$AB \in M$ ($\because |AB| = |A||B|$)

Here $|AB| \neq 0$
because $|A| \neq 0, |B| \neq 0$

(ii) Associative property:

matrices multiplication is associative.

Here $|AB| \neq 0$
because $|A| \neq 0, |B| \neq 0$

(ii) Associative property:
matrices multiplication is associative.

Scanned with CamScanner

1). Existence of left Identity:

i). Existence of left Identity :

17

$\forall A \in M, \exists B = I_{n \times n} \in M, |B| = 1 \neq 0$

$|A| \neq 0$

such that $IA = A$

$\therefore B = I_{n \times n}$ is the left identity in M .

ii) Existence of left Inverse!

$\therefore B = I_{n \times n}$ is the left identity in M .

(iv) Existence of left Inverse:

for each $A_{n \times n} \in M$; $|A| \neq 0$ $\exists A^{-1} = \frac{\text{adj } A}{|A|}$

$(\because |A| \neq 0)$

such that

$$A^{-1} A = I_{n \times n} \quad (\text{left Identity})$$

$\therefore A^{-1}$ is the left inverse of A in M with their elements as rational.

∴ A^{-1} is the left inverse of A in M with their elements as rational.

(v) Commutative Property:

$\forall A, B \in M; |A| \neq 0, |B| \neq 0 \Rightarrow AB \neq BA$

∴ (M, \cdot) is not an abelian group.

Note:
M is the set of all $n \times n$ non-singular mats
with their elements as integers is not a group
 X because there is no inverse of all m
in the given set.

Ex: $A = \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}; |A| = -4 \neq 0$

$$\therefore A^{-1} = \frac{\text{adj } A}{|A|} = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ \frac{3}{4} & -\frac{1}{4} \end{bmatrix}$$

$$\therefore A^{-1} = \frac{\text{adj } A}{|A|} = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ \frac{3}{4} & -\frac{1}{4} \end{bmatrix}$$

Now, we have —

$$A^{-1}A = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ \frac{3}{4} & -\frac{1}{4} \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_{2 \times 2}$$

But $A^{-1} \notin M$ because the elements of this matrix
are not integers -

Bored

S.T the set of matrices.

(19)

$$A_\alpha = \begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix} \text{ where } \alpha \text{ is a real}$$

number forms a group under matrix multiplication.

.) is b-o.

Sol: Let $G = \{A_\alpha | \alpha \in \mathbb{R}\}$ and \cdot is

$$(i) \text{ Let } A_\alpha, A_\beta \in G \Rightarrow A_\alpha A_\beta = A_{\alpha+\beta} \in G$$

Closure prop. where $\alpha, \beta \in \mathbb{R}$.

where $\alpha + \beta \in \mathbb{R}$

87

(1) Let $A_\alpha, A_\beta \in U$,closure prop. where $\alpha, \beta \in \mathbb{R}$.where $\alpha + \beta \in \mathbb{R}$

Since

$$\begin{aligned}
 A_\alpha A_\beta &= \begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix} \begin{bmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{bmatrix} \\
 &= \begin{bmatrix} \cos(\alpha + \beta) & -\sin(\alpha + \beta) \\ \sin(\alpha + \beta) & \cos(\alpha + \beta) \end{bmatrix}
 \end{aligned}$$

$$= A_{\alpha+\beta}$$

prop. is satisfied

(ii) Associative prop.
Matrix multiplication is associative

(iii) Existence of left Identity.

Since $0 \in \mathbb{R}$

$$\therefore A_0 = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G.$$

(iii) Existence of left Identity.

Since $0 \in \mathbb{R}$

$$\therefore A_0 = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G.$$

Scanned with CamScanner

Let $A_\alpha \in G$, $\alpha \in \mathbb{R}$ $\exists A_0 \in G$; $0 \in \mathbb{R}$,

such that $A_0 A_\alpha = A_0 + \alpha = A_\alpha$.

(iv) Existence of left inverse:

Since $\alpha \in \mathbb{R} \Rightarrow -\alpha \in \mathbb{R}$,

$\therefore A\alpha \in G \Rightarrow A_{-\alpha} \in G$

Now $A_{(-\alpha)} A_\alpha = A_{-\alpha+\alpha} = A_0$ (left Identity).

$\therefore A(-\alpha)$ is the left inverse of $A\alpha$.

\therefore Each element of G possesses left inverse.

$\therefore G$ is a group under X^n .

$\therefore G$ is a group

Note: The sets of all $n \times n$ matrices with the elements as rational, real, complex numbers are not groups w.r.t matrix multiplication because the $n \times n$ matrix with entries '0' has no inverse.

\Rightarrow S.T $G_2 = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a \text{ is any non-zero real number} \right\}$

is a commutative group w.r.t x^n .

$$\{1, a^{\frac{1}{n}}, a^{\frac{2}{n}}, \dots, a^{\frac{n-1}{n}}\}$$

are no 0 the $n \times n$ matrix
because
no inverse

\Rightarrow S.T $G_2 = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} / a \text{ is any non-zero real number} \right\}$
is a commutative group w.r.t x^n .

\Rightarrow S.T the set $G_3 = \left\{ x / x = 2^a 3^b \text{ and } a, b \in \mathbb{Z} \right\}$
is a group w.r.t x^n .

problems

Do the following sets form groups w.r.t the
 $b \circ a$ * on them as follows:

- (i) The set I of all integers with operation defined by $a * b = a + b + 1$.
- (ii) The set Q of all irrational numbers other than 1 defined by
 (i.e. $Q - \{1\}$) with operation $*_1 = a + b - ab$

(i) The set I of all integers $\omega^m - 1$
defined by $a * b = a + b + 1$.

(ii) The set Q of all rational numbers other than 1
(i.e. $Q - \{1\}$) with operation defined by
 $a * b = a + b - ab$

(iii) The set I of all integers with the operation
defined by $a * b = a + bt^2$

$a * b = ab$ $\forall a, b \in Q - \{1\}$.

defined by

solution:

(ii) since

$$a * b = a + b - ab \quad \forall a, b \in Q - \{1\}.$$

→ A

① closure prop.

Let $a, b \in Q - \{1\}$

$$a * b = a + b - ab$$

$\in Q - \{1\}$ (by ①)

closure prop. w.r.t *

$\therefore Q - \{1\}$ satisfies

② associative property:

$\forall a, b, c \in Q - \{1\}$.

11. A

⑥ Associative property:

$\forall a, b, c \in Q - \{1\}$.

$$(a+b-ab) * c \quad (\text{by } ⑤)$$

$$\Rightarrow (a * b) * c = (a+b-ab) * c$$

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

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

Scanned with CamScanner

$$= a + b + c - (ab + bc + ca) + abc.$$

Similarly \longrightarrow

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

$$= a + b + c - (ab + bc + ca) + abc \quad (2)$$

Similarly —

$$a * (b * c) = a + b + c - (ab + bc + ca) + abc.$$

$$\therefore (a * b) * c = a * (b * c),$$

$\therefore Q - \{1\}$ satisfies Associative prop. w.r.t *

③ Existence of left identity prop'

③ Existence of left identity prop'

Let $a \in Q - \{l\}$, $e \in Q - \{l\}$ -

then $e * a = a$

Now $e * a = a$

$$\Rightarrow e + a - ea = a$$

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

$$\Rightarrow e = 0 \quad (\because a \neq l)$$

$e \in Q - \{l\}$

$$\therefore e * a = a * a$$

$$\Rightarrow e = o \quad (\because a \neq l) \\ e \in Q - \{l\}$$

$$\therefore e * a = o * a \\ = o + a - o(a) \\ = a.$$

$\therefore \forall a \in Q - \{l\}, \exists o \in Q - \{l\}$ such that

$$o * a = a$$

$\therefore o$ is the left identity in $Q - \{l\}$.

Instance of left Inverse:

(23)

let $a \in \mathbb{Q} - \{1\}$, $b \in \mathbb{Q} - \{1\}$.

then $b * a = e$

Now

$$b * a = e \quad (\text{by } \textcircled{A})$$

$$\Rightarrow b + a - ba = 0$$

$$\Rightarrow b(1-a) = -a \quad (\because a \neq 1)$$

$$\Rightarrow b = \frac{-a}{1-a}$$

$$= \frac{a}{a-1}$$

$\in \mathbb{Q} - \{1\}$.

$$\Rightarrow b(1-a) = -a \quad (\because a \neq 1)$$

$$\Rightarrow b = \frac{-a}{1-a}$$

$$= \frac{a}{a-1} \quad \in Q - \{1\},$$

$$\therefore b * a = \frac{a}{a-1} * a$$

$$= \frac{a}{a-1} + a - \frac{a}{a-1} a$$

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

For each $a \in Q - \{1\}$, $\exists b = \frac{a}{a-1} \in Q - \{1\}$

for each a^*

such that $\frac{a}{a-1} \neq a = 0$

$$\therefore b = \frac{a}{a-1}$$

is left inverse of
in $\{0 - \{1\}\}$ w.r.t $*$.

$\therefore (\{0 - \{1\}\}, *)$ is a group.