Set-I (i)

Some sets of Numbers: GROUPS

→ $N = \{1, 2, 3, \cdots\}$

→ $W = \{0, 1, 2, 3, \cdots\}$

→ $I = \{\cdots -3, -2, -1, 0, 1, 2, \cdots\}$

→ The set of all rational numbers

$$Q = \left\{\frac{p}{q} \,/\, p, q \in I;\ q \neq 0\right\}$$

→ Q' = the numbers which cannot be expressed in the form of $\frac{p}{q}$, $(q \neq 0)$ are known as irrational numbers.

Ex: $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, e, $2+\sqrt{3}$ etc.

Note: (i) A rational number can be expressed either as a terminating decimal or a non-terminating recurring decimal.

(ii) An irrational number can be expressed as non-terminating non recurring decimal.

→ $R = Q \cup Q'$.

i.e, the set of all real numbers R which contains the set of rational and irrational numbers.

→ $C = \{a+ib \,/\, a, b \in R,\ i = \sqrt{-1}\}$

→ I^+, Q^+, R^+ are the sets of +ve members of I, Q, R respectively.

→ Z^*, Q^*, R^* and C^* are the sets of non-zero members of I, Q, R and C respectively.

→ I_o and I_e are the sets of odd and even numbers of I

Some definitions

→ Let A and B be two sets. If $a \in A$ and $b \in B$ then (a, b) is called an ordered pair. 'a' is called the first component (co-ordinate) and 'b' is called the second component of the ordered pair (a, b).

→ Let A and B be two sets then $\{(a, b) \,/\, a \in A, b \in B\}$ is called the cartesian product of A and B and is denoted by $A \times B$.

i.e, $A \times B = \{(a, b) \,/\, a \in A, b \in B\}$.

Ex: If $A = \{1, 2, 3\}$ and $B = \{3, 4\}$ then $A \times B = \{(1,3), (1,4), (2,3), (2,4), (3,3), (3,4)\}$.

Note: (1) If A and B are finite sets, $n(A) = m$ and $n(B) = k$ then $n(A \times B) = n(B \times A) = mk$.

(2) $A \times B \neq B \times A$ unless $A = B$

If one of A and B is empty then $A \times B$ is also empty.
i.e, $A \times \phi = \phi$, $\phi \times B = \phi$.

→ If A and B are non-empty sets, then any subset of $A \times B$ is called a relation from A to B.

→ Let A be a non-empty set then subset of $A \times A$ is called a binary relation on A.

Ex: If $A = \{1, 2, 3\}$, $B = \{4, 5\}$;

$A \times B = \{(1,4), (1,5), (2,4), (2,5), (3,4), (3,5)\}$.

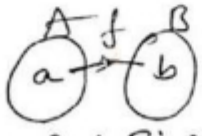
then $f = \{(1,4), (2,4)\} \subseteq A \times B$ is a relation from A to B.

and $A \times A = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}$.

then $g = \{(1,1), (2,1), (3,2), (3,3)\} \subseteq A \times A$ is a binary relation on A

function:

Let A and B be two non-empty sets and f be a relation from A to B. If for each elt $a \in A$ $\exists$ a unique $b \in B$ s.t. $(a,b) \in f$ then f is called function (or mapping) from A to B. or A into B. It is denoted by $f: A \to B$.



Binary operation (or) Binary Composition

→ Let S be a non-empty set,

$S \times S = \{(a,b) / a \in S, b \in S\}$.

If $f: S \times S \to S$ (i.e, for each ordered pair (a,b) of elts of S $\exists$ a uniquely defined an elt of S) then f is said to binary operation on S.

→ The image of the ordered pair (a,b) under the function f is denoted by $f((a,b))$ or $a f b$.

Ex:- Let $\mathbb{R}$ be the set of all real numbers.

$+^n$, $\times^n$, and $-^n$ of any two real numbers is again a real number

i.e, $\forall a,b \in \mathbb{R} \Rightarrow a+b \in \mathbb{R}$, $a \times b \in \mathbb{R}$ and $a-b \in \mathbb{R}$.

Now we define

$+: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $\times: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ and $-: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

are three mappings

$\therefore +((a,b))$ or $a+b \in \mathbb{R}$.

$\times((a,b))$ or $a \times b \in \mathbb{R}$

$-((a,b))$ or $a-b \in \mathbb{R}$.

→ An operation which combines two elements of a set to give another elt of the same set is called binary operation.

Generally the b-o is denoted by '$\circ$' or '$*$'

i.e, $\forall a,b \in S$ and $*$ is an operation if $a * b \in S$ then $*$ is called b-o on S.

Examples 1) $S = N, W, I, Q, R, C$.

$\forall a,b \in S \Rightarrow a+b \in S$ and $a.b \in S$.

IMS
MATHEMATICS
CELL NO 9999197625
By K. VENKANNA

$\therefore +^n$ and $\times^n$ are b-o operations on S.

Here '$-$' is b-o on I, Q, R & C.

i.e, $a, b \in I, Q, R, C \Rightarrow a-b \in I, Q, R, C$.

but '$-$' is not b-o on N and W.

i.e, $a, b \in N, W \Rightarrow a-b \notin N, W$

→ $a, b \in S \Rightarrow a \div b \notin S$.

$\therefore \div$ is not a b-o on S.

but $a, b \in Q, R, C$

$\Rightarrow a \div b \in Q, R, C$ if $b \neq 0$

$\therefore \div$ is a b-o on Q, R, C.

(2) $S = Q^*, R^*, C^*$ (Non zero sets)

$a, b \in S \Rightarrow a \div b \in S$

$\therefore \div$ is a b-o on S.

(3) Addition and subtraction are not b-o's on the set of odd integers.

Types of binary operations

* Closure operations:- A binary operation $*$ on a set 'S' is said to be closure if $a*b \in S \ \forall a, b \in S$.

Ex: (1) $S = N, W, I, Q, R, C$.

$\forall a, b \in S \Rightarrow a+b \in S$ & $a \cdot b \in S$.

$\therefore$ S is closed w.r.t b-o. $+^n$ & $\times^n$

→ $a, b \in I, Q, R, C \Rightarrow a-b \in I, Q, R, C$

$\therefore I, Q, R, C$ are closed under b-o '$-$',

but $a, b \in N, W \Rightarrow a-b \notin N, W$.

$\therefore N, W$ are not closed under b-o '$-$'

(2) $S = Q, R, C$

$a, b \in S \Rightarrow a \div b \in S$ if $b \neq 0$.

$\therefore$ S is closed w.r.t b-o $\div$

(3) $S = Q^*, R^*, C^*$

$a, b \in S \Rightarrow a \div b \in S$

$\therefore$ S is closed w.r.t b-o $\div$

Commutative operations:

A binary operation $*$ on a set 'S' is Commutative if $a*b = b*a \ \forall a, b \in S$.

Ex: $S = N, W, I, Q, R, C$

$\forall a, b \in S \Rightarrow a+b = b+a$

$a \cdot b = b \cdot a$.

$\therefore$ S is commutative w.r.t b-o $+$ & $\cdot$.

but $a, b \in S \Rightarrow a-b \neq b-a$

$\therefore$ S is not Commutative w.r.t b-o '$-$'

→ $S = Q^*, R^*, C^*$

$a, b \in S \Rightarrow a \div b \neq b \div a$.

$\therefore$ S is not commutative under $\div$

→ S = The set of all m×n matrices.

$\forall A, B \in S \Rightarrow A+B = B+A$.

$\therefore$ S is commutative under b-o $+^n$.

but $A, B \in S \Rightarrow A-B \neq B-A$.

→ S = The set of all n×n matrices

$\forall A, B \in S \Rightarrow A+B = B+A$

$A-B \neq B-A$

$A \cdot B \neq B \cdot A$.

→ S = The set of all matrices with real entries.

The usual matrix addition, Subtraction, x^n are not b-os on S.

[$\because A, B \in S \Rightarrow A+B, A-B$ & $A \cdot B$ are not defined]

→ S = The set of all vectors.

$\bar{a}, \bar{b} \in S \Rightarrow \bar{a}+\bar{b} = \bar{b}+\bar{a}$

$\bar{a}-\bar{b} \neq \bar{b}-\bar{a}$

$\bar{a} \times \bar{b} \neq \bar{b} \times \bar{a}$.

but the usual '.' is not b-o on S. [$\because \bar{a} \cdot \bar{b}$ is scalar. $\notin S$]

Associative operations:-

A binary operation * on S is said to be associative if

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

Ex:- $S = N, W, I, Q, R, C$.

$\forall a, b, c \in S \Rightarrow (a+b)+c = a+(b+c)$

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

but $(a-b)-c \neq a-(b-c)$.

→ S = The set of all n×n matrices

$\forall A, B, C \in S \Rightarrow (A+B)+C = A+(B+C)$

but $(A-B)-C \neq A-(B-C)$

→ S = The set of all n×n matrices

$\forall A, B, C \in S \Rightarrow (A+B)+C = A+(B+C)$

$(A \cdot B) \cdot C = A \cdot (B \cdot C)$

but $(A-B)-C \neq A-(B-C)$.

→ S = The set of all vectors.

$\forall \bar{a}, \bar{b}, \bar{c} \in S \Rightarrow (\bar{a}+\bar{b})+\bar{c} = \bar{a}+(\bar{b}+\bar{c})$

$(\bar{a}-\bar{b})-\bar{c} \neq \bar{a}-(\bar{b}-\bar{c})$.

Identity element:

Let S be a non-empty set and * be a b-o on S.

if $\exists$ an elt $b \in S$ s.t

$a*b = b*a = a$ $\forall a \in S$.

then b is called an identity element in S w.r.t b-o *.

→ The identity elt can be denoted by e. i.e, b = e.

Ex (1) $\exists$ an elt $b = 0 \notin N$ s.t $a+0 = 0+a = a$ $\forall a \in N$.

$\therefore$ 0 is not an identity elt in N w.r.t b-o +.

$\exists$ an elt $b = 1 \in N$ s.t

$a \cdot 1 = 1 \cdot a = a$ $\forall a \in N$.

$\therefore$ 1 is an identity elt in N w.r.t x^n.

(2) S = I, Q, R, C.

$\exists$ an elt $b = 0 \in S$ s.t $a+0 = 0+a = a$ $\forall a \in S$.

$\exists b = 1 \in S$ s.t $a \cdot 1 = 1 \cdot a = a$ $\forall a \in S$.

Note: In any number system identity elt w.r.t ordinary addition is zero. and w.r.t ordinary multiplication is 1.

(3) S = The set of all $m \times n$ matrices.

$A, B \in S \Rightarrow A+B = B+A = A$.

then $B = 0$ (null matrix) is the identity elt in S.

4) S = The set of all $n \times n$ matrices.

$A, B \in S \Rightarrow A \cdot B = B \cdot A = A$

then $B = I$ (unit matrix) is the identity elt in S.

Inverse element :-

Let S be a non-empty set and $*$ be a b-o on S.

for each $a \in G$ $\exists$ an elt $b \in S$ s.t

$a * b = b * a = e$

then 'b' is said to be an inverse of 'a' and is denoted by a^{-1} i.e, $b = a^{-1}$.

Ex:-

for each $a \in G$ $\exists$ an elt $b = -a \in I$

s.t $a+(-a) = 0 = (-a)+a$.

$\therefore -a$ is an inverse of a in I

(2)

for each $a \in G$ $\exists$ $b = \frac{1}{a} \notin I$ s.t $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$ $(a \neq 0)$

$\therefore 1/a$ is an inverse of a.

→ $S = Q, R, C$; for each $a \in S$ $\exists$ $b = -a \in S$ s.t

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

for each $a \in S$ $\exists$ $b = \frac{1}{a} \in S$ (if $a \neq 0$) s.t $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$

$\therefore \frac{1}{a}$ is an inverse of a.

→ S = The set of all $m \times n$ matrices.

for each $A \in S$ $\exists$ $B = -A \in S$ s.t

$A+(-A) = O_{m \times n} = (-A)+A$

then $-A$ is the inverse of A.

→ S = The set of all $n \times n$ matrices

$\exists$ $B = A^{-1} = \frac{\text{adj } A}{|A|}$ (if $|A| \neq 0$)

s.t $A \cdot A^{-1} = A^{-1} A = I$.

Note: In any number system the inverse of 'a' w.r.t ordinary addition is '$-a$' and the inverse of 'a' w.r.t ordinary multiplication is $1/a$.

Problems

Determine whether the binary operation $*$ defined is commutative and whether $*$ is associative.

1→ $*$ defined on Z by letting $a * b = a - b$.

2) $*$ defined on $\mathbb{Q}$ by letting $a*b = ab+1$

3) $*$ defined on $\mathbb{Q}$ by letting $a*b = \frac{ab}{2}$

4) $*$ defined on $\mathbb{Z}^+$ by letting $a*b = a^b$.

5) $*$ defined on $\mathbb{Z}$ by letting $a*b = a+b-ab$.

6) $*$ defined on $\mathbb{Q}$ by letting $a*b = \frac{ab}{3}$.

Determine whether the b-o $*$ defined is identity.

1) $*$ defined on $\mathbb{Q}$ by letting $a*b = \frac{ab}{3}$

8) $*$ defined on $\mathbb{Z}$ by letting $a*b = a+b+ab$

Answers:

1. Since $a*b = a-b \quad \forall a,b \in \mathbb{Z}$

$b*a = b-a$

$\therefore a*b \neq b*a$.

$\therefore *$ is not commutative in $\mathbb{Z}$.

Since $a*b = a-b \quad \forall a,b \in \mathbb{Z}$

Let $a,b,c \in \mathbb{Z}$

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

$= a-b-c$

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

$= a-(b-c)$

$= a-b+c$

$\therefore (a*b)*c \neq a*(b*c)$

$\therefore *$ is not associative in $\mathbb{Z}$.

(2) Not associative.

(3) not associative

(4) both not

(7) Since $a*b = \frac{ab}{3} \quad \forall a,b \in \mathbb{Q}$

Let $a \in \mathbb{Q}$, $e \in \mathbb{Q}$ then

$a*e = a = e*a$

Now $a*e = a \Rightarrow \frac{ae}{3} = a$

$\Rightarrow \frac{ae}{3} - a = 0$

$\Rightarrow \frac{a}{3}(e-3) = 0$

$\Rightarrow e-3 = 0$ (if $\frac{a}{3} \neq 0$)

$\Rightarrow e = 3$.

$\therefore a*e = \frac{ae}{3} = \frac{a}{3} \times 3$

$= a$

$= e*a$.

$\therefore 3$ is the identity elt in $\mathbb{Q}$.

Algebraic structure:

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

(or)

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

Ex: $(N,+)$, $(N,+,\cdot)$, $(I,+,\cdot,-)$ etc are algebraic structures.

but $(N,-)$, $(I,\div)$ etc are not algebraic structures.

Groupoid (or) Quasi group:-

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

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

Ex: $(N,+)$, $(I,+)$ etc are groupoids.

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 semigroup because it is closure but not associative.

Monoid:-

A semi group $(G,*)$ with an identity elt w.r.t $*$ is known as a monoid.

Ex:- A semigroup $(I,+)$ is a monoid and the identity is '0'.

- A semi group $(I,\cdot)$ is a monoid and the identity elt is 1.
- A semigroup $(N,+)$ is not monoid because the identity elt is $0 \notin N$.

Group:-

A monoid $(G,*)$ with the inverse elt 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: $\forall a,b \in G \Rightarrow a*b \in G$

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

(3) Existence of identity:

$\exists e \in G$ s.t $a*e = a = e*a$ $\forall a \in G$

'e' is called the identity elt in G.

(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.

Abelian or Commulative group:-

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

Otherwise it is known as non-abelian group.

finite and infinite group:-

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

Note 1) The order of infinite group is infinite.

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

Problems

(1) The algebraic structure $(I, +)$ where $I = \{\ldots -3, -2, -1, 0, 1, 2, \ldots\}$ is an abelian group.

Note: (i) The set Z^+ under $+^n$ is not a group. There is no identity elt for $+^n$ in Z^+

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

(2) The set I_E of all even integers is an abelian group w.r.t $+^n$.

Note: The set I_O of all odd integers is not a group w.r.t $+^n$. because the closure property is not satisfied.

(3) The sets Q, R and C of all rational, real and complex numbers are abelian groups under $+^n$.

(4) G = The set of $m \times n$ matrices is an abelian group w.r.t $+^n$.

5) G = The set of vectors is an abelian group w.r.t $+^n$.

6) The set $G = \{\ldots -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$ of multiple of integers by fixed integers m is an abelian group w.r.t. $+^n$.

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

8) The sets Q, R, C of all rational, real and complex numbers are not groups w.r.t x^n because the inverse of 0 is not defined.

(9) The sets Q^+ and R^+ of all +ve rational and real numbers are abelian groups under x^n.

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

11) Is the set of all rational numbers x s.t $0 < x \leq 1$, a group w.r.t x^n?

Soln Let $G = \{x / x$ is a rational no. and $0 < x \leq 1\}$

Then it is not a group under x^n because if $a \in G$ and $0 < a < 1$ then inverse of 'a' 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 +ve rational numbers forms an abelian group under the composition $*$ defined by $a * b = ab/2$.

Elementary properties of Groups

→ If G is a group with b-o '.' then the left and right cancellation laws hold in G.

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

and (ii) $ba = ca \Rightarrow b = c$ (R.C.L)

proof Given that G is a group w.r.t b-o '.'

for each $a \in G$ $\exists\ \bar{a}^1 \in G$ s.t $\bar{a}^1 a = a \cdot \bar{a}^1 = e$ (where e is identity)

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

multiplying both sides $\bar{a}^1$ on left

$\bar{a}^1(ab) = \bar{a}^1(ac)$

$\Rightarrow (\bar{a}^1 a) b = (\bar{a}^1 a) c$ (Asso. prop.)

$\Rightarrow eb = ec$ (Inverse law)

$\Rightarrow b = c$ (identity)

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

Note: If G is a group with b-o '+' then the left and right cancellation laws hold 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) $\forall a, b, c \in G$

→ If G is a group with b-o '.' and a & b are elts of G then the linear eqns $ax = b$ and $ya = b$ have unique soln's x and y in G

proof: Given that G is a group w.r.t b-o '.'

for each $a \in G$ $\exists\ \bar{a}^1 \in G$ s.t $a\bar{a}^1 = \bar{a}^1 a = e$ (where e is identity)

Now we have $ax = b$

multl. both sides $\bar{a}^1$ on left we get

$\bar{a}^1(ax) = \bar{a}^1 b$

$\Rightarrow (\bar{a}^1 a) x = \bar{a}^1 b$ (by Asso. prop)

$\Rightarrow ex = \bar{a}^1 b$ (by inverse)

$\Rightarrow x = \bar{a}^1 b$ (by identity)

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

$\Rightarrow \bar{a}^1 b \in G$

Now substituting $\bar{a}^1 b$ for x in the left hand side of the eqn $ax = b$.

we have $a(\bar{a}^1 b) = (a\bar{a}^1) b$

$= eb$

$= b$.

$\therefore x = \bar{a}^1 b$ 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's of the eqn $ax = b$ then $ax_1 = b$, $ax_2 = b$

$\therefore ax_1 = ax_2 \Rightarrow x_1 = x_2$ (By L.C.L)

$\therefore$ The soln is unique.

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

NOTE: If G is a group with the b-o + and a & b are two elements of G then the linear equations $a+x=b$ and $y+a=b$ have unique solutions x & y in G.

Note 1. Cancellation laws hold in a group i.e, $\forall a,b,c \in G$

$\Rightarrow$ (i) $ab=ac \Rightarrow b=c$ (LCL)

(ii) $ba=ca \Rightarrow b=c$ (RCL)

2. In a semigroup, 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 is b-o on S then S is a semi group but not satisfy the cancellations laws because if $A=\begin{bmatrix}1&0\\0&0\end{bmatrix}$, $B=\begin{bmatrix}0&0\\0&1\end{bmatrix}$

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

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

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

3. $(N,+)$ is a semigroup.

for $a,b,c \in N$ $a+b=a+c$

and $b+a=c+a$

$\Rightarrow b=c$

But $(N,+)$ is not a group.

$\therefore$ In a semi group even if cancellation laws hold, the semigroup is not a group.

4. A finite semigroup $(G,\cdot)$ satisfy the cancellation laws 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:

The identity element in a group is unique.

proof: Let $(G,\cdot)$ be the given group. if possible suppose that e_1 & e_2 are two identity elements in G.

Since e_1 is an identity in G then $e_1e_2=e_2=e_2e_1$ ——①

Since e_2 is identity in G then $e_1e_2=e_1=e_2e_1$ ——②

from ① & ② we have

$e_1=e_1e_2=e_2$

$\Rightarrow \boxed{e_1=e_2}$

→ 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' & a''.

Since a' is an inverse of a in G.

$\therefore aa' = a'a = e$ —— (1)

Since a'' is an inverse of a in G

$\therefore aa'' = a''a = e$ —— (2)

From (1) & (2) we have

$aa' = e = aa''$

$\Rightarrow aa' = aa''$

$\Rightarrow a' = a''$ (By LCL)

$\therefore$ inverse of $a \in G$ is unique.

Note: The identity element is its own inverse.

Since $ee = e$

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

→ If the inverse of a is $\bar{a}^{-1}$ then inverse of $\bar{a}^{-1}$ is a

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

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

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

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

Now $a\bar{a}^{-1} = e$

Multiplying bothsides with $(\bar{a}^{-1})^{-1}$ on the right.

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

$\Rightarrow a(\bar{a}^{-1}(\bar{a}^{-1})^{-1}) = (\bar{a}^{-1})^{-1}$ (By association and e is identity)

$\Rightarrow a(e) = (\bar{a}^{-1})^{-1}$ ($\because (\bar{a}^{-1})^{-1}$ is inverse of $\bar{a}^{-1}$)

$\Rightarrow a = (\bar{a}^{-1})^{-1}$ ($\because$ e is identity)

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

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

i.e, $-(-a) = a$.

→ Let $(G,\cdot)$ be a group.

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

proof Given that $(G,\cdot)$ is a group.

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

$a\bar{a}^{-1} = \bar{a}^{-1}a = e$ and

for each $b \in G$, $\exists\ \bar{b}^{-1} \in G$ such that $b\bar{b}^{-1} = \bar{b}^{-1}b = e$

and $a \in G$, $b \in G \Rightarrow ab \in G$

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

Now we have

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})\bar{a}^{-1}$ (by asso.)

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

$= a\bar{a}^{-1}$ by identity

$= e$ by inverse

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

Now we have

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

From (1) & (2) we have

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

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

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

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

(2) Generalization

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

* **Definition of a group based upon Left Axioms (or) Right Axioms:**

The algebraic structure $(G, \cdot)$ is said to be group if the binary operation '$\cdot$' satisfies the following properties.

(i) **Closure property:** $ab \in G \ \forall a, b \in G$

(ii) **Asso. prop:** $(ab)c = a(bc)$ $\forall a, b, c \in G$

(iii) **Existence of left identity:**

$\exists\, e \in G$ 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 $a \in G$ $\exists\, \bar{a}^1 \in G$ such that $\bar{a}^1 a = e$.

$\therefore$ The element $\bar{a}^1$ is called the left inverse of a in G.

Theorem:

The left identity is also the right identity i.e, if 'e' is the left identity then $ae = a$ $\forall a \in G$.

Proof: Let $(G, \cdot)$ be the given group. and let e be the left identity. 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.

$\therefore \bar{a}^1 a = e$

Now we have $\bar{a}^1(ae) = (\bar{a}^1 a) \cdot e$ (by Asso.)

$= ee$ (by inverse)

$= e$ (by identity i.e, e is left identity)

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

$\therefore \bar{a}^1(ae) = \bar{a}^1 a$

$\Rightarrow ae = a$ (by LCL in G)

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

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

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

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

IMS
CELL NO 9999197625
MATHEMATICS
By K. VENKANNA

Let $\bar{a}^{-1}$ be the left inverse of a then $\bar{a}^{-1}a = e$

To prove that $a\bar{a}^{-1} = e$

Now we have

$\bar{a}^{-1}(a\bar{a}^{-1}) = (\bar{a}^{-1}a)\bar{a}^{-1}$ (by Asso.)

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

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

$= \bar{a}^{-1}e$ ($\because$ e is also right identity)

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

$\Rightarrow a\bar{a}^{-1} = e$ (by LCL)

$\therefore$ If $\bar{a}^{-1}a = e$ then $a\bar{a}^{-1} = e$

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

Problems

(1) Show that the set $G = \{a + b\sqrt{2} / a, b \in \mathbb{Q}\}$ is a group w.r.t $+^n$.

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

(3) Show that the set of all $n \times n$ 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 $n \times n$ non-singular matrices with their elements as rational numbers.

(i) Closure prop:

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) Asso. prop:

Matrices Multiplication is associative.

(iii) Existence of left identity:

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

such that $IA = A$.

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

(iv) Existence of left inverse:

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

such that $\bar{A}^{-1}A = I_{n\times n}$. (left identity)

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

(v) Comm. prop:

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

$\Rightarrow AB \neq BA$.

$\therefore (M, \cdot)$ is not an abelian group.

Note: M is the set of all nxn non-singular matrices with their elements as integers is not a group w.r.t x^n because there is no inverse of all matrices in the given set.

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

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

Now we have

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

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

---

(4) S.T the set of matrices $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$ where α is a real number forms a group under matrix multiplication.

Soln: Let $G_1 = \{A_\alpha / \alpha \in \mathbb{R}\}$ and '.' is b-o.

(i) Let $A_\alpha, A_\beta \in G \Rightarrow A_\alpha A_\beta = A_{\alpha+\beta} \in G$ where $\alpha, \beta \in \mathbb{R}$ (Closure prop:)

Since $A_\alpha \cdot A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}\begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$

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

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

$\therefore$ closure prop. is satisfied.

(ii) Asso. prop: Matrix Multiplication is associative.

(iii) Existence of left identity:

Since $0 \in \mathbb{R}$

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

Let $A_\alpha \in G, \alpha \in \mathbb{R} \exists A_0 \in G, 0 \in \mathbb{R}$ such that $A_0 A_\alpha = A_{0+\alpha} = A_\alpha$.

$\therefore A_0$ is left identity

(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_α

$\therefore$ Each element of G_1 possesses left inverse.

$\therefore G_1$ is a group under x^n.

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

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

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

Problems:

→ Do the following sets form groups w.r.t the b-o * on them as follows.

(i) The set I of all integers with operation defined by $a * b = a+b+1$

(ii) The set $\mathbb{Q}$ of all Rational numbers otherthan 1 (i.e, $\mathbb{Q}-\{1\}$) with operation defined by

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

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

Sol^n: (ii) Since $a*b = a+b-ab \quad \forall a,b \in \mathbb{Q}-\{1\}$ ——— (A)

(1) Closure prop:

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

$a*b = a+b-ab \in \mathbb{Q}-\{1\}$ (by (A))

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

(2) Asso. property:

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

$$\Rightarrow (a*b)*c = (a+b-ab)*c \quad (\text{by (A)})$$
$$= a+b-ab+c-(a+b-ab)c$$
$$= a+b-ab+c-ac-b+abc$$
$$= a+b+c-(ab+bc+ca)+abc.$$

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

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

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

(3) Existence of left identity prop:

Let $a \in \mathbb{Q}-\{1\}$, $e \in \mathbb{Q}-\{1\}$

then $e * a = a$

Now $e * a = a$

$\Rightarrow e + a - ea = a$

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

$\Rightarrow e = 0 \quad (\because a \neq 1)$

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

$\therefore e * a = 0 * a.$

$= 0 + a - 0(a)$

$= a$

$\therefore \forall a \in \mathbb{Q}-\{1\}, \exists\ 0 \in \mathbb{Q}-\{1\}$ such that

$0 * a = a.$

$\therefore 0$ is the left identity in $\mathbb{Q}-\{1\}$.

(4) Existence of left inverse:

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

then $b * a = e$

Now $b * a = e$

$\Rightarrow b + a - ba = 0 \quad (\text{by } \textcircled{A})$

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

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

$= \frac{a}{a-1} \in \mathbb{Q}-\{1\}$

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

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

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

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

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

$\therefore b = \frac{a}{a-1}$ is left inverse of a in $Q-\{1\}$ w.r.t. $*$.

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

→ Let S be the set of all real numbers except -1. Define $*$ on S by $a*b = a+b+ab$

a) Show that $*$ gives a binary operation on S.

b) Show that $(S, *)$ is a group.

c) Find the solution of the equation $2*x*3 = 7$ in S.

Soln:

(a) Since S is the set of all real numbers except -1 and $*$ is an operation defined in $S = \mathbb{R}-\{-1\}$ such that

$a*b = a+b+ab$ ~~$\forall$~~ $a, b \in S$

when $a, b \in S$

$a*b = a+b+ab \in S$.

$\therefore a*b \in S$

$\therefore *$ is a b-o on S.

$\therefore a*b = a+b+ab$

~~$\forall$~~ $a, b \in S$.

If possible let
$a*b = -1$
$\Rightarrow a+b+ab = -1$
$\Rightarrow (a+1)+b(a+1) = 0$
$\Rightarrow (a+1)(b+1) = 0$
$\Rightarrow a+1 = 0$ or $b+1 = 0$
$\Rightarrow a = -1$ or $b = -1$
clearly which is contradiction to hypothesis $a \neq -1$, $b \neq -1$ in S. (1)

(b) (i) Closure prop:

~~$\forall$~~ $a, b \in S$

$a*b = a+b+ab \in S$ by (1)

$\therefore$ S is closed under $*$.

(ii) Associative prop:

$\forall a, b, c \in S \Rightarrow (a*b)*c = (a+b+ab)*c$

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

$= a+b+c+ab+bc+ca+abc$

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

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

$\therefore$ Associative law holds.

(iii) Existence of left identity:

Let $a \in S$, $e \in S$ then $e*a = a$

Now $e*a = a$

$\Rightarrow e+a+ea = a$

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

$\Rightarrow e = 0 \in S \quad (\because a \neq -1)$

$\therefore e*a = 0*a$

$= 0+a+0(a)$

$= a$

$\therefore \forall a \in S \; \exists \; 0 \in S$ such that $0*a = a$.

$\therefore 0$ is the left identity in S.

(iv) Existence of left inverse:

Let $a \in S$, $b \in S$ then $b*a = e$

Now $b*a = e$

$\Rightarrow b+a+ba = 0 \quad (\because e = 0)$

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

$\Rightarrow b = \frac{-a}{1+a} \in S \; (\because a \neq -1)$

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

$$= \frac{-a}{1+a} + a + \left(\frac{-a}{1+a}\right)a$$

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

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

$$= 0$$

for each $a \in S$ $\exists$ $b = \frac{-a}{1+a} \in S$ such that $\frac{-a}{1+a} * a = 0$

$\therefore$ $b = \frac{-a}{1+a}$ is left inverse of a in S w.r.t $*$.

$\therefore$ $(S, *)$ is a group.

(c) $2 * x * 3 = 7$

$\Rightarrow (2 + x + 2x) * 3 = 7$ by (1)

$\Rightarrow (2 + 3x) * 3 = 7$

$\Rightarrow (2+3x) + 3 + (2+3x)3 = 7$ by (1)

$\Rightarrow 5 + 3x + 6 + 9x = 7$

$\Rightarrow 11 + 12x = 7$

$\Rightarrow 12x = -4$

$\Rightarrow x = -\frac{1}{3} \in S$

Now $2 * (-\frac{1}{3}) * 3 = \left[2 + (-\frac{1}{3}) + 2(-\frac{1}{3})\right] * 3$ by (1)

$= \left(\frac{5}{3} - \frac{2}{3}\right) * 3$

$= 1 * 3$

$= 1 + 3 + 3$

$= 7$

$\therefore$ $x = -1/3$ is a solution of the equation $2 * x * 3 = 7$ in S

→ Let G be the set of all those ordered pairs (a, b) of real numbers for which $a \neq 0$ and define in G, an operation $\otimes$ as follows:

$(a,b) \otimes (c,d) = (ac, bc+d)$

Examine whether G is a group w.r.t the operation $\otimes$. If it is a group, is G abelian?

Soln: Let $G = \{(a,b) / a \neq 0, b \in \mathbb{R}\}$ and an operation $\otimes$ defined by

$$(a,b) \otimes (c,d) = (ac, bc+d) \quad \text{---} (1)$$

(i) Closure prop:

$\forall (a,b), (c,d) \in G$; $a,b,c,d \in \mathbb{R}$ & $a \neq 0, c \neq 0$.

$\Rightarrow (a,b) \otimes (c,d) = (ac, bc+d) \in G$

($\because a \neq 0, c \neq 0 \Rightarrow ac \neq 0$ & $bc+d \in \mathbb{R}$)

$\therefore$ G is closed under $\otimes$.

(ii) Asso. prop:

$\forall (a,b), (c,d), (e,f) \in G$ where $a,b,c,d,e,f \in \mathbb{R}$ & $a, c, e \neq 0$

$\Rightarrow [(a,b) \otimes (c,d)] \otimes (e,f) = (ac, bc+d) \otimes (e,f)$ by (1)

$= (ace, (bc+d)e+f)$

$= (ace, bce+de+f)$

Similarly $(a,b) \otimes [(c,d) \otimes (e,f)] = (ace, bce+de+f)$

$\therefore$ Asso. law holds.

(iii) Existence of left identity:

Let $(a,b) \in G$ where $a \neq 0$

Let $(x,y) \in G$ where $x \neq 0$ such that

$$(x,y) \otimes (a,b) = (a,b)$$

Now $(x,y) \otimes (a,b) = (a,b)$

$\Rightarrow (xa, ya+b) = (a,b)$ by (1)

$\Rightarrow xa = a$ & $ya+b = b$

$\Rightarrow x = 1$ & $ya = 0$

$\Rightarrow y = 0 \quad (\because a \neq 0)$

$\therefore x = 1$ & $y = 0$

$\therefore (1,0) \in G$ such that $(1,0) \otimes (a,b) = (a,b)$

$\therefore (1,0)$ is the left identity in G.

(iv) Existence of left inverse:

Let $(a,b) \in G$ where $a \neq 0$

Let $(x,y) \in G$ where $x \neq 0$ such that

$(x,y) \otimes (a,b) = (1,0)$

NOW $(x,y) \otimes (a,b) = (1,0)$

$\Rightarrow (xa, ya+b) = (1,0)$

$\Rightarrow xa = 1 \; ; \; ya + b = 0$

$\Rightarrow x = \frac{1}{a} \; ; \; y = -\frac{b}{a} \quad (\because a \neq 0)$

$\therefore (x,y) = \left(\frac{1}{a}, -\frac{b}{a}\right) \in G$ such that

$\left(\frac{1}{a}, -\frac{b}{a}\right) \otimes (a,b) = (1,0)$

$\therefore \left(\frac{1}{a}, -\frac{b}{a}\right)$ is the left inverse of (a,b) in G

$\therefore (G, \otimes)$ is a group.

(v) Comm. prop:

$\forall (a,b), (c,d) \in G \; ; \; a,b,c,d \in \mathbb{R} \; ; \; a \neq 0, c \neq 0$

$(a,b) \otimes (c,d) = (ac, bc+d) \quad (\text{by } ①)$

and $(c,d) \otimes (a,b) = (ca, da+b)$

$\therefore (a,b) \otimes (c,d) \neq (c,d) \otimes (a,b)$

$\therefore G$ is not commutative under $\otimes$

$\therefore$ the group $(G, \otimes)$ is not an abelian group.

→ Let R_0 be the set of all Real numbers except zero. Define a binary operation $*$ on R_0 as: $a * b = |a| \cdot b$, where $|a|$ denotes absolute value of a. Does $(R_0, *)$ form a group? Examine.

H.W → Let $G = \{(a,b) : a,b \in \mathbb{R} \text{ and not both zero}\}$ and $*$ be a binary operation defined by

$(a,b) * (c,d) = (ac-bd, ad+bc)$

Show that $(G,*)$ is a commutative group.

H.W → Let $G = \{(a,b) : a,b \in \mathbb{R}\}$ and $*$ be a b-o defined by $(a,b) * (c,d) = (a+c, b+d)$ $\forall a,b,c,d \in \mathbb{R}$

Show that $(G,*)$ is a commutative group.

Composition table for finite sets:

Let $G = \{a_1, a_2, a_3, \ldots, a_n\}$ be a finite set having n distinct elements. Suppose there is a binary operation $*$ on G can be shown in tabular form known as composition table.

- Write the elements of G in a horizontal row and vertical coloumn.
- If a_i, a_j are two elements of G then $a_i * a_j$ at the intersection of a row headed by a_i and coloumn headed by a_j.

(i) All the entries in the composition table are the elements of the set G.

∴ G is closed w.r.t $*$.

(ii) If any row of the composition table coincides with the top row of the composition table.

∴ Identity property is satisfied.

Extremely left coloumn of the corresponding row (first element) is the identity element.

(iii) from the composition table, every row and every coloumn contains the identity element.

∴ Inverse property is satisfied.

(iv) from the composition table, the rows and coloumns are interchanged, there is no change in the table.

i.e, if i^{th} row and j^{th} coloumn is a_{ij}

then $a_{ij} = a_{ji}$

∴ commutative property is satisfied.

Problems

→ Show that the fourth roots of unity $G = \{1, -1, i, -i\}$ is an abelian group w.r.t x^n.

Soln: $G = \{1, -1, i, -i\}$ and x^n is a b-o on G

Now construct the composition table for G w.r.t x^n.

×	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

(i) Closure prop:

Since all the entries in the composition table are the entries in the set G.

∴ Closure prop. is satisfied.

(ii) Asso. prop:

The elements of G are complex numbers and the multiplication of complex numbers is associative.

(iii) Existence of left identity:

From the composition table first row coincides with the top row.

Extremely left coloumn of corresponding row (first element) is the identity element.

i.e, $1(1)=1$, $1(-1)=-1$, $1(i)=i$, $1(-i)=-i$.

i.e, $1 \in G$ and $1a=a$ $\forall a \in G$

$\therefore$ 1 is the left identity in G.

(iv) Existence of left inverse:

from the composition table, every row & every coloumn contains the identity element.

i.e, $1\cdot1=1$, $(-1)(-1)=1$, $i(-i)=1$, $-i(i)=1$

for each $a \in G$ $\exists$ $b \in G$ such that $ba=e$

$\therefore$ b is the left inverse of a in G.

(v) Comm. prop's

from the composition table, the rows & coloumns are interchanged, there is no change in the table.

$\therefore$ Comm. prop. is satisfied.

$\therefore$ (G,·) is an abelian group. and $O(G)=4$

H.W. → S.T the set $G=\{1, \omega, \omega^2\}$ where ω is imaginary cube root of unity is an abelian group w.r.t x^n. $O(G)=3$

HW → S.T (i) $G=\{1,-1\}$ (ii) $G=\{1\}$ are abelian groups w.r.t x^n.

Note: Every group of order four and less is an abelian.

H.W → Show that the matrices $A=\begin{bmatrix}1&0\\0&1\end{bmatrix}$ $B=\begin{bmatrix}-1&0\\0&1\end{bmatrix}$ $C=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$, $D=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$ form an abelian group w.r.t x^n.

→ Show that the set of six transformations $f_1, f_2, f_3, f_4, f_5, f_6$ on the set of complex numbers except 0 and 1 (i.e, $A=C-\{0,1\}$) defined by $f_1(z)=z$, $f_2(z)=\frac{1}{z}$, $f_3(z)=1-z$

$f_4(z)=\frac{z}{z-1}$, $f_5(z)=\frac{1}{1-z}$, $f_6(z)=\frac{z-1}{z}$

forms a finite non-abelian group of order 6 w.r.t the composition known as composite of two functions (or) product of two functions.

Soln: $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$

Let x^n be the composition of the composite or product of two functions.

Let $f: A \to A$ & $g: A \to A$ then $(gf): A \to A$

such that $(gf)(x) = g(f(x))$ $\forall x \in A$.

∴ The function gf is called composite of the functions g & f.

Now we construct the composition table:

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

$(f_1 f_1)(z) = f_1(f_1(z)) = f_1(z) = z = f_1$

$(f_1 f_2)(z) = f_1(f_2(z)) = f_1\left(\frac{1}{z}\right) = \frac{1}{z} = f_2$

$(f_1 f_3)(z) = f_1(f_3(z)) = f_1(f_3(z)) = f_1(1-z) = 1-z = f_3$

Similarly $f_1 f_4 = f_4$ & $f_1 f_5 = f_5$; $f_2 f_1 = f_2$, $f_3 f_1 = f_3$

$f_4 f_1 = f_4$, $f_5 f_1 = f_5$ & $f_6 f_1 = f_6$

$(f_2 f_2)(z) = f_2(f_2(z)) = f_2\left(\frac{1}{z}\right) = z = f_1$

$(f_2 f_3)(z) = f_2(f_3(z)) = f_2(1-z) = \frac{1}{1-z} = f_5$

$(f_2 f_4)(z) = f_2\left(\frac{z}{z-1}\right) = \frac{z-1}{z} = f_6$

$(f_2 f_5)(z) = f_2\left(\frac{1}{1-z}\right) = 1-\frac{1}{1-z} = f_3$

$(f_2 f_6)(z) = f_2\left(\frac{z-1}{z}\right) = \frac{z}{z-1} = f_4$

$(f_3 f_2)(z) = f_3\left(\frac{1}{z}\right) = 1-\frac{1}{z} = \frac{z-1}{z} = f_6.$

Similarly we can easily find other products

(i) —

(ii) The composite of functions is an asso. composition.

Let $f: A \to A$, $g: A \to A$, $h: A \to A$.

then $h(gf) = (hg)f$.

(iii) —

(iv) —

(v) The composition is not commutative.

Since $f_2 f_3 = f_5$ & $f_3 f_2 = f_6$.

$\therefore f_2 f_3 \neq f_3 f_2$

$\therefore G$ is group but not commutative group w.r.t the composite composition.

$\boxed{O(G) = 6.}$

HW → Show that the bijective transformations f_1, f_2, f_3, f_4 on $A = \mathbb{R} - \{0\}$ given by $f_1(z) = z$, $f_2(z) = \frac{1}{z}$, $f_3(z) = -z$, $f_4(z) = -\frac{1}{z}$ w.r.t the operation composition of mappings is an abelian group.

→ Let S be any non-empty set and let $A(S)$ be the set of all one-to-one mappings of the set S onto itself. Then show that $A(S)$ is a group w.r.t composite of mappings as the composition. Is it an abelian group?

Sol^n: Let $A(S)$ be the set of all bijections from S to S

Let $f, g \in A(S)$ then f & g are both bijections from $S \to S$.

By the definition of composite of two functions f & g denoted by fg and fg is mapping from S to S given by

$$(fg)(x) = f(g(x)) \quad \forall x \in S$$

(i) Closure prop:

Let $f, g \in A(S) \Rightarrow fg \in A(S)$

Since f, g are bijections from $S \to S$.

$\therefore$ the composite mapping fg is also bijection from $S \to S$.

$\therefore$ $A(S)$ is closed w.r.t composite composition.

(ii) Asso. prop:

Let $f, g, h \in A(S) \Rightarrow (fg)h = f(gh)$

Since $\forall x \in S$

$$\begin{aligned}[(fg)h](x) &= (fg)[h(x)] \\ &= f[g(h(x))] \\ &= f[(gh)(x)] \\ &= [f(gh)](x).\end{aligned}$$

(iii) Existence of left identity:

Let e be the identity mapping from $S \to S$

$\therefore$ for $x \in S$, $e(x) = x$

Also e is bijection.

$\therefore e \in A(S)$

$\therefore f \in A(S) \Rightarrow ef = f$

since $(ef)(x) = e(f(x))$

$= f(x)$

$\therefore ef = f$

$\therefore e$ is the left identity element in $A(S)$.

Existence of left inverse:

Let $f \in A(S) \Rightarrow f: S \to S$ is bijection.

$\therefore f^{-1}: S \to S$ is bijection.

$\therefore f^{-1} \in A(S)$

$\therefore f \in A(S) \ \exists\ f^{-1} \in A(S)$ such that $f^{-1}f = e$.

Since $\forall x \in S$

$$(f^{-1}f)(x) = f^{-1}(\underbrace{f(x)}_{y}) = x = e(x)$$

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

$\therefore A(S)$ is a group w.r.t composite composition.

$S \xrightarrow{f} S$

$x \to y$

$f(x) = y$

$f^{-1}(y) = x$.

- If the set S has only one element then the set $A(S)$ has only one element and every group of order 1 is abelian.
- If the set S has two elements then the set $A(S)$ has also two elements and every group of order 2 is abelian.
- If the set S has more than two elements.

Let x, y, z be three distinct elements in S.

Let $f: S \to S$ & $g: S \to S$

$f(x) = y$, $f(y) = z$, $f(z) = x$

$g(x) = x$, $g(y) = z$, $g(z) = y$

Now $(fg)(x) = f(g(x)) = f(x) = y$.

and $(gf)(x) = g(f(x)) = g(y) = z$

$\therefore (fg)(x) \neq (gf)(x)$.

$\therefore$ Comm. prop. is not satisfied.

$\therefore A(S)$ is non-abelian group.

→ prove that the set of all n^{th} roots of unity forms a finite abelian group of order n w.r.t multiplication.

Sol^n: $1^{1/n} = (1+0i)^{1/n}$

$= (\cos 0 + i \sin 0)^{1/n}$

$= (\cos 2k\pi + i \sin 2k\pi)^{1/n}$

$= \left(\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}\right)$ where $k = 0, 1, 2, \ldots n-1$

$= e^{\frac{2k\pi i}{n}}$ (By DeMoivre's theorem)

Let $G = \left\{ e^{\frac{2k\pi i}{n}} / k = 0, 1, 2, \ldots n-1 \right\}$

(i) Closure prop:

Let $a, b \in G$ where $a = e^{\frac{2r\pi i}{n}}$, $b = e^{\frac{2s\pi i}{n}}$

$0 \le r, s \le n-1$

then $a \cdot b = e^{\frac{2(r+s)\pi i}{n}} \in G$

$(\because 0 \le r+s \le n-1)$

$\therefore G$ is closed under $\times^n$.

(ii) Asso. prop:

The elements of G are all complex numbers and multiplication of complex numbers is associative.

(iii) Existence of left identity:

$\forall a = e^{\frac{2r\pi i}{n}} \in G \quad \exists b = e^{\frac{2(0)\pi i}{n}} = 1 \in G$

$0 \le r \le n-1$

such that $ba = e^{\frac{2(0)\pi i}{n}} e^{\frac{2r\pi i}{n}}$

$= e^{\frac{2(0+r)\pi i}{n}}$

$= e^{\frac{2r\pi i}{n}}$

$= a$

$\therefore b = 1$ is the left identity element in G.

(iv) Existence of left inverse:

Since $1 \cdot 1 = 1$

we have left inverse of 1 is **1**.

Let $a = e^{\frac{2r\pi i}{n}} \in G$; $1 \le r \le n-1$

$\Rightarrow 1 \le n-r \le n-1$

$\Rightarrow e^{\frac{2(n-r)\pi i}{n}} \in G$

$r = 1, 2, 3, \ldots, n-1$

Now $e^{\frac{2(n-r)\pi i}{n}} \cdot e^{\frac{2r\pi i}{n}} = e^{2\pi i}$

$= \cos 2\pi + i \sin 2\pi$

$= 1$

$\therefore e^{\frac{2(n-r)\pi i}{n}}$ is the left inverse of $e^{\frac{2\pi r i}{n}}$ in G.

$\therefore$ Inverse prop is satisfied.

(v) Commutative prop:

The elements of G are all complex numbers and multiplication of complex numbers is commutative.

$\therefore (G, \cdot)$ is a finite abelian group.

Quaternion Group:

Let $T = \{\pm 1, \pm i, \pm j, \pm k\}$

Define a multiplicative b-o on T by setting

$i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$, $jk = -kj = i$

and $ki = -ik = j$

is non-abelian group of order 8.

(Note: This group is known as Quaternion group of order 8).

Hw: P.T the set G consisting of the following eight matrices $\pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $\pm\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $\pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ forms a Quaternion group under the operation of matrix multiplication.