app...

1.1. DEFINITION (GROUP)

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

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

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

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

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

then e is called the **identity element** of G w.r.t. the operation $*$

(Existence of identity)

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

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

then b is called the inverse of a and is denoted by a^{-1}.

(Existence of inverse)

Note 1. If the operation '$*$' is denoted by '+', the group is denoted by $<G, +>$.

2. If the operation $*$ is denoted by '$\cdot$', the group is denoted by $<G, \cdot>$.

1.1.0. Finite and Infinite Groups

If the set G in the group $<G, *>$ is a finite set, then it is called a **finite group** otherwise it is called an **infinite group**.

1.1.1. Order of a Group

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

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

1.1.2. Abelian and Non-abelian Groups

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

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

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

1.1.3. Groupoid, Semi-Group and Monoid

Groupoid : A non empty set G together with a binary operation $*$ defined on it is called a **Groupoid** if it satisfies the following axiom

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

Semi-Group : A non empty set G together with a binary operation $*$ defined on it is called a **Semi-group** if it satisfies the following axioms :

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

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

Monoid : A non empty set G together with a binary operation $*$ defined on it is called a **Monoid** if it satisfies the following axioms

(i) $a * b \in G \quad \forall\ a, b \in G.$

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

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

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

Here e is called the identity element of G w.r.t. the binary operation $*$.

1.1.4. ILLUSTRATIVE EXAMPLES

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

Sol. Let $N = \{1, 2, 3, 4, ...\}$ be the set of natural numbers.

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

$\therefore$ N is closed under addition.

(ii) **Associative Property :** Since

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

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

Hence N is a semi-group under addition.

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

a non-abelian group.

Example: Let $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ & $*$ denote "multiplication modulo 8" i.e. $x * y = (xy) \bmod 8$. Check whether the above algebraic structure form group or not.

Sol^n Here $(S, *) = (0, 1, 2, 3, 4, 5, 6, 7, \times_8)$

$\times_8$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(i) closure property holds $\because \forall a, b \in S \Rightarrow a \times_8 b \in S$.

(ii) Associative property holds

1 = The remainder when (xy) is divided by 8.

$\because a \times_8 (b \times_8 c) = (a \times_8 b) \times_8 c$.
let $a=1$, $b=2$, $c=3$
$1 \times_8 (2 \times_8 3) = 1 \times_8 (6) = 6$
$(1 \times_8 2) \times_8 3 = 2 \times_8 (3) = 6$. $\Rightarrow \boxed{1 \times_8 (2 \times_8 3) = (1 \times_8 2) \times_8 3}$

Sol^n

(iii) Existence of Identity:
Since 3rd row is same as first row $\therefore$ 1 is left identity.
Also 3rd column is same as 1st column $\therefore$ 1 is right identity.
$\therefore$ 1 is identity of S under $(\times_8)$.

(iv) Existence of Inverse :- Inverse of 0, 2, 4, 6 doesnot exists.

[$\because b * a = e = a * b$, then b is called inverse]
Now $b \times_8 0 = 1$ but $\nexists\, b \in S$ s.t $b \times_8 0 = 1$
$\therefore$ 0 doesnot have an inverse.
Hence S is not a group.

* Prove that inverse element of a group is unique.

$\therefore$ inverse element of a group is unique

<u>Ques</u> Consider an algebraic system $(G, *)$, where G is the set of all non-zero real numbers & $*$ binary operation defined by $a * b = \frac{ab}{4}$, show that $(G, *)$ is an abelian group.

Solⁿ G is set of all non-zero real numbers.

Binary operation $*$ on G is defined as

$$a*b = \frac{ab}{4}, \; \forall a,b \in G.$$

Closure Property: since $\forall a,b \in G$; $\frac{ab}{4}$ is also in G.

i.e $\frac{ab}{4} \in G \; \forall a,b \in G$. $\left[a=3, b=5 \Rightarrow \frac{ab}{4} = \frac{(3)(5)}{4} = \frac{15}{4} \in G\right]$

Thus closure property hold in G.

Associative Property: Let $a,b,c \in G$ then

$$a*(b*c) = a*\left(\frac{bc}{4}\right) = \frac{a\left(\frac{bc}{4}\right)}{4} = \frac{a(bc)}{16} = \frac{abc}{16}$$

$$(a*b)*c = \left(\frac{ab}{4}\right)*c = \frac{\left(\frac{ab}{4}\right)c}{4} = \frac{(ab)c}{16} = \frac{abc}{16}$$

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

Thus associative property holds in G.

Existence of identity: Let $\exists$ $e \in G$ s.t

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

$$\Rightarrow \boxed{\frac{ea}{4} = a} = \frac{ae}{4}$$

$\Rightarrow \frac{ea}{4} - a = 0 \Rightarrow a\left(\frac{e-4}{4}\right) = 0 \Rightarrow \boxed{e=4}$ $[\because a \in G \Rightarrow a \neq 0]$

Thus $4 \in G$ is indentity in G.

Existence of inverse: Let $a \in G$, let $\exists$ $b \in G$ s.t

$a*b = e = b*a$ i.e $\boxed{\frac{ab}{4} = 4} = \frac{ba}{4}$

$\Rightarrow \boxed{b = \frac{16}{a}} \in G$ is the inverse of element $a \in G$.

Commutativity: Let $a,b \in G$ be any elements, then

$$a*b = \frac{ab}{4} = \frac{ba}{4} = b*a$$

$\Rightarrow a*b = b*a \quad \forall a,b \in G$

$\therefore$ Commutative property hold in G.

Thus $(G,*)$ forms an abelian group.

Ques 1] Prove that set of all matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ form abelian group with respect to matrix multiplication.

Soln:- Let M is the set of all matrix & $\times$ is binary operation on M.

Closure Property: Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \in M$, then

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix} \in M, \quad \forall\ A, B \in M$$

$\therefore$ closure property holds.

Associative Property: Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$,

$C = \begin{bmatrix} e & f \\ -f & e \end{bmatrix} \in M$, then

$$A(BC) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\begin{bmatrix} e & f \\ -f & e \end{bmatrix}\right) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} ce-df & cf+de \\ -de-cf & -df+ce \end{bmatrix}$$

$$A(BC) = \begin{bmatrix} ace-adf-bde-bcf & acf+ade-bdf+bce \\ -bce+bdf-ade-acf & -bcf-bde-adf+ace \end{bmatrix} \quad — (1)$$

$$(AB)C = \left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right)\begin{bmatrix} e & f \\ -f & e \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix}\begin{bmatrix} e & f \\ -f & e \end{bmatrix}$$

$$(AB)C = \begin{bmatrix} ace-bde-adf-bcf & acf-bdf+ade+bce \\ -bce-ade+bdf-acf & -bcf-adf-bde+ace \end{bmatrix} \quad — (2)$$

from (1) & (2), we get

$(AB)C = A(BC)$. $\quad \forall\ A, B, C \in M$

$\therefore$ Associative Property holds

$$\Rightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & \\ ad-bc & -bd+ca \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

Taking first two, we get

$$ac-bd = a$$
$$ad+bc = b$$

3) Existence of Identity: Let $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M$, $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in M$

$$AE = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a+0 & 0+b \\ -b+0 & 0+a \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = A \quad -(1)$$

$$EA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a+0 & b+0 \\ 0-b & 0+a \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = A \quad -(2)$$

from (1), (2) we get

$AE = A = EA$. $\forall A \in M$.

$\therefore E$ is the identity of M.

) Existence of Inverse: - As we know that inverse of matrix exists if ~~mata~~ determin[ant] of matrix is non-zero.

Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in M$.

$$\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2+b^2 \neq 0 \Rightarrow A^{-1} \text{ exists} . \forall A \in$$

Commutative Property: Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \in M$

$$AB = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix}$$

$$BA = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} ac-bd & bc+ad \\ -da-bc & -bd+ca \end{bmatrix}$$

$\Rightarrow \boxed{AB = BA}$ $\forall A, B \in M$.

Hence Proved.

Example 8. Let $\mathbf{Q}^*$ denotes the set of all rational numbers except 1, then show that $\mathbf{Q}^*$ forms an infinite abelian group under the operation o defined by $a\, o\, b = a + b - a\, b$ for all $a, b \in \mathbf{Q}^*$.

(H.P.U. April 2008; G.N.D.U. Sept. 2011)

Sol. Let $\mathbf{Q}^*$ be the set of all rational numbers except 1. The binary composition o on $\mathbf{Q}^*$ is defined as

$$a\, o\, b = a + b - a\, b \ \forall\, a, b \in \mathbf{Q}^*.$$

To show that $< \mathbf{Q}^*, o >$ forms an infinite abelian group.

Closure Property : Let $a, b \in \mathbf{Q}^*$ be any elements.

If possible, let $\quad a + b - ab = 1$

$$\begin{aligned}
\Rightarrow \quad a + b - ab - 1 &= 0 \\
\Rightarrow \quad a - ab + b - 1 &= 0 \\
\Rightarrow \quad a(1 - b) - (1 - b) &= 0 \\
\Rightarrow \quad (a - 1)(1 - b) &= 0 \\
\Rightarrow \quad a - 1 &= 0 \quad \text{or} \quad 1 - b = 0
\end{aligned}$$

i.e. $\quad a = 1 \quad$ or $\quad b = 1$, which is not possible, as $a, b \in \mathbf{Q}^*$.

$\therefore \quad a + b - ab \neq 1$, also $a + b - ab \in \mathbf{Q}$ and so $a + b - ab \in \mathbf{Q}^*$.

$\therefore \quad a\, o\, b \in \mathbf{Q}^* \ \forall\ a, b \in \mathbf{Q}^*$.

Thus Closure Property holds in $\mathbf{Q}^*$.

Associativity : Let $a, b, c \in \mathbf{Q}^*$ be any three elements.

$$\begin{aligned}
(a\, o\, b)\, o\, c &= (a + b - a\, b)\, o\, c \\
&= a + b - a\, b + c - (a + b - a\, b)\, c \\
&= a + b + c - a\, b - b\, c - a\, c + a\, b\, c.
\end{aligned}$$

Scanned by CamScanner

Also, $a \circ (b \circ c) = a \circ (b + c - bc)$

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

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

$\therefore \quad (a \circ b) \circ c = a \circ (b \circ c).$

Thus associative property holds in $\mathbf{Q}^*$.

Existence of identity : Let $\exists\, e \in \mathbf{Q}^*$ such that

$$e \circ a = a = a \circ e, \ \forall\, a \in \mathbf{Q}^*$$

i.e. $e + a - ea = a = a + e - ae$

$\Rightarrow \quad e + a - ea = a \quad \Rightarrow \quad e - ea = 0$

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

$\therefore \quad e = 0 \in \mathbf{Q}^*$ works for the identity element in $\mathbf{Q}^*$.

Existence of inverse : Let $a \in \mathbf{Q}^*$ be any element, let $\exists\, b \in \mathbf{Q}^*$ s.t.

$$a \circ b = e = b \circ a$$

i.e. $a + b - ab = 0 = b + a - ba$

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

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

Clearly, $b = \dfrac{a}{a-1} \in \mathbf{Q}^*$, is the inverse of the element a in $\mathbf{Q}^*$.

Commutativity : Let $a, b \in \mathbf{Q}^*$ be any elements.

$\therefore \quad a \circ b = a + b - ab = b + a - ba = b \circ a.$

Also, as the set $\mathbf{Q}^*$ is infinite set. Thus $< \mathbf{Q}^*, o >$ forms an infinite abelian group.

Remark : We can check closed property, commutative property, existence of

Q: Show $G = \{1, -1, i, -i\}$ is abelian group wrt to multiplication.

Sol:

$*=\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

1.) closure Property: Since every element of table is part of set

$$\forall\ a, b \in G \Rightarrow a \cdot b \in G$$

2.) Associative

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

LHS $a \cdot (b \cdot c) = 1 \cdot (i \cdot -i)$

Let $a = 1$ $\quad = 1$

$b = i$ $\quad (a \cdot b) \cdot c = (1 \cdot i) \cdot -i$

$c = -i$ $\quad = 1$

3.) Identity: notation e

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

$i \cdot 1 = i$

$-i \cdot 1 = -i$ $\Rightarrow e = 1 \in G$ is identity

$-1 \cdot 1 = -1$

Scanned by CamScanner

4.) Inverse

Inverse of -1 is -1 given by $-1 \cdot (-1) = 1$

Inverse of i is $-i$ given by $i \cdot (-i) = 1$

$-i$ is i

Since every element has inverse exist

All property verified.

$\Rightarrow$ G is group

Subgroup

Defn:- A non-empty subset H of a group $(G, *)$ is said to be subgroup of G if $(H, *)$ is itself a group.

Note: Every group G has atleast two subgroups i.e. $\{e\}$ & G itself. These two are called trivial or improper subgroups.

Properties of a subgroup

1) The identity element of a subgroup is same as the identity element of the group.
2) The inverse of any element of a subgroup is same as the inverse of the element regarded as the elemen of the group.
3) Subgroup of an abelian group is abelian.
4) A non-abelian group may also have abelian or non-abelian subgroup

Imp **Note:-** A non-empty subset H of a group G is a subgroup iff $ab^{-1} \in H \ \forall a, b \in H$.

Theorem 1: Prove that the intersection of two subgro of a group is again a subgroup of the grou

Proof: Let H and K be two subgroups of a group G
$\therefore$ H and K are subsets of G
$\Rightarrow H \cap K \subseteq G$
Now let $x, y \in H \cap K$
$\therefore x, y \in H$ & $x, y \in K$

$\Rightarrow xy^{-1} \in H$ and $xy^{-1} \in k$ [$\because H, k$ are both subgroups]

$\Rightarrow xy^{-1} \in H \cap k$, $\forall x, y \in H \cap k$

$\therefore H \cap k$ is a subgroup of G.

Theorem 2] If H and k are two subgroups of G then prove $H \cup k$ may not be subgroup of G:

Proof: Let $G = \{0, 1, 2, 3, 4, 5\}$ under the operation addition modulo 6.

Let $H = \{0, 3\}$ and $k = \{0, 2, 4\}$ are subgroups of G

Then $H \cup k = \{0, 2, 3, 4\}$ is not a subgroup of G

$\because 2, 3 \in H \cup k$, but $2+3 = 5 \notin H \cup k$.

Thus union of subgroups of group may not be subgroup of G.

Cosets: Let H be a subgroup of G. If $a \in G$, then the set $Ha = \{ha : h \in H\}$ is called right coset of H in G determined by a. & the set $aH = \{ah : h \in H\}$ is called the left coset of H in G determined by a.

Eg: Find right cosets of the subgroup $\{1, -1\}$ of the group $\{1, -1, i, -i\}$ under multiplication.

Soln $G = \{1, -1, i, -i\}$ is a group under multiplication

$H = \{1, -1\}$ subgroup of G

The right coset of H in G are $H1$, $H(-1)$, Hi, $H(-i)$

$H \cdot 1 = \{1(1), -1(1)\} = \{1, -1\} = H$

$H(-1) = \{1(-1), -1(-1)\} = \{-1, 1\} = H$

$Hi = \{1(i), -1(i)\} = \{i, -i\}$

$H(-i) = \{1(-i), -1(-i)\} = \{-i, i\}$.

Imp Theorem 37 State and Prove Lagrange's Theorem.

Statement:- The order of each subgroup of a finite group is a divisor of the order of the group.

Proof:- Let G be a group of finite order n.
Let H be a subgroup of G & $O(H) = m$.
Suppose $h_1, h_2, \ldots, h_m$ be m distinct members of H.
Let $a \in G$. Then Ha is a right coset of H in G & we have $Ha = \{h_1a, h_2a, \ldots, h_ma\}$
Ha has m distinct members, since if $h_ia = h_ja$; $1 \le i, j \le m$; $i \ne j$

By right cancellation law
$\Rightarrow h_i = h_j$, a contradiction.
$\therefore$ each right coset of H in G has m distinct members.

Any two distinct right cosets of H in G are dis
Since G is finite group, the number of distinct right cosets of H in G will be finite, (say) equal to k
The union of these k distinct right cosets of H in G ~~will be finite~~ equal to G, Thus if
$Ha_1, Ha_2, \ldots, Ha_k$ are the distinct right cosets of H i
then $G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k$.

No. of elements in G = No. of elements in Ha_1 + No. of elements Ha_2 + ... + No. of elements in Ha_k

$O(G) = km \Rightarrow n = km \Rightarrow \boxed{k = \frac{n}{m}}$ $\quad$ [$\because Ha_i \cap Ha_j = \phi$]

m is divisor of n.
$O(H)$ is a divisor of $O(G)$.

— Hence Proved —

Cyclic Group: A group G is called cyclic if $\exists$ $a \in G$ s.t each element of G can be written as an integral power of a ie if $b \in G$, then $a \in G$ s.t $b = a^n$ for some integer n.

a is then called a generator of G.

It is denoted by $G = \langle a \rangle$.

group G

Theorem 27 Prove that every cyclic group is Abelian.

Proof: Consider a cyclic group generated by i.e. $G = \langle a \rangle$

let $x, y \in G$ be arbitrary elements.

$\therefore$ $x = a^n$ & $y = a^m$, for some integers n & m.

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

$\Rightarrow \boxed{xy = yx}$

$\therefore$ G is an abelian group.

<u>Normal</u> <u>Subgroup</u> :- A subgroup H of a group G is called normal subgroup of G iff $ghg^{-1} \in H$, for every $h \in H$, $g \in G$.

heorem 8) Show that intersection of two normal subgroups of G is a normal subgroup of G.

Solⁿ Let H and K are two normal subgroups of G

$\Rightarrow$ H & K are subgroups of G

$\therefore$ $H \cap K$ is also subgroup of G.

Prove! $H \cap K$ is normal subgroup of G.

Let $x \in G$ be any arbitrary element.

& Let $h \in H \cap K$.

$\Rightarrow$ $h \in H$ and $h \in K$.

But H is normal subgroup of G

$\therefore$ $x \in G$ & $h \in H$

$\Rightarrow$ $xhx^{-1} \in H$ —— (1)

Also K is normal subgroup of G.

$\therefore$ $x \in G$ & $h \in K$

$\Rightarrow$ $xhx^{-1} \in K$ —— (2).

from (1) & (2), we get

$xhx^{-1} \in H \cap K$.

$\therefore$ $H \cap K$ is also normal subgroup of G.

Hence Proved.

$\Rightarrow g$

Q: Every subgroup of abelian group is normal subgroup

Sol: Let H is subgroup of abelian group G

Let $h \in H \Rightarrow h \in G$ $\quad (H \subseteq G)$

Let $g \in G$

$\Rightarrow gh = hg$ [$\because$ G is an abelian group.

Post multiply by g^{-1}, we get

$ghg^{-1} = (hg) g^{-1}$

$\Rightarrow ghg^{-1} = h(gg^{-1})$

$\Rightarrow ghg^{-1} = h \in H.$ [$\because gg^{-1} = e$]

$\Rightarrow ghg^{-1} \in H$

$\therefore$ H is a normal subgroup

Hence Proved.

...7 Let G be a group & H be subgro...

Homomorphism :- ~~A let G~~ Let $<G, o>$ & $<G', *>$ be Two groups. Then the mapping $f : G \to G'$ is called a homomorphism if

$$f(a o b) = f(a) * f(b) \quad , \forall a, b \in G.$$

Isomorphism! A homomorphism which is 1-1 & o[illegible] is called isomorphism.

and onto.

3.1.8 Definition : Kernel of a Homomorphism : Let G and G$'$ be two groups and $f : G \to G'$ be a homomorphism. Then **kernel of f** is defined as follows :–

Kernel of $f = \{x \in G : f(x) = e'\}$, where e' is the identity element of G$'$.

Kernel of f is denoted as **Ker f.**

Let R is non empty set with two binary operation +, × then algebric structure (R, +, ×) is called ring

if ① R is abelian group under '+'

2.) R is semigroup under '×'

3.) Distributive Law

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

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

Field

① R is abelian group under '+'

② R is abelian group under '∘'

③ Distributive Law.

Zero divisor: An element of $a \in R$ is called zero divisor if $\exists\ b \neq 0$ such that $ab = 0 = ba$

* Integrial domain :- A commutative ring R is called an integral domain ~~if~~ ~~Resbase~~

$\forall\ a, b \in R$, If $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$

or If $a \neq 0$, $b \neq 0$ then $ab \neq 0$.

Theorem 4: Every field is an Integral Domain. But Converse is not true.

Proof: Let F be a field & $a, b \in F$ s.t. $a \neq 0$, & $ab = 0$

Since $a \neq 0 \in F$

$\therefore$ a posses an inverse element.

hence a^{-1} exists in F. Then

$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0 \Rightarrow (a^{-1}a)b = 0.$

$\Rightarrow 1 \cdot b = 0$

$\Rightarrow \boxed{b = 0}$

$\therefore$ F has no zero divisors.

Thus F is a commutative ring with $1 \neq 0$ and without zero divisors.

Hence F is an Integral domain.

converse is not true.

Converse is not true.

Example: The ring $\mathbb{Z}$ of integers is an integral domain which is not a field as every non-zero integer doesnot have inverse in $\mathbb{Z}$ under the operation multiplication.

(4)

Consider $X = \{0, 1, 2, 3, 4, 5, 6;\ a_6 * \cdot\}$ then prove that X is a commutative ring with unity under addition & multiplication modulo 6.

Composition table under addition modulo 6 ie. $(X, +_6)$ & multiplication modulo 6 ie. $(X, \times_6)$ is given by

$(X, +_6)$

$+_6$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6=0
1	1	2	3	4	5	0	1
2	2	3	4	5	0	1	2
3	3	4	5	0	1	2	3
4	4	5	0	1	2	3	4
5	5	0	1	2	3	4	5
6	0	1	2	3	4	5	0

Closure property holds :-

$x, y \in X \Rightarrow x +_6 y \in X$

Associative property holds

$\forall x, y, z \in X$

$\Rightarrow x +_6 (y +_6 z) = (x +_6 y) +_6 z$.

Existence of identity :

As 1st row & 2nd row of table is same $\Rightarrow 0$ is left identity.

ly 1st column & 2nd column of table is same $\Rightarrow 0$ is right identity $\Rightarrow 0$ is identity element under addition modulo 6.

$(X, \times_6)$

$\times_6$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	0
2	0	2	4	0	2	4	0
3	0	3	0	3	0	3	0
4	0	4	2	0	4	2	0
5	0	5	4	3	2	1	0
6	0	0	0	0	0	0	0

1) Closure property holds as $\forall x, y \in X \Rightarrow x \times_6 y \in X$.

2) Associative property holds $\because \forall x, y, z \in X$

$\Rightarrow x \times_6 (y \times_6 z) = (x \times_6 y) \times_6 z$.

3) Distributive property also holds as $\forall x, y, z \in X$

$x \times_6 (y +_6 z) = (x \times_6 y) +_6 (x \times_6 z)$

& $(x +_6 y) \times_6 z = (x \times_6 z) +_6 (y \times_6 z)$.

4) Commutative property holds $\because \forall x, y \in X$

$\Rightarrow x \times_6 y = y \times_6 x$.

4) Existence of Inverse: In each row & each column we get exactly only one zero therefore inverse of each element exists ie. $\forall x \in X \; \exists y \in X$ s.t. $x +_6 y = e = y +_6 x$.

5) Commutative property: Matrix is symmetric about its diagonal therefore commutative property holds under addition modulo 6 ie $\forall x, y \in X$.

$x +_6 y = y +_6 x$.

Hence $(\mathbb{Z}_6, *\cdot)$ is commutative ring.

Ques37:- Let G be group of real no.'s under addition & let G' " " "+ve" " " multiplication. Prove that mapping $f: G \to G'$ defined by $f(a) = 2^a$ is homomorphism.

Sol^n: Give $f: G \to G'$ defined by $f(a) = 2^a$, $\forall a \in G$ (set of real no's)

Here G be a group under addition & G' is a group under multiplication.

Let $a_1, a_2 \in G$.

$\therefore f(a_1) = 2^{a_1}$, $f(a_2) = 2^{a_2}$.

$f(a_1 + a_2) = 2^{a_1 + a_2} = 2^{a_1} \cdot 2^{a_2} = f(a_1) f(a_2)$

$\Rightarrow f(a_1 + a_2) = f(a_1) \cdot f(a_2) \quad \forall a_1, a_2 \in G$

$\therefore f$ is a homomorphism.

Hence Proved.

X

Ques Consider the group $G = \{0, 1, 2, 4, 5\}$ $+_6$

(a) find multiplication table of G.

(b) prove that G is a group.

Ques State & prove fundamental theorem of group homomorphism.

Fundamental Theorem on Homomorphism :-

Statement :- Let G and G' be two groups and $f : G \to G'$ Homomorphism of G onto G'.

If H is a kernal of f then

$$G/H \cong G'.$$

OR

Every Homomorphic image of a group is isomorphic to some quotient group of G.

Proof :- Given that f is homomorphism from $G \to G'$

i.e. $f(xy) = f(x) \cdot f(y)$

Also H is kernal of f

Define $\theta : G/H \longrightarrow G'$

by $\theta(Hx) = f(x)$, $H \Rightarrow \ker f$.

We have to show that θ is well defined, Homo, One-one and onto.

θ is well defined :-

Consider $Hx = Hy$.

$xy^{-1} \in H = \ker f$

$f(xy^{-1}) = e$, $e \in G'$

f is Homo.

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

$\Rightarrow f(x) = f(y)$

$\Rightarrow \theta(Hx) = \theta(Hy)$

$\therefore \theta$ is well defined.

θ is Homomorphism

Consider

$\theta(Hx Hy) = \theta(Hxy)$

$= f(xy)$

$= f(x) f(y)$

$= \theta(Hx)\,\theta(Hy)$

θ is Homo.

θ is One-One.

Let $\theta(Hx) = \theta(Hy)$

$f(x) = f(y)$

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

$f(xy^{-1}) = e.$

$xy^{-1} \in H = \ker f$

$\Rightarrow Kx = Ky.$

θ is Onto:-

Let $y \in G'$.

Since G' is the image of G under f

$\therefore \exists\ x \in G$ st $f(x) = y.$

$\Rightarrow \theta(Hx) = y.$ $[\because f(x) = \theta(Hx)$

$\Rightarrow \theta$ is onto.

Hence we have proved that θ is One-one, Homo, and onto

$\therefore G/H \cong G'.$

Scanned by CamScanner