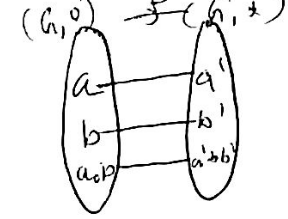
# * Homomorphism of Groups:-

→ Let $(G, \circ)$ be a group & $(G', *)$ be another group then a mapping $f: (G, \circ) \to (G', *)$ is said to be homomorphism if $f(a \circ b) = f(a) * f(b)$

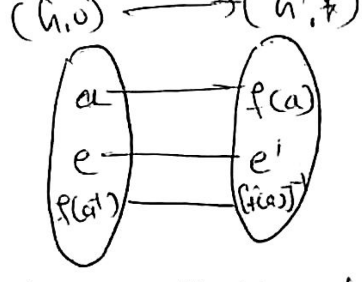



i.e combine first elements a & b of G with operation 'o' and then take the f image or first take f images of a & b i.e a', b' from G' and combine them by '*' operation i.e. $a' * b'$. If the resultant is same it is known as f preserves composition and f mapping is known as homomorphism from group $(G, \circ)$ to group $(G', *)$ and two groups G & G' are called homomorphic to each other.

# * Properties of Group Homomorphism :-

1) $f(e) = e'$ (Identities corresponds)

2) $f(a^{-1}) = [f(a)]^{-1}$ (Inverse corresponds)




Proof:- 1) Let $a \in G$, then $f(a) \in G'$.

$f(a) * e' = f(a)$ ($e'$ is identity of $G'$)

$= f(a \circ e)$ (e is " " G)

$= f(a) * f(e)$ (f is homo.)

$\Rightarrow e' = f(e)$ (As $G'$ is group, by left cancellation law).

2) Let $a \in G$, then $a^{-1} \in G$, as G is group.

Also $e' = f(e)$. $f(a \circ a^{-1}) = f(a) * f(a^{-1})$

$\Rightarrow f(a^{-1}) = [f(a)]^{-1}$

①.

**Ex:-** Let $G$ be a group with identity $e$. Show that function $f : G \to G$ defined by $f(a) = e$ for all $a \in G$ is a homomorphism. $f(a \circ b) = f(a) * f(b)$

$f : (G, \circ) \to (G', *)$

**Soln:-** $f : G \to G$, $f(a) = e$, $\forall a \in G$.

We have to prove that $f$ is a homomorphism.

Let $a, b \in G$.

Then $f(ab) = e = e\,e = f(a) . f(b)$

$\therefore$ $f$ is a homomorphism.

**Ex:-** Consider the two algebraic systems: $(I, \cdot)$ where $I$ is the set of all integers $\cdot$ is a ordinary multiplication operation of integers. $(B, \odot)$ where $B$ is set of all integers & $\odot$ is defined as

| $\odot$ | Positive | Negative | zero. |
|---|---|---|---|
| positive | Positive | Negative | zero |
| Negative | Negative | Positive | zero |
| zero | Zero. | zero. | zero. |

Show that $(I, \cdot)$ is homomorphic image of $(B, \odot)$.

**Soln:-** Let $a$ & $b$ any two elements of $B$.

We have to show that, $f : \underset{B}{G} \to \underset{I}{G'}$

if $f$ is a mapping from $(B, \odot)$ to $(I, \cdot)$.

i.e. $f : (B, \odot) \to (I, \cdot)$

Then $f$ is a homomorphism. To show that $f$ is a homomorphism from $B$ to $I$. We have to show that $f$ preserves composition.

i.e. $f(a \odot b) = f(a) \cdot f(b)$

Let $f(a) = a'$.

Where $a'$ is positive integer when $a$ is (+)ve, $a'$ is (-)ve integer when $a$ is negative and also $a' = 0$ when $a$ is zero.

Case:-1 If $a$ & $b$ both are positive then $a \odot b$ is positive integer.

Hence, $f(a \odot b) =$ Positive integer $= a' \cdot b'$.

Hence, $f(a \odot b) = f(a) \cdot f(b)$

Case:-2 If $a$ & $b$ both are negative then $a \odot b$ is positive integer.

Hence $f(a \odot b) =$ Positive integer

$= a' \cdot b'$ ($a'$ & $b'$ are (-)ve but the product is (+)ve).

$= f(a) \cdot f(b)$.

Case:-3 $a$ is positive and $b$ is negative.

i.e $a > 0, b < 0$, hence $a \odot b$ is negative

then $a' > 0$, $b' < 0$, $a' \cdot b' < 0$

And $f(a \odot b) =$ negative integer.

$= a' \cdot b' < 0$.

Hence $f(a \odot b) = f(a) \cdot f(b)$.

Case:- 4 $a=0$, $b=0$ then $a'=0$, $b'=0$, $a \odot b = 0$.

and $f(a \odot b) = 0 = a' \cdot b' = f(a) \cdot f(b)$

$\therefore$ f is a homomorphism from $(B, \odot)$ to $(I, \cdot)$.

Hence $(I, \cdot)$ is homomorphic image of $(B, \odot)$.

## *. Rings :-

Suppose R is a nonempty set equipped with two binary operation called addition and multiplication and denoted by '+' and '$\cdot$' respectively.

Then the algebraic structure $(R, +, \cdot)$ is known as ring if the following axioms (postulates) are satisfied.

1) $(R, +)$ is an abelian group.

i.e closure property for '+'.

i) $\forall a, b \in R \Rightarrow a+b \in R$.

ii) Associative property for '+'.

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

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

iii) Existence of identity element for '+'.

$\forall a \in R \;\; \exists \; 0 \in R$

such that $a + 0 = a = 0 + a$

0 is known as additive identity or zero element of the ring

(iv) Existence of inverse element for '+'.

$\forall\ a \in R,\ \exists\ -a \in R$.

such that $a + (-a) = 0 = -a + a$.

$-a$ is known as additive inverse of $a$.

2) $(R, \cdot)$ is a semi group.

(i) closure property for '$\cdot$'.

$\forall\ a, b \in R \Rightarrow a \cdot b \in R$.

(ii) Associative property for '$\cdot$'.

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

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

3) Multiplication '$\cdot$' distributes over addition '+' from left and also from right.

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

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

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

Eg:1) $(I, +, \cdot)$ is a ring

as 1) $(I, +)$ is an abelian group.

2) $(I, \cdot)$ is a semi group.

3) Multiplication distributes over addition.

i) $2 \cdot (3 + 4) = 2 \cdot 3 + 2 \cdot 4$

Also $(3 + 5) \cdot 2 = 3 \cdot 2 + 5 \cdot 2$

Eg:-2) $(Q, +, \cdot)$ is a ring.

Eg:-3) $(\mathbb{R}, +, \cdot)$ is a ring

Eg:-4 $(\mathbb{C}, +, \cdot)$ is a ring

* **Commutative Ring:-**

Ring $(R,+,\circ)$ is a commutative ring if $\forall\ a,b \in R$, $a.b = b.a$

Eg. $(I,+,\circ)$

* **Ring With Unity:-**

→ Ring $(R,+,\circ)$ is known as ring with unity if $\forall a \in R\ \exists\ 1 \in R.\ \ni\ a.1 = a = 1.a$.

eg. $(I,+,\circ)$

* **Commutative ring with Unity:-**

→ Ring $(R,+,\circ)$ is a commutative ring with unity, if $\forall a,b \in R$, $a.b = b.a$ and $\forall\ a \in R\ \exists\ 1 \in R\ \ni\ a.1 = a = 1.a$

Ex:- Set M of $2\times 2$ matrices where entries of matrices are real numbers ~~from~~ form a ring with unity with respect to addition $(+)$ and multiplication $(\cdot)$ of matrices.

Solⁿ:- 1) Let $A$ & $B \in M$.

Then $A+B \in M$ and $A.B \in M$.

So M is closed with respect to addition and multiplication of matrices.

2) $A, B, C \in M$.

Then $A+(B+C) = (A+B)+C$ Also, $A.(B.C) = (A.B).C$

Hence addition '+' and multiplication '$\cdot$' operations are associative on $M$.

3) Existence of identity for addition.

$\exists \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O \in M$.

Such that $A+O = A = O+A$.

4) $\exists \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \in M$

such that $A \cdot I = A = I \cdot A$

$I$ is multiplicative identity element of $M$.

5) Existence of additive inverse:-

$\forall A \in M \ \exists \ B \in M$

such that $A+B = O = B+A$.

6) Commutative property for addition.

$\forall A, B \in M$, $A+B = B+A$.

7) Distributive laws:-

$\forall A, B, C \in M$, $A \cdot (B+C) = A \cdot B + A \cdot C$

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

Hence $(M, +, \cdot)$ is a ring with unity.

* Properties of a Ring:-

→ If $R$ is a ring, then for all $a, b, c \in R$.

i) $a \cdot 0 = 0 \cdot a = 0$

ii) $a \cdot (-b) = -(ab) = (-a)b$

iii) $(-a) \cdot (-b) = a \cdot b$

iv) $a \cdot (b-c) = ab - ac$

v) $(b-c)\, a = b \cdot a - c \cdot a$