Module 4

18/03/2021

- extension of ~~ring~~ group theory

Ring Theory

Ring :- Let R be a non empty set over which two binary operation '+' & '·' are defined then R is called a ring if following property are satisfied.

1) R is an abelian group unde '+'

i.e. G_1 : $a, b \in R \Rightarrow a+b \in R$

G_2 : $a+(b+c) = (a+b)+c \quad [\forall\, a,b,c \in R]$

G_3 : $\exists\, 0 \in R$ such that $a+0 = 0+a = a \;\forall\, a \in R$

G_4 : for every $a \in R$

$\exists\, (-a) \in R$ such that

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

0 → zero element of R

$G_5 \Rightarrow a+b = b+a \quad \forall a,b \in R.$

2) Under '·' following properties are satisfied.

(semigroup) → G_1 & G_2 + distributive laws.

i) $a,b \in R \Rightarrow ab \in R$: G_1

ii) $a\cdot(b\cdot c) = (a\cdot b)\cdot c$: G_2

iii) $a\cdot(b+c) = a\cdot b + a\cdot c$: Left distributive law

iv) $(b+c)\cdot a = b\cdot a + c\cdot a$: right distributive law

[R is also called associative ring]

Unit element :- If there exist an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a \quad \forall a \in R$
then one (1) is called the unit element of ring R and ring R is called ring with unit element

with respect to '+' : e = zero element

with respect to '.' : e = unit element.

for '.' if G3 also holds then R is called ring with unit element.

Commutative ring:

if '.' is commutative in R i.e. $a \cdot b = b \cdot a \quad \forall a, b \in R$
the R is called commutative ring.

eg of rings:

1) The set of all integers Z is a ring under the binary operation of usual addition & multiplication
commutative ring → yes
ring with unit element → yes
2) The set of all rational no. Q is a ring under binary operation of usual addition and multiplication.

HW

$(Z_7, +_7, \cdot_7)$

integers modulo 7

$Z = \{0, 1, 2, 3, 4, 5, 6\}$

9/03/2021

$(R, +, \cdot)$ is a ring if R is

1) Abelian grp w.r.t. '+'
2) semigroup w.r.t '.'
3) distributive laws.
   i) $a \cdot (b+c) = a \cdot b + a \cdot c$
   ii) $(a \cdot b) + c = (a \cdot c) + b \cdot c$, $\forall\ a, b, c \in R$

$(Z_7, +_7, \cdot_7)$ → ring [commutative ring with unity]

$(Z_6, +_6, \cdot_6)$ → ring —11—

—x—x—

Ring with zero divisors

Let a, b are two non-zero elements of $(R, +, \cdot)$

[zero element is an identity element w.r.t first binary operation in R
unit element (if exist) is an identity element w.r.t. second binary operation '.'
]

$a \cdot b = 0$

then R is said to be ring with zero divisors.

eg:- let $(Z_6, +_6, \cdot_6)$ be a ring

$$2 \cdot_6 3 = \text{rem}\left[\frac{2 \times 3}{6}\right] = 0$$

$\therefore$ 2 is zero divisor of 3 (vice-versa)
and $(Z_6, +_6, \cdot_6)$ is a ring with zero divisor.

for $(Z_7, +_7, \cdot_7)$ is not a ring with zero divisor.

Ex. let $(M_{2\times2}(Z), +, \cdot)$ be a ring.

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times$$

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \rightarrow \text{zero element}$$

$\therefore (M_{2\times2}(Z), +, \cdot)$ is a ring with zero divisor.

Integral domain

A ring is said to be an integral domain if.

i) commutative ring with unit element.

[$(R, +)$ G1 - G5

$(R, \cdot)$ G1, G2, G5 & G3

+ distributive laws]

ii) is without zero divisor.

Example

$(Z_7, +_7, \cdot_7)$ is an integral domain. (for without zero)

whenever $a\,b = 0$

either $a = 0$

or $b = 0$

Example $(Z, +, \cdot)$ - yes it is

i) $(Z, +, \cdot)$ is commutative ring with unit element (1)

ii) $a \cdot b = 0$ only if $a = 0$ or $b = 0$

i.e. ring without zero divisor.

Example $(R, +, \cdot)$ -

i) $(R, +, \cdot)$ commutative ring with unit element 1

ii) $a \cdot b = 0$ only if $a = 0$ / $b = 0$

ie ring without zero divisor.

Example $(M_{2\times 2}(\mathbb{Z}), +, \cdot)$ Not an integral domain.

—x— x —

Division Ring

i) $(R, +)$ abelian group
ii) $(R, \cdot)$ G_1, G_2, G_3, [G_4 for non-zero elements]
iii) distributive laws for $\cdot$.

eg:- i) $(\mathbb{Z}, +, \cdot)$

zero element $= 0$, 1 = unit element of $\mathbb{Z}$.

G_4 property :- $a \cdot x = 1$

$\downarrow$ $1/a \notin \mathbb{Z}$

(multiplicative inverse)

$\therefore$ G_4 does not hold

$a \cdot x = 1$

$\therefore x = \frac{1}{a}$

but $\frac{1}{a} \notin \mathbb{Z}$.

? not a division ring.

eg:- 2) $(R, +, \cdot)$

- yes it is a division ring.

Field

i) A commutative division ~~div~~ ring is called as a field

ie. a) $(R,+)$ abelian grp

b) $(R,\cdot)$ abelian grp → (G.I for non-zero elements)

c) Distributive laws.

eg) 1) $(R,+,\cdot)$

2) complex nos. w.r.t usual addition & multiplication.

H.W.

$$A = \{ a+b\sqrt{2} \mid a,b \in z \}$$

i) is $(A,+,\cdot)$ a ring ?

ii) is $(A,+,\cdot)$ a commutative ring ?

iii) Is $(A,+,\cdot)$ ring with unit element ?

iv) Is $(A,+,\cdot)$ with zero divisor ?

v) Is $(A,+,\cdot)$ an integral domain ?

vi) Is $(A,+,\cdot)$ division ring ?

vii) Is $(A,+,\cdot)$ a field ?

$(R, +, \cdot)$ hyd

Example If R is a boolean ring

$(a^2 = a \;,\; \forall a \in R)$ → $a \cdot a$

prove that

1) $x + x = 0 \quad \forall x \in R$ — every element is inverse of itself

2) $x + y = 0 \Rightarrow x = y$

3) R is commutative ring.

Soln:-

1) let $x \in R$,

$\Rightarrow x + x \in R$ [by Cl property]

$\therefore (x+x)^2 = x + x$

$\Rightarrow (x+x)(x+x) = (x+x)$

$\Rightarrow x \cdot (x+x) + x \cdot (x+x) = x + x$

$\Rightarrow x \cdot x + x \cdot x + x \cdot x + x \cdot x = x + x$

$\Rightarrow x + x + x + x = x + x$

$\Rightarrow (x+x) + (x+x) = (x+x) + 0$

by left cancellation law. ($x+x$) ka inverse liya on both side so $x+x$ cancel hoEgaya

$(x+x) = 0$

2) Given:- $x + y = 0$ to prove $x = y$

$\because x + y = 0$

$\Rightarrow x + y = x + x$

$\Rightarrow$ by left cancellation law

$y = x$

iii) to prove :- R is commutative ring

to prove :- $x \cdot y = y x$.

Let $(x, y) \in R$

$\Rightarrow x+y \in R$.

$\therefore (x+y)^2 = x+y$

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

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

$\Rightarrow x \cdot x + x \cdot y + y \cdot x + y \cdot y = x+y$

$\Rightarrow x + x \cdot y + y \cdot x + y = x + 0 + y$.

$\Rightarrow x \cdot y + y \cdot x = 0$ (by left cancellation & right cancellation law)

by second part.

$x \cdot y = y \cdot x$

H.P.

20/03/2021

Page No.
Date

Q.x) Let A be the set of all integeres with composition $\circ$ & $*$ defined by.

$$a \circ b = a+b+1$$
$$a * b = ab+a+b$$

i) Is $(A, \circ, *)$ a commutative ring with unit element?

Soln:- primary → $\circ$ be abelian
$*$ must satisfy G1 G2 G5 + G3 (with unit element) + distributive laws.

i) To prove $(A, \circ)$ is abelian group.

G1 : let $a, b \in A$
$a \circ b = a+b+1$ is an integer
$\therefore a \circ b \in A$
G1 holds

G2 let $a, b, c \in A$
$a \circ (b \circ c) = a \circ (b+c+1)$
$= a + (b+c+1) + 1$
$= a+b+c+2$

$(a \circ b) \circ c = (a+b+1) \circ c$
$= a+b+1+c+1$
$= a+b+c+2$

G3 $a \circ \boxed{-1} = ?\ a$
$\Rightarrow a - 1 + 1 = a$
$\therefore -1$ is the zero element of A
G3 holds.

[G4] let $a \in G$

$a \circ x = -1$

$a + x + 1 = -1$

$x = -2 - a$

$\therefore x = (-a-2)$ which is integer.

$\therefore -a-2$ is an inverse of a w.r.t. '$\circ$'

$\therefore$ G5 holds.

[G5] $a \circ b = a + b + 1$

$b \circ a = b + a + 1$

$= a + b + 1$

$\forall a, b \in G$

$\therefore G_5$ holds

Thus $(A, \circ)$ is an abelian group.

(B) To prove $(A, *)$ is commutative monoid.

[G1] let $a, b \in A$.

$a * b = ab + a + b$ is also an integer.

$\therefore a * b \in A$

$\therefore$ G1 holds

[G2] let $a, b, c \in A$.

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

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

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

Page No.
Date

~~let~~

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

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

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

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

$\therefore$ G2 holds.

G3 let $a \in A$.

$\exists\, 0 \in A$ such that:

$a*0 = a$

$0+a+0 = a$

$\therefore$ '0' is the unit element of A

G3 holds

G5 $a*b = ab+a+b = ba+a+b = b*a$

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

$\therefore$ G5 holds.

Distributive laws $(R, +, \cdot) \rightarrow$ i) $a(b+c) = a\cdot b + a\cdot c$

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

let $a, b, c \in A$

$a*(b \circ c) =$ } should be

$(a*b) \circ (a*c) =$ } same

$$a*(b\circ c) = a*(b+c+1)$$
$$= a(b+c+1) + a + (b+c+1)$$
$$= ab + ac + a + a + b + c + 1$$
$$= ab + ac + 2a + b + c + 1$$

$$(a*b)\circ(a*c) = (ab+a+b)\circ(ac+a+0)$$
$$= (ab+a+b)+(ac+a+0)+1$$
$$= ab + a + b + ac + a + 1 + 1$$
$$= ab + ac + 2a + b + c + 1$$

$\therefore$ left distributive law hold

similarly

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

— holds right distributive element.

(4W)

Is it a ring with zero divisor?

$(A, \circ, *)$

zero element $= -1$

two non-zero element $\in A$

$a, b \in A$.

$a*b = -1$

$ab + a + b = -1$

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

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

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

$$= \frac{-(1+b)}{(1+b)} = -1$$

but $a = -1$ i.e. zero element.

so we observe that.

$a * b = -1$

any one of them will be -1 to satisfy this condition.

$\therefore$ $A, 0, *$ is not a ring with zero divisor.

Is it an integral domain?

- commutative ring with unit element
  +
  ring with no zero divisor

As $(A, 0, *)$ is commutative ring with unit element and without zero divisor.

$\therefore$ $(A, 0, *)$ is integral domain

Is it a division ring?

$a * b = 0$.

$ax + a + x = 0$.

$a(x+1) + x = 0$. $\Rightarrow$ $a(x+1) = -x$

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

$$ax + a + x = 0.$$

$$ax + x = -a$$

$$x(a+1) = -a$$

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

but $\frac{-a}{a+1}$ is not an integer always.

$\therefore$ G4 does not hold

$\therefore$ it is not a divison ring

also; $\because$ it is not a field.

—— x —— x —— x ——

Ex. Prove that every field is an integral domain.

Proof:- given $(R, +, \cdot)$ – bydefault is a field.

To prove :- $(R, +, \cdot)$ is an integral domain.

commutative ring with unit element and without zero divisors.

for integral domain :- [$(R, +)$ G1 – G5

$(R, \cdot)$ G1, G2, G3, G5

distributive laws.

$a \cdot b = 0$

$\Rightarrow a = 0$ or $b = 0$

for field :- commutative division ring.

[$(R, +)$ G1 - G5

$(R, \cdot)$ G1. - G5 G4 for non-zero elements.

Distributive laws.

].

Now to prove (else are already present)

$a, b \in R$

$\downarrow$

$a \cdot b = 0$ — ①.

$a = 0$ or $b = 0$

Let us assume that $a \neq 0$ (i.e. non-zero element is a)

$\therefore a^{-1}$ exists.

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

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

$\Rightarrow e\,b = 0$.

$\downarrow$

here 1

$\Rightarrow b = 0$.

Hy if we assume $b \neq 0$ we can prove $a = 0$.

Thus, $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$

General proof.

$a \cdot 0 = 0$.

LHS.

$a \cdot 0 = a \cdot (0 + 0)$

$= a \cdot 0 + a \cdot 0$

$a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$.

$-a$ $-a$ [left cancellation]

$0 = a \cdot 0$

$\therefore (R, +, \cdot)$ is an integral domain.

∴ Every field is an intergral domain

Ex. Prove that every finite integral domain is a field.

we have to prove whether $(R, +, \cdot)$ satisfies G4 or not for non-zero element.

i.e. find unit element.

Proof:- let $D = \{a_1, \ldots, a_n\}$ and $(D, +, \cdot)$ is an integral domain.

$|D| = n$ [finite]

such that all element are distinct.

$a_i \neq a_j$ for $i \neq j$. $i = j = 1, 2, \ldots n$

let $x \neq 0$ be an element of D.

↓

non-zero member.

then $xa_1, xa_2, \ldots, xa_n \in D$

[as G1 holds]

↓

all elements are distinct.

we can prove this by contradiction.

let $xa_i = xa_j$, $i \neq j$

$\Rightarrow xa_i - xa_j = xa_j - xa_j$ (G4 of +)

$\Rightarrow x \cdot (a_i - a_j) = 0.$

as we've integeral domain.

$ab = 0 \Rightarrow a = 0 \;/\; b = 0.$

Since $x \neq 0$

$\therefore a_i - a_j = 0.$

$\Rightarrow a_i = a_j$

i.e. a contradiction to the fact that $|D| = n$.

$\therefore$ we can write

$D = \{a_1, a_2, \cdots a_n\} = \{xa_1, xa_2, xa_3, \cdots xa_n\}.$

in particular $a_i = xa_j.$

$x \in D$

$\therefore x = xa_k$ for some 'k' $< n$

know we prove,

a_k is unit element.

[let $y \in D$

to prove $ya_k = y$]

let $y \in D$

$\therefore y = xa_j$ for some $j \leq n$

$y \cdot a_k = (xa_j) \cdot a_k$

$= a_j x \cdot a_k$ (G5 holds w.r.t '.')

$= a_j (x a_k)$ (G2 holds w.r.t. '.')

$= a_j x$

$= x a_j$ (G5 ..... '.')

$= y$

$\therefore a_k$ is unit element of D.

$x \neq 0$ in D.

$a_k = x\, a_m$

$1 = x\, a_m = a_m \cdot x$

$x^{-1} = a_m$. (w.r.t $\cdot$)

i.e. $x \neq 0$
then x^{-1} exists.

$\therefore$ D is a field.

25/03/2021

subring

i) $S \neq \phi$ → $a, b \in S$ and $a - b \in S$

ii) $(S, +)$ is a subgroup of $(R, +)$

iii) S is closed under '.' (i.e. G1 property)

↳ $a, b \in S$

$\therefore ab \in S$.

Q:-

i) $(\mathbb{Q}, +, \cdot)$ Ring of Rational no.

$\because (\mathbb{Z}, +, \cdot)$ is a ring and subset of $(\mathbb{Q})$

$\therefore (\mathbb{Z}, +, \cdot)$ is a subring.

ii) Consider a ring $(M_2(\mathbb{Z}), +, \cdot)$

$$A = \left\{ \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} / x \in \mathbb{Z} \right\}$$

at least one element should be present in A

i.e. identity element of $M_2(\mathbb{Z})$ w.r.t $+$

$\because 0 \in Z$

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in A$ and $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(Z)$

$\therefore A$ is non-empty subset of $M_2(Z)$

let $x = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}, y \begin{bmatrix} y & 0 \\ 0 & 0 \end{bmatrix} \in A$

Now

$$x - y = \begin{bmatrix} x-y & 0 \\ 0 & 0 \end{bmatrix} \in A \quad \because x - y \in Z$$

and

$$x \cdot y = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} y & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} xy & 0 \\ 0 & 0 \end{bmatrix} \in A \quad \text{w.r.t} \because$$

A is subgroup of $(G, *)$

if

1) $a, b \in A \Rightarrow a * b \in A$
2) $b \in A \Rightarrow b^{-1} \in A$

— x — x —

A is subgroup of $(G, +)$

1) $a, b \in A \Rightarrow a + b \in A$
2) $b \in A \Rightarrow -b \in A$

$\therefore a, b \in A \Rightarrow a - b \in A$

(in short)

— x — x — x —

Prove/disprove

1) Intersection two subring is a subring — prove
2) Union of two subring is a subring — disprove.

— x — x — x —

Ideal

$a - b \in A$
$\Uparrow$
$a, b \in A$

Let A be a non-empty subset of ring R such that A is an Additive subgroup of R then

i) A is a left ideal of R iff
$r a \in A \quad \forall a \in A$
$r \in R.$

ii) A is right ideal of R iff
$aR = A$, $\forall a \in A, R \in R$.

iii) A is an ideal of R iff it is both right & left ideal of R.

eg>

i)

for eg:-

let $(Z, +, \cdot)$ is a ring
& $(2Z, +, \cdot)$ $\longrightarrow$ i) $a, b \in 2Z$
$\Rightarrow a - b \in 2Z$
$\therefore (2Z, +)$ is a subgroup of $(Z, +)$

$\because (2Z, +)$ is a subgroup of $(Z, +)$

Now, let $x \in 2Z$ & $y \in Z$.
then
$xy \in 2Z$ also $yx \in 2Z$.
↓ ↓
2Z is right ideal of Z
2Z is a left ideal of Z.

$\therefore$ 2Z is an ideal of Z.

Page No.
Date

Eg) Consider a ring $(M_2(z), +, \cdot)$ and following subsets.

i) $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / a, b \in z \right\}$

Step 1: Prove A is subgroup w.r.t +.

let $A_1 = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix}$, $A_2 = \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} \in A$.

i.e. $A_1 - A_2 \in A$

$\Rightarrow \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & 0 \end{bmatrix} \in A$

$\because a_1 - a_2$ & $b_1 - b_2 \in z$.

$\therefore$ A is a subgroup of $M_2(z)$ w.r.t '+'
ie $(A, +)$ is a group of $(M_2(z), +)$

Step2

let $A_1 = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} \in A$, $A_2 = \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} \in M_2(z)$

$A_1 \cdot A_2 = \begin{bmatrix} a_1 a_2 & a_1 b_2 \\ 0 & 0 \end{bmatrix}$

$A_2 \cdot A_1 = \begin{bmatrix} a_2 a_1 & b_2 b_1 \\ 0 & 0 \end{bmatrix}$

Page No.
Date

Now

Let $W = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in M_2(z)$

$X = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} \in A.$

$XW = \begin{bmatrix} a_1p + b_1r & a_1q + b_1s \\ 0 & 0 \end{bmatrix} \in A$

$\therefore$ A is right ideal of $M_2(z)$

$WX = \begin{bmatrix} pa_1 & pb_1 \\ ra_1 & rb_1 \end{bmatrix} \notin A.$

$\therefore$ A is not left ideal of $M_2(z)$

HW

ii)

HW

iii)

Prove & disprove.

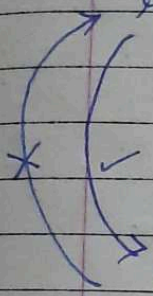
i) An ideal of a ring is a subring - true
ii) Every subring is an ideal of a ring - false.

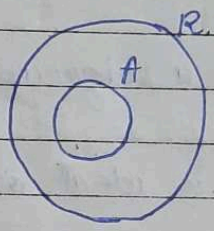
→ $(A, +)$ is a subgroup of $(R, +)$

$ra, ar \in A$

$\forall a \in A$

$r \in R$.





$ra, ar \in A$, $\forall a \in A$
$r \in A$

Q1 W.K.T.

Ex) If R is commutative ring and $a \in R$ then
$Ra = \{ra / r \in R\}$
Is Ra an ideal of R.

i) prove Ra is non-empty?

$0 \in R$.

$0 \cdot a = 0 \in Ra$

as $0 \in R$

$\therefore$ Ra is non-empty subset of R.

ii) Prove Ra is subgroup

let $x, y \in Ra$ where $x = r_1 a$

$y = r_2 a$.

$x - y = r_1 a - r_2 a$

$= r_1 a + (-r_2) a$

$= (r_1 - r_2) a$

$= (r_1 - r_2) a \in Ra$ ($\because r_1, r_2 \in R \Rightarrow r_1 - r_2 \in R$)

$\therefore (Ra, +)$ is a subgroup of R.

iii) Prove if Ra is ideal or not.

~~let~~ $r \in R$

$x \in Ra$

$xr = (r_1 a) r$

$= r_1 (ar)$

$= r_1 (ra)$

$= r_1 r a$ → $\because R$ is commutative.

$= (r_1 r) a \in R$ [if R is not commutative then false]

$\therefore Ra$ is right ideal of R.

$rx = r(r_1 a)$

$= r r_1 a \in Ra$

($\because r, r_1 \in R \Rightarrow r \cdot r_1 \in R$)

$\therefore Ra$ is left ideal of R.

$\therefore$ (Ra is an ideal of R.) → but bcoz of R is a commutative ring

zero element

0

Every ring become its ideal if ring is a commutative ring.

— x — x — x —

Ring Homomorphism

Let $(R, +, \cdot)$ & $(S, \circ, *)$ be two rings.
A mapping $\phi : R \to S$ is said to be ring homomorphism if

i) $\phi(x+y) = \phi(x) \circ \phi(y)$
ii) $\phi(x \cdot y) = \phi(x) * \phi(y)$

Kernel

Let $\phi : R \to S$ is a ring homomorphism. then kernel of ϕ is denoted and defined as,

K or $K\phi$ = { set of all elements of domain whose image under ϕ is zero element of codomain }

$= \{ x \in R \mid \phi(x) = \bar{0}$ where $\bar{0}$ is zero element of codomain $S \}$

representation

R → S

zero element ↓ 0 ; ↓ zero element $\bar{0}$

26/03/2021

$(R, +, \cdot)$ $\xrightarrow{\phi}$ $(\bar{R}, +, \cdot)$

Ex:- Let $\phi : R \to \bar{R}$ be a ring homomorphism with kernel K.
Prove / Disprove K is an ideal of R.

i) Prove K is non-empty subset of R (domain)

∵ K is kernel
$\phi(0) = \bar{0}$

$\phi(e) = \bar{e}$
$\phi(x^{-}) = [\phi(x)]^{-1}$

∴ $0 \in K$
i.e. K is non-empty subset of R.

ii) Prove if K is subgroup or not.

let $x, y \in K$, i.e. $\phi(x) = \bar{0}$
$\phi(y) = \bar{0}$

$\phi(x-y) = \phi(x + (-y))$
$= \phi(x) + \phi(-y)$
$= \phi(x) + [-\phi(y)]$ as $\phi(\vec{x}) = [\phi(x)^{-1}]$
$= \phi(x) - \phi(y)$ ∵ ϕ is homomorphism
$= \bar{0} - \bar{0}$
$= \bar{0}$

∴ $x - y \in K$
∴ K is additive subgroup of R.

iii) Now, $x \in K$, $r \in R$

$\phi(xr) = \phi(x) \cdot \phi(r)$ ($\because \phi$ is homomorphism)

$= \bar{0}\ \phi(r)$ as $\phi(x) = \bar{0}$ bcoz $x \in K$

$= \bar{0} \Rightarrow xr \in K$.

right ideal

Similarly

$\phi(rx) = \phi(r)\phi(x)$

$= \phi(r) \cdot \bar{0}$

$= \bar{0} \rightarrow rx \in K$

left ideal

$\therefore$ K is an ideal

Page No.
Date

Example let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} / a, b \in Z \right\}$ and f be a mapping that takes

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} \longrightarrow a - b$$ (image)

i) Show that f is a ring homomorphism
ii) Determine kernel of f.

Soln:-

domain codomain of mapping

$M_2(Z)$ i.e. R Z

$(Z, +, \cdot)$

$\Rightarrow$ $f : R \longrightarrow Z$ such that $f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = a - b$ (substraction of first row elem)

$(R, +, \cdot)$

we verify

$$f(x+y) = f(x) + f(y)$$
$$f(x \cdot y) = f(x) \cdot f(y)$$

i) Let $X = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$ & $Y = \begin{bmatrix} c & d \\ d & c \end{bmatrix}$

$$f(x+y) = f\left(\begin{bmatrix} a+c & b+d \\ b+d & c+a \end{bmatrix}\right) = (a+c) - (b+d)$$

$f(x+y) \in$ $\therefore x+y \in R$ & $(a+c)-(b+d) \in Z$.

$$f(x)+f(y) = f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) + f\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right)$$

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

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

$$\therefore \boxed{f(x+y) = f(x)+f(y)}$$

ii) $$f(x \cdot y) = f\left(\begin{bmatrix} ac+bd & ad+bc \\ ad+bc & bd+ac \end{bmatrix}\right) = (ac+bd)-(ad+bc)$$

$$f(x) \cdot f(y) = f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) \cdot f\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right)$$

$$= (a-b)\cdot(c-d)$$
$$= ac-ad-bc+bd$$
$$= (ac+bd)-(ad+bc)$$

$$\therefore \boxed{f(x \cdot y) = f(x) \cdot f(y)}$$

Thus, f is a ring homomorphism.

b)

To find kernel:-

$f(x) = 0$ → 0 element of codomain.

i.e. $f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = 0$

$\Rightarrow \quad a - b = 0$

$\Rightarrow \quad a = b$

Thus

$$K = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} / a \in Z \right\}$$

0 element of domain set → null matrix

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$