Ring theory

A algebraic structure $(R, +, \cdot)$ consisting of non-empty set R and two binary operation addition and multiplication is said to be ring provided the following postulates are satisfied.

R① The system $(R, +)$ is an abelian group, so we have the following properties

① Closure property: if $a \in R, b \in R \Rightarrow a+b \in R$, $\forall a, b \in R$.

② Associative property: $\forall a, b, c \in R$, $a+(b+c) = (a+b)+c$.

③ Existence of Identity: $\exists\ 0 \in R$ such that $a+0 = 0+a = a$, $\forall a \in R$.

④ Existence of inverse: $a+(-a) = 0$, $\forall a \in R$, $-a \in R$.

⑤ Commutativity: If $a, b \in R \Rightarrow a+b = b+a$ $\forall a, b \in R$.

R② The system $(R, \cdot)$ is a semigroup

Closure property: If $a \in R, b \in R \Rightarrow a \cdot b \in R$, $\forall a, b \in R$.

Associativity : If $a, b, c \in R \Rightarrow a.(b.c) = (a.b).c$
$\forall\ a, b, c \in R$.

(R3) Distributive law: The multiplication composition is right and left distributive over addition

Right distributive Law: If $a, b, c \in R$
$(a+b).c = ac + bc$, $\forall\ a, b, c \in R$.

Left distributive law : If $a, b, c \in R$
$a(b+c) = ab + ac$, $\forall\ a, b, c \in R$.

Def^n: An algebraic structure $(R, +, \cdot)$ is said to be a ring if (i) $(R, +)$ is abelian group.

(ii) $(R, \cdot)$ is semigroup.

(iii) Multiplication is distributive over addition
$a(b+c) = ab + ac$,
$(b+c)a = ba + ca$.

Eg: $(Z, +, \cdot)$, $(R, +, \cdot)$, $(Z_n, \oplus_n, \otimes_n)$, $(P, +, \cdot)$
$(\ , +, \cdot)$ are rings.

The ring $(Z_n, \oplus_n, \otimes_n)$ is known as modulo ring of integers $(M_n(Z), +, \cdot)$ is also a ring.

① Additive identity is called zero of the ring
Additive inverse of $a \in R$ is $-a$.

② Multiplicative identity if its exists then it is said to be unity of unit element of the ring.

(i) Suppose multiplicative inverse of $a \in R$ exists then a is said to be invertible.

(ii) The multiplicative inverse of a is denoted by a^{-1}, zero element has no inverse.

---

③ Suppose $a, b \in (R, +, \cdot)$ if $a \neq 0$, $b \neq 0$ but $a.b = 0$ then a and b are said to be zero divisors of the ring
a is Left zero divisor and b is called ring zero divisor

Ring has no zero divisors if $a \neq 0, b \neq 0$
$\Rightarrow ab \neq 0$, $\forall a, b \in R$.
In other words, ring has no zero divisors if $ab = 0$ ~~either~~ $a = 0$ or $b = 0$.

Suppose ring has zero divisors then it is said to be a ring with zero divisors

Suppose ring has no zero divisors then it is said to be a ring without zero divisors

If a ring $(R,+,\cdot)$ has unit element then it is said to be ring with unity.

A ring $(R,+,\cdot)$ is said to be commutative ring or abelian ring if multiplication is commutative i.e., $ab=ba$.

A commutative ring with unity and without zero divisors is said to be an integral domain.

A ring with atleast 2 elements in which unity exists and every non-zero element is invertible is known as division ring or skew-field.

A commutative division ring is known as field i.e., a ring $(R,+,\cdot)$ is said to be field if it

* is commutative.
* has unity
* Every non-zero element is invertible.

i.e., $(R,+,\cdot)$ is a field if $(R,+)$ & $(R,\cdot)$ are abelian group

Note: Every field is a division ring but every division ring need not be a field

We say cancellation laws hold in a ring if they hold good w.r.t to multiplication

$a \neq 0$, $ab = ac \Rightarrow b = c$ (LCL)

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

Eg: * $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_n, +_n, \times_n)$, $(\mathbb{C}, +, \cdot)$ are all commutative rings with unity

* $(2\mathbb{Z}, +, \cdot)$ is commutative without unity
* $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are integral domain.
* $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are fields but $(\mathbb{Z}, +, \cdot)$ is not a field (∵ all elements are not invertible)
* $(\mathbb{Z}, +, \cdot)$ is a integral domain not a field
* $(M_2(\mathbb{Z}), +, \cdot)$ is a ring with unity but not commutative and with zero divisors
* $(\mathbb{Z}_6, +_6, \times_6)$ is a commutative ring with unity with zero divisors
* $(\mathbb{Z}_7, +_7, \times_7)$, $(\mathbb{Z}_5, +_5, \times_5)$ are finite integral domains.

$(Z_7, +_7, \times_7)$ is a commutative ring with unity & without zero divisors

---

Theorems:

Let $(R, +, \cdot)$ be a ring then

(i) $a.0 = 0$ → zero of the ring or $0.a = 0$

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

(iii) $(-a)(-b) = ab$

(iv) $a(b-c) = ab - ac \quad \forall\, a, b, c \in R$
$(b-c)a = bc - ca,$

(i) $a.0 = a(0+0) = a.0 + a.0 \quad -(1)$

also $a.0 = a.0 + a.0 \quad -(2)$

(1) & (2) $\Rightarrow$ $a.0 + 0 = a.0 + a.0$

$\Rightarrow a.0 = 0$

$0.a = (0+0)a = 0.a + 0.a \quad -(3)$

(3) & (4) $\Rightarrow$ $0.a = 0.a + 0 \quad -(4)$

$0.a + 0 = 0.a + 0.a$

$\Rightarrow 0.a = 0$

(ii) Consider $a(-b) + ab = a(-b+b) = a.0 = 0$

$ab + a(-b) = a(b + (-b)) = a.0 = 0$

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

$\Rightarrow a(-b)$ is additive inverse of ab

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

Now consider $(-a)b+ab = (-a+a)b = 0.b = 0$

$ab+(-a)b = (a-a)b = 0.b = 0$

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

$\Rightarrow (-a)b$ is the additive inverse of ab

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

(iii) $(-a)(-b)$ put $-b = x$

$= -ax = -(ax) = -a(-b) = -(-ab) = ab$

(iv) $a(b-c) = a[b+(-c)] = ab+a(-c)$

$= ab-ac$

(v) $(b-c)a = [b+(-c)]a = ba+(-c)a$

$= ba-ca$

Theorem (2)

In a ring $(R,+,\cdot)$ cancellation laws holds good iff R is without zero divisors.

Let cancellation laws hold good in $(R,+,\cdot)$

Consider $ab=0$ where $a,b \in R$

Let $a \neq 0$, $ab=0$ $\quad a.0=0$

$ab = a.0$

$\Rightarrow b = 0$

Let $b \neq 0 \Rightarrow ab=0$

$ab = 0.b$

$a = 0$

thus $ab=0 \Rightarrow$ either $a=0$ or $b=0$

i.e., R is without zero divisors.

Conversely, Let R be without zero divisors

Let $ab=ac$ and $a\neq 0$

$$ab-ac = ac-ac$$
$$a(b-c) = 0 \Rightarrow a\neq 0 \Rightarrow b-c=0$$
$$b=c$$

but $a\neq 0$ $\therefore b-c=0$

$\Rightarrow b=c$.

Now, $ba=ca$ and $a\neq 0$

as $a\neq 0$, $b-c=0 \Rightarrow b=c$.

thus $ba=ca \Rightarrow b=c$

Theorem 3: Every field is an integral domain

Let $(R,+,\cdot)$ be a field.

$\Rightarrow$ R is a commutative ring with unity & every non zero element of R is invertible.

To prove: R is without zero divisors

Consider $ab=0$, where $a,b\in R$.

Let $a\neq 0 \Rightarrow a^{-1}$ exists ($\because$ R is a field)

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

let $b \neq 0 \Rightarrow b^{-1}$ exists

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

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

$a.1 = 0 \Rightarrow a = 0$

Then $ab = 0 \Rightarrow a = 0$ or $b = 0$.

$\therefore$ R is without zero divisors.

As R is commutative ring with unity and without zero divisors, hence R is an integral domain.

Note: Converse of the theorem need not be true, Eg: $(\mathbb{Z}, +, \cdot)$ is integral domain but not a field

Let $b \neq 0 \Rightarrow b^{-1}$ exists

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

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

$a.1 = 0 \Rightarrow a = 0$

Then $ab = 0 \Rightarrow a = 0$ or $b = 0$.

∴ R is without zero divisors.

As R is commutative ring with unity and without zero divisors, hence R is an integral domain.

Note: Converse of the theorem need not be true, Eg: $(\mathbb{Z}, +, \cdot)$ is integral domain but not a field

---

Theorem 4: A finite integral domain is a field.

Let $(R, +, \cdot)$ be a finite integral domain consisting of n distinct elemen

Let $R = \{0, 1, a_1, a_2, \ldots, a_i, \ldots a_{n-2}\}$

R is a commutative ring with unity and without zero divisors

T.P.T : Every non-zero element is invertible

Let $a_i (\neq 0) \in R$.
Consider $A = \{a_i \cdot 0, a_i \cdot 1, a_i \cdot a_1, a_i a_2, a_i a_{n-2}\}$.
A has n distinct elements (∵ if $a_i a_k = a_i a_l \Rightarrow a_k = a_l$ which contradicts that R has n distinct elements).
∴ A has n distinct elements.
As multiplication is binary operation in R all the elements of $A \in R$, In some order
$A = R$
⇒ every element of R is multiple of a_i.
In particular, $1 \in R$ ∴ $1 = a_i a_j$, for some $a_j \in R$.

$a_i \cdot a_j = 1 = a_j a_i$.
$a_i^{-1} = a_j \Rightarrow a_i$ is invertible.
As R is commutative ring with unity where all non-zero elements are invertible R is a field.
Thus every finite field integral domain is a field.

Theorem 5: $(Z_n, +_n, \times_n)$ is without zero divisors iff n is a prime number

OR

$(Z_n, +_n, \times_n)$ is an integral domain iff n is a prime no.

OR $(Z_n, +_n, \times_n)$ is a field iff n is prime no.

Pf: Let $(Z_n, +_n, \times_n)$ be without zero divisors.

Let n be a composite number

i.e., $n = ml$ where $1 < m, 1 < n$

$\Rightarrow m \times_n l = 0$

but $m \neq 0, l \neq 0$

$\Rightarrow Z_n$ is with zero divisors.

This contradicts that Z_n is without zero divisors.

$\therefore n$ is a prime number.

Converse, Let n be a prime number

Consider $a \times_n b = 0$ where $a, b \in Z_n$.

$n \mid ab \Rightarrow n \mid a$ or $n \mid b$ ($\because n$ is a prime no.) as $a, b \in Z_n$

$\therefore a, b < n$.

$\therefore n \mid a \Rightarrow a = 0$

or $n \mid b \Rightarrow b = 0$

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

Z_n is without zero divisors.

Hence the proof.

Theorem 6: $(R, +, \cdot)$ is an integral domain. Then $R^* = R - \{0\}$ = set of non zero elements of R, forms a semigroup w.r.to multiplication.

Let $a, b \in R^* \Rightarrow a \neq 0, b \neq 0$

we know that integral domain is ring without zero divisors.

$\Rightarrow ab \neq 0 \Rightarrow a, b \in R^*$

$\therefore$ R^* is closed under multiplication

As multiplication is associative in R it is associative in R^* also

$\therefore$ $(R^*, \times)$ is a semigroup.

Subrings of a Ring.

A non-empty subset 'S' of a ring $(R, +, \cdot)$ is said to be a subring of R iff $(S, +, \cdot)$ is also a ring

R and set containing $\{0\}$ are known as trivial or improper subring of R.

The subrings other than these two are known as non-trivial or proper subrings of R.

* $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Q}, +, \cdot)$
  $(2\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Z}, +, \cdot)$

Theorem:
A non-empty subset S of a ring R is a subring of R iff (i) $a-b \in S$, (ii) $ab \in S$ $\forall a, b \in S$

(OR) (The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring of R are $a-b \in S$ & $ab \in S$)

Let $(S, +, \cdot)$ be a subring of $(R, +, \cdot)$

$\Rightarrow (S, +, \cdot)$ is a ring

$\Rightarrow (S, +)$ is an abelian group.

$\Rightarrow (S, +)$ is a subgroup of $(R, +)$
$(\because S \subseteq R)$.

$\Rightarrow a-b \in S, \ \forall a, b \in S$

As $(S, +, \cdot)$ is a ring, it is closed under multiplication

$\therefore ab \in S \ \forall a \in S, b \in S$ [Necessary condition].

Converse., Let $a-b \in S$ and $ab \in S, \forall a, b \in S$

$a-b \in S \Rightarrow (S, +)$ is a subgroup of $(R, +) \Rightarrow (S, +)$ is a group.

As addition is commutative in R, it is Commutative in S also

$\therefore (S,+)$ is an abelian group.

Multiplication is associative in R,

$\therefore$ it is associative in S also

Distributive laws holds good in R.

$\therefore$ distributive laws holds good in S also.

S is closed w.r.to multiplication as $a,b \in R$, $\forall\ a,b \in S$.

$\therefore (S,+,\cdot)$ is a ring.

$\Rightarrow (S,+,\cdot)$ is a subring of $(R,+,\cdot)$

Theorem 2: A non-empty subset S of a ring $(R,+,\cdot)$ is a subring of R iff

(i) $S+(-S) = S$

(ii) $SS \subseteq S$

Let S be a subring of R

Consider $x \in S+(-S)$

$\Rightarrow x = a+(-b)$ for some $a \in S$

& $-b \in -S$

$\Rightarrow x = a-b \in S$.

$\Rightarrow S+(-S) \subseteq S$ — (1)

Let $y \in S \Rightarrow y = y+0$

$\Rightarrow y+(-0) \in S+(-S)$ (here $y \in S$, $+-0 \in -S$ or $0 \in S$).

$\Rightarrow S \subseteq S+(-S)$ — (2)

(1) & (2) $\Rightarrow S+(-S)=S$

(ii) Let $x \in SS$

$\Rightarrow x=ab$ for some $a, b \in S$.

$ab \in S$ ($\because S$ is a subring of R)

$\Rightarrow x \in S \therefore SS \subseteq S$.

Conversely, Let $S+(-S)=S$ — (1)

& $SS \subseteq S$ — (2)

Let $ab \in S \Rightarrow a \in S, -b \in -S$

$a+(-b) \in S+(-S)$

from (1), $a+(-b) \in S$ i.e., $a-b \in S$ — (3)

& Let $ab \in SS$.

from (2) $ab \in S$ — (4)

$\therefore$ (3) & (4) $\Rightarrow S$ is a subring of R.

Theorem: Intersection of any two subrings of a ring R is also a subring of R

Let S & T be two subrings of $(R, +, \cdot)$. $(S \cap T)$ is a non-empty subset of R. ($\because 0 \in S$ and $0 \in T$ & S and T are subrings).

Let $a, b \in S \cap T$

T.S.T: $a-b \in S \cap T$ & $ab \in S \cap T$

$a, b \in S \cap T$

$\Rightarrow a, b \in S$ & $a, b \in T$.

$\Rightarrow a-b \in S$ & $a-b \in T$

$ab \in S$ $ab \in T$

($\because$ S & T are subrings of R)

$\Rightarrow a-b \in S \cap T$ & $ab \in S \cap T$

$\therefore S \cap T$ is a subring of R.

i) This theorem can be generalized i.e., if $S_1, S_2, \ldots, S_n$ are subrings of R, then $S_1 \cap S_2 \cap \ldots \cap S_n$ is also a subring of R.

ii) Union of 2 subrings of R need not be a subring of R

Eg: $2\mathbb{Z}, 3\mathbb{Z}$ are subrings of $(\mathbb{Z}, +, \cdot)$

$2, \mathbb{Z} \in (2\mathbb{Z} \cup 3\mathbb{Z})$

but $3-1=1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

$\therefore 2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $(\mathbb{Z}, +, \cdot)$

Thm 4: The union of two subrings of R is a subring of R iff one is contained in another.

Let S & T be two subrings of $(R, +, \cdot)$

Consider SUT as a subring of R

To prove : $S \subseteq T$ or $T \subseteq S$.

Let $S \not\subseteq T$ or $T \not\subseteq S$

$\Rightarrow \exists\, \alpha \in S$ but $\alpha \notin T$ or $\exists\, \beta \in T$ but $\beta \notin S$.

$\alpha \in S$ & $\beta \in T \Rightarrow \alpha, \beta \in (SUT)$

$\Rightarrow \alpha - \beta$ and $\alpha\beta \in SUT$

(∵ SUT is a subring of R).

$\Rightarrow \alpha - \beta, \alpha\beta \in S$ and/or

$\alpha - \beta, \alpha\beta \in T$

we have $\alpha, \alpha - \beta \in S$.

$\Rightarrow \alpha - (\alpha - \beta) \in S$

$\Rightarrow \beta \in S$.

Contradiction to our assumption that $\beta \notin S$.

Again $\beta, \alpha - \beta \in T$

$\Rightarrow \beta + \alpha - \beta \in T$ (addition is binary).

$\Rightarrow \alpha \in T$.

(∵ closure law)

This is contradiction to our assumption that $\alpha \notin T$ ∴ $S \subseteq T$ or $T \subseteq S$.

Conversely, Let $S \subseteq T$ or $T \subseteq S$.

$S \subseteq T \Rightarrow S \cup T = T$

$T \subseteq S \Rightarrow S \cup T = S$

$\Rightarrow S \cup T$ is a subring of R as S & T are subrings of R.

Problems:

S.T. $(nZ, +, \cdot)$ is a subring of $(Z, +, \cdot)$

Let $x, y \in nZ$

$\Rightarrow x = na, y = nb$ for some $a, b \in Z$

$x - y = na - nb = n(a-b) \in nZ$ — (1)

$\because a - b \in Z$

$xy = nanb = n(anb) \in nZ$ — (2)

$\because anb \in Z$.

$\therefore$ (1), (2) $\Rightarrow nZ$ is a subring of $(Z, +, \cdot)$

S.T set of all matrices of the form $M = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / a, b \in Q \right\}$ is a non-commutative ring without unity w.r.to addition and multiplication of matrices.

M is a non-empty subset of $M_2(Q)$ (ring of square matrices of order 2 over Q)

Let $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$

$$A - B = \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in M$$

$$AB = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix} \in M$$

M is a subring of $M_2(\mathbb{Q}) \Rightarrow M$ is a ring.
Matrix multiplication is not commutative.
Suppose $AX = A = XA$ where $X = \begin{bmatrix} p & q \\ 0 & 0 \end{bmatrix} \in M$

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} p & q \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$$

$ap = a$, $aq = b$

$\Rightarrow p = 1$, $q = b/a$.

$XA = A$

$$\begin{bmatrix} p & q \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} pa & pb \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$$

$\Rightarrow pq = a \Rightarrow p = 1$ $\quad pb = b \Rightarrow p = 1$

As $q = b/a$, is not unique.
$\therefore X$ is not unique.
$\Rightarrow M$ is without unity.

S.T the set of all real nos. of the form $a+b\sqrt{2}$ where a & b are integers forms a integral domain.

$S = \{a+b\sqrt{2} \mid a, b \in Z\}$.

S is a non-empty subsets of ring of real nos. $(R, +, \cdot)$.

Let $x, y \in S \Rightarrow x = a+b\sqrt{2}$, $y = c+d\sqrt{2}$

$x-y = a-c+(b-d)\sqrt{2} \in S$

$xy = (a+b\sqrt{2})(c+d\sqrt{2})$

$= (ac+2bd)+(ad+bc)\sqrt{2} \in S$.

$\Rightarrow$ S is a subring of $(R, +, \cdot)$.

$\Rightarrow$ S is a ring w.r.to '+' & 'x'

As R is commutative, S is also commutative.

$(a+b\sqrt{2})(1+0\sqrt{2}) = a+b\sqrt{2}$.

$= (1+0\sqrt{2})(a+b\sqrt{2})$.

$\Rightarrow 1 = 1+0\sqrt{2} \in S$ is unity of S.

$ac+2bd = 0 \qquad ad+bc = 0$.

$\Rightarrow b = 0 \Rightarrow ac+2bd = 0$

$\Rightarrow ac = 0, \quad ad+bc = 0$

$\Rightarrow ad = 0$

$\Rightarrow a = 0, c = 0, d = 0$

$\because a, c, d \in Z$ which is without zero divisors

$\therefore x=0, y=0$ i.e., if $xy=0$.
then $x=0, y=0$.
$\therefore$ S is without zero divisors.
$\therefore$ Integral domain.

Ideals

A non-empty subset I of a ring $(R, +, \cdot)$ is said to be an ideal of R if $a-b, ra, ar \in I$, $\forall\, a, b \in I$ and $r \in R$.

A non-empty subset I of a ring $(R, +, \cdot)$ is said to be right ideal of R if $a-b, ar \in I$, $\forall\, a, b \in I$ & $r \in R$

A non-empty subset I of a ring $(R, +, \cdot)$ is said to be left ideal of R if $a-b, ra \in I$, $\forall\, a, b \in I$, $r \in R$.

The set containing $\{0\}$ and R are said to be improper or trivial ideals of R. The ideals other than these are known as proper or non-trivial ideals of R.

A ring is said to be simple ring if it has no proper ideal.

Theorems:

1. Every ideal (left or right) is a subring of R.

Let I be an ideal of $(R, +, \cdot)$

$\Rightarrow a-b, ar, ra \in I, \forall a, b \in I, r \in R$.

$b \in I \Rightarrow b \in R$.

$a \in I \Rightarrow a \in R \Rightarrow ab \in I$

$(\because ar \in I, \forall a \in I, r \in R)$

Thus $a-b$ and $ab \in I$, $\forall a, b \in I$.

$\therefore I$ is a subring of R.

Note: Every ideal is a subring but every subring need not be a ideal

i.e., Converse need not be true.

Eg: $(Z, +, \cdot)$ is a subring of $(Q, +, \cdot)$

Let $7 \in Z$, $8/3 \in Q$

$ab = 7 \times 8/3 \notin Z$

$\therefore Z$ is not an ideal of $(Q, +, \cdot)$

2. Intersection of any 2 ideals of a ring is also ideal of the ring

Let S and T be 2 ideals of a

ring $(R, +, \cdot)$

T.P.T : $S \cap T$ is an ideal of R.

S and T are non-empty subsets of R.

$\because 0 \in S, 0 \in I$ as S and T are ideals)

$\therefore 0 \in S \cap T$

Let $a, b \in S \cap T$ and $r \in R$.

$a, b \in S \cap T \Rightarrow a, b \in S, a, b \in T$.

Now $a, b \in S, r \in R \Rightarrow a-b, ar, ra \in S$

$a, b \in I, r \in R \Rightarrow a-b, ar, ra \in T$.

$\Rightarrow a-b, ar, ra \in S \cap T, \forall a, b \in S \cap T$ and $r \in R$.

$\therefore S \cap T$ is an ideal of R.

Note:

i) Intersection of any 2 right ideals of a ring is also a right ideal of the ring

ii) Intersection of any 2 left ideals of a ring is also a left ideal of the ring

iii) Suppose $S_1, S_2, \ldots, S_k$ are ideals of R then $S_1 \cap S_2 \cap \ldots \cap S_k$ are ideals of R

iv) Union of 2 ideals of R need not be an ideal of R

$2\mathbb{Z}, 3\mathbb{Z}$ are ideals of $(\mathbb{Z}, +, \cdot)$

$2 \in 2\mathbb{Z}$, $3 \in 3\mathbb{Z}$

$2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$

but $3 - 2 = 1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

$\therefore (2\mathbb{Z} \cup 3\mathbb{Z})$ is not an ideal of $(\mathbb{Z}, +, \cdot)$

3. The union of 2 ideals of a ring is an ideal of the ring iff one is contained in another.

Let S and T be 2 ideals of $(R, +, \cdot)$

Suppose $S \cup T$ is an ideal of R

To prove: $S \subseteq T$ or $T \subseteq S$

Consider $S \nsubseteq T$ or $T \nsubseteq S$

$\Rightarrow \exists\ \alpha \in S$ such that $\alpha \notin T$.

or $\exists\ \beta \in T$ such that $\beta \notin S$.

$\alpha, \beta \in S \cup T$.

$\Rightarrow \alpha - \beta \in S \cup T$ ($\because S \cup T$ is an ideal).

$\Rightarrow \alpha - \beta \in S$ and/or $\alpha - \beta \in T$

Now, $\alpha \in S$ and $\alpha - \beta \in S$.

$\Rightarrow \alpha - (\alpha - \beta) \in S$

$\Rightarrow \alpha - \alpha + \beta \in S$

$\Rightarrow \beta \in S$

This is a contradiction to our assumption that $\beta \notin S$

Again $\beta, \alpha - \beta \in T$

$\Rightarrow \beta + \alpha - \beta \in T \Rightarrow \alpha \in T$

Contradiction.

$\therefore$ Our assumption is wrong.

Hence $S \subseteq T$ ~~and~~ $T \subseteq S$.

Conversely,

Let $S \subseteq T$ or $T \subseteq S$.

$S \subseteq T \Rightarrow S \cup T = T$

$T \subseteq S \Rightarrow S \cup T = S$

$\Rightarrow S \cup T$ is an ideal of R as T and S are ideals of R.

Problems:

1. Show that nZ is an ideal of $(Z, +, \cdot)$

$x = na$, $y = nb$ for some $a, b \in Z$.

$x - y = n(a-b) \in nZ$ — (1)

$xr = (na)r = n(ar) \in nZ$ — (2)

$rx = r(na) = (rn)a = n(ra)$ — (3)

(1), (2), (3) $\Rightarrow nZ$ is an ideal of $(Z, +, \cdot)$

Let R be ring of all 2×2 matrices with their elements as integers.

a) $S = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a, b \in Z \right\}$ is a left ideal of R but not a right ideal.

b) $S = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / a, b \in Z \right\}$ is a right ideal of R but not a left ideal.

a) $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$, $B = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} \in S$.

$X = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in R$.

$A - B = \begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in S$ — (1).

$XA = \begin{bmatrix} p & q \\ r & s \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} ap+qb & 0 \\ ar+sb & 0 \end{bmatrix} \in S$ — (2)

$AX = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap & aq \\ bp & bs \end{bmatrix} \notin S$

$\therefore$ (1) & (2) $\Rightarrow$ S is an left ideal of R.
As $AX \notin S$ $\therefore$ S is not right ideal.

b) $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \in S$, $B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \in S$

$X = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in R$

$$A-B=\begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in S \quad -(1)$$

$$XA=\begin{bmatrix} p & q \\ r & s \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} ap & pb \\ ra & sb \end{bmatrix} \notin S \quad -(2)$$

$$AX=\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} p & q \\ r & s \end{bmatrix}=\begin{bmatrix} ap & aq \\ 0 & 0 \end{bmatrix} \in S \quad -(3)$$

(1), (2) & (3) $\Rightarrow$ S is a right ideal of R and not left ideal of R.

As R is a ring, $a \in R$ and $I=\{x \in R / ax=0\}$. Show that I is a right ideal of R.

Let $x, y \in I$, $r \in R$

$ax=0$, $ay=0$

$\Rightarrow ax-ay=a(x-y)=ax-ay=0$

$\Rightarrow x-y \in I \quad -(1)$

$a(xr)=(ax)r=0.r=0$

$\therefore xr \in I \quad -(2)$

(1) & (2) $\Rightarrow$ I is a right ideal of R.

Note: $I=\{x \in R / xa=0\}$ is a left ideal but not a right ideal of R.

Let $(R,+,\cdot)$ be a commutative ring and $a \in R$. Show that $aR = \{ar / r \in R\}$ is an ideal of R.

Let $x, y \in aR$ and $r \in R$

$\Rightarrow x = ar_1, \; y = ar_2$ for some $r_1, r_2 \in R$.

$\because r_1 - r_2 \in R$.

$x - y = ar_1 - ar_2 = a(r_1 - r_2) \in aR$.

or $x - y \in aR$

$xr = ar_1 r = a(r_1 r) \in aR$ — ②

$rx = xr$ ($\because R$ is commutative)

$= (ar_1)r = a(r_1 r) \in aR$

$rx \in aR$ — ③

$\therefore$ ①, ② & ③ $\Rightarrow$ aR is an ideal of R.

Note: If R is not commutative, then aR is right ideal and Ra is left ideal of R

Ideal aR.

Definition: Let R be a commutative ring and $a \in R$. The ideal $aR = \{ar / r \in R\}$ is known as principal ideal of the ring R generated by a

$aR = Ra$.

Homomorphism of Rings.

Definition: Homomorphism into: A mapping f from a ring R into a ring R' is said to be a homomorphism of R into R' if

① $f(a+b) = f(a) + f(b)$

② $f(ab) = f(a)f(b)$, $\forall\ a, b \in R$.

Homomorphism onto: A mapping f from a ring R onto a ring R' is said to be homomorphism of R into R' if

(i) $f(a+b) = f(a)+f(b)$,

(ii) $f(ab) = f(a)f(b)$, $\forall\ a, b \in R$

Let $(Z, +, \cdot)$ be the ring of integers, define $f: Z \to Z$ by $f(x) = x$, $\forall\ x \in Z$, Show that f is homomorphism.

$$f(x+y) = x+y = f(x)+f(y)$$
$$f(xy) = xy = f(x)f(y).$$

$\therefore$ f is a homomorphism of Z into Z.

Let $(Z, +, \cdot)$ be the ring of integers and $(2Z, +, \cdot)$ be the ring of integers. Define $f: Z \to 2Z$ by $f(x) = 2x$, $\forall\ x \in Z$

$$f(2) = 4, \quad f(3) = 6$$
$$f(2.3) = f(6) = 12$$
$$f(2).f(3) = 4.6 = 24$$
$$\Rightarrow f(a)f(b) \neq f(ab)$$

Let $(\mathbb{Z},+,\cdot)$ be the ring of integers & $(2\mathbb{Z},+,*)$ be the ring with integers, where $*$ is defined by $a*b = ab/2$. Define $f: \mathbb{Z} \to 2\mathbb{Z}$ by $f(x) = 2x$, $\forall x \in \mathbb{Z}$, Show that $f(z)$ is homomorphism.

$$f(x+y) = 2(x+y) = 2x+2y = f(x)+f(y)$$

$$f(xy) = 2xy; \quad f(x)*f(y) = 2x*2y$$

$$= \frac{2x \cdot 2y}{2} = 2xy.$$

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

$\therefore f$ is homomorphism.

Thm: If f is a homomorphism of a ring R into ring R' then

(i) $f(0) = 0'$ where 0 is the zero element of R and $0'$ is the zero element of R'

(ii) $f(-a) = -f(a)$, $\forall a \in R$.

Let $a \in R$, then $f(a) \in R'$

We have $f(a) + 0' = f(a)$

($\because 0'$ is the identity element of R')

$$= f(a) = f(a+0) = f(a)+f(0)$$

$$\Rightarrow f(a) + 0' = f(a) + f(0)$$

$$\Rightarrow 0' = f(0), \quad (LCL)$$

We have $0' = f(0) = f(a+(-a)) = f(a)+f(-a)$

($\because f$ is homomorphism)

$\therefore f(a) + f(-a) = 0'$

$\therefore f(-a)$ is the additive inverse of $f(a)$

$f(-a) = -f(a)$

Corollary: If $f: R \to R'$ is a homomorphism then $f(a-b) = f(a) - f(b)$

Pf: $f(a-b) = f(a+(-b)) = f(a) + f(-b)$
$= f(a) - f(b)$

Thm: Let R and R' be 2 rings and let the mapping $f: R \to R'$ be a homomorphism from R to R'. Then the homomorphic image $f(R)$ of R is a subring of R'.

Let $a', b' \in f(R)$. Then $\exists\ a, b \in R$ such that $f(a) = a'$ and $f(b) = b'$

Now $a' - b' = f(a) - f(b) = f(a) + f(-b)$
$= f(a-b) \in f(R)$

Again $a'b' = f(a)f(b) = f(ab) \in f(R)$

$a', b' \in f(R) \Rightarrow a' - b' \in f(R)$
& $a'.b' \in f(R)$.

Hence $f(R)$ is a subring of R'.

Kernel of a ring homomorphism.

Definition: Let $f: R \to R'$ be a ring homomorphism. Then the set of all those elements of R which are mapped onto the zero element of R' is called the Kernel of

the homomorphism f and denoted by $\ker f$ i.e., $\ker f = \{x \in R / f(x) = 0'\}$ where $0'$ is the zero element of R'.

If $f: R \to R'$ be a homomorphism of R into R' Then show that $\ker f$ is an ideal of R.

Let $K = \ker f = \{x \in R : f(x) = 0'\}$

Since $f(0) = 0' \therefore$ atleast $0 \in K$

$\therefore K \neq \phi$.

Let $a, b \in K$, then $f(a) = 0'$, $f(b) = 0'$

we have $f(a-b) = f(a+(-b))$

$= f(a) + f(-b) = f(a) - f(b) = 0' - 0' = 0$

$\therefore a - b \in K$, thus $a, b \in K, a - b \in K$

Also if $r \in R$ then $f(ar) = f(a)f(r)$

$= 0' f(r) = 0'$

$f(ra) = f(r)f(a) = f(r)f(0) = f(r)0' = 0'$

Thus $a \in K, r \in R \Rightarrow ar \in K$ and $ra \in K$

Hence $K = \ker f$ is an ideal of R.

Thm: If $f: R \to R'$ be a homomorphism of R and R' then show that $\ker f$ is a subring of R

Let $K = \ker f = \{x \in R / f(x) = 0'\}$.

$f(0) = 0' \Rightarrow 0 \in K \therefore K \neq \phi$

Let $a, b \in K$ then $f(a) = 0', f(b) = 0'$

Now $f(a-b) = f(a+(-b)) = f(a) - f(b)$

$= 0' - 0' = 0' \Rightarrow a - b \in K$.

Also $f(ab) = f(a)f(b) = 0'0' = 0' \Rightarrow ab \in K$

$\therefore K = \text{Ker} f$ is a subring of R.

If $f: R \to R'$ be a homomorphism with Kernel K, then f is 1-1 iff $K = \{0\}$

Let f be 1-1, $K = \{x \in R \mid f(x) = 0'\}$

Let $a \in K \Rightarrow f(a) = 0' \Rightarrow f(a) = f(0)$

$\Rightarrow a = 0$ ($\because f$ is 1-1)

$\Rightarrow K = \{0\}$.

Conversely, Let $K = \{0\}$

Let $f(a) = f(b) \Rightarrow f(a) - f(b) = 0'$

$\Rightarrow f(a-b) = 0'$

$\Rightarrow a - b \in K$

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

$\therefore f$ is 1-1.

Isomorphism of rings.

A mapping $f: R \to R'$ from the ring R into R' is said to be isomorphism if (i) f is homomorphism

i.e., $f(a+b) = f(a) + f(b)$; $f(ab) = f(a)f(b)$

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

(ii) $f(ab) = f(a)f(b)$

f is 1-1 and onto, then we write $R \cong R'$.

Properties of Isomorphism:

Thm: If $f: R \to R'$ be a homomorphism of rings R into R', then

(i) If R is a commutative ring then R' is also a commutative

(ii) If R is a without zero divisors, then R' is also without zero divisors.

(iii) If R is a ring with unity, then R' is also with unity.

(iv) If R is an integral domain, then R' is also an integral domain

(v) If R is field then R' is also a field.

(vi) If R is division ring then R' is also a division ring.

Pf: (i) Let $a', b' \in R' \Rightarrow a, b \in R$ such that

$f(a) = a'$, $f(b) = b'$