IDEALS Set - VIII

* **Definition:** Let $(R,+,\cdot)$ be a ring. A non-empty subset S of a ring R is called a left ideal of R, if

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

i.e. $\forall\ a,b\in S \Rightarrow a-b\in S$

(ii) $s\in S$ and $r\in R \Rightarrow rs\in S$

* **Definition:** Let $(R,+,\cdot)$ be a ring. A non-empty subset S of a ring R is called a right ideal of R, if

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

i.e. $\forall\ a,b\in S \Rightarrow a-b\in S$

(ii) $s\in S$ and $r\in R \Rightarrow sr\in S$

* **Definition:** Let $(R,+,\cdot)$ be a ring. A non-empty subset S of a ring R is called an ideal (or) a two sided ideal of R, if

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

i.e $\forall\ a,b\in S \Rightarrow a-b\in S$

(ii) $s\in S$ and $r\in R \Rightarrow sr\in S$ and $rs\in S$.

In otherwords, a non-empty subset 'S' of a ring R is an ideal of R, if S is both a left and right ideal of R.

→ R is a ring

(i) if $S = R\subseteq R$,

(1) $(R,+)$ itself is a subgroup of $(R,+)$

(2) $s \in R, r \in R \Rightarrow rs \in R$ & $s.r \in R$

$\therefore$ R itself is an ideal of R

— If R is a ring then R itself is an ideal of R. R is called unit ideal of R

(ii) If $S = \{0\} \subseteq R$,

(1) $0, 0 \in S \Rightarrow 0 - 0 = 0 \in S$

(2) $0 \in S, r \in R \Rightarrow 0r = 0 \in S$ & $r0 = 0 \in S$.

$\therefore S = \{0\}$ is an ideal of R.

— $S = \{0\}$ is called null ideal of R (or) zero ideal of R.

Note: (1) If R is a ring then the null ideal $\{0\}$ and the unit ideal R are called improper ideals of R.

Any other ideal of R is called a proper ideal of R.

(2) Every ring R always possesses two ideals (improper ideals)

(3) If R is a commutative ring, every left ideal is also a right ideal. Therefore in a commutative ring every left ideal or right ideal is a two-sided ideal.

Examples:

→ If I be the ring of integers and n be any fixed integer, then $S = (n) = \{nx / x \in I\}$ is an ideal of I.

Sol'n: Given that I is a ring

and $S = \{nx / x \in I\} \subseteq I$ where n is fixed integer.

Now let $a, b \in S$ choosing $a = nx$

$b = ny$; $x, y \in I$ & 'n' is a fixed integer.

then $a - b = nx - ny$

$= n(x - y)$

$\in S$ ($\because x, y \in I \Rightarrow x - y \in I$)

$\therefore S$ is a subgroup of I.

Now let $r \in I$, $a \in S$, choosing $a = nx$; $x \in I$ & n is fixed integer.

then $ra = r(nx) = (rn)x$

$= (nr)x$

$= n(rx)$

$\in S \quad (\because rx \in I)$.

and $ar = (nx)r = n(rx)$

$\in S \quad (\because rx \in I)$

$\therefore \forall\ a \in S$ and $r \in I$

$\Rightarrow ra \in S$ and

$ar \in S$

$\therefore S$ is an ideal of R and this ideal is a proper ideal.

Note: $(2) = \{ \ldots\ldots -6, -4, -2, 0, 2, 4 \ldots\ldots \}$,

$(3) = \{ \ldots\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\ldots \}$ etc are Ideals in I.

→ The set of integers I is only a subring but not an ideal of the ring of rational numbers $(\mathbb{Q}, +, \cdot)$

Sol'n: The product of a rational number and an integer is not necessarily an integer.

for example: $3 \in I$, $\frac{2}{5} \in \mathbb{Q}$

$\Rightarrow \left(\frac{2}{5}\right)3 = \frac{6}{5} \notin I$

$\therefore$ I is not an Ideal of the ring of rational numbers.

Note: (1) The set $\mathbb{Q}$ of rational numbers is only a subring but not an ideal of the ring of real numbers $(\mathbb{R}, +, \cdot)$

(2) The set $\mathbb{R}$ of real numbers is only a subring but not an ideal of the ring of complex numbers $(\mathbb{C}, +, \cdot)$.

Theorem: Every ideal of a ring R is a subring of R, but the converse need not be true.

Proof: Let S be an ideal of the given ring R.

Let $a, b \in S$, by definition of ideal $a-b \in S$.

further $a \in S$ and $b \in S \subseteq R$ (i.e. $b \in R$)

$$\Rightarrow ab \in S$$

$\therefore$ S is a subring of R.

But the converse is not true,

i.e. Every subring need not be an ideal.

for example:

The set $\mathbb{I}$ of integers is a subring of the ring $\mathbb{Q}$ of rational numbers.

but $\mathbb{I}$ is not an ideal of $\mathbb{Q}$.

Since $3 \in \mathbb{I}$, $\frac{1}{2} \in \mathbb{Q} \Rightarrow 3 \cdot \frac{1}{2} = \frac{3}{2} \notin \mathbb{I}$.

Theorem: If S is an ideal of a ring R with unit element and $1 \in S$ then $S = R$.

Proof: Given that R is a ring with unity and S is ideal of R

$$\therefore S \subseteq R \quad \text{---} \quad (1).$$

Let $r = x \in R$, $s = 1 \in S$ (by hyp)

$$\Rightarrow rs = x.1 = x \in S$$

and $sr = 1.x = x \in S$ ($\because$ S is an ideal)

$\therefore x \in R \Rightarrow x \in S$

$\therefore R \subseteq S$ ---- (2)

$\therefore$ From (1) & (2), we have $R = S$.

Theorem: A field has no proper ideals

(or)

The ideals of a field F are only $\{0\}$ and F itself

Proof: Let F be a field.

Let S be an ideal of F, so that $S = \{0\}$.

Now we prove that $S = F$:

By definition of ideal $S \subseteq F$ —— (1)

Let $S \neq \{0\}$

$\therefore$ S contains non-zero elements.

Let $a(\neq 0) \in S \subseteq F \Rightarrow a(\neq 0) \in F$

$\Rightarrow a^{-1} \in F$ ($\because$ the non-zero elts of F have inverse wrt $x'n$ in F)

Let $r = \bar{a}^1 \in F$, $s = a \in S$

$\Rightarrow rs = \bar{a}^1 a$

$= 1 \in S$

and $sr = a\bar{a}^1$

$= 1 \in S$ ($\because$ S is an ideal of F)

$\therefore \boxed{1 \in S}$

Now let $r = x \in F$, $s = 1 \in S$

$\Rightarrow rs = x \cdot 1$

$= x \in S$

and $s.r = x.1$

$= x \in S$ ($\because$ S is an ideal of F)

$\therefore x \in F \Rightarrow x \in S$

$\therefore F \subseteq S$ —— (2)

$\therefore$ From (1) and (2), we have

$S = F$

$\therefore$ A field F has no proper ideals.

Theorem The intersection of two left ideals of a ring R is left ideal of R.

Proof: Let R be the given ring.

Let S_1 and S_2 be two left ideals of a ring R.

Let $S = S_1 \cap S_2$

Let $a, b \in S \Rightarrow a, b \in S_1 \cap S_2$

$\Rightarrow a, b \in S_1$ and $a, b \in S_2$

$\Rightarrow a - b \in S_1$ and $a - b \in S_2$

$\Rightarrow a - b \in S_1 \cap S_2$

$\therefore S$ is a subgroup of R.

(ii) $r \in R, s \in S \Rightarrow r \in R, s \in S_1 \cap S_2$

$\Rightarrow r \in R, (s \in S_1$ and $s \in S_2)$

$\Rightarrow (r \in R, s \in S_1)$ and $(r \in R, s \in S_2)$

$\Rightarrow r.s \in S_1$ and $rs \in S_2$ ($\because S_1$ & S_2 are an left ideals of R)

$\Rightarrow r.s \in S_1 \cap S_2$

$\Rightarrow rs \in S$

$\therefore S$ is a left ideal of R.

Note: (1) The intersection of two right ideals of a ring R is a right ideal of R.

(2) The intersection of two ideals of a ring R is also an ideal of R

Theorem: The intersection of an arbitrary family of left ideals of a ring R is a left ideal of R.

Proof: Let $S_1, S_2, S_3 \ldots\ldots$ be left ideal of a ring R.

Let $S = S_1 \cap S_2 \cap S_3 \cap \ldots\ldots$

$= \bigcap_{i \in N} S_i$

Let $a, b \in S \Rightarrow a, b \in \bigcap_{i \in N} S_i$

$\Rightarrow a, b \in S_i \ \forall \ i \in N$

$\Rightarrow a - b \in S_i \ \forall \ i \in N$ ($\because S_i$ is a subgroup)

$\Rightarrow a - b \in S$

$\therefore S$ is a subgroup of R.

Let $r \in R, s \in S$

$\Rightarrow r \in R, s \in \bigcap_{i \in N} S_i$

$\Rightarrow r \in R, s \in S_i \ \forall \ i \in N$

$\Rightarrow rs \in S_i \ \forall \ i \in N$ ($\because S_i$ is a left ideal)

$\Rightarrow rs \in \bigcap_{i \in N} S_i$

$\Rightarrow rs \in S$

$\therefore S = \bigcap_{i \in N} S_i$ is a left ideal.

Note: (1) the intersection of an arbitrary family of right ideals of a ring R is a right ideal of R.

(2) The intersection of an arbitrary family of ideals of a ring R is an ideal of R.

Imp Note → the union of two ideals of a ring R need not be an ideal of R.

We know that

$A = (2) = \{\ldots -4, -2, 0, 2, 4, \ldots\} = \{2n / n \in I\}$

$B = (3) = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\} = \{3n / n \in I\}$

are two ideals of a ring I of integers.

Now $A \cup B = \{\ldots -9, -6, -4, -3, -2, 0, 3, 4, 6, 9, \ldots\}$

Now $2, 3 \in A \cup B$

$\Rightarrow 3-2 = 1 \notin A \cup B$

$\therefore A \cup B$ is not ideal of $\mathbb{I}$.

2003 The union of two ideals of a ring R is an ideal of R if and only if one is contained in the other.

Proof: Let S_1 and S_2 be two ideals of the ring R.

Let $S_1 \subset S_2$ or $S_2 \subset S_1$

if $S_1 \subset S_2$ then $S_1 \cup S_2 = S_2$ (S_2 is an ideal of R)

if $S_2 \subset S_1$ then $S_1 \cup S_2 = S_1$ (S_1 is an ideal of R)

$\therefore S_1 \cup S_2$ is an ideal of R.

Conversely suppose that $S_1 \cup S_2$ is an ideal of R.

Now we prove that $S_1 \subset S_2$ or $S_2 \subset S_1$

If possible, suppose that $S_1 \not\subset S_2$ or $S_2 \not\subset S_1$

since $S_1 \not\subset S_2$

Let $a \in S_1$ but $a \notin S_2$

since $S_2 \not\subset S_1$

Let $b \in S_2$ but $b \notin S_1$

Now $a \in S_1$ and $b \in S_2 \Rightarrow a, b \in S_1 \cup S_2$

$\Rightarrow a-b \in S_1 \cup S_2$ ($\because S_1 \cup S_2$ is an ideal of R)

$\Rightarrow a-b \in S_1$ or $a-b \in S_2$

Now $a \in S_1$ and $a-b \in S_1$

$\Rightarrow a-(a-b) = b \in S_1$ ($\because S_1$ is an ideal of R)

$\therefore$ which is contradiction to the fact $b \notin S_1$.

Now $b \in S_2$, $a-b \in S_2$

$\Rightarrow b+(a-b) \in S_2$ ($\because S_2$ is an ideal of R)

$\Rightarrow a \in S_2$

which is contradiction to fact $a \notin S_2$.

$\therefore$ our Supposition is wrong.

Hence $S_1 \subset S_2$ or $S_2 \subset S_1$.

Theorem: If R is commutative ring and $a \in R$ then $R = \{ra / r \in R\}$ is an ideal of R.

Proof: Given that R is commutative ring. $a \in R$

Now we Prove that $Ra = \{ra / r \in R\}$ is an ideal of R

For $0 \in R$, $0a \in Ra$

$\Rightarrow 0 \in Ra$

$\therefore Ra \neq \phi$ and $Ra \subseteq R$

Let $x, y \in Ra$ choosing $x = r_1 a$

$y = r_2 a$; $r_1, r_2 \in R$

then $x - y = r_1 a - r_2 a$

$= (r_1 - r_2)a$

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

$\therefore Ra$ is a subgroup of R w.r.t '+'.

Now let $x \in R$, $y \in Ra$ choosing $y = ra$, $r \in R$

then $xy = x(ra)$

$= (xr)a$

$= (rx)a$ ($\because$ R is commutative ring i.e. $x \in R, r \in R \Rightarrow xr = rx$)

$\in Ra$ ($\because rx \in R$)

Similarly $yx \in Ra$

$\therefore Ra$ is an ideal of R.

Note: (1) If R is a commutative ring and $a \in R$ then $aR = \{ar / r \in R\}$ is an ideal of R.

(2) If R is a ring and $a \in R$ then Ra is a left ideal and aR is a right ideal.

1979.

Theorem: A commutative ring R with unit element is a field if R has no proper ideals.

Proof: Given that R is a commutative ring with unity and R has no proper ideals.

Now we Prove that R is a field.

For this we are enough to prove that the non-zero elements of R possesses inverse w.r.t $\times$.

Let $a(\neq 0) \in R$,

Let $Ra = \{ra / r \in R\} \subseteq R$

Let $x, y \in Ra$; Choosing $x = r_1 a$

$y = r_2 a$; $r_1, r_2 \in R$

then $x - y = r_1 a - r_2 a$

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

$\therefore$ Ra is a subgroup of R w.r.t. $+n$.

Let $x \in R$, $y \in Ra$ Choosing $y = ra$; $r \in R$

then $xy = x(ra)$

$= (xr)a$

$= (rx)a$ $(\because$ R is commutative ring$)$

$\in Ra$ $(\because x \in R, a \in R \Rightarrow xa \in R)$

Similarly $yx \in Ra$

$\therefore$ Ra is an ideal of R.

Since $(a \neq 0) \in R$, $1 \in R$

$\Rightarrow 1.a \in Ra$

$\Rightarrow a \in Ra$

$\therefore$ Ra contains non-zero elements of R.

$\therefore Ra \neq \{0\}$

Since R has no proper ideals.

$\therefore Ra = R$.

Let the one of the element of Ra be I ($\because$ R is ring with unity)

Let $ba = 1$ for some $b \in R$.

Since R is commutative.

$\therefore ba = ab = 1$

$\Rightarrow a^{-1} = b$

$\therefore$ the non-zero elements of R have inverses w.r.t x^n.

$\therefore$ R is a field.

Note: If R is a ring with unit element and R has no proper ideals then R is a division ring.

Theorem: The sum of two ideals of a ring R is an ideal of R

(or)

If S_1 and S_2 are two ideals of a ring R, then

$S_1 + S_2 = \{x+y \mid x \in S_1, y \in S_2\}$ is an ideal of R.

Proof: Given that S_1 and S_2 are two ideals of a ring R.

$S_1 + S_2 = \{x+y \mid x \in S_1, y \in S_2\}$

Since $0 \in R$ be the zero element

then $0 \in S_1$, $0 \in S_2 \Rightarrow 0+0 \in S_1+S_2$

$\Rightarrow 0 \in S_1+S_2$

$\therefore S_1+S_2 \neq \phi$ and subset of R.

Let $a, b \in S_1+S_2$ choosing $a = x_1+y_1$

$b = x_2+y_2$; $x_1, x_2 \in S_1$, $y_1, y_2 \in S_2$.

then $a-b = (x_1+y_1)-(x_2+y_2)$

$= (x_1-x_2)+(y_1-y_2)$

$\in S_1+S_2$ $(\because x_1-x_2 \in S_1,\ y_1-y_2 \in S_2)$

$\therefore S_1+S_2$ is a subgroup of R.

Let $a \in R$, $b \in S_1+S_2$ choosing $b = x+y$; $x \in S_1$ & $y \in S_2$

then $ab = a(x+y)$

$= ax+ay$ $(\because ax \in S_1, ay \in S_2)$

$\in S_1+S_2$

Similarly $ba \in S_1+S_2$

$\therefore S_1+S_2$ is an ideal of R.

Note: since $S_1 \subseteq S_1+S_2$ and $S_2 \subseteq S_1+S_2$

$\therefore S_1+S_2$ is an ideal of R containing both S_1 and S_2.

1996 → If S is an ideal of ring R and T any subring of R, then Prove that S is an ideal of $S+T = \{s+t \mid s \in S, t \in T\}$

1984 theorem → If S_1 and S_2 are two ideals of ring R, then their product S_1S_2 defined as

$S_1S_2 = \{a_1b_1+a_2b_2+\cdots+a_nb_n \mid a_i \in S_1, b_i \in S_2$ and $1 \leq i \leq n$ & n is positive integer$\}$

is an ideal of R.

Proof: Since S_1 & S_2 are two ideals of R.

$\therefore 0 \in S_1$ and $0 \in S_2$

$\Rightarrow 0 = 0.0 \in S_1.S_2$

$\Rightarrow 0 \in S_1.S_2$

$\therefore S_1S_2 \neq \phi$ and subset of R.

Let $x, y \in S_1S_2$ choosing $x = a_1b_1 + a_2b_2 + \cdots + a_nb_n$

$y = \alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_m\beta_m$

where $a_i \in S_1$, $b_i \in S_2$

$\alpha_j \in S_1$, $\beta_j \in S_2$

$1 \leq i \leq n$, $1 \leq j \leq m$ } n, m are +ve integer.

then $x - y = (a_1b_1 + a_2b_2 + \cdots + a_nb_n) - (\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_m\beta_m)$

$= a_1b_1 + a_2b_2 + \cdots + a_nb_n + (-\alpha_1)\beta_1 + (-\alpha_2)\beta_2 + \cdots$

$\cdots + (-\alpha_m)\beta_m$

$= x_1y_1 + x_2y_2 + \cdots + x_ky_k$ ($\because k = m+n$)

$\in S_1S_2$ ($\because x_\ell \in S_1$, $y_\ell \in S_2$, $1 \leq \ell \leq k$, ℓ is +ve integer.

$\therefore x - y \in S_1S_2$

$\therefore S_1.S_2$ is a subgroup of R.

Let $r \in R$, $x \in S_1S_2$ choosing $x = a_1b_1 + a_2b_2 + \cdots + a_nb_n$

$a_i \in S_1$, $b_i \in S_2$

$1 \leq i \leq n$;

n is +ve integer

then $rx = r(a_1b_1 + a_2b_2 + \cdots + a_nb_n)$

$= (ra_1)b_1 + (ra_2)b_2 + \cdots + (ra_n)b_n$

$= c_1 b_1 + c_2 b_2 + \cdots + c_n b_n$

where $c_1 = ra_1$

$c_2 = ra_2, \cdots, c_n = ra_n$

and c is belong to S_1

$\in S_1 S_2$ $\quad 1 \le i \le n.$

Similarly $xr \in S_1 S_2$

$\therefore S_1 \cdot S_2$ is an ideal of R.

→ If A and B are two ideals of a ring R, then $AB \subseteq A \cap B$

Proof: Given that R is a ring

and A & B are ideals of R.

$\therefore$ AB and $A \cap B$ are ideals of R

Now we prove that $AB \subseteq A \cap B$

Let $x \in AB$ then $x = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$

where $a_i \in A$, $b_i \in B$; $1 \le i \le n$, n is +ve integer.

Now $a_i \in A, b_i \in R \Rightarrow a_i b_i \in A$ ($\because$ A is right ideal of R)

$\Rightarrow a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \in A$

$\Rightarrow x \in A$

Now $a_i \in R, b_i \in B \Rightarrow a_i b_i \in B$ ($\because$ B is left ideal of R)

$\Rightarrow a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \in B$

$\Rightarrow x \in B$

$\therefore x \in A \cap B$

$\therefore x \in AB \Rightarrow x \in A \cap B$

$\therefore AB \subseteq A \cap B$

→ If A and B are two ideals of a ring R, then $AB \subseteq A+B$

Sol'n: Given that R is a ring and A & B are ideals of R.

∴ AB and A+B are also ideals of R.

Now we Prove that $AB \subseteq A+B$

Let $x \in AB$ then $x = a_1b_1 + a_2b_2 + \cdots + a_nb_n$, where $a_i \in A, b_i \in B$, $1 \le i \le n$.

Now $a_1 \in A, b_1 \in R \Rightarrow a_1b_1 \in A$ (∵ A is right ideal of R)

Again $a_i \in R, b_i \in B \Rightarrow a_ib_i \in B$; $2 \le i \le n$ (∵ B is right ideal of R)

$\Rightarrow a_2b_2 + a_3b_3 + \cdots + a_nb_n \in B$

∴ $a_1b_1 + (a_2b_2 + a_3b_3 + \cdots + a_nb_n) \in A+B$

$\Rightarrow x \in A+B$

∴ if $x \in AB$ then $x \in A+B$

Hence $AB \subseteq A+B$

2007 VM → Let $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in Z \right\}$. show that R is a ring under matrix addition and multiplication.

Let $A = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a,b \in Z \right\}$. Then show that A is a left ideal of R but not a right ideal of R.

Sol'n: Let $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in Z \right\}$

Now we show that R is a ring w.r.t $+^n$ and $\times^n$.

(i) (1) Closure Prop:

$\forall A,B \in R \Rightarrow A+B \in R$

∴ R is closed under $+^n$

(ii) Associative Prop: $\forall A,B,C \in R \Rightarrow (A+B)+C = A+(B+C)$

∴ R is associative under $+^n$.

(iii) Existence of left identity :

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$; $a, b, c, d \in Z$

$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$, $0 \in Z$ then

$$O + A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= \begin{bmatrix} 0+a & 0+b \\ 0+c & 0+d \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (\because 0, a \in Z \Rightarrow 0+a = a)$$

$$= A$$

$\therefore \forall A \in R$, $\exists 0$ (null matrix) $\in R$ such that

$$0 + A = A.$$

$\therefore$ Identity prop. is satisfied w.r.t $+^n$.

Here 0 (null matrix) is the left identity in R.

(iv) Existence of left Inverse:

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$, $a, b, c, d \in Z$

$B = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in R$, $-a, -b, -c, -d \in Z$ then

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

$$= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad (\because -a+a = -b+b = -c+c = -d+d = 0)$$

$$= 0$$

$\therefore \forall A \in R$, $\exists B = -A \in R$ such that

$$B + A = 0$$

$\therefore B = -A$ is left inverse of A in R w.r.t $+^n$.

(V) Commutative Prop:

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

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

(VI) (i) Closure Prop:

$\forall A, B \in R \Rightarrow A \cdot B \in R$

(ii) Associative Prop:

$\forall A, B, C \in R \Rightarrow (A \cdot B) \cdot C = A \cdot (B \cdot C)$

$\therefore (R, \cdot)$ is a Semigroup.

(VII) Distributive laws:

$\forall A, B, C \in R$

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

R satisfies LDL

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

Given that $A = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a, b \in Z \right\} \subseteq R$

Since $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in A$

$\therefore A \neq \phi$

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

then $A_1 - A_2 = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$ $a_1, b_1, a_2, b_2, 0 \in Z$

$= \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & 0 \end{bmatrix} \in A \quad (\because a_1 - a_2, b_1 - b_2 \in Z)$

$\therefore$ A is a subgroup of R.

Let $A_1 = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} \in A$, $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$

$a_1, b_1 \in Z$ $\quad$ $a, b, c, d \in Z$

then $BA_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} = \begin{bmatrix} aa_1+bb_1 & 0 \\ ca_1+db_1 & 0 \end{bmatrix}$

$\in A \quad (\because aa_1+bb_1, ca_1+db_1 \in Z)$.

$\therefore$ A is the left ideal in R.

Now $A_1.B = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$= \begin{bmatrix} a_1a & a_1b \\ b_1a & b_1b \end{bmatrix} \notin A$

$\therefore$ A is not the right ideal in R.

H.W → show that the set $S = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / a, b \in I \right\}$ is a right ideal of M_2, the ring of 2×2 matrices over integers, which is not a left ideal of M_2.

→ Let R be a ring and $a \in R$, show that the set $S = \{r \in R / ra = 0\}$ is a left ideal of R.

Sol^n: Since $0a = 0$

$\therefore 0 \in S$

$\Rightarrow S \neq \phi$ and S subset of R.

Now let $r_1, r_2 \in S$, $r_1a = 0$, $r_2a = 0$.

Now $(r_1 - r_2)a = r_1a - r_2a$

$= 0 - 0$

$= 0$.

$\therefore \boxed{r_1 - r_2 \in S}$

$\therefore$ S is a subgroup of R.

For any $r \in R$ and $x \in S$,

$$(rx)a = r(xa)$$
$$= r(0)$$
$$= 0$$

$\therefore \boxed{rx \in S}$

Hence S is a left ideal of R.

→ Let R be the ring of all real valued, continuous functions on $[0,1]$. Show that the set $S = \{f \in R / f(\tfrac{1}{2}) = 0\}$ is an ideal of R.

Sol'n: Let $f, g \in S$. Then $f(\tfrac{1}{2}) = 0$ and $g(\tfrac{1}{2}) = 0$ —— (1)

Consider $(f-g)(\tfrac{1}{2}) = f(\tfrac{1}{2}) - g(\tfrac{1}{2})$

$= 0 - 0$

$= 0$ (by (1))

$\therefore (f-g)(\tfrac{1}{2}) = 0$

$\Rightarrow \boxed{f-g \in S}$

$\therefore$ S is a subgroup of R.

Let $f \in S$ and $h \in R$. Then

$$(fh)(\tfrac{1}{2}) = f(\tfrac{1}{2})\, h(\tfrac{1}{2})$$
$$= 0 \cdot h(\tfrac{1}{2}) \text{ (by (1))}$$
$$= 0$$

$\therefore (fh)(\tfrac{1}{2}) = 0$

$\Rightarrow \boxed{fh \in S}$

Now $(hf)(\tfrac{1}{2}) = h(\tfrac{1}{2}) f(\tfrac{1}{2})$

$= h(\tfrac{1}{2}) \cdot 0$ (by (1))

$= 0$

$\therefore \boxed{hf \in S}$

$\therefore fh, hf \in S \ \forall f \in S$ and $h \in R$

Hence S is an ideal of R.

→ Let R be the ring of all real valued continuous-functions on $[0,1]$. Show that the set $S = \{f \in R / f(2/3) = 0\}$ is an ideal of R

→ If U is an ideal of R, then Prove that $r(u) = \{x \in R / xu = 0 \ \forall u \in U\}$ is an ideal of R.

Sol'n: Since $0u = 0 \ \forall u \in U$

$\therefore 0 \in r(U)$

$\therefore r(U) \neq \phi$ and subset of R

Let $x, y \in r(U)$; $xu = 0$, $yu = 0 \ \forall u \in U$ —— (1)

Now we have

$$(x-y)(u) = x(u) - y(u)$$
$$= 0 - 0 \quad \forall u \in U \ (\text{by } (1))$$
$$= 0$$

$\therefore (x-y)(u) = 0$

$\therefore \boxed{x - y \in r(U)}$

$r(U)$ is a subgroup of R.

Let $a \in R$ and $x \in r(U)$, so that $xu = 0 \ \forall u \in U$ — (2)

Now $(ax)u = a(xu)$

$= a(0)$ (by (2))

$= 0$

$\therefore (ax)u = 0 \ \forall u \in U$

$\Rightarrow ax \in r(U)$

Again $(xa)u = x(au)$

$= xy$ where $y = au$.

Since U is an ideal of R,

So $a \in R$ and $u \in U \Rightarrow au \in U$

$\Rightarrow y \in U$ — (3)

from (2) and (3), we have,

$xy = 0$

$\Rightarrow x(au) = 0$

$\Rightarrow (xa)u = 0$

$\therefore (ra)u = 0 \quad \forall\, u \in U$

$\Rightarrow ra \in r(U)$

Hence $r(U)$ is an ideal of R.

HW → If R is a ring and L is a left ideal of R. then $\lambda(L) = \{x \in R / xa = 0 \ \forall\, a \in L\}$ is a two-sided ideal of R.

→ If U is an ideal of R, then Prove that $[R:U] = \{x \in R / rx \in U \text{ for every } r \in R\}$. is an ideal of R and that it Contains U.

Sol'n: Since U is an ideal of R,

So $0 \in U$, i.e. $r0 \in U \ \forall\, r \in R$

$\therefore 0 \in [R:U]$

and $[R:U] \neq \phi$ and subset of R.

Let $x, y \in [R:U]$, $rx \in U$ & $ry \in U$ —— ① $\forall\, r \in R$

Since U is an ideal of R.

$\therefore rx - ry \in U \ \forall\, r \in R$.

Now $r(x-y) = rx - ry \in U \ \forall\, r \in R$

$\Rightarrow x - y \in [R:U]$

$\therefore [R:U]$ is a subgroup of R.

Using ①, $(ra)x \in U \quad (\because ra \in R)$

we have

$r(ax) = (ra)x \in U \ \forall\, r \in R$

$\Rightarrow \boxed{ax \in [R:U]}$

Since U is an ideal of R,

So $rx \in U$ and $a \in R$

$\Rightarrow (\forall x) a \in U \Rightarrow r(xa) \in U \quad \forall r \in R$

$\Rightarrow \boxed{xa \in [R:U]}$

Hence $[R:U]$ is an ideal of R.

Now we show that $U \subseteq [R:U]$

Let $x \in U$. Then $rx \in U \ \forall r \in R$ ($\because U$ is an ideal of R)

Now $rx \in U \ \forall r \in R$

$\Rightarrow x \in [R:U]$

$\Rightarrow U \subseteq [R:U]$

Hence $[R:U]$ is an ideal of R containing U.

→ Prove that $Z(R)$, the centre of a ring R, is only a subring of R and need not be an ideal of R.

Sol'n: By definition, $Z(R) = \{a \in R / xa = ax \ \forall x \in R\}$

It can be easily shown that $Z(R)$ is a subring of R.
(Work done by student)

Let M_2 be the ring of all 2×2 matrices over the integers.

For any $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2$ and

$A = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \in M_2$

Now $Ax = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ap & bp \\ cp & dp \end{pmatrix}$

$= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} = xA$

Hence $Z(M_2) = \left\{ \begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix} \Big/ p \text{ is integer} \right\}$

Now we show that $Z(M_2)$ is not an ideal of M_2.

For $S = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in M_2$, $A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in Z(M_2)$

We have

$$SA = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} \notin Z(M_2)$$

Hence $Z(M_2)$ is not an ideal of M_2.

→ Let A and B be two ideals of a commutative ring R with unity such that $A+B=R$.

show that $AB = A \cap B$.

Sol^n: Given that A and B are two ideals of a commutative ring R with unity such that $A+B=R$.

Now we show that $AB = A \cap B$

Since A and B are two ideals of R

$\therefore AB \subseteq A \cap B$ — ①

Let $x \in A \cap B$ be arbitrary

Since $R = A+B$ and $1 \in R$

$\therefore 1 \in A+B$

$\Rightarrow 1 = a+b$ for some $a \in A$ & $b \in B$

Now $x = x.1$

$= x(a+b)$

$= xa+xb$ — ①

since $x \in A$ and $b \in B \Rightarrow xb \in AB$

$x \in B$ and $a \in A \Rightarrow ax \in AB$

$\Rightarrow xa \in AB$ ($\because$ R is Commutative)

$\therefore xa+xb \in AB$ ($\because$ AB is an ideal of R)

$\therefore$ By ①, $x \in AB$

$\therefore x \in A \cap B \Rightarrow x \in AB$

$\therefore A \cap B \subseteq AB$ —— (2)

$\therefore$ from (1) & (2) we have

$$AB = A \cap B$$

Note: Two ideals A and B of a ring R satisfying $A+B=R$ are called co-maximal ideal.

→ If A, B and C are ideals of a ring R, Prove that

$A(B+C) = AB+AC$.

Sol'n: Since A, B and C are ideals of a ring R.

$\therefore B+C$, AB, AC, $A(B+C)$ and $AB+AC$ are also ideals of R.

For any $b \in B$, $b = b+0 \in B+C$ $(\because 0 \in C)$

$\therefore B \subseteq B+C$ —— (1)

Similarly $C \subseteq B+C$ —— (2)

from (1) & (2) we have

$AB \subseteq A(B+C)$

and $AC \subseteq A(B+C)$

$\Rightarrow AB+AC \subseteq A(B+C)$ —— (3)

Now let $x \in A(B+C)$ be arbitrary.

Then $x = a_1t_1 + a_2t_2 + \cdots + a_nb_n$ where $a_i \in A$, $t_i \in B+C$.

Since $t_i \in B+C$

$\therefore t_i = b_i + c_i$ for some $b_i \in B$, $c_i \in C$

$\therefore x = a_1(b_1+c_1) + a_2(b_2+c_2) + \cdots + a_n(b_n+c_n)$

$= (a_1b_1 + a_2b_2 + \cdots + a_nb_n) + (a_1c_1 + a_2c_2 + \cdots + a_nc_n)$

$\in AB+AC$

$\therefore A(B+C) \subseteq AB+AC$ —— (4).

$\therefore$ from (3) & (4) we have

$A(B+C) = AB+AC$.

→ If A, B, C are ideals of a ring R such that $B \subseteq A$, Prove that $A \cap (B+C) = B + (A \cap C) = (A \cap B) + (A \cap C)$

Sol'n: Given that A, B, C are ideals of a ring R such that $B \subseteq A$

$\therefore B+C$, $A \cap C$ and $A \cap (B+C)$, $B + (A \cap C)$ are also ideals of R.

Let $x \in A \cap (B+C)$

Then $x \in A$ and $x \in B+C$

We have $x \in B+C \Rightarrow x = b+c$, for some $b \in B$, $c \in C$.

Thus $b+c \in A$ ($\because x \in A$)

and $b \in A$ ($\because B \subseteq A$)

$\Rightarrow b+c-b \in A$ ($\because A$ is an ideal of R)

$\Rightarrow c \in A$

$\therefore$ we have $c \in C$ & $c \in A$

$\Rightarrow c \in A \cap C$

$\therefore x = b+c \Rightarrow x \in B + (A \cap C)$

$\therefore A \cap (B+C) \subseteq B + (A \cap C)$ ——— (1)

Let $x \in B + (A \cap C)$

$\Rightarrow x = b_1 + c_1$, for some $b_1 \in B$, $c_1 \in A \cap C \Rightarrow c_1 \in A$ & $c_1 \in C$

$\Rightarrow x \in B+C$ as $b_1 \in B$, and $c_1 \in C$

Again $B \subseteq A \Rightarrow b_1 \in A$, Also $c_1 \in A$

$\Rightarrow x = b_1 + c_1 \in A$, as A is an ideal of R.

Thus $x \in A$ and also $x \in B+C$

$\Rightarrow x \in A \cap (B+C)$

$\therefore B + (A \cap C) \subseteq A \cap (B+C)$ ——— (2)

from (1) & (2)

We obtain $A \cap (B+C) = B + (A \cap C)$

Since $B \subseteq A$, so $A \cap B = B$.

Hence $A \cap (B+C) = B + (A \cap C) = (A \cap B) + (A \cap C)$

→ Let R be a commutative ring and let A be an ideal of R. Show that

$\sqrt{A} = \{x \in R \mid x^n \in A \text{ for some positive integer } n\}$ is an ideal of R such that (i) $A \subseteq \sqrt{A}$ (ii) $\sqrt{\sqrt{A}} = \sqrt{A}$ (iii) If R has unity and $\sqrt{A} = R$, then $A = R$

Sol'n: Let $a, b \in \sqrt{A}$

Then $a^m \in A$ and $b^n \in A$, for some positive integers m and n.

Since R is commutative ring.

$$(a-b)^{m+n} = a^{m+n} - (m+n)C_1 a^{m+n-1} b + \cdots + (-1)^{m+n} b^{m+n}$$

$$= a^m \cdot a^n - (m+n)C_1 a^m a^{n-1} b + \cdots + (-1)^{m+n} b^m b^n \in A$$

($\because a^m \in A, b^n \in A$ and A is an ideal of R)

$\therefore a - b \in \sqrt{A}$

For any $r \in A$, $a \in \sqrt{A}$;

we have $(ra)^m = r^m a^m$, Since R is commutative.

Again $r^m a^m \in A$, ($\because a^m \in A$, $r^m \in R$ and A is an ideal of R)

$\therefore ra \in \sqrt{A}$

Similarly, $ar \in \sqrt{A}$

Hence $\sqrt{A}$ is an ideal of R.

(i) Obviously, $A \subseteq \sqrt{A}$ ($\because x \in A \Rightarrow x^r \in A$, as A is an ideal of R)

(ii) we have $\sqrt{\sqrt{A}} = \sqrt{S}$ where $S = \sqrt{A}$

By part (i) $S \subseteq \sqrt{S} \Rightarrow \sqrt{A} \subseteq \sqrt{\sqrt{A}}$, —— (1)

Let $x \in \sqrt{\sqrt{A}} \Rightarrow x \in \sqrt{S} \Rightarrow x^n \in S$ for some $n \in N$.

$\Rightarrow x^n \in \sqrt{A}$

$\Rightarrow (x^n)^m \in A$, for some $m \in N$

$\Rightarrow (x^{nm}) \in A$, where $nm \in N$

$\Rightarrow x \in \sqrt{A}$

$\therefore$ we have $x \in \sqrt{\sqrt{A}} \Rightarrow x \in \sqrt{A}$

$\Rightarrow \sqrt{\sqrt{A}} \subseteq \sqrt{A}$ —— (2)

$\therefore$ from ① & ②

$$\sqrt{\sqrt{A}} = \sqrt{A}$$

(iii) Let $1 \in R$ and $\sqrt{A} = R$

Then $1 \in \sqrt{A} \Rightarrow 1^n \in A$, for some Positive integer n.

$\Rightarrow 1 \in A$ and A is an ideal of R

$\Rightarrow 1.r \in A \ \forall r \in R$

$\Rightarrow r \in A \ \forall r \in R$

$\Rightarrow R \subseteq A$

Obviously

Hence $A = R$

Note: $\sqrt{A}$ is often called the radical of A.

→ Let R be a ring with unity. If R has no right ideals except R and $\{0\}$, then Prove that R is a division ring.

(or)

Let R be ring with unit element, R not necessarily commutative, such that the only right ideals of R are $\{0\}$ and R. Prove that R is a division ring.

Soln: Given that R is a ring with unit element and R has no right ideals except R and $\{0\}$,

i.e. R has ideals $\{0\}$ and R.

Now we Prove that R is a division ring

For this we are enough to Prove that the non-zero elements of R Possesses inverse w.r.t x^n.

Let $a (\neq 0) \in R$

Let $aR = \{ar / r \in R\} \subseteq R$ —— ①

Since $0 \in R$, $a(0) \in aR$

$\Rightarrow 0 \in aR$

$\therefore aR \neq \phi$

$\therefore aR$ is a non-empty subset of R.

Let $x, y \in aR$ choosing $x = ar_1$,

$y = ar_2$; $r_1, r_2 \in R$

then we have $x - y = ar_1 - ar_2$

$= a(r_1 - r_2)$

$\in aR$ $(\because r_1 - r_2 \in R)$

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

Let $x \in R$, $y \in aR$ choosing $y = ar$; $r \in R$

then $yx = (ar)x$

$= a(rx)$

$\in aR$ $(\because r \in R, x \in R \Rightarrow rx \in R)$

$\therefore aR$ is a right ideal of R

Since $a(\neq 0) \in R$; $1 \in R$

$\therefore a \cdot 1 \in aR$

$\Rightarrow a \in aR$

$\therefore aR$ contains non-zero elements of R.

$\therefore aR \neq \{0\}$

Since R has no proper right ideals.

$\therefore aR = R$.

Let one of the element of aR be 1. ($\because R$ is ring with unity).

Let $ab = 1$ for some $b \in R$ ——— (1)

from (1), it follows that each non-zero element of R has a right inverse.

since $b(\neq 0) \in R$ (for otherwise, $1 = ab = 0$, a contradiction)

there exists some $c \in R$ such that $bc = 1$ ——— (2)

Now we have

$ba = ba \cdot 1$, 1 is the unity of R.

$= (ba)(bc)$ (by ②)

$= b(ab)c$ (by associative of R)

$= b(1)c$ (by ①)

$= bc$

$= 1$ (by ②)

$\therefore ab = ba = 1$

$\Rightarrow a^{-1} = b \in R$

Hence R is a division ring.

Note: Let R be a ring with unity. If R has no left ideals except R and $\{0\}$, then Prove that R is a division ring.

→ Let R be a ring having more than one element such that $aR = R \ \forall \ a \neq 0 \in R$, then R is a division ring.

Sol'n: Firstly we shall show that

$x \neq 0$ and $y \neq 0$ in R

$\Rightarrow x.y \neq 0$

(Or)

$xy = 0 \Rightarrow$ either $x = 0$ or $y = 0$, $x, y \in R$ ——— ①

If $x \neq 0$ and $y \neq 0$ then by given hypothesis

$xR = R$, $yR = R$ ——— ②

Now we have

$0 = xy \Rightarrow 0.R = (xy)R$

$= x(yR)$

$= xR$ (by ②)

$= R$ (by ②)

$\therefore 0.R = R.$

$\therefore R=\{0\}$, a contradiction to the fact that R has more than one element.

Hence ① is Proved.

Since $R \neq \{0\}$

i.e. R contains non-zero elements.

$\exists$ some $a \neq 0 \in R$ such that $aR=R$

Now $a \in R \Rightarrow a \in aR$

$\Rightarrow a=ae$ for some $e \in R$

It may be noted that

$e \neq 0$, for otherwise $a=ao=0$, a contradiction.

$\therefore ae=a$

$\Rightarrow ae^2=ae$

$\Rightarrow a(e^2-e)=0$

$\Rightarrow e^2-e=0$ (by ①)

$\Rightarrow e^2=e$ —— ②

Let $x \in R$ be arbitrary. Then

$(xe-x)e = xe^2-xe$

$= xe-xe$

$= 0$ (by ②)

$\therefore (xe-x)e=0$

Since $e \neq 0$ and using ①,

$xe-x=0$

$\Rightarrow xe=x \ \forall \ x \in R$

$\Rightarrow$ e is the right identity of R —— ③

Now we shall show that

each non-zero element of R has a right inverse.

Let $x \neq 0 \in R$ then by given hypothesis,

$xR=R$

Since $e \in R$, $e \in xR$

$\Rightarrow e=xy$ for some $y \in R$

$\Rightarrow$ y is the right inverse of x. —— ④

from ③ and ④, it follows that

R is a division ring.

* Ideal Generated By a Subset of Ring:

Let s be a subset of a ring R. An ideal U of the ring R is said to be generated by 's' if (i) $S \subseteq U$

(ii) for any ideal V of R, $S \subseteq V \Rightarrow U \subseteq V$

The ideal U generated by S is denoted by (S) or $\langle S \rangle$ or $\{S\}$ or $(S) = U$

Indeed, $\langle S \rangle$ is the smallest ideal containing 's'.

→ If A and B are any two ideals of a ring R. Show that A+B is an ideal of R generated by A∪B. i.e. $A+B = (A \cup B)$.

Sol'n: Given that A and B are two ideals of the ring R.

∴ A+B is also an ideal of R.

For any $a \in A$, $a = a+0 \in A+B$

$\therefore A \subseteq A+B$ —— ①

Similarly $B \subseteq A+B$ —— ②

∴ from ① & ② we have

$A \cup B \subseteq A+B$ —— ③

Let I be any ideal of R such that $A \cup B \subseteq I$ —— ④

Now we shall Prove that $A+B \subseteq I$ —— ⑤

Let $x \in A+B$ then $x = a+b$, $a \in A$, $b \in B$.

Since $A \subseteq A \cup B$ and $B \subseteq A \cup B$

$\therefore a, b \in A \cup B$

$\Rightarrow a, b \in I$ from (4)

$\Rightarrow a+b \in I$ ($\because I$ is an ideal of R)

$\Rightarrow x \in I$

$\therefore x \in A+B \Rightarrow x \in I$

$\therefore A+B \subseteq I$

from ③, ④ and ⑤, we have

$$A+B = (A \cup B)$$

* Principal Ideal:

If an ideal U of a ring R generated by a single element $S=\{a\}$ then U is called a principal Ideal of the ring R. The Principal ideal U of the ring R is the smallest ideal containing the element 'a'.

→ An ideal U of a ring R is said to be a Principal ideal of R, if $\exists\ a \in U$ such that for any ideal V of R and $a \in V \Rightarrow U \subset V$.

The principal ideal U of the ring R generated by the element 'a' is denoted by (a) or $\langle a \rangle$.

Note: 1. If R is a ring and $a \in R$. we can speak of left and right principal ideals.

2. U is a principal ideal of the ring R generated by the element $a \in R \Rightarrow$

(i) $a \in U$, (ii) U is an ideal of R and

(iii) V is any ideal of R and $a \in V$ then $U \subset V$.

3. The null ideal of a ring is the principal ideal generated by the zero element of the ring.
The unit ideal of a ring is the principal ideal generated by the unit element of the ring.

4. Since a field has no Proper ideals, every ideal of a field is a principal ideal.

Theorem: If R is commutative ring with unit element and $a \in R$, then the set $U = \{ra / r \in R\}$ is a principal ideal of R generated by the element 'a'.

Proof: For $1 \in R$, $1a = a \in U$

Let $x, y \in U$ and $s \in R$

Then $x = r_1 a$, $y = r_2 a$ where $r_1, r_2 \in R$

Now $x - y = r_1 a - r_2 a$

$= (r_1 - r_2) a$

$= r' a \in U$ where $r' = r_1 - r_2 \in R$

Now $sx = s(r_1 a)$

$= (sr_1) a$

$= r'' a \in U$ where $r'' = sr_1 \in R$

Since R is commutative,

$sx = rs$

$\therefore U$ is an ideal of R.

Let V be any other ideal of R such that $a \in V$

Now we shall show that $U \subseteq V$

Now $x \in U \Rightarrow x = r_1 a \in U$ where $r_1 \in R$

Since $a \in V$, $r_1 \in R$

and V is an ideal.

$\therefore r_1 a \in V$

$\Rightarrow x \in V$

$\therefore x \in U \Rightarrow x \in V$

$\Rightarrow U \subseteq V$.

Hence U is principal ideal of R generated by 'a'

Note: (1). If R is Commutative ring with unity and $a \in R$ then the set $\{ar / r \in R\}$ is the principal ideal generated by 'a' as $\{ar / r \in R\} = \{ra / r \in R\}$.

(2) If R is Commutative ring and $a \in R$ then the $\{ra + na / r \in R, n \in R\}$ is the principal ideal of R generated by 'a'.

Example: $R = I$ is a Commutative ring of integers with unit element. i.e. $R = \{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$

$S_1 = \{2n / n \in I\} = \{\ldots -6, -4, -2, 0, 2, 4, 6, \ldots\}$

$S_2 = \{3n / n \in I\} = \{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}$

$S_3 = \{4n / n \in I\} = \{\ldots -12, -8, -4, 0, 4, 8, 12 \ldots\}$

$S_4 = \{6n / n \in I\} = \{\ldots -18, -12, -6, 0, 6, 12, 18 \ldots\}$

Now

(1) $6 \in S_4 \subseteq S_2$, $S_4 \subseteq S_1$, $S_4 \subseteq I$

$\therefore S_4 = (6)$.

(2) $3 \in S_2 \subseteq I$

$\therefore S_2 = (3)$

(3) $4 \in S_3 \subseteq S_1 \subseteq I$

$\therefore S_3 = (4)$

(4) $S_1 = (2)$ $(\because S_1 \subseteq I)$

* Principal Ideal Ring:

A ring R is called a principal ideal ring if every ideal in R is a principal ideal.

A ring R is called a principal ideal ring if every ideal in R is a Poincipal ideal.

* Principal Ideal Domain (PID):

A commutative ring without zero divisors and with unity element is a principal ideal domain, if every ideal S in R is a poincipal ideal

i.e. if every ideal S in R is of the form $S=(a)$ for some $a \in S$.

Theorem: Every field is a principal ideal domain

proof: We know that a field has no proper ideals.

i.e. the ideals of the field F are $\{0\}$ and F

Let S be an ideal of R.

- If $S=\{0\}$ then it is a principal ideal generated by '0'.
- If $S \neq \{0\}$ then S contains non-zero elements.

Let $a(\neq 0) \in S \subseteq F$ —— ①

$\therefore a^{-1}$ exists in F

$\therefore a^{-1} \in F$, $a(\neq 0) \in S \Rightarrow a^{-1}a \in S$ ($\because S$ is an ideal)

$\Rightarrow 1 \in S$

$\therefore F \subseteq S$ —— ②

$\therefore$ from ① & ② we have

$F=S$

$\therefore$ Another ideal containing 1 is F

i.e. $S=F=(1)$

$\therefore$ The two ideals of F are principal ideals.

$\therefore$ F is a PID.

→ for example : $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are principal ideal domains.

Theorem: the ring of integers is a PID.

(or)

Every ideal of the ring of integers is a principal ideal.

Proof: Given that I be the ring of integers.

and I is commutative ring with unity and without zero divisors.

Let S be an ideal of I.

- If $S=\{0\}$ then it is a principal ideal generated by '0'.
- If $S\neq\{0\}$ then S contains non-zero elements.

Let $a(\neq 0) \in S$

$\Rightarrow -a \in S$ ($\because$ the ideal S is additive subgroup of I)

$\therefore S$ contains +ve and -ve integers.

Let s be the least +ve integer in S.

Let P be any element in 's'

$\therefore$ By divison algorithm, $\exists$ integers q, r

such that $P = sq + r \quad (0 \leq r < s)$

Now $q \in I, s \in S \Rightarrow sq \in S$ & $qs \in S$ ($\because S$ is an ideal)

$P \in S, sq \in S \Rightarrow P - sq \in S$ ($\because S$ is subgroup of $(I,+)$)

$\Rightarrow r \in S$ where $0 \leq r < s$

which contradicts the fact s is the least +ve integer that belongs to S.

$\therefore r = 0$

$\therefore P = sq$

$\therefore P \in S \Rightarrow p = sq$ for some $q \in I$.

Hence S is a principal ideal of I generated by s.

i.e. $S = (s)$

* Quotient Rings (or) Rings of Residue Classes:

Suppose R is an arbitrary ring and 's' is an ideal (two sided ideal) in R. then S is a subgroup of the additive abelian group of R.

therefore if $a \in R$ then the set

$S+a = \{s+a / s \in S\}$ is called right coset of S in R.

Since R is abelian group w.r.t $+^n$

$$S+a = a+S$$

i.e. the right coset is same as left coset.

we call $S+a$ as simply a coset of S in R.

Note: (1) if $a, b \in R$ then $S+a = S+b \Leftrightarrow a-b \in S$

(2) $a \in S \Leftrightarrow S+a = S$.

The cosets of S in R are called the residue classes of S in R. The set of all residue classes of S in R is denoted by the symbol $\frac{R}{S}$.

i.e. $\frac{R}{S} = \{S+a / a \in R, S \text{ is an ideal of } R\}$

Theorem If S is an ideal of a ring R, then the set $\frac{R}{S} = \{S+a / a \in R\}$ of all residue classes of S in R forms a ring for the two compositions in $\frac{R}{S}$ defined as follows:

$$(S+a)+(S+b) = S+(a+b) \quad \text{---(1)} \quad \text{(addition of residue classes)}$$

$$(S+a)(S+b) = S+ab \quad \text{---(2)} \quad \text{(multiplication of residue classes)}$$

Proof: First of all, we shall show that both $+^n$ and $\times^n$ in $\frac{R}{S}$ are well defined.

For this we are to show that

if $S+a = S+a'$ and

$S+b = S+b'$ then

$$(S+a)+(S+b) = (S+a')+(S+b')$$

and $(S+a)(S+b) = (S+a')(S+b')$

Now we have

$S+a = S+a' \Rightarrow a' \in S+a$ [$\because a' = 0+a' \in S+a'$
$\Rightarrow a' \in S+a' = S+a$
$\Rightarrow a' \in S+a$]

and $S+b = S+b' \Rightarrow b' \in S+b$

$\therefore \exists\ \alpha, \beta \in S$ such that $a' = \alpha + a$, $b' = \beta + b$

Now $a'+b' = (\alpha+a) + (\beta+b)$

$= (a+b) + (\alpha+\beta)$

$\Rightarrow (a'+b') - (a+b) = (\alpha+\beta \in S$ ($\because \alpha, \beta \in S$)

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

$\Rightarrow \boxed{S+(a'+b') = S+(a+b)}$

$\Rightarrow (S+a') + (S+b') = (S+a) + (S+b)$

$\therefore$ addition in $\frac{R}{S}$ is well defined.

Again $a'b' = (\alpha+a)(\beta+b)$

$= \alpha\beta + \alpha b + a\beta + ab$

$= ab + \alpha\beta + \alpha b + a\beta$

$\Rightarrow a'b' - ab = \alpha\beta + \alpha b + a\beta \in S$ ($\because S$ is an ideal therefore $\alpha, \beta \in S$ and $a, b \in R \Rightarrow \alpha b \in S, a\beta \in S, \alpha\beta \in S \Rightarrow \alpha\beta + \alpha b + a\beta \in S$)

Since $a'b' - ab \in S$

$\Rightarrow S + a'b' = S + ab$

$\Rightarrow (S+a')(S+b') = (S+a)(S+b)$

Hence multiplication in $\frac{R}{S}$ is well defined.

(i) Let $S+a, S+b \in \frac{R}{S}$; $a, b \in R$

then $(S+a) + (S+b) = S + (a+b)$ (by ①)

$\in \frac{R}{S}$ ($\because a+b \in R$)

and $(S+a)(S+b) = S + (ab)$ (by ②)

$\in \frac{R}{S}$ ($\because ab \in R$)

$\therefore$ closure is satisfied w.r.t $+_n$ & $\times_n$.

(ii) Let $S+a, S+b, S+c \in \frac{R}{S}$; $a,b,c \in R$

then $(S+a)+[(S+b)+(S+c)] = (S+a)+[S+(b+c)]$

$= S+[a+(b+c)]$

$= S+[(a+b)+c]$ ($\because R$ is a ring)

$= [S+(a+b)]+(S+c)$

$= [(S+a)+(S+b)]+(S+c)$

Associative property is satisfied w.r.t $+_n$.

(iii) $0 \in R \Rightarrow S+0 = S \in \frac{R}{S}$

Now $(S+a)+(S+0) = S+(a+0)$

$= S+a$ ($\because a+0=a \ \forall a \in R$)

Similarly $(S+0)+(S+a) = S+a$.

$\therefore \forall (S+a) \in \frac{R}{S}, a \in R, \exists S+0 = S \in \frac{R}{S}, 0 \in R$

such that $(S+a)+(S+0) = S+a = (S+0)+(S+a)$

Identity property is satisfied w.r.t $+_n$.

Here $S+0 = S$ is the identity element in $\frac{R}{S}$.

(iv) $a \in R \Rightarrow -a \in R$

$\forall S+a \in \frac{R}{S}, \exists S+(-a) \in \frac{R}{S}$ such that

$(S+a)+[S+(-a)] = S+[a+(-a)]$

$= S+0$ ($\because a+(-a)=0$ in R)

Similarly $[S+(-a)]+(S+a) = S+0$

$\therefore$ Inverse property is satisfied in $\frac{R}{S}$ w.r.t $+_n$

Here $S+(-a)$ is the inverse of $S+a$ in $\frac{R}{S}$.

(V) Let $S+a, S+b \in \frac{R}{S}$, $a, b \in R$ then

$$(S+a)+(S+b) = S+(a+b)$$
$$= S+(b+a) \quad (\because R \text{ is a ring})$$
$$= (S+b)+(S+a)$$

$\therefore$ Commutative property is satisfied w.r.t $+n$.

$\therefore \left(\frac{R}{S}, +\right)$ is an abelian group.

(VI) Let $S+a, S+b, S+c \in \frac{R}{S}$, $a, b, c \in R$

then $(S+a)[(S+b)(S+c)] = (S+a)[S+(bc)]$ (by ①)

$$= S+[a(bc)] \quad \text{by ②}$$
$$= S+[(ab)c]$$
$$= (S+(ab))(S+c)$$
$$= [(S+a)(S+b)](S+c)$$

$\therefore$ Associative Property is satisfied in $\frac{R}{S}$ w.r.t $\times n$.

$\therefore \left(\frac{R}{S}, \times\right)$ is a semigroup.

(VII) Let $S+a, S+b, S+c \in \frac{R}{S}$, $a, b, c \in R$

then $(S+a)[(S+b)+(S+c)] = (S+a)\cdot[S+(b+c)]$

$$= S+[a\cdot(b+c)]$$
$$= S+[a\cdot b + a\cdot c] \quad (\because R \text{ is a ring})$$
$$= (S+(ab))+(S+(ac))$$
$$= [(S+a)\cdot(S+b)]+[(S+a)\cdot(S+c)]$$

similarly $[(S+b)+(S+c)]\cdot(S+a) = (S+b)\cdot(S+a)+(S+c)\cdot(S+a)$

$\therefore$ multiplication is distributive w.r.t $+n$ in $\frac{R}{S}$.

$\therefore \left(\frac{R}{S}, +, \cdot\right)$ is a ring.

Definition → Let R be a ring and S be an ideal of R then the set $\frac{R}{S} = \{S+a \mid a \in R\}$ of all residue classes of S in R is a ring for the two compositions in R defined as follows

$(S+a)+(S+b) = S+(a+b)$ (addition of residue classes)

$(S+a)\cdot(S+b) = S+(ab)$ (multiplication of residue classes)

This ring $(\frac{R}{S}, +, \cdot)$ is called the quotient ring or factor ring or residue class ring.

Note: It is convenient, sometimes, to denote coset (residue class) $S+a$ in $\frac{R}{S}$ by the symbol $\bar{a}$ or $[a]$. Then we write sum and product of two cosets (residue classes) as $[a]+[b]=[a+b]$ and $[a].[b]=[ab]$

→ If $\frac{R}{S}$ is the quotient ring, prove that

(i) $\frac{R}{S}$ is commutative if R is commutative and

(ii) $\frac{R}{S}$ has unity element if R has unity element.

(iii) $\frac{R}{S}$ is boolean ring if R is the boolean ring

Sol'n: (i) Given that $\frac{R}{S}$ is the quotient ring and R is commutative.

Now we have

$\forall\ S+a, S+b \in \frac{R}{S}$; $a, b \in R$

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

$= S+(ba)$ ($\because$ R is commutative)

$= (S+b)(S+a)$

$\therefore \frac{R}{S}$ is commutative ring

(ii) Given that R has unity

i.e. $\forall\ a \in R, \exists\ 1 \in R$ such that $a.1 = 1.a = a$

Now we have

$\forall\ S+a \in \frac{R}{S}$, $a \in R$, $\exists\ S+1 \in \frac{R}{S}$, $1 \in R$

such that $(S+a)(S+1) = S+(a1)$

$= S+a \quad (\because a1 = 1a = a \text{ in } R)$

Similarly $(S+1)(S+a) = S+a$.

$\frac{R}{S}$ has unity.

$\therefore$ $S+1$ is the unity element in $\frac{R}{S}$.

(iii) we have $(S+a)^2 = (S+a)(S+a)$

$= S+a^2$

$= S+a \quad (\because a^2 = a\ \forall\ a \in R)$

$\forall\ S+a \in \frac{R}{S}$

$\therefore$ $\frac{R}{S}$ is boolean ring.

→ Consider $Z_6 = \{0,1,2,3,4,5\}$, the ring of integers modulo 6. Then $S = \{0,3\}$ is an ideal of Z_6. Determine the quotient ring $\frac{Z_6}{S}$.

Sol'n: Given that $Z_6 = \{0,1,2,3,4,5\}$, the ring of integers modulo 6

$S = \{0,3\} \subseteq Z_6$

Since S is a ring of Z_6

$\therefore (S, +_6)$ is a subgroup of $(Z_6, +_6, \times_6)$

Now let $s \in S$, $r \in Z_6 \Rightarrow sr \in S$ & $rs \in S$

i.e. let $s = 3 \in S$, $r = 4 \in Z_6$

$\Rightarrow s.r = 3 \times_6 4 = 0 \in S$

& $rs = 0 \in S$ etc

$\therefore$ S is an ideal of Z_6.

Now the cosets of S in R are as under:

$S+0 = \{0+0, 3+0\} = \{0,3\}$

$S+1 = \{0+1, 3+1\} = \{1,4\}$

$S+2 = \{0+2, 3+2\} = \{2,5\}$

$S+3 = \{0+3,\ 3+3\} = \{3, 0\} = S+0$

$S+4 = \{0+4, 3+4\} = \{4, 1\} = S+1$

$S+5 = \{0+5, 3+5\} = \{5, 2\} = S+2$

$\therefore \frac{Z_6}{S} = \{S+0, S+1, S+2\}$ is the quotient ring.

→ show that the set $S = \{5x \mid x \in Z\}$ is an ideal of Z. Determine the quotient ring $\frac{Z}{S}$.

Sol'n: It is easy to verify that 'S' is an ideal of Z.

Now we have

$S = \{\ldots -15, -10, -5, 0, 5, 10, 15, \ldots\}$

$S+1 = \{\ldots -14, -9, -4, 1, 6, 11, 16, \ldots\}$

$S+2 = \{\ldots -13, -8, -3, 2, 7, 12, 17, \ldots\}$

$S+3 = \{\ldots -12, -7, -2, 3, 8, 13, 18 \ldots\}$

$S+4 = \{\ldots -11, -6, -1, 4, 9, 14, 19, \ldots\}$

$S+5 = \{\ldots -10, -5, 0, 5, 10, 15, \ldots\}$

$= S+0,$

$S+6 = S+1,\ S+7 = S+2$ etc.

$\therefore \frac{Z}{S} = \{S+0, S+1, S+2, S+3, S+4\}$

* Prime Ideal and Maximal Ideal:

→ Let R be a ring. An ideal P of a ring R is called a prime ideal, if for any $a \in R$, $b \in R$; $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

For example:

(1) The ideal $P = \{0\}$ in Z (ring of integers) is a Prime ideal.

Because, let $a,b \in Z$ such that $a,b \in \{0\}$

$\Rightarrow ab = 0$

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

$\Rightarrow a \in \{0\}$ or $b \in \{0\}$

(2) For any prime numbers P,

$(P) = \{Px / x \in Z\}$ is a prime ideal of Z.

because, let $a,b \in Z$ be such that $ab \in (P)$

$\Rightarrow ab = px$ for some $x \in Z$

$\Rightarrow \frac{ab}{P} = x$ for some $x \in Z$

$\Rightarrow \frac{a}{P}$ or $\frac{b}{P}$

$\Rightarrow a = py$ or $b = pz$ ($\because$ P is prime)

for some $y, z \in Z$

$\Rightarrow a \in (P)$ or $b \in (P)$

In particular, the ideals,

$(2) = \{\cdots -4, -2, 0, 2, 4, \cdots\}$

$(3) = \{\cdots -6, -3, 0, 3, 6, \cdots\}$

$(5) = \{\cdots -10, -5, 0, 5, 10, \cdots\}$ etc are prime ideals of Z.

(3) The ideal $(4) = \{\cdots -12, -8, -4, 0, 4, 8, \cdots\}$ is not a prime ideal of Z.

Since $2.6 = 12 \in (4)$ but $2 \notin (4)$ and $6 \notin (4)$.

Theorem Let R be a Commutative ring. Prove that an ideal P of R is a prime ideal iff R/P is an integral domain.

Proof: Given that R is the Commutative ring and P is an ideal of R.

Let $\frac{R}{P}$ be an Integral Domain

we now Prove that P is a Prime ideal of R.

i.e. $a,b \in R$ and $ab \in P \Rightarrow a \in P$ or $b \in P$.

Now for any $a, b \in R$ and $ab \in P$

$\Rightarrow P+ab = P \quad (\because a \in P \Leftrightarrow P+a = P)$

$\Rightarrow (P+a)\cdot(P+b) = P+0$

$\Rightarrow (P+a) = P+0$ (or)

$P+b = P+0 \quad (\frac{R}{P}$ is an ID)

$\Rightarrow a \in P$ (or) $b \in P \quad (P+a \neq P \Leftrightarrow a \in P)$

$\therefore P$ is a Prime ideal of R.

Conversely suppose that

let P be a prime ideal of R

we now Prove that $\frac{R}{P}$ is an Integral domain.

$P+a, P+b \in \frac{R}{P}$; $a, b \in R$

$\Rightarrow (P+a)(P+b) = P+0$

$\Rightarrow P+ab = P+0 \quad (\because S+a = S+b \Rightarrow a-b \in S)$

$\Rightarrow ab - 0 \in P$

$\Rightarrow a \in P$ or $b \in P$ ($\because$ 'P' is a Prime ideal)

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

$\therefore \frac{R}{P}$ has no zero divisors.

and hence $\frac{R}{P}$ is an ID.

$\Rightarrow P+a = P+0$ (or) $P+b = P+0$

$\therefore \frac{R}{P}$ has no zero divisors.

and hence $\frac{R}{P}$ is an I.D.

* Maximal Ideal :

Let R be a ring and M be an ideal such that $M \neq R$. M is said to be a maximal ideal of R, if for any other ideal U of R such that $M \subset U \subset R$ then either $M = U$ (or) $U = R$.

In otherwords, an ideal $M \neq R$ is a maximal ideal of R, if there does not exist any proper ideal b/w M and R.

Note: ① An ideal M of a ring R is called a maximal ideal if M is not included in any other ideal of R except R itself.

for example :

Let $R = I$ (ring of integers)

$S_1 = \{2n \mid n \in I\} = \{\cdots -6, -4, -2, 0, 2, 4, 6 \cdots\}$

$S_2 = \{3n \mid n \in I\} = \{\cdots -9, -6, -3, 0, 3, 6, 9 \cdots\}$

$S_3 = \{4n \mid n \in I\} = \{\cdots -12, -8, -4, 0, 4, 8, 12, \cdots\}$

$S_4 = \{5n \mid n \in I\} = \{\cdots -15, -10, 0, 10, 15 \cdots\}$

$S_5 = \{6n \mid n \in I\} = \{\cdots -18, -12, -6, 0, 6, 12, 18 \cdots\}$

Since $S_5 \subset S_2 \subset I$, $S_5 \subset S_1 \subset I$

$S_4 \subset I$, $S_3 \subset S_1 \subset I$

$S_2 \subset I$, $S_1 \subset I$.

$\therefore S_1$, S_2 and S_4 are maximal.

S_3 and S_5 are not maximals.

Example (2) :

- $\{0, 2\}$ is a maximal ideal of the ring $Z_4 = \{0, 1, 2, 3\}$ modulo 4.
- $\{0, 4\}$ and $\{0, 2, 4, 6\}$ are maximal ideals of the ring.

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ mod 8.

$\because \nexists$ no proper ideals b/w $\{0,3\}$ and $\mathbb{Z}_8$ and $\{0,2,4,6\}$ and $\mathbb{Z}_8$.

further, $\{0,4\}$ is an ideal of $\mathbb{Z}_8$.

$(\because \{0,4\} \subset \{0,2,4,6\} \subset \mathbb{Z}_8)$.

problems:

→ Find the maximal ideals of $\mathbb{Z}_6$, the ring of integers modulo 6.

Sol'n: Given that $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ is the ring of integers $\mathbb{Z}_6$.

The Proper ideals of $\mathbb{Z}_6$ are

$(3) = \{0,3\}$, $(2) = \{0,2,4\}$

Since there does not exist any Proper ideal between (3) and $\mathbb{Z}_6$

(2) and $\mathbb{Z}_6$

$\therefore$ (3), (2) are maximal ideals of $\mathbb{Z}_6$.

→ Find the maximal ideals of $\mathbb{Z}_{12}$, the ring of integers modulo 12

Sol'n: Given that $\mathbb{Z}_{12} = \{0,1,2 \text{ --- } 11\}$

is the ring of integers modulo 12.

The Proper ideals of $\mathbb{Z}_{12}$ are.

$(2) = \{0,2,4,6,8,10\}$

$(3) = \{0,3,6,9\}$

$(4) = \{0,4,8\}$

$(6) = \{0,6\}$

Since there does not exist any Proper ideal between (3) and $\mathbb{Z}_{12}$

$\therefore$ (3) is the maximal ideal of $\mathbb{Z}_{12}$.

Similarly (2) is also a maximal ideal of $\mathbb{Z}_{12}$.

However (4) and (6) are not maximal ideals of $\mathbb{Z}_{12}$ [$\because (4) \subset (2) \subset \mathbb{Z}_{12}$ and $(6) \subset (3) \subset \mathbb{Z}_{12}$.]

→ show that $\{0\}$ is the only maximal ideal of a field F.

Sol'n: we know that a field F has only two ideals F and $\{0\}$.

Since $F \neq \{0\}$

$\{0\}$ is the only maximal ideal of f.

→ show that $(4) = \{\ldots -8, -4, 0, 4, 8 \ldots\}$ is the maximal ideal of the ring E of even integers.

Sol'n: Since $2 \notin (4)$, $(4) \neq E$.

Let U be any other ideal of E

Such that $(4) \subset U \subset E$, $(4) \neq U$

then $\exists$ some $x \in U$ such that $x \notin (4)$

$\Rightarrow x$ is an even integer not divisible by 4.

$\Rightarrow x = 4n+2$ for some integer 'n'

$\Rightarrow 2 = x - 4n$, where $x - 4n \in U$ ($\because$ U is an ideal i.e $x \in U$, $4n \in U \Rightarrow x - 4n \in U$)

$\Rightarrow 2 \in U$

$\Rightarrow (2) \subseteq U$

$\Rightarrow E = U$

Hence (4) is the a maximal ideal of E.

Imp → show that $M = (n_0)$ is a maximal ideal of $\mathbb{Z}$ iff n_0 is a prime number.

Sol'n: Let n_0 be a prime number

we prove that $M = (n_0)$ is a maximal ideal of $\mathbb{Z}$.

Such that $M \subset U \subset \mathbb{Z}$

Since $n_0 \in M$, $n_0 \in U \Rightarrow n_0 = nx$, for some $x \in \mathbb{Z}$

$\Rightarrow n = 1$ or $n = n_0$ ($\because n_0$ is prime)

If $n = 1$, then $U = (1) = \mathbb{Z}$

If $n = n_0$, then $U = M$

Hence $M = (n_0)$ is a maximal ideal of $\mathbb{Z}$

Conversely, let $M = (n_0)$ be a maximal ideal of $\mathbb{Z}$

we prove that n_0 is a prime number.

If possible, Suppose that n_0 is a composite number

Let $n_0 = ab$, $a \neq \pm 1$, $b \neq \pm 1$

Let $U = (a)$. (it is obvious)

Suppose x is an arbitrary element of M.

Then $x = n_0 r$ for some $r \in \mathbb{Z}$.

$\Rightarrow x = (ab)r$

$\Rightarrow x = a(br)$

$\Rightarrow x \in U$

$\therefore M \subset U \subset \mathbb{Z}$

Since M is a maximal ideal of $\mathbb{Z}$,

$\therefore$ either $M = U$ or $U = \mathbb{Z}$.

If $U = \mathbb{Z}$, then $a = 1$, which is a contradiction to $a \neq 1$.

If $U = M$, then $a = n_0 l$ for some integer l.

($\because$ Each element of M is multiple of n_0 i.e, $M = (n_0)$)

$\therefore n_0 = ab$

$= (n_0 l)b$

$= n_0(lb)$

Since $n_0 \neq 0$

$\therefore lb = 1$

$\Rightarrow b = 1$

which is a contradiction.

$\therefore$ our assumption that n_0 is composite number is wrong.

Hence n_0 must be a prime integer.

Note: (1) For the ring of integers $\mathbb{Z}$, any ideal generated by prime integer is a maximal ideal.

(2) A ring may have more than one maximal ideal.

For eg: the ring $\mathbb{Z}$ has $\langle 2 \rangle, (3), (5), \ldots$ as maximal Ideals.

1988
2001 → If R is a commutative ring with unity, then an ideal M of R is maximal iff $\frac{R}{M}$ is a field.

Proof: Given that R is a commutative ring with unity and M is an ideal.

∴ The quotient ring $\frac{R}{M} = \{a+M / a \in R\}$ is a commutative ring and has unity.

Zero element of $\frac{R}{M}$ is $0+M = M$ where $0 \in R$ is zero element in R.

unit element of $\frac{R}{M}$ is $1+M$ where $1 \in R$ is the unity element in R.

Now suppose that M is a maximal ideal of R

We prove that $\frac{R}{M}$ is a field.

To prove that $\frac{R}{M}$ is a field, we have to show that every non-zero element of $\frac{R}{M}$ has multiplicative inverse.

Let $a+M \in \frac{R}{M}$ and $a+M$ be non-zero element

$\therefore a+M \neq M$

$\Rightarrow a \notin M$ $\left(\because a+M \neq M \Leftrightarrow a \notin M \text{ (or) } M+a \neq M \Leftrightarrow a \notin M\right)$.

If $\langle a \rangle = \{ar / r \in R\}$ is a principal ideal of R then $\langle a \rangle + M$ is also an ideal of R (Since the sum of two ideals is again an ideal of R)

Again $a = a \cdot 1 + 0 \in \langle a \rangle + M$ and $a \notin M$

$\therefore M \subset \langle a \rangle + M \subseteq R$

Since M is a maximal ideal of R

$\therefore \langle a \rangle + M = R$

Since $1 \in R \Rightarrow 1 \in \langle a \rangle + M$

$\Rightarrow 1 = ar + m$ for some $r \in R, m \in M$.

$\Rightarrow 1+M = (ar+m)+M$

$= (ar+M)+(m+M)$

$= (ar+M)+M \quad (\because m \in M \Leftrightarrow m+M = M)$

$= ar+M \quad (\because$ By additive identity prop. of $R/M)$

$= (a+M)(r+M)$

$\therefore (a+M)(r+M) = (r+M)(a+M) = 1 \quad (\because R/M$ is Comm)

$\Rightarrow (a+M)^{-1} = r+M \in \frac{R}{M}$

Hence every non-zero element of $\frac{R}{M}$ is invertible

$\therefore \frac{R}{M}$ is field.

Conversly suppose that $\frac{R}{M}$ is a field.

We prove that M is maximal ideal of R

Let U be any ideal of R such that

$M \subset U \subseteq R$ and $M \neq U$

Now we shall show that $U = R$

Since $M \subset U$ and $M \neq U$, $\exists p \in U$ s.t $p \notin M$

i.e $p+M \neq M \quad (\because p+M = M \Leftrightarrow p \in M)$

i.e $p+M$ is non-zero element of $\frac{R}{M}$.

Since $\frac{R}{M}$ is a field

and $p+M$ is non-zero element of $\frac{R}{M}$

$\Rightarrow p+M$ has multiplicative inverse, say $q+M$

$\therefore (p+M)(q+M) = 1+M$

$\Rightarrow pq+M = 1+M$

$\Rightarrow 1-pq \in M \quad (\because a+M = b+M \Leftrightarrow (-a)+b \in M)$.

Since U is an ideal of R

So $p \in U$ and $q \in R$

$\Rightarrow pq \in U.$

$pq \in U$ and $1-pq \in U$

$\Rightarrow pq + (1-pq) \in U$

$\Rightarrow 1 \in U.$

$\therefore 1 \in U$ and U is an ideal of R

$\therefore U = R$ ($\because \forall x \in R$ and $1 \in U$
$\Rightarrow x.1 \in U$
$\Rightarrow x \in U$
$\because R \subset U$ & $U \subset R$
$\Rightarrow U = R$)

Hence M is Maximal ideal of R

1991 → For a commutative ring with unity, maximal ideal is a prime ideal.

Sol: Let R be a commutative ring with unity.

let U be a Maximal ideal of R

then $\frac{R}{U}$ is a field,

Since every field is an integral domain.

$\therefore \frac{R}{U}$ is an integral domain.

$\Rightarrow$ U is a prime ideal

($\because$ Let R be a Comm ring then an ideal P of R is Prime ideal $\Leftrightarrow \frac{R}{P}$ is an integral domain)

Thus every maximal ideal is prime ideal.

Note1 :- The converse of the above need not be true.

i.e. for a commutative ring with unity, a prime ideal need not be maximal ideal.

Let us consider the integral domain of integers Z.

Then, the null ideal = $\langle 0 \rangle$ is a prime ideal,

But $\langle 0 \rangle$ ideal is not maximal ideal,

because, there exists ideal $\langle 2 \rangle$ so that

$\langle 0 \rangle \subset \langle 2 \rangle \subset Z$ and $\langle 2 \rangle \neq \langle 0 \rangle$,

$\langle 2 \rangle \neq Z$.

Note②: for a commutative ring without unity a maximal ideal need not be a prime ideal.

Sol: Let $E = \{ 2n / n \in Z \}$

= the ring of even integers without unity element.

$= (2)$

Let $(4) = \{ 4n / n \in Z \}$

$= \{ \ldots\ldots -8, -4, 0, 4, 8, \ldots\ldots \}$ be an ideal of E

Since $2 \notin (4)$, $(4) \neq E$

Let U be any other ideal of E s.t.

$(4) \subset U \subset E$, $(4) \neq U$

Then $\exists$ some $x \in U$ s.t $x \notin (4)$

$\Rightarrow$ x is an even integer not divisible by 4

$\Rightarrow$ $x = 4n+2$ for some integer 'n'

$\Rightarrow$ $2 = x - 4n$ ——— ①

Since $x \in U$, $4n \in (4)$ and $(4) \subset U$

$x \in U$, $4n \in U$

$\Rightarrow x - 4n \in U$ ($\because U$ is an ideal)

$\Rightarrow 2 \in U$ (by ①)

$\Rightarrow (2) \subset U$ — ②

We know that $U \subset E = (2)$

From ② & ③, we have

$U = E$

$\therefore$ The ideal (4) is the maximal ideal

Now for $2, 2 \in E$

and $2.2 \in 4 \in (4)$

We do not have $2 \in (4)$.

$\therefore (4)$ is not prime ideal.

→ In a Commutative ring R with unity, if M is a maximal ideal of $x \in R$, then prove that there exists $\alpha \in R$ such that $x \notin M \Rightarrow 1 - x\alpha \in M$.

Sol: Given that R is a Commutative Ring with unity.

and M is maximal ideal of R

Let the principal ideal generated by $x \in R$ be $\langle x \rangle$

Since M, $\langle x \rangle$ are ideals of R

$\Rightarrow \langle x \rangle + M$ is ideal of R

Since M is maximal ideal of R

$\therefore \langle x \rangle + M = R$

Since $1 \in R \Rightarrow 1 \in \langle x \rangle + M$

$\therefore \exists\, a \in M$ and $\alpha \in R$ such that $x\alpha + a = 1$

$\therefore \exists\, \alpha \in R$ s.t $1 - x\alpha = a \in M$

$\Rightarrow 1 - x\alpha \in M$

Homomorphisms and Embedding of Rings

→ Let $(R,+,\cdot)$ and $(R',\oplus,\otimes)$ be two rings. A mapping $f:R\to R'$ is said to be a homomorphism, if

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

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

The above conditions imply that 'f' preserves the compositions of the rings R and R'.

However, if we agree to use the same compositions '+' and '.' for both R and R', then

→ A mapping $f: R\to R'$ is called a homorphism, if (i) $f(a+b) = f(a)+f(b)$

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

Note:- The operations +, . on the left handside of the properties (i), (ii) are of the ring R, while the operations +, . on R.H.S of the properties (i), (ii) are that of the ring R'

→ A ring R' is called a homomorphic image of a ring R if there exists a homomorphism 'f' of R onto R'.

i.e f is a homorphism and for each $r'\in R'$ there exists some $r\in R$ such that $f(r)=r'$.

→ A mapping $f:R\to R'$ is called an isomorphism, if (i) f is a homomorphism (ii) f is 1-1 i.e. $f(a)=f(b)\Rightarrow a=b$ for $a,b\in R$.

→ A ring R' called an isomorphic image of the ring R, if there exists a mapping $f: R \to R'$ such that

(i) f is a homomorphism
(ii) f is a one-one and
(iii) f is onto

Note:- If $f: R \to R'$ is an onto homomorphism then R' is the homomorphic image of R and we write $R \simeq R'$.

→ If $f: R \to R'$ is 1-1 & onto homomorphism then R' is isomorphic image of R or R is isomorphic to R'.

and we write $R \cong R'$.

→ If $f: R \to R'$ is an onto homomorphism then $f(R) = R'$.

→ If U is an ideal of the ring R, then $\frac{R}{U} = \{x+U / x \in R\}$ is also a ring w.r.t addition and multiplication of cosets. Then the mapping $f: R \to \frac{R}{U}$ defined by $f(x) = x+U$ for all $x \in R$ is called the natural homomorphism from R onto $\frac{R}{U}$.

* Examples of Homomorphisms:

→ If R is a ring, then the mapping $f: R \to R$ defined as $f(x) = x \; \forall \; x \in R$ is a homomorphism.

Sol:- For any $x, y \in R$

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

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

$\therefore f$ is a homomorphism.

→ If R is a ring, the mapping $f: R \to R$ defined as $f(x) = 0' \ \forall \ x \in R$ is a homomorphism.

Sol:- For any $x, y \in R$

$\Rightarrow x+y \in R$ & $xy \in R$

$\therefore f(x) = 0', f(y) = 0'$

By definition, $f(x+y) = 0'$

$= 0' + 0'$

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

and $f(xy) = 0'$

$= 0' \, 0'$

$= f(x) f(y)$

$\therefore f$ is a homomorphism from R into R',

This is called zero homomorphism.

→ If $Z[\sqrt{2}] = \{m+n\sqrt{2} / m, n \in I\}$, the mapping $f: Z[\sqrt{2}] \to Z[\sqrt{2}]$ defined as $f(m+n\sqrt{2}) = m-n\sqrt{2}$ is a homomorphism.

Sol: Let $x, y \in Z[\sqrt{2}]$ Choosing

$x = a+b\sqrt{2}$

$y = c+d\sqrt{2}$, $a, b, c, d \in Z[\sqrt{2}]$

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

$xy = (ac+2bd)+(ad+bc)\sqrt{2}$

We have

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

and $f(xy) = (ac+2bd)-(ad+bc)\sqrt{2}$

$$= (a-b\sqrt{2})(c-d\sqrt{2})$$
$$= f(x).f(y).$$

Thus f is a homomorphism.

→ Let $R = Z$ and $R' =$ set of all even integers.

Then $(R', +, *)$ is a ring, where $a * b = \frac{ab}{2}$ $\forall$ $a, b \in R'$. The mapping $f: R \to R'$ defined as $f(a) = 2a$ $\forall$ $a \in R$ is a homomorphism.

Sol:- for any $a, b \in R$,

We have $f(a+b) = 2(a+b)$

$$= 2a + 2b$$
$$= f(a)+f(b)$$

and $f(ab) = 2(ab)$

$$= \frac{(2a)(2b)}{2}$$
$$= (2a) * (2b)$$
$$= f(a) * f(b)$$

Thus f is a homomorphism.

Properties of Homomorphism:-

Theorem 1: Let $f:R \to R'$ be a homomorphism of a ring R into the ring R' and $0' \in R'$ be the zero elements Then

(1). $f(0) = 0'$

(2). $f(-a) = -f(a) \quad \forall a \in R$

(3). $f(a-b) = f(a) - f(b) \quad \forall a, b \in R$

Sol^n: (1) Since $0 \in R$, We have

$$0+0 = 0$$

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

$$\Rightarrow f(0) + f(0) = f(0) + 0', \; f(0) \in R'$$

$$\Rightarrow f(0) = 0' \text{ (by LCL of } R')$$

(2) Since $a \in R \Rightarrow -a \in R$ such that

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

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

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

$$\Rightarrow \boxed{f(-a) = -f(a)}$$

(3) For $a, b \in R$; $f(a-b) = f(a) + f(-b)$

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

Theorem 2: If f is a homomorphism from a ring R into R' then $f(R)$ is a subring of R'.

Sol: By definition

$$f(R) = \{f(a) / a \in R\} \subseteq R'$$

Since $0 \in R$, $f(0) \in f(R)$

$\Rightarrow 0' \in f(R)$ ($\because f(0) = 0'$ in R')

clearly $f(R)$ is non-empty subset of R'

To show that $(f(R), +, \cdot)$ is a subring of R'.

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

$\therefore \exists\ a, b \in R$ s.t

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

Since $a-b \in R$, $ab \in R$

and hence $f(a-b), f(ab) \in f(R)$.

Now we have $a'-b' = f(a) - f(b)$

$= f(a-b)$ ($\because f$ is homo)

$\in f(R)$.

and $a'b' = f(a).f(b)$

$= f(ab)$. ($\because f$ is homo).

$\in f(R)$.

$\therefore f(R)$ is a subring of R'.

i.e the homomorphic image of the ring R is a subring of R'.

i.e the homomorphic image of a ring is a ring.

Theorem 3: Every homomorphic image of a commutative ring is a commutative ring.

Soln: Let $(R, +, \cdot)$ be a comm. ring and $(R', +, \cdot)$ be a ring.

Let $f: R \to R'$ be homo. and onto.

$\therefore R'$ is homomorphic image of R

i.e $R' = f(R)$.

Let $a', b' \in R'$

$\therefore \exists$ elements $a, b \in R$ s.t

$f(a) = a'$ &

$f(b) = b'$.

Since R is comm. ring

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

$\Longrightarrow ab = ba$

Now $a'b' = f(a).f(b)$

$= f(ab)$ ($\because$ f is homo)

$= f(ba)$.

$= f(b)f(a)$ ($\because$ f is homo).

$= b'a'$.

$\therefore R'$ is Comm. ring.

Note: The converse of the above theorem need not be true. i.e if the homomorphic image of a ring R is Commutative then the ring R need not be comm. ring.

For example:

Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / a, b \in I \right\}$ be a ring

Then R is not a comm. ring

i.e let $A = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix}$ be in R

then $AB \neq BA$.

Now we shall show that the mapping $f: R \to Z$ defined as

$$f\left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \right\} = a \quad \text{---------} (1)$$

is an onto homo.

Let $x = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R$

$y = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in R$

We have $x+y = \begin{pmatrix} a+c & b+d \\ 0 & 0 \end{pmatrix}$

$xy = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}$

Now $f(x+y) = a+c$

$= f(x)+f(y)$ (by ①)

$f(xy) = ac$

$= f(x)\,f(y)$ (by ①)

$\therefore f$ is homo.

Since for any $x \in \mathbb{Z}$,

$\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \in R$ and

$f\left\{\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}\right\} = x$ (Here $y \in \mathbb{Z}$).

$\therefore f: R \to R'$ is onto.

Hence $\mathbb{Z}$ is homomorphic image of R.

Where $\mathbb{Z}$ is comm. ring but

R is not comm. ring.

Theorem : 4 : The homomorphic image of a ring with unity is also a ring with unity.

Soln:- Let $(R, +, .)$ be a ring with unity and $(R', +, .)$ be a ring.

Let $f: R \to R'$ be a homomorphism and onto.

$\therefore R'$ is the homomorphic image of R.

i.e $R' = f(R)$.

Let $a', b' \in R'$

$\therefore \exists$ elements $a, b \in R$ such that

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

Since R is ring unity

$\therefore \forall a \in R, \exists 1 \in R$ s.t

$1 \cdot a = a = a \cdot 1$

Now Since $1 \in R$ (unity in R).

We shall show that $f(1)$ is the unity in R'

We have

$$a' \cdot f(1) = f(a) \cdot f(1)$$
$$= f(a \cdot 1) \quad (\because f \text{ is homo})$$
$$= f(a) \quad (\because a \cdot 1 = a \text{ in } R)$$
$$= a'$$

Similarly, $f(1) \cdot a' = a'$.

$\therefore \forall a' \in R', \exists f(1) \in R'$ s.t.

$f(1) \cdot a' = a' \cdot f(1) = a'$

$\therefore R'$ is a ring with unity.

Note:- The Converse of the need not be true, i.e. if the homomorphic image of a ring R is ring with unity then the ring R need not be ring with unity.

for example:-

$R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / a, b \in Z \right\}$ is a ring without unity. and Z is a ring with unity.

The mapping $f: R \to Z$ defined as $f\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\right\} = a$ is an onto homomorphism.

Note:- Even f is an isomorphism

(1) Substitute 'isomorphism' for homomorphism in theorem. ① The same proof holds.

(ii) Substitute isomorphism for homomorphis in theorem ① and it is true. The same proof holds.

(iii) Substitute isomorphism onto for homomorphism onto in theorem ③ & ④ and it is true. The same proof hold.

* Kernal of a homomorphism :-

Let R, R' be two rings and $f: R \to R'$ be a homomorphism then Kernal of f, denoted by $\ker f$, is defined as

$$\ker f = \{x \in R / f(x) = 0', 0' \text{ is the +ve identity in } R'\} \subseteq R.$$

Note :- since $0 \in R$, $f(0) = 0'$ ($\because f$ is homo)

$\therefore 0 \in \ker f$.

$\therefore$ This shows that $\ker f$ is always non-empty

i.e $\ker f \neq \phi$.

→ If f is a homomorphism of a ring R into a ring R' then $\ker f$ is an ideal of R.

Proof :- Let $f: R \to R'$ be the homomorphism.

Let $\ker f = \{x \in R / f(x) = 0', 0' \text{ is the identity in } R'\} \subseteq R$.

To prove that K is an ideal of R.

Since $0 \in R$ (The zero elt of R)

$\therefore f(0) = 0'$, The zero element of R'.

$\therefore 0 \in \ker f$

$\Rightarrow \ker f \neq \phi$

$\therefore \ker f$ is non-empty subset of R.

Let $a, b \in \ker f \subseteq R$, then $f(a) = 0'$ & $f(b) = 0'$.

Now We have

$$f(a-b) = f(a) - f(b) \quad (\because f \text{ is homo})$$
$$= 0' - 0'$$
$$= 0'$$
$$\therefore f(a-b) = 0' \Rightarrow \boxed{a-b \in \text{Ker } f}$$

and $f(ar) = f(a)f(r)$
$= 0'.f(r)$
$= 0'$ and
$f(ra) = f(r).f(a)$
$= f(r).0'$
$= 0'$

$\therefore ar \in \text{Ker } f, ra \in \text{Ker } f$.

Hence Ker f is an ideal of R.

→ If f is a homomorphism of a ring R into the R' then f is an into isomorphism if and only if $\text{Ker } f = \{0\}$

Sol: Let $f: R \to R'$ be the homomorphism.
Let f be an into homomorphism
i.e. f is 1-1 homomorphism.

Let $\text{Ker } f = \{x \in R / f(x) = 0', 0' \text{ is the identity in } R'\} \subseteq R$

Now we prove that

$\text{Ker } f = \{0\}$,

Let $a \in \text{Ker } f$ then $f(a) = 0'$

$\Rightarrow f(a) = f(0)$ $(\because f(0) = 0'$ in homo$)$

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

$\therefore 0$ is the identity element in R which belongs to $\text{Ker}f$ $\therefore \text{Ker}f = \{0\}$

Converse:- Suppose $\text{Ker}f = \{0\}$

We prove that f is $1-1$.

Let $a, b \in R$ and

$f(a) = f(b)$

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

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

$\Rightarrow (a-b) \in \text{Ker}f$

$\Rightarrow a - b = 0$

$\Rightarrow a = b$

$\therefore f$ is $1-1$

Note :- $\text{Ker}f = \{0\} \Longleftrightarrow f$ is $1-1$

→ If U is an ideal of a ring R then the quotient ring $\frac{R}{U}$ is a homomorphic image of R.

(or)

Every quotient ring of a ring is a homomorphic image of the ring.

Proof :- Given that U is an ideal of the ring R

$\therefore \frac{R}{U}$ is a quotient ring

i.e Let $\frac{R}{U} = \{x+U / x \in R\}$ be a ring with respect $+^n$ and x^n cosets defined as

$(a+U) + (b+U) = (a+b)+U$

and $(a+U)(b+U) = ab+U$ Where $a+U, b+U \in \frac{R}{U}$.

Let $f: R \to \frac{R}{U}$ be a mapping defined by

$$f(a) = a+U \text{ for all } a \in R \quad \text{——} ①$$

First of we shall show that

f is well-defined:-

for, $a, b \in R$, $a = b \Rightarrow$

$$\Rightarrow a+U = b+U$$

$$\Rightarrow f(a) = f(b)$$

$\therefore$ the mapping f is well defined.

Now for $a, b \in R$

$$\Rightarrow a+b \in R$$

We have $f(a+b) = (a+b)+U$ (by ①)

$$= (a+U)+(b+U)$$

$$= f(a)+f(b) \text{ (by ①)}.$$

and $f(ab) = ab+U$

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

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

$\therefore f(ab) = f(a).f(b)$.

f is homomorphism.

Let $x+U \in \frac{R}{U}$ $\forall$ $x \in R$

For this $x \in R$, $f(x) = x+U$ (by ①)

$\therefore$ for each $x+U \in \frac{R}{U}$, $\exists$ $x \in R$ s.t

$$f(x) = x+U$$

$\therefore$ f is onto mapping.

Hence $f: R \to \frac{R}{U}$ is an onto homomorphism

Note:- The mapping $f: R \to \frac{R}{U}$ such that $f(x) = x+U \; \forall x \in R$ is called Natural homomorphism (or) Canonical homomorphism.

* **Fundamental theorem of homomorphism:-**

Let R, R' be two rings and $f: R \to R'$ be an onto homomorphism with $\text{Ker} f$. Then R' is isomorphic to $\frac{R}{\text{Ker} f}$.

i.e $R \simeq R' \Rightarrow \frac{R}{\text{Ker} f} \cong R'$

Proof: Let $f: R \to R'$ be a homomorphism and onto.

By definition of $\text{Ker} f$ is

$\text{Ker} f = \{ x \in R / f(x) = 0', \; 0' \text{ is the identity of } R' \} \subseteq R$

Let $\text{Ker} f = U$

We know that U is an ideal of R.

$\therefore$ The quotient ring $\frac{R}{U}$ is defined

Where $\frac{R}{U} = \{ x+U \; / x \in R \}$.

Given that $f: R \to R'$ is homomorphism and onto.

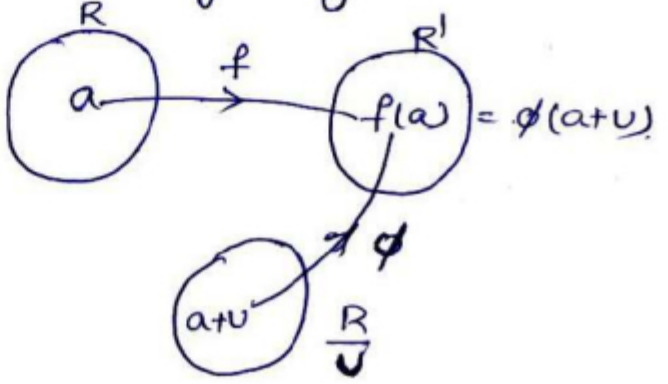
$\Rightarrow f(R) = R'$

$\Rightarrow R' = \{ f(a) / a \in R \}$.

Now we shall prove that $\frac{R}{U} \cong R'$

Now we define a mapping $\phi : \frac{R}{U} \to R'$ s.t

$\phi(a+U) = f(a) \; \forall \; a \in R$ ——— (1)



(i) Now we shall show that ϕ is well defined:-

Now $a+U,\ b+U \in \frac{R}{U}$

We have $a+U = b+U$

$\Rightarrow a-b \in U = \text{Ker} f$

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

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

$\Rightarrow f(a) = f(b)$

$\Rightarrow \phi(a+U) = \phi(b+U)$ (by ①)

$\therefore \phi$ is well defined

(ii) To prove ϕ is 1-1:-

For, $a, b \in R,\ a+U, b+U \in \frac{R}{U}$

Now we have $\phi(a+U) = \phi(b+U)$

$\Rightarrow f(a) = f(b)$ (by ①)

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

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

$\Rightarrow a-b \in U = \text{Ker} f$

$\Rightarrow a+U = b+U$ ($\because U$ is an ideal)

$\therefore \phi$ is 1-1

(iii) To prove that ϕ is onto:-

Let $x \in R'$

since $f: R \to R'$ is onto.

$\therefore \exists\ a \in R$ such that $f(a) = x$. —— (2)

Now for $a+U \in \frac{R}{U}$ and $\phi(a+U) = f(a) = x$.

$\therefore$ For each $a+U \in \frac{R}{U}$ $\exists\ x \in R'$ s.t $\phi(a+U) = x$.

$\therefore \phi$ is onto.

(iv) To prove ϕ is homomorphism :-

For $a, b \in R$ is $a+U, b+U \in \frac{R}{U}$

We have $\phi((a+U)+(b+U)) = \phi((a+b)+U)$

$= f(a+b)$ (by (1))

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

$= \phi(a+U) + \phi(b+U)$.

and $\phi((a+U).(b+U)) = \phi(ab+U)$ (by (1))

$= f(ab)$

$= f(a).f(b)$ ($\because$ f is hom)

$= \phi(a+U).\phi(b+U)$.

$\therefore \phi$ is homomorphism.

$\therefore \phi$ is isomorphism from $\frac{R}{U}$ onto R'

i.e, R' is an isomorphic image of $\frac{R}{U}$

i.e, $\frac{R}{U} \cong R'$

Note :- If $f: R \to R'$ is a homomorphism from a ring R onto R' and U is an ideal of R then $\frac{R}{U}$ is isomorphic to R'.

Ring of Endomorphisms of an Abelian group:-

Let $(G,+)$ be an abelian group. A homomorphism of G into itself is an endomorphism of G.

The set of all endomorphisms of G is denoted by $\text{Hom}(G,G)$.

Since the addition of two mappings is a mapping and the composition of two mappings is a mapping, we define addition $(+)$ and multiplication $(\cdot)$ of two endomorphisms as:

(i) $(f+g)(x) = f(x)+g(x)$

(ii) $(fg)(x) = f(g(x))$ for all $x \in G$.

Now we prove that $\text{Hom}(G,G)$ is a ring with respect to the addition and multiplication of endomorphisms.

Theorem: If $(G,+)$ is an abelian group then $\text{Hom}(G,G)$ is a ring under addition and composition of mappings.

Proof: $\text{Hom}(G,G)$ = the set of all endomorphisms of G.

If $f, g \in \text{Hom}(G,G)$ then

$f: G \to G$, $g: G \to G$ are homomorphisms.

$\therefore f(x+y) = f(x)+f(y)$ and

$g(x+y) = g(x)+g(y)$ $\forall x, y \in G$.

Now we show that $(\text{Hom}(G,G), +)$ is an abelian group.

(1) Closure Prop:

Let $f, g \in \text{Hom}(G, G)$

$\Rightarrow f+g$ is a mapping from G to G.

for $x, y \in G$;

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

($\because f(x), f(y), g(x), g(y) \in G$ and G is abelian).

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

$\therefore f+g$ is a homomorphism.

$\therefore f, g \in \text{Hom}(G,G) \Rightarrow f+g \in \text{Hom}(G,G)$.

So, addition of endomorphisms is a binary operation in $\text{Hom}(G,G)$.

(2) Comm. prop:

For $x \in G$, $(f+g)(x) = f(x) + g(x)$
$= g(x) + f(x)$
$= (g+f)(x)$

$\therefore f, g \in \text{Hom}(G,G) \Rightarrow f+g = g+f$.

$\therefore$ Addtion of endomorphisms is commutative.

(3) Asso. prop:

Let $f, g, h \in \text{Hom}(G,G)$.

For $x \in G$; $((f+g)+h)(x) = (f+g)(x) + h(x)$
$= (f(x)+g(x)) + h(x)$
$= f(x) + (g(x)+h(x))$

($\because f(x), g(x), h(x) \in G$ and G is a group).

$= f(x) + (g+h)(x)$
$= (f+(g+h))(x)$

$\therefore f, g, h \in \text{Hom}(G_1, G_1)$

$\Rightarrow (f+g)+h = f+(g+h)$.

$\therefore$ Addition is associative.

(4) Identity prop:

Define a mapping $0: G \to G$ by

$$0(x) = e, \forall x \in G.$$

Where 'e' is the identity in G.

For $x, y \in G$; $0(x+y) = e$ ($\because x, y \in G \Rightarrow x+y \in G$)

$= e+e$

$= 0(x)+0(y)$

$\therefore 0$ is a homomorphism and hence

$0 \in \text{Hom}(G_1, G_1)$.

For $f \in \text{Hom}(G_1, G)$ and $\forall x \in G$;

$(f+0)(x) = f(x)+0(x)$

$= f(x)+e$

$= f(x)$

and $(0+f)(x) = f(x)$.

$\therefore \exists\ 0 \in \text{Hom}(G_1, G)$ such that

$0+f = f+0 = f\ \forall f \in \text{Hom}(G_1, G)$.

(5) Inverse prop:

Let $f \in \text{Hom}(G_1, G)$

Then $f: G \to G$ is a mapping.

Consider the mapping $(-f): G \to G$ defined by

$$(-f)(x) = -f(x)\ \forall x \in G$$

For $x, y \in G$, $(-f)(x+y) = -(f(x+y))$

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

($\because f$ is homomorphism)

$= -f(x) - f(y)$ $(\because f(x), f(y) \in G_1)$

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

$\therefore -f$ is a homomorphism and hence

$-f \in \text{Hom}(G, G)$.

Also $\forall x \in G, (f + (-f))(x) = f(x) + (-f)(x)$

$= e$

$= 0(x)$.

$\therefore$ for $f \in \text{Hom}(G, G)$ $\exists -f \in \text{Hom}(G, G)$

such that $f + (-f) = 0$

Hence $(\text{Hom}(G, G), +)$ is an abelian group.

Now we show that $(\text{Hom}(G, G), \cdot)$ is semi-group.

closure prop:

for $f, g \in \text{Hom}(G, G)$, the composite function of f and $g = fg$ is a mapping from G to G.

$\forall x, y \in G, (fg)(x+y) = f(g(x+y))$

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

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

$= (fg)(x) + (fg)(y)$.

$\therefore fg$ is a homomorphism.

$\therefore f, g \in \text{Hom}(G, G) \Rightarrow fg \in \text{Hom}(G, G)$.

So, multiplication of two endomorphisms is a binary operation.

Asso. prop:

Let $f, g, h \in \text{Hom}(G, G)$

$\forall x \in G, ((fg)h)(x) = (fg)(h(x))$

$= f(g(h(x)))$

$= f((gh)(x))$

$= (f(gh))(x)$.

$\therefore f, g, h \in Hom(G,G)$

$\Rightarrow (fg)h = f(gh)$

$\therefore$ multiplication is associative.

Distributive law:

Let $f, g, h \in Hom(G,G)$

$\forall x \in G, (f(g+h))(x) = f((g+h)(x))$

$= f(g(x)+h(x))$

$= f(g(x)) + f(h(x))$

$= (fg)(x) + (fh)(x)$.

Similarly, $((g+h)f)(x) = (gf)(x) + (hf)(x)$.

$\therefore f(g+h) = fg+fh$ and

$(g+h)f = gf+hf$

Hence $(Hom(G,G), +, \cdot)$ is a ring.

* Imbedding of Rings:-

A ring 'R' is said to be imbedded in a ring R', if there exists an isomorphism of R into R' i.e there exists a mapping $f: R \to R'$

such that (i) f is a homomorphism and

(ii) f is 1-1

→ We also say that R' is an extension ring (or) over ring of R.

Note:- (1) Since f is an isomorphism of R into R', f(R) is a subring of R' and further R and f(R) are isomorphic rings.

② $f: R \to f(R)$ is an onto isomorphism and so $R \cong f(R)$.

③ Let R and R' be two rings.

A one-one homomorphism 'f' from R to R' is called an imbedding (embedding) mapping and in that case R' is called extension ring or over ring of R.

→ Every ring R can be imbedded in a ring with unity.

Proof: Let R be any ring.

Let $R' = R \times Z = \{(a,m) / a \in R, m \in Z\}$

Where Z denotes the ring of integers.

We now show that $R \times Z$ forms a ring with unity, under addition and multiplication defined by

$(r,m) + (s,n) = (r+s, m+n)$; $r, s \in R$ —— ① $m, n \in Z$

$(r,m) \cdot (s,n) = (rs + ms + nr, mn)$ —— ②

Addition is well-defined:

Let $(r,m) = (r',m')$ and $(s,n) = (s',n')$

then $r = r'$, $m = m'$ and $s = s'$, $n = n'$

$\Rightarrow r+s = r'+s'$; $m+n = m'+n'$

$\Rightarrow (r+s, m+n) = (r'+s', m'+n')$

Similarly we can show that multiplication is Well-defined.

We shall show that $(R \times Z, +)$ is an abelian group:

(i) Closure Prop:-

By ①, $R \times Z$ is closed under $+^n$.

(ii) Associative prop :-

Let $(r,m),(s,n),(t,k) \in R \times Z$;
$r, s, t \in R$,
$m, n, k \in Z$

then $(r,m)+[(s,n)+(t,k)] = (r,m)+(s+t, n+k)$ (by ①)

$= (r+(s+t), m+(n+k))$

$= ((r+s)+t, (m+n)+k)$ (by R & Z comm w.r.t. $+^n$)

$= (r+s, m+n)+(t,k)$

$= [(r,m)+(s,n)]+(t,k)$

(iii) Existence of left identity :-

$\forall (r,m) \in R \times Z$, $\exists (0,0) \in R \times Z$

$r \in R, m \in Z$

s.t $(0,0)+(r,m) = (0+r, 0+m)$ (by ①)

$= (r,m)$.

$\therefore (0,0)$ is the left identity in $R \times Z$

(iv) existence of left inverse :-

for each $(r,m) \in R \times Z$, $\exists (-r,-m) \in R \times Z$

s.t $(-r,-m)+(r,m) = ((-r)+r, (-m)+m)$ (by ①)

$= (0,0)$

$\therefore (-r,-m)$ is the left inverse of (r,m) in $R \times Z$

(v) Commutative prop :-

Let $(r,m),(s,n) \in R \times Z$

then we have

$(r,m)+(s,n) = (r+s, m+n)$

$= (s+r, n+m)$ ($\because$ R & Z are comm. under $+^n$)

$= (s,n)+(r,m)$

$\therefore$ $R \times Z$ is commutative under $+^n$

$\therefore (R \times Z, +)$ is an abelian group.

II We can easily show that $(R \times Z, \times)$ is a semigroup.

III We can easily show that multiplication is distributive over the addition in $R \times Z$.

$\therefore (R \times Z, +, \times)$ is a ring.

IV Existence of x^{ve} identity:

Since Z is a ring with unity

i.e $\forall\, m \in Z$, $\exists\, 1 \in Z$ s.t.

$1m = m1 = m$

Now for all $(r,m) \in R \times Z$, $\exists\, (0,1) \in R \times Z$

s.t. $(0,1) \times (r,m) = (0 \cdot r + 1 \cdot r + m(0), 1 \cdot m)$ (by ②)

$= (r,m)$

Similarly, $(r,m) \times (0,1) = (r,m)$.

$\therefore (0,1)$ will be unity in $R \times Z$.

$\therefore (R \times Z, +, \times)$ is a ring with unity.

Finally, we show that R can be embedded in $R \times Z$:

We now define a mapping:

$f : R \to R \times Z$ as $f(r) = (r,0)$ $\forall\, r \in R$. ——— ③

To show that f is well-defined:

Now we have

$$r, s \in R \Rightarrow r = s$$

$$\Rightarrow (r, 0) = (s, 0)$$

$$\Rightarrow f(r) = f(s)$$

$\therefore f$ is well-defd.

To show that f is 1-1:

Now we have $f(r) = f(s)$; $r, s \in R$

$$\Rightarrow (r, 0) = (s, 0)$$

$$\Rightarrow r = s$$

Next we shall show that f is homo:

Let $r, s \in R$ then by ③,

$$f(r) = (r, 0)$$

$$f(s) = (s, 0)$$

Since $r, s \in R \Rightarrow r + s \in R$ & $r \cdot s \in R$

Now $f(r+s) = (r+s, 0)$ (by ③)

$$= (r+s, 0+0)$$

$$= (r, 0) + (s, 0)$$

$$= f(r) + f(s).$$

and $f(r.s) = (r.s, 0)$ (by ③)

$$= (rs + 0s + 0r, 0.0)$$

$$= (r, 0) \times (s, 0) \quad \text{(by ②)}$$

$$= f(r) \times f(s).$$

$\therefore f$ is isomorphism of R into $R \times Z$.

and so R is imbedded in the ring $R \times Z$ with unity.

Note :- If R is any ring, not necessarily containing unity then its extension ring with unity is

$$R \times Z = \{(r, m) / r \in R, m \in Z\}.$$

* The field of quotients:

→ A ring R can be imbedded in a ring S if S contains a subset S' such that R is isomorphic to S'

If D is a commutative ring without zero divisors, then we shall see that it can be imbedded in a field F i.e there exists a field F which contains a subset D' isomorphic to D.

We shall construct a field F with the help of elements of D and this field F will contain a subset D' such that D is isomorphic to D'

This field F is called the "field of quotients" of D or simply the "quotient field" of D.

* Motivation for the construction of the quotient field:

We are all quite familiar with the ring I of Integers.

Also our familiar set Q of rational numbers is nothing but the set of quotients of the elements of I

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

— If we identify the rational numbers

$\cdots\cdots \frac{-3}{1}, \frac{-2}{1}, \frac{-1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \frac{3}{1} \cdots\cdots$

with the integers $\cdots\cdots -3,-2,-1,0,1,2,3\cdots$

then $I \subseteq Q$

Also $(Q,+,\cdot)$ is a field.

It is a smallest field containing I

Also if $\frac{a}{b}$ and $\frac{c}{d} \in Q$ then we have

(i) $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$

(ii) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

(iii) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

Taking motivation from these facts, we now proceed to construct the quotient field of an arbitrary integral domain.

We have the following theorem:

→ A Commutative ring with out zero divisors can be imbedded in a field.

(or)

Every integral domain can be imbedded in a field.

(or)

From the elements of an integral domain D, it is possible to construct a field F which contains a subset D' isomorphic to D.

(or)

An integral domain D can be embedded in a field F such that every element of F can be regarded as quotient of two elements of D.

Proof: Let D be an integral domain with atleast two elements.

Let us consider $S=\{(a,b) \mid a,b \in D, b \neq 0\}$ then $S \neq \phi$ and $S \subset D \times D$.

$\forall (a,b),(c,d) \in S$

define a relation '$\sim$' on 'S' as

$(a,b) \sim (c,d) \Leftrightarrow ad = bc$

we now prove that $\sim$ is an equivalence relation on S.

(1) for each $(a,b) \in S$

we have $ab = ba$.

which implies that $(a,b) \sim (a,b)$.

(2) for $(a,b),(c,d) \in S$

we have $(a,b) \sim (c,d)$

$\Rightarrow ad = bc$

$\Rightarrow cb = da$

$\Rightarrow (c,d) = (a,b)$.

(3) for $(a,b),(c,d),(e,f) \in S$

$(a,b) \sim (c,d)$, $(c,d) \sim (e,f)$

$\Rightarrow ad = bc$, $cf = de$

$\Rightarrow (ad)f = (bc)f$, $cf = de$

$\Rightarrow (af)d = b(de)$

$\Rightarrow (af)d = b(ed)$

$\Rightarrow (af)d = (be)d$

$\Rightarrow af = be \quad (\because d \neq 0)$

$\Rightarrow (a,b) \sim (e,f)$.

$\therefore \sim$ is an equivalence relation on 'S'.

Let $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$

Then $ab' = a'b$ and $cd' = c'd$ ——— (I)

Now (I) $\Rightarrow ab'dd' = a'bdd'$ and $bb'cd' = bb'c'd$

$\Rightarrow ab'dd' + bb'cd' = a'bdd' + bb'c'd$

$\Rightarrow (ad+bc)\,b'd' = (a'd'+b'c')\,bd$

$\Rightarrow \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$

Also (I) $\Rightarrow ab'cd' = a'bc'd$

$\Rightarrow (ac)(b'd') = (a'c')(bd)$

$\Rightarrow \frac{ac}{bd} = \frac{a'c'}{b'd'}$

$\therefore +^n$ and $\times^n$ of quotients are well-defined binary operations on F.

we now Prove that $(F,+,\cdot)$ is a field:

(1) For $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$; $\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f} = \frac{ad+bc}{bd}+\frac{e}{f}$

$= \frac{(ad+bc)f+(bd)e}{(bd)f}$

$= \frac{a(df)+(cf+de)b}{b(df)}$

$= \frac{a}{b}+\frac{cf+de}{df}$

$= \frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)$

$\therefore$ addition is associative.

(2) For $\frac{a}{b}, \frac{c}{d} \in F$; $\frac{a}{b}+\frac{c}{d} = \frac{ad+bc}{bd}$

$= \frac{bc+ad}{db}$

$= \frac{c}{d}+\frac{a}{b}$

$\therefore$ addition is commutative.

(3) For $a \neq 0 \in D$ we have $\frac{0}{a} \in F$ such that

$$\frac{0}{a} + \frac{a}{b} = \frac{0b + aa}{ab} = \frac{aa}{ab} = \frac{a}{b} \; \forall \; \frac{a}{b} \in F.$$

$\therefore \frac{0}{a} \in F$ is the zero element.

(4) Let $\frac{a}{b} \in F$. Then $\frac{-a}{b} \in F$ such that

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + (-a)b}{b^2} = \frac{0}{b^2} = \frac{0}{a} \quad (\because 0a = 0b^2)$$

$\therefore$ every element in F has additive inverse.

(5) For $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$; $\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f}$

$$= \frac{(ac)e}{(bd)f}$$

$$= \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b}\left(\frac{c}{d} \cdot \frac{e}{f}\right)$$

$\therefore$ multiplication is associative.

(6) For $\frac{a}{b}, \frac{c}{d} \in F$; $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}$

$\therefore$ multiplication is commutative.

(7) For $a \neq 0 \in D$ we have $\frac{a}{a} \in F$ such that

$$\frac{a}{b} \cdot \frac{a}{a} = \frac{aa}{ba} = \frac{a}{b} \; \forall \; \frac{a}{b} \in F.$$

$\therefore \frac{a}{a} \in F$ is the unity element.

(8) Let $\frac{a}{b} \in F$ and $\frac{a}{b} \neq \frac{0}{a}$

Then $aa \neq 0$ which implies that $a \neq 0$ as $a \neq 0$.

$\therefore b \neq 0$ and $a \neq 0 \Rightarrow \frac{b}{a} \in F$.

$\therefore$ for $\frac{a}{b}\left(\neq \frac{0}{a}\right) \in F$ there exists $\frac{b}{a} \in F$ such that

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ba}=\frac{u}{u} \qquad (\because (ab)u=(ba)u)$$

$\therefore$ Every non-zero element in F has multiplicative inverse.

(9). For $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in F$; $\frac{a}{b}\cdot\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\cdot\frac{cf+de}{df}$

$$=\frac{a(cf+de)}{b(df)}$$

$$=\frac{(acf+ade)(bdf)}{(bdf)(bdf)} \qquad \left[\because \frac{bdf}{bdf}=\frac{u}{u}\right]$$

$$=\frac{acf\,bdf+ade\,bdf}{bdf\;bdf}$$

$$=\frac{acf}{bdf}+\frac{ade}{bdf}$$

$$=\frac{ac}{bd}+\frac{ae}{bf}=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}$$

Similarly we can Prove that

$$\left(\frac{c}{d}+\frac{e}{f}\right)\cdot\frac{a}{b}=\frac{c}{d}\cdot\frac{a}{b}+\frac{e}{f}\cdot\frac{a}{b}.$$

$\therefore$ multiplication is distributive over addition.

In view of (1), (2), (3), (4), (5), (6), (7), (8) and (9) $(F,+,\cdot)$ is a field.

Now we have to Prove that D is embedded in the field F, that is, we have to show that there exists an isomorphism of D into F.

Define the mapping $\phi: D\to F$ by

$$\phi(a)=\frac{ax}{x} \;\forall\; a\in D \text{ and } x(\neq 0)\in D.$$

$a,b\in D$ and $\phi(a)=\phi(b)\Rightarrow \frac{ax}{x}=\frac{bx}{x}$

$$\Rightarrow (ax)x=(bx)x$$

$$\Rightarrow (a-b)x^2=0$$

$$\Rightarrow a-b=0 \text{ since } x^2\neq 0.$$

$$\Rightarrow a=b$$

$\therefore \phi$ is one-one

For $a,b\in D$; $\phi(a+b)=\frac{(a+b)x}{x}=\frac{(a+b)xx}{xx}$

$$= \frac{axx + bxx}{xx}$$

$$= \frac{ax}{x} + \frac{bx}{x} = \phi(a) + \phi(b)$$

$$\phi(ab) = \frac{(ab)x}{x} = \frac{(ab)xx}{xx} = \frac{ax}{x} \cdot \frac{bx}{x} = \phi(a) \cdot \phi(b)$$

$\therefore \phi$ is a homomorphism.

Hence ϕ is an isomorphism of D into F.

$\therefore$ the integral domain D is embedded in the field F.

Note 1: Every element in the field F is in the form of a quotient of two elements in D. so, the field F is called "field of quotients of D".

2. The equivalence class of (a,b)'s is also denoted as

$[(a,b)]$ or $[a,b]$ or (a,b)

then $[(a,b)] = [(c,d)] \Leftrightarrow ad = bc$,

$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$

$[(a,b)] \cdot [(c,d)] = [(ac, bd)]$

the zero element of $F = [(0,1)]$ and the unit element of $F = [(1,1)]$.

3. If D is the ring of integers then the field F, constructed in the above theorem, would be the field of rational numbers.

More on ideals

2003 Let R be the ring of all the real valued continuous functions on the closed unit interval. Show that $M = \{f \in R \mid f(\frac{1}{3}) = 0\}$ is maximal ideal of R.

Soln: Given that R be the ring of all the real valued continuous functions on the closed unit interval.

i.e., $R = \{f \mid f : [0,1] \longrightarrow \mathbb{R}$ is continuous on $[0,1]\}$

where $\mathbb{R}$ denote the set of all real numbers.

Here R is a ring w.r.t compositions:

$(f+g)(x) = f(x) + g(x)$

$(fg)(x) = f(x)\,g(x)$ $\forall x \in [0,1]$ and $f, g \in R$

Now we shall show that

$M = \{f \in R \mid f(\frac{1}{3}) = 0\}$ is maximal ideal.

first of all we shall show that M is an ideal of R.

Now for this, first of all we observe that M is non-empty because the real valued function 'e' on [0,1] defined by $e(x) = 0$ $\forall x \in [0,1]$.

$\therefore e \in M$.

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

Now let $f, g \in M$ then $f(\frac{1}{3}) = 0$, $g(\frac{1}{3}) = 0$.

we have $(f-g)(\frac{1}{3}) = f(\frac{1}{3}) - g(\frac{1}{3})$

$= 0 - 0$

$= 0$

$\therefore f-g \in M$

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

Let $f \in M$ and $h \in R$ then $f(1/3)=0$.

Now we have

$$(fh)(1/3) = f(1/3)\,h(1/3) = 0 \cdot h(1/3) = 0.$$

$\Rightarrow fh \in M$

Similarly $hf \in M$

$\therefore M$ is an ideal of R.

Finally we shall show that M is a maximal ideal of R.

Let us define, a function $\theta : [0,1] \to \mathbb{R}$.

such that $\theta(x) = 1 \quad \forall x \in [0,1]$

then θ is a continuous function.

$\therefore \theta \in R$, (ring)

But $\theta \notin M$ as $\theta(1/3) = 1 \neq 0$

$\therefore M \neq R$.

Let U be any other ideal of R such that $M \subset U \subset R$ and $M \neq U$.

we need to show that $U = R$.

Since $M \subset U$ and $M \neq U$,

there exists a function $\lambda \in U$ such that

$\lambda \notin M$ i.e $\lambda(1/3) \neq 0$

Let $\lambda(1/3) = c \neq 0$.

Let us define a function $\rho : [0,1] \to \mathbb{R}$ s.t

$\rho(x) = c \quad \forall x \in [0,1]$.

then $\rho \in R$

Let $\psi = \lambda - \rho$ then $\psi(1/3) = \lambda(1/3) - \rho(1/3)$

$= c - c$

$= 0$.

$\Rightarrow \psi \in M$

$\Rightarrow \psi \in U$ as $M \subset U$

i.e $\varphi = \lambda - \psi \in U$ $(\because \lambda, \psi \in U)$

If γ be a function from $[0,1]$ to $\mathbb{R}$

s.t $\gamma(x) = \frac{1}{c}$, $(c \neq 0)$

Then $\gamma \in R$.

Now we have

$(\gamma\varphi)(x) = \gamma(x)\,\varphi(x)$

$= \frac{1}{c} \cdot c$

$= 1$

$= e(x) \quad \forall x.$

$\Rightarrow \gamma\varphi = e$

Since $\varphi \in U$, $\therefore \gamma\varphi \in U$

we find $e \in U$

But e is the unity of the ring R.

thus U is an ideal containing unity.

$\Rightarrow U = R$

Hence M is Maximal ideal of the ring R.

Method(2) that M is maximal ideal can also be proved by using the fundamental Theorem of homomorphism.

Let us define function

$\Theta : R \longrightarrow \mathbb{R}$ such that

$\Theta(f) = f(1/3) \quad \forall f \in R$ ——— (1)

where $\mathbb{R}$ = set of real numbers.

Then Θ is a homomorphism as

$\Theta(f+g) = (f+g)(1/3)$

$= f(1/3) + g(1/3)$

$\boxed{\Theta(f+g) = \Theta(f) + \Theta(g)}$

&

$\Theta(fg) = (fg)(1/3)$

$= f(1/3)\, g(1/3)$

$\boxed{\Theta(fg) = \Theta(f)\,\Theta(g).}$

To check ontoness,

if $r \in \mathbb{R}$ be any element we can define another map $\phi : [0,1] \longrightarrow \mathbb{R}$ s.t

$\phi(x) = r \quad \forall x \in [0,1]$.

Then ϕ being constant function will be continuous.

Thus $\phi = R$.

Also $\Theta(\phi) = \phi(1/3)$,

showing that ϕ is pre-image of r under Θ.

i.e Θ is onto.

Thus by fundamental theorem of homomorphism

$$\frac{R}{\ker\theta} \cong \mathbb{R}$$

Now $f \in \ker\theta \iff \theta(f) = 0$

$\iff f(1/3) = 0$

$\iff f \in M.$

$\Rightarrow \ker\theta = M$

Hence $\frac{R}{M} \cong \mathbb{R}$, but being a field, $\frac{R}{M}$ will be a field

i.e. M is maximal ideal of R.

(∵ If R is a commutative ring with unity. An ideal M of R is maximal ideal of R $\iff \frac{R}{M}$ is a field.)

→ Let R be a commutative ring. An ideal P of R is a prime ideal iff for two ideals A, B of R, $AB \subseteq P \Rightarrow$ either $A \subseteq P$ or $B \subseteq P$.

Sol Let R be the commutative ring

Let P be a prime ideal of R and

Let A, B be two ideals of R s.t

$AB \subseteq P$.

suppose

$A \nsubseteq P$

$\therefore \exists$ some element $a \in A$ s.t $a \notin P$.

Since $AB \subseteq P$

In particular,

$aB \subseteq P$ $(\because a \in A)$

$\Rightarrow ab \in P \ \forall \ b \in B$. ——— (1)

Since P is prime ideal of R

we get either $a \in P$ or $b \in P$.

but $a \notin P$,

hence $b \in P \ \forall \ b \in B$.

$\Rightarrow B \subseteq P$.

Conversely, suppose that

for two ideals A, B of R,

$AB \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$.

TO P.T 'P' is a prime ideal of R.

Let $ab \in P$. ——— (1)

Let A and B be ideals generated by 'a' & 'b' then $A = (a)$, $B = (b)$.

If $x \in AB$ is any element then it is of the type

$x = a_1b_1 + a_2b_2 + \cdots + a_nb_n : a_i \in A, b_i \in B$.

$= (\alpha_1 a)(\beta_1 b) + (\alpha_2 a)(\beta_2 b) + \cdots + (\alpha_n a)(\beta_n b)$

for $\alpha_i, \beta_i \in R$ as $a_i \in A = (a)$,

$b_i \in B = (b)$.

Thus $x = (\alpha_1\beta_1)(ab) + (\alpha_2\beta_2)(ab) + \cdots\cdots$
$\cdots\cdots + (\alpha_n\beta_n)(ab)$.

$$x = (\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots\cdots + \alpha_n\beta_n)(ab)$$

Since $ab \in P$, P is an ideal,
all multiples of ab are in P.

Thus $x \in P$
i.e $AB \subseteq P$
$\Rightarrow A \subseteq R$ or $B \subseteq P$
$\Rightarrow (a) \subseteq P$ or $(b) \subseteq P$
$\Rightarrow a \in P$ or $b \in P$
$\Rightarrow$ P is prime ideal of R.

→ Let R be a commutative ring with unity. If every ideal of R is prime, show that R is a field.

Soln: To show that R is a field, we need show that every non-zero element of R has multiplicative inverse. We first show that R is an integral domain.

Let $a, b \in R$ such that $ab = 0$
Then $ab \in \{0\}$ which is an ideal of R and is, therefore, prime ideal.
$\Rightarrow a \in \{0\}$ or $b \in \{0\}$
$\Rightarrow a = 0$ or $b = 0$.
$\therefore$ R is an integral domain.

Let now $a \in R$ be any non-zero element and let $a^2R = \{a^2r / r \in R\}$

then it is easy to show that a^2R is an ideal of R.

$\therefore$ a^2R is an ideal of R and is therefore prime ideal.

Now $a.a = a^2 = a^2.1 \in a^2R$

$\Rightarrow a \in a^2R$

$\Rightarrow a = a^2b$ for some $b \in R$

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

$\Rightarrow 1-ab = 0$ as $a \neq 0$

$\Rightarrow ab = 1$

$\Rightarrow$ b is multiplicative inverse of a.

Hence R is a field.

→ Let R be a commutative ring with unity and let M be a maximal ideal of R such that $M^2 = \{0\}$. Show that if N is any maximal of R then $N = M$.

Sol^n: Let $m \in M$ be any element.

then $m.m \in M^2 = \{0\}$

$\Rightarrow m^2 = 0 \in N$ (N is an ideal)

By known theorem, we know that every maximal ideal of R is prime.

$\therefore$ N is prime ideal.

$\Rightarrow m \in N$

$\Rightarrow M \subseteq N$

Thus $M \subseteq N \subseteq R$

Since M is maximal, $N = M$ or $N = R$

But N is maximal in R, thus $N \neq R$

Hence $N = M$.

→ Show that in a Boolean ring R, every prime ideal $P \neq R$ is maximal.

Sol^n: Let P be prime and I be any ideal such that

$P \subseteq I \subseteq R$.

then $\exists$ some $x \in I$, such that $x \notin P$ and

as $x \in R$, $x^2 = x$.

Let now, $y \in R$ be any element, then

$x^2 y = xy$

$\Rightarrow x(xy - y) = 0 \in P$ (P is an ideal)

$\Rightarrow xy - y \in P$ as $x \notin P$ and P is prime.

$\Rightarrow xy - y = p$ for some $p \in P$.

Then $y = xy - p \in I$

as $x \in I$, $y \in R$, $xy \in I$ and also $p \in P \subseteq I$,

$y \in I$

$\Rightarrow R \subseteq I$

$\Rightarrow I = R$

$\Rightarrow$

Definition:

An ideal I of a commutative ring R is called semi prime ideal if $a^2 \in I \Rightarrow a \in I$, for all $a \in R$.

Clearly then every prime ideal is semi prime.

for example:

→ Consider the ideal $I = \{6n / n \in Z\}$ in the ring of integers.

Suppose $a^2 \in I$

Then a^2 is a multiple of 6.

i.e, $6 / a^2$

Since $2/6$, we find $2/a^2$

$\Rightarrow 2/a$ (as 2 is prime)

Similarly $3/a$.

$\Rightarrow 6/a$ as $g.c.d(2,3) = 1$

$\Rightarrow a \in I$.

Hence I is semi prime, but I is not prime as $2.3 = 6 \in I$ but $2, 3 \notin I$.

→ Show that intersection of two prime ideals is a semi prime ideal and so is the intersection of two semi prime ideals.

→ Let R the ring of all real-valued continuous functions on the closed unit interval.

Show that (i.) $M_1 = \{f \in R / f(1/5) = 0\}$

(ii.) $M_2 = \{f \in R / f(2/3) = 0\}$ are maximal ideals of R.
