UG - CBCS Study Materials.

Semester - 4th

Subject - Mathematics (Hons.)

Paper - C10T

Unit-1 : RING THEORY.

Name of the Teacher:

Dr. Sangita Chakraborty

Deptt. of Mathematics

Kharagpur College.

CORE COURSE (C-10) Unit-1. (Jan-June) 4th Sem.
RING THEORY
Paper-C10T

Definition → A non-empty set R w.r.t. two b.os forms a ring $(R,+,\cdot)$ if (i) $(R,+)$ is a commutative group,
(ii) $(R,\cdot)$ is a semi-group, and for any three elements $a,b,c \in R$
(iii) $a\cdot(b+c) = a\cdot b + a\cdot c$ (left distributive law)
$(b+c)\cdot a = b\cdot a + c\cdot a$ (right " ")

Commutative ring → If for any two elements $a, b \in R$, $a\cdot b = b\cdot a$ (multiplication is commutative), then $(R,+,\cdot)$ is called a commutative ring.
For a commutative ring the two distributive laws are identical and called only the " law.

Zero element in $(R,+,\cdot)$ → The additive identity in $(R,+,\cdot)$

Multiplicative identity in $(R,+,\cdot)$ → An element e in $(R,+,\cdot)$ is called a multiplicative identity if $e\cdot a = a\cdot e = a, \forall a \in R$.

Ring with unity → A ring $(R,+,\cdot)$ containing a multiplicative identity, denoted by I. I is unique. Because, if I & I' be two unity in $(R,+,\cdot)$, then
$I\cdot I' = I'$, by the property of I
$= I$, " " " " I'.
$\therefore \boxed{I = I'}$

EXAMPLES OF RINGS →
① $(\mathbb{Z},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are commutative rings with unity 1
② $(n\mathbb{Z},+,\cdot)$; $n \in \mathbb{N}$, is a commutative ring without unity.
③ Ring of real matrices :→ $M_2(\mathbb{R})$ be the set of all $n\times n$ matrices of real numbers, where $n \in \mathbb{N}$.
$(M_n(\mathbb{R}),+,\cdot)$ is a ring with unity I_n } non-commutative rings
$(M_n(\mathbb{C}),+,\cdot)$ " " " " " I_n }
$M_n(\mathbb{C})$ being the set of all $n\times n$ complex matrices.
④ Ring of integers modulo n :→
$(\mathbb{Z}_n,+,\cdot)$ is a commutative ring with unity $\bar{1}$.
$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$, for a fixed $n \in \mathbb{N}$, being the classes of residues of integers modulo n.

Let us consider the subset of $\mathbb{C}$ given by $\mathbb{Z}[i] = \{a+ib : a, b \in \mathbb{Z}\}$, forms a commutative ring with unity $1+0.i$ $(=1)$.

⑥ Ring of Gaussian numbers :⟶ $\mathbb{Q}[i] = \{a+ib : a, b \in \mathbb{Q}\}$, $\mathbb{Q}[i] \subset \mathbb{C}$, forms a commutative ring with unity $1 + i.0\ (=1)$.

⑦ Ring of Quaternions :- Let us consider the set H of 2×2 complex matrices given by

$$H = \left\{ \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} : \begin{matrix} a,b,c,d \in \mathbb{R} \\ \in \mathbb{Q} \\ \in \mathbb{Z} \end{matrix} \right\} \begin{matrix} \longrightarrow \text{Ring of real quaternions} \\ \longrightarrow \text{" " rational "} \\ \longrightarrow \text{" " integral "} \end{matrix}$$

$(H, +, \cdot)$ forms a ring with unity I_2 w.r.t. matrix addition and matrix multiplication.

$$\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} = aI + bJ + cK + dL, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$
$$K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ L = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

⑧ Polynomial rings :⟶ $R[x]$, the set of all polynomials over R; where R is a ring.
$(R[x], +, \cdot)$ is called the polynomial ring over R.
If R be a ring with unity, then $(R[x], +, \cdot)$ is also a ring with unity.
The identity element of the ring $(R[x], +, \cdot)$ is the constant polynomial 1 (1 being the unity in in ring R). Here, $a_0 = 1$, $a_i = 0$ for $i \geq 1$.
The zero element of the ring is the zero polynomial 0 $(a_i = 0, \forall i)$.

In particular, the set $S = \{a_0 + a_1x + \cdots + a_rx^r : a_i \in \mathbb{Z}, r \geq 0\}$ forms a commutative ring with unity under addition and multiplication of polynomials. This ring is denoted by $\mathbb{Z}[x]$.
Similarly, $\mathbb{Q}[x]$ is the ring of all polynomials over $\mathbb{Q}$. $R[x]$ " " " " " over R.
These are commutative ring with unity 1.

Note: Let $f(x), g(x) \in R[x]$ s.t. $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$.

$$f(x) + g(x) = (a_0+b_0) + (a_1+b_1)x + \cdots + (a_m+b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_nx^n \ (m<n)$$
$$= (a_0+b_0) + (a_1+b_1)x + \cdots + (a_n+b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_mx^m \ (m>n)$$
$$f(x) \cdot g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n}, \quad c_j = a_0b_j + a_1b_{j-1} + \cdots + a_jb_0$$

⑨ Ring of continuous functions :→ $C[a,b]$

Let S be the set of all real-valued continuous functions on the closed and bounded interval $[a,b]$.

Let $f:[a,b]\to\mathbb{R}$, $g:[a,b]\in\mathbb{R}$ be the elements of S.

$(f+g)(x) = f(x)+g(x),\quad x\in[a,b]$
$(f\cdot g)(x) = f(x)\cdot g(x),\quad x\in[a,b]$
} we define.

$(S,+,\cdot)$ is a commutative ring with unity, where

$i(x) = 1\ \forall\ x\in[a,b]$, is the unity.

$0(x) = 0\ \forall\ x\in[a,b]$ is the zero element.

ZERO RING & TRIVIAL RING

Let $(A,+)$ be an abelian group with the identity element 0.

Let us define multiplication $(\cdot)$ on A by

$\boxed{a\cdot b = 0}$ for any $a,b\in A$.

$\therefore$ A is closed w.r.t. $(\cdot)$

Let $a,b,c\in A$. Then $a\cdot(b\cdot c) = a\cdot 0 = 0$, by definition
& $(a\cdot b)\cdot c = 0\cdot c = 0$, " "

$\therefore$ $(\cdot)$ is associative on A.

Let $(A,\cdot)$ forms a semigroup.

$a,b,c\in A$. Then $a\cdot(b+c) = 0$ and $a\cdot b + a\cdot c = 0+0 = 0$

Also, $(b+c)\cdot a = 0$ and $b\cdot a + c\cdot a = 0+0 = 0$.

$\therefore$ Distributive laws hold in A.

$\therefore$ $(A,+,\cdot)$ forms a ring, called a zero ring.

In particular, the element 0 in the abelian group $(A,+)$ forms a ring by itself. This ring is called the TRIVIAL ring.

A non-trivial ring R means R has at least two elements.

PROPERTIES of Rings :→ In a ring $(R,+,\cdot)$

(i) $a\cdot 0 = 0\cdot a = 0$, $\forall\ a\in R$, 0 being the zero element in R.

$a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$
$\Rightarrow -(a\cdot 0) + a\cdot 0 = -(a\cdot 0) + [a\cdot 0 + a\cdot 0]$
$\Rightarrow 0 = [-(a\cdot 0) + a\cdot 0] + a\cdot 0$
$\Rightarrow 0 = 0 + a\cdot 0 \Rightarrow 0 = a\cdot 0$.

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

$[b+(-b)] = 0 \Rightarrow a\cdot[b+(-b)] = a\cdot 0 \Rightarrow a\cdot b + a\cdot(-b) = 0$
$\Rightarrow [-(a\cdot b) + a\cdot b] + a\cdot(-b) = -(a\cdot b) + 0 \Rightarrow a\cdot(-b) = -(a\cdot b)$

Also, $[a+(-a)]\cdot b = 0\cdot b = 0 \Rightarrow (-a)\cdot b = -(a\cdot b)$

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

(iii) $(-a)\cdot(-b) = a\cdot b$, $\forall\ a, b \in R$.

Let $p = -a \in R$. $(-a)\cdot(-b) = p\cdot(-b) = -(p\cdot b)$, by (ii)
$= -[(-a)\cdot b] = -[-(a\cdot b)]$, by (ii)
$= a\cdot b$, additive inverse of the " " of $(a\cdot b)$.

If R be a non-trivial ring with unity I, then $0 \neq I$

Since R is non-trivial, $\exists\ a(\neq 0) \in R$, i.e., a is a non-zero element.
Let us assume, $0 = I$.
Then $a\cdot 0 = a\cdot I \Rightarrow 0 = a$, a contradiction.

$\therefore$ $\underline{0 \neq I}$.

Divisors of zero :-

In a ring R, a non-zero element a is said to be a divisor of zero if there exists —
a non-zero element $b \in R$ s.t. $a\cdot b = 0$ (left divisor of zero)
or a " " " $c \in R$ s.t. $c\cdot a = 0$ (right " " ")

If R be a commutative ring then $a\cdot b = 0 = b\cdot a$
i.e., left & right divisor of zeros become identical.

Examples:

① Rings $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ contain no divisor of zero.
Since for any $a \neq 0$, $b \neq 0$, $a\cdot b \neq 0$ in $\mathbb{Z}$, $\mathbb{Q}$ & $\mathbb{R}$.

② The ring $(\mathbb{Z}_5, +, \cdot)$ contains no divisor of zero.
Since $n = 5$, is a prime, $n \neq p\cdot q$ for p & q are 1, 2, 3, 4.

③ The ring $(\mathbb{Z}_6, +, \cdot)$ contains divisors of zero as $\bar{2}, \bar{3}, \bar{4}$.
Since $n = 6$, is a composite number, $n = p\cdot q$, & $\bar{0} = \bar{n} = \bar{p}\cdot\bar{q}$.

④ The ring $M_2(R)$ contains divisors of zero.
$\begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix}\cdot\begin{pmatrix}2 & 6\\ -1 & -3\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix} \neq \begin{pmatrix}2 & 6\\ -1 & -3\end{pmatrix}\begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix}$.
$\therefore$ $\begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix}$ is a left divisor of zero..
& $\begin{pmatrix}2 & 6\\ -1 & -3\end{pmatrix}$ " " right " " " .

Theorem: The cancellation law holds in a ring R if and only if R has no divisor of zero.

Let R be a ring in which cancellation law holds.
Let $a, b \in R$ and $a\cdot b = 0$ where $a \neq 0$.
Then $a\cdot b = 0 = a\cdot 0 \Rightarrow b = 0 \Rightarrow$ a is not a left divisor of zero.
Let $a\cdot b = 0$ where $b \neq 0$
Then $a\cdot b = 0 = 0\cdot b \Rightarrow a = 0 \Rightarrow$ b is not a right " " ".
$\therefore$ R has no divisor of zero.

Conversely, Let R be a ring containing no divisors of zero.
Let $a, b, c \in R$ and $a \cdot b = a \cdot c$ where $a \neq 0$.
Then $a \cdot (b-c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$ (left cancellation)
Let $b \cdot a = c \cdot a$ where $a \neq 0$
Then $(b-c) \cdot a = 0 \Rightarrow b - c = 0 \Rightarrow b = c$ (right cancellation)
$\therefore$ The cancellation law holds in R.

Cancellation law in a ring R is said to hold, if for elements $a, b, c \in R$,
(i) $a \neq 0$ and $a \cdot b = a \cdot c \Rightarrow b = c$ (left cancellation law)
(ii) $a \neq 0$ and $b \cdot a = c \cdot a \Rightarrow b = c$ (right " ")
In a ring R, cancellation law does not hold, in general.

Theorem: A non-trivial finite ring having no divisor of zero is a ring with unity.

Proof: Let $a_0, a_1, \cdots, a_n$ be $(n+1)$ elements of a finite non-trivial ring R, where $a_0 = 0$.
$\therefore a_1 \cdot a_0 = 0$
Let us consider n elements $a_1 \cdot a_1, a_1 \cdot a_2, \cdots, a_1 \cdot a_n \in R$.
Since R contains no divisor of zero, none of $a_1 \cdot a_j$ $(j = 1, 2, \cdots, n)$ is zero. They all are distinct non-zero n elements of R.
since $a_1 \cdot a_i = a_1 \cdot a_j \Rightarrow a_i = a_j$ (as $a_1 \neq 0$, R contains no divisors of zero)
(not possible)
One of them must be a_1. Let $a_1 \cdot a_p = a_1 \longrightarrow$ (i)
Again, let us consider n elements $a_1 \cdot a_1, a_2 \cdot a_1, \cdots, a_n \cdot a_1 \in R$
By similar arguments, we can write
$$a_q \cdot a_1 = a_1 \longrightarrow \text{(ii)}$$
If $b \in R$ be any arbitrary non-zero element,
then let $a_1 \cdot a_r = b \longrightarrow$ (iii) & let $a_s \cdot a_1 = b \longrightarrow$ (iv)
Then $b \cdot a_p = (a_s \cdot a_1) \cdot a_p = a_s \cdot (a_1 \cdot a_p) = a_s \cdot a_1 = b$ [by (iv) & (i)]
& $a_q \cdot b = a_q \cdot (a_1 \cdot a_r) = (a_q \cdot a_1) \cdot a_r = a_1 \cdot a_r = b$ [by (iii) & (ii)]
Also $0 \cdot a_p = a_q \cdot 0 = 0$; if $b = 0$
$\therefore b \cdot a_p = b \ \forall b \in R \longrightarrow$ (v) & $a_q \cdot b = b \ \forall b \in R \longrightarrow$ (vi)
Now, $a_q \cdot a_p = a_q$ [by (v)], $a_q \cdot a_p = a_p$ [by (vi)]
$\therefore a_p = a_q$ and $a_p \cdot b = b \cdot a_p = b \ \forall b \in R$
$\Rightarrow a_p$ is the unity in R.

Unit: Let R be a non-trivial ring with unity I.
An element $a \in R$ is a unit if $\exists$ an element $b \in R$ s.t.
$a \cdot b = b \cdot a = I$.
b is said to be a multiplicative inverse of a, denoted by $\bar{a}^1$.
This inverse is unique.
If possible let b & c be two multiplicative inverses of a.
Then $a \cdot b = b \cdot a = I$, $a \cdot c = c \cdot a = I$.
Now, $c \cdot (a \cdot b) = (c \cdot a) \cdot b$ [by associative property]
$\therefore$ $c \cdot I = I \cdot b$
$\Rightarrow$ $c = b$.
If $a \in R$ be a unit, then $\bar{a}^1 \in R$ and $a \cdot \bar{a}^1 = \bar{a}^1 \cdot a = I$.

Examples:
① In the ring $(\mathbb{Z}, +, \cdot)$, 1 and -1 are the only units.
② " " " $(\mathbb{Q}, +, \cdot)$, each non-zero element is a unit.
③ " " " $(\mathbb{Z}_5, +, \cdot)$, " " " " " " "
④ " " " $(\mathbb{Z}_6, +, \cdot)$, $\bar{1}$ & $\bar{5}$ are units.
⑤ " " " $M_2(\mathbb{R})$, every non-singular 2×2 matrix is a unit

Theorem: In a non-trivial ring R, the zero element has no multiplicative inverse.
Case (i): – If R be a ring without unity, then no element in R can be a unit and hence 0 cannot be a unit.
Case (ii): – Let R be a ring with unity I. If possible, let 0 has 0^{-1} in R. $\therefore 0 \cdot 0^{-1} = \bar{0}^1 \cdot 0 = I$
Again $0 \cdot 0^{-1} = \bar{0}^1 \cdot 0 = 0$
$\therefore$ $I = 0$, which is a contradiction, because,
if $a (\neq 0) \in R$, then $a \cdot I = a \cdot 0 \Rightarrow a = 0$.
$\therefore$ 0^{-1} does not exist in R, or, 0 is not a unit in R.

Theorem: If a be a unit in a ring R with unity, then a is not a divisor of zero.
a be a unit in R $\Rightarrow$ $\bar{a}^1 \in R$. And $a \cdot \bar{a}^1 = \bar{a}^1 \cdot a = I$, $a \neq 0$.
Let $b \in R$ s.t. $a \cdot b = 0$. Then $\bar{a}^1 \cdot (a \cdot b) = \bar{a}^1 \cdot 0$
$\Rightarrow (\bar{a}^1 \cdot a) \cdot b = 0 \Rightarrow I \cdot b = 0$
$\Rightarrow b = 0$.
$\therefore$ a is not a left divisor of zero.
Let $c \in R$ s.t. $c \cdot a = 0$. Then $(c \cdot a) \cdot \bar{a}^1 = 0 \cdot \bar{a}^1$
$\Rightarrow c \cdot (a \cdot \bar{a}^1) = 0 \Rightarrow c \cdot I = 0$
$\Rightarrow c = 0$
$\therefore$ a is not also a right divisor of zero.

Note: If a be a divisor of zero in R, then a is not a unit in R
If a be a divisor of zero, then $a \neq 0, b \neq 0 \Rightarrow a \cdot b = 0$. If $\bar{a}^1 \in R$, then $\bar{a}^1 \cdot (a \cdot b) = \bar{a}^1 \cdot 0$
$\Rightarrow b = 0$, (contradiction)

Theorem: The set of all units in R with unity forms a group w.r.t. multiplication ($\cdot$)

Let I be the unity in R. Then I is a unit in R.
If U be the set of all units of R, then U is non-empty subset of R, as $I \in U$.

(i) Let $a \in U$, $b \in U$. Then $a^{-1} \in R$, $b^{-1} \in R$.
$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = (a \cdot I) \cdot a^{-1} = a \cdot a^{-1} = I$
& $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = I = (a \cdot b) \cdot (b^{-1} \cdot a^{-1})$
$\Rightarrow (a \cdot b)$ has a multiplicative inverse $b^{-1} \cdot a^{-1}$ in R.
$\Rightarrow a \cdot b$ is a unit in $R \Rightarrow a \cdot b \in U$
$\Rightarrow U$ is closed w.r.t. ($\cdot$)

(ii) Multiplication is associative on R and $U \subset R$,
$\therefore$ " " " on U.

(iii) $I \in U$ and $I \cdot a = a \cdot I = a \ \forall a \in U$.
$\Rightarrow I$ is also the identity element of U w.r.t. ($\cdot$)

(iv) Let $a \in U$, so $a^{-1} \in R$. And $a \cdot a^{-1} = a^{-1} \cdot a = I$.
$\Rightarrow a^{-1}$ is a unit in $R \Rightarrow a^{-1} \in U$

$\therefore (U, \cdot)$ forms a group.

Ex. In the ring $(\mathbb{Z}_n, +, \cdot)$, show that $\bar{m}$ is a unit iff the $\gcd(m, n) = 1$.

$(\mathbb{Z}_n, +, \cdot)$ is a commutative ring with unity $\bar{1}$.
Let $\bar{m}$ be a unit in the ring. Then $\bar{m}$ is a non-zero element and $\exists$ a non-zero $\bar{u}$ in $\mathbb{Z}_n$ s.t.
$\bar{m} \cdot \bar{u} = \bar{1} \Rightarrow mu \equiv 1 \pmod{n}$
$\therefore mu - 1 = vn$ for some $v \in \mathbb{Z}$.
i.e., $mu - vn = 1$, where $u, v \in \mathbb{Z}$.
$\therefore \gcd(m, n) = 1$.

Conversely, let $\bar{m} \in \mathbb{Z}_n$ s.t. $\gcd(m, n) = 1$.
$\therefore \exists\ p, q \in \mathbb{Z}$ s.t. $mp + nq = 1 \Rightarrow m \cdot p - 1 = n \cdot q$
$\Rightarrow m \cdot p \equiv 1 \pmod{n}$
Then $p \neq 0$. Let $p \equiv r \pmod{n}$ where $0 < r < n$.
$\Rightarrow mp \equiv rm \pmod{n}$
$\Rightarrow 1 \equiv rm \pmod{n} \Rightarrow \bar{r} \cdot \bar{m} = \bar{1}$.
$\therefore \bar{m} \cdot \bar{r} = \bar{r} \cdot \bar{m} = \bar{1}$, since the ring is commutative.
$\Rightarrow \bar{m}$ is a unit.

Note. (i) If n be a prime, every non-zero element in $(\mathbb{Z}_n, +, \cdot)$ is a unit.

(ii) $U_n = \{\bar{m} : \gcd(m, n) = 1\}$ be the set of units of $(\mathbb{Z}_n, +, \cdot)$
$(U_n, \cdot)$ forms a group. It is a finite group of $\phi(n)$ elements.
$\phi(1) = 1$, $n \geq 2$, $\phi(n)$ = Nos of +ve integers $< n$ & prime to n

Theorem: Every non-zero element in a finite ring having no divisor of zero is a unit.

Let $a_0, a_1, \ldots, a_n$ be $n+1$ elements of a ring R, where a_0 is the zero element.
Since R is finite & contains no divisor of zero, R contains the unity I.
Considering the products $a_1 \cdot a_0, a_1 \cdot a_1, a_1 \cdot a_2, \ldots, a_1 \cdot a_n$ which all $\in R$, and $a_1 \cdot a_0 = 0$, others are all n distinct non-zero element of R.
Let $a_1 \cdot a_u = I$. Similarly, let $a_v \cdot a_1 = I$.
Now, $a_v \cdot (a_1 \cdot a_u) = (a_v \cdot a_1) \cdot a_u$

$\Rightarrow a_v \cdot I = I \cdot a_u \Rightarrow a_u = a_v$.

$\because a_1 \cdot a_u = a_u \cdot a_1 = I \Rightarrow a_1$ is a unit.
proceeding with the same argument, we say every non-zero element is a unit of R.

Note: The above theorem does not hold if the ring contains infinite number of elements.
eg. $(\mathbb{Z}, +, \cdot)$ contains no divisor of zero but 1 & -1 are only the units of $(\mathbb{Z}, +, \cdot)$.

Characteristic of a ring: char R is the least +ve integer n (if exists) s.t. $na = 0 \ \forall\, a \in R$, where $na = a + a + \ldots + a$ (n times).
If no such n exists, char $R = 0$.
char $R = 1$ iff R is the trivial ring.

Note: char R is determined by the identity element I when R is a ring with unity. Show it.

To show: $nI = 0 \Rightarrow \text{char } R = n$.
Let $a \in R$. Then $na = a + a + \ldots + a$ (n times)
$= a \cdot (I + I + \ldots + I)$
$= a \cdot nI = a \cdot 0 = 0$

$\therefore na = 0 \ \forall\, a \in R \Rightarrow \text{char } R = n$.
If for no +ve integer n, $nI = 0$ holds, $\therefore na = 0$ does not hold for a " " n.
$\therefore$ **char $R = 0$**.

Examples:
① Let $R = (\mathbb{Z}, +, \cdot)$. Then char $R = 0$
② Let $R = (\mathbb{Z}_6, +, \cdot)$. Then char $R = 6$
③ Let $R = (\mathbb{Z}_n, +, \cdot)$ Then char $R = n$.

Integral domain: (I.D.)

A non-trivial ring R with unity is called an integral domain if it is commutative and contains no divisor of zero.

Examples:

① $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ are integral domains

② $(2\mathbb{Z}, +, \cdot)$ is Not an integral domain, since it is a ring without unity. It is commutative & contains no divisor of zero.

③ $(\mathbb{Z}_6, +, \cdot)$ is Not an integral domain, since it contains divisor of zero ($\bar{2} \cdot \bar{3} = \bar{0}$).

④ $(\mathbb{Z}_5, +, \cdot)$ is an integral domain, (5 being a prime)

⑤ The ring $M_n(\mathbb{Z})$ is a non-commutative ring. So it is Not an I.D.

⑥ The ring $\mathbb{Z} \times \mathbb{Z}$ is a commutative ring with unity. $(1,0) \cdot (0,1) = (0,0) \Rightarrow$ it contains divisors of zero. $\therefore \mathbb{Z} \times \mathbb{Z}$ is an I.D.

⑦ The set of all real-valued continuous functions $C[0,1]$ forms a ring. It is a commutative ring with unity 1 (the constant function). The ring contains divisors of zero, since for $f(x) \neq 0$, $g(x) \neq 0$, $f(x) \cdot g(x) = 0$, $x \in [0,1]$.

eg: Let $f(x) = 0, \; x \in [0, \frac{1}{2})$; $g(x) = x - \frac{1}{2}, \; x \in [0, \frac{1}{2})$
$= x - \frac{1}{2}, \; x \in [\frac{1}{2}, 1]$; $= 0, \; x \in [\frac{1}{2}, 1]$
} Then $f \neq 0, g \neq 0$ $\Rightarrow f \cdot g = 0$ in $[0,1]$

Ex①. Prove that the ring $(\mathbb{Z}_n, +, \cdot)$ is an I.D. iff n is a prime.

Let $(\mathbb{Z}_n, +, \cdot)$ be an I.D. $n \neq 1$, since it is a non-trivial ring.

To prove: n is prime. If possible, let $n = p \cdot q$, where $p, q \in \mathbb{Z}^+$ s.t. $1 < p < n$, $1 < q < n$.
$\therefore \bar{p}, \bar{q} \in \mathbb{Z}_n$, and $\bar{p} \cdot \bar{q} = \bar{n} = \bar{0} \Rightarrow (\mathbb{Z}_n, +, \cdot)$ contains divisors of zero, a contradiction.

Conversely, let n be a prime.

To prove: the ring $(\mathbb{Z}_n, +, \cdot)$ is an I.D.

We know $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring with unity $\bar{1}$.

Let $\bar{m} (\neq \bar{0}) \in \mathbb{Z}_n$. Then $0 < m < n$.

Since n is prime, $\gcd(m, n) = 1$. Then $\exists \; u, v \in \mathbb{Z}$, s.t.
$m \cdot u + n \cdot v = 1 \Rightarrow u \cdot m \equiv 1 \pmod{n} \Rightarrow u \not\equiv 0 \pmod{n}$

Let $u \equiv r \pmod n$, $0 < r < n$.

$\Rightarrow u \cdot m \equiv r \cdot m \pmod n$

$\Rightarrow 1 \equiv r \cdot m \pmod n$

$\Rightarrow \bar{r} \cdot \bar{m} = \bar{1} = \bar{m} \cdot \bar{r}$, since the ring is commutative.

$\therefore \bar{m}$ is a unit and hence $\bar{m}$ is not a divisor of zero.

$\therefore$ The ring $(Z_n, +, \cdot)$, when n is prime, contains no divisor of zero, hence it is an I.D.

Ex② Prove that the ring $Z[i] = \{a+bi : a, b \in Z\}$ of Gaussian integers is an I.D.

$Z[i]$ is a commutative ring with unity $1 (= 1+0i)$.

Let $(a+bi)(c+di) = 0$ and let $a+bi \neq 0$. Then $(a,b) \neq (0,0)$.

$\Rightarrow (ac-bd) + i(ad+bc) = 0 \Rightarrow$ $ac - bd = 0$ & $ad + bc = 0$ } homogeneous system in a, b having non-zero soln

$\therefore$ The coefficient determinant:

$$\begin{vmatrix} c & -d \\ d & c \end{vmatrix} = 0 \Rightarrow c^2 + d^2 = 0 \Rightarrow c = 0, d = 0.$$

Thus $(a+bi)(c+di) = 0$ with $a+ib \neq 0 \Rightarrow c+di = 0$.

$\therefore Z[i]$ contains no divisor of zero, hence an I.D.

Ex③. The rings: $Z[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in Z\}$,
$Z[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in Z\}$
$Z[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in Z\}$
$Z[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in Z\}$
- - - - - - -
etc.
} All are Integral domains.

Let us take $Z[\sqrt{5}]$; it is a commutative ring with unity $1 (= 1 + 0\sqrt{5})$.

Let $(a + b\sqrt{5}) \cdot (c + d\sqrt{5}) = 0$ and let $(a, b) \neq (0, 0)$.

$\Rightarrow (ac + 5bd) + \sqrt{5}(ad + bc) = 0$

$\Rightarrow$ $ac + 5bd = 0$ & $ad + bc = 0$ } Homogeneous system in a, b having $(a, b) \neq (0, 0)$

$\therefore \begin{vmatrix} c & 5d \\ d & c \end{vmatrix} = 0 \Rightarrow c^2 - 5d^2 = 0 \Rightarrow c = \sqrt{5}d$, holds only for $c = 0, d = 0$, since $c, d \in Z$

$\therefore (a + b\sqrt{5}) \cdot (c + d\sqrt{5}) = 0$ with $(a, b) \neq (0, 0)$

$\Rightarrow (c, d) = (0, 0)$

Hence $Z[\sqrt{5}]$ ring contains no divisor of zero.

$\therefore Z[\sqrt{5}]$ is an I.D.

Ex. Prove that the ring $\mathbb{Z}[x]$, the ring of all polynomials with integer coefficients, is an I.D.

$\mathbb{Z}[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : n \geq 0,\ a_i \in \mathbb{Z}\}$.

As the ring $\mathbb{Z}$ is a commutative ring with unity, the ring $\mathbb{Z}[x]$ is " " " " " 1, the constant polynomial $[a_0 = 1,\ a_i = 0, \forall i \geq 1]$.

The zero element in the ring $\mathbb{Z}[x]$ is 0, the constant polynomial $[a_0 = 0,\ a_i = 0\ \forall\ i \geq 1]$.

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, where $a_n \neq 0$.
& $g(x) = b_0 + b_1x + \cdots + b_mx^m \in \mathbb{Z}[x]$, where $b_m \neq 0$; $b_i \in \mathbb{Z}$.

Then $f(x)\cdot g(x) \in \mathbb{Z}[x]$, is a polynomial with a non zero term $a_nb_mx^{m+n}$ $[\because a_nb_m \neq 0]$

$\therefore f(x)\cdot g(x) \in \mathbb{Z}[x]$, is a non-zero polynomial.

This proves that $\mathbb{Z}[x]$ contains no divisor of zero and hence it is an I.D.

Ex: The polynomial ring $\mathbb{Z}_p[x]$ is an I.D. if p is a prime, but is not an I.D. if p is a composite number.

Case 1: when p is prime.

Proceeding as above only exception that $a_i, b_i \in \mathbb{Z}_p$.

Here the unity is I $(a_0 = I,\ a_i = \bar{0}\ \forall\ i \geq 1)$.

& the zero element is $\bar{0}$ $(a_0 = \bar{0},\ a_i = \bar{0}\ \forall i \geq 1)$.

$f(x)\cdot g(x) \in \mathbb{Z}_p[x]$ contains the non-zero term $a_nb_mx^{n+m}$, where $a_n \neq \bar{0}$, $b_m \neq \bar{0} \Rightarrow a_nb_m \neq \bar{0}$, since p is prime and $a_n, b_m \in \{\bar{1}, \bar{2}, \bar{3}, \cdots, \overline{p-1}\} = \mathbb{Z}_p$.

$\therefore f(x)\cdot g(x) \neq \bar{0}$, when p is prime.

$\therefore \mathbb{Z}_p[x]$ contains no divisor of zero.

$\therefore$ $\mathbb{Z}_p[x]$ is an I.D. when p is prime.

Case 2: when p is composite, say $p = p_1 \cdot p_2$, $1 < p_1, p_2 < p$ and $p_1, p_2 \in \mathbb{Z}^+$.

Then $\bar{p}_1 \in \mathbb{Z}_p$, $\bar{p}_2 \in \mathbb{Z}_p$ and $\bar{p}_1 \cdot \bar{p}_2 = \bar{p} = \bar{0}$.

$\therefore$ If we consider two polynomials $f(x), g(x) \in \mathbb{Z}_p[x]$ such that $f(x) \neq \bar{0}$ & $g(x) \neq \bar{0}$ with $f(x)\cdot g(x) \in \mathbb{Z}_p[x]$ containing the only term $a_nb_mx^{n+m}$, where $a_n = \bar{p}_1 (\neq \bar{0}) \in \mathbb{Z}_p$ and $b_m = \bar{p}_2 (\neq \bar{0}) \in \mathbb{Z}_p$. But $a_nb_m = \bar{p}_1 \cdot \bar{p}_2 = \bar{p} = \bar{0}$.

$\therefore f(x)\cdot g(x) = \bar{0}$ for $f(x) \neq \bar{0}$, $g(x) \neq \bar{0}$,

$\therefore$ ring $\mathbb{Z}_p[x]$ contains divisor of zero when p is composite.

$\therefore$ $\mathbb{Z}_p[x]$ is NOT an I.D. for p composite

Note: ① The polynomial ring $Z_p[x]$, when p is a prime, is an infinite I.D. having characteristic p.

Since for $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in Z_p[x]$,
then $pf(x) = pa_0 + pa_1x + pa_2x^2 + \cdots + pa_nx^n = \bar{0}$, $a_i \in Z_p$
$\therefore$ characteristic of the I.D. $Z_p[x]$ is p.

② The polynomial ring $Z_p[x]$, where p is a composite number, is an infinite ring having characteristic p.

Theorem:- A commutative ring R with unity is an I.D. if and only if for every non-zero element $a \in R$
$a.u = a.v \Rightarrow u = v$; $u, v \in R$.

Proof:- Let R be a commutative ring with unity and in R $a.u = a.v \Rightarrow u = v$; $u, v \in R$ for $a(\neq 0) \in R$.
Let us take $v = 0$, $\therefore a.u = a.0 \Rightarrow u = 0$
or, $a.u = 0 \Rightarrow u = 0$
$\Rightarrow$ a is not a left divisor of zero.
Since R is a commutative ring, a is not a right divisor of zero also.
$\therefore$ R contains no divisor of zero
$\therefore$ R is an I.D.
Conversely, let R be an I.D., and $a(\neq 0) \in R$.
Then $a.u = a.v \Rightarrow a.(u-v) = 0$
$\Rightarrow u - v = 0$, since R contains no divisor of zero.
$\Rightarrow u = v$.
proved.

Note: In an I.D., the cancellation law for multiplication holds inspite of non-existence of multiplicative inverses, in general.

Theorem:- The characteristic of an I.D. is either zero or a prime number.

Proof: Let the characteristic of an I.D. D be a +ve integer say m.
Now $m \neq 1$, since D is a non-trivial ring.
If possible, let m be a composite number. Then
$m = pq$ where $p, q \in Z$ s.t. $1 < p < m$, $1 < q < m$.
Let I be the unity in D. Since $\text{char } D = m$, m is the least +ve integer for which $mI = 0$. But $mI = (pI).(qI) = 0$.
Since D contains no divisor of zero, either $pI = 0$ or $qI = 0$.

RINGS & FIELDS

Exercises – 19 (S. K. Mapa).

① Define addition $\oplus$ and multiplication $\odot$ on $\mathbb{Z}$ by $a \oplus b = a+b-1$ and $a \odot b = a+b-ab$ for $a, b \in \mathbb{Z}$. Prove that $(\mathbb{Z}, \oplus, \odot)$ is an I.D.

To show first $(\mathbb{Z}, \oplus, \odot)$ is a non-trivial ring:-

(i) $(\mathbb{Z}, \oplus)$ is an abelian group $\longrightarrow$

for $a, b \in \mathbb{Z}$, $a \oplus b = a+b-1 \in \mathbb{Z}$ (closed w.r.t. $\oplus$).

For $a, b, c \in \mathbb{Z}$, $(a \oplus b) \oplus c = (a+b-1) \oplus c$

$= a+b-1+c-1 = a+b+c-2$

And $a \oplus (b \oplus c) = a \oplus (b+c-1) = a+b+c-1-1$

$= a+b+c-2$

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

Associative property w.r.t. $\oplus$ holds.

Let $a \oplus b = a \Rightarrow a+b-1 = a \Rightarrow b = 1 \in \mathbb{Z}$.

$\therefore$ 1 is the zero element in $(\mathbb{Z}, \oplus)$,

Let $a \oplus b = 1 \Rightarrow a+b-1 = 1 \Rightarrow b = 2-a \in \mathbb{Z}$.

$\therefore$ For $a \in \mathbb{Z}$, $\exists$ its additive identity as $(2-a)$.

Again $a \oplus b = a+b-1 = b+a-1 = b \oplus a$.

$\therefore (\mathbb{Z}, \oplus)$ becomes an abelian group.

(ii) $(\mathbb{Z}, \odot)$ is a semigroup $\longrightarrow$.

for $a, b \in \mathbb{Z}$, $a \odot b = a+b-ab \in \mathbb{Z}$.

$\therefore \mathbb{Z}$ is closed w.r.t. $\odot$

For $a, b, c \in \mathbb{Z}$, $(a \odot b) \odot c = (a+b-ab) \odot c$

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

$= a+b+c-(ab+bc+ca)+abc$.

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

$= a+b+c-(ab+bc+ca)+abc$.

$\therefore (a \odot b) \odot c = a \odot (b \odot c)$.

$\therefore (\mathbb{Z}, \odot)$ forms a semigroup.

Distributive property also holds.

(iii) $(\mathbb{Z}, \odot)$ is commutative $\longrightarrow$

$a \odot b = a+b-ab = b+a-ba = b \odot a$

(iv) For unity, let $a \odot b = a \Rightarrow a+b-ab = a$

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

$\Rightarrow b = 0, \forall a \in \mathbb{Z}$.

$\therefore$ 0 is the unity.

$(\mathbb{Z}, \oplus, \odot)$ is a non-trivial ring, because 0 & 1 are at least two elements of it.

∴ $(Z, \oplus, \odot)$ is a non-trivial commutative ring with unity.

Let us consider $a \odot b = 1$ (zero element), for $a \neq 1$.

$\therefore a+b-ab = 1$.

$a,\ b(1-a) = 1-a$.

$a,\ b = \frac{1-a}{1-a} = 1$ (zero element)

∴ The ring $(Z, \oplus, \odot)$ contains no divisor of zero. Hence it is an I.D.

(2) Let $D = \{2^n : n \in Z\}$. Define $\oplus$ & $\odot$ on D by $2^m \oplus 2^n = 2^{m+n}$; $2^m \odot 2^n = 2^{mn}$ for $m, n \in Z$.

Show that $(D, \oplus, \odot)$ is an I.D. Find the units in D.

First prove that $(D, \oplus, \odot)$ is a ring.

(i) Commutative ring → $2^m \odot 2^n = 2^{mn} = 2^{nm} = 2^n \odot 2^m$

(ii) Unity → Let $2^m \odot 2^n = 2^n \Rightarrow 2^{mn} = 2^n \Rightarrow mn = n$ ~~if $n \neq 0$, $n = 0$~~. $\forall n \in Z$

∴ $2^m \Rightarrow m = 1$, ~~it is the unity~~

To find the zero element → Let $2^m \oplus 2^n = 2^n$

$a,\ 2^{m+n} = 2^n \Rightarrow m+n = n$

$\Rightarrow m = 0$.

∴ $2^m = 2^0 = 1$ is the zero-element.

∴ $(D, +, \odot)$ is a commutative ring with unity. It is a non-trivial ring, since unity exists.

(iii) Let $2^m \odot 2^n = 1$ (zero-element) for $2^m \neq 1$ (i.e., $m \neq 0$)

$a,\ 2^{mn} = 2^0 \Rightarrow mn = 0 \Rightarrow n = 0$ for $m \neq 0$.

∴ $2^n = 2^0 = 1$ (zero element).

∴ It does not contain divisors of zero.

∴ $(D, \oplus, \odot)$ is an I.D.

To find the units:

Let $2^m \odot 2^n = 2$ (unity element)

$a,\ 2^{mn} = 2^1 \Rightarrow mn = 1 \Rightarrow m = 1, n = 1$ or $m = -1, n = -1$ $\}$ $m, n \in Z$.

∴ 2^1 & 2^{-1} are two units only in $(D, \oplus, \odot)$.

Ex. ④ D is an I.D. and $a, b \in D$.

(i) If $a^5 = b^5$ and $a^8 = b^8$, prove that $a = b$

(ii) If $a^m = b^m$ and $a^n = b^n$; m, n are +ve integers relatively prime, prove that $a = b$.

(i). $a^5 = b^5 \Rightarrow a^{15} = b^{15} \longrightarrow ①$

$a^8 = b^8 \Rightarrow a^{16} = b^{16} \Rightarrow a(a^{15}) = b(b^{15}) \Rightarrow a \cdot b^{15} = b \cdot b^{15}$ [by ①]

$\Rightarrow a = b$ [Since D is an I.D. & Cancellation law holds in D].

(ii) $a^m = b^m \longrightarrow ①$, $a^n = b^n \longrightarrow ②$

Since m, n are +ve integers relatively prime, $\exists$ two integers p & q s.t.

$$mp + nq = 1 \longrightarrow ③.$$

Now $a^m = b^m \Rightarrow a^{mp} = b^{mp} \longrightarrow ④$

$a^n = b^n \Rightarrow a^{nq} = b^{nq} \longrightarrow ⑤$

$\Rightarrow a^{mp} \cdot a^{nq} = b^{mp} \cdot b^{nq}$

$\Rightarrow a^{mp+nq} = b^{mp+nq}$

$\Rightarrow a^1 = b^1$ [by ③]

$\Rightarrow a = b$.

Ex. 5. Examine if the set S is a field.

(i) $S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ (ii) $S = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

(i) First to prove: $(S, +, \cdot)$ is a commutative ring with unity $1 (= 1 + 0\sqrt{2})$

Let $(a, b) \neq (0, 0)$, ~~$(c, d) \neq (0, 0)$~~, $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = 1$

$$\Rightarrow c + d\sqrt{2} = \frac{1}{a + b\sqrt{2}}$$

$$= \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

$$\Rightarrow c + d\sqrt{2} = \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a^2 - 2b^2}\sqrt{2},$$

exists, provided $a^2 - 2b^2 \neq 0$, or, $a \neq \sqrt{2}\, b$.

Now for $a, b \in \mathbb{Z}$, $a \neq \sqrt{2}\, b$. ~~$\forall (a,b) \neq (0,0)$ & $a, b \in \mathbb{Q}$, $a \neq \sqrt{2}\, b$. But for $a, b \in \mathbb{Q}$, $a \neq \sqrt{2}\, b$ for $a \neq 0, b \neq 0$; for $a \neq 0, b = 0$~~

$\therefore \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a^2 - 2b^2}\sqrt{2}$ is the multiplicative inverse of $a + b\sqrt{2}$.

$\therefore (a + b\sqrt{2})$ is a unit in $(S, +, \cdot)$

$\therefore$ Each non-zero element is a unit.

$\therefore$ (i) $S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a field.

$S = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is also a field for all $(a,b) \neq (0,0)$ & $(a,b) \in \mathbb{Q}$

Show that R/U contains unity element I+U, if R contains unity element I. [U being the proper ideal of R]

$(a+U)*(I+U) = a\cdot I + U = a+U$ and $(I+U)*(a+U) = I\cdot a + U = a+U$ $\Big\}\ \forall\ a+U \in R/U$.

Example:

① Let $R=(\mathbb{Z},+,\cdot)$, $U=(5\mathbb{Z},+,\cdot)$. Then U is an ideal of R. The quotient ring R/U is a commutative ring of 5 elements: U, 1+U, 2+U, 3+U, 4+U. 1+U is the identity element in R/U.

For $n>0$, $U=n\mathbb{Z}$ is an ideal of R, $R/U=\{\bar{0},\bar{1},\bar{2},\bar{3},\cdots,\overline{n-1}\}$ residue classes.

② Let $R=(2\mathbb{Z},+,\cdot)$, $U=(6\mathbb{Z},+,\cdot)$. Then U is an ideal of R. R/U is a commutative ring with 3 elements: U, 2+U, 4+U. Here 4+U is the identity element in R/U. Since $(4+U)*(2n+U) = (4\cdot 2n)+U$, $n\in\mathbb{Z}$

$= 8n+U = (6n+2n)+U$

$= (6n+U)+(2n+U)$

$= (0+U)+(2n+U) = (0+2n)+U$

$= 2n+U$.

But R is a ring without unity.

③ Let $R=(\mathbb{Z}_6,+,\cdot)$, and $U=\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4}\}$. Then U is an ideal of R.

$R/U=\{a+U : a\in\mathbb{Z}_6\}=\{\bar{0}+U,\bar{1}+U\}$

④ Let $R=(\mathbb{Z}_6,+,\cdot)$, and $U=\langle\bar{3}\rangle=\{\bar{0},\bar{3}\}$. Then U is an ideal of R. $R/U=\{a+U : a\in\mathbb{Z}_6\}=\{\bar{0}+U,\bar{1}+U,\bar{2}+U\}$.

-T=: Let R be a ring and I be an ideal of R. If J be an ideal of R s.t. $I \subset J \subset R$, then J/I is an ideal of R/I.

Proof: $I \subset J \subset R$. Since I is an ideal of R,
$a, b \in I \Rightarrow a-b \in I$ and $a \in I, r \in R \Rightarrow ra \in I, ar \in I$
Now, $a, b \in I \Rightarrow a-b \in I$ and $a \in I, s \in J \Rightarrow sa \in I, as \in I$,
since $s \in R$ also.
This proves that I is an ideal of J $\Rightarrow$ the quotient ring J/I exists
Since $I \subset J \subset R$, J/I is a non-empty subset of R/I.
Let $a+I \in J/I$, $bI \in J/I$. Then $a, b \in J$.
Since J is an ideal of R, $a \in J, b \in J \Rightarrow a-b \in J$ and
$a \in J, r \in R \Rightarrow r.a \in J$ and $a.r \in J$.
So, $(a-b)+I \in J/I$ and $(ra)+I \in J/I$,
$\Rightarrow (r+I)*(a+I) \in J/I$
Also $(a.r)+I \in J/I$
$\Rightarrow (a+I)*(r+I) \in J/I$.
$\therefore$ J/I is an ideal of R/I [Since $a+I \in J/I$, $r+I \in R/I$]

Th: In a commutative ring R with unity, an ideal P is a prime ideal iff the quotient ring R/P is an I.D.

Proof: Let P be a prime ideal in the ring R.
Since R is a commutative ring with unity,
R/P " also "
Let $(a+P)*(b+P) = 0+P$, where $a+P \in R/P$, $b+P \in R/P$
$\Rightarrow a.b+P = 0+P = P$ [zero element in R/P] [$a, b \in R$].
$\Rightarrow ab \in P \Rightarrow$ either $a \in P$ or $b \in P$ [$\because$ P is a prime ideal]
i.e., either $a+P = 0$ or $b+P = 0$
Thus R/P contains no divisor of zero, and so it is an I.D.

Conversely, let P be an ideal in the ring R such that R/P is an I.D.
Let $ab \in P$. Then $ab+P = P \Rightarrow (a+P)*(b+P) = P$, but P is the zero element in the quotient ring R/P.
Since R/P is an I.D., we have either $a+P = P$ or $b+P = P$
$\Rightarrow$ either $a \in P$ or $b \in P$. $\Rightarrow$ P is a prime ideal in R

Th: In a commutative ring R with unity, an ideal M is a maximal ideal iff the quotient ring R/M is a field.

Th: Every maximal ideal in a commutative ring with unity is a prime ideal.

Let M be a maximal ideal in a commutative ring R with unity. Then the quotient ring R/M is a field and hence R/M is an I.D. and therefore M is a prime ideal.

Ex: Find the maximal ideals and the prime ideals in the ring Z_6.

The ring Z_6 is a principal ideal ring.

The ideals of Z_6 are:

$\langle \bar{0} \rangle = \{\bar{0}\}$
$\langle \bar{1} \rangle = Z_6$
$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$
$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$
$\langle \bar{4} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$
$\langle \bar{5} \rangle = Z_6$

$\langle \bar{0} \rangle \subset \langle \bar{2} \rangle \subset Z_6$;
$\langle \bar{0} \rangle \subset \langle \bar{3} \rangle \subset Z_6$

There exists no proper ideal of Z_6 strictly containing $\langle \bar{2} \rangle$ and $\langle \bar{3} \rangle$

$\therefore$ The maximal ideals of Z_6 are $\langle \bar{2} \rangle$ and $\langle \bar{3} \rangle$

Since Z_6 is a commutative ring with unity, every maximal ideal of Z_6 is a prime ideal.

Let P be a prime ideal of $R = Z_6$. Then the quotient ring R/P is an I.D.

Since R is finite, R/P is finite $\Rightarrow R/P$ is a field and therefore the ideal P is maximal.

Hence the prime ideals of Z_6 are the maximal ideals, i.e., $\langle \bar{2} \rangle$ and $\langle \bar{3} \rangle$.

(11) Find the maximal ideals and the prime ideals in the ring Z_{12}.

$\langle \bar{0} \rangle = \{\bar{0}\}$, $\langle \bar{1} \rangle = Z_{12}$, $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$, $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$
$\langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$, $\langle \bar{5} \rangle = \{\bar{0}, \bar{1}, \cdots, \bar{11}\} = Z_{12}$, $\langle \bar{6} \rangle = \{\bar{0}, \bar{6}\}$

$\langle \bar{0} \rangle \subset \langle \bar{2} \rangle \subset Z_{12}$; $\langle \bar{0} \rangle \subset \langle \bar{3} \rangle \subset Z_{12}$

The maximal ideals are: $\langle \bar{2} \rangle$, $\langle \bar{3} \rangle$

" prime " " $\langle \bar{2} \rangle$, $\langle \bar{3} \rangle$.

Th 4:

(8) Let U be an ideal of a ring R. Then the mapping $\theta: R \to R/U$ defined by $\theta(x) = x+U$, $x \in R$ is an onto homomorphism with kernel U.

Proof: Let $x, y \in R$. Then $\theta(x) = x+U$, $\theta(y) = y+U$

$$\theta(x+y) = (x+y)+U = (x+U)+(y+U) = \theta(x)+\theta(y)$$

$$\theta(xy) = xy+U = (x+U)*(y+U) = \theta(x)*\theta(y)$$

$\therefore$ θ is a homomorphism.

The zero element in the quotient ring R/U is U.

$\text{Ker}\,\theta = \{x \in R : \theta(x) = U\}$

$\theta(x) = U \Rightarrow x+U = U \Rightarrow x \in U$

$\therefore$ $\text{Ker}\,\theta = U$.

Fundamental theorem of ring homomorphism:

Let ϕ be a homomorphism of a ring R onto a ring R' with kernel U. Then show that R' is isomorphic to the quotient ring R/U.

Let us define the map $\psi: R/U \to R'$ by

$$\psi(a+U) = \phi(a), \quad a+U \in R/U.$$

First to show that ψ is well-defined.

i.e., if $a'+U = a+U$, then $\psi(a'+U) = \psi(a+U) = \phi(a)$

$a'+U = a+U \Rightarrow a'-a \in U \Rightarrow \phi(a'-a) = 0'$, $\because \text{Ker}\,\phi = U$.

$\Rightarrow \phi(a') = \phi(a) \Rightarrow \psi(a'+U) = \phi(a)$

$\therefore$ ψ is well defined

Next to show that ψ is a homomorphism

$$\psi[(a+U)+(b+U)] = \psi[(a+b)+U] = \phi(a+b)$$
$$= \phi(a)+\phi(b) = \psi(a+U)+\psi(b+U)$$

And $\psi[(a+U)(b+U)] = \psi[ab+U] = \phi(ab) = \phi(a)\phi(b)$
$$= \psi(a+U)\,\psi(b+U)$$

$\Rightarrow$ ψ is a homomorphism.

ψ is one-to-one, because

$\psi(a+U) = \psi(b+U) \Rightarrow \phi(a) = \phi(b) \Rightarrow \phi(a)-\phi(b) = 0'$

$\Rightarrow \phi(a-b) = 0' \Rightarrow a-b \in U$

$\Rightarrow a+U = b+U$.

Finally, ψ is onto, because, each element of R'

Sem-1/2019. Paper-C10T:

UNIT-1.

1. (a) $a.a = a$. $(I-a).(I-a) = I.I - I.a - a.I + (a).(-a)$
$= I - a - a + a$
$= I - a + 0 = I - a$.
$\therefore (I-a).(I-a) = I-a$
$\Rightarrow$ I-a is also idempotent.

(b) An ideal $M \neq R$ is said to be a maximal ideal in R if for any ideal U of R satisfying $M \subset U \subset R$, either $U = M$ or $U = R$.
[i.e., $\exists$ no proper ideal of R strictly containing M]
example: ① For $R = \mathbb{Z}$, $2\mathbb{Z}$ is the maximal ideal in a simple ring/field
② the null ideal is a " "

(c) Char R: It is the least +ve integer n (if exists) s.t. $na = 0 \ \forall a \in R$.
If no such n exists, then char R = 0.
For trivial ring, char R = 1.

(d) $(ab)^2 = ab^2 + bab - b^2$
$\Rightarrow (ab)(ab) = (ab)b + bab - bb$
$\Rightarrow (aba)b = (ab + ba - b)b$
$\Rightarrow (aba)bb^{-1} = (ab + ba - b)bb^{-1}$ [$\because b \neq 0$]
$\Rightarrow aba = ab + ab - b$ [$\because bb^{-1} = I$, Field is commutative]
$\Rightarrow aab - 2ab + b = 0$
$\Rightarrow (aa - 2a + I)bb^{-1} = 0.b^{-1}$
$\Rightarrow aa - a - a + I = 0 \Rightarrow (a-I)(a-I) = 0$
$\Rightarrow a - I = 0 \Rightarrow a = I$ [$\because$ Field contains no divisors of zero]

(e) Let R be an I.D. & R[x] is a P.S. ring,
As R is a commutative ring with unity I (say) the ring R[x] is also a commutative ring, with unity I. The zero element of R, say 0 is also the zero " " R[x].
Let $f(x) := \sum_{i=0}^{\infty} a_i x^i$ & $g(x) = \sum_{i=0}^{\infty} b_i x^i \in R[x]$, are both non-zero p.s. in R[x], where $a_i, b_i \in R$.

Let $a_m \neq 0$ and $b_n \neq 0$.

Then $f(x)g(x)$ is also a P.S. in $R[x]$ with a non-zero term $a_m b_n x^{m+n}$, since $a_m \cdot b_n \neq 0$

[$\because$ R is an I.D. containing no divisor of zero, i.e., $a_m \neq 0, b_n \neq 0 \Rightarrow a_m \cdot b_n \neq 0$]

$\therefore$ $f(x)g(x)$ is a non-zero P.S. in $R[x]$ whenever $f(x)$ & $g(x)$ are both " in $R[x]$

$\therefore$ $R[x]$ is an I.D.

---

2 (a) Divisors of zero: In a ring R, a non-zero element a is said to be a divisor of zero if there exists a non-zero element $b \in R$ s.t. $a \cdot b = 0$, or a non-zero " $c \in R$ s.t. $c \cdot a = 0$.

$S = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in Q \right\}$.

Let $a, b \in Q$. And $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} = A \in S$, where $(a,b) \neq (0,0)$

Let $AB = 0$, where $B = \begin{pmatrix} p & q \\ 2q & p \end{pmatrix}$.

$ap + 2bq = 0$
$bp + aq = 0$
} Homogeneous system giving non-zero solns for p, q if $\begin{vmatrix} a & 2b \\ b & a \end{vmatrix} = 0 \Rightarrow a^2 - 2b^2 = 0$,

if $a, b \in Q$, then $a^2 - 2b^2 \neq 0$ for non-zero a, b.

But if $a, b \in R$, then $a^2 - 2b^2$ may be zero for non-zero a, b; say $a = \sqrt{2}, b = 1$,

$\therefore$ a non-zero matrix B exists s.t. $AB = 0$

$\therefore$ S contains divisor of zero if $a, b \in R$

S " no " " " if $a, b \in Q$.

2(b) Show that every field is an I.D. but the converse of the theorem is not necessarily true.

Let F be a field. Then F is a non-trivial commutative ring with unity and every non-zero element of F is a unit.

Let $a(\neq 0) \in F$. Then $\bar{a}^{-1} \in F$ and $a \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot a = 1$.

Let $a \cdot b = 0 \Rightarrow \bar{a}^{-1}(a \cdot b) = \bar{a}^{-1} \cdot 0 \Rightarrow (\bar{a}^{-1} \cdot a) b = 0$

$\Rightarrow 1 \cdot b = 0 \Rightarrow b = 0$

$\Rightarrow a$ is not a left divisor of zero

since F is commutative a is not a right divisor of zero also.

$\therefore$ F contains no divisor of zero. $\Rightarrow$ F is an I.D.

The converse is not True

eg. $(\mathbb{Z}, +, \cdot)$ is an I.D. but it is not a field as every non-zero element is not a unit.

(c) Every ideal of the ring $(\mathbb{Z}, +, \cdot)$ is a P.I.

~~$m\mathbb{Z}$ $(m \in \mathbb{Z}^+)$ are the~~ The subring $m\mathbb{Z}$ (m being a +ve integer) is an ideal of $(\mathbb{Z}, +, \cdot)$

We prove $m\mathbb{Z}$ is the smallest ideal of $\mathbb{Z}$ containing the element m. It is the ideal generated by m.

Let U be any ideal of $\mathbb{Z}$ containing m. Then $m \cdot a \in U$ for all $a \in \mathbb{Z}$, $\Rightarrow m\mathbb{Z} \subset U$.

$\Rightarrow m\mathbb{Z}$ is the smallest ideal.

$\therefore m\mathbb{Z}$ is a principal ideal of $\mathbb{Z}$.

Since all ideals in the ring $\mathbb{Z}$ are given by $m\mathbb{Z}$, it follows that every ideal of the ring $\mathbb{Z}$ is a P.I.

To prove: every subring of the $\mathbb{Z}$ is an ideal.

The subrings are $m\mathbb{Z}$, $m \geq 0$, a integer.

When $m = 0$, $m\mathbb{Z}$ is the null ideal $\{0\}$.

When m is a +ve integer. Let $S = m\mathbb{Z}$.

Let $p \in S$. Then $p = mu$ for some $u \in \mathbb{Z}$.

For an arbitrary $r \in \mathbb{Z}$, $pr = mur \in S$,

$\therefore p \in S, r \in \mathbb{Z} \Rightarrow pr \in S, rp \in S$.

$\therefore S$ is an ideal of $\mathbb{Z}$.

UG- CBCS Study Materials.

Semester - 4th

Subject - Mathematics (Hons.)

Paper - C10T

Unit-1 : RING THEORY.

Name of the Teacher:

Dr. Sangita Chakraborty

Deptt. of Mathematics

Kharagpur College.

Whatsup No.- 9434455417

Email: sangita_m_y2k@yahoo.com

If any concerned student has queries, he/she can contact me in the above number.