Unit - IV - Ring theory

Ring:- A non-empty set R satisfy abelian group under addition and closure, associative Property under multiplication and distributive laws under (+ and .) is called ring.

definition - Associative ring:-

A non empty set R is said to be an associative ring. if in R there are defined two operations, denoted by + and . respectively such that for all a, b, c in R.

(i) $a+b$ is in R (closure)

(ii) $a+b = b+a$ (Commutative)

(iii) $(a+b)+c = a+(b+c)$ (associative)

(iv) There is an element 0 in R such that $a+0 = a$ (for every a in R) (Identity)

(v) There exists an element $-a$ in R such that $a+(-a) = 0$ (Inverse)

(vi) $a.b$ is in R (Closure)

(vii) $a.(b.c) = (a.b).c$ (Associative)

(viii) $a.(b+c) = a.b + a.c$ & $(b+c).a = b.a + c.a$ (two distributive laws)

Non - associative:- A ring is said to be non-associative ring, When it does not satisfy the associative Property under multiplication.

Ring With Unit element:-

A ring R is said to be ring with Unit element when $1 \in R$ such that $a.1 = a = 1.a$ $\forall a \in R$.

Commutative ring:-

A ring which satisfies $\forall a, b \in R$ $a.b = b.a$ (ie) Commutative Property under multiplication is said to be Commutative ring.

Example: 3.1.1

R is the set of integers, positive, negative, and 0; + is the Usual addition and . the Usual multiplication of Integers.

Solution:-

* $\forall\ a,b \in R \Rightarrow a+b \in R$
* $\forall a,b,c \in R \Rightarrow a+(b+c) = (a+b)+c$
* $\exists\ 0 \in R,\ \forall a \in R \therefore a+0 = a = 0+a$
* $\forall\ a \in R,\ \exists\ a^{-1} \in R \therefore a+a^{-1} = 0 = a^{-1}+a$
* $\forall\ a,b \in R,\ a+b = b+a$
* $\forall\ a,b \in R,\ a.b \in R$
* $\forall\ a,b,c \in R,\ a.(b.c) = (a.b).c$
* $\forall\ a \in R,\ \exists\ 1 \in R \therefore a.1 = a = 1.a$
* $\forall\ a,b \in R,\ a.b = b.a$
* $\forall\ a,b, \in R,\ a.(b+c) = a.b+a.c$ &

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

Hence, the Set R is a Commutative ring along with the Unit element.

$\therefore$ R is a Commutative ring with Unit element.

Example: 3.1.2:-

R is the Set of even integers under the Usual operations of addition and multiplication.

Solution:-

* $\forall\ a,b \in R,\ a+b \in R$
* $\forall\ a,b,c \in R,\ a+(b+c) = (a+b)+c$
* $\forall\ a \in R,\ \exists\ 0 \in R \therefore a+0 = a = 0+a$.
* $\forall a \in R, \exists a^{-1} \in R \therefore a+a^{-1} = 0 = a^{-1}+a$
* $\forall\ a,b \in R,\ a+b = b+a$
* $\forall\ a,b \in R,\ a.b \in R$
* $\forall\ a,b,c \in R,\ a.(b.c) = (a.b).c$
* $\forall\ a,b \in R.\ a.b = b.a$

* $\forall a,b,c \in R \quad a.(b+c) = (a.b)+(a.c)$ &

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

Where Set R does not Contain the Unit element 1.

Hence, the Set R is a Commutative ring with no Unit element.

$\therefore$ R is a Commutative ring with no Unit element.

Example 3.1.3 :- R is the set of rational numbers under the usual addition and Multiplication of rational numbers.

Solution:-

* $\forall \ a,b \in R, \ a+b \in R$
* $\forall \ a,b,c \in R \quad a+(b+c) = (a+b)+c$
* $\forall \ a \in R, \exists \ 0 \in R \ \ni \ a+0 = a = 0+a$
* $\forall \ a \in R, \exists \ a^{-1} \in R \ \ni \ a+a^{-1} = 0 = a^{-1}+a$
* $\forall \ a,b \in R, \ a+b = b+a$
* $\forall \ a,b \in R \ , \ a.b \in R$
* $\forall \ a,b,c, \in R \ , \ a.(b.c) = (a.b).c$
* $\forall \ a,b,c \in R \ , \ a.(b+c) = (a.b)+(a.c)$

$\forall \ a,b,c \in R \quad (b+c).a = (b.a)+(c.a)$

* $\forall a \in R, \ \exists \ 1 \in R \ \ni \ a.1 = a = 1.a$
* $\forall a \in R, \ \exists \ a^{-1} \in R \ \ni \ a.a^{-1} = 1 = a^{-1}.a$
* $\forall \ a,b \in R \quad a.b = b.a$

Where R is a Commutative ring with Unit element.

Note that the set R satisfies abelian group under both addition & Multiplication Hence, R is a field.

Example 3.1.4 :- R is the set of Integers mod 7 under the addition and Multiplication mod 7. that is the elements of R are Seven Symbols. $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$.

Solution:-

* $\forall a,b \in R.\ a+b \in R.$ [eg: $\bar{4}+\bar{5}=\bar{2}$) $\Rightarrow$ 4+5=9
9-7=2

* $\forall a,b,c \in R\ \ a+(b+c)=(a+b)+c$

* $\forall a \in R,\ \exists\ 0 \in R \ \because\ a+0=a=0+a$

* $\forall a \in R,\ \exists\ \bar{a}^{1} \in R \ \because\ a+\bar{a}^{1}=0=\bar{a}^{1}+a$ $[\bar{2}+\bar{5}=\bar{7}+\bar{6}=\bar{3}+\bar{4}=\bar{0}]$

* $\forall a,b \in R,\ a+b=b+a$

* $\forall a,b,\in R,\ a.b \in R$ $[eg: \bar{4}.\bar{3}=\bar{5}.] \Rightarrow 4.3=12/7=5$

* $\forall a,b,c \in R.\ \ a.(b.c)=(a.b).c$

* $\forall a \in R,\ \exists\ 1 \in R \ \because\ a.1=a=1.a$

* $\forall a \in R,\ \exists\ \bar{a}^{1} \in R \ \because\ a.a^{-1}=1=\bar{a}^{1}.a$

$[\bar{2}.\bar{4}=\bar{5}.\bar{3}=\bar{7}.\bar{7}=\bar{6}.\bar{6}=\bar{1}]$

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

* $\forall a,b,c \in R,\ \ a.(b+c)=a.b+a.c$ and

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

$$eg:\begin{bmatrix} \bar{2}.(\bar{4}+\bar{5})=\bar{2}.\bar{2}=\bar{4} \\ \bar{2}.\bar{4}+\bar{2}.\bar{5}=\bar{1}+\bar{3}=\bar{4} \end{bmatrix}$$

Hence R is a Commutative ring.

With unit element. Note that R satisfies abelian group under addition and multiplication, Hence R is a field where the number of elements in R is finite,

$\therefore$ R is a finite field.

Example 3.15 R is the set of integers mod 6 under addelition and Multiplication mod 6. if we donote the elements in R. by $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$

$\bar{2}.\bar{3}=\bar{0}$, yet $\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$. Thus it is Possible in a ring R. $a.b=0$, With neither $a=0$ nor $b=0$.

this R is Commutative ring.

Example 3.16 R will be the set of all symbols.

$$\alpha_{11}e_{11} + \alpha_{12}e_{12} + \alpha_{21}e_{21} + \alpha_{22}e_{22} = \sum_{i,j=1}^{2} \alpha_{ij}e_{ij}$$

Where all the α_{ij} are rational numbers

$$\sum_{i,j=1}^{2} \alpha_{ij}e_{ij} = \sum_{ij=1}^{2} \beta_{ij}e_{ij}$$

if and only if for all $i, j = 1, 2$ $\alpha_{ij} = \beta_{ij}$

$$\sum_{i,j=1}^{2} a_{ij}e_{ij} + \sum_{i,j=1}^{2} \beta_{ij}e_{ij} = \sum_{i,j=1}^{2} (\alpha_{ij} + \beta_{ij})e_{ij}$$

$$\left(\sum_{i,j=1}^{2} \alpha_{ij}e_{ij}\right) \cdot \left(\sum_{i,j=1}^{2} \beta_{ij}e_{ij}\right) = \sum_{i,j=1}^{2} \gamma_{ij}e_{ij}$$

$$\gamma_{ij} = \sum_{v=1}^{2} \alpha_{iv}\beta_{vj} = \alpha_{i1}\beta_{1j} + \alpha_{i2}\beta_{2j}$$

$$e_{ij} \cdot e_{kl} = 0 \quad \text{for } j \neq k$$

$$e_{ij} \cdot e_{jl} = e_{il}$$

if $a = e_{11} - e_{21} + e_{22}$ $\quad b = e_{22} + 3e_{12}$

$$a \cdot b = (e_{11} - e_{21} + e_{22}) \cdot (e_{22} + 3e_{12})$$

$$= e_{11} \cdot e_{22} + 3(e_{11} \cdot e_{12}) - e_{21} \cdot e_{22} - 3(e_{21} \cdot e_{12}) + e_{22} \cdot e_{22} + 3(e_{22} \cdot e_{12})$$

$$= 0 + 3e_{12} - 0 - 3e_{22} + 1e_{22} + 0$$

$$= 3e_{12} - 2e_{22}$$

$$e_{11} \cdot e_{12} = e_{12} \qquad e_{12} \cdot e_{11} = 0$$

$a \cdot b \neq b \cdot a$. $e_{11} \cdot e_{12} \neq e_{12} \cdot e_{11}$

R is not classified Commutative

$\therefore$ R is non commutative ring

Some Special Classes of rings:-

Definition - Zero-divisor:-

if R is a Commutative ring, then $a \neq 0, \in R$ said to be a Zero divisor if there exists $a, b \in R, b \neq 0$ Such that $ab = 0$.

Integral domain:- A Commutative ring is an integral domain if it has no Zero-divisors.

The ring of integers is an example of an integral domain

division ring:- A ring is said to be a division ring if its non-Zero elements form a group under multiplication

Field:-

* A field is a Commutative division ring
* A ring which forms abelian group under multiplication is called field.

Lemma: 3.2.1:-

if R is a ring, then for all $a, b \in R$.

1) $a0 = 0a = 0$
2) $a(-b) = (-a)(b) = -(ab)$
3) $(-a)(-b) = ab$

if in addition, R has a Unit element, then

4) $(-1)a = -a$
5) $(-1)(-1) = 1$

Proof:- Given R is a ring and $\forall a, b \in R$

1) $a.0 = 0.a = 0$

We Know that $a \in R$.

$a0 = a(0+0) = a0 + a0 = 0 + 0 \rightarrow (1)$ (Right distributive Law)

$0a = (0+0)a = 0a + 0a = 0 + 0 = 0 \rightarrow (2)$ (Left distributive Law)

From ① & ② We get $a0 = 0a = 0$

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

We Know that $a + (-a) = 0$

$\therefore ab + (-ab) = 0 \rightarrow ③$

It is enough to Prove $ab + a(-b) = 0$

$\therefore a[b + (-b)] = a(0) = 0 \quad (\because a0 = 0) \rightarrow ④$

Why $ab + (-a)b = [a + (-a)]b$

$= 0(b) = 0 \rightarrow ⑤) \quad (\because 0a = 0)$

From ③, ④, ⑤ We get,

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

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

We Know that $a(-b) = -ab$

$(-a)(-b) = -[a(-b)]$

$= -[-ab]$

$\therefore (-a)(-b) = ab$ Hence Proved

4) $(-1)a = -a$

$1 \in R$, then $(-1)a = -a \quad [\because (-a)b = -ab]$

Hence Proved.

5) $(-1)(-1) = 1$

We Know that $(-a)(-b) = ab$

Let $a = 1, b = 1$

Thus, $(-1)(-1) = (1)(1) = 1$

Hence, $(-1)(-1) = 1$. Hence Proved.

The Pigeonhole Principle:-

If "n objects are distributed over m places, and if $n > m$, then Some place receives at least two objects.

Lemma: 3.2.2:- A finite Integral domain is a field.

~~Solution~~: Proof:-

Let D be a finite integral domain.

We have to Prove that. D is a field.

(ie) Enought to Prove that.

(i) Exist an element $1 \in D$ Such that $a.1 = 1.a = a$. $\forall a \in D$

(ii) For every element $a \neq 0 \in D$. exist an element $b \in D$ such that $ab = 1$

Let $x_1, x_2, x_3 \cdots x_n$ be the element to $\S$ D and

Let $a \neq 0 \in D$

Since D is Commutative and finite.

$\therefore a x_1, a x_2, a x_3, \cdots\cdots a x_n \in D$

We have to claim that $ax_1, ax_2, \cdots ax_n$ are all distinct elements Suppose, $ax_i = ax_j$ for $i \neq j$

$$ax_i - ax_j = 0$$

$$a(x_i - x_j) = 0$$

Since $a \neq 0$, $\therefore x_i - x_j = 0$

$$x_i = x_j, \text{ for } i \neq j$$

Which is a Contradiction

$\therefore ax_1, ax_2, ax_3 \cdots ax_n$ all are distinct elements.

$\therefore D$ has exactly n elements

Then for every $y \in D$ Can be Written as.

$y = ax_i$ for Some $x_i \in D$.

Since $a \in D$, and D is Commutative.

$$\therefore a = a x_{i_0} = x_{i_0} a$$

$\Rightarrow x_{i_0}$ act as a Unit element for every element $\S$ D.

Where $y \in D$. $y = ax_i$ for Some $x_i \in D$

Now, $x_{i0}\, y = x_{i0}(ax_i)$

$= (x_{i0}\, a)\, x_i \quad (\because y = ax_i)$

$= (a\, x_{i0})\, x_i$

$x_{i0}\, y = a x_{i0} = y$

Thus x_{i0} is a Unit element of D.

$\therefore x_{i0} = 1 \in D$ is a Unit element. Now $1 \in D$,

$\therefore$ There exist $a, b \in D$.

Such that $1 = ab$

Hence D is a field.

Corollary: if p is a Prime number then J_p, the ring of Integers mod p, is a field.

Proof:- Given p is a Prime number.

W.K.T "every finite Integral domain is a field"

Since J_p, the ring of Integers mod p is finite.

(ie) enough to Prove that J_p is an integral domain.

Let $a, b \in J_p$

We have to claim that J_p has no Zero divisors.

if $a, b \in J_p$ and $ab \equiv 0$

$\Rightarrow$ p must divide ab (ie) $\frac{ab}{p}$

Since p is a Prime number,

We get $\frac{a}{p}$ (or) $\frac{b}{p}$

(ie) either $a \equiv 0 \pmod p$ (or) $b \equiv 0 \bmod p$

$\rightarrow$ either $a \equiv 0$ (or) $b \equiv 0$

$\therefore J_p$ has no Zero divisor.

$\therefore J_p$ is an Integral domain

By Using ① We get.

J_p is field //

Definition:- Characteristic "0" :-

An integral domain D is said to be of "characteristic 0" if the relation $ma = 0$ where $a \neq 0$, is in D, and where 'm' is an Integer. if $m = 0$.

finite Characteristic :-

An Integral domain D is said to be of finite characteristic if there exists a positive integer "m" such that $ma = 0$ for all $a \in D$.

3.3. Homomorphisms

Definition A mapping ϕ from the ring R into the ring R' is said to be a homomorphism if,

1. $\phi(a+b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.

Lemma: 3.3.1 if ϕ is a homomorphism of R into R' then

1. $\phi(0) = 0$. 2. $\phi(-a) = -\phi(a)$ for every $a \in R$.

(i) Consider $\phi(a) = \phi(a+0)$ → *

$\phi(a+0) = \phi(a) + \phi(0)$ [$\because \phi$ is homomorphism]

~~$\phi(0) = 0$~~ [by Using left cancellation Law]

$\phi(a) = \phi(a) + \phi(0)$ →

$\boxed{0 = \phi(0)}$

(ii) Consider $\phi(0) = \phi[(a) + (-a)]$ → *

$\phi[(a) + (-a)] = \phi(a) + \phi(-a)$ [ϕ is homomorphism]

~~$\phi[(a) + (-a)] =$~~

$\phi(0) = \phi(a) + \phi(-a)$.

$\boxed{\phi(0) = 0}$

$0 = \phi(a) + \phi(-a)$.

$\phi(a) = 0$.

Definition:- Kernel of ϕ:-

if ϕ is a homomorphism of R into R' then the Kernel of ϕ, $I(\phi)$. is the set of all elements $a \in R$ such that $\phi(a) = 0$. the Zero element of R'

$$K\phi = \{a \in R / \phi(a) = 0\}.$$

isomorphism:- A homomorphism of R into R' is said to be an isomorphism if it is a one to one mapping.

isomorphic:- Two rings are said to be isomorphic if there is an isomorphism of one onto the other.

3.4. ideals and Quotient Rings:-

Definition:- ideal of R:-

A Non empty subset U of R is said to be a ideal of R. if (i) U is a Subgroup of R Under Addition.

(ii) For every $u \in U$ and $r \in R$. both ur and ru are in

Lemma: 3.4.1 if U is an ideal of the ring R, then R/U, is a ring. and is a homomorphic image of R

Proof: Given U is an ideal of the ring R.

Let R/U be the set of all distinct Coset of U in R.

Since U is an ideal of R,

U is a Subgroup of R Under addition.

Let $R/U = \{a+U / a \in R\}$

Where we have to Prove, R/U is a ring.

R/U defines addition, and Multiplication as

$$(a+U) + (b+U) = (a+b) + U$$

$$(a+U)(b+U) = (ab) + U \quad \forall\ a+U, b+U \in R/U$$

We have to claim "+" is well defined.

Suppose, $a+U = a'+U$ and $b+U = b'+U$

$a-a' \in U$ and $b-b' \in U$

$a-a' \in U_1$ and $b-b' = U_2$

$a = a'+U_1$ & $b = b'+U_2$

(ie) $(a+U)+(b+U) = [(a'+U_1)+U] + [(b'+U_2)+U]$

$= [(a'+U)+U] + [(b'+U)+U]$

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

∴ We get "+" is well defined.

Now, we claim Multiplication is well defined.

$a+U = a'+U$, $b+U = b'+U$

$a-a' \in U$ $b-b' \in U$

$a = a'+U_1$ $b = b'+U_2$

Now $(a'+U_1)(b'+U_2) = [a'b'+a'U_2+b'U_1+U_1U_2]$

Now, $ab+U = a'b'+U$

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

∴ Multiplication is well defined.

We have to claim R/U is an abelian group under the operation addition and closure, associative, under "." and distributive Law.

(i) Closure Property under "+"

$a+U, b+U \in R/U$

Where $(a+U)+(b+U) = (a+b)+U \in R/U$

∴ Closure Property is ture under "+"

(ii) Associative under "+"

$$(a+U)+[(b+U)+(c+U)] = (a+U)+[(b+c)+U]$$
$$= [a+(b+c)]+U$$
$$= [(a+b)+c]+U$$
$$\therefore (a+U)+[(b+U)+(c+U)] = [(a+U)+(b+U)]+(c+U)$$

(iii) Commutative under "+"

$$(a+U)+(b+U) = (a+b)+U$$
$$= (b+a)+U$$
$$\therefore (a+U)+(b+U) = (b+U)+(a+U)$$

Hence, Commutative is true.

(iv) Identity under "+"

Let $U = a+U \in R/U$

if $a+U \in R/U$

$\Rightarrow (0+U)+(a+U) = (0+a)+U$ | $(a+U)+(0+U) = (a+0)+$
$= a+U$ | $= a+U$

$\Rightarrow (a+U)+(0+U) = (0+U)+(a+U)$

$= a+U$

$\therefore$ Identity is true.

~~$\therefore (a+U)+(0+U) = (0+U)+(a+U)$~~

(v) Inverse under "+"

Let $a+U \in R/U$

then, $[(-a)+U]+(a+U) = [(-a)+a]+U$

$= 0+U$

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

$= 0+U$

$\therefore [(-a)+U]+(a+U) = (a+U)+[(-a)+U] = 0+U$

Inverse is ture.

(vi) Closure under "·"

$a+U,\ b+U \in R/U$

Where $(a+U)\cdot(b+U) = (ab)+U \in R/U$

$\therefore$ closure is true under "·"

(vii) Associative under "·"

$$(a+U)\cdot[(b+U)(c+U)] = a+U[(b\cdot c)+U]$$
$$= [a(bc)]+U$$
$$= [(ab)+c]+U$$
$$= (ab+U)\cdot(c+U)$$

$\therefore (a+U)[(b+U)(c+U)] = [(a+U)(b+U)](c+U)$

(viii) Distributive Law:-

$$(a+U)[(b+U)+(c+U)] = (a+U)[(b+c)+U]$$
$$= [a(b+c)]+U$$
$$= [ab+ac]+U$$
$$= [ab+U]+[ac+U]$$

$\therefore (a+U)[(b+U)+(c+U)] = (a+U)(b+U)+(a+U)(c+U)$

$\therefore$ Distributive Law is true.

Hence, R/U is a ring.

Note, We have to Prove

R/U is a homomorphic image of R.

Let $\phi: R \to R/U$ defined by $\phi(a) = a+U$.

claim that ϕ is onto,

Let $a+U \in R/U$ Where $a \in R$.

$\therefore$ For every element $a+U \in R/U$, there exist an element

$a \in R$. such that

$$\phi(a) = a + U$$

$\therefore \phi$ is onto.

Now claim ϕ is homomorphism.

(ie) to Prove.

(i) $\phi(a+b) = \phi(a) + \phi(b)$.

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

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

$$= (U+a) + (U+b)$$

$$= \phi(a) + \phi(b)$$

$\therefore \phi(a+b) = \phi(a) + \phi(b)$.

$$\phi(ab) = (ab) + U$$

$$= (a+U)(b+U)$$

$$\phi(ab) = \phi(a)\,\phi(b)$$

$\therefore \phi$ is homomorphism.

We get R/U is a homomorphic image of R.

Hence Proved.

3.5 More ideals and Quotient Rings:-

Maximal ideal:-

An ideal $M \neq R$ in a ring R is said to be Maximal ideal of R. if Whenever U is an ideal of R. such that $M \subset U \subset R$, then either $R = U$. (or) $M = U$.

Lemma: 3.5.1 Let R be a Commutative ring Which Unit element Whose only ideals are (0) and R itself. Then. R is a field.

Proof:- Given, R is a Commutative ring. With Unit element and, Ideal (0) and R are Ideals of R.

We have to Prove, R is a field.

We Know that,

"A finite Integral domain is a field, A Commutative division ring is field".

Enough to Prove that every NON-Zero element in R has a multiplicative inverse in R.

(ie) to Prove,

for any $a \neq 0 \in R$, there exists an element $b \neq 0 \in R$ Such that $a.b = 1$

Consider the set $Ra = \{xa \mid x \in R\}$ are have to claim that

Ra is non-empty.

Since $0 \in R$, We get,

$0 = 0a \in Ra$.

$\therefore$ Ra is non-empty.

Now, claim that Ra is an Subgroup of R.

Under addition,

$$Ra = \{xa \mid x \in R\}$$

Let $u \in Ra$ and $r \in R$.

then $ru \in Ra$.

if $u, v \in Ra$ then $u = r_1 a$, $v = r_2 a$ for Some $r_1, r_2 \in R$.

$$u+v = r_1 a + r_2 a = (r_1 + r_2)a \in Ra$$

$\therefore$ Ra is an Subgroup of R under addition

Where $ru = ur$

$\therefore$ Ra is an ideal of R.

Given the only ideals of R are ideal (0) and R

$\therefore$ We get Ra = ideal (0) (or)

$$Ra = R$$

$\therefore$ Ra $\neq$ ideal (0) [Since Ra is non-empty]

$\therefore$ Ra = R

In particular $1 \in R$.

for $a \neq 0 \in R$. there exist $b \neq 0 \in R$. Such that

$$1 = ba$$

Since R is a Commutative ring.

$\therefore$ $ab = ba = 1$

$\Rightarrow$ every non-zero element in R has multiplicative inver

$\therefore$ We get R is a field.

Hence Proved.

Theorem : 3.5.1 If R is a Commutative ring with Unit elem and M is an ideal of R then M is maximal ideal of R if and only if R/M is a field.

Proof:- Given R is a Commutative ring with Unit element and. M is an ideal of R.

TO Prove. M is an maximal ideal of R.

assume that R/M is a field.

Since R/M is a field its only ideals are ideal (0) and itself.

By the theorem,

"There is a one to one Corresponding between the Set of ideals of R/M and the Set of ideals of R which Contain M"

We get, The ideal R of R Corresponds to the ideal (0) of R/M Whose as. the ideal R of R Corresponds to the ideal R/M of R/M in this one-to-one mapping.

Thus, there is no ideal between M and R.

∴. M is a maximal ideal of R.

Conversely,

Assume that M is a maximal ideal of R

To Prove, R/M is a field.

Enough to Prove that R/M has no Proper ideals.

Since M is a maximal ideal of R

∴. The only ideals of R/M are ideal (0) and R/M.

(ie) R/M has no Proper ideals

Since R is a Commutative Ring With Unit element.

By the theorem.

"Let R be a Commutative Ring With Unit element Whose only ideals R itself, then R is a field."

We get. R/M is a field.

Example: 3.5.1

Let R be the ring of integes and U be an ideal of R. then Prime number is maximal ideal of R.

Proof:- Given R is a ring of Integers and U be an ideal of R.

P is a Prime number, then $P = (p)$ is maximal ideal of R if U is an ideal of R and $U \supset P$ then $U(n_0)$ for some integer n_0.

Since $P \subset P \subset U$, $p = mn_0$ for some integer m.

p is a Prime number

$\Rightarrow n_0 = 1$ (or) $n_0 = p$

then $1 \in U$. Hence $r.1 = r \in U$ for all $r \in R$ When $U = R$ follows.

Thus n_0 is ideal other than R (or) p itself.

$\therefore$ P is maximal ideal.

On the other hand,

$M = (n_0)$ is a maximal ideal of R We have to claim that n_0 must be a Prime number.

for if $n_0 = ab$ Where a, b are positive Integers.

then $U = [a] \supset M$. Hence $U = R$ (or) $U = M$.

if $U = R$ then $a = 1$.

if $U = M$, then $a \in M$ and So $a = rn_0$ for Some Integer r.

Since every element of M is a multiple of n_0.

But then $n_0 = ab = rn_0 b$.

From Which We get $rb = 1$

$\therefore b = 1$ and $a = n_0$

Thus n_0 is a Prime number //.

Example: 3.5.2:- Let R be the ring of all the real-Valued Continuous functions on the closed Unit interval.

Solution:- [closed Interval $= [0, 1]$

Let $M = \{ f(x) \in R \mid f(1/2) = 0 \}$

f is certainly an ideal of R. Moreover, it is a maximal ideal of R, for if the ideal U contains M and $U \neq M$, then there is a function $g(x) \in U$, $h(x) \notin M$, Since $g(x) \notin M$. $g(1/2) = \alpha$

Now, $h(x) = g(x) - \alpha$ is such that $h(1/2) = g(1/2) - \alpha = 0$

So that $h(x) \in M \subset U$. But $g(x)$ is also in U.

$\therefore \alpha = g(x) - h(x) \in U$.

$1 = \alpha\alpha^{-1} \in U$.

$t(x) \in R$.

$t(x) = 1\, t(x) \in U$.

in Consequence of Which $U = R$.

* M is therefore a maximal ideal of R.

Ully if γ is a real Number $0 \leq \gamma \leq 1$.

then, $M\gamma = \{ f(x) \in R \mid f(\gamma) = 0 \}$ is a maximal ideal of R. [It can be shown that every maximal ideal is of this form]. Thus here the maximal ideals Correspond to the Points on the Unit Interval.

Unit - V

3.6 The Field of Quotients of an integral domain:-

[Corollary]

Lemma: 3.3.3 The homomorphism ϕ of R into R' is an isomorphism if and only if $I(\phi) = (0)$

Proof:- Given $\phi : R \to R'$ is a homomorphism with Kernel $K\phi$.

Assume that ϕ is an isomorphism.

We have to Prove $I(\phi) = 0$

$\left[I(\phi) = \{a \in R \mid \phi(a) = 0\} \right]$

Let $x \in I(\phi)$

$\phi(x) = 0$

Since ϕ is an homomorphism.

$\phi(e) = 0$.

We get $\phi(x) = 0 = \phi(e)$

Thus $\phi(x) = \phi(e)$.

Since ϕ is an isomorphism We get ϕ is one to one.

$\therefore \phi(x) = \phi(e) \Rightarrow x = e$.

$\therefore$ We get $I(\phi) = 0$.

Conversely. Assume that $I(\phi) = (0)$

We have to Prove ϕ is an isomorphism

(ie) to Prove ϕ is homomorphism,

ϕ is one to one.

Given ϕ is homomorphism,

We have to claim ϕ is one to one.

Let $x, y \in G$.

We have to Prove, $\phi(x) = \phi(y) \Rightarrow x = y$.

$\phi(x) = \phi(y)$

$\phi(x) - \phi(y) = 0$

$\phi(x-y) = 0$ $\quad (x-y) \in I(\phi)$

$$x - y = I(\phi) = 0$$

$$x - y = 0$$

$$x = y$$

$\therefore \phi(x) = \phi(y) \Rightarrow x = y$

Thus, We get ϕ is one to one and, ϕ is isomorphism.

Hence, $\phi : R \to R'$ is an isomorphism of R into R' if and only if $I(\phi) = 0$

Hence Proved.

Lemma: 3.3.2 If ϕ is a homomorphism of R into R' with Kernel $I(\phi)$, then 1. $I(\phi)$ is a subgroup of R Under addition.

2. if $a \in I(\phi)$ and $r \in R$. then both ar and ra are in $I(\phi)$.

Proof: (i) Given, ϕ is a homomorphism of R into R'

$I(\phi)$ is a Kernel of ϕ.

To Prove, $I(\phi)$ is Subgroup of R.

Let $I(\phi) = \{ x \in R / \phi(x) = \bar{0} \}$ Where $\bar{0}$ is identity element of R'

We have to claim, $I(\phi)$ is non empty.

Since We have $\phi(0) = \bar{0}$

We get $0 \in I(\phi)$.

Hence $I(\phi)$ is non empty.

We have to claim: $I(\phi)$ is a Subgroup of R

Let $x, y \in I(\phi)$

$\neq 0$. , is well def :. ,

$$\phi(x) = \overline{0}, \quad \phi(y) = \overline{0}$$

Where $\overline{0}$ is identity element of R'

$$\phi(x+y) = \phi(x) + \phi(y)$$
$$= \overline{0} + \overline{0}$$
$$= \overline{0} \quad [\phi \text{ is a homomorphism}]$$

$$\phi(x+y) = \overline{0}$$
$$x+y \in I(\phi)$$

We Know that. $\phi(-x) = -\phi(x)$.

if $x \in I(\phi)$ $\phi(x) = \overline{0}$

$\phi(-x) = -(\overline{0}) = \overline{0}$, $x^{-1} \in I(\phi)$

[We Know that,
A non empty subset H of the group G is a subgroup of G, if and only if
(i) $a, b \in H \Rightarrow ab \in H$
(ii) $\bar{a} \in H \Rightarrow \bar{a}^{-1} \in H$.]

$\therefore$ $I(\phi)$ is a subgroup of R.

(ii) $a \in I(\phi)$, $r \in R$.

then $\phi(a) = 0$.

So that, $\phi(ar) = \phi(a) \cdot \phi(r)$
$= 0 \cdot \phi(r)$

$\phi(ar) = 0$. [$\{I(\phi) = a \in R / \phi(a) = 0\}$]

$\phi(ar) = \phi(ra) = 0$.

$\therefore$ $ar, ra \in I(\phi)$,

Example: 3.3.1

Let R and R' be two arbitary rings and define $\phi(a) = 0$ for all $a \in R$. Trivially ϕ is a homomorphism. and $I(\phi) = R$, ϕ is ca the Zero - homomorphism.

Example: 3.3.2 Let R be a ring $R' = R$ and define $\phi(x) = x$ for every $x \in R$. clearly ϕ is a homomorphism and $I(\phi)$ Consists only $\{0\}$.