Rings And Modules

Groupoid:- A non-empty set closed under some binary operation is called a groupoid.

For example.

$(\mathbb{Z}, +)$ is a groupoid

$(\mathbb{Z}, \cdot)$ is " "

$\mathbb{Z}$ is not groupoid under division

$\div$ is not a b.o in $\mathbb{Z}$.

Semi group:- A non-empty set closed under some association b.o is called a semi group e.g.

$(\mathbb{Z}, +)$ is a semi-group.

$(\mathbb{Z}, \cdot)$ " " "

$(\mathbb{Z}, -)$ is not a semi group

$\because$ $-$ is not association

$(a-b)-c \neq a-(b-c)$

Group:- A non-empty set G is said to be group if it satisfies the following four axioms

1) G is closed under some b.o $*$.

or G satisfies closure Property,

2) $*$ is association in G

3) G satisfies identity law.
4) G satisfies Inverse law.

Sub-group:- Let G be a group and H be a non-empty subset of G. Then H is a sub-group of G if H is itself a group under the b-O defined in G.

NOTE A non-empty subset H of a group G is a sub-group of G iff

$$ab^{-1} \in H \quad \forall a, b \in H$$

NOTE H is a sub-group of a group $(G, +)$ iff

$$a - b \in H \quad \forall a, b \in H.$$

$(\mathbb{Z}, +)$ is a group
$(\mathbb{Q}, +)$ " "
$(\mathbb{R}, +)$ " "

$(\mathbb{C}, +)$ " "
$(2\mathbb{Z}, +)$ " "
$(3\mathbb{Z}, +)$ " "

$(n\mathbb{Z}, +)$ " "

Ring:- A non-empty set R is said to be ring if it satisfies the following axioms

1) $(R, +)$ is an abelian group
2) $(R - \{0\}, \cdot)$ is a semi-group

i.e the set of non-zero elements of R form a semi group.

3) Left and Right distributive laws hold in R.

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

$(b+c)a = ba + ca$

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all are Rings.

Field:- A non-empty set F is said to be field if it satisfies the following axioms.

1) $(F, +)$ is an abelian group.
2) $(F - \{0\}, \cdot)$ is an abelian group.
3) $a(b+c) = ab + ac$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields But $\mathbb{Z}$ is not a field.

Vector Space :-

Let F be any field and V be a non-empty set in which an operation of addition is defined and for all $a \in F$ & $v \in V$

$av \in V$

Then V is called a vector space over F if it satisfies following axiom.

1) $(V, +)$ is an abelian group.

2) $a(v_1 + v_2) = av_1 + av_2 \quad \forall a \in F$, $v_1, v_2 \in V$

3) $(a+b)v = av + bv \quad \forall a, b \in F$, $v \in V$

4) $a(bv) = ab(v) = (ab)v \quad \forall a, b \in F$, $v \in V$

5) $1(v) = v. \quad \forall v \in V$

Examples.- $\mathbb{R}$ is a vector space over $\mathbb{R}$.

$\mathbb{R}^2$ is a V. Space over $\mathbb{R}$ where

$\mathbb{R}^2 = \{(a, b) : a, b \in \mathbb{R}\}$

(i.e. the set of all ordered pair of real no.)

$\mathbb{R}^3 = \{(a,b,c) : a,b,c \in \mathbb{R}\}$
is a vector space over $\mathbb{R}$

$\mathbb{R}^4 = \{(a,b,c,d) : a,b,c,d \in \mathbb{R}\}$
is a vector space over $\mathbb{R}$

$\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{R}\}$

i.e The set of all order n-tuples of real numbers is vector-space over $\mathbb{R}$.

All the above sets are vector spaces under ordinary addition and scalar multiplication.

i.e.

$$(a,b) + (c,d) = (a+c, b+d)$$
$$n(a,b) = (na, nb).$$

$W_1 = \{(x,y,0) : x,y \in \mathbb{R}\}$

$W_2 = \{(0,y,z) : y,z \in \mathbb{R}\}$

$W_3 = \{(x,0,z) : x,z \in \mathbb{R}\}$

$W_4 = \{(x,0,0) : x \in \mathbb{R}\}$

$W_5 = \{(0,y,0) : y \in \mathbb{R}\}$

$W_6 = \{(0,0,z)^T : z \in \mathbb{R}\}$

are all vector spaces

$\frac{x}{1} = \frac{y}{2} = \frac{z}{3} = t$ is equation of line

where (1, 2, 3) are directors ratios

$x = t$

$y = 2t$

$z = 3t$

$W = \{(t, 2t, 3t) : t \in \mathbb{R}\}$

is also a Vector-space.

Module :-

The Concept of module is the generalization of a vector space over a field F.

Def:- A non-empty set M is said to be a left module over a ring R. (or a left R-module) if it is an abelian group under addition and for every $r \in R$ and $m \in M$. There exist a unique element $rm \in M$. Subject to the following conditions

1) $r(a+b) = ra + rb \quad \forall r \in R$, $a, b \in M$

2) $(r+s)a = ra + sa \quad \forall r, s \in R$, $a \in M$

3) $r(sa) = (rs)a \quad \forall r, s \in R$
$a \in M$

Unital R Module.

if R is ring with unity Then a module M over R is said to be unital if $1 \cdot m = m \quad \forall m \in M$
$1 \in R$

Examples:-

2) every ring R is a left R-module.
OR (every ring R is a module over itself).

22) every vector space V over a field F is a module over R.

111) if R is a ring Then $R[x]$ i.e the Ring of all polynomials of x of degree n. over R is a module.

Sub-module:-

Let M be a left module over a ring R and S be a non-empty subset of M.
Then S is said to be submodule of M if it is itself a module over R.

grp

Theorem:- Let M be a module over a ring R and S be a non-empty subset of M. Then S is a sub-module over R iff

i) $a-b \in S \quad \forall a, b \in S$

ii) $rm \in S \quad \forall r \in R$, $m \in S$

Proof:- Let S be a non-empty subset of a module M over R in which

i) $a-b \in S \quad \forall a, b \in S$

ii) $rm \in S \quad m \in S$

now we shall prove that S is a submodule of M.

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

$\Rightarrow S$ is a subgroup of M under addition

Since M is abelian

$\therefore$ its subset S is also abelian

$\therefore S$ is an abelian group under addition.

The other axioms of a module are satisfied in S. because they are satisfied in its superset M.

$\therefore S$ is a module over R

Hence S is submodule of M over R.

Conversely:- Suppose S is a submodule of M over R then S itself is module. Then obviously the two conditions hold in S. i.e

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

& $rm \in S$ $\forall r \in R$

$, m \in S.$

Theorem:- The intersection of two submodules of a module M over R is also a submodule of M over R.

Proof:- Let M is module over a ring R, and let A and B are two submodules of M. we shall prove that $A \cap B$ is also a submodule of M.

For this

Let $a, b \in A \cap B$

$\Rightarrow a, b \in A$ and $a, b \in B$

$\Rightarrow a-b \in A$ and $a-b \in B$

because A and B are submodules of M over R.

$\Rightarrow a-b \in A \cap B$

Again $r \in R$ and $m \in A \cap B$

$\Rightarrow m \in A$ & $m \in B$

$\Rightarrow rm \in A \quad \& \quad rm \in B$
because A and B are submodules
$\Rightarrow rm \in A \cap B$
Hence $A \cap B$ is a submodule of M over R.

Theorem:— Any finite ~~Collection~~ Intersection of submodules of a module M over R is also a submodule of M.

Proof:— Let S_i ; $i = 1, 2, 3, \ldots$ — n be a finite collection of submodule of a module M over R, we shall Prove that $\bigcap_{i=1}^{n} S_i$ is also a submodule of M.

For this let $a, b \in \bigcap_{i=1}^{n} S_i$

$\Rightarrow a, b \in S_i$ for each $i = 1, 2, \ldots, n$

$\Rightarrow a - b \in S_i$ for each $i = 1, 2, \ldots, n$

because each S_i is a submodule of M

$\therefore a - b \in \bigcap_{i=1}^{n} S_i$

$\therefore$ First Condition of submodule is Satisfied

Again $r \in R$ and $m \in \bigcap_{i=1}^{n} S_i$

$\Rightarrow m \in S_i$ for each $i = 1, 2, \ldots, n$

$\Rightarrow rm \in S_i$ for each $i = 1, 2, \ldots, n$

$\therefore$ each S_i is submodule of M

$\Rightarrow \sum_{i=1}^{n} a_i \in \bigcap_{i=1}^{n} S_i$

$\therefore$ Second Condition of Submodule also satisfied.

Hence $\bigcap_{i=1}^{n} S_i$ is a Submodule of M

Sum of Two Submodules

Let A and B are Submodules of a module M over R.

Sum of A and B is denoted by A+B and is defined as

$$A+B = \{a+b : a \in A \& b \in B\}$$

Theorem:- If A and B are two Submodules of a module M over R Then the Sum A+B is also a Submodule of M Containing both A and B.

Proof:- Let $x, y \in A+B$

where $x = a_1 + b_1$ where $a_1, a_2 \in A$

$y = a_2 + b_2$ where $b_1, b_2 \in B$

$x - y = (a_1 + b_1) - (a_2 + b_2)$

$= (a_1 - a_2) + (b_1 - b_2) \in A+B$

$\because a_1 - a_2 \in A$

& $b_1 - b_2 \in B$

because A and B are Submodules

$\Rightarrow x - y \in A+B \quad \forall x, y \in A+B$

$\therefore$ 1st Condition of Submodule is satisfied

ii) Let $r \in R$ and $m \in A+B$

where $m = a+b \quad a \in A$ & $b \in B$

$rm = r(a+b)$

$\Rightarrow ra + rb \in A+B$

$\because ra \in A$ & $rb \in B$

because A and B are Submodules of M.

$\therefore rm \in A+B \quad \forall r \in R$ & $m \in A+B$

$\Rightarrow$ 2nd Condition of Submodule satisfied

Hence $A+B$ is a Submodule of M.

$a \in A \Rightarrow a+0 \in A+B \quad \because 0 \in B$

$\Rightarrow a \in A+B$

$\Rightarrow A \subseteq A+B$

Similarly $B \subseteq A+B$

$\therefore A+B$ Contains both A and B.

Module Homomorphism :-

Let M and N are two module over a ring R.

A mapping $f : M \to N$ is said to be a Homomorphism if

i) $f(a+b) = f(a) + f(b) \quad \forall a, b \in M$

ii) $f(rm) = r f(m) \quad \forall r \in R$, $m \in M$

Monomorphism:- if f is 1-1. Then it is called monomorphism.

Epimorphism:- if f is onto. Then it is called Epimorphism.

Homomorphism:- if f is bijective. Then it is called Homomorphism.

Kernal of Homomorphism:-

Let $T: M \to N$ be a module Homomorphism. Then set of those elements of M which are mapped to zero (additive identity of N) is called Kernal of T and is denoted by $K(T)$ &

$$K(T) = \{m \in M : T(m) = 0\}$$

Theorem:- if M and N are two R-modules And $T: M \to N$ is a Homomorphism. Then $K(T)$ is a Submodule of M.

Proof:- Let M and N are two R-modules and $T: M \to N$ is a Homomorphism we have to Prove that $K(T)$ is a

submodule of M.

Since $T(0) = 0 \Rightarrow 0 \in \ker T$

$K(T) \neq \emptyset$

Let $m_1, m_2 \in K(T)$

$\Rightarrow T(m_1) = 0$ and $T(m_2) = 0$

$T(m_1 - m_2) = T(m_1) - T(m_2)$ ($\because T$ is a Homo.

$= 0 - 0$

$= 0$

$\Rightarrow m_1 - m_2 \in K(T)$

$\therefore$ 1st Condition is Satisfied

Again

Let $r \in R$ and $m \in K(T)$

$\Rightarrow T(m) = 0$

$T(rm) = rT(m)$ ($\because T$ is a Homo.

$= r(0)$

$= 0$

$\Rightarrow rm \in K(T)$

$\therefore$ Second Condition is also Satisfied.

Hence $K(T)$ is submodule of M.

Range of T:- or Im T

Let $T: M \to N$ be module Homomorphism. The set of images of elements of M under T is called Range of T and is denoted by R(T). i.e $R(T) = \{T(m) \in N : m \in M\}$

if $T: M \to N$ is onto. Then $R(T) = N$.

Theorem:- Let M and N are two R-modules and $T: M \to N$ is a Homomorphism. Then R(T) is a submodule of N.

Soln Since $T(0) = 0$

$\Rightarrow 0 \in R(T)$

$\therefore R(T) \neq \phi$

To show that R(T) is a submodule of N.

Let $T(m_1), T(m_2) \in R(T)$

where $m_1, m_2 \in M$

$T(m_1) - T(m_2) = T(m_1 - m_2) \in R(T)$

$\Rightarrow m_1 - m_2 \in M$

($\because$ M is a module over R)

$\therefore$ IInd Condition of submodule satisfied. Again let $r \in R$ and $T(m) \in R(T)$

$r(T(m)) = T(rm) \in R(T)$

$\therefore rm \in M$

$\therefore$ & T is Homo

(∵ M is a module over R)

∴ 2nd Condition is also satisfied

Hence K(T) is a sub module of N.

Theorem:- Let T: M → N be a Homomorphism from M onto N. Then T is an isomorphism iff K(T) = {0}

Proof:- Suppose T: M → N is an isomorphism. We shall Prove that K(T) = {0}

For this let x ∈ K(T) is an arbitrary element of K(T)

⇒ T(x) = 0

but T(0) = 0

⇒ T(x) = T(0)

⇒ x = 0 (∵ T is 1-1

Since x is arbitrary

∴ K(T) = {0}

Conversely:-

Suppose K(T) = {0}

now we have to Show that T is 1-1.

For this let

T(m₁) = T(m₂) where m₁, m₂ ∈ M

⇒ T(m₁) − T(m₂) = 0

$\Rightarrow T(m_1 - m_2) = 0$

$\Rightarrow m_1 - m_2 \in K(T)$

but $K(T) = \{0\}$

$\therefore m_1 - m_2 = 0$

$\Rightarrow m_1 = m_2$

$\Rightarrow T$ is 1-1.

Hence T is an isomorphism.

✓ V. Imp

Theorem:- For any abelian group A, let $End(A)$ be the ring of all endomorphisms of A. (i.e. $End(A)$ is a ring)

Let R be a ring. Then A is a left R-module iff there exist a Ring Homomorphism.

$\psi : R \longrightarrow End(A)$

~~Proof:- Let A be a left R-module~~

Proof:- Let us define a mapping

$\psi : R \longrightarrow End(A)$ by

$$\psi(r) = \phi_r \quad \forall\, r \in R$$

where $\phi_r : A \to A$ is defined as

$$\phi_r(a) = ra \quad \forall\, a \in A$$

We have to show that ψ is

a Ring Homomorphism.

Let $r, s \in R$

$$\psi(r+s) = \phi_{r+s}$$

$$\phi_{r+s}(a) = (r+s)a = ra + sa$$
$$= \phi_r(a) + \phi_s(a)$$
$$= (\phi_r + \phi_s)(a)$$

$$\Rightarrow \phi_{r+s} = \phi_r + \phi_s$$

$$\Rightarrow \psi(r+s) = \psi(r) + \psi(s)$$

Again $\psi(rs) = \phi_{rs}$

Now $\phi_{rs}(a) = rs(a) = r(sa)$
$$= r(\phi_s(a))$$
$$= \phi_r(\phi_s(a))$$
$$= \phi_r \phi_s(a)$$

$$\Rightarrow \phi_{rs} = \phi_r \phi_s$$

$$\Rightarrow \psi(rs) = \psi(r)\psi(s)$$

$\Rightarrow \psi$ is a ring Homomorphism.

Conversely:- Suppose $\psi : R \to End(A)$ is a ring homomorphism.

define a mapping $* : (R \times A) \to A$ by

$$*(r,a) = \psi_r(a) \quad | \quad \because \psi_r(a) = ra$$

OR

$$ra = \psi(r)a \quad | \quad \text{where } \psi_r(a) = \psi(r)a \Rightarrow \psi_a = \psi(r)$$

now we shall prove that A is a left R-module.

A is an abelian group under addition — (given)

For any $r, s \in R$ & $a, b \in A$

i) $r(a+b) = \psi(r)(a+b)$

$= \psi(r)a + \psi(r)b$

$= ra + rb$

ii) $(r+s)a = \psi(r+s)a$ ($\because \psi$ is Hom^{n})

$= (\psi(r) + \psi(s))a$

$= \psi(r)a + \psi(s)a$

$= ra + sa$

iii) $(rs)a = \psi(rs)a$

$= \psi(r)\psi(s)(a)$ ($\because \psi$ is Hom^{n})

$= \psi(r)(\psi(s)a)$

$= \psi(r)(sa)$

$= r(sa)$

$\therefore$ A is a left R-module.

Quotient Module

Let M be a left R-module & $N \neq \phi$ is a submodule of M over R. Then the set of all left cosets of N by M is denoted by M/N where

$$M/N = \{x+N : x \in M\}$$

The set M/N is a left R-module under the addition and scalar multiplication defined as

i) $(x+N)+(y+N) = x+y+N$

ii) $r(x+N) = rx+N$

This module is called Quotient module.

Theorem:- If $N \neq \phi$ is a submodule of then left cosets of N in M

$M/N = \{x+N : x \in M\}$ is a left R-module under addition and scalar multiplication defined by

$(x+N)+(y+N) = x+y+N \quad \forall x+N, y+N \in M/N$

$r(x+N) = rx+N \quad \forall r \in R$

Proof:- First we shall Prove that

The addition and Scalar multiplication in M/N is well defined
That is
if $x+N = x'+N \in M/N$
$y+N = y'+N \in M/N$
Then $x+y+N = x'+y'+N$
and if $r = r' \in R$
and $x+N = x'+N$
Then $rx+N = r'x'+N$.

Let $x+N = x'+N$
& $y+N = y'+N$
we want to show that
$x+y+N = x'+y'+N$
Since
$x+N = x'+N$
$\Rightarrow x-x'+N = N$
$\Rightarrow x-x' \in N$
Again $y+N = y'+N$
$\Rightarrow y-y'+N = N$
$\Rightarrow y-y' \in N$
$\Rightarrow (x-x')+(y-y') \in N$
$\Rightarrow (x+y)-(x'+y') \in N$

$\Rightarrow x+y \in (x'+y')+N$
but
$x+y \in (x+y)+N$
$\Rightarrow (x+y)+N = (x'+y')+N$

addition is M/N is well defined

Ag dis

Let $x, x' \in R$

& $x = x'$

$x+N = x'+N \in M/N$

such that

$x+N = x'+N$

we have to show that

$ax+N = ax'+N$

Since $x+N = x'+N$

$\Rightarrow x - x' + N = N$

$\Rightarrow x - x' \in N$

$\Rightarrow a(x-x') \in N$ ($\because N$ is a submodule of M

$\Rightarrow ax - ax' \in N$

$\Rightarrow ax \in ax' + N$

but $ax \in ax + N$

$\Rightarrow ax + N = ax' + N$ | $\because$ left cosets are either disjoint or identical

$\Rightarrow ax + N = a'x' + N$ ($\because a = a'$

$\therefore$ multiplication is well defined

Now we shall prove that M/N is a left R-module

1) M/N is closed under addition

2) for $x+N, y+N, z+N \in M/N$

$\therefore M/N$ is a left module over R.

First Fundamental Theorem of Homomorphism:-

Statement:- Let $f: M \to M'$ be module Homomorphism then
i) $\ker f$ is Submodule of M.
ii) $M/\ker f \cong \text{Im}(f)$

Proof:- i) Already Proved
ii) define a mapping

$\psi : M/\ker f \to \text{Im}(f)$ as

$\psi(x+K) = f(x) \quad \forall\, x+K \in M/K$

First we Shall Prove that ψ is well defined

For this let $x+K, y+K \in M/K$ and

$$x+K = y+K$$
$$\Rightarrow x-y+K = K$$
$$\Rightarrow x-y \in K$$
$$\Rightarrow x-y = k \text{ for some } k \in K$$
$$\Rightarrow x = y+k$$

Now $\psi(x+K) = f(x) = f(y+h_n)$

$= f(y) + f(h_n)$

$= f(y) + 0$

$= \psi(y+h_n)$

$\therefore x+K = y+K$

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

$\therefore \psi$ is well defined

ψ is a Homomorphism

Let $x+K, y+K \in M/\ker f$

$\psi((x+K)+(y+K)) = \psi(x+y+K)$

$= f(x+y)$

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

$= \psi(x+K) + \psi(y+K)$

Again let $x+K \in M/\ker f$

and $r \in R$

$\therefore \psi(r(x+K)) = \psi(rx+K)$

$= f(rx)$

$= r(f(x))$ $\therefore f$ is a Homomorphism

$= r\psi(x+K)$

$= r * \psi(x+K)$

$\therefore \psi$ is a Homomorphism.

ψ is 1-1

Let $\psi(x+K) = \psi(y+K)$

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

$\Rightarrow f(x) - f(y) = 0$

$\Rightarrow f(x-y) = 0$ $\therefore f$ is Homo.

$\Rightarrow x-y \in \ker f$

$\Rightarrow x-y = h$ for some $h \in K$

$x = y+h$

$\Rightarrow x+K = y+h+K$

$\Rightarrow x+K = y+K$

ψ is onto :-

Let $x' \in Im(f)$ be any arbitrary elements of $Im(f)$

Then exist an element $x \in M$ such that $f(x) = x'$

$\therefore x \in M \Rightarrow x+K \in M/\ker f$

$\therefore \psi(x+K) = f(x) = x'$

since x' is arbitrary

$\therefore$ for each $x' \in Im(f)$

Then exist an element

$x+K \in M/\ker f$ such that

$x' = \psi(x+K)$

ψ is onto

$\therefore \psi : M/\ker f \longrightarrow \mathrm{Im}(f)$

is an Isomorphism

$\therefore \dfrac{M}{\ker f} \cong \mathrm{Im}(f)$

2nd Isomorphism Theorem :-

Statement :- Let L and N be two Submodule of an R-module M Then

$$\frac{L+N}{N} \cong \frac{L}{L \cap N}$$

Proof :- We know that $L+N$ is a Submodule of M containing both L and N

also $L \cap N$ is a Submodule of L.

let $L \cap N = P$

define a mapping $\phi : L+N \to L/P$ as

$\phi(l+n) = l+P$

ϕ is well defined :-

Let $l+n, l'+n' \in L+N$

where $l+n = l'+n'$

$\Rightarrow l - l' = n' - n \in L \cap N = P$

$\Rightarrow l - l' \in P$

$\Rightarrow l \in l' + P$

but $l \in l + P$

$\Rightarrow l + P = l' + P$

$\Rightarrow \phi(l+n) = \phi(l'+n')$

$\therefore \phi$ is well defined

ϕ is onto :-

Let $l + P \in L/P$

$\Rightarrow l \in L$

but $l = l + 0 \in L + N$

and $\phi(l+0) = l + P$

which shows that each element of L/P is image of same element of $L+N$.

$\therefore \phi$ is onto

ϕ is Homomorphism :-

Let $l+n, l'+n' \in L+N$ and $\lambda \in R$

$\phi[(l+n)+(l'+n')] = \phi(l+l'+n+n')$

$= l + l' + P$

$$= (l+P) + (l'+P)$$
$$= \phi(l+m) + \phi(l'+m')$$

Again
$$\phi(r(l+m)) = \phi(rl+rm)$$
$$= rl+P$$
$$= r(l+P)$$
$$= r\phi(l+m)$$

$\therefore \phi$ is a Homo.

Since $\phi : L+N \to L/P$
is an onto Homomorphism
Therefore by Fundamental Theorem
of Homomorphism.

$$\frac{L+N}{\ker\phi} \cong L/P$$

Now we shall Prove that

$$\ker\phi = N$$

$$\ker\phi = \{l+m \in L+N : \phi(l+m) = P\}$$

$$= \{l+m \in L+N : l+P = P\}$$

$$= \{l+m \in L+N : l \in P\}$$

$$= \{l+m \in L+N : l \in L \cap N\}$$

$= \{l+n \in L+N : l \in N\}$

$= \{l+n \in L+N : L \subseteq N\}$

$= \{l+n \in L+N : L+N = N\}$

$\ker\phi = N$

Hence $\frac{L+N}{N} \cong \frac{L}{L \cap N}$

Fundamental Theorem of Homomorphism :-

Theorem :- If $f : M \to M'$ be a surjective (onto) module homomorphism then

$$\frac{M}{\ker f} \cong M'$$

Proof :- First we shall prove that $\ker f$ is a submodule of M (already proved)

define a mapping

$\phi : \frac{M}{\ker f} \to M'$ as $\phi(K) = K$ where $\ker f = K$

$\phi(x+K) = f(x) \quad \forall x \in M$

$\because x+K \in \frac{M}{K}$ where $\ker f = K$

φ is well defined:-

Let $x+K, y+K \in M/K$

$x+K = y+K$

$\Rightarrow x-y+K = K$

$\Rightarrow x-y \in K$

$\Rightarrow x-y = k$ for some $k \in K$

$\Rightarrow x = y+k$

$\therefore \varphi(x+K) = f(x) = f(y+k)$

$= f(y) + f(k)$

$= f(y) + 0$

$= \varphi(y+K)$

$\therefore \varphi$ is well defined.

φ is Homomorphism:-

Let $x+K, y+K \in M/K$

$\varphi((x+K)+(y+K)) = \varphi(x+y+K)$

$= f(x+y)$

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

$= \varphi(x+K) + \varphi(y+K)$

Again let $x+K \in M/K$ and $s \in R$

$\varphi(s(x+K)) = \varphi(sx+K)$

$= f(sx)$

$= \alpha f(x)$ $\because f$ is Homo.

$= \alpha \phi(x+K)$

$\therefore \phi$ is Homomorphism.

ϕ is 1-1 :-

Let $\phi(x+K) = \phi(y+K)$

$\Rightarrow f(x) = f(y)$ when $x+K \in M/K$

$\Rightarrow f(x) - f(y) = 0$ $y+K \in M/K$

$\Rightarrow f(x-y) = 0$ f is Homo

$\Rightarrow x-y \in \ker f$ | $\because$ Two cosets are either distinct or identical.

$\Rightarrow x-y \in K$

$\Rightarrow x \in y+K$

but $x \in x+K$

$\Rightarrow x+K = y+K$

$\therefore \phi$ is 1-1

ϕ is onto :-

Let $x' \in M'$

Since $f: M \to M'$ is onto

Therefore there exist an element $a \in M$ such that

$f(a) = x'$

$\therefore$ There exists $a+K \in M/K$ s.t

$\phi(a+K) = f(a) = x'$

x' is image of some element $a+K \in M/K$ under ϕ

Since x' is arbitrary

$\therefore \varphi$ is onto

$\therefore \varphi : M/K \to M'$ is an homomorphism

Hence M/K is homomorphism to M'

or $M/K \cong M'$

or

$$M/\ker\varphi \cong M' \quad ; \ker\varphi = K$$

---

* Q.t State and Prove 3rd Homomorphism Theorem

Statements- If L and N are two submodules of an R-module M such that $N \subseteq L$ then

$$\frac{M/N}{L/N} \cong M/L$$

Proof:- define a mapping

$\varphi : M/N \to M/L$

$\varphi(x+N) = x+L \quad \forall x+N \in M/N$

φ is well defined

Let $x+N, y+N \in M/N$

Then $x+N = y+N$

$\Rightarrow x-y+N \supseteq N$

$\Rightarrow x-y \in N$

$\Rightarrow x-y \in L$ $\because N \subseteq L$

$\Rightarrow x \in y+L$

but $x \in x+L$

$\Rightarrow x+L = y+L$ because two left cosets are either disjoint or identical

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

ϕ is well defined

ϕ is onto :- Let $x+L \in M/L$ be any arbitrary element of M/L

$\Rightarrow x \in M$

$\Rightarrow x+N \in M/L$ as $N \subseteq L$

and $\phi(x+N) = x+L$

$\therefore \phi$ is onto

ϕ is homomorphism :-

Let $x+N, y+N \in M/N$ and $a \in R$

$\phi((x+N)+(y+N))$

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

$= x+y+L$

$= x + b + (y + b)$

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

Again

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

$= rx + L$

$= r(x+L) = r\phi(x+N)$

$\therefore \phi$ is a Homomorphism

Since $\phi : M/N \to M/L$ is an onto Homomorphism (epimorphism)

$\therefore$ By fundamental Theorem of Homomorphism

$$\frac{M/N}{\ker\phi} \cong M/L$$

Now we shall prove that $\ker\phi = L/N$

$\ker\phi = \{x+N \in M/N : \phi(x+N) = L\}$

$= \{x+N \in M/N : x+L = L\}$

$= \{x+N \in M/L : x \in L\}$

$= \{x+N \in M/L : x+N \in L/N\}$

Since x is arbitrary

$\therefore \quad \ker \varphi = L/N$

Hence $\dfrac{M/N}{L/N} \cong M/L$

As required

Internal Direct Sum:-

M is called internal direct sum of its submodule $M_1, M_2, \ldots, M_n$ if

1) $M = \sum_{i=1}^{n} M_i$

2) $M_i \cap \sum_{j \neq i} M_j = \{0\}$

written as

$M = M_1 \oplus M_2 \oplus \ldots \oplus M_n$

Theorem:- If $M_1, M_2, \ldots, M_n$ be submodules of M. Then following are equivalent.

1) M is Direct Sum of $M_i, i = 1, 2, \ldots, n$

2) each $m \in M$ can be uniquely expressed as

$m = m_1 + m_2 + \ldots + m_n$

where $m_i \in M_i \quad 1 \leq i \leq n$

Proof:- (1) ⇒ (2)

Suppose M is Direct sum of $M_i : i = 1, 2, \ldots, n$.

Then

i) $M = \sum_{i=1}^{n} M_i$ — (I

ii) $M_i \cap \sum_{j \neq i} M_j = \{0\}$ — (II

Then for $m \in M = \sum_{(i)}^{n} M_i$

it can be written as

$m = m_1 + m_2 + \ldots + m_n \; ; m_i \in M$

Let $m = m_1' + m_2' + \ldots + m_n'$

be another expression of m.

$\Rightarrow m_1 + m_2 + \ldots + m_n = m_1' + m_2' + \ldots + m_n'$

$m_i - m_i' = m_1' - m_1 + m_2' - m_2 + \ldots$

$+ m_{i-1}' - m_{i-1} + m_{i+1}' - m_{i+1} + \ldots + m_n' - m_n$

$m_i - m_i' = \sum_{j \neq i} m_j' - m_j \to (A) \; ; m_i, m_i' \in M_i$

$i = 1, 2, \ldots, n$

$\because m_i, m_i' \in M_i \Rightarrow m_i - m_i' \in M_i$

since $m_j', m_j \in M_j$

$\therefore m_j' - m_j \in M_j$

$\sum_{j \neq i} (m_j' - m_j) \in \sum_{j \neq i} M_j$

$m_i^* - m_i' \in \sum_{j \neq i} M_j$ Using (A)

$\Rightarrow m_i' - m_i \in M_i \cap \sum_{j \neq i} M_j = \{0\}$

$\Rightarrow m_i' - m_i = 0$

$\Rightarrow m_i' = m_i \quad \forall (i = 1, 2, \ldots, n)$

$\Rightarrow$ So expression is unique.

(2) $\Rightarrow$ (1) uniquely given But each $m \in M$ can be written as

$m = m_1 + m_2 + \cdots + m_n$ where $m_i \in M_i$

$\Rightarrow m = \sum_{(i=1)}^{n} m_i \qquad (i = 1, 2, \ldots, n)$

Then clearly

$$M = \sum_{i=1}^{n} M_i$$

now to Prove

$$M_i \cap \sum_{j \neq i} M_j = \{0\}$$

Let $m \in M_i \cap \sum_{j \neq i} M_j$

$\Rightarrow m \in M_i$ and $m \in \sum_{j \neq i} M_j$

$m = 0 + 0 + \cdots + m + 0 + 0 + \cdots + 0$

m is at ith place.

also $m \in \sum_{j \neq i} M_j$

$\Rightarrow m = m_1 + m_2 + \cdots + m_{i-1} + 0 + m_{i+1} + \cdots + m_n$

$\therefore$ m has unique expression

$\Rightarrow m_1 = 0, m_2 = 0, \ldots, m_n = 0$

if $m = 0$

$\Rightarrow M_i \cap \sum_{j \neq i} M_j = \{0\}$

As m is Arbitrary

$\Rightarrow M$ is Direct Sum of $M_1, M_2, \ldots M_n$

External Direct Sum :-

If $M_1, M_2, \ldots, M_n$ are R module Then $E = M_1 \times M_2 \times M_3 \ldots \times M_n$ is an R module under the operation defined below is called External direct sum.

$E = \{(m_1, m_2, \ldots, m_n) ; m_i \in M_i\}$

$1 \leq i \leq n$

for $x, y \in E$

$x = (m_1, m_2, \ldots, m_n)$

$y = (m_1', m_2', \ldots, m_n')$

$x + y = (m_1 + m_1', m_2 + m_2', \ldots, m_n + m_n')$

and for $r \in R$

$rx = r(m_1, m_2, \ldots m_n)$

$rx = (rm_1, rm_2, \ldots, rm_n)$

Verify that it is R-module.

since we write as

$E = M_1 \oplus M_2 \oplus M_3 \oplus \ldots \oplus M_n$

Finitely Generated Module:-

An R-module M is called finitely generated if it can be generated by a finite subset of M. i.e if $M = Rx$ where $x \neq \phi$ is a finite subset of M.

Cylic Module:-

A module M is called cylic if it can be generated by a single element:-

NOTE:- if M is cylic generated by x over R. Then

$M = Rx$.

V.V.Imp

Lemma:- Let M be an R-module Then

1) M is sum of finitly many finitly Generated R-module. Then M is F.G (Finitly Generated).

2) if M can be generated by "s" elements. Then M/N also generated by "s" elements:- where N is submodule of M.

3) if $M = M_1 \oplus M_2$

And M can be generated by "s" element Then M_1 Can be generated by "s" elements.

Proof:- Suppose That $M_1, M_2, \ldots M_n$ are finitly generated R-module

$M = M_1 + M_2 + \cdots + M_n$

Let $x_{i1}, x_{i2}, \cdots, x_{is_i}$ be the generated by M_i — generates M_i

Then for $m \in M$.

$m = m_1 + m_2 + \cdots + m_n$; $m_i \in M_i$

As $x_{i1}, x_{i2}, \cdots, x_{is_i}$ be generated by M_i. Then — generates M_i

$m_i = a_{i1}x_{i1} + a_{i2}x_{i2} + \cdots + a_{is_i}x_{is_i}$

$\Rightarrow m = (a_{11}x_{11} + a_{12}x_{12} + \cdots + a_{1s_1}x_{1s_1})$
$+ (a_{21}x_{21} + a_{22}x_{22} + \cdots + a_{2s_2}x_{2s_2}) + \cdots$
$\cdots + a_{n1}x_{n1} + a_{n2}x_{n2} + \cdots + a_{ns_n}x_{ns_n}$

Then

$x_{11}, x_{12}, \cdots x_{1s_1}, x_{21}, x_{22}, \cdots, x_{2s_2}, \cdots, x_{n1}, x_{n2}, \cdots, x_{ns_n}$

all generator of M.

which are $s_1 + s_2 + s_3 \cdots + s_n$ in number

which is finite so M is Finitely generated.

II). Let $\{m_1, m_2, \cdots, m_s\}$ be the generating set for M.

Then for $m \in M$

$m = a_1m_1 + a_2m_2 + \cdots + a_sm_s$

$m + N = a_1m_1 + a_2m_2 + \cdots + a_sm_s + N$

$$= (a_1 m_1 + N) + (a_2 m_2 + N) + \cdots + (a_s m_s + N)$$

$$m + N = a_1 (m_1 + N) + a_2 (m_2 + N) + \cdots + a_s (m_s + N)$$

$\forall\ m + N \in M/N$

Can be generated by M/N generated by

$m_1 + N, m_2 + N, \cdots, m_s + N$ "s" elements

So M/N is generated by "s" element.

III) Let $\{m_1, m_2, \cdots, m_s\}$ be the generated set for M.

Ans

$M = M_1 \oplus M_2$ & $M_1 \cap M_2 = \{0\}$

By 2nd Isomorphic Theorem.

$$\frac{M_1 \oplus M_2}{M_2} \cong \frac{M_1}{M_1 \cap M_2}$$

$$\Rightarrow \frac{M}{M_2} \cong \frac{M_1}{\{0\}} \cong M_1$$

$$\frac{M}{M_2} \cong M_1$$

By part II if M is generated by "s" elements

$\therefore$ M/M_2 is generated by "s" elements

and Hence M_f is generated by "1" element.

Q# Give example of a Finitely Generating Module which has ~~not~~ Submodule which is not Finitely Generating.

OR Question - C.O.N

Theorem:- Prove That every Direct Sum of Finitely Generating Module is Finitely Generating Module Can have Submodule which ~~is~~ is not Finitely Generated.

Proof:- Let R be a ring of all mapping from $R \to R$ under the operation i.e $R = \{f : R \to R\}$

$$(f+g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x)\, g(x)$$

Then R is Commutative ring with identity with ~~identity~~ mapping "i" which map every element of R to 1 of R.

i.e $i(x) = 1 \quad \forall x \in R$

i.e $(f \cdot i)(x) = f(x)\, i(x)$

$= f(x) \cdot 1$

$(f \cdot i)(x) = f(x)$

Let $h \in R$, $f \in N$

$f(x) = 0 \quad \forall |x| \geq |n|$

$(hf)(x) = h(x) f(x) = h(x)(0) = 0$

$(hf)(x) = 0 \quad \forall |x| \geq |n|$

$\Rightarrow hf \in N$

$\Rightarrow N$ is submodule of M.

Now we claim that N is not finitely generated.

Otherwise

if $\{f_1, f_2, \ldots, f_n\}$ generate N

and $f_i(x) = 0 \quad \forall |x| \geq |n_i|$

$; i = 1, 2, 3, \ldots, n$

Let f be a function such that

$$f(x) = \begin{cases} 1 & \forall x \in [-(n+1), n+1] \\ 0 & \forall x \notin [-(n+1), n+1] \end{cases}$$

Then $f \in N$

and

$f = a_1 f_1 + a_2 f_2 + \cdots + a_n f_n$

$f(x) = a_1 f_1(x) + a_2 f_2(x) + \cdots + a_n f_n(x)$

$f.i = f$

also $i.f = f$

now Consider $M = R^R$

i.e M is R module over R

Then $M = R^R$ is Cyclic.

$\Rightarrow$ M is Finitely Generated

Let N be the set of all $f \in R$ which vanish outside of some finite Interval.

i.e $N = \{f \in R \mid f(x) = 0 \ \forall x \notin [-n, n]\}$

or $\forall |x| \geq n$

Let $f_1, f_2 \in N$

Then $\exists\ n_1, n_2 \in$ integers $\mathbb{R}$ s.t.

$f_1(x) = 0 \quad \forall |x| > |n_1| \Rightarrow x \notin [-n_1, n_1]$

$f_2(x) = 0 \quad \forall |x| > |n_2| \Rightarrow x \notin [-n_2, n_2]$

if $n_2 > n_1$

$(f_1 - f_2)(x) = f_1(x) - f_2(x)$

$= 0 - 0 \quad \forall |x| > |n_2|$

$(f_1 - f_2)(x) = 0 \quad \forall |x| > |n_2|$

$\Rightarrow f_1 - f_2 \in N$ i.e $|x| > n_2$

Torsion Free Module:-

A module which has not any torsion element is called torsion free module.

Lemma:- Let R be a Commutative Ring with identity and M be an R-module Then for $m \in M$.

$O(m) = \{r \in R : rm = 0\}$; is an ideal of R called order ideal of m. (i.e the ideal Corresponding to m).

Proof:- As $0 \cdot m = 0$

$\Rightarrow 0 \in O(m)$

$\Rightarrow O(m) \neq \phi$

Let $r_1, r_2 \in O(m)$

$r_1 m = 0 \; , \; r_2 m = 0$

As $(r_1 - r_2)m = r_1 m - r_2 m$

$= 0 - 0$

$= 0$

$\Rightarrow r_1 - r_2 \in O(m)$

for $r \in R$ $r_1 \in O(m)$

$r_1 m = 0$

Now $(rr_1)m = r(r_1 m)$

$= r(0)$

$(rr_1)m = 0$

$\Rightarrow rr_1 \in O(m)$

if $\alpha \notin [-n, n]$

but $\alpha \in [-(n+1), n+1]$

$1 = 0 + 0 + \cdots + 0$

$1 = 0$ which is not possible.

$\Rightarrow \{f_1, f_2, \ldots, f_n\}$ can not Generate N

$\Rightarrow N$ is not Finitely Generated.

Torsion Element:-

An element "m" of an R-module M is called Torsion element if there exist a non-zero $r \in R$ such that

$rm = 0$

Remark:- $0 \in M$ is always torsion element

Torsion Module:- A module where every element is torsion element is called Torsion module.

Torsion free element:-

An element which is not torsion is called Torsion free.

~~**Torsion Free Module:-**~~

if $rm = 0$ whenever $r = 0$ m is torsion free element.

$[(x+N)+(y+N)]+(z+N) = ((x+y)+N)+z+N$

$= (x+y)+z+N$

($\because R$ is a ring)

$= (x+N)+(y+z)+N$

$= (x+N)+(y+N)+(z+N)$

$\therefore$ $+'$ in M/N is associative

Since (3) Since $0 \in M$

$\therefore 0+N \in M/N$ & it is

Then additive identity of M/N

$\therefore$ For any $x+N$

$(0+N)+(x+N) = (0+x)+N$

$= x+N$

Since for any $x+N \in M/N$

where $x \in M$

Then exist $-x \in M$

$\Rightarrow -x+N \in M/N$

and it is the inverse of $x+N$

$\therefore$ Inverse law hold in M/N

For any $x+N, y+N \in M/N$

$(x+N)+(y+N) = (x+y)+N$

$= (y+x)+N$

$= (y+N)+(x+N)$

$\therefore M/N$ is an abelian group under $+'$.

The Next Three axioms of a module are satisfied

~~is M/N because Thus~~

is M/N is as follow.

4) Let $\lambda \in R$

& $x+N, y+N \in M/N$

, $xy \in M$

Then $\lambda[(x+N)+(y+N)]$

$= \lambda[(x+y)+N]$

$= \lambda(x+y)+N$

$= \lambda x + \lambda y + N$

$= (\lambda x + N) + (\lambda y + N)$

$= \lambda(x+N) + \lambda(y+N)$

$\forall \lambda \in R$ & $x+N, y+N \in M/N$

4) Let $\lambda, \delta \in R$ & $x+N \in M/N$

$(\lambda+\delta)(x+N) = (\lambda+\delta)x + N$

$= \lambda x + \delta x + N$

$= \lambda x + N + \delta x + N$

$= \lambda(x+N) + \delta(x+N)$

$\forall \lambda, \delta \in R$ & $x+N \in M/N$

5) Let $\lambda, \delta \in R$ & $x+N \in M/N$

~~$(\lambda\delta)(x+N)$~~

$\lambda(\delta(x+N)) = \lambda(\delta x + N)$

$= \lambda\delta x + N$

$= \lambda\delta(x+N)$

$\forall \lambda, \delta \in R$ & $x+N \in M/N$

$(r_1 r_2)m = r_1(r_2 m)$

$= (r_2 r_1)m$ $\because R$ is commutative

$= r_2(r_1 m)$

$= r(0)$

$(r_1 r_2)m = 0$

$\Rightarrow r_1 r_2 \in O(m)$

$\Rightarrow O(m)$ is ideal of R.

Example:- Let $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ be a cyclic which is Abelian so taken as a module over $\mathbb{Z}$.

Find $O(1)$ & $O(2)$

Sol:- $O(1) = \{n \in \mathbb{Z} : n \cdot 1 = 0\}$

In modulo 3

$n \cdot 1 = 0$ iff n is multiple of 3.

i.e $n = 0, \pm 3, \pm 6, \pm 9, \ldots$

$\therefore O(1) = \{0, \pm 3, \pm 6, \ldots\}$

$O(1) = 3\mathbb{Z}$

Similarly

$O(2) = \{n \in \mathbb{Z} : n \cdot 2 = 0\}$

$n \cdot 2 = 0$ iff n is multiple of 3.

$\therefore O(2) = \{0, \pm 3, \pm 6, \ldots\}$

So Again $O(2) = 3\mathbb{Z}$

Remarks:- A Vector Space V over a field K Considered as a K-module is Torsion free.

Proof:-

Let $v \in V$ & $v \neq 0$

$\{ v \cdot v = 0$

i.e. v is torsion element.

$0 \neq v \in K$, K is field

$\Rightarrow v^{-1} \in K$

$\Rightarrow v^{-1}(vv) = v^{-1}0$

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

$\Rightarrow v = 0$

V has only "0" Torsion element.

so V is Torsion Free.

Theorem:- Let M be a module over an Integral Domain R and T denoted the set of torsion element of M. Then T is submodule of M. and M/T is Torsion Free.

Proof:- As "0" is Torsion element

$0 \in T \Rightarrow T \neq \phi$

let $t_1, t_2 \in T$

Then $\exists\ r_1, r_2 \in R$ & $r_1, r_2 \neq 0$

$r_1 t_1 = 0$ $r_2 t_2 = 0$

Consider

$(r_1 r_2)(t_1 - t_2) = (r_1 r_2)t_1 - (r_1 r_2)t_2$

Note: Commutative Ring with identity which has no zero divisor) i.e. $r_1, r_2 \neq 0 \Rightarrow r_1 r_2 \neq 0$

$= r_2(r_1 t_1) - r_1(r_2 t_2)$

$= 0 - 0$

$r_1 r_2 (t_1 - t_2) = 0$

And $r_1 r_2 \neq 0$ $\because R$ is an Integral domain

$t_1 - t_2 \in T$

Let $r \in R$, $t_1 \in T$

$r_1 t_1 = 0$; $r_1 \neq 0$

Now $r_1(r t_1) = (r_1 r) t_1$ $\because R$ is I.D.

$= r(r_1 t)$

$= r(0) = 0$

$r_1(r t_1) = 0$

$\Rightarrow r t_1 \in T$

$\Rightarrow T$ is Submodule of M.

To Show that M/T is Torsion free

Let $m+T \in M/T$ for $m \in M$ as a vector

as a Torsion element. (i.e mT is Torsion element)

Now

$r(m+T) = T$

$rm+T = T$; $r \in R$, $r \neq 0$

$\Rightarrow rm \in T$

Then $\exists\ s \in R$

$s(rm) = 0$, $s \neq 0$

$(sr)m = 0$

$s, r \in R$

$sr \in R$

$sr \neq 0$ $\because R$ is I-D

$\Rightarrow m$ is Torsion element.

i.e $m \in T$

$\Rightarrow m+T = T$

$\Rightarrow$ The only Torsion element in M/T is its identity T.

so M/T is Torsion free.

Note $M/T = \{m+T : m \in M\}$

Freely Generated Module:-

Let M be an R-module and let X be a subset of M. we say M is freely generated by X if

1) X generate M as a Module.
2) Every mapping of X into an R-module can be extended to an R-module Homomorphism of M.

The module generated in this way is called free module.
The set X is called free basis.

Remark:— The Extended Homo. in freely generated module is unique.

Proof:— Let ψ and ψ' be

The two extended Homomorphism of f."
and
Let $S = \{m \in M : \psi(m) = \psi'(m)\}$

To Show S is Submodule

As $\psi(0) = \psi'(0) = 0$

$\Rightarrow 0 \in S \Rightarrow S \neq \phi$

Let $s_1, s_2 \in S$

$\psi(s_1) = \psi'(s_1)$ & $\psi(s_2) = \psi'(s_2)$

$\psi(s_1 - s_2) = \psi(s_1) - \psi(s_2)$

$= \psi'(s_1) - \psi'(s_2)$

$\psi(s_1 - s_2) = \psi'(s_1 - s_2)$

$s_1 - s_2 \in S$

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

$\Rightarrow \psi(s) = \psi'(s)$

$\psi(rs) = r\psi(s)$ $\because \psi$ is Homo.

$= r\psi'(s)$

$\psi(rs) = \psi'(rs)$ $\therefore \psi'$ is Homo.

$rs \in S$

$\Rightarrow S$ is Submodule.

Also since ψ and ψ' are extension of f on X.

So $\psi(x) = \psi'(x) \quad \forall x \in X$

Let $m \in M$

Then $m = \sum_{i=1}^{n} r_i x_i$

$\psi(m) = \psi\left(\sum_{i=1}^{n} r_i x_i\right)$ ($\because$ M is freely Generated.

$= \sum_{i=1}^{n} r_i \psi(x_i)$

$= \sum_{i=1}^{n} r_i \psi'(x_i)$

$= \sum_{i=1}^{n} \psi'(r_i x_i)$

$\psi(m) = \psi'\left(\sum_{i=1}^{n} r_i x_i\right)$

$\psi(m) = \psi'(m)$

$\Rightarrow m \in S$

$\Rightarrow M \subseteq S$

but $S \subseteq M$

$\Rightarrow M = S$

$\Rightarrow \psi$ and ψ' are unique.

Linearly Independent & Dependent Set:

A set $\{m_1, m_2, \ldots, m_n\}$ in an R-module is called L.I. independent if

$r_1 m_1 + r_2 m_2 + \cdots + r_n m_n = 0$

$\Rightarrow r_i = 0 \quad \forall i$

and is called Linearly dependent if at least one

$r_i \neq 0$

---

c.o.N

Theorem:- Prove that every Irreducible R-module is Cyclic. (; R is a Ring with unity).

Proof:- Let M be Irreducible R-module Then only sub-module of M are M and $\{0\}$.

if $M = \{0\}$ Then it is cyclic.

if $M \neq \{0\}$

Then let $m_0 \in M$ and $m_0 \neq 0$

Let $A = \{rm_0 ; r \in R\}$

we Show that A is submodule of M.

Let $x, y \in A$

$x = r_1 m_0$, $y = r_2 m_0$; $r_1, r_2 \in R$

Then $x - y = r_1 m_0 - r_2 m_0$

$= (r_1 - r_2) m_0$

$x - y = r_3 m_0 \in A$; $r_3 = r_1 - r_2 \in R$

iii) Now $x \in A$ & $r \in R$

$\Rightarrow rx = r(r_1 m_0)$

$= (rr_1) m_0 = r_4 m_0 \in A$

Then $\Rightarrow$ A is Submodule of M.

$\because 1 \cdot m_0 = m_0 \quad ; 1 \in R$

$m_0 \in A$

$m_0 \neq 0 \quad \{A \neq \{0\}$

$\Rightarrow A = M$

$\therefore$ A is cyclic generated by m_0.

so M is cyclic generated by m_0.

Q# Every Abelian Group is a module over the Ring of Integers.

Proof:- Let A be an Abelian group under "+" defined on

$a \in A$ s.t

$a + a = 2a$

$a + a + a = 3a$

$a + a + a + \underbrace{\quad}_{n \text{ times}} + a = na$

with $0 \in A$ is identity and if n is -ve

Let $n = -m$

Then $na = (-m)a = -ma$

Then we know A is module over $\mathbb{Z}$

For this we have

I) $m(a+b) = ma + mb$ for $m \in M$ & $a, b \in A$

II) $(m+n)a = ma + na$ for $m, n \in M$ & $a \in A$

III) $m(na) = (mn)a$ for $a \in A$

IV) $1 \cdot a = a$

Theorem:- Let M be an R-module and let $\{m_1, m_2, \ldots, m_s\}$ be a finite subset of M. The following are equivalent.

1) $\{m_1, m_2, \ldots, m_s\}$ generate freely M.

2) $\{m_1, m_2, \ldots, m_s\}$ is linearly independent and generates M.

3) Every element $m \in M$ is uniquely expressible in the form of

$$\sum_{i=1}^{s} r_i m_i \quad \text{with } r_i \in R$$

4) Each m_i is torsion free and

$$M = Rm_1 \oplus Rm_2 \oplus \cdots \oplus Rm_s$$

Proof:- (1) $\Rightarrow$ (2) C.O.N

As M is freely generated by $\{m_1, m_2, \ldots, m_s\}$

It is true But it is linearly independent

Let $\sum_{i=1}^{s} r_i m_i = 0$

$$r_1 m_1 + r_2 m_2 + \cdots + r_s m_s = 0$$

Note that

$$N = R^R \oplus R^R \oplus \cdots \oplus R^R \quad (s \text{ times})$$

is an R-module under "+" & "·" defined as

$$(r_1, r_2, \ldots, r_s) + (t_1, t_2, \ldots, t_s)$$

$$= (r_1 + t_1, \ldots, r_s + t_s)$$

and

$$r(r_1, r_2, \ldots, r_s) = (rr_1, rr_2, \ldots, rr_s)$$

Let

f, $X \to$ be defined as

$X = \{m_1, m_2, \ldots, m_s\}$

$f(m_i) = e_i = (0, 0, \ldots, 1, 0, 0, \ldots, 0)$

"1" is at ith place.

Since M is freely generated. so that f can be extended to a module homomorphism say

$$\phi : M \to N$$

such that

$$f \circ I = \phi \quad (\text{Composition of } f \text{ and } I)$$

now $\phi(0) = 0$

$$\phi\left(\sum_{i=1}^{s} r_i m_i\right) = 0$$

$$\sum_{i=1}^{s} r_i \phi(m_i) = 0$$

$$\sum_{i=1}^{s} r_i (f \circ I)(m_i) = 0$$

$$\sum_{i=1}^{s} r_i \cdot f(I(m_i)) = 0$$

$$\sum_{i=1}^{s} r_i \cdot f(m_i) = 0 \quad \because I(m_i) = m_i$$

$$\sum_{i=1}^{s} r_i e_i = 0$$

$$r_i e_i = 0$$

$$\Rightarrow r_i = 0 \quad \because e_i \neq 0$$

$\forall\ i = 1, 2, \ldots s$

so $\{m_1, m_2, \ldots, m_s\}$ is linearly independent

(2) $\Rightarrow$ (3) e.o.N

Let $\{m_1, m_2, \ldots, m_s\}$ is linearly independent.

and $m = \sum_{i=1}^{s} r_i \cdot m_i$

& $m = \sum_{i=1}^{s} r_i' m_i$

be two expression

$$\sum_{i=1}^{s} r_i m_i = \sum_{i=1}^{s} r_i' m_i$$

$$\sum_{i=1}^{s} r_i \cdot m_i - \sum_{i=1}^{s} r_i' \cdot m_i = 0$$

$$\sum_{i=1}^{s} (r_i - r_i') m_i = 0$$

$\{m_1, m_2, \ldots, m_s\}$ is linearly independent

$\therefore r_i - r_i' = 0$

$r_i = r_i' \quad \forall i = 1, 2, \ldots, s$

$\Rightarrow$ Expression is unique.

(3) $\Rightarrow$ (4) c.o.N

Let $r \in R$ and $rm_i = 0$

also $0m_i = 0$

As expression is unique

$\therefore rm_i = 0m_i$

$\Rightarrow r = 0$

m_i is torsion free.

As

$Rm_i \subseteq M \quad \forall i$

$$\sum_{i=1}^{s} Rm_i \subseteq M \quad \text{---} (A)$$

now let $m \in M$

Then

$$m = \sum_{i=1}^{s} r_i m_i \qquad \exists r_i \in R$$

$\exists r_i \in R$

Then $r_i m_i \in Rm_i$

$$\sum_{i=1}^{s} r_i m_i \in \sum_{i=1}^{s} Rm_i$$

$$\Rightarrow m \in \sum_{i=1}^{s} Rm_i$$

$$\Rightarrow M \subseteq \sum_{i=1}^{s} Rm_i \quad \text{---} (B)$$

From (A) & (B)

$$M = \sum_{i=1}^{s} Rm_i$$

To Prove

$$Rm_i \cap \sum_{j \neq i} Rm_j = \{0\}$$

Let $m \in Rm_i \cap \sum_{j \neq i} Rm_j$

$m \in Rm_i$ and $m \in \sum_{j \neq i} Rm_j$

$m = r_i m_i$

and $m = \sum_{j \neq i} r_j m_j$

$m = 0 + 0 + \cdots + m + 0 + \cdots + 0$

and

$m = r_1 m_1 + r_2 m_2 + \cdots + r_{i-1} m_{i-1} + 0 + r_{i+1} m_{i+1} + \cdots + r_s m_s$

As Expression is unique

$\Rightarrow r_i = 0 \quad \forall i$

$\Rightarrow m = 0$

$\Rightarrow Rm_i \cap \sum_{j \neq i} Rm_j = \{0\}$

$\Rightarrow M = Rm_1 \oplus Rm_2 \oplus \cdots \oplus Rm_s$

(4) $\Rightarrow$ (3)

$M = Rm_1 \oplus Rm_2 \oplus \cdots \oplus Rm_s$

Then let $m = \sum_{i=1}^{s} r_i m_i$

and $m = \sum_{i=1}^{s} r_i' m_i$

$\Rightarrow \sum_{i=1}^{s} r_i' m_i = \sum_{i=1}^{s} r_i m_i$

$\sum_{i=1}^{s} (r_i' - r_i) m_i = 0$

$\Rightarrow (r_i' - r_i) m_i = 0$

$\because m_i$ is torsion free $\forall i$

$\therefore r_i' - r_i = 0$

$r_i' = r_i$

So Expression is unique.

$\because (3) \Rightarrow (2)$

Since each $m \in M$ has unique expression as

$m = \sum_{i=1}^{s} r_i m_i$

M is generated by $\{m_1, m_2, \ldots, m_s\}$

Let N be R-module and $\phi : A \to N$

be defined as

$\phi(m_i) = n_i \in N$

be a mapping from A into N

As $m \in M$ can be written as

$$m = \sum_{i=1}^{s} r_i m_i \quad ; r_i \in R$$

define $\psi : M \to N$ as

$$\psi(m) = \sum_{i=1}^{s} r_i m_i$$

As $\psi(0) = 0$

and let $m_1, m_2 \in M$

$$m_1 = \sum_{i=1}^{s} r_i m_i \quad ; \quad m_2 = \sum_{i=1}^{s} r_i' m_i$$

$$\psi(m_1 + m_2) = \psi\left(\sum_{i=1}^{s} r_i m_i + \sum_{i=1}^{s} r_i' m_i\right)$$

$$= \psi\left(\sum_{i=1}^{s} (r_i' + r_i) m_i\right)$$

$$= \sum_{i=1}^{s} (r_i' + r_i) m_i$$

$$= \sum_{i=1}^{s} r_i' m_i + \sum_{i=1}^{s} r_i m_i$$

$$\psi(m_1 + m_2) = \psi(m_1) + \psi(m_2)$$

Also for $r \in R$

$$\psi(rm) = \psi\left(r\left(\sum_{i=1}^{s} r_i m_i\right)\right)$$

$$= \psi\left(\sum_{i=1}^{s} (r r_i) m_i\right)$$

$$= \sum_{i=1}^{s} (r r_i) m_i$$

$$= r\left(\sum_{i=1}^{s} r_i m_i\right)$$

$\psi(rm) = r\psi(m)$

$\Rightarrow \psi$ is Homomorphism.

Clearly ψ is an extension of ϕ.

So M is freely generated by x.

Theorem:- Two Cyclic R module are Isomorphic iff they have same order ideal.

Proof:- Let Mand N be two Cyclic R-module. Let M is generated by "m"

Then $M = Rm$; $m \in M$

define a mapping

$\phi : R \longrightarrow M = Rm$ by

$\phi(r) = rm \quad \forall\, r \in R$

Then ϕ is onto:-

Let $m' \in M$

Then $m' = rm$ for some $r \in R$

$\therefore M$ is generated by m

So for $s \in R$ s.t

$\phi(s) = sm = m'$

ϕ is Homo:- Let $r, s \in R$

$$\phi(r+s) = (r+s)m$$
$$= rm + sm \quad \because m \text{ is module}$$
$$= \phi(r) + \phi(s)$$

by Property of module.

for any $t \in R$, $r \in R$

$$\phi(tr) = (tr)m = t(rm)$$
$$= t\phi(rm)$$

ϕ is Homo.

Then by fundamental Theorem of Homomorphism

$$\frac{R}{\ker\phi} \cong M$$

Now $\ker\phi = \{r \in R : \phi(r) = 0\}$

$$= \{r \in R : rm = 0\}$$

By definition of order Ideal

$$O(m) = \{r \in R : rm = 0\}$$

Then

$$\ker\phi = O(m)$$

Thus

$$\frac{R}{\ker\phi} \cong M$$

$$\Rightarrow \frac{R}{O(m)} \cong M$$

Similarly if $n \in N$ $\therefore N = R_n$

Then $\frac{R}{O(n)} \cong N$

Now suppose the two cyclic R-modules M and N have the same order ideal s.t $O(m) = O(n)$

$$M \cong \frac{R}{O(m)} = \frac{R}{O(n)} \cong N$$

$$\Rightarrow M \cong N$$

Conversely:-

Suppose $M \cong N$

Then M and N are strictly same and so they have same order ideal

Note $M = Rm$, $N = Rn$

Then $f(m) = n$ is homomorphism from $M \to N$

$$x \in O(m) \Leftrightarrow xm = 0$$

$$\Leftrightarrow f(xm) = f(0) = 0$$

$\because f$ is Homo.

$$\Leftrightarrow xf(m) = xn = 0$$

$\because f(m) = n$

$$\Leftrightarrow x \in O(n)$$

C. A. NOTES

Theorem:- Every Finitely Generated R-module is Homomorphic Image of free R-module.

Proof:- Let M be a Finitely Generated R-module generated by

$\{m_1, m_2, \ldots, m_n\}$

Let F be a free R-module generated by

$X = \{x_1, x_2, \ldots, x_n\}$

Let

$i : X \to F$

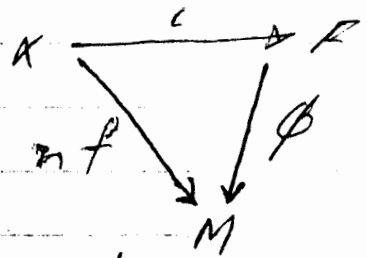
$i(x_i) = x_i$

and let inclusion map defined by

$f : X \to M$

$f(x_i) = m_i$

$\forall i = 1, 2, \ldots, n$



Since F is generated by X.

Therefore f an Homomorphism

$\phi : F \to M$

s.t $\phi i = f$

Since Image ϕ is a submodule of M and

$\{m_1, m_2, \ldots, m_n\} \subseteq \text{Im}\,\phi$

since $\sum x_i m_i \in \text{Im}\phi$ $x_i \in R, m_i \in M$

$\Rightarrow \phi_i = f$ $\forall m \in M$, $m = \sum_{i=1}^{n} x_i m_i$

$\therefore \phi(x_i) = x_i$

$\phi(\sum x_i m_i) = f(m_i)$

$\phi(x_i) = m_i \in \text{Im}\phi$

Therefore

$\text{Im}\phi = M$

Thus M is the Homomorphic Image of R.

Hence the Proof.

C.O.N before Converse.

Question:- M is freely Generated by 's' elements if and only if

$M \equiv R \oplus R \oplus \cdots \oplus R$ with s R's

Proof:- Let

$M \equiv (R^R)^S$ To Prove M is freely generated by s element

it will be Convenient to write $R^{R;S}$ for the external direct sum of R^R with itself "s" times, Let e_i denote the "s" tuple whose only non-zero coordinate is "1" in the sth Place,

$(R^R)^S = R^R \oplus R^R \oplus R^R \oplus \cdots \oplus R^R$ (S times)

i.e. $e_i = (0, 0, \ldots, 1, 0, \ldots, 0)$, 1 is at i^{th} place

If $x \in (R^R)^S$

Then

$$x = (r_1, r_2, \ldots, r_S) = \sum_{i=1}^{S} r_i e_i$$

and so

$(e_1, e_2, \ldots, e_S)$ generates $(R^R)^S$.

Since the set is clearly linearly independent, it generates $(R^R)^S$ freely.

Clearly any module isomorphic to a free module is freely generated by the same number of elements

So M is generated by S-element freely.

Conversely:- If M is freely generated by $\{m_1, m_2, \ldots, m_S\}$, then since

$\{e_1, e_2, \ldots, e_S\}$ generate $(R^R)^S$ freely

There exist Homomorphism

$\phi : M \to (R^R)^S$

and $\psi : (R^R)^S \to M$

defining $m_i \to e_i$ & $e_i \to m_i$

respectively.

Thus $\phi\psi$ maps e_i to e_i and so map every linearly combination of the e_i's to itself

Thus $\phi\psi$ is the identity map of M. Therfore each of ϕ and ψ is an isomorphism,

as required

so $M \equiv (R^R)^S$

Definition:- If M is a Cyclic R module over a Commutative ring R with 1, the order Ideal of any generator of M is called the order Ideal of M.

Theorem:- A Module M is Cyclic iff $M = Rx$ for some $x \in M$.

Proof:-

Let M is Cyclic Then let M is generated by some $x \in M$.

so for any $m \in M$ $r \in R$

s.t $m = rx$

so $M = \{rx : r \in R\}$ — (A)

As $r \in R$

$rx \in Rx \quad \forall r \in R$

$m \in Rx$; m is arbitrary

$M \subseteq Rx$

Now let $r' \in Rx$, Then $\exists$ some $r \in R$ s.t

$r' = rx \in M$ By (A)

$Rx \subseteq M$

$M = Rx$

Conversely:-

Let $M = Rx$

and let $m' \in M$ be arbitrary

Then $m' \in Rx$ so $\exists$ some $r' \in R$ s.t

$m' = r'x$

so for each $m \in M$ $\exists$ some $r \in R$ s.t

$m = rx$

i.e every element is linearly combination of x.

so M can be generated by a single element x.

so M is cyclic.

RING:-

A non-empty set R together with two binary operation usually '+' and '·' is called ring if.

1) (R, +) is abelian group under '+'

2) (R, ·) is semi group under '·'
(ie) '·' is closed and associative

3) Distributive laws holds

I) $a \cdot (b+c) = ab + ac$ (Left-Dist

II) $(a+b) \cdot c = ac + bc$ (Right-Dist

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

Then R is called ring written as $(R, +, \cdot)$.

Examples:- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$

Subring:-

Let $S \subseteq R$ and S is also ring Then S is called subring of R if

I) $a - b \in S \quad \forall a, b \in S$

II) $ab \in S$

Then S is called subring of R

Ideal:- A subring I of R is called ideal of R if for $a \in I, r \in R$

$ar \in I$ and $ra \in I$

OR Let $I \subseteq R$
Then I is called ideal
if $a-b \in I \quad \forall a,b \in I$
$ar \in I$ & $ra \in I \quad \forall a \in I, r \in R$.

Fields:- A non-empty set F having at least two elements along with two binary operations '+' and '.' is called Field if

1) $(F,+)$ is abelian group
2) $(F\setminus\{0\},\cdot)$ is abelian group
3) Left or Right distributive law holds

Then F is called field written as $(F,+,\cdot)$
e.g $(\mathbb{R},+,\cdot)$ is a field.

Construction of new Rings:-

Let $R_1, R_2, \ldots, R_n$ be a finite collection of rings Then Cartesian Product of R_i $(i=1,2,\ldots,n)$ defined as

$R_1 \times R_2 \times \cdots \times R_n = \{(r_1, r_2, \ldots, r_n) : r_i \in R_i$
$; i = 1,2,\ldots,n\}$

NOTE $A = \{a, b, c\}$
$B = \{e, f, g\}$

$A \times B = \{(x, y) : x \in A \wedge y \in B\}$ and is written as $R = \prod_{i=1}^{n} R_i$

Even if R is a ring under $+$ and $\cdot$ defined as

$x = (x_1, x_2, \ldots, x_n) \in R = \prod_{i=1}^{n} R_i$

$y = (y_1, y_2, \ldots, y_n) \in R = \prod_{i=1}^{n} R_i$

where $x_i, y_i \in R_i$; $i = 1, 2, \ldots, n$

$x + y = (x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n)$

$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$

and

$xy = (x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n)$

$x \cdot y = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$

so that $R = \prod_{i=1}^{n} R_i$ is ring

NOTE that $0 = (0, 0, \ldots, 0)_n$ is additive identity in $R = \prod_{i=1}^{n} R_i$

and $-(x_1, x_2, \ldots, x_n) = (-x_1, -x_2, \ldots, -x_n)$

is additive inverse of $(x_1, x_2, \ldots, x_n)$

Then this is called External Direct sum of ring $R_1, R_2, \dots R_n$ written as

$$R = R_1 \oplus R_2 \oplus R_3 \dots \oplus R_n$$

Internal Direct Sum:-

Let R be a ring and $\{I_i ; i = 1, 2, \dots n\}$ be the collection of finite numbers of Ideals of R. Then R is called internal direct sum of $I_i ; i = 1, 2, \dots n$

if I) $R = \sum_{i=1}^{n} I_i$

II) $I_i \cap \sum_{i \neq j} I_j = \{0\}$

NOTE we use same notation for External and internal direct sum ...

$R = I_1 \oplus I_2 \oplus \dots \oplus I_n$ is In External Direct Sum of R form Ideal direct Sum.

Examples:-

Let $\mathbb{Z}_{30} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{29}\}$

be a ring.

and $I = \{\bar{0}, \bar{15}\}$

$J = \{\bar{0}, \bar{10}, \bar{20}\}$

$K = \{\bar{0}, \bar{6}, \bar{12}, \bar{18}, \bar{24}\}$ are Ideals of $\mathbb{Z}_{30}$

Prove that $\mathbb{Z}_{30}$ is Internal Direct Sum of I, J and K.

Proof:-

$I + J$

+	0	10	20
0	0	10	20
15	15	25	5

$I + J = \{0, 5, 10, 15, 20, 25\}$

$I + J + K =$

+	$\bar{0}$	$\bar{6}$	$\bar{12}$	$\bar{18}$	$\bar{24}$
0	0	6	12	18	24
5	5	11	17	23	29
10	10	16	22	28	4
15	15	21	27	3	29
20	20	26	2	8	14
25	25	1	7	3	19

$I + J + K = \{0, 1, 2, \ldots, 29\}$

Hence

$I + J + K = \mathbb{Z}_{30}$ Condition (1) holds

now $(\bar{I}+J)\cap K = \{\bar{0}, \bar{5}, \bar{10}, \bar{15}, \bar{20}, \bar{25}\}$

$\cap \{\bar{0}, \bar{6}, \bar{12}, \bar{18}\}$

$(\bar{I}+J)\cap K = \{\bar{0}\}$

Similarly $\bar{I}\cap(J+K) = \{\bar{0}\}$

and

$(\bar{I}+K)\cap J = \{\bar{0}\}$

① and ② holds

Hence Z_{30} is Internal Direct Sum of $\bar{I}, J, K$

Examples:- Let $Z_2 = \{\bar{0}, \bar{1}\}$

$Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Then

$Z = Z_2 \times Z_3 \times Z_5$

$Z = Z_2 \oplus Z_3 \oplus Z_5$

Then Z is ring called External direct sum of Z_2, Z_3, Z_5

C.O.N

Example:- Prove that Z_6 is isomorphic to Direct sum of Z_2 and Z_3

$$Z_6 \cong Z_2 \oplus Z_3$$

NOTE $Z_2 = \frac{Z}{2Z}$ => left Cosets

& $Z_3 = \frac{Z}{3Z}$, $Z_6 = \frac{Z}{6Z}$

Proof:- Let $V_2 : Z \longrightarrow \frac{Z}{2Z}$

and $V_3 : Z \longrightarrow \frac{Z}{3Z}$

be the epimorphisms. (onto Homo.)

Now define

$$\phi : Z \longrightarrow Z_2 \oplus Z_3$$

as

$$\phi(n) = (V_2(n), V_3(n))$$

$$Z_2 \oplus Z_3 = Z_2 \times Z_3$$

ϕ is Homomorphism:-

Let $n_1, n_2 \in Z$

$$\phi(n_1 + n_2) = (V_2(n_1+n_2), V_3(n_1+n_2))$$

$$= (V_2(n_1) + V_2(n_2), V_3(n_1) + V_3(n_2))$$

$\because V_2$ & V_3 are Homo.

$$\phi(n_1+n_2) = (V_2(n_1), V_3(n_1)) + (V_2(n_2), V_3(n_2))$$

$$= \phi(n_1) + \phi(n_2)$$

now

$$\phi(n_1 n_2) = (v_2(n_1 n_2), v_3(n_1 n_2))$$

$$= (v_2(n_1)\cdot v_2(n_2), v_3(n_1) v_3(n_2))$$

$\because v_2$ & v_3 are Homo.

$$= (v_2(n_1), v_3(n_1)) \cdot (v_2(n_2), v_3(n_2))$$

$$\phi(n_1 n_2) = \phi(n_1)\cdot\phi(n_2)$$

Then ϕ is Homomorphism.

now for $\ker\phi$

if $n \in \ker\phi$

$\Leftrightarrow \phi(n) = (0_2, 0_3)$ where $0_2, 0_3$ are additive identity of Z_2 & Z_3

$\Leftrightarrow (v_2(n), v_3(n)) = (0_2, 0_3)$

$\Leftrightarrow v_2(n) = 0_2 \; ; \; v_3(n) = 0_3$

$\Leftrightarrow n \in \ker v_2 \; ; \; n \in \ker v_3$

$\Leftrightarrow n \in 2\mathbb{Z} \; ; \; n \in 3\mathbb{Z}$

$\Leftrightarrow n \in 2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$

~~$n \in \ker\phi$~~

$n \in \ker\phi \Leftrightarrow n \in 6\mathbb{Z}$

$\Rightarrow \ker\phi = 6\mathbb{Z}$

Then by Homomorphism Theorem

$$Z_6 = \frac{Z}{\ker \phi} \cong \text{Im}(\phi) = \phi(Z)$$

denote the image of Z

There are '6' elements in Z_6 - also $Z_2 \times Z_3$ contains '6' order pair of the form (a, b) in $Z_2 \oplus Z_3$ having 6 elements.

$$\Rightarrow \text{Im}\,\phi(Z) \cong Z_2 \times Z_3$$

$$\Rightarrow Z_6 \cong Z_2 \oplus Z_3$$ (by Fundamental of Isomorphism.)

Lemma:- Suppose that a ring R is the internal direct sum of its ideals $I_1, I_2, I_3, \ldots, I_n$. Then every element $r \in R$ has a unique expression of the form

$$r = r_1 + r_2 + \cdots + r_n$$

$r_i \in I_i$ $(i = 1, 2, \ldots, n)$

Proof:- As R is I.D sum of $I_1, I_2, \ldots, I_n$ Then

$$R = \sum_{(i)}^{n} I_i \quad \& \quad I_i \cap \sum_{j \neq i} I_j = \{0\}$$

$$R = I_1 + I_2 + \cdots + I_n$$

Let $x \in R$ Then x has at least one expression of the form.

$$x = r_1 + r_2 + \cdots + r_n \quad \text{---(1}$$

$$; r_i \in I_i \quad i = 1, 2, \ldots n$$

also let

$$x = s_1 + s_2 + s_3 + \cdots + s_n \quad \text{---(2}$$

$$s_i \in I_i$$

$$i = 1, 2, \ldots, n$$

be another expression of x.

(1) & (2) $\Rightarrow$

$$r_1 + r_2 + \cdots + r_{i-1} + r_i + r_{i+1} + \cdots + r_n$$

$$= s_1 + s_2 + \cdots + s_{i-1} + s_i + s_{i+1} + \cdots + s_n$$

$$; r_i \in I_i$$

$$s_i \in I_i$$

$$i = 1, 2, \ldots n$$

$$\therefore r_i - s_i = s_1 - r_1 + s_2 - r_2 + \cdots$$

$$\cdots + s_{i-1} - r_{i-1} + s_{i+1} - r_{i+1} + \cdots$$

$$\cdots + s_n - r_n$$

$$r_i \in I_i$$

$$s_i \in I_i$$

$$i = 1, 2, 3, \ldots n$$

$$r_i - s_i = \sum_{j \neq i}^{n} (s_j - r_j) \quad \text{---(3}$$

As $x_i, s_i \in I_i$ ——— (a

$i = 1, 2, 3, \ldots n$

$\Rightarrow x_i - s_i \in I_i$

also $s_j - t_j \in I_j$

$\sum_{j \neq i} (s_j - t_j) \in \sum_{j \neq i} I_j$

$\Rightarrow x_i - s_i \in \sum_{j \neq i} I_j$ ——— (b

by (a)

$\Rightarrow x_i - s_i \in I_i \cap \sum_{j \neq i} I_j = \{0\}$

(∵ R is I.D Sum)

$x_i - s_i = 0 \quad i = 1, 2, 3, \ldots n$

$x_i = s_i \quad i = 1, 2, 3, \ldots n$

$\Rightarrow x_1 = s_1$

$x_2 = s_2$

|

$x_n = s_n$

Hence expression is unique.

Polynomial:- An expression of the form

$$a_0 x^0 + a_1 x^1 + \cdots + a_n x^n$$

where $a_0, a_1, a_2, \ldots, a_n$ are constant and $a_n \neq 0$ where 'n' is non-negative integer is called polynomial of degree n denoted by $P(x)$, $f(x)$ or $C(x)$

Polynomial Ring:-

Let R be a ring Then a polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

can be written as

$f(x) = (a_0, a_1, a_2, \ldots, a_n)$

e.g. where $a_i \in R$

$2x^2 + 3 \Rightarrow 2x^2 + 0x + 3$

$f(x) = (2, 0, 3)$ ~~wrong~~ false

$f(x) = (3, 0, 2)$ ✓ Correct

Then $f(x)$ is called polynomial over R

now if $R[x]$ is the collection of all polynomial defined on R

Then $R[x]$ is a ring under some operation $(+, \cdot)$ of

Polynomial, called polynomial Ring.
in one indeterminate x.

Addition of Polynomial

if $f(x) = a_0 + a_1x + a_2x + \cdots + a_nx^n$
$; a_n \neq 0$
and
$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$
$; b_m \neq 0$
be two polynomial of degree n & m
Then their sum is defined as

$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots$

$$= \sum_{i=0}^{\max(m,n)} (a_i + b_i)x^i$$

e.g $f(x) = 2x^3 + 3x^2 + 5x + 6$
$g(x) = 3x^5 + 2x^4 + 3x^3 + 2x^2 + x + 1$;

$f(x) + g(x) = (3+0)x^5 + (2+0)x^4 + (3+2)x$

clearly The sum of two polynomials over R is also a polynomial over R.

Multiplication of Polynomial

If $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$; $a_n \neq 0$

$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$; $b_m \neq 0$.

Then the Product

$f(x)\cdot g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + \cdots + (a_nb_m)x^{n+m}$

$\Rightarrow f(x)\cdot g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_rx^r$

where

$c_r = a_0b_r + a_1b_{r-1} + a_2b_{r-2} + \cdots + a_rb_0$

Degree of Polynomial :-

The highest power of the variable x whose co-efficient is not zero is called degree of Polynomial.

Zero Polynomial :-

A polynomial in which $a_i = 0\ \forall i$ is called Zero polynomial. its degree can never be defined.

$\because 0 = 0 + 0x + 0x^2 + 0x^3 + 0x^4 + \cdots$

Constant Polynomial,-

A polynomial consists only one constant term i-e is which degree of polynomial is zero is called constant polynomial.

degree of polynomial is denoted by

$$\deg(f(x)) = \deg f \text{ or } \partial f$$

☆ **Lemma:-** if $P, q \in R[x]$ Then

1) $\deg(P+q) \leq \max(\deg P, \deg q)$

2) $\deg(Pq) \leq \deg P + \deg q$

3) if R is an Integral domain Then

$$\deg(Pq) = \deg P + \deg q.$$

Proof:- 1) Let $P = r_0 + r_1 x + r_2 x^2 + \cdots + r_n x^n$

$q = s_0 + s_1 x + s_2 x^2 + \cdots + s_m x^m$

; $r_n \neq 0$

$s_m \neq 0$

be The polynomial of degree n & m

Let $l = \max(m, n)$

Then $P+Q = \sum_{i=0}^{\max(m,n)} (r_i + s_i) x^i$

$$P+Q = \sum_{i=0}^{l} (r_i + s_i) x^i$$

$\Rightarrow \deg(P+Q) \leq l$

~~$\Rightarrow \deg(P+Q) = \max(\deg P, \deg Q)$~~

$\Rightarrow \deg(P+Q) \leq \max(\deg P, \deg Q)$

II) Now

$$PQ = r_0 s_0 + (r_0 s_1 + r_1 s_0) x + \cdots + r_n s_n x^{n+m}$$

now it may be possible that $r_n s_n \neq 0$ (in case of ~~modulo~~ multiplication)

$\Rightarrow \deg(PQ) \leq n+m$

$$\deg(PQ) \leq \deg P + \deg Q$$

III) if R is an integral domain

then $r_n s_m \neq 0 \iff r_n \neq 0, s_m \neq 0$

$\Rightarrow \deg(PQ) = n+m$

$$\deg(PQ) = \deg P + \deg Q.$$

Division Algorithm:-

Theorem:- Let $a, b \in K[x]$ and $b \neq 0$

Then there exist $q, r \in K[x]$ such that $a = bq + r$ with

$r = 0$ OR $\deg(r) < \deg(b)$

moreover q & r are unique.

Proof:- The Proof of existence of q & r is followed by induction on degree of a.

if a is zero

Then $0 = 0b + 0$

$\Rightarrow q = 0 \quad r = 0 \quad ; b \neq 0$

& $\deg r < \deg b$

now suppose that it is true for the polynomial when

$$\deg a \leq n-1$$

Let $a = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \quad ; a_n \neq 0$

and $b = b_0 + b_1 x + b_2 x^2 + \cdots + b_\ell x^\ell \quad b_\ell \neq 0$

Consider

$$a - a_n b_\ell^{-1} x^{n-\ell} b = c \ (\text{say}) \quad \text{---(A)}$$

we arrange matter so that degree of c is $\leq n-1$

Precisely

$$\deg c = n-1$$

Then by supposition $\exists\ q_0$ & $r \in K(x)$

$$c = bq_0 + r \qquad \deg r < \deg b$$

---(B)

(A) $\Rightarrow$ $a = a_n b_\ell^{-1} x^{n-\ell} b + c$

using value of c.

$$a = a_n b_l^{-1} x^{n-l} b + bq_0 + r$$

$$a = b(a_n b_l^{-1} x^{n-l} + q_0) + r$$

$\deg r < \deg b$

$$a = bq + r \quad ; \deg r < \deg b$$

$$a = bq + r \quad ; \deg r < \deg b$$

where $q = a_n b_l^{-1} x^{n-l} + q_0$

For uniqueness:-

Let $a = bq + r \quad \deg r < \deg b$

$a = bq' + r' \quad \deg r' < \deg b$

$$\Rightarrow bq + r = bq' + r'$$

$$b(q - q') = r' - r \quad \text{——} (c)$$

$$\deg(b(q - q')) = \deg(r' - r)$$

$$\deg(r' - r) \leq \max(\deg r', \deg r)$$

but

$$\Rightarrow \deg(r' - r) < \deg b \quad \because \deg r < \deg b \text{ & } \deg r' < \deg b$$

$$\Rightarrow \deg(b(q - q')) < \deg b \quad \text{——} (1)$$

$= \deg(r - r')$
$< \deg b$

$\Rightarrow$ also

$$\deg[b(q-q')] \leq \deg b + \deg(q-q')$$

As K is a field

$$\deg[b(q-q')] = \deg b + \deg(q-q')$$

using in (2) we get

$$\deg b + \deg(q-q') < \deg(b)$$

$\Rightarrow \deg(q-q') < 0$

it holds only ~~$\deg(q-q') > 0$~~

if $q-q'$ is zero polynomial

i.e $q-q' = 0$

$q = q'$ put putting in (1)

(1) $\Rightarrow$ $0 = r'-r$

$\Rightarrow r' = r$

So ~~expression~~ q & r are unique.

Remainder Theorem:-

Let $c \in K$ and $a(x) \in K[x]$ if $a(x)$ is divided by $x-c$ Then remainder is $a(c)$.

Proof:- Let $b(x) = x-c \neq 0$

Then $\exists\ q(x), r(x) \in K[x]$

s.t. $a(x) = b(x)q(x) + r(x)$

$\deg r < \deg b$

$a(x) = (x-c)q(x) + r(x)$

$\deg r < 1 \Rightarrow \deg r = 0$

$\therefore \Rightarrow r$ is Constant ∵ Here $\deg b = 1$

Putting $x = c$

$a(c) = (c-c)q(c) + r(c)$

$a(c) = r(c)$ (where $r(c)$ is remainder

$\Rightarrow$ Remainder $= r(c) = a(c)$

---

* Zeros of The Polynomial

These elements $c \in K$ are called zero's of the polynomial $p(x) \in K[x]$ for which

$$p(c) = 0$$

e.g $p(x) = x^2 - 1$

$c = \pm 1$ are zero of $p(x)$

* Roots of The Equations -

Root of an equation $p(x) = 0$ are those elements $c \in K$ for which $p(c) = 0$

Here c is root of $p(x) = 0$

Conversely:- Let $x-c$ is factor of $a(x)$, $a(x) \in K[x]$
Then $a(x) = (x-c)q(x)$ — (1) for some $q(x) \in K[x]$
put $x = c$ in (1)
$\Rightarrow a(c) = (c-c)q(c)$
$\Rightarrow a(c) = 0$.
$\Rightarrow x = c$ is the root of $a(x) = 0$

Factor Theorem:-

The polynomial $x-c$ is a factor of a polynomial $a(x) \in K[x]$.

iff

$x = c$ is root of $a(x) = 0$

Proof:- As for $a(x) \in K[x]$
There exist $q(x)$ and $r(x)$
$a(x) = (x-c)q(x) + r(x)$
where $\deg r(x) < \deg(x-c)$
$\deg r(x) < 1$
$\Rightarrow r(x)$ is constant say R
$a(x) = (x-c)q(x) + R$ —— (2)
where R is Remainder
If $x = c$ is root of $a(x) = 0$
Then $a(c) = 0$.

1) $\Rightarrow a(c) = (c-c)q(c) + R$

$0 = 0 + R \Rightarrow R = 0$

Then (2) becomes
$a(x) = (x-c)q(x)$
Then $(x-c)$ is a factor of $a(x)$

Conversely:-
Let $x-c$ is a factor of Then $a(x) = (x-c)q(x)$
$\Rightarrow a(c) = 0$
$x = c$ is root of $a(x) = 0$

Theorem:- A polynomial $f(x) \in K[x]$ of degree $n \geq 0$ has at most n distinct roots in K.

Proof:- Let $c_1, c_2, \ldots, c_k$ be the k distinct roots of $f(x)$ in K firstly we Show that by induction that

$(x-c_1)(x-c_2)\ldots(x-c_k)$ divide $f(x)$

For $k=1$

i.e c_1 is root of $f(x)$

Then $x-c_1$ divide $f(x)$

So $f(x) = (x-c_1)q(x)$

$c=1$ is satisfied

We Suppose that

$(x-c_1)(x-c_2)\ldots(x-c_i)$ divide $f(x)$ & $i<k$

Then

$f(x) = (x-c_1)(x-c_2)\ldots(x-c_i)q(x)$ for some $q(x)$

As

c_{i+1} is root of $f(x)$

Then

$(c_{i+1}-c_1)(c_{i+1}-c_2)\ldots(c_{i+1}-c_i)q(c_{i+1}) = 0$

Since $c_1, c_2, \ldots, c_k$ are distinct

Then $(c_{i+1}-c_i) \neq 0 ; 1 \leq i < k$

Here $q'(x) \neq \frac{d}{dx}(q(x))$ does not mean

$\Rightarrow q'(c_{i+1}) = 0$

c_{i+1} is root of $q'(x) = 0$

$\Rightarrow x - c_{i+1}$ is factor of $q(x)$

Then $q'(x) = (x - c_{i+1}) q''(x)$

for some $q''(x)$

Then

$q(x) = (x-c_1)(x-c_2) \cdots (x-c_i)(x-c_{i+1}) (q''(x))$

$\Rightarrow (x-c_1)(x-c_2) \cdots (x-c_i)(x-c_{i+1})$ divides $q(x)$

So $(x-c_1)(x-c_2) \cdots (x-c_k)$ divide $q(x)$ by induction

$\therefore q(x) = (x-c_1)(x-c_2) \cdots (x-c_k) q'''(x)$

for some $q'''(x)$

now

$\deg q(x) = \deg [(x-c_1)(x-c_2) \cdots (x-c_k) q'''(x)]$

K is a field

$\deg q(x) = \deg (x-c_1) + \deg (x-c_2) + \cdots + \deg (x-c_k) + \deg q'''(x)$

$n = 1 + 1 + 1 \cdots + 1 (k\text{-factors}) + \deg q'''(x)$

$n \geq k + \deg g''(x)$ $\because g''(x) \neq 0$
or $\deg g''(x) \geq 0$

$n \geq k$
$\Rightarrow$ no. of distinct roots of $f(x)$ of $m \geq k$ are at most n.

Existence Theorem:-

every polynomial $f(x) \in C[x]$ of degree $n \geq 1$ has at least one root in C.

Theorem:- Every polynomial $f(x) \in C[x]$ of degree $n \geq 1$ has a root over C.

Proof:- Let
$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$
be a nth degree polynomial; $a_n \neq 0$ in $C[x]$. Then by existence of Theorem. The $f(x)$ has at least one root (α_1) c_1 in C.
Then
$f(x) = (x - c_1) g_1(x)$ — (1)
and $g_1(x)$ is polynomial of $\deg g_1(x) = n-1$

Again by existence Theorem,

$q_1(x)$ has at least one root (say) c_2 in F

Then

$$q_1(x) = (x - c_2)\, q_2(x) \quad \text{---(2}$$

for some $q_2(x)$

2) $\Rightarrow$ $f(x) = (x - c_1)(x - c_2)\, q_2(x)$

---(3

and

$\deg q_2(x) = n - 2$

Again by substance, Theorem the $q_2(x)$ has at least one root (say) c_3 in F

Then

$$q_2(x) = (x - c_3)\, q_3(x)$$

(3) $\Rightarrow$ $f(x) = (x - c_1)(x - c_2)(x - c_3)\, q_3(x)$

& $\deg q_3(x) = n - 3$

by continuing this process after n the step we get

$$f(x) = (x - c_1)(x - c_2)(x - c_3) \cdots (x - c_n)\, q_n(x)$$

with

$$\deg q_n(x) = n - n = 0$$

i.e

$q_n(x) = \alpha$ where α is a constant

Then

$$f(x) = a(x-c_1)(x-c_2)\cdots(x-c_n)$$

So $f(x)$ has n distinct root in F.

2nd Statement - of above Theorem; every polynomial of deg n in $C[x]$ can be divided into 'n' linear factors.

Theorem:- Let $f(x) \in F[x]$ of degree $n > 0$ and leading co-efficient of $f(x)$ is "a".

If $c_1, c_2, \ldots, c_n$ be the "n" distinct roots of $f(x)$ Then

$$f(x) = a(x-c_1)(x-c_2)\cdots(x-c_n)$$

Proof:- We Prove it by induction for $n=1$

Then $f(x) = ax + a_1$ — (1

and c_1 be its root

Then $0 = f(c_1) = ac_1 + a_1$

Then $0 = f(c_1) = ac_1 + a_1$

$$ac_1 + a_1 = 0$$

$$a_1 = -ac_1$$

Note: leading co-efficient means the co-efficient of higher degree power of x i.e co-efficient of dagree term.

$\therefore c_1, c_2, \ldots, c_k, c_{k+1}$ are distinct

$\Rightarrow f(c_j) = 0$; $j = 2, 3, 4, \ldots, k+1$

$\Rightarrow c_2, c_3, c_4, \ldots, c_k, c_{k+1}$

are k roots of $f(x)$

Then by ~~Suppositin~~ Induction Hypothesis

$$f(x) = a(x-c_2)(x-c_3)\cdots(x-c_{k+1}) \quad \text{---(4)}$$

Using (4) in (2)

$$f(x) = a(x-c_1)(x-c_2)\cdots(x-c_{k+1})$$

Hence result is true for all $n \geq 0$

Integral Domain:-

A Commutative ring R with identity element is called an Integral domain if it has no zero divisor.

i-e

$$x_1 \cdot x_2 = 0$$

$$\Rightarrow x_1 = 0 \text{ or } x_2 = 0$$

OR

$$x_1 \neq 0 \text{ & } x_2 \neq 0$$

$$\Rightarrow x_1 x_2 \neq 0$$

1) $\Rightarrow$ $d(x) = ax - ac_1$

$d(x) = a(x - c_1)$

for $n=1$ it is true

next suppose that result is true for $n=k$

i.e $d(x) = a(x-c_1)(x-c_2)\cdots(x-c_k)$

now suppose that $d(x)$ is of degree $k+1$ and $c_1, c_2, \ldots, c_k, c_{k+1}$ be its roots with 'a' as its leading coefficient.

As c_1 is root of $d(x)$

Then $d(x) = (x-c_1)g(x)$ — (2

where $g(x)$ is polynomial of deg k

and for c_j ; $1 < j \leq k+1$

2) $\Rightarrow$ $d(c_j) = (c_j - c_1)g(c_j)$ — (3

where c_j ; $1 < j \leq k+1$ are roots of $d(x)$

$\Rightarrow d(c_j) = 0$; $1 < j \leq k+1$

3) $\Rightarrow$ $0 = (c_j - c_1)g(c_j)$

$1 < j \leq k+1$

$c_j - c_1 \neq 0$

$1 < j \leq k+1$

Proof:- Let s/t

Then $t = xs$ for some $x \in R$

As $xR \subseteq R$; $x \in R$

$s(xR) \subseteq sR$

$(sx)R \subseteq sR$ for $s \in R$

$(xs)R \subseteq sR$

$tR \subseteq sR$ $\because sx = xs$

$\because R$ is L.D.

Conversely:-

Let $tR \subseteq sR$

$t \in tR \subseteq sR$

Then $t \in sR$

$t = sx$ for some $x \in R$

$\Rightarrow s/t$

NOTE
$sR \subseteq 2R$
as
$s \in 2\mathbb{Z}$
$\Rightarrow 2/s$

---

2) Let u is unit

$\Rightarrow u/1$

By part 1) $uR \supseteq 1 \cdot R$

$i.e.\ 1R \subseteq uR$ —(1

Obviously

$uR \subseteq R$ for $u \in R$ —(2

(1) & (2) $\Rightarrow$

$R = uR$

Conversely:- Let $R = uR$

$\because 1 \in R$

Then $1 \in uR$

$\Rightarrow 1 = ur$ for some $r \in R$

$\Rightarrow u/1$

Then u is unit

3) U = Set of units of R

$U = \{u \in R : uv = 1 \text{ for some } v \in R\}$

i) Let $u_1, u_2 \in U \subseteq R$

$u_1 v_1 = 1$, $u_2 v_2 = 1$

for some $u_1, v_2 \in R$

Consider

$(u_1 u_2)(v_1 v_2) = (u_1 v_1)(u_2 v_2)$

$\because u_1, u_2, v_1, v_2 \in R$

$\because R$ is I.P

$= 1 \cdot 1$

$= 1$

$(u_1 u_2)(v_1 \cdot v_2) = 1$

$\Rightarrow u_1 u_2 \in U$ closure law holds.

ii) Associative law holds in U as it is subset of R.
& associative law holds in R.

iii) As $1 \in R$ and $1 \cdot 1 = 1$

So $1 | 1$

$\Rightarrow 1 \in U$

iv) As for $u \in U$

Then $\exists\ v \in R$

such that $uv = 1$

So v is inverse of u.

also $v | 1 \Rightarrow v \in U$

Gaussian Integer :- And Ring of Gaussian Integer :-

The Integer of the form $a+ib$ where $a, b \in \mathbb{Z}$ are called Gaussian integers and set of Gaussian Integer form the structure of Ring under the addition and multiplication of complex number.

i.e $\mathbb{Z}[i] = \{a+ib : a, b \in \mathbb{Z}\}$

Divisor if $r, s \in R$ where R is integral domain then we say 'r' divides s written as r/s if $\exists\ t \in R$ such that $s = rt$.

Units of Ring :-

if R is an Integral domain (I.D) then a unit of R is defined as divisor of 1 i.e. $U \in R$ is called unit of R if $U/1$

i.e $Ur = 1$ for some $r \in R$

Associates:- Let R be an I.D then the elements $r, s \in R$ are said to be associates if r/s and s/r

Result:- If $a \in R$ where R is (I.D) and U is unit of R. Then U/a

Proof:- Since U is unit

$U \cdot V = 1$ for some $v \in R$

$\therefore a = 1 \cdot a$

$= (U \cdot V) a$

$= U (Va)$

$a = uw \quad \because w = va \in R$

$\Rightarrow U/a$

~~$\in \cdot 0 \cdot N(P \cdot U)$~~

1st Lemma:- Let R be an I.D (Integral Domain) Then

1) s/t iff $sR \supseteq tR$

2) u is a unit iff $uR = R$

3) The Set U of units is an abelian group under multiplication and if $u \in U$ and v/u Then $v \in U$

4) The Relation "a is an associate of" is an equivalence Relation denoted by "$\sim$" (Tilda)

5) Two elements a and b are associates iff $a = ub$ for some unit.

As $n(\alpha_1), n(\alpha_2)$ are +ve integer

Then

$$n(\alpha_1) = 1, 2, 4$$

if $n(\alpha_1) = 1$ α_1 is unit

Contradiction

if $n(\alpha_1) = 4$

Then $n(\alpha_2) = 1$

so α_2 is unit

A contradiction

now if $n(\alpha_1) = 2$

Let $\alpha_1 = a + b\sqrt{-5}$

$$n(\alpha_1) = a^2 + 5b^2 = 2$$

$$a^2 + 5b^2 = 2$$

This equation has no solution in $\mathbb{Z}$

so $n(\alpha_2) \neq 2$

Then 2 is irreducible

Similarly we can show

$3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible

Since unit of R has norm 1,

Then associate element has equal norm.

$N(u) = 1$

$|u|^2 = 1$

$a^2 + 5b^2 = 1 \quad ; a, b \in \mathbb{Z}$

It holds only if $a^2 = 1, \ b^2 = 0$

$\Rightarrow a = \pm 1$

So only units of R are $1, -1$

Now as

$6 = 6 + 0\sqrt{-5} \in R$

and

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

$1 \cdot 2 \cdot 3 = 1 \cdot (1+\sqrt{-5})(1-\sqrt{-5})$

We claim that four elements $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible in R

Otherwise Suppose

$2 = \alpha_1 \cdot \alpha_2$

where $\alpha_1, \alpha_2 \in R$

and both α_1, α_2 are non-unit

$N(2) = N(\alpha_1 \alpha_2)$

$4 = N(\alpha_1) \cdot N(\alpha_2)$

$\Rightarrow N(\alpha_1) \cdot N(\alpha_2) = 4$

Then 2 is not associate to any one of $1+\sqrt{-5}$, $1-\sqrt{-5}$, ~~are Then non is not equal and Then non is equal~~

$\because N(2) = 4$

$N(1+\sqrt{-5}) = 6$

$N(1-\sqrt{-5}) = 6$

$4 \neq 6$

So UR_2 also not hold

R is not UFD.

Definition:- Prime:-

An element p of an Integral domain R is called Prime in R if

1) p is neither zero nor a unit.

2) when $a, b \in R$ and $p \mid ab$ Then either

$p \mid a$ or $p \mid b$

Proposition:- Let R be an Integral domain. Then in R every Prime is irreducible.

Proof:- Let p be a Prime in R Then p is not zero and not unit and Suppose

$p = ab$ — (1) $\Rightarrow p/ab$

Then since p is Prime

p/a or p/b

if p/a

$a = pc$ for some $c \in R$

using in (1)

$p = (pc)b$

$p = p(cb)$

$1 = cb \Rightarrow bc = 1 \quad b \in R$

$\Rightarrow b/1 \quad c \in R$

$\Rightarrow b$ is unit

Similarly

if p/b Then

we can Show that a is unit

So p is irreducible.

Counter Example:-

If

$R = \{a + b\sqrt{-5} \; , \; a, b \in \mathbb{Z}\}$

2 is not prime in R

As $2/6$

$\Rightarrow 2/(1+\sqrt{-5})(1-\sqrt{-5})$

v) Commutative law holds in U as it holds in R & $U \subseteq R$

Hence U is abelian group under multiplication.

b) now if $u \in U$ and v/u

Then

$u = vv'$ for some $v' \in R$

and $u/1$

$u \cdot w = 1$

Consider

$v(v'w) = (vv')w$

$= u \cdot w = 1$; $v'w \in R$

$\Rightarrow v/1$

$\Rightarrow v \in U$

(v) Let Relation being associate is denoted by '$\sim$'

1) '$\sim$' is Reflexive :-

$a = a \cdot 1$

$\Rightarrow a/a$ & a/a

$a \sim a$

2) '$\sim$' is Symmetric :-

if $a \sim b$

$\Rightarrow a/b$ & b/a

$\Rightarrow b/a$ and a/b

$\Rightarrow b \sim a$

c) '$\sim$' is Transitive:-

if $a \sim b$ and $b \sim c$

as $a \sim b$

$\Rightarrow a/b$ and b/a

also $b \sim c$

$\Rightarrow b/c$ and c/b

$\Rightarrow a/b$ and b/c

also b/a & c/b

$\Rightarrow a/c$ also c/b and b/a

$\Rightarrow a/c$ also c/a

$\Rightarrow a \sim c$

---

5) $a \sim b$ iff $a = ub$ for some u is unit: $u \in R$

Proof. Let $a \sim b$

$\Rightarrow a/b$ and b/a

$b = ua$ for some u.

& $a = vb$ for some $v \in R$

$a = v(ua)$

$a = (vu)a$

$1 = u \cdot v \qquad u \cdot v = v \cdot u$

$\Rightarrow v \mid 1$; v is unit

For which $a = vb$

replacing u by v

$a = ub$

Conversely:- — (I)

Let $a = ub$ for some u

$\Rightarrow b \mid a$

$\because u$ is unit

$\Rightarrow u \mid 1$

$\Rightarrow u \cdot v = 1$ for some $v \in R$

now

$va = v(ub)$ by using (I)

$= (vu)b$

$= (uv)b \quad \because u \cdot v = v \cdot u$

$= 1 \cdot b$

$va = b$

$\Rightarrow a \mid b$

$\Rightarrow a \sim b$

Theorem:- If R is an I.D then $R[x]$ is also Integral domain.

Proof:-

As R is a Ring and $R[x]$ is also a ring under the addition and multiplication defined as in Complete

Irreducible Element:-

Let R be an I.D. an element $x \in R$ is called irreducible in R. if

i) $x \in R$ is not a unit (i.e $x \neq 1$ ($\because x.1 = 1$ for ever)

ii) when $x = ab$

Then either a is unit or b is unit (i.e if $a/1$ or $b/1$).

Irreducible polynomial over field

Let F be a field and $f(x) \neq 0$ and non-unit poly in $F[x]$. Then $f(x)$ is said to be irreducible over F if it has no proper divisor (or factor) in $F[x]$ and it is reducible if it has Proper divisor (factor) in $F[x]$.

Monic Polynomials:-

A polynomial is called monic if its leading co-efficient is 1.

define $d: \mathbb{Z}^* \to \mathbb{Z}_{\geq 0}$

$$d(a) = |a|$$

ED-I

$a, b \in \mathbb{Z}^* \Rightarrow a \neq 0, b \neq 0$

and $a/b \Rightarrow b = ac$ for $c \in \mathbb{Z}$

$\Rightarrow |b| = |ac|$

$|b| = |a||c|$

$|a| \leq |b| \quad \because |c| \geq 1$

$d(a) \leq d(b)$

ED-II if $a = 0$ & $b \neq 0$

Then $0 = b \cdot 0 + 0$

$\Rightarrow q = 0, r = 0$

if $d(a) < d(b)$

Then

$a = b \cdot 0 + r$

$a = r \qquad q = 0$

$r = a$

$\Rightarrow d(r) = d(a) < d(b)$

$d(r) < d(b)$

if $d(a) \geq d(b)$

Then

$a = bq + r$ with $0 \leq r < b$

either $r = 0$

or $d(a) \leq d(b)$

Hence $\mathbb{Z}$ is Euclidean Domain.

Ex If K is field.

Then $K[x]$ is E.D

$\therefore K[x]$ is E.D

$d : K[x] \to \mathbb{Z}_{\geq 0}$

$d(f(x)) = \deg(f(x))$

Ex If K is field Then $K[x]$ is E.D (Euclidean Domain)

Proof:- As $K[x]$ is I.D (Integral Domain)

we define

$d : K^*[x] \to \mathbb{Z}_{\geq 0}$

$d(f(x)) = \deg(f(x))$; $K^* = K - \{0\}$

$\forall f(x) \in K^*[x]$

E.D, Let $g, h \in K^*[x]$

$g \neq 0$, $h \neq 0$

and g/h

Then $h = gf$ for some $f \in K^*[x]$

now

$d(h) = d(gf)$

$= \deg(gf)$

$d(h) = \deg(g) + \deg f$

$d(h) \geq \deg(g)$

$d(g) \leq d(h)$

Unique Factorization Domain:-

U.F.D

An Integral Domain R is called U.F.D OR some time Gaussian Domain if

UF$_1$ every element $r \in R^*$ $[R^* = R - \{0\}]$, can be written in the form.

$r = u a_1 a_2 \cdots a_n$

where u is a unit of R and a_i, $i = 1, 2, \cdots, n$ are irreducible in R.

UF$_2$ if

$u a_1 a_2 \cdots a_n = u' b_1 b_2 \cdots b_m$

where u and u' are units in R and a_i, $i = 1, 2, \cdots, n$, b_j, $j = 1, 2, \cdots, m$ are irreducible in R

Then

$n = m$

and $a_i \sim b_j$ for some j.

Q# Show that $\mathbb{Z}[\sqrt{-5}]$

$R = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

is not a U.F.D.

Solⁿ Let $a+b\sqrt{-5}$, $c+d\sqrt{-5}$ are two elements in R. Then

1) $(a+b\sqrt{-5}) - (c+d\sqrt{-5})$
$= (a-c) + (b-d)\sqrt{-5} \in R$

$(a+b\sqrt{-5})(c+d\sqrt{-5})$
$= (ac-5bd) + (ad+bc)\sqrt{-5}$
$\in R$

i.e. $x+y\sqrt{-5} \in R$; $x, y \in \mathbb{Z}$

2) $1 = 1 + 0\sqrt{-5}$ $\quad 0 \in \mathbb{Z}$
$1 \in R$

As $R \subseteq \mathbb{C}$

& R is Integral Domain

now we define

$N : R \longrightarrow \mathbb{Z}_{\geq 0}$; $\mathbb{Z}_{\geq 0} = \mathbb{Z}^+ \cup \{0\}$

as

$N(\alpha) = |\alpha|^2$

Then N has Property

$N(\alpha\beta) = N(\alpha) N(\beta)$.

now Let $U \in R$ be a unit Then

$U \cdot V = 1$ for some $V \in R$

$N(U \cdot V) = N(1)$ $\quad (|u|^2 = 1 \Rightarrow |u| = 1)$

$N(U) \cdot N(V) = 1$

$\Rightarrow N(U) = 1$, $N(V) = 1$

but if $U = a + b\sqrt{-5}$

$\alpha - \beta\gamma = \delta$ For suitable values of γ & δ

$\alpha = \delta + \beta\gamma$

with $|\delta| = \frac{1}{\sqrt{2}}|\beta|$

$\Rightarrow |\delta| < |\beta|$

$|\delta|^2 < |\beta|^2$

$\Rightarrow d(\delta) < d(\beta)$

Hence Proved.

Different

Show That $\mathbb{Z}$ is Principle Ideal Domain.

Proof:- First we Show that each sub-ring of the form

$n\mathbb{Z} = \{na, a \in \mathbb{Z}\}$

Let S is any sub-ring of $\mathbb{Z}$

If $S = \{0\}$ Then $S = 0\mathbb{Z}$

ii) If $S \neq \{0\}$

Then S Contains some non-zero element say s.

As S is sub-ring so it Contains $-s$.

Then one of s or $-s$ is the integer.

* now any set of +ve integers contains a smallest integer say n.
i.e $n \in S$. (i.e n is the smallest integer of S)
we claim that

$$S = n\mathbb{Z}$$

Let $na \in n\mathbb{Z}$ for some $a \in \mathbb{Z}$
Then

$$na = (n+n+\text{---}+n) \text{ a times}$$

Since S is sub-ring
and $n \in S$; $a \in \mathbb{Z}$

$$(n+n+\text{---}+n) = na \in S$$
(a times)

$$\Rightarrow n\mathbb{Z} \subseteq S \quad \text{---} (1$$

As $s \in S$ and $n \in S$
Then

$$s = nq + r \quad ; \quad 0 \le r < n$$
$$\Rightarrow r = 0 \quad \because n \text{ is smallest}$$

$$s = nq \qquad q \in S \ \& \in \mathbb{Z}$$

$$s = nq \in n\mathbb{Z}$$
$$\Rightarrow s \in n\mathbb{Z}$$
$$S \subseteq n\mathbb{Z} \quad \text{---} \quad (2)$$

From (1) & (2)

$$S = n\mathbb{Z}$$

now since clearly ($\because$ I is ideal $\Rightarrow IR \subseteq I$)

$$(n\mathbb{Z})\mathbb{Z} \subseteq n\mathbb{Z}$$

$\Rightarrow n\mathbb{Z}$ is Ideal of $\mathbb{Z}$ generated by n.

define $d : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$

$$d(\alpha) = |\alpha|^2 = a^2 + b^2$$

E.D.1 :-

If $\alpha, \beta \in \mathbb{Z}[i]$ & $\beta | \alpha$ $\quad \alpha \neq 0$, $\beta \neq 0$

$\Rightarrow \alpha = \beta\gamma$ for some $\gamma \in \mathbb{Z}[i]$

$$|\alpha|^2 = |\beta\gamma|^2 = |\beta|^2 |\gamma|^2 \quad ; \gamma \neq 0$$

$$|\alpha|^2 \geq |\beta|^2 \quad \because |\gamma|^2 \geq 1$$

$$d(\alpha) \geq d(\beta)$$

$$d(\beta) \leq d(\alpha)$$

E.D.2 Let $\alpha, \beta \in \mathbb{Z}[i]$; $\beta \neq 0$

Let ~~$\gamma' = \alpha/\beta$~~ $\gamma' = \frac{\alpha}{\beta}$

Then we can choose γ such that

$$|\gamma' - \gamma| \leq \frac{1}{\sqrt{2}}$$

$$\left|\frac{\alpha}{\beta} - \gamma\right| \leq \frac{1}{\sqrt{2}}$$

$$\left|\frac{\alpha - \beta\gamma}{\beta}\right| \leq \frac{1}{\sqrt{2}}$$

$$|\alpha - \beta\gamma| \leq \frac{|\beta|}{\sqrt{2}} = |\delta|$$

$|\alpha - \beta\gamma| \leq |\delta|$ with $|\delta| = \frac{1}{\sqrt{2}}|\beta|$

E.D. Let $h \in K[x]$

$g \in K^*[x]$ $g \neq 0$

1) if $h = 0$

Then $0 = g \cdot 0 + 0$ $r = 0$

2) If $h \neq 0$ and $d(h) < d(g)$ then $h = g \cdot 0 + r$

$q = 0$

$r = h$

$h = g \cdot 0 + r$

$h = gq + r$ with $d(r) = d(h) < d(g)$

$\Rightarrow d(r) < d(g)$

3) If $d(h) > d(g)$

$\deg(h) > \deg(g)$

Then $h = g \cdot q + r$ $0 \leq r < g$

either $r = 0$

or $\deg r < \deg g$.

Examples - The Ring of Gaussian Integer $\mathbb{Z}(i)$ is E.D.

Soln

If $\alpha \in \mathbb{Z}(i)$

Then α is of the type

$\alpha = a + ib$; $a, b \in \mathbb{Z}$

$\mathbb{Z}(i)$ is an E.D

So $n\mathbb{Z}$ is Principle Ideal.
& $\mathbb{Z}$ is P. I. D.

c. d-N (real)

Theorem:- Every Euclidean Domain is Principle Ideal Domain.

Proof:- Let R be an E-D (Euclidean Domain).
And J be an Ideal of R
if $J = \{0\}$ Then it is P-Ideal generated by 0.

if $J \neq \{0\}$ and R is E-D
Then there exist an Euclidean function d. such that

$$d : R^* \longrightarrow \mathbb{Z}_{\geq 0} \quad ; R^* = R - \{0\}$$

Then the set of d Value of non-zero element of J is a non-empty set of Integers ≥ 0
and so it Contain a Smallest +ve Integer
and let b be the element of J whose d-Value is Smallest
we claim that
$J = bR$
As $b \in J$
Let $x \in bR$

$x = br$

for $b \in J$, $r \in R$

J is Ideal

$\Rightarrow br \in J$

$x \in J$

$bR \subseteq J$

Now Let $a \in J$ and $b \in J$ $b \neq 0$

Then by E.D$_2$

$a = bq + r$

and either $r = 0$

OR $d(r) < d(b)$

but $d(b)$ is least so $r = 0$

$a = bq$ for some $q \in R$

$a = bq \in bR$

$\Rightarrow J \subseteq bR$ $\because a \in J$ is arbitrary

$\Rightarrow J = bR$

So J is P.I (Principle Ideal).

C.O.N (Science) ☆

Theorem:- Every Principle Ideal Domain is U.F.D.

Proof:- Let R be a Principle Ideal Domain and A be the set of all element x of R such that x can not be written as product of irreducible elements in R.

i.e

which cannot satisfy U.F,

we will show $A = \phi$

Now

Let $T = \{xR : x \in A\}$ is a family of Principle Ideal generated by A.

we claim that T has a maximal element

for this we use Zorn's lemma

Let $T_0 = \bigcup_{I \in T} I$

$T = \{xR : x \in A\}$

which is an Ideal on R and this is a chain of ideal and

$$T_0 = \bigcup_{I \in T} I$$

is their upper bound of chain in T.

so is maximal Ideal in T.

As R is Principle Ideal domain.

so T_0 is Principle Ideal.

Let $T_0 = aR$ for $a \in A$

then

$a \in A$

Then $a = bc$ for some non-unit b & c.

and b/a & c/a

$aR \subseteq bR$

and $aR \subseteq cR$

$\Rightarrow b, c \notin \Omega$.

$\therefore aR$ is maximal in Γ_0 for $a \in R$

$\Rightarrow$ both b and c can be written as Product of irreducible

i.e in Style of UF_1

so that New Product $a = bc$ is Product of irreducible

$\Rightarrow a \notin \Omega$ a Contradiction

i.e $a \in R$

so $\Omega = \phi$

so UF_1 satisfied.

$\underline{UF_2}$ next we will show that each irreducible of R is Prime in R

Let p is some irreducible

in R.

Then P is not zero

and not unit.

To Prove that P is Prime

Let $a, b \in R$

P/ab

and suppose P/a

and also Prove P/b

Consider the Ideal aR, bR

and Then $pR + aR$

and Then This is Ideal of R

$\therefore$ R is Principle Ideal Domain

so $pR + aR$ is Principle Ideal

Let $aR + bR = dR$

for some $d \in R$

But

$a = p.0 + a.1 \in dR$

$P = P.1 + a.0 \in dR$

and $a = dr_1 \quad r_1 \in R$

$P = dr_2 \quad r_2 \in R$

$\Rightarrow d/a$ and d/p

$\therefore p$ is ~~Prime~~ irreducible.

So d is either a unit or some associate of p.

if p is associate $p \mid d$

$\Rightarrow p \mid a$ not possible

So d is unit in R

Then $pR + aR = R$

now as $1 \in R = pR + aR$

$1 = ps + at$ for some $s, t \in R$

multiplying by b.

$b = bps + abt$

$\because p \mid ab \Rightarrow p \mid abt$

Then $p \mid p \Rightarrow p \mid bps$

$\Rightarrow p \mid bps + abt$

$\Rightarrow p \mid p$

Similarly if $p \nmid b$

Then we must have $p \mid a$

$\Rightarrow$ p is Prime
so every element of R satisfy UF

Theorem:- An Integral Domain R is U.F.D iff R is factorization Domain (it satisfies UF) and every irreducible element in R is Prime.

Proof:- let R is U.F.D
it is obviously factorization Domain (i.e it satisfies UF)
let a be an irreducible in R and

a/xy for $x,y \in R\setminus\{0\}$

Then there exist $b \in R\setminus\{0\}$
such that

$$ab = xy \quad \text{---} (1$$

Since R is U.F.D
and $x, y \in R\setminus\{0\}$
Then

$$x = u p_1 p_2 \text{ --- } p_r$$

$$y = v q_1 q_2 \text{ --- } q_s$$

where $p_i = i = 1, 2, \text{---}, r$

$q_j = j = 1, 2, \text{---}, s$

are irreducible and u, v are unit

$$\Rightarrow ab = xy = uv p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

$$\Rightarrow ab = u_1 p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s \quad \because u_1 = uv$$

As R is U.F.D

$\Rightarrow$ by UE_2 a is associates of some p_i or q_j.

Let a is associate to p_i

$\Rightarrow a \sim p_i \Rightarrow a/p_i$ & p_i/a for some i

$p_i = \alpha a$ for some unit α (by Previous Theorem)

Now

$$x = u p_1 p_2 \cdots p_{i-1} p_i p_{i+1} \cdots p_r$$

$$\Rightarrow x = u p_1 p_2 \cdots p_{i-1} \alpha a p_{i+1} \cdots p_r$$

$x = ax'$ where $x' = u\alpha p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_r$

$\Rightarrow a/x$

Similarly if

$a \sim q_j$

for some $j = 1, 2, \ldots s$

Then we can show a/y

Here ~~Hence~~ if a/xy

$\Rightarrow a/x$ or a/y

$\Rightarrow a$ is Prime

Hence every irreducible is Prime

Conversely let R is factorization Domain i.e it satisfies UF_1 and every irreducible is Prime in R.

Let $x \in R \setminus \{0\}$ has two factorization

$x = u p_1 p_2 \cdots p_r$

$x = v q_1 q_2 \cdots q_s$

with u, v are unit and

$p_i = 1, 2, \cdots r$ $q_j = j = 1, 2, \cdots s$

are irreducible

if $r = 0$ Then $x = (1) v$

Then x is unit

So it satisfies UF_2

Now suppose that Result is true for $r > 0$ ~~$x = r-1$~~ $r \geq 0$

As p_1 / x

and p_1 is irreducible

$\Rightarrow p_1$ is Prime

since p_1 / q_1 & $p_1 / q_1 q_2 \cdots q_s$

$\Rightarrow p_1 / q_1 q_2 \cdots q_s$

and $p_1 / q_1 q_2 \cdots q_s$

$\Rightarrow p_1 / q_j$ for some j

p_1 is associate of q_j i.e $p_1 \sim q_j$

so $q_j = \alpha p_1$ for some unit α

now

$x = u p_1 p_2 \cdots p_r = v q_1 q_2 \cdots q_s$

$\Rightarrow u p_1 p_2 \cdots p_r = v q_1 q_2 \cdots q_{j-1} (\alpha p_1) q_{j+1} \cdots q_s$

so it satisfies UF2

Hence it is U.F.D for any $r \geq 0$

Theorem:- Let R be an E.D and $a \in R^*$ Then a is unit iff $\phi(ab) = \phi(b)$ for some Euclidean function ϕ.

Proof:- Let a is unit Then $a/1$ and R is E.D

by ED$_1$ $a/1$

$\Rightarrow \phi(a) \leq \phi(1)$

also $1/a$ $\therefore a$ is unit

$\Rightarrow \phi(1) \leq \phi(a)$

$\Rightarrow \phi(u) = \phi(1)$

Conversely:- Let $\phi(u) = \phi(1)$

we have to show that u is unit.

Since $u, 1 \in R$; $u \neq 0$

Then by ED$_2$ $\exists$ q and r such that

$1 = uq + r$ with $r = 0$

or $\phi(r) < \phi(u)$

Since $\phi(u) = \phi(1)$

$\therefore \phi(r) < \phi(u) \Rightarrow \phi(r) < \phi(1)$

As $1 \nmid r$

by ED$_1$ $\phi(1) \leq \phi(r)$, $\phi(r) = \phi(u)$.

a contradiction

So $r = 0$

Then $1 = uq \Rightarrow u \mid 1$

$\Rightarrow u$ is unit.

e.o.N(R.U)

Q.4 Find all the unit of Gaussian Integer Ring.

$G = \{a + ib : a, b \in \mathbb{Z}\}$

Soln As $1 \in G$ is the unit of G

Suppose $x + iy$ be any unit in G

Then $\exists$ $x_1 + iy_1 \in G$; $x, y, x_1, y_1 \in \mathbb{Z}$

such that

$(x + iy)(x_1 + iy_1) = 1$

$(xx_1 - yy_1) + i(xy_1 + x_1 y) = 1 + i0$

Comparing Real & Imaginary Part

$$xx_1 - yy_1 = 1 \quad \text{—(1}$$

$$xy_1 + x_1y = 0 \quad \text{—(2}$$

By putting and adding

$$(x^2+y^2)(x_1^2+y_1^2) = 1$$

$\because x, y, x_1, y_1 \in \mathbb{Z}$

so it holds only if

$$x^2+y^2 = 1$$

$$x_1^2+y_1^2 = 1$$

as $x^2+y^2 = 1$

so we have two possibility

1) $x^2 = 1 \qquad y^2 = 0$

$x = \pm 1 \qquad y = 0$

2) $x^2 = 0 \qquad y^2 = 1$

$x = 0 \qquad y = \pm 1$

so units of G are

Case-I

$$x+iy = \pm 1 + 0i = \pm 1$$

Case-II $\quad x+iy = 0 + i(\pm 1)$

$$x+iy = \pm i$$

$\Rightarrow 1, -1, i, -i$ are units of G.

★ Different

Q #1 Prove that the polynomial x^2+x+4 is irreducible over the field of integers modulo 11.

Sol:// Let $f(x) = x^2+x+4=0$

$P = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots, \bar{10}\}$

$f(0) = 0+0+4 \neq 0$

$f(1) = 6 \neq 0$

$f(2) = 10 \neq 0$ $\quad f(3) = 9+3+4 = 16 = 5 \neq 0$

$f(4) = 24-22 = 2 \neq 0$

$f(10) \neq 0$ $\quad f(10) = 114 = 4 \neq 0$

So $f(a) \neq 0 \ \forall a \in P$

So $x = a$ is not root

$\Rightarrow x-a$ is not factor. Hence $f(x)$ is irreducible.

Q # Let R be an I.D and $P \subset R^*$

$\therefore R^* = R - \{0\}$

Then P is Prime iff R/PR is an I.D.

Sol:// Let P is Prime

Then P is not unit Then $P \neq 1$

$1 \notin PR$

$1 + PR \neq PR$

Let $(a+pR)(b+pR) = pR$
where $a, b \in R$
$\therefore pR$ is zero of R/pR (i.e pR is additive identity of R/pR)

$ab + pR = pR$
$\Rightarrow ab \in pR$
$\Rightarrow p/ab$

Since p is Prime
$\Rightarrow p/a$ or p/b $\Rightarrow a = pr$ or $b = pr$

$\Rightarrow a \in pR$ or $b \in pR$
$a + pR = pR$ or $b + pR = pR$

so R/pR is I.D

Conversely:- Let $p \in R^*$
and R/pR is I.D

As $1 + pR \neq pR$
$\Rightarrow 1 \notin pR$
$\Rightarrow p/1$

$\Rightarrow p$ is not unit
also let p/ab
$\Rightarrow ab \in pR$
$ab + pR = pR$

$(a+pR)(b+pR) = pR$

R/pR is I.D with pR is zero of R/pR

$\Rightarrow a+pR = pR$ or $b+pR = pR$

$\Rightarrow a \in pR$ or $b \in pR$

$\Rightarrow a = pr$ or $b = pr$

p/a or p/b

$\Rightarrow p$ is Prime.

Q# Let R be an E.D and a, b are two non-zero elements in R Then

1) If b is unit in R Then
$\phi(ab) = \phi(a)$

2) If b is non unit
Then $\phi(ab) > \phi(a)$
where ϕ is E.D function.

Proof:- 1) Since R is E.D and a/ab by ED1

$\phi(a) \leq \phi(ab)$ ——(1

now as b is non-zero $\because b$ is unit
Then

$a = (ab)b^{-1}$

and $\phi(a) = \phi((ab)(b^{-1}))$

$\phi(a) = \phi(ab)\phi(b^{-1})$

$\phi(a) \geq \phi(ab)$ — (2)

(1) & (2) $\Rightarrow$

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

As Required

2) As b is non-unit and a, b are non-zero

also $ab \neq 0$

As $a, ab \in R$

by ED $\exists$ q and r such that

$a = (ab)q + r$

either $r = 0$ or $\phi(r) < \phi(ab)$

if $r = 0$

$\Rightarrow a = (ab)q$

$a(1 - bq) = 0 \quad a \neq 0$

$\Rightarrow 1 - bq = 0$

$1 = bq$

$b/1 \Rightarrow b$ is unit

A Contradiction $\because r \neq 0$

Then $\phi(r) < \phi(ab)$ — (a)

also $a - abq = r$

$r = a(1 - bq) \Rightarrow a/r$

$\phi(r) = \phi(a(1-bq)) \Rightarrow \phi(a) \leq \phi(r)$ — (b)

$\phi(r) = \phi(a)\phi(1-bq)$

$\phi(r) \geq \phi(a)$ — (b

(a) & (b) $\Rightarrow$

$\phi(a) \leq \phi(r) < \phi(ab)$

$\phi(a) < \phi(ab)$

but $2 \in (1+\sqrt{-5})$ & $2 \in (2+\sqrt{-5})$

So 2 is not Prime in R.

Principle Ideal :-

An Ideal I of a ~~Integral domain~~ Ring is called Principle if it is generated by a single element.

Note that R and {0} be trivial Principle Ideal generated by 1 & 0 respectively.

Principle ~~Integral~~ Ideal Domain :-

A ~~Integral~~ Ring R is called Principle Ideal ~~Integral~~ domain if its each Ideal is a principle Ideal.

If R is an Integral domain then Ideal of R are only {0} and R which are Principle Ideal. So it is Principle ~~Ideal~~ Ideal ~~Integral~~ domain.

~~Integral~~ Any field K is Principle ~~Ideal~~ Ideal domain

Ideal It is Principle ~~Integral~~ Ideal Domain.

NOTE $\mathbb{Z}_0 = \mathbb{Z}^* = \mathbb{Z} - \{0\}$

C.O.N.C.E.P.T.S

Euclidean Domain:-

An Euclidean Domain is an Integral domain R together with a function :-

$d : R^* \to \mathbb{Z}_0$

such that $R^* = R - \{0\}$

ED-1 for $a, b \in R^*$ i.e $a \neq 0, b \neq 0$

if $a/b \Rightarrow d(a) \leq d(b)$

ED-2 for $a \in R$ $b \in R^*$ i.e $b \neq 0$

There exist $q, r \in R$

such that

$a = bq + r$

with $d(r) < d(b)$

OR $r = 0$

$$\begin{array}{r|l} & q \\ b & a \\ & bq \\ \hline & r \end{array}$$

NOTE That the function d is called Euclidean function defined on R. There may be different function which make a given Integral domain into a Euclidean domain.

(P.O.I)

Example:- $\mathbb{Z}$ is Euclidean Domain

Solution Since $\mathbb{Z}$ is Integral domain

For $a \neq 0$; $a \in \mathbb{Z}$

End Of Ring

Factorization Domain :-

A commutative ~~ring~~ Integral Domain R with Identity is called F.D if for every $x \neq 0 \in R$ can be written as a unit times a finite Product of irreducible elements i.e

$x = u x_1 x_2 \cdots x_r$

; u is unit and x_i ; $i = 1, 2, \ldots$ are irreducible