Ring Theory

Def^n:- A ring 'R' is a set with two binary operations called $(+)$ addition and multiplication $(\cdot)$ which satisfying the following properties :-

1.) $(R, +)$ is an abelian group with identity 0.

2.) Multiplication is associative i.e.,
$(ab)c = a(bc)$ $\forall\ a, b, c \in R$.

3.) $\exists\ 1 \in R$ s.t $a \cdot 1 = 1 \cdot a = a$ $\forall\ a \in R$

4.) Distributive law.
$(a+b)c = ac + bc$
$c(a+b) = ca + cb$ $\forall\ a, b, c \in R$

If in addition $ab = ba$ $\forall\ a, b \in R$
then R is called commutative ring.

Example :-

1.) $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ are all commutative ring.

2.) $M_n(R)$ = set of all $n \times n$ matrices over R.
It is ring which is not commutative for $n \geq 2$.

3.) $C(R) = \{f : R \to R \mid f$ is continous $\}$
is a ring w.r.t
$(f+g)x = f(x) + g(x)$ and
$(fg)(x) = f(x) \cdot g(x)$ which is commutative.

4.) Let R be any ring. $R[x]$ = set of all polynomials in x with coeff. in R.
→ If R is commutative then $R[x]$ is a commutative ring.

5.) Any field is a ring.

6) The zero ring $R = \{0\}$ consists of a single element 0. In which the multiplicative identity is same as additive identity.

Remark:- Let R be a ring in which $1 = 0$, then R is the zero ring.

Proof:- Let $a \in R$, then $a = a \cdot 1 = a \cdot 0 = 0$.
$\therefore$ R is a zero ring.

Def:- An element $u \neq 0 \in R$ is called a unit in R if there is some $v \in R$ s.t $uv = vu = 1$.
The set of units in R is denoted by $R^\times$.

Examples. 1.) The units in $\mathbb{Z}$ are called 1 and -1.

2.) In $R[x]$ the units are non-zero constant polynomials.

Def:- Let R be a ring. A non zero element $a \in R$ is called a zero divisor if $\exists$ a non-zero element $b \in R$ s.t $ab = 0$ or $ba = 0$.

Examples:- consider the ring $\mathbb{Z}/6\mathbb{Z}$.

$\bar{2} \cdot \bar{3} = \bar{0}$, but $\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$
So, $\bar{2}$ is a zero divisor.

* Observe that a zero divisor can never be a unit. Suppose that 'a' is a unit and a zero divisor then $\exists$ non-zero 'b' s.t $a \cdot b = 0$.
But if 'a' is a unit, then $\exists$ $a' \in R$

s.t, $a \cdot a' = a' \cdot a = 1$

$= a'(ab) = a' \cdot 0$

$= (a'a)\, b = 0$

$= b = 0$

Def^n:- A subring of a ring R is a subgroup of R which closed under multiplication, ~~and contain 2~~ and contains 1.

Example:- $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{Q}$ is a subring of R.

Proposition:- Let R be a ring. Then,

1.) $0 \cdot a = a \cdot 0 = 0 \quad \forall\, a \in R$.

2.) $(-a) \cdot b = a \cdot (-b) = -ab \quad \forall\, a, b \in R$.

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

4.) $(-a) = (-1) \cdot a \quad \forall\, a \in R$.

* **Ring Homomorphism:-**

Let R and S be two rings. Then a map $\phi: R \to S$ is called a ring homomorphism if,

✓ $\phi(a+b) = \phi(a) + \phi(b)$.

✓ $\phi(ab) = \phi(a) \cdot \phi(b)$,

and ✓ $\phi(0_R) = 0_S$. → additive identity preserve.

When homomorphism is in unit rings:- (not used in all books).

then one more property of multiply. identity pres.

$\phi(1_R) = 1_S$.

↳ in case of unit ring.

Def^n:- Let,

then, ke

Ex:- Is th

* Subring

It i

the st

$(S, +, \cdot, 0$

a su

Asian elephants live in the tropical forests and grasslands

Def^{n}:- Let, $\phi : R \to S$ be a ring homomorphism then, $\ker \phi = \{ a \in R \mid \phi(a) = 0 \}$

Ex:- Is the $\ker \phi$ a subring of R?

---

* Subring :-

It is a subset of $(R, +, \cdot, 0, 1)$ that preserve the structure of the ring, i.e., a ring $(S, +, \cdot, 0, 1)$ with $S \subseteq R$. Equivalently it is both a subgroup of $(R, +, 0)$ and a submonoid of $(R, \cdot, 1)$.

5/3/19. Always assume rings are always w.r.t multiplication.

Defⁿ:- Let, $\phi: R \to S$ be a ring homo. Then

$\ker \phi = \{a \in R \mid f(a) = 0\}$.

An bijective homo. is called an isomorphism.

→ ~~This is the subring~~.

Proposition:- Let $\phi: R \to S$ be a ring homo.

(1) The image of ϕ is a subring of S.

(2) The kernel of ϕ is not a subring of R unless it is the whole ring. Furthermore, if $\alpha \in \ker\phi$ then, $r\alpha$ and $\alpha \cdot r \in \ker\phi$ $\forall$ $r \in R$.

Proof(2):- For any $r \in R$ and $\alpha \in \ker\phi$.

$$\phi(\alpha \cdot r) = \phi(\alpha) \cdot \phi(r) = 0 \cdot \phi(r) = 0$$

$\therefore \alpha \cdot r \in \ker(\phi)$.

Defⁿ:- Let R be a ring and I be a subset of R. Then I is said to be a left ideal; if I is a subgroup of $(R, +)$, and I is closed under left multiplication.

i.e., $r \cdot I \subseteq I$.

and I is said to be a right ideal if I is a subgroup of $(R, +)$ and I is closed under right multiplication i.e., $I \cdot r \subseteq I$.

A subset I which is both a left ideal and a right ideal is called the ideal of R.

Ex:- (1) $f: \mathbb{Z} \to$ ... $f($ ... check that ...

(2) consider, $f($ ...

check ...

(3) Define ... $\phi($ ...

$\ker(\phi) = \{$ ...

claim :-

Note that ... linear ...

Let, ... → $r(x)$ ... → where, ... $r(x$ ... → $r(\mathbb{Z}$ ...

$\therefore \ker(\phi$ ...

☆ In a ... part ... prin... done.

Ex: (1) $f: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$f(m) = \overline{m}$

check that 'f' is a ring homo.

(2) consider, $f: R[x] \longrightarrow R$

$f\left(\sum_{i=0}^{n} a_i x^i\right) \Rightarrow \sum_{i=0}^{n} a_i \cdot \alpha^i$ where, $\alpha \in R$.

check 'f' is a ring homo.

(3) Define $\phi: \mathbb{Q}[x] \longrightarrow R$ by

$\phi(f(x)) = f(\sqrt{2})$

$\ker(\phi) = \{ f(x) \in \mathbb{Q}[x] \mid \phi(f(x)) = 0 \}$

claim :- $\ker(\phi) = \{ (x^2-2)\, q(x) \mid q(x) \in \mathbb{Q}[x] \}$

Note that if, $f \in \ker(\phi)$, then 'f' cannot be a linear polynomial.

Also, $(x^2-2) \in \ker(\phi)$.

Let, $g(x) \in \ker(\phi)$. and $g(x) = (x^2-2)q(x) + r(x)$.

→ $r(x)$ is strictly linear or const.

→ where, degree of $r(x) < 2$ or $r(x) = 0$.

$r(x) = g(x) - (x^2-2)\, q(x)$

→ $r(\sqrt{2}) = 0 \Rightarrow r(x) \in \ker\phi$

$\Rightarrow r(x) = 0$.

$\therefore \ker(\phi) = \{(x^2-2)\, q(x) \mid q(x) \in \mathbb{Q}[x]\}$

☆ In any ring 'R', the set of multiples of a particular element 'a' form an ideal called principal ideal generated by 'a' and is denoted by, $(a) = \{ar \mid r \in R\}$ [Here R is commutati

We may consider the ideal of elements $a_1, a_2, \ldots, a_n \in R$ which is defined to be the smallest ideal containing these elements and it is denoted by,

$$(a_1, a_2, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n\} \quad \forall\ r_i \in R.$$

In any ring R, the set consisting of zero alone is an ideal called the zero ideal and it is principal ideal. and the whole ring is called the unit ideal denoted by (1).

The unit ideal is the only ideal which contain an unit.

An ideal I is said to be proper if it is not (0) or (1).

Proposition.

(1) Let F be a field. The only ideals of F are zero and unit ideal.

(2) conversely, if a ring R has exactly two ideals then R is a field.

Proof (2) :-

Assume that R has exactly two ideals.

WTS, $1 \neq 0$.

If $1 = 0$, then it is the zero ring and then it will have only one ideal, which is a contradiction.

$\therefore 1 \neq 0$. Then (1) and (0) are two different ideals. Let $a \neq 0$ be an element of R. $(a) = (1)$.

i.e., $\exists\ b \in R$ s.t, $ab = 1$. $\therefore$ a is a unit.

Proposition:-
Let F be a field and R' be a non-zero ring and $\phi : F \to R'$ be a ring homo.
Then ϕ is injective.

Proof:- Since F is a field, therefore $\ker\phi$ is either (0) or (1). But if $\ker\phi = (1)$ then R' will be the zero ring.

$\therefore \ker(\phi) = (0)$. Thus ϕ is injective.

Def^n A ring in which all ideals are principal // ideal is called a principal ideal ring (PIR).

Proposition:- Every ideal in $\mathbb{Z}$ is principal ideal.

Proposition:- Let F be a field. Every ideal in $F[x]$ is a principal ideal.

Proof: Let, $0 \subseteq I \subseteq F[x]$ be a proper ideal.
$\exists$ a poly of (+)ve degree in I. Let, $f(x) \in I$ having the smallest (+)ve degree. Let $g(x) \in I$.
Then by division algorithm we have,

$$g(x) = f(x) \cdot q(x) + r(x).$$

where, degree of $r(x)$ < degree of $f(x)$
or $r(x) = 0$ {identically equal}.

$\to r(x) = g(x) - f(x) \cdot q(x) \in I$

$\Rightarrow r(x) = 0$ [by minimality of deg $f(x)$]

$\therefore g(x) = f(x) \cdot q$

Remark: $\mathbb{Z}[x]$, suppose ideal is gen. by two elements

$I = (2, x) = (f)$ where $f \in \mathbb{Z}[x]$.

Since, $2 \in (f)$ $\therefore$ $2 = f \cdot g \Rightarrow f$ is a const. poly.

$\rightarrow$ Since, degree $2 = 0 \Rightarrow \deg f = 0$.

and $f \mid 2 \Rightarrow f = \pm 1$ or ± 2.

Since, $(1) = (-1) = \mathbb{Z}[x] \neq I$.

$\therefore f = \pm 2$, but ± 2 doesn't divide x,

So, $x \notin (2)$ or (-2).

$\therefore (2, x)$ is not a principal ideal.

So, $\mathbb{Z}[x]$ is not a principal ideal ring.

Remark: $\mathbb{Z}$, $F[x]$ where F is a field are PIR.

★ Integral Domain :-

An integral domain R is a non zero ring having no zero divisors i.e., if $ab = 0$ then $a = 0$, or $b = 0$.

Example :- (1) Fields are int. domain.

(2) $\mathbb{Z}$ is an int. domain.

(3) $F[x]$ where F is a field is an int. domain.

(4) $C(R) = \{ f : R \to R \mid f$ is a contnous $f^n \}$

$C(R)$ is not an int. domain.

Define, $f: R \to R$ by $f(x) = \begin{cases} 0 & \forall\ x \le 0 \\ x & \forall\ x > 0 \end{cases}$

and $g: R \to R$ by $g(x) = \begin{cases} x & \forall\ x \le 0 \\ 0 & \forall\ x > 0 \end{cases}$

Then, $f \cdot g = 0$ but, $f \neq 0$ and $g \neq 0$.

Proposition:- Let R be an int. domain then $R[x]$ is also an int. domain.

Proposition:- Let R be an int. domain if $ab = ac$ and $a \neq 0$ then $b = c$.

Proof:- $ab = ac \Rightarrow a(b-c) = 0$.

$\therefore$ R is int. domain, $* \ a \neq 0 \Rightarrow b - c = 0$

$\Rightarrow b = c$.

Proposition:- A finite int. domain is a field.

Proof:- Let R be a finite int. domain. Let $0 \neq x \in R$.

WTS, x is a unit.

Consider the element $x, x^2, x^3, \ldots$

$\therefore$ R is finite: $\exists$ $r > s$ s.t,

$x^r = x^s$.

$\Rightarrow x^s (x^{r-s} - 1) = 0$.

$\Rightarrow x^{r-s} = 1 \quad [\because x^s \neq 0]$

$\Rightarrow x \cdot x^{r-s-1} = 1$.

$\therefore$ x is an inverse. //

Thus R is a field.

★ Quotient Ring :-

Let R be a ring and I be an ideal of R. Then we have already seen that the set of all cosets of I forms a group R/I.

Want To show :-

R/I has a ring structure, want to define multiplication of two cosets.

$$(a+I)(b+I) = ab+I$$

well defined ?

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

want to show :-

$$ab+I = a'b'+I.$$

$\Rightarrow a-a' \in I \;\&\; b-b' \in I$

say, $a-a' = I_1 \;;\; b-b' = I_2$

$$ab = (a'+I_1)(b'+I_2)$$
$$= a'b' + a'I_2 + b'I_1 + I_1I_2$$
$$ab = a'b' + i \text{ , where } i \in I$$

$\Rightarrow ab - a'b' \in I$

This is well defined !

→ I^st Isomorphism Theorem :-

let, $f: R \to S$ be a surjective ring homomorphism $I = \ker f$. Then $R/\ker f \cong S$

Proof

$\bar{f} : R/I$

$\bar{f}(a+I)$

$\bar{f}$ is well de

$\bar{f}((a+I)(b+I$

LHS = $\bar{f}$ (a

$\therefore \bar{f}$

[not shown follow

→ since, $\bar{f}$

$\ker \bar{f} = \{$

$= \{$

$\therefore$

hence,

Example :-

ϕ

ϕ is

→ chec

Ker ϕ

Note th

Proof: $\bar{f} : R/I \to S$

$\bar{f}(a+I) = f(a)$

$\bar{f}$ is well defined? check.

→ $\bar{f}((a+I)(b+I)) = \bar{f}(a+I) \cdot \bar{f}(b+I)$?

LHS $= \bar{f}(ab+I) = f(ab)$

$= f(a) \cdot f(b)$ [as f is ring homomorphism]

$= \bar{f}(a+I) \cdot \bar{f}(b+I)$

$\therefore \bar{f}$ is a ring homomorphism

[not shown other prop. For homomorphism as follows from group theory.]

→ Since, f is surjective, so $\bar{f}$ is surjective.

$\ker \bar{f} = \{ a+I \in R/I \mid \bar{f}(a+I) = 0 \}$

$= \{ a+I \in R/I \mid f(a) = 0 \} = \{ I \}$

$\therefore \bar{f}$ is injective.

hence, $\bar{f}$ is an isomorphism.

$\therefore R/I \cong S$.

Example:- $\phi : R[x] \to C$

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

$\phi(x) = i$

ϕ is a ring homomorphism.

→ check its surjectiveness.

$\phi(a+bx) = a+bi$.

$\ker \phi = \{ f(x) \in R[x] \mid f(i) = 0 \}$

Note that, $\boxed{x^2+1 \in \ker \phi}$

Let, $g(x) \in \ker \phi$. Then by division algo.

$g(x) = (x^2+1).q(x) + r(x)$, where deg. $r(x) < 2$

or, $r(x) = 0$.

$r(x) = g(x) - (x^2+1).q(x)$

$r(i) = g(i) - 0 = 0$

$r(x) \in \ker \phi$.

$\Rightarrow r(x) = 0$ (as $r(x)$ cannot have degree 2)

$\therefore g(x) = (x^2+1).q(x)$

$\therefore$ By 1st Isomorphism theorem,

$R[x]/(x^2+1) \cong \mathbb{C}$

$x^2+1 = 0$, $x^2 = -1$

any element, $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

$= a + bx$ (replacing x^2)

How this look like;

$\frac{R[x]}{(x^2)}$; $\frac{R[x,y]}{(y^3)}$ } → degree y atmost 2.

↓

deg. x → atmost 1

* $\phi : \mathbb{Z}[x] \to \mathbb{Z}[i] := \{a+bi \mid a,b \in \mathbb{Z}\}$

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

$\ker \phi$? (x^2+1) ?

Ex:- Show that, $\mathbb{Z}[i]/(1+3i) \cong \mathbb{Z}/10\mathbb{Z}$

$1+3i = 0 \Rightarrow 3i = -1 \Rightarrow 9i^2 = 1 \Rightarrow 10 \dots$

12/3/14

Proof:- 1st step. WTS:- $f(J)$ is an ideal of S.

clearly $f(J)$ is a subgroup of S. Let $s \in S$ and $a \in f(J)$. WTS $sa \in f(J)$.

since f is surjective $\exists\ x \in R$ s.t $f(x) = s$.

and $\exists\ b \in J$ s.t $a = f(b)$.

$$sa = f(x) \cdot f(b) = f(xb) \in f(J).$$

2nd step:- $f^{-1}(I) = \{ a \in R \mid f(a) \in I \} \geq K$

WTS $f^{-1}(I)$ is an ideal of R.

clearly $f^{-1}(I)$ is a subgroup of R.

Let $a \in R$ and $x \in f^{-1}(I)$.

WTS, $ax \in f^{-1}(I)$.

$$f(ax) = f(a) \cdot f(x) \in I.$$

Thus, $f^{-1}(I)$ is an ideal of R.

3rd step:- WTS $f^{-1}(f(J)) = J$

and, $f(f^{-1}(I)) = I$

It is clear that $J \subseteq f^{-1}(f(J))$

WTS $f^{-1}(f(J)) \subseteq J$.

Let $a \in f^{-1}(f(J)) = f(a) \in f(J)$.

$= f(a) = f(y)$

where, $y \in J$.

$\to f(a-y) = 0$

$\Rightarrow a-y \in K \quad (\ker f)$

$\to K \subseteq J$

so, $a \in J$

$\therefore f^{-1}(f(J)) = J$

It is clear that $f(f^{-1}(I)) \subseteq I$

WTS. $I \subseteq f(f^{-1}(I))$

Let, $a \in I$. $\because f$ is surjective $\exists x \in R$ s.t. $f(x) = a \in I$.

$\Rightarrow x \in f^{-1}(I)$.

$\therefore I \subseteq f(f^{-1}(I))$

Theorem:- Let R be a ring and I is an ideal of R. $R \xrightarrow{\pi} R/I$.

$\pi(a) = a + I$.

Is this a surjective ring homomorphism?

$\to$ Yes.

* By Previous theorem, $\exists$ a bijection

$\{$ideals of $R \supseteq \ker \pi\} \leftrightarrow \{$ideals of $R/I\}$.

Ex:- Let, $R = \mathbb{Z}$ and $I = 6\mathbb{Z}$. Then find the ideals of R/I. (proper)

Sol:- $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$.

$\to \{0, 2, 4\}$ & $\{0, 3\}$

Theorem:- Let, f homo. and $f^{-1}(J)$ is a

Proof:- $R \xrightarrow{f} S$

Then, $\pi \circ f$

$\ker(\pi \circ f) =$

$=$

$=$

$=$

Thus, by

Remark:-

homom

Let, J (ideal)

By pr

Remark:-

where

Theorem:- Let, $f: R \to S$ be a surjective ring homo. and $J \leq S$ be an ideal. Then, $f^{-1}(J)$ is an ideal of R and $R/f^{-1}(J) \cong S/J$.

Proof:- $R \xrightarrow{f} S \xrightarrow{\pi} S/J$

Then, $\pi \circ f : R \to S/J$ is a surjective ring homo.

$$\ker(\pi \circ f) = \{a \in R \mid (\pi \circ f)(a) \in J\}$$
$$= \{a \in R \mid f(a) + J \in J\}$$
$$= \{a \in R \mid f(a) \in J\}.$$
$$= f^{-1}(J).$$

Thus, by 1st isomorphism theorem;

$$R/f^{-1}(J) \cong S/J.$$

Remark:- Let, $\pi : R \to R/I$ be natural ring homomorphism defined by $\pi(a) = a + I$.

Let, $J \supseteq I$ (ideal). $J/I = \{a + I \mid a \in J\}$

By previous theorem,

$$R/J \cong \frac{R/I}{J/I}$$

because, $\pi^{-1}(J/I) = J$.

Remark:- Ideals of R/I have the form $J/I = \{b + I \mid b \in J\}$ where, J is an ideal of $R \supseteq I$.

★ Construction of rationals from integers?

consider the $\mathcal{F} = \{(a,b) \mid a, b \in \mathbb{Z}, b \neq 0\}$

Define a relation of $\mathcal{F}$

$(a,b) \sim (c,d)$, $ad - bc = 0$

→ $(a_1,b_1) \sim (a_2,b_2)$

$(a_2,b_2) \sim (a_3,b_3)$

WTS. $(a_1,b_1) \sim (a_3,b_3)$

↳ $a_1b_2 - a_2b_1 = 0$ and $a_2b_3 - a_3b_2 = 0$

$a_1b_2b_3 - a_2b_1b_3 = 0$ & $a_2b_3b_1 - a_3b_2b_1 = 0$

(+)

$a_1b_2b_3 - a_3b_2b_1 = 0$

$\Rightarrow b_2(a_1b_3 - a_3b_1) = 0$

$\Rightarrow a_1b_3 - a_3b_1 = 0$ (proved transitive)

$\therefore \sim$ is an equivalence relation.

So, rational numbers are nothing but the equivalence classes.

→ Equivalence class of $(a,b) \in \mathcal{F}$ is denoted by $\frac{a}{b}$

→ $\mathbb{Q}$ is the set of all equivalence classes.

Define (+) and (·) in $\mathbb{Q}$ by,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Theorem:-

Proof: Con

Define

iff a

~

Equiva

by

F

Define (+

$\frac{a}{b} + \frac{c}{d}$

WTS.

th

∴

ker ϕ

Theorem:- Let R be an integral domain. Then $\exists$ a field F and an injective ring homo. $R \to F$.

Proof: Consider the $F = \{(a,b) \mid a, b \in R, b \neq 0\}$.

Define a relation on F by $(a,b) \sim (c,d)$ iff $ad - bc = 0$.

$\sim$ is an equivalence relation.

Equivalence classes of $(a,b) \in F$ is denoted by $\frac{a}{b}$.

F = The set of all equivalence classes.

Define $(+)$ and $(\cdot)$ as follows:-

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \& \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

WTS. F is a field.

Let, $\frac{a}{b} \neq \frac{0}{1} \Rightarrow a \neq 0$.

then, $\frac{b}{a} \in F$ which is the inverse of $\frac{a}{b}$.

$\therefore$ F is a field.

$\phi : R \to F$.

$\phi(r) = \frac{r}{1}$, check ϕ is a ring homo.

$$\ker \phi = \left\{ r \in R \mid \frac{r}{1} = \frac{0}{1} \right\}$$

$$= \{0\}$$

$\therefore$ ϕ is injective ring homomorphism.

→ We identify R with $\phi(R) = \left\{ \frac{r}{1} \mid r \in R \right\} \subseteq F$.

Def^n:- F is called the quotient field of R and is denoted by $Q(R)$.

Ex^t (1) Q is the quotient field of $\mathbb{Z}$

(2) For $k[x]$ the quotient field is the field of rational functions,

$$k(x) = \left\{ \frac{f(x)}{g(x)} \mid g(x) \neq 0 \right\}.$$

Question:- Let R be a ring and I be an ideal of R. When is R/I an integral domain?

Let $a, b \in R$ and $\bar{a} = a+I$, $\bar{b} = b+I$.

i.e., $\bar{a}, \bar{b} \in R/I$. Let, $\bar{a} \cdot \bar{b} = \bar{0}$.

If R/I is an integral domain then either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$.

Now, it means that if $ab \in I$ then either $a \in I$ or $b \in I$.

Def^n:- An ideal $I \subsetneq R$ is called a prime ideal if $ab \in I$ then either $a \in I$ or $b \in I$.

Proposition:- Let R be a ring. Then an ideal P is a prime ideal of R iff R/P is an integral domain.

Ex^t (1) $n\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ iff n is a prime number.

(2) Let us
$k[x]$

→ A polyno
be irre
constant
product
polynom

Q: when
prin

$(f(x))$
then
→ if

⇒ WTS.
is
→ If

∴ I

(2) Let us consider the polynomial ring $k[x]$ where, k is a field.

→ A polynomial with coeff. in k is said to be irreducible over k if it is non constant and can't be factored into the product of two or more non-constant polynomials with coeff. in k.

Q. When an ideal $(f(x)) \subset k[x]$ is a prime ideal?

$(f(x))$ is a prime ideal i.e., if $gh \in f(x)$ then, either $g \in (f(x))$ or $h \in (f(x))$.

if $f(x) \mid gh$ then either $f \mid g$ or $f \mid h$.

⇒ WTS. If $f(x)$ is irreducible then $(f(x))$ is a prime ideal.

→ If $f(x) \nmid g$ then $\gcd(f, g) = 1$.

$gh = f^{a'}$

$1 = fp + gq$.

$\Rightarrow h = fph + ghq = f \cdot p \cdot h + f \cdot q \cdot q'$

$= f(ph + q \cdot q')$

$\Rightarrow h \in (f)$

∴ If f is irreducible poly. then $(f(x))$ is a prime ideal.

14/3/19

Proposition:- A ring R is an integral domain iff (0) is a prime ideal.

Example:- In $\mathbb{Z}[i]$ consider the ideal (2). is not a prime ideal because $(1+i)(1-i) = 2$, but $(1+i) \notin (2)$ and $(1-i) \notin (2)$. suppose $(1+i) \in (2)$, $(1+i) = 2(a+ib)$

$\Rightarrow 1 = 2a$, $1 = 2b$

which is not possible.

Q.] when is R/I a field?

Q.] Now we investigate surjective homomorphism $\phi: R \to F$ where F is a field & R is a ring?

Def":- An ideal M of a ring R is called a maximal ideal if whenever $M \subset I \subset R$ then either $I = M$ or $I = R$.

i.e., M is not contained in any ideal other

than M and R.

Zorn's Lemma:-

Let S be a partially ordered set. If every totally ordered subset of S has an upper bound then S contain a maximal element.

{Maximal ideal is not necessarily unique}

Proposition:-

Maximal ideal exists in a non-zero ring.

proof:- consider the set $S = \{I \mid I$ is a proper ideal of $R\}$.

→ under inclusion, S is a partially ordered set. Let J be a totally ordered subset of S i.e., for all $I, J \in T$ either $I \subset J$ or $J \subset I$.

Let, $U = \bigcup \{I \mid I \in T\}$. Then U is an ideal of R and U is proper.

By Zorn's Lemma 'S' has a maximal element.

Proposition:-

An ideal M of R is a maximal ideal iff R/M is a field.

proof:- Let M be a maximal ideal. R/M has only two ideals $(\bar{0})$ and $R/M = (\bar{1})$.

Since R/M has exactly two ideals so, R/M is a field.

⇒ Prove the converse of above?

Remark: Every maximal ideal is a prime ideal but the converse is not true. Eg.; in $\mathbb{Z}$, (0) is a prime ideal but not a maximal ideal as $(0) \subsetneq (n)$.

Ex: $R[x,y]$. Then (x) is not a maximal ideal.

$$R[x,y]/(x) \cong R[y].$$

$\therefore$ (x) is a prime ideal but not a maximal ideal.

Corollary: The zero ideal is a maximal ideal iff R is a field.

Example ①: In $\mathbb{Z}$, the maximal ideals are generated by prime integers.

② consider the $k[x]$.

Every maximal ideal is generated by an irreducible polynomial.

$f(x) \subset m$

$(f(x)) \subset (g(x))$

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

$\Rightarrow$ In $C[x]$ every maximal ideal is generated by a linear polynomial say $(x-a)$

$m_a = (x-a) \longleftrightarrow c$

{ maximal ideals of $C[x]$ } $\longleftrightarrow$ { c }

correspondence.

$C[x_1, x_2, \ldots, x_n] \longleftrightarrow C^n$.

Ex: What is the structure of maximal ideals in $C[x_1, x_2, \ldots, x_n]$.

18/3/19

$C[x] \longrightarrow C$

$\phi(f(x)) = f(a)$; $a \in C$

$\ker(\phi) = \{(x-a)g(x) \mid g(x) \in C[x]\}$.

$$\frac{C[x]}{\ker \phi} \cong C$$

$\therefore \ker\phi$ is a maximal ideal.

Every maximal ideal of $C[x]$ is of the form $m_a = (x-a)$; $a \in C$.

$$\left\{\begin{matrix}\text{maximal ideals} \\ \text{of } C[x]\end{matrix}\right\} \longleftrightarrow \{\text{pts. of } C\}$$

→ Extension of above theorem to several variable is one of the most important theorem which connects algebra and geometry.

Theorem:

Hilberts Nulls Tollensatz :-

→ The maximal ideals of the poly. ring $R = C[x_1, x_2, \ldots, x_n]$ are in 1-1 correspondence with the pts. in C^n.

A pt. $a = (a_1, \ldots, a_n) \in C^n$.

$C[x_1, x_2, \ldots, x_n] \longrightarrow C^n$

$f(x_1, \ldots, x_n) \rightsquigarrow f(a_1, a_2, \ldots, a_n)$.

kernel of the map $= (x_1-a_1, x_2-a_2, \ldots, x_n-a_n)$

Infact, every maximal ideal of $C[x_1, \ldots, x_n]$ is of the form, $m_a = (x_1-a_1, \ldots, x_n-a_n)$.

No proof ∴ proof in Atlin's Book.

Defⁿ: Let V be a subset of C^n. If V can be defined as the set of common zeroes of a finite number of polynomials in n-variables. then 'V' is called an algebraic variety.

$$V = Z(f_1, \ldots, f_n).$$

Examples: In C^2 every point is a variety because $Z(x-a, y-b)$.

complex line in C^2 is $Z(ax+by+c)$ is a variety.

Theorem:- Let $f_1, f_2, \ldots, f_n$ be polynomials in $C[x_1, \ldots, x_n]$ and $V = Z(f_1, \ldots, f_n)$.

Let $I = (f_1, \ldots, f_n)$.

The maximal ideals of the quotient sings $R = \frac{C[x_1, \ldots, x_n]}{I}$ is in bijective correspondence with the pts. of V.

proof: The maximal ideals of R corresponds to those maximal ideals of $C[x_1, \ldots, x_n]$ which contains I.

Any maximal ideal of the form $(x_1-a_1, \ldots, x_n-a_n)$

Now, $(x_1-a_1, x_2-a_2, \ldots, x_n-a_n) \supset I = (f_1, \ldots, f_n)$.

The maxim
the genera
so, it
which

corollary:-
Let, f_1
in $C[x$
$f_1 = f_2 =$
in C^n

where,

proof:-
$V = Z($
there
Therefore

Example:-

The maximal ideal contains I iff it contains the generator of $f_1, \ldots, f_n$ of I.

So, if $f_i \in m_{\underline{a}}$ iff $f_i(\underline{a}) = 0 \ \forall\ i$.

which implies $\underline{a} \in V(I)$.

corollary:-

Let, $f_1, f_2, \ldots, f_n$ be polynomials in $C[x_1, x_2, \ldots, x_n]$. If the system of eq^{n}s, $f_1 = f_2 = \ldots = f_n = 0$ has no solution in C^n then $1 = \sum_{i=1}^{n} g_i f_i$.

where, $g_i \in C[x_1, x_2, \ldots, x_n]$

proof:-

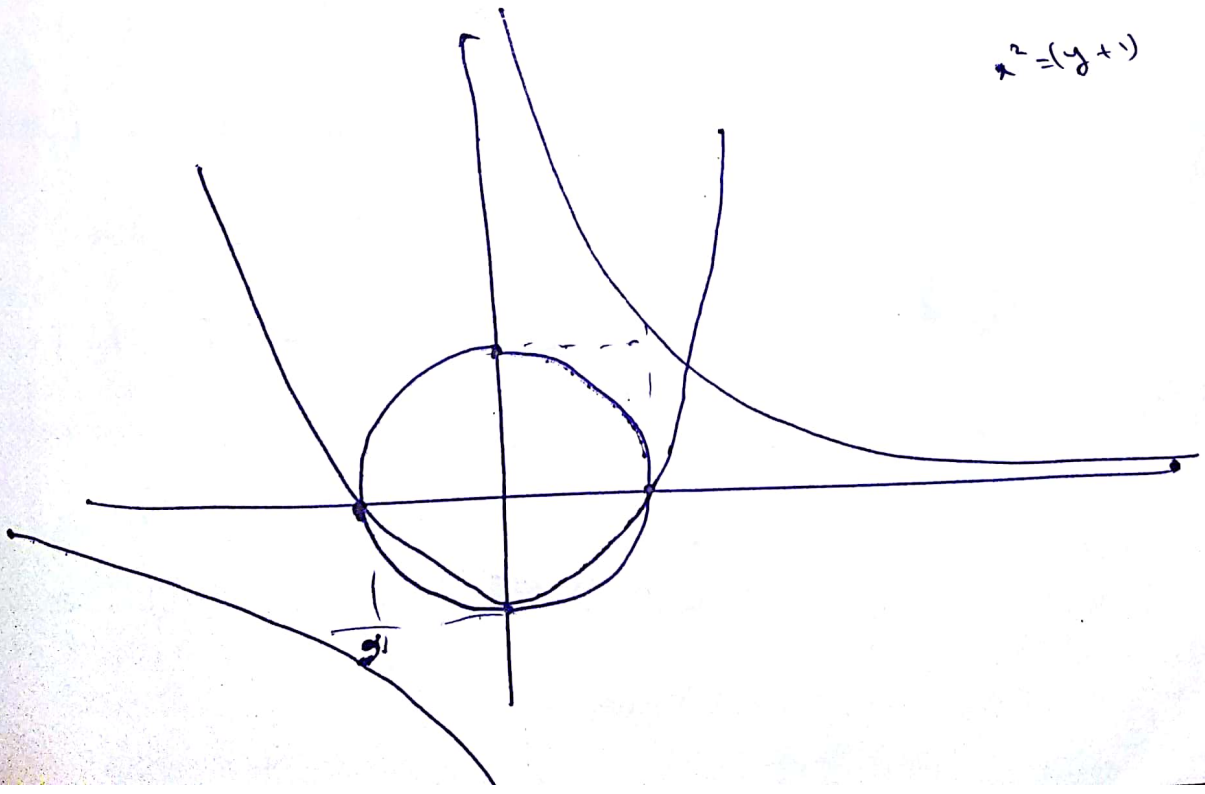
$V = Z(f_1, f_2, \ldots, f_n) = \phi$ which means there is no maximal ideal containing I.

Therefore I is the whole ring i.e. $1 \in I$.

$\therefore \quad 1 = \Sigma\, g_i f_i$

Example:- $f_1 = x^2 + y^2 - 1$; $f_2 = x^2 - y + 1$; $f_3 = xy - 1$

f_1 ↓ circle, f_2 ↓ para., f_3 ↓ hyper.



So, here,

$V(f_1, f_2, f_3) = \phi$ ⟹ $f_0, 1 \in (f_1, f_2, f_3)$.

✱ Unique Factorization Domain :-

Let R be an integral Domain through out.

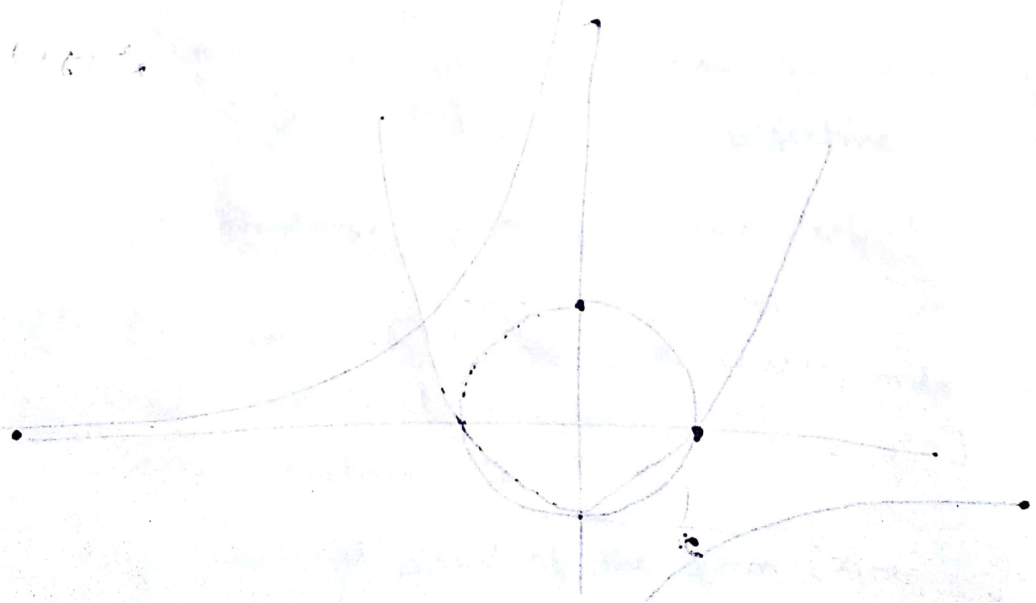
Defⁿ :-

We say an element 'a' divides another 'b' then (a|b) if $b = aq$ for some $q \in R$.

The element 'a' is a proper divisor of 'b' if neither 'a' nor 'q' is an unit.

A non-zero element 'd' of R is called irreducible if 'd' is not a unit and has no proper divisor. [i.e, if $a = bc$ then either 'b' or 'c' is an unit].

We say an element 'a' is prime if (a) is a prime ideal.



18/3/19

Proposition.
Let R be an integral domain and $0 \neq a \in R$.
If a is prime element, then it is irreducible.

Proof (a) is a prime ideal. If $a = bc$, then either b or $c \in (a)$.

WLOG, say $b \in (a) \Rightarrow b = ad$, $d \in R$

$$\therefore \quad a = bc = (ad)c$$

$$a = adc$$

$$\Rightarrow dc = 1 \quad (\because R \text{ is an int. domain})$$

$\Rightarrow$ 'c' is a unit. Hence 'a' is irreducible.

Example: (1) The irreducible elements of $\mathbb{Z}$ are prime numbers.

(2) The irreducible elements of $K[x]$ are irreducible polynomials.

Example: $R = \mathbb{Z}[\sqrt{-3}] = \{ a + b\sqrt{-3} \mid a, b \in \mathbb{Z} \}$

Consider 2.

$$2 = (a + ib\sqrt{3})(e + id\sqrt{3}) \; ; \quad a, b, c, d \in \mathbb{Z}$$

$$2 \cdot \bar{2} = (a+ib\sqrt{3})(a-ib\sqrt{3})(e+id\sqrt{3})(e-id\sqrt{3})$$

$$4 = (a^2+3b^2)(e^2+3d^2)$$

$\therefore (a^2+3b^2)$ must divide 4, and a^2+3b^2 cannot be 2 $\longrightarrow$ Hence, $a^2+3b^2 = 4$ and $e^2+3d^2 = 1$. (and vice-versa).

$\Rightarrow d = 0$, $e = \pm 1$.

∵ one of the factors of 2 is an unit

⇒ Thus, 2 is an irreducible element

$(1+\sqrt{-3}).(1-\sqrt{-3}) = 4 \in (2)$.

But neither $(1+\sqrt{-3})$ nor $(1-\sqrt{-3}) \in (2)$

∴ (2) is not a prime ideal

Hence 2 is not a prime ideal.

Defⁿ: A unique factorization domain (UFD) is an int. domain R satisfying that :-

1.) every element $0 \neq a \in R$ can be written as a product of irreducible factors say, $p_1, \ldots, p_n$ upto units namely

$$a = x p_1 p_2 \cdots p_n .$$

2.) The above factorization is unique if

$$a = u p_1 p_2 \cdots p_n = v a q_1 \cdots q_m$$

are two factorization and irreducible elements p_i and q_i with units 'u' and 'v' then $n=m$ and p_i and q_i are associats.

proposition:-

We say that two elements $a, b \in R$ are associates if $a = xb$ for some unit $x \in R$.

Examples:-

① $\mathbb{Z}$, $K[x]$ are UFD.

proposition:- In a

iff a

proof:- let : a

WTS (a)

Let

since,

into ir

(v b1 ...

since

be a

⇒

proposition

Let

① 'a'

②

③

④

⑤

proposition:- In a UFD, an element 'a' is irreducible iff a is a prime.

proof:- Let 'a' be a non-zero irreducible element
WTS (a) is a prime ideal.
Let $bc \in (a)$

$\Rightarrow bc = ad$; $d \in R$

Since, R is a UFD, it can be decomposed into irreducible factors.

$(vb_1 \dots b_s)(w c_1 \dots c_t) = a \cdot (u d_1 \dots d_n)$

Since the factorization is unique, 'a' must be associate to some c_i or b_i

$\Rightarrow$ 'a' divides 'b' or 'c'.

$\Rightarrow$ Hence (a) is a prime ideal.

proposition:-
Let 'R' be an integral domain and $a, b \in R$, Then,

① 'a' is a unit iff $(a) = R$.

② 'a' and 'b' are associates iff
$(a) = (b)$.

③ a/b iff $(b) \subseteq (a)$

④ 'a' is a proper divisor of 'b' iff
$(b) \subseteq (a) \subseteq R$.

⑤ 'a' is irreducible iff (a) is maximal among proper principal ideals of R.

Def'n: An integral domain R is called factorization domain if every non-zero element of R can be written as a product of irreducible elements.

Proposition: Let R be an integral domain:

TFAE

① For every non-zero element $a \in R$, which is not a unit, the process of factoring a terminates after finitely many steps and result a factorisation of a into irreducible elements.

② R doesn't contain an infinite increasing chain of principal ideals.

$$\alpha (a_1) \subset (a_2) \subset (a_3) \subset$$

proof: R contains an infinite increasing sequence, $(a_1) \subset (a_2) \subset \dots \subset (1)$

for all n.

Since, $(a_{n-1}) \subset (a_n)$, $\rightarrow a_{n-1} = a_n b_n$

where, a_n, b_n are not units.

$\Rightarrow a_1 = a_2 b_2 = a_3 b_3 b_2 = \dots$

Ex: Do the converse.

Example:

Let

where,

and

→ we

and

GC

In

N

I

In

propo

of

irr

Example: consider the polynomial ring $k[x_1]$.

Let $R = k[x_1, x_2, \ldots]$

where, $x_2^2 = x_1$, $x_3^2 = x_2$, $x_4^2 = x_3$, $x_5^2 = x_4$, ...

and we can factor x_1 as :-

$$x_1 = x_2^2 = (x_3^2)^2 = \ldots$$

→ we can factor x_1 indefinitely in the Ring R, and get an infinite chain.

$$(x_1) \subset (x_2) \subset (x_3) \subset \ldots$$

GCD

In $\mathbb{Z}$: $a, b \in \mathbb{Z}$

$$(a,b) = (d) \qquad [\mathbb{Z} \text{ is a PID}]$$

Now, $d = \gcd(a,b)$

If $\gcd(a,b) = 1$

then $(a,b) = (1)$

$\Rightarrow 1 = ar + bs$.

In $\mathbb{Z}[x]$, consider $(2,x)$

Now, $\gcd(2,x) = 1$

but, $1 \neq 2r + xs$.

Proposition:

Let 'a' and 'b' be two non-zero elements of a UFD, and let,

$$a = u p_1^{e_1} \ldots p_m^{e_m} \qquad (p_i\text{'s are distinct})$$

$$b = v p_1^{b_1} \ldots p_m^{b_m}$$

are unique factorizations of a, b into irreducible where u, v are units, and p_i's are distinct.

Let the element $d = p_1^{\min(r_1,s_1)} \cdots p_n^{\min(r_n,s_n)}$ is the gcd of 'a' and 'b'.

~~Ex~~

* An integral domain 'R' is called a principal ideal domain (PID) if every ideal of R is principal ideal.

Ex:- $\mathbb{Z}$, $k[x]$. are PID.

⇒ In a PID, irreducible elements are prime.

Let p be an irreducible element.

WTS (p) is a prime.

Let $ab \in (p) \Rightarrow p \mid ab$

let, $p \nmid a$. Then $(p) \subsetneq (p, a)$

** (p) is maximal among all the principal ideals, $(p, a) = (1)$.

$\Rightarrow 1 = pc + ad$ for $c, d \in R$.

$b = pcb + abd \in (p)$ $(ab \in p)$

$\therefore (p)$ is a prime ideal.

→ Every non-zero prime ideal in a PID is a maximal ideal.

proof:- Let (p) is
Then,
$\Rightarrow p$
Since,
then
If
ideal
some,

Corollary
a PI

proof:-

$\Rightarrow$
Since,
max

Ex:-

Proof:- Let (p) be a non-zero prime ideal, and (p) is not a maximal ideal.

Then, $\exists$ a maximal ideal s.t $(p) \subset (m)$.

$\Rightarrow p = rm$ for some $r \in R$.

Since, (p) is a prime ideal, and $rm \in (p)$ then either $r \in (p)$ or $m \in (p)$.

If $m \in (p)$, then $(p) = (m)$ is a maximal ideal of $r \in (p)$, then $r = p \cdot s$ for some, $s \in R$.

$\therefore p = psm \Rightarrow sm = 1$ ($\because$ R is integral domain).

$\Rightarrow$ 'm' is a unit.

Hence its proved.

Corollary:- Let 'R' be any ring and $R[x]$ is a PID. Then R is a field.

Proof:- $\frac{R[x]}{(x)} \cong R$

$R \subset R[x]$

↳ R is an integral domain.

$\Rightarrow (x)$ is a prime ideal.

Since, $R[x]$ is a PID, so (x) is a maximal ideal. Hence R is a field.

Ex:- A PID is an UFD.

25/3/19

Proposition:- A 'PID' is an 'UFD'.

proof:- WTS. Existence of factorisation in R. which is equivalent to show, R contain no infinite increasing chain of principal ideal.

suppose, $(a_1) \subset (a_2) \subset \ldots\ldots$

is an infinite chain of principal ideals.

Let I be the union of this chain of principal ideals Then I is an ideal.

Since 'R' is a PID, so $I = (b)$.

Now, since 'b' is in the union of the ideals (a_n), it is one of these ideals $b \in (a_n)$.

On the other hand.

$$(a_n) \subset (a_{n+1}) \subset (b).$$

$$\therefore (a_n) = (a_{n+1}) = (b).$$

which is a contradiction.

→ Therefore every element of R can be written as products of irreducible elements. Since every irreducible elements. Since every irreducible is prime so 'R' is an 'UFD'.

Example:- $\mathbb{Z}[x]$ is an UFD. but not a PID. ??

→ Euclidean Domain.

Let us now abstract the procedure of division with remainder. To do this we need notion of size of an element of a ring. In general a size of an integral domain 'R'

will be any function fn

$N : R \setminus \{0\} \to \{0, 1, 2, \ldots\}$

from the set of non-zero elements of R to the set of non-negative integers.

Def^n: An integral domain 'R' is an Euclidean domain if there is a size function N on R s.t for all $a, b \in R$ s.t $b \neq 0$ there are elements $q, r \in R$ s.t $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$ where q is called the quotient and 'r' is the remainder.

Ex:- (1) Fields are E.D where if $N(a) = 0 \; \forall \; a$ then $a = qb + 0$ where, $q = ab^{-1}$.

(2) $\mathbb{Z}$ is an E.D with $N(a) = |a|$.

(3) If F is a field the $F[x]$ is ED with $N(f(x)) = \deg(f(x))$.

***

(4.) $\mathbb{Z}[i]$:= Ring of Gaussian integers.

$= \{a + bi \mid a, b \in \mathbb{Z}\}$.

is an E.D with $N(a+ib) = a^2 + b^2$.

→ Let $\alpha = a + ib$; $\beta = c + id \neq 0$.

$$\frac{\alpha}{\beta} = \frac{a+ib}{c+id} \times \frac{c-id}{c-id} = \frac{(ac+bd) + i(bc-ad)}{c^2+d^2}$$

$= r + is \notin \mathbb{Z}[i]$

$\in \mathbb{Q}[i]$.

Let p and q be integers closest to r & s respectively.

$\therefore |r-p|$ & $|s-q|$ are atmost $1/2$.

$$\theta = (r-p) + i(s-q).$$

$$\gamma = \beta \cdot \theta = \beta[(r-p) + i(s-q)]$$

$$= \beta(r+is) - \beta(p+iq).$$

$$= \alpha - \beta(p+iq)$$

$\therefore \alpha = \beta(p+iq) + \gamma$.

$$N(\gamma) = N(\beta \cdot \theta) \xrightarrow{\text{EXERCISE.}} = N(\beta) \cdot N(\theta)$$

$$= N(\beta) \cdot [(r-p)^2 + (s-q)^2]$$

$$\leq N(\beta) \cdot \left[\frac{1}{4} + \frac{1}{4}\right]$$

$$\leq \frac{1}{2} \cdot N(\beta).$$

$\therefore$ $N(\gamma) < N(\beta)$.

$\therefore$ $\mathbb{Z}[i]$ is an E.D.

H.W

Theorem:-

Let R be an E.D then R is a PID.

Ex:- Find the units in $\mathbb{Z}[i]$.

26/3/19.

Field $\subset$ E.D $\subset$ PID $\subset$ UFD $\subset$ Int. domain.

- $\mathbb{Z}$ is an E.D but not a field.
- $\mathbb{Z}\left[\frac{(1+\sqrt{-19})}{2}\right]$ is a PID but not ED.
- $\mathbb{Z}[x]$ is an UFD but not a PID.
- $\mathbb{Z}[\sqrt{-3}]$ is an int. domain but not UFD.

$\mathbb{Z}[i]$ → Ring of Gaussian integers.

If $u \in \mathbb{Z}[i]$ is a unit in $\mathbb{Z}[i]$ then, $N(u) = 1$ and the units are $\pm 1, \pm i$.

Defⁿ A prime element in $\mathbb{Z}[i]$ is called a Gaussian prime.

Propositions:

1.) if $N(a+ib) = a^2+b^2 = p$ is a prime number then $a+ib$ is a gaussian prime.

2.) If π is a Gaussian prime then, $N(\pi) = \pi \cdot \bar{\pi}$ is either a prime number or a square of a prime number.

Proof (1.) Let $\alpha = a+ib$ st $N(\alpha) = p$.

WTS, α is a prime element.

Since, $\mathbb{Z}[i]$ is an ED so it is an UFD, have prime is equivalent to irreducible element. WTS α is an irreducible element.

⇒ Let, $\alpha = \beta \cdot \gamma$ where, $\beta, \gamma \in \mathbb{Z}[i]$

Then, $N(\alpha) =$

Hence it

Thus α is

(2.) Let π b

WTS. $N(\pi$

square

$(\pi) \cap \mathbb{Z}$

integer

→ $(\pi) \cap \mathbb{Z}$

Exercise S

Hence,

∴

∴

N

N(p

Theorem:-

Th

in

1.) $p =$

2.) $p =$

3.) x

4.)

Then, $N(\alpha) = N(\beta\gamma) = N(\beta) \cdot N(\gamma) = p$.

Hence either, $N(\beta)$ or $N(\gamma)$ is an unit.

Thus α is irreducible have a prime element.

(2) Let π be a Gaussian prime.

WTS. $N(\pi)$ is either a prime number or square of a prime number.

$(\pi) \cap \mathbb{Z} \neq (0)$ since $\overline{\pi} \cdot \pi$ is a non-zero integer.

→ $(\pi) \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$. and it's a subgroup.

Exercise6 Show that $(\pi) \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.

Hence, $(\pi) \cap \mathbb{Z} = (p)$, for some prime number p.

$\therefore p \in (\pi)$.

$\therefore p = \pi \cdot \mu$ → element of the Gaussian prime.

$N(p) = N(\pi \cdot \mu) = N(\pi) \cdot N(\mu)$.

$N(p) = p^2 = N(\pi) \cdot N(\mu)$.

$N(\pi) = p$ or p^2.

Theorem:-

The following are equivalent for prime integer p.

1) $p = \pi \cdot \overline{\pi}$, where π is a Gaussian prime.

2) $p = a^2 + b^2$, for $a, b \in \mathbb{Z}$.

3) $x^2 \equiv -1 \pmod{p}$ has an integral sol^n.

4) $p = 2$ or $p \equiv 1 \pmod{4}$.

proof (1) ⇒ (2).

Let, $\pi = a+ib \in \mathbb{Z}[i]$.

Then, $\pi \cdot \bar{\pi} = a^2+b^2 = p$.

(2) ⇒ (3)

If $p = a^2+b^2$ then $a, b \neq 0$.

$$a^2 \equiv -b^2 \pmod{p}.$$

Since, $\mathbb{Z}/p\mathbb{Z}$ is a field.

$$\therefore (ab^{-1})^2 \equiv -1 \pmod{p}.$$

(3) ⇒ (4)

Assuming (3) is true we have to prof (4) is true:

Let, p be an odd prime.

Let $a \in \mathbb{Z}/p\mathbb{Z}$ and $a^2 \equiv -1 \pmod{p}$.

Then, $O(a) = 4$ in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$.

Hence, $4 \mid p-1$ (→ divides) $\Rightarrow p \equiv 1 \pmod 4$.

(4) ⇒ (3)

For $p = 2$.

→ 1 is a solution to, $x^2 \equiv -1 \pmod{p}$.

Now let $p \equiv 1 \pmod 4 \Rightarrow 4 \mid p-1$.

Consider the group $(\mathbb{Z}/p\mathbb{Z})^*$ whose order is $p-1$.

{Go to Sylow's th^m once}.

→ Since, $4 \mid p-1$, so there is a subgroup of order 4 is there in $(\mathbb{Z}/p\mathbb{Z})^*$.

Let H be the
and let H
$a^4 \equiv 1$

$\Rightarrow p \mid a^4-1 \Rightarrow$

If $p \mid a^2-1$
which is

$\therefore p \mid a^2+$

Claim:-
$(\mathbb{Z}/p\mathbb{Z})$

If $m^2 \equiv$

$\Rightarrow p \mid (m+1)$

$m \equiv -1 \pmod$

So, -1
order

(3) ⇒ (1)

$\mathbb{Z}$

$\mathbb{Z}[i]$
(p)

and let H is cyclic subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ of order 4
$a^4 \equiv 1 \pmod p$. $\Rightarrow \exists$ 'a' s.t

$\Rightarrow p \mid a^4-1 \Rightarrow p \mid (a^2-1)(a^2+1)$

If $p \mid a^2-1$ then $a^2 \equiv 1 \pmod p$
which is a contradiction since $o(a) = 4$.

$\therefore p \mid a^2+1 \Rightarrow a^2 \equiv -1 \pmod p$.

Claim:-
$(\mathbb{Z}/p\mathbb{Z})^*$ contains a unique element of order 2.

If $m^2 \equiv 1 \pmod p \Rightarrow p \mid m^2-1 \Rightarrow p \mid (m-1)(m+1)$

$\Rightarrow p \mid (m+1)$ or $p \mid (m-1)$.

$\downarrow\!\downarrow$ $\qquad$ $\downarrow\!\downarrow$

$m \equiv -1 \pmod p$; $m \equiv 1 \pmod p$

So, -1 is the unique residue class of order 2 in $(\mathbb{Z}/p\mathbb{Z})^*$.

(3) $\Rightarrow$ (1)

$\mathbb{Z}[i] \overset{\text{isomorphic}}{\cong} \frac{\mathbb{Z}[x]}{(1+x^2)}$

$\frac{\mathbb{Z}[i]}{(p)} \cong \frac{\mathbb{Z}[x]}{(p, 1+x^2)}$

$\frac{\mathbb{Z}[x]/(1+x^2)}{p \cdot \mathbb{Z}[x]/(1+x^2)} \cong \frac{\mathbb{Z}[x]/(1+x^2)}{(p, x^2+1)/(1+x^2)} \cong \frac{\mathbb{Z}[x]}{(p, x^2+1)}$

$$\frac{\mathbb{Z}[x]}{(p, x^2+1)} \cong \frac{\mathbb{Z}[x]/p\mathbb{Z}[x]}{(p, x^2+1)/p\cdot\mathbb{Z}[x]} \cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+\bar{1})}$$, image of

---

Ex:- $\frac{\mathbb{Z}[x]}{p\cdot\mathbb{Z}[x]} \cong \frac{\mathbb{Z}}{p\cdot\mathbb{Z}[x]}$

→ We have $x^2 \equiv -1 \pmod{p}$ has a solution,

$\exists$ 'a' s.t, $a^2 \equiv -1 \pmod{p}$.

Thus, 'p' is not an irreducible element in $\mathbb{Z}[i]$

Let, $p = \pi \cdot \delta$, where δ and π are not unit

$\therefore N(p) = N(\pi) \cdot N(\delta) = p^2$.

Thus, $N(\pi) = p \cdot = \pi \cdot \bar{\pi}$

Corollary: [Fermet's two square theorem]

Let 'p' be a prime no. then p is a sum of two square iff $p = 2$ or $p \equiv 1 \pmod{4}$.

Corollary:

The irreducible elements of $\mathbb{Z}[i]$ are:

1.) $(1+i)$ and its associates.

2.) Rational primes 'p' s.t, $p \equiv 3 \pmod{4}$. (then the p itself is a Gaussian prime)

3.) $a+ib$, $a-ib$ the distinct irreducible factor of $p = a^2+b^2$. for the prime $p \equiv 1 \pmod{4}$. {in this case factors of 'p' are Gaussian prime}.

⇒ Polynomial rings over UFD:-

Q.) Let R be an UFD. Is R[x] an UFD?

→ We know that F[x] is an UFD where F is field. Let K be the quotient field of R. Then R[x] is a subring of K[x]. Since K[x] is an UFD. we try to relate factorization in R[x] and K[x].

Q.) Let $f(x) \in Z[x]$ is reducible then is it reducible in $\mathbb{Q}[x]$?

Q.) Is an irreducible polynomial over Z[x] remains irreducible over $\mathbb{Q}[x]$?

E.g:- consider the polynomial $2x \in Z[x]$. Then $2x = 2 \cdot x$ in $Z[x]$ and 2 is not an unit so $2x$ is reducible. But $2x$ is irreducible over $\mathbb{Q}[x]$. because 2 is a unit in $\mathbb{Q}$.

Def:- Let R be an UFD. The content of $f(x) \in R[x]$ denoted by $c(f)$ is the gcd of coefficients of $f(x)$. If $c(f) = 1$ we say $f(x)$ is "primitive"

Theorem: Let R be an UFD. If $f(x), g(x) \in R[x]$ are primitive then $f(x) \cdot g(x)$ is also primitive.

Proof: Suppose $f(x) \cdot g(x)$ is not primitive. Let p be a prime in R dividing the coefficients of $f(x) \cdot g(x)$.

Consider the following map $\pi : R[x] \to R[x]$

$$\pi\left(\sum a_n x^n\right) = \sum \bar{a}_n x^n \quad \{ \text{here, } \bar{a}_n = a_n + p \}$$

Then, $\overline{f(x) \cdot g(x)} = \bar{0}$

$\Rightarrow \bar{f}(x) \cdot \bar{g}(x) = \bar{0}$ in $\frac{R}{p}[x]$.

$\rightarrow$ Since, $\frac{R}{p}[x]$ is an integral domain. so either $\bar{f}(x) = \bar{0}$ or $\bar{g}(x) = \bar{0}$.

Hence, either $p \mid c(f)$ or $p \mid c(g)$, which is a contradiction.

Corollary: For $f(x), g(x) \in R[x]$ we have

$$c(fg) = c(f) \cdot c(g).$$

Proof: Let $c(f) = a$ and $c(g) = b$.

Then, $f(x) = a \cdot f_1(x)$ and $g(x) = b \cdot g_1(x)$.

where, $c(f_1) = 1$ and $c(g_1) = 1$.

$$f(x) \cdot g(x) = ab \cdot f_1(x) \cdot g_1(x).$$

Since $f_1(x), g_1(x)$ are primitive so $f_1(x) \cdot g_1(x)$ is also primitive.

Hence $c(fg) = ab = c(f) \cdot c(g)$.

$\Rightarrow$ suppose $f(x)$ and $f(x)$ & $g(x)$

b) Is $f(x)$ & g

proposition: Let R be a

If $f(x)$, $g(x)$ associate associate

proof: Let $f(x)$

Then, $b \cdot$

since, $c($ $b \cdot f$

since in multiple u is

$\therefore f($

***** proposition:**

* Let R and in $K[$

More pre non co

Then s.t.

and

is a

i) suppose $f(x)$, $g(x) \in R[x]$ both primitive and $f(x)$ & $g(x)$ are associates in $K[x]$.

ii) Is $f(x)$ & $g(x)$ are associates in $R[x]$?

proposition: Let R be an UFD with quotient field K. If $f(x)$, $g(x) \in R[x]$ are primitive and associates in $K[x]$ then, they are associates in $R[x]$.

proof: Let $f(x) = \frac{a}{b} \cdot g(x)$ $b \neq 0$ and $a, b \in R$

Then, $b \cdot f(x) = a \cdot g(x)$.

Since, $f(x)$ and $g(x)$ are primitive so $c(b \cdot f) = b$ and $c(a \cdot g) = a$.

Since in a UFD the gcd is unique upto multiple by a unit so, $a = ub$. where u is a unit in R.

$\therefore f(x) = u \cdot g(x)$. where $u \in R$ is an unit.

***proposition: [Gauss lemma]

* Let R be an UFD with quotient field K and let $p(x) \in R[x]$. If $p[x]$ is reducible in $K[x]$ then $p(x)$ is reducible in $R[x]$.

More precisely, if $p(x) = A(x) \cdot B(x)$ for some non constant polynomials $A(x)$ and $B(x) \in K[x]$.

Then there are non-zero elements $r, s \in K$ s.t, $r \cdot A(x) = a(x)$ and $s \cdot B(x) = b(x)$.

and $p(x) = a(x) \cdot b(x)$ where $a(x), b(x) \in R[x]$ is a factorization in $R[x]$.

[Try its prove]