

28th Feb

Ring: A ring R is a set with 2 binary operations called addition (+) and multiplication (\cdot) which satisfies the foll. prop.

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

(2) Multiplication is associative i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ & $a, b, c \in R$

(3) $\exists 1 \in R$ s.t. $1 \cdot a = a \cdot 1 = a \forall a \in R$ is called multiplicative identity.

(4) Distributive law

$$(a+b) \cdot c = ac + bc \text{ &}$$

$$c(a+b) = ca + cb \text{ & } a, b, c \in R$$

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

Example: ① $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ are all commutative ring

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

③ $C(\mathbb{R}) = \{f: \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ is continuous}\}$
is a ring w.r.t

$$(f+g)(x) = f(x) + g(x) \text{ &}$$

$(fg)(x) = f(x) \cdot g(x)$ which is commutative

④ Let R be a ring.

$R[x] =$ The 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 the additive identity.

Remark: Let R be a ring in which
 $1 = 0$ (add. id. = mult. id.). Then R is
the 0 ring. (using associativity)

Let $a \in R$. $a = a \cdot 1 = a \cdot 0 = 0$
 $\therefore R$ is a zero ring

Defn: An element $0 \neq u \in R$ 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 $1, -1$.
② $R[x]$ the units are non zero constant polynomials.

Definition: Let R be a Ring. A non zero element $a \in R$ is called a zero divisor.

if \exists a non zero elt. ~~s.t. that~~ $b \in R$ s.t. $a \cdot b = 0$ or $b \cdot a = 0$.

Ex consider the Ring $\mathbb{Z}/6\mathbb{Z}$.

$$\bar{2} \cdot \bar{3} = \bar{0}$$

$$\bar{2} \neq \bar{0}, \bar{3} \neq \bar{0}.$$

$\therefore \bar{2}$ is a ~~zero divisor~~ zero divisor.

Observe that a zero divisor can never be a unit. Suppose that a is a unit and a zero divisor. Then \exists nonzero b s.t. $ab = 0$. If a is a unit. Then $\exists a' \in R$ s.t.

$$aa' = a'a = 1 \quad \therefore a'(ab) = 0$$

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

$$\Rightarrow b = 0 \quad \Rightarrow$$

Definition: A subring of a ring R is a subgroup of R which is closed under multiplication and contain 1.

Example: ① \mathbb{Z} is a subring of \mathbb{Q} and \mathbb{Q} is a subring of \mathbb{R} .



Propositions Let R be a ~~ring~~ ring. Then

- i) $0 \cdot a = a \cdot 0 = 0 \quad \forall a \in R$
- ii) $(-a) \cdot b = a \cdot (-b) = -ab \quad \forall a, b \in R$
- iii) $(-a) \cdot (-b) = ab \quad \forall a, b \in R$
- iv) $(-a) = (-1) \cdot (a) \quad \forall a \in R$

Ring Homomorphism

Let R and S be 2 rings.

Then a map $\phi: R \rightarrow S$ is called a ring homomorphism.

$$\text{if } \phi(a+b) = \phi(a) + \phi(b)$$

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

and $\phi(1_R) = 1_S$. \rightarrow [It is not used in all books]

Defⁿ: Let $\phi: R \rightarrow S$ be a ring home.

$$\text{Then } \ker \phi = \{a \in R \mid \phi(a) = 0\}$$

Qⁿ Is $\ker \phi$ a subring of R ?

3rd March

Let $\phi: R \rightarrow S$ be a ring homomorphism
 $\text{ker } \phi = \{a \in R \mid \phi(a) = 0\}$

A bijection homo is called an ^{isomorphism}

A bijection homo is called a ring homo.

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

The image of ϕ is a subring of S .

① The kernel of ϕ is not a subring of R

unless it is the whole ring R .

Furthermore, if $x \in \text{ker } \phi$ then xz and

$zx \in \text{ker } \phi$ for $z \in R$.

$xr \in \text{ker } \phi$ & $r \in R$.

Proof: For any $r \in R$ & $x \in \text{ker } \phi$.

$$\phi(xr) = \phi(x)\phi(r) = 0 \cdot \phi(r) = 0$$

$\therefore xr \in \text{ker } \phi$.

Similarly $rx \in \text{ker } \phi$.

Definition: 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. $rI \subseteq I$.

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. $Ir \subseteq I$

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

Example

① $f: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$.

$f(m) = \bar{m}$
check that f is a ring homomorphism

② consider $f: \mathbb{R}[x] \rightarrow \mathbb{R}$

$$f(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n a_i x^i \quad \text{where } a_i \in \mathbb{R}$$

check f is a ring homomorphism

③ Define $\phi: \mathbb{Q}[x] \rightarrow \mathbb{R}$

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

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

Claim: $\text{Ker } \phi = \{(x^2 - 2)q(x) \mid q(x) \in \mathbb{Q}[x]\}$

Note that: if $f \in \text{Ker } \phi$ then f cannot be a linear polynomial.

Also $(x^2 - 2) \in \text{Ker } \phi$.

Let $g(x) \in \text{Ker } \phi$.

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

where $\deg r(x) < 2$ or $r(x) = 0$.

$$r(x) = g(x) - (x^2 - 2)q_1(x)$$

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

$$\Rightarrow r(x) = 0.$$

$$\Rightarrow g(x) = (x^2 - 2)(q_1(x))$$
$$\therefore \ker \phi = \{(x^2 - 2)q_1(x) \mid q_1(x) \in \mathbb{Q}[x]\}$$

In any ring R , the set of multiples of a particular element ' a ' forms an ideal called principal Ideal generated by a . and is denoted by $(a) = \{ar \mid r \in R\}$ [Hence R is commutative]

Note: Assume now onwards that the rings are commutative
In a ring of integers the ideals are of the form $n\mathbb{Z}$, or are formed by the single element

We may consider the ideal generated by a set of elements $a_1, a_2, \dots, a_n \in R$

which is defined to be the smallest ideal containing these elements and it is denoted by $(a_1, a_2, \dots, a_n) = \{r_1a_1 + \dots + r_na_n \mid r_i \in R\}$

In any ring R , the set consisting of zero alone is an ideal called the zero ideal and it is the called the unit ideal denoted by (1) . The unit ideal is the only ideal which contains a unit

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

There is no proper ideal in a field.

Proposition: ① Let F be a field. The ideals of F are zero and unit ideal.
② Conversely, if a ring R has exactly 2 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 2 different ideals. Let $a \neq 0$ be an element of R .
(a) $= (1)$, i.e. $\exists b \in R$ s.t. $a = b \cdot 1 \therefore a$ is a unit.

Proposition: Let F be a field and R' be a non zero ring and $\phi: F \rightarrow R'$ be a mapping hom.

Proof: Since F is a field therefore

$\ker \phi$ is either (0) or (1) .

But if $\ker(\phi) = (1)$ then R' will be

a 0 zero ring

$\Rightarrow \Leftarrow$

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

Definition: 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 is 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 polynomial of $f(x)$ having smallest positive degree in I .

Let $f(x) \in I$ having smallest positive degree. Let $g(x) \in I$. Then by division algo we have

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

where $\deg(r(x)) < \deg f(x)$ or $r(x) = 0$.

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

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

$$\therefore g(x) = f(x)q(x) \in (f(x)).$$

Remark: $\mathbb{Z}[x]$ is not a Principal Ideal.

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

Since $2 \in (f)$. $\therefore 2 = f \cdot g$.

Since $\deg(2) = 0 \Rightarrow \deg(f) = 0$

$\Rightarrow f | 2 \Rightarrow f = \pm 1, \pm 2$.

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

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

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

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

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

Integral Domains

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

Example: ① Fields are PIR domains.
② \mathbb{Z} is an PIR domain.
③ $F[x]$ where F is a field is an integral domain.

④ $C(\mathbb{R}) = \{f: \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ is cont}\}$

$C(\mathbb{R})$ is not an integral domain.

Define: $f: \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = \begin{cases} 0 & \forall x \leq 0 \\ x & \forall x > 0 \end{cases}$

$g: \mathbb{R} \rightarrow \mathbb{R}$ by $g(x) = \begin{cases} x & \forall x < 0 \\ 0 & \forall x \geq 0 \end{cases}$

Then $f.g = 0$ but $f \neq 0$ & $g \neq 0$

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

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

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

$\therefore R$ is integral domain

$$\Rightarrow a \neq 0$$

$$\Rightarrow b - c = 0 \Rightarrow \underline{\underline{b=c}}$$

Proposition: A finite integral domain is a field

Proof: Let R be a finite integral domain

Let $0 \neq x \in R$. WTS x is a unit.

Consider the element x, x^2, x^3, \dots

$\therefore R$ is a finite set $\exists r > s$ s.t.

$$x^r = x^s$$

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

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

(As it is an integral domain $x^s \neq 0$)

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

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

$\therefore x$ has an inverse

$\Rightarrow R$ is a field

F. - F

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 form a group R/I . Now want to show R/I has a ring structure. Want to define multiplication of two cosets.

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

Well Defined: $a+I = a'+I$
 $b+I = b'+I$

WTS: $ab+I = a'b'+I$

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

Say $a=a'+i_1$, & $b=b'+i_2$.

$$\Rightarrow ab = (a'+i_1)(b'+i_2)$$

$$= a'b' + \underbrace{a'i_2 + i_1b' + i_1i_2}_{\in I}$$

$$= a'b' + i$$

$$\Rightarrow ab - a'b' = i$$

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

1st Isomorphism Theorem

Let $f: R \rightarrow S$ be a surjective ring homomorphism.
 Let $I = \ker f$. Then $R/I \cong S$.

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

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

Exercise Check \bar{f} is well defined WTS

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

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

$$= f(ab) = f(a)f(b)$$

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

$\therefore \bar{f}$ is a Ring homomorphism.

Since f is surjective so \bar{f} is surjective

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

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

$$= \{I\} \quad \therefore \bar{f} \text{ is injective}$$

(Take 0 as representative)

Hence \bar{f} is an isomorphism.

$$\therefore R/I \cong S$$

Example: $\mathbb{R}[x]$.

$$\phi: \mathbb{R}[x] \rightarrow \mathbb{C}$$

$$\phi(r) = r \quad \forall r \in \mathbb{R}$$

$$\phi(x) = i$$

ϕ is a ring homomorphism

ϕ is a surjective ring homomorphism

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

Note that $(x^2 + 1) \in \text{ker } \phi$.

Let $g(x) \in \text{ker } \phi$.

By division algorithm.

$$\Rightarrow g(x) = (x^2 + 1) q_r(x) + r(x)$$

where either $\deg r(x) < 2$ or $r(x) = 0$

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

$$r(i) = g(i) - 0 \cdot q(i)$$

$$\underline{\underline{r(i) = 0}}$$

$\Rightarrow r(x) \in \text{ker } \phi$.

$r(x) = 0$. Since $\deg r(x) < 2$.

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

\therefore By first isomorphism theorem.

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

$$\hookrightarrow x^2 + 1 = 0 \Rightarrow x^2 = -1$$

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

$$\hookrightarrow a + bi$$

$$\frac{\mathbb{R}[x]}{(x^2)}$$

$$\frac{\mathbb{R}[x, y]}{(y^2)}$$

$$\text{Ex. } \phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[i] := \left\{ \frac{a+bi}{a, b \in \mathbb{Z}} \right\}$$

Gaussian
Integers

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

Ex: show that $\frac{\mathbb{Z}[i]}{1+3i} \cong \frac{\mathbb{Z}}{10\mathbb{Z}}$

$$\mathbb{Z}[i] = a + bi$$

$$\mathbb{Z}[i]/1+3i =$$

Homomorphism Theorem

Let $f: R \rightarrow S$ be a surjective ring hom. Then
 \exists a bijection b/w the set
 {all ideals of R containing K } \longleftrightarrow {all ideals of S }

$$J \rightsquigarrow f(J)$$

$$f^{-1}(I) \leftarrow I$$

Proof Step 1: WTS
 $f(J)$ is an ideal of S . Clearly $f(J)$ is a
 subgp of S . Let $s \in S$ & $a \in f(J)$. WTS $sa \in f(J)$
 since f is surj. $\exists x \in R$ s.t. $f(x) = s$
 & $\exists b \in J$ s.t. $a = f(b)$
 $sa = f(x) \cdot f(b) = f(xb) \in f(J)$

2nd Step $f^{-1}(I) = \{a \in R \mid f(a) \in I\} \cong K$

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

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

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

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

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

\downarrow
 $\in I$

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

(We have shown that a Ring Homomorphism maps to an ideal too. Also the preimage of an ideal on a Ring homomorphism need not map to the ideal. Note: Homo need not be invertible) Note:

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

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

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

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

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

$$\Rightarrow f(a) \in f(J)$$

$$\Rightarrow f(a) = f(y) \quad y \in J$$

$$\Rightarrow f(a-y) = 0 \quad (K \rightarrow \text{Kernel})$$

$$\Rightarrow a-y \in K \subseteq J$$

$$\Rightarrow a \in J \quad (\text{Because Kernel Ideal is contained in the Ideal})$$

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

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

Let $a \in I$.

$\therefore f$ is surjective

$$\exists x \in R \text{ s.t. } f(x) = a \in I$$

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

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

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

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

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

By previous Thm, \exists a bijection between $\{\text{ideals of } R\}$ and $\{\text{ideals of } R/I\}$.

IDEALS OF $R = \{k \in \mathbb{Z}\} \leftrightarrow \{\text{ideal of } R/I\}$. Then $I = 6\mathbb{Z}$.

Exercise: Let $R = \mathbb{Z}$ and $I = 6\mathbb{Z}$. Then find the ideals of R/I .

$$T(R) = \{T(I)\}$$

$$T = \{I\}$$



Thm: Let $f: R \rightarrow S$ be a surjective ring homomorphism and $J \subseteq S$ 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 $\pi \circ f: R \rightarrow S/J$ is a surjective ring homomorphism

$$\ker(\pi \circ f) = \{a \in R \mid \pi(f(a)) \in J\}$$

$$= \{a \in R \mid f(a) \in J\}$$

$$\ker(\pi \circ f) = f^{-1}(J)$$

Using 1st Isomorphism Thm

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

Remark: Let $\pi: R \rightarrow R/I$

be the natural ring homomorphism defined by ~~$f(a)$~~ $\pi(a) = a + I$.

$$\text{Let } J \supseteq I. J/I = \{a+I \mid a \in J\}$$

By previous theorem,

$$R/I \mid J/I \cong R/J$$

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 the ideal of R 2 I .

Construction of Rationals from Integers

Consider the set of all ordered pair

$$f = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}$$

define a relation of f

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

$$(a_1, b_1) \sim (a_2, b_2) \quad \cancel{a_1 \neq a_2, b_1 \neq b_2}$$

$$\text{and } (a_2, b_2) \sim (a_3, b_3)$$

$$\underline{\text{WTS}} \quad (a_1, b_1) \sim (a_3, b_3)$$

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} \Rightarrow a_1 b_2 - a_2 b_1 = 0 \quad \text{---(1)}$$

$$a_2 b_3 - b_2 a_3 = 0 \quad \text{---(2)}$$

$$a_1 b_2 b_3 - a_2 b_1 b_3 = 0$$

$$a_2 b_1 b_3 - b_2 b_1 a_3 = 0$$

$$\Rightarrow a_1 b_2 b_3 - b_2 b_1 a_3 = 0$$

$$\Rightarrow b_2 (a_1 b_3 - b_1 a_3) = 0$$

As $b_2 \neq 0$

$$\Rightarrow a_1 b_3 - b_1 a_3 = 0$$

$\therefore \sim$ is an equivalence relation

* Rational numbers are nothing but the equivalence classes.

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

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

Define '+' & \cdot in \mathbb{Q} by

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

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

Thm: Let R be an integral domain.

Then \exists a field F and a mapping

$$\text{onto } R \rightarrow F$$

Pf: Consider the $f = \{(a, b) \mid a, b \in R, b \neq 0\}$

Define a relation on f by

$$(a, b) \sim (c, d) \text{ iff } ad - bc = 0$$

\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 $(+)$ & (\cdot) as follows:

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

Check that they are well defined.

F is a ring wrt $(+)$ & (\cdot) defined with

0 and $\frac{1}{1}$

\downarrow
add identity \downarrow
mult identity

closure

WTS: F is a Field.

\exists $\frac{a}{b} \neq \frac{0}{1} \Rightarrow a \neq 0$.
which is the inverse of
Then $(b, a) \in F$.

(a, b) or $\frac{a}{b}$.

$\therefore F$ is a Field.

$\phi: R \rightarrow F$

$$\phi(r) = \frac{r}{1}$$

Check ϕ is a

ring homo.

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

$$\ker \phi = \{0\}$$

$\Rightarrow \phi$ is injective.

$$\phi(R) = \left\{ \frac{r}{1} \mid r \in R \right\}$$

\therefore We identify R with $\phi(R)$

Defn: F is called the quotient field of R and is denoted by \mathbb{Q}_F .

- Example: ① \mathbb{Q} is the quotient field of \mathbb{Z} .
 ② $k[x]$. the quotient field is the field of Rational functions

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

Philosophical

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

Let $a, b \in R$ such that $\bar{a} = a + I, \bar{b} = b + I$

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

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

$$\Rightarrow ab + I = 0 + I$$

$$\Rightarrow \underline{ab \in I}$$

if R/I is an integral domain

\Rightarrow if $ab \in I \Rightarrow$ either $a \in I$ or $b \in I$.

Definition: An ideal $I \subset R$ 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 prime ideal of R iff R/P is an integral domain.

Example: ① $n\mathbb{Z}$ is a prime ideal in \mathbb{Z}
if n is a prime number.

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 not be factored into the product
of two more non-constant polynomials with
coeff in k .

③ 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 $f(x) | gh \Rightarrow$ Either $f | g$ or $f | h$.

WTS If $f(x)$ is irreducible then

$(f(x))$ is a prime ideal.

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

$$1 = fp + gq$$

$$\Rightarrow h = fph + \underbrace{ghq}_{h} = f \cdot p \cdot h + fgh' \\ = f(ph + qh')$$

$$\Rightarrow h \in f(x)$$

\therefore If f is irreducible polynomial then
 $(f(x))$ is a prime ideal.

$\gamma(I) = \{x \in A \mid x^n \in I\}$ radical(i) $I \subseteq \gamma(I)$ (ii) $\phi: A \rightarrow A/a$

$$\phi^{-1}(n(A/a)) = \gamma(a)$$

 $\phi: \mathbb{R} \rightarrow \mathbb{R}$
 $(\mathbb{Z}/12\mathbb{Z})$ $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/12\mathbb{Z}$ $\phi: \mathbb{R} \rightarrow \mathbb{R}$

ring hom

$$\phi(x_1 + x_2) = \phi(x_1) + \phi(x_2)$$

$$\text{Show for } Q \quad f(m/n) = \frac{m}{n}$$

if $a \geq 0$

$$\phi(a) \geq 0$$

$$\phi(a) = \sqrt{a}\sqrt{a}$$

$$\phi(a) = \phi(\sqrt{a})(\sqrt{a})$$

$$\Rightarrow \phi(a) = (\phi(\sqrt{a}))^2$$

$$\Rightarrow \phi(a) \geq 0.$$

A ring has nilradical = set of nilpotent elements

(i) $x = \text{nilradical} = \bigcap_{P \text{ prime ideals}} P$

Read

(ii) Maximal Ideal.

- ① Zorn's Lemma,
- ② Posets.

$S \subset T$
 $\#_S \leq \#_T$
 $a_1 \leq a_2 \leq \dots \leq a_n$

$\mathcal{I} = \{ I \mid I \text{ is a proper ideal of } A \}$

$I_1 \leq I_2 \iff I_1 \subseteq I_2$

$\emptyset \in \mathcal{I}$

$I_1 \subseteq I_2 \subseteq \dots \iff \dots$

To show \mathcal{I} is a poset w.r.t. \leq

$\bigcup I_i$ is a proper ideal.
pf: $x, y \in \bigcup I_i \Rightarrow \exists i \in S \text{ s.t. } x, y \in I_i$
 $x, y \in I_i \subseteq I_m \subseteq I$

$\therefore \bigcup I_i \subseteq I$

Exercise: Every maximal ideal is a prime ideal.

$\{ A \}$

A/I is an integral domain
 \Downarrow
 I is a prime ideal

(2) A/I is a field
 \Downarrow
 I is a maximal ideal

$\cap_m = J(A) \Rightarrow I \in \{x\}$
maximal ideal Jacobson radical

(3) $x \in J(A) \Leftrightarrow 1 - xy$ is a unit
 $\forall y \in A$.

(4) Collection of prime ideals have a mutual element

$$I \in \bigcup_i$$

$X = \text{Spec}(A) \rightarrow$ affine scheme of ring
= {collection of all prime ideals of A }

$$E \subseteq A$$

$$V(E) = \{p \in X \mid p \supseteq E\}$$

(1) A^a is ideal generated by E ,

$$V(E) = V(a)$$

$$\vee(0) = X$$

$$\vee(1) = \emptyset$$

$$E^o, \vee(\cup E^o) = \cap V(E^o)$$

(iii) $\vee(a \wedge b) = V(a) \cup V(b) = V(ab)$

(iv) X topology defined by closed sets of
 X the form $V(E)$.
↓
Zariski Topology in X .

Prime Ideal

Let $k[x]$ be a poly. ring.
In a poly ring $k[x]$ every ideal is gen by
a poly. and if the poly. is irreducible
then the ideal becomes a prime ideal

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 $2 = (1+i)(1-i)$
& $(1+i) \notin (2)$ & $(1-i) \notin (2)$. Suppose $(1+i) \in (2)$

$$1+i = 2(a+ib)$$

$$\Rightarrow 1 = 2a, 2b = 2 \text{ which is not possible}$$

Q: When is R/I is a field?

Now we investigate the suff. homo
 $\varphi: R \rightarrow F$ where F is a field &
 R is a ring.

Defⁿ: An ideal M of a ring R is called 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 contains a maximal element.

Proposition: Maximal ideal exists in a non zero ring.

Consider the set $S = \{I \mid I \text{ is a proper ideal}\}$

under inclusion S is a partially ordered set. Let T be a totally ordered subset of S i.e. $\forall I, J \in T$

i.e. either $I \subset J$ or $J \subset I$.

$$\text{Let } u = \cup \{ I \mid I \in T \}$$

↓
due to chain of ideal.

This u is an ideal of R and
 u is proper

By Zorn's lemma, S has a maximal ideal.

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 2 ideals $(\bar{0})$ and $R/M = (\bar{1})$

↓ (Because M is the maximum possible ideal)

Since R/M has exactly 2 ideals then

R/M is a field.

Ex: Prove the converse

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 $(0) \subsetneq (n)$.

Converse Ex: $\mathbb{R}[x, y]$. Then (x) is not a maximal ideal

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

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

(0). The zero ideal is a maximal ideal iff R is a field.

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

② Consider the $R[x]$.

Every maximal ideal is generated by an irreducible polynomial

$$f(x) \in \mathfrak{m}$$

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

$$f(x) = g(x)h(x).$$

In $\mathbb{C}[x]$ every maximal ideal is generated by a linear polynomial $(x-a)$.

$$m_a = (x-a) \longleftrightarrow \mathbb{C}$$

$$\{\text{max. ideals}(\mathbb{C}[x])\} \longleftrightarrow \mathbb{C}.$$

$$\mathbb{C}[x_1, x_2, \dots, x_n] \longleftrightarrow \mathbb{C}^n$$

Ex What is the structure of the maximal ideals in $\mathbb{C}[x_1, x_2, \dots, x_n]$.

Thm HILBERT'S NULLSTELLENSATZ

The maximal ideals of the polynomial ring $R = \mathbb{C}[x_1, x_2, \dots, x_n]$ are in 1-1 correspondence with the pts in \mathbb{C}^n .

A pt $a = (a_1, \dots, a_n) \in \mathbb{C}^n$

$$\mathbb{C}[x_1, x_2, \dots, x_n] \longrightarrow \mathbb{C}^n.$$

$$f(x_1, \dots, x_n) \rightsquigarrow f(a_1, \dots, a_n)$$

Kernel of this map = $(x_1 - a_1, \dots, x_n - a_n)$

In fact every maximal ideal of $\mathbb{C}[x_1, \dots, x_n]$

is of the form

$$ma = (x_1 - a_1, \dots, x_n - a_n)$$

Defⁿ: Variety: Let V be a subset of \mathbb{C}^n

If V can be defined as the set of common zeros of a finite number of polynomials in n variables, then V is called an algebraic variety.

$$V = Z(f_1, \dots, f_n)$$

Examples: In \mathbb{C}^2 every point is a variety

$$\text{because } Z(x-a, y-b).$$

Complex line in \mathbb{C}^2 is $Z(ax + by + c)$ is a variety.

Theorem: Let f_1, \dots, f_n be polynomials in $\mathbb{C}[x_1, \dots, x_n]$ and $V = Z(f_1, \dots, f_n)$. Let $I = (f_1, \dots, f_n)$, The maximal ideals of the quotient ring $R = \frac{\mathbb{C}[x_1, \dots, x_n]}{I}$ is in bijective correspondence with the pts of V .

Proof: The maximal ideals of R corresponds to those maximal ideals of $\mathbb{C}[x_1, \dots, x_n]$ which contain I . Any maximal ideal is of the form $(x_1 - a_1, \dots, x_n - a_n)$. Now $(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n) \supset I = (f_1, \dots, f_n)$. The maximal ideal contains I iff it contains the generator of f_1, \dots, f_n of I . So if $f_i \in \text{ma}$ iff $f_i(a) = 0 \forall i$. which implies that $a \in V(I)$.

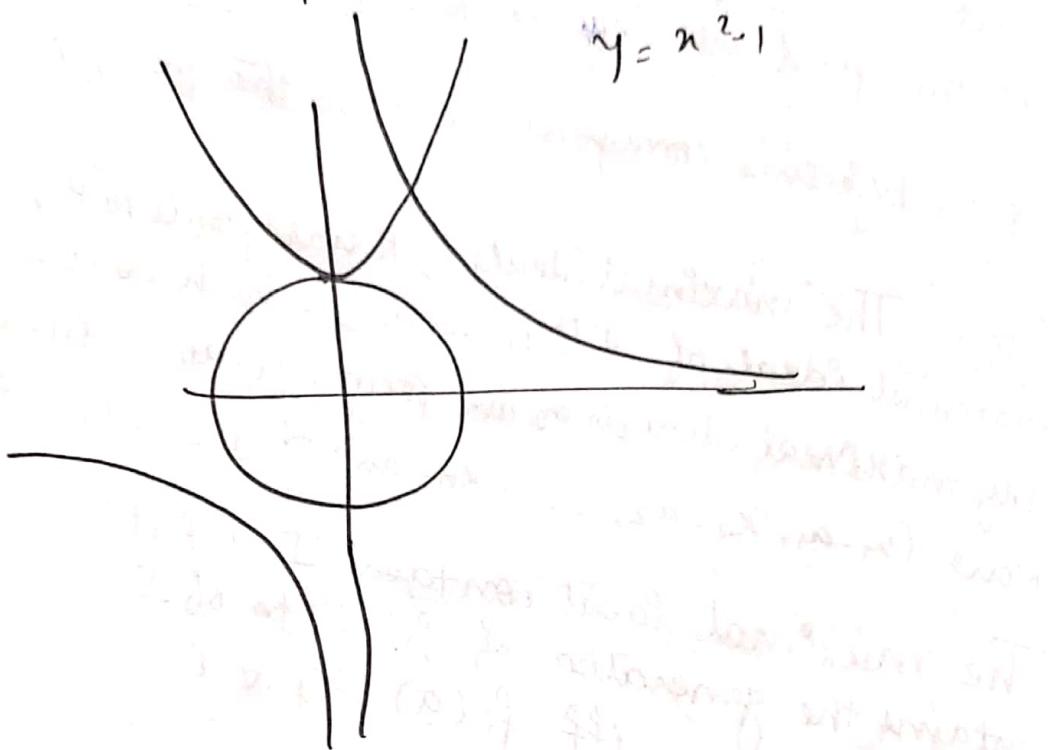
Corollary: Let f_1, \dots, f_n be polynomials in $\mathbb{C}[x_1, \dots, x_n]$. If the system of equations $f_1 = f_2 = \dots = f_n = 0$, has no solution in \mathbb{C}^n , Then $I = \sum_{i=1}^n g_i f_i$ where $g_i \in \mathbb{C}[x_1, \dots, x_n]$

Proof: $V = Z(f_1, \dots, f_n) = \emptyset$ which means there is no maximal ideal containing I . Therefore I is the whole ring i.e. $I \subset V$. $\therefore I = \sum g_i f_i$

Example: $f_1 = x^2 + y^2 - 1$

$$f_2 = x^2 - y + 1$$

$$f_3 = xy - 1$$



$$\text{Here } V(f_1, f_2, f_3) = \emptyset$$

$$\Rightarrow 1 \in (f_1, f_2, f_3)$$

Unique Factorization Domain: (consider only Integral Domain)
Let R be an integral domain throughout.

elt b divides another elt a if $a = bq$ for some $q \in R$.

Definition: We say an elt a divides another elt b ($a | b$) if $b = aq$ for some $q \in R$.

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

A non-zero element a of $\#R$ is called irreducible if a is not a unit and has no proper divisors. (i.e. $a = bc$ then either b or c is a unit)

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

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

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

$\Rightarrow b = ad$ where $d \in R$.

$$\therefore a = bc = adc$$

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

Example: ① The irreducible elements of

\mathbb{Z} are prime elements.

② The irreducible elements of $\mathbb{K}[x]$ are
irreducible polynomials.

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

Consider 2.

$$2 = \cancel{a+b\sqrt{-3}}(c+d\sqrt{-3})$$

$$2 = ac - 3bd + \cancel{(bc+ad)\sqrt{-3}}$$

$$2 \cdot \bar{2} = (a^2 + 3b^2)(c^2 + 3d^2)$$

$$4 = (a^2 + 3b^2)(c^2 + 3d^2) \quad \text{can't}$$

$\therefore (a^2 + 3b^2)$ must divide 4 and $(a^2 + 3b^2)$ be 2

$$\text{Hence } (a^2 + 3b^2) = 4 \quad \& \quad c^2 + 3d^2 = 1$$

$$\Rightarrow d = 0, c = \pm 1$$

\therefore one of the factors of 2 is a unit
Thus 2 is irreducible el.

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

But neither $(1 + \sqrt{-3})$ or $(1 - \sqrt{-3}) \in 2$
 $\therefore (2)$ is not a prime ideal.
It can have two representations/factorizations
and it restricts the prime ideals, irreducible
elements to generate a prime ideal.

UNIQUE FACTORIZATION DOMAIN

UFD is an integral domain satisfying that

1. Every non zero element $\neq 0$

can be written as product
of irreducible factors say $p_1 \dots p_n$
upto namely

$$a = u p_1 \dots p_n$$

2. The above factorization is unique

if $a = u_1 p_1 \dots p_n = v_1 q_1 \dots q_m$
are two factorizations into irreducible

elements

$p_i \in q_j$ with units u, v then
 ~~$n = m$~~ $p_i \in q_j$ are associates

Def: Two elements $a, b \in R$ are called associates if $a = ub$ for some unit $u \in R$.

Examples: i) \mathbb{Z} , $k[x]$ are UFD.

① \mathbb{Z} , $k[x]$ are UFD. an elt a is irreducible iff a is prime

Proof: In an UFD iff a is prime

Prime: Let a be an irreducible elt $\neq 0$.

(a) a is prime

WTS: (a) a is prime

Let $a | bc$ for some $a \in R$

$\Rightarrow bc = ad$ for some $d \in R$

\Rightarrow since R is an UFD, we can decompose b, c, d into irreducible elts.

$b = b_1 \dots b_s$ w.c. $c = c_1 \dots c_t$ $d = d_1 \dots d_r$

$(r+t) = s+t$

Since the factorization is unique, a must

be associated to b_i or c_j

$\Rightarrow a$ divides b_i or c_j

$\Rightarrow a$ divides $b^r c^t$ or c^t

$\Rightarrow (a)$ is prime ideal.

\Rightarrow Prime ideal

Proposition: Let R be an integral domain

and $a, b \in R$. Then

(i) a is a unit iff $(a) = R$

(ii) a and b are associates iff $(a) = (b)$.

(iii) $a \mid b$ iff $(b) \subset (a)$.

(iv) a is a proper divisor of b iff

$(b) \subset (a) \subset R$.

(v) a is irreducible iff (a) is maximal among proper principle ideals of R

Defn: An int. domain R is called Factorization domain if every non zero element of R can be written as product of irreducible elements.

Proposition: Let R be an int domain

TFAE

(1) For every nonzero elt $b \in R$ which is not a unit, the process of factoring b terminates after finitely many steps and result a factorizations of b into irreducible elements

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

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

Noetherian ring

Proof: suppose R contains an infinite increasing sequence of principal ideals

$$(a_1) \subset (a_2) \subset \dots \subset (a_n)$$

for all n .

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

where a_n and b_n are not units.

$$a_1 = a_2 b_2 = a_3 b_2 b_3 = a_1 b_2 b_3 b_4 \dots$$

$$a_1 = a_2 b_2 = a_3 b_3$$

Exercise Do the converse.

Example: Consider the polynomial $R[x]$.

$$\text{let } R = k[x_1, x_2, x_3, \dots]$$

$$\text{where } x_2^2 = x_4, x_3^2 = x_2, x_4^2 = x_3$$

& so on. \therefore We can factor x_1 indefinitely in the Ring R and get an infinite chain of principal ideals.

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

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

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

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

$$1 = br + as$$

In $\mathbb{Z}[x]$

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

Proposition: let a and b be non zero elements of an UFD and let $a = p_1^{e_1} \dots p_n^{e_n}$

$b = p_1^{f_1} \dots p_m^{f_m}$ are unique factorization

can be written into irreducible factors where
 a, b are units and p_i 's are distinct
and $e_i, f_i \geq 0$. Then the element
 $d = p_1^{e_1} \cdots p_n^{e_n}$

is a gcd of a and b .

Proof: Ex.

Defn: An integral domain R is called
principal ideal domain (PID) if every
ideal of R is principal.

Example: \mathbb{Z} , $R[x]$ are PID.

Proposition: In a PID irreducible elements
are prime.

Proof: Let p be an irreducible element

WTS: (p) is a prime ideal

$$\text{Let } ab \in (p) \Rightarrow ab = cp \text{ for some } c \in R$$

$$\Rightarrow p \mid ab$$

Let $p \nmid a^2$. Then $(p) \subsetneq (p, a)$

since p is maximal among all
the principal ideals.

$$(p, a) = (1)$$

$$\Rightarrow 1 = pc + ad \text{ for } c, d \in R$$

$$\Rightarrow 1 = pcb + abd$$

$$\Rightarrow 1 = p(ab + cd)$$

$$\Rightarrow b = p(cb + ad) \in (p)$$

$$\Rightarrow b \in (p)$$

$\therefore p$ is a prime ideal.

\Rightarrow Every irreducible element is a prime element in a PID.

Prop: Every non zero prime ideal in a PID is a maximal ideal.

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

Then there 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 maximal ideal.

If $r \in (p)$, then $r = p.s$ for some $s \in R$

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

$\Rightarrow m$ is a unit

Hence the proof.

corollary: Let R be any ring and $R[x]$ is a PID, then R is a field.

$$R[x]/(x) \cong R \quad R \subset R[x]$$

\downarrow
is int domain

But $R[x]$
 $\Rightarrow (x)$ is a prime ideal.

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

Exercise: A PID is an UFD.

25th March

Proposition:

WTS: Existence of factorization in R . which is equivalent to show that R contains no infinite increasing chain of ~~in~~ principal ideals.

suppose $(a_1) \subset (a_2) \subset (a_3) \dots$ is an infinite chain of principal ideals.

Let I be the union of this chain of principal ideals. Then I is an ideal generated by a single element: since R is a PID so I will be

generated by a single element:

$$\text{so } I = (b)$$

Now since b is in the union of this ideals (a_n) it

$$\Rightarrow b \in (a_n)$$

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 product of irreducible elements.
since every irreducible is prime so R is an UFD.

Example
 $\mathbb{Z}[x]$ is a UFD but not a PID.
(How?)

EUCLIDEAN DOMAIN

Let us now abstract the procedure of division with remainder. To do this we need the notion of size of an element of a ring. In general a size f^n on an integral domain R will be any f^n .

$$N: R \setminus \{0\} \rightarrow \{0, 1, 2, 3, \dots\}$$

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

Defⁿ: 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

Example (1) Fields are E.D. when if
 $N(a) = 0 \wedge a \neq 0$

$$a = qb + 0$$

$$\text{where } q = ab^{-1}$$

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

(3) If F is a field then $F[x]$ is E.D.
with $\# N(f(x)) = \deg f(x)$.

(4) $\mathbb{Z}[i] = \text{Ring of Gaussian Integers}$
 $= \{a+bi \mid a, b \in \mathbb{Z}\}$

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

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

$$\alpha/\beta = \frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{c^2+d^2}$$

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

$$\alpha/\beta = r+ps \in \mathbb{Q}[i]$$

Let p and q be integers

closed to r & s .

$\therefore |r-p| \& |s-q|$ are at most $1/2$

$$0 = (r-p) + p(s-q)$$

$$\boxed{\gamma = \beta \alpha} = \beta [(r-p) + p(s-q)]$$

$$= \beta [(r+is) + (p+iq)]$$

~~$\in \mathbb{Z}[i]$~~

$\hookrightarrow \mathbb{Z}[i]$

$$\Rightarrow \alpha = \beta(\rho + i\alpha) + \gamma$$

$$\begin{aligned} N(\gamma) &= N(\beta \alpha) \stackrel{\text{Exercise}}{=} N(\beta) \cdot N(\alpha) \\ &= N(\beta) [(\rho - \rho)^2 + (\alpha - \alpha)^2] \\ &\leq N(\beta) [\frac{1}{4} + \frac{1}{4}] \\ &\leq \frac{N(\beta)}{2} \end{aligned}$$

$$\therefore \boxed{N(\gamma) < N(\beta)}$$

$\therefore \mathbb{Z}[i]$ is an E.D. then R is a PID.

Thm: Let R be an E.D. then R is a PID.
Exercise: Find the units in $\mathbb{Z}[i]$.

!

26th March

Field C.E.D. \subset PID \subset UFD \subset Integral Domain

Field C.E.D. \subset PID \subset UFD \subset Integral Domain

\mathbb{Z} is a ED but not a field

w.r.t. $\mathbb{Z}[(1+\sqrt{-19})/2]$ is a PID but not ED.

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

- $\mathbb{Z}[\sqrt{-3}]$ is an integral 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 $\pm 1, \pm i$.

Definition: A prime elt in $\mathbb{Z}[i]$ is called a Gaussian Prime

Proposition: 1) If $N(a+bi) = a^2 + b^2 = p$ is a prime number then $a+bi$ is a Gaussian Prime

2) If π is a gaussian prime then

$N(\pi) = \pi\bar{\pi}$ is either a prime number or square of a prime number

Pf ① Let $\alpha = a+bi$ s.t. $N(\alpha) = p$

WTS α is a prime elt.

Since $\mathbb{Z}[i]$ is an E.D. so it is an UFD.

have prime \Leftrightarrow equivalent to irreducible element. WTS α is an irreducible elt. let $\alpha = \beta\nu$ where $\beta, \nu \in \mathbb{Z}[i]$

Then $N(\alpha) = N(\beta)N(\nu) = p$

Hence either $N(\beta)$ or $N(\gamma)$ is unit.
Hence either β or γ is unit.
Thus α is irreducible element. Hence
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 $\pi \bar{\pi} \in \mathbb{Z} \neq 0$.

Note that $(\pi) \cap \mathbb{Z}$ is an ideal of \mathbb{Z} .

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

Hence

$$\therefore p \in (\pi) \quad \text{where } \mu \in \mathbb{Z} \text{ s.t.}$$

$$\therefore p = \pi \mu$$

$$p^2 = N(p) = \frac{N(\pi) N(\mu)}{N(\pi)} = p \text{ or } p^2$$

~~p~~

The following are equivalent

Thm: The following are equivalent
for prime element p .

(1) $p = \pi \bar{\pi}$ where π is a gaussian integer

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

(3) $x^2 \equiv -1 \pmod{p}$ has an integer solution

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

Proof:

① \Rightarrow ②

$$p = \pi\bar{\pi}$$

Let $\pi = a + b\sqrt{-1}$

$$\Rightarrow \pi\bar{\pi} = a^2 + b^2 = p$$

② \Rightarrow ③

$$p = a^2 + b^2 \text{ for } a, b \in \mathbb{Z},$$
$$a, b \neq 0.$$

~~$$p = a^2 + b^2$$~~

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

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

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

$$\Rightarrow x^2 \equiv -1 \pmod{p}$$

③ \Rightarrow ④

Let p be an odd prime.

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

Then $\text{o}(a) = 4$ in the multiplicative
gp $(\mathbb{Z}/p\mathbb{Z})^\times$

$$\text{Hence } 4 \mid p-1$$

$$\Rightarrow p \equiv 1 \pmod{4}.$$

$\textcircled{A} \Rightarrow \textcircled{B}$

For $p=2$ 1 is solution to
 $x^2 \equiv -1 \pmod{p}$

Now let $p \equiv 1 \pmod{4}$

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

Consider the gp $(\mathbb{Z}/p\mathbb{Z})^*$.

since $4 \mid p-1$, so there is a subgroup
of order 4 in $(\mathbb{Z}/p\mathbb{Z})^*$
(Sylow's Theorem)

Let H be the subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ of
order 4 and let H be a cyclic group.
so $\exists a$ s.t. $a^4 \equiv 1 \pmod{p}$.

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

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

\Rightarrow If $p \mid a^2 - 1$ then $a^2 \equiv 1 \pmod{p}$
which says that $O(a) = 2$ assumed
which is a contradiction. ($O(a) = 4$)

$$\Rightarrow p \mid a^2 + 1$$

$$\Rightarrow a^2 \equiv -1 \pmod{p}$$

$\Rightarrow a$ is a solution of $x^2 \equiv -1 \pmod{p}$

$\Rightarrow a$ is a solution of $x^2 \equiv -1 \pmod{p}$

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

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

$$\Rightarrow p \mid m+1 \text{ or } p \mid m-1$$

$$m \stackrel{4}{=} -1 \pmod{p} \quad m \stackrel{4}{=} 1 \pmod{p} \quad \times$$

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

$(3) \Rightarrow (1)$

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

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

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

Ex $\frac{\mathbb{Z}[x]}{p\mathbb{Z}[x]} \cong (\mathbb{Z}/p\mathbb{Z})^{[x]}$

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

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

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

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 $\mathbb{Z}[p]$.

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

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

$$\text{Thus } N(\pi) = p = \pi\bar{\pi}.$$

Corollary (Fermat's two square Thm)
let p be prime number 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. $p \equiv 3 \pmod{4}$.
 - ③ If ~~$a+ib$~~ $a+ib, a-ib$ the distinct
irreducible factors of $p = a^2 + b^2$
for the prime $p \equiv 1 \pmod{4}$

Polynomials over UFD

- Q) Let R be an UFD. Is $R[x]$ an UFD?
We know that $F[x]$ is UFD where F is a field. Let K be the quotient field of R . Then R is a subring of $K[x]$. Since $K[x]$ is an UFD, we try to relate factorization in $R[x]$ and $K[x]$.

$$\mathbb{Z}[x] \quad \mathbb{Q}[x].$$

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

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

Eg.: Consider the poly. $2x \in \mathbb{Z}[x]$

Then $2x = 2 \cdot x$ in $\mathbb{Z}[x]$ 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'n.: Let R be an UFD. The constant of $f(x) \in R[x]$ denoted by $c(f)$ is the gcd of coeff. of $f(x)$. If $c(f) = 1$ we say $f(x)$ is primitive

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

Pf: Suppose $f(x)g(x)$ is not primitive

$$\Rightarrow \gcd(fg) \neq 1$$

Let p be a prime in R dividing the coefficients of $f(x)g(x)$.

Consider the following map

$$\pi: R[x] \rightarrow R/p[x]$$

$$\pi(\sum a_n x^n) = \sum \bar{a}_n x^n.$$

$$(\phi: R \rightarrow R/p \text{ then } \phi(a_n) = \bar{a}_n)$$

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

R/p is an integral domain.

$$\Rightarrow \overline{f(x)g(x)} = \bar{0}$$

$$\Rightarrow f(\bar{x})g(\bar{x}) = 0$$

$$\Rightarrow f(\bar{x}) = 0 \text{ or } g(\bar{x}) = 0$$

$\Rightarrow \exists p$ that divides the content of either $f(x)$ or $g(x)$

$$\Rightarrow \cancel{\text{content}(f) \neq 1 \text{ or content}(g) \neq 1}$$

$\Rightarrow \Leftarrow$ (contradiction)

Corollary:

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

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

Proof let ~~assume~~ $c(f) = a$ and $c(g) = b$

$$\text{Then } f(x) = a \cdot f_1(x)$$

$$g(x) = b \cdot g_1(x)$$

$$\Rightarrow f(x)g(x) = a \cdot b \cdot f_1(x)g_1(x)$$

From last Thm f_1g_1 is primitive since f_1, g_1 are primitive

$$\Rightarrow c(fg) = ab$$

$$\Rightarrow c(fg) = c(f)c(g)$$

Proposition

$f(x), g(x) \in R[x]$ both primitive

and $f(x) & g(x)$ are associates in $R[x]$

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 $R[x]$.

Pf: let $f(x) = \frac{a}{b}g(x)$ where $a, b \in R$

~~and~~ $b \neq 0$

Then $b \nmid a$ $\therefore b \nmid f(x) = a g(x)$.

since $f(x)$ and $g(x)$ are primitive

$$\therefore c(bf) = b \quad \& \quad c(ag) = a.$$

since in a UFD the gcd is unique
upto multiple by unit.

so $a = ub$, where u is a unit in R .
 $\therefore f(x) = ug(x)$, where $u \in R$ is a unit.

Propn [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 $p(x) = A(x)B(x)$ for some non constant polynomials

$A(x), B(x) \in K[x]$, then there are

non-zero elts $r, s \in K$ s.t.

$rA(x) = a(x)$ and $sB(x) = b(x)$

and $p(s) = a(s)s^r b(s)^s$ where $a(x), b(x) \in R[x]$

is a factorization in $R[x]$

QUESTION \exists an UFD?

2nd April

Proof: Let $p(x) = A(x)B(x)$, where

$A(x), B(x) \in K[x]$.

Now multiplying by common denominator for all of these coefficients, we obtain

$$d p(x) = a'(x) b'(x)$$

where $a'(x), b'(x) \in R[x]$ and d is

a non zero element of R . If d is a

unit in R , then the proposition is done

(multiply both sides by d^{-1}). Assume that

d is not an unit in R .

since R is an UFD so let $d = p_1 \dots p_n$

where p_i 's are irreducible elts of R

$$p_1 p_2 \dots p_n p(x) = a'(x) b'(x)$$

(p_1) is a prime ideal of R

Hence $R/I_p[x]$ is an integral domain.

$$\bar{0} = \overline{a'(x)} \overline{b'(x)} \quad [\text{Reducing the equation modulo } I_p]$$

which implies

$$\text{either } \overline{a'(x)} = \bar{0} \text{ or } \overline{b'(x)} = \bar{0}.$$

$$\text{say } \overline{a'(x)} \neq \bar{0}$$

\Rightarrow all the coefficients of $a'(x)$ are divisible by p_i .

$$\text{so } \frac{1}{p_i} a'(x) \in R[x].$$

Therefore by proceeding in the same direction and cancelling all the irreducible elements (p_1, p_2, \dots, p_n) from both side we have the eqn.

$$\Rightarrow P(x) = a(x) b(x)$$

$$\text{where } a(x), b(x) \in R[x]$$

and the relation b/w $A(x)$ & $a(x)$

$$\text{is } dA(x) = a'(x) \text{ and}$$

$$\frac{1}{p_i} a'(x) = a(x).$$

$$\therefore \frac{d}{p_i} A(x) = a(x) \text{ i.e.}$$

$$\gamma A(x) = a(x)$$

for some $\gamma \in K$

Remark: $a(x), b(x)$ need not be R multiples of $A(x), B(x)$

(x) \rightarrow $a(x)$

Obs: The elements of the ring R becomes units in UFD $K[x]$. e.g. $7x$ (factor into two irreducible 7 and x in $\mathbb{Z}[x]$) but is irreducible in $\mathbb{Q}[x]$ because 7 is a unit in $\mathbb{R}[x]$.

Corollary: Let R be an UFD and K be the quotient field of R and let $p(x) \in R[x]$ with $(p(x)) = 1$. Then $p(x)$ is irreducible in $R[x]$ iff $p(x)$ is irreducible in $K[x]$.
Proof: By Gauss's lemma if $p(x)$ is reducible over $R[x]$ then $p(x)$ is reducible over $K[x]$. Conversely let $p(x)$ is irreducible over $R[x]$, i.e. $p(x) = a(x)b(x)$ are non constant polynomials $\in R[x]$ i.e. $a(x)$ & $b(x)$ are not units in $K[x]$.

Thus the same factorization shows that $p(x)$ is irreducible over $K[x]$.

that $p(x)$ is irreducible over $K[x]$ iff $R[x]$ is an UFD.

Thm: R is a UFD iff $R[x]$ is an UFD.

Proof: Let R be a UFD.

WTS: $R[x]$ is a UFD.

Let K be the quotient field of R and $p(x) \in R[x]$ be non zero elt

WLOG: we may assume $p(x)$ is primitive (if $p(x)$ is not primitive we can write $p(x) = d p'(x)$ where $d \in R$ and $p'(x)$ is primitive, so d has unique factor) and $p(x)$ is not unit in $R[x]$

i.e. $\deg p(x) > 0$. since $K[x]$ is an UFD, $p(x)$ can be factored uniquely into

Irreducibles in $K[x]$.

By Gauss' Lemma

such a factorization implies, there is a factorization of $p[x]$ in $R[x]$.

since $p[x]$ is primitive each factor

of $p[x]$ is primitive. By previous

corollary each factor is irreducible in $R[x]$. This shows that $p(x)$ can be written as a finite product of irreducibles in $R[x]$.

Uniqueness

Let $p(x)$ can be factorized into 2 different factors in $R[x]$

$$p(x) = q_1(x) \dots q_r(x) = q'_1(x) \dots q'_s(x)$$

Now viewing it as a factorization in $K[x]$ we get $r = s$ and q_i is associate to some q'_i . Then by previous proposition, they are associates. Therefore $R[x]$ is an UFD.

Q $R[x, y] = (R[x])[y] \rightarrow$ is an UFD
↓
UFD.

Proposition

Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$
 If $\frac{r}{s} \in \mathbb{Q}$, $(r,s) = 1$ is a root of $p(x)$ then
 If $r | a_0$ and $s | a_n$, In particular if
 $p(x)$ is monic and $p(d) \neq 0$ for all
 integer d dividing the constant term of
 $p(x)$, then $p(s)$ has no root in \mathbb{Q} .

Proof:

$$p\left(\frac{r}{s}\right) = 0$$

$$a_n \frac{r^n}{s^n} + a_{n-1} \left(\frac{r}{s}\right)^{n-1} + \dots + a_0 s^{n-1} = 0$$

$$a_n r^n + a_{n-1} r^{n-1} s + \dots + a_0 s^{n-1} = 0.$$

$$a_n r^n + a_{n-1} r^{n-1} s + \dots + a_0 s^{n-1} = -s(a_{n-1} r^{n-1} s + \dots + a_0 s^{n-1})$$

Thus $a_n r^n = -s(a_{n-1} r^{n-1} s + \dots + a_0 s^{n-1})$

$$\Rightarrow s | a_n r^n \quad \text{as } \gcd(s, r) = 1$$

Similarly $r | a_0$.

Example The Polynomial $x^3 - 3x - 1 \in \mathbb{Z}[x]$

This is not irreducible over $\mathbb{Q}[x]$.
 The possible roots are ± 1 . None of
 them satisfy the eqn so it is irreducible.

Propⁿ: Let I be a proper ideal in UFD R .
 and let $P(x)$ be a non constant monic
 polynomial in $R[x]$. If the image of $p(x)$
 in $R/I(x)$ can not be factored into
 2 polynomials of smaller deg than
 $p(x)$ is irreducible in $R[x]$.

Proof: Suppose $p(x)$ can not be factored in $R/I[x]$ but $p(x)$ is reducible in $R[x]$ i.e. $p(x) = a(x)b(x)$ where $a(x), b(x)$ monic poly. in $R[x]$

Now reducing the coeffs mod I gives a factorization in $(R/I)[x]$ with non constant factors which

is a contradiction.
Ps a contradiction
(since $p(x)$ is monic $I \neq I$
then I does not vanish)

Example

$$x^3 + x + 1 \in \mathbb{Z}[x]$$

is irreducible over $\mathbb{Z}[x]$
as it is irreducible over $\mathbb{Z}/2\mathbb{Z}[x]$.

Example $x^2 + 1 \in \mathbb{Z}[x]$ in $\mathbb{Z}/2\mathbb{Z}[x]$

the polynomial $f(x)$ is not irreducible.

In $\mathbb{Z}/3\mathbb{Z}$ $f(x)$ is irreducible.

$\therefore f(x)$ is irreducible over $\mathbb{Z}[x]$.

Propn: Eisenstein's criterion.

Eisenstein's criterion: If p is a prime Pideal of an UFD

let p be a prime Pideal of an UFD

Let $f(x) = a_n x^n + \dots + a_0$

R and let $f(x)$ be a poly. in $R[x]$. suppose

a_n be a poly. in $R[x]$ and $a_n \in p$

$a_{n-1}, a_{n-2}, \dots, a_0 \in p$ and $a_n \notin p^2$

and $a_0 \notin p^2$. Then $f(x)$ has no

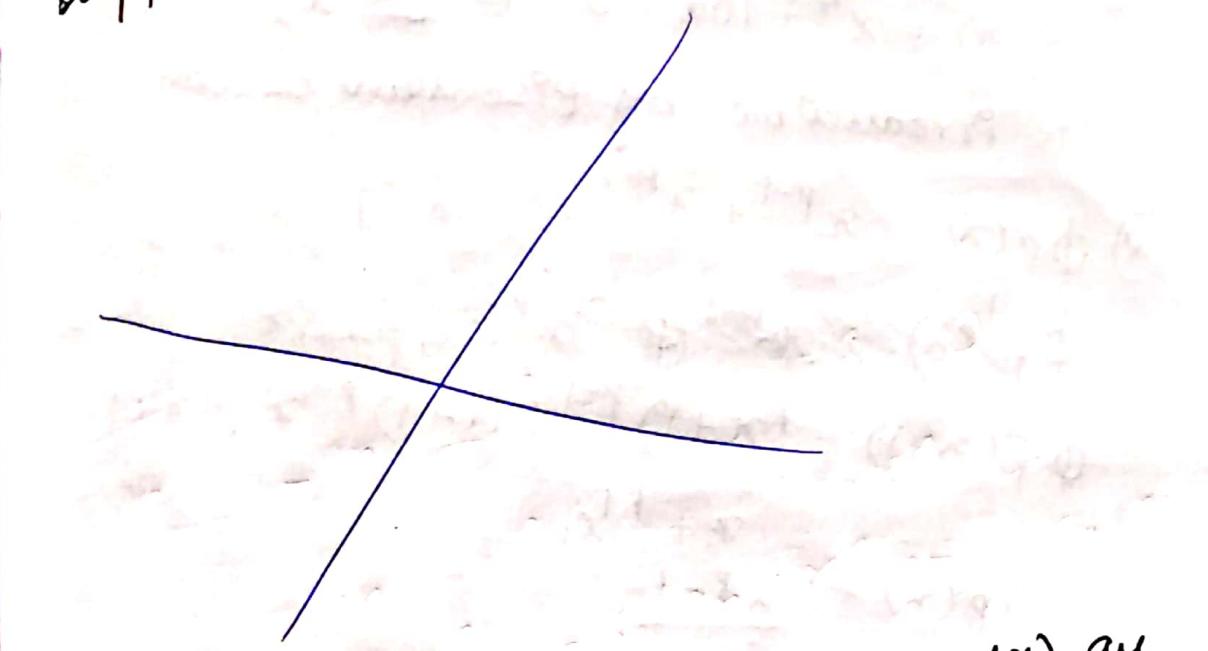
divisor of deg d and $1 \leq d \leq n-1$

i.e. $f(x)$ is irreducible over $F[x]$ and

If $f(x)$ is monic then f is irreducible over $R[x]$.

Proposition

Let P be a prime ideal in an UFD R .
and let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in P[x]$
suppose $a_0, \dots, a_{n-2}, a_{n-1} \in P$.



Proof. Let $f(x) = p(x)q(x)$ where $p(x) \neq q(x)$ are given $\deg \in R[x]$

Reduce the coeffs modulo P . Then

$$\bar{a}_n x^n = \bar{f}(x) = \bar{p}(x)\bar{q}(x)$$

Thus the leading coefficients of $p(x)$ & $q(x)$ do not belong to P . It also follows that

$$p(0), q(0) \in P \text{ which implies } f(0) \in P^2$$

$$f(0) = p(0)q(0) \in P^2$$

Let

$$p(x) = a_0 x^2 + a_1 x + a_2 \rightarrow \notin P$$
$$q(x) = b_0 x^2 + b_1 x + b_2 \rightarrow b_1 \in (P)$$
$$p(x)q(x) = a_0 b_0 x^4 + (a_0 b_1 + a_1 b_0)x^3 + a_1 b_1 x^2 + a_2 b_0 x + a_2 b_1 \rightarrow \notin P$$

Hence both the constant terms should $\in (P)$.

but $f(0) \notin P^2$ which is contradiction.
 Thus $f(x)$ is irreducible

Example:

$$f(x) = x^4 + 10x + 5 \in \mathbb{Z}[x]$$

is irreducible by Eisenstein criterion

$$\textcircled{2} \quad \phi_p(x) = x^{p-1} + x^{p-2} + \dots + 1$$

~~$$\phi_p(x) = x^{p-1} + (x-1)^{p-2} + \dots + 1$$~~

$$\phi_p(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + \dots + 1$$

$$= x + pC_1$$

$$\phi_p(x) = \frac{x^{p-1}}{x-1}$$

$$\phi_p(x+1) = \frac{(x+1)^p - 1}{x}$$

$$\phi_p(x+1) = x^{p-1} + xP_{C_1}x^{p-2} + \dots + P_{C_4}$$

Then by EC with prime ideal P ,
 $f(x)$ is irreducible. Thus $\phi_p(x)$ is irreducible

Exercise: By EC show that
 polynomial $f(x) = x^4 + 1$ is
 irreducible over $\mathbb{Z}[x]$.

Example: Let R be an integral domain and $f(x) \in R[x]$ is a monic irreducible polynomial, then $f(x)$ need not be irreducible over $K[x]$ where K is the quotient field of R .

Example: Let $R = \mathbb{Z}[2i] = \{a + b2i \mid a, b \in \mathbb{Z}\}$ be a subring of an integral domain \Rightarrow integral domain. Consider the polynomial $f(x) = x^2 + 1 \in \mathbb{Z}[2i][x]$. Note that $f(x)$ is irreducible over $R[x]$. Let K be the quotient field of R . Then ~~$K = \mathbb{Q}(i)$~~ $K = \mathbb{Q}(i)$ [Ex]. Thus $f(x)$ is reducible over $K[x]$. Prove that $\mathbb{Z}[2i]$ is not an

Exercise
UFD.

8th April Chinese Remainder Theorem

$$G_1, G_2 \quad G_1 \times G_2 = \{(a, b) \mid a \in G_1, b \in G_2\}$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

$$(a_1, b_1) * (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$$

$$(a_1, b_1) * (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$$

If R_1 and R_2 are two rings then
 $R_1 \times R_2$ has a ring structure.

In \mathbb{Z} , $\gcd(a, b) = 1$, then $1 = ra + sb$
where $r, s \in \mathbb{Z}$ i.e. $(a) + (b) = 1$

Definition
We say that

Def

Let R be a ring and I and J are 2 proper ideals in R .

we say I & J are co-maximal

if $I+J = R$

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/mn\mathbb{Z}$$

iff $(m, n) = 1$

Thm. **Chinese Remainder Theorem**

Let R be a ring and I_1, \dots, I_n be ideals of R s.t. ~~$I_i + I_j = R$~~ for all $1 \leq i, j \leq n$ and $i \neq j$. Then

$$R/\bigcap_{i=1}^n I_i \cong R/I_1 \times R/I_2 \times \dots \times R/I_n$$

Pf: $f: R \longrightarrow R/I_1 \times R/I_2 \times \dots \times R/I_n$

$$a \mapsto (a+I_1, a+I_2, \dots, a+I_n)$$

Exercise: Check that f is a Ring Homomorphism

$$\ker f = \{a \in R \mid a \in I_i \forall i = 1, \dots, n\}$$

$$\begin{aligned} &= \bigcap_{i=1}^n I_i \\ &= \bigcap_{i=1}^n I_i \end{aligned}$$

WTS f is surjective i.e. want to find
 $a \in R$ s.t. $f(a) = (a_1 + I_1, a_2 + I_2, \dots, a_n + I_n)$

For $j > 1$ we have by assumption

$$I_1 + I_j = R.$$

$\therefore \exists b_j \in I_1$ and $d_j \in I_j$

s.t. $b_j + d_j = 1$ for $j = 2, \dots, n$.

$$\Rightarrow \prod_{j=2}^n (b_j + d_j) = 1$$

$$(b_2 + d_2)(b_3 + d_3) \dots (b_n + d_n)$$

$$(b_2 b_3 + d_3 b_2 + d_2 b_3 + d_2 d_3) \dots (b_n + d_n)$$

$$\underbrace{(b_2 b_3 + d_3 b_2 + d_2 b_3 + d_2 d_3)}_{I_1} \underbrace{\dots}_{I_2 I_3} \dots$$

If we multiply, then we see that all the elements $\in I_1$ except ~~d_j~~ $\forall j$

$$c_1 = \prod_{j=2}^n d_j \in \prod_{j=2}^n I_j$$

Thus $c_1 \equiv 1 \pmod{I_1}$

and $c_1 \equiv 0 \pmod{I_j}$ for $j \neq 1$

More generally, for all i we can find

c_i with $c_i \equiv 1 \pmod{I_i}$

and $c_i \equiv 0 \pmod{I_j}$ for $j \neq i$

Now the arbitrary els $a_1, a_2, \dots, a_n \in R$

and set

$$a = a_1 c_1 + a_2 c_2 + \dots + a_n c_n$$

Take $(\text{mod } I_1) + \dots + (\text{mod } I_n)$

$$\text{Then } f(a) = (a_1 + I_1, a_2 + I_2, \dots, a_n + I_n)$$

Ex

$\therefore f$ is surjective ring hom
 $a - a_i \equiv 0 \pmod{I_i}$

Thm: Hilbert's Nullstellensatz

The maximal ideals of the polynomial ring $R = \mathbb{C}[x_1, x_2, \dots, x_n]$ are in 1-1 correspondence with the points in \mathbb{C}^n .

For $n=1$ Maximal ideals in $\mathbb{C}[x]$ are in 1-1 correspondence with the pts of \mathbb{C} .

Here every maximal ideal of $\mathbb{C}[x]$ will be generated by an irreducible polynomial and irreducible polynomials are linear polynomials of the form say $x-a$, then this maximal ideal corresponds to the point $a \in \mathbb{C}$

Proof of the Theorem:

Consider a point $a = (a_1, a_2, \dots, a_n)$ consider the ideal $m_a = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$

First we will show that m_a is maximal ideal of R and then we show that every maximal ideal of R is of the form m_a for some $a \in \mathbb{C}^n$.

1st step: $\delta_a : \mathbb{C}[x_1, \dots, x_n] \rightarrow \mathbb{C}$
where $a \in \mathbb{C}^n$. $f(x_1, \dots, x_n) \mapsto f(a_1, \dots, a_n)$

By 1st Isomorphism Thm,

$$R/\ker(\delta_a) \cong \mathbb{C}$$

Field

Thus $\ker(\delta_a)$ is a maximal ideal.

Writing down the Taylor series expansion
of $f(x_1, x_2, \dots, x_n)$ around (a_1, \dots, a_n)
we get

$$\begin{aligned} f(x_1, \dots, x_n) &= f(a_1, a_2, \dots, a_n) + \sum c_i (x_i - a_i) \\ &\quad + \sum_{i,j} c_{ij} (x_i - a_i)(x_j - a_j) \dots \end{aligned}$$

Let $f \in \ker \delta_a$ then $f(a_1, \dots, a_n) = 0$

$\therefore f(x) \in (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$

$\therefore \ker \delta_a = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$