Ring Theory

Lecture 21

16/03/2022

<u>Remark</u> R/I is an int domain iff I is a prime ideal.

An ideal $I \subsetneq R$ is said to be a prime ideal if $ab \in I$ then either $a \in I$ or $b \in I$.

<u>Propn</u>. Let $R = k[x]$ where k is a field. Let $I = (f(x))$ is an ideal then I is a prime ideal if $f(x)$ is irreducible poly.

<u>Pf</u>. Let $gh \in (f(x))$.

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

Let $g(x) \notin (f(x))$.

Since $gh \in (f(x)) \Rightarrow f(x) \mid gh$.

and $g(x) \notin (f(x)) \Rightarrow f(x) \nmid g(x)$,

$\gcd(f(x), g(x)) = 1$.

$\Rightarrow 1 = f(x)p(x) + g(x)q(x)$

where $p(x), q(x) \in k[x]$.

$$h = f(x)p(x)h(x) + g(x)q(x)h(x).$$

$$= fph + fq_1 q$$

$$= f(ph + q_1 q) \in (f(x)).$$

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

<u>Remark</u>. Every nonzero prime ideal of $k[x]$ is gen by an irreducible poly.

<u>Example</u>. $R = \mathbb{Z}[i]$. Is (2) is a prime ideal ?

<u>No</u>. $2 = (1+i)(1-i)$.

But $(1+i) \notin (2)$ & $(1-i) \notin (2)$.

Suppose $(1+i) \in (2)$.

$\Rightarrow (1+i) = 2(a+bi) = 2a + i2b$

$\Rightarrow 2a = 1. \Rightarrow a = \frac{1}{2}$ which is a contradiction.

Hence $(1+i) \notin (2)$. Similarly $(1-i) \notin (2)$.

(2) is not a prime ideal in $\mathbb{Z}[i]$.

<u>Q</u>. For which ideal I in R R/I is a field ?

If R/I is a field then

R/I has exactly two ideals

(0) and (1) in R/I.

$$\begin{array}{ccc} (0) & & (1) \\ \updownarrow & & \updownarrow \\ I & & 1+I \end{array}$$ in R/I.

$I \subset R$.

$I \subset M \subset R$.

$(0) \subset M+I \subset (1)$ R/I.

<u>Defn</u>. An ideal I of a ring R is called a maximal ideal if whenever $I \subset M \subset R$ then either $M=I$ or $M=R$.

i.e I is not contained in any ideal other that I and R.

<u>Propn</u>. Maximal ideal always exists in a non-zero ring.

<u>Zorn's Lemma</u>: Let S be partially ordered set. If every totally ordered subset of S has an upper bound then S contains a maximal elt.

<u>Pf. of Propn</u>: Consider the set

$$S = \{ I \mid I \text{ is a proper ideal of } R \}.$$

Let T be a totally ordered subset of S i.e for all $I, J \in T$ then 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 ideal.

By Zorn's lemma S has a maximal elt.

<u>Propn</u>. An ideal M of R is maximal ideal iff R/M is a field.

<u>Ex</u>.

Cor The zero ideal is a maximal ideal of R iff R is a field.

Q Is every maximal ideal a prime ideal?

Ans Yes. If I is a maximal ideal then R/I is a field so R/I is an int domain and hence I is a prime ideal.

Q Is every prime ideal maximal ideal?

Ans No. (0) is a prime ideal in $\mathbb{Z}$. But (0) is not a maximal ideal as $(0) \subsetneq (p)$

Example. $\mathbb{C}[x,y]$.

$$(0) \subset (x) \subset (x,y).$$

Here (x) is a prime ideal but not maximal ideal.

$$(x,y) = p(x,y)\,x + q(x,y)\,y.$$

where $p(x,y), q(x,y) \in \mathbb{C}[x,y]$.

$$\frac{\mathbb{C}[x,y]}{(x,y)} \cong \mathbb{C}.$$

$$\frac{\mathbb{C}[x,y]}{(x)} \cong \mathbb{C}[y].$$ is an int domain

Hence (x) is a prime ideal.

<u>Example</u> What are the maximal ideals of $\mathbb{Z}$?

Any non-zero prime ideal of $\mathbb{Z}$ is a maximal ideal.

<u>Example</u> What are the maximal ideal of $k[x]$?

Since every maximal ideal is prime therefore every maximal ideal will be gen by an irr poly.

$I = (f(x))$ where $f(x)$ is irreducible.

<u>WTS</u> I is a maximal ideal.

let $g(x) \in k[x] \setminus I$. ie $\overline{g(x)} \neq 0$ in R/I.

Since $f(x)$ is irreducible and $g(x) \notin I$. thus $\gcd(f(x), g(x)) = 1$.

$$1 = g(x)p(x) + f(x)q(x).$$

for some $p(x), q(x) \in k[x]$.

Thus $\bar{1} = \bar{g}(x)\,\bar{p}(x)$ in $k[x]/I$.

$\therefore$ $k[x]/I$ is a field

and hence I is a maximal ideal.

<u>Remark</u>. In $k[x]$ every maximal ideal is gen by an irreducible poly.

Q What are the maximal ideals of $\mathbb{C}[x]$?

By FTA any poly $f(x) \in \mathbb{C}[x]$ of (+)ve deg is a product of linear poly's. Hence the maximal ideals of $\mathbb{C}[x]$ are of the form $m_a = (x-a)$ where $a \in \mathbb{C}$.

$$\begin{array}{ccc} \mathbb{C} & & \mathbb{C}[x] \\ a & \rightsquigarrow & m_a = (x-a). \end{array}$$

Hence there is a 1-1 correspondence betwn the pts in $\mathbb{C}$ and the set of maximal ideals in $\mathbb{C}[x]$

Note that $\varphi : \mathbb{C}[x] \longrightarrow \mathbb{C}$

defined by $\varphi(f(x)) = f(a)$.

$\ker \varphi = (x-a)$.

$$\frac{\mathbb{C}[x]}{(x-a)} \cong \mathbb{C}.$$

The extension of the above fact to several variable is one of the most important Thm about polynom.

$\mathbb{C}^n$ $\qquad\qquad$ $\mathbb{C}[x_1, x_2, \ldots, x_n]$

$\underline{a} = (a_1, \ldots, a_n)$ $\qquad\qquad$ $m_{\underline{a}} = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$

[Hilbert's Nullstellensatz]:

The maximal ideals of the poly ring $R = \mathbb{C}[x_1, \dots, x_n]$ are in 1-1 correspondence with the pts in $\mathbb{C}^n$. A pt $\underline{a} = (a_1, \dots, a_n) \in \mathbb{C}^n$ corresponds to the kernel of the map

$$S_{\underline{a}} : \mathbb{C}[x_1, \dots, x_n] \longrightarrow \mathbb{C}.$$

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

The kernel of $S_{\underline{a}}$ is the ideal gen by $(x_1 - a_1, \dots, x_n - a_n)$

$= m_{\underline{a}}$

$$\underline{\mathbb{C}[x_1, x_2] \xrightarrow{\varphi} \mathbb{C}}.$$

$\underline{a} = (2, 3)$

$$f(x_1, x_2) \rightsquigarrow f(2, 3)$$

$$f(x_1, x_2) \in \ker \varphi = (x_1 - 2,\ x_2 - 3).$$

$$f(x_1, x_2) = f_1(x_1, x_2)(x_1 - 2) + f_2(x_1, x_2)(x_2 - 3).$$

$$f(2, 3) = 0.$$

<u>Remark</u>, You know how to solve a system of linear eq$^{\underline{n}}$.

<u>Q</u> How to solve a system of non-linear eq$^{\underline{n}}$s ?

Gröbner Bases.

<u>Defn</u>. 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 polys in n-variables then V is called an algebraic variety.

<u>Example</u>. $(a,b) \in \mathbb{C}^2$ Every pt is a variety $Z(x-a, y-b)$.

$$Z(\underbrace{x-a}_{f_1}, \underbrace{y-b}_{f_2}) \qquad \mathbb{C}[x,y]$$

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

$\{(x, \sin x) \mid x \in \mathbb{C}\} \subseteq \mathbb{C}^2$.

is not a variety.

Note that if $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$

then $V = Z(f_1, \dots, f_n) := \{(a_1, \dots, a_n) \in \mathbb{C}^n \mid f_i(a_1, \dots, a_n) = 0\}$.

$\cap|$

$\mathbb{C}^n$.

$f_i \in \mathbb{C}[x_1, \dots, x_n]$

If $f = 0$. $Z(f) = \mathbb{C}$.

If $f = 1$. $Z(f) = \emptyset$.

$\boxed{\text{Zariski Top.}}$

Thm. Let $f_1, \ldots, f_r$ be polys in $\mathbb{C}[x_1, \ldots, x_n]$ and $V = Z(f_1, \ldots, f_r)$. Let $I = (f_1, \ldots, f_r)$. The maximal ideals of the quotient ring

$$R = \frac{\mathbb{C}[x_1, \ldots, x_n]}{I}$$

are in bijective correspondence with pts in V.

Pf: The maximal ideals of R corresponds to those maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ which contain I. A maximal ideal of $\mathbb{C}[x_1, \ldots, x_n]$ is of the form $m_{\underline{a}} = (x_1 - a_1, \ldots, x_n - a_n)$ for some $\underline{a} = (a_1, \ldots, a_n) \in \mathbb{C}^n$.

Thus if it is a maximal ideal of R then $m_{\underline{a}} \supseteq I = (f_1, \dots, f_n)$.

So $f_i \in m_{\underline{a}} = (x_1 - a_1, \dots, x_n - a_n)$.

$\Rightarrow \quad f_i = p_1(x_1 - a_1) + \dots + p_n(x_n - a_n)$.

$\Rightarrow \quad f_i(a_1, \dots, a_n) = 0. \quad \forall i.$

which implies that $\underline{a} \in Z(f_1, \dots, f_n)$.

<u>Cor</u>. Let $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$

If the system of eqns $f_1 = 0, \dots, f_n = 0$ has no soln. in $\mathbb{C}^n$ then $(f_1, \dots, f_n) = 1$.

Pf: $Z(f_1, \ldots, f_r) = \phi$.

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

$$\frac{\mathbb{C}[x_1, \ldots, x_n]}{I}.$$

which means there is no maximal ideal containing $I = (f_1, \ldots, f_r)$. Therefore I is the unit ideal.

Hence $(f_1, \ldots, f_r) = (1)$.