Discussion of Tut 7

Gaussian prime $\longrightarrow$

A prime elt in $\mathbb{Z}[i]$ is called gaussian prime.

p is prime integer.

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

Here p is a prime in $\mathbb{Z}$.

But p is not a prime elt in $\mathbb{Z}[i]$ i.e p is not a gaussian prime.

2 is prime $\mathbb{Z}$.

$2 = (1+i)(1-i)$ is not a gaussian prime.

$n=1$ Case

$\mathbb{C}$ $\qquad\qquad$ $\mathbb{C}[x]$.

Q How does the maximals ideals of $\mathbb{C}[x]$ looks like?

Every maximal ideal is of the form $\langle (x-a) \rangle = m_a$

$a \in \mathbb{C}$.

$$\begin{tikzcd}
\mathbb{C} \arrow[d, phantom, "\rotatebox{90}{$\in$}"] & \mathbb{C}[x] \\
a \arrow[r, squiggly, bend left] & m_a = (x-a). \arrow[l, squiggly, bend left]
\end{tikzcd}$$

Hilbert's Nullstellensatz

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

$$\underline{a} = (a_1, a_2, \dots, a_n) \rightsquigarrow m_{\underline{a}}$$

where $a_i \in \mathbb{C}$. $\qquad = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$

$$\frac{\mathbb{C}[x_1, \dots, x_n]}{(x_1 - a_1, \dots, x_n - a_n)} \cong \mathbb{C}.$$

Remark: Every maximal ideal of $\mathbb{C}[x_1, \dots, x_n]$ is of the form

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

for some pt $\underline{a} = (a_1, \dots, a_n) \in \mathbb{C}^n$.

Tut 7.

Q2. Every finite integral domain is a field.

Let F be a finite field.

$$\underbrace{1+1+\cdots+1} = n\cdot 1.$$

Then $\exists$ some int n s.t. $n\cdot 1 = 0$.

$n = m_1 m_2$.

$n\cdot 1 = m_1 1 \; m_2 1 = 0$.

$\Rightarrow$

The smallest int for which $n\cdot 1 = 0$

has to be a prime no.

$ch(F) =$ smallest n s.t. $n\cdot 1 = 0$

$=$ prime number.

If F is a finite field then $ch(F) = p$ where p is a prime number.

$$\boxed{\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}.}$$

F is a finite field of ch p

then $\underline{\mathbb{F}_p} \subseteq F$.

Can I consider F as a vector sp over $\underline{\underline{\mathbb{F}_p}}$?

$$\begin{array}{c} F \\ | \\ \mathbb{F}_p \end{array}$$

Let $\underline{\alpha} \in \mathbb{F}_p$. and $a \in \underline{F}$.

$\underline{\underline{\alpha \cdot a}}$

Suppose $\dim_{\mathbb{F}_p} F = n$.

$|F| = p^n$.

$a_1, \ldots, a_n \in F$ is a basis of F over $\mathbb{F}_p$.

$\alpha \in F \qquad \alpha = \alpha_1 a_1 + \cdots + \alpha_n a_n.$

where $\alpha_i \in \mathbb{F}_p$.

$$|F| = p^n.$$

<u>Remark</u>. Every finite field has cardinality p^n for some prime p and (+)ve int n.

<u>Q3</u>. R is an int domain.

$$Q(R) = \left\{ \frac{a}{b} \;\middle|\; a, b \in R \text{ and } b \neq 0 \right\}.$$

$$Q(R[x]) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in R[x] \text{ and } g(x) \neq 0 \right\}.$$

Q4

$$R = \boxed{\frac{\mathbb{F}_5[x]}{(x^2+x+1)}}$$

$\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$

Since $\mathbb{F}_5[x]$ is a poly ring over a field $\mathbb{F}_5$ every prime ideal is gen by an irreducible poly. $\mathbb{F}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

let $f(x) = x^2+x+1$

$f(\bar{0}) \neq 0$, $f(\bar{1}) \neq 0$

$f(\bar{2}) = \bar{2} \neq 0$. $f(\bar{3}) = \bar{3} \neq \bar{0}$

$f(\bar{4}) = \bar{1} \neq 0$.

i.e $f(x)$ is irreducible over $\mathbb{F}_5[x]$.

$\therefore$ $(f(x))$ is prime ideal here R is int dom

Q6 $\quad m = (x+y^2, y+x^2+2xy^2+y^4)$

$= (\underline{x+y^2}, \underline{y+(x+y^2)^2})$

$= (x+y^2, y)$

$= (x, y)$

$\dfrac{\mathbb{C}[x,y]}{(x,y)} \cong \mathbb{C}$ which is a field

$\therefore (x,y)$ is a maximal ideal.

Q7. $R = \boxed{\mathbb{C}[x,y]/(x^3+y^2-17).}$

The maximals of R is of the form $m_{\underline{a}}$ s.t $m_{\underline{a}} \supseteq (x^3+y^2-17)$

$$x^3+y^2-17 \in (x-a_1, y-a_2).$$

$$\qquad\qquad\qquad\qquad\qquad \| $$

$$\qquad\qquad\qquad\qquad\qquad m_{\underline{a}}$$

$$\underline{a} = (a_1, a_2)$$

$$x^3+y^2-17 = p_1(x,y)(x-a_1) + p_2(x,y)(y-a_2).$$

i.e $a_1^3+a_2^2-17 = 0$.

The maximal ideals of R is of the form $m_{\underline{a}}$ s.t $\underline{a} = (a_1, a_2)$ is a root of the poly x^3+y^2-17.

Q10. $\phi: R \longrightarrow \mathbb{R}$

$$\phi(f) = f(0).$$

ϕ is a ring homo.

ϕ is surjective.

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

$$= I.$$

By 1st isomorphism Thm

$$R/I \cong \mathbb{R}. \sim \text{field}.$$

$\Rightarrow I$ is maximal ideal.

$\mathbb{Z}[x]$

maximal ideal $= (p, f(x))$

where p is a prime int

and $f(x)$ is irreducible

over $\mathbb{Z}/p\mathbb{Z}\,[x]$.

(x)

$\mathbb{Z}[x]/(x) \cong \mathbb{Z}.$

This is not a maximal ideal.