Lecture 36

(36.0) Recall - the results on rings and ideals so far.

Assume : R is commutative

- $I \subset R$ is an ideal if it is a subgroup s.t. $RI \subset I$.
- $x \in R$ is a zero-divisor if $\exists\, y \in R \setminus \{0\}$ s.t. $xy = 0$.
- $a \in R$ is a unit (or 'a' is invertible) if $\exists\, b \in R$ s.t. $ab = 1$.

$R^{\times}$ = set of units in R (group under multiplication).

Definition : We say R is an integral domain if $\boxed{x \in R \text{ is a zero divisor} \Rightarrow x = 0}$.

We say R is a principal ideal ring if every ideal in R is of the form (a) (namely, $\{ra \mid r \in R\}$, also denoted by Ra). (i.e. principal).

P.I.D. (short for principal ideal domain) = integral domain which is also a principal ideal ring.

e.g. $\mathbb{Z}$, K (any field), $K[X]$ (polynomials in 1-variable with coefficients from a field K)

$\mathbb{Z}[\sqrt{-1}]$ are examples of P.I.D.'s. (see Lecture 35.)

$\mathbb{Z}[X]$, $K[X, Y]$ are integral domains, but NOT P.I.D.'s.

(36.1) Recall : R is a field if $R^\times = R \setminus \{0\}$ (it is commutative today, remember!).

We proved earlier that $R^\times \cap \text{ZeroDivisors}(R) = \phi$. Hence

$$\boxed{\text{Every field is an integral domain}}.$$

<u>Characteristic of a ring.</u> Let R be a commutative ring.

($0_R, 1_R \in R$; $0_R \neq 1_R$ - remember!)

We automatically get a ring homomorphism

$$\mathbb{Z} \xrightarrow{\phi} R$$

$$n \longmapsto \begin{cases} \underbrace{1+1+\cdots+1}_{n\text{-times}} & \text{if } n \geq 0 \quad (= 0_R \text{ if } n = 0) \\ -(\underbrace{1+\cdots+1}_{-n\text{-times}}) & \text{if } n < 0 \end{cases}$$

(for some $p \in \mathbb{Z}_{\geq 0}$; $p \neq 1$)

Let $I = (p)\ (= p \cdot \mathbb{Z}) \subset \mathbb{Z}$ be the kernel of φ.

(recall : $\text{Ker}(\varphi) = \{x \in \mathbb{Z} \mid \phi(x) = 0\} \subsetneq \mathbb{Z}$ is an ideal

Ideals in $\mathbb{Z}$ (proper) $= \{\{0\}, p\mathbb{Z}\ (p \in \mathbb{Z}_{\geq 2})\}$)

because $\varphi(1) = 1_R \neq 0_R$.

<u>Warning</u> : I am <u>not</u> claiming that <u>p is a prime</u>.

We say p is <u>the characteristic of R</u>.

(36.2) Continuing with $\phi : \mathbb{Z} \longrightarrow R$; $\mathrm{Ker}(\phi) = p\mathbb{Z} \subset \mathbb{Z}$

$(p \in \mathbb{Z}_{\geq 0}\, ;\ p \neq 1)$.

By 1^{st} iso. thm., we must get an <u>injective ring homomorphism</u>

$$\mathbb{Z}/p\mathbb{Z} \xhookrightarrow{\ \bar{\phi}\ } R.$$

<u>Lemma</u>. If R is an integral domain then p is a prime; or $p=0$.

<u>Proof</u>. If $p = p_1 \cdot p_2$ is non-zero, not a prime; then

$$\exists\ a, b \in \left(\mathbb{Z}/p\mathbb{Z}\right) \setminus \{\bar{0}\} \text{ s.t. } ab = 0.$$

$\Rightarrow \bar{\phi}(a) \cdot \bar{\phi}(b) = 0_R$. But $\bar{\phi}$ is injective, so

$\bar{\phi}(a), \bar{\phi}(b) \neq 0$; contradicting the fact that R is an integral domain $\square$

Conclusion: Characteristic of an integral domain = 0 or prime.

(e.g. $\mathrm{Char}(\mathbb{Z}/p\mathbb{Z}) = p$ for a prime # p.)

a field, hence integral domain

(36.3) Prime ideals and Maximal ideals.

Let R be a commutative ring. Let $I \subsetneq R$ be a proper ideal.

Consider the quotient ring $\overline{R} = R/I$.

We say that I is a prime (resp. maximal) ideal if

$\overline{R} = R/I$ is an integral domain (resp. field).

Proposition. (1) $I \subsetneq R$ is a prime ideal if, and only if

I is an ideal (proper) and $\boxed{ab \in I \Rightarrow a \in I \text{ or } b \in I.}$

(2) $I \subsetneq R$ is a maximal ideal if, and only if, I is a proper ideal; and

$$\boxed{\begin{array}{l} J \subset R \text{ (an ideal)};\ I \subset J \Rightarrow I = J \text{ or } J = R \\ \text{"maximal with respect to inclusion."} \end{array}}$$

(3) Maximal $\Rightarrow$ Prime.

Proof (3) is obvious, since every field is an integral domain

(1): Let $I \subsetneq R$ be a proper ideal.

I is prime $\iff$ R/I is an integral domain

$$\iff \begin{cases} a \pmod{I} \cdot b \pmod{I} = 0 \\ \quad \Rightarrow a = 0 \pmod{I} \text{ or } b = 0 \pmod{I} \end{cases}$$

$$\iff \boxed{ab \in I \Rightarrow a \in I \text{ or } b \in I}.$$

(2). $I \subsetneq R$ a proper ideal.

I is Maximal $\iff$ R/I is a field.

$\overset{\iff}{(*)}$ Ideals in R/I $=$ $\{\{0\}, R/I\}$

see Lemma below

(remember Ideals in R/I $\longleftrightarrow$ Ideals in R containing I - (Lecture 35))

So I is maximal $\iff$ Set of ideals of R containing I $=$ $\{I, R\}$ $\square$

<u>Lemma.</u> A commutative ring K is a field if and only if Ideals in K $=$ $\{\{0\}; K\}$.

<u>Proof.</u> Recall K is a field $\iff$ $K \setminus \{0\} = K^{\times}$ (every non-zero element is invertible).

We have already seen the proof of forward implication (if $I \neq \{0\}$, an ideal in K, then some $\lambda \in K \setminus \{0\}$ is in I

$\Rightarrow$ $I \supset K.\lambda \ni \lambda^{-1}\lambda = 1$

$\Rightarrow$ $I \supset K.1 = K$. Hence $I = K$.)

Conversely, let $a \in K \setminus \{0\}$ and $I = (a)$ ideal generated by a

$= K.a$

$= \{\lambda a \mid \lambda \in K\}$.

As $a \in I \setminus \{0\}$, $I \neq \{0\}$.

But that means $I = K$. Hence $\exists\, \lambda \in K$ s.t $\lambda a = 1$

(only ideals are $\{0\}$ & K) i.e. $a \in K^{\times}$. $\square$

(36.4) Some examples.

Proper ideals in $\mathbb{Z}$ = $\{0\}$ or $n\mathbb{Z}$ $(n \in \mathbb{Z}_{\geq 2})$

Prime ideals in $\mathbb{Z}$ = $\{0\}$ or $\boxed{p\mathbb{Z} \ (p \in \mathbb{Z}_{\geq 2} \text{ is prime.})}$

only prime; non-maximal ideal

Maximal ideals in $\mathbb{Z}$

Proper ideals in $\mathbb{C}[X]$ = $\{0\}$ or $(g(x))$ $g(x) \in \mathbb{C}[X]$

prime ideal

$d = \text{degree}(g) \geq 1$

g is monic

(i.e. $g(x) = 1.x^d + a_{d-1}x^{d-1} + \dots + a_0$)

Note : $(0) \subset R$ is a prime ideal $\iff$ R is an integral domain ($R = R/(0)$ - put in the definition)

Over $\mathbb{C}$, every polynomial factors $g(x) = (X - z_1)(X - z_2) \dots (X - z_d)$

$z_1, \dots, z_d \in \mathbb{C}$

(not necessarily distinct).

Lemma. Let $g(X) \in \mathbb{C}[X]$ be monic of degree $d \geq 1$.

Then $(g(X)) \subsetneq \mathbb{C}[X]$ is prime $\Rightarrow$ degree of $g(X) = 1$

$\Rightarrow (g(X))$ is maximal.

<u>Proof.</u> Assume $g(X) = (X-z_1)(X-z_2)\dots(X-z_d)$.

$I := (g(X)) \subsetneq \mathbb{C}[X]$. Use Prop. (36.3) to say: if

$$\boxed{\begin{array}{l} I \text{ is prime} \\ \& \ (X-z_1)\cdot\big((X-z_2)\dots(X-z_d)\big) \in I \end{array}}$$

then $X - z_1 \in I$
or $(X-z_2)\dots(X-z_d) \in I$

(recall: $g(X)$ is <u>the</u> element of smallest degree in $I \setminus \{0\}$)

As d is smallest, we get $d = 1$.

Thus $g(X) = (X - z)$ for some $z \in \mathbb{C}$.

But then $\mathbb{C}[X]/I = \mathbb{C}[X]/(X-z) \cong \mathbb{C}$ as a ring, <u>hence a field.</u>

$$\begin{array}{ccc} \mathbb{C}[X]/(X-z) & \cong & \mathbb{C} \\ \Uparrow & & \Uparrow \\ f(X) & \longmapsto & f(z) \end{array}$$

$\Rightarrow (X - z)$ is maximal. $\square$

Conclusion: Prime ideals of $\mathbb{C}[X]$ $\longleftrightarrow$ $\{0\}$ <u>union</u> $\{(X-z) : z \in \mathbb{C}\}$

Maximal ideals in $\mathbb{C}[X]$.