Note Title 10/18/2022

# Lecture 28 and 29 — Oct 17 and Oct 18

Ex: Let $R$ be a ring and $a \in R$. Then,

- $Ra = \{ra \mid r \in R\}$ is a left ideal.
- $aR = \{ar \mid r \in R\}$ is a right ideal.

Ex: Let $\{A_\alpha \mid \alpha \in \Delta\}$ be a family of ideals in a ring $R$.

Then $\bigcap_{\alpha \in \Delta} A_\alpha$ is again an ideal in $R$.

Definition: Let $X$ be a subset of a ring $R$. The smallest ideal in $R$ which contains $X$ is called the ideal generated by $X$.

Notation: $\cdot$ $(X)$ denotes the smallest ideal containing $X$.
If $X = \{x_1, x_2, \ldots, x_n\}$, then $(X)$ is denoted by $(x_1, x_2, \ldots, x_n)$.

- Let $X \subseteq R$. Let $\{A_\alpha \mid \alpha \in \Delta\}$ be the family of all the ideals of $R$ which contains $X$. Then, $\bigcap_{\alpha \in \Delta} A_\alpha$ is an ideal and clearly $\bigcap_{\alpha \in \Delta} A_\alpha$ is the smallest ideal containing $X$.
- Let $R$ be a ring and $a \in R$. Then,

$$(a) = \text{the smallest ideal in } R \text{ containing the element '}a\text{'}$$
$$= \left\{ ra + as + na + \sum_{i=0}^{m} r_i a s_i \;\middle|\; \begin{array}{l} m \geq 0,\ r, r_i, s_i \in R, \\ n \in \mathbb{Z} \end{array} \right\}.$$

- If $R$ is commutative, then $(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$
- If $R$ is commutative with identity, then $(a) = Ra$.

__Definition (Prime ideal):__ An ideal $I$ in a ring is said to be prime if $I \neq R$ and if $a \cdot b \in I$ for $a, b \in R$, then either $a \in I$ or $b \in I$.

__Ex:__ • In $\mathbb{Z}$, the prime ideals are $\{0\}$ and $p\mathbb{Z}$, where $p$ is a prime.

- In an integral domain $R$, $\{0\}$ is a prime ideal.
- In a field $F$, $\{0\}$ is the only prime ideal (in fact, the only proper ideal).

__Theorem:__ Let $R$ be a commutative ring with identity. Let $I$ be a proper ideal. Then, $I$ is a prime ideal $\Leftrightarrow$ $R/I$ is an integral domain.

<u>Proof</u>: Let $I$ be a prime ideal. <u>claim</u>: $R/I$ is an integral domain.

Since $R$ is commutative with identity, so $R/I$ is also commutative with identity $1+I$.

Let $(a+I)\cdot(b+I) = I$.

Then, $ab + I = I \Rightarrow ab \in I \Rightarrow$ Either $a \in I$ or $b \in I$.

$\Rightarrow a + I = I$ or $b + I = I$ $\quad$ ($\because$ $I$ is a prime ideal)

$\therefore$ $R/I$ has no zero divisor.

$\Rightarrow$ $R/I$ is an integral domain.

Conversely, suppose that $R/I$ is an integral domain, $I \neq R$.

Let $ab \in I$ for some $a, b \in R$.

Then, $ab + I = I \Rightarrow (a+I)\cdot(b+I) = I$

$\Rightarrow a + I = I$ or $b + I = I$

$\Rightarrow a \in I$ or $b \in I$. ($\because R/I$ has no zero divisor)

This proves that $I$ is a prime ideal.

—— x ——

#

<u>Ex</u>: Let $R$ be a ring with identity. Let $I$ be an ideal.

Then, $I = R \Leftrightarrow I$ contains a unit.

<u>Ex</u>: Let $A_1, A_2, \ldots, A_n$ be ideals in $R$. Then,

$A_1 + \cdots + A_n = \{a_1 + \cdots + a_n \mid a_i \in A_i, i = 1, 2, \ldots, n\}$ is an ideal in $R$.

<u>Maximal ideal:</u> Let $R$ be a ring and let $I$ be a proper ideal in $R$. $I$ is called a maximal ideal if $I \subseteq J \subseteq R$ where $J$ is an ideal, then either $I = J$ or $J = R$.

That is, there is no proper ideal lying between $I$ and $R$ properly containing $I$.

<u>Ex:</u>
- In $(\mathbb{Z}, +, \cdot)$, $p\mathbb{Z}$ is maximal for every prime $p$.
- In $\mathbb{Z}$, $\{0\}$ is a prime ideal which is not a maximal ideal.
- In $2\mathbb{Z}$, $4\mathbb{Z}$ is a maximal ideal.

__Theorem:__ In a ring $\boxed{\text{with identity}}$ maximal ideal always exists.

__Proof:__ The proof requires Zorn's lemma. So, we don't give the proof.

__Theorem:__ Let $R$ be a commutative ring with identity. An ideal $I$ is a maximal ideal $\Leftrightarrow$ $R/I$ is a field.

__Proof:__ Let $I$ be a maximal ideal. __Claim:__ $R/I$ is a field.

Since $R$ is commutative with identity, so $R/I$ is also commutative with identity.

Let $a+I \neq I$, (that is, $a+I$ is nonzero in $R/I$).

Then, $a \notin I$. Consider the ideal $I + aR$.

Since $1 \in R$, so $a \in aR$.

Also, $a \notin I$, so $I \subsetneq I + aR$

Since $I$ is maximal, so $I + aR = R$

$\Rightarrow 1 \in I + aR$

$\Rightarrow 1 = c + ab$ where $c \in I$ and $b \in R$.

Now, $1 + I = (c + ab) + I = ab + I \quad (\because c \in I)$

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

$\therefore$ $b + I$ is the inverse of $a + I \Rightarrow a + I$ is a unit.

Thus, every nonzero element of $R/I$ is a unit.

This proves that $R/I$ is a field.

Conversely, suppose that $R/I$ is a field.

Let $I \subsetneq J \subseteq R$, where $J$ is an ideal, $J \neq I$.

Let $a \in J$ and $a \notin I$. Then, $a + I \neq I$ and hence $a + I$ is a unit in $R/I$ ($\because R/I$ is a field).

$\Rightarrow \exists\, b \in R$ s.t. $(a+I)(b+I) = 1 + I$

$\Rightarrow ab + I = 1 + I \Rightarrow 1 - ab \in I \Rightarrow 1 - ab \in J.$

Now, $1 = \underbrace{(1-ab)}_{\in J} + \underbrace{ab}_{\in J} \in J$

$\left[\begin{array}{l} a \in J \\ \Rightarrow ab \in J \end{array}\right.$

$\therefore\ J = R.$

This proves that $I$ is a maximal ideal. #

**Theorem:** In a commutative ring with identity, every maximal ideal is a prime ideal.

**Proof:** Let $R$ be a commutative ring with identity. Let $M$ be a maximal ideal. Then, $R/M$ is a field $\Rightarrow$ $R/M$ is an integral domain.

$\Rightarrow$ $M$ is a prime ideal. #

If a ring does not have identity, maximal ideals need not be prime ideals. For example, in $2\mathbb{Z}$, $4\mathbb{Z}$ is a maximal ideal but $4\mathbb{Z}$ is <u>not</u> a prime ideal.

---

§ <u>Ring homomorphism</u>: Let $R$ and $S$ be rings.

A function $f : R \to S$ is called a ring homomorphism

$$\left.\begin{array}{l} \text{if } f(x+y) = f(x) + f(y) \\ \text{and } f(xy) = f(x)f(y) \end{array}\right\} \forall\, x, y \in R$$

If $f$ is 1-1 and onto, then $f$ is said to be an isomorphism.

Given a ring homomorphism $f: R \to S$, its kernel is defined as $\ker(f) = \{ r \in R \mid f(r) = 0 \}$.

<u>Ex</u>: $\ker(f)$ is an ideal in $R$.

$\mathrm{Im}(f) = \{ f(r) \mid r \in R \}$ is a subring of $S$.

<u>Theorem</u> (<u>1st isomorphism theorem</u>): Let $f: R \to S$ be a ring homomorphism. Then, $R/_{\ker f} \cong \mathrm{Im}(f)$.

#