# Lecture 7: Third Isomorphism theorem, prime and maximal ideals.

First isom thm: $\varphi: A \to B$ be a surj ring homo then the induced map $A/\ker(\varphi) \longrightarrow B$ is an isomorphism.

second isom thm: $R$ a comm ring with unity. $S \subseteq R$ subring $I$ an $R$-ideal. Then

$$S/S\cap I \cong S+I/I$$

$$r + S\cap I \longmapsto r + I \quad \text{for } r \in S$$

Third isom thm: Let $R$ be a comm ring with unity. $I \subseteq J$ be ideals of $R$. Then

$$R/J \cong \frac{R/I}{J/I}$$

$(R/I, +$

$(R, +$

$(R/$

Pf: Note that $J/I$ is an ideal of $R/I$.

Let $\varphi: R/I \longrightarrow R/J$ be the ring homo

$$a+I \longmapsto a+J$$

Note $\varphi$ is well-defined. $(a+I = a'+I \Rightarrow a-a' \in I \subseteq J$
$\Rightarrow a+J = a'+J$

$$\varphi((a+I) \underset{R/I}{\cdot} (a'+I)) = \varphi(aa'+I)$$
$$= aa'+J = (a+J) \overset{R/J}{\cdot} (a'+J)$$
$$= \varphi(a+I)\,\varphi(a'+I)$$

$\varphi$ is surjective ✓

Claim: $\ker(\varphi) = J/I$

$a+I \in \ker\varphi \iff \varphi(a+I) = 0$ in $R/J$
$\iff a+J = 0$ in $R/J$
$\iff a \in J \iff a+I \in J/I$

Hence by 1st isom thm

$$R/I \big/ J/I \cong R/J$$

■

Notation: $R$ a ring $a, b \in R$ then the ideal $(a, b)R$ is also denoted by $(a, b)$ if it clear from the context to which ring this ideal belongs.

Examples: $\dfrac{\mathbb{Z}[X]}{\underset{n\mathbb{Z}[X]}{(n)}} \cong \mathbb{Z}/\underset{n\mathbb{Z}}{(n)}[X]$

$$\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/n\mathbb{Z}[X]$$
$$f \longmapsto f \pmod n$$
$$a_m X^m + a_{m-1}X^{m-1} + \dots + a_0 \longmapsto [a_m]_n X^m + [a_{m-1}]_n X^{m-1} + \dots + [a_0]_n$$

$$\varphi(f+g) = (f+g) \pmod n = f \pmod n + g \pmod n$$
$$= \varphi(f) + \varphi(g)$$

$\varphi$ is a ring homo & surj is clear.

$||^{ly}$ $\varphi(fg) = \varphi(f)\varphi(g)$

$$\ker \varphi = \{ f \in \mathbb{Z}[X] \mid f \pmod n = 0 \text{ in } \mathbb{Z}/n\mathbb{Z}[X] \}$$
$$= \{ f \in \mathbb{Z}[X] \mid n \mid f(x) \} = n\mathbb{Z}[X]$$

So $\dfrac{\mathbb{Z}[X]}{n\mathbb{Z}[X]} \cong \mathbb{Z}/n\mathbb{Z}[X]$

Examples: $\dfrac{\mathbb{Z}[X]}{(5, X^2-2)} \cong \dfrac{\mathbb{Z}/5\mathbb{Z}[X]}{(X^2 - [2]_5)}$

$= \mathbb{Z}[X]$

$$I = 5\mathbb{Z}[X], \quad J = (5, X^2-2)\mathbb{Z}[X]$$

$$R/J \cong \frac{R/I}{J/I}$$

$$\frac{\mathbb{Z}[X]}{(5, X^2-2)} \qquad \frac{\mathbb{Z}[X]}{5\mathbb{Z}[X]} \Big/ \frac{(5, X^2-2)\mathbb{Z}[X]}{5\mathbb{Z}[X]}$$

$$\cong \quad \mathbb{Z}/5\mathbb{Z}[X] \Big/ (X^2 - [2]_5)\,\mathbb{Z}/5\mathbb{Z}[X]$$

$$= \frac{\mathbb{Z}/5\mathbb{Z}[X]}{(X^2 - [2]_5)}$$

$\circledast$ $\dfrac{\mathbb{Z}[X]}{(2, X^2-2)} \cong \dfrac{\mathbb{Z}/2\mathbb{Z}[X]}{(X^2)}$ not reduced

$\underline{\text{Def}^n}$: Prime ideals: Let $R$ be a comm ring with unity. An ideal $P$ of $R$ is said to be a prime ideal if $P \subsetneq R$ and $ab \in P$ for some $a, b \in R \Rightarrow a \in P$ or $b \in P$.

Example: In $\mathbb{Z}$, $n\mathbb{Z}$ is prime ideal iff $n$ is a prime number or $n = 0$.

Pf: $(0)$ is prime ideal ($\because$ $ab = 0 \overset{\mathbb{Z} \text{ is an int domain}}{\Rightarrow} a = 0$ or $b = 0$)

$n \neq 0$: $n$ a prime. Let $ab \in n\mathbb{Z} \Leftrightarrow n \mid ab$
$\overset{n \text{ a prime}}{\Rightarrow} n \mid a$ or $n \mid b \Leftrightarrow a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$ $\Rightarrow$ $n\mathbb{Z}$ is a prime ideal

$n\mathbb{Z}$ a prime ideal. Let $n \mid ab \Leftrightarrow ab \in n\mathbb{Z}$
$\Rightarrow a \in n\mathbb{Z}$ or $b \in n\mathbb{Z} \Leftrightarrow n \mid a$ or $n \mid b$ $\Rightarrow$ $n$ is prime ■

(*) $R$ is an int domain $\Leftrightarrow$ $(0)$ is a prime ideal of $R$.

Prop: Let $R$ be a comm ring with unity and $I \subseteq R$ be an ideal. The ring $R/I$ is an integral domain iff $I$ is a prime ideal.

Pf: Note that $R/I = 0$ iff $I = R$.

$R/I$ is an int domain $\Leftrightarrow$ $I \neq R$ & for $\alpha, \beta \in R/I$
$\alpha\beta = 0 \Rightarrow \alpha = 0$ or $\beta = 0$

$\Updownarrow$

$I \neq R$ & $\alpha = \bar{a}$ & $\beta = \bar{b}$ for some $a, b \in R$
$\overline{ab} = \bar{a}\bar{b} = 0 \Rightarrow \bar{a} = 0$ or $\bar{b} = 0$ in $R/I$

$\Longleftrightarrow$

$I \subsetneq R$ & for $a, b \in R$
$ab \in I \Rightarrow a \in I$ or $b \in I$

$\Updownarrow$

$I$ is a prime ideal of $R$.

Ex 1) $p\mathbb{Z}[x]$ is a prime ideal of $\mathbb{Z}[x]$ if $p$ is a prime. ($\because$ $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong \underbrace{\mathbb{Z}/p\mathbb{Z}[x]}_{\text{Int domain}}$ )

2) $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[\sqrt{2}] \Rightarrow (x^2-2)$ in $\mathbb{Q}[x]$ is a prime ideal.

3) In $\mathbb{Z}[x]$, $(x - n)$ is a prime ideal for $n \in \mathbb{Z}$.

4) $6\mathbb{Z}$ is not a prime ideal of $\mathbb{Z}$

Def$^n$: Maximal ideals: Let $R$ be comm ring with unity. An ideal $m$ of $R$ is called a maximal ideal if $m$ is maximal among proper ideals of $R$, i.e. $m \subseteq I \subseteq R$, $I$ an ideal then

$$I = m \text{ OR } I = R.$$

Prop: Let $R$ be a nonzero comm ring with unity then $R$ contains a maximal ideal.

Ex: In $\mathbb{Z}$, let $p$ be a prime numbes then $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

$$p\mathbb{Z} \subseteq I \subseteq \mathbb{Z}$$

$n \in I \setminus p\mathbb{Z} \Rightarrow (n, p) = 1$ ($\because$ only factors of $p$ are $1$ & $p$)

$\Rightarrow \exists a, b \in \mathbb{Z}$

$an + bp = 1 \in I$

$\Rightarrow I = \mathbb{Z}$

Hence $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

If $n$ is not a prime then $n\mathbb{Z}$ is not maximal

$n = pq$ where $|p|, |q| > 1$

$n\mathbb{Z} \subseteq p\mathbb{Z} \subseteq \mathbb{Z}$; Hence $n\mathbb{Z}$ is not maximal.