Lec 10/17

Wednesday, October 17, 2018 11:32

Ring = abelian gp $+$, bilinear unital associative $\cdot$

$I \subset R$ is an 2-sided/left/right ideal if $(I,+)$ is an ab gp and $IR = RI = I$

f ring homomorphism $R \longrightarrow S$

$Ker(f) \subset R$ is a 2-sided ideal in R.

$Im(f) \subset S$ is a subring of S.

<u>Ideals examples</u>:

(i) $R = K$ a field. $I \subset K$ an ideal. Assume $I \neq \{0\}$.

$\exists\ \lambda \in K \setminus \{0\} = K^{\times}$ s.t. $\lambda \in I$. so $\lambda^{-1} \cdot \lambda = 1 \in I$. then $r = r \cdot 1 \in I\ \forall r \in K$

So ideals of a field are $\{0\}$ and K.

<u>Lemma</u>: R: commutative ring, $I \subset R$ an ideal s.t. $I \cap R^{\times} \neq \emptyset$. then $I = R$.

<u>Pf</u>. pick $\lambda \in I \cap R^{\times}$. then $\lambda^{-1} \cdot \lambda = 1 \in I \Rightarrow r \cdot 1 = r \in I\ \forall r \in R$.

<u>Ex</u>: $\mathbb{R} \supset R$ subring e.g. $\mathbb{Z}[\sqrt{2}]$; $\mathbb{Z}$; $\mathbb{Q}$; $\mathbb{Z}[\pi]$

$\cup$

I ideal only $\{0\}$ or $\mathbb{R}$

<u>Ex</u>. Set of ideals of integers $= \{ n\mathbb{Z} : n = 0, 1, 2, \dots \}$

$\mathbb{Z}_{\geq 0}$		Set of ideals of $\mathbb{Z}$
n	$\longleftrightarrow$	$I_n = n\mathbb{Z} \subset \mathbb{Z}$
$m \mid n$	$\longleftrightarrow$	$I_n \subset I_m$
$d = \gcd(m,n)$	$\longleftrightarrow$	$\underbrace{I_n + I_m}_{\text{smallest ideal containing both.}} = I_d$

$d = \gcd(m,n) \longleftrightarrow \underbrace{I_n + I_m}_{\text{smallest ideal containing both.}} = I_d$

$l = \text{lcm}(m,n) \longleftrightarrow \underbrace{I_n \cap I_m}_{\text{largest ideal contained in both.}} = I_l$

Lemma: The smallest ideal containing ideals I & J is $I+J$.

Pf: This is an ideal containing I & J: $r(a+b) = ra + rb$.

If L is an ideal containing I & J then it contains $I+J$.

Quotient rings:

R: ring, $I \subsetneq R$ 2-sided ideal.

if $I = R$, $R/I = \{0\}$ the 0-ring.

$(R/I, +)$ as an abelian subgroup of $(R, +)$

$a + I \ni \; = a \pmod I$. $a \equiv b \pmod I$ if $a - b \in I$

$$a \pmod I + b \pmod I = a+b \pmod I$$

$$a \pmod I \cdot b \pmod I := a \cdot b \pmod I$$

Check that this $\cdot$ is well-defined:

$$\left.\begin{array}{l} a \equiv a' \pmod I \\ b \equiv b' \pmod I \end{array}\right. \Longrightarrow a \cdot b \equiv a' \cdot b' \pmod I$$

$ab - a'b' \in I$ to prove

$+ab' - ab'$

$\parallel$

$a\underbrace{(b-b')} + \underbrace{(a-a')}b' \in I$ ✓

$$\underbrace{\underbrace{\overset{\substack{\in \\ I}}{}}_{\substack{\in \\ I}}\qquad\underbrace{\overset{\substack{\in \\ I}}{}}_{\substack{\in \\ I}}}_{\text{since } I \text{ is 2-sided ideal.}}$$

$$1_{R/I} := 1 \mod I \neq 0_{R/I} := 0 \pmod{I}$$

R/I is called quotient ring

$n\mathbb{Z} \subset \mathbb{Z} \Rightarrow \mathbb{Z}/n\mathbb{Z}$ is a quotient ring

$$\mathbb{Z}[\underset{\substack{\uparrow \\ -1}}{\sqrt{2}}] = \mathbb{Z}[x]/\underset{\substack{\nearrow \\ -1}}{(x^2-2)}\mathbb{Z}[x]$$

Analogue of 1st Iso thm:

$f : R \longrightarrow S$ a ring homomorphism.

$$\bar{f} : R/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

$$a \pmod{\mathrm{Ker}(f)} \longmapsto f(a)$$

(for any 2-sided proper ideal $I \subsetneq R$, we have a ring hom $\begin{aligned} R &\longrightarrow R/I \\ a &\longmapsto a \pmod{I} \end{aligned}$)

(inj)∘(iso)∘(surj)

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\pi"] & S \\ R/I \arrow[r, "\cong", "\bar{f}"'] & \mathrm{Im}(f) \arrow[u, phantom, "\bigcup"] \end{tikzcd}$$

subring

"Commutative" diagram.

$$\begin{array}{c} \downarrow \\ R/_{Ker(f)} \xrightarrow[\bar{f}]{\cong} Im(f) \end{array}$$

3 things to check:

(1) $\bar{f}$ is well-defined : $a \equiv b \bmod K \Rightarrow a-b \in K \Rightarrow f(a-b)=0 \Rightarrow f(a)=f(b)$.

(2) $\bar{f}$ is a ring hom : $\bar{f}(a(\bmod K) \cdot b(\bmod K)) = \bar{f}(ab(\bmod K)) = f(ab) = f(a)f(b) = \bar{f}(a(\bmod K)) \cdot \bar{f}(b(\bmod K))$

(3) $\bar{f}$ is bijective : Surj by defn of $Im(f)$. Inj since $a \in Ker(f) \Leftrightarrow f(a) = 0_S \Leftrightarrow a \in Ker(f) \Leftrightarrow a \equiv 0 (\bmod K)$.

Let R be a commutative ring and $I, J \subset R$ be two ideals.

$$I \cdot J := \left\{ a_1b_1 + a_2b_2 + \cdots + a_nb_n \;\middle|\; n \in \mathbb{N}, \begin{array}{l} a_1, \ldots, a_n \in I \\ b_1, \ldots, b_n \in J \end{array} \right\}$$

<u>Lemma</u>: $I \cdot J$ is an ideal

<u>pf</u> $r(ab) \in I \cdot J$, $I \cdot J \leq R$.

$I \cdot J \subset I \cap J$ because each $ab \in I$ and J.

$I \cap J$ is an ideal obviously.

eg in $\mathbb{Z}$, $I_m \cdot I_n = I_{mn}$

$\quad\quad\quad\quad\;\; I_m \cap I_n = I_{lcm(m,n)}$ — $\neq$ if m & n are not coprime