Lec 10/16

Tuesday, October 16, 2018 11:37

$R^\times$ = invertible elements / units. A group under multiplication

$a \in R$ is a zero divisor if $ab = 0$ for some nonzero $b \in R$.

Integral domains have no nontrivial zero divisors.

eg $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Z}[x, y, z]$

What goes wrong in non-comm ring?

$H = \{(a_1, a_2, \dots) : a_i \in \mathbb{Z}\} = \mathbb{Z}^{\mathbb{N}}$

Component-wise addition turns H into an abelian gp.

$R = \mathrm{End}_{gp}(H)$. $f_1, f_2 \in R$

$$f_1 + f_2 = \lambda x. (f_1(x) + f_2(x))$$

$$f_1 \cdot f_2 = f_1 \circ f_2$$

$$0_R = \{h \longmapsto 0\}$$

$$1_R = \{h \longmapsto h\}$$

$$\begin{aligned} \varphi : H &\longrightarrow H \\ (a_1, a_2, \dots) &\longmapsto (0, a_1, a_2, \dots) \end{aligned}$$

$$\begin{aligned} \psi : H &\longrightarrow H \\ (a_1, a_2, \dots) &\longmapsto (a_2, a_3, \dots) \end{aligned}$$

$\Rightarrow \psi \cdot \varphi = 1_R$

$$\begin{array}{ccc} \pi : H & \longrightarrow & H \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ (a_1, a_2, \dots) & \longmapsto & (a_1, 0, \dots) \end{array} \qquad \Rightarrow \qquad \pi \cdot \varphi = 0_R$$

Lemma: If R is commutative & $a \in R^\times$ then a is not a zero divisor.

Pf $\exists b$ s.t. $ab = 1 = ba$. If $ac = 0$ then $c = cab = 0b = 0$.

Defn Ring homomorphism. Obvious.

Defn $A \subseteq R$ is a subring if it's a ring w/ $+_R, \cdot_R, 0_R, 1_R$. ↗ eg $\mathbb{Z} \subset \mathbb{Q}$

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

$\mathrm{Ker}(f) := \{x \in R : f(x) = 0_S\}$

$\mathrm{Im}(f) := \{f(x) : x \in R\}$

Lemma: $\mathrm{Im}(f) \subset S$ is a subring.

(but $\mathrm{Ker}(f) \subset R$ is not since $1_R \notin \mathrm{Ker}(f)$).

Pf: $0_R \xmapsto{f} 0_S$ so $0_S \in \mathrm{Im}(f)$.

$1_R \xmapsto{f} 1_S$ so $1_S \in \mathrm{Im}(f)$.

$f(a) \pm f(a') = f(a \pm a')$

$f(x) \cdot f(y) = f(x \cdot y)$

Defn Let R be a ring, $I \subset R$. I is a left ideal if

$\underbrace{I \text{ is an abelian gp under } +_R}$, and $\forall x \in I, r \in R, rx \in I$ (i.e. $RI = I$).

I is a right ideal if and $IR = I$. If $IR = RI = I$, I is a two-sided ideal.

Lemma. $Ker(f) \subset R$ is a two-sided ideal.

pf $r \in R$, $x \in ker(f) \Rightarrow f(rx) = f(r)f(x) = f(r) \cdot 0_S = 0_S$.

eg $R = \mathbb{Z}$. **Claim:** every ideal is $I_n = n \cdot \mathbb{Z} \subset \mathbb{Z}$.

$\rightarrow$ Only subring of $\mathbb{Z}$ is $\mathbb{Z}$ (easy)

this is n=0 case.

Let $I \subset \mathbb{Z}$ be an ideal. Suppose $I \neq \{0\}$.

take k = smallest positive element of I.

Claim: $\forall x \in I$, $k \mid x$ so $I \subset k\mathbb{Z}$
$\begin{matrix} I \\ \cup \\ k\mathbb{Z} \end{matrix}$

pf euclid's algorithm:

$\forall \ell \in I$, $\ell = qk + r$ where $0 \leq r < k$

and $r = \ell - qk$ is in I so $r = 0$.

Properties in $\mathbb{Z}$

$$\text{Set of ideals} = \{ \overset{\overset{I_n}{\parallel}}{n\mathbb{Z}} : n = 0, 1, \dots \}$$

$$I_n \subset I_m \Leftrightarrow m \mid n$$

$$I_n + I_m = I_{gcd(n,m)}$$

$$I_n \cdot I_m = I_{lcm(n,m)}$$

smallest ideal containing I_n and I_m

largest ideal contained in both of them.