Lecture 30

Wednesday, March 18, 2015 8:15 AM

$\boxed{R \text{ a ring w/ } 1}$

Recall $I \subseteq R$ is an ideal (two-sided) if

- I is a subring of R
- $\forall r \in R,\ a \in I,\quad ra,\ ar \in I.$

When I is an ideal of R, write $I \trianglelefteq R$.

For $I \trianglelefteq R$, we get a ring R/I & a natural "projection" / "reduction" hom

$$R \longrightarrow R/I \quad \text{w/ kernel } I.$$

Defn If $A \subseteq R$,

(1) $$(A) = \bigcap_{\substack{I \trianglelefteq R \\ A \subseteq I}} I = \text{smallest ideal of } R \text{ containing } A$$

(2) $$R \cdot A = \Big\{ \sum_{\text{finite}} r_i \cdot a_i \;\Big|\; r_i \in R,\ a_i \in A \Big\}$$

$$A \cdot R = \Big\{ \sum_{\text{finite}} a_i \cdot r_i \;\Big|\; \text{—"—} \Big\}$$

$$R \cdot A \cdot R = \Big\{ \sum_{\text{finite}} r_i' \cdot a_i \cdot r_i \;\Big|\; \text{—"—},\ r_i' \in R \Big\}.$$

<u>Note</u> $RAR = (A)$. If R is comm, $RA = AR = RAR = (A)$.

③ For $a \in R$, write $(a) = (\{a\})$ an call this the <u>principal</u> <u>ideal</u> generated by a.

④ If $|A| < \infty$, $A = \{a_1, \dots, a_n\}$, then

$$(a_1, \dots, a_n) = (A)$$

is a <u>finitely</u> <u>generated</u> <u>ideal</u>,

<u>Note</u>

- $\{\text{ideals of } \mathbb{Z}\} = \{n\mathbb{Z} \mid n \in \mathbb{Z}\}$

  $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ subgp of $(\mathbb{Z}, +)$

  Note that $n\mathbb{Z} = (n) = (-n)$.

  <u>Every</u> ideal in $\mathbb{Z}$ is principal.

- $(2, x) \trianglelefteq \mathbb{Z}[x]$ is not principal:

$$\begin{array}{c} (2,x) \\ \parallel \\ \{f(x) = \sum a_i x^i \in \mathbb{Z}[x] \mid a_0 \text{ is even}\} \end{array}$$

  Suppose for ⨳ that $(2, x) = (a(x))$.

  Then $2 \in (a(x)) \Rightarrow 2 = a(x) \cdot f(x)$ for $f(x)$ some $\in \mathbb{Z}[x]$. $\Rightarrow \deg(a(x)) = 0$.

Thus $a(x) = \pm 1$ or ± 2.

Note that $(1) = (-1) = \mathbb{Z}[x]$

$(2) = (-2) = 2 \cdot \mathbb{Z}[x]$

But $(2, x) \neq \mathbb{Z}[x]$

& x is not a mult of 2, so $(2, x) \neq 2 \cdot \mathbb{Z}[x]$

$\Rightarrow (2, x)$ is <u>not</u> a principal ideal.

<u>Prop</u> $I \trianglelefteq R$. ① $I = R \iff I \cap R^{\times} \neq \emptyset$

② If R is comm, then

R is a field iff $\{\text{ideals of } R\} = \{0, R\}$

<u>Pf</u> ① $\Rightarrow$: If $I = R$, $1 \in I \cap R^{\times} \neq \emptyset$.

$\Leftarrow$: Take $u \in I \cap R^{\times}$ w/ inverse $v \in R$.

Then $\forall r \in R$, $r = r \cdot 1 = r \cdot (\cancel{uv}\ vu)$

$= \underbrace{(r\cancel{u}\ v)}_{\in R}\ \underbrace{\cancel{v}\ u}_{\in I} \in I$

so $I = R$.

② $\Rightarrow$: $R^{\times} = R - \{0\}$ so if $0 \neq I \trianglelefteq R$ then

$\exists$ unit of R in I $\underset{①}{\Rightarrow}$ $I = R$.

$\Leftarrow$: If $0, R$ are all ideals of R, let $u \in R \setminus \{0\}$. Then $(u) = R$ so $1 \in (u)$

$\Rightarrow 1 = u \cdot r$ for some $r \in R$

$\Rightarrow u \in R^\times \Rightarrow R$ is a field. $\square$

<u>Cor</u> If R is a field & S is any ring, then any nontrivial homomorphism

$R \longrightarrow S$ is injective.

<u>Pf</u> The kernel is either 0 or R so the hom is either injective or trivial. $\square$

<u>Defn</u> $m \trianglelefteq R$ is <u>maximal</u> if $m \neq R$ and if

$I \trianglelefteq R$ w/ $m \subseteq I$, then $I = m$ or R.

<u>Prop</u> In a ring w/ 1, every proper ideal is contained in a maximal ideal.

Partially ordered sets:

$(A, \leq)$ is a <u>poset</u> if $\leq$ is a binary relation on the set A which is

- reflexive: $a \leq a \quad \forall a \in A$
- anti-symmetric: $a \leq b \ \& \ b \leq a \Rightarrow b = a$
  $\forall a, b \in A$
- transitive: $\forall a, b, c \in A$, if $a \leq b \ \& \ b \leq c$, then $a \leq c$.

<u>e.g.</u> · B a set, $\mathcal{P}(B) = \{$ subsets of $B \}$

$(\mathcal{P}(B), \subseteq)$ is a poset

· $\mathbb{N} = \{0, 1, 2, \ldots\}$, $(\mathbb{N}, |)$

<u>Defn</u> A <u>chain</u> in a poset $(A, \leq)$ is

$a_1 \leq a_2 \leq a_3 \leq \cdots$

Zorn's Lemma Suppose $(A, \leq)$ is a poset with the property that every chain has an upper bound in A. Then A contains a maximal element.

Pf of Prop R a ring w/ 1, $I \trianglelefteq_{\neq} R$.

$\mathcal{S} = \{ J \trianglelefteq_{\neq} R \mid J \supseteq I \}$ a nonempty poset under inclusion.

$\mathcal{C}$ is a chain in $\mathcal{S}$, define $K = \bigcup_{J \in \mathcal{C}} J$.

check: K is an ideal.

If $K = R$ then $1 \in K \Rightarrow 1 \in J$ for some $J \in \mathcal{C} \Rightarrow J = R$ ⚔

Thus each chain in $\mathcal{S}$ has an upper bd.

By Zorn's lemma, $\mathcal{S}$ has a max'l elt m

$\Leftrightarrow$ $m \trianglelefteq R$ max'l, $I \subseteq m$. $\square$