April15

Thursday, April 15, 2021 12:44 PM

Recall

Defn Let R be a ring. A subring $I \subseteq R$ is called

1) A left ideal if $\forall r \in R$, $i \in I$

   $ri \in I$ $(rI \subseteq I)$

2) A right ideal if $\forall r \in R$, $i \in I$

   $ir \in I$ $(Ir \subseteq I)$

3) An ideal if I is both left & right ideal.

Facts (Last time / HW 11)

1) If $\phi : R \longrightarrow S$ is a ring hom

   $\implies \ker\phi \subseteq R$ is an ideal.

2) If $I \subseteq R$ is an ideal, then the set of cosets R/I is a ring under

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

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

Rmk i) makes R/I into an abelian group b/c $(R,+)$ is an abelian gp & $I \trianglelefteq R$.

ii) Hard part was show mult rule was well defined (equiv. to I an ideal).

Once we have that ring axioms were easy.

Ex (x) = ideal of polynomials whose constant term is 0 $\subseteq \mathbb{Z}[x]$

Showed $\mathbb{Z}[x]/(x) = \mathbb{Z}$.

2) (x^2) = ideal of polynomials whose constant & linear terms are 0. $\subseteq \mathbb{Z}[x]$.

$$f = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots \in (x^3)$$

$$\iff \underline{a_0 = a_1 = 0}$$

$$\iff f = x^2 \cdot g \quad \text{some } g \in \mathbb{Z}[x].$$

pf/ $x^2 g = g_0 x^2 + g_1 x^3 + \dots \in (x^2)$ $\Longleftarrow$

$g = g_0 + g_1 x + \dots$

$$\Longrightarrow a_2 x^2 + a_3 x^3 + \dots = x^2 (a_2 + a_3 x + \dots)$$

So (x^2) = "multiples of x^2"

$f \in \mathbb{Z}[x]$ $\quad g \in (x^2)$ $\quad g = x^2 \cdot h$

$fg = x^2 \cdot fh \in (x^2)$ so ideal!

What is $\mathbb{Z}[x]/(x^2)$??

$$\overline{a_0 + a_1 x + a_2 x^2 + \dots} = \overline{b_0 + b_1 x + b_2 x^2 + \dots}$$

$$\iff a_0 - b_0 + (a_1 - b_1)x + (a_2 - b_2)x^2 + \cdots \in (x^2)$$

$$\iff a = b_0 \ \& \ a_1 = b_1$$

The coset is determined by constant & linear terms.

$$\frac{\mathbb{Z}[x]}{(x^2)} \longleftrightarrow \{\underline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{Z}\}$$

$$\overline{a_0 + a_1 x + a_2 x^2} \longmapsto a_0 + a_1 x$$

Question How do I multiply?

$$\overline{(a_0 + a_1 x)}\,\overline{(b_0 + b_1 x)} = \overline{a_0 b_0 + (a_1 b_0 + a_0 b_1)x + a_1 b_1 x^2}$$

$$= a_0 b_0 + (a_1 b_0 + a_0 b_1)x$$

Slogan

$$\mathbb{Z}[x]/(x^2) \longleftarrow \boxed{\text{Set } x^2 = 0}$$

Observe Get zero divisors & nilpotents.

$$\overline{2x}, \overline{5x} \neq 0. \qquad \overline{2x} \cdot \overline{5x} = \overline{10x^2} = 0 \in \frac{\mathbb{Z}[x]}{(x^2)}$$

Another interesting ideal of $\mathbb{Z}[x]$

$$\mathbb{Z}[x] \xrightarrow{\varepsilon} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z}$$

A surjective homomorphism of rings.

$\ker(\pi \circ \varepsilon) = I = \left(\text{polynomials w/ even const term}\right)$

$$\pi \circ \varepsilon\,(a_0 + a_1x + a_2x^2 + \dots)$$

$$= \pi(a_0)$$

$$= \overline{a_0} \in \mathbb{Z}/2\mathbb{Z}.$$

$= 0 \iff a_0$ is even

First iso theorem

$$\frac{\mathbb{Z}[x]}{\left(\text{polys w/ even const term}\right)} \simeq \mathbb{Z}/2\mathbb{Z}.$$

---

*

$$\mathbb{Z}[x] \xrightarrow{\pi} (\mathbb{Z}/n\mathbb{Z})[x]$$

$$\sum a_i x^i \longmapsto \sum \overline{a_i}\, x^i$$

$\ker \pi$
$= \{n f(x) : f \in \mathbb{Z}[x]\}$

Exercise

If $f : R \longrightarrow S$ a homomorphism of commutative unital rings

$$f[x] : R[x] \longrightarrow S[x]$$

$$\sum a_i x^i \longmapsto \sum f(a_i)\, x^i$$

is a ring hom.

Exercise

$$\begin{tikzcd} \mathbb{Z}[x] \arrow[r, "\varepsilon"] \arrow[d, "\pi"] & \mathbb{Z} \arrow[d, "\pi"] \\ (\mathbb{Z}/2\mathbb{Z})[x] \arrow[r, "\varepsilon"] & \mathbb{Z}/2\mathbb{Z} \end{tikzcd}$$

Check this commutes.

One sided ideals

$$L = \left\{ \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R}).$$

Additive subgroup ✓

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & ax+by \\ 0 & az+bw \end{pmatrix} \in L$$

so L is a left ideal.

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} az & aw \\ bz & bw \end{pmatrix} \notin L$$

$a, b, z \neq 0$ $\notin L$.

Not a right ideal.

No quotient.

Example

X a set. R a ring.

$$\mathrm{Maps}(X,R) = \{ f : X \longrightarrow R \}$$ (Cring HW 10 #6)

Given $x \in X$, define

$$\begin{aligned} \varepsilon_x : \mathrm{Maps}(X,R) &\longrightarrow R \\ f &\longmapsto f(x) \end{aligned}$$

Exercise

This is a surjective homomorphism.

$$\ker(\varepsilon_x) = M_x = \{ f : X \longrightarrow R \ : \ f(x) = 0 \}$$

This is a 2-sided ideal!

First iso thm

$$\frac{\mathrm{Maps}(X,R)}{M_x} \simeq R.$$

Exercise $x \neq y \implies M_x \neq M_y.$ $\leftarrow$

Constructed a function

$$\begin{tikzcd} \left\{\begin{array}{l}\text{Points}\\ x \in X\end{array}\right\} \arrow[r, hook, "\text{injective}"] & \left\{\begin{array}{l}\text{Ideals } I \subseteq \mathrm{Maps}(X,R)\\ \text{s.t. } \underline{\mathrm{Maps}(X,R)/I} \cong R\end{array}\right\} \\ x \arrow[r, mapsto] & M_x \end{tikzcd}$$

?

Maybe something non algebraic

Algebraic!

Upshot

This construction & ones like it build important bridges between mathematic branches.

Isomorphism Theorems for Rings

First iso thm

$\phi : R \longrightarrow S$ a ring homomorphism then $\ker\phi$ is an ideal & $R/\ker\phi \simeq \operatorname{im}\phi$

Second isomorphism Theorem

$A \subseteq R$ a subring
$B \subseteq R$ an ideal

Then $A+B = \{a+b \mid a \in A, b \in B\}$ is a subring of R.

And $A \cap B$ is an ideal. of A

$$\begin{tikzcd}
 & R \arrow[d, dash] & \\
 & A+B \arrow[dl, dash] \arrow[dr, dash] & \\
A \arrow[dr, dash] & & B \arrow[dl, dash] \\
 & A \cap B \arrow[d, dash] & \\
 & 0 &
\end{tikzcd}$$

$$\frac{A+B}{B} \simeq \frac{A}{A \cap B} \longleftarrow$$

Third isomorphism theorem

$I \subseteq J \subseteq R$ $\quad I, J$ ideals.

Then $J/I \subseteq R/I$ is an ideal and

$$\frac{R/I}{J/I} \simeq R/J \longleftarrow$$

Fourth isomorphism theorem.

$I \leq R$ is an ideal.

$$\left\{\begin{matrix}\text{subrings of } R\\ \text{containing } I\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{subrings of}\\ R/I\end{matrix}\right\}$$

$$A \longmapsto A/I$$

is an inclusion preserving bijection &

A is an ideal $\Longleftrightarrow$ A/I is.

Proof

Strategy Know holds on level of groups, Check ring theoretic compatibility.

Second

$A+B$ subring ①

$A \cap B$ ideal of A ②

$$\frac{B}{A\cap B} \longrightarrow \frac{A+B}{B} \quad ③$$

$$a+(A\cap B) \longmapsto a+B$$

is a ring hom. (know bijective group hom).

① $A+B$ is abelian subgroup.

$$(a_1+b_1)\cdot(a_2+b_2) \in A+B$$

$$(a_1+b_1)(a_2+b_2) = \underbrace{a_1a_2}_{\in A} + \underbrace{b_1a_2}_{\substack{\in B \\ \uparrow \\ \text{ideal}}} + \underbrace{a_1b_2}_{\in B} + \underbrace{b_1b_2}_{\in B} \subset A+B.$$

② Know $A \cap B \trianglelefteq A$ by 2nd iso thm.

$b \in A\cap B$, $a \in A$. $\Longrightarrow$ $ab \in A$ ⟵ subring

$ab \in B$ ⟵ ideal

so $ab \in A \cap B$ (same for ba). ✓

③ $\phi : \dfrac{A}{A\cap B} \longrightarrow \dfrac{A+B}{B}$

$$\phi\Big(\big(a+(A\cap B)\big)\big(a'+(A\cap B)\big)\Big) = \phi\big(aa' + (A\cap B)\big)$$
$$= aa' + B \quad ✓$$

$$\phi(a + A\cap B)\,\phi(a' + A\cap B) = (a+B)(a'+B)$$
$$= aa' + B \quad ✓$$

Third & Fourth Exercise.

Operations & Properties of Ideals

$I, J \subseteq R$ are ideals.

→ i) $I + J = \{a+b \mid a\in I,\ b \in J\}$

2) $IJ = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I,\ b_i \in J \right\} \longleftarrow$

3) $I^n = (I^{n-1}) \cdot I$

$$= \left\{ \sum_{i=1}^{t} a_{i1} a_{i2} \cdots a_{in} \mid a_{ij} \in I \right\}.$$

Exercise

1) $I + J$ is the smallest ideal containing I & J.

2) $IJ \subseteq I \cap J \longleftarrow$ an ideal

But $IJ \neq I \cap J$ in general.

Example

$I \subseteq \mathbb{Z}[x]$ ideal of elts w/ even constant term.

$$x^2 + 4 = \underset{I^2}{\underset{\uparrow}{\overset{\downarrow}{(x \cdot x)}}} + \underset{I^2}{\underset{\uparrow}{\overset{\downarrow}{(2 \cdot 2)}}} \in I^2$$

But x^2+4 is irreducible in $\mathbb{Z}[x]$ so can't be a product of 2 elts of I.

Need to include Σ in I^2.

For rest of today, R is a ring with $1 \neq 0$

Study ideals generated by subsets.

Def$^{\underline{n}}$

Let $A \subseteq R$ be a subset

1) (A) = ideal generated by A

= smallest ideal containing A

$$= \bigcap_{\substack{\text{ideals} \\ I \supseteq A}} I$$

Exercise
intersection of ideals is an ideal.

2) $RA = \{r_1 a_1 + \dots + r_n a_n \mid r_i \in R,\ a_i \in A\}$

$AR = \{a_1 r_1 + \dots + a_n r_n \mid a_i \in A,\ r_i \in R\}$

$RAR = \{r_1 a_1 r_1' + \dots + r_n a_n r_n' \mid r_i, r_i' \in R,\ a_i \in A\}$

3) An ideal is principle if it is generated by a single element. ($I = (x)$ $x \in R$)

4) An ideal is finitely generated if it is generated by a finite set.

analogous to a cyclic subgroup.

Lemma $(1 \neq 0)$

$$RAR = (A) \leftarrow$$

Proof

1) Show RAR is an ideal.

i) Subgroup. Clear.

ii) $x = \sum r_i a_i r_i' \in RAR$ $s \in R$

$$sx = \sum \underbrace{s r_i}_{\in R} a_i r_i' \in RAR$$

$\longrightarrow$ $xs = \sum r_i a_i r_i' s \in RAR$ ✓

2) $A \subseteq RAR. \leftarrow$

i) $a \in A.$ $\longrightarrow$ $1 \cdot a \cdot 1 \in RAR.$ ✓

2) $\Rightarrow$ $(A) \subseteq RAR. \leftarrow$

3) $A \subseteq I$ then $RAR \subseteq I$ $\left(\Rightarrow RAR \subseteq \underset{=(A)}{\cap I}\right)$

$\sum r_i a_i r_i' \in RAR.$

$$a_i \in I \xRightarrow{\text{ideal}} r_i a_i \in I \xRightarrow{\text{ideal}} r_i a_i r_i' \in I$$

$$\xRightarrow{\text{subgroup.}} \sum r_i a_i r_i' \in I$$

Exercise: Similar arguments show

i) RA = left ideal generated by A.

ii) AR = right ideal generated by A.

Corollary

If R is commutative $(1 \neq 0)$

Then $(A) = RAR = RA = AR.$

Remarks

1) R is commutative w/ $1 \neq 0$. $a \in R$.

$$(a) = Ra = \left\{ \sum r_i \cdot a \ : \ r_i \in R \right\}$$

$$= \left\{ \left(\sum r_i\right) \cdot a \ : \ r_i \in R \right\}$$

$$= \{ r \cdot a \ : \ r \in R \}$$

$$= \text{"multiples of } a\text{"}$$

2) ⚠ Not true if R not commutative.

$$(a) \neq \{ r a r' \,;\, r, r' \in R \}$$

↑ Not closed under +.

But $Ra = \{ ra \}$

Examples

* $(1) = R$ principle. pf/ $\supseteq$ $1 \in (1)$, $f \cdot 1 = f \in (1)$ $\forall f \in R$ ∅.

$(0) = \{0\} \subseteq R$ principle

* The ideals in $\mathbb{Z}$ are $n\mathbb{Z} = (n)$

pf/ Any ideal is a subgroups.

Any $n\mathbb{Z}$ is an ideal! ∅

All ideals in $\mathbb{Z}$ are principle!

Exercise

$\underline{(n, m) = (g)}$ w/ $g = \gcd(n, m)$

* $(2, x) \in \mathbb{Z}[x]$

$$\| $$

$$\{ 2 \cdot p(x) + x \cdot q(x) \mid p(x), q(x) \in \mathbb{Z}[x] \}$$

$\|$ (I)✓ (UI)

poly's w/ even const term.

Pf/ $2n + xa_1 + x^2a_2 + \cdots$

$= 2n + x(a_1 + xa_2 + \cdots) \in (2, x)$

So $(2, x) = \ker(\mathbb{Z}[x] \longrightarrow \mathbb{Z}/2\mathbb{Z})$

& $\dfrac{\mathbb{Z}[x]}{(2, x)} \simeq \mathbb{Z}/2\mathbb{Z}.$

Fact $(2, x) \subseteq \mathbb{Z}[x]$ not a principle ideal.

Pf/ if $(2, x) = (p(x))$

Then $\exists\ q(x)$ s.t. $p(x)q(x) = 2$.

So $p(x), q(x) = \{\pm 1, \pm 2\}$.

But $p(x) \neq \pm 1$ b/c const term is even.

So $p(x) = \pm 2$.

But $x \notin (\pm 2)$

Bc linear term of $\pm 2h(x)$ always even so x can't be a multiple of ± 2.

↯

So $(2, x)$ no principle