More on ideals

R has $1 \neq 0$

Recall: If $A \subset R$, then $(A) = \bigcap_{\substack{I \subset R \\ \text{ideal} \\ A \subset I}} I$

Define: for fixed sets $A, B \subset R$

$$A \cdot B := \left\{ a_1 b_1 + \_\_ + a_n b_n \;\middle|\; \begin{array}{l} a_1, \_\_, a_n \in A \\ b_1, \_\_, b_n \in B \end{array} \quad n \in \mathbb{N} \right\}$$

<u>Prop</u>: If $A \subset R$ is any subset,

Then ① $R \cdot A$ is the left ideal generated by A

② $A \cdot R$ is the right ideal generated by A

③ $R \cdot A \cdot R$ is the (two-sided) ideal generated by A.

Note: • If $A = \emptyset$, then we say $RA = AR = RAR = \{0\}$

• If R is comm., then $RA = AR = RAR$

<u>Pf</u>: we will only check for the left ideal.

The others are similar.

Subring criterion for $RA \subset R$

① $0 = 0 \cdot a \in RA \implies RA \neq \emptyset$

② Let $x, y \in RA$

$\exists\, r_1, \_\_, r_n \in R,\ a_1, \_\_, a_n \in A$

$r_1', \_\_, r_m' \in R \quad a_1', \_\_, a_m' \in A$

s.t. $x = r_1a_1 + r_2a_2 + \_\_\_ + r_na_n$

$y = r_1'a_1' + r_2'a_2' + \_\_\_ + r_m'a_m'$

- $x - y = (r_1a_1 + \_\_\_ + r_na_n) - (r_1'a_1' + \_\_\_ + r_m'a_m')$

$= r_1a_1 + \_\_\_ + r_na_n + (-r_1')a_1' + \_\_\_ + (-r_m')a_m' \in RA$

- $xy = (r_1a_1 + \_\_\_ + r_na_n)\cdot(r_1'a_1' + \_\_\_ + r_m'a_m')$

$= (r_1a_1 r_1')a_1' + \_\_\_ + (r_1a_1 r_m')a_m' \in RA$.

$+ \dots$

$+ (r_na_nr_1')a_1' + \_\_\_ + (r_na_n r_m')a_m'$

$\Longrightarrow$ RA is a subring.

To see RA is an ideal: Let $r \in R$, $x \in RA$ as above.

$r\cdot x = r\cdot(r_1a_1 + \_\_\_ + r_na_n) = (rr_1)a_1 + \_\_\_ + (rr_n)a_n \in RA$.

Moreover. $A \subset RA$: $(1 \in R \Longrightarrow \forall a \in A,\ 1\cdot a = a \in RA)$

So RA is an ideal containing A

$\Longrightarrow$ $(A) \subset RA$

On the other hand, if I is a left ideal s.t. $A \subset I$

Then $a \in A$, $r \in R$, $\Longrightarrow$ $r\cdot a \in I$

$\Longrightarrow$ For any finite list $r_1, \_, r_n \in R$, $a_1, \_\_\_, a_n \in A$

$r_1a_1, \_\_\_, r_na_n \in I$

$\Longrightarrow$ $r_1a_1 + \_\_\_ + r_na_n \in I \Longrightarrow RA \subset I$ $\square$

Prop: If $I, J \subset R$ are ideals,

Then $I \cdot J$ is an ideal, $I \cdot J \subset I \cap J$

$$\begin{tikzcd}[column sep=small]
 & R \arrow[dl, dash] \arrow[dr, dash] & \\
I \arrow[dr, dash] & & J \arrow[dl, dash] \\
 & I \cap J \arrow[d, dash] & \\
 & IJ &
\end{tikzcd}$$

Note: $I \cdot I = I^2$

$I \cdot I \cdot I = I^3$

$\vdots$

$\underbrace{I \cdot \ldots \cdot I}_{n\text{-times}} = I^n$

Example 1: $2\mathbb{Z}, 3\mathbb{Z} \subset \mathbb{Z}$

- $2\mathbb{Z} \cdot 3\mathbb{Z} = \left\{ \sum_{k=1}^{n} 2 \cdot a_k \cdot 3 b_k \;\middle|\; a_k, b_k \in \mathbb{Z} \right\}$

$$= \left\{ 6 \cdot \left(\sum_{k=1}^{n} a_k \cdot b_k \right) \right\} = 6\mathbb{Z}$$

- $2\mathbb{Z} \cap 3\mathbb{Z} = \{ 2n = 3m \} = 6\mathbb{Z}$

$2 \mid m,\ 3 \mid n$

In this case $2\mathbb{Z} \cdot 3\mathbb{Z} = 2\mathbb{Z} \cap 3\mathbb{Z}$.

Example 2: Consider the ring $R = \mathbb{Z}[x]$

$(x) := \{ p(x) \cdot x \mid p(x) \in R \}$

$(x^2) := \{ q(x) \cdot x^2 \mid q(x) \in R \}$

- $(x) \cdot (x^2) = \{ (p_1(x) \cdot x) \cdot (q_1(x) \cdot x^2) + \_\_\_ + (p_n(x) \cdot x) \cdot (q_n(x) x^2) \}$

$$= \{ (p_1 q_1(x) + \_\_\_ + p_n q_n(x)) \, x^3 \} = (x^3)$$

- $(x) \cap (x^2) = (x^2) \Longrightarrow (x) \cdot (x^2) \subsetneq (x) \cap (x^2)$

Ideals in R and Arithmetic in R

Assume R is comm. ring w/ $1 \neq 0$.

If $a \in R$, then

$$(a) = \{ ra \mid a \in R \} \quad \text{(the "multiples" of } a\text{)}$$

e.g. $2\mathbb{Z} = \{ 2n \mid n \in \mathbb{Z} \} = (2)$

<u>Note</u>: we sometimes write

$$(a) = R \cdot a = a \cdot R$$

we also say that if $b \in (a)$, that a <u>divides</u> b, i.e. $a \mid b$

<u>Obs</u>: $b \in (a)$ iff $(b) \subset (a)$.

$\ulcorner$ $b \in (a) \implies \exists\, r \in R$ s.t. $b = r \cdot a$.

$\implies c \in (b)$, $\exists\, s \in R$ s.t. $c = s \cdot b = s \cdot (ra) = (s \cdot r) \cdot a \in (a)$

$\implies (b) \subset (a)$

On other hand, if $(b) \subset (a)$, then $b \in (b) \subset (a)$ $\lrcorner$

<u>Defn</u>: Let R be a comm. ring.

An ideal $P \neq R$ is called a <u>prime ideal</u> if

$\forall\, a, b \in R$ s.t. $a \cdot b \in P$

Then either $a \in P$ or $b \in P$

Example: $2\mathbb{Z}$ is prime.

$6\mathbb{Z}$ is not. e.g. $2 \cdot 3 = 6 \in 6\mathbb{Z}$

$2, 3 \notin 6\mathbb{Z}$

$(x) \subset \mathbb{R}[x]$ is prime

(x^2) is not, e.g. $x \cdot x = x^2 \in (x^2)$

$x \notin (x^2)$

Obs: $\{0\} \subset \mathbb{Z}$ is prime.

i.e. if $a \cdot b = 0$, $a, b \in \mathbb{Z}$
then either $a = 0$ or $b = 0$.] Integral

Prop: R is an integral domain iff $\{0\}$ is prime.

Thm: Assume R is comm.

An ideal $P \subset R$ is prime iff R/P is an integral domain.

Pf: Suppose P prime, $\bar{a}, \bar{b} \in R/P$

s.t. $\bar{a} \cdot \bar{b} = \bar{0}$

we want $\bar{a} = \bar{0}$ or $\bar{b} = 0$.

Pick rep's $a \in \bar{a}$, $b \in \bar{b}$, $\Longrightarrow \overline{a \cdot b} = \bar{0}$, i.e. $a \cdot b \in P$

But P prime, either $a \in P$ or $b \in P$, i.e. $\bar{a} = \bar{0}$, $\bar{b} = \bar{0}$

If R/P is integral, $a \cdot b \in P$

Then $\overline{a \cdot b} = \bar{0} \Longrightarrow \bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$ b/c R/P is integral

$\Longrightarrow a \in P$ or $b \in P$ $\square$