Lecture 6

More on Ideals

Let R be a ring with $1 \neq 0$.
Recall that if $A \subset R$, then

$$(A) = \bigcap_{\substack{I \subset R \text{ ideals} \\ A \subset I}} I$$

Definition 6.1

For fixed sets $A, B \subset R$, we define **ring multiplication** as

$$A \cdot B \coloneqq \{a_1 b_1 + \cdots + a_n b_n \mid a_1, \ldots, a_n \in A,\ b_1, \ldots, b_n \in B,\ n \in \mathbb{N}\}$$

Proposition 6.1

If $A \subset R$ is any subset, then:

(i) $R \cdot A$ is the left ideal generated by A
(ii) $A \cdot R$ is the right ideal generated by A
(iii) $R \cdot A \cdot R$ is the (two-sided) ideal generated by A

Note: If

- $A = \emptyset$, then we say $RA = AR = RAR = \{0\}$
- R is commutative, then $RA = AR = RAR$.

Proof. We will only check for the left ideal, the others follow similarly.
First the subring criterion for $RA \subset R$
(i) $0 = 0 \cdot a \in RA \implies RA \neq \emptyset$
(ii) Let $x, y \in RA$, then there exist

$$\begin{gathered} r_1, \ldots r_n \in R,\ a_1, \ldots, a_n \in A \\ r'_1, \ldots r'_m \in R,\ a'_1, \ldots, a'_m \in A \end{gathered}$$

such that

$$\begin{aligned} x &= r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \\ y &= r'_1 a'_1 + r'_2 a'_2 + \cdots + r'_m + a'_m \end{aligned}$$

then

$$\begin{aligned} x - y &= (r_1 a_2 + \cdots + r_n a_n) - (r'_1 a'_1 + \cdots + r'_m a'_m) \\ &= r_1 a_1 + \cdots + r_n a_n + (-r'_1) a'_1 + \cdots + (-r'_m) a'_m \in RA \end{aligned}$$

and

$$\begin{aligned} xy &= (r_1 a_2 + \cdots + r_n a_n) \cdot (r'_1 a'_1 + \cdots + r'_m a'_m) \\ &= (r_1 a_1 r'_1) a'_1 + \cdots + (r_1 a_1 r'_m) a'_m \\ &+ \vdots \\ &+ (r_n a_n r'_1) a'_1 + \cdots + (r_n a_n r'_m) a'_m \in RA \end{aligned}$$

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

$$r \cdot x = r \cdot (r_1 a_2 + \cdots + r_n a_n) = (rr_1)a_1 + \cdots + (rr_n)a_n \in RA$$

Moreover

$$A \subset RA \quad (1 \in R \implies \forall a \in A,\, 1 \cdot a = a \in RA)$$

So RA is an ideal containing A i.e

$$(A) \subset RA$$

On the other hand, if I is a left ideal such that $A \subset I$, then $a \in A, r \in R \implies r \cdot a \in I$ which implies for any finite list $r_1, \ldots, r_n \in R$, $a_1, \ldots, a_n \in A$

$$r_1 a_1, \ldots, r_n a_n \in I \implies r_1 a_1 + \cdots + r_n a_n \in I \implies RA \subset I$$

and since (A) is a left ideal, we have

$$RA = (A)$$

and specifically this is the smallest ideal needed to contain A. ■

Proposition 6.2

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: $I \cdot I = I^2, \ldots, \underbrace{I \cdot I \cdot \ldots \cdot I}_{n-\text{times}} = I^n$

Example 6.1 Consider $2\mathbb{Z}, 3\mathbb{Z} \subset Z$, then

$$2\mathbb{Z} \cdot 3\mathbb{Z} = \left\{ \sum_{k=1}^{n} 2a_k \cdot 3b_k \,\middle|\, a_k, b_k \in Z \right\} = \left\{ 6 \left(\sum_{k=1}^{n} a_k \cdot b_k \right) \,\middle|\, a_k, b_k \in Z \right\} = 6\mathbb{Z}$$

and

$$2\mathbb{Z} \cap 3\mathbb{Z} = \{\underbrace{2n = 3m}_{2|m, 3|n}\} = 6\mathbb{Z}$$

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

Example 6.2 Consider the ring $R = \mathbb{Z}[x]$ with

$$(x) \coloneqq \{p(x) \cdot x \mid p(x) \in R\}$$
$$(x^2) \coloneqq \{q(x) \cdot x^2 \mid q(x) \in R\}$$

Then

$$\begin{aligned}(x) \cdot (x^2) &= \{(p_1(x) \cdot x) \cdot (q_1(x) \cdot x^2) + \cdots + (p_n(x) \cdot x) \cdot (q_n(x) \cdot x^2)\} \\ &= \{(p_1 \cdot q_1(x) + \cdots + p_n \cdot q_n(x)) \cdot x^3\} = (x^3)\end{aligned}$$

On the other hand, since multiples of x^2 are also multiples of x, we get

$$(x) \cap (x^2) = (x^2)$$

and so

$$(x) \cdot (x^2) = (x^3) \subsetneq (x) \cap (x^2) = (x^2)$$

Since a multiple of x^3 is a multiple of x^2 but there is no multiple of x^3 which is equal to ax^2 for nonzero $a \in R$.

Ideals in R and Arithmetic in R

Assume R is a commutative ring w/ $1 \neq 0$.
If $a \in R$, then

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

e.g. $2\mathbb{Z} = \{2n \mid n \in Z\} = (2)$
Note: We sometimes write

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

We also say that if $b \in (a)$, that a **divides** b, i.e $a \mid b$.

Claim: $b \in (a)$ *iff* $(b) \subset (a)$

Proof. Let $b \in (a)$ then there exists $r \in R$ such that $b = r \cdot a$. In particular,

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

On the other hand, if $(b) \subset (a)$, then $b \in (b) \subset (a)$. ∎

Definition 6.2

Let R be a commutative ring.
An ideal $P \neq R$ is called a **prime ideal** if for all $a, b \in R$ such that $a \cdot b \in P$, then either $a \in P$ or $b \in P$.

Example 6.3

- $2\mathbb{Z}$ is prime
- $6\mathbb{Z}$ is **not** prime e.g $2 \cdot 3 = 6 \in 6\mathbb{Z}$ but $2, 3 \notin 6\mathbb{Z}$
- $\{0\} \subset \mathbb{Z}$ is prime. If $a \cdot b = 0, a, b \in \mathbb{Z}$ then either $a = 0$ or $b = 0$ (integral domain).
- $(x) \subset \mathbb{R}[x]$ is prime
- (x^2) is **not**, e.g. $x \cdot x = x^2 \in (x^2)$ but $x \notin (x^2)$.

Proposition 6.3

R is an integral domain *iff* $\{0\}$ is prime

Theorem 6.1

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

Proof.
$\Rightarrow$
Suppose P is prime and $\overline{a}, \overline{b} \in R/P$ such that $\overline{a} \cdot \overline{b} = \overline{0}$.
We want $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.
Pick representatives $a \in \overline{a}, b \in \overline{b}$. This implies $\overline{a \cdot b} = \overline{0}$, i.e $a \cdot b \in P$.
But P is prime, so either $a \in P$ or $b \in P$, i.e $\overline{a} = \overline{0}, \overline{b} = \overline{0}$.
$\Leftarrow$
If R/P is integral and $a \cdot b \in P$, then

$$\overline{a \cdot b} = \overline{0} \implies \underbrace{\overline{a} = \overline{0} \text{ or } \overline{b} = \overline{0}}_{R/P \text{ integral}} \implies a \in P \text{ or } b \in P$$

∎