Previously.

- Domains
- Integral Domains
- Fields

This Section.

- Ideals
- Principal Ideals
- Prime Ideals
- Maximal Ideals

Recall. Consider the ring $(R, +, \cdot)$. Recall that $(R, +)$ is an abelian group. So any subgroup $S \leq R$ is automatically normal. In particular, we can construct R/S, the set of cosets of S in R as a group.

Example. The ring $R = \mathbb{Z}[i]$ is a group under addition and it has the subroup

$$S = \{ai \ : \ a \in \mathbb{Z}\} = i\mathbb{Z}.$$

The cosets of S are of the form $r + S = r + i\mathbb{Z}$ where $r \in R$.
Some cosets are

$$\begin{aligned} 2 + S &= \{2 + ai \ : \ a \in \mathbb{Z}\} \\ (5 - i) + S &= \{5 - i + ai \ : \ a \in \mathbb{Z}\} = \{5 + bi \ : \ b \in \mathbb{Z}\} \end{aligned}$$

On question we might ask is "Is R/S a ring?"

Exercise 1. Take the $R = \mathbb{Z}[i]$ and $S = i\mathbb{Z}$ as in the example above. Let's try multiplying cosets.

(a) (Elements) Try the following. Take generic elements $ai, bi \in S = \mathbb{Z}i$ and compute

$$(2 + ai)((5 - i) + bi).$$

(b) (Sets) What would we expect for the product

$$(2 + S)((5 - i) + S)?$$

(c) (Verification) Is the value you computed for the first part of this exercise in this expected set?

Lemma. $(S,+) \leq (R,+)$, then

$$(a+S)(b+S) = (ab)+S$$

is well-defined if and only if

$$rS \subseteq S \quad \text{and} \quad Sr \subseteq S, \quad \text{for all } r \in R.$$

Exercise 2. Do some FOILing of $(a+S)(b+S)$ and see how this relates to the containment of $rS \subseteq S$ and $Sr \subseteq S$.

Definition. Let $(R,+,\cdot)$ be a ring. An additive subgroup $(I,+)$ of $(R,+)$ is an `ideal of` R if $rI \subseteq I$ and $Ir \subseteq I$ for all $r \in R$.

Exercise 3. Verify that $i\mathbb{Z}$ is an ideal of $\mathbb{Z}[i]$.

Definition. Equivalent definitions of an `ideal` I of a ring R: (given $(I,+) \leq (R,+)$)

- for all $i \in I$, $iR \subseteq I$ and $Ri \subseteq I$
- for all $i \in I$ and $r \in R$, $ir \in I$ and $ri \in I$.

Note. Some may call this a "two-sided ideal". By considering just one of the containments, we could also define "left ideals" and "right ideals". In a commutative ring, every ideal is two-sided. WHY??

Warning. Not all subgroups are ideals, as we will see in the following exercise!

Exercise 4. Show that $\mathbb{Z}$ is not an ideal of the ring $\mathbb{Q}$.

Theorem 3.3.1. Let I be an ideal of the ring R (with unity). Then the additive group $(R/I, +)$ becomes a ring with multiplication $(r + I)(s + I) = rs + I$ called the `factor ring` or `quotient ring`. The unity of R/I is $1 + I$ and if R is commutative, then R/I is commutative.

Observations. Let R be a ring (with unity)

1. $\{0\}$ and R are ideals of R.

2. $R/R \cong \{0\}$ and $R/\{0\} \cong R$

3. Everything from quotient groups extends to quotient rings

(a) $r + I = s + I$ if and only if $r - s \in I$
(b) $(r + I) + (s + I) = (r + s) + I$
(c) $0 + I = I$
(d) $-(r + I) = -r + I$
(e) $k(r + I) = kr + I$ for all $k \in \mathbb{Z}$

Theorem 3.3.2. If I is an ideal of the ring R (that has unity), then the following are equivalent

1. $1 \in I$

2. I contains a unit

3. $I = R$

Principal Ideals

Given a fixed element a in a ring R, we can get an ideal easily by taking all of the multiples of that element.

$$Ra = \{ra \mid r \in R\}$$
$$aR = \{ar \mid r \in R\}$$

Definition. If $a \in Z(R)$, then $Ra = aR$ and we call this set the `principal ideal of` R `generated by` a. Denote this set by (a).

Exercise 5. Show that if $a \in Z(R)$, then $Ra = aR$ is an ideal of R by showing that (1) Ra is a subgroup of R under addition and (2) for all $r \in R$, we have $r(Ra) \subseteq Ra$ and $(Ra)r \subseteq Ra$.

Warning. The book uses $\langle a \rangle$ for the ideal generated by a. To avoid mixing it up with cyclic groups, we'll use (a) in these notes.

Exercise 6. Is the set of multiples of 6 a principal ideal of $\mathbb{Z}$?

Exercise 7. Consider $R = \mathbb{Z}[i]$ and $I = (2+i)$. Follow the listed steps to show that

$$R/I = \{0 + I, 1 + I, 2 + I, 3 + I, 4 + I\}.$$

(a) Show that $5 \in I$ by writing $5 = r(2 + i)$ for some $r \in \mathbb{Z}[i]$.

(b) Show that if $n \in \mathbb{Z}$, then $n + I$ is the same as one of $0 + I, 1 + I, 2 + I, 3 + I, 4 + I$.

(c) Show that $i + I = -2 + I$. (Hint: Observation 3a on page 3 of the packet.)

(d) Show that if $a + bi \in \mathbb{Z}[i]$ then $(a + bi) + I = (a - 2b) + I$.

(e) Conclude that every coset of I in $Z[i]$ is equal to one of $0 + I, 1 + I, 2 + I, 3 + I, 4 + I$.

(f) (Challenge) Show that if $0 \leq m < n \leq 4$, then $m + I \neq n + I$.

Note. There are many examples of ideals that are not principal. One example of this is the ideal
$$(2, 1+\sqrt{-5}) = \{r(2) + s(1+\sqrt{-5}) \mid r, s \in \mathbb{Z}[\sqrt{-5}]\}$$
of $\mathbb{Z}[\sqrt{-5}]$. See: https://math.stackexchange.com/questions/543216/proving-that-a-ring-is-not-a-principal-ideal-domain

Definition. We call a proper ideal P of a ring R `prime` if
$$rs \in P \quad \Rightarrow \quad r \in P \text{ or } s \in P.$$

Example. Let $R = \mathbb{Z}$, what ideals are prime? (This is a thought exercise, and the answer is what you expect, but why??)

Theorem 3.3.3. If R is a commutative ring, an ideal $P \neq R$ of R is a prime ideal if and only if R/P is an integral domain.

Theorem 3.3.4. Let I be an ideal of the ring R. There is a correspondence
$$\left\{ \begin{array}{c} \text{ideals of } R \\ \text{containing } I \end{array} \right\} \leftrightarrow \{\text{ideals of } R/I\}.$$

Moreover, this correspondence respects containment.

Definition. Let R be a ring (not necessarily commutative), and let M be an ideal of R. We call M a `maximal ideal` of R if

1. $M \neq R$, and
2. if I is an ideal of R satisfying $M \subseteq I \subseteq R$, then $I = M$ or $I = R$.

Exercise 8. Is $5\mathbb{Z}$ maximal in $\mathbb{Z}$?

Is $6\mathbb{Z}$ maximal in $\mathbb{Z}$?

Definition. A ring R is a `simple ring` if $R \neq \{0\}$ and the only ideals of R are $\{0\}$ and R.

Example. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$

Example. A less trivial example, $M_2(\mathbb{R})$, or any matrix ring over a field.

Theorem 3.3.5. If R is a commutative ring with identity, then R is simple if and only if it is a field.

Theorem 3.3.6. Let M be an ideal of a ring R. Then M is maximal if and only if R/A is simple.

Corollary 1. Let R be a commutative ring, with unity. Let M be an ideal of R. Then M is maximal if and only if R/M is a field.

Corollary 2. Let R be a commutative ring, with unity. If M is a maximal ideal of R, then M is a prime ideal.

Exercise 9. Show that the converse of the second corollary is false:
Let $R = \mathbb{Z} \times \mathbb{Z}$ and $I = \{(a, 0) \mid a \in \mathbb{Z}\}$.

1. Verify I is an ideal of R.

2. Verify that I is a prime ideal.

3. Let $J = \{(a, 2b) \mid a, b \in \mathbb{Z}\}$. Show that J is also an ideal of R and $I \subset J \subset R$ with $I \neq J \neq R$. Thus showing I is not maximal.

These will be important in Math 426.

Lemma 3.3.3. Let R be a ring with unity and $n \geq 1$. Every ideal of $M_n(R)$ has the form $M_n(A)$ for some ideal A of R.

Theorem 3.3.7. If R is a ring with unity then $M_n(R)$ is simple if and only if R is simple.

Corollary. If R is a division ring then $M_n(R)$ is simple.

Note. This last one is HUGE in my research!