Sections 7.3, Homomorphisms, Quotients, Ideals

Recall An ideal \( I \subseteq R \) is a subring for which \( rI \subseteq I \) and \( Ir \subseteq I \).

**Left ideal** \( I \subseteq R \) if \( rI \subseteq I \).

**Right ideal** \( I \subseteq R \) if \( Ir \subseteq I \).

Given an ideal \( I \subseteq R \), \( R/I = \{ r+I \mid r \in R \} \) is a ring with operations \((r+I) + (s+I) = (r+s)+I\), \((r+I)(s+I) = rs+I\). Addition identity is \( I \).

**Theorem 7 (First Isomorphism Theorem for Rings)**

Suppose \( \varphi : R \to S \) is a ring homomorphism. Then:

1. \( \ker \varphi \) is an ideal in \( R \), and \( R/\ker \varphi \cong \varphi(R) \subseteq S \).
2. \( \varphi = \theta \circ \pi \) in following diagram, and \( \theta \) is an isomorphism.

\[
\begin{array}{ccc}
R & \xrightarrow{\varphi} & \varphi(R) \subseteq S \\
\downarrow{\pi} & & \downarrow{\theta} \\
R/\ker \varphi & \xrightarrow{\cong} & \varphi(R) \\
\end{array}
\]

Also, if \( I \subseteq R \) is any ideal, then \( I + \ker \varphi \) is the kernel of the homomorphism \( \pi : R \to R/I \), \( \pi(r) = r+I \).

**Example** \( \varphi : \mathbb{R}[x] \to \mathbb{R} \) by \( \varphi(f) = f(0) \) (eval. hom.)

\( \ker \varphi = \{ \alpha_0 + \alpha_1x + \cdots + \alpha_nx^n \mid \alpha_i \in \mathbb{R}, n \geq 1 \} \)

\( \mathbb{R}[x]/\ker \varphi \cong \mathbb{R} \).

In this example, the kernel takes up "almost all" of \( \mathbb{R}[x] \). In fact there is no larger proper ideal \( I \subseteq \mathbb{R}[x] \) with \( \ker \varphi \subseteq I \subseteq \mathbb{R}[x] \).

**Definition** An ideal \( M \subseteq R \) is **maximal** if there is no ideal \( I \) with \( M \subseteq I \subseteq R \).

**Proposition 11** In a ring with 1, every ideal is contained in some maximal ideal.

**Proposition 12** Suppose \( R \) commutative. Then \( M \) maximal \( \iff \) \( R/M \) is a field.

**Not** \( M \) not maximal

\( \iff \exists M \subseteq I \subseteq R \)

\( \iff \exists a \in M-M \)

\( \iff (a+I)(r+I) = 0+I \iff I = 1+I \)
Definition: An ideal \( P \) in a commutative ring \( R \) is prime if for all \( a, b \in R \), \( ab \in P \Rightarrow a \in P \) or \( b \in P \).

If \( p \in \mathbb{Z} \) is prime, then \( \{ n \in \mathbb{Z} : \exists \, k \in \mathbb{Z}, nk = p \} \) is a principal ideal generated by \( p \).

Example: \( 8 \notin \mathbb{Z} \) is not prime in \( \mathbb{Z} \). However, \( 3 \), \( 4 \notin \mathbb{Z} \), \( 3 \cdot 4 = 12 \notin \mathbb{Z} \).

\[ 5\mathbb{Z} \] is prime in \( \mathbb{Z} \). If \( ab \in 5\mathbb{Z} \) then one of \( a, b \) is a multiple of \( 5 \).

Proposition 13: Suppose \( R \) is commutative. Then \( p \) is a prime ideal in \( R \) if and only if \( R/p \) is an integral domain.

By previous two propositions, every maximal ideal is prime.

In \( p \in \mathbb{Z} \) is a maximal \( \Rightarrow \mathbb{Z}/p \) is a field \( \Rightarrow \mathbb{Z}/p \) is an integral domain.

By previous two propositions, every maximal ideal is prime.

Not every prime ideal is maximal:

Example: \( 2\mathbb{Z} \) is prime because \( \mathbb{Z}/P \) is an integral domain.

It is not maximal, as follows:

\( \mathbb{Z}/P \subset \{ 2a + a_{1}x + a_{2}x^{2} + \ldots + a_{n}x^{n} | a_{i} \in \mathbb{Z} \} \subset \mathbb{Z} \).

Definition: If \( a \in R \), the principal ideal generated by \( a \) is

\[ (a) = \{ \sum x_{i}a_{i} \mid x_{i} \in \mathbb{Z}, a_{i} \in R \} \subset \mathbb{Z} \]

This is the smallest ideal containing \( a \). If \( R \) is commutative,

\[ (a) = \{ ra \mid r \in R \} \subset \mathbb{Z} \]

Example: \( 5 \in \mathbb{Z} \), \( (5) = 5\mathbb{Z} \), \( x \in (5) \iff 5 | x \).

\( a \in R \), \( x \in (a) \iff a | x \).

Principal ideals are key instruments in describing "arithmetic" in rings.

\[ \mathbb{Z}/(x) = \{ 0 + a_{1}x + a_{2}x^{2} + \ldots + a_{n}x^{n} \mid a_{i} \in \mathbb{Z} \} \subset R[x] \]

\((x) = \{ 0 \} \subset R[x] \), \( R[x]/(x) \to R \), \( f(x) \to f(0) \).
Ideals Generated by Sets

Definition: If $A \subseteq R$, then the ideal generated by $A$ is

$$(A) = \bigcap_{A \subseteq \mathbb{R}} I = \left\{ \sum_{i=1}^{k} r_i a_i s_i \mid r_i \in \mathbb{Z}^+, a_i \in A, r_i s_i \in R \right\}$$

This is the smallest ideal containing $A$. If $R$ is commutative, then

$$(A) = \bigcap_{A \subseteq \mathbb{R}} I = \left\{ \sum_{i=1}^{k} r_i a_i \mid a_i \in A, r_i \in R \right\}$$