3.2 Ideals

Ideals to the rings are as normal subgroups to the groups.

**Def.** Let \((R, +, \cdot)\) be a ring.

- \(S\) is a **subring** of \(R\), denoted \(S \subseteq R\), if \(S \subseteq R\) and \((S, +, \cdot)\) is a ring.

- A subring \(I\) is a **left ideal** [resp. **right ideal**] of \(R\) if \(r \in R\) and \(x \in I\) implies that \(rx \in I\) [resp. \(xr \in I\)].

- A subring \(I\) is an **ideal** of \(R\), denoted \(I \trianglelefteq R\), if it is both a left and right ideal.

- An ideal \(I\) is **proper** if \(I \neq 0\) and \(I \neq R\).

If \(R\) has unity \(1_R\), then a nonzero ideal is proper iff it contains no units of \(R\).

**Ex.** The **center** of a ring \(R\) is \(C = \{c \in R \mid cr = rc\text{ for all }r \in R\}\). It is a subring but not necessarily an ideal.

**Thm 3.5.** A nonempty subset \(I\) of a ring \(R\) is an ideal iff for all \(a, b \in I\) and \(r \in R\):

1. \(a, b \in I\) implies that \(a - b \in I\); and
2. \(a \in I, r \in R\) implies that \(ar, ra \in I\).

**Cor 3.6.** If \(\{A_i \mid i \in I\}\) is a family of ideals of \(R\), then \(\bigcap_{i \in I} A_i\) is an ideal of \(R\).

**Def.**

- Let \(X \subseteq R\). Let \(\{A_i \mid i \in I\}\) be the family of ideals that contain \(X\). Then \((X) := \bigcap_{i \in I} A_i\) is called the **ideal** generated by \(X\). The elements of \(X\) are called the **generators** of the ideal \((X)\).

- If an ideal \(I = (X)\) where \(|X|\) is finite, then \(I\) is **finitely generated**.

- An ideal \((x)\) generated by an element is a **principal ideal**.

- A **principal ideal ring** (PIR) is a ring in which every ideal is principal.

- A **principal ideal domain** (PID) is a domain as well as a PIR.

**Thm 3.7.** Let \(R\) be a ring, \(a \in R\), and \(X \subseteq R\).

- The **principal ideal**

  \[
  (a) = \left\{ ra + as + na + \sum_{i=1}^{m} r_isi \mid r, s, r_i, s_i \in R, \ n \in \mathbb{Z}, \ m \in \mathbb{N}^* \right\}.
  \]
3.2. IDEALS

1. If $R$ has unity, then $(a) = \{ \sum_{i=1}^{m} r_i a_i s_i \mid r_i, s_i \in R, \ m \in \mathbb{N}^* \}.$
2. If $a$ is in the center of $R$, then $(a) = \{ ra + na \mid r \in R, \ n \in \mathbb{Z} \}.$

- $Ra = \{ ra \mid r \in R \}$ is a left ideal of $R$. If $R$ has unity, then $a \in Ra$.
- If $R$ has unity and $X$ is in the center of $R$, then $(X) = \{ \sum_{i=1}^{m} r_i a_i \mid n \in \mathbb{N}^*, \ r_i, a_i \in X \}.$

Thm 3.8. Let $A, B, C, A_1, \cdots, A_n$ be [left] ideals of a ring $R$.

1. $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are [left] ideals.
2. $(A + B) + C = A + (B + C)$.
3. $(AB)C = ABC = A(BC)$.
4. $B(\sum_{i=1}^{n} A_i) = \sum_{i=1}^{n} BA_i$ and $(\sum_{i=1}^{n} A_i)C = \sum_{i=1}^{n} A_i C$.

When $I$ is a subring of $R$, the set

$$R/I = \{ a + I \mid a \in I \}$$

is a well defined additive group. To make it a ring, we must have

$$(a + I)(b + I) = ab + aI + Ib + I = ab + I.$$

That is, $aI, Ib \subseteq I$. Therefore, $I$ must be an ideal of $R$. It shows that ideals to rings are like normal subgroups to groups.

Thm 3.9. Let $R$ be a ring and $I \subseteq R$. Then $R/I$ is a ring with the multiplication $(a+I)(b+I) = ab + I$. If $R$ is commutative or has an unity, then the same is true of $R/I$.

Thm 3.10. Let $f : R \to S$ be a ring homomorphism. Then $\text{Ker} f \subseteq R$ and $\text{Im} f \subseteq S$. Conversely, for any ideal $I \subseteq R$, there is the canonical projection $\pi : R \to R/I$, defined by $a \mapsto a + I$, such that $\text{Ker} \pi = I$.

Thm 3.11.

1. (First Isomorphism Theorem) Every ring homomorphism $f : R \to S$ induces a ring isomorphism

$$R/\text{Ker} f \simeq \text{Im} f$$

by $a + \text{Ker} f \mapsto f(a)$. 
2. (Second Isomorphism Theorem) If \( I, J \subseteq R \), then
\[
I/(I \cap J) \simeq (I + J)/J.
\]

3. (Third Isomorphism Theorem) If \( I, J \subseteq R \) and \( I \subseteq J \), then \( J/I \trianglelefteq R/I \) and
\[
(R/I)/(J/I) \simeq R/J.
\]

**Remark.** There is a one-to-one correspondence between the set of all ideals of \( R \) which contain \( I \) and the set of all ideals of \( R/I \), given by \( J \mapsto J/I \).

**Def.** An ideal \( P \) of a ring \( R \) is **prime** if \( P \neq R \) and for any \( A, B \subseteq R \):
\[
AB \subseteq P \quad \Rightarrow \quad A \subseteq P \quad \text{or} \quad B \subseteq P.
\]

**Thm 3.12.** Suppose \( P \subseteq R \) and \( P \neq R \). If for all \( a, b \in R \),
\[
ab \in P \quad \Rightarrow \quad a \in P \quad \text{or} \quad b \in P,
\]
then \( P \) is prime. Conversely, if \( R \) is commutative with unity and \( P \) is prime, then (3.1) holds.

**Proof.** Suppose \( ab \in P \) implies that \( a \in P \) or \( b \in P \). Given \( A, B \subseteq R \) with \( AB \subseteq P \), if \( A \not\subseteq P \), then there is \( a \in A \setminus P \). Then \( ab \in P \) for all \( b \in B \), which implies that \( b \in P \). So \( B \subseteq P \). Thus \( P \) is prime.

Conversely, if \( R \) is commutative with unity and \( P \) is prime, then \( (a) = aR \) and for \( a, b \in R \) with \( ab \in P \), \( (a)(b) = (ab) \subseteq P \) so that \( (a) \subseteq P \) or \( (b) \subseteq P \), that is, \( a \in P \) or \( b \in P \). \( \Box \)

**Thm 3.13.** Suppose \( R \) is a commutative ring with unity \( 1_R \neq 0 \). Then an ideal \( P \) is prime iff \( R/P \) is an integral domain.

**Proof.** Let \( P \triangleleft R \). Then \( R/P \) is a commutative ring with unity.

Suppose that \( P \) is prime in \( R \). Then \( (a + P)(b + P) = P \) iff \( ab \in P \), iff \( a \in P \) or \( b \in P \), iff \( a + P = P \) or \( b + P = P \). So \( R/P \) is an integral domain.

Conversely, suppose that \( R/P \) is an integral domain. Then \( ab \in P \) iff \( (a + P)(b + P) = P \), iff \( a + P = P \) or \( b + P = P \), iff \( a \in P \) or \( b \in P \). So \( P \) is prime. \( \Box \)

**Def.** An \([left]\) ideal \( M \) in a ring \( R \) is said to be **maximal** if \( M \neq R \) and there is no proper \([left]\) ideal containing \( M \).
3.2. IDEALS


Proof. Use Zorn’s Lemma.

Thm 3.15. Let \( R \) be a ring with unity, and \( M \subseteq R \).

1. If \( R \) is commutative and \( M \) is maximal, then \( R/M \) is a field.

2. If \( R/M \) is a division ring, then \( M \) is maximal.

Proof.

1. Suppose \( R \) is commutative with unity and \( M \) is maximal. Then \( R/M \) is commutative with unity. For any \( a \in R\setminus M \), if \( a + M \) is not a unit in \( R/M \), then \( (a + M) = \{ b + M \mid b \in (a) \} \) is a proper ideal of \( R/M \), whence \( (a) + M \) is a proper ideal of \( R \) that contains \( M \), a contradiction to the maximality of \( M \). Therefore \( R/M \) is a field.

2. If \( R/M \) is a division ring, then it contains no nonzero proper ideal. Hence there is no proper ideal of \( R \) that strictly contains \( M \). So \( M \) is maximal.

Cor 3.16. If \( R \) is a commutative ring with unity, then every maximal ideal \( M \) is prime.

Proof. If \( M \) is maximal, then \( R/M \) is a field, which is a domain. So \( M \) is prime.

Remark. The converse is false. e.g. \((0)\) is prime in \( \mathbb{Z} \), but \((0)\) is not maximal.

Cor 3.17. A commutative ring \( R \) with unity is a field iff \((0)\) is a maximal ideal.

Let \( \{ A_i \mid i \in I \} \) be a family of rings. The external/internal direct product \( \prod_{i \in I} A_i \) in additive group category becomes a ring with the induced addition and multiplication, which is the external/internal direct product of \( \{ A_i \mid i \in I \} \) in ring category.

Def. Let \( A \subseteq R \) and \( a,b \in R \). Then \( a \) is said to congruent to \( b \) modulo \( A \), denoted \( a \equiv b \pmod{A} \), if \( a - b \in A \) or \( a + A = b + A \).

Lem 3.18. If \( a_1 \equiv a_2 \pmod{A} \) and \( b_1 \equiv b_2 \pmod{A} \), then

\[ a_1 + b_1 \equiv a_2 + b_2 \pmod{A}, \quad a_1b_1 \equiv a_2b_2 \pmod{A}. \]

Thm 3.19 (Chinese Remainder Theorem). Let \( R \) be a ring with unity. Let \( A_1, \ldots, A_n \) be ideals of \( R \) such that \( A_i + A_j = R \) for all \( i \neq j \). Then for any \( b_1, \ldots, b_n \in R \), there exists \( b \in R \) such that

\[ b \equiv b_i \pmod{A_i} \quad (i = 1, 2, \cdots, n). \]

Furthermore \( b \) is uniquely determined up to congruence modulo the ideal \( A_1 \cap A_2 \cap \cdots \cap A_n \).
Chapter 3. Rings

Proof. We have \( R = A_1 + A_2 \). Assume inductively that
\[
R = A_1 + (A_2 \cap \cdots \cap A_{k-1}).
\]
Then
\[
R = R^2 = (A_1 + (A_2 \cap \cdots \cap A_{k-1}))(A_1 + A_k) \subseteq A_1 + (A_2 \cap \cdots \cap A_{k-1} \cap A_k).
\]
Therefore, \( R = A_1 + (A_2 \cap \cdots \cap A_k) \) and the induction step is proved.

Now for \( 1 \leq k \leq n \), \( R = A_k + \left( \bigcap_{i \neq k} A_i \right) \).
For any \( b_k \in R \), there is \( a_k \in A_k \) and \( r_k \in \bigcap_{i \neq k} A_i \) such that \( b_k = a_k + r_k \). Then
\[
r_k \equiv b_k \mod A_k, \quad \text{and} \quad r_k \equiv 0 \mod A_i \quad \text{for} \quad i \neq k.
\]
Denote \( b := r_1 + \cdots + r_n \). Verify that
\[
b \equiv b_i \mod A_i \quad (i = 1, 2, \ldots, n).
\]
If \( c \in R \) such that \( c \equiv b_i \mod A_i \) for all \( i \), then \( c - b \equiv 0 \mod A_i \) for all \( i \). Therefore \( c - b \in \bigcap_{i=1}^n A_i \) for all \( i \) and \( c \equiv b \mod \bigcap_{i=1}^n A_i \).

Cor 3.20. Let \( m_1, \ldots, m_n \in \mathbb{N}^* \) such that \( \gcd(m_i, m_j) = 1 \) for \( i \neq j \). If \( b_1, \ldots, b_m \in \mathbb{Z} \), then the system of congruence equation
\[
x \equiv b_i \mod m_i \quad (i = 1, \ldots, n)
\]
has a integral solution unique modulo \( m = m_1m_2 \cdots m_n \).

Proof. Let \( A_i = (m_i) \). Then \( \bigcap_{i=1}^n A_i = (m) \) where \( m = \text{lcm}(m_1, \ldots, m_n) \). Note that \( \gcd(m_i, m_j) = 1 \) iff \( A_i + A_j = \mathbb{Z} \). Apply Theorem 3.19 to prove the result.

Cor 3.21. If \( A_1, \ldots, A_n \) are ideals in a ring \( R \) with unity, then there is a ring monomorphism
\[
\theta : R/(A_1 \cap \cdots \cap A_n) \rightarrow (R/A_1) \times (R/A_2) \times \cdots \times (R/A_n)
\]
defined by \( r + (A_1 \cap \cdots \cap A_n) \mapsto (r + A_1, \ldots, r + A_n) \). If \( A_i + A_j = R \) for all \( i \neq j \), then \( \theta \) is a ring isomorphism.

Proof. Define \( \pi : R \rightarrow (R/A_1) \times \cdots \times (R/A_n) \) by \( r \mapsto (r + A_1, \ldots, r + A_n) \). Then \( \pi \) is a ring homomorphism with \( \ker \pi = \bigcap_{i=1}^n A_i \). This induces the monomorphism \( \theta \). If \( A_i + A_j = R \) for all \( i \neq j \), then Chinese Remainder Theorem says that \( \theta \) is an epimorphism and thus an isomorphism.