Lecture 4: Ideals and Factor Rings

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Ideals

Definition (Ideal)

Let R be a ring. $\emptyset \neq I \subseteq R$ is an ideal of R if the followings hold:
$(i)\ \forall a, b \in I,\ a - b \in I$ (i.e. $(I, +)$ is a subgroup of $(R, +)$)
$(ii)\ \forall a \in I, \forall r \in R, ar \in I, ra \in I.$

In particular, if $ar \in I$ $(ra \in I)$, I is called a right (left) ideal of R.

Remarks:

- If R is a commutative ring, then every left (right) ideal is also a right (left) ideal.
- Let R is a ring with unity and I be an ideal of R. If $1_R \in I$,then $I = R$.
- Every ideal I is also a subring of R, but the converse may not be true.

Examples:

1. $\{0_R\}$ is an ideal of R. (zero ideal)

2. R is an ideal of R.

The ideals $\{0_R\}$ and R are called the *trivial* ideals. An ideal I of R is called a *proper* ideal if $I \neq R$.

3. Let $R = M_2(\mathbb{Z})$.

$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ is a left ideal of R, but not a right ideal.

$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ is a right ideal of R, but not a left ideal.

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a subring of R, but not an ideal.

4. $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. Actually, every subring of $\mathbb{Z}$ is an ideal.

Principle Ideal Domain (PID)

Let R be a ring and $a \in R$. Then

$$\langle a \rangle = \left\{ na + ra + as + \sum_{i=1}^{k} r_i a s_i \mid n \in \mathbb{Z}, r, s, r_i, s_i \in R, k \in \mathbb{N} \right\}.$$

If R is a commutative ring with unity, then $\langle a \rangle = \{ar \mid r \in R\} = aR$. It can easily be shown that $\langle a \rangle$ is an ideal of R. The ideal $\langle a \rangle$ of R is called **the principal ideal** generated by a. In general, for $a_1, a_2, ..., a_n \in R$, the ideal

$$\langle a_1, a_2, ..., a_n \rangle = \{a_1 r_1, a_2 r_2, ..., a_n r_n \mid a_1, a_2, ..., a_n \in R\}$$

is called **the ideal generated by** $a_1, a_2, ..., a_n$.

Example: Consider the ring $2\mathbb{Z}$ which is a commutative ring without unity. Then $\langle 2 \rangle = \{n2 + 2r \mid n \in \mathbb{Z}, r \in R\}$.

Remark: Let R be a ring and $\emptyset \neq A \subseteq R$. The intersection of all ideals of R that contain A, denoted by $\langle A \rangle$, is called the ideal generated by A. If $A = \emptyset$, then $\langle A \rangle$ is the zero ideal.

Principle Ideal Domain (PID)

Definition

Let D be an integral domain. If every ideal of D is a principal ideal, then D is called the **principal ideal domain** (PID).

Theorem

$\mathbb{Z}$ is a PID.

The principal ideal of $\mathbb{Z}$ generated by $n \in \mathbb{Z}$ is $\langle n \rangle = \{nr \mid r \in \mathbb{Z}\} = n\mathbb{Z}$.

Theorem

Let R be a commutative ring with unity. Then

$$R \text{ has no nontrivial ideals} \Leftrightarrow R \text{ is a field.}$$

Corollary

1. The only ideals of a field F are $\{0_F\}$ and F.

2. An ideal is proper $\Leftrightarrow$ It does not contain a unit.

Sum and Product of Ideals

Definition

Let I and J be two ideals of a ring R. The sum and product of the ideals I and J are defined as follows:

$$I + J \ : \ = \{a + b \mid a \in I, b \in J\}$$
$$I.J \ : \ = \left\{ \sum_{k=1}^{n} a_k b_k \mid a_k \in I, b_k \in J, n \in \mathbb{N} \right\}.$$

Theorem

Let I and J be ideals of a ring R. Then
(i) $I \cap J$ is an ideal of R.
(ii) $I + J$ is an ideal of R. Moreover, $I \subset I + J$ and $J \subset I + J$.
(iii) $I.J$ is an ideal of R. Moreover, $I.J \subset I \cap J$.
(iv) $I + J = \langle I \cup J \rangle$.

Note that $I \cup J$ need not be an ideal of R.

Sum and Product of Ideals

Now we give some properties of ideals of $\mathbb{Z}$.

Theorem

For positive integers n, m, we have

1. $\langle n\rangle \cap \langle m\rangle = \langle \mathrm{lcm}\,(n, m)\rangle$
2. $\langle n\rangle + \langle m\rangle = \langle \gcd\,(n, m)\rangle$
3. $\langle n\rangle . \langle m\rangle = \langle nm\rangle$
4. $\langle n\rangle \subseteq \langle m\rangle \Leftrightarrow m \mid n.$

Remark: Let R be an integral domain and $a, b \in R$. Then $\langle a\rangle . \langle b\rangle = \langle ab\rangle$.

Examples:

1. $\langle 2\rangle \cap \langle 3\rangle = \langle 6\rangle = 6\mathbb{Z}$

2. $\langle 2\rangle + \langle 3\rangle = \{2a + 3b \mid a, b \in \mathbb{Z}\} = \langle 1\rangle = \mathbb{Z}$

3. $\langle 2\rangle . \langle 3\rangle = \{2a_1 3b_1 + 2a_2 3b_2 + \cdots + 2a_k 3b_k \mid a_i, b_i \in \mathbb{Z}\}$

$$= \{6t_1 + 6t_2 + \cdots + 6t_k \mid t_i = a_i b_i \in \mathbb{Z}\} = 6$$

4. $\langle 4\rangle \subseteq \langle 2\rangle$.

To determine all ideals of $\mathbb{Z}_n$ we need to consider the subgroups $(I,+) < (\mathbb{Z}_n,+)$. We know that each subgroup of $\mathbb{Z}_n$ is cyclic, since $\mathbb{Z}_n = \langle\overline{1}\rangle$. Hence,

$$I = \langle\overline{a}\rangle \text{ is an ideal of } \mathbb{Z}_n \Leftrightarrow a \mid n.$$

Example: All ideals of $\mathbb{Z}_{12}$ are

$$\begin{aligned}
\langle\overline{1}\rangle &= \mathbb{Z}_{12} \\
\langle\overline{2}\rangle &= \{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10}\} \\
\langle\overline{3}\rangle &= \{\overline{0},\overline{3},\overline{6},\overline{9}\} \\
\langle\overline{4}\rangle &= \{\overline{0},\overline{4},\overline{8}\} \\
\langle\overline{6}\rangle &= \{\overline{0},\overline{6}\} \\
\langle\overline{12}\rangle &= \langle\overline{0}\rangle = \{\overline{0}\}\,.
\end{aligned}$$

Factor Rings

Let R be a ring and I be an ideal of R. For $a, b \in R$, the relation $\sim$ defined by "$a \sim b \Leftrightarrow a - b \in I$" is an equivalence relation on R. The set of all equivalence classes is

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

Theorem

Let R be a ring and I be an ideal of R. Define two binary operations $+$ and $\cdot$ on R/I by

$$\begin{aligned} (a+I)+(b+I) \quad &: \quad = (a+b)+I \\ (a+I)\cdot(b+I) \quad &: \quad = (ab)+I \end{aligned}$$

for $a + I, b + I \in R/I$. Then $(R/I, +, .)$ is a ring.

Factor Rings

Definition

The ring $(R/I, +, .)$ is called the **factor(quotient) ring** of R by I.

Remarks:

- If R is a ring with unity 1_R, then $1_R + I \in R/I$ is the unity of R/I.
- If R is a commutative ring, then R/I is also commutative.
- If R has no zero divisors, then R/I may have zero divisors. $\mathbb{Z}$ has no zero divisors, but $\mathbb{Z}/12\mathbb{Z}$ has zero divisors; $(3 + 12\mathbb{Z})(4 + 12\mathbb{Z}) = 0 + 12\mathbb{Z}$.
- $\mathbb{Z}_6$ has zero divisors, but $\mathbb{Z}_6 / \left\langle \left(\overline{0}, \overline{3}\right) \right\rangle$ is a field.

Examples:

1. If n is prime, then $\mathbb{Z}/n\mathbb{Z}$ is a field.

2. Let $R = \mathbb{Z}$ and $I = 4\mathbb{Z}$.Then

$$\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$$

is the quotient ring of $\mathbb{Z}$ by $4\mathbb{Z}$.

3. Let $R = 3\mathbb{Z}$ and $I = 3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$. Then

$$3\mathbb{Z}/12\mathbb{Z} = \{0 + 12\mathbb{Z}, 3 + 12\mathbb{Z}, 6 + 12\mathbb{Z}, 9 + 12\mathbb{Z}\} .$$