Week 10

10.1 Ideals

Definition. An **ideal** I in a commutative ring R is a subset of R which satisfies the following properties:

1. $0 \in I$;
2. If $a, b \in I$, then $a + b \in I$.
3. For all $a \in I$, we have $ar \in I$ for all $r \in R$.

If an ideal I is a proper subset of R, we say it is a **proper ideal**.

Remark. Note that if an ideal I contains 1, then $r = 1 \cdot r \in I$ for all $r \in R$, which implies that $I = R$.

Example 10.1.1. For any commutative ring R, the set $\{0\}$ is an ideal, since $0+0 = 0$, and $0 \cdot r = 0$ for all $r \in R$.

R itself is also an ideal.

An ideal $I \subsetneq R$ is called **proper** and an ideal $\{0\} \subsetneq I \subset R$ is called **nontrivial**.

Example 10.1.2. For all $m \in \mathbb{Z}$, the set $I = m\mathbb{Z} := \{mn : n \in \mathbb{Z}\}$ is an ideal:

1. $0 = m \cdot 0 \in I$;
2. $mn_1 + mn_2 = m(n_1 + n_2) \in I$.
3. Given $mn \in I$, for all $l \in \mathbb{Z}$, we have $mn \cdot l = m \cdot nl \in I$.

Example 10.1.3. Generalizing the above example, consider a commutative ring R. Let $a \in R$. Then

$$(a) := \{ra : r \in R\}$$

is an ideal, called the **principal ideal** generated by a.

Proof.

1. $0 = 0a \in (a)$;
2. Given $r_1a, r_2a \in (a)$, we have $r_1a + r_2a = (r_1 + r_2)a \in (a)$.
3. For all $ra \in (a)$ and $a \in R$, we have $s(ra) = (sr)a \in (a)$.

□

More generally, given any nonempty subset $A \subset R$, the set of finite linear combinations of elements in A:

$$(A) := \{r_1a_1 + r_2a_2 + \cdots + rka_k : k \in \mathbb{Z}_{>0}, r_i \in R, a_i \in A\}$$

is an ideal in R, called the **ideal generated by** A.

Proposition 10.1.4. *If $\phi : R \to R'$ is a ring homomorphism, then $\ker\phi$ is an ideal of R.*

Proof.

1. Since ϕ is a homomorphism, we have $\phi(0) = 0$. Hence, $0 \in \ker\phi$.
2. If $a, b \in \ker\phi$, then $\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$. Hence, $a + b \in \ker\phi$.
3. Given any $a \in \ker\phi$, for all $r \in R$ we have $\phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0$. Hence, $ar \in \ker\phi$ for all $r \in R$.

□

Example 10.1.5. Recall the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_m$ defined by $\phi(n) = \overline{n}$. The kernel of ϕ is:

$$\ker\phi = m\mathbb{Z} = (m).$$

Proposition 10.1.6. *A nonzero commutative ring R is a field if and only if its only ideals are $\{0\}$ and R.*

Proof. Suppose a nonzero commutative ring R is a field. If an ideal I of R is nonzero, it contains at least one nonzero element a of R. Since R is a field, a has a multiplicative inverse a^{-1} is R. Since I is a ideal, and $a \in I$, we have $1 = a^{-1}a \in I$. So, I is an ideal which contains 1, hence it must be the whole field R.

Conversely, let R be a nonzero commutative ring whose only ideals are $\{0\}$ and R. Given any nonzero element $a \in R$, the principal ideal (a) generated by a is nonzero because it contains $a \neq 0$. Hence, by hypothesis the ideal (a) is necessarily the whole ring R. In particular, the element 1 lies in (a), which means that there is an $r \in R$ such that $ar = 1$. This shows that any nonzero element of R is a unit. Hence, R is a field. □

Proposition 10.1.7. *Let F be a field, and R a nonzero ring. Any ring homomorphism $\phi : F \to R$ is necessarily one-to-one.*

Proof. Since R is not a zero ring, it contains $1 \neq 0$. So, $\phi(1) = 1 \neq 0$, which implies that $\ker\phi$ is a proper ideal of F. Since F is a field, we must have $\ker\phi = \{0\}$. It now follows from a previous claim that ϕ is one-to-one. $\square$

10.2 Quotient Rings

Let R be a commutative ring. Let I be an ideal of R. Then in particular I is an additive subgroup of $(R, +)$. Let R/I denote the set of all cosets of I in $(R, +)$, namely, the set of elements of the form

$$\overline{r} = r + I = \{r + a : a \in I\}, \quad r \in R.$$

Terminology: We sometimes call $\overline{r}$ the **residue** of r in R/I.

Note that $\bar{r} = \bar{0}$ if and only if $r \in I$; more generally, $\bar{r} = \bar{r'}$ if and only if $r - r' \in I$.

Remark. Recall that R/I is nothing but the set of equivalence classes of the following relation on R:

$$a \sim b, \quad \text{if } b - a \in I.$$

Notation/Terminology: If $a \sim b$, we say that a is **congruent modulo** I to b, and write:

$$a \equiv b \mod I.$$

It is tempting to define addition and multiplication on R/I using those operations on R:

$$\overline{r} + \overline{r'} = \overline{r + r'},$$
$$\overline{r} \cdot \overline{r'} = \overline{rr'},$$

for any $\overline{r}, \overline{r'} \in R/I$.

Observe that: for all $r, r' \in R$, and $a, a' \in I$, we have

$$(r + a) + (r' + a') = (r + r') + (a + a') \in (r + r') + I = \overline{r + r'},$$

which implies $\overline{(r + a) + (r' + a')} = \overline{r + r'}$. So addition $+$ is indeed well-defined on R/I. Note that this only used the fact that I is an additive subgroup of $(R, +)$.

On the other hand, we have the following

Theorem 10.2.1. *Given any additive subgroup $I < (R, +)$. The multiplication*

$$\overline{r} \cdot \overline{r'} = \overline{rr'}$$

is well-defined on R/I if and only if I is an ideal in R.

Proof. Suppose that I is an ideal. Then for any $r, r' \in R$, and $a, a' \in I$, we have

$$(r+a)\cdot(r'+a') = rr' + ra' + r'a + aa' \in rr' + I = \overline{rr'}.$$

Hence the multiplication is well-defined.

Conversely, suppose the multiplication is well-defined, meaning that for any $r, r' \in R$ and $a, a' \in I$, we have $\overline{(r+a')(r'+a)} = \overline{rr'}$. In particular, we have $\overline{ra} = \overline{(r+0)(0+a)} = \overline{r0} = I$ which implies $ra \in I$ for any $r \in R$ and $a \in I$. So I is an ideal. □

Proposition 10.2.2. *The set R/I, equipped with the addition $+$ and multiplication $\cdot$ defined above, is a commutative ring.*

Proof. We note here only that the additive identity element of R/I is $\overline{0} = 0 + I$, the multiplicative identity element of R/I is $\overline{1} = 1 + I$, and that $-\overline{r} = \overline{-r}$ for all $r \in R$.

We leave the rest of the proof (additive and multiplicative associativity, commutativity, distributive laws) as an **Exercise.** □

Proposition 10.2.3. *The map $\pi : R \to R/I$, defined by*

$$\pi(r) = \overline{r}, \quad \forall r \in R.$$

is a surjective ring homomorphism with kernel $\ker \pi = I$.

Proof. **Exercise.** □

Theorem 10.2.4 (First Isomorphism Theorem)**.** *Let $\phi : R \longrightarrow R'$ be a ring homomorphism. Then:*

$$R/\ker\phi \cong \operatorname{im}\phi,$$

(i.e. $R/\ker\phi$ is isomorphic to $\operatorname{im}\phi$*.)*

Proof. We define a map $\overline{\phi} : R/\ker\phi \longrightarrow \operatorname{im}\phi$ as follows:

$$\overline{\phi}(\overline{r}) = \phi(r), \quad \forall\, r \in R,$$

where $\overline{r}$ is the residue of r in $R/\ker\phi$.

We first need to check that ϕ is well-defined. Suppose $\overline{r} = \overline{r'}$, then $r' - r \in \ker\phi$. We have:

$$\overline{\phi}(\overline{r'}) - \overline{\phi}(\overline{r}) = \phi(r') - \phi(r) = \phi(r' - r) = 0.$$

Hence, $\overline{\phi}(\overline{r'}) = \overline{\phi}(\overline{r})$. So, $\overline{\phi}(\overline{r})$ is defined regardless of the choice of representative for the equivalence class $\overline{r}$.

Next, we show that $\overline{\phi}$ is a homomorphism:

- $\overline{\phi}(\overline{1}) = \phi(1) = 1$;
- $\overline{\phi}(\overline{a} + \overline{b}) = \overline{\phi}(\overline{a+b}) = \phi(a+b) = \phi(a) + \phi(b) = \overline{\phi}(\overline{a}) + \overline{\phi}(\overline{b})$;
- $\overline{\phi}(\overline{a} \cdot \overline{b}) = \overline{\phi}(\overline{ab}) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(\overline{a})\overline{\phi}(\overline{b})$.

Finally, we show that $\overline{\phi}$ is a bijection, i.e. one-to-one and onto.

For any $r' \in \operatorname{im}\phi$, there exists $r \in R$ such that $\phi(r) = r'$. Since $\overline{\phi}(\overline{r}) = \phi(r) = r'$, $\overline{\phi}$ is onto.

Let r be an element in R such that $\overline{\phi}(\overline{r}) = \phi(r) = 0$. We have $r \in \ker\phi$, which implies that $\overline{r} = 0$ in $R/\ker\phi$. Hence, $\ker\overline{\phi} = \{0\}$, and it follows that $\overline{\phi}$ is one-to-one. □

Corollary 10.2.5. *If a ring homomorphism $\phi : R \longrightarrow R'$ is surjective, then:*

$$R' \cong R/\ker\phi$$

Example 10.2.6. Let m be a natural number. The remainder or mod m map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ defined by:

$$\phi(n) = \overline{n}, \quad \forall\, n \in \mathbb{Z},$$

where $\overline{n}$ is the remainder of the division of n by m, is a surjective homomorphism such that $\ker\phi = (m) = m\mathbb{Z}$. So, it follows from the First Isomorphism Theorem that:

$$\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}.$$

Example 10.2.7. The ring $\mathbb{Z}[i]/(1+3i)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z}$.

Proof. Define a map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}[i]/(1+3i)$ as follows:

$$\phi(n) = \overline{n}, \quad \forall\, n \in \mathbb{Z},$$

where $\overline{n}$ is the equivalence class of $n \in \mathbb{Z}[i]$ modulo $(1+3i)$.

It is clear that ϕ is a homomorphism (**Exercise**).

Observe that in $\mathbb{Z}[i]$, we have:

$$1 + 3i \equiv 0 \mod (1+3i),$$

which implies that:

$$i \equiv 3 \mod (1+3i).$$

Hence, for all $a, b \in \mathbb{Z}$,

$$\overline{a+bi} = \overline{a+3b} = \phi(a+3b)$$

in $\mathbb{Z}[i]/(1+3i)$. Hence, ϕ is surjective.

Suppose n is an element of $\mathbb{Z}$ such that $\phi(n) = \overline{n} = 0$. Then, by the definition of the quotient ring we have:

$$n \in (1+3i).$$

This means that there exist $a, b \in \mathbb{Z}$ such that:

$$n = (a+bi)(1+3i) = (a-3b) + (3a+b)i,$$

which implies that $3a + b = 0$, or equivalently, $b = -3a$. Hence:

$$n = a - 3b = a - 3(-3a) = 10a,$$

which implies that $\ker\phi \subseteq 10\mathbb{Z}$. Conversely, for all $m \in \mathbb{Z}$, we have:

$$\phi(10m) = \overline{10m} = \overline{(1+3i)(1-3i)m} = 0$$

in $\mathbb{Z}[i]/(1+3i)$. This shows that $10\mathbb{Z} \subseteq \ker\phi$. Hence, $\ker\phi = 10\mathbb{Z}$.

It now follows from the First Isomorphism Theorem that:

$$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}[i]/(1+3i).$$

□

Example 10.2.8. The rings $\mathbb{R}[x]/(x^2+1)$ and $\mathbb{C}$ are isomorphic.

Proof. Define a map $\phi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ as follows:

$$\phi(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} a_k i^k.$$

Exercise: ϕ is a homomorphism.

For all $a + bi$ $(a, b \in \mathbb{R})$ in $\mathbb{C}$, we have:

$$\phi(a + bx) = a + bi.$$

Hence, ϕ is surjective.

It remains to compute $\ker\phi = \{f(x) = \sum_{k=0}^{n} a_k x^k : f(i) = 0\}$. Note that $f(x)$ is a real polynomial, so $f(i) = 0$ also implies that $f(-i) = 0$. Hence both $\pm i$ are roots of $f(x)$ if it lies in $\ker\phi$. Factor Theorem then tells us that $(x^2+1) = (x-i)(x+i) \mid f(x)$. So $\ker\phi \subset (x^2+1)$. On the other hand, i is a root of x^2+1, so we have $(x^2+1) \subset \ker\phi$. We conclude that $\ker\phi = (x^2+1)$.

It now follows from the First Isomorphism Theorem that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

□