1. Ring Homomorphisms and the Fundamental Theorems of Isomorphism

1.1. Ring Homomorphisms

To understand better rings and their properties we have to look at maps between ring that preserve the structure, namely that preserve both addition and multiplication. This maps are called ring-homomorphisms.

Definition 1.1. Let A and B be rings. A map $\psi\colon A \to B$ is a **ring-homomorphism** if, for all $a, b \in A$,

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$, and

(ii) $\psi(a \cdot b) = \psi(a)\psi(b)$.

A bijective ring-homomorphism is called a **ring-isomorphism**. If there is an isomorphism between A and B, we say these rings are isomorphic, which is denoted by $A \cong B$.

Note that condition (i) means ψ is a group-homomorphism from $(A, +_A)$ to $(B, +_B)$. This implies that $\psi(0_A) = 0_B$ since $\psi(0_A) = \psi(0_A + 0_A) = \psi(0_A) + \psi(0_A)$ whence $\psi(0_A) = 0_B$ by subtraction. A ring-homomorphism from A to A is called an **endomorphism** of A.

Remark 1.1.1. If both A and B are rings with unity, a ring-homomorphism $\psi\colon A \to B$ must in addition satisfy $\psi(1_A) = 1_B$.

Given a homomorphism of rings $\psi\colon A \to B$, the kernel of ψ is

$$\operatorname{Ker}\psi = \{x \in A \mid \varphi(x) = 0\}.$$

The image of ψ is $\operatorname{Im}\psi = \psi(A)$.

Exercise 1. Prove $\operatorname{Ker}\psi$ is an ideal of A and $\operatorname{Im}\psi$ is a subring of B. Why is it not necessarily true that $\operatorname{Im}\psi$ is an ideal of B?

Example 1. (i) If B is a subring of a ring A, the canonical injection $\iota\colon B \to A\colon b \mapsto b$ is a ring-homomorphism. In particular, the identity $\operatorname{Id}_A\colon A \to A$ is an isomorphism.

(ii) If A is a ring and $I \trianglelefteq A$ an ideal, the canonical projection $\pi\colon A \to A/I$ is a surjective homomorphism of rings. Indeed, we have

$$\pi(a_1) + \pi(a_2) = (a_1 + I) + (a_2 + I) = (a_1 + a_2) + I = \pi(a_1 + a_2), \quad \text{and}$$
$$\pi(a_1)\pi(a_2) = (a_1 + I)(a_2 + I) = (a_1 a_2) + I = \pi(a_1 a_2).$$

In particular, the projection $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a ring homomorphism, called **reduction modulo** n.

(iii) If $(A_\lambda)_{\lambda \in \Lambda}$ is a family of rings, the αth canonical projection $p_\alpha \colon \prod_{\lambda \in \Lambda} A_\lambda \to A_\alpha$ is a surjective ring-homomorphism.

(iv) The rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic. If there were an isomorphism $\psi : 2\mathbb{Z} \to 3\mathbb{Z}$ such that $\psi(2) = 3k$ for some integer $k \neq 0$, then

$$\psi(4) = \psi(2+2) = \psi(2) + \psi(2) = 6k,$$

but

$$\psi(4) = \psi(2 \cdot 2) = \psi(2) \cdot \psi(2) = 9k^2.$$

Thus $6k = 9k^2$, and since $k \neq 0$, then $2 = 3k$, which is impossible. Therefore $2\mathbb{Z} \ncong 3\mathbb{Z}$.

(v) Let A be a commutative ring with unity, then the map

$$\psi : A[x] \to A \quad : \quad p(x) \mapsto p(0)$$

is a ring homomorphism that maps a polynomial to its constant term. In general, the evaluation map $\psi_\alpha : A[x] \to A$ defined by

$$\psi_\alpha \left(a_0 + a_1 x + \cdots + a_n x^n\right) = a_0 + a_1 \alpha + \cdots + a_n \alpha^n,$$

where $\alpha \in A$ is fixed, is a homomorphism of $A[x]$ onto A.

(vi) There is no ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ for any $n \in \mathbb{Z}^+$.

1.2. Properties of Ring Homomorphisms

Proposition 1.2. *Let $\psi \colon A \to B$ be a morphism of rings. Then*

(i) *$f(-a) = -f(a)$ for all $a \in A$*

(ii) *$f(na) = nf(a)$ for all $a \in A$ and $n \in \mathbb{Z}$*

(iii) *$f(a^n) = f(a)^n$ for all $a \in A$ and $n \in \mathbb{Z}^+$*

(iv) *$\operatorname{Ker} \psi$ is an ideal of A*

(v) *$\operatorname{Im} \psi$ is a subring of B*

(vi) *ψ is injective if and only of $\operatorname{Ker} \psi = 0$*

(vii) *if $a \in A$ is invertible, so is $\psi(a)$*

(viii) *if $\mathfrak{p}$ is an ideal of B, then $\psi^{-1}(\mathfrak{p})$ is an ideal of A.*

(ix) *if $\mathfrak{p}$ is a maximal (prime) ideal of B, then $\psi^{-1}(\mathfrak{p})$ is a maximal (prime) ideal of A.*

(x) *the composition of ring homomorphisms is a ring homomorphism*

Proof. Straight from the definitions and left as an exercise to the student. $\qquad\square$

1.3. Fundamental Theorems of Isomorphism

The significance of the following results lies in their usefulness to simplify computations by allowing us to replace a ring with another that is more convenient, provided a ring isomorphism can be established. The proofs of these results are left as exercises for the reader, while the accompanying diagrams serve to illustrate the concepts and serve as mnemonic aids.

Theorem 1.3 (Fundamental Theorem on Ring-Homomorphisms). *Let $\psi : A \to B$ be a ring-homomorphism and I an ideal of A with $I \subseteq \operatorname{Ker} \psi$. Then there is a unique ring-homomorphism $\overline{\psi} \colon A/I \to B$ such that $\psi = \overline{\psi} \circ \pi$, i.e.,*

$$\overline{\psi}(a + I) = \psi(a) \quad \text{for all } a \in A.$$

In other words, such that the following diagram commutes

$$
\begin{array}{ccc}
A & \xrightarrow{\ \psi\ } & B \\
{\scriptstyle \pi}\big\downarrow & \nearrow & \\
A/I & {\scriptstyle \overline{\psi}} &
\end{array}
$$

Moreover

(i) $\operatorname{Im} \overline{\psi} = \operatorname{Im} \psi$,

(ii) $\operatorname{Ker} \overline{\psi} = (\operatorname{Ker} \psi)/I$

(iii) $\overline{\psi}$ *is an isomorphism if and only if ψ is an epimorphism and $I = \operatorname{Ker} \psi$.*

Proof (Sketch). Define $\overline{\psi} \colon A/I \to B$ by $\overline{\psi}(a + I) = \psi(a)$. By using the fact that $I \subseteq \operatorname{Ker} \psi$, we show $\overline{\psi}$ is well-defined. This shows the existence. If $\varphi \colon A/I \to B$ is another ring-homomorphism such that $\psi = \varphi \circ \pi$, then $\overline{\psi} \circ \pi = \varphi \circ \pi$. Since π is surjective, it has a right inverse and thus $\overline{\psi} = \varphi$. This shows the uniqueness. On the other hand, (i) $\psi(a) \in \operatorname{Im} \psi$ if and only if $\psi(a) = \overline{\psi}(a + I) \in \operatorname{Im} \overline{\psi}$. Hence $\operatorname{Im} \psi = \operatorname{Im} \overline{\psi}$. Note (ii)

$$
\begin{aligned}
\operatorname{Ker} \overline{\psi} &= \{a + I \in A/I \mid \overline{\psi}(a + I) = 0\} \\
&= \{a + I \in A/I \mid \psi(a) = 0\} \\
&= \{a + I \in A/I \mid a \in \operatorname{Ker} \psi\} \\
&= \operatorname{Ker} \psi / I
\end{aligned}
$$

Finally, (i) shows $\overline{\psi}$ is surjective if and only if ψ is, and (ii) implies $\overline{\psi}$ is injective if $\operatorname{Ker} \psi = I$ since $\operatorname{Ker} \overline{\psi} = I/I = I$. These facts imply (iii). $\qquad\square$

The following corollaries are known as the fundamental theorems of ring-homomorphisms. Their proof follows from the fundamental theorem of ring-homomorphisms and thus we leave the details to the reader.

Corollary 1.4 (First Isomorphism Theorem)**.** *If $\psi\colon A \to B$ is a ring-homomorphism, then ψ induces an isomorphism of rings $A/\operatorname{Ker}\psi \cong \operatorname{Im}\psi$. Furthermore, the following diagram commutes.*

$$
\begin{array}{ccc}
A & \xrightarrow{\ \psi\ } & B \\
{\scriptstyle p}\big\downarrow & & \big\uparrow{\scriptstyle j} \\
A/\operatorname{Ker}\psi & \dashrightarrow{\ \tilde{\psi}\ } & \operatorname{Im}\psi
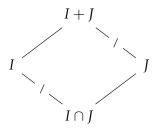\end{array}
$$

Corollary 1.5 (Second Isomorphism Theorem)**.** *Let I and J be ideals in a ring A. Then*

$$
\frac{I}{I \cap J} \cong \frac{I+J}{J}.
$$

Corollary 1.6 (Third Isomorphism Theorem)**.** *Let I and J be ideals in a ring A with $J \subseteq I$. Then*

$$
\frac{A/J}{I/J} \cong \frac{A}{I}.
$$

This corollary, also known as the diamond (or parallelogram) theorem, indicates that the opposite sides of the parallelogram (with a slash) are isomorphic.

$$
\begin{array}{ccc}
 & I+J & \\
I & & J \\
 & I \cap J &
\end{array}
$$

Corollary 1.7 (Fourth Isomorphism Theorem)**.** *If I is an ideal in a ring A, then there is a one-to-one correspondence between the set of all ideals of A which contain I and the set of all ideals of A/I, given by $J \mapsto J/I$. Hence every ideal in A/I is of the form J/I, where J is an ideal of A which contains I.*

Example 2. Let $A = \mathbb{Z}$ and $I = 12\mathbb{Z}$. By the fourth isomorphism theorem, the ideals of A/I are in bijective correspondence with the ideals of $\mathbb{Z}$ containing $12\mathbb{Z}$, namely with

$$
2\mathbb{Z},\ 3\mathbb{Z},\ 4\mathbb{Z},\ 6\mathbb{Z},\ 12\mathbb{Z}.
$$

Therefore, the ideals of A/I are

$$
2\mathbb{Z}/12\mathbb{Z},\quad 3\mathbb{Z}/12\mathbb{Z},\quad 4\mathbb{Z}/12\mathbb{Z},\quad 6\mathbb{Z}/12\mathbb{Z},\quad 12\mathbb{Z}/12\mathbb{Z}.
$$

1.4. Additional properties of rings

Proposition 1.8. *If $\psi\colon F \to A$ is a nonzero ring-homomorphism and F is a field, then ψ is injective.*

Proof. Recall the kernel of any ring homomorphism is an ideal. Since ψ is nonzero, its kernel cannot be F. Because F is a field, its only ideals are 0 and F. Hence $\operatorname{Ker}\psi = 0$. Therefore ψ is injective. $\qquad\square$

Theorem 1.9. *Let A be a commutative ring and M and P two ideals of A.*

  (i) M is maximal if and only if A/M is a field.

  (ii) P is prime if and only if A/P is an integral domain.

Proof.   (i) The first part of the theorem follows from the Fourth Isomorphism Theorem (FIT) and the fact that a field has only the two trivial ideals. Indeed, by definition, the ideal M is maximal if there is no ideal J such that

$$M \subsetneq J \subsetneq A.$$

The ideals of A containing M correspond bijectively with the ideals of A/M. Therefore, M is maximal if the only ideals of A/M are 0 and A/M. Hence, M is maximal if A/M is a field.

  (ii) Let us denote the class of a in A/P by $\bar{a}$. If P is a prime ideal and

$$\bar{a}\,\bar{b} = \overline{ab} = 0_{A/P} = P,$$

then $ab \in P$. Since P is a prime ideal, $a \in P$ or $b \in P$. Therefore $\bar{a} = 0$ or $\bar{b} = 0$. Hence, A/P is an integral domain.

Conversely, if A/P is an integral domain and $ab \in P$ with $a, b \in A$, then since

$$\bar{a}\,\bar{b} = \overline{ab} = 0$$

and A/P is an integral domain, we have that

$$\bar{a} = 0 \quad \text{or} \quad \bar{b} = 0,$$

but this is equivalent to $a \in P$ or $b \in P$. Therefore, P is a prime ideal.

$\square$

Proposition 1.10. *Let A be a commutative ring. Then every maximal ideal of A is a prime ideal.*

Proof. Let M be a maximal ideal of A. Then A/M is a field. Every field is an integral domain. Thus, A/M is an integral domain. Therefore M is a prime ideal. $\square$

Example 3.   (i) The ideal $p\mathbb{Z}$ is a maximal ideal if and only if p is prime since $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is prime.

  (ii) Consider the surjective evaluation homomorphism

$$\theta : \mathbb{Z}[x] \to \mathbb{Z}, \quad p(x) \mapsto p(0).$$

Then

$$\mathrm{Ker}(\theta) = \{p(x) \in \mathbb{Z}[x] \mid p(0) = 0\} = \langle x \rangle$$

and

$$\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}.$$

Therefore $\langle x \rangle$ is prime since $\mathbb{Z}$ is an integral domain.