CHAPTER 7

Ring Homomorphisms and Ideals

7.1. Ring Homomorphisms

DEFINITION. Suppose that R and S are rings. A function $\phi : R \to S$ is said to be a ring homomorphism if the following conditions are satisfied:

(RH1) For every $x, y \in R$, $(x + y)\phi = x\phi + y\phi$.
(RH2) For every $x, y \in R$, $(xy)\phi = x\phi y\phi$.

DEFINITION. Suppose that R and S are rings, and that $\phi : R \to S$ is a ring homomorphism. Then the image $R\phi$ and the kernel $\ker \phi$ of $\phi : R \to S$ are defined by

$$R\phi = \{x\phi : x \in R\} \quad \text{and} \quad \ker \phi = \{x \in R : x\phi = 0\}.$$

REMARK. Condition (RH1) implies that $\phi : R \to S$ is a group homomorphism from $(R, +)$ to $(S, +)$.

DEFINITION. Suppose that R and S are rings. A function $\phi : R \to S$ is said to be a ring isomorphism if the following conditions are satisfied:

(RI1) $\phi : R \to S$ is a ring homomorphism.
(RI2) $\phi : R \to S$ is one-to-one.
(RI3) $\phi : R \to S$ is onto.

DEFINITION. A ring isomorphism from a ring R to itself is called an automorphism of the ring R.

DEFINITION. We say that two rings R and S are isomorphic if there exists a ring isomorphism $\phi : R \to S$.

EXAMPLES. (1) The complex conjugation function $\phi : \mathbb{C} \to \mathbb{C}$, defined by $z\phi = \overline{z}$ for every $z \in \mathbb{C}$, is an automorphism on $\mathbb{C}$.
(2) Let $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$. The conjugation function $\phi : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{3})$, defined by $(a + b\sqrt{3})\phi = a - b\sqrt{3}$ for every $a, b \in \mathbb{Q}$, is an automorphism on $\mathbb{Q}(\sqrt{3})$.

Various basic results concerning ring homomorphisms correspond to basic results concerning group homomorphisms.

Our first two results below correspond to Theorem 4.2 and Proposition 4.3 respectively.

THEOREM 7.1. *Suppose that R and S are rings, and that $\phi : R \to S$ is a ring homomorphism. Then $R\phi$ is a subring of S.*

PROOF. By Theorem 4.2, $(S, +)$ is a subgroup of $(R, +)$, so it remains to check that (SR) holds. Clearly if $x\phi, y\phi \in R\phi$, then since $xy \in R$, we must have $x\phi y\phi = (xy)\phi \in R\phi$. ◯

PROPOSITION 7.2. *Suppose that R is a ring, and that $+$ and $\cdot$ are binary operations on a set X. Suppose further that the function $\phi : R \to X$ satisfies the conditions that $(x + y)\phi = x\phi + y\phi$ and $(xy)\phi = x\phi y\phi$ for every $x, y \in R$. Then the set $R\phi = \{x\phi : x \in R\}$, together with the binary operations $+$ and $\cdot$ on X, forms a ring.*

The proof is left as an exercise.

PROPOSITION 7.3. *Suppose that R and S are rings, and that $\phi : R \to S$ is a ring homomorphism.*

(i) *If R is commutative, then $R\phi$ is commutative.*
(ii) *If R has unity 1 and $1\phi \neq 0$, then $R\phi$ has unity 1ϕ.*
(iii) *If R has unity 1 and $1\phi = 0$, then $R\phi = \{0\}$.*
(iv) *If R is a field and $1\phi \neq 0$, then $R\phi$ is a field.*

PROOF. (i) Since R is commutative, $x\phi y\phi = (xy)\phi = (yx)\phi = y\phi x\phi$ for every $x, y \in R$.
(ii) If $1\phi \neq 0$, then $1\phi x\phi = (1x)\phi = x\phi$ and $x\phi 1\phi = (x1)\phi = x\phi$ for every $x \in R$.
(iii) If $1\phi = 0$, then $x\phi = (x1)\phi = x\phi 1\phi = x\phi \cdot 0 = 0$ for every $x \in R$.
(iv) By (i) and (ii), $R\phi$ is commutative and has unity 1ϕ. Now suppose that $x\phi \neq 0$ in $R\phi$. Since $0\phi = 0$, it follows that $x \neq 0$; since R is a field, it follows that $x^{-1} \in R$. Now $x^{-1}\phi x\phi = (x^{-1}x)\phi = 1\phi$ and $x\phi x^{-1}\phi = (xx^{-1})\phi = 1\phi$. ◯

REMARK. It is almost trivial to check that $\phi : \mathbb{Z} \to \mathbb{Z}_4$, defined by reduction modulo 4, is a ring homomorphism. Note that $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}_4$ is not. It follows that Proposition 7.3 cannot have a statement concerning integral domains.

7.2. Ideals

In our study of group homomorphisms, normal subgroups play an important role. The corresponding role in ring theory is played by ideals.

DEFINITION. Suppose that R is a ring. A non-empty subset I of R is said to be an ideal in R if the following conditions are satisfied:

(I1) $(I, +)$ is a subgroup of $(R, +)$.
(I2) For every $x \in I$ and every $a \in R$, the elements $xa, ax \in I$.

REMARK. Note that $(I, +)$ is a normal subgroup of $(R, +)$. Why?

Corresponding to Proposition 4.6, we have the following result.

PROPOSITION 7.4. *Suppose that R and S are rings, and that $\phi : R \to S$ is a ring homomorphism. Then* $\ker \phi$ *is an ideal in R.*

PROOF. Note that (I1) is satisfied in view of Proposition 4.6. On the other hand, if $x \in \ker \phi$ and $a \in R$, then $(xa)\phi = x\phi a\phi = 0 \cdot a\phi = 0$ and $(ax)\phi = a\phi x\phi = a\phi \cdot 0 = 0$, so that $xa, ax \in \ker \phi$. ◯

The proof of the following result is very simple, and is left as an exercise.

PROPOSITION 7.5. *Suppose that R is a commutative ring, and that $x \in R$. Then the set*

$$\langle x \rangle = \{ax : a \in R\}$$

is an ideal in R.

DEFINITION. The ideal $\langle x \rangle$ in Proposition 7.5 is called the principal ideal generated by x.

An important result concerning ideals is on the non-existence of proper ideals under certain conditions.

PROPOSITION 7.6.

(i) *Suppose that R is a field. Then the only ideals in R are $\{0\}$ and R.*
(ii) *Suppose that R is a commutative ring with unity, and having $\{0\}$ and R as the only ideals. Then R is a field.*

PROOF. (i) Clearly $\{0\}$ is an ideal. Suppose now that I is a non-zero ideal in R. Let $x \in I$ be non-zero. Since R is a field, $x^{-1} \in R$. It follows that for every element $a \in R$, $ax^{-1} \in R$ and so $a = ax^{-1}x \in I$. Hence $I = R$.
(ii) Let $x \in R$ be non-zero. Then $\langle x \rangle$ is an ideal in R by Proposition 7.5. Clearly $\langle x \rangle \neq \{0\}$, so we must have $\langle x \rangle = R$. In particular, $1 \in \langle x \rangle$. It follows that $1 = ax$ for some $a \in R$. Clearly a is the multiplicative inverse of x. Hence R is a field. ◯

We are now in a position to prove the following useful result.

PROPOSITION 7.7. *Suppose that R is a field and S is a ring, and that $\phi : R \to S$ is a ring homomorphism. Then precisely one of the following two statements holds:*

(i) $R\phi = \{0\}$.
(ii) $\phi : R \to S$ *is one-to-one.*

PROOF. By Proposition 7.4, $\ker \phi$ is an ideal in R. By Proposition 7.6(i), either $\ker \phi = R$ or $\ker \phi = \{0\}$. These correspond to cases (i) and (ii) respectively. ◯

Our last result in this section concerns pre-images, and corresponds to Proposition 4.9.

PROPOSITION 7.8. *Suppose that R and S are rings, and that $\phi : R \to S$ is a ring homomorphism.*

(i) *If I is an ideal in S, then $I\phi^{-1}$ is an ideal in R.*
(ii) *If T is a subring of S, then $T\phi^{-1}$ is a subring of R.*

PROOF. (i) It follows from Proposition 4.9 that $(I\phi^{-1}, +)$ is a subgroup of $(R, +)$. On the other hand, if $x \in I\phi^{-1}$ and $a \in R$, then $x\phi \in I$ and $(ax)\phi = a\phi x\phi \in I$, so that $ax \in I\phi^{-1}$. Similarly $xa \in I\phi^{-1}$.
(ii) is simpler. ◯

7.3. Quotient Rings

Suppose that R is a ring, and that $(I, +)$ is a subgroup of the group $(R, +)$. We can consider cosets of the type $x + I$, where $x \in R$. Since $(R, +)$ is abelian, every subgroup is normal, and so we can define addition of cosets as in Chapter 4; for every $x, y \in R$, we have

$$(x + I) + (y + I) = (x + y) + I. \tag{7.1}$$

We now turn to the question of multiplication of cosets. Corresponding to Theorem 4.11, we have the following result.

THEOREM 7.9. *Suppose that R is a ring, and that I is an ideal in R. Then the multiplication of cosets*

$$(x + I)(y + I) = xy + I \tag{7.2}$$

is well defined. In other words, if $x_1, x_2, y_1, y_2 \in R$ and $x_1 + I = x_2 + I$ and $y_1 + I = y_2 + I$, then $x_1y_1 + I = x_2y_2 + I$.

PROOF. By Proposition 4.10, $x_1y_1 + I = x_2y_2 + I$ if and only if

$$(-(x_1y_1)) + x_2y_2 \in I. \tag{7.3}$$

Now

$$\begin{aligned} (-(x_1y_1)) + x_2y_2 &= x_2y_1 + (-(x_1y_1)) + x_2y_2 + (-(x_2y_1)) \\ &= (x_2 + (-x_1))y_1 + x_2(y_2 + (-y_1)). \end{aligned} \tag{7.4}$$

Since $x_1+I = x_2+I$ and $y_1+I = y_2+I$, it follows from Proposition 4.10 that $x_2+(-x_1), y_2+(-y_1) \in I$. Since I is an ideal, (7.3) clearly follows from (7.4). ◯

Having obtained two binary operations, we now show that there is a ring structure. Corresponding to Theorem 4.12, we have the following important result.

THEOREM 7.10. *Suppose that R is a ring, and that I is an ideal in R. Then the set*

$$R/I = \{x + I : x \in R\}$$

of all cosets of I, together with addition and multiplication defined by (7.1) *and* (7.2) *respectively, forms a ring.*

DEFINITION. The ring R/I in Theorem 7.10 is called the quotient ring R modulo I.

PROOF OF THEOREM 7.10. By Theorem 4.12, $(R/I, +)$ forms an abelian group. (R6) is obvious from (7.2), on noting that $xy \in R$ for every $x, y \in R$. Finally, (R7), (R8) and (R9) follow respectively from (R7), (R8) and (R9) for the ring R. ◯

EXAMPLE. The ring $\mathbb{Z}_4$ is isomorphic to the quotient ring $\mathbb{Z}/\langle 4\rangle$. It can be checked that the function $\phi : \mathbb{Z}_4 \to \mathbb{Z}/\langle 4\rangle$, defined by $x\phi = x + \langle 4\rangle$ for $x = 0, 1, 2, 3$, is an isomorphism.

The proof of the following result is left as a simple exercise.

PROPOSITION 7.11. *Suppose that R is a ring, and that I is an ideal in R.*

(i) *If R is commutative, then R/I is commutative.*
(ii) *If R has unity 1 and $I \neq R$, then R/I has unity $1 + I$.*

7.4. Fundamental Theorem of Ring Homomorphisms

Corresponding to Theorem 4.15, we prove the following fundamental result.

THEOREM 7.12 (Fundamental theorem of ring homomorphisms). *Suppose that R and S are rings, and that $\phi : R \to S$ is a ring homomorphism. Then $R/\ker\phi$ is isomorphic to $R\phi$.*

PROOF. For simplicity, write $\ker\phi = I$. Then I is an ideal in R. Define a function $\psi : R/I \to R\phi$ in the following way. For every element $x + I \in R/I$, let $(x + I)\psi = x\phi$. Note now that $(I, +)$ is a normal subgroup of $(R, +)$, and so it follows from the proof of Theorem 4.15 that the function $\psi : R/I \to R\phi$ is a group isomorphism from $(R/I, +)$ to $(R\phi, +)$. To show that $\psi : R/I \to R\phi$ is a ring isomorphism, it remains to verify (RH2). Clearly, for every $x, y \in R$, we have

$$((x + I)(y + I))\psi = (xy + I)\psi = (xy)\phi = x\phi y\phi = (x + I)\psi(y + I)\psi,$$

as required. ◯

7.5. Prime and Maximal Ideals

DEFINITION. Suppose that R is a commutative ring. An ideal I in R is said to be prime if the following conditions are satisfied:

(i) $I \neq R$.
(ii) For every $x, y \in R$ such that $xy \in I$, either $x \in I$ or $y \in I$.

THEOREM 7.13. *Suppose that R is a commutative ring with unity, and that I is a prime ideal in R. Then R/I is an integral domain.*

PROOF. Clearly R/I is a commutative ring with unity. Suppose that $x, y \in R$, and that $(x + I)(y + I) = I$. Then $xy + I = I$, so that $xy \in I$. It follows that $x \in I$ or $y \in I$, so that $x + I = I$ or $y + I = I$. Hence R/I has no zero divisors. ◯

DEFINITION. Suppose that R is a commutative ring. An ideal I in R is said to be maximal if the following conditions are satisfied:

(i) $I \neq R$.
(ii) For every ideal J in R such that $I \subseteq J \subseteq R$, either $J = I$ or $J = R$.

THEOREM 7.14. *Suppose that R is a commutative ring with unity, and that I is a maximal ideal in R. Then R/I is a field.*

PROOF. Let U be a non-zero ideal of R/I. Consider $U\phi^{-1}$, where $\phi : R \to R/I$ is the natural homomorphism. By Proposition 7.8(i), $U\phi^{-1}$ is an ideal. Since U is a non-zero ideal, it contains a coset $z + I$ where $z \notin I$. Hence $z \in U\phi^{-1}$, so that $I \subsetneq U\phi^{-1}$. It follows that $U\phi^{-1} = R$, whence $U = (U\phi^{-1})\phi = R\phi = R/I$. This means that the only ideals in R/I are the two trivial ideals. The result follows from Proposition 7.6(ii). ◯

Problems for Chapter 7

1. For each of the following functions, determine whether the function is a ring homomorphism; and if so, determine also the image and kernel:

(i) $\phi : \mathbb{Z}_6 \to \mathbb{Z}_6$, where $x\phi = 3x$

(ii) $\phi : \mathbb{Z}_4 \to \mathbb{Z}_4$, where $x\phi = 2x$

2. Suppose that $n \in \mathbb{N} \setminus \{1\}$. Determine which values $a \in \{0, 1, 2, \ldots, n-1\}$ satisfy the following condition: The function $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$, defined by $x\phi = ax$ for every $x \in \mathbb{Z}_n$, is a ring homomorphism.

[*Hint*: Examine Question 1 closely.]

3. Suppose that R is a ring, and that R contains a non-zero element. Show that there are at least two homomorphisms from R to R.

4. Suppose that R is a ring, and that $\mathcal{S}$ is the set of all ring automorphisms of R. Prove that $\mathcal{S}$ forms a group under composition of functions.

5. Suppose that I is an ideal in $\mathbb{Z}$. Show that there exists $m \in \mathbb{Z}$ such that $I = \langle m \rangle$.

[*Hint*: Note that if I is an ideal of a ring R, then $(I, +)$ is a subgroup of $(R, +)$.]

6. Suppose that R is a ring, and that I and J are ideals in R. Prove that

$$I + J = \{x + y : x \in I \wedge y \in J\}$$

is an ideal in R.

7. Suppose that R and S are rings, and that $\phi : R \to S$ is a ring homomorphism. Suppose further that I is an ideal in R. Prove that $I\phi$ is an ideal in $R\phi$. Give an example to show that $I\phi$ may not be an ideal in S.

8. Prove Theorem 7.10 by using Proposition 7.2.