4. Ring Homomorphisms and Ideals

Definition 4.1. Let $\phi: R \rightarrow S$ be a function between two rings. We say that $\phi$ is a ring homomorphism if for every $a$ and $b \in R$,

$$\phi(a + b) = \phi(a) + \phi(b)$$

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b),$$

and in addition $\phi(1) = 1$.

Note that this gives us a category, the category of rings. The objects are rings and the morphisms are ring homomorphisms. Just as in the case of groups, one can define automorphisms.

Example 4.2. Let $\phi: \mathbb{C} \rightarrow \mathbb{C}$ be the map that sends a complex number to its complex conjugate. Then $\phi$ is an automorphism of $\mathbb{C}$. In fact $\phi$ is its own inverse.

Let $\phi: R[x] \rightarrow R[x]$ be the map that sends $f(x)$ to $f(x + 1)$. Then $\phi$ is an automorphism. Indeed the inverse map sends $f(x)$ to $f(x - 1)$.

By analogy with groups, we have

Definition 4.3. Let $\phi: R \rightarrow S$ be a ring homomorphism. The kernel of $\phi$, denoted $\ker \phi$, is the inverse image of zero.

As in the case of groups, a very natural question arises. What can we say about the kernel of a ring homomorphism? Since a ring homomorphism is automatically a group homomorphism, it follows that the kernel is a normal subgroup. However since a ring is an abelian group under addition, in fact all subgroups are automatically normal.

Definition-Lemma 4.4. Let $R$ be a ring and let $I$ be a subset of $R$. We say that $I$ is an ideal of $R$ and write $I \triangleleft R$ if $I$ is an additive subgroup of $R$ and for every $a \in I$ and $r \in R$, we have

$$ra \in I \quad \text{and} \quad ar \in I.$$

Let $\phi: R \rightarrow S$ be a ring homomorphism and let $I$ be the kernel of $\phi$. Then $I$ is an ideal of $R$.

Proof. We have already seen that $I$ is an additive subgroup of $R$. Suppose that $a \in I$ and $r \in R$. Then

$$\phi(ra) = \phi(r)\phi(a)$$

$$= \phi(r)0$$

$$= 0.$$

Thus $ra$ is in the kernel of $\phi$. Similarly for $ar$. \qed
As before, given an additive subgroup $H$ of $R$, we let $R/H$ denote the group of left cosets of $H$ in $R$.

**Proposition 4.5.** Let $R$ be a ring and let $I$ be an ideal of $R$, such that $I \neq R$.

Then $R/I$ is a ring. Furthermore there is a natural ring homomorphism

$$u: R \rightarrow R/I$$

which sends $a$ to $a + I$.

**Proof.** As $I$ is an ideal, and addition in $R$ is commutative, it follows that $R/I$ is a group, with the natural definition of addition inherited from $R$. Further we have seen that $u$ is a group homomorphism. It remains to define a multiplication in $R/I$.

Given two left cosets $a + I$ and $b + I$ in $R/I$, we define multiplication in the obvious way,

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

In fact this is forced by requiring that $u$ be a ring homomorphism.

As before the problem is to check that this is well-defined. Suppose that $a' + I = a + I$ and $b' + I = b + I$. Then we may find $i$ and $j$ in $I$ such that $a' = a + i$ and $b' = b + j$. We have

$$a'b' = (a + i)(b + j) = ab + ia + bj + ij.$$ 

As $I$ is an ideal, $ia + bj + ij \in I$. It follows that $a'b' + I = ab + I$ and multiplication is well-defined. The rest is easy to check. \qed

As before the quotient of a ring by an ideal is a categorical quotient.

**Theorem 4.6.** Let $R$ be a ring and $I$ an ideal not equal to all of $R$. Let $u: R \rightarrow R/I$ be the natural map. Then $u$ is universal amongst all ring homomorphisms whose kernel contains $I$.

That is, suppose $\phi: R \rightarrow S$ is any ring homomorphism, whose kernel contains $I$. Then there is a unique ring homomorphism $\psi: R/I \rightarrow S$, which makes the following diagram commute,
Proof. Since $\phi$ is a group homomomorphism the existence and uniqueness of the induced map $\psi$ is clear; this follows by invoking the universal property of $R/I$ as a categorical group quotient. From there it is straightforward to check that $\psi$ is a ring homomorphism. \hfill $\Box$

**Theorem 4.7** (Isomorphism Theorem). Let $\phi: R \to S$ be a homomorphism of rings. Suppose that $\phi$ is onto and let $I$ be the kernel of $\phi$.

Then $S$ is isomorphic to $R/I$.

**Example 4.8.** Let $R = \mathbb{Z}$. Fix a non-zero integer $n$ and let $I$ consist of all multiples of $n$. It is easy to see that $I$ is an ideal of $\mathbb{Z}$. The quotient, $\mathbb{Z}/I$ is $\mathbb{Z}_n$ the ring of integers modulo $n$.

**Definition-Lemma 4.9.** Let $R$ be a commutative ring and let $a \in R$ be an element of $R$.

The set

$$I = \langle a \rangle = \{ ra \mid r \in R \},$$

is an ideal and any ideal of this form is called **principal**.

**Proof.** We first show that $I$ is an additive subgroup.

Suppose that $x$ and $y$ are in $I$. Then $x = ra$ and $y = sa$, where $r$ and $s$ are two elements of $R$. In this case

$$x + y = ra + sa$$

$$= (r + s)a.$$  

Thus $I$ is closed under addition. Further $-x = -ra = (-r)a$, so that $I$ is closed under inverses. It follows that $I$ is an additive subgroup.

Now suppose that $x \in I$ and that $s \in R$. Then

$$sx = s(ra)$$

$$= (sr)a \in I.$$  

It follows that $I$ is an ideal. \hfill $\Box$

**Definition-Lemma 4.10.** Let $R$ be a ring. We say that $u \in R$ is a **unit**, if $u$ has a multiplicative inverse.

Let $I$ be an ideal of a ring $R$. If $I$ contains a unit, then $I = R$.

**Proof.** Suppose that $u \in I$ is a unit of $R$. Then $vu = 1$, for some $v \in R$. It follows that

$$1 = vu \in I.$$  

Pick $a \in R$. Then

$$a = a \cdot 1 \in I.$$  

$\Box$
Proposition 4.11. Let \( R \) be a division ring. Then the only ideals of \( R \) are the zero ideal and the whole of \( R \). In particular if \( \phi: R \rightarrow S \) is any ring homomorphism then \( \phi \) is injective.

Proof. Let \( I \) be an ideal, not equal to \( \{0\} \). Pick \( u \in I, u \neq 0 \). As \( R \) is a division ring, it follows that \( u \) is a unit. But then \( I = R \).

Now let \( \phi: R \rightarrow S \) be a ring homomorphism and let \( I \) be the kernel. Then \( I \) cannot be the whole of \( R \), so that \( I = \{0\} \). But then \( \phi \) is injective. \( \Box \)

Example 4.12. Let \( X \) be a set and let \( R \) be a ring. Let \( F \) denote the set of functions from \( X \) to \( R \). We have already seen that \( F \) forms a ring, under pointwise addition and multiplication.

Let \( Y \) be a subset of \( X \) and let \( I \) be the set of those functions from \( X \) to \( R \) whose restriction to \( Y \) is zero.

Then \( I \) is an ideal of \( F \). Indeed \( I \) is clearly non-empty as the zero function is an element of \( I \). Given two functions \( f \) and \( g \) in \( F \), whose restriction to \( Y \) is zero, then clearly the restriction of \( f + g \) to \( Y \) is zero. Finally, suppose that \( f \in I \), so that \( f \) is zero on \( Y \) and suppose that \( g \) is any function from \( X \) to \( R \). Then \( gf \) is zero on \( Y \). Thus \( I \) is an ideal.

Now consider \( F/I \). I claim that this is isomorphic to the space of functions \( G \) from \( Y \) to \( R \). Indeed there is a natural map from \( F \) to \( G \) which sends a function to its restriction to \( Y \),

\[
f \rightarrow f|_Y
\]

It is clear that the kernel is \( I \). Thus the result follows by the Isomorphism Theorem. As a special case, one can take \( X = [0,1] \) and \( R = \mathbb{R} \). Let \( Y = \{1/2\} \). Then the space of maps from \( Y \) to \( \mathbb{R} \) is just a copy of \( \mathbb{R} \).

Example 4.13. Let \( R \) be the ring of Gaussian integers, that is, those complex numbers of the form \( a + bi \), where \( a \) and \( b \) are integers.

Let \( I \) be the subset of \( R \) consisting of those numbers such \( 2|a \) and \( 2|b \). I claim that \( I \) is an ideal of \( R \). In fact suppose that \( a + bi \in I \) and \( c + di \in I \). Then

\[
(a + bi) + (c + di) = (a + c) + (b + d)i.
\]

As \( a \) and \( c \) are even, then so is \( a + c \) and similarly as \( b \) and \( d \) are even, then so is \( b + d \).

Thus \( I \) is an additive subgroup. On the other hand, if \( a + bi \in I \) and \( c + di \in R \) then

\[
(c + di)(a + bi) = (ac - bd) + (bc + ad)i.
\]
By assumption $a$ and $b$ are even. It is easy to see that $ac - bd$ and $bc + ad$ are even, so that the product is in $I$ and so $I$ is an ideal.