16. Ring Homomorphisms and Ideals

Definition 16.1. *Let $\phi\colon R \longrightarrow S$ be a function between two rings. We say that ϕ 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 16.2. *Let $\phi\colon \mathbb{C} \longrightarrow \mathbb{C}$ be the map that sends a complex number to its complex conjugate. Then ϕ is an automorphism of $\mathbb{C}$. In fact ϕ is its own inverse.*

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

By analogy with groups, we have

Definition 16.3. *Let $\phi\colon R \longrightarrow S$ be a ring homomorphism.*

The **kernel** *of ϕ, denoted $\operatorname{Ker}\phi$, 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 16.4. *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 a an additive subgroup of R and for every $a \in I$ and $r \in R$, we have*

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

Let $\phi\colon R \longrightarrow S$ be a ring homormphism and let I be the kernel of ϕ. 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

$$\begin{aligned}\phi(ra) &= \phi(r)\phi(a)\\ &= \phi(r)0\\ &= 0.\end{aligned}$$

Thus ra is in the kernel of ϕ. Similarly for ar. □

As before, given an additive subgroup H of R, we let R/H denote the group of left cosets of H in R.

Proposition 16.5. *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

$$u \colon R \longrightarrow R/I$$

which sends r to $r + I$.

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 ϕ is a group homomorphism. It remains to define a multiplication in R/I.

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

$$(r + I)(s + I) = rs + I.$$

In fact this is forced by requiring that u is a ring homorphism.

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

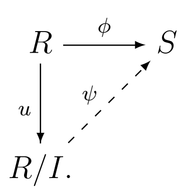
$$\begin{aligned} r's' &= (r + i)(s + j) \\ &= rs + is + rj + ij. \end{aligned}$$

As I is an ideal, $is + rj + ij \in I$. It follows that $r's' + I = rs + I$ and multiplication is well-defined. The rest is easy to check. $\square$

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

Theorem 16.6. *Let R be a ring and I an ideal not equal to all of R. Let $u \colon R \longrightarrow R/I$ be the obvious map. Then u is universal amongst all ring homomorphisms whose kernel contains I.*

That is, suppose $\phi \colon R \longrightarrow S$ is any ring homomorphism, whose kernel contains I. Then there is a unique ring homomomorphism $\psi \colon R/I \longrightarrow S$, which makes the following diagram commute,



Theorem 16.7. *(Isomorphism Theorem) Let $\phi \colon R \longrightarrow S$ be a homomorphism of rings. Suppose that ϕ is onto and let I be the kernel of ϕ.*

Then S is isomorphic to R/I.

Example 16.8. *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 16.9. *Let R be a commutative ring and let $a \in R$ be an element of R.*

The set

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

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

$$\begin{aligned} x + y &= ra + sa \\ &= (r + s)a. \end{aligned}$$

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

$$\begin{aligned} sx &= s(ra) \\ &= (sr)a \in I. \end{aligned}$$

It follows that I is an ideal. □

Definition-Lemma 16.10. *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

$$a = a \cdot 1 \in I.$$ □

Proposition 16.11. *Let R be a division ring. Then the only ideals of R are the zero ideal and the whole of R. In particular if $\phi\colon R \longrightarrow S$ is any ring homomorphism then ϕ is injective.*

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

Now let $\phi\colon R \longrightarrow S$ be a ring homomorphism and let I be the kernel. Then I cannot be the whole of R, so that $I = \{0\}$. But then ϕ is injective. □

Example 16.12. *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,

$$f \longrightarrow f|_Y.$$

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 16.13. *Let R be the ring of Gaussian integers, that is, those complex numbers of the form $a + bi$.*

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 closed under addition. Similarly I is closed under inverses.

Now suppose that $a + bi \in I$ and $r = c + di$ is a Gaussian integer. Then

$$(c + di)(a + bi) = (ac - bd) + (ad + bc)i.$$

As a and b are even, so are $ac - bd$ and $ad + bc$ and so I is an ideal.