18. Ideals and Quotient Rings

The theory of ideals and quotient rings parallels the theory of normal subgroups and quotient groups. We start with the basic properties:

Proposition 18.1. *Let $\phi\colon R \longrightarrow R'$ be a homomorphism of rings*

1. *If $0 \in R$ is the additive identity then $\phi(0) \in R'$ is the additive identity in R'.*
2. *If $a \in R$ then $\phi(-a) = -\phi(a)$.*
3. *If S is a subring of R then $\phi[S]$ is a subring of R'.*
4. *If S' is a subring of R' then $\phi^{-1}[S']$ is a subring of R.*
5. *If R has unity 1 then $\phi(1)$ is unity in $\phi[R]$.*

Proof. As ϕ is a ring homomorphism it is a group homomorphism of the underlying additive groups. (1) and (2) follow from the case of groups homomorphisms.

For (3) we already know that $\phi[S]$ is an an additive subgroup of R'. If $\phi(a)$ and $\phi(b) \in \phi[S]$ then

$$\phi(a)\phi(b) = \phi(ab) \in \phi[S].$$

Thus $\phi[S]$ is closed under multiplication and so $\phi[S]$ is a subring of R'. This is (3).

For (4) we already know that $\phi^{-1}[S']$ is an an additive subgroup of R. If a and $b \in \phi^{-1}[S]$ then $\phi(a)$ and $\phi(b) \in S'$ and we have

$$\phi(ab) = \phi(a)\phi(b) \in \phi^{-1}[S'].$$

It follows that $ab \in \phi^{-1}[S']$. Thus $\phi^{-1}[S']$ is closed under multiplication and so $\phi^{-1}[S']$ is a subring of R. This is (4).

Now suppose that $\phi(a) \in \phi[R]$. Then

$$\begin{aligned} \phi(1)\phi(a) &= \phi(1a) \\ &= \phi(a). \end{aligned}$$

Thus $\phi(1)$ acts as unity in $\phi[R]$. This is (5). $\square$

We recall the definition of the kernel.

Definition 18.2. *If $\phi\colon R \longrightarrow R'$ is a homomorphism of rings then the subring*

$$\phi^{-1}[0'] = \{\, r \in R \mid \phi(r) = 0' \,\}$$

is called the ***kernel*** *of ϕ, denoted $\operatorname{Ker}\phi$.*

Proposition 18.3. *If $\phi\colon R \longrightarrow R'$ is a homomorphism of rings and $H = \operatorname{Ker}\phi$ is the kernel then*

$$\phi^{-1}[\phi(a)] = a + H.$$

Proof. Immediate since ϕ is a group homomorphism. □

Corollary 18.4. *A homomorphism of rings $\phi\colon R \longrightarrow R'$ is a one to one if and only if* $\operatorname{Ker}\phi = \{0\}$.

Proof. Immediate since ϕ is a group homomorphism. □

Theorem 18.5 (First isomorphism theorem)**.** *Let $\phi\colon R \longrightarrow R'$ be a ring homomorphism with kernel H.*

Then R/H, the set of left cosets under addition, is a ring, with the following addition and multiplication:

$$(a+H)+(b+H) = a+b+H \qquad \textit{and} \qquad (a+H)(b+H) = ab+H.$$

Furthermore the map

$$\mu\colon R/H \longrightarrow \phi[R] \qquad \textit{given by} \qquad \mu(a+H) = \phi(a),$$

is an isomorphism.

Proof. As usual, we only need to check the new part, the part which relates to multiplication.

The key is to check that the given rule for multiplication is well-defined. Suppose that

$$a_1 + H = a + H \qquad \text{and} \qquad b_1 + H = b + H.$$

Then $a_1 = a + h_1$ and $b_1 = b + h_2$ for some h_1 and $h_2 \in H$. Consider the product

$$\begin{aligned} c_1 &= a_1 b_1 \\ &= (a+h_1)(b+h_2) \\ &= ab + ah_2 + h_1 b + h_1 h_2. \end{aligned}$$

We have to show that c_1 belongs to the same left coset as ab. If we apply ϕ to both sides we get

$$\begin{aligned} \phi(c_1) &= \phi(ab + ah_2 + h_1 b + h_1 h_2) \\ &= \phi(c) + \phi(a)\phi(h_2) + \phi(h_1)\phi(b) + \phi(h_1)\phi(h_2) \\ &= \phi(c) + \phi(a)0 + 0\phi(b) + 00 \\ &= \phi(c). \end{aligned}$$

Thus $\phi(c_1 - c) = 0$ so that $c_1 - c \in H$ and so $a_1 b_1 + H = ab + H$.

The fact that multiplication is associative and satisfies the distributive now follows easily.

We already know that μ is well-defined, it is one to one, onto $\phi[R]$ and a group homomorphism. We only have to check that μ respects multiplication. This is again standard:

$$\begin{aligned}\mu((a+H)(b+H)) &= \mu(ab+H)\\ &= \phi(ab)\\ &= \phi(a)\phi(b)\\ &= \mu(a+H)\mu(b+H).\end{aligned}$$ □

It is natural to try to isolate the key property of the kernel that makes all of this work. We already understand that the kernel has to be a normal subgroup for the set of left cosets R/H to be a group under addition. The proof of (18.5) suggests that we should require also that if $h \in H$ then ah and hb belong to H for any a and b.

Lemma 18.6. *Let H be a subring of the ring R.*

Then the rule

$$(a+H)(b+H) = ab+H$$

gives a well-defined multiplication if and only if ah and hb belong to H for all a and b in R and $h \in H$.

Proof. Suppose first that ah and hb belong to H for all a and b in R and $h \in H$.

Suppose that $a_1 + H = a + H$ and $b_1 + H = b + H$. Then we may find h_1 and h_2 such that $a_1 = a + h_1$ and $b_1 = b + h_2$. Let $c_1 = a_1 b_1$ and $c = ab$. The fact that multiplication is well-defined is equivalent to saying that c_1 lies in the same left coset as c.

We check this:

$$\begin{aligned}c_1 &= a_1 b_1\\ &= (a+h_1)(b+h_2)\\ &= ab + ah_2 + h_1 a_1 + h_1 h_2.\end{aligned}$$

Now ah_2, $h_1 b$ and $h_1 h_2$ belong to H (the third product for two reasons). Thus the sum $h = ah_2 + h_1 a_1 + h_1 h_2$ belongs to H. Therefore $c_1 = c + h$ so that $c_1 + H = c + H$. Hence the given rule of multiplication is well-defined.

Conversely suppose that the given rule of multiplication is well-defined. Pick $a \in H$ and consider the product $(a+H)H$. The standard way to compute this product is:

$$\begin{aligned}(a+H)H &= (a+H)(0+H)\\ &= a0 + H\\ &= 0 + H\\ &= H.\end{aligned}$$

But if $h \in H$ then we can also compute this product as:

$$\begin{aligned}(a+H)H &= (a+H)(h+H)\\ &= ah+H.\end{aligned}$$

For the product to be well-defined we must have $ah + H = H$, that is, $ah \in H$.

By symmetry we must have $bh \in H$, computing the product $H(b+H)$. □

Definition 18.7. *An* ***ideal*** *I in a ring R is an additive subgroup such that*

$$aI \subset I \qquad \textit{and} \qquad Ib \subset I,$$

for all a and $b \in R$.

Example 18.8. *$n\mathbb{Z}$ is an ideal.*

We already know it is an additive subgroup. As

$$a(rn) = (ra)n \in n\mathbb{Z} \qquad \text{and} \qquad (rn)b = (rb)n \in n\mathbb{Z}$$

it is also an ideal.

Example 18.9. *Let F be the ring of all functions from $\mathbb{R}$ to $\mathbb{R}$ and let C be the subring of all constant functions. Then C is not an ideal.*

Indeed, $2 \in C$ is a constant function and e^x belongs to F but $2e^x$ is not a constant function.

Example 18.10. *Let F be the ring of all functions from $\mathbb{R}$ to $\mathbb{R}$ and let I be the subring of all functions which vanish at -3. Then I is an ideal.*

Suppose that $f(x) \in I$ and $g(x) \in F$. Then

$$\begin{aligned}(fg)(-3) &= f(-3)g(-3)\\ &= 0g(-3)\\ &= 0.\end{aligned}$$

Thus I is an ideal.

Corollary 18.11. *Let R be a ring and let I be an ideal.*

Then R/I is a ring with the following addition and multiplication:

$$(a+H)+(b+H) = a+b+H \qquad \textit{and} \qquad (a+H)(b+H) = ab+H.$$

Definition 18.12. *The ring R/I above is called the* ***quotient ring****.*

Theorem 18.13. *Let R be a ring and let I be an ideal.*

Then the natural map

$$\gamma\colon R \longrightarrow R/I \qquad \text{given by} \qquad r \longrightarrow r + I,$$

is a ring homomorphism with kernel I.

Proof. The only thing to check is that γ respects multiplication:

$$\begin{aligned}\gamma(xy) &= xy + I \\ &= (x + I)(y + I) \\ &= \gamma(x)\gamma(y).\end{aligned}$$

□

As before, putting all of this together we get:

Theorem 18.14 (First isomorphism theorem)**.** *Let $\phi\colon R \longrightarrow R'$ be a ring homomorphism with kernel I. Then $\phi[R]$ is a ring and the map*

$$\mu\colon R/I \longrightarrow \phi[R] \qquad \text{given by} \qquad \gamma(r + I) = \phi(r)$$

is an isomorphism. If the map

$$\gamma\colon R \longrightarrow R/I \qquad \text{is given by} \qquad \gamma(r) = r + I$$

then $\phi(r) = \mu(\gamma(r))$.