3.3 Factor Rings

Suppose that R is a ring and that I is a (two-sided) ideal of R. Then we can use R and I to create a new ring, called "the factor ring of R modulo I". This ring is denoted R/I (read "R mod I"), and its elements are certain subsets of R associated to I. The most well known examples are the rings $\mathbb{Z}/n\mathbb{Z}$, created from the ring $\mathbb{Z}$ of integers and its ideals.

Definition 3.3.1 *Let R be a ring and let I be a (two-sided) ideal of R. If $a \in R$, the* coset *of I in R determined by a is defined by*

$$a + I = \{a + r : r \in I\}.$$

Thus $a + I$ is a subset of R; it consists of all those elements of R that differ from a by an element of I. Note that $a + I$ does not generally have algebraic structure in its own right, it is typically not closed under the addition or multiplication of R. We will show that the set of cosets of I in R is itself a ring, with addition and multiplication defined in terms of the operations of R.

NOTES

1. $a + I$ is a coset of the subgroup $(I, +)$ of the additive group of R.

2. Suppose $R = \mathbb{Z}$ and $I = \langle 5 \rangle = 5\mathbb{Z}$. Then

$$2 + I = \{2 + 5n,\ n \in \mathbb{Z}\} = \{\dots, -3, 2, 7, 12, \dots\}.$$

   This is the congruence class of 2 modulo 5. So in $\mathbb{Z}$, the cosets of $n\mathbb{Z}$ in Z are the congruence classes modulo n - there is a finite number n of them and each has exactly one representative in the range $0, \dots, n-1$ (this is guaranteed by the division algorithm in $\mathbb{Z}$).

3. Let F be a field and let I be an ideal in $F[x]$. Then $I = \langle f(x) \rangle$ for some polynomial $f(x)$, by Lemma 3.2.3. If $g(x) \in F[x]$ then the coset $g(x) + I$ contains all those polynomials that differ from $g(x)$ by a multiple of $f(x)$.

   If F is infinite then the number of cosets of I in $F[x]$ is infinite but each has exactly one representative of degree less than that of $f(x)$.

   QUESTION FOR THE SEMINAR: Why is this?

   If F is finite (e.g. $F = \mathbb{Z}/p\mathbb{Z}$ for some prime p), then the number of cosets of I in $F[x]$is finite.

Lemma 3.3.2 *Let a and b be elements of a ring R in which I is a two-sided ideal. Then*

(i) If $a - b \in I$, $a + I = b + I$.

(ii) If $a - b \notin I$, *the cosets* $a + I$ *and* $b + I$ *are disjoint subsets of* R.

Proof: (i): Suppose $a - b \in I$ and let $x \in a + I$. Then $x = a + m$ for some $m \in I$ and we can write

$$x = a - b + b + m = b + (a - b) + m.$$

Since $a - b \in I$ and $m \in I$ this means $(a - b) + m \in I$ and so $x \in b + I$. Thus $a + I \subseteq b + I$.
Now $a - b$ belongs to I and so $b - a = -(a - b)$ does also. It then follows from the above argument that $b + I \subseteq a + I$. Thus $a + I = b + I$.

(ii) Suppose $a - b \notin I$ and let $c \in (a + I) \cap (b + I)$. Then

$$c = a + m_1 = b + m_2$$

where $m_1, m_2 \in I$. It follows that $a - b = m_2 - m_1$ which is a contradiction since $a - b \notin I$. □

Lemma 3.3.2 shows that the different cosets of I in R are disjoint subsets of R. We note that their union is all of R since every element a of R belongs to *some* coset of I in R : $a \in a + I$. The set of cosets of I in R is denoted R/I. We can define addition and multiplication in R/I as follows.
Let $a + I$, $b + I$ be cosets of I in R. We define their *sum* by

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

Claim: This addition is well-defined.

QUESTION FOR THE SEMINAR: What is this claim saying? Why is there doubt about the definition of addition given above?

What the claim is concerned with is the following : if $a + I = a_1 + I$ and $b + I = b_1 + I$, how do we know that $(a + b) + I = (a_1 + b_1) + I$? How do we know that the coset sum $(a + I) + (b + I)$ as defined above does not depend on the choice a and b of representatives of these cosets to be added in R?

PROOF OF CLAIM: Suppose

$$a + I = a_1 + I \text{ and } b + I = b_1 + I$$

for elements a_1, b_1 of R. Then $a - a_1 \in I$ and $b - b_1 \in I$, by Lemma 3.3.2. Hence $(a - a_1) + (b - b_1) = (a + b) - (a_1 + b_1)$ belongs to I. Thus

$$(a + b) + I = (a_1 + b_1) + I,$$

by Lemma 3.3.2 again.

Multiplication in R/I is defined by

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

for cosets $a + I$ and $b + I$ of I in R.

Claim: Multiplication is well-defined in R/I
(i.e. the coset $ab + I$ does not depend on the choice of representatives of $a + I$ and $b + I$).

PROOF OF CLAIM: Suppose that

$$a + I = a_1 + I \text{ and } b + I = b_1 + I$$

for elements a_1, b_1 of R. Then $a - a_1 \in I$ and $b - b_1 \in I$, by Lemma 3.3.2. We need to show that

$$ab + I = a_1 b_1 + I.$$

By Lemma 3.3.2, this means showing that $ab - a_1 b_1 \in I$. To see this observe that

$$\begin{aligned} ab - a_1 b_1 &= ab - a_1 b + a_1 b - a_1 b_1 \\ &= (a - a_1)b + a_1(b - b_1). \end{aligned}$$

Now since I is a two-sided ideal we know that $(a - a_1)b \in I$ and $a(b - b_1) \in I$. Thus

$$(a - a_1)b + a_1(b - b_1) = ab - a_1 b_1 \in I,$$

and this proves the claim. □

That addition and multiplication in R/I satisfy the ring axioms follows easily from the fact that these axioms are satisfied in R. The ring R/I, with addition and multiplication defined as above, is called the *factor ring* "R modulo "I".

NOTES:

1. The zero element of R/I is the coset $0_R + I = I$.
2. It is clear that R/I has some properties in common with R. For example
   - R/I is commutative if R is commutative.
   - If R contains an identity element 1_R for multiplication, then $1_R + I$ is an identity element for multiplication in R/I
   - If u is a unit in R with inverse u^{-1}, then $u + I$ is a unit in R/I, with inverse $u^{-1} + I$.
3. However, R/I can be structurally quite different from R. For example, R/I can contain zero-divisors, even if R does not. It is also possible for R/I to be a field if R is not.
   QUESTION FOR THE SEMINAR: Find examples of both of these phenomena.

In the next section we will look at conditions on I under which R/I is an integral domain or a field, for a commutative ring R.
Our final goal in this section is to prove the *Fundamental Homomorphism Theorem* for rings, which states that if $\phi : R \longrightarrow S$ is a ring homomorphism, then the image of ϕ is basically a copy of the factor ring $R/\ker\phi$.

Definition 3.3.3 *Let $\phi : R \longrightarrow S$ be a ring homomorphism. Then ϕ is called an isomorphism if*

1. *ϕ is surjective (onto); i.e.* $\mathrm{Im}\phi = S$*, and*
2. *ϕ is injective (one-to-one) i.e. $\phi(r_1) \neq \phi(r_2)$ whenever $r_1 \neq r_2$ in R.*

NOTE: ϕ is injective if and only if $\ker\phi$ is the zero ideal of R.
To see this first suppose ϕ is injective. Then $\ker\phi = \{0_R\}$, otherwise if $r \in \ker\phi$ for some $r \neq 0$ we would have $\phi(r) = \phi(0_R)$, contrary to the injectivity of ϕ.
On the other hand suppose $\ker\phi = \{0_R\}$. Then if there exist elements r_1 and r_2 of R with $\phi(r_1) = \phi(r_2)$ we must have $\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) = 0_S$. This means $r_1 - r_2 \in \ker\phi$, so $r_1 - r_2 = 0_R$ and ϕ is injective.

The characterisation of injectivity in the above note can be very useful.

If $\phi : R \longrightarrow S$ is an isomorphism, then S is an "exact copy" of R. This means that S and R are structurally identical, and only differ in the way their elements are labelled. We say that R and S are *isomorphic* and write $R \cong S$.

Theorem 3.3.4 *(The Fundamental Homomorphism Theorem) Let $\phi : R \longrightarrow S$ be a homomorphism of rings. Then the image of ϕ is isomorphic to the factor ring $R/\ker\phi$.*

Proof: Let I denote the kernel of ϕ, so I is a two-sided ideal of R. Define a function $\bar{\phi} : R/I \longrightarrow \mathrm{Im}\phi$ by

$$\bar{\phi}(a + I) = \phi(a) \text{ for } a \in R.$$

1. $\bar{\phi}$ is well-defined (i.e. the image of $a + I$ does not depend on a choice of coset representative). Suppose that $a + I = a_1 + I$ for some $a, a_1 \in R$. Then $a - a_1 \in I$ by Lemma 3.3.2. Hence $\phi(a - a_1) = 0_S = \phi(a) - \phi(a_1)$. Thus $\phi(a) = \phi(a_1)$ as required.

2. $\bar{\phi}$ is a ring homomorphism.
   Suppose $a + I, b + I$ are elements of R/I. Then

$$\begin{aligned} \bar{\phi}\left((a + I) + (b + I)\right) &= \bar{\phi}\left((a + b) + I\right) \\ &= \phi(a + b) \\ &= \phi(a) + \phi(b) \\ &= \bar{\phi}(a + I) + \bar{\phi}(b + I). \end{aligned}$$

So ϕ is additive.

Also

$$\begin{aligned} \bar{\phi}\left((a+I)(b+I)\right) &= \bar{\phi}(ab+I) \\ &= \phi(ab) \\ &= \phi(a)\phi(b) \\ &= \bar{\phi}(a+I)\bar{\phi}(b+I). \end{aligned}$$

So $\bar{\phi}$ is multiplicative - $\bar{\phi}$ is a ring homomorphism.

3. $\bar{\phi}$ is injective.
   Suppose $a + I \in \ker \bar{\phi}$. Then $\bar{\phi}(a+I) = 0_S$ so $\phi(a) = 0_S$. This means $a \in \ker \phi$, so $a \in I$. Then $a + I = I = 0_R + I$, $a + I$ is the zero element of R/I. Thus $\ker \bar{\phi}$ contains only the zero element of R/I.

4. $\bar{\phi}$ is surjective.
   Let $s \in \mathrm{Im}\phi$. Then $s = \phi(r)$ for some $r \in R$. Thus $s = \bar{\phi}(r+I)$ and every element of $\mathrm{Im}\phi$ is the image under $\bar{\phi}$ of some coset of I in R.

Thus $\bar{\phi} : R/\ker\phi \longrightarrow \mathrm{Im}\phi$ is a ring isomorphism, and $\mathrm{Im}\phi$ is isomorphic to the factor ring $R/\ker\phi$. □