Arkansas Tech University
MATH 4033: Elementary Modern Algebra
Dr. Marcel B. Finan

26 Ideals and Quotient Rings

In this section we develop some theory of rings that parallels the theory of groups discussed in ealrier sections of the book. We shall see that the concept of an **ideal** in a ring is analogous to that of a normal subgroup in a group. Using ideals we will construct quotient rings.

Definition 26.1
A subring I of a ring R is an **ideal** *if whenever $r \in R$ and $a \in I$, then $ra \in I$ and $ar \in I$.*

Example 26.1
1. The subrings $I = \{0\}$ and $I = R$ are always ideals of a ring R.
2. The set E of even integers is an ideal of $\mathbb{Z}$.
3. The set $I = \{[0], [2], [4]\}$ is an ideal of $\mathbb{Z}_6$.■

Remark 26.1
Note that if R is a ring with unity element e and I is an ideal of R then from the above definition, for any $r \in R$ we have $re = er = r \in I$. That is, $R = I$.

Example 26.1(1) can be generalized to the set of all multiples of any fixed integer n as shown in the next lemma.

Lemma 26.1
Let R be a commutative ring with unity element e. The set

$$(a) = \{ar : r \in R\}$$

is an ideal of R.

Proof.
First, we will show that (a) is a subring of R. Since $a = ae$ then $a \in (a)$ and so $(a) \neq \emptyset$. Let $ax \in (a)$ and $ay \in (a)$. Then $ax - ay = a(x - y) \in (a)$ since $x - y \in R$. Thus, $ax - ay \in (a)$. Also, $(ax)(ay) = a(xy) \in (a)$ since $xy \in R$. Thus, by Theorem 25.4, (a) is a subring of R. Finally, for any $ar \in (a)$ and all $t \in R$ we have $t(ar) = t(ra) = (tr)a \in (a)$ and $(ar)t = a(rt) = (rt)a \in (a)$. Thus, (a) is an ideal of R.

Definition 26.2
Let R be a commutative ring with unity and $a \in R$. Then the ideal (a) is called the **principal ideal** *generated by a in R.*

Theorem 26.1
Every ideal in the ring $\mathbb{Z}$ is a principal ideal.

Proof.
Let I be an ideal in R. If $I = \{0\}$ then there is nothing to prove since $\{-\} = (0)$. So assume that $I \neq \{0\}$. Since $I \neq \{0\}$ then there exists an $m \in I$ such that $m \neq 0$. Since I is an ideal and $-1 \in \mathbf{Z}$ then $-m \in I$. Thus, both m and $-m$ belong to I so that I contains positive integers. Let $M = \{m \in I : m > 0\}$. By Theorem 10.1, M contains a smallest element, call it n.
Now, for any $k \in I$, by the Division algorithm there exist integers q and r such that

$$k = nq + r \quad 0 \leq r < n.$$

Thus, $r = k - nq$. Since I is a subring of R then by closure $r \in I$. By the definition of n we must have $r = 0$. This implies that $k = nq$ and so $I \subseteq (n)$. Since $(n) \subseteq I$ then we conclcude that $I = (n)$. This establsihes a proof of the theorem.■

In analogy to congruence in $\mathbf{Z}$ and $\mathbf{Z}_n = \mathbf{Z}/ < n >$ we now will build a ring R/I for any ideal I in any ring R. For $a, b \in R$, we say a is *congruent to b modulo I* [and write $a \equiv b(mod\ I)$] if and only if $a - b \in I$. Note that when $I = (n) \subseteq \mathbf{Z}$ is the principal ideal generated by n, then $a - b \in I \iff n|(a - b)$, so this is our old notion of congruence.

Theorem 26.2
Let I be an ideal of a ring R. Then congruence modulo I is an equivalence relation on R. For any $a \in R$ we have

$$[a] = \{r \in R : a \equiv r(mod\ I)\} = \{a + i : i \in I\}.$$

Proof.
Reflexive: $a - a = 0 \in I$ since I is a subring.
Symmetric: Assume that $a \equiv b(mod\ I)$. Then $a - b \in I$. Since I is a subring, its additive inverse, $b - a$ is also in I, so $b \equiv a(mod\ I)$.
Transitive: Assume $a \equiv b(mod\ I)$ and $b \equiv c(mod\ I)$. Then $a - b \in I$ and $b - c \in I$. Hence, by closure, $a - c = (a - b) + (b - c) \in I$. That is, $a \equiv c(mod\ I)$.
Now, for any $a \in R$, the equivalence class of a is the set

$$[a] = \{r \in R : a \equiv r(mod\ I)\}.$$

But $a \equiv r(mod\ I)$ if and only if $a - r \in I$ and this is equivalent to saying that $a - r = i \in I$. That is,

$$[a] = \{a + i : i \in I\}.■$$

We denote the equivalence class of $a \in R$ by $a + I$.

Remark 26.2
Note that by Theorem 9.2, $a \equiv b(mod\ I) \iff a - b \in I \iff a + I = b + I$.

Next, consider the set R/I of all cosets $a + I$ where $a \in R$. On this set, we define addition as follows:

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

Theorem 26.3
The set R/I is an Abelian group with respect to addition.

Proof.
First, we show that addition is well-defined. Suppose that $(a+I, b+I) = (c+I, d+I)$. Then $a+I = c+I$ and $b+I = d+I$. Thus, $a-c \in I$ and $b-d \in I$. By the closure of addition in I we have $(a-c)+(b-d) = (a+b)-(c+d) \in I$. Hence, $(a+b)+I = (c+d)+I$.
Addition is commutative since $(a+I)+(b+I) = (a+b)+I = (b+a)+I = (b+I)+(a+I)$ since addition is R is commutative. Similarly, since addition in R is associative then addition is R/I is associative. The coset I is the zero element and the additive inverse of $a+I$ is $(-a)+I$. Hence, $(R/I, +)$ is an Abelian group.■

In order to turn R/I into a ring we need to introduce a multiplication on R/I. For $a+I \in R/I$ and $b+I \in R/I$ we define

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

Theorem 26.4
(a) R/I is closed with respect to multiplication.
(b) Multiplication is associative.
(c) Multiplication is distributive with respect to addition.

Proof.
(a) Suppose that $(a+I, b+I) = (c+I, d+I)$. Then $a+I = c+I$ and $b+I = d+I$. Thus, $a-c \in I$ and $b-d \in I$. It follows that $a = c+x$ and $b = d+y$ for some $x, y \in I$. Thus, $ab = (c+x)(d+y) = cd+cy+dx+xy$. Since I is an ideal then $cy, dx, xy \in I$. By the closure of addition in I we have $w = cy+dx+xy \in I$. Hence, $ab = cd+w$ with $w \in I$ and this means that $ab-cd \in I$ so that $ab \equiv cd(mod\ I)$ and consequently $ab+I = cd+I$.
(b)Multiplication is associative.

$$\begin{aligned}
(a+I)[(b+I)(c+I)] &= (a+I)(bc+I) \\
&= a(bc)+I \\
&= (ab)c+I \qquad (\textit{since multiplication is associative in } R) \\
&= (ab+I)(c+I) \\
&= [(a+I)(b+I)](c+I)
\end{aligned}$$

(c) We will verify the left distributive law. The proof of the right distributive law is similar.

$$\begin{aligned}
(a+I)[(b+I)+(c+I)] &= (a+I)(b+c+I) \\
&= a(b+c)+I \\
&= ab+ac+I \qquad (\textit{by the distributive law in } R) \\
&= (ab+I)(ac+I) \\
&= (a+I)(b+I)+(a+I)(c+I)\blacksquare
\end{aligned}$$

It follows from Theorem 26.4 and Theorem 26.3 that R/I is a ring.

Definition 26.3
If I is an ideal of a ring R then with the operations of addition and multiplication defined above, R/I is a ring called the **quotient ring** *of R by I.*

Review Problems

Exercise 26.1
Consider the ring

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}.$$

Show that the set

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Z} \right\}.$$

is an ideal of R.

Exercise 26.2
Prove that $x\mathbb{R}[x]$ is an ideal of $\mathbb{R}[x]$.

Exercise 26.3
Show that the set $I_r = \{f \in \mathcal{M}(\mathbb{R}) : f(r) = 0\}$, where $r \in \mathbb{R}$ is fixed, is an ideal of $\mathcal{M}(\mathbb{R})$. Can we replace the 0 by any number and still get an ideal?

Exercise 26.4
Show that the set

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R} \right\}.$$

is not an ideal of the ring of all 2×2 matrices.

Exercise 26.5
Let R be a commutative ring with unity element e. Let $c_1, c_2, \cdots, c_n \in R$. Show that the set $I = \{r_1c_1 + r_2c_2 + \cdots + r_nc_n : r_1, r_2, \cdots, r_n \in R\}$ is an ideal of R.

Exercise 26.6
Let I be an ideal of a ring R. Prove that if $a \equiv b (mod\ I)$ and $c \equiv d (mod\ I)$ then $a + c \equiv b + d (mod\ I)$ and $ac \equiv bd (mod\ I)$.

Exercise 26.7
Prove that every subring of $\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Exercise 26.8
Prove that if R is a commutative ring with unity, and $a \in R$, then (a) is the smallest ideal of R containing a.

Exercise 26.9
Let m and n be nonzero integers. Prove that $(m) \subseteq (n)$ if and only if $n|m$.

Exercise 26.10
An element a in a commutative ring is said to be **nilpotent** *if $a^n = 0$ for some positive integer n. Prove that the set of all nilpotent elements in a commutative ring R is an ideal of R.*

Exercise 26.11
Prove that a nonempty susbet I ofa ring R is an ideal of R if and only if I satisfies:

(i) if $a, b \in I$ then $a - b \in I$;
(ii) if $r \in R$ and $a \in I$ then $ar \in I$ and $ra \in I$.

Exercise 26.12
Let R be a commutatvie ring with unity and I an ideal of R. Prove that the set of all $a \in I$ such that $a^n \in I$ for some $n \in \mathbb{N}$ is an ideal of R.

Exercise 26.13
Prove that an arbitrary intersection of ideals of a ring R is an ideal of R.

Exercise 26.14
Find two ideals I_1 and I_2 of the ring $\mathbf{Z}$ such that $I_1 \cup I_2$ is not an ideal.

Exercise 26.15
An ideal P of a commutative ring R is called **prime** *ideal if $P \neq R$ and if $a, b \in R$ then either $a \in P$ or $b \in P$. Prove that if n is a positive integer then (n) is a prime ideal of $\mathbf{Z}$ if and only if n is prime.*

Exercise 26.16
Prove that if I is an ideal of a ring R then R/I is commutative if and only if $ab - ba \in I$ for all $a, b \in R$.

Exercise 26.17
Prove that if R is commutative and I is an ideal of R then R/I is commutative.

Exercise 26.18
Prove that if R has unity e, then $I + e$ is a unity for R/I.

Exercise 26.19
Assume that R is a commutative ring with unity and $P \neq R$ is an ideal of R. Prove that R is a prime ideal if and only if R/I is an integral domain.

Exercise 26.20
Prove that if I is a subring of a ring R, and the operations of addition and multiplication on the collection of all right cosets R/I are well-defined then I is an ideal of R.