CHAPTER 3

RINGS

In this chapter we introduce another algebraic system called a ring. We will define ring and prove several elementary theorems about rings. Then several examples will be considered in detail before we study subrings and ideals and homomorphisms and isomorphisms.

A ring is, first of all, a nonempty set. However, it differs from a group in that a ring must have two binary operations defined on it instead of just one, as in a group. Each of the binary operations must satisfy certain axioms, and both must satisfy an axiom relating the two binary operations. As will be clear later, these axioms are chosen because of the many concrete examples which satisfy them.

3.1 DEFINITION OF A RING

3.1.1 Definition. *A nonempty set R is said to be a* **ring** *if there are defined on R two binary operations, denoted by $+$ and $\cdot$ and called addition and multiplication, which satisfy the following axioms.*

R1 $a + b \in R$ *for all* $a, b \in R$. *(closure law of addition)*

R2 $(a + b) + c = a + (b + c)$ *for all* $a, b, c \in R$. *(associative law of addition)*

R3 *There exists an element* $0 \in R$ *such that* $0 + a = a$ *for all* $a \in R$. *(existence of additive identity)*

R4 *For each* $a \in R$, *there exists* $x \in R$ *such that* $a + x = 0$. *(existence of additive inverses)*

R5 $a + b = b + a$ *for all* $a, b \in R$. *(commutative law of addition)*

R6 $a \cdot b \in R$ *for all* $a, b \in R$. *(closure law of multiplication)*

R7 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all* $a, b, c \in R$. *(associative law of multiplication)*

R8 $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *and* $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ *for all* $a, b, c \in R$. *(distributive laws)*

Notice that axioms R1–R4 simply state that a ring is a group under the binary operation addition; i.e., if one ignores the binary operation called

multiplication, the set R and the binary operation called addition fulfill the requirements that R be a group. Furthermore, R5 states that R considered as a group with binary operation addition is abelian. Consequently, axioms R1–R5 may be summarized by saying that R is an abelian group with binary operation addition. Axiom R6 is simply a reiteration of the fact that multiplication is a binary operation on R. Axiom R7 states that multiplication is associative. Axiom R8 shows the relationship between addition and multiplication. In particular, R8 states that multiplication is right-distributive and left-distributive over addition.

In view of the above discussion, we can restate the definition of a ring in the following way.

3.1.2 Definition (alternative). *A nonempty set R is said to be a* ***ring*** *if there is defined on R two binary operations $+$ and $\cdot$ such that*

a) *R is an abelian group with respect to $+$,*
b) *$\cdot$ is an associative binary operation on R, and*
c) *$\cdot$ is left- and right-distributive over $+$.*

Let us consider the additive group of R for a moment. We proved in Section 2.2 that the identity element was unique and that each element had a unique inverse. Applying these facts to the additive group of R tells us that the additive identity of R is unique and that each element has a unique additive inverse. We will use the symbol 0 for the unique additive identity of R, and we call 0 the *zero* of the ring R. For each element a of R, its unique inverse will be denoted by $-a$ and will be called "negative a."

The most obvious example of a ring is the set I of integers with the usual addition and multiplication. That the axioms R1–R8 hold for I follows from well-known properties of the addition and multiplication of integers. The zero of the ring is the integer "zero." Another easy example of a ring is the set Q of all rational numbers with the ordinary addition and multiplication.

Compared with the addition on a ring R, the multiplication on R is relatively unknown to us. For instance, the definition of ring does not guarantee the existence of a multiplicative identity; nor does it guarantee the existence of multiplicative inverses. Moreover, the multiplication may not be commutative. Therefore, we consider several special classes of rings.

3.1.3 Definition. *Let R be a ring. We say R is a* ***ring with unity element*** *if there exists $e \in R$ such that $a \cdot e = e \cdot a = a$ for all $a \in R$. If such an element e exists, it is called a* ***unity element*** *of R.*

3.1.4 Definition. *Let R be a ring with unity element. We say R is a* ***division ring*** *if for each nonzero element $a \in R$, there exists an element $x \in R$ such that $a \cdot x = x \cdot a = e$ where e is a unity element of R. If such an x exists, we say x is a* ***multiplicative inverse of a.***

In other words, a ring R with unity element is a *division ring* if each nonzero element of R has a *multiplicative inverse* in R. Observe that in order that the multiplicative inverse of a nonzero element a of R may be discussed, R must have a unity element.

3.1.5 Definition. *Let R be a ring. Then R is said to be a* ***commutative ring*** *if $a \cdot b = b \cdot a$ for all $a, b \in R$.*

If $c \cdot d \neq d \cdot c$ for some pair of elements c, d of a ring R, we say R is a *noncommutative ring*.

The ring I of integers and the ring Q of rational numbers both have a unity element—namely 1. Furthermore, one can easily see that both are commutative. But Q is a division ring, whereas I is not. For any nonzero element a/b of Q, $b/a \in Q$ and $(a/b)(b/a) = (b/a)(a/b) = 1$. On the other hand, $3 \in I$ has no multiplicative inverse in I, so I is not a division ring.

Notice that a commutative ring need not have a unity element and, moreover, a ring with unity element need not be commutative. Examples will be given (Section 3.3) of rings which are commutative and have a unity element, which are noncommutative and have a unity element, which are commutative and do not have a unity element, and which are noncommutative and do not have a unity element. Those examples will establish the complete independence of Definitions 3.1.2 and 3.1.4. It is worthwhile to note also that a division ring need not be commutative.

3.2 SIMPLE PROPERTIES OF A RING

In this section we state and prove some elementary properties of a ring. First of all, we show that, if a ring has a unity element, it is unique. As in Section 2.2, to prove uniqueness of the unity element, we assume that there are two and then prove that they are equal. The details are left as an exercise.

3.2.1 Theorem. *Let R be a ring with unity element. Then the unity element of R is unique.*

Observe that, since a ring need not have a unity element, it was necessary in Theorem 3.2.1 to require that R have a unity element in order to prove that it was unique.

Next we show that if a nonzero element of a ring with unity element has a multiplicative inverse, the multiplicative inverse must be unique. We will follow the same procedure for proving uniqueness that was used before.

3.2.2 Theorem. *Let R be a ring with unity element e and let a be a nonzero element of R which has a multiplicative inverse in R. Then the multiplicative inverse of a is unique.*

Proof. Let s and t be multiplicative inverses of a. Then, by definition of multiplicative inverses,

(1) $$a \cdot s = s \cdot a = e$$

and

(2) $$a \cdot t = t \cdot a = e.$$

Then

$$\begin{aligned} s &= s \cdot e && \text{(definition of unity element)} \\ &= s \cdot (a \cdot t) && \text{(by (2))} \\ &= (s \cdot a) \cdot t && \text{(associative law of multiplication)} \\ &= e \cdot t && \text{(by (1))} \\ &= t \cdot && \text{(definition of unity element)} \end{aligned}$$

Hence $s = t$, so that the multiplicative inverse of a is unique, as asserted.

Since we now know that if an element a of a ring with unity has a multiplicative inverse, it is unique, then we may speak of "the" multiplicative inverse of a. The symbol a^{-1} will be used to denote the unique multiplicative inverse of the element a.

An effort must be made to avoid confusion because of the terminology associated with the two binary operations addition and multiplication defined on a ring. Since there are two binary operations, a ring may have two identities—one for each binary operation. The additive identity will always be denoted by 0 and called the "zero of the ring" and the multiplicative identity will be denoted by either e or 1 and called the "unity element of the ring." Similarly each nonzero element x of a ring may have two inverses. The additive inverse of x is denoted by $-x$ and is called "negative x" or "the negative of x," whereas the multiplicative inverse of x is denoted by x^{-1} and is called "the multiplicative inverse of x." Furthermore, R5 guarantees that the addition of a ring is always commutative; hence, when one speaks of the commutativity or noncommutativity of a ring, one is referring to the multiplication.

3.2.3 Theorem. *Let* 0 *be the zero of a ring* R. *Then*

$$a \cdot 0 = 0 \cdot a = 0$$

for all $a \in R$.

Proof. Let $a \in R$. Then $a = a + 0$. Multiply both sides of this equation on the right by a. Thus

$$a \cdot a = (a + 0) \cdot a = a \cdot a + 0 \cdot a$$

by the right-distributivity of $\cdot$ over $+$. Thus

(1) $$a \cdot a + 0 = a \cdot a + 0 \cdot a.$$

Since R is a group with respect to addition, we can apply Theorem 2.2.2 (Cancellation Law of Addition) to (1). Thus $0 = 0 \cdot a$. That $0 = a \cdot 0$ can be proved in a similar manner.

Theorem 3.2.3 allows us to prove several computational results. For convenience of notation, we will write $a - b$ instead of $a + (-b)$ for elements a, b of a ring.

3.2.4 Theorem. *Let a, b, c be arbitrary elements of a ring R. Then the following are true.*

1) $a \cdot (-b) = -(a \cdot b)$.
2) $(-a) \cdot b = -(a \cdot b)$.
3) $(-a) \cdot (-b) = a \cdot b$.
4) $a \cdot (b - c) = (a \cdot b) - (a \cdot c)$.
5) $(a - b) \cdot c = (a \cdot c) - (b \cdot c)$.

Proof. We will prove (1) and leave the remaining parts as exercises. Note that $-(a \cdot b)$ is the symbol for the unique additive inverse of $a \cdot b$, and observe that

$$\begin{aligned} (a \cdot b) + a \cdot (-b) &= a \cdot (b + (-b)) && \text{(distributive law)} \\ &= a \cdot (0) && \text{(definition of } -b) \\ &= 0. && \text{(Theorem 3.2.3)} \end{aligned}$$

Since addition is commutative in R,

$$a \cdot (-b) + a \cdot b = 0.$$

These two expressions imply that $a \cdot (-b)$ is also an additive inverse of $a \cdot b$. Since the additive inverse of $a \cdot b$ is unique, we must have

$$a \cdot (-b) = -(a \cdot b).$$

3.2.5 Notation. It is quite common to use *juxtaposition* to indicate multiplication; i.e., one may write ab for $a \cdot b$. Furthermore, multiplication will always take preference over addition, so that $ab + ac$ means $(a \cdot b) + (a \cdot c)$. For convenience, these notational conventions will be used throughout the rest of this book. Their value can be seen by comparing (4) and (5) of Theorem 3.2.4 with the same statements when they are expressed in the following form:

4) $a(b - c) = ab - ac$
5) $(a - b)c = ac - bc$.

However, there will be instances when the original notation using $\cdot$ to indicate multiplication is retained for clarity and emphasis.

3.2.6 Exercises

1. Prove Theorem 3.2.1.
2. Use the fact that $0 + 0 = 0$ to obtain a different proof of Theorem 3.2.3.
3. Suppose R is a ring such that $x^2 = x$ for all $x \in R$. Prove that R is commutative.
4. Prove parts (2) through (5) of Theorem 3.2.4.

3.3 EXAMPLES OF RINGS

In this section several examples of rings will be discussed. For each example, the reader should verify that all the axioms R1–R8 for a ring hold; in particular, the zero and the additive inverse should be made explicit. The reader should also answer the following questions with regard to each example. Does the ring have a unity element? What is it? If the ring has a unity element, which elements have multiplicative inverses? Is the ring commutative?

Example 1. Let E be the set of even integers. Let $+$ and $\cdot$ be the ordinary addition and multiplication of integers respectively. Then E is a commutative ring. However E does not have a unity element since there is no even integer e such that $x \cdot e = x$ for all even integers x.

Example 2. Let I be the set of all integers and let n be a fixed positive integer. We have shown that the definition

$$a \equiv b \pmod{n} \qquad \text{if } a - b \text{ is a multiple of } n$$

defines an equivalence relation on I. In Example 2 of Section 2.3, we showed that the integers modulo n

$$I/(n) = \{[0], [1], \ldots, [n-1]\}$$

are an abelian group with addition defined by

$$[m] + [k] = [m + k]$$

for all $[m], [k] \in I/(n)$. The reader should review that work.

Define a multiplication of $I/(n)$ by setting

$$[m] \cdot [k] = [mk]$$

for all $[m], [k] \in I/(n)$. To show that $I/(n)$ is a ring with respect to this addition and multiplication, we need only to show that the multiplication is well defined and associative and that the distributive laws hold. The associativity part is included here, and the rest is left as an exercise.

Let $[m]$, $[k]$, and $[j] \in I/(n)$. Then $[m] \cdot ([k] \cdot [j]) = [m] \cdot [kj] = [m(kj)] = [(mk)j] = [mk] \cdot [j] = ([m] \cdot [k]) \cdot [j]$, proving that the multiplication of $I/(n)$ is associative.

Example 3. Let M denote the set of 2×2 matrices over the ring of integers; i.e., M consists of all symbols of the form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $a, b, c, d \in I$. (See Example 3, Section 2.3.) Recall that two elements

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

of M are equal if and only if $a = e$, $b = f$, $c = g$, and $d = h$. Addition is defined by the formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in M.$$

In Example 3 of Section 2.3, we verified that M is an abelian group with this addition. The additive identity (i.e., the zero) is

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

and the additive inverse of an element

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{of } M \text{ is} \quad \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}.$$

Now define a multiplication of matrices by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in M.$$

Then it is easy to show that this multiplication is associative and that the distributive laws hold. We will show that one distributive law holds and leave to the reader the remainder of the verification that M is a ring with the addition and multiplication defined here. Let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} m & n \\ p & q \end{pmatrix}$$

be arbitrary elements of M. Then

$$\begin{aligned}
&\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left[\begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} m & n \\ p & q \end{pmatrix} \right] \\
&\quad = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e+m & f+n \\ g+p & h+q \end{pmatrix} \\
&\quad = \begin{pmatrix} a(e+m)+b(g+p) & a(f+n)+b(h+q) \\ c(e+m)+d(g+p) & c(f+n)+d(h+q) \end{pmatrix} \\
&\quad = \begin{pmatrix} (ae+am)+(bg+bp) & (af+an)+(bh+bq) \\ (ce+cm)+(dg+dp) & (cf+cn)+(dh+dq) \end{pmatrix} \\
&\quad = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} + \begin{pmatrix} am+bp & an+bq \\ cm+dp & cn+dq \end{pmatrix} \\
&\quad = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} m & n \\ p & q \end{pmatrix},
\end{aligned}$$

proving that multiplication is left-distributive over addition. The ring M has a unity element, namely

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

However, M is not commutative. (Find a counterexample showing M is not commutative.)

The ring I of integers is a commutative ring with unity element; E of Example 1 is commutative but does not have a unity element; and M of Example 3 has a unity element but is not commutative. Furthermore, the set N of all 2×2 matrices over E, i.e., all symbols of the form

$$\begin{pmatrix} r & s \\ u & v \end{pmatrix}$$

where r, s, u, v are *even* integers, with the addition and multiplication as defined in Example 3, is a ring which is not commutative and does not have a unity element. These four examples establish the independence of the notions of commutativity and the existence of a unity element, as was promised in the discussion following Definition 3.1.5.

Example 4. Let R be the set $\{a, b, c, d\}$, and define addition and multiplication by these tables.

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	b	a
c	a	c	c	a
d	a	d	d	a

For example, the product $c \cdot b$ is at the intersection of the row of c and the column of b; hence $c \cdot b = c$.

The verification of the ring axioms is essentially a process of detailed enumeration of possible cases of each of the axioms. In the case of commutativity, either of addition or multiplication, we may check by seeing if the operation table is symmetric with respect to the main diagonal, that is, the diagonal from upper left to lower right. Thus, addition is commutative, as it must be in a ring, while multiplication is not commutative. The additive identity, or zero element, is a. This fact can be used to decrease the number of cases one must consider when verifying the axioms. For instance, when checking the left distributivity of multiplication over addition it is sufficient to use all possible arrangements of b, c, and d. The reader should observe that the ring in this example does not have a unity element.

Example 5. Let S be a fixed set. Let R be the set of all subsets of S. We define an addition and a multiplication on R by

$$A + B = \{x \in S \mid x \in A \text{ or } x \in B, \text{ but } x \notin A \cap B\}$$

and

$$A \cdot B = A \cap B$$

for all $A, B \in R$ (i.e., for all subsets A, B of S). Then clearly for $A, B \in R$, $A + B$ and $A \cdot B$ are elements of R. Moreover, it is clear that for all $A, B, C \in R$, $A + B = B + A$, $A \cdot B = B \cdot A$, and $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ by definition of $+$ and properties of the intersection of sets. A pictorial description of $A + B$ is given by the Venn diagram in Fig. 3.1, where A is the circle on the left, B is the circle on the right and $A + B$ is the shaded area. The zero is the empty set $\emptyset$ since $A + \emptyset = A$ for all $A \in R$. The additive inverse of an element A of R is the set A itself. The associativity of addition and one of the distributive laws can be verified or can be illustrated using Venn diagrams. Thus R is a ring; this ring is called the *ring of all subsets of S*. Does this ring have a unity element? What is it?

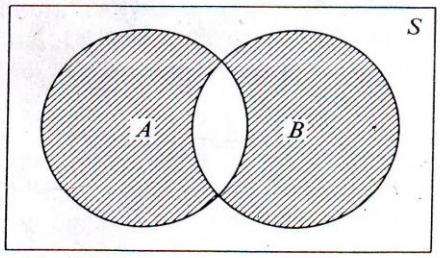

Figure 3.1

Example 6. For this example the student must recall some elementary facts from calculus. The symbol [0, 1] will denote the set $\{x \mid x \text{ is a real number and } 0 \leq x \leq 1\}$. Recall that if f is a continuous function on [0, 1], then for $x \in [0, 1]$ $f(x)$ is the *value of f at x*. Let C be the set of all continuous functions on [0, 1]. Recall the definition of equality of functions

(Section 1.2). For $f, g \in C$, define their sum $f + g$ by $(f + g)(x) = f(x) + g(x)$ for all $x \in [0, 1]$; i.e., the value of $f + g$ at x is the sum of the value of f at x and the value of g at x. Also for $f, g \in C$, define the product fg of f and g by $(fg)(x) = f(x)g(x)$ for all $x \in [0, 1]$; i.e., the value of fg at x is the product of the values of f and g at x.

From our experience with calculus, we know that the sum of continuous functions on $[0, 1]$ is a continuous function on $[0, 1]$ and the product of continuous functions on $[0, 1]$ is a continuous function on $[0, 1]$. Also if f, g, and h are elements of C, then for all $x \in [0, 1]$,

$$\begin{aligned}
[(f + g) + h](x) &= (f + g)(x) + h(x) \\
&= \big(f(x) + g(x)\big) + h(x) \\
&= f(x) + \big(g(x) + h(x)\big) && \text{(associativity of the} \\
&= f(x) + (g + h)(x) && \text{real numbers)} \\
&= [f + (g + h)](x).
\end{aligned}$$

Therefore $(f + g) + h = f + (g + h)$. Similarly, one shows that $(fg)h = f(gh)$. Furthermore, the commutativity of addition and multiplication on C is inherited from the real numbers as well as the distributivity of multiplication over addition.

What is the zero? Let $\bar{0}$ be the function on $[0, 1]$ defined by $\bar{0}(x) = 0$ for all $x \in [0, 1]$; i.e., $\bar{0}$ is a constant function. Then for any $f \in C$, $(f + \bar{0})(x) = f(x) + \bar{0}(x) = f(x) + 0 = f(x)$ for all $x \in [0, 1]$. Thus $f + \bar{0} = f$ and so $\bar{0}$ is the zero. For each $f \in C$, we let f^* be the function defined by $f^*(x) = -f(x)$ for all $x \in [0, 1]$. Then $f + f^* = \bar{0}$ since $(f + f^*)(x) = f(x) + f^*(x) = f(x) - f(x) = 0 = \bar{0}(x)$ for all $x \in [0, 1]$. Hence f^* is negative f. This proves that C is a commutative ring! Does C have a unity element?

3.3.1 Exercises

1. Which of the following sets and binary operations are rings? Of those that are rings, which have a unity element? Which are division rings? Which are commutative?

   a) $P = \{m + n\sqrt{2} \mid m, n \in I\}$ with the usual addition and multiplication.

   b) $M = \{m - n\sqrt{2} \mid m, n \in I\}$ with the usual addition and multiplication.

   c) $K =$ set of 2×2 matrices of the form

   $$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

   where $a, b, c \in I$ with the usual addition and multiplication of matrices.

   d) $T = \{(s, t, u) \mid s, t, u \in I\}$ with addition and multiplication defined by

   $$(s, t, u) + (x, y, z) = (s + x, t + y, u + z)$$

   and

   $$(s, t, u) \cdot (x, y, z) = (sx, sy + tz, uz)$$

   for all $(s, t, u), (x, y, z) \in T$.

e) $U = \{u, v, w, x\}$ and addition and multiplication are defined by the following tables.

$+$	u	v	w	x
u	u	v	w	x
v	v	u	x	w
w	w	x	u	v
x	x	w	v	u

$\cdot$	u	v	w	x
u	u	u	u	u
v	u	u	u	u
w	u	v	w	x
x	u	v	w	x

You may assume that both addition and multiplication are associative in U.

2. Prove that the multiplication in $I/(n)$ is well defined. Verify that the distributive laws hold in $I/(n)$. Also prove that $I/(n)$ is a commutative ring with unity element.
3. Write out addition and multiplication tables for $I/(5)$ and $I/(6)$. Is either a division ring? What can you conjecture about $I/(n)$?
4. Define addition $\oplus$ and multiplication $\odot$ on the set of integers by

$$m \oplus n = m + n - 1$$

and

$$m \odot n = m + n - mn$$

for all $m, n \in I$. Prove that I is a commutative ring with unity element and with these definitions of addition and multiplication.

5. Following are the addition and multiplication tables for a ring having four elements $\{a, b, c, d\}$.

$+$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	$-$	a	c
c	a	a	a	$-$
d	a	c	a	$-$

Use the distributive laws to fill in the blanks in the multiplication table.

6. Let R be a ring with unity element e which has more than one element; prove that $e \neq 0$.

3.4 GENERALIZED SUMS AND PRODUCTS

Let R be a ring and let $a_1, a_2, \ldots, a_n$ be a collection of elements from R. The addition of R is a binary operation, so we know how to add any *two* of these elements. But what if we desire to add three or more of them together? If so, we must define precisely what is meant by the sum of more than two elements. For three elements we define

$$a_1 + a_2 + a_3 = (a_1 + a_2) + a_3.$$

By the associativity of addition, $a_1 + a_2 + a_3 = a_1 + (a_2 + a_3)$; therefore the way we group the terms is irrelevant. In general, we must make an inductive definition.

3.4.1 Definition. *Let R be a ring and let $a_1, a_2, \ldots, a_{k+1}$ be elements of R. Whenever $a_1 + \cdots + a_k$ is defined, define*

$$a_1 + \cdots + a_{k+1} = (a_1 + \cdots + a_k) + a_{k+1}.$$

Thus, by the Principle of Mathematical Induction, the sum of any finite number of elements of a ring is defined. Such a sum is referred to as a *generalized sum.*

3.4.2 Theorem. *Let R be a ring and let n be any positive integer. Then for elements $a_1, \ldots, a_n$ of R,*

$$a_1 + \cdots + a_n = (a_1 + \cdots + a_s) + (a_{s+1} + \cdots + a_n)$$

where s is any integer such that $1 \leq s < n$. In other words, the sum of $a_1, \ldots, a_n$ with parentheses in any position is equal to $a_1 + \cdots + a_n$, as defined above.

Proof. The proof will be by mathematical induction. Let S_n be the statement of the theorem. For $n = 2$, we have $a_1 + a_2 = a_1 + a_2$. Hence S_2 is true. Assume that S_k is true; i.e., assume that

$$a_1 + \cdots + a_k = (a_1 + \cdots + a_s) + (a_{s+1} + \cdots + a_k)$$

where s is any integer such that $1 \leq s < k$. Then for $1 \leq s < k$, we have

$$\begin{aligned} a_1 + \cdots + a_{k+1} &= (a_1 + \cdots + a_k) + a_{k+1} && \text{(by 3.4.1)} \\ &= ((a_1 + \cdots + a_s) + (a_{s+1} + \cdots + a_k)) + a_{k+1} && \text{(by } S_k\text{)} \\ &= (a_1 + \cdots + a_s) + ((a_{s+1} + \cdots + a_k) + a_{k+1}) && \text{(by R2)} \\ &= (a_1 + \cdots + a_s) + (a_{s+1} + \cdots + a_{k+1}). && \text{(by 3.4.1)} \end{aligned}$$

Furthermore, if $s = k$, then

$$a_1 + \cdots + a_{k+1} = (a_1 + \cdots + a_s) + (a_{s+1} + \cdots + a_{k+1})$$

by definition. Consequently S_{k+1} is true. Therefore, by the Principle of Mathematical Induction, S_n is true for all positive integers n. Thus the theorem is proved.

3.4.3 Remark. *Generalized products* are defined similarly to generalized sums. Moreover, since the proof of Theorem 3.4.2 uses only the associativity of addition, the same proof can be used to prove that the generalized product of $a_1, \ldots, a_n$ is $(a_1 \cdots a_s)(a_{s+1} \cdots a_n)$ where s is any integer such that $1 \leq s < n$.

Other formulas can be generalized in a similar fashion. We will list two such generalizations and prove one, leaving the other as an exercise.

3.4.4 Theorem. *Let R be a ring and let n be any positive integer. For $a_1, \ldots, a_n \in R$,*

$$a_1 + \cdots + a_n = a_{i_1} + \cdots + a_{i_n}$$

where $i_1, i_2, \ldots, i_n$ is any rearrangement of $1, 2, \ldots, n$.

3.4.5 Corollary. *Let R be a commutative ring and let n be any positive integer. For $a_1, \ldots, a_n \in R$,*

$$a_1 a_2 \cdots a_n = a_{i_1} a_{i_2} \cdots a_{i_n}$$

where $i_1, i_2, \ldots, i_n$ is any rearrangement of $1, 2, \ldots, n$.

3.4.6 Theorem. *Let R be a ring and let n be any positive integer. For $a, b_1, \ldots, b_n \in R$,*

$$a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n.$$

Theorem 3.4.4 and Corollary 3.4.5 are *generalized commutative laws*, and Theorem 3.4.6 is a *generalized distributive law*. We will now prove Theorem 3.4.6.

Proof. Let S_n be the statement of the theorem. Then S_2 is true by the distributive law (R8). Assume that S_k is true; i.e., assume that

$$a(b_1 + \cdots + b_k) = ab_1 + \cdots + ab_k.$$

Then

$$\begin{aligned} a(b_1 + \cdots + b_{k+1}) &= a((b_1 + \cdots + b_k) + b_{k+1}) && \text{(by 3.4.1)} \\ &= a(b_1 + \cdots + b_k) + ab_{k+1} && \text{(by R8)} \\ &= (ab_1 + \cdots + ab_k) + ab_{k+1} && \text{(by } S_k\text{)} \\ &= ab_1 + \cdots + ab_{k+1} && \text{(by 3.4.1)} \end{aligned}$$

Hence S_{k+1} is true, and so, by the Principle of Mathematical Induction, S_n is true for all positive integers n. This proves the theorem.

3.4.7 Exercises

1. Give an explicit definition of generalized product, and state and prove a theorem similar to Theorem 3.4.2.
2. Prove Theorem 3.4.4 and Corollary 3.4.5.
3. Let R be a ring and let n be any positive integer. For $a_1, \ldots, a_n \in R$, prove that

$$(-a_1)(-a_2)\cdots(-a_n) = \begin{cases} a_1 a_2 \cdots a_n & \text{if } n \text{ is even.} \\ -(a_1 a_2 \cdots a_n) & \text{if } n \text{ is odd.} \end{cases}$$

4. Theorem 3.4.6 gives one generalized distributive law. State and prove another generalized distributive law.

3.5 SUBRINGS AND IDEALS

When we studied groups, we investigated subsets of groups that were groups in their own right. Such subsets were called subgroups and they played an important role in the development of the theory of groups. Here we carry out the same procedure for rings.

3.5.1 Definition. *A nonempty set S is a* ***subring*** *of a ring R if S is a subset of R and if S itself is a ring with respect to the addition and multiplication of R.*

The ring E of even integers (Example 1 above) is a subring of the ring I of all integers. The ring N discussed in Example 3 above is a subring of M of the same example.

The next theorem simplifies the procedure for showing that a subset of a ring is actually a subring.

3.5.2 Theorem. *Let R be a ring and let S be a nonempty subset of R. Then S is a subring of R if and only if*

1) $a + b \in S$ *for all* $a, b \in S$,

2) $-a \in S$ *for all* $a \in S$, *and*

3) $a \cdot b \in S$ *for all* $a, b \in S$.

This theorem says that in order to prove a subset S of a ring R is a subring of R, one needs only to prove that addition and multiplication are closed on S and that every element of S has an additive inverse in S. The set S "inherits" the other essential properties of a ring from R. The proof of this theorem is simple and is left as an exercise. Note that (1) and (2) simply state that S is a subgroup of R under addition.

A comparison of examples shows that subrings do not necessarily inherit the property of having a unity element, for the ring E of even integers is a subring of the ring I of all integers, and I has a unity element, whereas E does not. On the other hand, every subring of a commutative ring is commutative. To see this, let S be a subring of a commutative ring R and let a, b be elements of S. Since S is a subset of R, a and b must also belong to R. Since R is commutative, $ab = ba$. Hence, for all $a, b \in S$, $ab = ba$, so S is commutative.

Next we will consider a very important type of subring.

3.5.3 Definition. *Let R be a ring. A nonempty subset U of R is an* ***ideal*** *of R if*

1) *U is a subring of R, and if,*

2) *for all $r \in R$, $u \in U$, ru and ur belong to U.*

In other words, an ideal U of a ring R is a subring of R with the additional property that U "swallows up" multiplication; i.e., the product of an element of U and an element of R must belong to U. Ideals play a role in the development of ring theory similar to the role played by normal subgroups in group theory. However, an intensive study of ideals is beyond the scope of this course. Hence we will end the discussion of subrings and ideals by considering some examples and proving a theorem which characterizes the ideals of the ring of integers.

Example 1. The ring E of even integers is an ideal of the ring I of all integers. We have previously shown that E is a subring of I, so it is sufficient to show that (2) holds. Let $x \in E$ and $n \in I$. Then $x = 2m$ for some integer m. Hence

$$xn = (2m)n = 2(mn) \quad \text{and} \quad nx = n(2m) = 2(nm),$$

and so xn and nx both belong to E. Thus E is an ideal of I.

Example 2. Let R be a commutative ring. Let a be an element of R and let

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

We will show that (a) is an ideal. Two arbitrary elements of (a) are as and at for $s, t \in R$. Then $as + at = a(s + t)$ by the distributive law. Hence $as + at \in (a)$. Also, the additive inverse of as is $a(-s)$ since

$$as + a(-s) = a\big(s + (-s)\big) = a \cdot 0 = 0.$$

Moreover, $a(-s) \in (a)$. Finally,

$$(as)(at) = a\big(s(at)\big) \in (a).$$

Hence, by Theorem 3.5.2, (a) is a subring of R. Now let $r \in R$ and $as \in (a)$. Then

$$r(as) = (ra)s = (ar)s = a(rs) \in (a),$$

and

$$(as)r = a(sr) \in (a).$$

Hence (a) is an ideal.

This ideal (a) is important enough to warrant a special name.

3.5.4 Definition. *Let R be a commutative ring and let $a \in R$. The ideal $(a) = \{ar \mid r \in R\}$ is called the* ***principal ideal generated by a.***

Principal ideals are often associated with commutative rings which have a unity element, for in that case $a \in (a)$. This may not be true if the ring does not have a unity element. As we will see in Theorem 3.5.5, every ideal in I is a principal ideal. But first, another example.

Example 3. Let R be a ring with unity element. If U is an ideal of R such that $1 \in U$, then $U = R$. For, clearly, $U \subseteq R$. Now let r be an arbitrary

element of R. Since U is an ideal and $1 \in U$, $r = r \cdot 1 \in U$. Thus $R \subseteq U$ and hence $R = U$, as claimed.

The next theorem tells us that every ideal of the ring I of all integers with ordinary addition and multiplication is a principal ideal.

3.5.5. Theorem *Every ideal of the ring of integers is principal.*

Proof. Let U be an ideal of I. We must show that $U = (v)$ for some $v \in I$. If U consists of the zero element alone, then $U = (0) = \{0 \cdot r \mid r \in I\}$, and hence U is principal. Thus we now assume that U contains a nonzero integer, say u. If u is negative, then $-u \in U$ and $-u$ is positive. Hence there is a smallest positive integer in U. We know such a "smallest" positive integer v exists since the set of positive integers in U is nonempty.

We want to show that $U = (v)$. Clearly $(v) \subseteq U$. Let $w \in U$. By the division algorithm (Lemma 1.6.1), there exist integers q, r such that $w = qv + r$ and $0 \leq r < v$. But since U is an ideal and $v \in U$, we must have $qv \in U$, and thus $r = w - qv \in U$. If $r \neq 0$, then we have $r \in U$ and $0 < r < v$, contradicting the fact that v is the smallest positive integer in U. Hence r must be zero. This implies that $w = qv$; hence $w \in (v)$. Since w is an arbitrary element of U, this proves that $U \subseteq (v)$. Hence $U = (v)$, proving the theorem.

3.5.6 Exercises

1. Prove Theorem 3.5.2.
2. Let L be the set of all 2×2 matrices of the form

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$$

where $a, b \in I$. Show that L is a subring of the ring M of all 2×2 matrices discussed in Example 3, Section 3.3. Is this subring an ideal?

3. a) Let A and B be subrings of a ring R. Prove that $A \cap B$ is a subring.
   b) If A and B are ideals of R, prove that $A \cap B$ is an ideal.
4. If A and B are ideals of a ring R, define $A + B = \{a + b \mid a \in A, b \in B\}$. Prove that $A + B$ is an ideal.
5. Recall the ring C of continuous functions on $[0, 1]$ of Example 6, Section 3.3. Let $D = \{f \in C \mid f(\frac{1}{2}) = 0\}$.
   a) Prove that D is an ideal of C.
   b) Prove that the only proper ideal of C which contains D is C itself.
6. Let R be a ring and let U be an ideal of R. Let R/U be the set of all (additive) left cosets of U in R; that is,

$$R/U = \{r + U \mid r \in R\}.$$

Define addition and multiplication on R/U as follows:

$$(r + U) + (s + U) = (r + s) + U$$

and

$$(r + U) \cdot (s + U) = rs + U$$

for all $r, s \in R$.

a) Prove in detail that this makes R/U into a ring.
b) Point out where you make use of the fact that U is an ideal of R.
c) What properties could R have that will always remain as properties of R/U? For instance, will R commutative imply R/U commutative?

3.6 HOMOMORPHISMS

In Section 2.7, we defined and discussed homomorphisms between two groups. Homomorphisms were defined as those mappings between two groups that preserved the binary operations on those groups. Since rings have two binary operations defined on them, rather than one, it is not unusual that a homomorphism between two rings must preserve both the addition and multiplication of the rings.

3.6.1 Definition. *Let R and S be rings. A (ring)* ***homomorphism*** *is a mapping α from R to S such that*

(1) $$\alpha(a + b) = \alpha(a) + \alpha(b)$$

and

(2) $$\alpha(a \cdot b) = \alpha(a) \cdot \alpha(b)$$

for all $a, b \in R$.

The name "homomorphism" is used for mappings between groups *and* between rings. No confusion should arise, however; one simply understands that Definition 3.6.1 applies when one is speaking of rings and Definition 2.7.1 applies when one is speaking of groups. To emphasize the fact that the algebraic objects in question are groups or rings, one may use the names "group homomorphism" or "ring homomorphism" for "homomorphism." In (1) above, the addition on the right-hand side is that of the ring S, whereas the addition on the left-hand side is that of the ring R. Similarly, $a \cdot b$ in (2) means multiplication in R and $\alpha(a) \cdot \alpha(b)$ means multiplication in S.

Observe that (1) simply states that α is a group homomorphism from the additive group of R into the additive group of S. Hence the results of Section 2.7 apply. In particular, the following theorem is simply a restatement of Theorem 2.7.3.

3.6.2 Theorem. *Let R and S be rings and let α be a homomorphism from R to S. Then*

1) $\alpha(0) = 0$ *and*

2) *for all* $r \in R$, $\alpha(-r) = -\alpha(r)$.

3.6.3 Definition. *Let R and S be rings and let α be a homomorphism from R to S.*

1) $Im(\alpha) = \{s \in S \mid \alpha(r) = s \text{ for some } r \in R\}$ *is called the* ***image set*** *under α.*

2) $Ker(\alpha) = \{r \in R \mid \alpha(r) = 0\}$ *is called the* ***kernel*** *of α.*

3) *If α is onto S, then α is called an* ***epimorphism.***

4) *If α is one-to-one, then α is called a* ***monomorphism.***

5) *If α is both an epimorphism and a monomorphism, then α is called an* ***isomorphism.***

It is important to notice that the kernel of a ring homomorphism is the set of elements whose image is zero, the additive identity of the ring. Consequently, the kernel of a ring homomorphism is just the kernel of the group homomorphism between the additive groups of the rings. Therefore, by Theorem 2.7.3, the kernel of a ring homomorphism is an abelian subgroup of the additive group of the ring on which the homomorphism is defined. In fact, the following theorem is evident from the definitions given above and the results obtained in Section 2.7.

3.6.4 Theorem. *Let α be a homomorphism from the ring R to the ring S Then the following are true.*

1) $Im(\alpha)$ *is a subring of* S.

2) $Ker(\alpha)$ *is a subring of* R.

3) *α is an epimorphism if and only if* $Im(\alpha) = S$.

4) *α is a monomorphism if and only if* $Ker(\alpha) = \{0\}$.

The only assertion of this theorem which has not been proved previously is that $Im(\alpha)$ and $Ker(\alpha)$ are closed with respect to the multiplications in S and R respectively. The proof of this is left as an exercise.

3.6.5 Theorem. *Let α be an isomorphism from a ring R onto a ring S.*

1) *The ring R has a unity element if and only if S has a unity element.*

2) *Suppose R has a unity element. Then R is a division ring if and only if S is a division ring.*

3) *The ring R is commutative if and only if S is commutative.*

Proof. We will prove (1) and leave the proof of (2) and (3) as exercises. Suppose R has a unity element e. Let $s \in S$; since α is an epimorphism,

there exists $r \in R$ such that $a(r) = s$. Then $r \cdot e = e \cdot r = r$ and hence, since α is a homomorphism,

$$s = \alpha(r) = \alpha(r \cdot e) = \alpha(r) \cdot \alpha(e) = s \cdot \alpha(e)$$

and

$$s = \alpha(r) = \alpha(e \cdot r) = \alpha(e) \cdot \alpha(r) = \alpha(e) \cdot s.$$

Since s is an arbitrary element of S, this proves that $\alpha(e)$ is the unity element of S.

Conversely, suppose that S has a unity element e'. Since α is an isomorphism, there exists a unique $e \in R$ such that $\alpha(e) = e'$. Let $r \in R$. Then, since α is a homomorphism,

$$\alpha(r \cdot e) = \alpha(r) \cdot \alpha(e) = \alpha(r) \cdot e' = \alpha(r).$$

Since α is one-to-one, this implies that $r \cdot e = r$. Moreover, $\alpha(e \cdot r) = \alpha(r)$ and so $e \cdot r = r$. Hence e is the unity element of R.

The concept of isomorphism between two rings is important enough to deserve additional comment. If R and S are isomorphic rings, then there is a one-to-one mapping from R onto S, and furthermore, this mapping preserves the additive and multiplicative structure. In addition, Theorem 3.6.5 shows that R and S have essentially the same properties. In other words, R and S are essentially the same rings; the only difference is in the naming of the elements of each. Moreover, quite often in modern algebra, one *identifies* the elements of R and the elements of S; i.e., no distinction is made between elements of R and elements of S since they differ only in name.

3.6.6 Exercises

Let R and S denote arbitrary rings.

1. Prove that the mapping $\alpha: R \to S$ defined by $\alpha(r) = 0$ for all $r \in R$ is a homomorphism. What is $Ker(\alpha)$ and $Im(\alpha)$?
2. Let
$$P = \{m + n\sqrt{2} \mid m, n \in I\} \quad \text{and} \quad M = \{m - n\sqrt{2} \mid m, n \in I\}.$$
We have seen that P and M are rings with the usual multiplication and addition. Define a mapping $\alpha: P \to M$ by $\alpha(m + n\sqrt{2}) = m - n\sqrt{2}$ for all $m + n\sqrt{2} \in P$. Prove or disprove that α is a monomorphism.
3. Recall the rings K and T of Exercise 1(c) and (d), Section 3.3.1. Define a mapping $\beta: K \to T$ by
$$\beta\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = (a, b, c).$$
Prove that β is an isomorphism.
4. If α is a homomorphism from R to S, prove that
a) $Ker(\alpha)$ is an ideal of R, and b) $Im(\alpha)$ is a subring of S.

5. Let α be an isomorphism from R onto S. Let e and e' denote the unity elements of R and S respectively. If an element $r \in R$ has a multiplicative inverse r^{-1}, prove that $\alpha(r^{-1}) = (\alpha(r))^{-1}$. Using this fact, prove Theorem 3.6.5 (2).
6. Prove Theorem 3.6.5 (3).
7. If α is an epimorphism from R onto S, and if U is an ideal of R, then $\alpha(U) = \{\alpha(u) \mid u \in U\}$ is an ideal of S.

ADDITIONAL REFERENCES FOR CHAPTER 3

BARNES, WILFRED E., *Introduction to Abstract Algebra*, Boston: Heath and Company (1963).

HERSTEIN, I. N., *Topics in Algebra*, New York: Blaisdell (1964).

MCCOY, NEAL H., *Introduction to Modern Algebra*, Boston: Allyn and Bacon (1960).

WHITESITT, J. ELDON, *Principles of Modern Algebra*, Reading, Massachusetts: Addison-Wesley (1964).