24 Rings: Definition and Basic Results

In this section, we introduce another type of algebraic structure, called ring. A group is an algebraic structure that requires one binary operation. A ring is an algebraic structure that requires two binary operations that satisfy some conditions listed in the following definition.

**Definition 24.1**
A ring is a nonempty set $R$ with two binary operations (usually written as addition and multiplication) such that for all $a, b, c \in R$,

1. $R$ is closed under addition: $a + b \in R$.
2. Addition is associative: $(a + b) + c = a + (b + c)$.
3. Addition is commutative: $a + b = b + a$.
4. $R$ contains an additive identity element, called zero and usually denoted by $0$ or $0_R$: $a + 0 = 0 + a = a$.
5. Every element of $R$ has an additive inverse: $a + (-a) = (-a) + a = 0$.
6. $R$ is closed under multiplication: $ab \in R$.
7. Multiplication is associative: $(ab)c = a(bc)$.
8. Multiplication distributes over addition: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

If $ab = ba$ for all $a, b \in R$ then we call $R$ a commutative ring.

In other words, a ring is a commutative group with the operation $+$ and an additional operation, multiplication, which is associative and is distributive with respect to $+$.

**Remark 24.1**
Note that we don’t require a ring to be commutative with respect to multiplication, or to have multiplicative identity, or to have multiplicative inverses. A ring may have these properties, but is not required to. These additional properties will be discussed at the end of the section.

**Example 24.1**
The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, with the usual operations of multiplication and addition form commutative rings.

**Example 24.2**
The set $\mathbb{Z}_n$ with the operations of multiplication and addition modulo $n$ forms a commutative ring for any $n \in \mathbb{N}$. The only properties left to establish are the distributive laws. We will show that $[a] \odot ([b] \oplus [c]) = [a] \odot [b] \oplus [a] \odot [c]$. The
proof of \((a \oplus [b]) \odot [c] = [a] \odot [b] \oplus [b] \odot [c]\) is similar.

\[
[a] \odot ([b] \oplus [c]) = [a] \odot [b + c] = [a(b + c)] = [ab + ac] = [ab] \oplus [ac] = [a] \odot [b] \oplus [a] \odot [c]
\]

**Example 24.3**
The set of even integers together with the usual addition and multiplication in \(\mathbb{Z}\) is a commutative ring.

We next turn to discussing some basic properties of rings.

**Theorem 24.1**
The following hold in any ring \(R\).

(i) \(a + b = a + c\) implies \(b = c\) for all \(a, b, c \in R\).

(ii) \(a0 = 0a = 0\) for all \(a \in R\);

(iii) \((-a)b = (-a)a = -(ab)\) for all \(a, b \in R\);

(iv) \(-(-a) = a\).

(v) \(-a + b = (-a) + (-b)\).

(vi) \((-a)(-b) = ab\) for all \(a, b \in R\);

(vii) \(a(b - c) = ab - ac\) and \((a - b)c = ac - bc\) for all \(a, b, c \in R\), where we \(a - b\) stands for \(a + (-b)\).

(viii) \((-1)a = -a\) if \(R\) has a multiplicative identity, i.e. \(1_R a = a1_R = a\) for all \(a \in R\).

**Proof.**

(i) \(b = 0 + b = ((-a) + a) + b = (-a) + (a + b) = (-a) + (a + c) = ((-a) + a) + c = 0 + c = c\).

(ii) \(a0 = a(0 + 0) = a0 + a0\). Thus, \(0 + a0 = a0 = a0 + a0\) so that by the right cancellation property of the additive group we have \(a0 = 0\). A similar argument holds for \(0a = 0\).

(iii) Since \(ab + (-a)b = (a + (-a))b = 0b = 0\) then \((-a)b\) is the additive inverse of \(ab\). That is, \(-xab = (-a)b\). Similarly, since \(ab + a(-b) = a(b + (-b)) = 0\) then \(-ab = a(-b)\).

(iv) Follows from the definition of additive inverse.

(v) Since \((a + b) + ((-a) + (-b)) = [(a + b) + (-a)] + (-b) = [(-a) + (a + b)] + (-b) = [((-a) + a) + b] + (-b) = (0 + b) + (-b) = 0 + (b + (-b)) = 0 + 0 = 0\) then \((-a) + (-b)\) is the additive inverse of \(a + b\). That is, \((-a + b) = (-a) + (-b)\).

(vi) Using (iii), we have \((-a)(-b) = -[a(-b)] = -[-(ab)] = ab\).

(vii) We prove that \(a(b - c) = ab - ac\). The prove that \((a - b)c = ac - bc\) is similar.

\[
a(b - c) = a(b + (-c)) = ab + a(-c)\text{ by Definition 24.1(8)} = ab - ac \text{ by (ii)}
\]
As we pointed out earlier in the section, the multiplicative operation in a ring does not necessarily have to satisfy either the commutative law or have an identity element. The following definition introduces the terminology used when multiplication is either commutative or has an identity element.

**Definition 24.2**

Let $R$ be a ring such that $ab = ba$ for all $a, b \in R$. Then we call $R$ a **commutative ring**. If $e \in R$ is such that $ae = ea = a$ for all $a \in R$ then $e$ is called a **unity** for the ring and the ring is called **unitary ring**.

**Example 24.4**

1. $\mathbb{Z}, \mathbb{Q},$ and $\mathbb{R}$ are commutative rings with unity $1$.
2. The ring of even integers is a commutative ring with no unity.
3. The ring of integers modulo $n$ is a commutative ring with unity $[1]$.
4. The ring $\mathcal{M}$ of $2 \times 2$ matrices is noncommutative with unity the matrix

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

When a unity in a ring exists then it must be unique.

**Theorem 24.2**

If $R$ is a ring and $e_1$ and $e_2$ are unity elements then we must have $e_1 = e_2$.

**Proof.**

Since $e_1$ is a unity then $e_1a = a$ for all $a \in R$. In particular, letting $a = e_2$ to obtain $e_1e_2 = e_2$. Similarly, since $e_2$ is a unity then $ae_2 = a$ for all $a \in R$. Letting $a = e_1$ to obtain $e_1e_2 = e_1$. Thus, $e_1 = e_2$.

As in the case of a group, the existence of the unity element leads to the discussion of multiplicative inverses.

**Definition 24.3**

Let $R$ be a ring with unity $e$. We say that $x$ is a **multiplicative inverse** (or a **unit element**) of an element $a \in R$ if $ax = xa = e$.

Multiplicative inverses are unique according to the following theorem.

**Theorem 24.3**

Let $R$ be a ring with unity $e$. Let $a \in R$ and suppose that $x$ and $y$ are multiplicative inverses of $a$. Then $x = y$.

**Proof.**

Since $x$ and $y$ are multiplicative inverses of $a$ then we have $ax = xa = e$ and $ay = ya = e$. Thus, $x = ex = (ya)x = y(ax) = ye = y$.

**Notation**

Let $R$ be a ring with unity. If $a \in R$ has a multiplicative inverse then we will denote the inverse by $a^{-1}$. 3
Example 24.5
In a ring $R$, it is possible that some of the elements have multiplicative inverses whereas others don’t. For example, in the ring $\mathbb{Z}_{10}$, [1] and [9] are their own multiplicative inverses, [3] and [7] are inverses of each other. The remaining elements of $\mathbb{Z}_{10}$ have no multiplicative inverses.
Review Problems

Exercise 24.1

Exercise 24.2
Let $\mathcal{M}$ be the collection of all 2 by 2 matrices with entry in $\mathbb{R}$. Show that $(\mathcal{M}, +, \cdot)$ is a non commutative ring, where addition and multiplication as defined in Exercises 3.15 and 3.16.

Exercise 24.3
Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[\sqrt{2}]$ with the usual addition and multiplication in $\mathbb{Z}$ is a commutative ring.

Exercise 24.4
Let $\mathcal{M}(\mathbb{R})$ be the collection of all mappings from $\mathbb{R}$ to $\mathbb{R}$. Define addition by $(f + g)(x) = f(x) + g(x)$ and multiplication by $(fg)(x) = f(x)g(x)$. Show that $(\mathcal{M}(\mathbb{R}), +, \cdot)$ is a commutative ring.

Exercise 24.5
Let $E$ be the set of even integers. Prove that with the usual addition, and with the multiplication $mn = \frac{1}{2}mn$, $E$ is a ring. Is there a unity?

Exercise 24.6
Find the elements of $\mathbb{Z}_8$ that have multiplicative inverses.

Exercise 24.7
Let $R$ and $S$ be two rings. Show that the Cartesian product $R \times S$ together with the operations

\[
(a, b) + (c, d) = (a + c, b + d)
\]

\[
(a, b)(c, d) = (ac, bd)
\]

is a ring.

Exercise 24.8
The addition table and part of the multiplication table for the ring $R = \{a, b, c\}$ are given below. Use the distributive laws to complete the multiplication table.

<table>
<thead>
<tr>
<th>+</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>a</td>
<td>b</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>\cdot</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a</td>
<td>c</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>a</td>
<td></td>
</tr>
</tbody>
</table>

Exercise 24.9
Let $(R, +)$ be an Abelian group. Define multiplication by $ab = 0$ for all $a, b \in R$. Show that $(R, +, \cdot)$ is a commutative ring.

Exercise 24.10
In the ring of integers, if $ab = ac$, with $a \neq 0$, then $b = c$. Is this true for all rings?
Exercise 24.11
Prove that in a ring \( R \) we have
\[
(x + y)(z + t) = xz + xt + yz + yt
\]
for all \( x, y, z, t, \in R \).

Exercise 24.12
Let \( R \) be a ring in which \( a^2 = a \) for all \( a \in R \). Prove that \( R \) is commutative and that \( a + a = 0 \) for all \( a \in R \). (Hint: Consider \((a + a)^2\) and \((a + b)^2\).)

Exercise 24.13
Prove that \((a + b)^2 = a^2 + 2ab + b^2\) for all \( a, b \) in a ring \( R \) if and only if \( R \) is commutative.

Exercise 24.14
Prove that if \( R \) is a commutative ring, \( a, b \in R \), and \( n \in \mathbb{N} \) then
\[
(a + b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n
\]
where
\[
\binom{n}{p} = \frac{n!}{p!(n-p)!}
\]

Exercise 24.15
An element \( a \) of a ring \( R \) is said to be nilpotent if \( a^n = 0 \) for some positive integer \( n \). Prove that if \( R \) is commutative and if \( a \) and \( b \) are nilpotent, then so is \( a + b \).

Exercise 24.16
Show that the set
\[
R = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R} \right\}
\]
with the usual matrix addition and multiplication is a ring.

Exercise 24.17
A (real) polynomial is a formal expression of the form
\[
p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,
\]
where \( a_0, \ldots, a_n \in \mathbb{R} \) and \( x \) is a variable. Polynomials can be added and multiplied as usual. With these operations, show that the set \( \mathbb{R}[x] \) of all polynomials is a ring.

Exercise 24.18
Suppose that \( R \) is a ring in which all elements \( a \) satisfy \( a^2 = a \). (Such a ring is called a Boolean ring.)

(i) Prove that \( a = -a \) for all \( a \in R \).
(ii) Prove that \( R \) is commutative.