1 Rings and Fields

1.1 Introduction

Definition 1.1 (Binary Operation)**.** An **internal binary operation** defined on a set S is a mapping $f : S \times S \to S$.

In this document, we will refer to these simply as **binary operations**.

The following are examples of binary operations:

1. Addition on the set of nonnegative integers $\mathbb{Z}_{\geq 0}$.

2. Subtraction on the set of integers $\mathbb{Z}$.

3. Multiplication on the set of $n \times n$ matrices with real number entries $\mathbb{R}^{n \times n}$.

The following are not binary operations:

1. Subtraction on the set of nonnegative integers $\mathbb{Z}_{\geq 0}$, because $0 - 1 = -1$ is not in $\mathbb{Z}_{\geq 0}$.

2. Division on the set of rational numbers $\mathbb{Q}$, because $1/0$ is not defined.

Definition 1.2 (Ring)**.** A **ring** is a set R with two binary operations—addition $(+)$ and multiplication $(\cdot)$—satisfying the following **ring axioms**:

1. Addition is associative, meaning $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.

2. Addition is commutative, meaning $a + b = b + a$ for all $a, b \in R$.

3. There is an identity element with respect to addition, meaning there exists $0 \in R$ satisfying $a + 0 = a$ and $0 + a = a$ for all $a \in R$.

4. Every element has an inverse with respect to addition, meaning that for all $a \in R$, there exists $b \in R$ satisfying $a + b = 0$ and $b + a = 0$.

5. Multiplication is associative, meaning $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

6. There is an identity element with respect to multiplication, meaning there exists $1 \in R$ satisfying $a \cdot 1 = a$ and $1 \cdot a = a$ for all $a \in R$.

7. Multiplication is distributive over addition, meaning $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.

The following are examples of rings.

1. The set of integers $\mathbb{Z}$ with addition and multiplication defined conventionally.

2. The set of $n \times n$ matrices with entries from a ring R, along with the addition and multiplication operations copied from R.

By convention, the addition operation of a ring is denoted $(+)$, and the multiplication operation of a ring is denoted $(\cdot)$. Furthermore, adding an additive inverse is usually written as "subtraction", meaning $a + (-b) \equiv a - b$, and the multiplication operation is usually written without $(\cdot)$, meaning $a \cdot b \equiv ab$. We will adopt all of these these conventions.

Some texts do not require condition (6) to hold, that is, their rings do not necessarily an identity element with respect to multiplication. See this Wikipedia article for more information. As a subjective opinion, this seems to be somewhat of a stylistic choice: if there is no multiplicative identity, then we cannot take the product of an arbitrary collection of elements, because this would be undefined if the collection is empty. On the other hand, sometimes it simply does not make sense to force the existence of a multiplicative identity. This may not be the best example, but later we will define a special type of "subring" called an ideal, which should not be defined as requiring a multiplicative identity.

Definition 1.3 (Commutative ring)**.** A **commutative ring** is a ring R with the additional property that the multiplication operation is commutative, meaning $ab = ba$ for all $a, b \in R$.

Proposition 1.1. *Let R be a ring, then R has exactly one additive identity.*

Proof. By definition, we know that R has at least one additive identity, so we will show it has at most one. Let $r, s \in R$ be two additive identities, and see that $r + s = s$ because r is an additive identity. But also, we see that $r + s = r$, because s is an additive identity, so it follows that $s = r$. This means every additive identity is the same, so there is at most one. $\square$

Proposition 1.2. *Let R be a ring, then R has exactly one multiplicative identity.*

Proof. Refer to the proof of the uniqueness of the additive identity, and replace addition with multiplication. $\square$

Remark 1.1. *Since we now know that rings contain exactly one additive and multiplicative identity, we can (and will) denote these values with 0 and 1 respectively.*

Proposition 1.3. *Let R be a ring, and $r \in R$. Then r has exactly one additive inverse.*

Proof. By definition, we know that r has at least one additive inverse, so we show it has at most one. Suppose $s, t \in R$ are both additive inverses of r, and see the following:

$$r + s = 0 \text{ and } r + t = 0 \implies s + (r + s) = s + (r + t) \tag{1}$$
$$\iff (s + r) + s = (s + r) + t \tag{2}$$
$$\iff 0 + s = 0 + t \tag{3}$$
$$\iff s = t \tag{4}$$

This means every additive inverse of r is the same, so there is at most one. $\square$

Remark 1.2. *Let R be a ring, and $r \in R$. Since we now know the additive inverse of r is unique, we can (and will) denote this value with $-r$.*

Proposition 1.4. *Let R be a ring, and $r \in R$. Then $0r = 0$.*

Proof. See that

$$(0 + 0)r = 0r \iff 0r + 0r = 0r \tag{5}$$
$$\iff 0r + 0r - 0r = 0r - 0r \tag{6}$$
$$\iff 0r = 0 \tag{7}$$

$\square$

Proposition 1.5. *Let R be a ring, and $r, s \in R$. Then $(-r)s = -(rs) = r(-s)$.*

Proof. For the first equality, we use multiplication by zero to see that

$$0s = 0 \iff ((-r) + r)s = 0 \tag{8}$$
$$\iff (-r)s + rs = 0 \tag{9}$$
$$\iff (-r)s + rs - (rs) = 0 - (rs) \tag{10}$$
$$\iff (-r)s = -(rs) \tag{11}$$

For the second equality, we use the same approach to see that

$$r0 = 0 \iff r((-s) + s) = 0 \tag{12}$$
$$\iff r(-s) + rs = 0 \tag{13}$$
$$\iff r(-s) + rs - (rs) = 0 - (rs) \tag{14}$$
$$\iff r(-s) = -(rs) \tag{15}$$

$\square$

Remark 1.3. *From these last two proofs, we see that it is allowed to "cancel out" identical addition terms from both sides of an equation. This is due to the associativity and commutativity of addition, along with the existence of an additive identity for every element. Keep this in mind as, in the future, we may not explicitly write the subtraction on both sides.*