8  Rings and Fields

A. Axioms

In this chapter we describe a number of axioms for sets on which addition and multiplication are defined. These axioms were originally found by isolating the basic properties of addition and multiplication which are common to all or most of the examples we already know: \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \). A ring, a commutative ring, or a field will be defined as a set with addition and multiplication satisfying certain of the axioms.

The value of these definitions is twofold. First, having the notion of field, for example, gives us a way of examining new sets with addition and multiplication. We shall ask: Is \( \mathbb{Z}_m \) a field? We shall look for other examples of fields. By the end of the book we shall have found a vast array of new fields. Second, since a commutative ring or a field shares, by definition, many of the properties of \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \) etc., examples we already know, then, if we find a new example of a field or a commutative ring, we shall know we can manipulate its elements in the same way we would manipulate numbers—rearranging sums, rearranging products, collecting common factors of sums, etc. In Chapter 9 we shall observe that much of the elementary linear algebra you may (or may not) have learned works when the scalars come from any commutative ring with identity, and in some later chapters, when we use linear algebra it will be with scalars in some of the new fields and rings we are about to discover.

We begin with the most general concept.

**Definition.** A *ring (with identity)* is a set \( R \) with three operations, \( +, \cdot, \) and \(-\), and two special elements, 0 and 1, which satisfy the various properties listed below as axioms (i)–(vii). The operations \(+\) and \(\cdot\) may each be
thought of as functions from $R \times R$ (ordered pairs of elements of the set $R$) to $R$, so that for any pair $(a, b)$, $a, b$ in $R$, $a + b$ is an element of $R$, and $a \cdot b$ is an element of $R$. The operation $-$ similarly is a function from $R$ to $R$ which takes $a$ in $R$ to $-a$ in $R$.

The set $R$, together with the operations $+$, $\cdot$ and $-$ and special elements $0, 1$, is a ring with identity if the following axioms hold:

(i) for any $a, b, c$ in $R$, $(a + b) + c = a + (b + c)$ (associativity of addition);
(ii) for any $a, b$ in $R$, $a + b = b + a$ (commutativity of addition);
(iii) for all $a$ in $R$, $a + 0 = a$ (0 is a zero element);
(iv) for any $a$ in $R$, $a + (-a) = 0$ ($-a$ is the negative of $a$);
(v) for any $a, b, c$ in $R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativity of multiplication);
(vi) for all $a$ in $R$, $a \cdot 1 = 1 \cdot a = a$ (1 is an identity element).
(vii) for any $a, b, c$ in $R$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (distributive laws).

These basic axioms are all satisfied by $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_m$, and the set of $n \times n$ real matrices (see Section 9B).

Some examples of sets which are not rings are:

the set of natural numbers $\mathbb{N}$;
the set of nonnegative real numbers $\mathbb{R}_+$, with the usual $+$ and $\cdot$;
the set $\mathbb{Z} - \{3\}$ of all integers except 3.

The set $\mathbb{Z} - \{3\}$ is not a ring with respect to the usual addition and multiplication in $\mathbb{Z}$ for the reason that if $a, b$ are in $\mathbb{Z} - \{3\}$ then $a + b$ need not be in $\mathbb{Z} - \{3\}$. For example, $1 + 2 = 3$: 1 and 2 are in $\mathbb{Z} - \{3\}$ but 3 is not. When this kind of thing occurs we say that $\mathbb{Z} - \{3\}$ is not closed under addition, by which we mean that $\mathbb{Z} - \{3\}$ is a subset of a bigger set, $\mathbb{Z}$, on which addition and multiplication always makes sense, and if we take the sum in $\mathbb{Z}$ of two elements of $\mathbb{Z} - \{3\}$ the result in some cases is not in $\mathbb{Z} - \{3\}$. The notion of (not) closed under multiplication is similar.

We now state some axioms which are satisfied by special types of rings.

(viii) For all $a, b$ in $R$, $a \cdot b = b \cdot a$ (commutativity of multiplication).

A ring (like $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_m$) which satisfies this axiom is called a commutative ring.

(ix) For all $a, b$ in $R$, if $a \cdot b = 0$, then $a = 0$ or $b = 0$.

A ring satisfying this axiom is said to have no zero divisors. Examples are $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_m$ for some but not all $m$.

E1. Give examples of $m_1, m_2 > 6$ so that $\mathbb{Z}_{m_1}$ has zero divisors and $\mathbb{Z}_{m_2}$ does not.