# 3.1 Definition and Examples of Rings

There are lots of situations in math where we have operations of addition, subtraction, and multiplication, but not necessarily division. (We've seen that this holds for the integers. It also holds for polynomials: the sum, difference, or product of two polynomials is another polynomial. Another example – this time with non-commutative multiplication – is $n \times n$ matrices. Informally speaking, we will use the word "ring" to refer to a set with addition, subtraction, and multiplication. By studying rings abstractly, we will be able to prove theorems that will apply equally well whether we are interested in integers, or polynomials, or matrices, etc.

Our first task is to give a formal definition of what a ring is. We want to impose the bare minimum requirements to ensure that addition and multiplication in our ring behave like ordinary addition and multiplication. (Otherwise we could take any two meaningless operations and name them "addition" and "multiplication." If there were no restrictions at all, we couldn't possibly hope to say anything interesting about rings in general.)

## Definition of a Ring

**Definition.** A *ring* is a nonempty set $R$ equipped with two operations (usually called addition and multiplication, and written in the usual notation for those operations) that satisfy the following axioms. For all $a, b, c \in R$:

1. If $a \in R$ and $b \in R$, then $a + b \in R$. [Closure for addition]
2. $a + (b + c) = (a + b) + c$. [Associative addition]
3. $a + b = b + a$. [Commutative addition]
4. There is an element $0_R$ in $R$ such that $a + 0_R = a = 0_R + a$ for every $a \in R$. [Additive identity]
5. For each $a \in R$, the equation $a + x = 0_R$ has a solution in $R$. [Additive inverse]
6. If $a, b \in R$, then $ab \in R$. [Closure for multiplication]
7. $a(bc) = (ab)c$. [Associative multiplication]
8. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$. [Distributive laws]

As promised above, these properties are the bare minimum requirements for us to say that the operations of "addition" and "multiplication" in $R$ resemble ordinary addition and multiplication. We will frequently want our rings to have additional properties:

**Definition.** A *commutative ring* is a ring $R$ that satisfies:

9. $ab = ba$ for all $a, b \in R$. [Commutative multiplication]

**Definition.** A *ring with identity* is a ring $R$ that contains an element $1_R$ satisfying:

10. $a1_R = a = 1_R a$ for all $a \in R$. [Multiplicative identity]

**Definition.** An *integral domain* is a commutative ring $R$ with identity $1_R \neq 0_R$ such that[1]

11. Whenever $a, b \in R$ and $ab = 0_R$, then $a = 0_R$ or $b = 0_R$. [No zero divisors]

**Definition.** A *field* is a commutative ring $R$ with identity $1_R \neq 0_R$ that satisfies the axiom:

12. For each $a \neq 0_R$ in $R$, the equation $ax = 1_R$ has a solution in $R$. [Multiplicative inverse]

In a field, the existence of a multiplicative inverse allows us to divide by any nonzero element of the field. (This matches our experience with real numbers: division is the same as multiplying by the multiplicative inverse.) You can use this observation to prove that a field does not have any zero divisors; in other words, every field is an integral domain. (This is Theorem 3.8 from the textbook, but you might want to try to prove it yourself.)

## Examples of rings

**Example.** With the usual addition and multiplication,[2] $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative rings with identity. They are all integral domains. Furthermore, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields, while $\mathbb{Z}$ is not.

**Example.** For any positive integer $m$, the set $\mathbb{Z}/m\mathbb{Z}$ with the usual addition and multiplication of classes is a commutative ring with identity. We proved in the previous section that if $p$ is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field. You can easily check that if $m$ is composite, then $\mathbb{Z}/m\mathbb{Z}$ is not an integral domain.

**Example.** The set $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$ of even integers is a commutative ring, but it does not contain a multiplicative identity. Make sure you can prove that $2\mathbb{Z}$ is in fact a commutative ring.

**Example.** The set of odd integers is **not** a ring; it is not closed under addition, and it does not have an additive identity.

**Example.** For any positive integer $n$, let $M_n(\mathbb{Z})$ denote the set of all $n \times n$ matrices with entries in $\mathbb{Z}$. You can check that $M_n(\mathbb{Z})$ is a ring with identity. (If $n > 1$, then it is a noncommutative ring.)

**Example.** More generally, if $R$ is any commutative ring, then $M_n(R)$ is a ring. [If you proved that $M_n(\mathbb{Z})$ is a ring, then you can prove that $M_n(R)$ is a ring. Note that the only properties

[1] The condition $1_R \neq 0_R$ serves only to ensure that the zero ring – the single-element ring $\{0_R\}$ – does not count as an integral domain. Make sure you can prove that the only ring with $0_R = 1_R$ is the zero ring.

[2] I mention "the usual addition and multiplication" here to emphasize that rings can sometimes have unusual addition and multiplication, so technically we need to specify not just a set, but also what addition and multiplication we are using, in order to fully specify a ring. In practice, this is rarely done – if a familiar ring is mentioned without specifying the ring operations, you may assume they are the usual ring operations.

of $\mathbb{Z}$ that you needed in your proof that $M_n(\mathbb{Z})$ is a ring were the ring properties, so the exact same proof works for $M_n(R)$.]

**Example.** Let $T$ be the set of all function $f\colon \mathbb{R} \to \mathbb{R}$. We can define addition and multiplication in the usual way: namely, given $f, g \in T$, we define $f + g$ and $fg$ by

$$(f+g)(x) = f(x)g(x) \qquad \text{and} \qquad (fg)(x) = f(x)g(x).$$

You can check that $T$ is a commutative ring with identity. (In particular, make sure you check the "with identity" part. What is the multiplicative identity in $T$?) Is $T$ an integral domain? Is $T$ a field?

## Cartesian Product

Recall that if $R$ and $S$ are sets, we define their *Cartesian product* to be the set of ordered pairs

$$R \times S = \{(r,s) \mid r \in R \text{ and } s \in S\}.$$

If $R$ and $S$ are rings, then there is a natural way to define addition and multiplication in $R \times S$, namely componentwise. That is, we define addition and multiplication in $R \times S$ by

$$(r,s) + (r',s') = (r+r', s+s'),$$

$$(r,s)(r',s') = (rr', ss').$$

With these operations, $R \times S$ is a ring. You can check this by verifying that all the ring axioms are satisfied.

**Theorem.** *Let $R$ and $S$ be rings. With the above operations, $R \times S$ is a ring. If $R$ and $S$ are both commutative, so is $R \times S$. If both $R$ and $S$ have a multiplicative identity, then so does $R \times S$.*

*Proof.* Left as an exercise. (Even if you don't bother checking all the ring axioms, at least check the last claim: what is the multiplicative identity in $R \times S$?) □

## Subrings

**Definition.** If $R$ is a ring and $S$ is a subset of $R$ which is itself a ring under the operations in $R$, then we say that $S$ is a *subring* of $R$. Similarly, if $F$ is a field and $E$ is a subset of $F$ which is itself a field under the operations in $F$, then we say that $E$ is a *subfield* of $F$.

**Example.** $\mathbb{Z}$ is a subring of $\mathbb{Q}$. $M_2(\mathbb{R})$ is a subring of $M_2(\mathbb{C})$. $\mathbb{Q}$ is a subfield of $\mathbb{R}$.

Proving that a ring is really a ring may seem tedious; there are a lot of axioms to check. But in practice, we usually don't need to check all of them. For example, we already know that addition in $\mathbb{R}$ is commutative and associative, so when we prove that $\mathbb{Z}$ is a ring, there's nothing to check. For example, we already know that $a+b=b+a$ for all $a,b \in \mathbb{R}$, so certainly $a+b=b+a$ for all $a,b \in \mathbb{Z}$.

In other words, if $S$ is a subset of a ring $R$ (with the same operations), then in order to prove that $S$ is a subring of $R$, we don't need to check that addition is commutative. We already know that addition is commutative in $R$, so addition is automatically commutative in $S$. Similarly, several of the other ring axioms will also automatically hold for $S$. Going through the list of axioms, we see that there are only a few that we need to check:

**Theorem.** *Suppose $R$ is a ring and $S$ is a subset of $R$ such that*

- *$S$ is closed under addition.*
- *$S$ is closed under multiplication.*
- *$0_R \in S$.*
- *If $a \in S$, then the solution to the equation $a + x = 0_R$ is in $S$.*

*Then $S$ is a subring of $R$.*

In practice, we will rarely want to prove that a certain set $S$ is a ring by going back to all of the axioms. Usually, $S$ will be a subset of some ring $R$, so we need only check $S$ for closure under addition, closure under multiplication, an additive identity, and additive inverses.

**Example.** The set

$$\mathbb{Z}[\sqrt{6}] = \{a + b\sqrt{6} \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{R}$. To prove this, we check the following. It is closed under addition because

$$(a+b\sqrt{6}) + (c+d\sqrt{6}) = (a+c) + (b+d)\sqrt{6} \in \mathbb{Z}[\sqrt{6}].$$

It is closed under multiplication because

$$(a+b\sqrt{6})(c+d\sqrt{6}) = (ac+6bd) + (ad+bc)\sqrt{6} \in \mathbb{Z}[\sqrt{6}].$$

It contains the additive identity: $0 = 0 + 0\sqrt{6} \in \mathbb{Z}[\sqrt{6}]$. It contains additive inverses: the additive inverse of $a + b\sqrt{6}$ is $(-a) + (-b)\sqrt{6} \in \mathbb{Z}[\sqrt{6}]$.

**Example.** The set of all differentiable functions $f\colon \mathbb{R} \to \mathbb{R}$ is a subring of the ring $T$ of all functions $f\colon \mathbb{R} \to \mathbb{R}$ (mentioned earlier). We know from calculus that the sum and product of two continuous functions are differentiable, the zero function is differentiable, and if $f$ is differentiable, then so is $-f$.