Rings

**Definition.** A **ring** is an abelian group \( R \) with binary operation \(+\) ("addition"), together with a second binary operation \( \cdot \) ("multiplication"). The operations satisfy the following axioms:

1. **Multiplication is associative:** For all \( a, b, c \in R \),

   \[
   (a \cdot b) \cdot c = a \cdot (b \cdot c).
   \]

2. The **Distributive Law** holds: For all \( a, b, c \in R \),

   \[
   a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c.
   \]

**Remarks.** 1. To say that \( R \) is an abelian group under addition means that the following axioms holds:

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

   b. (Identity) There is an element \( 0 \in R \) such that \( a + 0 = a \) and \( 0 + a = a \) for all \( a \in R \).

   c. (Inverses) For all \( a \in R \), there is an element \(-a \in R\) such that \( a + (-a) = 0 \) and \((-a) + a = 0\).

   d. (Commutativity) \( a + b = b + a \) for all \( a, b \in R \).

2. A ring \( R \) has a **multiplicative identity** if there is an element \( 1 \in R \) such that \( 1 \neq 0 \), and such that for all \( a \in R \),

   \[
   1 \cdot a = a \quad \text{and} \quad a \cdot 1 = a.
   \]

   A ring satisfying this axiom is called a **ring with 1**, or a **ring with unity**.

   **Warning:** Unity refers to the multiplicative identity, if there is one. A **unit** in a ring, on the other hand, is an element which has a multiplicative inverse.

3. I’ll often suppress the multiplication symbol and simply write \( "ab" \) for \( "a \cdot b" \). As usual, \( a^2 \) means \( a \cdot a \), \( a^3 \) means \( a \cdot a \cdot a \), and so on.

   However, note that *negative powers* of elements are not always defined: An element in a ring might not have a multiplicative inverse. This means that you don’t always have “division”; you do have “subtraction”, since that’s the same as adding the additive inverse.

4. **Multiplication need not be commutative:** It isn’t necessarily true that \( ab = ba \) for all \( a, b \in R \). If \( ab = ba \) for all \( a, b \in R \), \( R \) is a **commutative ring**.  

**Example.** \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) are commutative rings with unity under the usual operations.  

**Example.** Consider the set

\[
\mathbb{H} = \{ w + xi + yj + zk \mid w, x, y, z \in \mathbb{R} \}.
\]

\( \mathbb{H} \) is referred to as the **ring of quaternions**. (The “\( H \)” honors William Rowan Hamilton, who discovered the quaternions in the 1840’s.)
Multiply elements using the following multiplication table:

<table>
<thead>
<tr>
<th>×</th>
<th>1</th>
<th>-1</th>
<th>i</th>
<th>-i</th>
<th>j</th>
<th>-j</th>
<th>k</th>
<th>-k</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>i</td>
<td>-i</td>
<td>j</td>
<td>-j</td>
<td>k</td>
<td>-k</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>-i</td>
<td>1</td>
<td>-j</td>
<td>j</td>
<td>k</td>
<td>-k</td>
</tr>
<tr>
<td>i</td>
<td>i</td>
<td>1</td>
<td>i</td>
<td>-1</td>
<td>i</td>
<td>-j</td>
<td>j</td>
<td>-j</td>
</tr>
<tr>
<td>-i</td>
<td>-i</td>
<td>i</td>
<td>1</td>
<td>-1</td>
<td>-k</td>
<td>k</td>
<td>j</td>
<td>-j</td>
</tr>
<tr>
<td>j</td>
<td>j</td>
<td>-j</td>
<td>-k</td>
<td>k</td>
<td>-1</td>
<td>i</td>
<td>-i</td>
<td></td>
</tr>
<tr>
<td>-j</td>
<td>-j</td>
<td>j</td>
<td>k</td>
<td>-k</td>
<td>1</td>
<td>-1</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>k</td>
<td>k</td>
<td>-k</td>
<td>j</td>
<td>-i</td>
<td>i</td>
<td>-1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>-k</td>
<td>-k</td>
<td>k</td>
<td>-j</td>
<td>j</td>
<td>i</td>
<td>-i</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

(This is the multiplication table for the group of the quaternions \( \mathbb{H} \); in \( \mathbb{H} \), 1, i, j, and k can be multiplied by real numbers as if they were vectors. In fact, ignoring the multiplication, \( \mathbb{H} \) is just a 4-dimensional vector space over \( \mathbb{R} \).)

For example,

\[
(3i - 2k) \cdot (3 + 2j) = 15i.
\]

\( \mathbb{H} \) is a noncommutative ring, since (e.g.) \( ij = k \) but \( ji = -k \). In fact, Hamilton apparently was stuck on this point for many years. He knew that complex numbers could be used to represent rotations in two dimensions, and he was trying to construct an algebraic system for representing rotations in three dimensions. The problem is that rotations in three dimensions don’t commute, whereas he expected his algebraic system to have a commutative multiplication — as did all the number systems known up to that time.

Verifying the other ring axioms is routine, but very tedious!

---

**Example.** \( \mathbb{Z}_3 \) is an abelian group under addition. You can multiply elements of \( \mathbb{Z}_3 \) in the obvious way — multiply them as if they were integers, then reduce mod 3. Here’s the multiplication table:

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

For example, \( 2 \cdot 2 = 1 \), since as integers \( 2 \cdot 2 = 4 \), and 4 reduces to 1 mod 3.

With these operations, \( \mathbb{Z}_3 \) becomes a commutative ring with 1.

In general, \( \mathbb{Z}_n \) is a commutative ring with 1.

---

**Example.** The set of even integers \( 2\mathbb{Z} \) with the usual operations is a ring without 1.

---

**Example.** \( M(2, \mathbb{R}) \) is the set of \( 2 \times 2 \) matrices with real entries. The operations are the usual matrix addition and multiplication. \( M(2, \mathbb{R}) \) is a noncommutative ring.

---

**Example.** \( C[0,1] \) is the set of continuous functions \( f : [0,1] \to \mathbb{R} \). Operations are pointwise addition and multiplication:

\[
(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x).
\]
$C[0, 1]$ is a commutative ring. The constant functions 0 and 1 are the additive and multiplicative identities, respectively. $lacksquare$

**Example.** Let $R$ be a commutative ring. $R[x]$ denotes the ring of polynomials in one variable with coefficients in $R$. Add and multiply polynomials as usual.

For example, $\mathbb{R}[x]$ consists of all polynomials with real coefficients: things like

$$x + 2, \quad 3 - 7x^2 + 54x^{17}, \quad 42, \ldots$$

The formal, precise way to define $R[x]$ is to define it to be the collection of finite ordered $n$-tuples

$$\{(r_0, r_1, \ldots, r_n) \mid n \geq 0, r_i \in R\}.$$  

(That is, a polynomial is the "vector" of its coefficients.) Now you can define addition and multiplication by writing down some ugly, unenlightening formulas. The point of this pedantry is that there is no flim-flam going on in talking about "formal sums in powers of $x$" — the usual way you think of polynomials.

Note that polynomials are not functions in this context. For example, let $R = \mathbb{Z}_2$ and look at $f(x) = x^2 + x$. This is not zero as a polynomial, even though $f(0) = 0$ and $f(1) = 1$; i.e., even though it vanishes on every element of the ring. $lacksquare$

**Definition.** Let $R$ be a ring. A zero divisor is a nonzero element $a \in R$ such that $ab = 0$ for some nonzero $b \in R$.

A commutative ring with 1 having no zero divisors is an integral domain (or a domain for short).

**Definition.** Let $R$ be a ring with 1, and let $a \in R$. A multiplicative inverse of $a$ is an element $a^{-1} \in R$ such that

$$a \cdot a^{-1} = 1 \quad \text{and} \quad a^{-1} \cdot a = 1.$$  

An element which has a multiplicative inverse is called a unit. (Do not confuse this with the term "ring with unity", where "unity" refers to the multiplicative identity 1.)

A ring with 1 in which every nonzero element has a multiplicative inverse is called a division ring. A commutative ring with 1 in which every nonzero element has a multiplicative inverse is called a field.

**Example.** $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are integral domains — in fact, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. It happens to be true that every field is an integral domain; $\mathbb{Z}$ is an example of an integral domain which is not a field. (The element $2 \in \mathbb{Z}$ doesn’t have a multiplicative inverse in $\mathbb{Z}$.) $lacksquare$

**Example.** $\mathbb{Z}_4$ is not an integral domain, since $2 \cdot 2 = 0$. In fact, I’ll show later that $\mathbb{Z}_n$ is an integral domain — in fact, a field — if and only if $n$ is prime. $lacksquare$

**Example.** $C[0, 1]$ is not an integral domain. For example, let

$$f(x) = \begin{cases} 
0 & \text{if } 0 \leq x \leq \frac{1}{2} \\
 x - \frac{1}{2} & \text{if } \frac{1}{2} < x \leq 1 
\end{cases}$$

$$g(x) = \begin{cases} 
\frac{1}{2} - x & \text{if } 0 \leq x \leq \frac{1}{2} \\
0 & \text{if } \frac{1}{2} < x \leq 1 
\end{cases}$$
Then $f, g \neq 0$, but $fg = 0$. \[\square\]

**Stupid ring tricks.** Most elementary algebraic operations work the way you’d expect. Here are some easy ones. Let $R$ be a ring.

1. If $r \in R$, then $r \cdot 0 = 0 = 0 \cdot r$.

   Note that
   
   \[
   r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0.
   \]

   Therefore $0 = r \cdot 0$. \[\square\]

2. Let $r \in R$, and let $-r$ denote the additive inverse of $r$. If $R$ is a ring with unity, then $(-1) \cdot r = -r$.

   Compute:
   
   \[
   (-1) \cdot r + r = (-1) \cdot r + 1 \cdot r = (-1 + 1) \cdot r = 0 \cdot r = 0.
   \]

   Therefore, $(-1) \cdot r$ is the additive inverse of $r$, i.e. $(-1) \cdot r = -r$. \[\square\]

3. Let $r, s \in R$. Then $(-r) \cdot s = -(rs) = r \cdot (-s)$.

   The proof is similar to the proof of 2. \[\square\]

**Convention.** If $R$ is a ring and $n$ is a positive integer, $nr$ is short for $r + r + \cdots + r$ ($n$ summands). Likewise, if $n$ is a negative integer, $nr$ is $(-n) \cdot r$. (This is the usual convention for an abelian group.)

Notice that, for example, $13 \cdot 1 \in \mathbb{Z}_6$ makes sense according to this convention: It is 1 added to itself 13 times. However, you should not write “$13 \in \mathbb{Z}_6$”, since 13 is not an element of $\mathbb{Z}_6$. \[\square\]

**Lemma.** (Cancellation) Let $R$ be a commutative ring with 1. $R$ is a domain if and only if for all $r, s, t \in R$, $rs = rt$ and $r \neq 0$ implies $s = t$.

In other words, you can “cancel” nonzero factors in a domain.

**Proof.** Suppose $R$ is a domain. Let $r, s, t \in R$, where $r \neq 0$, and suppose $rs = rt$. Then $rs - rt = 0$, so $r(s - t) = 0$. Since $r \neq 0$ and since $R$ has no zero divisors, $s - t = 0$. Therefore, $s = t$.

Conversely, suppose for all $r, s, t \in R$, $rs = rt$ and $r \neq 0$ implies $s = t$. I will show that $R$ has no zero divisors. Suppose $ab = 0$, where $a \neq 0$. Now $ab = 0 = a \cdot 0$, and by cancellation, $b = 0$. This shows that $R$ has no zero divisors, so $R$ is a domain. \[\square\]

**Example.** $x^2 + 3x - 4 \in \mathbb{Z}_{12}[x]$ has roots 1, 4, 5, 8 in $\mathbb{Z}_{12}$.

<table>
<thead>
<tr>
<th>$x$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^2 + 3x - 4 \pmod{12}$</td>
<td>8</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x$</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>$x^2 + 3x - 4 \pmod{12}$</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td>8</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

Thus, a polynomial of degree $n$ can have more than $n$ roots in a ring. The problem is that $\mathbb{Z}_{12}$ is not a domain: $(x + 4)(x - 1) = 0$ does not imply one of the factors must be zero. \[\square\]
Remark. Here is a picture which shows how the various types of rings are related:

\[
\begin{array}{ccc}
\text{ring} & \downarrow & \text{commutative ring} \\
\downarrow & & \downarrow \\
\text{domain} & & \text{division ring} \\
\downarrow & & \downarrow \\
\text{field} & & \\
\end{array}
\]

Thus, a field is a special case of a division ring, just as a division ring is a special case of a ring.

The objects of mathematics are primarily built up from sets by adding axioms to make more complicated structures. For instance, a group is a set with one binary operation satisfying certain axioms. A ring is a set with two binary operations, satisfying certain axioms. You get special kinds of rings by adding axioms to the basic ring definition.

There are many advantages to doing things this way. For one, if you prove something about a simple structure, you know the result will be true about more complicated structures which are built from the simple structure. For another, by using the smallest number of axioms to prove results, you get a deeper understanding of why the result is true.

\textbf{Lemma.} Fields are integral domains.

\textbf{Proof.} Let \( F \) be a field. I must show that \( F \) has no zero divisors. Suppose \( ab = 0 \) and \( a \neq 0 \). Then \( a \) has an inverse \( a^{-1} \), so \( a^{-1}ab = a^{-1} \cdot 0 \), or \( b = 0 \). Therefore, \( F \) has no zero divisors, and \( F \) is a domain.

\textbf{Example.} The ring of quaternions
\[
\mathbb{H} = \{ w + xi + yj + zk \mid w, x, y, z \in \mathbb{R} \}
\]
is a division ring, but not a field (it’s not commutative).

\textbf{Example.} Consider
\[
\mathbb{Q}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}.
\]

Use the operations inherited from the reals. This is clearly a commutative ring. To show that it’s a field, suppose \( a + b\sqrt{2} \neq 0 \). Then
\[
a + b\sqrt{2} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.
\]

I must show that \( a^2 - 2b^2 \neq 0 \).

If \( a = 0 \) and \( b \neq 0 \) or if \( a \neq 0 \) and \( b = 0 \), then \( a^2 - 2b^2 \neq 0 \). Since \( a + b\sqrt{2} \neq 0 \), the only other possibility is \( a, b \neq 0 \).

Thus, \( a^2 = 2b^2 \) with \( a, b \neq 0 \). Clearing denominators if necessary, I may assume that \( a \) and \( b \) are integers — in fact, positive integers, thanks to the squares. Now 2 divides \( 2b^2 \), so \( 2 \mid a^2 \). This forces \( 2 \mid a \), so \( a = 2c \) for some integer \( c \). Plugging in gives \( 4c^2 = 2b^2 \), or \( 2c^2 = b^2 \).

Repeat the argument: \( 2 \mid b^2 \), so \( 2 \mid b \), so \( b = 2d \). Plugging in gives \( 2c^2 = 4d^2 \), or \( c^2 = 2d^2 \).

I can continue this process indefinitely. Notice that \( a > c > \ldots \) and \( b > d > \ldots \). This yields infinite descending sequences of positive integers, contradicting well-ordering. Therefore, \( a^2 - 2b^2 \neq 0 \). (This is called an argument by \textit{infinite descent}.)

It follows that every nonzero element of \( \mathbb{Q}[\sqrt{2}] \) is invertible, so \( \mathbb{Q}[\sqrt{2}] \) is a field.

\textbf{Proposition.} A finite integral domain is a field.
**Proof.** Let \( R \) be a finite domain. Say
\[
R = \{ r_1, r_2, \ldots, r_n \}.
\]

I must show that nonzero elements are invertible. Let \( r \in R, r \neq 0 \).

Consider the products \( r r_1, r r_2, \ldots, r r_n \). If \( r r_i = r r_j \), then \( r_i = r_j \) by cancellation. Therefore, the \( r r_i \) are distinct. Since there are \( n \) of them, they must be exactly all the elements of \( R \):
\[
R = \{ r r_1, r r_2, \ldots, r r_n \}.
\]

Then \( 1 \in R \) equals \( r r_i \) for some \( i \), so \( r \) is invertible. \( \square \)

I need the following lemma, whose proof I’ll defer.

**Lemma.** Let \( m \) and \( n \) be integers, not both 0. There are integers \( a \) and \( b \) (not unique) such that
\[
(m, n) = am + bn.
\]

In other words, the greatest common divisor of two numbers can be written as a linear combination of the numbers.

**Proposition.** \( m \in \mathbb{Z}_n \) is a zero divisor if and only if \( (m, n) \neq 1 \).

**Proof.** First, I’ll show that if \( (m, n) = 1 \), then \( m \) is not a zero divisor. Suppose \( (m, n) = 1 \), so \( am + bn = 1 \) for some \( a, b \in \mathbb{Z} \). Reducing the equation mod \( n \), \( a'm = 1 \) for some \( a' \in \mathbb{Z}_n \), where \( a = a' \) mod \( n \).

Now suppose \( k \in \mathbb{Z}_n \) and \( mk = 0 \). Then
\[
a'm = 1, \quad a'mk = k, \quad 0 = k.
\]

Therefore, \( m \) is not a zero divisor.

Conversely, suppose that \( (m, n) = k > 1 \). Say \( n = ka \), where \( 1 < a < n \). In particular, I may regard \( a \) as a nonzero element of \( \mathbb{Z}_n \).

The order of \( m \) in \( \mathbb{Z}_n \) is
\[
\frac{n}{(m, n)} = \frac{n}{k} = a.
\]

Thus, \( ma = 0 \) in \( \mathbb{Z}_n \), and \( m \) is a zero divisor. \( \square \)

**Example.** (a) Find the zero divisors in \( \mathbb{Z}_{15} \).

The zero divisors are those elements in \( \{1, 2, \ldots, 14\} \) which are *not* relatively prime to 15:
\[
3, 5, 6, 9, 10, 12.
\]

For example, \( 5 \cdot 12 = 0 \in \mathbb{Z}_{15} \) shows directly that 5 and 12 are zero divisors. \( \square \)

(b) Find the zero divisors in \( \mathbb{Z}_7 \).

Since 7 is prime, all the elements in \( \{1, 2, 3, 4, 5, 6\} \) are relatively prime to 7. There are no zero divisors in \( \mathbb{Z}_7 \). In fact, \( \mathbb{Z}_7 \) is an integral domain; since it’s finite, it’s also a field by an earlier result. \( \square \)

The last example can be generalized in the following way.

**Corollary.** \( \mathbb{Z}_n \) is a field if and only if \( n \) is prime.

**Proof.** If \( n \) is composite, I may find \( a, b \) such that \( 1 < a, b < n \) and \( ab = n \). Regarding \( a \) and \( b \) as elements of \( \mathbb{Z}_n \), I obtain \( ab = 0 \) in \( \mathbb{Z}_n \). Therefore, \( \mathbb{Z}_n \) has zero divisors, and is not a domain. Since fields are domains, \( \mathbb{Z}_n \) is not a field.

Suppose \( n \) is prime. The nonzero elements \( 1, \ldots, n-1 \) are all relatively prime to \( n \). Hence, they are not zero divisors in \( \mathbb{Z}_n \), by the preceding result. Therefore, \( \mathbb{Z}_n \) is a domain. Since it’s finite, it’s a field. \( \square \)
The fields $\mathbb{Z}_p$ for $p$ prime are examples of fields of **finite characteristic**.

**Definition.** The **characteristic** of a ring $R$ is the smallest positive integer $n$ such that $n \cdot 1 = 0$. If there is no such integer, the ring has **characteristic** 0. Denote the characteristic of $R$ by char $R$.

**Example.** $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ are fields of characteristic 0. If $p$ is prime, $\mathbb{Z}_p$ is a field of characteristic $p$.

More generally, if $F$ is a field of characteristic $n \neq 0$, then $n$ is prime. For if $n$ is composite, write $n = rs$, where $1 < r, s < n$. Then

$$(r \cdot 1)(s \cdot 1) = rs \cdot 1 = n \cdot 1 = 0.$$

But $r \cdot 1 \neq 0$ and $s \cdot 1 \neq 0$ since $r, s < n$. Therefore, $F$ has zero divisors, contradicting the fact that fields are domains.

Note, however, that $\mathbb{Z}_p$ for $p$ prime is not the only field of characteristic $p$. In fact, for each $n \neq 0$, there is a unique field $F$ of characteristic $p$ such that $|F| = p^n$. □

**Lemma.** char $R = n$ if and only if $nr = 0$ for all $r \in R$.

**Proof.** ($\Rightarrow$) Suppose char $R = n$. If $r \in R$, then $r \cdot 1 = r$, so $n \cdot (r \cdot 1) = n \cdot r$.

$$n \cdot (r \cdot 1) = r \cdot 1 + \ldots + r \cdot 1 = r \cdot (1 + \ldots + 1) = r \cdot (n \cdot 1) = 0.$$ (n times) (n times)

($\Leftarrow$) $n \cdot r = 0$ for all $r \in R$ implies $n \cdot 1 = 0$. □

**Example.** $6 \cdot x = 0$ for all $x \in \mathbb{Z}_6$. Thus, $\mathbb{Z}_6$ has characteristic 6.

On the other hand, consider

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}.$$

This is an abelian group under addition, and becomes a commutative ring when multiplication is defined componentwise:

$$(a, b)(c, d) = (ac, bd).$$

For instance,

$$(1, 0)(0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0).$$

Note that $2(a, b) = (0, 0)$ for all $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$. It follows that $\mathbb{Z}_2 \times \mathbb{Z}_2$ has characteristic 2. □