Section 6.5 Rings and Fields

<table>
<thead>
<tr>
<th>Purpose of Section</th>
<th>To introduce the concept of an algebraic ring and a very specialized and important type of ring called a field.</th>
</tr>
</thead>
</table>

Introduction to Rings

Sets are often endowed with two binary operations, called addition and multiplication. Many examples come to mind, including the integers, rational, real, and complex numbers, as well as matrices, functions and polynomials. When we studied these sets as groups, we focused only on one operation, generally called addition, and ignored multiplication. However, in many situations, it is important to focus on both operations, which brings us to the algebraic structure called a ring\(^1\), initiated (in part) by the German mathematician Richard Dedekind (1831–1916) in the late 1800s.

Definition

A set \(\{R, +, \times\}\) with two (closed) binary operations \(+\) (addition) and \(\times\) (multiplication) is called a **ring** if:

1. The system with operation \(+\) forms a commutative group.
2. The operation \(\times\) is associative, that is
   \[
   (a \times b) \times c = a \times (b \times c).
   \]
3. The operation \(\times\) **distributive** over \(+\) both on the left and right:
   \[
   a \times (b + c) = (a \times b) + (a \times c) \\
   (b + c) \times a = (b \times a) + (c \times a)
   \]
   for all \(a, b, c \in R\).

We shamelessly call the ring operations \(+\) **and** \(\times\) *addition* and *multiplication*, although they do not necessarily denote addition and multiplication of numbers. Also, we often denote ring multiplication as \(ab\) for short. We also call the additive identity in the ring the **zero** (or **additive identity**) of the ring and often denote it by 0, and the multiplicative identity, naturally the **multiplicative identity** and often denote it by 1.

\(^1\) The word ring was coined by the German mathematician David Hilbert (1862-1943).
Note: Roughly, a `ring' is a set of elements having two operations, normally called addition and multiplication, which behave in many ways like the integers. You can add, subtract, multiply, but not (in general) divide. We must wait until we get to the general structure of a field to divide.

Special Kinds of Rings

• **Commutative Rings** A ring in which multiplication is commutative is called a **commutative ring**. (We don’t worry about addition here since addition is always commutative in a ring.)

• **Rings with Multiplicative Identity:** A ring which has a multiplicative identity, called the **multiplicative identity** (or **multiplicative unit**), is called a **ring with identity** or **ring with unity**.

• **Ring with Zero Divisors:** Nonzero elements \(a, b \in R\) in a ring are called **zero divisors** if their product is zero; that is \(ab = 0\) or \(ba = 0\) (0 being the additive identity in the ring). This condition may appear strange to the reader since the familiar rings of integers, rational, and real numbers with ordinary addition and multiplication do not have zero divisors.

**Example 1 (Common Infinite Rings) \(\mathbb{Z}, \mathbb{Q}, \mathbb{R}\)** The sets \(\mathbb{Z}, \mathbb{Q}, \mathbb{R}\) with the usual binary operations of addition and multiplication are all rings. The additive identity in each of these rings is 0 and the multiplicative identity is 1. None of these rings have zero divisors since \(ab \neq 0\) for nonzero \(a, b\).

**Note:** Although a general ring is not the integers with usual addition and multiplication, thinking of everything you know about the integers when working with general rings often helps bridge the gap to the abstract world.

**Example 2 (Polynomial Rings)** The set \(P(\mathbb{R})\) of all polynomials

\[
p_n(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0
\]

in the variable \(x\) and coefficients \(a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R}\) is a ring\(^2\) with the usual operations of polynomial addition and multiplication. The ring is commutative with multiplicative unit 1 (the constant polynomial \(p(x) \equiv 1\)). The ring has no zero divisors since the product of nonzero polynomials is never the zero (the zero polynomial).

---

\(^2\) It is also a ring if the coefficients are rational or complex numbers.
Historical Note: To give some idea of the mathematical prestige of the German university Gottingen in the mid 1800s, the great German Carl Gauss was winding down his monumental career. His last Ph.D student was Richard Dedekind, instrumental in the development of abstract algebra, and close friend and colleague of Peter Dirichlet, whose name we have seen before. If that weren’t enough, within a few weeks of Dedekind getting his Ph.D, so did another influential mathematician of the 19th century, Georg Riemann.

Example 3 (Ring of Order 2) The set $R = \{a, b\}$ with addition and multiplication defined by the tables

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th></th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>×</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a</td>
<td></td>
<td>b</td>
<td>a</td>
</tr>
</tbody>
</table>

is a commutative ring with no multiplicative unit and no divisors of zero. The proof is left to the reader. (See Problem 1.)

Example 4 (Ring of Matrices)

The set of all $2 \times 2$ matrices

$$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z} \right\}$$

under matrix addition and multiplication is a ring with respective additive and multiplicative identities

$$O_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The ring is not commutative since in general matrix multiplication does not commute. The ring does have zero divisors (infinitely many) since there are

---

3 This ring has no meaning related to ordinary arithmetic beyond these tables.
4 It is also a ring for $n \times n$ matrices.
nonzero matrices $A, B$ whose product is the zero matrix (additive identity). An example is

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

**Example 5 (Ring of Even Integers)** The set of even integers

$$2\mathbb{Z} = \{0, \pm 2, \pm 4, \cdots \}$$

is a commutative ring with operations of addition and multiplication. However, the ring does not have a multiplicative identity since it does not include 1. The ring also does not have zero divisors (considered a good thing).

**Examples of rings lacking particular conditions:**

1. Ring without multiplicative identity: even integers $2\mathbb{Z}$.
2. Ring without multiplicative commutativity: matrices.
3. Ring without multiplicative associativity: octonians\(^5\).
4. Ring without multiplicative inverse: integers.

**Algebraic Fields**

The history of mathematics is the history of inventing new number systems to solve existing problems that have “no solutions” in existing number systems. The invention of the negative numbers was a direct consequence of seeking solutions to equations like $x + 8 = 5$, which has now solution in the natural number system. By a similar token, the invention of the rational numbers had its motivation in solving equations like $3x = 7$, which has no solution in the ring of integers. This leads us to invent an algebraic structure for which the rational numbers is a prototype. Such a structure is called a field.

**Definition** A field is a set $F$ with at least two elements with two (closed) binary operations $+$ and $\times$ such that:

- $i)$ $F$ is a commutative group under $+$

\(^5\) Octonians are eight dimensional hyper-complex numbers which are extensions of the two dimensional field of complex numbers.
The nonzero elements of \( F \) form a commutative group under \( \times \).

\( \times \) is distributive over \( + \).

**Note:** Roughly, a field is a set of elements having two operations, usually called addition and multiplication, which behaves in many ways like the rational numbers. You can add and multiply the elements in a field and you can divide elements by any non-zero element to get another element in the field. The prototypical field is the rational numbers \( \mathbb{Q} \) with the usual addition and multiplication.

Although we are apt to think of fields as the standard fields from analysis, like the rational numbers \( \mathbb{Q} \), real numbers \( \mathbb{R} \), or the complex numbers \( \mathbb{C} \) with standard operations of addition and multiplication, it may come as a surprise that there are finite fields as well. In fact, for any prime number there is finite field \( F_p = \mathbb{Z}/p\mathbb{Z} \) consisting of integers \( 0,1,2,...,p-1 \) with addition and multiplication reduced modulo a prime number\(^6\) \( p \). Finite fields (often called Galois fields) are important in computer science and coding theory. There are also finite fields for every prime power \( p^k, k = 1,2,... \), which means there are fields \( 3^3 = 27 \) and \( 2^7 = 128 \) elements, although it is not a trivial matter to find them. On the other hand there are no fields with 6 or 10 elements.

**Example 6 (Rational Numbers)**

The prototypical field is the field of rational numbers \( \mathbb{Q} \) with the usual operations of addition and multiplication. The additive inverse of each fraction \( a/b \) is simply \(-a/b\), and the multiplicative inverse of \( a/b \) is \( b/a \), both can be verified by observing

\[
\frac{a}{b} + \left( -\frac{a}{b} \right) = 0
\]

\[
\frac{a}{b} \times \frac{b}{a} = 1
\]

Multiplication is also a distributive operation which can be seen from the simple calculations:

---

\(^6\) If \( p \) is not prime the set \( \mathbb{Z}/n\mathbb{Z} \) is never a field.
Example 7 (Boolean Field) The simplest field is the Boolean field \( F = \{0,1\} \) with two binary operations \( + \) (addition mod 2) and \( \times \) (multiplication mod 2), which is the mathematics of electrical circuits, with 1 being "on" and 0 being "off." It is an easy matter but tedious matter to show this is an algebraic field. See Problem 1.

\[
\begin{array}{c|c|c}
+ & 0 & 1 \\
\hline
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}
\begin{array}{c|c|c}
\times & 0 & 1 \\
\hline
0 & 0 & 0 \\
1 & 1 & 0 \\
\end{array}
\]

Boolean Field \( F_2 \)

Rings which are not Fields

- **(Polynomial Rings)** The ring of polynomials with real coefficients with the usual addition and multiplication is a ring but not a field since polynomials don't in general have multiplicative inverses. For example \( p(x) = x^2 + 2x + 1 \) has no multiplicative inverse (i.e. no polynomial \( q(x) \) so that \( p(x)q(x) = 1 \) for all \( x \)).

- **(Matrix Rings)** The ring of \( n \times n \) matrices with the usual matrix addition and multiplication is a ring, but not a field since matrices with zero determinant do not have multiplicative inverses.

- **(Mod \( n \) Rings with Composite Modulo)** The set \( \{0,1,2,\ldots,n-1\} \), where addition and multiplication are performed modulo \( n \), where \( n \) is a composite number (not a prime) is a ring but not a field. Example 8 illustrates this idea for composite \( n = 4 \).
Example 8 (What Goes Wrong with $\mathbb{Z}_4$?)

The set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with ordinary addition and multiplication modulo 4 (i.e. regular addition and multiplication but when a number gets past 3, one begins anew at 0). The addition and multiplication are defined by the following tables.

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\]

Addition table

\[
\begin{array}{c|cccc}
\times & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 0 & 2 \\
3 & 0 & 3 & 2 & 1 \\
\end{array}
\]

Multiplication Table

$\mathbb{Z}_4$ is a commutative ring with multiplicative identity 1, but is not a field since 2 has no inverse (i.e. there is no element $x$ which makes $2x = 1$).

However, the set $\mathbb{Z}_p$ with $p$ prime is a field as the following example illustrates.

Example 9 (Modulo Prime Number Field $\mathbb{Z}_5$)

The set $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ with mod 5 arithmetic, defined by the following tables, is a field.

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 & 4 \\
\hline
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 & 0 \\
2 & 2 & 3 & 4 & 0 & 1 \\
3 & 3 & 4 & 0 & 1 & 2 \\
4 & 4 & 0 & 1 & 2 & 3 \\
\end{array}
\]

Addition table
The German mathematician Richard Dedekind called a set of real or complex numbers closed under the four arithmetic operations of addition, subtraction, multiplication, and division a field. He used the German word “korper” (body) for this concept. The word “ring” was originally used by German mathematician David Hilbert.

### Roots of Equations and Field Extensions

Although the polynomial equation \( x^2 - 2 = 0 \) does not have a root in the field of rational numbers \( \mathbb{Q} \), we can extend the field to a larger one (of which \( \mathbb{Q} \) is a subfield) that contains the roots \( \pm \sqrt{2} \) of our equation \( x^2 - 2 = 0 \). We can do this taking the extended number field

\[
\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \}
\]

which can easily been seen to be a field with the two binary operations

\[
(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}
\]

\[
(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}
\]

Note that any nonzero \( a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \) has a multiplicative inverse

\[
(a + b\sqrt{2}) \left( \frac{1}{a + b\sqrt{2}} \right) = 1
\]

which is also a member of \( \mathbb{Q}[\sqrt{2}] \) which can be seen from
as required for members in a field. This new “enlarged” field contains the rational numbers and also contains the roots \( \pm \sqrt{2} \) when \( a = 0, b = \pm 1 \).

The history of mathematics is a history of seeking new number systems for problems that have no solution in existing number systems. Continuing further, the equation \( x^2 + 1 = 0 \) has no root in the field of real numbers, so we extend the real numbers to the complex numbers by forming

\[
\mathbb{R}[\sqrt{-1}] = \{ a + b\sqrt{-1} : a, b \in \mathbb{Z} \} = \{ a + bi : a, b \in \mathbb{Z} \}
\]

where we define \( i = \sqrt{-1} \). This field extension of \( \mathbb{R} \) is called the complex numbers and denoted by \( \mathbb{C} = \mathbb{R}[i] \), and has binary operations

\[
(a + bi) + (c + di) = (a + c) + (b + d)i
\]

\[
(a + bi)(c + di) = (ac - bd) + (ad + bc)i
\]

is a field. Note too that any nonzero \( a + bi \in \mathbb{C} \) has a multiplicative inverse

\[
(a + bi)\left(\frac{1}{a + bi}\right) = 1
\]

which can be seen from

\[
\frac{1}{a + bi} = \left(\frac{1}{a + bi}\right)\left(\frac{a - bi}{a - bi}\right)
\]

\[
= \frac{a - bi}{a^2 + b^2}
\]

\[
= \left(\frac{a}{a^2 + b^2}\right) + i\left(\frac{-b}{a^2 + b^2}\right) \in \mathbb{C}
\]

as required for elements in a field. This new field contains the rational numbers and also contains the roots \( \pm i \) when \( a = 0, b = \pm 1 \).
Fortunately, in 1799 with the proof of the Fundamental Theorem of Algebra by Carl Gauss, every \( n \)th order polynomial equation with complex (which includes real) coefficients, has exactly \( n \) (included repeated) roots which are all complex (which includes real numbers). This shows there is no need to extend number systems beyond the complex numbers to larger number fields insofar as seeking solutions to polynomial equations.

There are larger number systems than the complex numbers, such as \textbf{quaternions} and \textbf{octonians}, called \textbf{hypercomplex numbers}, which are 4 and 8 dimensional extensions of the two-dimensional complex numbers, but these systems are not fields. The quaternions constitute what is called an associative algebra where multiplication is not commutative.
Problems

1. **(Boolean Ring)** Show that the Boolean ring in Example 1 is a ring.

2. **Ring of Matrices** Show that the set of all 2 by 2 matrices

   \[
   R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z} \right\}
   \]

   is a ring under matrix addition and matrix multiplication is a ring with a multiplicative element, but it is not commutative and it is not a field.

3. **(Integral Domains)** A commutative ring \( R \) with multiplicative identity that has no divisors of zero is called an integral domain. Show that in any ring that is an integral domain for which \( a,b,c \in R, \ a \neq 0 \), the cancellation law

   \[ ab = ac \Rightarrow b = c \]

   holds. Are the rings \( \mathbb{Z}, \mathbb{Q}, \mathbb{R} \) with ordinary addition and multiplication integral domains?

4. **(Gaussian Integers)** A complex number \( a + bi \) where \( a,b \in \mathbb{Z} \) are integers is called a Gaussian integer, named after the German mathematician Karl Gauss (1777–1856) who first studied them. Show that the Gaussian integers are a ring with respect to ordinary addition and multiplication, where addition and multiplication are defined by

   \[
   \begin{align*}
   (a + bi) + (c + di) &= (a + c) + (b + d)i \\
   (a + bi)(c + di) &= (ac - bd) + i(bc + ad)
   \end{align*}
   \]

5. **(Principle Ideals in \( \mathbb{Z} \))** In the ring of integers \( \mathbb{Z} \) with operations of addition and multiplication, for any fixed \( n \in \mathbb{Z} \) the set of all multiples

   \[ \langle n \rangle = \{ nx : x \in \mathbb{Z} \} \]

   is called the principal ideal generated by \( n \in \mathbb{Z} \).

   a) What is the principle ideal generated by 1?
   b) What is the principal ideal generated by 2?
   c) What is the principle ideal generated by 5?
d) Show that the principle ideal generated by \( n \) is a subset of any principle ideal generated by any factor \( m \) of \( n \). For example \( \langle 10 \rangle \subseteq \langle 5 \rangle \).

e) If \( m \mid n \) (i.e. \( m \) divides \( n \)) then \( \langle n \rangle \subseteq \langle m \rangle \).

6. **(Fun Problem)** Show that the square of a number ending in 5, say \( A5 \) (such as 75 where \( A = 7 \) or 125 where \( A = 12 \)) is equal to \( A(A+1) \) with a 25 after it. For example \( 65^2 \) is \( 6(7) = 42 \) followed by 25, or 4225. Hint: Use the distributive property of multiplication over addition and the place value system of natural numbers.

7. **(Subrings)** A subring of a ring is a subset of a ring which is a ring in its own right using the binary operations of the ring. Show that the subset

\[
D = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R} \right\}
\]

is a subring of the ring of all \( 2 \times 2 \) matrices with real elements.

8. **(Field Extension of \( \mathbb{Q} \))** Show that the set

\[
\mathbb{Q}[\sqrt{2}] = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \right\}
\]

with ordinary addition and multiplication is a field.

---

7 This problem was discovered in Foundations of Mathematics by Thomas Q. Sibley