Section 6.5 Rings and Fields

Purpose of Section To introduce the concept of an algebraic ring and an important type of ring called a field. We also hint at the idea of a field extension.

Introduction to Rings

An algebraic group is a set with one binary operation. The most common algebraic system we have all studied since grade school has two binary operation, addition and multiplication. This leads us to the abstract study of rings and fields. We begin with one of the most important abstract systems with two binary operations called a ring[1]. You have seen examples of rings before. The integers $\mathbb{Z}$ with ordinary addition $(+)$ and multiplication $(\times)$ is an example of an algebraic ring. In this regard, you might think of a ring as a generalization of the integers. The study of rings was 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 of $+$ (addition) and $\times$ (multiplication) is called a **ring** if:

a) The system with operation $+$ forms a **commutative group**.
b) The operation $\times$ is **associative**. In the language of predicate logic:

$$(\forall a,b,c \in R)\left[(a\times b)\times c = a\times(b\times c)\right].$$

c) The operation $\times$ **distributive** over $+$ both on the left and right. In other words

- $(\forall a,b,c \in R)\left[a\times(b+c) = (a\times b)+(a\times c)\right]$
- $(\forall a,b,c \in R)\left[(b+c)\times a = (b\times a)+(c\times a)\right]$

We call the ring operation $+$ addition and $\times$ multiplication, although they do not necessarily denote addition and multiplication of numbers. We also often denote ring multiplication by ab for shorthand. We also call the additive identity in the ring, the **zero** (or **additive identity**) of the ring, and denote it by 0. A ring need not have a multiplicative identity, but when it does, we say the ring has a **multiplicative identity** (or **unity**) and is denoted by, you guessed it, 1.

[1] The word ring was coined by the German mathematician David Hilbert (1862-1943).

Important 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, and multiply elements in a ring but not, in general divide them. We must wait until we get to the general structure of a field before we can add, subtract, multiply, and divide.

Special Kinds of Rings

• **Commutative Rings** If multiplication commutes, i.e. $ab = ba$, then the ring is called a **commutative ring.** We don't worry about addition since addition always commutates in a ring.

• **Rings with Multiplicative Identity:** A ring with a multiplicative identity is called a **ring with identity**. Again, we don't worry about an additive identity since rings always have an additive identity.

• **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. But some rings, such as rings of matrices with ordinary addition and multiplication, have non-zero matrices whose product is the zero matrix.

Common Rings

• **Example 1** The integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ with usual addition and multiplication is a commutative ring with the multiplicative identity of 1.

• **Example 2** The set $\mathbb{Z}[x]$ of all polynomials in x with integer coefficients and usual addition and multiplication is a commutative ring with multiplicative identity $f(x) = 1$.

• **Example 3** The set $2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$ of even integers with usual addition and multiplication is a commutative ring without a multiplicative identity.

• **Example 4** The set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with addition and multiplication modulo n is a commutative ring with multiplicative identity 1. This ring is called the ring of integers modulo n.

• **Example 5** The set $M_2(\mathbb{Z})$ of all 2×2 matrices with integer entries is a non-commutative ring with multiplicative identity

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

- **Example 6** The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ with the usual addition and multiplication are all rings. The additive identity in each of these rings is 0 and the multiplicative identity is 1.

Important Note: You can't always solve simple linear algebraic equations in rings. In the ring of integers $\mathbb{Z}$ with ordinary addition and multiplication, you can't solve the equation $2x = 1$ since 1/2 is not in the ring. Rings are meant for adding, subtracting, and multiplying, not dividing.

Example 7 Special Ring Draw the addition and multiplication tables for the ring $\mathbb{Z}_3 = \{0,1,2\}$ with addition and multiplication modulo the prime number 3,

Solution: Carrying out these operations, we find

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

addition modulo 3

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

multiplication modulo 3

Note that the addition table forms a commutative group, and if we only look at the nonzero members $\{1,2\}$ of the multiplication table, they form a commutative group of order 2. This is special kind of group is called a field. But not all rings are so nice as the following example illustrates.

Example 8 The Cyclic Group Ring Draw the addition and multiplication tables for the ring

$$\mathbb{Z}_6 = \{0,1,2,3,4,5\}$$

with addition and multiplication modulo 6,

Solution Carrying out these operations, we find

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

addition modulo 6

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

multiplication modulo 6

Although the addition table for $\mathbb{Z}_6$ forms a commutative group with additive identity 0, the nonzero members of the multiplication table do not form a group for several reasons. The numbers 2, 3 and 4 do not have multiplicative inverses. This can be seen since there is no member of the ring that satisfies the equations $2\times a=1,\ 3\times a=1,\ 4\times a=1.$

Important Note: Roughly, a ring is an abstract system where you can add, subtract and multiply but not divide. To divide, you need the additional structure of an algebraic field.

Example 9 Ring of Sets There are structures in mathematics that have nothing to do with numbers which form rings. For example, the power set $P(X)$ of a set X is a ring if the ring addition $\oplus$ and multiplication $\otimes$ are defined by

- $A \oplus B = (A-B)\cup(B-A)$
- $A \otimes B = A \cap B$

Find the addition and multiplication tables for this ring for the power set of $X=\{a,b\}$.

Solution: The power set is $P(X)=\{\varnothing,\{a\},\{b\},\{a,b\}\}$ and the addition and multiplication tables are

$\oplus$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\varnothing$	$\{a,b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\varnothing$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\varnothing$

$\otimes$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
$\{a\}$	$\varnothing$	$\{a\}$	$\varnothing$	$\{a\}$
$\{b\}$	$\varnothing$	$\varnothing$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$

The empty set $\varnothing$ is the additive zero of the group. The additive inverse of each member of the ring is itself. There is no multiplicative identity in the ring.

Historical Note: Emmy Noether (1882-1935) was a German mathematician who made groundbreaking contributions to ring theory and theoretical physics. She was described by Albert Einstein as the most important woman in the history of mathematics. *Noether's theorem* has been called one of the most significant results in theoretical physics and gives a fundamental connection between symmetry and conservation laws.

Problem with Rings (No Division) Although rings are important algebraic structures in the study of many mathematical structures[2], they sometimes are too restrictive. For example, it is possible that a and b are nonzero elements of a ring but their product $ab = 0$ is zero. An example of a ring of this type is the set of 2×2 matrices with the usual addition and multiplication of matrices. Note that

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

where the product of two non-zero members of the ring have a zero product. There are also rings where division is not possible for non-zero members. For example, in the ring of integers $\mathbb{Z}$ under ordinary addition and multiplication, we cannot divide 3 by 5 to obtain a member of the ring. This leads us to the study of the algebraic field.

[2] Ring theory is fundamental in algebraic geometry where rings of polynomials are important.

Algebraic Fields Rings allow for addition, subtraction, and multiplication, but no division. The equation $3x = 7$ has no solution in the ring of integers, but does have a solution in the *field* of rational numbers.

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

- F is a commutative group under $+$.
- The nonzero elements of F form a commutative group under $\times$.
- $\times$ is distributive over $+$.

Important Note: A field is a ring with some extra requirements. In particular a field is a ring where the nonzero members form a group under multiplication. What this means is that for any $b \in F, b \neq 0$, its multiplicative inverse $b^{-1} \in F$ also belongs to the field, and hence for any $a, b \in F, b \neq 0$ the "quotient" $a/b \equiv a \times b^{-1}$ also belongs to F. Hence, we now have division in the mix.

When one thinks of a field, one thinks of a structure with two operations resembling addition and multiplication where one can add, subtract, multiply, and divide. The reader is well aware of three common fields from analysis, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$.

Finite Fields

There are other important fields in mathematics, however, like finite fields which contain only a finite number of elements. Finite fields play an important role in many areas of mathematics, including algebraic geometry and number theory, as well as applied areas like coding theory and cryptography.

An interesting aspect of finite fields is that they exist only for certain orders. For example, there is a finite field of order 2, 3, 4, and 5, but none of order six. There is a field of order 7, 8, 9, but none of 10. To be specific, there is a field of order p^n, $n = 1, 2, \ldots$ where p is any prime number, but no others. These finite fields are called **Galois fields** and denoted by GF(p^n)[3]. For example, there exist fields of orders

[3] GF(p^n) stands for Galois field in honor of the French mathematician Evariste Galois (1811-1832) who first studied them.

$$2, 2^2, 2^3, \ldots, 2^n, \ldots$$
$$3, 3^2, 3^3, \ldots, 3^n, \ldots$$
$$5, 5^2, 5^3, \ldots, 5^m, \ldots$$
$$7, 7^2, 7^3, \ldots, 7^n, \ldots$$
$$\ldots \quad \ldots$$

However, there are no fields of order 6, 10, 12, 14, 15, 18, 20, 21,…

There are two main classifications in the study of finite fields. The first is the study of fields GF(p) of prime order, and the more involved fields when $n > 1$. When $n = 1$ the field GF(p) is the field of permutations $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ of integers with addition and multiplication modulo p .However, we saw in Example 8 that the multiplication table for $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, omitting 0, was not a field. In other words, $\mathbb{Z}_n$ is a field only when n is a prime number.

Important Note: Groups, rings and fields are examples of what one calls "abstract algebras." Other abstract algebras are integral domains, vector spaces, modules, associative algebras, Boolean algebras, skew fields, …. .

Example 9: Galois Field Draw the addition and multiplication table for the Galois field

$$\mathrm{GF}(7) = \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}.$$

and find the additive and multiplicative inverses of each element 0,1,2,…, 6.

Solution: Performing addition and multiplication modulo 7, we arrive at the tables in Table 1. The additive inverse of a number is found by moving across the number's row until reaching 0, where the additive inverse is the column number. A similar principle holds for multiplicative inverses.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Multiplication modulo 7

a	$-a$	a^{-1}
0	0	–
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Additive and multiplicative inverses modulo 7

Arithmetic operations for the field $\mathrm{GF}(7) = \mathbb{Z}_7$

Table 1

Example 10: Subtraction and Division mod 7 Since $\text{GF}(7) = \mathbb{Z}_7$ is a field, we should be able to carry out all four arithmetic operations: addition, subtraction, multiplication, division. Table 2 shows us how to add and multiply. What are the values of $2-5$ and 5/3?

Solution

To find the difference $x = 2-5$, we seek the value of x which satisfies $x+5=2$. From Table 2 we find $x=4$. To find the quotient $5/3 = 5\times 3^{-1}$ realize that $3^{-1}=5$ since $3\times 5 = 1$. Hence,

$$5/3 = 5\times 3^{-1} = 5\times 5 = 4.$$ ∎

Multiplication in the Galois Field $\text{GF}(2^2)$

In the Galois field $\text{GF}(2) = \mathbb{Z}_2 = \{0,1\}$ arithmetic is carried out mod 2, both for addition and multiplication as shown in Table 2.

+	0	1		×	0	1
0	0	1		0	0	0
1	1	0		1	0	1

Arithmetic in $\text{GF}(2) = \mathbb{Z}_2$

Table 2

There is only one set of four elements where one can define an "arithmetic system" satisfying the axioms of a field, and that system is the Galois field $\text{GF}(2^2) = \{0,1,a,b\}$ defined by the addition and multiplication tables in Table 3.

+	0	1	*a*	*b*		×	0	1	*a*	*b*
0	0	1	*a*	*b*		0	0	0	0	0
1	1	0	*b*	*a*		1	0	1	*a*	*b*
a	*a*	*b*	0	1		*a*	0	*a*	*b*	1
b	*b*	*a*	1	0		*b*	0	*b*	1	*a*

Only finite group of order 4

Table 3

Important Note: The late 1800s and early 1900s saw a shift in the philosophy of mathematics. The emphasis moved from the study of concrete objects to a more general theory. For instance, the study of various permutation groups morphed into the general notion of an abstract group.

The question then is, how does one construct the addition and multiplication tables in Figure 3? To do this, we denote the elements of the field by

$$\mathrm{GF}(2^2) = \{0, 1, x, x+1\}$$

where $x, x+1$ are linear polynomials in x, and addition and multiplication in the field are carried out mod (x^2+x+1),where the coefficients of x^2+x+1 obey mod 2 arithmetic. For example (watch carefully),

$$(x+1)\times(x+1) = x^2+2x+1 = x^2+1$$

(Remember, 0 = 2 and 1 = -1 in mod 2 arithmetic.) We then reduce x^2+1 modulo (x^2+x+1), getting

$$\frac{x^2+1}{x^2+x+1} = 1 - \frac{x}{x^2+x+1}$$

which gives a remainder of $-x$. But $-x = (-1)\times x = 1\times x = x$ in $\mathbb{Z}_2$ arithmetic, so we have the product as

$$(x+1)\times(x+1) = x.$$

Addition can also be carried out using these rules, We have

$$x + (x+1) = (2x+1) \bmod (x^2+x+1) = 1$$

The reader can fill in the rest of the addition and multiplication tables shown in Table 4. See Problem 9.

$+$	0	1	x	$x+1$		$\times$	0	1	x	$x+1$
0	0	1	x	$x+1$		0	0	0	0	0
1	1	0	$x+1$	x		1	0	1	x	$x+1$
x	x	$x+1$	0	1		x	0	x	$x+1$	1
$x+1$	$x+1$	x	1	0		$x+1$	0	$x+1$	1	x

Arithmetic in the field $\mathrm{GF}(2^2)$

Table 4

Historical Note: 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.

Problems

1. **True or False**

   a) A ring can be finite or infinite.
   b) In a ring $\{R, +, \times\}$, the set R with $\times$ is a group.
   c) In a ring $\{R, +, \times\}$, the set R with $+$ is a group.
   d) The ring $\mathbb{Z}_{11}$ is also a field.
   e) The ring $\mathbb{Z}_8$ is also a field.
   f) There are fields where $a \times b = 0$ but neither a, b are zero.

2. **Multiplicative Identity** For each of the following rings, tell if the ring is commutative and if there exists a multiplicative identity. If a multiplicative identity exists, what is it?

   a) The ring of integers $\mathbb{Z}$ with usual addition and multiplication
   b) The ring of even integers $2\mathbb{Z}$ with usual addition and multiplication.
   c) The ring $C(\mathbb{R})$ of real-valued continuous functions with usual addition and multiplication.
   d) The ring consisting of the set
   $$\mathbb{Z}\left[\sqrt{2}\right] = \left\{m + n\sqrt{2} : m, n \in \mathbb{Z}\right\}$$
   with usual addition and multiplication.
   e) The ring $\mathbb{Z}[x]$ of all polynomials in x whose coefficients are integer with ordinary addition and multiplication.
   f) The ring $\mathbb{Q}$ of rational numbers with ordinary addition and multiplication.
   g) The ring consisting of the set $\mathbb{Z}_3 = \{0, 1, 2\}$ where addition and multiplication are defined modulo 3.

3. **Rings Lacking Properties** Find rings which lack the given property.

   a) Ring without multiplicative identity.
   b) Ring where multiplication does not commute.
   c) Ring without a multiplicative inverse. .

4. **Ring of Matrices** Show that the set of all 2×2 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, but not a field.

5. **Rings which are not Fields** Why are the following rings not fields ?

a) The ring of polynomials with real coefficients with the usual addition and multiplication.

b) The ring of $n \times n$ matrices with the usual matrix addition and multiplication.

c) The set $\mathbb{Z}_n = \{0,1,2,...,n-1\}$, where the operations of addition and multiplication are performed mod n, where n is a composite natural number.

6. **Mod 3 Field** The addition and multiplication tables for $\mathbb{Z}_3$ is shown below. What are the additive and multiplicative inverses for every member of the field.

+	0	1	2		×	0	1	2
0	0	1	2		0	0	0	0
1	1	2	0		1	0	1	2
2	2	0	1		2	0	2	1

7. **Arithmetic in** $\mathbb{Z}_3$ In the field $\mathrm{GF}(3) = \mathbb{Z}_3$ compute

a) $1+2$ Ans: 0
b) $1-2$ Ans: 2
c) 2×2
d) $1/2$

8. **Modular Arithmetic** Find an integer x such that it satisfies the following equations.

a) $2x = 1 \pmod 3,\ x \in \mathbb{Z}_3$
b) $3x = 2 \pmod 5,\ x \in \mathbb{Z}_5$
c) $4x = 3 \pmod 7,\ x \in \mathbb{Z}_7$

9**. Galois Field** $GF(2^2)$ Verify the addition and multiplication tables for $GF(2^2)$ shown in Table 4.

10. **Multiplicative Inverse** The integers $\mathbb{Z}$ under usual addition and multiplication form a commutative ring with unity 1. Do any members of this ring have multiplicative inverses? If so, what are they?

11.**Type of Ring** The set $\{0,a,b,c\}$ with operations of addition and multiplication, defined by the following tables, forms a ring. Is this group commutative and does it have a multiplicative identity?

$\oplus$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$\otimes$	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	b	c	a
c	0	c	a	b

Zero Divisors and Integral Domains

In some rings, things don't obey the arithmetic you learned in grade school. For example, in the ring $\mathbb{Z}_4 = \{0,1,2,3\}$ modulo 4 arithmetic, we found $2 \times 2 = 0$. In this case, we say that 2 is a zero divisor for this ring. In general, an element $a \in R$ in a ring is a **zero divisor** if there is a nonzero element $b \in R$ in the ring such that $ab = 0$. Matrix rings also have zero divisors.

12. **Zero Divisors** Find a zero divisor in the ring of 3×3 matrices with integer entries using the usual operations of addition and multiplication?

ΓΣΘΨΞΠΩ