Chapter 8
Introduction to Rings

We now move on to the second major type of algebraic object that we are considering: the ring. At first blush, rings look a bit more complicated than groups. Indeed, a ring is an abelian group written additively, and we must still impose a multiplication operation along with several new rules. But in another sense, rings are easier to deal with, because they are more familiar. Indeed, when we think of a ring, we tend to think of the integers (although, as we shall see, the integers are actually a special sort of ring).

In this chapter, we will define a ring and prove some properties of rings and subrings. We shall also discuss two well-behaved types of rings; namely, integral domains and fields.

8.1 Rings

Let us now define a ring.

Definition 8.1. A **ring** is a set R together with two binary operations, written as addition and multiplication, such that

1. R is an abelian group under addition;
2. if $a, b \in R$, then $ab \in R$ (closure under multiplication);
3. if $a, b, c \in R$, then $(ab)c = a(bc)$ (associativity of multiplication);
4. if $a, b, c \in R$, then $a(b + c) = ab + ac$ (distributive law); and
5. if $a, b, c \in R$, then $(a + b)c = ac + bc$ (distributive law).

As usual when we have an additive group, we will use additive notation. In particular, we write 0 for the additive identity of a ring, and $-a$ for the additive inverse of a. Notice that we do not insist that the multiplication operation be commutative.

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1_8

Definition 8.2. A ring R is said to be a **commutative ring** if $ab = ba$ for all $a, b \in R$.

Also, while there is an identity for the addition operation, there does not have to be one for the multiplication operation.

Definition 8.3. A ring R is said to be a **ring with identity** if R has an element, denoted 1, such that $1a = a1 = a$ for all $a \in R$. In this case, we call 1 the **identity** of R.

Note that if we refer to the identity in a ring, we mean the multiplicative identity 1 (if it exists), not the additive identity 0.

Example 8.1. As we observed in Section 2.4, the sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all commutative rings with identity, under the usual addition and multiplication operations. Also, we saw in Section 2.5 that the same can be said for $\mathbb{Z}_n$, for any positive integer $n \geq 2$.

Example 8.2. The set of even integers, $2\mathbb{Z}$, can easily be seen to be a commutative ring without an identity. There is no even integer that can be multiplied by 2 to get 2.

Example 8.3. The set of all polynomials with real coefficients is a commutative ring with identity, using the usual polynomial addition and multiplication operations. We denote it by $\mathbb{R}[x]$. The same can be said for the polynomials with integer coefficients, $\mathbb{Z}[x]$. In each case, the identity is the constant polynomial, 1.

How about an example of a noncommutative ring?

Example 8.4. Let n be a positive integer. Then the $n \times n$ matrices with real entries form a ring under matrix addition and multiplication. The identity matrix is the identity of the ring. However, if $n > 1$, then it is not a commutative ring as, for instance, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We denote this ring by $M_n(\mathbb{R})$. In fact, as we observe in Appendix B, we can substitute entries from any ring R in place of the real numbers, and we obtain a new ring, $M_n(R)$. If R is a ring with identity, then we can form the identity matrix, so $M_n(R)$ is also a ring with identity. The conditions under which it is a commutative ring are discussed in Exercise 8.10.

We also have a way of constructing new rings from old, simply extending the idea of the direct product of groups.

Definition 8.4. Let R and S be rings. Then the **direct sum** of R and S, denoted $R \oplus S$, is the Cartesian product $R \times S$ under the operations

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ and } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2),$$

for all $r_i \in R$, $s_i \in S$.

Theorem 8.1. *Let R and S be rings. Then $R \oplus S$ is a ring. Furthermore, if R and S are commutative rings, then so is $R \oplus S$. Also, if R and S are rings with identity, then so is $R \oplus S$.*

Proof. The proof is very similar to that of Theorem 3.1. The ring properties all hold in the direct sum because they hold in R and S. We will prove one of the distributive laws, and leave the rest as Exercise 8.6.

Take $r_i \in R$, $s_i \in S$. Then

$$\begin{aligned}(r_1, s_1)((r_2, s_2) + (r_3, s_3)) &= (r_1, s_1)(r_2 + r_3, s_2 + s_3)\\ &= (r_1(r_2 + r_3), s_1(s_2 + s_3))\\ &= (r_1r_2 + r_1r_3, s_1s_2 + s_1s_3)\\ &= (r_1r_2, s_1s_2) + (r_1r_3, s_1s_3)\\ &= (r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3).\end{aligned}$$

□

Example 8.5. In $\mathbb{Z}_5 \oplus \mathbb{Z}_6$, we have $(3, 5)+(4, 2) = (7, 7) = (2, 1)$ and $(3, 5)(4, 2) = (12, 10) = (2, 4)$.

One additional point is important to keep in mind. A ring is a group under addition, not under multiplication! While the multiplication operation satisfies the closure and associativity properties, a ring does not have to have an identity. And even if it does, elements do not have to have inverses. For instance, $\mathbb{Z}$ has an identity, but there is nothing we can multiply by 2 to obtain 1.

Exercises

8.1. Write the addition and multiplication tables for the ring $\mathbb{Z}_5$.

8.2. Write the addition and multiplication tables for the ring $\mathbb{Z}_3 \oplus \mathbb{Z}_2$.

8.3. Let $R = \{0, 3, 6, 9, 12\}$ with addition and multiplication in $\mathbb{Z}_{15}$. Is R a ring? If so, is it commutative, and does it have an identity?

8.4. Let R be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$, under addition and multiplication of functions. Is R a ring? If so, is it commutative, and does it have an identity?

8.5. Let R be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$. Let the addition operation be the usual addition of functions, but let the multiplication operation be composition. That is, the product of α and β is $\alpha \circ \beta$. Is R a ring? If so, is it commutative, and does it have an identity?

8.6. Complete the proof of Theorem 8.1.

8.7. Let R be the set of matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, for all $a, b, c \in \mathbb{Z}$. Is R a ring under matrix addition and multiplication? If so, is it commutative, and does it have an identity?

8.8. Show that every ring with a prime number of elements is commutative.

8.9. Must a ring with a prime number of elements be a ring with identity?

8.10. Let R be a ring and n a positive integer. Under what conditions is $M_n(R)$ commutative?

8.2 Basic Properties of Rings

Let us mention a few straightforward properties of rings.

Theorem 8.2. *Let R be a ring. Then the additive identity, 0, is unique. If R has a multiplicative identity 1, then it too is unique.*

Proof. As R is a group under addition, we see from Theorem 3.2 that 0 is unique. Suppose that a and b are both multiplicative identities for R. As a is an identity, $ab = b$. But as b is an identity, $ab = a$. Thus, $a = b$. □

Theorem 8.3. *Let R be a ring. If $a, b \in R$, then*

1. $0a = a0 = 0$;
2. $(-a)b = a(-b) = -(ab)$; *and*
3. $(-a)(-b) = ab$.

Proof. (1) As $0 = 0 + 0$, we have $0a = (0 + 0)a = 0a + 0a$. Adding $-0a$ to both sides, we get $0 = 0a$. The proof that $a0 = 0$ is similar.

(2) Notice that $ab + (-a)b = (a + (-a))b = 0b = 0$, by (1). As adding $(-a)b$ to ab gives 0, we have $(-a)b = -(ab)$. The proof that $a(-b) = -(ab)$ is similar.

(3) By (2), we have $(-a)(-b) = -(a(-b)) = -(-(ab))$. But remember that R is a group under addition, and hence $-(-(ab)) = ab$, as required. □

Corollary 8.1. *If R is a ring with identity, then $(-1)a = -a$, for any $a \in R$.*

Proof. By the preceding theorem, $(-1)a = -(1a) = -a$. □

As a ring is a group under addition, we know from Theorem 3.3 that an expression such as $a_1 + a_2 + \cdots + a_n$ is unambiguous, without the need for brackets. Even though the ring is not a group under multiplication, we can apply precisely the same proof as that of Theorem 3.3 to show that the expression $a_1 a_2 \cdots a_n$ also does not require brackets.

Theorem 8.4. *Let R be any ring, and $a_1, a_2, \ldots, a_n \in R$. Then regardless of how the product $a_1 a_2 \cdots a_n$ is bracketed, the result equals $(\cdots(((a_1 a_2)a_3)a_4)\cdots a_{n-1})a_n$.*

In order to avoid mistakes, it is also important to recognize which rules cannot be applied in general. For instance, in ordinary arithmetic using the real numbers, we take for granted that if $ab = 0$, then $a = 0$ or $b = 0$. This is simply not the case in an arbitrary ring.

Example 8.6. In $\mathbb{Z}_6$, we have $2 \cdot 3 = 0$, but $2 \neq 0$ and $3 \neq 0$.

Example 8.7. In $M_2(\mathbb{R})$, we have

$$\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} \begin{pmatrix} -2 & 4 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

but

$$\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} -2 & 4 \\ 1 & -2 \end{pmatrix}.$$

In dealing with groups, we have the cancellation law. We are used to something similar happening in ordinary arithmetic; that is, if $ab = ac$ and $a \neq 0$, then $b = c$. Again, this does not have to hold in rings.

Example 8.8. In $\mathbb{Z}_{12}$, we have $3 \cdot 1 = 3 \cdot 5$, but $3 \neq 0$ and $1 \neq 5$.

Finally, in a group G, we note that if there exists a $b \in G$ such that $ab = b$, then a is the identity. (Just multiply on the right by b^{-1}.) But even if a ring has an identity, the fact that $ab = b$ does not mean that $a = 1$. Indeed, the previous example points us in the right direction.

Example 8.9. In $\mathbb{Z}_{12}$, we have $5 \cdot 3 = 3$, but $5 \neq 1$.

Thus, to check that a ring element a is the identity, we must make sure that $ab = b = ba$ for every $b \in R$, not just for one such b.

Exercises

8.11. Let a and b be elements of a ring R. Simplify the following expressions as far as possible.

1. $(a + b)(a - b)$
2. $(a - b)^3$

8.12. Let R be a ring with identity. Suppose that there exist $a, b, c \in R$ such that $ab = ba = 1$ and $ac = 0$. Show that $c = 0$.

8.13. Let R be a ring with identity. Suppose there exist $a, b, c \in R$ such that $ba = ac = 1$. Does it follow that $b = c$? Show that it does, or find an explicit counterexample.

8.14. Let R be a ring and $n > 2$ a positive integer. Show that if there exists $0 \neq a \in R$ such that $a^n = 0$, then there exists $0 \neq b \in R$ such that $b^2 = 0$.

8.15. Let R be a ring with identity. Suppose that $a(a - 1) = 0$ for every $a \in R$. Does it follow that $a \in \{0, 1\}$ for every $a \in R$? Either prove that it does, or construct an explicit counterexample.

8.16. Let R be a ring in which $a^2 = a$ for every $a \in R$.

1. Show that $a + a = 0$ for every $a \in R$.
2. Show that R is commutative.

8.3 Subrings

Just as we have the notion of a subgroup, we can discuss subrings.

Definition 8.5. Let R be a ring. Then a subset S of R is said to be a **subring** if S is a ring under the same addition and multiplication operations as in R.

Example 8.10. We see that $\mathbb{Z}$ is a subring of $\mathbb{Q}$, and both are subrings of $\mathbb{R}$.

Example 8.11. The matrix ring $M_2(\mathbb{Q})$ is a subring of $M_2(\mathbb{R})$.

Example 8.12. For any ring R, $\{0\}$ and R are subrings of R.

How can we test if a subset is a subring?

Theorem 8.5. *Let R be a ring and S a subset of R. Then S is a subring of R if and only if*

1. *$0 \in S$;*
2. *if $a, b \in S$, then $a - b \in S$; and*
3. *if $a, b \in S$, then $ab \in S$.*

Proof. Suppose that S is a subring of R. Then it is an additive subgroup. By Theorem 3.13, (1) and (2) hold. As a ring is closed under multiplication, (3) holds as well. Conversely, suppose that (1)–(3) hold. Then by Theorem 3.13, S is an additive subgroup of R. By (3), S is closed under multiplication. The remaining ring properties (associativity and the distributive laws) hold in R, hence in any subset of R. Thus, S is indeed a subring. □

Note that for condition (1), it is actually sufficient to check that S is not the empty set.

Example 8.13. Let us show that $2\mathbb{Z}$ is a subring of $\mathbb{Z}$. Certainly $0 \in 2\mathbb{Z}$. If $2a, 2b \in 2\mathbb{Z}$, for some $a, b \in \mathbb{Z}$, then $2a - 2b = 2(a - b) \in 2\mathbb{Z}$. Also, $(2a)(2b) = 2(2ab) \in 2\mathbb{Z}$.

Example 8.14. Let $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$. Then letting $a = 0$, we see that S contains the zero matrix. Also, if $a, b \in \mathbb{R}$, then

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a - b & 0 \\ 0 & 0 \end{pmatrix} \in S$$

and

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in S.$$

Thus, S is a subring of $M_2(\mathbb{R})$.

We recall that the centre of every group is a subgroup. A similar thing happens for rings.

Definition 8.6. Let R be a ring. Then the **centre** of R is the set $\{z \in R : az = za \text{ for all } a \in R\}$; that is, it is the set of elements of R that commute with everything in R.

Theorem 8.6. *The centre of any ring is a subring.*

Proof. Let R be a ring and Z its centre. If $a \in R$, then $0a = 0 = a0$, so $0 \in Z$. Take any $y, z \in Z$. Then for any $a \in R$, we have $a(y-z) = ay-az = ya-za = (y-z)a$, since y and z are central. Thus, $y - z \in Z$. Also, $ayz = yaz = yza$, and hence $yz \in Z$. By Theorem 8.5, we are done. □

Example 8.15. If R is a commutative ring, then its centre is all of R.

Example 8.16. The centre of $M_2(\mathbb{R})$ is the set of all matrices of the form $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$, for all real numbers r. See Exercise 8.26.

One particular type of subring deserves special mention.

Definition 8.7. Let R be a ring with identity 1. Then a subring S of R is said to be a **unital** subring if $1 \in S$.

Example 8.17. We observe that $\mathbb{Z}$ is a unital subring of $\mathbb{Q}$, but $2\mathbb{Z}$ is not a unital subring.

Note that a subring can fail to be a unital subring because it does not have an identity (as is the case with $2\mathbb{Z}$ above), but it can also have an identity which is not the same as that for R.

Example 8.18. Let $R = \mathbb{Z}_6$ and $S = \{0, 3\}$. Theorem 8.5 shows us that S is a subring of R. It does not contain 1, so it is not a unital subring. However, S is still a ring with identity, as $3 \cdot 0 = 0$ and $3 \cdot 3 = 3$. That is, 3 is the identity of S.

Exercises

8.17. Let $R = \{a + bi : a, b \in \mathbb{Z}\}$. Show that R is a subring of $\mathbb{C}$. Is it a ring with identity? If so, is it unital?

8.18. Let $R = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$. Show that R a subring of $M_3(\mathbb{R})$. Is it a ring with identity? If so, is it a unital subring?

8.19. Let R be the set of matrices of the form $\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$ for all real numbers a. Show that R is a subring of $M_2(\mathbb{R})$. Is it a ring with identity? If so, is it a unital subring?

8.20. Let R be a ring with subrings S and T. Show that $S \cap T$ is a subring. Extend this to show the intersection of any collection of subrings of R is also a subring.

8.21. Let R and S be rings. Show that $T = \{(r, 0) : r \in R\}$ is a subring of $R \oplus S$.

8.22. Find a ring R and an additive subgroup S of R such that S is not a subring of R.

8.23. Let R be a ring and $a \in R$. Show that $S = \{ra : r \in R\}$ is a subring of R.

8.24. Let R be a ring and $a \in R$. Let $S = \{r \in R : ra = 0\}$. Is S necessarily a subring of R? Prove that it is, or find an explicit counterexample.

8.25. Let R be a ring and $a \in R$. Fix a subring S of R, and let $T = \{r \in R : ra \in S\}$. Is T necessarily a subring of R? Prove that it is, or find an explicit counterexample.

8.26. Show that the centre of $M_2(\mathbb{R})$ is the set of matrices of the form $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$, for all $r \in \mathbb{R}$.

8.4 Integral Domains and Fields

Let us discuss a couple of special sorts of rings.

Definition 8.8. Let R be a commutative ring. Then a nonzero element $a \in R$ is said to be a **zero divisor** if there exists a nonzero $b \in R$ such that $ab = 0$.

Example 8.19. In $\mathbb{Z}_6$, we note that 4 is a zero divisor, as $4 \cdot 3 = 0$. On the other hand, 5 is not a zero divisor.

Example 8.20. The ring of integers has no zero divisors.

As we mentioned at the beginning of the chapter, while we tend to think of the integers when we work with rings, they are actually rather special, and this is the reason why.

Definition 8.9. An **integral domain** is a commutative ring R with identity $1 \neq 0$ having no zero divisors.

The condition that $1 \neq 0$ may seem a bit curious. In fact, if $1 = 0$, then for any $a \in R$, we have $a = 1a = 0a = 0$. Thus, $R = \{0\}$. So we are only ruling out one ring with that restriction.

Example 8.21. The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all integral domains.

Example 8.22. The polynomial ring $\mathbb{R}[x]$ is an integral domain. Indeed, we know that it is a commutative ring with identity. Also, if $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$, with $a_i, b_i \in \mathbb{R}$ and $a_n \neq 0 \neq b_m$, then the unique term of highest degree in $f(x)g(x)$ is $a_nb_mx^{m+n}$. As $\mathbb{R}$ is an integral domain, $a_nb_m \neq 0$. Thus, $f(x)g(x)$ is not the zero polynomial.

Example 8.23. The rings $2\mathbb{Z}$, $\mathbb{Z}_6$ and $M_2(\mathbb{R})$ all fail to be integral domains. The first lacks an identity, the second has zero divisors and the third is not commutative.

As we discussed in Section 8.2, rings in general do not enjoy a cancellation law. However, integral domains do.

Theorem 8.7 (Cancellation Law). *Let R be an integral domain. Suppose that $a, b, c \in R$ and $ab = ac$. If $a \neq 0$, then $b = c$.*

Proof. If $ab = ac$, then $ab - ac = 0$, and hence $a(b - c) = 0$. Since R is an integral domain, either $a = 0$ (which is not true), or $b - c = 0$, as required. □

We also wish to discuss a stronger restriction on the ring. We need a definition first.

Definition 8.10. Let R be a ring with identity. Then we say that an element $a \in R$ is a **unit** if there exists an element $b \in R$ such that $ab = ba = 1$. In this case, we call b the **inverse** of a and write $b = a^{-1}$. We write $U(R)$ for the set of all units of R, and call it the **unit group** of R.

Theorem 8.8. *Let R be a ring with identity. Then $U(R)$ is a group under multiplication.*

Proof. Let $a, b \in U(R)$. Then $abb^{-1}a^{-1} = a1a^{-1} = aa^{-1} = 1$, and $b^{-1}a^{-1}ab = b^{-1}1b = b^{-1}b = 1$. Thus, $b^{-1}a^{-1} = (ab)^{-1}$, and $ab \in U(R)$. Multiplication in a ring is associative. Plainly, $1 \in U(R)$, as $1 \cdot 1 = 1$. Also, if $a \in U(R)$, then $aa^{-1} = a^{-1}a = 1$. That is, a is the inverse of a^{-1}, hence $a^{-1} \in U(R)$. We are done. □

Example 8.24. By definition, $U(M_n(\mathbb{R})) = GL_n(\mathbb{R})$.

Example 8.25. The unit group of $\mathbb{Z}$ is $\{\pm 1\}$.

Example 8.26. The unit group of $\mathbb{Z}_n$ is $U(n)$. See Exercise 8.30.

Example 8.27. Every element other than 0 in $\mathbb{R}$ is a unit. The same can be said for $\mathbb{Q}$ and $\mathbb{C}$.

This last example leads us to our next definition.

Definition 8.11. Let F be a commutative ring with identity $1 \neq 0$. Then F is said to be a **field** if $U(F)$ consists of every element of F other than 0.

Example 8.28. As we noted above, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

Lemma 8.1. *Let R be a commutative ring with identity. Then a unit in R cannot be a zero divisor.*

Proof. See Exercise 8.12. □

This immediately yields the following result.

Theorem 8.9. *Every field is an integral domain.*

Of course, the integers are an integral domain, but not a field. However, we can say something for finite integral domains. As we might expect, if $a \in R$, and n is a positive integer, we write

$$a^n = \underbrace{aa \cdots a}_{n \text{ times}}.$$

Theorem 8.10. *Let R be a finite integral domain. Then R is a field.*

Proof. By definition, R is a commutative ring with identity $1 \neq 0$. It remains only to check that each nonzero element is a unit. Take $0 \neq a \in R$. Consider the set $\{a^i : i > 0\}$. It consists of infinitely many powers of a. But R is finite. Thus, there cannot be infinitely many distinct powers. Let us say that $a^i = a^j$ with $i > j > 0$. Then $a^j a^{i-j} = a^i = a^j$. More importantly, $a^j a^{i-j} = a^j \cdot 1$. Now, a is a nonzero element of an integral domain, and products of nonzero elements in such a domain do not become zero. Thus, $a^j \neq 0$. By the cancellation law, $a^{i-j} = 1$. If $i - j = 1$, then $a = 1$, which is surely a unit. Otherwise, $aa^{i-j-1} = 1$. Since $i - j - 1$ is a positive integer, $a^{i-j-1} \in R$, and we have an inverse for a. □

We can now handle a particular collection of finite rings of interest.

Theorem 8.11. *Let $n \geq 2$ be a positive integer. Then the following are equivalent:*

1. *$\mathbb{Z}_n$ is an integral domain;*
2. *$\mathbb{Z}_n$ is a field; and*
3. *n is prime.*

Proof. In view of Theorems 8.9 and 8.10, we know that (1) and (2) are equivalent. We need only show that they are equivalent to (3). If n is composite, then write $n = kl$, where k and l are positive integers smaller than n. Then k and l are not 0 in $\mathbb{Z}_n$, and yet $kl = 0$ in $\mathbb{Z}_n$. Thus, $\mathbb{Z}_n$ is not an integral domain. On the other hand, suppose that n is prime. Surely $\mathbb{Z}_n$ is a commutative ring with identity $1 \neq 0$. Suppose we have integers i and j such that $ij = 0$ in $\mathbb{Z}_n$. Then $n|ij$. By Theorem 2.7, $n|i$ or $n|j$. That is, $i = 0$ or $j = 0$ in $\mathbb{Z}_n$. Thus, $\mathbb{Z}_n$ is an integral domain. □

Just as we have subrings, it will also be necessary to know about subfields.

Definition 8.12. Let F be a field. Then a subring K of F is said to be a **subfield** if it is a field using the same addition and multiplication operations.

Example 8.29. $\mathbb{Q}$ is a subfield of $\mathbb{R}$, which in turn is a subfield of $\mathbb{C}$.

But how do we test if a subset is a subfield?

Theorem 8.12. *Let F be a field. Then a subset S of F is a subfield of F if and only if*

1. $1 \in S$;
2. *if* $a, b \in S$, *then* $a - b \in S$; *and*
3. *if* $a, b \in S$, *and* $b \neq 0$, *then* $ab^{-1} \in S$.

Proof. Suppose that S is a subfield of F. Then S contains an identity $f \neq 0$. We must check that f is 1, the identity of F. But as f is the identity for S, we have $ff = f$. Now, f is a unit in F, so multiplying by f^{-1}, we get $f = 1$. Thus, (1) is proved. Since S is a subring of F, (2) follows from Theorem 8.5. As S is a field, every element except 0 has an inverse. This inverse is unique, as $U(F)$ is a group. Therefore, if $0 \neq b \in S$, then $b^{-1} \in S$. Since S is a subring, we get (3) as well.

Conversely, suppose that (1)–(3) hold. In view of (1) and (2), we see that $0 = 1-1 \in S$. Take any $a, b \in S$. By (2), $a-b \in S$. If $b = 0$, then $ab = 0 \in S$. Otherwise, we have $b^{-1} = 1b^{-1} \in S$, and therefore $ab = a(b^{-1})^{-1} \in S$. By Theorem 8.5, S is a subring of F. It certainly has an identity $1 \neq 0$, and it is commutative, since F is. Thus, it remains only to check that every nonzero element has an inverse in S. But we just did that! If $0 \neq b \in S$, then $b^{-1} = 1b^{-1} \in S$. Therefore, S is indeed a subfield of F. □

A small word of caution. It is not sufficient to replace (1) with the condition that S is not empty; indeed, if we did so, then we would accept $\{0\}$ as a field, which is wrong. It would be sufficient to assume that S contains a nonzero element b, for then (3) would give $1 = bb^{-1} \in S$.

Example 8.30. Let $F = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. We claim that F is a subfield of $\mathbb{R}$. Let us check the conditions. Certainly $1 = 1 + 0\sqrt{2} \in F$, so (1) holds. If $a_i, b_i \in \mathbb{Q}$, then $(a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{2} \in F$, and we have (2). Let us check the final condition. To begin with, we shall show that F is closed under multiplication. But $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in$

F. Thus, if we can show that every nonzero element of F has an inverse in F, then we will be done, as we can obtain (3). Take $0 \neq a + b\sqrt{2} \in F$. If $b = 0$, then $0 \neq a \in \mathbb{Q}$, and certainly $a^{-1} \in \mathbb{Q} \subseteq F$. Assume that $b \neq 0$. Notice that $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Q}$. Also, $a^2 - 2b^2 \neq 0$. Otherwise, we would have $(ab^{-1})^2 = 2$, meaning that $\sqrt{2}$ is rational, which is not the case. Thus, $a^2 - 2b^2$ has an inverse $c \in \mathbb{Q}$. But then $(a + b\sqrt{2})(ac - bc\sqrt{2}) = (a^2 - 2b^2)c = 1$. Hence, $a + b\sqrt{2}$ has an inverse in F, and F is a subfield of $\mathbb{R}$.

Exercises

8.27. Let $R = \{a + bi : a, b \in \mathbb{Q}\}$. Show that R is a subfield of $\mathbb{C}$.

8.28. For each of the following rings, which elements are units? Which are zero divisors?

1. $\mathbb{Z}_{18}$
2. $\mathbb{Z}_3 \oplus \mathbb{Z}_9$

8.29. Let R and S be rings with identity. Show that $U(R \oplus S) = U(R) \times U(S)$.

8.30. Let $n \geq 2$ be a positive integer. Show that $U(\mathbb{Z}_n) = U(n)$.

8.31. Show that every integral domain contains exactly two elements a satisfying $a^2 = a$.

8.32. Let R and S be rings. Under precisely what circumstances is $R \oplus S$ an integral domain?

8.33. Let F be a field with subfields K and L. Show that $K \cap L$ is a subfield of F. Extend this to show that the intersection of any collection of subfields is a subfield.

8.34. Let p be a prime and F a field with p^2 elements. Show that F cannot have more than one proper subfield.

8.35. Let R be an integral domain. Suppose that we have $a, b \in R$ such that $a^{13} = b^{13}$ and $a^{10} = b^{10}$. Show that $a = b$.

8.36. Let R be a finite commutative ring having no zero divisors. Show that R is $\{0\}$ or an integral domain.

8.5 The Characteristic of a Ring

One rather important property of a ring is its characteristic. Letting R be a ring, recall that using additive notation, if we have $a \in R$ and some positive integer n, then

$$na = \underbrace{a + a + \cdots + a}_{n \text{ times}}.$$

Definition 8.13. Let R be a ring. Then the **characteristic** of R, denoted char R, is the smallest positive integer n such that $na = 0$ for all $a \in R$. If no such n exists, then char $R = 0$.

Example 8.31. The characteristic of $\mathbb{Z}_n$ is n, as clearly $na = 0$ for any $a \in \mathbb{Z}_n$, whereas no smaller value than n will work if we take $a = 1$.

Example 8.32. The ring of integers has characteristic zero.

In fact, for rings with identity, we only need to look at the identity.

Theorem 8.13. *Let R be a ring with identity. Regarding R as an additive group, if the order of 1 is $n < \infty$, then R has characteristic n. If 1 has infinite order, then R has characteristic zero.*

Proof. If 1 has infinite order, then there is no positive integer n such that $n1 = 0$, and therefore char $R = 0$. Suppose 1 has order $n < \infty$. Then no number $1 \leq m < n$ can be the characteristic, as $m1 \neq 0$. But on the other hand, if $a \in R$, then

$$na = \underbrace{a + a + \cdots + a}_{n \text{ times}} = \underbrace{1a + 1a + \cdots + 1a}_{n \text{ times}} = (\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}})a = 0a = 0.$$

Thus, n is the characteristic. □

Corollary 8.2. *Let R be a ring with identity. Then every unital subring of R has the same characteristic as R.*

Proof. The same identity has the same order. □

The corollary does not apply to subrings that are not unital. For instance, if $R = \mathbb{Z}_6$, then char $R = 6$, but taking the subring $S = \{0, 2, 4\}$, we see that char $S = 3$.

In a commutative ring of prime characteristic, we have the following interesting fact.

Theorem 8.14 (Freshman's Dream). *Let R be a commutative ring of prime characteristic p. Then for any $a, b \in R$, we have*

$$(a + b)^p = a^p + b^p.$$

Proof. Let us apply the Binomial Theorem. (We are really only familiar with it for real numbers, but the proof in any commutative ring is the same.) We have

$$(a + b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p.$$

Now, if $1 < k < p$, then

$$\binom{p}{k} = \frac{p!}{(p-k)!k!}.$$

Notice that the numerator is divisible by p. However, p does not divide any of the terms in the denominator and, therefore, it does not divide the denominator. Thus, p divides each $\binom{p}{k}$, with $1 < k < p$. As our ring has characteristic p, multiplying any element by p, and hence by any multiple of p, gives 0. We have our result. □

We tend to encounter commutative rings with prime characteristic a lot in the context of integral domains.

Theorem 8.15. *The characteristic of an integral domain is either zero or a prime.*

Proof. Let R be an integral domain. There is nothing to do if char $R = 0$, so let char $R = n > 0$. We cannot have $n = 1$, for then 1 has additive order 1, but only 0 has that order. The only remaining problem is if n is composite. Suppose that $n = kl$, with $1 < k, l < n$. Then we have

$$0 = n1 = (kl)1 = \underbrace{1 + \cdots + 1}_{kl \text{ times}} = (\underbrace{1 + \cdots + 1}_{k \text{ times}})(\underbrace{1 + \cdots + 1}_{l \text{ times}}) = (k1)(l1).$$

Since R is an integral domain, $k1 = 0$ or $l1 = 0$. But the additive order of 1 is n, and we have a contradiction. □

Exercises

8.37. Find the characteristic of each of the following rings.

1. $3\mathbb{Z}_{21} = \{0, 3, \ldots, 18\}$
2. $\mathbb{R}[x]$

8.38. Find the characteristic of each of the following rings.

1. $\mathbb{Z}_4 \oplus \mathbb{Z}_{10}$
2. $M_2(\mathbb{Z}_3)$

8.39. Show that a finite integral domain R must have order p^n for some prime p and positive integer n.

8.40. Let F be a field of prime characteristic p. Show that for every positive integer n, $\{a \in F : a^{p^n} = a\}$ is a subfield of F.

8.41. Let R be a commutative ring with identity, and suppose that $a \in R$ satisfies $a^n = 0$ for some positive integer n.

1. Show that $1 + a \in U(R)$.
2. If char R is prime, show that $1 + a$ has finite order in $U(R)$.

8.42. Let $F = \{0, 1, a, b\}$ be a field with four elements. Write the addition and multiplication tables for F.