23.9 Example Show that although $\mathbb{Z}_2$ is an integral domain, the matrix ring $M_2(\mathbb{Z}_2)$ has divisors of zero.

Solution We need only observe that

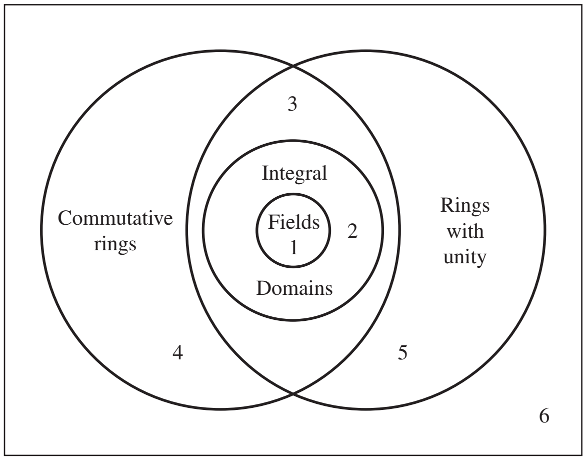
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

▲

In a field, every nonzero element is a unit. We saw that units cannot be divisors of 0, so in a field there are no divisors of 0. Since multiplication in a field is commutative, every field is an integral domain.

Figure 23.10 gives a Venn diagram view of containment for the algebraic structures having two binary operations with which we will be chiefly concerned. In Exercise 26 we ask you to redraw this figure to include strictly skew fields as well.

We have seen that $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_p$ for p a prime number are all fields. Theorem 23.3 implies that if $\mathbb{Z}_n$ is an integral domain, then $\mathbb{Z}_n$ is a field. In fact, the next theorem says that any finite integral domain is a field. The proof of this theorem is a personal favorite of both authors. It is done by counting, one of the most powerful techniques in mathematics.



23.10 Figure A collection of rings.

23.11 Theorem Every finite integral domain is a field.

Proof Let R be a finite integral domain and a a nonzero element of R. We wish to show there is an element $b \in R$ such that $ab = 1$. To this end, we define a function $f : R \to R$ by

$$f(x) = ax.$$

We first show that f is a one-to-one function. Suppose that $f(x_1) = f(x_2)$, then

$$ax_1 = ax_2$$
$$x_1 = x_2$$

since $a \neq 0$ and cancellation holds in an integral domain. Thus f is one-to-one. Since R is finite and $f : R \to R$ is one-to-one, f must also map onto R. Therefore, there is a $b \in R$ such that

$$1 = f(a) = ab = ba$$

which verifies that a is a unit. ◆

The finite condition in Theorem 23.11 is necessary since $\mathbb{Z}$ is an infinite integral domain, which is not a field. The counting argument fails in the case where the integral domain is infinite since there are one-to-one functions from an infinite set to itself that are not onto. For example, multiplication by 2 is a one-to-one function mapping $\mathbb{Z}$ to $\mathbb{Z}$, but 1 is not in the range of the function.

In Section 39 we will see that other than $\mathbb{Z}_p$ there are many finite integral domains and therefore fields.

The Characteristic of a Ring

Let R be any ring. We might ask whether there is a positive integer n such that $n \cdot a = 0$ for all $a \in R$, where $n \cdot a$ means $a + a + \cdots + a$ for n summands, as explained in Section 22. For example, the integer m has this property for the ring $\mathbb{Z}_m$.

23.12 Definition If for a ring R a positive integer n exists such that $n \cdot a = 0$ for all $a \in R$, then the least such positive integer is the **characteristic of the ring** R. If no such positive integer exists, then R is of **characteristic** 0. ■

We shall use the concept of a characteristic chiefly for fields. Exercise 35 asks us to show that the characteristic of an integral domain is either 0 or a prime p.

23.13 Example The ring $\mathbb{Z}_n$ is of characteristic n, while $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ all have characteristic 0. ▲

At first glance, determination of the characteristic of a ring seems to be a tough job, unless the ring is obviously of characteristic 0. Do we have to examine *every* element a of the ring in accordance with Definition 23.12? Our final theorem of this section shows that if the ring has unity, it suffices to examine only $a = 1$.

23.14 Theorem Let R be a ring with unity. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{Z}^+$, then R has characteristic 0. If $n \cdot 1 = 0$ for some $n \in \mathbb{Z}^+$, then the smallest such integer n is the characteristic of R.

Proof If $n \cdot 1 \neq 0$ for all $n \in \mathbb{Z}^+$, then surely we cannot have $n \cdot a = 0$ for all $a \in R$ for some positive integer n, so by Definition 23.12, R has characteristic 0.

Suppose that n is a positive integer such that $n \cdot 1 = 0$. Then for any $a \in R$, we have

$$n \cdot a = a + a + \cdots + a = a(1 + 1 + \cdots + 1) = a(n \cdot 1) = a0 = 0.$$

Our theorem follows directly. ◆

■ EXERCISES 23

Computations

1. Find all solutions of the equation $x^3 - 2x^2 - 3x = 0$ in $\mathbb{Z}_{12}$.

2. Solve the equation $3x = 2$ in the field $\mathbb{Z}_7$; in the field $\mathbb{Z}_{23}$.

3. Find all solutions of the equation $x^2 + 2x + 2 = 0$ in $\mathbb{Z}_6$.

4. Find all solutions of $x^2 + 2x + 4 = 0$ in $\mathbb{Z}_6$.

In Exercises 5 through 10, find the characteristic of the given ring.

5. $2\mathbb{Z}$

6. $\mathbb{Z} \times \mathbb{Z}$

7. $\mathbb{Z}_3 \times 3\mathbb{Z}$

8. $\mathbb{Z}_3 \times \mathbb{Z}_3$

9. $\mathbb{Z}_3 \times \mathbb{Z}_4$

10. $\mathbb{Z}_6 \times \mathbb{Z}_{15}$

In Exercises 11 through 16, classify each nonzero element of the ring as a unit, a divisor of 0, or neither.

11. $\mathbb{Z}_6$

12. $\mathbb{Z}_8$

13. $\mathbb{Z}_{15}$

14. $\mathbb{Z}$

15. $\mathbb{Z}_3 \times \mathbb{Z}_3$

16. $\mathbb{Z}_4 \times \mathbb{Z}_5$

17. Let R be a commutative ring with unity of characteristic 4. Compute and simplify $(a + b)^4$ for $a, b \in R$.

18. Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a + b)^9$ for $a, b \in R$.

19. Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a + b)^6$ for $a, b \in R$.

20. Show that the matrix $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a divisor of zero in $M_2(\mathbb{Z})$.

Concepts

In Exercises 21 and 22, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

21. If $ab = 0$, then a and b are *divisors of zero*.

22. If $n \cdot a = 0$ for all elements a in a ring R, then n is the *characteristic of* R.

23. Determine whether each of the following is true or false.

a. $n\mathbb{Z}$ has zero divisors if n is not prime.

b. Every field is an integral domain.

c. The characteristic of $n\mathbb{Z}$ is n.

d. As a ring, $\mathbb{Z}$ is isomorphic to $n\mathbb{Z}$ for all $n \geq 1$.

e. The cancellation law holds in any ring that is isomorphic to an integral domain.

f. Every integral domain of characteristic 0 is infinite.

g. The direct product of two integral domains is again an integral domain.

h. A divisor of zero in a commutative ring with unity can have no multiplicative inverse.

i. $n\mathbb{Z}$ is a subdomain of $\mathbb{Z}$.

j. $\mathbb{Z}$ is a subfield of $\mathbb{Q}$.

24. Each of the six numbered regions in Fig. 23.10 corresponds to a certain type of a ring. Give an example of a ring in each of the six cells. For example, a ring in the region numbered 3 must be commutative (it is inside the commutative circle), have unity, but not be an integral domain.

25. (For students who have had a semester of linear algebra) Let F be a field. Give five different characterizations of the elements A of $M_n(F)$ that are divisors of 0.

26. Redraw Fig. 23.10 to include a subset corresponding to strictly skew fields.

Proof Synopsis

27. Give a one-sentence synopsis of the proof of the "if" part of Theorem 23.6.

28. Give a two-sentence synopsis of the proof of Theorem 23.11.

Theory

29. An element a of a ring R is **idempotent** if $a^2 = a$. Show that a division ring contains exactly two idempotent elements.

30. Show that an intersection of subdomains of an integral domain D is again a subdomain of D.

31. Show that a finite ring R with unity $1 \neq 0$ and no divisors of 0 is a division ring. (It is actually a field, although commutativity is not easy to prove. See Theorem 32.10.) [*Note:* In your proof, to show that $a \neq 0$ is a unit, you must show that a "left multiplicative inverse" of $a \neq 0$ in R is also a "right multiplicative inverse."]

32. Let R be a ring that contains at least two elements. Suppose for each nonzero $a \in R$, there exists a unique $b \in R$ such that $aba = a$.

a. Show that R has no divisors of 0.

b. Show that $bab = b$.

c. Show that R has unity.

d. Show that R is a division ring.

33. Show that the characteristic of a subdomain of an integral domain D is equal to the characteristic of D.

34. Show that if D is an integral domain, then $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ is a subdomain of D contained in every subdomain of D.

35. Show that the characteristic of an integral domain D must be either 0 or a prime p. [*Hint:* If the characteristic of D is mn, consider $(m \cdot 1)(n \cdot 1)$ in D.]

36. This exercise shows that every ring R can be enlarged (if necessary) to a ring S with unity, having the same characteristic as R. Let $S = R \times \mathbb{Z}$ if R has characteristic 0, and $R \times \mathbb{Z}_n$ if R has characteristic n. Let addition in S be the usual addition by components, and let multiplication be defined by

$$(r_1, n_1)(r_2, n_2) = (r_1r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1n_2)$$

where $n \cdot r$ has the meaning explained in Section 22.

a. Show that S is a ring.

b. Show that S has unity.

c. Show that S and R have the same characteristic.

d. Show that the map $\phi : R \to S$ given by $\phi(r) = (r, 0)$ for $r \in R$ maps R isomorphically onto a subring of S.

SECTION 24 FERMAT'S AND EULER'S THEOREMS

Fermat's Theorem

We know that as additive groups, $\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$ are naturally isomorphic, with the coset $a + n\mathbb{Z}$ corresponding to a for each $a \in \mathbb{Z}_n$. Furthermore, addition of cosets in $\mathbb{Z}/n\mathbb{Z}$ may be performed by choosing any representatives, adding them in $\mathbb{Z}$, and finding the coset of $n\mathbb{Z}$ containing their sum. It is easy to see that $\mathbb{Z}/n\mathbb{Z}$ can be made into a ring by multiplying cosets in the same fashion, that is, by multiplying any chosen representatives. While we will be showing this later in a more general situation, we do this special case now. We need only show that such coset multiplication is well defined, because the associativity of multiplication and the distributive laws will follow immediately from those properties of the chosen representatives in $\mathbb{Z}$. To this end, choose representatives $a + rn$ and $b + sn$, rather than a and b, from the cosets $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$. Then

$$(a + rn)(b + sn) = ab + (as + rb + rsn)n,$$

which is also an element of $ab + n\mathbb{Z}$. Thus the multiplication is well-defined, and our cosets form a ring isomorphic to the ring $\mathbb{Z}_n$.

Exercise 39 in Section 22 asks us to show that the units in a ring form a group under the multiplication operation of the ring. This is a very useful fact that we will use to provide simple proofs for both Fermat's Little Theorem and Euler's generalization. We start with Fermat's Theorem.

24.1 Theorem **(Little Theorem of Fermat)** If $a \in \mathbb{Z}$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$, that is, $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$.

Proof The ring $\mathbb{Z}_p$ is a field, which implies that all the nonzero elements are units. Thus $\langle \mathbb{Z}_p^*, \cdot \rangle$ is a group with $p - 1$ elements. Any b in the group $\mathbb{Z}_p^*$ has order a divisor of $|\mathbb{Z}_p^*| = p - 1$. Therefore