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 19.13? Our final theorem of this section shows that if the ring has unity, it suffices to examine only $a = 1$.

19.15 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 19.13, 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 19

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

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

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

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

14. 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 15 and 16, 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.

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

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

17. Mark each of the following 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 $\mathbb{Q}$.

18. Each of the six numbered regions in Fig. 19.10 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.

19. (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.

20. Redraw Fig. 19.10 to include a subset corresponding to strictly skew fields.

Proof Synopsis

21. Give a one-sentence synopsis of the proof of the "if" part of Theorem 19.5.

22. Give a one-sentence synopsis of the proof of Theorem 19.11.

Theory

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

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

25. 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 24.10.) [*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."]

26. 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.

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

28. 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.

29. 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.]

30. 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 $S = R \times Z$ 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

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

where $n \cdot r$ has the meaning explained in Section 18.

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 20 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 $\mathbb{Z}_n$.

The following is a special case of Exercise 37 in Section 18.

> For any field, the nonzero elements form a group under the field multiplication.

In particular, for $\mathbb{Z}_p$, the elements

$$1, 2, 3, \cdots, p - 1$$

form a group of order $p - 1$ under multiplication modulo p. Since the order of any element in a group divides the order of the group, we see that for $b \neq 0$ and $b \in \mathbb{Z}_p$, we have $b^{p-1} = 1$ in $\mathbb{Z}_p$. Using the fact that $\mathbb{Z}_p$ is isomorphic to the ring of cosets of the form $a + p\mathbb{Z}$ described above, we see at once that for any $a \in \mathbb{Z}$ not in the coset $0 + p\mathbb{Z}$, we must have

$$a^{p-1} \equiv 1 \pmod{p}.$$

This gives us at once the so-called Little Theorem of Fermat.

20.1 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 $a \not\equiv 0 \pmod{p}$.

20.2 Corollary If $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$ for any prime p.