Finally, be careful not to confuse our use of the words *unit* and *unity*. *Unity* is the multiplicative identity element, while a *unit* is any element having a multiplicative inverse. Thus the multiplicative identity element or unity is a unit, but not every unit is unity. For example, -1 is a unit in $\mathbb{Z}$, but -1 is not unity, that is, $-1 \neq 1$.

■ Historical Note

Although fields were implict in the early work on the solvability of equations by Abel and Galois, it was Leopold Kronecker (1823–1891) who in connection with his own work on this subject first published in 1881 a definition of what he called a "domain of rationality": "The domain of rationality $(R', R'', R''', \cdots)$ contains $\cdots$ every one of those quantities which are rational functions of the quantities $R', R'', R''', \cdots$ with integral coefficients." Kronecker, however, who insisted that any mathematical subject must be constructible in finitely many steps, did not view the domain of rationality as a complete entity, but merely as a region in which took place various operations on its elements.

Richard Dedekind (1831–1916), the inventor of the Dedekind cut definition of a real number, considered a field as a completed entity. In 1871, he published the following definition in his supplement to the second edition of Dirichlet's text on number theory: "By a field we mean any system of infinitely many real or complex numbers, which in itself is so closed and complete, that the addition, subtraction, multiplication, and division of any two numbers always produces a number of the same system." Both Kronecker and Dedekind had, however, dealt with their varying ideas of this notion as early as the 1850s in their university lectures.

A more abstract definition of a field, similar to the one in the text, was given by Heinrich Weber (1842–1913) in a paper of 1893. Weber's definition, unlike that of Dedekind, specifically included fields with finitely many elements as well as other fields, such as function fields, which were not subfields of the field of complex numbers.

■ EXERCISES 18

Computations

In Exercises 1 through 6, compute the product in the given ring.

1. $(12)(16)$ in $\mathbb{Z}_{24}$

2. $(16)(3)$ in $\mathbb{Z}_{32}$

3. $(11)(-4)$ in $\mathbb{Z}_{15}$

4. $(20)(-8)$ in $\mathbb{Z}_{26}$

5. $(2,3)(3,5)$ in $\mathbb{Z}_5 \times \mathbb{Z}_9$

6. $(-3,5)(2,-4)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{11}$

In Exercises 7 through 13, decide whether the indicated operations of addition and multiplication are defined (closed) on the set, and give a ring structure. If a ring is not formed, tell why this is the case. If a ring is formed, state whether the ring is commutative, whether it has unity, and whether it is a field.

7. $n\mathbb{Z}$ with the usual addition and multiplication

8. $\mathbb{Z}^+$ with the usual addition and multiplication

9. $\mathbb{Z} \times \mathbb{Z}$ with addition and multiplication by components

10. $2\mathbb{Z} \times \mathbb{Z}$ with addition and multiplication by components

11. $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ with the usual addition and multiplication

12. $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ with the usual addition and multiplication

13. The set of all pure imaginary complex numbers ri for $r \in \mathbb{R}$ with the usual addition and multiplication

In Exercises 14 through 19, describe all units in the given ring

14. $\mathbb{Z}$ **15.** $\mathbb{Z} \times \mathbb{Z}$ **16.** $\mathbb{Z}_5$

17. $\mathbb{Q}$ **18.** $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ **19.** $\mathbb{Z}_4$

20. Consider the matrix ring $M_2(\mathbb{Z}_2)$.

a. Find the **order** of the ring, that is, the number of elements in it.

b. List all units in the ring.

21. If possible, give an example of a homomorphism $\phi : R \to R'$ where R and R' are rings with unity $1 \neq 0$ and $1' \neq 0'$, and where $\phi(1) \neq 0'$ and $\phi(1) \neq 1'$.

22. (Linear algebra) Consider the map det of $M_n(\mathbb{R})$ into $\mathbb{R}$ where $\det(A)$ is the determinant of the matrix A for $A \in M_n(\mathbb{R})$. Is det a ring homomorphism? Why or why not?

23. Describe all ring homomorphisms of $\mathbb{Z}$ into $\mathbb{Z}$.

24. Describe all ring homomorphisms of $\mathbb{Z}$ into $\mathbb{Z} \times \mathbb{Z}$.

25. Describe all ring homomorphisms of $\mathbb{Z} \times \mathbb{Z}$ into $\mathbb{Z}$.

26. How many homomorphisms are there of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ into $\mathbb{Z}$?

27. Consider this solution of the equation $X^2 = I_3$ in the ring $M_3(\mathbb{R})$.

$X^2 = I_3$ implies $X^2 - I_3 = 0$, the zero matrix, so factoring, we have $(X - I_3)(X + I_3) = 0$

whence either $X = I_3$ or $X = -I_3$.

Is this reasoning correct? If not, point out the error, and if possible, give a counterexample to the conclusion.

28. Find all solutions of the equation $x^2 + x - 6 = 0$ in the ring $\mathbb{Z}_{14}$ by factoring the quadratic polynomial. Compare with Exercise 27.

Concepts

In Exercises 29 and 30, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a from acceptable for publication.

29. A *field* F is a ring with nonzero unity such that the set of nonzero elements of F is a group under multiplication.

30. A *unit* in a ring is an element of magnitude 1.

31. Give an example of a ring having two elements a and b such that $ab = 0$ but neither a nor b is zero.

32. Give an example of a ring with unity $1 \neq 0$ that has a subring with nonzero unity $1' \neq 1$. [*Hint:* Consider a direct product, or a subring of $\mathbb{Z}_6$.]

33. Mark each of the following true or false.

_____ **a.** Every field is also a ring.

_____ **b.** Every ring has a multiplicative identity.

_____ **c.** Every ring with unity has at least two units.

_____ **d.** Every ring with unity has at most two units.

_____ **e.** It is possible for a subset of some field to be a ring but not a subfield, under the induced operations.

_____ **f.** The distributive laws for a ring are not very important.

_____ **g.** Multiplication in a field is commutative.

_____ **h.** The nonzero elements of a field form a group under the multiplication in the field.

_____ **i.** Addition in every ring is commutative.

_____ **j.** Every element in a ring has an additive inverse.

Theory

34. Show that the multiplication defined on the set F of functions in Example 18.4 satisfies axioms $\mathscr{R}_2$ and $\mathscr{R}_3$ for a ring.

35. Show that the evaluation map ϕ_a of Example 18.10 satisfies the multiplicative requirement for a homomorphism.

36. Complete the argument outlined after Definitions 18.12 to show that isomorphism gives an equivalence relation on a collection of rings.

37. Show that if U is the collection of all units in a ring $\langle R, +, \cdot \rangle$ with unity, then $\langle U, \cdot \rangle$ is a group. [*Warning:* Be sure to show that U is closed under multiplication.]

38. Show that $a^2 - b^2 = (a + b)(a - b)$ for all a and b in a ring R if and only if R is commutative.

39. Let $(R, +)$ be an abelian group. Show that $(R, +, \cdot)$ is a ring if we define $ab = 0$ for all $a, b \in R$.

40. Show that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic. Show that the fields $\mathbb{R}$ and $\mathbb{C}$ are not isomorphic.

41. (Freshman exponentiation) Let p be a prime. Show that in the ring $\mathbb{Z}_p$ we have $(a + b)^p = a^p + b^p$ for all $a, b \in \mathbb{Z}_p$. [*Hint:* Observe that the usual binomial expansion for $(a + b)^n$ is valid in a *commutative* ring.]

42. Show that the unity element in a subfield of a field must be the unity of the whole field, in contrast to Exercise 32 for rings.

43. Show that the multiplicative inverse of a unit a ring with unity is unique.

44. An element a of a ring R is **idempotent** if $a^2 = a$.

a. Show that the set of all idempotent elements of a commutative ring is closed under multiplication.

b. Find all idempotents in the ring $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

45. (Linear algebra) Recall that for an $m \times n$ matrix A, the *transpose* A^T of A is the matrix whose jth column is the jth row of A. Show that if A is an $m \times n$ matrix such that A^TA is invertible, then the *projection matrix* $P = A(A^TA)^{-1}A^T$ is an idempotent in the ring of $n \times n$ matrices.

46. An element a of a ring R is **nilpotent** if $a^n = 0$ for some $n \in \mathbb{Z}^+$. Show that if a and b are nilpotent elements of a *commutative* ring, then $a + b$ is also nilpotent.

47. Show that a ring R has no nonzero nilpotent element if and only if 0 is the only solution of $x^2 = 0$ in R.

48. Show that a subset S of a ring R gives a subring of R if and only if the following hold:

$$0 \in S;$$
$$(a - b) \in S \text{ for all } a, b \in S;$$
$$ab \in S \text{ for all } a, b \in S.$$

49. **a.** Show that an intersection of subrings of a ring R is again a subring of R.

b. Show that an intersection of subfields of a field F is again a subfield of F.

50. Let R be a ring, and let a be a fixed element of R. Let $I_a = \{x \in R \mid ax = 0\}$. Show that I_a is a subring of R.

51. Let R be a ring, and let a be a fixed element of R. Let R_a be the subring of R that is the intersection of all subrings of R containing a (see Exercise 49). The ring R_a is the **subring of R generated by a**. Show that the abelian group $\langle R_a, + \rangle$ is generated (in the sense of Section 7) by $\{a^n \mid n \in \mathbb{Z}^+\}$.

52. (Chinese Remainder Theorem for two congruences) Let r and s be positive integers such that $\gcd(r, s) = 1$. Use the isomorphism in Example 18.15 to show that for $m, n \in \mathbb{Z}$, there exists an integer x such that $x \equiv m \pmod{r}$ and $x \equiv n \pmod{s}$.

53. **a.** State and prove the generalization of Example 18.15 for a direct product with n factors.

b. Prove the Chinese Remainder Theorem: Let $a_i, b_i \in \mathbb{Z}^+$ for $i = 1, 2, \cdots, n$ and let $\gcd(b_i, b_j) = 1$ for $i \neq j$. Then there exists $x \in \mathbb{Z}^+$ such that $x \equiv a_i \pmod{b_i}$ for $i = 1, 2, \cdots, n$.

54. Consider $\langle S, +, \cdot \rangle$, where S is a set and $+$ and $\cdot$ are binary operations on S such that

$\langle S, + \rangle$ is a group,

$\langle S^*, \cdot \rangle$ is a group where S^* consists of all elements of S except the additive identity element,

$a(b + c) = (ab) + (ac)$ and $(a + b)c = (ac) + (bc)$ for all $a, b, c \in S$.

Show that $\langle S, +, \cdot \rangle$ is a division ring. [*Hint:* Apply the distributive laws to $(1 + 1)(a + b)$ to prove the commutativity of addition.]

55. A ring R is a **Boolean ring** if $a^2 = a$ for all $a \in R$, so that every element is idempotent. Show that every Boolean ring is commutative.

56. (For students having some knowledge of the laws of set theory) For a set S, let $\mathscr{P}(S)$ be the collection of all subsets of S. Let binary operations $+$ and $\cdot$ on $\mathscr{P}(S)$ be defined by

$$A + B = (A \cup B) - (A \cap B) = \{x \mid x \in A \text{ or } x \in B \text{ but } x \notin (A \cap B)\}$$

and

$$A \cdot B = A \cap B$$

for $A, B \in \mathscr{P}(S)$.

a. Give the tables for $+$ and $\cdot$ for $\mathscr{P}(S)$, where $S = \{a, b\}$. [*Hint:* $\mathscr{P}(S)$ has four elements.]

b. Show that for *any* set S, $\langle \mathscr{P}(S), +, \cdot \rangle$ is a Boolean ring (see Exercise 55).

SECTION 19 INTEGRAL DOMAINS

While a careful treatment of polynomials is not given until Section 22, for purposes of motivation we shall make intuitive use of them in this section.

Divisors of Zero and Cancellation

One of the most important algebraic properties of our usual number system is that a product of two numbers can only be 0 if at least one of the factors is 0. We have used this fact many times in solving equations, perhaps without realizing that we were using it. Suppose, for example, we are asked to solve the equation

$$x^2 - 5x + 6 = 0.$$

The first thing we do is to factor the left side:

$$x^2 - 5x + 6 = (x - 2)(x - 3).$$