Proof For Property 1, note that by axioms $\mathscr{R}_1$ and $\mathscr{R}_2$,

$$a0 + a0 = a(0 + 0) = a0 = 0 + a0.$$

Then by the cancellation law for the additive group $\langle R, + \rangle$, we have $a0 = 0$. Likewise,

$$0a + 0a = (0 + 0)a = 0a = 0 + 0a$$

implies that $0a = 0$. This proves Property 1.

In order to understand the proof of Property 2, we must remember that, by *definition*, $-(ab)$ is the element that when added to ab gives 0. Thus to show that $a(-b) = -(ab)$, we must show precisely that $a(-b) + ab = 0$. By the left distributive law,

$$a(-b) + ab = a(-b + b) = a0 = 0,$$

since a0 = 0 by Property 1. Likewise,

$$(-a)b + ab = (-a + a)b = 0b = 0.$$

For Property 3, note that

$$(-a)(-b) = -(a(-b))$$

by Property 2. Again by Property 2,

$$-(a(-b)) = -(-(ab)),$$

and $-(-(ab))$ is the element that when added to $-(ab)$ gives 0. This is ab by definition of $-(ab)$ and by the uniqueness of an inverse in a group. Thus, $(-a)(-b) = ab$. ◆

Based on high school algebra it seems natural to begin a proof of Property 2 in Theorem 22.8 by writing $(-a)b = ((-1)a)b$. In Exercise 30 you will be asked to find an error in a "proof" of this sort.

It is important that you *understand* the preceding proof. The theorem allows us to use our usual rules for signs.

Homomorphisms and Isomorphisms

From our work in group theory, it is quite clear how a structure-relating map of a ring R into a ring R' should be defined.

22.9 Definition For rings R and R', a map $\phi : R \to R'$ is a **homomorphism** if the following two conditions are satisfied for all $a, b \in R$:

1. $\phi(a + b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$. ■

In the preceding definition, Condition 1 is the statement that ϕ is a group homomorphism mapping the abelian group $\langle R, + \rangle$ into $\langle R', + \rangle$. Condition 2 requires that ϕ relate the multiplicative structures of the rings R and R' in the same way. Since ϕ is also a group homomorphism, all the results concerning group homomorphisms are valid for the additive structure of the rings. In particular, ϕ is one-to-one if and only if its **kernel** $\text{Ker}(\phi) = \{a \in R \mid \phi(a) = 0'\}$ is just the subset $\{0\}$ of R. The homomorphism ϕ of the group $\langle R, + \rangle$ gives rise to a factor group. We expect that a ring homomorphism will give rise to a factor ring. This is indeed the case. We delay discussion of this to Section 30, where the treatment will parallel our treatment of factor groups in Section 12.

22.10 Example Let F be the ring of all functions mapping $\mathbb{R}$ into $\mathbb{R}$ defined in Example 22.4. For each $a \in \mathbb{R}$, we have the **evaluation homomorphism** $\phi_a : F \to \mathbb{R}$, where $\phi_a(f) = f(a)$ for $f \in F$. We will work a great deal with this homomorphism in the rest of this text, for finding a real solution of a polynomial equation $p(x) = 0$ amounts precisely to finding $a \in \mathbb{R}$ such that $\phi_a(p) = 0$. Much of the remainder of this text deals with solving polynomial equations. We leave the demonstration of the homomorphism properties for ϕ_a to Exercise 37. ▲

22.11 Example The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ where $\phi(a)$ is the remainder of a modulo n is a ring homomorphism for each positive integer n. We know $\phi(a + b) = \phi(a) + \phi(b)$ by group theory. To show the multiplicative property, write $a = q_1 n + r_1$ and $b = q_2 n + r_2$ according to the division algorithm. Then $ab = n(q_1 q_2 n + r_1 q_2 + q_1 r_2) + r_1 r_2$. Thus $\phi(ab)$ is the remainder of $r_1 r_2$ when divided by n. Since $\phi(a) = r_1$ and $\phi(b) = r_2$, Example 22.6 indicates that $\phi(a)\phi(b)$ is also this same remainder, so $\phi(ab) = \phi(a)\phi(b)$. From group theory, we anticipate that the ring $\mathbb{Z}_n$ might be isomorphic to a factor ring $\mathbb{Z}/n\mathbb{Z}$. This is indeed the case; factor rings will be discussed in Section 30. ▲

We realize that in the study of any sort of mathematical structure, an idea of basic importance is the concept of two systems being *structurally identical*, that is, one being just like the other except for names. In algebra this concept is always called *isomorphism*. The concept of two things being just alike except for names of elements leads us, just as it did for groups, to the following definition.

22.12 Definition An **isomorphism** $\phi : R \to R'$ from a ring R to a ring R' is a homomorphism that is one-to-one and onto R'. The rings R and R' are then **isomorphic**. ■

From our work in group theory, we expect that isomorphism gives an equivalence relation on any collection of rings. We need to check that the multiplicative property of an isomorphism is satisfied for the inverse map $\phi^{-1} : R' \to R$ (to complete the symmetry argument). Similarly, we check that if $\mu : R' \to R''$ is also a ring isomorphism, then the multiplicative requirement holds for the composite map $\mu\phi : R \to R''$ (to complete the transitivity argument). We ask you to do this in Exercise 38.

22.13 Example As abelian groups, $\langle \mathbb{Z}, + \rangle$ and $\langle 2\mathbb{Z}, + \rangle$ are isomorphic under the map $\phi : \mathbb{Z} \to 2\mathbb{Z}$, with $\phi(x) = 2x$ for $x \in \mathbb{Z}$. Here ϕ is *not* a ring isomorphism, for $\phi(xy) = 2xy$, while $\phi(x)\phi(y) = 2x2y = 4xy$. ▲

Multiplicative Questions: Fields

Many of the rings we have mentioned, such as $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, have a multiplicative identity element 1. However, $2\mathbb{Z}$ does not have an identity element for multiplication. Note also that multiplication is not commutative in the matrix rings described in Example 22.3.

It is evident that $\{0\}$, with $0 + 0 = 0$ and $(0)(0) = 0$, gives a ring, the **zero ring.** Here 0 acts as multiplicative as well as additive identity element. By Theorem 22.8, this is the only case in which 0 could act as a multiplicative identity element, for from $0a = 0$, we can then deduce that $a = 0$. Theorem 1.15 shows that if a ring has a multiplicative identity element, it is unique. We denote a multiplicative identity element in a ring by 1.

22.14 Definition A ring in which the multiplication is commutative is a **commutative ring.** A ring with a multiplicative identity element is a **ring with unity;** the multiplicative identity element 1 is called "**unity.**" ■

In a ring with unity 1 the distributive laws show that

$$\underbrace{(1+1+\cdots+1)}_{n \text{ summands}}\ \underbrace{(1+1+\cdots+1)}_{m \text{ summands}} = \underbrace{(1+1+\cdots+1)}_{nm \text{ summands}},$$

that is, $(n \cdot 1)(m \cdot 1) = (nm) \cdot 1$. The next example gives an application of this observation.

22.15 Example We claim that for integers r and s where $\gcd(r, s) = 1$, the rings $\mathbb{Z}_{rs}$ and $\mathbb{Z}_r \times \mathbb{Z}_s$ are isomorphic. Additively, they are both cyclic abelian groups of order rs with generators 1 and (1, 1) respectively. Thus $\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ defined by $\phi(n \cdot 1) = n \cdot (1, 1)$ is an additive group isomorphism. To check the multiplicative Condition 2 of Definition 22.9, we use the observation preceding this example for the unity (1, 1) in the ring $\mathbb{Z}_r \times \mathbb{Z}_s$, and compute.

$$\phi(nm) = (nm) \cdot (1, 1) = [n \cdot (1, 1)][m \cdot (1, 1)] = \phi(n)\phi(m). \quad \blacktriangle$$

Note that a direct product $R = R_1 \times R_2 \times \cdots \times R_n$ of rings is commutative if and and only if each ring R_i is commutative. Furthermore, R has a unity if and only if each R_i has a unity.

The set $\mathbb{R}^*$ of nonzero real numbers forms a group under multiplication. However, the nonzero integers do not form a group under multiplication since only the integers 1 and -1 have multiplicative inverses in $\mathbb{Z}$. In general, a **multiplicative inverse** of an element a in a ring R with unity $1 \neq 0$ is an element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. Precisely as for groups, a multiplicative inverse for an element a in R is unique, if it exists at all (see Exercise 45). Theorem 22.8 shows that it would be hopeless to have a multiplicative inverse for 0 except for the ring $\{0\}$, where $0 + 0 = 0$ and $(0)(0) = 0$, with 0 as both additive and multiplicative identity element. We are thus led to discuss the existence of multiplicative inverses for nonzero elements in a ring with nonzero unity. There is unavoidably a lot of terminology to be defined in this introductory section on rings. We are almost done.

22.16 Definition Let R be a ring with unity $1 \neq 0$. An element u in R is a **unit** of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a **division ring** (or **skew field**). A **field** is a commutative division ring. A noncommutative division ring is called a "**strictly skew field.**" ■

22.17 Example Let us find the units in $\mathbb{Z}_{14}$. Of course, 1 and $-1 = 13$ are units. Since $(3)(5) = 1$ we see that 3 and 5 are units; therefore $-3 = 11$ and $-5 = 9$ are also units. None of the remaining elements of $\mathbb{Z}_{14}$ can be units, since no multiple of 2, 4, 6, 7, 8, or 10 can be one more than a multiple of 14; they all have a common factor, either 2 or 7, with 14. Section 24 will show that the units in $\mathbb{Z}_n$ are precisely those $m \in \mathbb{Z}_n$ such that $\gcd(m, n) = 1$. ▲

22.18 Example $\mathbb{Z}$ is not a field, because 2, for example, has no multiplicative inverse, so 2 is not a unit in $\mathbb{Z}$. The only units in $\mathbb{Z}$ are 1 and -1. However, $\mathbb{Q}$ and $\mathbb{R}$ are fields. An example of a strictly skew field is given in Section 32. ▲

We have the natural concepts of a subring of a ring and a subfield of a field. A **subring of a ring** is a subset of the ring that is a ring under induced operations from the whole ring; a **subfield** is defined similarly for a subset of a field. In fact, let us say here once and for all that if we have a set, together with a certain specified type of *algebraic structure* (group, ring, field, integral domain, vector space, and so on), then any subset of this set, together with a natural induced algebraic structure *that yields an algebraic structure of the same type*, is a *substructure*. If K and L are both structures, we shall let $K \leq L$ denote that K is a substructure of L and $K < L$ denote that $K \leq L$ but $K \neq L$. Exercise 50 gives criteria for a subset S of a ring R to form a subring of R.

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.

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, $-1 \neq 1$.

EXERCISES 22

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.

29. Find all solutions to the equations $x^2 + x - 6 = 0$ in the ring $\mathbb{Z}_{13}$ by factoring the quadratic polynomial. Why are there not the same number of solutions in Exercise 28?

30. What is wrong with the following attempt at a proof of Property 2 in Theorem 22.8?

$(-a)b = ((-1)a)b = (-1)(ab) = -(ab)$.

Concepts

In Exercises 31 and 32, 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.

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

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

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

34. 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 $\mathbb{Z}_6$.]

35. Determine whether each of the following is 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

36. Show that the multiplication defined on the set F of functions in Example 22.4 satisfies axioms $\mathscr{R}_2$ and $\mathscr{R}_3$ for a ring.

37. Show that the evaluation map ϕ_a of Example 22.10 is a ring homomorphism.

38. Complete the argument outlined after Definitions 22.12 to show that isomorphism gives an equivalence relation on a collection of rings.

39. 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.]

40. 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.

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

42. 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.

43. (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.]

44. Show that the unity element in a subfield of a field must be the unity of the whole field, in contrast to Exercise 34 for rings.

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

46. 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 $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

47. (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.

48. 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.

49. 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.

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

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

51. **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.

52. 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.

53. 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 51). 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 $\{a^n \mid n \in \mathbb{Z}^+\}$.

54. (Chinese Remainder Theorem for two congruences) Let r and s be positive integers such that $\gcd(r, s) = 1$. Use the isomorphism in Example 22.15 to show that for $m, n \in \mathbb{Z}$, there exists an integer x such that $x \equiv m \pmod{r}$ and $x \equiv n \pmod{s}$.

55. **a.** State and prove the generalization of Example 22.15 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 $i = 1, 2, \cdots, n$.

56. 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.]

57. 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.

58. (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 57).

SECTION 23 INTEGRAL DOMAINS

While a careful treatment of polynomials is not given until Section 27, 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 be 0 only 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 factor the left side:

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

Then we conclude that the only possible values for x are 2 and 3. Why? The reason is that if x is replaced by any number a, the product $(a - 2)(a - 3)$ of the resulting numbers is 0 if and only if either $a - 2 = 0$ or $a - 3 = 0$.

23.1 Example Solve the equation $x^2 - 5x + 6 = 0$ in $\mathbb{Z}_{12}$.

Solution The factorization $x^2 - 5x + 6 = (x - 2)(x - 3)$ is still valid if we think of x as standing for any number in $\mathbb{Z}_{12}$. But in $\mathbb{Z}_{12}$, not only is $0a = a0 = 0$ for all $a \in \mathbb{Z}_{12}$, but also

$$\begin{aligned}(2)(6) = (6)(2) = (3)(4) = (4)(3) = (3)(8) = (8)(3)\\ = (4)(6) = (6)(4) = (4)(9) = (9)(4) = (6)(6) = (6)(8)\\ = (8)(6) = (6)(10) = (10)(6) = (8)(9) = (9)(8) = 0.\end{aligned}$$

We find, in fact, that our equation has not only 2 and 3 as solutions, but also 6 and 11, for $(6 - 2)(6 - 3) = (4)(3) = 0$ and $(11 - 2)(11 - 3) = (9)(8) = 0$ in $\mathbb{Z}_{12}$. ▲

These ideas are of such importance that we formalize them in a definition.

23.2 Definition If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are **divisors of 0** (or **0 divisors**). ■