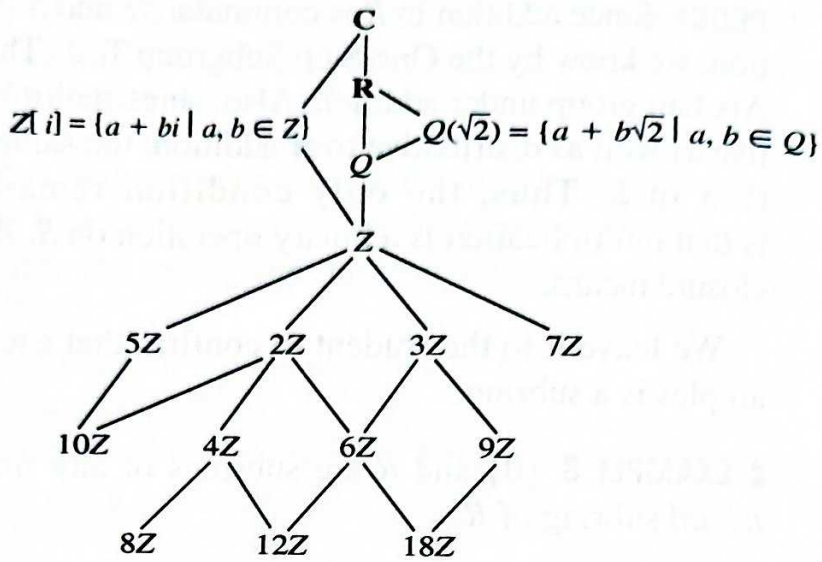

Figure 12.1 Partial subring lattice diagram of C.

In the next several chapters, we will see that many of the fundamental concepts of group theory can be naturally extended to rings. In particular, we will introduce ring homomorphisms and factor rings.

Exercises

There is no substitute for hard work.

Thomas Alva Edison, *Life*

1. Give an example of a finite noncommutative ring. Give an example of an infinite noncommutative ring that does not have a unity.
2. The ring $\{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10 has a unity. Find it.
3. Give an example of a subset of a ring that is a subgroup under addition but not a subring.
4. Show, by example, that for fixed nonzero elements a and b in a ring, the equation $ax = b$ can have more than one solution. How does this compare with groups?
5. Prove Theorem 12.2.
6. Find an integer n that shows that the rings Z_n need not have the following properties that the ring of integers has.
   a. $a^2 = a$ implies $a = 0$ or $a = 1$.
   b. $ab = 0$ implies $a = 0$ or $b = 0$.
   c. $ab = ac$ and $a \neq 0$ imply $b = c$.
   Is the n you found prime?
7. Show that the three properties listed in Exercise 6 are valid for Z_p, where p is prime.

8. Show that a ring is commutative if it has the property that $ab = ca$ implies $b = c$ when $a \neq 0$.
9. Prove that the intersection of any collection of subrings of a ring R is a subring of R.
10. Verify that Examples 8 through 13 in this chapter are as stated.
11. Prove rules 3 through 6 of Theorem 12.1.
12. Let a, b, and c be elements of a commutative ring, and suppose that a is a unit. Prove that b divides c if and only if ab divides c.
13. Describe all the subrings of the ring of integers.
14. Let a and b belong to a ring R and let m be an integer. Prove that $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$.
15. Show that if m and n are integers and a and b are elements from a ring, then $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$. (This exercise is referred to in Chapters 13 and 15.)
16. Show that if n is an integer and a is an element from a ring, then $n \cdot (-a) = -(n \cdot a)$.
17. Show that a ring that is cyclic under addition is commutative.
18. Let a belong to a ring R. Let $S = \{x \in R \mid ax = 0\}$. Show that S is a subring of R.
19. Let R be a ring. The *center of* R is the set $\{x \in R \mid ax = xa$ for all a in $R\}$. Prove that the center of a ring is a subring.
20. Describe the elements of $M_2(Z)$ (see Example 4) that have multiplicative inverses.
21. Suppose that $R_1, R_2, \ldots, R_n$ are rings that contain nonzero elements. Show that $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ has a unity if and only if each R_i has a unity.
22. Let R be a commutative ring with unity and let $U(R)$ denote the set of units of R. Prove that $U(R)$ is a group under the multiplication of R. (This group is called the *group of units of* R.)
23. Determine $U(Z[i])$ (see Example 11).
24. If $R_1, R_2, \ldots, R_n$ are commutative rings with unity, show that $U(R_1 \oplus R_2 \oplus \cdots \oplus R_n) = U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$.
25. Determine $U(Z[x])$. (This exercise is referred to in Chapter 17.)
26. Determine $U(\mathbf{R}[x])$.
27. Show that a unit of a ring divides every element of the ring.
28. In Z_6, show that $4 \mid 2$; in Z_8, show that $3 \mid 7$; in Z_{15}, show that $9 \mid 12$.
29. Suppose that a and b belong to a commutative ring R with unity. If a is a unit of R and $b^2 = 0$, show that $a + b$ is a unit of R.
30. Suppose that there is an integer $n > 1$ such that $x^n = x$ for all elements x of some ring. If m is a positive integer and $a^m = 0$ for some a, show that $a = 0$.

31. Give an example of ring elements a and b with the properties that $ab = 0$ but $ba \neq 0$.

32. Let n be an integer greater than 1. In a ring in which $x^n = x$ for all x, show that $ab = 0$ implies $ba = 0$.

33. Suppose that R is a ring such that $x^3 = x$ for all x in R. Prove that $6x = 0$ for all x in R.

34. Suppose that a belongs to a ring and $a^4 = a^2$. Prove that $a^{2n} = a^2$ for all $n \geq 1$.

35. Find an integer $n > 1$ such that $a^n = a$ for all a in Z_6. Do the same for Z_{10}. Show that no such n exists for Z_m when m is divisible by the square of some prime.

36. Let m and n be positive integers and let k be the least common multiple of m and n. Show that $mZ \cap nZ = kZ$.

37. Explain why every subgroup of Z_n under addition is also a subring of Z_n.

38. Is Z_6 a subring of Z_{12}?

39. Suppose that R is a ring with unity 1 and a is an element of R such that $a^2 = 1$. Let $S = \{ara \mid r \in R\}$. Prove that S is a subring of R. Does S contain 1?

40. Let $M_2(Z)$ be the ring of all 2×2 matrices over the integers and let $R = \left\{ \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} \middle| \, a, b \in Z \right\}$. Prove or disprove that R is a subring of $M_2(Z)$.

41. Let $M_2(Z)$ be the ring of all 2×2 matrices over the integers and let $R = \left\{ \begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} \middle| \, a, b \in Z \right\}$. Prove or disprove that R is a subring of $M_2(Z)$.

42. Let $R = \left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} \middle| \, a, b \in Z \right\}$. Prove or disprove that R is a subring of $M_2(Z)$.

43. Let $R = Z \oplus Z \oplus Z$ and $S = \{(a, b, c) \in R \mid a + b = c\}$. Prove or disprove that S is a subring of R.

44. Suppose that there is a positive even integer n such that $a^n = a$ for all elements a of some ring. Show that $-a = a$ for all a in the ring.

45. Let R be a ring with unity 1. Show that $S = \{n \cdot 1 \mid n \in Z\}$ is a subring of R.

46. Show that $2Z \cup 3Z$ is not a subring of Z.

47. Determine the smallest subring of Q that contains 1/2. (That is, find the subring S with the property that S contains 1/2 and, if T is any subring containing 1/2, then T contains S.)

48. Determine the smallest subring of Q that contains 2/3.

49. Let R be a ring. Prove that $a^2 - b^2 = (a + b)(a - b)$ for all a, b in R if and only if R is commutative.

50. Suppose that R is a ring and that $a^2 = a$ for all a in R. Show that R is commutative. [A ring in which $a^2 = a$ for all a is called a *Boolean* ring, in honor of the English mathematician George Boole (1815–1864).]

51. Give an example of a Boolean ring with four elements. Give an example of an infinite Boolean ring.

52. If a, b, and c are elements of a ring, does the equation $ax + b = c$ always have a solution x? If it does, must the solution be unique? Answer the same questions given that a is a unit.

53. Let R and S be commutative rings. Prove that (a, b) is a zero-divisor in $R \oplus S$ if and only if a or b is a zero-divisor or exactly one of a or b is 0.

54. Show that $4x^2 + 6x + 3$ is a unit in $Z_8[x]$.

55. Let R be a commutative ring with more than one element. Prove that if for every nonzero element a of R we have $aR = R$, then R has a unity and every nonzero element has an inverse.

56. Find an example of a commutative ring R with unity such that a, $b \in R$, $a \neq b$, $a^n = b^n$, and $a^m = b^m$, where n and m are positive integers that are relatively prime. (Compare with Exercise 39, part b, in Chapter 13.)

57. Suppose that R is a ring with the property that $xy = 0$ implies that $x = 0$ or $y = 0$ and that R contains a nonzero element b such that $b^2 = b$. Show that b is the unity for R.

Computer Exercises

Software for the computer exercises in this chapter is available at the website:

http://www.d.umn.edu/~jgallian

Suggested Reading

D. B. Erickson, "Orders for Finite Noncommutative Rings," *American Mathematical Monthly* 73 (1966): 376–377.

In this elementary paper, it is shown that there exists a noncommutative ring of order $m > 1$ if and only if m is divisible by the square of a prime.

Exercises

It looked absolutely impossible. But it so happens that you go on worrying away at a problem in science and it seems to get tired, and lies down and lets you catch it.

William Lawrence Bragg[†]

1. Verify that Examples 1 through 8 are as claimed.
2. Which of Examples 1 through 5 are fields?
3. Show that a commutative ring with the cancellation property (under multiplication) has no zero-divisors.
4. List all zero-divisors in Z_{20}. Can you see a relationship between the zero-divisors of Z_{20} and the units of Z_{20}?
5. Show that every nonzero element of Z_n is a unit or a zero-divisor.
6. Find a nonzero element in a ring that is neither a zero-divisor nor a unit.
7. Let R be a finite commutative ring with unity. Prove that every nonzero element of R is either a zero-divisor or a unit. What happens if we drop the "finite" condition on R?
8. Let $a \neq 0$ belong to a commutative ring. Prove that a is a zero-divisor if and only if $a^2b = 0$ for some $b \neq 0$.
9. Find elements a, b, and c in the ring $Z \oplus Z \oplus Z$ such that ab, ac, and bc are zero-divisors but abc is not a zero-divisor.
10. Describe all zero-divisors and units of $Z \oplus Q \oplus Z$.
11. Let d be an integer. Prove that $Z[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in Z\}$ is an integral domain. (This exercise is referred to in Chapter 18.)
12. In Z_7, give a reasonable interpretation for the expressions $1/2$, $-2/3$, $\sqrt{-3}$, and $-1/6$.
13. Give an example of a commutative ring without zero-divisors that is not an integral domain.
14. Find two elements a and b in a ring such that both a and b are zero-divisors, $a + b \neq 0$, and $a + b$ is not a zero-divisor.
15. Let a belong to a ring R with unity and suppose that $a^n = 0$ for some positive integer n. (Such an element is called *nilpotent*.) Prove that $1 - a$ has a multiplicative inverse in R. [*Hint:* Consider $(1 - a)(1 + a + a^2 + \cdots + a^{n-1})$.]
16. Show that the nilpotent elements of a commutative ring form a subring.

[†]Bragg, at age 24, won the Nobel Prize for the invention of x-ray crystallography. He remains the youngest person ever to receive the Nobel Prize.

17. Show that 0 is the only nilpotent element in an integral domain.
18. A ring element a is called an *idempotent* if $a^2 = a$. Prove that the only idempotents in an integral domain are 0 and 1.
19. Let a and b be idempotents in a commutative ring. Show that each of the following is also an idempotent: ab, $a - ab$, $a + b - ab$, $a + b - 2ab$.
20. Show that Z_n has a nonzero nilpotent element if and only if n is divisible by the square of some prime.
21. Let R be the ring of real-valued continuous functions on $[-1, 1]$. Show that R has zero-divisors.
22. Prove that if a is a ring idempotent, then $a^n = a$ for all positive integers n.
23. Determine all ring elements that are both nilpotent elements and idempotents.
24. Find a zero-divisor in $Z_5[i] = \{a + bi \mid a, b \in Z_5\}$.
25. Find an idempotent in $Z_5[i] = \{a + bi \mid a, b \in Z_5\}$.
26. Find all units, zero-divisors, idempotents, and nilpotent elements in $Z_3 \oplus Z_6$.
27. Determine all elements of a ring that are both units and idempotents.
28. Let R be the set of all real-valued functions defined for all real numbers under function addition and multiplication.
    a. Determine all zero-divisors of R.
    b. Determine all nilpotent elements of R.
    c. Show that every nonzero element is a zero-divisor or a unit.
29. (Subfield Test) Let F be a field and let K be a subset of F with at least two elements. Prove that K is a subfield of F if, for any a, b $(b \neq 0)$ in K, $a - b$ and ab^{-1} belong to K.
30. Let d be a positive integer. Prove that $Q[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in Q\}$ is a field.
31. Let R be a ring with unity 1. If the product of any pair of nonzero elements of R is nonzero, prove that $ab = 1$ implies $ba = 1$.
32. Let $R = \{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10. Prove that R is a field.
33. Formulate the appropriate definition of a subdomain (that is, a "sub" integral domain). Let D be an integral domain with unity 1. Show that $P = \{n \cdot 1 \mid n \in Z\}$ (that is, all integral multiples of 1) is a subdomain of D. Show that P is contained in every subdomain of D. What can we say about the order of P?
34. Prove that there is no integral domain with exactly six elements. Can your argument be adapted to show that there is no integral domain

with exactly four elements? What about 15 elements? Use these observations to guess a general result about the number of elements in a finite integral domain.

35. Let F be a field of order 2^n. Prove that char $F = 2$.

36. Determine all elements of an integral domain that are their own inverses under multiplication.

37. Characterize those integral domains for which 1 is the only element that is its own multiplicative inverse.

38. Determine all integers $n > 1$ for which $(n - 1)!$ is a zero-divisor in Z_n.

39. Suppose that a and b belong to an integral domain.

a. If $a^5 = b^5$ and $a^3 = b^3$, prove that $a = b$.

b. If $a^m = b^m$ and $a^n = b^n$, where m and n are positive integers that are relatively prime, prove that $a = b$.

40. Find an example of an integral domain and distinct positive integers m and n such that $a^m = b^m$ and $a^n = b^n$, but $a \neq b$.

41. If a is an idempotent in a commutative ring, show that $1 - a$ is also an idempotent.

42. Construct a multiplication table for $Z_2[i]$, the ring of Gaussian integers modulo 2. Is this ring a field? Is it an integral domain?

43. The nonzero elements of $Z_3[i]$ form an Abelian group of order 8 under multiplication. Is it isomorphic to Z_8, $Z_4 \oplus Z_2$, or $Z_2 \oplus Z_2 \oplus Z_2$?

44. Show that $Z_7[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in Z_7\}$ is a field. For any positive integer k and any prime p, determine a necessary and sufficient condition for $Z_p[\sqrt{k}] = \{a + b\sqrt{k} \mid a, b \in Z_p\}$ to be a field.

45. Show that a finite commutative ring with no zero-divisors and at least two elements has a unity.

46. Suppose that a and b belong to a commutative ring and ab is a zero-divisor. Show that either a or b is a zero-divisor.

47. Suppose that R is a commutative ring without zero-divisors. Show that all the nonzero elements of R have the same additive order.

48. Suppose that R is a commutative ring without zero-divisors. Show that the characteristic of R is 0 or prime.

49. Let x and y belong to a commutative ring R with prime characteristic p.

a. Show that $(x + y)^p = x^p + y^p$.

b. Show that, for all positive integers n, $(x + y)^{p^n} = x^{p^n} + y^{p^n}$.

c. Find elements x and y in a ring of characteristic 4 such that $(x + y)^4 \neq x^4 + y^4$. (This exercise is referred to in Chapter 20.)

50. Let R be a commutative ring with unity 1 and prime characteristic. If $a \in R$ is nilpotent, prove that there is a positive integer k such that $(1 + a)^k = 1$.

51. Show that any finite field has order p^n, where p is a prime. *Hint:* Use facts about finite Abelian groups. (This exercise is referred to in Chapter 22.)

52. Give an example of an infinite integral domain that has characteristic 3.

53. Let R be a ring and let $M_2(R)$ be the ring of 2×2 matrices with entries from R. Explain why these two rings have the same characteristic.

54. Let R be a ring with m elements. Show that the characteristic of R divides m.

55. Explain why a finite ring must have a nonzero characteristic.

56. Find all solutions of $x^2 - x + 2 = 0$ over $Z_3[i]$. (See Example 9.)

57. Consider the equation $x^2 - 5x + 6 = 0$.
    a. How many solutions does this equation have in Z_7?
    b. Find all solutions of this equation in Z_8.
    c. Find all solutions of this equation in Z_{12}.
    d. Find all solutions of this equation in Z_{14}.

58. Find the characteristic of $Z_4 \oplus 4Z$.

59. Suppose that R is an integral domain in which $20 \cdot 1 = 0$ and $12 \cdot 1 = 0$. (Recall that $n \cdot 1$ means the sum $1 + 1 + \cdots + 1$ with n terms.) What is the characteristic of R?

60. In a commutative ring of characteristic 2, prove that the idempotents form a subring.

61. Describe the smallest subfield of the field of real numbers that contains $\sqrt{2}$. (That is, describe the subfield K with the property that K contains $\sqrt{2}$ and if F is any subfield containing $\sqrt{2}$, then F contains K.)

62. Let F be a finite field with n elements. Prove that $x^{n-1} = 1$ for all nonzero x in F.

63. Let F be a field of prime characteristic p. Prove that $K = \{x \in F \mid x^p = x\}$ is a subfield of F.

64. Suppose that a and b belong to a field of order 8 and that $a^2 + ab + b^2 = 0$. Prove that $a = 0$ and $b = 0$. Do the same when the field has order 2^n with n odd.

65. Let F be a field of characteristic 2 with more than two elements. Show that $(x + y)^3 \neq x^3 + y^3$ for some x and y in F.

66. Suppose that F is a field with characteristic not 2, and that the nonzero elements of F form a cyclic group under multiplication. Prove that F is finite.

67. Suppose that D is an integral domain and that ϕ is a nonconstant function from D to the nonnegative integers such that $\phi(xy) = \phi(x)\phi(y)$. If x is a unit in D, show that $\phi(x) = 1$.

68. Let F be a field of order 32. Show that the only subfields of F are F itself and $\{0, 1\}$.

69. Suppose that F is a field with 27 elements. Show that for every element $a \in F$, $5a = -a$.

Computer Exercises

Computer exercises for this chapter are available at the website:

http://www.d.umn.edu/~jgallian

Suggested Readings

Eric Berg, "A Family of Fields," *Pi Mu Epsilon* 9 (1990): 154–155.

In this article, the author uses properties of logarithms and exponents to define recursively an infinite family of fields starting with the real numbers.

N. A. Khan, "The Characteristic of a Ring," *American Mathematical Monthly* 70 (1963): 736–738.

Here it is shown that a ring has nonzero characteristic n if and only if n is the maximum of the orders of the elements of R.

K. Robin McLean, "Groups in Modular Arithmetic," *The Mathematical Gazette* 62 (1978): 94–104.

This article explores the interplay between various groups of integers under multiplication modulo n and the ring Z_n. It shows how to construct groups of integers in which the identity is not obvious; for example, 1977 is the identity of the group $\{1977, 5931\}$ under multiplication modulo 7908.

When a commutative ring has a unity, it follows from Theorems 14.3 and 14.4 that a maximal ideal is a prime ideal. The next example shows that a prime ideal need not be maximal.

EXAMPLE 17 The ideal $\langle x \rangle$ is a prime ideal in $Z[x]$ but not a maximal ideal in $Z[x]$. To verify this, we begin with the observation that $\langle x \rangle = \{f(x) \in Z[x] \mid f(0) = 0\}$ (see Exercise 31). Thus, if $g(x)h(x) \in \langle x \rangle$, then $g(0)h(0) = 0$. And since $g(0)$ and $h(0)$ are integers, we have $g(0) = 0$ or $h(0) = 0$.

To see that $\langle x \rangle$ is not maximal, we simply note that $\langle x \rangle \subset \langle x, 2 \rangle \subset Z[x]$ (see Exercise 39). ∎

Exercises

One Problem after another presents itself and in the solving of them we can find our greatest pleasure.

Karl Menninger

1. Verify that the set defined in Example 3 is an ideal.
2. Verify that the set A in Example 4 is an ideal and that $A = \langle x \rangle$.
3. Verify that the set I in Example 5 is an ideal and that if J is any ideal of R that contains $a_1, a_2, \ldots, a_n$, then $I \subseteq J$. (Hence, $\langle a_1, a_2, \ldots, a_n \rangle$ is the smallest ideal of R that contains $a_1, a_2, \ldots, a_n$.)
4. Find a subring of $Z \oplus Z$ that is not an ideal of $Z \oplus Z$.
5. Let $S = \{a + bi \mid a, b \in Z, b \text{ is even}\}$. Show that S is a subring of $Z[i]$, but not an ideal of $Z[i]$.
6. Find all maximal ideals in
   a. Z_8. **b.** Z_{10}. **c.** Z_{12}. **d.** Z_n.
7. Let a belong to a commutative ring R. Show that $aR = \{ar \mid r \in R\}$ is an ideal of R. If R is the ring of even integers, list the elements of $4R$.
8. Prove that the intersection of any set of ideals of a ring is an ideal.
9. If n is an integer greater than 1, show that $\langle n \rangle = nZ$ is a prime ideal of Z if and only if n is prime. (This exercise is referred to in this chapter.)
10. If A and B are ideals of a ring, show that the *sum* of A and B, $A + B = \{a + b \mid a \in A, b \in B\}$, is an ideal.
11. In the ring of integers, find a positive integer a such that
    a. $\langle a \rangle = \langle 2 \rangle + \langle 3 \rangle$.
    b. $\langle a \rangle = \langle 6 \rangle + \langle 8 \rangle$.
    c. $\langle a \rangle = \langle m \rangle + \langle n \rangle$.

12. If A and B are ideals of a ring, show that the *product* of A and B, $AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a_i \in A, b_i \in B, n \text{ a positive integer}\}$, is an ideal.
13. Find a positive integer a such that
    a. $\langle a \rangle = \langle 3 \rangle \langle 4 \rangle$.
    b. $\langle a \rangle = \langle 6 \rangle \langle 8 \rangle$.
    c. $\langle a \rangle = \langle m \rangle \langle n \rangle$.
14. Let A and B be ideals of a ring. Prove that $AB \subseteq A \cap B$.
15. If A is an ideal of a ring R and 1 belongs to A, prove that $A = R$. (This exercise is referred to in this chapter.)
16. If A and B are ideals of a commutative ring R with unity and $A + B = R$, show that $A \cap B = AB$.
17. If an ideal I of a ring R contains a unit, show that $I = R$.
18. If R is a finite commutative ring with unity, prove that every prime ideal of R is a maximal ideal of R.
19. Give an example of a ring that has exactly two maximal ideals.
20. Suppose that R is a commutative ring and $|R| = 30$. If I is an ideal of R and $|I| = 10$, prove that I is a maximal ideal.
21. Let R and I be as described in Example 10. Prove that I is an ideal of R.
22. Let $I = \langle 2 \rangle$. Prove that $I[x]$ is not a maximal ideal of $Z[x]$ even though I is a maximal ideal of Z.
23. Verify the claim made in Example 10 about the size of R/I.
24. Give an example of a commutative ring that has a maximal ideal that is not a prime ideal.
25. Show that the set B in the latter half of the proof of Theorem 14.4 is an ideal of R. (This exercise is referred to in this chapter.)
26. If R is a commutative ring with unity and A is a proper ideal of R, show that R/A is a commutative ring with unity.
27. Prove that the only ideals of a field F are $\{0\}$ and F itself.
28. Let R be a commutative ring with unity. Suppose that the only ideals of R are $\{0\}$ and R. Show that R is a field.
29. List the distinct elements in the ring $Z[x]/\langle 3, x^2 + 1 \rangle$. Show that this ring is a field.
30. Show that $\mathbf{R}[x]/\langle x^2 + 1 \rangle$ is a field.
31. In $Z[x]$, the ring of polynomials with integer coefficients, let $I = \{f(x) \in Z[x] \mid f(0) = 0\}$. Prove that $I = \langle x \rangle$. (This exercise is referred to in this chapter and in Chapter 15.)
32. Show that $A = \{(3x, y) \mid x, y \in Z\}$ is a maximal ideal of $Z \oplus Z$. Generalize. What happens if $3x$ is replaced by $4x$? Generalize.

33. Let R be the ring of continuous functions from $\mathbf{R}$ to $\mathbf{R}$. Show that $A = \{f \in R \mid f(0) = 0\}$ is a maximal ideal of R.

34. Let $R = Z_8 \oplus Z_{30}$. Find all maximal ideals of R, and for each maximal ideal I, identify the size of the field R/I.

35. How many elements are in $Z[i]/\langle 3 + i\rangle$? Give reasons for your answer.

36. In $Z[x]$, the ring of polynomials with integer coefficients, let $I = \{f(x) \in Z[x] \mid f(0) = 0\}$. Prove that I is not a maximal ideal.

37. In $Z \oplus Z$, let $I = \{(a, 0) \mid a \in Z\}$. Show that I is a prime ideal but not a maximal ideal.

38. Let R be a ring and let I be an ideal of R. Prove that the factor ring R/I is commutative if and only if $rs - sr \in I$ for all r and s in R.

39. In $Z[x]$, let $I = \{f(x) \in Z[x] \mid f(0)$ is an even integer$\}$. Prove that $I = \langle x, 2\rangle$. Is I a prime ideal of $Z[x]$? Is I a maximal ideal? How many elements does $Z[x]/I$ have? (This exercise is referred to in this chapter.)

40. Prove that $I = \langle 2 + 2i\rangle$ is not a prime ideal of $Z[i]$. How many elements are in $Z[i]/I$? What is the characteristic of $Z[i]/I$?

41. In $Z_5[x]$, let $I = \langle x^2 + x + 2\rangle$. Find the multiplicative inverse of $2x + 3 + I$ in $Z_5[x]/I$.

42. Let R be a ring and let p be a fixed prime. Show that $I_p = \{r \in R \mid$ additive order of r is a power of $p\}$ is an ideal of R.

43. An integral domain D is called a *principal ideal domain* if every ideal of D has the form $\langle a\rangle = \{ad \mid d \in D\}$ for some a in D. Show that Z is a principal ideal domain. (This exercise is referred to in Chapter 18.)

44. Let $R = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \middle| \, a, b, d \in Z\right\}$ and $S = \left\{\begin{bmatrix} r & s \\ 0 & t \end{bmatrix} \middle| \, r, s, t \in Z, s \text{ is even}\right\}$. If S is an ideal of R, what can you say about r and t?

45. If R and S are principal ideal domains, prove that $R \oplus S$ is a principal ideal ring. (See Exercise 41 for the definition.)

46. In a principal ideal domain, show that every nontrivial prime ideal is a maximal ideal.

47. Let R be a commutative ring and let A be any subset of R. Show that the *annihilator* of A, $\text{Ann}(A) = \{r \in R \mid ra = 0$ for all a in $A\}$, is an ideal.

48. Let R be a commutative ring and let A be any ideal of R. Show that the *nil radical* of A, $N(A) = \{r \in R \mid r^n \in A$ for some positive integer n (n depends on r)$\}$, is an ideal of R. [$N(\langle 0\rangle)$ is called the *nil radical* of R.]

49. Let $R = Z_{27}$. Find

a. $N(\langle 0\rangle)$. **b.** $N(\langle 3\rangle)$. **c.** $N(\langle 9\rangle)$.

50. Let $R = Z_{36}$. Find

a. $N(\langle 0\rangle)$. **b.** $N(\langle 4\rangle)$. **c.** $N(\langle 6\rangle)$.

51. Let R be a commutative ring. Show that $R/N(\langle 0\rangle)$ has no nonzero nilpotent elements.

52. Let A be an ideal of a commutative ring. Prove that $N(N(A)) = N(A)$.

53. Let $Z_2[x]$ be the ring of all polynomials with coefficients in Z_2 (that is, coefficients are 0 or 1, and addition and multiplication of coefficients are done modulo 2). Show that $Z_2[x]/\langle x^2 + x + 1\rangle$ is a field.

54. List the elements of the field given in Exercise 51, and make an addition and multiplication table for the field.

55. Show that $Z_3[x]/\langle x^2 + x + 1\rangle$ is not a field.

56. Let R be a commutative ring without unity, and let $a \in R$. Describe the smallest ideal I of R that contains a (that is, if J is any ideal that contains a, then $I \subseteq J$).

57. Let R be the ring of continuous functions from $\mathbf{R}$ to $\mathbf{R}$. Let $A = \{f \in R \mid f(0) \text{ is an even integer}\}$. Show that A is a subring of R, but not an ideal of R.

58. Show that $Z[i]/\langle 1 - i\rangle$ is a field. How many elements does this field have?

59. If R is a principal ideal domain and I is an ideal of R, prove that every ideal of R/I is principal (see Exercise 43).

60. How many elements are in $Z_5[i]/\langle 1 + i\rangle$?

61. Show, by example, that the intersection of two prime ideals need not be a prime ideal.

62. Let $\mathbf{R}$ denote the ring of real numbers. Determine all ideals of $\mathbf{R} \oplus \mathbf{R}$. What happens if $\mathbf{R}$ is replaced by any field F?

63. Find the characteristic of $Z[i]/\langle 2 + i\rangle$.

64. Show that the characteristic of $Z[i]/\langle a + bi\rangle$ divides $a^2 + b^2$.

65. Prove that the set of all polynomials whose coefficients are all even is a prime ideal in $Z[x]$.

66. Let $R = Z[\sqrt{-5}]$ and let $I = \{a + b\sqrt{-5} \mid a, b \in Z, a - b \text{ is even}\}$. Show that I is a maximal ideal of R.

67. Let R be a commutative ring with unity that has the property that $a^2 = a$ for all a in R. Let I be a prime ideal in R. Show that $|R/I| = 2$.

68. Let R be a commutative ring with unity, and let I be a proper ideal with the property that every element of R that is not in I is a unit of R. Prove that I is the unique maximal ideal of R.

69. Let $I_0 = \{f(x) \in Z[x] \mid f(0) = 0\}$. For any positive integer n, show that there exists a sequence of strictly increasing ideals such that $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_n \subset Z[x]$.

70. Let $R = \{(a_1, a_2, a_3, \ldots)\}$, where each $a_i \in Z$. Let $I = \{(a_1, a_2, a_3, \ldots)\}$, where only a finite number of terms are nonzero. Prove that I is not a principal ideal of R.

71. Let R be a commutative ring with unity and let $a, b \in R$. Show that $\langle a, b\rangle$, the smallest ideal of R containing a and b, is $I = \{ra + sb \mid r, s \in R\}$. That is, show that I contains a and b and that any ideal that contains a and b also contains I.

Computer Exercises

Computer exercises for this chapter are available at the website:

http://www.d.umn.edu/~jgallian

Suggested Reading

Thomas Sonar, "Brunswick's Second Mathematical Star: Richard Dedekind (1831–1916)," *The Mathematical Intelligencer* 34:2 (2012): 63–67.

This beautifully illustrated short biographical sketch of Dedekind emphasizes the breadth of his talent and interests. Dedekind was the last doctoral student of Gauss, and a steadfast friend of Bernhard Riemann. He gave the first lectures on Galois theory in Germany, edited the collective works of Lejeune Dirichlet, and promoted the work of Georg Cantor. He was also an accomplished musician on the piano and the cello, and played chamber music with Brahms in the home of Dirichlet, whose wife Rebecka Mendelssohn was the sister of Felix Mendelssohn. As the first president of the Technical University of Brunswick, Dedekind supervised the construction of the new university. In his honor, the council of mathematics students at the university still call themselves the Dedekinder, the "children of Dedekind".

Exercises

We can work it out.

John Lennon and Paul McCartney,
"We Can Work It Out," single*

1. Prove Theorem 15.1.
2. Prove Theorem 15.2.
3. Prove Theorem 15.3.
4. Prove Theorem 15.4.
5. Show that the correspondence $x \to 5x$ from Z_5 to Z_{10} does not preserve addition.
6. Show that the correspondence $x \to 3x$ from Z_4 to Z_{12} does not preserve multiplication.
7. Show that the mapping $\phi: D \to F$ in the proof of Theorem 15.6 is a ring homomorphism.
8. Prove that every ring homomorphism ϕ from Z_n to itself has the form $\phi(x) = ax$, where $a^2 = a$.
9. Suppose that ϕ is a ring homomorphism from Z_m to Z_n. Prove that if $\phi(1) = a$, then $a^2 = a$. Give an example to show that the converse is false.
10. **a.** Is the ring $2Z$ isomorphic to the ring $3Z$?
    b. Is the ring $2Z$ isomorphic to the ring $4Z$?
11. Prove that the intersection of any collection of subfields of a field F is a subfield of F. (This exercise is referred to in this chapter.)
12. Let $Z_3[i] = \{a + bi \mid a, b \in Z_3\}$ (see Example 9 in Chapter 13). Show that the field $Z_3[i]$ is ring-isomorphic to the field $Z_3[x]/\langle x^2 + 1\rangle$.
13. Let

$$S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| \, a, b \in \mathbf{R} \right\}.$$

Show that $\phi: \mathbf{C} \to S$ given by

$$\phi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

is a ring isomorphism.

14. Let $Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Z\}$ and

$$H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \middle| \, a, b \in Z \right\}.$$

Show that $Z[\sqrt{2}]$ and H are isomorphic as rings.

---

*Copyright © 1965 (Renewed) Stony/ATV Tunes LLC. All rights administered by Sony/ATV Music Publishing, 8 Music Square West, Nashville, TN 37203. All rights reserved.

15. Consider the mapping from $M_2(Z)$ into Z given by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to a$. Prove or disprove that this is a ring homomorphism.

16. Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| a, b, c \in Z \right\}$. Prove or disprove that the mapping $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \to a$ is a ring homomorphism.

17. Is the mapping from Z_5 to Z_{30} given by $x \to 6x$ a ring homomorphism? Note that the image of the unity is the unity of the image but not the unity of Z_{30}.

18. Is the mapping from Z_{10} to Z_{10} given by $x \to 2x$ a ring homomorphism?

19. Describe the kernel of the homomorphism given in Example 3.

20. Recall that a ring element a is called an idempotent if $a^2 = a$. Prove that a ring homomorphism carries an idempotent to an idempotent.

21. Determine all ring homomorphisms from Z_6 to Z_6. Determine all ring homomorphisms from Z_{20} to Z_{30}.

22. Determine all ring isomorphisms from Z_n to itself.

23. Determine all ring homomorphisms from Z to Z.

24. Suppose ϕ is a ring homomorphism from $Z \oplus Z$ into $Z \oplus Z$. What are the possibilities for $\phi((1, 0))$?

25. Determine all ring homomorphisms from $Z \oplus Z$ into $Z \oplus Z$.

26. In Z, let $A = \langle 2 \rangle$ and $B = \langle 8 \rangle$. Show that the group A/B is isomorphic to the group Z_4 but that the ring A/B is not ring-isomorphic to the ring Z_4.

27. Let R be a ring with unity and let ϕ be a ring homomorphism from R onto S where S has more than one element. Prove that S has a unity.

28. Show that $(Z \oplus Z)/(\langle a \rangle \oplus \langle b \rangle)$ is ring-isomorphic to $Z_a \oplus Z_b$.

29. Determine all ring homomorphisms from $Z \oplus Z$ to Z.

30. Prove that the sum of the squares of three consecutive integers cannot be a square.

31. Let m be a positive integer and let n be an integer obtained from m by rearranging the digits of m in some way. (For example, 72345 is a rearrangement of 35274.) Show that $m - n$ is divisible by 9.

32. (Test for Divisibility by 11) Let n be an integer with decimal representation $a_k a_{k-1} \cdots a_1 a_0$. Prove that n is divisible by 11 if and only if $a_0 - a_1 + a_2 - \cdots (-1)^k a_k$ is divisible by 11.

33. Show that the number 7,176,825,942,116,027,211 is divisible by 9 but not divisible by 11.

34. If m and n are positive integers, prove that the mapping from Z_m to Z_n given by $\phi(x) = x \bmod n$ is a ring homomorphism if and only if n divides m.

35. (Test for Divisibility by 3) Let n be an integer with decimal representation $a_k a_{k-1} \cdots a_1 a_0$. Prove that n is divisible by 3 if and only if $a_k + a_{k-1} + \cdots + a_1 + a_0$ is divisible by 3.

36. (Test for Divisibility by 4) Let n be an integer with decimal representation $a_k a_{k-1} \cdots a_1 a_0$. Prove that n is divisible by 4 if and only if $a_1 a_0$ is divisible by 4.

37. For any integer $n > 1$, prove that $Z_n[x]/\langle x \rangle$ is isomorphic to Z_n.

38. For any integer $n > 1$, prove that $\langle x \rangle$ is a maximal ideal of $Z_n[x]$ if and only if n is prime.

39. Give an example of a ring homomorphism from a commutative ring R to a ring S that maps a zero-divisor in R to the unity of S.

40. Prove that any automorphism of a field F is the identity from the prime subfield to itself.

41. In your head, determine $(2 \cdot 10^{75} + 2)^{100} \bmod 3$ and $(10^{100} + 1)^{99} \bmod 3$.

42. Determine all ring homomorphisms from Q to Q.

43. Let R and S be commutative rings with unity. If ϕ is a homomorphism from R onto S and the characteristic of R is nonzero, prove that the characteristic of S divides the characteristic of R.

44. Let R be a commutative ring of prime characteristic p. Show that the *Frobenius* map $x \to x^p$ is a ring homomorphism from R to R.

45. Is there a ring homomorphism from the reals to some ring whose kernel is the integers?

46. Show that a homomorphism from a field onto a ring with more than one element must be an isomorphism.

47. Suppose that R and S are commutative rings with unities. Let ϕ be a ring homomorphism from R onto S and let A be an ideal of S.
    a. If A is prime in S, show that $\phi^{-1}(A) = \{x \in R \mid \phi(x) \in A\}$ is prime in R.
    b. If A is maximal in S, show that $\phi^{-1}(A)$ is maximal in R.

48. A *principal ideal ring* is a ring with the property that every ideal has the form $\langle a \rangle$. Show that the homomorphic image of a principal ideal ring is a principal ideal ring.

49. Let R and S be rings.
    a. Show that the mapping from $R \oplus S$ onto R given by $(a, b) \to a$ is a ring homomorphism.
    b. Show that the mapping from R to $R \oplus S$ given by $a \to (a, 0)$ is a one-to-one ring homomorphism.
    c. Show that $R \oplus S$ is ring-isomorphic to $S \oplus R$.

50. Show that if m and n are distinct positive integers, then mZ is not ring-isomorphic to nZ.

51. Prove or disprove that the field of real numbers is ring-isomorphic to the field of complex numbers.

52. Show that the only ring automorphism of the real numbers is the identity mapping.

53. Determine all ring homomorphisms from $\mathbf{R}$ to $\mathbf{R}$.

54. Suppose that n divides m and that a is an idempotent of Z_n (that is, $a^2 = a$). Show that the mapping $x \to ax$ is a ring homomorphism from Z_m to Z_n. Show that the same correspondence need not yield a ring homomorphism if n does not divide m.

55. Show that the operation of multiplication defined in the proof of Theorem 15.6 is well-defined.

56. Let $Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$ and $Q[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in Q\}$. Show that these two rings are not ring-isomorphic.

57. Let $Z[i] = \{a + bi \mid a, b \in Z\}$. Show that the field of quotients of $Z[i]$ is ring-isomorphic to $Q[i] = \{r + si \mid r, s \in Q\}$. (This exercise is referred to in Chapter 18.)

58. Let F be a field. Show that the field of quotients of F is ring-isomorphic to F.

59. Let D be an integral domain and let F be the field of quotients of D. Show that if E is any field that contains D, then E contains a subfield that is ring-isomorphic to F. (Thus, the field of quotients of an integral domain D is the smallest field containing D.)

60. Explain why a commutative ring with unity that is not an integral domain cannot be contained in a field. (Compare with Theorem 15.6.)

61. Show that the relation $\equiv$ defined in the proof of Theorem 15.6 is an equivalence relation.

62. Give an example of a ring without unity that is contained in a field.

63. Prove that the set T in the proof of Corollary 3 to Theorem 15.5 is ring-isomorphic to the field of rational numbers.

64. Suppose that $\phi: R \to S$ is a ring homomorphism and that the image of ϕ is not $\{0\}$. If R has a unity and S is an integral domain, show that ϕ carries the unity of R to the unity of S. Give an example to show that the preceding statement need not be true if S is not an integral domain.

65. Let $f(x) \in \mathbf{R}[x]$. If $a + bi$ is a complex zero of $f(x)$ (here $i = \sqrt{-1}$), show that $a - bi$ is a zero of $f(x)$. (This exercise is referred to in Chapter 32.)

66. Let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| \, a, b \in Z \right\}$, and let ϕ be the mapping that takes $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ to $a - b$.

a. Show that ϕ is a homomorphism.
b. Determine the kernel of ϕ.
c. Show that $R/\text{Ker}\,\phi$ is isomorphic to Z.
d. Is Ker ϕ a prime ideal?
e. Is Ker ϕ a maximal ideal?

67. Show that the prime subfield of a field of characteristic p is ring-isomorphic to Z_p and that the prime subfield of a field of characteristic 0 is ring-isomorphic to Q. (This exercise is referred to in this chapter.)

68. Let n be a positive integer. Show that there is a ring isomorphism from Z_2 to a subring of Z_{2n} if and only if n is odd.

69. Show that Z_{mn} is ring-isomorphic to $Z_m \oplus Z_n$ when m and n are relatively prime.

Suggested Readings

J. A. Gallian and J. Van Buskirk, "The Number of Homomorphisms from Z_m into Z_n," *American Mathematical Monthly* 91 (1984): 196–197.

In this article, formulas are given for the number of group homomorphisms from Z_m into Z_n and the number of ring homomorphisms from Z_m into Z_n.

Lillian Kinkade and Joyce Wagner, "When Polynomial Rings Are Principal Ideal Rings," *Journal of Undergraduate Mathematics* 23 (1991): 59–62.

In this article written by undergraduates, it is shown that $R[x]$ is a principal ideal ring if and only if $R \approx R_1 \oplus R_2 \oplus \cdots \oplus R_n$, where each R_i is a field.

Mohammad Saleh and Hasan Yousef, "The Number of Ring Homomorphisms from $Z_{m1} \oplus \cdots \oplus Z_{mr}$ into $Z_{k1} \oplus \cdots \oplus Z_{ks}$," *American Mathematical Monthly* 105 (1998): 259–260.

This article gives a formula for the number described in the title.