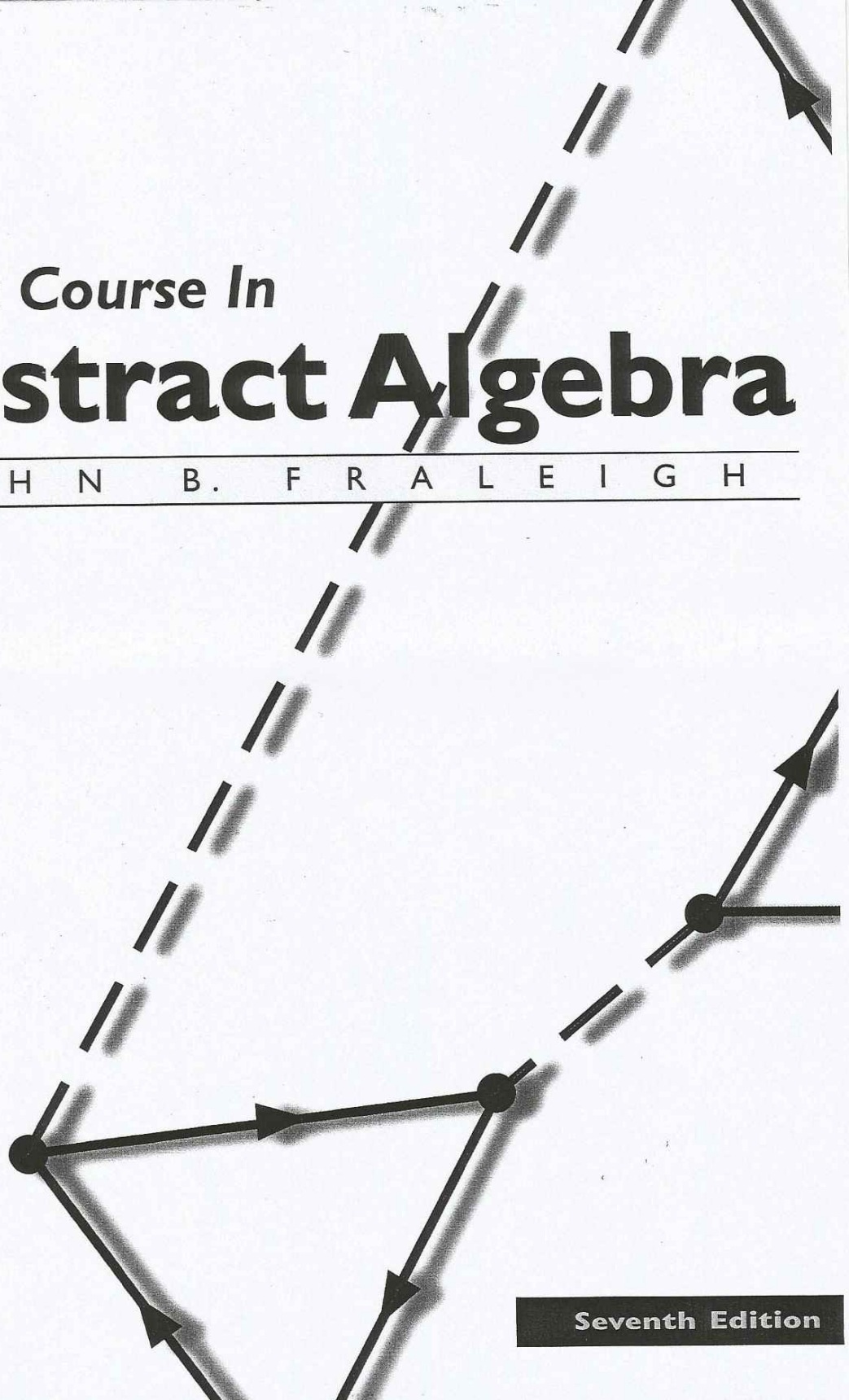
A First Course In

Abstract Algebra

JOHN B. FRALEIGH



Seventh Edition

† Not required for the remainder of the text.

‡ This section is a prerequisite for Sections 17 and 36 only.

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 ... 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 ... 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 ...

nature of these solutions of polynomial equations. We need have no fear in approaching this material. *We shall be dealing with familiar topics of high school algebra. This work should seem much more natural than group theory.*

In conclusion, we remark that the machinery of factor rings and ring homomorphisms is not really necessary in order for us to achieve our *basic goal*. For a direct demonstration, see Artin [27, p. 29]. However, factor rings and ring homomorphisms are fundamental ideas that we should grasp, and our *basic goal* will follow very easily once we have mastered them.

EXERCISES 22

Computations

In Exercises 1 through 4, find the sum and the product of the given polynomials in the given polynomial ring.

1. $f(x) = 4x - 5, g(x) = 2x^2 - 4x + 2$ in $\mathbb{Z}_8[x]$.
2. $f(x) = x + 1, g(x) = x + 1$ in $\mathbb{Z}_2[x]$.
3. $f(x) = 2x^2 + 3x + 4, g(x) = 3x^2 + 2x + 3$ in $\mathbb{Z}_6[x]$.
4. $f(x) = 2x^3 + 4x^2 + 3x + 2, g(x) = 3x^4 + 2x + 4$ in $\mathbb{Z}_5[x]$.
5. How many polynomials are there of degree ≤ 3 in $\mathbb{Z}_2[x]$? (Include 0.)
6. How many polynomials are there of degree ≤ 2 in $\mathbb{Z}_5[x]$? (Include 0.)

In Exercises 7 and 8, $F = E = \mathbb{C}$ in Theorem 22.4. Compute for the indicated evaluation homomorphism.

7. $\phi_2(x^2 + 3)$
8. $\phi_i(2x^3 - x^2 + 3x + 2)$

In Exercises 9 through 11, $F = E = \mathbb{Z}_7$ in Theorem 22.4. Compute for the indicated evaluation homomorphism.

9. $\phi_3[(x^4 + 2x)(x^3 - 3x^2 + 3)]$
10. $\phi_5[(x^3 + 2)(4x^2 + 3)(x^7 + 3x^2 + 1)]$
11. $\phi_4(3x^{106} + 5x^{99} + 2x^{53})$ [*Hint:* Use Fermat's theorem.]

In Exercises 12 through 15, find all zeros in the indicated finite field of the given polynomial with coefficients in that field. [*Hint:* One way is simply to try all candidates!]

12. $x^2 + 1$ in $\mathbb{Z}_2$
13. $x^3 + 2x + 2$ in $\mathbb{Z}_7$
14. $x^5 + 3x^3 + x^2 + 2x$ in $\mathbb{Z}_5$
15. $f(x)g(x)$ where $f(x) = x^3 + 2x^2 + 5$ and $g(x) = 3x^2 + 2x$ in $\mathbb{Z}_7$
16. Let $\phi_a : \mathbb{Z}_5[x] \to \mathbb{Z}_5$ be an evaluation homomorphism as in Theorem 22.4. Use Fermat's theorem to evaluate $\phi_3(x^{231} + 3x^{117} - 2x^{53} + 1)$.
17. Use Fermat's theorem to find all zeros in $\mathbb{Z}_5$ of $2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}$.

Concepts

In Exercises 18 and 19, 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.

By a similar argument, say $q_2(x) = u_2 p_2(x)$, so

$$p_3(x) \cdots p_r(x) = u_1 u_2 q_3(x) \cdots q_s(x).$$

Continuing in this manner, we eventually arrive at

$$1 = u_1 u_2 \cdots u_r q_{r+1}(x) \cdots q_s(x).$$

This is only possible if $s = r$, so that this equation is actually $1 = u_1 u_2 \cdots u_r$. Thus the irreducible factors $p_i(x)$ and $q_j(x)$ were the same except possibly for order and unit factors. ◆

23.21 Example Example 23.4 shows a factorization of $x^4 + 3x^3 + 2x + 4$ in $\mathbb{Z}_5[x]$ is $(x-1)^3(x+1)$. These irreducible factors in $\mathbb{Z}_5[x]$ are only unique up to units in $\mathbb{Z}_5[x]$, that is, nonzero constants in $\mathbb{Z}_5$. For example, $(x-1)^3(x+1) = (x-1)^2(2x-2)(3x+3)$. ▲

EXERCISES 23

Computations

In Exercises 1 through 4, find $q(x)$ and $r(x)$ as described by the division algorithm so that $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or of degree less than the degree of $g(x)$.

1. $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ and $g(x) = x^2 + 2x - 3$ in $\mathbb{Z}_7[x]$.
2. $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ and $g(x) = 3x^2 + 2x - 3$ in $\mathbb{Z}_7[x]$.
3. $f(x) = x^5 - 2x^4 + 3x - 5$ and $g(x) = 2x + 1$ in $\mathbb{Z}_{11}[x]$.
4. $f(x) = x^4 + 5x^3 - 3x^2$ and $g(x) = 5x^2 - x + 2$ in $\mathbb{Z}_{11}[x]$.

In Exercises 5 through 8, find all generators of the cyclic multiplicative group of units of the given finite field. (Review Corollary 6.16.)

5. $\mathbb{Z}_5$ 6. $\mathbb{Z}_7$ 7. $\mathbb{Z}_{17}$ 8. $\mathbb{Z}_{23}$

9. The polynomial $x^4 + 4$ can be factored into linear factors in $\mathbb{Z}_5[x]$. Find this factorization.
10. The polynomial $x^3 + 2x^2 + 2x + 1$ can be factored into linear factors in $\mathbb{Z}_7[x]$. Find this factorization.
11. The polynomial $2x^3 + 3x^2 - 7x - 5$ can be factored into linear factors in $\mathbb{Z}_{11}[x]$. Find this factorization.
12. Is $x^3 + 2x + 3$ an irreducible polynomial of $\mathbb{Z}_5[x]$? Why? Express it as a product of irreducible polynomials of $\mathbb{Z}_5[x]$.
13. Is $2x^3 + x^2 + 2x + 2$ an irreducible polynomial in $\mathbb{Z}_5[x]$? Why? Express it as a product of irreducible polynomials in $\mathbb{Z}_5[x]$.
14. Show that $f(x) = x^2 + 8x - 2$ is irreducible over $\mathbb{Q}$. Is $f(x)$ irreducible over $\mathbb{R}$? Over $\mathbb{C}$?
15. Repeat Exercise 14 with $g(x) = x^2 + 6x + 12$ in place of $f(x)$.
16. Demonstrate that $x^3 + 3x^2 - 8$ is irreducible over $\mathbb{Q}$.
17. Demonstrate that $x^4 - 22x^2 + 1$ is irreducible over $\mathbb{Q}$.

In Exercises 18 through 21, determine whether the polynomial in $\mathbb{Z}[x]$ satisfies an Eisenstein criterion for irreducibility over $\mathbb{Q}$.