one unit of distance, they maintained that all numbers are integers. This idea of commensurability can be rephrased according to our ideas as an assertion that all numbers are rational, for if a and b are rational numbers, then each is an integral multiple of the reciprocal of the least common multiple of their denominators. For example, if $a = \frac{7}{12}$ and $b = \frac{19}{15}$, then $a = (35)(\frac{1}{60})$ and $b = (76)(\frac{1}{60})$.

The Pythagoreans knew, of course, what is now called the *Pythagorean theorem;* that is, for a right triangle with legs of lengths a and b and a hypotenuse of length c,

$$a^2 + b^2 = c^2.$$

They also had to grant the existence of a hypotenuse of a right triangle having two legs of equal length, say one unit each. The hypotenuse of such a right triangle would, as we know, have to have a length of $\sqrt{2}$. Imagine then their consternation and dismay when one of their society—according to some stories it was Pythagoras himself—came up with the embarrassing fact that is stated in our terminology in the following theorem.

27.11 Theorem The polynomial $x^2 - 2$ has no zeros in the rational numbers. Thus $\sqrt{2}$ is not a rational number.

Proof Suppose that m/n for $m, n \in \mathbb{Z}$ is a rational number such that $(m/n)^2 = 2$. We assume that we have canceled any factors common to m and n, so that the fraction m/n is in lowest terms with $\gcd(m, n) = 1$. Then

$$m^2 = 2n^2,$$

where both m^2 and $2n^2$ are integers. Since m^2 and $2n^2$ are the same integer, and since 2 is a factor of $2n^2$, we see that 2 must be one of the factors of m^2. But as a square, m^2 has as factors the factors of m repeated twice. Thus m^2 must have two factors 2. Then $2n^2$ must have two factors 2, so n^2 must have 2 as a factor, and consequently n has 2 as a factor. We have deduced from $m^2 = 2n^2$ that both m and n must be divisible by 2, contradicting the fact that the fraction m/n is in lowest terms. Thus we have $2 \neq (m/n)^2$ for any $m, n \in \mathbb{Z}$. ◆

■ HISTORICAL NOTE

The solution of polynomial equations has been a goal of mathematics for nearly 4000 years. The Babylonians developed versions of the quadratic formula to solve quadratic equations. For example, to solve $x^2 - x = 870$, the Babylonian scribe instructed his students to take half of 1 ($\frac{1}{2}$), square it ($\frac{1}{4}$), and add that to 870. The square root of $870\frac{1}{4}$, namely $29\frac{1}{2}$, is then added to $\frac{1}{2}$ to give 30 as the answer. What the scribes did not discuss, however, was what to do if the square root in this process was not a rational number. Chinese mathematicians, however, from about 200 B.C., discovered a method similar to what is now called *Horner's method* to solve quadratic equations numerically; since they used a decimal system, they were able in principle to carry out the computation to as many places as necessary and could therefore ignore the distinction between rational and irrational solutions. The Chinese, in fact, extended their numerical techniques to polynomial equations of higher degree. In the Arab world, the Persian poet–mathematician Omar Khayyam (1048–1131) developed methods for solving cubic equations geometrically by finding the point(s) of intersection of appropriately chosen conic sections, while Sharaf al-Din al-Tusi (died 1213) used, in effect, techniques of calculus to determine whether or not a cubic equation had a real positive root. It was the Italian Girolamo Cardano (1501–1576) who first published a procedure for solving cubic equations algebraically.

Thus the Pythagoreans ran right into the question of a solution of a polynomial equation, $x^2 - 2 = 0$. We refer the student to Shanks [36, Chapter 3], for a lively and totally delightful account of this Pythagorean dilemma and its significance in mathematics.

In our motivation of the definition of a group, we commented on the necessity of having negative numbers, so that equations such as $x + 2 = 0$ might have solutions. The introduction of negative numbers caused a certain amount of consternation in some philosophical circles. We can visualize 1 apple, 2 apples, and even $\frac{13}{11}$ apples, but how can we point to anything and say that it is -17 apples? Finally, consideration of the equation $x^2 + 1 = 0$ led to the introduction of the number i. The very name of an "imaginary number" given to i shows how this number was regarded. Even today, many students are led by this name to regard i with some degree of suspicion. The negative numbers were introduced to us at such an early stage in our mathematical development that we accepted them without question.

We first met polynomials in high school freshman algebra. The first problem there was to learn how to add, multiply, and factor polynomials. Then, in both freshman algebra and in the second course in algebra in high school, considerable emphasis was placed on solving polynomial equations. These topics are exactly those with which we shall be concerned. The difference is that while in high school, only polynomials with real number coefficients were considered, *we shall be doing our work for polynomials with coefficients from any field*.

Once we have developed the machinery of homomorphisms and factor rings in Section 30, we will proceed with our **basic goal**: to show that given any polynomial of degree ≥ 1, where the coefficients of the polynomial may be from any field, we can find a zero of this polynomial in some field containing the given field. After the machinery is developed in Sections 30 and 31, the achievement of this goal will be very easy, and is really a very elegant piece of mathematics.

All this fuss may seem ridiculous, but just think back in history. This is the *culmination of more than 2000 years of mathematical endeavor in working with polynomial equations*. After achieving our *basic goal,* we shall spend the rest of our time studying the 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 27

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 27.4. 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 27.4. 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 27.4. 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.

18. A *polynomial with coefficients in a ring R is an infinite formal sum*

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

where $a_i \in R$ for $i = 0, 1, 2, \cdots$.

19. Let F be a field and let $f(x) \in F[x]$. A *zero of* $f(x)$ is an $\alpha \in F$ such that $\phi_\alpha(f(x)) = 0$, where $\phi_\alpha : F(x) \to F$ is the evaluation homomorphism mapping x into α.

20. Consider the element

$$f(x, y) = (3x^3 + 2x)y^3 + (x^2 - 6x + 1)y^2 + (x^4 - 2x)y + (x^4 - 3x^2 + 2)$$

of $(\mathbb{Q}[x])[y]$. Write $f(x, y)$ as it would appear if viewed as an element of $(\mathbb{Q}[y])[x]$.

21. Consider the evaluation homomorphism $\phi_5 : \mathbb{Q}[x] \to \mathbb{R}$. Find six elements in the kernel of the homomorphism ϕ_5.

22. Find a polynomial of degree >0 in $\mathbb{Z}_4[x]$ that is a unit.

23. Determine whether each of the following is true or false.

a. The polynomial $(a_n x^n + \cdots + a_1 x + a_0) \in R[x]$ is 0 if and only if $a_i = 0$, for $i = 0, 1, \cdots, n$.

b. If R is a commutative ring, then $R[x]$ is commutative.

c. If D is an integral domain, then $D[x]$ is an integral domain.

d. If R is a ring containing divisors of 0, then $R[x]$ has divisors of 0.

e. If R is a ring and $f(x)$ and $g(x)$ in $R[x]$ are of degrees 3 and 4, respectively, then $f(x)g(x)$ may be of degree 8 in $R[x]$.

f. If R is any ring and $f(x)$ and $g(x)$ in $R[x]$ are of degrees 3 and 4, respectively, then $f(x)g(x)$ is always of degree 7.

g. If F is a subfield of E and $\alpha \in E$ is a zero of $f(x) \in F[x]$, then α is a zero of $h(x) = f(x)g(x)$ for all $g(x) \in F[x]$.

h. If F is a field, then the units in $F[x]$ are precisely the units in F.

i. If R is a ring with unity, then x is never a divisor of 0 in $R[x]$.

j. If R is a ring, then the zero divisors in $R[x]$ are precisely the zero divisors in R.

Theory

24. Prove that if D is an integral domain, then $D[x]$ is an integral domain.

25. Let D be an integral domain and x an indeterminate.

a. Describe the units in $D[x]$.
b. Find the units in $\mathbb{Z}[x]$.
c. Find the units in $\mathbb{Z}_7[x]$.

26. Prove the left distributive law for $R[x]$, where R is a ring and x is an indeterminate.

27. Let F be a field of characteristic zero and let D be the formal polynomial differentiation map, so that

$$D\big(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\big) = a_1 + 2 \cdot a_2x + \cdots + n \cdot a_nx^{n-1}.$$

a. Show that $D : F[x] \to F[x]$ is a group homomorphism of $\langle F[x], +\rangle$ into itself. Is D a ring homomorphism?
b. Find the kernel of D.
c. Find the image of $F[x]$ under D.

28. Let F be a subfield of a field E.

a. Define an *evaluation homomorphism*

$$\phi_{\alpha_1,\cdots,\alpha_n} : F[x_1, \cdots, x_n] \to E \qquad \text{for} \quad \alpha_i \in E,$$

stating the analog of Theorem 27.4.
b. With $E = F = \mathbb{Q}$, compute $\phi_{-3,2}({x_1}^2{x_2}^3 + 3{x_1}^4x_2)$.
c. Define the concept of a *zero of a polynomial* $f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ in a way analogous to the definition in the text of a zero of $f(x)$.

29. Let R be a ring, and let R^R be the set of all functions mapping R into R. For $\phi, \psi \in R^R$, define the sum $\phi + \psi$ by

$$(\phi + \psi)(r) = \phi(r) + \psi(r)$$

and the product $\phi \cdot \psi$ by

$$(\phi \cdot \psi)(r) = \phi(r)\psi(r)$$

for $r \in R$. Note that $\cdot$ is *not* function composition. Show that $\langle R^R, +, \cdot\rangle$ is a ring.

30. Referring to Exercise 29, let F be a field. An element ϕ of F^F is a **polynomial function on** F, if there exists $f(x) \in F[x]$ such that $\phi(a) = f(a)$ for all $a \in F$.

a. Show that the set P_F of all polynomial functions on F forms a subring of F^F.
b. Show that the ring P_F is not necessarily isomorphic to $F[x]$. [*Hint:* Show that if F is a finite field, P_F and $F[x]$ don't even have the same number of elements.]

31. Refer to Exercises 29 and 30 for the following questions.

a. How many elements are there in ${\mathbb{Z}_2}^{\mathbb{Z}_2}$? in ${\mathbb{Z}_3}^{\mathbb{Z}_3}$?
b. Classify $\langle {\mathbb{Z}_2}^{\mathbb{Z}_2}, +\rangle$ and $\langle {\mathbb{Z}_3}^{\mathbb{Z}_3}, +\rangle$ by Theorem 9.12, the Fundamental Theorem of finitely generated abelian groups.
c. Show that if F is a finite field, then $F^F = P_F$. [*Hint:* Of course, $P_F \subseteq F^F$. Let F have as elements $a_1, \cdots, a_n$. Note that if

$$f_i(x) = c(x - a_1) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n),$$

then $f_i(a_j) = 0$ for $j \neq i$, and the value $f_i(a_i)$ can be controlled by the choice of $c \in F$. Use this to show that every function on F is a polynomial function.]

32. Let $\phi : R_1 \to R_2$ be a ring homomorphism. Show that there is a unique ring homomorphism $\psi : R_1[x] \to R_2[x]$ such that $\psi(a) = \phi(a)$ for any $a \in R_1$ and $\psi(x) = x$.