If $g(x)$ and $h(x)$ are both irreducible, we stop here. If not, at least one of them factors into polynomials of lower degree. Continuing this process, we arrive at a factorization

$$f(x) = p_1(x)p_2(x) \cdots p_r(x),$$

where $p_i(x)$ is irreducible for $i = 1, 2, \cdots, r$.

It remains for us to show uniqueness. Suppose that

$$f(x) = p_1(x)p_2(x) \cdots p_r(x) = q_1(x)q_2(x) \cdots q_s(x)$$

are two factorizations of $f(x)$ into irreducible polynomials. Then by Corollary 28.20, $p_1(x)$ divides some $q_j(x)$, let us assume $q_1(x)$. Since $q_1(x)$ is irreducible,

$$q_1(x) = u_1 p_1(x),$$

where $u_1 \neq 0$, but u_1 is in F and thus is a unit. Then substituting $u_1 p_1(x)$ for $q_1(x)$ and canceling, we get

$$p_2(x) \cdots p_r(x) = u_1 q_2(x) \cdots q_s(x).$$

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. ◆

28.22 Example Example 28.5 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 28

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 6.17.)

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 $\mathbb{Q}$.

18. $x^2 - 12$

19. $8x^3 + 6x^2 - 9x + 24$

20. $4x^{10} - 9x^3 + 24x - 18$

21. $2x^{10} - 25x^3 + 10x^2 - 30$

22. Find all zeros of $6x^4 + 17x^3 + 7x^2 + x - 10$ in $\mathbb{Q}$. (This is a tedious high school algebra problem. *You* might use a bit of analytic geometry and calculus and make a graph, or use Newton's method to see which are the best candidates for zeros.)

Concepts

In Exercises 23 and 24, 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.

23. A polynomial $f(x) \in F[x]$ is *irreducible over the field F* if and only if $f(x) \neq g(x)h(x)$ for any polynomials $g(x), h(x) \in F[x]$.

24. A nonconstant polynomial $f(x) \in F[x]$ is *irreducible over the field F* if and only if in any factorization of it in $F[x]$, one of the factors is in F.

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

a. $x - 2$ is irreducible over $\mathbb{Q}$.

b. $3x - 6$ is irreducible over $\mathbb{Q}$.

c. $x^2 - 3$ is irreducible over $\mathbb{Q}$.

d. $x^2 + 3$ is irreducible over $\mathbb{Z}_7$.

e. If F is a field, the units of $F[x]$ are precisely the nonzero elements of F.

f. If F is a field, the units of $F(x)$ are precisely the nonzero elements of F.

g. A polynomial $f(x)$ of degree n with coefficients in a field F can have at most n zeros in F.

h. A polynomial $f(x)$ of degree n with coefficients in a field F can have at most n zeros in any given field E such that $F \leq E$.

i. Every polynomial of degree 1 in $F[x]$ has at least one zero in the field F.

j. Each polynomial in $F[x]$ can have at most a finite number of zeros in the field F.

26. Find all prime numbers p such that $x + 2$ is a factor of $x^4 + x^3 + x^2 - x + 1$ in $\mathbb{Z}_p[x]$.

In Exercises 27 through 30, find all irreducible polynomials of the indicated degree in the given ring.

27. Degree 2 in $\mathbb{Z}_2[x]$

28. Degree 3 in $\mathbb{Z}_2[x]$

29. Degree 2 in $\mathbb{Z}_3[x]$

30. Degree 3 in $\mathbb{Z}_3[x]$

31. Find the number of irreducible quadratic polynomials in $\mathbb{Z}_p[x]$, where p is a prime. [*Hint:* Find the number of reducible polynomials of the form $x^2 + ax + b$, then the number of reducible quadratics, and subtract this from the total number of quadratics.]

Proof Synopsis

32. Give a synopsis of the proof of Corollary 28.6.

33. Give a synopsis of the proof of Corollary 28.7.

Theory

34. Show that for p a prime, the polynomial $x^p + a$ in $\mathbb{Z}_p[x]$ is not irreducible for any $a \in \mathbb{Z}_p$.

35. If F is a field and $a \neq 0$ is a zero of $f(x) = a_0 + a_1x + \cdots + a_nx^n$ in $F[x]$, show that $1/a$ is a zero of $a_n + a_{n-1}x + \cdots + a_0x^n$.

36. (Remainder Theorem) Let $f(x) \in F[x]$ where F is a field, and let $\alpha \in F$. Show that the remainder $r(x)$ when $f(x)$ is divided by $x - \alpha$, in accordance with the division algorithm, is $f(\alpha)$.

37. Let $\sigma_m : \mathbb{Z} \to \mathbb{Z}_m$ be the natural homomorphism given by $\sigma_m(a) =$ (the remainder of a when divided by m) for $a \in \mathbb{Z}$.

a. Show that $\overline{\sigma_m} : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ given by

$$\overline{\sigma_m}\big(a_0 + a_1x + \cdots + a_nx^n\big) = \sigma_m(a_0) + \sigma_m(a_1)x + \cdots + \sigma_m(a_n)x^n$$

is a homomorphism of $\mathbb{Z}[x]$ onto $\mathbb{Z}_m[x]$.

b. Show that if $f(x) \in \mathbb{Z}[x]$ and $\overline{\sigma_m}(f(x))$ both have degree n and $\overline{\sigma_m}(f(x))$ does not factor in $\mathbb{Z}_m[x]$ into two polynomials of degree less than n, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

c. Use part (b) to show that $x^3 + 17x + 36$ is irreducible in $\mathbb{Q}[x]$. [*Hint:* Try a prime value of m that simplifies the coefficients.]

The goal of Exercises 38 through 40 is to prove Theorem 28.12.

38. Let $f(x) \in \mathbb{Z}[x]$. We say that $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ is **primitive** if the greatest common divisor of the coefficients $a_0, a_1, \ldots, a_n$ is 1. Prove the product of two primitive polynomials is primitive.

39. Let $f(x) \in \mathbb{Z}[x]$. The **content** of $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ is defined to be the greatest common divisor of $a_0, a_1, \ldots, a_n$ and it is denoted cont($f(x)$). Prove that $\text{cont}(f(x)g(x)) = \text{cont}(f(x)) \cdot \text{cont}(g(x))$ for any $f(x), g(x) \in \mathbb{Z}[x]$. (Hint: Use Exercise 38.)

40. Prove Theorem 28.12. (Hint: Use Exercise 39.)

SECTION 29 †ALGEBRAIC CODING THEORY

Suppose you wish to send a message, but occasionally the transmission line makes an error. When an error occurs, it would be nice if the receiver could detect that there is an error and ask you to resend the message. In other situations, such as a space probe transmitting images back to earth, it may be impossible to resend the data. In this case, it would be desirable if the receiving earthling could not only detect, but also correct a transmission error.

We will think of a message as an element in $\mathbb{Z}_2^k = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$. Each message consists of a string of zeros and ones of length k. Each of the $\mathbb{Z}_2$ entries will be referred to as a **bit**. Coding theory in general allows transmitted messages to be in F^n for any finite field F, but for our introduction to the subject we will restrict our attention to $F = \mathbb{Z}_2$.

29.1 Example A common way to detect a single-bit error is to use a parity check bit. Instead of transmitting a byte consisting of eight bits, that is, an element in $\mathbb{Z}_2^8$, nine bits are transmitted with the last bit being the sum in $\mathbb{Z}_2$ of the first eight bits. The message

$$(1, 1, 0, 1, 0, 0, 1, 1)$$

would be transmitted as

$$(1, 1, 0, 1, 0, 0, 1, 1, 1).$$

Regardless of whether the 8-bit message has an even or odd number of ones, the transmitted string of 9 bits has an even number of ones. If the sum of the nine bits of the received message is not zero, then a transmission error must have occurred. ▲

[†] This section is not used in the remainder of the text.

29.2 Example An inefficient, but possible method of correcting transmission errors is to send a message three times. If two of the received messages agree, then that common message is accepted as the most likely correct message. In this case, if there is only one error, the original message will be retrieved. ▲

29.3 Definition A **code** is a subset $C \subseteq \mathbb{Z}_2^n$. An element of C is a **code word**. The **length** of a code word in $C \subseteq \mathbb{Z}_2^n$ is n. ■

In practice, when a message is to be sent, it is broken into shorter pieces consisting of k bits. A predetermined one-to-one function $f : \mathbb{Z}_2^k \to C$ mapping all possible k bit messages to code words is then applied to the message pieces and transmitted. The receiver then checks that each received message piece is in the range of f. If so, the sent code word is most likely the received code word and the message corresponding to the received code word can be computed since f is one-to-one. If the received message is not a code word, then a transmission error occurred. We will not concern ourselves with the function f. Instead, we will investigate certain types of codes. We restrict our attention to linear codes as defined below.

29.4 Definition A **linear code** is a subgroup C of $\mathbb{Z}_2^n$. Since C is a subgroup of $\mathbb{Z}_2^n$, the order of C is 2^k for some integer k. The **information rate** or **rate** of the linear code is the ratio $\frac{k}{n}$. A linear code is **cyclic** if for any code word $(a_0, a_1, \ldots, a_{n-1})$, $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is also a code word. That is, a linear code is cyclic if a cyclic shift of any code word is a code word. ■

An information rate of $\frac{k}{n}$ means that in order to transmit a message of length k, n bits are required. It is clearly desirable to make the information rate as large as possible subject to the desired number of bit errors that can be detected or corrected.

29.5 Example Let $C \subseteq \mathbb{Z}_2^9$ be the set of all strings of length 9 such that the sum of the bits is 0 modulo 2 as in Example 29.1. Note that C is the kernel of the group homomorphism

$$\phi : \mathbb{Z}_2^9 \to \mathbb{Z}_2$$

given by

$$\phi(a_0, a_1, \ldots, a_8) = a_0 + a_1 + \cdots + a_8 \pmod 2.$$

Thus C is a subgroup of $\mathbb{Z}_2^9$ and therefore C is a linear code. In this example, $n = 9$ and $k = 8$ since C is a subgroup of $\mathbb{Z}_2^9$ with index 2. Thus C has an information rate of $\frac{8}{9}$. Furthermore, the code is cyclic since any cyclic shift of a code word does not change the number of ones. ▲

If two code words differ in only one position, then it would not be possible to detect every error that occurs in just one bit. If any pair of code words differ in two or more positions, then any error of just one bit could be detected, that is, it could be determined that there is an error, but it may not be possible to reconstruct the original code word. Furthermore, if any pair of code words differ at three or more positions, then an error of just one bit could not only be detected, but it could be corrected since only one code word would differ from the erroneous word at one position.

29.6 Definition The **Hamming weight** or **weight** of a string in $\mathbb{Z}_2^n$ is the number of ones in the string. The **Hamming distance** or **distance** between two strings in $\mathbb{Z}_2^n$ is the number of bits where the two strings differ. ■

29.7 Example The Hamming weight of the string $(1, 0, 0, 1, 1, 0, 1, 1)$ is 5. The Hamming distance between the code words $(1, 0, 0, 0, 1, 1, 0, 1)$ and $(1, 1, 0, 1, 0, 0, 0, 1)$ is 4. ▲