rate. The next theorem gives us insight into the nature of the field $F(\alpha)$ in the case where α is algebraic over F.

39.19 Theorem Let $E = F(\alpha)$ be a simple extension of a field F with α algebraic over F. Let $n = \deg(\alpha, F)$. Then every $\beta \in F(\alpha)$ can be uniquely expressed in the form

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1},$$

where the b_i are in F.

Proof Let $\beta \in F(\alpha)$. Then $\beta = f(\alpha)$ for some polynomial $f(x) \in F[x]$ by the definition of $F[\alpha]$. The division algorithm says that there are unique polynomials $q(x), r(x) \in F[x]$ such that either $r(x) = 0$ or the degree of $r(x)$ is less than n, and

$$f(x) = \mathrm{irr}(\alpha, F)q(x) + r(x).$$

Applying the evaluation homomorphism ϕ_α, we see that $f(\alpha) = r(\alpha)$. Thus

$$\beta = f(\alpha) = r(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}$$

for some elements b_i in F.

To show uniqueness, we assume that $s(x) \in F[x]$ is any polynomial with $r(\alpha) = s(\alpha)$, and $s(x)$ is either zero or else its degree is less than n. Let $d(x) = r(x) - s(x)$. Then $d(\alpha) = 0$, and either $d(x) = 0$ or $\deg(d(x)) < n$. Since the degree of the minimal polynomial for α over F is n, $d(x)$ is the zero polynomial and $r(x) = s(x)$. Thus the representation of β as

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1},$$

where the b_i are in F, is unique. ◆

We give an impressive example illustrating Theorem 39.19.

39.20 Example The polynomial $p(x) = x^2 + x + 1$ in $\mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2$ by Theorem 28.11, since neither element 0 nor element 1 of $\mathbb{Z}_2$ is a zero of $p(x)$. By Theorem 39.3, we know that there is an extension field E of $\mathbb{Z}_2$ containing a zero α of $x^2 + x + 1$. By Theorem 39.19, $\mathbb{Z}_2(\alpha)$ has as elements $0 + 0\alpha, 1 + 0\alpha, 0 + 1\alpha$, and $1 + 1\alpha$, that is, 0, 1, α, and $1 + \alpha$. *This gives us a new finite field, of four elements!* The addition and multiplication tables for this field are shown in Tables 39.21 and 39.22. For example, to compute $(1 + \alpha)(1 + \alpha)$ in $\mathbb{Z}_2(\alpha)$, we observe that since $p(\alpha) = \alpha^2 + \alpha + 1 = 0$, then

$$\alpha^2 = -\alpha - 1 = \alpha + 1.$$

Therefore,

$$(1 + \alpha)(1 + \alpha) = 1 + \alpha + \alpha + \alpha^2 = 1 + \alpha^2 = 1 + \alpha + 1 = \alpha.$$ ▲

We can use Theorem 39.19 to fulfill our promise of Example 39.4 and show that $\mathbb{R}[x]/\langle x^2 + 1\rangle$ is isomorphic to the field $\mathbb{C}$ of complex numbers. We saw in Example 39.4 that we can view $\mathbb{R}[x]/\langle x^2 + 1\rangle$ as an extension field of $\mathbb{R}$. Let

39.21 Table

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

39.22 Table

	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

$$\alpha = x + \langle x^2 + 1 \rangle.$$

Then $\mathbb{R}(\alpha) = \mathbb{R}[x]/\langle x^2+1\rangle$ and consists of all elements of the form $a+b\alpha$ for $a, b \in \mathbb{R}$, by Theorem 39.19. But since $\alpha^2 + 1 = 0$, we see that α plays the role of $i \in \mathbb{C}$, and $a + b\alpha$ plays the role of $(a+bi) \in \mathbb{C}$. Thus $\mathbb{R}(\alpha) \simeq \mathbb{C}$. *This is the elegant algebraic way to construct $\mathbb{C}$ from $\mathbb{R}$.*

39.23 Corollary Let E be an extension field of F and let $\alpha \in E$ be algebraic over F. If $\deg(\alpha, F) = n$, then $F(\alpha)$ is a vector space over F with dimension n and basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Furthermore, every element β of $F(\alpha)$ is algebraic over F and $\deg(\beta, F) \leq \deg(\alpha, F)$.

Proof Since F is a subfield of $F(\alpha)$, $F(\alpha)$ is a vector space over F. Theorem 39.19 shows that the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ spans $F(\alpha)$. If

$$0 = b_0(1) + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1},$$

by uniqueness of the coefficients in Theorem 39.19, each b_i is 0. We have that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is linearly independent over F, and therefore a basis of $F(\alpha)$ over F. Thus the dimension of $F(\alpha)$ over F is $n = \deg(\alpha, F)$.

For any $\beta \in F(\alpha)$, $F \leq F(\beta) \leq F(\alpha)$, so any set of more than n vectors in $F(\beta)$ is not linearly independent over F. The set $\{1, \beta, \beta^2, \ldots, \beta^n\}$ either has fewer than $n+1$ elements or else it is not linearly independent over F. In the first case, $\beta^r = \beta^s$ for some $r \neq s$ and in the second case, there are elements $b_i \in F$, not all zero, such that

$$b_0(1) + b_1\beta + b_2\beta^2 + \cdots + b_n\beta^n = 0.$$

In either case, we see that β is algebraic over F. Furthermore the dimension of $F(\beta)$ over F, k, is at most n and we have

$$\deg(\beta, F) = k \leq n = \deg(\alpha, F). \qquad \blacklozenge$$

39.24 Example The number $i \in \mathbb{C}$ has minimal polynomial $x^2 + 1$ over $\mathbb{R}$ and $\mathbb{C} = \mathbb{R}(i)$. By Corollary 39.23, for every complex number β, $\deg(\beta, \mathbb{R}) \leq 2$. This implies that every complex number that is not a real number is a zero of some irreducible polynomial of degree two in $\mathbb{R}[x]$. Of course, this fact can also be verified using the techniques of Example 39.10. ▲

EXERCISES 39

Computations

In Exercises 1 through 5, show that the given number $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ by finding $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$.

1. $1 + \sqrt{2}$ **2.** $\sqrt{2} + \sqrt{3}$ **3.** $1 + i$

4. $\sqrt{1 + \sqrt[3]{2}}$ **5.** $\sqrt{\sqrt[3]{2} - i}$

In Exercises 6 through 8, find $\text{irr}(\alpha, \mathbb{Q})$ and $\deg(\alpha, \mathbb{Q})$ for the given algebraic number $\alpha \in \mathbb{C}$. Be prepared to prove that your polynomials are irreducible over $\mathbb{Q}$ if challenged to do so.

6. $\sqrt{3 - \sqrt{6}}$ **7.** $\sqrt{(\frac{1}{3}) + \sqrt{7}}$ **8.** $\sqrt{2} + i$

In Exercises 9 through 16, classify the given $\alpha \in \mathbb{C}$ as algebraic or transcendental over the given field F. If α is algebraic over F, find $\deg(\alpha, F)$.

9. $\alpha = i, F = \mathbb{Q}$

10. $\alpha = 1 + i, F = \mathbb{R}$

11. $\alpha = \sqrt{\pi}, F = \mathbb{Q}$

12. $\alpha = \sqrt{\pi}, F = \mathbb{R}$

13. $\alpha = \sqrt{\pi}, F = \mathbb{Q}(\pi)$

14. $\alpha = \pi^2, F = \mathbb{Q}$

15. $\alpha = \pi^2, F = \mathbb{Q}(\pi)$

16. $\alpha = \pi^2, F = \mathbb{Q}(\pi^3)$

17. Refer to Example 39.20 of the text. The polynomial $x^2 + x + 1$ has a zero α in $\mathbb{Z}_2(\alpha)$ and thus must factor into a product of linear factors in $(\mathbb{Z}_2(\alpha))[x]$. Find this factorization. [*Hint:* Divide $x^2 + x + 1$ by $x - \alpha$ by long division, using the fact that $\alpha^2 = \alpha + 1$.]

18. **a.** Show that the polynomial $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$.

b. Let α be a zero of $x^2 + 1$ in an extension field of $\mathbb{Z}_3$. As in Example 39.20, give the multiplication and addition tables for the nine elements of $\mathbb{Z}_3(\alpha)$, written in the order 0, 1, 2, $\alpha, 2\alpha, 1 + \alpha, 1 + 2\alpha, 2 + \alpha$, and $2 + 2\alpha$.

Concepts

In Exercises 19 through 22, 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.

19. An element α of an extension field E of a field F is *algebraic over* F if and only if α is a zero of some polynomial.

20. An element β of an extension field E of a field F is *transcendental over* F if and only if β is not a zero of any polynomial in $F[x]$.

21. A *monic polynomial in* $F[x]$ is one having all coefficients equal to 1.

22. A field E is a *simple extension* of a subfield F if and only if there exists some $\alpha \in E$ such that no proper subfield of E contains α.

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

a. The number π is transcendental over $\mathbb{Q}$.

b. $\mathbb{C}$ is a simple extension of $\mathbb{R}$.

c. Every element of a field F is algebraic over F.

d. $\mathbb{R}$ is an extension field of $\mathbb{Q}$.

e. $\mathbb{Q}$ is an extension field of $\mathbb{Z}_2$.

f. Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$ of degree n. If $f(\alpha) = 0$ for nonzero $f(x) \in \mathbb{Q}[x]$, then $\deg(f(x)) \geq n$.

g. Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$ of degree n. If $f(\alpha) = 0$ for nonzero $f(x) \in \mathbb{R}[x]$, then $\deg(f(x)) \geq n$.

h. Every nonconstant polynomial in $F[x]$ has a zero in some extension field of F.

i. Every nonconstant polynomial in $F[x]$ has a zero in every extension field of F.

j. If x is an indeterminate, $\mathbb{Q}[\pi] \simeq \mathbb{Q}[x]$.

24. We have stated without proof that π and e are transcendental over $\mathbb{Q}$.

a. Find a subfield F of $\mathbb{R}$ such that π is algebraic of degree 3 over F.

b. Find a subfield E of $\mathbb{R}$ such that e^2 is algebraic of degree 5 over E.

25. **a.** Show that $x^3 + x^2 + 1$ is irreducible over $\mathbb{Z}_2$.

b. Let α be a zero of $x^3 + x^2 + 1$ in an extension field of $\mathbb{Z}_2$. Show that $x^3 + x^2 + 1$ factors into three linear factors in $(\mathbb{Z}_2(\alpha))[x]$ by actually finding this factorization. [*Hint:* Every element of $\mathbb{Z}_2(\alpha)$ is of the form

$$a_0 + a_1\alpha + a_2\alpha^2 \quad \text{for} \quad a_i = 0, 1.$$

Divide $x^3 + x^2 + 1$ by $x - \alpha$ by long division. Show that the quotient also has a zero in $\mathbb{Z}_2(\alpha)$ by simply trying the eight possible elements. Then complete the factorization.]

26. Let E be an extension field of $\mathbb{Z}_2$ and let $\alpha \in E$ be algebraic of degree 3 over $\mathbb{Z}_2$. Classify the groups $\langle \mathbb{Z}_2(\alpha), + \rangle$ and $\langle (\mathbb{Z}_2(\alpha))^*, \cdot \rangle$ according to the Fundamental Theorem of finitely generated abelian groups. As usual, $(\mathbb{Z}_2(\alpha))^*$ is the set of nonzero elements of $\mathbb{Z}_2(\alpha)$.

27. Definition 39.15 defined the terms **irreducible polynomial for** α **over** F and **minimal polynomial for** α **over** F to mean the same polynomial. Why are both designations appropriate?

Proof Synopsis

28. Give a two- or three-sentence synopsis of Theorem 39.3.

Theory

29. Let E be an extension field of F, and let $\alpha, \beta \in E$. Suppose α is transcendental over F but algebraic over $F(\beta)$. Show that β is algebraic over $F(\alpha)$.

30. Let E be an extension field of a finite field F, where F has q elements. Let $\alpha \in E$ be algebraic over F of degree n. Prove that $F(\alpha)$ has q^n elements.

31. **a.** Show that there exists an irreducible polynomial of degree 3 in $\mathbb{Z}_3[x]$.

b. Show from part (a) that there exists a finite field of 27 elements. [*Hint:* Use Exercise 30.]

32. Consider the prime field $\mathbb{Z}_p$ of characteristic $p \neq 0$.

a. Show that, for $p \neq 2$, not every element in $\mathbb{Z}_p$ is a square of an element of $\mathbb{Z}_p$. [*Hint:* $1^2 = (p-1)^2 = 1$ in $\mathbb{Z}_p$. Deduce the desired conclusion *by counting*.]

b. Using part (a), show that there exist finite fields of p^2 elements for every prime p in $\mathbb{Z}^+$.

33. Let E be an extension field of a field F and let $\alpha \in E$ be transcendental over F. Show that every element of $F(\alpha)$ that is not in F is also transcendental over F.

34. Show that $\{a + b(\sqrt[3]{2}) + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$ by using the ideas of this section, rather than by a formal verification of the field axioms. [*Hint:* Use Theorem 39.19.]

35. Following the idea of Exercise 31, show that there exists a field of 8 elements; of 16 elements; of 25 elements.

36. Let F be a finite field of characteristic p. Show that every element of F is algebraic over the prime field $\mathbb{Z}_p \leq F$. [*Hint:* Let F^* be the set of nonzero elements of F. Apply group theory to the group $\langle F^*, \cdot \rangle$ to show that every $\alpha \in F^*$ is a zero of some polynomial in $\mathbb{Z}_p[x]$ of the form $x^n - 1$.]

37. Use Exercises 30 and 36 to show that every finite field is of prime-power order, that is, it has a prime-power number of elements.

38. Prove the uniqueness of the polynomial in Corollary 39.14.

SECTION 40 ALGEBRAIC EXTENSIONS

Finite Extensions

In Corollary 39.23 we saw that if E is an extension field of a field F and $\alpha \in E$ is algebraic over F, then every element of $F(\alpha)$ is algebraic over F. In studying zeros of polynomials in $F[x]$, we shall be interested almost exclusively in extensions of F containing only elements algebraic over F.

40.1 Definition An extension field E of a field F is an **algebraic extension of** F if every element in E is algebraic over F. ■

40.2 Definition If an extension field E of a field F is of finite dimension n as a vector space over F, then E is a **finite extension of degree** n **over** F. We shall let $[E : F]$ be the degree n of E over F. ■