39.11 Definition An element of $\mathbb{C}$ that is algebraic over $\mathbb{Q}$ is an **algebraic number.** A **transcendental number** is an element of $\mathbb{C}$ that is transcendental over $\mathbb{Q}$. ■

There is an extensive and elegant theory of algebraic numbers. (See the Bibliography.)

The next theorem gives a useful characterization of algebraic and transcendental elements over F in an extension field E of F. It also illustrates the importance of our evaluation homomorphisms ϕ_α. *Note that once more we are describing our concepts in terms of mappings.*

39.12 Theorem Let E be an extension field of a field F and let $\alpha \in E$. Let $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism of $F[x]$ into E such that $\phi_\alpha(a) = a$ for $a \in F$ and $\phi_\alpha(x) = \alpha$. Then α is transcendental over F if and only if ϕ_α gives an isomorphism of $F[x]$ with a subdomain of E, that is, if and only if ϕ_α is a one-to-one map.

Proof The element α is transcendental over F if and only if $f(\alpha) \neq 0$ for all nonzero $f(x) \in F[x]$, which is true (by definition) if and only if $\phi_\alpha(f(x)) \neq 0$ for all nonzero $f(x) \in F[x]$, which is true if and only if the kernel of ϕ_α is $\{0\}$, that is, if and only if ϕ_α is a one-to-one map. ◆

The Irreducible Polynomial for α over F

Consider the extension field $\mathbb{R}$ of $\mathbb{Q}$. We know that $\sqrt{2}$ is algebraic over $\mathbb{Q}$, being a zero of $x^2 - 2$. Of course, $\sqrt{2}$ is also a zero of $x^3 - 2x$ and of $x^4 - 3x^2 + 2 = (x^2 - 2)(x^2 - 1)$. Both these other polynomials having $\sqrt{2}$ as a zero were multiples of $x^2 - 2$. The next theorem shows that this is an illustration of a general situation. This theorem plays a central role in our later work.

39.13 Theorem Let E be a field extension of F, and let $\alpha \in E$ be algebraic over F. Then $\{f(x) \in F[x] \mid f(\alpha) = 0\} = \langle p(x) \rangle$ for some polynomial $p(x) \in F[x]$. Furthermore, $p(x)$ is irreducible over F.

Proof Let $I = \{f(x) \in F[x] \mid f(\alpha) = 0\}$. Then I is the kernel of the evaluation homomorphism $\phi_\alpha : F[x] \to E$, which implies that I is an ideal in $F[x]$. By Theorem 31.24, I is a principal ideal generated by a polynomial $p(x) \in F[x]$. Thus $I = \langle p(x) \rangle$.

It remains to show that $p(x)$ is irreducible over F. The degree of $p(x)$ is at least 1, which implies that $p(x)$ is neither 0 nor a unit in $F[x]$. Suppose that $p(x) = r(x)s(x)$ is a factorization of $p(x)$ over the field F. Then applying the evaluation homomorphism, either $r(\alpha) = 0$ or $s(\alpha) = 0$, since E is a field. We relabel r and s, if necessary, so that $r(\alpha) = 0$. Then $r(x) \in I = \langle p(x) \rangle$. Thus

$$p(x) = r(x)s(x) = p(x)r_1(x)s(x)$$

for some $r_1(x) \in F[x]$. Canceling $p(x)$ shows that $s(x)$ is a unit. Therefore, $p(x)$ is irreducible. ◆

By multiplying by a suitable constant in F, we can assume that the coefficient of the highest power of x appearing in $p(x)$ of Theorem 39.13 is 1. Such a polynomial having 1 as the coefficient of the highest power of x appearing is a **monic polynomial.**

39.14 Corollary Let E be an extension field of F, and let $\alpha \in E$ be algebraic over F. Then there is a unique irreducible polynomial $p(x) \in F[x]$ such that $p(x)$ is monic, $p(\alpha) = 0$, and for any polynomial $f(x) \in F[x]$ with $f(\alpha) = 0$, $p(x)$ divides $f(x)$.

Proof Let $p(x)$ be the polynomial of Theorem 39.13. By multiplying $p(x)$ with an appropriate element of F, we can assume that $p(x)$ is monic. Since $\{f(x) \mid f(\alpha) = 0\} = \langle p(x) \rangle$, $p(\alpha) = 0$ and for any $f(x) \in F[x]$ with $f(\alpha) = 0$, $p(x)$ divides $f(x)$.

You are asked to prove uniqueness in Exercise 38. ◆

39.15 Definition Let E be a field extension of a field F, and let $\alpha \in E$ be algebraic over F. The unique monic polynomial $p(x)$ in Corollary 39.14 is called the **irreducible polynomial for** α **over** F or the **minimal polynomial for** α **over** F, and it is denoted $\operatorname{irr}(\alpha, F)$. The degree of the polynomial $\operatorname{irr}(\alpha, F)$ is called the **degree of** α **over** F and this number is denoted by $\deg(\alpha, F)$. ■

39.16 Example We know that $\operatorname{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$. Referring to Example 39.10, we see that for $\alpha = \sqrt{1 + \sqrt{3}}$ in $\mathbb{R}, \alpha$ is a zero of $x^4 - 2x^2 - 2$, which is in $\mathbb{Q}[x]$. Since $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$ (by Eisenstein with $p = 2$, or by application of the technique of Example 28.15), we see that

$$\operatorname{irr}(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2.$$

Thus $\sqrt{1 + \sqrt{3}}$ is algebraic of degree 4 over $\mathbb{Q}$. ▲

Just as we must speak of an element α as *algebraic over F* rather than simply as *algebraic,* we must speak of the *degree of α over F* rather than the *degree of α*. To take a trivial illustration, $\sqrt{2} \in \mathbb{R}$ is algebraic of degree 2 over $\mathbb{Q}$ but algebraic of degree 1 over $\mathbb{R}$, for $\operatorname{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$.

The quick development of the theory here is due to the machinery of homomorphisms and ideal theory that we now have at our disposal. Note especially our constant use of the evaluation homomorphisms ϕ_α.

Simple Extensions

Let E be an extension field of a field F, and let $\alpha \in E$. Let ϕ_α be the evaluation homomorphism of $F[x]$ into E with $\phi_\alpha(a) = a$ for $a \in F$ and $\phi_\alpha(x) = \alpha$, as in Theorem 27.4. We use two cases to define the field $F(\alpha)$.

Case I *Suppose α is algebraic over F.* Then as in Corollary 39.14, the kernel of ϕ_α is $\langle \operatorname{irr}(\alpha, F) \rangle$ and by Theorem 31.25, $\langle \operatorname{irr}(\alpha, F) \rangle$ is a maximal ideal of $F[x]$. Therefore, $F[x]/\langle \operatorname{irr}(\alpha, F) \rangle$ is a field and is isomorphic to the image $\phi_\alpha[F[x]]$ in E. This subfield $\phi_\alpha[F[x]]$ of E is then the smallest subfield of E containing F and α. We shall denote this field by $F(\alpha)$.

Case II *Suppose α is transcendental over F.* Then by Theorem 39.12, ϕ_α gives an isomorphism of $F[x]$ with a subdomain of E. Thus in this case $\phi_\alpha[F[x]]$ is *not* a field but an integral domain that we shall denote by $F[\alpha]$. By Corollary 26.9, E contains a field of quotients of $F[\alpha]$, which is thus the smallest subfield of E containing F and α. As in Case I, we denote this field by $F(\alpha)$.

39.17 Example Since π is transcendental over $\mathbb{Q}$, the field $\mathbb{Q}(\pi)$ is isomorphic to the field $\mathbb{Q}(x)$ of rational functions over $\mathbb{Q}$ in the indeterminate x. Thus from a structural viewpoint, an element that is transcendental over a field F behaves as though it were an indeterminate over F. ▲

39.18 Definition An extension field E of a field F is a **simple extension of** F if $E = F(\alpha)$ for some $\alpha \in E$. ■

Many important results appear throughout this section. We have now developed so much machinery that results are starting to pour out of our efficient plant at an alarming