as follows. If a polynomial $f(x)$ in $F[x]$ has no zero in F, then adjoin a zero α of such an $f(x)$ to F, thus obtaining the field $F(\alpha)$. *Theorem 39.3, Kronecker's theorem, is strongly used here, of course*. If $F(\alpha)$ is still not algebraically closed, then continue the process further. The trouble is that, contrary to the situation for the algebraic closure $\mathbb{C}$ of $\mathbb{R}$, we may have to do this a (possibly large) infinite number of times. It can be shown (see Exercises 33 and 36) that $\overline{\mathbb{Q}}$ is isomorphic to the field of all algebraic numbers, and that we cannot obtain $\overline{\mathbb{Q}}$ from $\mathbb{Q}$ by adjoining a finite number of algebraic numbers. We shall have to first discuss some set-theoretic machinery, *Zorn's lemma*, in order to be able to handle such a situation. This machinery is a bit complex, so we are putting the proof under a separate heading. The existence theorem for $\overline{F}$ is very important, and we state it here so that we will know this fact, even if we do not study the proof.

40.17 Theorem Every field F has an **algebraic closure**, that is, an algebraic extension $\overline{F}$ that is algebraically closed.

The Fundamental Theorem of Algebra stating that $\mathbb{C}$ is an algebraically closed field is well known. Interestingly, the simplest and shortest proofs of the Fundamental Theorem of Algebra are not algebraic proofs. There are much shorter and easier-to-follow proofs using either analysis or topology. However, behind both the analytical and the topological proofs lies a significant amount of machinery, so perhaps comparing the proofs is not completely fair. At any rate, we include a short proof for students who have studied functions of a complex variable and are familiar with Liouville's Theorem.

40.18 Theorem **(Fundamental Theorem of Algebra)** The field $\mathbb{C}$ of complex numbers is an algebraically closed field.

Proof Let the polynomial $f(z) \in \mathbb{C}[z]$ have no zero in $\mathbb{C}$. Then $1/f(z)$ gives an entire function; that is, $1/f(z)$ is analytic everywhere. Also if $f(z) \notin \mathbb{C}$, $\lim_{|z|\to\infty} |f(z)| = \infty$, so $\lim_{|z|\to\infty} |1/f(z)| = 0$. Thus $1/f(z)$ must be bounded in the plane. Hence by Liouville's theorem of complex function theory, $1/f(z)$ is constant, and thus $f(z)$ is constant. Therefore, a nonconstant polynomial in $\mathbb{C}[z]$ must have a zero in $\mathbb{C}$, so $\mathbb{C}$ is algebraically closed. ◆

Proof of the Existence of an Algebraic Closure

We shall prove that every field has an algebraic extension that is algebraically closed. Mathematics students should have the opportunity to see some proof involving the *Axiom of Choice* by the time they finish college. This is a natural place for such a proof. We shall use an equivalent form, *Zorn's lemma*, of the Axiom of Choice. To state Zorn's lemma, we have to give a set-theoretic definition.

40.19 Definition A **partial ordering of a set** S is given by a relation $\leq$ defined for certain ordered pairs of elements of S such that the following conditions are satisfied:

1. $a \leq a$ for all $a \in S$ **(reflexive law).**
2. If $a \leq b$ and $b \leq a$, then $a = b$ **(antisymmetric law).**
3. If $a \leq b$ and $b \leq c$, then $a \leq c$ **(transitive law).** ■

In a *partially* ordered set, not every two elements need be **comparable;** that is, for $a, b \in S$, we need not have either $a \leq b$ or $b \leq a$. As usual, $a < b$ denotes $a \leq b$ but $a \neq b$.

A subset T of a partially ordered set S is a **chain** if every two elements a and b in T are comparable, that is, either $a \leq b$ or $b \leq a$ (or both). An element $u \in S$ is an

upper bound for a subset A of partially ordered set S if $a \leq u$ for all $a \in A$. Finally, an element m of a partially ordered set S is **maximal** if there is no $s \in S$ such that $m < s$.

40.20 Example The collection of all subsets of a set forms a partially ordered set under the relation $\leq$ given by $\subseteq$. For example, if the whole set is $\mathbb{R}$, we have $\mathbb{Z} \subseteq \mathbb{Q}$. Note, however, that for $\mathbb{Z}$ and $\mathbb{Q}^+$, neither $\mathbb{Z} \subseteq \mathbb{Q}^+$ nor $\mathbb{Q}^+ \subseteq \mathbb{Z}$. ▲

40.21 Zorn's Lemma If S is a partially ordered set such that every chain in S has an upper bound in S, then S has at least one maximal element.

We do not prove Zorn's lemma. Instead we point out that it can be shown that Zorn's lemma is equivalent to the Axiom of Choice. Thus we are really taking Zorn's lemma here as an *axiom* for our set theory. Refer to the literature for a statement of the Axiom of Choice and a proof of its equivalence to Zorn's lemma. (See Edgerton [47].)

Zorn's lemma is often useful when we want to show the existence of a largest or maximal structure of some kind. If a field F has an algebraic extension $\overline{F}$ that is algebraically closed, then $\overline{F}$ will certainly be a maximal algebraic extension of F, for since $\overline{F}$ is algebraically closed, it can have no proper algebraic extensions.

The idea of our proof of Theorem 40.17 is very simple. Given a field F, we shall first describe a class of algebraic extensions of F that is so large that it must contain (up to isomorphism) any conceivable algebraic extension of F. We then define a partial ordering, the ordinary subfield ordering, on this class, and show that the hypotheses of Zorn's lemma are satisfied. By Zorn's lemma, there will exist a maximal algebraic extension $\overline{F}$ of F in this class. We shall then argue that, as a maximal element, this extension $\overline{F}$ can have no proper algebraic extensions, so it must be algebraically closed.

Our proof differs a bit from the one found in many texts. We like it because it uses no algebra other than that derived from Theorems 39.3 and 40.4. Thus it throws into sharp relief the tremendous strength of both Kronecker's theorem and Zorn's lemma. The proof looks long, but only because we are writing out every little step. To the professional mathematician, the construction of the proof from the information in the preceding paragraph is a routine matter. This proof was suggested to the author during his graduate student days by a fellow graduate student, Norman Shapiro, who also had a strong preference for it.

We are now ready to carry out our proof of Theorem 40.17, which we restate here.

40.22 Restated Theorem 40.17 Every field F has an algebraic closure $\overline{F}$.

Proof It can be shown in set theory that given any set, there exists a set with *strictly more* elements. Suppose we form a set

$$A = \{\omega_{f,i} \mid f \in F[x]; i = 0, \cdots, (\text{degree } f)\}$$

that has an element for every possible zero of any $f(x) \in F[x]$. Let Ω be a set with strictly more elements than A. Replacing Ω by $\Omega \cup F$ if necessary, we can assume $F \subset \Omega$. Consider all possible fields that are algebraic extensions of F and that, as sets, consist of elements of Ω. One such algebraic extension is F itself. If E is any extension field of F, and if $\gamma \in E$ is a zero $f(x) \in F[x]$ for $\gamma \notin F$ and $\deg(\gamma, F) = n$, then renaming γ by ω for $\omega \in \Omega$ and $\omega \notin F$, and renaming elements $a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1}$ of $F(\gamma)$ by distinct elements of Ω as the a_i range over F, we can consider our renamed $F(\gamma)$ to be an algebraic extension field $F(\omega)$ of F, with $F(\omega) \subset \Omega$ and $f(\omega) = 0$. The set Ω has enough elements to form $F(\omega)$, since Ω has more than enough elements to provide n different zeros for each element of each degree n in any subset of $F[x]$.

All algebraic extension fields E_j of F, with $E_j \subseteq \Omega$, form a set

$$S = \{E_j \mid j \in J\}$$

HISTORICAL NOTE

The Axiom of Choice, although used implicitly in the 1870s and 1880s, was first stated explicitly by Ernst Zermelo in 1904 in connection with his proof of the well-ordering theorem, the result that for any set A, there exists an order–relation $<$ such that every nonempty subset B of A contains a least element with respect to $<$. Zermelo's Axiom of Choice asserted that, given any set M and the set S of all subsets of M, there always exists a "choice" function, a function $f : S \to M$ such that $f(M') \in M'$ for every M' in S. Zermelo noted, in fact, that "this logical principle cannot . . . be reduced to a still simpler one, but it is applied without hesitation everywhere in mathematical deduction." A few years later he included this axiom in his collection of axioms for set theory, a collection that was slightly modified in 1930 into what is now called Zermelo–Fraenkel set theory, the axiom system generally used today as a basis of that theory.

Zorn's lemma was introduced by Max Zorn (1906–1993) in 1935. Although he realized that it was equivalent to the well-ordering theorem (itself equivalent to the Axiom of Choice), he claimed that his lemma was more natural to use in algebra because the well-ordering theorem was somehow a "transcendental" principle. Other mathematicians soon agreed with his reasoning. The lemma appeared in 1939 in the first volume of Nicolas Bourbaki's *Eléments de Mathématique: Les Structures Fondamentales de I'Analyse*. It was used consistently in that work and quickly became an essential part of the mathematician's toolbox.

that is partially ordered under our usual subfield inclusion $\leq$. One element of S is F itself. The preceding paragraphs shows that if F is far away from being algebraically closed, there will be many fields E_j in S.

Let $T = \{E_{j_k}\}$ be a chain in S, and let $W = \cup_k E_{j_k}$. We now make W into a field. Let $\alpha, \beta \in W$. Then there exist $E_{j_1}, E_{j_2} \in S$, with $\alpha \in E_{j_1}$ and $\beta \in E_{j_2}$. Since T is a chain, one of the fields E_{j_1} and E_{j_2} is a subfield of the other, say $E_{j_1} \leq E_{j_2}$. Then $\alpha, \beta \in E_{j_2}$, and we use the field operations of E_{j_2} to *define* the sum of α and β in W as $(\alpha + \beta) \in E_{j_2}$ and, likewise, the product as $(\alpha\beta) \in E_{j_2}$. These operations are well defined in W; they are independent of our choice of E_{j_2}, since if $\alpha, \beta \in E_{j_3}$ also, for E_{j_3} in T, then one of the fields E_{j_2} and E_{j_3} is a subfield of the other, since T is a chain. Thus we have operations of addition and multiplication defined on W.

All the field axioms for W under these operations now follow from the fact that these operations were defined in terms of addition and multiplication in fields. Thus, for example, $1 \in F$ serves as multiplicative identity in W, since for $\alpha \in W$, if $1, \alpha \in E_{j_1}$, then we have $1\alpha = \alpha$ in E_{j_i}, so $1\alpha = \alpha$ in W, by definition of multiplication in W. As further illustration, to check the distributive laws, let $\alpha, \beta, \gamma \in W$. Since T is a chain, we can find one field in T containing all three elements α, β, and γ, and in this field the distributive laws for α, β, and γ hold. Thus they hold in W. Therefore, we can view W as a field, and by construction, $E_{j_k} \leq W$ for every $E_{j_k} \in T$.

If we can show that W is algebraic over F, then $W \in S$ will be an upper bound for T. But if $\alpha \in W$, then $\alpha \in E_{j_1}$ for some E_{j_1} in T, so α is algebraic over F. Hence W is an algebraic extension of F and is an upper bound for T.

The hypotheses of Zorn's lemma are thus fulfilled, so there is a maximal element $\overline{F}$ of S. We claim that $\overline{F}$ is algebraically closed. Let $f(x) \in \bar{F}[x]$, where $f(x) \notin \overline{F}$. Suppose that $f(x)$ has no zero in $\overline{F}$. Since Ω has many more elements than $\overline{F}$ has, we can take $\omega \in \Omega$, where $\omega \notin \overline{F}$, and form a field $\overline{F}(\omega) \subseteq \Omega$, with ω a zero of $f(x)$, as we saw in the first paragraph of this proof. Let β be in $\overline{F}(\omega)$. Then by Theorem 39.19, β is a zero of a polynomial

$$g(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$$