To say that a field E is a finite extension of a field F does *not* mean that E is a finite field. It just asserts that E is a finite-dimensional vector space over F, that is, that $[E : F]$ is finite.

We shall often use the fact that if E is a finite extension of F, then, $[E : F] = 1$ if and only if $E = F$. We need only observe that by Theorem 33.18, $\{1\}$ can always be enlarged to a basis for E over F. Thus $[E : F] = 1$ if and only if $E = F(1) = F$.

We show that a finite extension E of a field F must be an algebraic extension of F.

40.3 Theorem A finite extension field E of a field F is an algebraic extension of F.

Proof We must show that for $\alpha \in E, \alpha$ is algebraic over F. By Theorem 33.18 if $[E : F] = n$, then

$$1, \alpha, \cdots, \alpha^n$$

cannot be linearly independent elements, so there exist $a_i \in F$ such that

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0,$$

and not all $a_i = 0$. Then $f(x) = a_nx^n + \cdots + a_1x + a_0$ is a nonzero polynomial in $F[x]$, and $f(\alpha) = 0$. Therefore, α is algebraic over F. ◆

We cannot overemphasize the importance of our next theorem. It plays a role in field theory analogous to the role of the theorem of Lagrange in group theory. While its proof follows easily from our brief work with vector spaces, it is a tool of incredible power. An elegant application of it in the section that follows shows the impossibility of performing certain geometric constructions with a straightedge and a compass. *Never underestimate a theorem that counts something.*

40.4 Theorem If E is a finite extension field of a field F, and K is a finite extension field of E, then K is a finite extension of F, and

$$[K : F] = [K : E][E : F].$$

Proof Let $\{\alpha_i \mid i = 1, \cdots, n\}$ be a basis for E as a vector space over F, and let the set $\{\beta_j \mid j = 1, \cdots, m\}$ be a basis for K as a vector space over E. The theorem will be proved if we can show that the mn elements $\alpha_i\beta_j$ form a basis for K, viewed as a vector space over F. (See Fig. 40.5.)

Let γ be any element of K. Since the β_j form a basis for K over E, we have

$$\gamma = \sum_{j=1}^{m} b_j\beta_j$$

for some $b_j \in E$. Since the α_i form a basis for E over F, we have

$$b_j = \sum_{i=1}^{n} a_{ij}\alpha_i$$

for some $a_{ij} \in F$. Then

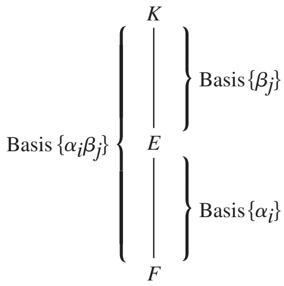
$$\gamma = \sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{ij}\alpha_i\right)\beta_j = \sum_{i,j} a_{ij}(\alpha_i\beta_j),$$

so the mn vectors $\alpha_i\beta_j$ span K over F.

It remains for us to show that the mn elements $\alpha_i\beta_j$ are independent over F. Suppose that $\Sigma_{i,j}c_{ij}(\alpha_i\beta_j) = 0$, with $c_{ij} \in F$. Then

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{n} c_{ij}\alpha_i\right)\beta_j = 0,$$

and $(\Sigma_{i=1}^{n} c_{ij}\alpha_i) \in E$. Since the elements β_j are independent over E, we must have



40.5 Figure

$$\sum_{i=1}^{n} c_{ij}\alpha_i = 0$$

for all j. But now the α_i are independent over F, so $\sum_{i=1}^{n} c_{ij}\alpha_i = 0$ implies that $c_{ij} = 0$ for all i and j. Thus the $\alpha_i\beta_j$ not only span K over F but also are independent over F. Thus they form a basis for K over F. ◆

Note that we proved this theorem by actually exhibiting a basis. It is worth remembering that if $\{\alpha_i \mid i = 1, \cdots, n\}$ is a basis for E over F and $\{\beta_j \mid j = 1, \cdots, m\}$ is a basis for K over E, for fields $F \leq E \leq K$, then the set $\{\alpha_i\beta_j\}$ of mn products is a basis for K over F. Figure 40.5 gives a diagram for this situation. We shall illustrate this further in a moment.

40.6 Corollary If F_i is a field for $i = 1, \cdots, r$ and F_{i+1} is a finite extension of F_i, then F_r is a finite extension of F_1, and

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1].$$

Proof The proof is a straightforward extension of Theorem 40.4 by induction. ◆

40.7 Corollary If E is an extension field of F, $\alpha \in E$ is algebraic over F, and $\beta \in F(\alpha)$, then $\deg(\beta, F)$ divides $\deg(\alpha, F)$.

Proof By Corollary 39.23, $\deg(\alpha, F) = [F(\alpha) : F]$ and $\deg(\beta, F) = [F(\beta) : F]$. We have $F \leq F(\beta) \leq F(\alpha)$, so by Corollary 40.6 $[F(\beta) : F]$ divides $[F(\alpha) : F]$. ◆

The following example illustrates a type of argument one often makes using Theorem 40.4 or its corollaries.

40.8 Example By Corollary 40.7, there is no element of $\mathbb{Q}(\sqrt{2})$ that is a zero of $x^3 - 2$. Note that $\deg(\sqrt{2}, \mathbb{Q}) = 2$, while a zero of $x^3 - 2$ is of degree 3 over $\mathbb{Q}$, but 3 does not divide 2. ▲

Let E be an extension field of a field F, and let α_1, α_2 be elements of E, not necessarily algebraic over F. By definition, $F(\alpha_1)$ is the smallest extension field of F in E that contains α_1. Similarly, $(F(\alpha_1))(\alpha_2)$ can be characterized as the smallest extension field of F in E containing both α_1 and α_2. We could equally have started with α_2, so $(F(\alpha_1))(\alpha_2) = (F(\alpha_2))(\alpha_1)$. We denote this field by $F(\alpha_1, \alpha_2)$. Similarly, for $\alpha_i \in E, F(\alpha_1, \cdots, \alpha_n)$ is the smallest extension field of F in E containing all the α_i for $i = 1, \cdots, n$. We obtain the field $F(\alpha_1, \cdots, \alpha_n)$ from the field F by **adjoining to F the elements** α_i in E. Exercise 51 of Section 22 shows that, analogous to an intersection of subgroups of a group, an intersection of subfields of a field E is again a subfield of E. Thus $F(\alpha_1, \cdots, \alpha_n)$ can be characterized as the intersection of all subfields of E containing F and all the α_i for $i = 1, \cdots, n$.

40.9 Example Consider $\mathbb{Q}(\sqrt{2})$. Corollary 39.23 shows that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Using the technique demonstrated in Example 39.10, we can easily discover that $\sqrt{2}+\sqrt{3}$ is a zero of $x^4 - 10x^2 + 1$. By the method demonstrated in Example 28.15, we can show that this polynomial is irreducible in $\mathbb{Q}[x]$. Thus $\operatorname{irr}(\sqrt{2}+\sqrt{3}, \mathbb{Q}) = x^4 - 10x^2 + 1$, so $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$. Thus $(\sqrt{2}+\sqrt{3}) \notin \mathbb{Q}(\sqrt{2})$, so $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Consequently, $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$. The proof of Theorem 40.4 (see the comment following the theorem) then shows that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. ▲

40.10 Example Let $2^{1/3}$ be the real cube root of 2 and $2^{1/2}$ be the positive square root of 2. Then $2^{1/2} \notin \mathbb{Q}(2^{1/3})$ because $\deg(2^{1/2}, \mathbb{Q}) = 2$ and 2 is not a divisor of $3 = \deg(2^{1/3}, \mathbb{Q})$. Thus $[\mathbb{Q}(2^{1/3}, 2^{1/2}) : \mathbb{Q}(2^{1/3})] = 2$. Hence $\{1, 2^{1/3}, 2^{2/3}\}$ is a basis for $\mathbb{Q}(2^{1/3})$ over $\mathbb{Q}$ and $\{1, 2^{1/2}\}$ is a basis for $\mathbb{Q}(2^{1/3}, 2^{1/2})$ over $\mathbb{Q}(2^{1/3})$. Furthermore, by Theorem 40.4 (see the comment following the theorem),

$$\{1, 2^{1/2}, 2^{1/3}, 2^{5/6}, 2^{2/3}, 2^{7/6}\}$$

is a basis for $\mathbb{Q}(2^{1/2}, 2^{1/3})$ over $\mathbb{Q}$. Because $2^{7/6} = 2(2^{1/6})$, we have $2^{1/6} \in \mathbb{Q}(2^{1/2}, 2^{1/3})$. Now $2^{1/6}$ is a zero of $x^6 - 2$, which is irreducible over $\mathbb{Q}$, by Eisenstein's criterion, with $p = 2$. Thus

$$\mathbb{Q} \leq \mathbb{Q}(2^{1/6}) \leq \mathbb{Q}(2^{1/2}, 2^{1/3})$$

and by Theorem 40.4

$$\begin{aligned} 6 &= [\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}] = [\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/6})][\mathbb{Q}(2^{1/6}) : \mathbb{Q}] \\ &= [\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/6})](6). \end{aligned}$$

Therefore, we must have

$$[\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/6})] = 1,$$

so $\mathbb{Q}(2^{1/2}, 2^{1/3}) = \mathbb{Q}(2^{1/6})$, by the comment preceding Theorem 40.3. ▲

Example 40.10 shows that it is possible for an extension $F(\alpha_1, \cdots, \alpha_n)$ of a field F to be actually a simple extension, even though $n > 1$.

Let us characterize extensions of F of the form $F(\alpha_1, \cdots, \alpha_n)$ in the case that all the α_i are algebraic over F.

40.11 Theorem Let E be an algebraic extension of a field F. Then there exist a finite number of elements $\alpha_1, \cdots, \alpha_n$ in E such that $E = F(\alpha_1, \cdots, \alpha_n)$ if and only if E is a finite-dimensional vector space over F, that is, if and only if E is a finite extension of F.

Proof Suppose that $E = F(\alpha_1, \cdots, \alpha_n)$. Since E is an algebraic extension of F, each α_i is algebraic over F, so each α_i is algebraic over every extension field of F in E. Thus $F(\alpha_1)$ is algebraic over F, and in general, $F(\alpha_1, \cdots, \alpha_j)$ is algebraic over $F(\alpha_i, \cdots, \alpha_{j-1})$ for $j = 2, \cdots, n$. Corollary 40.6 applied to the sequence of finite extensions

$$F, F(\alpha_1), F(\alpha_1, \alpha_2), \cdots, F(\alpha_1, \cdots, \alpha_n) = E$$

then shows that E is a finite extension of F.

Conversely, suppose that E is a finite algebraic extension of F. If $[E : F] = 1$, then $E = F(1) = F$, and we are done. If $E \neq F$, let $\alpha_1 \in E$, where $\alpha_1 \notin F$. Then $[F(\alpha_1) : F] > 1$. If $F(\alpha_1) = E$, we are done; if not, let $\alpha_2 \in E$, where $\alpha_2 \notin F(\alpha_1)$. Continuing this process, we see from Theorem 40.4 that since $[E : F]$ is finite, we must arrive at α_n such that

$$F(\alpha_1, \cdots, \alpha_n) = E.$$ ◆

Algebraically Closed Fields and Algebraic Closures

We have not yet observed that if E is an extension of a field F and $\alpha, \beta \in E$ are algebraic over F, then so are $\alpha + \beta, \alpha\beta, \alpha - \beta$, and α/β, if $\beta \neq 0$. This follows from Theorem 40.3 and is also included in the following theorem.

40.12 Theorem Let E be an extension field of F. Then

$$\bar{F}_E = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$$

is a subfield of E, the **algebraic closure of** F **in** E.

Proof Let $\alpha, \beta \in \bar{F}_E$. Then Theorem 40.11 shows that $F(\alpha, \beta)$ is a finite extension of F, and by Theorem 40.3 every element of $F(\alpha, \beta)$ is algebraic over F, that is, $F(\alpha, \beta) \subseteq \bar{F}_E$. Thus $\bar{F}_E$ contains $\alpha + \beta, \alpha\beta, \alpha - \beta$, and also contains α/β for $\beta \neq 0$, so $\bar{F}_E$ is a subfield of E. ◆

40.13 Corollary The set of all algebraic numbers forms a field.

Proof Proof of this corollary is immediate from Theorem 40.12, because the set of all algebraic numbers is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. ◆

It is well known that the complex numbers have the property that every nonconstant polynomial in $\mathbb{C}[x]$ has a zero in $\mathbb{C}$. This is known as the *Fundamental Theorem of Algebra*. An analytic proof of this theorem is given in Theorem 40.18. We now give a definition generalizing this important concept to other fields.

40.14 Definition A field F is **algebraically closed** if every nonconstant polynomial in $F[x]$ has a zero in F. ■

Note that a field F can be the algebraic closure of F in an extension field E without F being algebraically closed. For example, $\mathbb{Q}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{Q}(x)$, but $\mathbb{Q}$ is not algebraically closed because $x^2 + 1$ has no zero in $\mathbb{Q}$.

The next theorem shows that the concept of a field being algebraically closed can also be defined in terms of factorization of polynomials over the field.

40.15 Theorem A field F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ factors in $F[x]$ into linear factors.

Proof Let F be algebraically closed, and let $f(x)$ be a nonconstant polynomial in $F[x]$ Then $f(x)$ has a zero $a \in F$. By Corollary 28.4, $x - a$ is a factor of $f(x)$, so $f(x) = (x - a)g(x)$. Then if $g(x)$ is nonconstant, it has a zero $b \in F$, and we have $f(x) = (x - a)(x - b)h(x)$. Continuing, we get a factorization of $f(x)$ in $F[x]$ into linear factors.

Conversely, suppose that every nonconstant polynomial of $F[x]$ has a factorization into linear factors. If $ax - b$ is a linear factor of $f(x)$, then b/a is a zero of $f(x)$. Thus F is algebraically closed. ◆

40.16 Corollary An algebraically closed field F has no proper algebraic extensions, that is, no algebraic extensions E with $F < E$.

Proof Let E be an algebraic extension of F, so $F \leq E$. Then if $\alpha \in E$, we have $\operatorname{irr}(\alpha, F) = x - \alpha$, by Theorem 40.15, since F is algebraically closed. Thus $\alpha \in F$, and we must have $F = E$. ◆

In a moment we shall show that just as there exists an algebraically closed extension $\mathbb{C}$ of the real numbers $\mathbb{R}$, for any field F there exists similarly an algebraic extension $\overline{F}$ of F, with the property that $\overline{F}$ is algebraically closed. Naively, to find $\overline{F}$ we proceed