Theorem 9. *Every element w of a finite extension K of F is algebraic over F and satisfies an equation irreducible over F of degree at most n, where $n = [K:F]$ is the degree of the given extension.*

Proof. The $n + 1$ powers $1, w, w^2, \cdots, w^n$ of the given element w are elements of the n-dimensional vector space K, hence must be linearly dependent over F (Chap. VII, Theorem 4, Corollary 2). There must, therefore, be a linear relation $b_0 + b_1 w + \cdots + b_n w^n = 0$ with not all coefficients zero. Interpreted as a polynomial, this relation implies that w is algebraic over F.

Corollary. *Every element of a simple algebraic extension $F(u)$ is algebraic over F.*

This important conclusion assures us that a transcendental element would never appear in a simple algebraic extension.

In working with a particular simple algebraic extension $F(u)$, the irreducible polynomial $p(x)$ for u must be used systematically, for by Theorem 2 an element $g(u)$ in the extension is zero if and only if the polynomial $g(x)$ is divisible by $p(x)$. Suppose, for instance, that $\mathbf{Q}(u)$ is an extension of degree 3 over the field $\mathbf{Q}$ of rationals, generated by a root u of $x^3 - 2x + 2$. This polynomial is irreducible by the Eisenstein irreducibility criterion (Chap. III, §10). The element $w = u^2 - u$ in this extension $\mathbf{Q}(u)$ must satisfy some polynomial equation of degree at most 3. To find this equation, express the powers $w^2 = u^4 - 2u^3 + u^2$ and $w^3 = u^6 - 3u^5 + 3u^4 - u^3$ linearly in terms of 1, u, and u^2, as in Theorem 4. This is done by applying repeatedly the given equation $u^3 = 2u - 2$. This gives

$$w = u^2 - u, \qquad w^2 = 3u^2 - 6u + 4, \qquad w^3 = 16u^2 - 28u + 18.$$

To obtain the linear relation which must hold between 1, w, w^2, and w^3, one may solve the equations for w and w^2 linearly to get u and u^2, as

$$u = -w^2/3 + w + 4/3, \qquad u^2 = -w^2/3 + 2w + 4/3. \tag{6}$$

These, substituted in the expression for w^3, give the desired equation

$$w^3 - 4w^2 - 4w - 2 = 0.$$

This equation is irreducible over $\mathbf{Q}$, by the Eisenstein theorem. Alternatively, one may argue by equation (6) that u is in $\mathbf{Q}(w)$, so that $\mathbf{Q}(u) = \mathbf{Q}(w)$ and u and w generate the same extension, and by the Corollary to Theorem 8 have the same degree 3 over $\mathbf{Q}$. This means that any equation of degree 3 for w must be irreducible.

EXERCISES

1. Each of the following numbers is in a simple algebraic extension of $\mathbf{Q}$, hence is algebraic over $\mathbf{Q}$. Find in each case the monic irreducible equation satisfied by the number. (a) $2 + \sqrt{3}$; (b) $\sqrt[4]{5} + \sqrt{5}$; (c) $\sqrt[3]{2} + \sqrt[3]{4}$; (d) $u^2 - 1$, where u satisfies $u^3 = 2u + 2$; (e) $u^2 + u$, where u satisfies $u^3 = -3u^2 + 3$.

2. Prove that every finite extension of the field $\mathbf{R}$ of real numbers is either $\mathbf{R}$ itself or is isomorphic to the field $\mathbf{C}$ of complex numbers.

3. Prove that the field of all complex numbers has no proper finite extensions.

4. (a) If K is an extension of degree 2 over the field $\mathbf{Q}$ of rationals, prove that $K = \mathbf{Q}(\sqrt{d})$, where d is an integer which is not a square and which has no factors which are squares of integers.

(b) How much of this result remains true if $\mathbf{Q}$ is replaced by a field F of characteristic ∞? by a field F of any characteristic?

5. Is the field $F(x)$ of rational forms in the indeterminate x a finite extension of F? Why?

6. Prove that the number of elements in a finite field of characteristic p is a power of p.

7. (a) Prove that there are exactly $(p^2 - p)/2$ monic irreducible quadratic polynomials over the field $\mathbf{Z}_p$ of integers modulo p.

(b) Prove that for each p there exists a field of characteristic p with p^2 elements.

***8.** Prove that there are exactly $(p^3 - p)/3$ monic irreducible cubic polynomials over the field $\mathbf{Z}_p$ of integers modulo p.

***9.** Let F be any field contained in an integral domain D. Prove:

(a) D is a vector space over F;

(b) If, as a vector space, D has a finite dimension over F, then D is a field.

5. Iterated Algebraic Extensions

Finite extensions of a field F may be built up by repeated simple extensions. If F has characteristic ∞, one may prove that any such iterated extension can be generated by a suitably chosen single element. We shall omit this proof, and discuss the properties of iterated extensions directly. In general, if K is any extension of F containing elements $c_1, c_2, \cdots, c_r$ the symbol $F(c_1, c_2, \cdots, c_r)$ denotes the subfield of K generated by $c_1, \cdots, c_r$ and the elements of F (the subfield consisting of all elements rationally expressible in terms of $c_1, \cdots, c_r$ over F). Alternatively, such a multiple extension may be obtained by iterated simple extensions; thus, $F(c_1, c_2)$ is the simple extension $L(c_2)$ of the simple extension $L = F(c_1)$.

Iterated algebraic extensions may arise in the solution of equations, where it is often useful to introduce appropriate auxiliary equations. For example, the equation $x^4 - 2x^2 + 9 = 0$ may be written as

$$x^4 - 2x^2 + 9 = (x^4 - 6x^2 + 9) + 4x^2 = (x^2 - 3)^2 + 4x^2 = 0.$$

The equation, therefore, is $[(x^2 - 3)/2x]^2 = -1$. This formula indicates that any field which contains a root u of the given equation also contains a root $i = (u^2 - 3)/2u$ of the equation $y^2 = -1$. If we adjoin the auxiliary quantity i to the field $\mathbf{Q}$ of rationals, the original equation becomes

reducible over $\mathbf{Q}(i)$, for

$$x^4 - 2x^2 + 9 = (x^2 - 3 + 2xi)(x^2 - 3 - 2xi).$$

By the usual formula, the factor $x^2 - 3 - 2ix$ has a root $u = i + \sqrt{2}$. The original equation thus has a root in the field $K = \mathbf{Q}(i, \sqrt{2})$. This field K could have been obtained by adjoining to $\mathbf{Q}$ first $\sqrt{2}$, then i. The intermediate field $\mathbf{Q}(\sqrt{2})$ consists of real numbers, hence cannot contain i. The quadratic equation $y^2 + 1 = 0$ for i must therefore remain irreducible over the real field $\mathbf{Q}(\sqrt{2})$, so that the extension $\mathbf{Q}(\sqrt{2}, i)$ has over $\mathbf{Q}(\sqrt{2})$ a degree 2 and a basis of two elements 1 and i. The field $\mathbf{Q}(\sqrt{2})$ in turn has a basis 1, $\sqrt{2}$ over $\mathbf{Q}$. Therefore any element w in the whole field $\mathbf{Q}(\sqrt{2}, i)$ can be expressed as

$$(7) \quad w = (a + b\sqrt{2}) + (c + d\sqrt{2})i = a + b\sqrt{2} + ci + d\sqrt{2}i,$$

with rational coefficients a, b, c, and d. The four elements $1, \sqrt{2}, i, \sqrt{2}i$ thus form a basis for the whole extension $K = \mathbf{Q}(\sqrt{2}, i)$ over $\mathbf{Q}$. This method of compounding bases can be stated in general, as follows:

Theorem 10. *If the elements $u_1, \cdots, u_n$ form a basis for a finite extension K of F, while $w_1, \cdots, w_m$ constitute a basis for an extension L of K, then the mn products $u_i w_j$, for $i = 1, \cdots, n$ and $j = 1, \cdots, m$, form a basis for L over F.*

Proof. Any element y in L can be represented as a linear combination $y = \sum_j r_j w_j$ of the given basis, with coefficients r_j in K. Each coefficient r_j is in turn some combination $r_j = \sum_i a_{ij} u_i$ of the basis elements of K, with each a_{ij} in F. On substitution of these values,

$$y = \sum_j \sum_i a_{ij} u_i w_j$$

appears as a linear combination of the suggested elements $u_i w_j$, with coefficients in F. The same type of successive argument proves that these mn elements are linearly independent over F, hence do constitute a basis for K, Q.E.D.

Many consequences flow from Theorem 10. In the first place, one may state the result without reference to the particular bases used, as follows:

Corollary 1. *If K is a finite extension of F and L a finite extension of K, then L is a finite extension of F, and its degree is*

$$(8) \qquad [L:F] = [L:K][K:F] \qquad (L \supset K \supset F).$$

Corollary 2. *If K is a finite extension of degree $n = [K:F]$ over F, every element u of K has over F a degree which is a divisor of n.*

Proof. The element u generates a simple extension $F(u)$; hence by (8), $n = [K:F(u)][F(u):F]$, where the second factor is the degree of u under consideration.

Corollary 3. *An element u of a finite extension $K \supset F$ generates the whole extension if and only if $[K:F] = [u:F]$.*

Proof. If u satisfies over F an irreducible equation of degree $[K:F]$, then u generates a subfield $F(u)$ of degree n over F. By (8) this subfield must include all of K.

Corollary 4. *If $K = F(y_1, y_2, \cdots, y_r)$ is a field generated by r quantities y_i, where each successive y_i is algebraic over the field $F(y_1, \cdots, y_{i-1})$ generated by the preceding $i - 1$ quantities, then K is a finite extension of F, and every element in K is algebraic over F.*

Proof. Every degree $[F(y_1, \cdots, y_{i-1}, y_i):F(y_1, \cdots, y_{i-1})]$ is finite; hence by Corollary 1 the whole degree $[K:F]$ is finite. By Theorem 9, every element in K is then algebraic over F.

Corollary 5. *If $p(x)$ is an irreducible cubic polynomial over a field F, and if K is an extension of F of degree 2^m, then $p(x)$ is irreducible over K.*

This corollary means in particular that an irreducible cubic equation could never be solved by successive square roots, for the adjunction of a square root to a field F either will give no extension at all or will give an extension of degree 2, so that the extension $K = F(\sqrt{a}, \sqrt{b}, \sqrt{c}, \cdots)$ obtained by any number of square roots will have as degree some power 2^m of 2. By Corollary 5, this extension will never contain a root of the given irreducible cubic.

For a proof, suppose $p(x)$ reducible over the field K of degree 2^m. Then the cubic $p(x)$ must have at least one linear factor $x - u$, so that K contains a root u of $p(x)$. But such an element u of degree 3 over F cannot be contained in a field K of degree 2^m over F, by Corollary 2. This proves $p(x)$ irreducible.

This corollary is the algebraic basis of the theorem that it is impossible to solve the classical problem of duplicating a general cube or trisecting a general angle by ruler and compass alone. Any such construction problem may be reduced to analytic terms. The data of the problem consist of a number of points and lines. Relative to some set of axes, the coordinates of these points (and the ratios of the coefficients in the equations for these lines) are a set of real numbers which generates a certain field F of real numbers. Each step in a ruler and compass construction provides certain new points and lines. It can be shown† that the corresponding new field of numbers is either F itself, or a quadratic extension of F. Hence repeated

† This depends essentially on the fact that the equation of a circle (compass) is quadratic and the equation of a straight line (ruler) is linear.