$s_k = s_k(x_1,\ldots,x_n) = x_1^k + \cdots + x_n^k \in R[x_1,\ldots,x_n]$ *for* $k \geqslant 1$. *Then the formula*

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 + \cdots + (-1)^{m-1}s_{k-m+1}\sigma_{m-1} + (-1)^m \frac{m}{n} s_{k-m}\sigma_m = 0$$

holds for $k \geqslant 1$, *where* $m = \min(k, n)$.

1.76. Theorem (Waring's Formula). *With the same notation as in Theorem* 1.75, *we have*

$$s_k = \sum (-1)^{i_2+i_4+i_6+\cdots} \frac{(i_1+i_2+\cdots+i_n-1)!k}{i_1!i_2!\cdots i_n!} \sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_n^{i_n}$$

for $k \geqslant 1$, *where the summation is extended over all n-tuples* $(i_1,\ldots,i_n)$ *of nonnegative integers with* $i_1 + 2i_2 + \cdots + ni_n = k$. *The coefficient of* $\sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_n^{i_n}$ *is always an integer.*

4. FIELD EXTENSIONS

Let F be a field. A subset K of F that is itself a field under the operations of F will be called a *subfield* of F. In this context, F is called an *extension* (*field*) of K. If $K \neq F$, we say that K is a *proper subfield* of F.

If K is a subfield of the finite field $\mathbb{F}_p$, p prime, then K must contain the elements 0 and 1, and so all other elements of $\mathbb{F}_p$ by the closure of K under addition. It follows that $\mathbb{F}_p$ contains no proper subfields. We are thus led to the following concept.

1.77. Definition. A field containing no proper subfields is called a *prime field*.

By the above argument, any finite field of order p, p prime, is a prime field. Another example of a prime field is the field $\mathbb{Q}$ of rational numbers.

The intersection of any nonempty collection of subfields of a given field F is again a subfield of F. If we form the intersection of *all* subfields of F, we obtain the *prime subfield* of F. It is obviously a prime field.

1.78. Theorem. *The prime subfield of a field* F *is isomorphic to either* $\mathbb{F}_p$ *or* $\mathbb{Q}$, *according as the characteristic of* F *is a prime* p *or* 0.

1.79. Definition. Let K be a subfield of the field F and M any subset of F. Then the field $K(M)$ is defined as the intersection of all subfields of F containing both K and M and is called the extension (field) of K obtained by *adjoining* the elements in M. For finite $M = \{\theta_1,\ldots,\theta_n\}$ we write $K(M) = K(\theta_1,\ldots,\theta_n)$. If M consists of a single element $\theta \in F$, then $L = K(\theta)$ is said to be a *simple extension* of K and θ is called a *defining element* of L over K.

Obviously, $K(M)$ is the smallest subfield of F containing both K and M. We define now an important type of extension.

1.80. Definition. Let K be a subfield of F and $\theta \in F$. If θ satisfies a nontrivial polynomial equation with coefficients in K, that is, if $a_n\theta^n + \cdots + a_1\theta + a_0 = 0$ with $a_i \in K$ not all being 0, then θ is said to be *algebraic* over K. An extension L of K is called *algebraic* over K (or an *algebraic extension* of K) if every element of L is algebraic over K.

Suppose $\theta \in F$ is algebraic over K, and consider the set $J = \{f \in K[x]: f(\theta) = 0\}$. It is easily checked that J is an ideal of $K[x]$, and we have $J \neq (0)$ since θ is algebraic over K. It follows then from Theorem 1.54 that there exists a uniquely determined monic polynomial $g \in K[x]$ such that J is equal to the principal ideal (g). It is important to note that g is irreducible in $K[x]$. For, in the first place, g is of positive degree since it has the root θ; and if $g = h_1h_2$ in $K[x]$ with $1 \leqslant \deg(h_i) < \deg(g)$ $(i = 1,2)$, then $0 = g(\theta) = h_1(\theta)h_2(\theta)$ implies that either h_1 or h_2 is in J and so divisible by g, which is impossible.

1.81. Definition. If $\theta \in F$ is algebraic over K, then the uniquely determined monic polynomial $g \in K[x]$ generating the ideal $J = \{f \in K[x]: f(\theta) = 0\}$ of $K[x]$ is called the *minimal polynomial* (or *defining polynomial*, or *irreducible polynomial*) of θ over K. By the *degree* of θ over K we mean the degree of g.

1.82. Theorem. *If $\theta \in F$ is algebraic over K, then its minimal polynomial g over K has the following properties:*

(i) *g is irreducible in $K[x]$.*
(ii) *For $f \in K[x]$ we have $f(\theta) = 0$ if and only if g divides f.*
(iii) *g is the monic polynomial in $K[x]$ of least degree having θ as a root.*

Proof. Property (i) was already noted and (ii) follows from the definition of g. As to (iii), it suffices to note that any monic polynomial in $K[x]$ having θ as a root must be a multiple of g, and so it is either equal to g or its degree is larger than that of g. □

We note that both the minimal polynomial and the degree of an algebraic element θ depend on the field K over which it is considered, so that one must be careful not to speak of the minimal polynomial or the degree of θ without specifying K, unless the latter is amply clear from the context.

If L is an extension field of K, then L may be viewed as a vector space over K. For the elements of L (= "vectors") form, first of all, an abelian group under addition. Moreover, each "vector" $\alpha \in L$ can be multiplied by a "scalar" $r \in K$ so that $r\alpha$ is again in L (here $r\alpha$ is simply the

product of the field elements r and α of L) and the laws for multiplication by scalars are satisfied: $r(\alpha+\beta)=r\alpha+r\beta$, $(r+s)\alpha=r\alpha+s\alpha$, $(rs)\alpha=r(s\alpha)$, and $1\alpha=\alpha$, where $r,s\in K$ and $\alpha,\beta\in L$.

1.83. Definition. Let L be an extension field of K. If L, considered as a vector space over K, is finite-dimensional, then L is called a *finite extension* of K. The dimension of the vector space L over K is then called the *degree* of L over K, in symbols $[L:K]$.

1.84. Theorem. *If L is a finite extension of K and M is a finite extension of L, then M is a finite extension of K with*

$$[M:K]=[M:L][L:K].$$

Proof. Put $[M:L]=m$, $[L:K]=n$, and let $\{\alpha_1,\ldots,\alpha_m\}$ be a basis of M over L and $\{\beta_1,\ldots,\beta_n\}$ a basis of L over K. Then every $\alpha\in M$ is a linear combination $\alpha=\gamma_1\alpha_1+\cdots+\gamma_m\alpha_m$ with $\gamma_i\in L$ for $1\leqslant i\leqslant m$, and writing each γ_i in terms of the basis elements β_j we get

$$\alpha=\sum_{i=1}^{m}\gamma_i\alpha_i=\sum_{i=1}^{m}\left(\sum_{j=1}^{n}r_{ij}\beta_j\right)\alpha_i=\sum_{i=1}^{m}\sum_{j=1}^{n}r_{ij}\beta_j\alpha_i$$

with coefficients $r_{ij}\in K$. If we can show that the mn elements $\beta_j\alpha_i$, $1\leqslant i\leqslant m$, $1\leqslant j\leqslant n$, are linearly independent over K, then we are done. So suppose we have

$$\sum_{i=1}^{m}\sum_{j=1}^{n}s_{ij}\beta_j\alpha_i=0$$

with coefficients $s_{ij}\in K$. Then

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

and from the linear independence of the α_i over L we infer

$$\sum_{j=1}^{n}s_{ij}\beta_j=0\quad\text{for } 1\leqslant i\leqslant m.$$

But since the β_j are linearly independent over K, we conclude that all s_{ij} are 0. □

1.85. Theorem. *Every finite extension of K is algebraic over K.*

Proof. Let L be a finite extension of K and put $[L:K]=m$. For $\theta\in L$, the $m+1$ elements $1,\theta,\ldots,\theta^m$ must then be linearly dependent over K, and so we get a relation $a_0+a_1\theta+\cdots+a_m\theta^m=0$ with $a_i\in K$ not all being 0. This just says that θ is algebraic over K. □

For the study of the structure of a simple extension $K(\theta)$ of K obtained by adjoining an algebraic element, let F be an extension of K and let $\theta \in F$ be algebraic over K. It turns out that $K(\theta)$ is a finite (and therefore an algebraic) extension of K.

1.86. Theorem. *Let $\theta \in F$ be algebraic of degree n over K and let g be the minimal polynomial of θ over K. Then:*

(i) *$K(\theta)$ is isomorphic to $K[x]/(g)$.*
(ii) *$[K(\theta): K] = n$ and $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis of $K(\theta)$ over K.*
(iii) *Every $\alpha \in K(\theta)$ is algebraic over K and its degree over K is a divisor of n.*

Proof. (i) Consider the mapping $\tau: K[x] \to K(\theta)$, defined by $\tau(f) = f(\theta)$ for $f \in K[x]$, which is easily seen to be a ring homomorphism. We have $\ker \tau = \{f \in K[x]: f(\theta) = 0\} = (g)$ by the definition of the minimal polynomial. Let S be the image of τ; that is, S is the set of polynomial expressions in θ with coefficients in K. Then the homomorphism theorem for rings (see Theorem 1.40) yields that S is isomorphic to $K[x]/(g)$. But $K[x]/(g)$ is a field by Theorems 1.61 and 1.82(i), and so S is a field. Since $K \subseteq S \subseteq K(\theta)$ and $\theta \in S$, it follows from the definition of $K(\theta)$ that $S = K(\theta)$, and (i) is thus shown.

(ii) Since $S = K(\theta)$, any given $\alpha \in K(\theta)$ can be written in the form $\alpha = f(\theta)$ for some $f \in K[x]$. By the division algorithm, $f = qg + r$ with $q, r \in K[x]$ and $\deg(r) < \deg(g) = n$. Then $\alpha = f(\theta) = q(\theta)g(\theta) + r(\theta) = r(\theta)$, and so α is a linear combination of $1, \theta, \ldots, \theta^{n-1}$ with coefficients in K. On the other hand, if $a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} = 0$ for certain $a_i \in K$, then the polynomial $h(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in K[x]$ has θ as a root and is thus a multiple of g by Theorem 1.82(ii). Since $\deg(h) < n = \deg(g)$, this is only possible if $h = 0$—that is, if all $a_i = 0$. Therefore, the elements $1, \theta, \ldots, \theta^{n-1}$ are linearly independent over K and (ii) follows.

(iii) $K(\theta)$ is a finite extension of K by (ii), and so $\alpha \in K(\theta)$ is algebraic over K by Theorem 1.85. Furthermore, $K(\alpha)$ is a subfield of $K(\theta)$. If d is the degree of α over K, then (ii) and Theorem 1.84 imply that $n = [K(\theta): K] = [K(\theta): K(\alpha)][K(\alpha): K] = [K(\theta): K(\alpha)]d$, hence d divides n. □

The elements of the simple algebraic extension $K(\theta)$ of K are therefore polynomial expressions in θ. Any element of $K(\theta)$ can be uniquely represented in the form $a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$ with $a_i \in K$ for $0 \leqslant i \leqslant n-1$.

It should be pointed out that Theorem 1.86 operates under the assumption that both K and θ are embedded in a larger field F. This is necessary in order that algebraic expressions involving θ make sense. We now want to construct a simple algebraic extension *ab ovo*—that is, without

reference to a previously given larger field. The clue to this is contained in part (i) of Theorem 1.86.

1.87. Theorem. *Let $f \in K[x]$ be irreducible over the field K. Then there exists a simple algebraic extension of K with a root of f as a defining element.*

Proof. Consider the residue class ring $L = K[x]/(f)$, which is a field by Theorem 1.61. The elements of L are the residue classes $[h] = h + (f)$ with $h \in K[x]$. For any $a \in K$ we can form the residue class $[a]$ determined by the constant polynomial a, and if $a, b \in K$ are distinct, then $[a] \neq [b]$ since f has positive degree. The mapping $a \mapsto [a]$ gives an isomorphism from K onto a subfield K' of L, so that K' may be identified with K. In other words, we can view L as an extension of K. For every $h(x) = a_0 + a_1x + \cdots + a_mx^m \in K[x]$ we have $[h] = [a_0 + a_1x + \cdots + a_mx^m] = [a_0] + [a_1][x] + \cdots + [a_m][x]^m = a_0 + a_1[x] + \cdots + a_m[x]^m$ by the rules for operating with residue classes and the identification $[a_i] = a_i$. Thus, every element of L can be written as a polynomial expression in $[x]$ with coefficients in K. Since any field containing both K and $[x]$ must contain these polynomial expressions, L is a simple extension of K obtained by adjoining $[x]$. If $f(x) = b_0 + b_1x + \cdots + b_nx^n$, then $f([x]) = b_0 + b_1[x] + \cdots + b_n[x]^n = [b_0 + b_1x + \cdots + b_nx^n] = [f] = [0]$, so that $[x]$ is a root of f and L is a simple algebraic extension of K. □

1.88. Example. As an example of the formal process of root adjunction in Theorem 1.87, consider the prime field $\mathbb{F}_3$ and the polynomial $f(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$, which is irreducible over $\mathbb{F}_3$. Let θ be a "root" of f; that is, θ is the residue class $x + (f)$ in $L = \mathbb{F}_3[x]/(f)$. The other root of f in L is then $2\theta + 2$, since $f(2\theta + 2) = (2\theta + 2)^2 + (2\theta + 2) + 2 = \theta^2 + \theta + 2 = 0$. By Theorem 1.86(ii), or by the known structure of a residue class field, the simple algebraic extension $L = \mathbb{F}_3(\theta)$ consists of the nine elements $0, 1, 2, \theta, \theta + 1, \theta + 2, 2\theta, 2\theta + 1, 2\theta + 2$. The operation tables for L can be constructed as in Example 1.62. □

We observe that in the above example we may adjoin either the root θ or the root $2\theta + 2$ of f and we would still obtain the same field. This situation is covered by the following result, which is easily established.

1.89. Theorem. *Let α and β be two roots of the polynomial $f \in K[x]$ that is irreducible over K. Then $K(\alpha)$ and $K(\beta)$ are isomorphic under an isomorphism mapping α to β and keeping the elements of K fixed.*

We are now asking for an extension field to which all roots of a given polynomial belong.

1.90. Definition. Let $f \in K[x]$ be of positive degree and F an extension field of K. Then f is said to *split in F* if f can be written as a product of

linear factors in $F[x]$—that is, if there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ such that

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

where a is the leading coefficient of f. The field F is a *splitting field* of f over K if f splits in F and if, moreover, $F = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

It is clear that a splitting field F of f over K is in the following sense the smallest field containing all the roots of f: no proper subfield of F that is an extension of K contains all the roots of f. By repeatedly applying the process used in Theorem 1.87, one obtains the first part of the subsequent result. The second part is an extension of Theorem 1.89.

1.91. Theorem (Existence and Uniqueness of Splitting Field). *If K is a field and f any polynomial of positive degree in $K[x]$, then there exists a splitting field of f over K. Any two splitting fields of f over K are isomorphic under an isomorphism which keeps the elements of K fixed and maps roots of f into each other.*

Since isomorphic fields may be identified, we can speak of *the* splitting field of f over K. It is obtained from K by adjoining finitely many algebraic elements over K, and therefore one can show on the basis of Theorems 1.84 and 1.86(ii) that the splitting field of f over K is a finite extension of K.

As an illustration of the usefulness of splitting fields, we consider the question of deciding whether a given polynomial has a multiple root (compare with Definition 1.65).

1.92. Definition. Let $f \in K[x]$ be a polynomial of degree $n \geqslant 2$ and suppose that $f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_n)$ with $\alpha_1, \ldots, \alpha_n$ in the splitting field of f over K. Then the *discriminant* $D(f)$ of f is defined by

$$D(f) = a_0^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

It is obvious from the definition of $D(f)$ that f has a multiple root if and only if $D(f) = 0$. Although $D(f)$ is defined in terms of elements of an extension of K, it is actually an element of K itself. For small n this can be seen by direct calculation. For instance, if $n = 2$ and $f(x) = ax^2 + bx + c = a(x-\alpha_1)(x-\alpha_2)$, then $D(f) = a^2(\alpha_1 - \alpha_2)^2 = a^2((\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2) = a^2(b^2a^{-2} - 4ca^{-1})$, hence

$$D(ax^2 + bx + c) = b^2 - 4ac,$$

a well-known expression from the theory of quadratic equations. If $n = 3$ and $f(x) = ax^3 + bx^2 + cx + d = a(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, then $D(f) = a^4(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$, and a more involved computation yields

$$D(ax^3 + bx^2 + cx + d) = b^2c^2 - 4b^3d - 4ac^3 - 27a^2d^2 + 18abcd. \quad (1.9)$$

In the general case, consider first the polynomial $s \in K[x_1,\ldots,x_n]$ given by

$$s(x_1,\ldots,x_n) = a_0^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2.$$

Then s is a symmetric polynomial, and by a result in Example 1.74 it can be written as a polynomial expression in the elementary symmetric polynomials $\sigma_1,\ldots,\sigma_n$—that is, $s = h(\sigma_1,\ldots,\sigma_n)$ for some $h \in K[x_1,\ldots,x_n]$. If $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = a_0(x-\alpha_1)\cdots(x-\alpha_n)$, then the definition of the elementary symmetric polynomials (see again Example 1.74) implies that $\sigma_k(\alpha_1,\ldots,\alpha_n) = (-1)^k a_k a_0^{-1} \in K$ for $1 \leqslant k \leqslant n$. Thus,

$$\begin{aligned} D(f) = s(\alpha_1,\ldots,\alpha_n) &= h\big(\sigma_1(\alpha_1,\ldots,\alpha_n),\ldots,\sigma_n(\alpha_1,\ldots,\alpha_n)\big) \\ &= h\big(-a_1a_0^{-1},\ldots,(-1)^n a_n a_0^{-1}\big) \in K. \end{aligned}$$

Since $D(f) \in K$, it should be possible to calculate $D(f)$ without having to pass to an extension field of K. This can be done via the notion of resultant. We note first that if a polynomial $f \in K[x]$ is given in the form $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ and we accept the possibility that $a_0 = 0$, then n need not be the degree of f. We speak of n as the *formal degree* of f; it is always greater than or equal to $\deg(f)$.

1.93. Definition. Let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in K[x]$ and $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m \in K[x]$ be two polynomials of formal degree n resp. m with $n, m \in \mathbb{N}$. Then the *resultant* $R(f,g)$ of the two polynomials is defined by the determinant

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & & \cdots & a_n \\ b_0 & b_1 & \cdots & & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & & b_m & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & b_0 & b_1 & & \cdots & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$

of order $m+n$.

If $\deg(f) = n$ (i.e., if $a_0 \neq 0$) and $f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_n)$ in the splitting field of f over K, then $R(f,g)$ is also given by the formula

$$R(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i). \tag{1.10}$$

In this case, we obviously have $R(f,g) = 0$ if and only if f and g have a common root, which is the same as saying that f and g have a common divisor in $K[x]$ of positive degree.