CHAPTER V

Algebraic Extensions

In this first chapter concerning polynomial equations, we show that given a polynomial over a field, there always exists some extension of the field where the polynomial has a root, and we prove the existence of an algebraic closure. We make a preliminary study of such extensions, including the automorphisms, and we give algebraic extensions of finite fields as examples.

§1. FINITE AND ALGEBRAIC EXTENSIONS

Let F be a field. If F is a subfield of a field E, then we also say that E is an **extension field** of F. We may view E as a vector space over F, and we say that E is a **finite** or **infinite** extension of F according as the dimension of this vector space is finite or infinite.

Let F be a subfield of a field E. An element α of E is said to be **algebraic** over F if there exist elements $a_0, \ldots, a_n$ $(n \geqq 1)$ of F, not all equal to 0, such that

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

If $\alpha \neq 0$, and α is algebraic, then we can always find elements a_i as above such that $a_0 \neq 0$ (factoring out a suitable power of α).

Let X be a variable over F. We can also say that α is algebraic over F if the homomorphism

$$F[X] \to E$$

S. Lang, *Algebra*
© Springer Science+Business Media LLC 2002

which is the identity on F and maps X on α has a non-zero kernel. In that case the kernel is an ideal which is principal, generated by a single polynomial $p(X)$, which we may assume has leading coefficient 1. We then have an isomorphism

$$F[X]/(p(X)) \approx F[\alpha],$$

and since $F[\alpha]$ is entire, it follows that $p(X)$ is irreducible. Having normalized $p(X)$ so that its leading coefficient is 1, we see that $p(X)$ is uniquely determined by α and will be called THE irreducible polynomial of α over F. We sometimes denote it by $\mathrm{Irr}(\alpha, F, X)$.

An extension E of F is said to be **algebraic** if every element of E is algebraic over F.

Proposition 1.1. *Let E be a finite extension of F. Then E is algebraic over F.*

Proof. Let $\alpha \in E$, $\alpha \neq 0$. The powers of α,

$$1, \alpha, \alpha^2, \ldots, \alpha^n,$$

cannot be linearly independent over F for all positive integers n, otherwise the dimension of E over F would be infinite. A linear relation between these powers shows that α is algebraic over F.

Note that the converse of Proposition 1.1 is not true; there exist infinite algebraic extensions. We shall see later that the subfield of the complex numbers consisting of all algebraic numbers over $\mathbf{Q}$ is an infinite extension of $\mathbf{Q}$.

If E is an extension of F, we denote by

$$[E : F]$$

the dimension of E as vector space over F. It may be infinite.

Proposition 1.2. *Let k be a field and $F \subset E$ extension fields of k. Then*

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

If $\{x_i\}_{i \in I}$ is a basis for F over k and $\{y_j\}_{j \in J}$ is a basis for E over F, then $\{x_i y_j\}_{(i,j) \in I \times J}$ is a basis for E over k.

Proof. Let $z \in E$. By hypothesis there exist elements $\alpha_j \in F$, almost all $\alpha_j = 0$, such that

$$z = \sum_{j \in J} \alpha_j y_j.$$

For each $j \in J$ there exist elements $b_{ji} \in k$, almost all of which are equal to 0, such that

$$\alpha_j = \sum_{i \in I} b_{ji} x_i,$$

and hence

$$z = \sum_j \sum_i b_{ji} x_i y_j.$$

This shows that $\{x_i y_j\}$ is a family of generators for E over k. We must show that it is linearly independent. Let $\{c_{ij}\}$ be a family of elements of k, almost all of which are 0, such that

$$\sum_j \sum_i c_{ij} x_i y_j = 0.$$

Then for each j,

$$\sum_i c_{ij} x_i = 0$$

because the elements y_j are linearly independent over F. Finally $c_{ij} = 0$ for each i because $\{x_i\}$ is a basis of F over k, thereby proving our proposition.

Corollary 1.3. *The extension E of k is finite if and only if E is finite over F and F is finite over k.*

As with groups, we define a **tower** of fields to be a sequence

$$F_1 \subset F_2 \subset \cdots \subset F_n$$

of extension fields. The tower is called **finite** if and only if each step is finite.

Let k be a field, E an extension field, and $\alpha \in E$. We denote by $k(\alpha)$ the smallest subfield of E containing both k and α. It consists of all quotients $f(\alpha)/g(\alpha)$, where f, g are polynomials with coefficients in k and $g(\alpha) \neq 0$.

Proposition 1.4. *Let α be algebraic over k. Then $k(\alpha) = k[\alpha]$, and $k(\alpha)$ is finite over k. The degree $[k(\alpha) : k]$ is equal to the degree of* $\operatorname{Irr}(\alpha, k, X)$.

Proof. Let $p(X) = \operatorname{Irr}(\alpha, k, X)$. Let $f(X) \in k[X]$ be such that $f(\alpha) \neq 0$. Then $p(X)$ does not divide $f(X)$, and hence there exist polynomials $g(X)$, $h(X) \in k[X]$ such that

$$g(X)p(X) + h(X)f(X) = 1.$$

From this we get $h(\alpha)f(\alpha) = 1$, and we see that $f(\alpha)$ is invertible in $k[\alpha]$. Hence $k[\alpha]$ is not only a ring but a field, and must therefore be equal to $k(\alpha)$. Let $d = \deg p(X)$. The powers

$$1, \alpha, \ldots, \alpha^{d-1}$$

are linearly independent over k, for otherwise suppose

$$a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} = 0$$

with $a_i \in k$, not all $a_i = 0$. Let $g(X) = a_0 + \cdots + a_{d-1}X^{d-1}$. Then $g \neq 0$ and $g(\alpha) = 0$. Hence $p(X)$ divides $g(X)$, contradiction. Finally, let $f(\alpha) \in k[\alpha]$, where $f(X) \in k[X]$. There exist polynomials $q(X)$, $r(X) \in k[X]$ such that $\deg r < d$ and

$$f(X) = q(X)p(X) + r(X).$$

Then $f(\alpha) = r(\alpha)$, and we see that $1, \alpha, \ldots, \alpha^{d-1}$ generate $k[\alpha]$ as a vector space over k. This proves our proposition.

Let E, F be extensions of a field k. If E and F are contained in some field L then we denote by EF the smallest subfield of L containing both E and F, and call it the **compositum** of E and F, in L. If E, F are not given as embedded in a common field L, then we cannot define the compositum.

Let k be a subfield of E and let $\alpha_1, \ldots, \alpha_n$ be elements of E. We denote by

$$k(\alpha_1, \ldots, \alpha_n)$$

the smallest subfield of E containing k and $\alpha_1, \ldots, \alpha_n$. Its elements consist of all quotients

$$\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$$

where f, g are polynomials in n variables with coefficients in k, and

$$g(\alpha_1, \ldots, \alpha_n) \neq 0.$$

Indeed, the set of such quotients forms a field containing k and $\alpha_1, \ldots, \alpha_n$. Conversely, any field containing k and

$$\alpha_1, \ldots, \alpha_n$$

must contain these quotients.

We observe that E is the union of all its subfields $k(\alpha_1, \ldots, \alpha_n)$ as $(\alpha_1, \ldots, \alpha_n)$ ranges over finite subfamilies of elements of E. We could define the *compositum of an arbitrary subfamily of subfields of a field* L as the smallest subfield containing all fields in the family. We say that E is **finitely generated** over k if there is a finite family of elements $\alpha_1, \ldots, \alpha_n$ of E such that

$$E = k(\alpha_1, \ldots, \alpha_n).$$

We see that E is the compositum of all its finitely generated subfields over k.

Proposition 1.5. *Let E be a finite extension of k. Then E is finitely generated.*

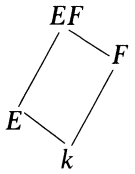
Proof. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of E as vector space over k. Then certainly

$$E = k(\alpha_1, \ldots, \alpha_n).$$

If $E = k(\alpha_1, \ldots, \alpha_n)$ is finitely generated, and F is an extension of k, both F, E contained in L, then

$$EF = F(\alpha_1, \ldots, \alpha_n),$$

and EF is finitely generated over F. We often draw the following picture:



Lines slanting up indicate an inclusion relation between fields. We also call the extension EF of F the **translation** of E to F, or also the **lifting** of E to F.

Let α be algebraic over the field k. Let F be an extension of k, and assume $k(\alpha)$, F both contained in some field L. Then α is algebraic over F. Indeed, the irreducible polynomial for α over k has *a fortiori* coefficients in F, and gives a linear relation for the powers of α over F.

Suppose that we have a tower of fields:

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \ldots, \alpha_n),$$

each one generated from the preceding field by a single element. Assume that each α_i is algebraic over k, $i = 1, \ldots, n$. As a special case of our preceding remark, we note that α_{i+1} is algebraic over $k(\alpha_1, \ldots, \alpha_i)$. Hence each step of the tower is algebraic.

Proposition 1.6. *Let $E = k(\alpha_1, \ldots, \alpha_n)$ be a finitely generated extension of a field k, and assume α_i algebraic over k for each $i = 1, \ldots, n$. Then E is finite algebraic over k.*

Proof. From the above remarks, we know that E can be obtained as the end of a tower each of whose steps is generated by one algebraic element, and is therefore finite by Proposition 1.4. We conclude that E is finite over k by Corollary 1.3, and that it is algebraic by Proposition 1.1.

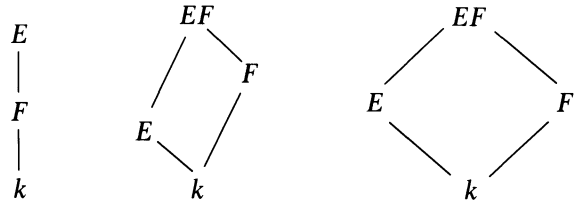
Let $\mathfrak{C}$ be a certain class of extension fields $F \subset E$. We shall say that $\mathfrak{C}$ is **distinguished** if it satisfies the following conditions:

(1) Let $k \subset F \subset E$ be a tower of fields. The extension $k \subset E$ is in $\mathfrak{C}$ if and only if $k \subset F$ is in $\mathfrak{C}$ and $F \subset E$ is in $\mathfrak{C}$.

(2) If $k \subset E$ is in $\mathfrak{C}$, if F is any extension of k, and E, F are both contained in some field, then $F \subset EF$ is in $\mathfrak{C}$.

(3) If $k \subset F$ and $k \subset E$ are in $\mathfrak{C}$ and F, E are subfields of a common field, then $k \subset FE$ is in $\mathfrak{C}$.

The diagrams illustrating our properties are as follows:



(1) (2) (3)

These lattice diagrams of fields are extremely suggestive in handling extension fields.

We observe that (3) follows formally from the first two conditions. Indeed, one views EF over k as a tower with steps $k \subset F \subset EF$.

As a matter of notation, it is convenient to write E/F instead of $F \subset E$ to denote an extension. There can be no confusion with factor groups since we shall never use the notation E/F to denote such a factor group when E is an extension field of F.

Proposition 1.7. *The class of algebraic extensions is distinguished, and so is the class of finite extensions.*

Proof. Consider first the class of finite extensions. We have already proved condition (1). As for (2), assume that E/k is finite, and let F be any extension of k. By Proposition 1.5 there exist elements $\alpha_1, \ldots, \alpha_n \in E$ such that $E = k(\alpha_1, \ldots, \alpha_n)$. Then $EF = F(\alpha_1, \ldots, \alpha_n)$, and hence EF/F is finitely generated by algebraic elements. Using Proposition 1.6 we conclude that EF/F is finite.

Consider next the class of algebraic extensions, and let

$$k \subset F \subset E$$

be a tower. Assume that E is algebraic over k. Then *a fortiori*, F is algebraic over k and E is algebraic over F. Conversely, assume each step in the tower to be algebraic. Let $\alpha \in E$. Then α satisfies an equation

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

with $a_i \in F$, not all $a_i = 0$. Let $F_0 = k(a_n, \ldots, a_0)$. Then F_0 is finite over k by Proposition 1.6, and α is algebraic over F_0. From the tower

$$k \subset F_0 = k(a_n, \ldots, a_0) \subset F_0(\alpha)$$

and the fact that each step in this tower is finite, we conclude that $F_0(\alpha)$ is finite over k, whence α is algebraic over k, thereby proving that E is algebraic over k and proving condition (1) for algebraic extensions. Condition (2) has already been observed to hold, i.e. an element remains algebraic under lifting, and hence so does an extension.

Remark. It is true that finitely generated extensions form a distinguished class, but one argument needed to prove part of (1) can be carried out only with more machinery than we have at present. Cf. the chapter on transcendental extensions.

§2. ALGEBRAIC CLOSURE

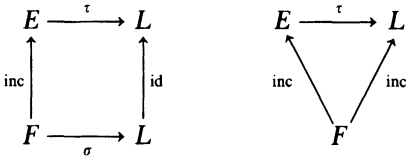
In this and the next section we shall deal with embeddings of a field into another. We therefore define some terminology.

Let E be an extension of a field F and let

$$\sigma: F \to L$$

be an embedding (i.e. an injective homomorphism) of F into L. Then σ induces an isomorphism of F with its image σF, which is sometimes written F^σ. An embedding τ of E in L will be said to be **over** σ if the restriction of τ to F is equal to σ. We also say that τ **extends** σ. If σ is the identity then we say that τ is an embedding of E **over** F.

These definitions could be made in more general categories, since they depend only on diagrams to make sense:



We shall use exponential notation (to avoid parentheses), so we write F^σ instead of σF, and f^σ instead of σf for a polynomial f, applying σ to the coefficients. Cf. Chapter II, §5.

Remark. Let $f(X) \in F[X]$ be a polynomial, and let α be a root of f in E. Say $f(X) = a_0 + \cdots + a_n X^n$. Then

$$0 = f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

If τ extends σ as above, then we see that $\tau\alpha$ is a root of f^σ because

$$0 = \tau(f(\alpha)) = a_0^\sigma + a_1^\sigma(\tau\alpha) + \cdots + a_n^\sigma(\tau\alpha)^n.$$

In our study of embeddings it will also be useful to have a lemma concerning embeddings of algebraic extensions into themselves. For this we note that if $\sigma: E \to L$ is an embedding over k (i.e. inducing the identity on k), then σ can be viewed as a k-homomorphism of vector spaces, because both E, L can be viewed as vector spaces over k. Furthermore σ is injective.

Lemma 2.1. *Let E be an algebraic extension of k, and let $\sigma: E \to E$ be an embedding of E into itself over k. Then σ is an automorphism.*

Proof. Since σ is injective, it will suffice to prove that σ is surjective. Let α be an element of E, let $p(X)$ be its irreducible polynomial over k, and let E' be the subfield of E generated by all the roots of $p(X)$ which lie in E. Then E' is finitely generated, hence is a finite extension of k. Furthermore, σ must map a root of $p(X)$ on a root of $p(X)$, and hence σ maps E' into itself. We can view σ as a k-homomorphism of vector spaces because σ induces the identity on k. Since σ is injective, its image $\sigma(E')$ is a subspace of E' having the same dimension $[E' : k]$. Hence $\sigma(E') = E'$. Since $\alpha \in E'$, it follows that α is in the image of σ, and our lemma is proved.

Let E, F be extensions of a field k, contained in some bigger field L. We can form the ring $E[F]$ generated by the elements of F over E. Then $E[F] = F[E]$, and EF is the quotient field of this ring. It is clear that the elements of $E[F]$ can be written in the form

$$a_1 b_1 + \cdots + a_n b_n$$

with $a_i \in E$ and $b_i \in F$. Hence EF is the field of quotients of these elements.

Lemma 2.2. *Let E_1, E_2 be extensions of a field k, contained in some bigger field E, and let σ be an embedding of E in some field L. Then*

$$\sigma(E_1 E_2) = \sigma(E_1)\sigma(E_2).$$

Proof. We apply σ to a quotient of elements of the above type, say

$$\sigma\left(\frac{a_1 b_1 + \cdots + a_n b_n}{a_1' b_1' + \cdots + a_m' b_m'}\right) = \frac{a_1^\sigma b_1^\sigma + \cdots + a_n^\sigma b_n^\sigma}{a_1'^\sigma b_1'^\sigma + \cdots + a_m'^\sigma b_m'^\sigma},$$

and see that the image is an element of $\sigma(E_1)\sigma(E_2)$. It is clear that the image $\sigma(E_1 E_2)$ is $\sigma(E_1)\sigma(E_2)$.

Let k be a field, $f(X)$ a polynomial of degree $\geqq 1$ in $k[X]$. We consider the problem of finding an extension E of k in which f has a root. If $p(X)$ is an irreducible polynomial in $k[X]$ which divides $f(X)$, then any root of $p(X)$ will also be a root of $f(X)$, so we may restrict ourselves to irreducible polynomials.

Let $p(X)$ be irreducible, and consider the canonical homomorphism

$$\sigma: k[X] \to k[X]/(p(X)).$$

Then σ induces a homomorphism on k, whose kernel is 0, because every nonzero element of k is invertible in k, generates the unit ideal, and 1 does not lie in the kernel. Let ξ be the image of X under σ, i.e. $\xi = \sigma(X)$ is the residue class of X mod $p(X)$. Then

$$p^\sigma(\xi) = p^\sigma(X^\sigma) = \big(p(X)\big)^\sigma = 0.$$

Hence ξ is a root of p^σ, and as such is algebraic over σk. We have now found an extension of σk, namely $\sigma k(\xi)$ in which p^σ has a root.

With a minor set-theoretic argument, we shall have:

Proposition 2.3. *Let k be a field and f a polynomial in $k[X]$ of degree $\geqq 1$. Then there exists an extension E of k in which f has a root.*

Proof. We may assume that $f = p$ is irreducible. We have shown that there exists a field F and an embedding

$$\sigma: k \to F$$

such that p^σ has a root ξ in F. Let S be a set whose cardinality is the same as that of $F - \sigma k$ (= the complement of σk in F) and which is disjoint from k. Let $E = k \cup S$. We can extend $\sigma: k \to F$ to a bijection of E on F. We now define a field structure on E. If $x, y \in E$ we define

$$xy = \sigma^{-1}(\sigma(x)\sigma(y)),$$

$$x + y = \sigma^{-1}(\sigma(x) + \sigma(y)).$$

Restricted to k, our addition and multiplication coincide with the given addition and multiplication of our original field k, and it is clear that k is a subfield of E. We let $\alpha = \sigma^{-1}(\xi)$. Then it is also clear that $p(\alpha) = 0$, as desired.

Corollary 2.4. *Let k be a field and let $f_1, \ldots, f_n$ be polynomials in $k[X]$ of degrees $\geqq 1$. Then there exists an extension E of k in which each f_i has a root, $i = 1, \ldots, n$.*

Proof. Let E_1 be an extension in which f_1 has a root. We may view f_2 as a polynomial over E_1. Let E_2 be an extension of E_1 in which f_2 has a root. Proceeding inductively, our corollary follows at once.

We define a field L to be **algebraically closed** if every polynomial in $L[X]$ of degree $\geqq 1$ has a root in L.

Theorem 2.5. *Let k be a field. Then there exists an algebraically closed field containing k as a subfield.*

Proof. We first construct an extension E_1 of k in which every polynomial in $k[X]$ of degree $\geqq 1$ has a root. One can proceed as follows (Artin). To each polynomial f in $k[X]$ of degree $\geqq 1$ we associate a letter X_f and we let S be the set of all such letters X_f (so that S is in bijection with the set of polynomials in $k[X]$ of degree $\geqq 1$). We form the polynomial ring $k[S]$, and contend that the ideal generated by all the polynomials $f(X_f)$ in $k[S]$ is not the unit ideal. If it is, then there is a finite combination of elements in our ideal which is equal to 1:

$$g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) = 1$$

with $g_i \in k[S]$. For simplicity, write X_i instead of X_{f_i}. The polynomials g_i will involve actually only a finite number of variables, say $X_1, \ldots, X_N$ (with $N \geqq n$). Our relation then reads

$$\sum_{i=1}^{n} g_i(X_1, \ldots, X_N) f_i(X_i) = 1.$$

Let F be a finite extension in which each polynomial $f_1, \ldots, f_n$ has a root, say α_i is a root of f_i in F, for $i = 1, \ldots, n$. Let $\alpha_i = 0$ for $i > n$. Substitute α_i for X_i in our relation. We get $0 = 1$, contradiction.

Let $\mathfrak{m}$ be a maximal ideal containing the ideal generated by all polynomials $f(X_f)$ in $k[S]$. Then $k[S]/\mathfrak{m}$ is a field, and we have a canonical map

$$\sigma: k[S] \to k[S]/\mathfrak{m}.$$

For any polynomial $f \in k[X]$ of degree $\geqq 1$, the polynomial f^σ has a root in $k[S]/\mathfrak{m}$, which is an extension of σk. Using the same type of set-theoretic argument as in Proposition 2.3, we conclude that there exists an extension E_1 of k in which every polynomial $f \in k[X]$ of degree $\geqq 1$ has a root in E_1.

Inductively, we can form a sequence of fields

$$E_1 \subset E_2 \subset E_3 \subset \cdots \subset E_n \cdots$$

such that every polynomial in $E_n[X]$ of degree $\geqq 1$ has a root in E_{n+1}. Let E be the union of all fields E_n, $n = 1, 2, \ldots$. Then E is naturally a field, for if $x, y \in E$ then there exists some n such that $x, y \in E_n$, and we can take the product or sum xy or $x + y$ in E_n. This is obviously independent of the choice of n such that $x, y \in E_n$, and defines a field structure on E. Every polynomial in $E[X]$ has its coefficients in some subfield E_n, hence a root in E_{n+1}, hence a root in E, as desired.

Corollary 2.6. *Let k be a field. There exists an extension k^a which is algebraic over k and algebraically closed.*

Proof. Let E be an extension of k which is algebraically closed and let k^a be the union of all subextensions of E, which are algebraic over k. Then k^a is algebraic over k. If $\alpha \in E$ and α is algebraic over k^a then α is algebraic over k by Proposition 1.7. If f is a polynomial of degree $\geqq 1$ in $k^a[X]$, then f has a root α in E, and α is algebraic over k^a. Hence α is in k^a and k^a is algebraically closed.

We observe that if L is an algebraically closed field, and $f \in L[X]$ has degree $\geqq 1$, then there exists $c \in L$ and $\alpha_1, \ldots, \alpha_n \in L$ such that

$$f(X) = c(X - \alpha_1) \cdots (X - \alpha_n).$$

Indeed, f has a root α_1 in L, so there exists $g(X) \in L[X]$ such that

$$f(X) = (X - \alpha_1) g(X).$$

If $\deg g \geqq 1$, we can repeat this argument inductively, and express f as a

product of terms $(X - \alpha_i)$ $(i = 1, \ldots, n)$ and an element $c \in L$. Note that c is the leading coefficient of f, i.e.

$$f(X) = cX^n + \text{terms of lower degree.}$$

Hence if the coefficients of f lie in a subfield k of L, then $c \in k$.

Let k be a field and $\sigma: k \to L$ an embedding of k into an algebraically closed field L. We are interested in analyzing the extensions of σ to algebraic extensions E of k. We begin by considering the special case when E is generated by one element.

Let $E = k(\alpha)$ where α is algebraic over k. Let

$$p(X) = \operatorname{Irr}(\alpha, k, X).$$

Let β be a root of p^σ in L. Given an element of $k(\alpha) = k[\alpha]$, we can write it in the form $f(\alpha)$ with some polynomial $f(X) \in k[X]$. We define an extension of σ by mapping

$$f(\alpha) \mapsto f^\sigma(\beta).$$

This is in fact well defined, i.e. independent of the choice of polynomial $f(X)$ used to express our element in $k[\alpha]$. Indeed, if $g(X)$ is in $k[X]$ and such that $g(\alpha) = f(\alpha)$, then $(g - f)(\alpha) = 0$, whence $p(X)$ divides $g(X) - f(X)$. Hence $p^\sigma(X)$ divides $g^\sigma(X) - f^\sigma(X)$, and thus $g^\sigma(\beta) = f^\sigma(\beta)$. It is now clear that our map is a homomorphism inducing σ on k, and that it is an extension of σ to $k(\alpha)$. Hence we get:

Proposition 2.7. *The number of possible extensions of σ to $k(\alpha)$ is $\leqq \deg p$, and is equal to the number of distinct roots of p in k^a.*

This is an important fact, which we shall analyze more closely later. For the moment, we are interested in extensions of σ to arbitrary algebraic extensions of k. We get them by using Zorn's lemma.

Theorem 2.8. *Let k be a field, E an algebraic extension of k, and $\sigma: k \to L$ an embedding of k into an algebraically closed field L. Then there exists an extension of σ to an embedding of E in L. If E is algebraically closed and L is algebraic over σk, then any such extension of σ is an isomorphism of E onto L.*

Proof. Let S be the set of all pairs (F, τ) where F is a subfield of E containing k, and τ is an extension of σ to an embedding of F in L. If (F, τ) and (F', τ') are such pairs, we write $(F, \tau) \leqq (F', \tau')$ if $F \subset F'$ and $\tau' | F = \tau$. Note that S is not empty [it contains (k, σ)], and is inductively ordered: If $\{(F_i, \tau_i)\}$ is a totally ordered subset, we let $F = \bigcup F_i$ and define τ on F to be equal to τ_i on each F_i. Then (F, τ) is an upper bound for the totally ordered subset. Using Zorn's lemma, let (K, λ) be a maximal element in S. Then λ is an extension of σ, and we contend that $K = E$. Otherwise, there exists $\alpha \in E$,

$\alpha \notin K$. By what we saw above, our embedding λ has an extension to $K(\alpha)$, thereby contradicting the maximality of (K, λ). This proves that there exists an extension of σ to E. We denote this extension again by σ.

If E is algebraically closed, and L is algebraic over σk, then σE is algebraically closed and L is algebraic over σE, hence $L = \sigma E$.

As a corollary, we have a certain uniqueness for an "algebraic closure" of a field k.

Corollary 2.9. *Let k be a field and let E, E' be algebraic extensions of k. Assume that E, E' are algebraically closed. Then there exists an isomorphism*

$$\tau: E \to E'$$

of E onto E' inducing the identity on k.

Proof. Extend the identity mapping on k to an embedding of E into E' and apply the theorem.

We see that an algebraically closed and algebraic extension of k is determined up to an isomorphism. Such an extension will be called an **algebraic closure** of k, and we frequently denote it by k^a. In fact, unless otherwise specified, we use the symbol k^a only to denote algebraic closure.

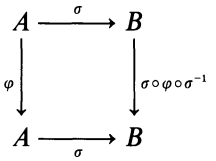
It is now worth while to recall the general situation of isomorphisms and automorphisms in general categories.

Let $\mathfrak{C}$ be a category, and A, B objects in $\mathfrak{C}$. We denote by $\mathrm{Iso}(A, B)$ the set of isomorphisms of A on B. Suppose there exists at least one such isomorphism $\sigma: A \to B$, with inverse $\sigma^{-1}: B \to A$. If φ is an automorphism of A, then $\sigma \circ \varphi: A \to B$ is again an isomorphism. If ψ is an automorphism of B, then $\psi \circ \sigma: A \to B$ is again an isomorphism. Furthermore, the groups of automorphisms $\mathrm{Aut}(A)$ and $\mathrm{Aut}(B)$ are isomorphic, under the mappings

$$\varphi \mapsto \sigma \circ \varphi \circ \sigma^{-1},$$

$$\sigma^{-1} \circ \psi \circ \sigma \hookleftarrow \psi,$$

which are inverse to each other. The isomorphism $\sigma \circ \varphi \circ \sigma^{-1}$ is the one which makes the following diagram commutative:



We have a similar diagram for $\sigma^{-1} \circ \psi \circ \sigma$.

Let $\tau: A \to B$ be another isomorphism. Then $\tau^{-1} \circ \sigma$ is an automorphism of A, and $\tau \circ \sigma^{-1}$ is an automorphism of B. Thus two isomorphisms differ by an automorphism (of A or B). We see that the group $\mathrm{Aut}(B)$ operates on the

set $\mathrm{Iso}(A, B)$ on the left, and $\mathrm{Aut}(A)$ operates on the set $\mathrm{Iso}(A, B)$ on the right.

We also see that $\mathrm{Aut}(A)$ is determined up to a mapping analogous to a conjugation. This is quite different from the type of uniqueness given by universal objects in a category. Such objects have only the identity automorphism, and hence are determined up to a unique isomorphism.

This is not the case with the algebraic closure of a field, which usually has a large amount of automorphisms. Most of this chapter and the next is devoted to the study of such automorphisms.

Examples. It will be proved later in this book that the complex numbers are algebraically closed. Complex conjugation is an automorphism of $\mathbf{C}$. There are many more automorphisms, but the other automorphisms $\neq \mathrm{id}$. are not continuous. We shall discuss other possible automorphisms in the chapter on transcendental extensions. The subfield of $\mathbf{C}$ consisting of all numbers which are algebraic over $\mathbf{Q}$ is an algebraic closure $\mathbf{Q}^a$ of $\mathbf{Q}$. It is easy to see that $\mathbf{Q}^a$ is denumerable. In fact, prove the following as an exercise:

If k is a field which is not finite, then any algebraic extension of k has the same cardinality as k.

If k is denumerable, one can first enumerate all polynomials in k, then enumerate finite extensions by their degree, and finally enumerate the cardinality of an arbitrary algebraic extension. We leave the counting details as exercises.

In particular, $\mathbf{Q}^a \neq \mathbf{C}$. If $\mathbf{R}$ is the field of real numbers, then $\mathbf{R}^a = \mathbf{C}$.

If k is a finite field, then algebraic closure k^a of k is denumerable. We shall in fact describe in great detail the nature of algebraic extensions of finite fields later in this chapter.

Not all interesting fields are subfields of the complex numbers. For instance, one wants to investigate the algebraic extensions of a field $\mathbf{C}(X)$ where X is a variable over $\mathbf{C}$. The study of these extensions amounts to the study of ramified coverings of the sphere (viewed as a Riemann surface), and in fact one has precise information concerning the nature of such extensions, because one knows the fundamental group of the sphere from which a finite number of points has been deleted. We shall mention this example again later when we discuss Galois groups.

§3. SPLITTING FIELDS AND NORMAL EXTENSIONS

Let k be a field and let f be a polynomial in $k[X]$ of degree $\geqq 1$. By a **splitting field** K of f we shall mean an extension K of k such that f splits into linear factors in K, i.e.

$$f(X) = c(X - \alpha_1) \cdots (X - \alpha_n)$$

with $\alpha_i \in K$, $i = 1, \ldots, n$, and such that $K = k(\alpha_1, \ldots, \alpha_n)$ is generated by all the roots of f.

Theorem 3.1. *Let K be a splitting field of the polynomial $f(X) \in k[X]$. If E is another splitting field of f, then there exists an isomorphism $\sigma: E \to K$ inducing the identity on k. If $k \subset K \subset k^a$, where k^a is an algebraic closure of k, then any embedding of E in k^a inducing the identity on k must be an isomorphism of E onto K.*

Proof. Let K^a be an algebraic closure of K. Then K^a is algebraic over k, hence is an algebraic closure of k. By Theorem 2.8 there exists an embedding

$$\sigma: E \to K^a$$

inducing the identity on k. We have a factorization

$$f(X) = c(X - \beta_1) \cdots (X - \beta_n)$$

with $\beta_i \in E$, $i = 1, \ldots, n$. The leading coefficient c lies in k. We obtain

$$f(X) = f^\sigma(X) = c(X - \sigma\beta_1) \cdots (X - \sigma\beta_n).$$

We have unique factorization in $K^a[X]$. Since f has a factorization

$$f(X) = c(X - \alpha_1) \cdots (X - \alpha_n)$$

in $K[X]$, it follows that $(\sigma\beta_1, \ldots, \sigma\beta_n)$ differs from $(\alpha_1, \ldots, \alpha_n)$ by a permutation. From this we conclude that $\sigma\beta_i \in K$ for $i = 1, \ldots, n$ and hence that $\sigma E \subset K$. But $K = k(\alpha_1, \ldots, \alpha_n) = k(\sigma\beta_1, \ldots, \sigma\beta_n)$, and hence $\sigma E = K$, because

$$E = k(\beta_1, \ldots, \beta_n).$$

This proves our theorem.

We note that a polynomial $f(X) \in k[X]$ always has a splitting field, namely the field generated by its roots in a given algebraic closure k^a of k.

Let I be a set of indices and let $\{f_i\}_{i \in I}$ be a family of polynomials in $k[X]$, of degrees $\geqq 1$. By a **splitting field** for this family we shall mean an extension K of k such that every f_i splits in linear factors in $K[X]$, and K is generated by all the roots of all the polynomials f_i, $i \in I$. In most applications we deal with a finite indexing set I, but it is becoming increasingly important to consider infinite algebraic extensions, and so we shall deal with them fairly systematically. One should also observe that the proofs we shall give for various statements would not be simpler if we restricted ourselves to the finite case.

Let k^a be an algebraic closure of k, and let K_i be a splitting field of f_i in k^a. Then the compositum of the K_i is a splitting field for our family,

since the two conditions defining a splitting field are immediately satisfied. Furthermore Theorem 3.1 extends at once to the infinite case:

Corollary 3.2. *Let K be a splitting field for the family $\{f_i\}_{i \in I}$ and let E be another splitting field. Any embedding of E into K^a inducing the identity on k gives an isomorphism of E onto K.*

Proof. Let the notation be as above. Note that E contains a unique splitting field E_i of f_i and K contains a unique splitting field K_i of f_i. Any embedding σ of E into K^a must map E_i onto K_i by Theorem 3.1, and hence maps E into K. Since K is the compositum of the fields K_i, our map σ must send E onto K and hence induces an isomorphism of E onto K.

Remark. If I is finite, and our polynomials are $f_1, \ldots, f_n$, then a splitting field for them is a splitting field for the single polynomial $f(X) = f_1(X) \cdots f_n(X)$ obtained by taking the product. However, even when dealing with finite extensions only, it is convenient to deal simultaneously with sets of polynomials rather than a single one.

Theorem 3.3. *Let K be an algebraic extension of k, contained in an algebraic closure k^a of k. Then the following conditions are equivalent:*

NOR 1. *Every embedding of K in k^a over k induces an automorphism of K.*

NOR 2. *K is the splitting field of a family of polynomials in $k[X]$.*

NOR 3. *Every irreducible polynomial of $k[X]$ which has a root in K splits into linear factors in K.*

Proof. Assume **NOR 1**. Let α be an element of K and let $p_\alpha(X)$ be its irreducible polynomial over k. Let β be a root of p_α in k^a. There exists an isomorphism of $k(\alpha)$ on $k(\beta)$ over k, mapping α on β. Extend this isomorphism to an embedding of K in k^a. This extension is an automorphism σ of K by hypothesis, hence $\sigma\alpha = \beta$ lies in K. Hence every root of p_α lies in K, and p_α splits in linear factors in $K[X]$. Hence K is the splitting field of the family $\{p_\alpha\}_{\alpha \in K}$ as α ranges over all elements of K, and **NOR 2** is satisfied.

Conversely, assume **NOR 2**, and let $\{f_i\}_{i \in I}$ be the family of polynomials of which K is the splitting field. If α is a root of some f_i in K, then for any embedding σ of K in k^a over k we know that $\sigma\alpha$ is a root of f_i. Since K is generated by the roots of all the polynomials f_i, it follows that σ maps K into itself. We now apply Lemma 2.1 to conclude that σ is an automorphism.

Our proof that **NOR 1** implies **NOR 2** also shows that **NOR 3** is satisfied. Conversely, assume **NOR 3**. Let σ be an embedding of K in k^a over k. Let $\alpha \in K$ and let $p(X)$ be its irreducible polynomial over k. If σ is an embedding of K in k^a over k then σ maps α on a root β of $p(X)$, and by hypothesis β lies in K. Hence $\sigma\alpha$ lies in K, and σ maps K into itself. By Lemma 2.1, it follows that σ is an automorphism.

An extension K of k satisfying the hypotheses **NOR 1**, **NOR 2**, **NOR 3** will be said to be **normal**. It is not true that the class of normal extensions is distinguished. For instance, it is easily shown that an extension of degree 2 is normal, but the extension $\mathbf{Q}(\sqrt[4]{2})$ of the rational numbers is not normal (the complex roots of $X^4 - 2$ are not in it), and yet this extension is obtained by successive extensions of degree 2, namely

$$E = \mathbf{Q}(\sqrt[4]{2}) \supset F \supset \mathbf{Q},$$

where

$$F = \mathbf{Q}(\alpha), \qquad \alpha = \sqrt{2} \quad \text{and} \quad E = F(\sqrt{\alpha}).$$

Thus a tower of normal extensions is not necessarily normal. However, we still have some of the properties:

Theorem 3.4. *Normal extensions remain normal under lifting. If $K \supset E \supset k$ and K is normal over k, then K is normal over E. If K_1, K_2 are normal over k and are contained in some field L, then K_1K_2 is normal over k, and so is $K_1 \cap K_2$.*

Proof. For our first assertion, let K be normal over k, let F be any extension of k, and assume K, F are contained in some bigger field. Let σ be an embedding of KF over F (in F^a). Then σ induces the identity on F, hence on k, and by hypothesis its restriction to K maps K into itself. We get $(KF)^\sigma = K^\sigma F^\sigma = KF$ whence KF is normal over F.

Assume that $K \supset E \supset k$ and that K is normal over k. Let σ be an embedding of K over E. Then σ is also an embedding of K over k, and our assertion follows by definition.

Finally, if K_1, K_2 are normal over k, then for any embedding σ of K_1K_2 over k we have

$$\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2)$$

and our assertion again follows from the hypothesis. The assertion concerning the intersection is true because

$$\sigma(K_1 \cap K_2) = \sigma(K_1) \cap \sigma(K_2).$$

We observe that if K is a finitely generated normal extension of k, say

$$K = k(\alpha_1, \ldots, \alpha_n),$$

and $p_1, \ldots, p_n$ are the respective irreducible polynomials of $\alpha_1, \ldots, \alpha_n$ over k then K is already the splitting field of the finite family $p_1, \ldots, p_n$. We shall investigate later when K is the splitting field of a single irreducible polynomial.

§4. SEPARABLE EXTENSIONS

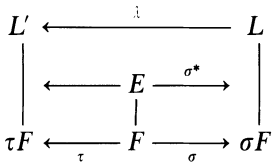
Let E be an algebraic extension of a field F and let

$$\sigma: F \to L$$

be an embedding of F in an algebraically closed field L. We investigate more closely extensions of σ to E. Any such extension of σ maps E on a subfield of L which is algebraic over σF. Hence for our purposes, we shall assume that L is algebraic over σF, hence is equal to an algebraic closure of σF.

Let S_σ be the set of extensions of σ to an embedding of E in L.

Let L' be another algebraically closed field, and let $\tau: F \to L'$ be an embedding. We assume as before that L' is an algebraic closure of τF. By Theorem 2.8, there exists an isomorphism $\lambda: L \to L'$ extending the map $\tau \circ \sigma^{-1}$ applied to the field σF. This is illustrated in the following diagram:



We let S_τ be the set of embeddings of E in L' extending τ.

If $\sigma^* \in S_\sigma$ is an extension of σ to an embedding of E in L, then $\lambda \circ \sigma^*$ is an extension of τ to an embedding of E into L', because for the restriction to F we have

$$\lambda \circ \sigma^* = \tau \circ \sigma^{-1} \circ \sigma = \tau.$$

Thus λ induces a mapping from S_σ into S_τ. It is clear that the inverse mapping is induced by λ^{-1}, and hence that S_σ, S_τ are in bijection under the mapping

$$\sigma^* \mapsto \lambda \circ \sigma^*.$$

In particular, the cardinality of S_σ, S_τ is the same. Thus this cardinality depends only on the extension E/F, and will be denoted by

$$[E:F]_s.$$

We shall call it the **separable degree** of E over F. It is mostly interesting when E/F is finite.

Theorem 4.1. *Let $E \supset F \supset k$ be a tower. Then*

$$[E:k]_s = [E:F]_s[F:k]_s.$$

Furthermore, if E is finite over k, then $[E:k]_s$ is finite and

$$[E:k]_s \leqq [E:k].$$

The separable degree is at most equal to the degree.

Proof. Let $\sigma: k \to L$ be an embedding of k in an algebraically closed field L. Let $\{\sigma_i\}_{i \in I}$ be the family of distinct extensions of σ to F, and for each i, let $\{\tau_{ij}\}$ be the family of distinct extensions of σ_i to E. By what we saw before, each σ_i has precisely $[E:F]_s$ extensions to embeddings of E in L. The set of embeddings $\{\tau_{ij}\}$ contains precisely

$$[E:F]_s[F:k]_s$$

elements. Any embedding of E into L over σ must be one of the τ_{ij}, and thus we see that the first formula holds, i.e. we have multiplicativity in towers.

As to the second, let us assume that E/k is finite. Then we can obtain E as a tower of extensions, each step being generated by one element:

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \ldots, \alpha_r) = E.$$

If we define inductively $F_{v+1} = F_v(\alpha_{v+1})$ then by Proposition 2.7,

$$[F_v(\alpha_{v+1}):F_v]_s \leqq [F_v(\alpha_{v+1}):F_v].$$

Thus our inequality is true in each step of the tower. By multiplicativity, it follows that the inequality is true for the extension E/k, as was to be shown.

Corollary 4.2. *Let E be finite over k, and $E \supset F \supset k$. The equality*

$$[E:k]_s = [E:k]$$

holds if and only if the corresponding equality holds in each step of the tower, i.e. for E/F and F/k.

Proof. Clear.

It will be shown later (and it is not difficult to show) that $[E:k]_s$ divides the degree $[E:k]$ when E is finite over k. We define $[E:k]_i$ to be the quotient, so that

$$[E:k]_s[E:k]_i = [E:k].$$

It then follows from the multiplicativity of the separable degree and of the degree in towers that the symbol $[E:k]_i$ is also multiplicative in towers. We shall deal with it at greater length in §6.

Let E be a finite extension of k. We shall say that E is **separable** over k if $[E:k]_s = [E:k]$.

An element α algebraic over k is said to be **separable** over k if $k(\alpha)$ is separable over k. We see that this condition is equivalent to saying that the irreducible polynomial $\mathrm{Irr}(\alpha, k, X)$ has no multiple roots.

A polynomial $f(X) \in k[X]$ is called **separable** if it has no multiple roots.

If α is a root of a separable polynomial $g(X) \in k[X]$ then the irreducible polynomial of α over k divides g and hence α is separable over k.

We note that if $k \subset F \subset K$ and $\alpha \in K$ is separable over k, then α is separable over F. Indeed, if f is a separable polynomial in $k[X]$ such that $f(\alpha) = 0$, then f also has coefficients in F, and thus α is separable over F. (We may say that a separable element remains separable under lifting.)

Theorem 4.3. *Let E be a finite extension of k. Then E is separable over k if and only if each element of E is separable over k.*

Proof. Assume E is separable over k and let $\alpha \in E$. We consider the tower

$$k \subset k(\alpha) \subset E.$$

By Corollary 4.2, we must have $[k(\alpha):k] = [k(\alpha):k]_s$ whence α is separable over k. Conversely, assume that each element of E is separable over k. We can write $E = k(\alpha_1, \ldots, \alpha_n)$ where each α_i is separable over k. We consider the tower

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \ldots, \alpha_n).$$

Since each α_i is separable over k, each α_i is separable over $k(\alpha_1, \ldots, \alpha_{i-1})$ for $i \geqq 2$. Hence by the tower theorem, it follows that E is separable over k.

We observe that our last argument shows: If E is generated by a finite number of elements, each of which is separable over k, then E is separable over k.

Let E be an arbitrary algebraic extension of k. We define E to be **separable** over k if every finitely generated subextension is separable over k, i.e., if every extension $k(\alpha_1, \ldots, \alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in E$ is separable over k.

Theorem 4.4. *Let E be an algebraic extension of k, generated by a family of elements $\{\alpha_i\}_{i \in I}$. If each α_i is separable over k then E is separable over k.*

Proof. Every element of E lies in some finitely generated subfield

$$k(\alpha_{i_1}, \ldots, a_{i_n}),$$

and as we remarked above, each such subfield is separable over k. Hence every element of E is separable over k by Theorem 4.3, and this concludes the proof.

Theorem 4.5. *Separable extensions form a distinguished class of extensions.*

Proof. Assume that E is separable over k and let $E \supset F \supset k$. Every element of E is separable over F, and every element of F is an element of E, so separable over k. Hence each step in the tower is separable. Conversely, assume that $E \supset F \supset k$ is some extension such that E/F is separable and F/k is separable. If E is finite over k, then we can use Corollary 4.2. Namely, we have an equality of the separable degree and the degree in each step of the tower, whence an equality for E over k by multiplicativity.

If E is infinite, let $\alpha \in E$. Then α is a root of a separable polynomial $f(X)$ with coefficients in F. Let these coefficients be $a_n, \ldots, a_0$. Let $F_0 = k(a_n, \ldots, a_0)$. Then F_0 is separable over k, and α is separable over F_0. We now deal with the finite tower

$$k \subset F_0 \subset F_0(\alpha)$$

and we therefore conclude that $F_0(\alpha)$ is separable over k, hence that α is separable over k. This proves condition (1) in the definition of "distinguished."

Let E be separable over k. Let F be any extension of k, and assume that E, F are both subfields of some field. Every element of E is separable over k, whence separable over F. Since EF is generated over F by all the elements of E, it follows that EF is separable over F, by Theorem 4.4. This proves condition (2) in the definition of "distinguished," and concludes the proof of our theorem.

Let E be a finite extension of k. The intersection of all normal extensions K of k (in an algebraic closure E^a) containing E is a normal extension of k which contains E, and is obviously the smallest normal extension of k containing E. If $\sigma_1, \ldots, \sigma_n$ are the distinct embeddings of E in E^a, then the extension

$$K = (\sigma_1 E)(\sigma_2 E) \cdots (\sigma_n E),$$

which is the compositum of all these embeddings, is a normal extension of k, because for any embedding of it, say τ, we can apply τ to each extension $\sigma_i E$. Then $(\tau\sigma_1, \ldots, \tau\sigma_n)$ is a permutation of $(\sigma_1, \ldots, \sigma_n)$ and thus τ maps K into itself. Any normal extension of k containing E must contain $\sigma_i E$ for each i, and thus *the smallest normal extension of k containing E is precisely equal to the compositum*

$$(\sigma_1 E) \cdots (\sigma_n E).$$

If E is separable over k, then from Theorem 4.5 and induction we conclude that the smallest normal extension of k containing E is also separable over k.

Similar results hold for an infinite algebraic extension E of k, taking an infinite compositum.

In light of Theorem 4.5, the compositum of all separable extensions of a field k in a given algebraic closure k^a is a separable extension, which will be denoted by k^s or k^{sep}, and will be called the **separable closure** of k. As a matter of terminology, if E is an algebraic extension of k, and σ any embedding of E in k^a over k, then we call σE a **conjugate** of E in k^a. *We can say that the smallest normal extension of k containing E is the compositum of all the conjugates of E in E^a.*

Let α be algebraic over k. If $\sigma_1, \ldots, \sigma_r$ are the distinct embeddings of $k(\alpha)$ into k^a over k, then we call $\sigma_1\alpha, \ldots, \sigma_r\alpha$ the **conjugates** of α in k^a. These elements are simply the distinct roots of the irreducible polynomial of α over k. The smallest normal extension of k containing one of these conjugates is simply $k(\sigma_1\alpha, \ldots, \sigma_r\alpha)$.

Theorem 4.6. (Primitive Element Theorem). *Let E be a finite extension of a field k. There exists an element $\alpha \in E$ such that $E = k(\alpha)$ if and only if there exists only a finite number of fields F such that $k \subset F \subset E$. If E is separable over k, then there exists such an element α.*

Proof. If k is finite, then we know that the multiplicative group of E is generated by one element, which will therefore also generate E over k. We assume that k is infinite.

Assume that there is only a finite number of fields, intermediate between k and E. Let $\alpha, \beta \in E$. As c ranges over elements of k, we can only have a finite number of fields of type $k(\alpha + c\beta)$. Hence there exist elements c_1, $c_2 \in k$ with $c_1 \neq c_2$ such that

$$k(\alpha + c_1\beta) = k(\alpha + c_2\beta).$$

Note that $\alpha + c_1\beta$ and $\alpha + c_2\beta$ are in the same field, whence so is $(c_1 - c_2)\beta$, and hence so is β. Thus α is also in that field, and we see that $k(\alpha, \beta)$ can be generated by one element.

Proceeding inductively, if $E = k(\alpha_1, \ldots, \alpha_n)$ then there will exist elements $c_2, \ldots, c_n \in k$ such that

$$E = k(\xi)$$

where $\xi = \alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$. This proves half of our theorem.

Conversely, assume that $E = k(\alpha)$ for some α, and let $f(X) = \mathrm{Irr}(\alpha, k, X)$. Let $k \subset F \subset E$. Let $g_F(X) = \mathrm{Irr}(\alpha, F, X)$. Then g_F divides f. We have unique factorization in $E[X]$, and any polynomial in $E[X]$ which has leading coefficient 1 and divides $f(X)$ is equal to a product of factors $(X - \alpha_i)$ where $\alpha_1, \ldots, \alpha_n$ are the roots of f in a fixed algebraic closure. Hence there is only a finite number of such polynomials. Thus we get a mapping

$$F \mapsto g_F$$

from the set of intermediate fields into a finite set of polynomials. Let F_0 be

the subfield of F generated over k by the coefficients of $g_F(X)$. Then g_F has coefficients in F_0 and is irreducible over F_0 since it is irreducible over F. Hence the degree of α over F_0 is the same as the degree of α over F. Hence $F = F_0$. Thus our field F is uniquely determined by its associated polynomials g_F, and our mapping is therefore injective. This proves the first assertion of the theorem.

As to the statement concerning separable extensions, using induction, we may assume without loss of generality that $E = k(\alpha, \beta)$ where α, β are separable over k. Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of $k(\alpha, \beta)$ in k^a over k. Let

$$P(X) = \prod_{i \neq j} (\sigma_i\alpha + X\sigma_i\beta - \sigma_j\alpha - X\sigma_j\beta).$$

Then $P(X)$ is not the zero polynomial, and hence there exists $c \in k$ such that $P(c) \neq 0$. Then the elements $\sigma_i(\alpha + c\beta)$ $(i = 1, \ldots, n)$ are distinct, whence $k(\alpha + c\beta)$ has degree at least n over k. But $n = [k(\alpha, \beta) : k]$, and hence

$$k(\alpha, \beta) = k(\alpha + c\beta),$$

as desired.

If $E = k(\alpha)$, then we say that α is a **primitive element** of E (over k).

§5. FINITE FIELDS

We have developed enough general theorems to describe the structure of finite fields. This is interesting for its own sake, and also gives us examples for the general theory.

Let F be a finite field with q elements. As we have noted previously, we have a homomorphism

$$\mathbf{Z} \to F$$

sending 1 on 1, whose kernel cannot be 0, and hence is a principal ideal generated by a prime number p since $\mathbf{Z}/p\mathbf{Z}$ is embedded in F and F has no divisors of zero. Thus F has characteristic p, and contains a field isomorphic to $\mathbf{Z}/p\mathbf{Z}$.

We remark that $\mathbf{Z}/p\mathbf{Z}$ has no automorphisms other than the identity. Indeed, any automorphism must map 1 on 1, hence leaves every element fixed because 1 generates $\mathbf{Z}/p\mathbf{Z}$ additively. We identify $\mathbf{Z}/p\mathbf{Z}$ with its image in F. Then F is a vector space over $\mathbf{Z}/p\mathbf{Z}$, and this vector space must be

finite since F is finite. Let its degree be n. Let $\omega_1, \ldots, \omega_n$ be a basis for F over $\mathbf{Z}/p\mathbf{Z}$. Every element of F has a unique expression of the form

$$a_1\omega_1 + \cdots + a_n\omega_n$$

with $a_i \in \mathbf{Z}/p\mathbf{Z}$. Hence $q = p^n$.

The multiplicative group F^* of F has order $q - 1$. Every $\alpha \in F^*$ satisfies the equation $X^{q-1} = 1$. Hence every element of F satisfies the equation

$$f(X) = X^q - X = 0.$$

This implies that the polynomial $f(X)$ has q distinct roots in F, namely all elements of F. Hence f splits into factors of degree 1 in F, namely

$$X^q - X = \prod_{\alpha \in F} (X - \alpha).$$

In particular, F is a splitting field for f. But a splitting field is uniquely determined up to an isomorphism. Hence if a finite field of order p^n exists, it is uniquely determined, up to an isomorphism, as the splitting field of $X^{p^n} - X$ over $\mathbf{Z}/p\mathbf{Z}$.

As a matter of notation, we denote $\mathbf{Z}/p\mathbf{Z}$ by $\mathbf{F}_p$. Let n be an integer $\geqq 1$ and consider the splitting field of

$$X^{p^n} - X = f(X)$$

in an algebraic closure $\mathbf{F}_p^a$. We contend that this splitting field is the set of roots of $f(X)$ in $\mathbf{F}_p^a$. Indeed, let α, β be roots. Then

$$(\alpha + \beta)^{p^n} - (\alpha + \beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0,$$

whence $\alpha + \beta$ is a root. Also,

$$(\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0,$$

and $\alpha\beta$ is a root. Note that 0, 1 are roots of $f(X)$. If $\beta \neq 0$ then

$$(\beta^{-1})^{p^n} - \beta^{-1} = (\beta^{p^n})^{-1} - \beta^{-1} = 0$$

so that β^{-1} is a root. Finally,

$$(-\beta)^{p^n} - (-\beta) = (-1)^{p^n}\beta^{p^n} + \beta.$$

If p is odd, then $(-1)^{p^n} = -1$ and we see that $-\beta$ is a root. If p is even then $-1 = 1$ (in $\mathbf{Z}/2\mathbf{Z}$) and hence $-\beta = \beta$ is a root. This proves our contention.

The derivative of $f(X)$ is

$$f'(X) = p^n X^{p^n - 1} - 1 = -1.$$

Hence $f(X)$ has no multiple roots, and therefore has p^n distinct roots in $\mathbf{F}_p^a$. Hence its splitting field has exactly p^n elements. We summarize our results:

Theorem 5.1. *For each prime p and each integer $n \geqq 1$ there exists a finite field of order p^n denoted by $\mathbf{F}_{p^n}$, uniquely determined as a subfield of an algebraic closure $\mathbf{F}_p^a$. It is the splitting field of the polynomial*

$$X^{p^n} - X,$$

and its elements are the roots of this polynomial. Every finite field is isomorphic to exactly one field $\mathbf{F}_{p^n}$.

We usually write $p^n = q$ and $\mathbf{F}_q$ instead of $\mathbf{F}_{p^n}$.

Corollary 5.2. *Let $\mathbf{F}_q$ be a finite field. Let n be an integer $\geqq 1$. In a given algebraic closure $\mathbf{F}_q^a$, there exists one and only one extension of $\mathbf{F}_q$ of degree n, and this extension is the field $\mathbf{F}_{q^n}$.*

Proof. Let $q = p^m$. Then $q^n = p^{mn}$. The splitting field of $X^{q^n} - X$ is precisely $F_{p^{mn}}$ and has degree mn over $\mathbf{Z}/p\mathbf{Z}$. Since $\mathbf{F}_q$ has degree m over $\mathbf{Z}/p\mathbf{Z}$, it follows that $\mathbf{F}_{q^n}$ has degree n over $\mathbf{F}_q$. Conversely, any extension of degree n over $\mathbf{F}_q$ has degree mn over $\mathbf{F}_p$ and hence must be $\mathbf{F}_{p^{mn}}$. This proves our corollary.

Theorem 5.3. *The multiplicative group of a finite field is cyclic.*

Proof. This has already been proved in Chapter IV, Theorem 1.9.

We shall determine all automorphisms of a finite field.

Let $q = p^n$ and let $\mathbf{F}_q$ be the finite field with q elements. We consider the **Frobenius mapping**

$$\varphi: \mathbf{F}_q \to \mathbf{F}_q$$

such that $\varphi(x) = x^p$. Then φ is a homomorphism, and its kernel is 0 since $\mathbf{F}_q$ is a field. Hence φ is injective. Since $\mathbf{F}_q$ is finite, it follows that φ is surjective, and hence that φ is an isomorphism. We note that it leaves $\mathbf{F}_p$ fixed.

Theorem 5.4. *The group of automorphisms of $\mathbf{F}_q$ is cyclic of degree n, generated by φ.*

Proof. Let G be the group generated by φ. We note that $\varphi^n = \mathrm{id}$ because $\varphi^n(x) = x^{p^n} = x$ for all $x \in \mathbf{F}_q$. Hence n is an exponent for φ. Let d be the period of φ, so $d \geqq 1$. We have $\varphi^d(x) = x^{p^d}$ for all $x \in \mathbf{F}_q$. Hence each $x \in \mathbf{F}_q$ is a root of the equation

$$X^{p^d} - X = 0.$$

This equation has at most p^d roots. It follows that $d \geqq n$, whence $d = n$.

There remains to be proved that G is the group of all automorphisms of $\mathbf{F}_q$. Any automorphism of $\mathbf{F}_q$ must leave $\mathbf{F}_p$ fixed. Hence it is an auto-

morphism of $\mathbf{F}_q$ over $\mathbf{F}_p$. By Theorem 4.1, the number of such automorphisms is $\leqq n$. Hence $\mathbf{F}_q$ cannot have any other automorphisms except for those of G.

Theorem 5.5. *Let m, n be integers $\geqq 1$. Then in any algebraic closure of $\mathbf{F}_p$, the subfield $\mathbf{F}_{p^n}$ is contained in $\mathbf{F}_{p^m}$ if and only if n divides m. If that is the case, let $q = p^n$, and let $m = nd$. Then $\mathbf{F}_{p^m}$ is normal and separable over $\mathbf{F}_q$, and the group of automorphisms of $\mathbf{F}_{p^m}$ over $\mathbf{F}_q$ is cyclic of order d, generated by φ^n.*

Proof. All the statements are trivial consequences of what has already been proved and will be left to the reader.

§6. INSEPARABLE EXTENSIONS

This section is of a fairly technical nature, and can be omitted without impairing the understanding of most of the rest of the book.

We begin with some remarks supplementing those of Proposition 2.7.

Let $f(X) = (X - \alpha)^m g(X)$ be a polynomial in $k[X]$, and assume $X - \alpha$ does not divide $g(X)$. We recall that m is called the multiplicity of α in f. We say that α is a **multiple** root of f if $m > 1$. Otherwise, we say that α is a **simple** root.

Proposition 6.1. *Let α be algebraic over k, $\alpha \in k^a$, and let*

$$f(X) = \operatorname{Irr}(\alpha, k, X).$$

If $\operatorname{char} k = 0$, *then all roots of f have multiplicity* 1 (*f is separable*). *If*

$$\operatorname{char} k = p > 0,$$

then there exists an integer $\mu \geqq 0$ such that every root of f has multiplicity p^μ. We have

$$[k(\alpha) : k] = p^\mu [k(\alpha) : k]_s,$$

and α^{p^μ} is separable over k.

Proof. Let $\alpha_1, \ldots, \alpha_r$ be the distinct roots of f in k^a and let $\alpha = \alpha_1$. Let m be the multiplicity of α in f. Given $1 \leqq i \leqq r$, there exists an isomorphism

$$\sigma : k(\alpha) \to k(\alpha_i)$$

over k such that $\sigma\alpha = \alpha_i$. Extend σ to an automorphism of k^a and denote

this extension also by σ. Since f has coefficients in k we have $f^\sigma = f$. We note that

$$f(X) = \prod_{j=1}^{r} (X - \sigma\alpha_j)^{m_j}$$

if m_j is the multiplicity of α_j in f. By unique factorization, we conclude that $m_i = m_1$ and hence that all m_i are equal to the same integer m.

Consider the derivative $f'(X)$. If f and f' have a root in common, then α is a root of a polynomial of lower degree than $\deg f$. This is impossible unless $\deg f' = -\infty$, in other words, f' is identically 0. If the characteristic is 0, this cannot happen. Hence if f has multiple roots, we are in characteristic p, and $f(X) = g(X^p)$ for some polynomial $g(X) \in k[X]$. Therefore α^p is a root of a polynomial g whose degree is $< \deg f$. Proceeding inductively, we take the smallest integer $\mu \geqq 0$ such that α^{p^μ} is the root of a separable polynomial in $k[X]$, namely the polynomial h such that

$$f(X) = h(X^{p^\mu}).$$

Comparing the degree of f and g, we conclude that

$$[k(\alpha) : k(\alpha^p)] = p.$$

Inductively, we find

$$[k(\alpha) : k(\alpha^{p^\mu})] = p^\mu.$$

Since h has roots of multiplicity 1, we know that

$$[k(\alpha^{p^\mu}) : k]_s = [k(\alpha^{p^\mu}) : k],$$

and comparing the degree of f and the degree of h, we see that the number of distinct roots of f is equal to the number of distinct roots of h. Hence

$$[k(\alpha) : k]_s = [k(\alpha^{p^\mu}) : k]_s.$$

From this our formula for the degree follows by multiplicativity, and our proposition is proved. We note that the roots of h are

$$\alpha_1^{p^\mu}, \ldots, \alpha_r^{p^\mu}.$$

Corollary 6.2. *For any finite extension E of k, the separable degree $[E : k]_s$ divides the degree $[E : k]$. The quotient is 1 if the characteristic is 0, and a power of p if the characteristic is $p > 0$.*

Proof. We decompose E/k into a tower, each step being generated by one element, and apply Proposition 6.1, together with the multiplicativity of our indices in towers.

If E/K is finite, we call the quotient

$$\frac{[E:k]}{[E:k]_s}$$

the **inseparable degree** (or **degree of inseparability**), and denote it by $[E:k]_i$ as in §4. We have

$$[E:k]_s[E:k]_i = [E:k].$$

Corollary 6.3. *A finite extension is separable if and only if* $[E:k]_i = 1$.

Proof. By definition.

Corollary 6.4 *If* $E \supset F \supset k$ *are two finite extensions, then*

$$[E:k]_i = [E:F]_i[F:k]_i.$$

Proof. Immediate by Theorem 4.1.

We now assume throughout that k is a field of characteristic $p > 0$.

An element α algebraic over k is said to be **purely inseparable** over k if there exists an integer $n \geqq 0$ such that α^{p^n} lies in k.

Let E be an algebraic extension of k. We contend that the following conditions are equivalent:

P. Ins. 1. We have $[E:k]_s = 1$.

P. Ins. 2. Every element α of E is purely inseparable over k.

P. Ins. 3. For every $\alpha \in E$, the irreducible equation of α over k is of type $X^{p^n} - a = 0$ with some $n \geqq 0$ and $a \in k$.

P. Ins. 4. There exists a set of generators $\{\alpha_i\}_{i \in I}$ of E over k such that each α_i is purely inseparable over k.

To prove the equivalence, assume **P. Ins. 1**. Let $\alpha \in E$. By Theorem 4.1, we conclude that $[k(\alpha):k]_s = 1$. Let $f(X) = \mathrm{Irr}(\alpha, k, X)$. Then f has only one root since

$$[k(\alpha):k]_s$$

is equal to the number of distinct roots of $f(X)$. Let $m = [k(\alpha):k]$. Then $\deg f = m$, and the factorization of f over $k(\alpha)$ is $f(X) = (X - \alpha)^m$. Write $m = p^n r$ where r is an integer prime to p. Then

$$\begin{aligned} f(X) &= (X^{p^n} - \alpha^{p^n})^r \\ &= X^{p^n r} - r\alpha^{p^n} X^{p^n(r-1)} + \text{lower terms.} \end{aligned}$$

Since the coefficients of $f(X)$ lie in k, it follows that

$$r\alpha^{p^n}$$

lies in k, and since $r \neq 0$ (in k), then α^{p^n} lies in k. Let $a = \alpha^{p^n}$. Then α is a root of the polynomial $X^{p^n} - a$, which divides $f(X)$. It follows that $f(X) = X^{p^n} - a$.

Essentially the same argument as the preceding one shows that **P. Ins. 2** implies **P. Ins. 3**. It is trivial that the third condition implies the fourth.

Finally, assume **P. Ins. 4**. Let E be an extension generated by purely inseparable elements α_i ($i \in I$). Any embedding of E over k maps α_i on a root of

$$f_i(X) = \operatorname{Irr}(\alpha_i, k, X).$$

But $f_i(X)$ divides some polynomial $X^{p^n} - a$, which has only one root. Hence any embedding of E over k is the identity on each α_i, whence the identity on E, and we conclude that $[E : k]_s = 1$, as desired.

An extension satisfying the above four properties will be called **purely inseparable**.

Proposition 6.5. *Purely inseparable extensions form a distinguished class of extensions.*

Proof. The tower theorem is clear from Theorem 4.1, and the lifting property is clear from condition **P. Ins. 4**.

Proposition 6.6. *Let E be an algebraic extension of k. Let E_0 be the compositum of all subfields F of E such that $F \supset k$ and F is separable over k. Then E_0 is separable over k, and E is purely inseparable over E_0.*

Proof. Since separable extensions form a distinguished class, we know that E_0 is separable over k. In fact, E_0 consists of all elements of E which are separable over k. By Proposition 6.1, given $\alpha \in E$ there exists a power of p, say p^n such that α^{p^n} is separable over k. Hence E is purely inseparable over E_0, as was to be shown.

Corollary 6.7. *If an algebraic extension E of k is both separable and purely inseparable, then $E = k$.*

Proof. Obvious.

Corollary 6.8. *Let K be normal over k and let K_0 be its maximal separable subextension. Then K_0 is also normal over k.*

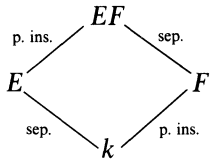
Proof. Let σ be an embedding of K_0 in K^a over k and extend σ to an embedding of K. Then σ is an automorphism of K. Furthermore, σK_0 is separable over k, hence is contained in K_0, since K_0 is the maximal separable subfield. Hence $\sigma K_0 = K_0$, as contended.

Corollary 6.9. *Let E, F be two finite extensions of k, and assume that E/k is separable, F/k is purely inseparable. Assume E, F are subfields of a common field. Then*

$$[EF:F] = [E:k] = [EF:k]_s,$$

$$[EF:E] = [F:k] = [EF:k]_i.$$

Proof. The picture is as follows:



The proof is a trivial juggling of indices, using the corollaries of Proposition 6.1. We leave it as an exercise.

Corollary 6.10. *Let E^p denote the field of all elements x^p, $x \in E$. Let E be a finite extension of k. If $E^p k = E$, then E is separable over k. If E is separable over k, then $E^{p^n} k = E$ for all $n \geqq 1$.*

Proof. Let E_0 be the maximal separable subfield of E. Assume $E^p k = E$. Let $E = k(\alpha_1, \ldots, \alpha_n)$. Since E is purely inseparable over E_0 there exists m such that $\alpha_i^{p^m} \in E_0$ for each $i = 1, \ldots, n$. Hence $E^{p^m} \subset E_0$. But $E^{p^m} k = E$ whence $E = E_0$ is separable over k. Conversely, assume that E is separable over k. Then E is separable over $E^p k$. Since E is also purely inseparable over $E^p k$ we conclude that $E = E^p k$. Similarly we get $E = E^{p^n} k$ *for* $n \geqq 1$, as was to be shown.

Proposition 6.6 shows that any algebraic extension can be decomposed into a tower consisting of a maximal separable subextension and a purely inseparable step above it. Usually, one cannot reverse the order of the tower. However, there is an important case when it can be done.

Proposition 6.11. *Let K be normal over k. Let G be its group of automorphisms over k. Let K^G be the fixed field of G (see Chapter* VI, §1*). Then K^G is purely inseparable over k, and K is separable over K^G. If K_0 is the maximal separable subextension of K, then $K = K^G K_0$ and $K_0 \cap K^G = k$.*

Proof. Let $\alpha \in K^G$. Let τ be an embedding of $k(\alpha)$ over k in K^a and extend τ to an embedding of K, which we denote also by τ. Then τ is an automorphism of K because K is normal over k. By definition, $\tau\alpha = \alpha$ and hence τ is the identity on $k(\alpha)$. Hence $[k(\alpha):k]_s = 1$ and α is purely inseparable. Thus K^G is purely inseparable over k. The intersection of K_0

and K^G is both separable and purely inseparable over k, and hence is equal to k.

To prove that K is separable over K^G, assume first that K is finite over k, and hence that G is finite, by Theorem 4.1. Let $\alpha \in K$. Let $\sigma_1, \ldots, \sigma_r$ be a maximal subset of elements of G such that the elements

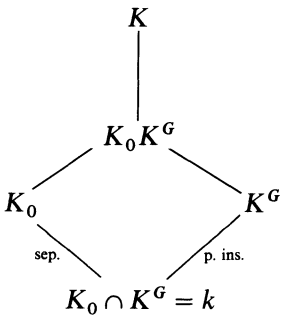
$$\sigma_1\alpha, \ldots, \sigma_r\alpha$$

are distinct, and such that σ_1 is the identity, and α is a root of the polynomial

$$f(X) = \prod_{i=1}^{r} (X - \sigma_i\alpha).$$

For any $\tau \in G$ we note that $f^\tau = f$ because τ permutes the roots. We note that f is separable, and that its coefficients are in the fixed field K^G. Hence α is separable over K^G. The reduction of the infinite case to the finite case is done by observing that every $\alpha \in K$ is contained in some finite normal subextension of K. We leave the details to the reader.

We now have the following picture:



By Proposition 6.6, K is purely inseparable over K_0, hence purely inseparable over K_0K^G. Furthermore, K is separable over K^G, hence separable over K_0K^G. Hence $K = K_0K^G$, thereby proving our proposition.

We see that every normal extension decomposes into a compositum of a purely inseparable and a separable extension. We shall define a Galois extension in the next chapter to be a normal separable extension. Then K_0 is Galois over k and the normal extension is decomposed into a Galois and a purely inseparable extension. The group G is called the **Galois group** of the extension K/k.

A field k is called **perfect** if $k^p = k$. (Every field of characteristic zero is also called perfect.)

Corollary 6.12. *If k is perfect, then every algebraic extension of k is separable, and every algebraic extension of k is perfect.*

Proof. Every finite algebraic extension is contained in a normal extension, and we apply Proposition 6.11 to get what we want.

EXERCISES

1. Let $E = \mathbf{Q}(\alpha)$, where α is a root of the equation

$$\alpha^3 + \alpha^2 + \alpha + 2 = 0.$$

Express $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ and $(\alpha - 1)^{-1}$ in the form

$$a\alpha^2 + b\alpha + c$$

with $a, b, c \in \mathbf{Q}$.

2. Let $E = F(\alpha)$ where α is algebraic over F, of odd degree. Show that $E = F(\alpha^2)$.

3. Let α and β be two elements which are algebraic over F. Let $f(X) = \operatorname{Irr}(\alpha, F, X)$ and $g(X) = \operatorname{Irr}(\beta, F, X)$. Suppose that $\deg f$ and $\deg g$ are relatively prime. Show that g is irreducible in the polynomial ring $F(\alpha)[X]$.

4. Let α be the real positive fourth root of 2. Find all intermediate fields in the extension $\mathbf{Q}(\alpha)$ of $\mathbf{Q}$.

5. If α is a complex root of $X^6 + X^3 + 1$, find all homomorphisms $\sigma: \mathbf{Q}(\alpha) \to \mathbf{C}$. [*Hint*: The polynomial is a factor of $X^9 - 1$.]

6. Show that $\sqrt{2} + \sqrt{3}$ is algebraic over $\mathbf{Q}$, of degree 4.

7. Let E, F be two finite extensions of a field k, contained in a larger field K. Show that

$$[EF : k] \leqq [E : k][F : k].$$

If $[E : k]$ and $[F : k]$ are relatively prime, show that one has an equality sign in the above relation.

8. Let $f(X) \in k[X]$ be a polynomial of degree n. Let K be its splitting field. Show that $[K : k]$ divides $n!$

9. Find the splitting field of $X^{p^8} - 1$ over the field $\mathbf{Z}/p\mathbf{Z}$.

10. Let α be a real number such that $\alpha^4 = 5$.
    (a) Show that $\mathbf{Q}(i\alpha^2)$ is normal over $\mathbf{Q}$.
    (b) Show that $\mathbf{Q}(\alpha + i\alpha)$ is normal over $\mathbf{Q}(i\alpha^2)$.
    (c) Show that $\mathbf{Q}(\alpha + i\alpha)$ is not normal over $\mathbf{Q}$.

11. Describe the splitting fields of the following polynomials over $\mathbf{Q}$, and find the degree of each such splitting field.
    (a) $X^2 - 2$ (b) $X^2 - 1$
    (c) $X^3 - 2$ (d) $(X^3 - 2)(X^2 - 2)$
    (e) $X^2 + X + 1$ (f) $X^6 + X^3 + 1$
    (g) $X^5 - 7$

12. Let K be a finite field with p^n elements. Show that every element of K has a unique p-th root in K.

13. If the roots of a monic polynomial $f(X) \in k[X]$ in some splitting field are distinct, and form a field, then char $k = p$ and $f(X) = X^{p^n} - X$ for some $n \geqq 1$.

14. Let char $K = p$. Let L be a finite extension of K, and suppose $[L:K]$ prime to p. Show that L is separable over K.

15. Suppose char $K = p$. Let $a \in K$. If a has no p-th root in K, show that $X^{p^n} - a$ is irreducible in $K[X]$ for all positive integers n.

16. Let char $K = p$. Let α be algebraic over K. Show that α is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all positive integers n.

17. Prove that the following two properties are equivalent:
    (a) Every algebraic extension of K is separable.
    (b) Either char $K = 0$, or char $K = p$ and every element of K has a p-th root in K.

18. Show that every element of a finite field can be written as a sum of two squares in that field.

19. Let E be an algebraic extension of F. Show that every subring of E which contains F is actually a field. Is this necessarily true if E is not algebraic over F? Prove or give a counterexample.

20. (a) Let $E = F(x)$ where x is transcendental over F. Let $K \neq F$ be a subfield of E which contains F. Show that x is algebraic over K.
    (b) Let $E = F(x)$. Let $y = f(x)/g(x)$ be a rational function, with relatively prime polynomials f, $g \in F[x]$. Let $n = \max(\deg f, \deg g)$. Suppose $n \geqq 1$. Prove that

$$[F(x):F(y)] = n.$$

21. Let $\mathbf{Z}^+$ be the set of positive integers, and A an additive abelian group. Let $f: \mathbf{Z}^+ \to A$ and $g: \mathbf{Z}^+ \to A$ be maps. Suppose that for all n,

$$f(n) = \sum_{d|n} g(d).$$

    Let μ be the Möbius function (cf. Exercise 12 of Chapter II). Prove that

$$g(n) = \sum_{d|n} \mu(n/d) f(d).$$

22. Let k be a finite field with q elements. Let $f(X) \in k[X]$ be irreducible. Show that $f(X)$ divides $X^{q^n} - X$ if and only if deg f divides n. Show the multiplication formula

$$X^{q^n} - X = \prod_{d|n} \prod_{f_d \text{ irr}} f_d(X),$$

    where the inner product is over all irreducible polynomials of degree d with leading coefficient 1. Counting degrees, show that

$$q^n = \sum_{d|n} d\psi(d),$$

    where $\psi(d)$ is the number of irreducible polynomials of degree d. Invert by

Exercise 21 and find that

$$n\psi(n) = \sum_{d|n} \mu(d) q^{n/d}.$$

23. (a) Let k be a finite field with q elements. Define the **zeta function**

$$Z(t) = (1-t)^{-1} \prod_{p} (1 - t^{\deg p})^{-1},$$

where p ranges over all irreducible polynomials $p = p(X)$ in $k[X]$ with leading coefficient 1. Prove that $Z(t)$ is a rational function and determine this rational function.

(b) Let $\pi_q(n)$ be the number of primes p as in (a) of degree $\leqq n$. Prove that

$$\pi_q(m) \sim \frac{q}{q-1} \frac{q^m}{m} \qquad \text{for} \quad m \to \infty.$$

Remark. This is the analogue of the prime number theorem in number theory, but it is essentially trivial in the present case, because the Riemann hypothesis is trivially verified. Things get more interesting fast after this case. Consider an equation $y^2 = x^3 + ax + b$ over a finite field $\mathbf{F}_q$ of characteristic $\neq 2$, 3, and having q elements. Assume $-4a^3 - 27b^2 \neq 0$, in which case the curve defined by this equation is called an **elliptic curve**. Define N_n by

$N_n - 1 =$ number of points (x, y) satisfying the above equation with $x, y \in \mathbf{F}_{q^n}$ (the extension of $\mathbf{F}_q$ of degree n).

Define the **zeta function** $Z(t)$ to be the unique rational function such that $Z(0) = 1$ and

$$Z'/Z(t) = \sum N_n t^{n-1}.$$

A famous theorem of Hasse asserts that $Z(t)$ is a rational function of the form

$$Z(t) = \frac{(1 - \alpha t)(1 - \bar{\alpha} t)}{(1-t)(1-qt)},$$

where α is an imaginary quadratic number (not real, quadratic over $\mathbf{Q}$), $\bar{\alpha}$ is its complex conjugate, and $\alpha\bar{\alpha} = q$, so $|\alpha| = q^{1/2}$. See Hasse, "Abstrakte Bergrundung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern," *Abh. Math. Sem. Univ. Hamburg* **10** (1934) pp. 325–348.

24. Let k be a field of characteristic p and let t, u be algebraically independent over k. Prove the following:
(a) $k(t, u)$ has degree p^2 over $k(t^p, u^p)$.
(b) There exist infinitely many extensions between $k(t, u)$ and $k(t^p, u^p)$.

25. Let E be a finite extension of k and let $p^r = [E : k]_i$. We assume that the characteristic is $p > 0$. Assume that there is no exponent p^s with $s < r$ such that $E^{p^s}k$ is separable over k (i.e., such that α^{p^s} is separable over k for each α in E). Show that E can be generated by one element over k. [*Hint*: Assume first that E is purely inseparable.]

26. Let k be a field, $f(X)$ an irreducible polynomial in $k[X]$, and let K be a finite normal extension of k. If g, h are monic irreducible factors of $f(X)$ in $K[X]$, show that there exists an automorphism σ of K over k such that $g = h^\sigma$. Give an example when this conclusion is not valid if K is not normal over k.

27. Let $x_1, \ldots, x_n$ be algebraically independent over a field k. Let y be algebraic over $k(x) = k(x_1, \ldots, x_n)$. Let $P(X_{n+1})$ be the irreducible polynomial of y over $k(x)$. Let $\varphi(x)$ be the least common multiple of the denominators of the coefficients of P. Then the coefficients of $\varphi(x)P$ are elements of $k[x]$. Show that the polynomial

$$f(X_1, \ldots, X_{n+1}) = \varphi(X_1, \ldots, X_n)P(X_{n+1})$$

is irreducible over k, as a polynomial in $n + 1$ variables.

Conversely, let $f(X_1, \ldots, X_{n+1})$ be an irreducible polynomial over k. Let $x_1, \ldots, x_n$ be algebraically independent over k. Show that

$$f(x_1, \ldots, x_n, X_{n+1})$$

is irreducible over $k(x_1, \ldots, x_n)$.

If f is a polynomial in n variables, and $(b) = (b_1, \ldots, b_n)$ is an n-tuple of elements such that $f(b) = 0$, then we say that (b) is a **zero** of f. We say that (b) is **non-trivial** if not all coordinates b_i are equal to 0.

28. Let $f(X_1, \ldots, X_n)$ be a homogeneous polynomial of degree 2 (resp. 3) over a field k. Show that if f has a non-trivial zero in an extension of odd degree (resp. degree 2) over k, then f has a non-trivial zero in k.

29. Let $f(X, Y)$ be an irreducible polynomial in two variables over a field k. Let t be transcendental over k, and assume that there exist integers m, $n \neq 0$ and elements $a, b \in k$, $ab \neq 0$, such that $f(at^n, bt^m) = 0$. Show that after inverting possibly X or Y, and up to a constant factor, f is of type

$$X^m Y^n - c$$

with some $c \in k$.

The answer to the following exercise is not known.

30. **(Artin conjecture).** Let f be a homogeneous polynomial of degree d in n variables, with rational coefficients. If $n > d$, show that there exists a root of unity ζ, and elements

$$x_1, \ldots, x_n \in \mathbf{Q}[\zeta]$$

not all 0 such that $f(x_1, \ldots, x_n) = 0$.

31. **Difference equations.** Let $u_1, \ldots, u_d$ be elements of a field K. We want to solve for infinite vectors $(x_0, x_1, \ldots, x_n, \ldots)$ satisfying

(*) $$x_n = u_1 x_{n-1} + \cdots + u_d x_{n-d} \quad \text{for} \quad n \geqq d.$$

Define the **characteristic polynomial** of the system to be

$$X^d - (u_1 X^{d-1} + \cdots + u_d) = f(X).$$

Suppose α is a root of f.

(a) Show that $x_n = \alpha^n$ $(n \geqq 0)$ is a solution of (*).

(b) Show that the set of solutions of (*) is a vector space of dimension d.

(c) Assume that the characteristic polynomial has d distinct roots $\alpha_1, \ldots, \alpha_d$. Show that the solutions $(\alpha_1^n), \ldots, (\alpha_d^n)$ form a basis for the space of solutions.

(d) Let $x_n = b_1\alpha_1^n + \cdots + b_d\alpha_d^n$ for $n \geqq 0$, show how to solve for $b_1, \ldots, b_d$ in terms of $\alpha_1, \ldots, \alpha_d$ and $x_0, \ldots, x_{d-1}$. (Use the Vandermonde determinant.)

(e) Under the conditions of (d), let $F(T) = \sum x_n T^n$. Show that $F(T)$ represents a rational function, and give its partial fraction decomposition.

32. Let $d = 2$ for simplicity. Given $a_0, a_1, u, v, w, t \in K$, we want to find the solutions of the system

$$a_n = ua_{n-1} - vta_{n-2} - t^n w \qquad \text{for} \quad n \geqq 2.$$

Let α_1, α_2 be the roots of the characteristic polynomial, that is

$$1 - uX + vtX^2 = (1 - \alpha_1 X)(1 - \alpha_2 X).$$

Assume that α_1, α_2 are distinct, and also distinct from t. Let

$$F(X) = \sum_{n=0}^{\infty} a_n X^n.$$

(a) Show that there exist elements A, B, C of K such that

$$F(X) = \frac{A}{1 - \alpha_1 X} + \frac{B}{1 - \alpha_2 X} + \frac{C}{1 - tX}.$$

(b) Show that there is a unique solution to the difference equation given by

$$a_n = A\alpha_1^n + B\alpha_2^n + Ct^n \qquad \text{for} \quad n \geqq 0.$$

(To see an application of this formalism to modular forms, as in the work of Manin, Mazur, and Swinnerton-Dyer, cf. my *Introduction to Modular Forms*, Springer-Verlag, New York, 1976, Chapter XII, §2.)

33. Let R be a ring which we assume entire for simplicity. Let

$$g(T) = T^d - a_{d-1}T^{d-1} - \cdots - a_0$$

be a polynomial in $R[T]$, and consider the equation

$$T^d = a_0 + a_1 T + \cdots + a_{d-1}T^{d-1}.$$

Let x be a root of $g(T)$.

(a) For any integer $n \geqq d$ there is a relation

$$x^n = a_{0,n} + a_{1,n}x + \cdots + a_{d-1,n}x^{d-1}$$

with coefficients $a_{i,j}$ in $\mathbf{Z}[a_0, \ldots, a_{d-1}] \subset R$.

(b) Let $F(T) \in R[T]$ be a polynomial. Then

$$F(x) = a_0(F) + a_1(F)x + \cdots + a_{d-1}(F)x^{d-1}$$

where the coefficients $a_i(F)$ lie in R and depend linearly on F.

(c) Let the Vandermonde determinant be

$$V(x_1, \ldots, x_d) = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{d-1} \\ 1 & x_2 & \cdots & x_2^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_d & \cdots & x_d^{d-1} \end{vmatrix} = \prod_{i<j} (x_j - x_i).$$

Suppose that the equation $g(T) = 0$ has d roots and that there is a factorization

$$g(T) = \prod_{i=1}^{d} (T - x_i).$$

Substituting x_i for x with $i = 1, \ldots, d$ and using Cramer's rule on the resulting system of linear equations, yields

$$\Delta a_j(F) = \Delta_j(F)$$

where Δ is the Vandermonde determinant, and $\Delta_j(F)$ is obtained by replacing the j-th column by ${}^t(F(x_1), \ldots, F(x_d))$, so

$$\Delta_j(F) = \begin{vmatrix} 1 & x_1 & \cdots & F(x_1) & \cdots & x_1^{d-1} \\ 1 & x_2 & \cdots & F(x_2) & \cdots & x_2^{d-1} \\ \vdots & \vdots & & \vdots & & \vdots \\ 1 & x_d & \cdots & F(x_d) & \cdots & x_d^{d-1} \end{vmatrix}$$

If $\Delta \neq 0$ then we can write

$$a_j(F) = \Delta_j(F)/\Delta.$$

Remark. If $F(T)$ is a power series in $R[[T]]$ and if R is a complete local ring, with $x_1, \ldots, x_d$ in the maximal ideal, and $x = x_i$ for some i, then we can evaluate $F(x)$ because the series converges. The above formula for the coefficients $a_j(F)$ remains valid.

34. Let $x_1, \ldots, x_d$ be independent variables, and let A be the ring

$$\mathbf{Q}[[x_1, \ldots, x_d]][T]/\prod_{i=1}^{d} (T - x_i).$$

Substituting some x_i for T induces a natural homomorphism φ_i of A onto

$$\mathbf{Q}[[z_1, \ldots, x_d]] = R,$$

and the map $z \mapsto (\varphi_1(z), \ldots, \varphi_d(z))$ gives an embedding of A into the product of R with itself d times.

Let k be an integer, and consider the formal power series

$$F(T) = e^{kT} \prod_{i=1}^{d} \frac{(T - x_i)e^{T - x_i}}{e^{T - x_i} - 1} = e^{kT} \prod_{i=1}^{d} h(T - x_i)$$

where $h(t) = te^t/(e^t - 1)$. It is a formal power series in T, $T - x_1$, $\ldots$, $T - x_d$. Under substitution of some x_j for T it becomes a power series in x_j and $x_j - x_i$, and thus converges in $\mathbf{Q}[[x_1, \ldots, x_d]]$.

(a) Verify that

$$F(T) \equiv a_0(F) + \cdots + a_{d-1}(F)T^{d-1} \bmod \prod_{i=1}^{d} (T - x_i)$$

where $a_0(F), \ldots, a_{d-1}(F) \in \mathbf{Q}[[x_1, \ldots, x_d]]$, and that the formula given in the preceding exercise for these coefficients in terms of Vandermonde determinants is valid.

(b) Show that $a_{d-1}(F) = 0$ if $-(d-1) \leqq k < 0$ and $a_{d-1}(F) = 1$ if $k = 0$.

Remark. The assertion in (a) is a simple limit. The assertion in (b) is a fact which has been used in the proof of the Hirzebruch–Grothendieck–Riemann–Roch theorem and as far as I know there was no simple known proof until Roger Howe pointed out that it could be done by the formula of the preceding exercise as follows. We have

$$V(x_1, \ldots, x_n)a_{d-1}(F) = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{d-2} & F(x_1) \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_d & \cdots & x_d^{d-2} & F(x_d) \end{vmatrix}.$$

Furthermore,

$$F(x_j) = e^{kx_j} \prod_{n \neq j} \frac{(x_j - x_n)e^{x_j - x_n}}{e^{x_j - x_n} - 1}.$$

We use the inductive relation of Vandermonde determinants

$$V(x_1, \ldots, x_d) = V(x_1, \ldots, \hat{x}_j, \ldots, x_d)(-1)^{d-j} \prod_{n \neq j} (x_j - x_n).$$

We expand the determinant for $a_{d-1}(F)$ according to the last column to get

$$a_{d-1}(F) = \sum_{j=1}^{d} e^{(k+d-1)x_j} \prod_{n \neq j} \frac{1}{e^{x_j} - e^{x_n}}.$$

Using the inductive relation backward, and replacing x_i by e^{x_i} which we denote by y_i for typographical reasons, we get

$$V(y_1, \ldots, y_d)a_{d-1}(F) = \begin{vmatrix} 1 & y_1 & \cdots & y_1^{d-2} & y_1^{k+d-1} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & y_d & \cdots & y_d^{d-2} & y_d^{k+d-1} \end{vmatrix}$$

If $k \neq 0$ then two columns on the right are the same, so the determinant is 0. If $k = 0$ then we get the Vandermonde determinant on the right, so $a_{d-1}(F) = 1$. This proves the desired value.