Part Two

ALGEBRAIC EQUATIONS

This part is concerned with the solutions of algebraic equations, in one or several variables. This is the recurrent theme in every chapter of this part, and we lay the foundations for all further studies concerning such equations.

Given a subring A of a ring B, and a finite number of polynomials $f_1, \ldots, f_n$ in $A[X_1, \ldots, X_n]$, we are concerned with the n-tuples

$$(b_1, \ldots, b_n) \in B^{(n)}$$

such that

$$f_i(b_1, \ldots, b_n) = 0$$

for $i = 1, \ldots, r$. For suitable choices of A and B, this includes the general problem of diophantine analysis when A, B have an "arithmetic" structure.

We shall study various cases. We begin by studying roots of one polynomial in one variable over a field. We prove the existence of an algebraic closure, and emphasize the role of irreducibility.

Next we study the group of automorphisms of algebraic extensions of a field, both intrinsically and as a group of permutations of the roots of a polynomial. We shall mention some major unsolved problems along the way.

It is also necessary to discuss extensions of a ring, to give the possibility of analyzing families of extensions. The ground work is laid in Chapter VII.

In Chapter IX, we come to the zeros of polynomials in several variables, essentially over algebraically closed fields. But again, it is advantageous to

consider polynomials over rings, especially $\mathbf{Z}$, since in projective space, the conditions that homogeneous polynomials have a non-trivial common zero can be given universally over $\mathbf{Z}$ in terms of their coefficients.

Finally we impose additional structures like those of reality, or metric structures given by absolute values. Each one of these structures gives rise to certain theorems describing the structure of the solutions of equations as above, and especially proving the existence of solutions in important cases.

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

$$F[X] \to E$$

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.*

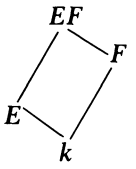
Proof. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of E as vector space over k. Then certainly

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

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.

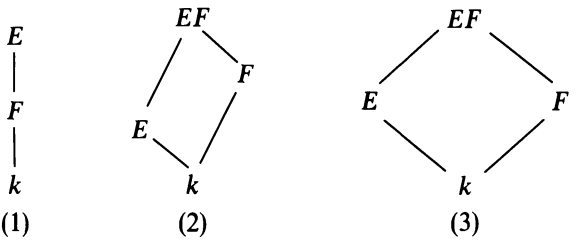
Let $\mathfrak{C}$ be a certain class of extension fields $F \subset E$. We shall say that $\mathfrak{C}$ is **distinguished** if it satisfies the following conditions:

(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

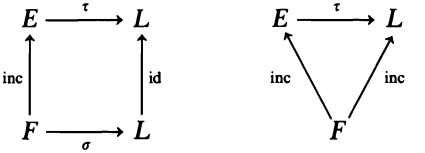
In this and the next section we shall deal with embeddings of a field into another. We therefore define some terminology.

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:



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

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

Here we have written a^σ instead of $\sigma(a)$. This exponential notation is frequently convenient and will be used again in the sequel. Similarly, we write F^σ instead of $\sigma(F)$ or σF.

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 $\leqq$ the number of roots of p, and is equal to the number of distinct roots of p.*

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:

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & B \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\sigma\circ\varphi\circ\sigma^{-1}} \\ A & \xrightarrow[\sigma]{} & B \end{array}$$

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 $\neq$ 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

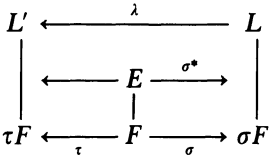
Let E be an algebraic extension of a field F and let

$$\sigma: F \to L$$

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.*

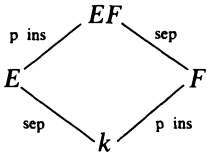
Proof. Let σ be an embedding of K_0 in K^a over k and extend σ to an embedding of K. Then σ is an automorphism of K. Furthermore, σK_0 is separable over k, hence is contained in K_0, since K_0 is the maximal separable subfield. Hence $\sigma K_0 = K_0$, as contended.

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 $E^pk = E$, 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 $E^pk = E$. 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^pk. Since E is also purely inseparable over E^pk we conclude that $E = E^pk$. 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 $K = K^GK_0$ 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

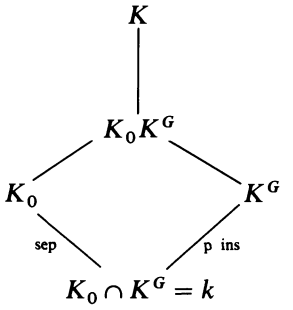
$$\sigma_1\alpha, \ldots, \sigma_r\alpha$$

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 root 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, $T - x_1$, ..., $T - x_d$. 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.

CHAPTER VI

Galois Theory

This chapter contains the core of Galois theory. We study the group of automorphisms of a finite (and sometimes infinite) Galois extension at length, and give examples, such as cyclotomic extensions, abelian extensions, and even non-abelian ones, leading into the study of matrix representations of the Galois group and their classifications. We shall mention a number of fundamental unsolved problems, the most notable of which is whether given a finite group G, there exists a Galois extension of $\mathbf{Q}$ having this group as Galois group. Three surveys give recent points of view on those questions and sizeable bibliographies:

B. MATZAT, *Konstruktive Galoistheorie*, Springer Lecture Notes **1284**, 1987

B. MATZAT, Über das Umkehrproblem der Galoisschen Theorie, *Jahrsbericht Deutsch. Mat.-Verein.* **90** (1988), pp. 155–183

J. P. SERRE, *Topics in Galois theory*, course at Harvard, 1989, Jones and Bartlett, Boston 1992

More specific references will be given in the text at the appropriate moment concerning this problem and the problem of determining Galois groups over specific fields, especially the rational numbers.

§1. GALOIS EXTENSIONS

Let K be a field and let G be a group of automorphisms of K. We denote by K^G the subset of K consisting of all elements $x \in K$ such that $x^\sigma = x$ for all $\sigma \in G$. It is also called the **fixed field** of G. It is a field because if $x, y \in K^G$ then

$$(x + y)^\sigma = x^\sigma + y^\sigma = x + y$$

for all $\sigma \in G$, and similarly, one verifies that K is closed under multiplication, subtraction, and multiplicative inverse. Furthermore, K^G contains 0 and 1, hence contains the prime field.

An algebraic extension K of a field k is called **Galois** if it is normal and separable. We consider K as embedded in an algebraic closure. The group of automorphisms of K over k is called the **Galois group** of K over k, and is denoted by $G(K/k)$, $G_{K/k}$, $\mathrm{Gal}(K/k)$, or simply G. It coincides with the set of embeddings of K in K^a over k.

For the convenience of the reader, we shall now state the main result of the Galois theory for finite Galois extensions.

Theorem 1.1. *Let K be a finite Galois extension of k, with Galois group G. There is a bijection between the set of subfields E of K containing k, and the set of subgroups H of G, given by $E = K^H$. The field E is Galois over k if and only if H is normal in G, and if that is the case, then the map $\sigma \mapsto \sigma | E$ induces an isomorphism of G/H onto the Galois group of E over k.*

We shall give the proofs step by step, and as far as possible, we give them for infinite extensions.

Theorem 1.2. *Let K be a Galois extension of k. Let G be its Galois group. Then $k = K^G$. If F is an intermediate field, $k \subset F \subset K$, then K is Galois over F. The map*

$$F \mapsto G(K/F)$$

from the set of intermediate fields into the set of subgroups of G is injective.

Proof. Let $\alpha \in K^G$. Let σ be any embedding of $k(\alpha)$ in K^a, inducing the identity on k. Extend σ to an embedding of K into K^a, and call this extension σ also. Then σ is an automorphism of K over k, hence is an element of G. By assumption, σ leaves α fixed. Therefore

$$[k(\alpha) : k]_s = 1.$$

Since α is separable over k, we have $k(\alpha) = k$ and α is an element of k. This proves our first assertion.

Let F be an intermediate field. Then K is normal and separable over F by Theorem 3.4 and Theorem 4.5 of Chapter V. Hence K is Galois over F. If $H = G(K/F)$ then by what we proved above we conclude that $F = K^H$. If F, F' are intermediate fields, and $H = G(K/F)$, $H' = G(K/F')$, then

$$F = K^H \quad \text{and} \quad F' = K^{H'}.$$

If $H = H'$ we conclude that $F = F'$, whence our map

$$F \mapsto G(K/F)$$

is injective, thereby proving our theorem.

We shall sometimes call the group $G(K/F)$ of an intermediate field the group **associated** with F. We say that a subgroup H of G **belongs** to an intermediate field F if $H = G(K/F)$.

Corollary 1.3. *Let K/k be Galois with group G. Let F, F' be two intermediate fields, and let H, H' be the subgroups of G belonging to F, F' respectively. Then $H \cap H'$ belongs to FF'.*

Proof. Every element of $H \cap H'$ leaves FF' fixed, and every element of G which leaves FF' fixed also leaves F and F' fixed and hence lies in $H \cap H'$. This proves our assertion.

Corollary 1.4. *Let the notation be as in Corollary* 1.3. *The fixed field of the smallest subgroup of G containing H, H' is $F \cap F'$.*

Proof. Obvious.

Corollary 1.5. *Let the notation be as in Corollary* 1.3. *Then $F \subset F'$ if and only if $H' \subset H$.*

Proof. If $F \subset F'$ and $\sigma \in H'$ leaves F' fixed then σ leaves F fixed, so σ lies in H. Conversely, if $H' \subset H$ then the fixed field of H is contained in the fixed field of H', so $F \subset F'$.

Corollary 1.6. *Let E be a finite separable extension of a field k. Let K be the smallest normal extension of k containing E. Then K is finite Galois over k. There is only a finite number of intermediate fields F such that $k \subset F \subset E$.*

Proof. We know that K is normal and separable, and K is finite over k since we saw that it is the finite compositum of the finite number of conjugates of E. The Galois group of K/k has only a finite number of subgroups. Hence there is only a finite number of subfields of K containing k, whence *a fortiori* a finite number of subfields of E containing k.

Of course, the last assertion of Corollary 1.6 has been proved in the preceding chapter, but we get another proof here from another point of view.

Lemma 1.7. *Let E be an algebraic separable extension of k. Assume that there is an integer $n \geqq 1$ such that every element α of E is of degree $\leqq n$ over k. Then E is finite over k and $[E : k] \leqq n$.*

Proof. Let α be an element of E such that the degree $[k(\alpha) : k]$ is maximal, say $m \leqq n$. We contend that $k(\alpha) = E$. If this is not true, then there exists an element $\beta \in E$ such that $\beta \notin k(\alpha)$, and by the primitive element theorem, there exists an element $\gamma \in k(\alpha, \beta)$ such that $k(\alpha, \beta) = k(\gamma)$. But from the tower

$$k \subset k(\alpha) \subset k(\alpha, \beta)$$

we see that $[k(\alpha, \beta) : k] > m$ whence γ has degree $> m$ over k, contradiction.

Theorem 1.8. (Artin). *Let K be a field and let G be a finite group of automorphisms of K, of order n. Let $k = K^G$ be the fixed field. Then K is a finite Galois extension of k, and its Galois group is G. We have $[K : k] = n$.*

Proof. Let $\alpha \in K$ and let $\sigma_1, \ldots, \sigma_r$ be a maximal set of elements of G such that $\sigma_1\alpha, \ldots, \sigma_r\alpha$ are distinct. If $\tau \in G$ then $(\tau\sigma_1\alpha, \ldots, \tau\sigma_r\alpha)$ differs from $(\sigma_1\alpha, \ldots, \sigma_r\alpha)$ by a permutation, because τ is injective, and every $\tau\sigma_i\alpha$ is among the set $\{\sigma_1\alpha, \ldots, \sigma_r\alpha\}$; otherwise this set is not maximal. Hence α is a root of the polynomial

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

and for any $\tau \in G$, $f^\tau = f$. Hence the coefficients of f lie in $K^G = k$. Furthermore, f is separable. Hence every element α of K is a root of a separable polynomial of degree $\leqq n$ with coefficients in k. Furthermore, this polynomial splits in linear factors in K. Hence K is separable over k, is normal over k, hence Galois over k. By Lemma 1.7, we have $[K : k] \leqq n$. The Galois group of K over k has order $\leqq [K:k]$ (by Theorem 4.1 of Chapter V), and hence G must be the full Galois group. This proves all our assertions.

Corollary 1.9. *Let K be a finite Galois extension of k and let G be its Galois group. Then every subgroup of G belongs to some subfield F such that $k \subset F \subset K$.*

Proof. Let H be a subgroup of G and let $F = K^H$. By Artin's theorem we know that K is Galois over F with group H.

Remark. When K is an infinite Galois extension of k, then the preceding corollary is not true any more. This shows that some counting argument must be used in the proof of the finite case. In the present treatment, we have used an old-fashioned argument. The reader can look up Artin's own proof in his book *Galois Theory*. In the infinite case, one defines the Krull topology on the Galois group G (cf. exercises 43–45), and G becomes a compact totally disconnected group. The subgroups which belong to the intermediate fields are the *closed* subgroups. The reader may disregard the infinite case entirely throughout our discussions without impairing understanding. The proofs in the infinite case are usually identical with those in the finite case.

The notions of a Galois extension and a Galois group are defined completely algebraically. Hence they behave formally under isomorphisms the way one expects from objects in any category. We describe this behavior more explicitly in the present case.

Let K be a Galois extension of k. Let

$$\lambda : K \to \lambda K$$

be an isomorphism. Then λK is a Galois extension of λk.

$$\begin{array}{ccc} K & \xrightarrow{\lambda} & \lambda K \\ | & & | \\ k & \xrightarrow[\lambda]{} & \lambda k \end{array}$$

Let G be the Galois group of K over k. Then the map

$$\sigma \mapsto \lambda \circ \sigma \circ \lambda^{-1}$$

gives a homomorphism of G into the Galois group of λK over λk, whose inverse is given by

$$\lambda^{-1} \circ \tau \circ \lambda \longleftarrow \tau.$$

Hence $G(\lambda K/\lambda k)$ is isomorphic to $G(K/k)$ under the above map. We may write

$$G(\lambda K/\lambda k)^{\lambda} = G(K/k)$$

or

$$G(\lambda K/\lambda k) = \lambda G(K/k)\lambda^{-1},$$

where the exponent λ is "conjugation,"

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

There is no avoiding the contravariance if we wish to preserve the rule

$$(\sigma^{\lambda})^{\omega} = \sigma^{\lambda\omega}$$

when we compose mappings λ and ω.

In particular, let F be an intermediate field, $k \subset F \subset K$, and let $\lambda : F \to \lambda F$ be an embedding of F in K, which we assume is extended to an automorphism of K. Then $\lambda K = K$. Hence

$$G(K/\lambda F)^{\lambda} = G(K/F)$$

and

$$G(K/\lambda F) = \lambda G(K/F)\lambda^{-1}.$$

Theorem 1.10. *Let K be a Galois extension of k with group G. Let F be a subfield, $k \subset F \subset K$, and let $H = G(K/F)$. Then F is normal over k if and only if H is normal in G. If F is normal over k, then the restriction map $\sigma \mapsto \sigma | F$*

is a homomorphism of G onto the Galois group of F over k, whose kernel is H. We thus have $G(F/k) \approx G/H$.

Proof. Assume F is normal over k, and let G' be its Galois group. The restriction map $\sigma \to \sigma|F$ maps G into G', and by definition, its kernel is H. Hence H is normal in G. Furthermore, any element $\tau \in G'$ extends to an embedding of K in K^a, which must be an automorphism of K, so the restriction map is surjective. This proves the last statement. Finally, assume that F is not normal over k. Then there exists an embedding λ of F in K over k which is not an automorphism, i.e. $\lambda F \neq F$. Extend λ to an automorphism of K over k. The Galois groups $G(K/\lambda F)$ and $G(K/F)$ are conjugate, and they belong to distinct subfields, hence cannot be equal. Hence H is not normal in G.

A Galois extension K/k is said to be **abelian** (resp. **cyclic**) if its Galois group G is abelian (resp. cyclic).

Corollary 1.11. *Let K/k be abelian (resp. cyclic). If F is an intermediate field, $k \subset F \subset K$, then F is Galois over k and abelian (resp. cyclic).*

Proof. This follows at once from the fact that a subgroup of an abelian group is normal, and a factor group of an abelian (resp. cyclic) group is abelian (resp. cyclic).

Theorem 1.12. *Let K be a Galois extension of k, let F be an arbitrary extension and assume that K, F are subfields of some other field. Then KF is Galois over F, and K is Galois over $K \cap F$. Let H be the Galois group of KF over F, and G the Galois group of K over k. If $\sigma \in H$ then the restriction of σ to K is in G, and the map*

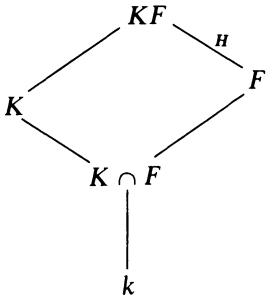
$$\sigma \mapsto \sigma|K$$

gives an isomorphism of H on the Galois group of K over $K \cap F$.

Proof. Let $\sigma \in H$. The restriction of σ to K is an embedding of K over k, whence an element of G since K is normal over k. The map $\sigma \mapsto \sigma|K$ is clearly a homomorphism. If $\sigma|K$ is the identity, then σ must be the identity of KF (since every element of KF can be expressed as a combination of sums, products, and quotients of elements in K and F). Hence our homomorphism $\sigma \mapsto \sigma|K$ is injective. Let H' be its image. Then H' leaves $K \cap F$ fixed, and conversely, if an element $\alpha \in K$ is fixed under H', we see that α is also fixed under H, whence $\alpha \in F$ and $\alpha \in K \cap F$. Therefore $K \cap F$ is the fixed field. If K is finite over k, or even KF finite over F, then by Theorem 1.8, we know that H' is the Galois group of K over $K \cap F$, and the theorem is proved in that case.

(In the infinite case, one must add the remark that for the Krull topology, our map $\sigma \mapsto \sigma|K$ is continuous, whence its image is closed since H is compact. See Theorem 14.1; Chapter I, Theorem 10.1; and Exercise 43.)

The diagram illustrating Theorem 1.12 is as follows:



It is suggestive to think of the opposite sides of a parallelogram as being equal.

Corollary 1.13. *Let K be a finite Galois extension of k. Let F be an arbitrary extension of k. Then $[KF : F]$ divides $[K : k]$.*

Proof. Notation being as above, we know that the order of H divides the order of G, so our assertion follows.

Warning. The assertion of the corollary is not usually valid if K is not Galois over k. For instance, let $\alpha = \sqrt[3]{2}$ be the real cube root of 2, let ζ be a cube root of 1, $\zeta \neq 1$, say

$$\zeta = \frac{-1 + \sqrt{-3}}{2},$$

and let $\beta = \zeta\alpha$. Let $E = \mathbf{Q}(\beta)$. Since β is complex and α real, we have

$$\mathbf{Q}(\beta) \neq \mathbf{Q}(\alpha).$$

Let $F = \mathbf{Q}(\alpha)$. Then $E \cap F$ is a subfield of E whose degree over $\mathbf{Q}$ divides 3. Hence this degree is 3 or 1, and must be 1 since $E \neq F$. But

$$EF = \mathbf{Q}(\alpha, \beta) = \mathbf{Q}(\alpha, \zeta) = \mathbf{Q}(\alpha, \sqrt{-3}).$$

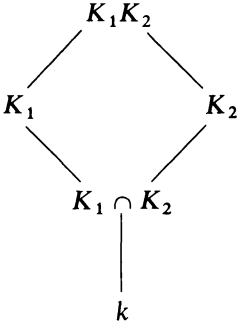
Hence EF has degree 2 over F.

Theorem 1.14. *Let K_1 and K_2 be Galois extensions of a field k, with Galois groups G_1 and G_2 respectively. Assume K_1, K_2 are subfields of some field. Then K_1K_2 is Galois over k. Let G be its Galois group. Map $G \to G_1 \times G_2$ by restriction, namely*

$$\sigma \mapsto (\sigma | K_1, \sigma | K_2).$$

This map is injective. If $K_1 \cap K_2 = k$ then the map is an isomorphism.

Proof. Normality and separability are preserved in taking the compositum of two fields, so K_1K_2 is Galois over k. Our map is obviously a homomorphism of G into $G_1 \times G_2$. If an element $\sigma \in G$ induces the identity on K_1 and K_2 then it induces the identity on their compositum, so our map is injective. Assume that $K_1 \cap K_2 = k$. According to Theorem 1.12, given an element $\sigma_1 \in G_1$ there exists an element σ of the Galois group of K_1K_2 over K_2 which induces σ_1 on K_1. This σ is *a fortiori* in G, and induces the identity on K_2. Hence $G_1 \times \{e_2\}$ is contained in the image of our homomorphism (where e_2 is the unit element of G_2). Similarly, $\{e_1\} \times G_2$ is contained in this image. Hence their product is contained in the image, and their product is precisely $G_1 \times G_2$. This proves Theorem 1.14.



Corollary 1.15. *Let $K_1, \ldots, K_n$ be Galois extensions of k with Galois groups $G_1, \ldots, G_n$. Assume that $K_{i+1} \cap (K_1 \cdots K_i) = k$ for each $i = 1, \ldots, n-1$. Then the Galois group of $K_1 \cdots K_n$ is isomorphic to the product $G_1 \times \cdots \times G_n$ in the natural way.*

Proof. Induction.

Corollary 1.16. *Let K be a finite Galois extension of k with group G, and assume that G can be written as a direct product $G = G_1 \times \cdots \times G_n$. Let K_i be the fixed field of*

$$G_1 \times \cdots \times \{1\} \times \cdots \times G_n$$

where the group with 1 element occurs in the i-th place. Then K_i is Galois over k, and $K_{i+1} \cap (K_1 \cdots K_i) = k$. Furthermore $K = K_1 \cdots K_n$.

Proof. By Corollary 1.3, the compositum of all K_i belongs to the intersection of their corresponding groups, which is clearly the identity. Hence the compositum is equal to K. Each factor of G is normal in G, so K_i is Galois over k. By Corollary 1.4, the intersection of normal extensions belongs to the product of their Galois groups, and it is then clear that $K_{i+1} \cap (K_1 \cdots K_i) = k$.

Theorem 1.17. *Assume all fields contained in some common field.*

(i) *If K, L are abelian over k, so is the composite KL.*

(ii) *If K is abelian over k and E is any extension of k, then KE is abelian over E.*

(iii) *If K is abelian over k and $K \supset E \supset k$ where E is an intermediate field, then E is abelian over k and K is abelian over E.*

Proof. Immediate from Theorems 1.12 and 1.14.

If k is a field, the composite of all abelian extensions of k in a given algebraic closure k^a is called the **maximum abelian extension** of k, and is denoted by k^{ab}.

Remark on notation. We have used systematically the notation:

k^a = algebraic closure of k;

k^s = separable closure of k;

k^{ab} = abelian closure of k = maximal abelian extension.

We have replaced other people's notation $\bar{k}$ (and mine as well in the first edition) with k^a in order to make the notation functorial with respect to the ideas.

§2. EXAMPLES AND APPLICATIONS

Let k be a field and $f(X)$ a separable polynomial of degree $\geqq 1$ in $k[X]$. Let

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

be its factorization in a splitting field K over k. Let G be the Galois group of K over k. We call G the **Galois group** of f over k. Then the elements of G permute the roots of f. Thus we have an injective homomorphism of G into the symmetric group S_n on n elements. Not every permutation need be given by an element of G. We shall discuss examples below.

Example 1. Quadratic extensions. Let k be a field and $a \in k$. If a is not a square in k, then the polynomial $X^2 - a$ has no root in k and is therefore irreducible. Assume char $k \neq 2$. Then the polynomial is separable (because $2 \neq 0$), and if α is a root, then $k(\alpha)$ is the splitting field, is Galois, and its Galois group is cyclic of order 2.

Conversely, given an extension K of k of degree 2, there exists $a \in k$ such that $K = k(\alpha)$ and $\alpha^2 = a$. This comes from completing the square and the quadratic formula as in elementary school. The formula is valid as long as the characteristic of k is $\neq 2$.

Example 2. Cubic extensions. Let k be a field of characteristic $\neq 2$ or 3. Let

$$f(X) = X^3 + aX + b.$$

Any polynomial of degree 3 can be brought into this form by completing the cube. Assume that f has no root in k. Then f is irreducible because any factorization must have a factor of degree 1. Let α be a root of $f(X)$. Then

$$[k(\alpha): k] = 3.$$

Let K be the splitting field. Since char $k \neq 2, 3$, f is separable. Let G be the Galois group. Then G has order 3 or 6 since G is a subgroup of the symmetric group S_3. In the second case, $k(\alpha)$ is not normal over k.

There is an easy way to test whether the Galois group is the full symmetric group. We consider the discriminant. If $\alpha_1, \alpha_2, \alpha_3$ are the distinct roots of $f(X)$, we let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) \quad \text{and} \quad \Delta = \delta^2.$$

If G is the Galois group and $\sigma \in G$ then $\sigma(\delta) = \pm\delta$. Hence σ leaves Δ fixed. Thus Δ is in the ground field k, and in Chapter IV, §6, we have seen that

$$\Delta = -4a^3 - 27b^2.$$

The set of σ in G which leave δ fixed is precisely the set of even permutations. Thus G is the symmetric group if and only if Δ is not a square in k. We may summarize the above remarks as follows.

Let $f(X)$ be a cubic polynomial in $k[X]$, and assume char $k \neq 2, 3$. *Then:*

(a) *f is irreducible over k if and only if f has no root in k.*

(b) *Assume f irreducible. Then the Galois group of f is S_3 if and only if the discriminant of f is not a square in k. If the discriminant is a square, then the Galois group is cyclic of order* 3, *equal to the alternating group A_3 as a permutation of the roots of f.*

For instance, consider

$$f(X) = X^3 - X + 1$$

over the rational numbers. Any rational root must be 1 or -1, and so $f(X)$ is irreducible over $\mathbf{Q}$. The discriminant is -23, and is not a square. Hence the Galois group is the symmetric group. The splitting field contains a subfield of degree 2, namely $k(\delta) = k(\sqrt{\Delta})$.

On the other hand, let $f(X) = X^3 - 3X + 1$. Then f has no root in $\mathbf{Z}$, whence no root in $\mathbf{Q}$, so f is irreducible. The discriminant is 81, which is a square, so the Galois group is cyclic of order 3.

Example 3. We consider the polynomial $f(X) = X^4 - 2$ over the rationals $\mathbf{Q}$. It is irreducible by Eisenstein's criterion. Let α be a real root.

Let $i = \sqrt{-1}$. Then $\pm\alpha$ and $\pm i\alpha$ are the four roots of $f(X)$, and

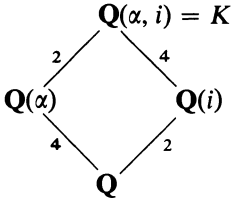
$$[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4.$$

Hence the splitting field of $f(X)$ is

$$K = \mathbf{Q}(\alpha, i).$$

The field $\mathbf{Q}(\alpha) \cap \mathbf{Q}(i)$ has degree 1 or 2 over $\mathbf{Q}$. The degree cannot be 2 otherwise $i \in \mathbf{Q}(\alpha)$, which is impossible since α is real. Hence the degree is 1. Hence i has degree 2 over $\mathbf{Q}(\alpha)$ and therefore $[K : \mathbf{Q}] = 8$. The Galois group of $f(X)$ has order 8.

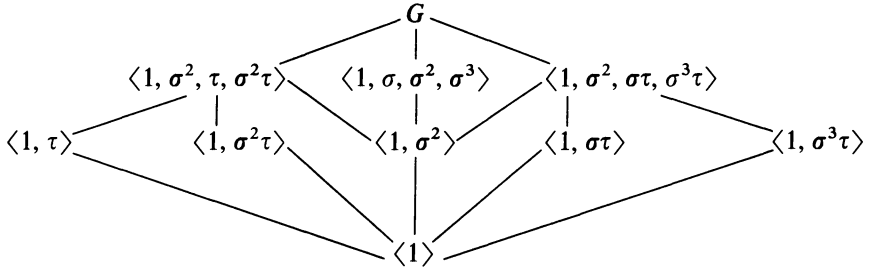
There exists an automorphism τ of K leaving $\mathbf{Q}(\alpha)$ fixed, sending i to $-i$, because K is Galois over $\mathbf{Q}(\alpha)$, of degree 2. Then $\tau^2 = \mathrm{id}$.



By the multiplicativity of degrees in towers, we see that the degrees are as indicated in the diagram. Thus $X^4 - 2$ is irreducible over $\mathbf{Q}(i)$. Also, K is normal over $\mathbf{Q}(i)$. There exists an automorphism σ of K over $\mathbf{Q}(i)$ mapping the root α of $X^4 - 2$ to the root $i\alpha$. Then one verifies at once that $1, \sigma, \sigma^2, \sigma^3$ are distinct and $\sigma^4 = \mathrm{id}$. Thus σ generates a cyclic group of order 4. We denote it by $\langle\sigma\rangle$. Since $\tau \notin \langle\sigma\rangle$ it follows that $G = \langle\sigma, \tau\rangle$ is generated by σ and τ because $\langle\sigma\rangle$ has index 2. Furthermore, one verifies directly that

$$\tau\sigma = \sigma^3\tau,$$

because this relation is true when applied to α and i which generate K over $\mathbf{Q}$. This gives us the structure of G. It is then easy to verify that the lattice of subgroups is as follows:



Example 4. Let k be a field and let $t_1, \ldots, t_n$ be algebraically independent over k. Let $K = k(t_1, \ldots, t_n)$. The symmetric group G on n letters operates on K by permuting $(t_1, \ldots, t_n)$ and its fixed field is the field of symmetric functions, by definition the field of those elements of K fixed under G. Let $s_1, \ldots, s_n$ be the elementary symmetric polynomials, and let

$$f(X) = \prod_{i=1}^{n} (X - t_i).$$

Up to a sign, the coefficients of f are $s_1, \ldots, s_n$. We let $F = K^G$. We contend that $F = k(s_1, \ldots, s_n)$. Indeed,

$$k(s_1, \ldots, s_n) \subset F.$$

On the other hand, K is the splitting field of $f(X)$, and its degree over F is $n!$. Its degree over $k(s_1, \ldots, s_n)$ is $\leqq n!$ and hence we have equality, $F = k(s_1, \ldots, s_n)$.

The polynomial $f(X)$ above is called the general polynomial of degree n. We have just constructed a Galois extension whose Galois group is the symmetric group.

Using the Hilbert irreducibility theorem, one can construct a Galois extension of $\mathbf{Q}$ whose Galois group is the symmetric group. (Cf. Chapter VII, end of §2, and [La 83], Chapter IX.) It is unknown whether given a finite group G, there exists a Galois extension of $\mathbf{Q}$ whose Galois group is G. By specializing parameters, Emmy Noether remarked that one could prove this if one knew that every field E such that

$$\mathbf{Q}(s_1, \ldots, s_n) \subset E \subset \mathbf{Q}(t_1, \ldots, t_n)$$

is isomorphic to a field generated by n algebraically independent elements. However, matters are not so simple, because Swan proved that the fixed field of a cyclic subgroup of the symmetric group is not necessarily generated by algebraically independent elements over k [Sw 69], [Sw 83].

Example 5. *We shall prove that the complex numbers are algebraically closed.* This will illustrate almost all the theorems we have proved previously.

We use the following properties of the real numbers $\mathbf{R}$: It is an ordered field, every positive element is a square, and every polynomial of odd degree in $\mathbf{R}[X]$ has a root in $\mathbf{R}$. We shall discuss ordered fields in general later, and our arguments apply to any ordered field having the above properties.

Let $i = \sqrt{-1}$ (in other words a root of $X^2 + 1$). Every element in $\mathbf{R}(i)$ has a square root. If $a + bi \in \mathbf{R}(i)$, $a, b \in \mathbf{R}$, then the square root is given by $c + di$, where

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2} \quad \text{and} \quad d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}.$$

Each element on the right of our equalities is positive and hence has a square root in $\mathbf{R}$. It is then trivial to determine the sign of c and d so that $(c + di)^2 = a + bi$.

Since $\mathbf{R}$ has characteristic 0, every finite extension is separable. Every finite extension of $\mathbf{R}(i)$ is contained in an extension K which is finite and Galois over $\mathbf{R}$. We must show that $K = \mathbf{R}(i)$. Let G be the Galois group over $\mathbf{R}$ and let H be a 2-Sylow subgroup of G. Let F be its fixed field. Counting degrees and orders, we find that the degree of F over $\mathbf{R}$ is odd. By the primitive element theorem, there exists an element $\alpha \in F$ such that $F = \mathbf{R}(\alpha)$. Then α is the root of an irreducible polynomial in $\mathbf{R}[X]$ of odd degree. This can happen only if this degree is 1. Hence $G = H$ is a 2-group.

We now see that K is Galois over $\mathbf{R}(i)$. Let G_1 be its Galois group. Since G_1 is a p-group (with $p = 2$), if G_1 is not the trivial group, then G_1 has a subgroup G_2 of index 2. Let F be the fixed field of G_2. Then F is of degree 2 over $\mathbf{R}(i)$; it is a quadratic extension. But we saw that every element of $\mathbf{R}(i)$ has a square root, and hence that $\mathbf{R}(i)$ has no extensions of degree 2. It follows that G_1 is the trivial group and $K = \mathbf{R}(i)$, which is what we wanted.

(The basic ideas of the above proof were already in Gauss. The variation of the ideas which we have selected, making a particularly efficient use of the Sylow group, is due to Artin.)

Example 6. Let $f(X)$ be an irreducible polynomial over the field k, and assume that f is separable. Then the Galois group G of the splitting field is represented as a group of permutations of the n roots, where $n = \deg f$. Whenever one has a criterion for this group to be the full symmetric group S_n, then one can see if it applies to this representation of G. For example, it is an easy exercise (cf. Chapter I, Exercise 38) that for p prime, S_p is generated by $[123 \cdots p]$ and any transposition. We then have the following result.

Let $f(X)$ be an irreducible polynomial with rational coefficients and of degree p prime. If f has precisely two nonreal roots in the complex numbers, then the Galois group of f is S_p.

Proof. The order of G is divisible by p, and hence by Sylow's theorem, G contains an element of order p. Since G is a subgroup of S_p which has order $p!$, it follows that an element of order p can be represented by a p-cycle $[123 \cdots p]$ after a suitable ordering of the roots, because any smaller cycle has order less than p, so relatively prime to p. But the pair of complex conjugate roots shows that complex conjugation induces a transposition in G. Hence the group is all of S_p.

A specific case is easily given. Drawing the graph of

$$f(X) = X^5 - 4X + 2$$

shows that f has exactly three real roots, so exactly two complex conjugate roots. Furthermore f is irreducible over $\mathbf{Q}$ by Eisenstein's criterion, so we can apply the general statement proved above to conclude that the Galois group of f over $\mathbf{Q}$ is S_5. See also Exercise 17 of Chapter IV.

Example 7. The preceding example determines a Galois group by finding some subgroups passing to an extension field of the ground field. There are other possible extensions of $\mathbf{Q}$ rather than the reals, for instance p-adic fields which will be discussed later in this book. However, instead of passing to an extension field, it is possible to use reduction mod p. For our purposes here, we assume the following statement, which will be proved in Chapter VII, theorem 2.9.

Let $f(X) \in \mathbf{Z}[X]$ be a polynomial with integral coefficients, and leading coefficient 1. Let p be a prime number. Let $\bar{f}(X) = f(X) \bmod p$ be the polynomial obtained by reducing the coefficients mod p. Assume that $\bar{f}$ has no multiple roots in an algebraic closure of $\mathbf{F}_p$. Then there exists a bijection

$$(\alpha_1, \ldots, \alpha_n) \mapsto (\bar{\alpha}_1, \ldots, \bar{\alpha}_n)$$

of the roots of f onto those of $\bar{f}$, and an embedding of the Galois group of $\bar{f}$ as a subgroup of the Galois group of f, which gives an isomorphism of the action of those groups on the set of roots.

The embedding will be made precise in Chapter VII, but here we just want to use this result to compute Galois groups.

For instance, consider $X^5 - X - 1$ over $\mathbf{Z}$. Reducing mod 5 shows that this polynomial is irreducible. Reducing mod 2 gives the irreducible factors

$$(X^2 + X + 1)(X^3 + X^2 + 1) \pmod 2.$$

Hence the Galois group over the rationals contains a 5-cycle and a product of a 2-cycle and a 3-cycle. The third power of the product of the 2-cycle and 3-cycle is a 2-cycle, which is a transposition. Hence the Galois group contains a transposition and the cycle $[123 \cdots p]$, which generate S_p (cf. the exercises of Chapter I on the symmetric group). Thus the Galois group of $X^5 - X - 1$ is S_p.

Example 8. The technique of reducing mod primes to get lots of elements in a Galois group was used by Schur to determine the Galois groups of classical polynomials [Schur 31]. For instance, Schur proves that the Galois group over $\mathbf{Q}$ of the following polynomials over $\mathbf{Q}$ is the symmetric group:

(a) $f(X) = \sum_{m=0}^{n} X^m/m!$ (in other words, the truncated exponential series), if n is not divisible by 4. If n is divisible by 4, he gets the alternating group.

(b) Let

$$H_m(X) = (-1)^m e^{X^2/2} \frac{d^m}{dX^m}(e^{-X^2/2})$$

be the m-th Hermite polynomial. Put

$$H_{2n}(X) = K_n^{(0)}(X^2) \quad \text{and} \quad H_{2n+1}(X) = XK_n^{(1)}(X^2).$$

Then the Galois group of $K_n^{(i)}(X)$ over $\mathbf{Q}$ is the symmetric group S_n for $i = 0$, 1, provided $n > 12$. The remaining cases were settled in [Schulz 37].

Example 9. This example is addressed to those who know something about Riemann surfaces and coverings. Let t be transcendental over the complex numbers $\mathbf{C}$, and let $k = \mathbf{C}(t)$. The values of t in $\mathbf{C}$, or ∞, correspond to the points of the Gauss sphere S, viewed as a Riemann surface. Let $P_1, \ldots, P_{n+1}$ be distinct points of S. The finite coverings of $S - \{P_1, \ldots, P_{n-1}\}$ are in bijection with certain finite extensions of $\mathbf{C}(t)$, those which are unramified outside $P_1, \ldots, P_{n-1}$. Let K be the union of all these extension fields corresponding to such coverings, and let $\pi_1^{(n)}$ be the fundamental group of

$$S - \{P_1, \ldots, P_{n+1}\}.$$

Then it is known that $\pi_1^{(n)}$ is a free group on n generators, and has an embedding in the Galois group of K over $\mathbf{C}(t)$, such that the finite subfields of K over $\mathbf{C}(t)$ are in bijection with the subgroups of $\pi_1^{(n)}$ which are of finite index. Given a finite group G generated by n elements $\sigma_1, \ldots, \sigma_n$ we can find a surjective homomorphism $\pi_1^{(n)} \to G$ mapping the generators of $\pi_1^{(n)}$ on $\sigma_1, \ldots, \sigma_n$. Let H be the kernel. Then H belongs to a subfield K^H of K which is normal over $\mathbf{C}(t)$ and whose Galois group is G. In the language of coverings, H belongs to a finite covering of

$$S - \{P_1, \ldots, P_{n+1}\}.$$

Over the field $\mathbf{C}(t)$ one can use analytic techniques to determine the Galois group. The Galois group is the completion of a free group, as proved by Douady [Dou 64]. For extensions to characteristic p, see [Pop 95]. A fundamental problem is to determine the Galois group over $\mathbf{Q}(t)$, which requires much deeper insight into the number theoretic nature of this field. Basic contributions were made by Belyi [Be 80], [Be 83], who also considered the field $\mathbf{Q}(\mu)(t)$, where $\mathbf{Q}(\mu)$ is the field obtained by adjoining all roots of unity to the rationals. Belyi proved that over this latter field, essentially all the classical finite groups occur as Galois groups. See also Conjecture 14.2 below.

For Galois groups over $\mathbf{Q}(t)$, see the survey [Se 88], which contains a bibliography. One method is called the rigidity method, first applied by Shih [Shi 74], which I summarize because it gives examples of various notions defined throughout this book. The problem is to descend extensions of $\mathbf{C}(t)$ with a given Galois group G to extensions of $\mathbf{Q}(t)$ with the same Galois group. If this extension is K over $\mathbf{Q}(t)$, one also wants the extension to be regular over $\mathbf{Q}$ (see the definition in Chapter VIII, §4). To give a sufficient condition, we need some definitions. Let G be a finite group with trivial center. Let C_1, C_2, C_3 be conjugacy classes. Let $P = P(C_1, C_2, C_3)$ be the set of elements

$$(g_1, g_2, g_3) \in C_1 \times C_2 \times C_3$$

such that $g_1 g_2 g_3 = 1$. Let P' be the subset of P consisting of all elements $(g_1, g_2, g_3) \in P$ such that G is generated by g_1, g_2, g_3. We say that the family (C_1, C_2, C_3) is **rigid** if G operates transitively on P', and P' is not empty.

We define a conjugacy class C of G to be **rational** if given $g \in C$ and a positive integer s relatively prime to the order of g, then $g^s \in C$. (Assuming that the reader knows the terminology of characters defined in Chapter XVIII, this condition of rationality is equivalent to the condition that every character χ of G has values in the rational numbers $\mathbf{Q}$.) One then has the following theorem, which is contained in the works of Shih, Fried, Belyi, Matzat and Thompson.

Rigidity theorem. *Let G be a finite group with trivial center, and let C_1, C_2, C_3 be conjugacy classes which are rational, and such that the family (C_1, C_2, C_3) is rigid. Then there exists a Galois extension of $\mathbf{Q}(t)$ with Galois group G (and such that the extension is regular over $\mathbf{Q}$).*

Bibliography

[Be 80] G. BELYI, Galois extensions of the maximal cyclotomic field, *Izv. Akad. Nauk SSR* **43** (1979) pp. 267–276 (= *Math. USSR Izv.* **14** (1980), pp. 247–256

[Be 83] G. BELYI, On extensions of the maximal cyclotomic field having a given classical Galois group, *J. reine angew. Math.* **341** (1983), pp. 147–156

[Dou 64] A. DOUADY, Determination d'un groupe de Galois, *C.R. Acad. Sci.* **258** (1964), pp. 5305–5308

[La 83] S. LANG, *Fundamentals of Diophantine Geometry.* Springer Verlag 1983

[Pop 95] F. POP, Etale Galois covers of affine smooth curves, *Invent. Math.* **120** (1995), pp. 555–578

[Se 88] J.-P.. SERRE, Groupes de Galois sur $\mathbf{Q}$, *Séminaire Bourbaki*, 1987–1988 *Astérisque* **161–162**, pp. 73–85

[Shi 74] R.-Y. SHIH, On the construction of Galois extensions of function fields and number fields, *Math. Ann.* **207** (1974), pp. 99–120

[Sw 69] R. SWAN, Invariant rational functions and a problem of Steenrod, *Invent. Math.* **7** (1969), pp. 148–158

[Sw 83] R. SWAN, Noether's problem in Galois theory, *Emmy Noether in Bryn Mawr*, J. D. Sally and B. Srinivasan, eds., Springer Verlag, 1983, pp. 40

§3. ROOTS OF UNITY

Let k be a field. By a **root of unity** (in k) we shall mean an element $\zeta \in k$ such that $\zeta^n = 1$ for some integer $n \geqq 1$. If the characteristic of k is p, then the equation

$$X^{p^m} = 1$$

has only one root, namely 1, and hence there is no p^m-th root of unity except 1.

Let n be an integer > 1 and not divisible by the characteristic. The polynomial

$$X^n - 1$$

is separable because its derivative is $nX^{n-1} \neq 0$, and the only root of the derivative is 0, so there is no common root. Hence in k^a the polynomial $X^n - 1$ has n distinct roots, which are roots of unity. They obviously form a group, and we know that every finite multiplicative group in a field is cyclic (Chapter IV, Theorem 1.9). Thus the group of n-th roots of unity is cyclic. A generator for this group is called a **primitive** n-th root of unity.

If μ_n denotes the group of all n-th roots of unity in k^a and m, n are relatively prime integers, then

$$\mu_{mn} \approx \mu_m \times \mu_n.$$

This follows because μ_m, μ_n cannot have any element in common except 1, and because $\mu_m\mu_n$ consequently has mn elements, each of which is an mn-th root of unity. Hence $\mu_m\mu_n = \mu_{mn}$, and the decomposition is that of a direct product.

As a matter of notation, to avoid double indices, especially in the prime power case, we write $\mu[n]$ for μ_n. So if p is a prime, $\mu[p^r]$ is the group of p^r-th roots of unity. Then $\mu[p^\infty]$ denotes the union of all $\mu[p^r]$ for all positive integers r. See the comments in §14.

Let k be any field. Let n be not divisible by the characteristic p. Let $\zeta = \zeta_n$ be a primitive n-th root of unity in k^a. Let σ be an embedding of $k(\zeta)$ in k^a over k. Then

$$(\sigma\zeta)^n = \sigma(\zeta^n) = 1$$

so that $\sigma\zeta$ is an n-th root of unity also. Hence $\sigma\zeta = \zeta^i$ for some integer $i = i(\sigma)$, uniquely determined mod n. It follows that σ maps $k(\zeta)$ into itself, and hence that $k(\zeta)$ is normal over k. If τ is another automorphism of $k(\zeta)$ over k then

$$\sigma\tau\zeta = \zeta^{i(\sigma)i(\tau)}.$$

Since σ and τ are automorphisms, it follows that $i(\sigma)$ and $i(\tau)$ are prime to n (otherwise, $\sigma\zeta$ would have a period smaller than n). In this way we get a homomorphism of the Galois group G of $k(\zeta)$ over k into the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^*$ of integers prime to n, mod n. Our homomorphism is clearly injective since $i(\sigma)$ is uniquely determined by σ mod n, and the effect of σ on $k(\zeta)$ is determined by its effect on ζ. *We conclude that $k(\zeta)$ is abelian over k.*

We know that the order of $(\mathbf{Z}/n\mathbf{Z})^*$ is $\varphi(n)$. Hence the degree $[k(\zeta):k]$ divides $\varphi(n)$.

For a specific field k, the question arises whether the image of $G_{\kappa(\zeta)/\kappa}$ in $(\mathbf{Z}/n\mathbf{Z})^*$ is all of $(\mathbf{Z}/n\mathbf{Z})^*$. Looking at $\kappa = \mathbf{R}$ or $\mathbf{C}$, one sees that this is not always the case. We now give an important example when it is the case.

Theorem 3.1. *Let ζ be a primitive n-th root of unity. Then*

$$[\mathbf{Q}(\zeta):\mathbf{Q}] = \varphi(n),$$

where φ is the Euler function. The map $\sigma \mapsto i(\sigma)$ gives an isomorphism

$$G_{\mathbf{Q}(\zeta)/\mathbf{Q}} \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^*.$$

Proof. Let $f(X)$ be the irreducible polynomial of ζ over $\mathbf{Q}$. Then $f(X)$ divides $X^n - 1$, say $X^n - 1 = f(X)h(X)$, where both f, h have leading coefficient 1. By the Gauss lemma, it follows that f, h have integral coefficients. We shall now prove that if p is a prime number not dividing n, then ζ^p is also a root of f. Since ζ^p is also a primitive n-th root of unity, and since any primitive n-th root of unity can be obtained by raising ζ to a succession of prime powers, with primes not dividing n, this will imply that all the primitive n-th roots of unity are roots of f, which must therefore have degree $\geqq \varphi(n)$, and hence precisely $\varphi(n)$.

Suppose ζ^p is not a root of f. Then ζ^p is a root of h, and ζ itself is a root of $h(X^p)$. Hence $f(X)$ divides $h(X^p)$, and we can write

$$h(X^p) = f(X)g(X).$$

Since f has integral coefficients and leading coefficient 1, we see that g has integral coefficients. Since $a^p \equiv a \pmod{p}$ for any integer a, we conclude that

$$h(X^p) \equiv h(X)^p \pmod{p},$$

and hence

$$h(X)^p \equiv f(X)g(X) \pmod{p}.$$

In particular, if we denote by $\bar{f}$ and $\bar{h}$ the polynomials in $\mathbf{Z}/p\mathbf{Z}$ obtained by reducing f and h respectively mod p, we see that $\bar{f}$ and $\bar{h}$ are not relatively prime, i.e. have a factor in common. But $X^n - \bar{1} = \bar{f}(X)\bar{h}(X)$, and hence $X^n - \bar{1}$ has multiple roots. This is impossible, as one sees by taking the derivative, and our theorem is proved.

Corollary 3.2. *If n, m are relative prime integers $\geqq 1$, then*

$$\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_m) = \mathbf{Q}.$$

Proof. We note that ζ_n and ζ_m are both contained in $\mathbf{Q}(\zeta_{mn})$ since ζ_{mn}^n is a primitive m-th root of unity. Furthermore, $\zeta_m\zeta_n$ is a primitive mn-th root of unity. Hence

$$\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m) = \mathbf{Q}(\zeta_{mn}).$$

Our assertion follows from the multiplicativity $\varphi(mn) = \varphi(m)\varphi(n)$.

Suppose that n is a prime number p (having nothing to do with the characteristic). Then

$$X^p - 1 = (X - 1)(X^{p-1} + \cdots + 1).$$

Any primitive p-th root of unity is a root of the second factor on the right of this equation. Since there are exactly $p - 1$ primitive p-th roots of unity, we conclude that these roots are precisely the roots of

$$X^{p-1} + \cdots + 1.$$

We saw in Chapter IV, §3 that this polynomial could be transformed into an Eisenstein polynomial over the rationals. This gives another proof that $[\mathbf{Q}(\zeta_p)\colon \mathbf{Q}] = p - 1$.

We investigate more closely the factorization of $X^n - 1$, and suppose that we are in characteristic 0 for simplicity.

We have

$$X^n - 1 = \prod_{\zeta}(X - \zeta),$$

where the product is taken over all n-th roots of unity. Collect together all terms belonging to roots of unity having the same period. Let

$$\Phi_d(X) = \prod_{\text{period } \zeta = d}(X - \zeta)$$

Then

$$X^n - 1 = \prod_{d|n}\Phi_d(X).$$

We see that $\Phi_1(X) = X - 1$, and that

$$\Phi_n(X) = \frac{X^n - 1}{\prod\limits_{\substack{d|n \\ d<n}} \Phi_d(X)}.$$

From this we can compute $\Phi(X)$ recursively, and we see that $\Phi_n(X)$ is a polynomial in $\mathbf{Q}[X]$ because we divide recursively by polynomials having coefficients in $\mathbf{Q}$. All our polynomials have leading coefficient 1, so that in fact $\Phi_n(X)$ has *integer coefficients* by Theorem 1.1 of Chapter IV. Thus our construction is essentially universal and would hold over any field (whose characteristic does not divide n).

We call $\Phi_n(X)$ the n-th **cyclotomic polynomial**.

The roots of Φ_n are precisely the primitive n-th roots of unity, and hence

$$\deg \Phi_n = \varphi(n).$$

From Theorem 3.1 we conclude that Φ_n is irreducible over $\mathbf{Q}$, *and hence*

$$\Phi_n(X) = \operatorname{Irr}(\zeta_n, \mathbf{Q}, X).$$

We leave the proofs of the following recursion formulas as exercises:

1. If p is a prime number, then

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1,$$

and for an integer $r \geqq 1$,

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}}).$$

2. Let $n = p_1^{r_1} \cdots p_s^{r_s}$ be a positive integer with its prime factorization. Then

$$\Phi_n(X) = \Phi_{p_1 \cdots p_s}(X^{p_1^{r_1-1} \cdots p_s^{r_s-1}}).$$

3. If n is odd > 1, then $\Phi_{2n}(X) = \Phi_n(-X)$.
4. If p is a prime number, not dividing n, then

$$\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}.$$

On the other hand, if $p \mid n$, then $\Phi_{pn}(X) = \Phi_n(X^p)$.

5. We have

$$\Phi_n(X) = \prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)}.$$

As usual, μ is the Möbius function:

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by } p^2 \text{ for some prime } p, \\ (-1)^r & \text{if } n = p_1 \cdots p_r \text{ is a product of distinct primes,} \\ 1 & \text{if } n = 1. \end{cases}$$

As an exercise, show that

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Example. In light of Exercise 21 of Chapter V, we note that the association $n \mapsto \Phi_n(X)$ can be viewed as a function from the positive integers into the multiplicative group of non-zero rational functions. The multiplication formula $X^n - 1 = \prod \Phi_d(X)$ can therefore be inverted by the general formalism of convolutions. Computations of a number of cyclotomic polynomials show that for low values of n, they have coefficients equal to 0 or ± 1. However, I am indebted to Keith Conrad for bringing to my attention an extensive literature on the subject, starting with Bang in 1895. I include only the first and last items:

A. S. BANG, Om Ligningen $\Phi_m(X) = 0$, *Nyt Tidsskrift for Matematik* **(B) 6** (1895), pp. 6–12

H. L. MONTGOMERY and R. C. VAUGHN, The order of magnitude of the m-th coefficients of cyclotomic polynomials, *Glasgow Math. J.* **27** (1985), pp. 143–159

In particular, if $\Phi_n(X) = \Sigma a_{nj}X^j$, define $L(j) = \log \max_n |a_{nj}|$. Then Montgomery and Vaughn prove that

$$\frac{j^{1/2}}{(\log j)^{1/4}} \ll L(j) \ll \frac{j^{1/2}}{(\log j)^{1/4}}$$

where the sign $\ll$ means that the left-hand side is at most a positive constant times the right-hand side for $j \to \infty$. Bang also points out that $\Phi_{105}(X)$ is a cyclotomic polynomial of smallest degree having coefficients $\neq 0$ or ± 1: the coefficient of X^7 and X^{41} is -2 (all others are 0 or ± 1).

If ζ is an n-th root of unity and $\zeta \neq 1$, then

$$\frac{1 - \zeta^n}{1 - \zeta} = 1 + \zeta + \cdots + \zeta^{n-1} = 0.$$

This is trivial, but useful.

Let $\mathbf{F}_q$ be the finite field with q elements, q equal to a power of the odd prime number p. Then $\mathbf{F}_q^*$ has $q - 1$ elements and is a cyclic group. Hence we have the index

$$(\mathbf{F}_q^* : \mathbf{F}_q^{*2}) = 2.$$

If v is a non-zero integer not divisible by p, let

$$\left(\frac{v}{p}\right) = \begin{cases} 1 & \text{if } v \equiv x^2 \pmod{p} \text{ for some } x, \\ -1 & \text{if } v \not\equiv x^2 \pmod{p} \text{ for all } x. \end{cases}$$

This is known as the **quadratic symbol**, and depends only on the residue class of v mod p.

From our preceding remark, we see that there are as many quadratic residues as there are non-residues mod p.

Theorem 3.3. *Let ζ be a primitive p-th root of unity, and let*

$$S = \sum_v \left(\frac{v}{p}\right)\zeta^v,$$

the sum being taken over non-zero residue classes mod p. Then

$$S^2 = \left(\frac{-1}{p}\right)p.$$

Every quadratic extension of $\mathbf{Q}$ is contained in a cyclotomic extension.

Proof. The last statement follows at once from the explicit expression of $\pm p$ as a square in $\mathbf{Q}(\zeta)$, because the square root of an integer is contained in the

field obtained by adjoining the square root of the prime factors in its factorization, and also $\sqrt{-1}$. Furthermore, for the prime 2, we have $(1+i)^2 = 2i$. We now prove our assertion concerning S^2. We have

$$S^2 = \sum_{\nu,\mu} \left(\frac{\nu}{p}\right)\left(\frac{\mu}{p}\right)\zeta^{\nu+\mu} = \sum_{\nu,\mu} \left(\frac{\nu\mu}{p}\right)\zeta^{\nu+\mu}.$$

As ν ranges over non-zero residue classes, so does $\nu\mu$ for any fixed μ, and hence replacing ν by $\nu\mu$ yields

$$S^2 = \sum_{\nu,\mu} \left(\frac{\nu\mu^2}{p}\right)\zeta^{\mu(\nu+1)} = \sum_{\nu,\mu} \left(\frac{\nu}{p}\right)\zeta^{\mu(\nu+1)}$$

$$= \sum_{\mu} \left(\frac{-1}{p}\right)\zeta^0 + \sum_{\nu \neq -1} \left(\frac{\nu}{p}\right) \sum_{\mu} \zeta^{\mu(\nu+1)}.$$

But $1 + \zeta + \cdots + \zeta^{p-1} = 0$, and the sum on the right over μ consequently yields -1. Hence

$$S^2 = \left(\frac{-1}{p}\right)(p-1) + (-1) \sum_{\nu \neq -1} \left(\frac{\nu}{p}\right)$$

$$= p\left(\frac{-1}{p}\right) - \sum_{\nu} \left(\frac{\nu}{p}\right)$$

$$= p\left(\frac{-1}{p}\right),$$

as desired.

We see that $\mathbf{Q}(\sqrt{p})$ is contained in $\mathbf{Q}(\zeta, \sqrt{-1})$ or $\mathbf{Q}(\zeta)$, depending on the sign of the quadratic symbol with -1. An extension of a field is said to be **cyclotomic** if it is contained in a field obtained by adjoining roots of unity. We have shown above that quadratic extensions of $\mathbf{Q}$ are cyclotomic. A theorem of Kronecker asserts that every abelian extension of $\mathbf{Q}$ is cyclotomic, but the proof needs techniques which cannot be covered in this book.

§4. LINEAR INDEPENDENCE OF CHARACTERS

Let G be a monoid and K a field. By a **character** of G in K (in this chapter), we shall mean a homomorphism

$$\chi: G \to K^*$$

of G into the multiplicative group of K. The **trivial character** is the homo-

morphism taking the constant value 1. Functions $f_i: G \to K$ are called **linearly independent** over K if whenever we have a relation

$$a_1 f_1 + \cdots + a_n f_n = 0$$

with $a_i \in K$, then all $a_i = 0$.

Examples. Characters will occur in various contexts in this book. First, the various conjugate embeddings of an extension field in an algebraic closure can be viewed as characters. These are the characters which most concern us in this chapter. Second, we shall meet characters in Chapter XVIII, when we shall extend the next theorem to a more general kind of character in connection with group representations.

Next, one meets characters in analysis. For instance, given an integer m, the function $f: \mathbf{R}/\mathbf{Z} \to \mathbf{C}^*$ such that $f(x) = e^{2\pi i m x}$ is a character on $\mathbf{R}/\mathbf{Z}$. It can be shown that all continuous homomorphisms of $\mathbf{R}/\mathbf{Z}$ into $\mathbf{C}^*$ are of this type. Similarly, given a real number y, the function $x \mapsto e^{2\pi i x y}$ is a continuous character on $\mathbf{R}$, and it is shown in Fourier analysis that all continuous characters of absolute value 1 on $\mathbf{R}$ are of this type.

Further, let X be a compact space and let R be the ring of continuous complex-valued functions on X. Let R^* be the group of units of R. Then given $x \in X$ the evaluation map $f \mapsto f(x)$ is a character of R^* into $\mathbf{C}^*$. (Actually, this evaluation map is a ring homomorphism of R onto $\mathbf{C}$.)

Artin found a neat way of expressing a linear independence property which covers all these cases, as well as others, in the following theorem [Ar 44].

Theorem 4.1. (Artin). *Let G be a monoid and K a field. Let $\chi_1, \ldots, \chi_n$ be distinct characters of G in K. Then they are linearly independent over K.*

Proof. One character is obviously linearly independent. Suppose that we have a relation

$$a_1 \chi_1 + \cdots + a_n \chi_n = 0$$

with $a_i \in K$, not all 0. Take such a relation with n as small as possible. Then $n \geqq 2$, and no a_i is equal to 0. Since χ_1, χ_2 are distinct, there exists $z \in G$ such that $\chi_1(z) \neq \chi_2(z)$. For all $x \in G$ we have

$$a_1 \chi_1(xz) + \cdots + a_n \chi_n(xz) = 0,$$

and since χ_i is a character,

$$a_1 \chi_1(z)\chi_1 + \cdots + a_n \chi_n(z)\chi_n = 0.$$

Divide by $\chi_1(z)$ and subtract from our first relation. The term $a_1\chi_1$ cancels, and we get a relation

$$\left(a_2 \frac{\chi_2(z)}{\chi_1(z)} - a_2\right)\chi_2 + \cdots = 0.$$

The first coefficient is not 0, and this is a relation of smaller length than our first relation, contradiction.

As an application of Artin's theorem, one can consider the case when K is a finite normal extension of a field k, and when the characters are distinct automorphisms $\sigma_1, \ldots, \sigma_n$ of K over k, viewed as homomorphisms of K^* into K^*. This special case had already been considered by Dedekind, who, however, expressed the theorem in a somewhat different way, considering the determinant constructed from $\sigma_i \omega_j$ where ω_j is a suitable set of elements of K, and proving in a more complicated way the fact that this determinant is not 0. The formulation given above and its particularly elegant proof are due to Artin.

As another application, we have:

Corollary 4.2. *Let $\alpha_1, \ldots, \alpha_n$ be distinct non-zero elements of a field K. If $a_1, \ldots, a_n$ are elements of K such that for all integers $\nu \geqq 0$ we have*

$$a_1 \alpha_1^\nu + \cdots + a_n \alpha_n^\nu = 0$$

then $a_i = 0$ for all i.

Proof. We apply the theorem to the distinct homomorphisms

$$\nu \mapsto \alpha_i^\nu$$

of $\mathbf{Z}_{\geqq 0}$ into K^*.

Another interesting application will be given as an exercise (relative invariants).

§5. THE NORM AND TRACE

Let E be a finite extension of k. Let $[E:k]_s = r$, and let

$$p^\mu = [E:k]_i$$

if the characteristic is $p > 0$, and 1 otherwise. Let $\sigma_1, \ldots, \sigma_r$ be the distinct embeddings of E in an algebraic closure k^a of k. If α is an element of E, we define its **norm** from E to k to be

$$N_{E/k}(\alpha) = N_k^E(\alpha) = \prod_{\nu=1}^{r} \sigma_\nu \alpha^{p^\mu} = \left(\prod_{\nu=1}^{r} \sigma_\nu \alpha \right)^{[E:k]_i}.$$

Similarly, we define the **trace**

$$\mathrm{Tr}_{E/k}(\alpha) = \mathrm{Tr}_k^E(\alpha) = [E:k]_i \sum_{\nu=1}^{r} \sigma_\nu \alpha.$$

The trace is equal to 0 if $[E:k]_i > 1$, in other words, if E/k is not separable.

Thus if E is separable over k, we have

$$N_k^E(\alpha) = \prod_\sigma \sigma\alpha$$

where the product is taken over the distinct embeddings of E in k^a over k.

Similarly, if E/k is separable, then

$$\mathrm{Tr}_k^E(\alpha) = \sum_\sigma \sigma\alpha.$$

Theorem 5.1. *Let E/k be a finite extension. Then the norm N_k^E is a multiplicative homomorphism of E^* into k^* and the trace is an additive homomorphism of E into k. If $E \supset F \supset k$ is a tower of fields, then the two maps are transitive, in other words,*

$$N_k^E = N_k^F \circ N_F^E \quad \text{and} \quad \mathrm{Tr}_k^E = \mathrm{Tr}_k^F \circ \mathrm{Tr}_F^E.$$

If $E = k(\alpha)$, and $f(X) = \mathrm{Irr}(\alpha, k, X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, then

$$N_k^{k(\alpha)}(\alpha) = (-1)^n a_0 \quad \text{and} \quad \mathrm{Tr}_k^{k(\alpha)}(\alpha) = -a_{n-1}.$$

Proof. For the first assertion, we note that α^{p^μ} is separable over k if $p^\mu = [E : k]_i$. On the other hand, the product

$$\prod_{v=1}^{r} \sigma_v \alpha^{p^\mu}$$

is left fixed under any isomorphism into k^a because applying such an isomorphism simply permutes the factors. Hence this product must lie in k since α^{p^μ} is separable over k. A similar reasoning applies to the trace.

For the second assertion, let $\{\tau_j\}$ be the family of distinct embeddings of F into k^a over k. Extend each τ_j to an automorphism of k^a, and denote this extension by τ_j also. Let $\{\sigma_i\}$ be the family of embeddings of E in k^a over F. (Without loss of generality, we may assume that $E \subset k^a$.) If σ is an embedding of E over k in k^a, then for some j, $\tau_j^{-1}\sigma$ leaves F fixed, and hence $\tau_j^{-1}\sigma = \sigma_i$ for some i. Hence $\sigma = \tau_j\sigma_i$ and consequently the family $\{\tau_j\sigma_i\}$ gives all distinct embeddings of E into k^a over k. Since the inseparability degree is multiplicative in towers, our assertion concerning the transitivity of the norm and trace is obvious, because we have already shown that N_F^E maps E into F, and similarly for the trace.

Suppose now that $E = k(\alpha)$. We have

$$f(X) = ((X - \alpha_1) \cdots (X - \alpha_r))^{[E:k]_i}$$

if $\alpha_1, \ldots, \alpha_r$ are the distinct roots of f. Looking at the constant term of f gives us the expression for the norm, and looking at the next to highest term gives us the expression for the trace.

We observe that the trace is a k-linear map of E into k, namely

$$\mathrm{Tr}_k^E(c\alpha) = c\,\mathrm{Tr}_k^E(\alpha)$$

for all $\alpha \in E$ and $c \in k$. This is clear since c is fixed under every embedding of E over k. Thus the trace is a k-linear functional of E into k. For simplicity, we write $\mathrm{Tr} = \mathrm{Tr}_k^E$.

Theorem 5.2. *Let E be a finite separable extension of k. Then $\mathrm{Tr} : E \to k$ is a non-zero functional. The map*

$$(x, y) \mapsto \mathrm{Tr}(xy)$$

of $E \times E \to k$ is bilinear, and identifies E with its dual space.

Proof. That Tr is non-zero follows from the theorem on linear independence of characters. For each $x \in E$, the map

$$\mathrm{Tr}_x : E \to k$$

such that $\mathrm{Tr}_x(y) = \mathrm{Tr}(xy)$ is obviously a k-linear map, and the map

$$x \mapsto \mathrm{Tr}_x$$

is a k-homomorphism of E into its dual space $E^\vee$. (We don't write E^* for the dual space because we use the star to denote the multiplicative group of E.) If Tr_x is the zero map, then $\mathrm{Tr}(xE) = 0$. If $x \neq 0$ then $xE = E$. Hence the kernel of $x \mapsto \mathrm{Tr}_x$ is 0. Hence we get an injective homomorphism of E into the dual space $\hat{E}$. Since these spaces have the same finite dimension, it follows that we get an isomorphism. This proves our theorem.

Corollary 5.3. *Let $\omega_1, \ldots, \omega_n$ be a basis of E over k. Then there exists a basis $\omega_1', \ldots, \omega_n'$ of E over k such that $\mathrm{Tr}(\omega_i \omega_j') = \delta_{ij}$.*

Proof. The basis $\omega_1', \ldots, \omega_n'$ is none other than the dual basis which we defined when we considered the dual space of an arbitrary vector space.

Corollary 5.4. *Let E be a finite separable extension of k, and let $\sigma_1, \ldots, \sigma_n$ be the distinct set of embeddings of E into k^a over k. Let $w_1, \ldots, w_n$ be elements of E. Then the vectors*

$$\xi_1 = (\sigma_1 w_1, \ldots, \sigma_1 w_n),$$
$$\cdots$$
$$\xi_n = (\sigma_n w_1, \ldots, \sigma_n w_n)$$

are linearly independent over E if $w_1, \ldots, w_n$ form a basis of E over k.

Proof. Assume that $w_1, \ldots, w_n$ form a basis of E/k. Let $\alpha_1, \ldots, \alpha_n$ be elements of E such that

$$\alpha_1 \xi_1 + \cdots + \alpha_n \xi_n = 0.$$

Then we see that

$$\alpha_1 \sigma_1 + \cdots + \alpha_n \sigma_n$$

applied to each one of $w_1, \ldots, w_n$ gives the value 0. But $\sigma_1, \ldots, \sigma_n$ are linearly independent as characters of the multiplicative group E^* into k^{a*}. It follows that $\alpha_i = 0$ for $i = 1, \ldots, n$, and our vectors are linearly independent.

Remark. In characteristic 0, one sees much more trivially that the trace is not identically 0. Indeed, if $c \in k$ and $c \neq 0$, then $\mathrm{Tr}(c) = nc$ where $n = [E : k]$, and $n \neq 0$. This argument also holds in characteristic p when n is prime to p.

Proposition 5.5. *Let $E = k(\alpha)$ be a separable extension. Let*

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

and let $f'(X)$ be its derivative. Let

$$\frac{f(X)}{(X - \alpha)} = \beta_0 + \beta_1 X + \cdots + \beta_{n-1} X^{n-1}$$

with $\beta_i \in E$. Then the dual basis of $1, \alpha, \ldots, \alpha^{n-1}$ is

$$\frac{\beta_0}{f'(\alpha)}, \ldots, \frac{\beta_{n-1}}{f'(\alpha)}.$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of f. Then

$$\sum_{i=1}^{n} \frac{f(X)}{(X - \alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)} = X^r \qquad \text{for} \quad 0 \leqq r \leqq n - 1.$$

To see this, let $g(X)$ be the difference of the left- and right-hand side of this equality. Then g has degree $\leqq n - 1$, and has n roots $\alpha_1, \ldots, \alpha_n$. Hence g is identically zero.

The polynomials

$$\frac{f(X)}{(X - \alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)}$$

are all conjugate to each other. If we define the trace of a polynomial with coefficients in E to be the polynomial obtained by applying the trace to the coefficients, then

$$\mathrm{Tr}\left[\frac{f(X)}{(X - \alpha)} \frac{\alpha^r}{f'(\alpha)}\right] = X^r.$$

Looking at the coefficients of each power of X in this equation, we see that

$$\mathrm{Tr}\left(\alpha^i \frac{\beta_j}{f'(\alpha)}\right) = \delta_{ij},$$

thereby proving our proposition.

Finally we establish a connection with determinants, whose basic properties we now assume. Let E be a finite extension of k, which we view as a finite dimensional vector space over k. For each $\alpha \in E$ we have the k-linear map

multiplication by α,

$$m_\alpha: E \to E \quad \text{such that} \quad m_\alpha(x) = \alpha x.$$

Then we have the determinant $\det(m_\alpha)$, which can be computed as the determinant of the matrix M_α representing m_α with respect to a basis. Similarly we have the trace $\mathrm{Tr}(m_\alpha)$, which is the sum of the diagonal elements of the matrix M_α.

Proposition 5.6. *Let E be a finite extension of k and let $\alpha \in E$. Then*

$$\det(m_\alpha) = N_{E/k}(\alpha) \quad \textit{and} \quad \mathrm{Tr}(m_\alpha) = \mathrm{Tr}_{E/k}(\alpha).$$

Proof. Let $F = k(\alpha)$. If $[F : k] = d$, then $1, \alpha, \ldots, \alpha^{d-1}$ is a basis for F over k. Let $\{w_1, \ldots, w_r\}$ be a basis for E over F. Then $\{\alpha^i w_j\}$ $(i = 0, \ldots, d-1; j = 1, \ldots, r)$ is a basis for E over k. Let

$$f(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0$$

be the irreducible polynomial of α over k. Then $N_{F/k}(\alpha) = (-1)^d a_0$, and by the transitivity of the norm, we have

$$N_{E/k}(\alpha) = N_{F/k}(\alpha)^r.$$

The reader can verify directly on the above basis that $N_{F/k}(\alpha)^r$ is the determinant of m_α on F, and then that $N_{F/k}(\alpha)^d$ is the determinant of m_α on E, thus concluding the proof for the determinant. The trace is handled exactly in the same way, except that $\mathrm{Tr}_{E/k}(\alpha) = r \cdot \mathrm{Tr}_{F/k}(\alpha)$. The trace of the matrix for m_α on F is equal to $-a_{d-1}$. From this the statement identifying the two traces is immediate, as it was for the norm.

§6. CYCLIC EXTENSIONS

We recall that a finite extension is said to be cyclic if it is Galois and its Galois group is cyclic. The determination of cyclic extensions when enough roots of unity are in the ground field is based on the following fact.

Theorem 6.1. (Hilbert's Theorem 90). *Let K/k be cyclic of degree n with Galois group G. Let σ be a generator of G. Let $\beta \in K$. The norm $N_k^K(\beta) = N(\beta)$ is equal to 1 if and only if there exists an element $\alpha \neq 0$ in K such that $\beta = \alpha/\sigma\alpha$.*

Proof. Assume such an element α exists. Taking the norm of β we get $N(\alpha)/N(\sigma\alpha)$. But the norm is the product over all automorphisms in G. Inserting σ just permutes these automorphisms. Hence the norm is equal to 1.

It will be convenient to use an exponential notation as follows. If $\tau, \tau' \in G$ and $\xi \in K$ we write

$$\xi^{\tau+\tau'} = \xi^\tau \xi^{\tau'}.$$

By Artin's theorem on characters, the map given by

$$\mathrm{id} + \beta\sigma + \beta^{1+\sigma}\sigma^2 + \cdots + \beta^{1+\sigma+\cdots+\sigma^{n-2}}\sigma^{n-1}$$

on K is not identically zero. Hence there exists $\theta \in K$ such that the element

$$\alpha = \theta + \beta\theta^{\sigma} + \beta^{1+\sigma}\theta^{\sigma^2} + \cdots + \beta^{1+\sigma+\cdots+\sigma^{n-2}}\theta^{\sigma^{n-1}}$$

is not equal to 0. It is then clear that $\beta\alpha^{\sigma} = \alpha$ using the fact that $N(\beta) = 1$, and hence that when we apply σ to the last term in the sum, we obtain θ. We divide by α^{σ} to conclude the proof.

Theorem 6.2. *Let k be a field, n an integer > 0 prime to the characteristic of k, and assume that there is a primitive n-th root of unity in k.*

(i) *Let K be a cyclic extension of degree n. Then there exists $\alpha \in K$ such that $K = k(\alpha)$, and α satisfies an equation $X^n - a = 0$ for some $a \in k$.*

(ii) *Conversely, let $a \in k$. Let α be a root of $X^n - a$. Then $k(\alpha)$ is cyclic over k, of degree d, $d \mid n$, and α^d is an element of k.*

Proof. Let ζ be a primitive n-th root of unity in k, and let K/k be cyclic with group G. Let σ be a generator of G. We have $N(\zeta^{-1}) = (\zeta^{-1})^n = 1$. By Hilbert's theorem 90, there exists $\alpha \in K$ such that $\sigma\alpha = \zeta\alpha$. Since ζ is in k, we have $\sigma^i\alpha = \zeta^i\alpha$ for $i = 1, \ldots, n$. Hence the elements $\zeta^i\alpha$ are n distinct conjugates of α over k, whence $[k(\alpha) : k]$ is at least equal to n. Since $[K : k] = n$, it follows that $K = k(\alpha)$. Furthermore,

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \alpha^n.$$

Hence α^n is fixed under σ, hence is fixed under each power of σ, hence is fixed under G. Therefore α^n is an element of k, and we let $a = \alpha^n$. This proves the first part of the theorem.

Conversely, let $a \in k$. Let α be a root of $X^n - a$. Then $\alpha\zeta^i$ is also a root for each $i = 1, \ldots, n$, and hence all roots lie in $k(\alpha)$ which is therefore normal over k. All the roots are distinct so $k(\alpha)$ is Galois over k. Let G be the Galois group.

If σ is an automorphism of $k(\alpha)/k$ then $\sigma\alpha$ is also a root of $X^n - a$. Hence $\sigma\alpha = \omega_\sigma\alpha$ where ω_σ is an n-th root of unity, not necessarily primitive. The map $\sigma \mapsto \omega_\sigma$ is obviously a homomorphism of G into the group of n-th roots of unity, and is injective. Since a subgroup of a cyclic group is cyclic, we conclude that G is cyclic, of order d, and $d \mid n$. The image of G is a cyclic group of order d. If σ is a generator of G, then ω_σ is a primitive dth root of unity. Now we get

$$\sigma(\alpha^d) = (\sigma\alpha)^d = (\omega_\sigma\alpha)^d = \alpha^d.$$

Hence α^d is fixed under σ, and therefore fixed under G. It is an element of k, and our theorem is proved.

We now pass to the analogue of Hilbert's theorem 90 in characteristic p for cyclic extensions of degree p.

Theorem 6.3. (Hilbert's Theorem 90, Additive Form). *Let k be a field and K/k a cyclic extension of degree n with group G. Let σ be a generator of G. Let $\beta \in K$. The trace $\mathrm{Tr}_k^K(\beta)$ is equal to 0 if and only if there exists an element $\alpha \in K$ such that $\beta = \alpha - \sigma\alpha$.*

Proof. If such an element α exists, then we see that the trace is 0 because the trace is equal to the sum taken over all elements of G, and applying σ permutes these elements.

Conversely, assume $\mathrm{Tr}(\beta) = 0$. There exists an element $\theta \in K$ such that $\mathrm{Tr}(\theta) \neq 0$. Let

$$\alpha = \frac{1}{\mathrm{Tr}(\theta)} [\beta\theta^{\sigma} + (\beta + \sigma\beta)\theta^{\sigma^2} + \cdots + (\beta + \sigma\beta + \cdots + \sigma^{n-2}\beta)\theta^{\sigma^{n-1}}].$$

From this it follows at once that $\beta = \alpha - \sigma\alpha$.

Theorem 6.4. (Artin-Schreier) *Let k be a field of characteristic p.*

(i) *Let K be a cyclic extension of k of degree p. Then there exists $\alpha \in K$ such that $K = k(\alpha)$ and α satisfies an equation $X^p - X - a = 0$ with some $a \in k$.*

(ii) *Conversely, given $a \in k$, the polynomial $f(X) = X^p - X - a$ either has one root in k, in which case all its roots are in k, or it is irreducible. In this latter case, if α is a root then $k(\alpha)$ is cyclic of degree p over k.*

Proof. Let K/k be cyclic of degree p. Then $\mathrm{Tr}_k^K(-1) = 0$ (it is just the sum of -1 with itself p times). Let σ be a generator of the Galois group. By the additive form of Hilbert's theorem 90, there exists $\alpha \in K$ such that $\sigma\alpha - \alpha = 1$, or in other words, $\sigma\alpha = \alpha + 1$. Hence $\sigma^i\alpha = \alpha + i$ for all integers $i = 1, \ldots, p$ and α has p distinct conjugates. Hence $[k(\alpha) : k] \geqq p$. It follows that $K = k(\alpha)$. We note that

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha.$$

Hence $\alpha^p - \alpha$ is fixed under σ, hence it is fixed under the powers of σ, and therefore under G. It lies in the fixed field k. If we let $a = \alpha^p - \alpha$ we see that our first assertion is proved.

Conversely, let $a \in k$. If α is a root of $X^p - X - a$ then $\alpha + i$ is also a root for $i = 1, \ldots, p$. Thus $f(X)$ has p distinct roots. If one root lies in k then all roots lie in k. Assume that no root lies in k. We contend that the

polynomial is irreducible. Suppose that

$$f(X) = g(X)h(X)$$

with $g, h \in k[X]$ and $1 \leqq \deg g < p$. Since

$$f(X) = \prod_{i=1}^{p}(X - \alpha - i)$$

we see that $g(X)$ is a product over certain integers i. Let $d = \deg g$. The coefficient of X^{d-1} in g is a sum of terms $-(\alpha + i)$ taken over precisely d integers i. Hence it is equal to $-d\alpha + j$ for some integer j. But $d \neq 0$ in k, and hence α lies in k, because the coefficients of g lie in k, contradiction. We know therefore that $f(X)$ is irreducible. All roots lie in $k(\alpha)$, which is therefore normal over k. Since $f(X)$ has no multiple roots, it follows that $k(\alpha)$ is Galois over k. There exists an automorphism σ of $k(\alpha)$ over k such that $\sigma\alpha = \alpha + 1$ (because $\alpha + 1$ is also a root). Hence the powers σ^i of σ give $\sigma^i\alpha = \alpha + i$ for $i = 1, \ldots, p$ and are distinct. Hence the Galois group consists of these powers and is cyclic, thereby proving the theorem.

For cyclic extensions of degree p^r, see the exercises on Witt vectors and the bibliography at the end of §8.

§7. SOLVABLE AND RADICAL EXTENSIONS

A finite extension E/k (which we shall assume separable for convenience) is said to be **solvable** if the Galois group of the smallest Galois extension K of k containing E is a solvable group. This is equivalent to saying that there exists a solvable Galois extension L of k such that $k \subset E \subset L$. Indeed, we have $k \subset E \subset K \subset L$ and $G(K/k)$ is a homomorphic image of $G(L/k)$.

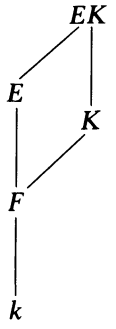
Proposition 7.1. *Solvable extensions form a distinguished class of extensions.*

Proof. Let E/k be solvable. Let F be a field containing k and assume E, F are subfields of some algebraically closed field. Let K be Galois solvable over k, and $E \subset K$. Then KF is Galois over F and $G(KF/F)$ is a subgroup of $G(K/k)$ by Theorem 1.12. Hence EF/F is solvable. It is clear that a subextension of a solvable extension is solvable. Let $E \supset F \supset k$ be a tower, and assume that E/F is solvable and F/k is solvable. Let K be a finite solvable Galois extension of k containing F. We just saw that EK/K is solvable. Let L be a solvable Galois extension of K containing EK. If σ is any embedding of L over k in a given algebraic closure, then $\sigma K = K$ and hence σL is a solvable extension of K. We let M be the compositum of all extensions σL for all embeddings σ of L over k.

Then M is Galois over k, and is therefore Galois over K. The Galois group of M over K is a subgroup of the product

$$\prod_{\sigma} G(\sigma L/K)$$

by Theorem 1.14. Hence it is solvable. We have a surjective homomorphism $G(M/k) \to G(K/k)$ by Theorem 1.10. Hence the Galois group of M/k has a solvable normal subgroup whose factor group is solvable. It is therefore solvable. Since $E \subset M$, our proof is complete.



A finite extension F of k is said to be **solvable by radicals** if it is separable and if there exists a finite extension E of k containing F, and admitting a tower decomposition

$$k = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_m = E$$

such that each step E_{i+1}/E_i is one of the following types:

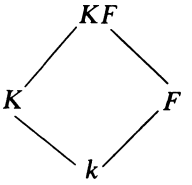
1. It is obtained by adjoining a root of unity.
2. It is obtained by adjoining a root of a polynomial $X^n - a$ with $a \in E_i$ and n prime to the characteristic.
3. It is obtained by adjoining a root of an equation $X^p - X - a$ with $a \in E_i$ if p is the characteristic > 0.

One can see at once that the class of extensions which are solvable by radicals is a distinguished class.

Theorem 7.2. *Let E be a separable extension of k. Then E is solvable by radicals if and only if E/k is solvable.*

Proof. Assume that E/k is solvable, and let K be a finite solvable Galois extension of k containing E. Let m be the product of all primes unequal to the characteristic dividing the degree $[K : k]$, and let $F = k(\zeta)$ where ζ is a primitive m-th root of unity. Then F/k is abelian. We lift K over F. Then KF is solvable over F. There is a tower of subfields between F and KF such that each step is cyclic of prime order, because every solvable group admits a tower of sub-

groups of the same type, and we can use Theorem 1.10. By Theorems 6.2 and 6.4, we conclude that KF is solvable by radicals over F, and hence is solvable by radicals over k. This proves that E/k is solvable by radicals.



Conversely, assume that E/k is solvable by radicals. For any embedding σ of E in E^a over k, the extension $\sigma E/k$ is also solvable by radicals. Hence the smallest Galois extension K of E containing k, which is a composite of E and its conjugates is solvable by radicals. Let m be the product of all primes unequal to the characteristic dividing the degree $[K : k]$ and again let $F = k(\zeta)$ where ζ is a primitive m-th root of unity. It will suffice to prove that KF is solvable over F, because it follows then that KF is solvable over k and hence $G(K/k)$ is solvable because it is a homomorphic image of $G(KF/k)$. But KF/F can be decomposed into a tower of extensions, such that each step is prime degree and of the type described in Theorem 6.2 or Theorem 6.4, and the corresponding root of unity is in the field F. Hence KF/F is solvable, and our theorem is proved.

Remark. One could modify our preceding discussion by not assuming separability. Then one must deal with normal extensions instead of Galois extensions, and one must allow equations $X^p - a$ in the solvability by radicals, with p equal to the characteristic. Then we still have the theorem corresponding to Theorem 7.2. The proof is clear in view of Chapter V, §6.

For a proof that every solvable group is a Galois group over the rationals, I refer to Shafarevich [Sh 54], as well as contributions of Iwasawa [Iw 53].

[Iw 53] K. IWASAWA, On solvable extension of algebraic number fields, *Ann. of Math.* **58** (1953), pp. 548–572

[Sh 54] I. SHAFAREVICH, Construction of fields of algebraic numbers with given solvable Galois group, *Izv. Akad. Nauk SSSR* **18** (1954), pp. 525–578 (*Amer. Math. Soc. Transl.* **4** (1956), pp. 185–237)

§8. ABELIAN KUMMER THEORY

In this section we shall carry out a generalization of the theorem concerning cyclic extensions when the ground field contains enough roots of unity.

Let k be a field and m a positive integer. A Galois extension K of k with group G is said to be of **exponent** m if $\sigma^m = 1$ for all $\sigma \in G$.

We shall investigate abelian extensions of exponent m. We first assume that m is prime to the characteristic of k, and that k contains a primitive m-th root of unity. We denote by μ_m the group of m-th roots of unity. We assume that all our algebraic extensions in this section are contained in a fixed algebraic closure k^a.

Let $a \in k$. The symbol $a^{1/m}$ (or $\sqrt[m]{a}$) is not well defined. If $\alpha^m = a$ and ζ is an m-th root of unity, then $(\zeta\alpha)^m = a$ also. We shall use the symbol $a^{1/m}$ to denote any such element α, which will be called an m-th root of a. Since the roots of unity are in the ground field, we observe that the field $k(\alpha)$ is the same no matter which m-th root α of a we select. We denote this field by $k(a^{1/m})$.

We denote by k^{*m} the subgroup of k^* consisting of all m-th powers of non-zero elements of k. It is the image of k^* under the homomorphism $x \mapsto x^m$.

Let B be a subgroup of k^* containing k^{*m}. We denote by $k(B^{1/m})$ or K_B the composite of all fields $k(a^{1/m})$ with $a \in B$. It is uniquely determined by B as a subfield of k^a.

Let $a \in B$ and let α be an m-th root of a. The polynomial $X^m - a$ splits into linear factors in K_B, and thus K_B is Galois over k, because this holds for all $a \in B$. Let G be the Galois group. Let $\sigma \in G$. Then $\sigma\alpha = \omega_\sigma\alpha$ for some m-th root of unity $\omega_\sigma \in \mu_m \subset k^*$. The map

$$\sigma \mapsto \omega_\sigma$$

is obviously a homomorphism of G into μ_m, i.e. for $\tau, \sigma \in G$ we have

$$\tau\sigma\alpha = \omega_\tau\omega_\sigma\alpha = \omega_\sigma\omega_\tau\alpha.$$

We may write $\omega_\sigma = \sigma\alpha/\alpha$. This root of unity ω_σ is independent of the choice of m-th root of a, for if α' is another m-th root, then $\alpha' = \zeta\alpha$ for some $\zeta \in \mu_m$, whence

$$\sigma\alpha'/\alpha' = \zeta\sigma\alpha/\zeta\alpha = \sigma\alpha/\alpha.$$

We denote ω_σ by $\langle \sigma, a \rangle$. The map

$$(\sigma, a) \mapsto \langle \sigma, a \rangle$$

gives us a map

$$G \times B \to \mu_m.$$

If $a, b \in B$ and $\alpha^m = a$, $\beta^m = b$ then $(\alpha\beta)^m = ab$ and

$$\sigma(\alpha\beta)/\alpha\beta = (\sigma\alpha/\alpha)(\sigma\beta/\beta).$$

We conclude that the map above is bilinear. Furthermore, if $a \in k^{*m}$ it follows that $\langle \sigma, a \rangle = 1$.

Theorem 8.1. *Let k be a field, m an integer > 0 prime to the characteristic of k, and assume that a primitive m-th root of unity lies in k. Let B be a subgroup of k^* containing k^{*m} and let $K_B = k(B^{1/m})$. Then K_B is Galois, and abelian of exponent m. Let G be its Galois group. We have a bilinear map*

$$G \times B \to \mu_m \quad \text{given by} \quad (\sigma, a) \mapsto \langle \sigma, a \rangle.$$

If $\sigma \in G$ and $a \in B$, and $\alpha^m = a$ then $\langle \sigma, a \rangle = \sigma\alpha/\alpha$. The kernel on the left is 1 *and the kernel on the right is k^{*m}. The extension K_B/k is finite if and only if $(B : k^{*m})$ is finite. If that is the case, then*

$$B/k^{*m} \approx G^\wedge,$$

and in particular we have the equality

$$[K_B : k] = (B : k^{*m}).$$

Proof. Let $\sigma \in G$. Suppose $\langle \sigma, a \rangle = 1$ for all $a \in B$. Then for every generator α of K_B such that $\alpha^m = a \in B$ we have $\sigma\alpha = \alpha$. Hence σ induces the identity on K_B and the kernel on the left is 1. Let $a \in B$ and suppose $\langle \sigma, a \rangle = 1$ for all $\sigma \in G$. Consider the subfield $k(a^{1/m})$ of K_B. If $a^{1/m}$ is not in k, there exists an automorphism of $k(a^{1/m})$ over k which is not the identity. Extend this automorphism to K_B, and call this extension σ. Then clearly $\langle \sigma, a \rangle \neq 1$. This proves our contention.

By the duality theorem of Chapter I, §9 we see that G is finite if and only if B/k^{*m} is finite, and in that case we have the isomorphism as stated, so that in particular the order of G is equal to $(B : k^{*m})$, thereby proving the theorem.

Theorem 8.2. *Notation being as in Theorem* 8.1, *the map $B \mapsto K_B$ gives a bijection of the set of subgroups of k^* containing k^{*m} and the abelian extensions of k of exponent m.*

Proof. Let B_1, B_2 be subgroups of k^* containing k^{*m}. If $B_1 \subset B_2$ then $k(B_1^{1/m}) \subset k(B_2^{1/m})$. Conversely, assume that $k(B_1^{1/m}) \subset k(B_2^{1/m})$. We wish to prove $B_1 \subset B_2$. Let $b \in B_1$. Then $k(b^{1/m}) \subset k(B_2^{1/m})$ and $k(b^{1/m})$ is contained in a finitely generated subextension of $k(B_2^{1/m})$. Thus we may assume without loss of generality that B_2/k^{*m} is finitely generated, hence finite. Let B_3 be the subgroup of k^* generated by B_2 and b. Then $k(B_2^{1/m}) = k(B_3^{1/m})$ and from what we saw above, the degree of this field over k is precisely

$$(B_2 : k^{*m}) \quad \text{or} \quad (B_3 : k^{*m}).$$

Thus these two indices are equal, and $B_2 = B_3$. This proves that $B_1 \subset B_2$.

We now have obtained an injection of our set of groups B into the set of abelian extensions of k of exponent m. Assume finally that K is an abelian extension of k of exponent m. Any finite subextension is a composite of cyclic extensions of exponent m because any finite abelian group is a product of cyclic groups, and we can apply Corollary 1.16. By Theorem 6.2, every cyclic extension can be obtained by adjoining an m-th root. Hence K can be obtained by adjoining a family of m-th roots, say m-th roots of elements $\{b_j\}_{j \in J}$ with $b_j \in k^*$. Let B be the subgroup of k^* generated by all b_j and k^{*m}. If $b' = ba^m$ with $a, b \in k$ then obviously

$$k(b'^{1/m}) = k(b^{1/m}).$$

Hence $k(B^{1/m}) = K$, as desired.

When we deal with abelian extensions of exponent p equal to the characteristic, then we have to develop an additive theory, which bears the same relationship to Theorems 8.1 and 8.2 as Theorem 6.4 bears to Theorem 6.2.

If k is a field, we define the operator $\wp$ by

$$\wp(x) = x^p - x$$

for $x \in k$. Then $\wp$ is an additive homomorphism of k into itself. The subgroup $\wp(k)$ plays the same role as the subgroup k^{*m} in the multiplicative theory, whenever m is a prime number. The theory concerning a power of p is slightly more elaborate and is due to Witt.

We now assume k has characteristic p. A root of the polynomial $X^p - X - a$ with $a \in k$ will be denoted by $\wp^{-1}a$. If B is a subgroup of k containing $\wp k$ we let $K_B = k(\wp^{-1}B)$ be the field obtained by adjoining $\wp^{-1}a$ to k for all $a \in B$. We emphasize the fact that B is an *additive* subgroup of k.

Theorem 8.3. *Let k be a field of characteristic p. The map $B \mapsto k(\wp^{-1}B)$ is a bijection between subgroups of k containing $\wp k$ and abelian extensions of k of exponent p. Let $K = K_B = k(\wp^{-1}B)$, and let G be its Galois group. If $\sigma \in G$ and $a \in B$, and $\wp\alpha = a$, let $\langle \sigma, a \rangle = \sigma\alpha - \alpha$. Then we have a bilinear map*

$$G \times B \to \mathbf{Z}/p\mathbf{Z} \quad \text{given by} \quad (\sigma, a) \to \langle \sigma, a \rangle.$$

The kernel on the left is 1 and the kernel on the right is $\wp k$. The extension K_B/k is finite if and only if $(B : \wp k)$ is finite and if that is the case, then

$$[K_B : k] = (B : \wp k).$$

Proof. The proof is entirely similar to the proof of Theorems 8.1 and 8.2. It can be obtained by replacing multiplication by addition, and using the "$\wp$-th root" instead of an m-th root. Otherwise, there is no change in the wording of the proof.

The analogous theorem for abelian extensions of exponent p^n requires Witt vectors, and will be developed in the exercises.

Bibliography

[Wi 35] E. WITT, Der Existenzsatz für abelsche Funktionenkörper, *J. reine angew. Math.* **173** (1935), pp. 43–51

[Wi 36] E. WITT, Konstruktion von galoisschen Körpern der Charakteristik p mit vorgegebener Gruppe der Ordung p^f, *J. reine angew. Math.* **174** (1936), pp. 237–245

[Wi 37] E. WITT, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p, *J. reine angew. Math.* **176** (1937), pp. 126–140

§9. THE EQUATION $X^n - a = 0$

When the roots of unity are not in the ground field, the equation $X^n - a = 0$ is still interesting but a little more subtle to treat.

Theorem 9.1. *Let k be a field and n an integer $\geqq 2$. Let $a \in k, a \neq 0$. Assume that for all prime numbers p such that $p|n$ we have $a \notin k^p$, and if $4|n$ then $a \notin -4k^4$. Then $X^n - a$ is irreducible in $k[X]$.*

Proof. Our first assumption means that a is not a p-th power in k. We shall reduce our theorem to the case when n is a prime power, by induction.

Write $n = p^r m$ with p prime to m, and p odd. Let

$$X^m - a = \prod_{v=1}^{m} (X - \alpha_v)$$

be the factorization of $X^m - a$ into linear factors, and say $\alpha = \alpha_1$. Substituting X^{p^r} for X we get

$$X^n - a = X^{p^r m} - a = \prod_{v=1}^{m} (X^{p^r} - \alpha_v).$$

We may assume inductively that $X^m - a$ is irreducible in $k[X]$. We contend that α is not a p-th power in $k(\alpha)$. Otherwise, $\alpha = \beta^p$, $\beta \in k(\alpha)$. Let N be the norm from $k(\alpha)$ to k. Then

$$-a = (-1)^m N(\alpha) = (-1)^m N(\beta^p) = (-1)^m N(\beta)^p.$$

If m is odd, a is a p-th power, which is impossible. Similarly, if m is even and p is odd, we also get a contradiction. This proves our contention, because m is prime to p. If we know our theorem for prime powers, then we conclude that $X^{p^r} - \alpha$ is irreducible over $k(\alpha)$. If A is a root of $X^{p^r} - \alpha$ then $k \subset k(\alpha) \subset k(A)$ gives a tower, of which the bottom step has degree m and the top step has degree p^r. It follows that A has degree n over k and hence that $X^n - a$ is irreducible.

We now suppose that $n = p^r$ is a prime power.

If p is the characteristic, let α be a p-th root of a. Then $X^p - a = (X - \alpha)^p$ and hence $X^{p^r} - a = (X^{p^{r-1}} - \alpha)^p$ if $r \geqq 2$. By an argument even more trivial than before, we see that α is not a p-th power in $k(\alpha)$, hence inductively $X^{p^{r-1}} - \alpha$ is irreducible over $k(\alpha)$. Hence $X^{p^r} - a$ is irreducible over k.

Suppose that p is not the characteristic. We work inductively again, and let α be a root of $X^p - a$.

Suppose a is not a p-th power in k. We claim that $X^p - a$ is irreducible. Otherwise a root α of $X^p - a$ generates an extension $k(\alpha)$ of degree $d < p$ and $\alpha^p = a$. Taking the norm from $k(\alpha)$ to k we get $N(\alpha)^p = a^d$. Since d is prime to p, it follows that α is a p-th power in k, contradiction.

Let $r \geqq 2$. We let $\alpha = \alpha_1$. We have

$$X^p - a = \prod_{\nu=1}^{p} (X - \alpha_\nu)$$

and

$$X^{p^r} - a = \prod_{\nu=1}^{p} (X^{p^{r-1}} - \alpha_\nu).$$

Assume that α is not a p-th power in $k(\alpha)$. Let A be a root of $X^{p^{r-1}} - \alpha$. If p is odd then by induction, A has degree p^{r-1} over $k(\alpha)$, hence has degree p^r over k and we are done. If $p = 2$, suppose $\alpha = -4\beta^4$ with $\beta \in k(\alpha)$. Let N be the norm from $k(\alpha)$ to k. Then $-a = N(\alpha) = 16N(\beta)^4$, so $-a$ is a square in k. Since $p = 2$ we get $\sqrt{-1} \in k(\alpha)$ and $\alpha = (\sqrt{-1}\, 2\beta^2)^2$, a contradiction. Hence again by induction, we find that A has degree p^r over k. We therefore assume that $\alpha = \beta^p$ with some $\beta \in k(\alpha)$, and derive the consequences.

Taking the norm from $k(\alpha)$ to k we find

$$-a = (-1)^p N(\alpha) = (-1)^p N(\beta^p) = (-1)^p N(\beta)^p.$$

If p is odd, then a is a p-th power in k, contradiction. Hence $p = 2$, and

$$-a = N(\beta)^2$$

is a square in k. Write $-a = b^2$ with $b \in k$. Since a is not a square in k we conclude that -1 is not a square in k. Let $i^2 = -1$. Over $k(i)$ we have the factorization

$$X^{2^r} - a = X^{2^r} + b^2 = (X^{2^{r-1}} + ib)(X^{2^{r-1}} - ib).$$

Each factor is of degree 2^{r-1} and we argue inductively. If $X^{2^{r-1}} \pm ib$ is reducible over $k(i)$ then $\pm ib$ is a square in $k(i)$ or lies in $-4(k(i))^4$. In either case, $\pm ib$ is a square in $k(i)$, say

$$\pm ib = (c + di)^2 = c^2 + 2cdi - d^2$$

with $c, d \in k$. We conclude that $c^2 = d^2$ or $c = \pm d$, and $\pm ib = 2cdi = \pm 2c^2 i$. Squaring gives a contradiction, namely

$$a = -b^2 = -4c^4.$$

We now conclude by unique factorization that $X^{2^r} + b^2$ cannot factor in $k[X]$, thereby proving our theorem.

The conditions of our theorem are necessary because

$$X^4 + 4b^4 = (X^2 + 2bX + 2b^2)(X^2 - 2bX + 2b^2).$$

If $n = 4m$ and $a \in -4k^4$ then $X^n - a$ is reducible.

Corollary 9.2. *Let k be a field and assume that $a \in k$, $a \neq 0$, and that a is not a p-th power for some prime p. If p is equal to the characteristic, or if p is odd, then for every integer $r \geqq 1$ the polynomial $X^{p^r} - a$ is irreducible over k.*

Proof. The assertion is logically weaker than the assertion of the theorem.

Corollary 9.3. *Let k be a field and assume that the algebraic closure k^a of k is of finite degree > 1 over k. Then $k^a = k(i)$ where $i^2 = -1$, and k has characteristic 0.*

Proof. We note that k^a is normal over k. If k^a is not separable over k, so char $k = p > 0$, then k^a is purely inseparable over some subfield of degree $>$ 1 (by Chapter V, §6), and hence there is a subfield E containing k, and an element $a \in E$ such that $X^p - a$ is irreducible over E. By Corollary 9.2, k^a cannot be of finite degree over E. (The reader may restrict his or her attention to characteristic 0 if Chapter V, §6 was omitted.)

We may therefore assume that k^a is Galois over k. Let $k_1 = k(i)$. Then k^a is also Galois over k_1. Let G be the Galois group of k^a/k_1. Suppose that there is a prime number p dividing the order of G, and let H be a subgroup of order p. Let F be its fixed field. Then $[k^a : F] = p$. If p is the characteristic, then Exercise 29 at the end of the chapter will give the contradiction. We may assume that p is not the characteristic. The p-th roots of unity $\neq 1$ are the roots of a polynomial of degree $\leqq p - 1$ (namely $X^{p-1} + \cdots + 1$), and hence must lie in F. By Theorem 6.2, it follows that k^a is the splitting field of some polynomial $X^p - a$ with $a \in F$. The polynomial $X^{p^2} - a$ is necessarily reducible. By the theorem, we must have $p = 2$ and $a = -4b^4$ with $b \in F$. This implies

$$k^a = F(a^{1/2}) = F(i).$$

But we assumed $i \in k_1$, contradiction.

Thus we have proved $k^a = k(i)$. It remains to prove that char $k = 0$, and for this I use an argument shown to me by Keith Conrad. We first show that a sum of squares in k is a square. It suffices to prove this for a sum of two squares, and in this case we write an element $x + iy \in k(i) = k^a$ as a square.

$$x + iy = (u + iv)^2, \qquad x, y, u, v \in k,$$

and then $x^2 + y^2 = (u^2 + v^2)^2$. Then to prove k has characteristic 0, we merely observe that if the characteristic is > 0, then -1 is a finite sum $1 + \ldots + 1$, whence a square by what we have just shown, but $k^a = k(i)$, so this concludes the proof.

Corollary 9.3 is due to Artin; see [Ar 24], given at the end of Chapter XI. In that chapter, much more will be proved about the field k.

Example 1. Let $k = \mathbf{Q}$ and let $G_{\mathbf{Q}} = G(\mathbf{Q}^a/\mathbf{Q})$. Then the only non-trivial torsion elements in $G_{\mathbf{Q}}$ have order 2. It follows from Artin's theory (as given in Chapter XI) that all such torsion elements are conjugate in $G_{\mathbf{Q}}$. One uses Chapter XI, Theorems 2.2, 2.4, and 2.9.)

Example 2. Let k be a field of characteristic not dividing n. Let $a \in k$, $a \neq 0$ and let K be the splitting field of $X^n - a$. Let α be one root of $X^n - a$, and let ζ be a primitive n-th root of unity. Then

$$K = k(\alpha, \zeta) = k(\alpha, \mu_n).$$

We assume the reader is acquainted with matrices over a commutative ring. Let $\sigma \in G_{K/k}$. Then $(\sigma\alpha)^n = a$, so there exists some integer $b = b(\sigma)$ uniquely determined mod n, such that

$$\sigma(\alpha) = \alpha\zeta^{b(\sigma)}.$$

Since σ induces an automorphism of the cyclic group μ_n, there exists an integer $d(\sigma)$ relatively prime to n and uniquely determined mod n such that $\sigma(\zeta) = \zeta^{d(\sigma)}$. Let $G(n)$ be the subgroup of $GL_2(\mathbf{Z}/n\mathbf{Z})$ consisting of all matrices

$$M = \begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix} \text{ with } b \in \mathbf{Z}/n\mathbf{Z} \quad \text{and} \quad d \in (\mathbf{Z}/n\mathbf{Z})^*.$$

Observe that $\#G(n) = n\varphi(n)$. We obtain an injective map

$$\sigma \mapsto M(\sigma) = \begin{pmatrix} 1 & 0 \\ b(\sigma) & d(\sigma) \end{pmatrix} \quad \text{of } G_{K/k} \hookrightarrow G(n),$$

which is immediately verified to be an injective homomorphism. The question arises, when is it an isomorphism? The next theorem gives an answer over some fields, applicable especially to the rational numbers.

Theorem 9.4. *Let k be a field. Let n be an odd positive integer prime to the characteristic, and assume that $[k(\mu_n) : k] = \varphi(n)$. Let $a \in k$, and suppose that for each prime $p|n$ the element a is not a p-th power in k. Let K be the splitting field of $X^n - a$ over k. Then the above homomorphism $\sigma \mapsto M(\sigma)$ is an isomorphism of $G_{K/k}$ with $G(n)$. The commutator group is $\mathrm{Gal}(K/k(\mu_n))$, so $k(\mu_n)$ is the maximal abelian subextension of K.*

Proof. This is a special case of the general theory of §11, and Exercise 39, taking into account the representation of $G_{K/k}$ in the group of matrices. One need only use the fact that the order of $G_{K/k}$ is $n\varphi(n)$, according to that exercise, and so $\#(G_{K/k}) = \#G(n)$, so $G_{K/k} = G(n)$. However, we shall given an independent proof as an example of techniques of Galois theory. We prove the theorem by induction.

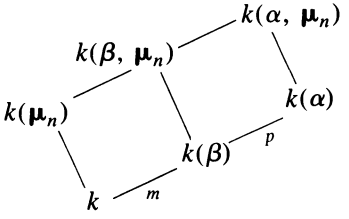
Suppose first $n = p$ is prime. Since $[k(\mu_p) : k] = p - 1$ is prime to p, it follows that if α is a root of $X^p - a$, then $k(\alpha) \cap k(\mu_p) = k$ because $[k(\alpha) : k] = p$. Hence $[K : k] = p(p - 1)$, so $G_{K/k} = G(p)$.

A direct computation of a commutator of elements in $G(n)$ for arbitrary n shows that the commutator subgroup is contained in the group of matrices

$$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}, \; b \in \mathbf{Z}/n\mathbf{Z},$$

and so must be that subgroup because its factor group is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$ under the projection on the diagonal. This proves the theorem when $n = p$.

Now let $p \mid n$ and write $n = pm$. Then $[k(\mu_m) : k] = \varphi(m)$, immediately from the hypothesis that $[k(\mu_n) : k] = \varphi(n)$. Let α be a root of $X^n - a$, and let $\beta = \alpha^p$. Then β is a root of $X^m - a$, and by induction we can apply the theorem to $X^m - a$. The field diagram is as follows.



Since α has degree pm over k, it follows that α cannot have lower degree than p over $k(\beta)$, so $[k(\alpha) : k(\beta)] = p$ and $X^p - \beta$ is irreducible over $k(\beta)$. We apply the first part of the proof to $X^p - \beta$ over $k(\beta)$. The property concerning the maximal abelian subextension of the splitting field shows that

$$k(\alpha) \cap k(\beta, \mu_n) = k(\beta).$$

Hence $[k(\alpha, \mu_n) : k(\beta, \mu_n)] = p$. By induction, $[k(\beta, \mu_n) : k(\mu_n)] = m$, again because of the maximal abelian subextension of the splitting field of $X^m - a$ over k. This proves that $[K : k] = n\varphi(n)$, whence $G_{K/k} = G(n)$, and the commutator statement has already been proved. This concludes the proof of Theorem 9.4.

Remarks. When n is even, there are some complications, because for instance $\mathbf{Q}(\sqrt{2})$ is contained in $\mathbf{Q}(\mu_8)$, so there are dependence relations among the fields in question. The non-abelian extensions, as in Theorem 9.4, are of intrinsic interest because they constitute the first examples of such extensions that come to mind, but they arose in other important contexts. For instance, Artin used them to give a probabilistic model for the density of primes p such that 2 (say) is a primitive root mod p (that is, 2 generates the cyclic group $(\mathbf{Z}/p\mathbf{Z})^*$. Instead of 2 he took any non-square integer $\neq \pm 1$. At first, Artin did not realize explicitly the above type of dependence, and so came to an answer that was off by some factor in some cases. Lehmer discovered the discrepancy by computations. As Artin then said, one has to multiply by the "obvious" factor which reflects the field dependencies. Artin never published his conjecture, but the matter is discussed in detail by Lang-Tate in the introduction to his collected papers (Addison-Wesley, Springer Verlag).

Similar conjectural probabilistic models were constructed by Lang-Trotter in connection with elliptic curves, and more generally with certain p-adic representations of the Galois group, in "Primitive points on elliptic curves", *Bull. AMS* **83** No. 2 (1977), pp. 289–292; and [LaT 75] (end of §14).

For further comments on the p-adic representations of Galois groups, see §14 and §15.

§10. GALOIS COHOMOLOGY

Let G be a group and A an abelian group which we write additively for the general remarks which we make, preceding our theorems. Let us assume that G operates on A, by means of a homomorphism $G \to \mathrm{Aut}(A)$. By a **1-cocycle** of G in A one means a family of elements $\{\alpha_\sigma\}_{\sigma \in G}$ with $\alpha_\sigma \in A$, satisfying the relations

$$\alpha_\sigma + \sigma\alpha_\tau = \alpha_{\sigma\tau}$$

for all $\sigma, \tau \in G$. If $\{\alpha_\sigma\}_{\sigma \in G}$ and $\{\beta_\sigma\}_{\sigma \in G}$ are 1-cocycles, then we can add them to get a 1-cocycle $\{\alpha_\sigma + \beta_\sigma\}_{\sigma \in G}$. It is then clear that 1-cocycles form a group, denoted by $Z^1(G, A)$. By a **1-coboundary** of G in A one means a family of elements $\{\alpha_\sigma\}_{\sigma \in G}$ such that there exists an element $\beta \in A$ for which $\alpha_\sigma = \sigma\beta - \beta$ for all $\sigma \in G$. It is then clear that a 1-coboundary is a 1-cocycle, and that the 1-coboundaries form a group, denoted by $B^1(G, A)$. The factor group

$$Z^1(G, A)/B^1(G, A)$$

is called the **first cohomology group** of G in A and is denoted by $H^1(G, A)$.

Remarks. Suppose G is cyclic. Let

$$\mathrm{Tr}_G\colon A \to A \text{ be the homomorphism } a \mapsto \sum_{\sigma \in G} \sigma(a).$$

Let γ be a generator of G. Let $(1 - \gamma)A$ be the subgroup of A consisting of all elements $a - \gamma(a)$ with $a \in A$. Then $(1 - \gamma)A$ is contained in $\ker \mathrm{Tr}_G$. The reader will verify as an exercise that there is an isomorphism

$$\ker \mathrm{Tr}_G/(1 - \gamma)A \approx H^1(G, A).$$

Then the next theorem for a cyclic group is just Hilbert's Theorem 90 of §6. *Cf.* also the cohomology of groups, Chapter XX, Exercise 4, for an even more general context.

Theorem 10.1. *Let K/k be a finite Galois extension with Galois group G. Then for the operation of G on K^* we have $H^1(G, K^*) = 1$, and for the operation of G on the additive group of K we have $H^1(G, K) = 0$. In other words, the first cohomology group is trivial in both cases.*

Proof. Let $\{\alpha_\sigma\}_{\sigma \in G}$ be a 1-cocycle of G in K^*. The multiplicative cocycle relation reads

$$\alpha_\sigma \alpha_\tau^\sigma = \alpha_{\sigma\tau}.$$

By the linear independence of characters, there exists $\theta \in K$ such that the element

$$\beta = \sum_{\tau \in G} \alpha_\tau \tau(\theta)$$

is $\neq 0$. Then

$$\sigma\beta = \sum_{\tau \in G} \alpha_\tau^\sigma \sigma\tau(\theta) = \sum_{\tau \in G} \alpha_{\sigma\tau} \alpha_\sigma^{-1} \sigma\tau(\theta)$$

$$= \alpha_\sigma^{-1} \sum_{\tau \in G} \alpha_{\sigma\tau} \sigma\tau(\theta) = \alpha_\sigma^{-1} \beta.$$

We get $\alpha_\sigma = \beta/\sigma\beta$, and using β^{-1} instead of β gives what we want.

For the additive part of the theorem, we find an element $\theta \in K$ such that the trace $\mathrm{Tr}(\theta)$ is not equal to 0. Given a 1-cocycle $\{\alpha_\sigma\}$ in the additive group of K, we let

$$\beta = \frac{1}{\mathrm{Tr}(\theta)} \sum_{\tau \in G} \alpha_\tau \tau(\theta).$$

It follows at once that $\alpha_\sigma = \beta - \sigma\beta$, as desired.

The next lemma will be applied to the non-abelian Kummer theory of the next section.

Lemma 10.2. (Sah). *Let G be a group and let E be a G-module. Let τ be in the center of G. Then $H^1(G, E)$ is annihilated by the map $x \mapsto \tau x - x$ on E. In particular, if this map is an automorphism of E, then $H^1(G, E) = 0$.*

Proof. Let f be a 1-cocycle of G in E. Then

$$f(\sigma) = f(\tau\sigma\tau^{-1}) = f(\tau) + \tau(f(\sigma\tau^{-1})$$
$$= f(\tau) + \tau[f(\sigma) + \sigma f(\tau^{-1})].$$

Therefore

$$\tau f(\sigma) - f(\sigma) = -\sigma\tau f(\tau^{-1}) - f(\tau).$$

But $f(1) = f(1) + f(1)$ implies $f(1) = 0$, and

$$0 = f(1) = f(\tau\tau^{-1}) = f(\tau) + \tau f(\tau^{-1}).$$

This shows that $(\tau - 1)f(\sigma) = (\sigma - 1)f(\tau)$, so f is a coboundary. This proves the lemma.

§11. NON-ABELIAN KUMMER EXTENSIONS

We are interested in the splitting fields of equations $X^n - a = 0$ when the n-th roots of unity are not contained in the ground field. More generally, we want to know roughly (or as precisely as possible) the Galois group of simultaneous equations of this type. For this purpose, we axiomatize the pattern of proof to an additive notation, which in fact makes it easier to see what is going on.

We fix an integer $N > 1$, and we let M range over positive integers dividing N. We let P be the set of primes dividing N. We let G be a group, and let:

A = G-module such that the isotropy group of any element of A is of finite index in G. We also assume that A is divisible by the primes $p|N$, that is

$$pA = A \qquad \text{for all } p \in P.$$

Γ = finitely generated subgroup of A such that Γ is pointwise fixed by G.

We assume that A_N is finite. Then $\frac{1}{N}\Gamma$ is also finitely generated. Note that

$$\frac{1}{N}\Gamma \supset A_N.$$

Example. For our purposes here, the above situation summarizes the properties which hold in the following situation. Let K be a finitely generated field over the rational numbers, or even a finite extension of the rational numbers. We let A be the multiplicative group of the algebraic closure K^a. We let $G = G_K$ be the Galois group $\mathrm{Gal}(K^a/K)$. We let Γ be a finitely generated subgroup of the multiplicative group K^*. Then all the above properties are satisfied. We see that $A_N = \mu_N$ is the group of N-th roots of unity. The group written $\frac{1}{N}\Gamma$ in additive notation is written $\Gamma^{1/N}$ in multiplicative notation.

Next we define the appropriate groups analogous to the Galois groups of Kummer theory, as follows. For any G-submodule B of A, we let:

$G(B)$ = image of G in $\mathrm{Aut}(B)$,

$G(N) = G(A_N)$ = image of G in $\mathrm{Aut}(A_N)$,

$H(N)$ = subgroup of G leaving A_N pointwise fixed,

$\mathrm{H}_\Gamma(M, N)$ (for $M|N$) = image of $H(N)$ in $\mathrm{Aut}\left(\frac{1}{M}\Gamma\right)$.

Then we have an exact sequence:

$$0 \to H_\Gamma(M, N) \to G\left(\frac{1}{M}\Gamma + A_N\right) \to G(N) \to 0.$$

Example. In the concrete case mentioned above, the reader will easily recognize these various groups as Galois groups. For instance, let A be the multiplicative group. Then we have the following lattice of field extensions with corresponding Galois groups:

$$G(\Gamma^{1/M}\mu_N)\begin{cases} K(\mu_N, \Gamma^{1/M}) \\ | \\ K(\mu_N) \\ | \\ K \end{cases}\begin{matrix} \} H_\Gamma(M, N) \\ \\ \} G(N) \end{matrix}$$

In applications, we want to know how much degeneracy there is when we translate $K(\mu_M, \Gamma^{1/M})$ over $K(\mu_N)$ with $M \mid N$. This is the reason we play with the pair M, N rather than a single N.

Let us return to a general Kummer representation as above. We are interested especially in that part of $(\mathbf{Z}/N\mathbf{Z})^*$ contained in $G(N)$, namely the group of integers n (mod N) such that there is an element $[n]$ in $G(N)$ such that

$$[n]a = na \qquad \text{for all } a \in A_N.$$

Such elements are always contained in the center of $G(N)$, and are called **homotheties**.

Write

$$N = \prod p^{n(p)}$$

Let S be a subset of P. We want to make some non-degeneracy assumptions about $G(N)$. We call S the **special set**.

There is a product decomposition

$$(\mathbf{Z}/N\mathbf{Z})^* = \prod_{p \mid N} (\mathbf{Z}/p^{n(p)}\mathbf{Z})^*.$$

If $2 \mid N$ we suppose that $2 \in S$. For each $p \in S$ we suppose that there is an integer $c(p) = p^{f(p)}$ with $f(p) \geqq 1$ such that

$$G(A_N) \supset \prod_{p \in S} U_{c(p)} \times \prod_{p \notin S} (\mathbf{Z}/p^{n(p)}\mathbf{Z})^*,$$

where $U_{c(p)}$ is the subgroup of $\mathbf{Z}(p^{n(p)})$ consisting of those elements $\equiv 1 \bmod c(p)$.

The product decomposition on the right is relative to the direct sum decomposition

$$A_N = \bigoplus_{p \mid N} A_{p^{n(p)}}.$$

The above assumption will be called the non-degeneracy assumption. The integers $c(p)$ measure the extent to which $G(A_N)$ is degenerate.

Under this assumption, we observe that

$$[2] \in G(A_M) \quad \text{if} \quad M \mid N \text{ and } M \text{ is not divisible by primes of } S;$$

$$[1 + c] \in G(A_M) \quad \text{if} \quad M \mid N \text{ and } M \text{ is divisible only by primes of } S,$$

where

$$c = c(S) = \prod_{p \in S} c(p).$$

We can then use $[2] - [1] = [1]$ and $[1 + c] - [1] = [c]$ in the context of Lemma 10.2, since $[1]$ and $[c]$ are in the center of G.

For any M we define

$$c(M) = \prod_{\substack{p \mid M \\ p \in S}} c(p).$$

Define

$$\Gamma' = \frac{1}{N} \Gamma \cap A^G$$

and the **exponent**

$$e(\Gamma'/\Gamma) = \text{smallest positive integer } e \text{ such that } e\Gamma' \subset \Gamma.$$

It is clear that degeneracy in the Galois group $H_\Gamma(M, N)$ defined above can arise from lots of roots of unity in the ground field, or at least degeneracy in the Galois group of roots of unity; and also if we look at an equation

$$X^M - a = 0,$$

from the fact that a is already highly divisible in K. This second degeneracy would arise from the exponent $e(\Gamma'/\Gamma)$, as can be seen by looking at the Galois group of the divisions of Γ. The next theorem shows that these are the only sources of degeneracy.

We have the abelian Kummer pairing for $M \mid N$,

$$H_\Gamma(M, N) \times \Gamma/M\Gamma \to A_M \quad \text{given by} \quad (\tau, x) \mapsto \tau y - y,$$

where y is any element such that $My = x$. The value of the pairing is indepen-

dent of the choice of y. Thus for $x \in \Gamma$, we have a homomorphism

$$\varphi_x : H_\Gamma(M, N) \to A_M$$

such that

$$\varphi_x(\tau) = \tau y - y, \qquad \text{where } My = x.$$

Theorem 11.1. *Let $M|N$. Let φ be the homomorphism*

$$\varphi : \Gamma \to \mathrm{Hom}(H_\Gamma(M, N), A_M)$$

and let Γ_φ be its kernel. Let $e_M(\Gamma) = \text{g.c.d.}\ (e(\Gamma'/\Gamma), M)$. Under the non-degeneracy assumption, we have

$$c(M)e_M(\Gamma)\Gamma_\varphi \subset M\Gamma.$$

Proof. Let $x \in \Gamma$ and suppose $\varphi_x = 0$. Let $My = x$. For $\sigma \in G$ let

$$y_\sigma = \sigma y - y.$$

Then $\{y_\sigma\}$ is a 1-cocycle of G in A_M, and by the hypothesis that $\varphi_x = 0$, this cocycle depends only on the class of σ modulo the subgroup of G leaving the elements of A_N fixed. In other words, we may view $\{y_\sigma\}$ as a cocycle of $G(N)$ in A_M. Let $c = c(N)$. By Lemma 10.2, it follows that $\{cy_\sigma\}$ splits as a cocycle of $G(N)$ in A_M. In other words, there exists $t_0 \in A_M$ such that

$$cy_\sigma = \sigma t_0 - t_0,$$

and this equation in fact holds for $\sigma \in G$. Let t be such that $ct = t_0$. Then

$$c\sigma y - cy = \sigma ct - cy,$$

whence $c(y - t)$ is fixed by all $\sigma \in G$, and therefore lies in $\frac{1}{N}\Gamma$. Therefore

$$e(\Gamma'/\Gamma)c(y - t) \in \Gamma.$$

We multiply both sides by M and observe that $cM(y - t) = cMy = cx$. This shows that

$$c(N)e(\Gamma'/\Gamma)\Gamma_\varphi \subset M\Gamma.$$

Since $\Gamma/M\Gamma$ has exponent M, we may replace $e(\Gamma'/\Gamma)$ by the greatest common divisor as stated in the theorem, and we can replace $c(N)$ by $c(M)$ to conclude the proof.

Corollary 11.2. *Assume that M is prime to $2(\Gamma' : \Gamma)$ and is not divisible by any primes of the special set S. Then we have an injection*

$$\varphi : \Gamma/M\Gamma \to \mathrm{Hom}(H_\Gamma(M, N), A_M).$$

If in addition Γ is free with basis $\{a_1, \ldots, a_r\}$, and we let $\varphi_i = \varphi_{a_i}$, then the map

$$H_\Gamma(M, N) \to A_M^{(r)} \quad \text{given by} \quad \tau \to (\varphi_1(\tau), \ldots, \varphi_r(\tau))$$

is injective. If A_M is cyclic of order M, this map is an isomorphism.

Proof. Under the hypotheses of the corollary, we have $c(M) = 1$ and $c_M(\Gamma) = 1$ in the theorem.

Example. Consider the case of Galois theory when A is the multiplicative group of K^a. Let $a_1, \ldots, a_r$ be elements of K^* which are multiplicatively independent. They generate a group as in the corollary. Furthermore, $A_M = \mu_M$ is cyclic, so the corollary applies. If M is prime to $2(\Gamma' : \Gamma)$ and is not divisible by any primes of the special set S, *we have an isomorphism*

$$\varphi : \Gamma/M\Gamma \to \operatorname{Hom}(H_\Gamma(M, N), \mu_M).$$

§12. ALGEBRAIC INDEPENDENCE OF HOMOMORPHISMS

Let A be an additive group, and let K be a field. Let $\lambda_1, \ldots, \lambda_n : A \to K$ be additive homomorphisms. We shall say that $\lambda_1, \ldots, \lambda_n$ are **algebraically dependent** (over K) if there exists a polynomial $f(X_1, \ldots, X_n)$ in $K[X_1, \ldots, X_n]$ such that for all $x \in A$ we have

$$f(\lambda_1(x), \ldots, \lambda_n(x)) = 0,$$

but such that f does not induce the zero function on $K^{(n)}$, i.e. on the direct product of K with itself n times. We know that with each polynomial we can associate a unique reduced polynomial giving the same function. If K is infinite, the reduced polynomial is equal to f itself. In our definition of dependence, we could as well assume that f is reduced.

A polynomial $f(X_1, \ldots, X_n)$ will be called **additive** if it induces an additive homomorphism of $K^{(n)}$ into K. Let $(Y) = (Y_1, \ldots, Y_n)$ be variables independent from (X). Let

$$g(X, Y) = f(X + Y) - f(X) - f(Y)$$

where $X + Y$ is the componentwise vector addition. Then the total degree of g viewed as a polynomial in (X) with coefficients in $K[Y]$ is strictly less than the total degree of f, and similarly, its degree in each X_i is strictly less than the degree of f in each X_i. One sees this easily by considering the difference of monomials,

$$M_{(\nu)}(X + Y) - M_{(\nu)}(X) - M_{(\nu)}(Y)$$
$$= (X_1 + Y_1)^{\nu_1} \cdots (X_n + Y_n)^{\nu_n} - X_1^{\nu_1} \cdots X_n^{\nu_n} - Y_1^{\nu_1} \cdots Y_n^{\nu_n}.$$

A similar assertion holds for g viewed as a polynomial in (Y) with coefficients in $K[X]$.

If f is reduced, it follows that g is reduced. Hence if f is additive, it follows that g is the zero polynomial.

Example. Let K have characteristic p. Then in one variable, the map

$$\xi \mapsto a\xi^{p^m}$$

for $a \in K$ and $m \geqq 1$ is additive, and given by the additive polynomial aX^{p^m}. We shall see later that this is a typical example.

Theorem 12.1. (Artin). *Let $\lambda_1, \ldots, \lambda_n : A \to K$ be additive homomorphisms of an additive group into a field. If these homomorphisms are algebraically dependent over K, then there exists an additive polynomial*

$$f(X_1, \ldots, X_n) \neq 0$$

in $K[X]$ such that

$$f(\lambda_1(x), \ldots, \lambda_n(x)) = 0$$

for all $x \in A$.

Proof. Let $f(X) = f(X_1, \ldots, X_n) \in K[X]$ be a reduced polynomial of lowest possible degree such that $f \neq 0$ but for all $x \in A$, $f(\Lambda(x)) = 0$, where $\Lambda(x)$ is the vector $(\lambda_1(x), \ldots, \lambda_n(x))$. We shall prove that f is additive.

Let $g(X, Y) = f(X + Y) - f(X) - f(Y)$. Then

$$g(\Lambda(x), \Lambda(y)) = f(\Lambda(x + y)) - f(\Lambda(x)) - f(\Lambda(y)) = 0$$

for all $x, y \in A$. We shall prove that g induces the zero function on $K^{(n)} \times K^{(n)}$. Assume otherwise. We have two cases.

Case 1. We have $g(\xi, \Lambda(y)) = 0$ for all $\xi \in K^{(n)}$ and all $y \in A$. By hypothesis, there exists $\xi' \in K^{(n)}$ such that $g(\xi', Y)$ is not identically 0. Let $P(Y) = g(\xi', Y)$. Since the degree of g in (Y) is strictly smaller than the degree of f, we have a contradiction.

Case 2. There exist $\xi' \in K^{(n)}$ and $y' \in A$ such that $g(\xi', \Lambda(y')) \neq 0$. Let $P(X) = g(X, \Lambda(y'))$. Then P is not the zero polynomial, but $P(\Lambda(x)) = 0$ for all $x \in A$, again a contradiction.

We conclude that g induces the zero function on $K^{(n)} \times K^{(n)}$, which proves what we wanted, namely that f is additive.

We now consider additive polynomials more closely.

Let f be an additive polynomial in n variables over K, and assume that f is reduced. Let

$$f_i(X_i) = f(0, \ldots, X_i, \ldots, 0)$$

with X_i in the i-th place, and zeros in the other components. By additivity, it follows that

$$f(X_1, \ldots, X_n) = f_1(X_1) + \cdots + f_n(X_n)$$

because the difference of the right-hand side and left-hand side is a reduced polynomial taking the value 0 on $K^{(n)}$. Furthermore, each f_i is an additive polynomial in one variable. We now study such polynomials.

Let $f(X)$ be a reduced polynomial in one variable, which induces a linear map of K into itself. Suppose that there occurs a monomial $a_r X^r$ in f with coefficient $a_r \neq 0$. Then the monomials of degree r in

$$g(X, Y) = f(X + Y) - f(X) - f(Y)$$

are given by

$$a_r(X + Y)^r - a_r X^r - a_r Y^r.$$

We have already seen that g is identically 0. Hence the above expression is identically 0. Hence the polynomial

$$(X + Y)^r - X^r - Y^r$$

is the zero polynomial. It contains the term $rX^{r-1}Y$. Hence if $r > 1$, our field must have characteristic p and r is divisible by p. Write $r = p^m s$ where s is prime to p. Then

$$0 = (X + Y)^r - X^r - Y^r = (X^{p^m} + Y^{p^m})^s - (X^{p^m})^s - (Y^{p^m})^s.$$

Arguing as before, we conclude that $s = 1$.

Hence if f is an additive polynomial in one variable, we have

$$f(X) = \sum_{v=0}^{m} a_v X^{p^v},$$

with $a_v \in K$. In characteristic 0, the only additive polynomials in one variable are of type aX with $a \in K$.

As expected, we define $\lambda_1, \ldots, \lambda_n$ to be **algebraically independent** if, whenever f is a reduced polynomial such that $f(\Lambda(x)) = 0$ for all $x \in K$, then f is the zero polynomial.

We shall apply Theorem 12.1 to the case when $\lambda_1, \ldots, \lambda_n$ are automorphisms of a field, and combine Theorem 12.1 with the theorem on the linear independence of characters.

Theorem 12.2. *Let K be an infinite field, and let $\sigma_1, \ldots, \sigma_n$ be the distinct elements of a finite group of automorphisms of K. Then $\sigma_1, \ldots, \sigma_n$ are algebraically independent over K.*

Proof. (Artin). In characteristic 0, Theorem 12.1 and the linear independence of characters show that our assertion is true. Let the characteristic be $p > 0$, and assume that $\sigma_1, \ldots, \sigma_n$ are algebraically dependent.

There exists an additive polynomial $f(X_1, \ldots, X_n)$ in $K[X]$ which is reduced, $f \neq 0$, and such that

$$f(\sigma_1(x), \ldots, \sigma_n(x)) = 0$$

for all $x \in K$. By what we saw above, we can write this relation in the form

$$\sum_{i=1}^{n} \sum_{r=1}^{m} a_{ir} \sigma_i(x)^{p^r} = 0$$

for all $x \in K$, and with not all coefficients a_{ir} equal to 0. Therefore by the linear independence of characters, the automorphisms

$$\{\sigma_i^{p^r}\} \qquad \text{with} \quad i = 1, \ldots, n \quad \text{and} \quad r = 1, \ldots, m$$

cannot be all distinct. Hence we have

$$\sigma_i^{p^r} = \sigma_j^{p^s}$$

with either $i \neq j$ or $r \neq s$. Say $r \leqq s$. For all $x \in K$ we have

$$\sigma_i(x)^{p^r} = \sigma_j(x)^{p^s}.$$

Extracting p-th roots in characteristic p is unique. Hence

$$\sigma_i(x) = \sigma_j(x)^{p^{s-r}} = \sigma_j(x^{p^{s-r}})$$

for all $x \in K$. Let $\sigma = \sigma_j^{-1}\sigma_i$. Then

$$\sigma(x) = x^{p^{s-r}}$$

for all $x \in K$. Taking $\sigma^n = \mathrm{id}$ shows that

$$x = x^{p^{n(s-r)}}$$

for all $x \in K$. Since K is infinite, this can hold only if $s = r$. But in that case, $\sigma_i = \sigma_j$, contradicting the fact that we started with distinct automorphisms.

§13. THE NORMAL BASIS THEOREM

Theorem 13.1. *Let K/k be a finite Galois extension of degree n. Let $\sigma_1, \ldots, \sigma_n$ be the elements of the Galois group G. Then there exists an element $w \in K$ such that $\sigma_1 w, \ldots, \sigma_n w$ form a basis of K over k.*

Proof. We prove this here only when k is infinite. The case when k is finite can be proved later by methods of linear algebra, as an exercise.

For each $\sigma \in G$, let X_σ be a variable, and let $t_{\sigma,\tau} = X_{\sigma^{-1}\tau}$. Let $X_i = X_{\sigma_i}$. Let

$$f(X_1, \ldots, X_n) = \det(t_{\sigma_i, \sigma_j}).$$

Then f is not identically 0, as one sees by substituting 1 for X_{id} and 0 for X_σ if $\sigma \neq \mathrm{id}$. Since k is infinite, f is reduced. Hence the determinant will not be 0 for all $x \in K$ if we substitute $\sigma_i(x)$ for X_i in f. Hence there exists $w \in K$ such that

$$\det(\sigma_i^{-1}\sigma_j(w)) \neq 0.$$

Suppose $a_1, \ldots, a_n \in k$ are such that

$$a_1\sigma_1(w) + \cdots + a_n\sigma_n(w) = 0.$$

Apply σ_i^{-1} to this relation for each $i = 1, \ldots, n$. Since $a_j \in k$ we get a system of linear equations, regarding the a_j as unknowns. Since the determinant of the coefficients is $\neq 0$, it follows that

$$a_j = 0 \qquad \text{for} \quad j = 1, \ldots, n$$

and hence that w is the desired element.

Remark. In terms of representations as in Chapters III and XVIII, the normal basis theorem says that the representation of the Galois group on the additive group of the field is the regular representation. One may also say that K is free of dimension 1 over the group ring $k[G]$. Such a result may be viewed as the first step in much more subtle investigations having to do with algebraic number theory. Let K be a number field (finite extension of $\mathbf{Q}$) and let $\mathfrak{o}_K$ be its ring of algebraic integers, which will be defined in Chapter VII, §1. Then one may ask for a description of $\mathfrak{o}_K$ as a $\mathbf{Z}[G]$ module, which is a much more difficult problem. For fundamental work about this problem, see A. Fröhlich, *Galois Module Structures of Algebraic Integers*, Ergebnisse der Math. 3 Folge Vol. 1, Springer Verlag (1983). See also the reference [CCFT 91] given at the end of Chapter III, §1.

§14. INFINITE GALOIS EXTENSIONS

Although we have already given some of the basic theorems of Galois theory already for possibly infinite extensions, the non-finiteness did not really appear in a substantial way. We now want to discuss its role more extensively.

Let K/k be a Galois extension with group G. For each finite Galois subextension F, we have the Galois groups $G_{K/F}$ and $G_{F/k}$. Put $H = G_{K/F}$. Then H has finite index, equal to $\#(G_{F/k}) = [F : k]$. This just comes as a special case of the general Galois theory. We have a canonical homomorphism

$$G \to G/H = G_{F/k}.$$

Therefore by the universal property of the inverse limit, we obtain a homomorphism

$$G \to \lim_{H \in \mathfrak{F}} G/H,$$

where the limit is taken for H in the family $\mathfrak{F}$ of Galois groups $G_{K/F}$ as above.

Theorem 14.1. *The homomorphism $G \to \lim G/H$ is an isomorphism.*

Proof. First the kernel is trivial, because if σ is in the kernel, then σ restricted to every finite subextension of K is trivial, and so is trivial on K. Recall that an element of the inverse limit is a family $\{\sigma_H\}$ with $\sigma_H \in G/H$, satisfying a certain compatibility condition. This compatibility condition means that we may define an element σ of G as follows. Let $\alpha \in K$. Then α is contained in some finite Galois extension $F \subset K$. Let $H = \mathrm{Gal}(K/F)$. Let $\sigma\alpha = \sigma_H\alpha$. The compatibility condition means that $\sigma_H\alpha$ is independent of the choice of F. Then it is immediately verified that σ is an automorphism of K over k, which maps to each σ_H in the canonical map of G into G/H. Hence the map $G \to \varprojlim G/H$ is surjective, thereby proving the theorem.

Remark. For the topological interpretation, see Chapter I, Theorem 10.1, and Exercise 43.

Example. Let $\boldsymbol{\mu}[p^\infty]$ be the union of all groups of roots of unity $\boldsymbol{\mu}[p^n]$, where p is a prime and $n = 1, 2, \ldots$ ranges over the positive integers. Let $K = \mathbf{Q}(\boldsymbol{\mu}[p^\infty])$. Then K is an abelian infinite extension of $\mathbf{Q}$. Let $\mathbf{Z}_p$ be the ring of p-adic integers, and $\mathbf{Z}_p^*$ the group of units. From §3, we know that $(\mathbf{Z}/p^n\mathbf{Z})^*$ is isomorphic to $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}[p^n]/\mathbf{Q}))$. These isomorphisms are compatible in the tower of p-th roots of unity, so we obtain an isomorphism

$$\mathbf{Z}_p^* \to \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}[p^\infty]/\mathbf{Q})).$$

Towers of cyclotomic fields have been extensively studied by Iwasawa. Cf. a systematic exposition and bibliography in [La 90].

For other types of representations in a group $GL_2(\mathbf{Z}_p)$, see Serre [Se 68], [Se 72], Shimura [Shi 71], and Lang-Trotter [LaT 75]. One general framework in which the representation of Galois groups on roots of unity can be seen has to do with commutative algebraic groups, starting with elliptic curves. Specifically, consider an equation

$$y^2 = 4x^3 - g_2x - g_3$$

with $g_2, g_3 \in \mathbf{Q}$ and non-zero discriminant: $\Delta = g_2^3 - 27g_3^2 \neq 0$. The set of solutions together with a point at infinity is denoted by E. From complex analysis (or by purely algebraic means), one sees that if K is an extension of $\mathbf{Q}$, then the set of solutions $E(K)$ with $x, y \in K$ and ∞ form a group, called the group of rational points of E in K. One is interested in the torsion group, say $E(\mathbf{Q}^a)_{\text{tor}}$ of points in the algebraic closure, or for a given prime p, in the group $E(\mathbf{Q}^a)[p^r]$ and $E(\mathbf{Q}^a)[p^\infty]$. As an abelian group, there is an isomorphism

$$E(\mathbf{Q}^a)[p^r] \approx (\mathbf{Z}/p^r\mathbf{Z}) \times (\mathbf{Z}/p^r\mathbf{Z}),$$

so the Galois group operates on the points of order p^r via a representation in $GL_2(\mathbf{Z}/p^r\mathbf{Z})$, rather than $GL_1(\mathbf{Z}/p^r\mathbf{Z}) = (\mathbf{Z}/p^r\mathbf{Z})^*$ in the case of roots of unity. Passing to the inverse limit, one obtains a representation of $\text{Gal}(\mathbf{Q}^a/\mathbf{Q}) = G_{\mathbf{Q}}$ in $GL_2(\mathbf{Z}_p)$. One of Serre's theorems is that the image of $G_{\mathbf{Q}}$ in $GL_2(\mathbf{Z}_p)$ is a subgroup of finite index, equal to $GL_2(\mathbf{Z}_p)$ for all but a finite number of primes p, if $\text{End}_{\mathbf{C}}(E) = \mathbf{Z}$.

More generally, using freely the language of algebraic geometry, when A is a commutative algebraic group, say with coefficients in $\mathbf{Q}$, then one may consider its group of points $A(\mathbf{Q}^a)_{\text{tor}}$, and the representation of $G_{\mathbf{Q}}$ in a similar way. Developing the notions to deal with these situations leads into algebraic geometry.

Instead of considering cyclotomic extensions of a ground field, one may also consider extensions of cyclotomic fields. The following conjecture is due to Shafarevich. See the references at the end of §7.

Conjecture 14.2. *Let $k_0 = \mathbf{Q}(\boldsymbol{\mu})$ be the compositum of all cyclotomic extensions of $\mathbf{Q}$ in a given algebraic closure $\mathbf{Q}^a$. Let k be a finite extension of k_0. Let $G_k = \text{Gal}(\mathbf{Q}^a/k)$. Then G_k is isomorphic to the completion of a free group on countably many generators.*

If G is the free group, then we recall that the completion is the inverse limit $\varprojlim G/H$, taken over all normal subgroups H of finite index. Readers should view this conjecture as being in analogy to the situation with Riemann surfaces, as mentioned in Example 9 of §2. It would be interesting to investigate the extent to which the conjecture remains valid if $\mathbf{Q}(\boldsymbol{\mu})$ is replaced by $\mathbf{Q}(A(\mathbf{Q}^a)_{\text{tor}})$, where A is an elliptic curve. For some results about free groups occurring as Galois groups, see also Wingberg [Wi 91].

Bibliography

[La 90] S. LANG, *Cyclotomic Fields I and II*, Second Edition, Springer Verlag, 1990 (Combined edition from the first editions, 1978, 1980)

[LaT 75] S. LANG and H. TROTTER, *Distribution of Frobenius Elements in GL_2-Extensions of the Rational Numbers*, Springer Lecture Notes **504** (1975)

[Se 68] J.-P. SERRE, *Abelian l-adic Representations and Elliptic Curves*, Benjamin, 1968

[Se 72] J.-P. SERRE, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), pp. 259–331

[Shi 71] G. SHIMURA, *Introduction to the arithmetic theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971

[Wi 91] K. WINGBERG, On Galois groups of p-closed algebraic number fields with restricted ramification, I, *J. reine angew. Math.* **400** (1989), pp. 185–202; and II, *ibid.*, **416** (1991), pp. 187–194

§15. THE MODULAR CONNECTION

This final section gives a major connection between Galois theory and the theory of modular forms, which has arisen since the 1960s.

One fundamental question is whether given a finite group G, there exists a Galois extension K of $\mathbf{Q}$ whose Galois group is G. In Exercise 23 you will prove this when G is abelian.

Already in the nineteenth century, number theorists realized the big difference between abelian and non-abelian extensions, and started understanding abelian extensions. Kronecker stated and gave what are today considered incomplete arguments that every finite abelian extension of $\mathbf{Q}$ is contained in some extension $\mathbf{Q}(\zeta)$, where ζ is a root of unity. The difficulty lay in the peculiarities of the prime 2. The trouble was fixed by Weber at the end of the nineteenth century. Note that the trouble with 2 has been systematic since then. It arose in Artin's conjecture about densities of primitive roots as mentioned in the remarks after Theorem 9.4. It arose in the Grunwald theorem of class field theory (corrected by Wang, cf. Artin-Tate [ArT 68], Chapter 10). It arose in Shafarevich's proof that given a solvable group, there exists a Galois extension of $\mathbf{Q}$ having that group as Galois group, mentioned at the end of §7.

Abelian extensions of a number field F are harder to describe than over the rationals, and the fundamental theory giving a description of such extensions is called class field theory (see the above reference). I shall give one significant example exhibiting the flavor. Let R_F be the ring of algebraic integers in F. It can be shown that R_F is a Dedekind ring. (*Cf.* [La 70], Chapter I, §6, Theorem 2.) Let P be a prime ideal of R_F. Then $P \cap \mathbf{Z} = (p)$ for some prime number p.

Furthermore, R_F/P is a finite field with q elements. Let K be a finite Galois extension of F. It will be shown in Chapter VII that there exists a prime Q of R_K such that $Q \cap R_F = P$. Furthermore, there exists an element

$$\mathrm{Fr}_Q \in G = \mathrm{Gal}(K/F)$$

such that $\mathrm{Fr}_Q(Q) = Q$ and for all $\alpha \in R_K$ we have

$$\mathrm{Fr}_Q \alpha \equiv \alpha^q \bmod Q.$$

We call Fr_Q a **Frobenius element** in the Galois group G associated with Q. (See Chapter VII, Theorem 2.9.) Furthermore, for all but a finite number of Q, two such elements are conjugate to each other in G. We denote any of them by Fr_P. If G is abelian, then there is only one element Fr_P in the Galois group.

Theorem 15.1. *There exists a unique finite abelian extension K of F having the following property. If P_1, P_2 are prime ideals of R_F, then $\mathrm{Fr}_{P_1} = \mathrm{Fr}_{P_2}$ if and only if there is an element α of K such that $\alpha P_1 = P_2$.*

In a similar but more complicated manner, one can characterize all abelian extensions of F. This theory is known as class field theory, developed by Kronecker, Weber, Hilbert, Takagi, and Artin. The main statement concerning the Frobenius automorphism as above is Artin's Reciprocity Law. Artin-Tate's notes give a cohomological account of class field theory. My *Algebraic Number Theory* gives an account following Artin's first proof dating back to 1927, with later simplifications by Artin himself. Both techniques are valuable to know.

Cyclotomic extensions should be viewed in the light of Theorem 15.1. Indeed, let $K = \mathbf{Q}(\zeta)$, where ζ is a primitive n-th root of unity. For a prime $p \nmid n$, we have the Frobenius automorphism Fr_p, whose effect on ζ is $\mathrm{Fr}_p(\zeta) = \zeta^p$. Then

$$\mathrm{Fr}_{p_1} = \mathrm{Fr}_{p_2} \quad \text{if and only if} \quad p_1 \equiv p_2 \bmod n.$$

To encompass both Theorem 15.1 and the cyclotomic case in one framework, one has to formulate the result of class field theory for generalized ideal classes, not just the ordinary ones when two ideals are equivalent if and only if they differ multiplicatively by a non-zero field element. See my *Algebraic Number Theory* for a description of these generalized ideal classes.

The non-abelian case is much more difficult. I shall indicate briefly a special case which gives some of the flavor of what goes on. The problem is to do for non-abelian extensions what Artin did for abelian extensions. Artin went as far as saying that the problem was not to give proofs but to formulate what was to be proved. The insight of Langlands and others in the sixties shows that actually Artin was mistaken. The problem lies in both. Shimura made several computations in this direction involving "modular forms" [Sh 66]. Langlands gave a number of conjectures relating Galois groups with "automorphic forms", which showed that the answer lay in deeper theories, whose formulations, let alone their proofs, were difficult. Great progress was made in the seventies by Serre and Deligne, who proved a first case of Langland's conjecture [DeS 74].

The study of non-abelian Galois groups occurs via their linear "representations". For instance, let l be a prime number. We can ask whether $GL_n(\mathbf{F}_l)$, or $GL_2(\mathbf{F}_l)$, or $PGL_2(\mathbf{F}_l)$ occurs as a Galois group over $\mathbf{Q}$, and "how". The problem is to find natural objects on which the Galois group operates as a linear map, such that we get in a natural way an isomorphism of this Galois group with one of the above linear groups. The theories which indicate in which direction to find such objects are much beyond the level of this course, and lie in the theory of modular functions, involving both analysis and algebra, which form a background for the number theoretic applications. Again I pick a special case to give the flavor.

Let K be a finite Galois extension of $\mathbf{Q}$, with Galois group

$$G = \mathrm{Gal}(K/\mathbf{Q}).$$

Let

$$\rho\colon G \to GL_2(\mathbf{F}_l)$$

be a homomorphism of G into the group of 2×2 matrices over the finite field $\mathbf{F}_l$ for some prime l. Such a homomorphism is called a **representation** of G. From elementary linear algebra, if

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is a 2×2 matrix, we have its trace and determinant defined by

$$\mathrm{tr}(M) = a + d \quad \text{and} \quad \det M = ad - bc.$$

Thus we can take the trace and determinant $\mathrm{tr}\ \rho(\sigma)$ and $\det \rho(\sigma)$ for $\sigma \in G$.

Consider the infinite product with a variable q:

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} a_n q^n.$$

The coefficients a_n are integers, and $a_1 = 1$.

Theorem 15.2. *For each prime l there exists a unique Galois extension K of $\mathbf{Q}$, with Galois group G, and an injective homomorphism*

$$\rho\colon G \to GL_2(\mathbf{F}_l)$$

having the following property. For all but a finite number of primes p, if a_p is the coefficient of q^p in $\Delta(q)$, then we have

$$\mathrm{tr}\ \rho(\mathrm{Fr}_p) \equiv a_p \bmod l \quad \text{and} \quad \det \rho(\mathrm{Fr}_p) \equiv p^{11} \bmod l.$$

Furthermore, for all primes $l \neq 2, 3, 5, 7, 23, 691$, the image $\rho(G)$ in $GL_2(\mathbf{F}_l)$ consists of those matrices $M \in GL_2(\mathbf{F}_l)$ such that det M *is an eleventh power in $\mathbf{F}_l^*$.*

The above theorem was conjectured by Serre in 1968 [Se 68]. A proof of the existence as in the first statement was given by Deligne [De 68]. The second statement, describing how big the Galois group actually is in the group of matrices $GL_2(\mathbf{F}_l)$ is due to Serre and Swinnerton-Dyer [Se 72], [SwD 73].

The point of $\Delta(q)$ is that if we put $q = e^{2\pi iz}$, where z is a variable in the upper half-plane, then Δ is a modular form of weight 12. For definitions and an introduction, see the last chapter of [Se 73], [La 73], [La 76], and the following comments. The general result behind Theorem 15.2 for modular forms of weight $\geqq 2$ was given by Deligne [De 73]. For weight 1, it is due to Deligne-Serre [DeS 74]. We summarize the situation as follows.

Let N be a positive integer. To N we associate the subgroups

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$$

of $SL_2(\mathbf{Z})$ defined by the conditions for a matrix $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$:

$\alpha \in \Gamma(N)$ if and only if $a \equiv d \equiv 1 \bmod N$ and $b \equiv c \equiv 0 \bmod N$;

$\alpha \in \Gamma_1(N)$ if and only if $a \equiv d \equiv 1 \bmod N$ and $c \equiv 0 \bmod N$;

$\alpha \in \Gamma_0(N)$ if and only if $c \equiv 0 \bmod N$.

Let f be a function on the upper half-plane $\mathfrak{H} = \{z \in \mathbf{C}, \operatorname{Im}(z) > 0\}$. Let k be an integer. For

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{R}),$$

define $f \circ [\gamma]_k$ (an operation on the right) by

$$f \circ [\gamma]_k(z) = (cz + d)^{-k} f(\gamma z) \quad \text{where} \quad \gamma z = \frac{az + b}{cz + d}.$$

Let Γ be a subgroup of $SL_2(\mathbf{Z})$ containing $\Gamma(N)$. We define f to be **modular of weight k on Γ** if:

$\mathbf{M_k}$ 1. f is holomorphic on $\mathfrak{H}$;

$\mathbf{M_k}$ 2. f is holomorphic at the cusps, meaning that for all $\alpha \in SL_2(\mathbf{Z})$, the function $f \circ [\alpha]_k$ has a power series expansion

$$f \circ [\alpha]_k(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z/N};$$

$\mathbf{M_k}$ 3. We have $f \circ [\gamma]_k = f$ for all $\gamma \in \Gamma$.

One says that f is **cuspidal** if in **$\mathbf{M_k}$ 2** the power series has a zero; that is, the power starts with $n \geqq 1$.

Suppose that f is modular of weight k on $\Gamma(N)$. Then f is modular on $\Gamma_1(N)$ if and only if $f(z+1) = f(z)$, or equivalently f has an expansion of the form

$$f(z) = f_\infty(q_z) = \sum_{n=0}^{\infty} a_n q^n \quad \text{where} \quad q = q_z = e^{2\pi i z}.$$

This power series is called the q-**expansion** of f.

Suppose f has weight k on $\Gamma_1(N)$. If $\gamma \in \Gamma_0(N)$ and γ is the above written matrix, then $f \circ [\gamma]_k$ depends only on the image of d in $(\mathbf{Z}/N\mathbf{Z})^*$, and we then denote $f \circ [\gamma]_k$ by $f \circ [d]_k$. Let

$$\varepsilon\colon (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$$

be a homomorphism (also called a **Dirichlet character**). One says that ε is **odd** if $\varepsilon(-1) = -1$, and **even** if $\varepsilon(-1) = 1$. One says that f is **modular of type** (k, ε) on $\Gamma_0(N)$ if f has weight k on $\Gamma_1(N)$, and

$$f \circ [d]_k = \varepsilon(d) f \quad \text{for all} \quad d \in (\mathbf{Z}/N\mathbf{Z})^*.$$

It is possible to define an algebra of operators on the space of modular forms of given type. This requires more extensive background, and I refer the reader to [La 76] for a systematic exposition. Among all such forms, it is then possible to distinguish some of them which are eigenvectors for this Hecke algebra, or, as one says, eigenfunctions for this algebra. One may then state the Deligne-Serre theorem as follows.

Let $f \neq 0$ be a modular form of type $(1, \varepsilon)$ on $\Gamma_0(N)$, so f has weight 1. Assume that ε is odd. Assume that f is an eigenfunction of the Hecke algebra, with q-expansion $f_\infty = \sum a_n q^n$, normalized so that $a_1 = 1$. Then there exists a unique finite Galois extension K of $\mathbf{Q}$ with Galois group G, and a representation $\rho\colon G \to GL_2(\mathbf{C})$ (actually an injective homomorphism), such that for all primes $p \nmid N$ the characteristic polynomial of $\rho(\mathrm{Fr}_p)$ is

$$X^2 - a_p X + \varepsilon(p).$$

The representation ρ is irreducible if and only if f is cuspidal.

Note that the representation ρ has values in $GL_2(\mathbf{C})$. For extensive work of Serre and his conjectures concerning representations of Galois groups in $GL_2(\mathbf{F})$ when $\mathbf{F}$ is a finite field, see [Se 87]. Roughly speaking, the general philosophy started by a conjecture of Taniyama-Shimura and the Langlands conjectures is that everything in sight is "modular". Theorem 15.2 and the Deligne-Serre theorem are prototypes of results in this direction. For "modular" representations in $GL_2(\mathbf{F})$, when $\mathbf{F}$ is a finite field, Serre's conjectures have been proved, mostly by Ribet [Ri 90]. As a result, following an idea of Frey, Ribet also showed how the Taniyama-Shimura conjecture implies Fermat's last theorem [Ri 90b]. Note that Serre's conjectures that certain representations in $GL_2(\mathbf{F})$ are modular imply the Taniyama-Shimura conjecture.

Bibliography

[ArT 68] E. ARTIN and J. TATE, *Class Field Theory*, Benjamin-Addison-Wesley, 1968 (reprinted by Addison-Wesley, 1991)

[De 68] P. DELIGNE, Formes modulaires et représentations l-adiques, *Séminaire Bourbaki* 1968–1969, exp. No. 355

[De 73] P. DELIGNE, Formes modulaires et représentations de $GL(2)$, *Springer Lecture Notes* **349** (1973), pp. 55–105

[DeS 74] P. DELIGNE and J. P. SERRE, Formes modulaires de poids 1, *Ann. Sci. ENS* **7** (1974), pp. 507–530

[La 70] S. LANG, *Algebraic Number Theory*, Springer Verlag, reprinted from Addison-Wesley (1970)

[La 73] S. LANG, *Elliptic functions*, Springer Verlag, 1973

[La 76] S. LANG, *Introduction to modular forms*, Springer Verlag, 1976

[Ri 90a] K. RIBET, On modular representations of $\mathrm{Gal}(\overline{Q}/Q)$ arising from modular forms, *Invent. Math.* **100** (1990), pp. 431–476

[Ri 90b] K. RIBET, From the Taniyama-Shimura conjecture to Fermat's last theorem, *Annales de la Fac. des Sci. Toulouse* (1990), pp. 116–139

[Se 68] J.-P. SERRE, Une interprétation des congruences relatives à la fonction de Ramanujan, *Séminaire Delange-Pisot-Poitou*, 1967–1968

[Se 72] J.-P. SERRE, Congruences et formes modulaires (d'après Swinnerton-Dyer), *Séminaire Bourbaki*, 1971–1972

[Se 73] J.-P. SERRE, *A course in arithmetic*, Springer Verlag, 1973

[Se 87] J.-P. SERRE, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{Q}/Q)$, *Duke Math. J.* **54** (1987), pp. 179–230

[Shi 66] G. SHIMURA, A reciprocity law in non-solvable extensions, *J. reine angew. Math.* **221** (1966), pp. 209–220

[Shi 71] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton University Press, 1971

[SwD 73] H. P. SWINNERTON-DYER, On l-adic representations and congruences for coefficients of modular forms, (Antwerp conference) *Springer Lecture Notes* **350** (1973)

EXERCISES

1. What is the Galois group of the following polynomials?
   (a) $X^3 - X - 1$ over $\mathbf{Q}$.
   (b) $X^3 - 10$ over $\mathbf{Q}$.
   (c) $X^3 - 10$ over $\mathbf{Q}(\sqrt{2})$.
   (d) $X^3 - 10$ over $\mathbf{Q}(\sqrt{-3})$.
   (e) $X^3 - X - 1$ over $\mathbf{Q}(\sqrt{-23})$.
   (f) $X^4 - 5$ over $\mathbf{Q}$, $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{-5})$, $\mathbf{Q}(i)$.
   (g) $X^4 - a$ where a is any integer $\neq 0, \neq \pm 1$ and is square free. Over $\mathbf{Q}$.

(h) $X^3 - a$ where a is any square-free integer $\geqq 2$. Over $\mathbf{Q}$.
(i) $X^4 + 2$ over $\mathbf{Q}$, $\mathbf{Q}(i)$.
(j) $(X^2 - 2)(X^2 - 3)(X^2 - 5)(X^2 - 7)$ over $\mathbf{Q}$.
(k) Let $p_1, \ldots, p_n$ be distinct prime numbers. What is the Galois group of $(X^2 - p_1) \cdots (X^2 - p_n)$ over $\mathbf{Q}$?
(l) $(X^3 - 2)(X^3 - 3)(X^2 - 2)$ over $\mathbf{Q}(\sqrt{-3})$.
(m) $X^n - t$, where t is transcendental over the complex numbers $\mathbf{C}$ and n is a positive integer. Over $\mathbf{C}(t)$.
(n) $X^4 - t$, where t is as before. Over $\mathbf{R}(t)$.

2. Find the Galois groups over $\mathbf{Q}$ of the following polynomials.
(a) $X^3 + X + 1$ (b) $X^3 - X + 1$ (g) $X^3 + X^2 - 2X - 1$
(c) $X^3 + 2X + 1$ (d) $X^3 - 2X + 1$
(e) $X^3 - X - 1$ (f) $X^3 - 12X + 8$

3. Let $k = \mathbf{C}(t)$ be the field of rational functions in one variable. Find the Galois group over k of the following polynomials:
(a) $X^3 + X + t$ (b) $X^3 - X + t$
(c) $X^3 + tX + 1$ (d) $X^3 - 2tX + t$
(e) $X^3 - X - t$ (f) $X^3 + t^2X - t^3$

4. Let k be a field of characteristic $\neq 2$. Let $c \in k$, $c \notin k^2$. Let $F = k(\sqrt{c})$. Let $\alpha = a + b\sqrt{c}$ with $a, b \in k$ and not both $a, b = 0$. Let $E = F(\sqrt{\alpha})$. Prove that the following conditions are equivalent.
(1) E is Galois over k.
(2) $E = F(\sqrt{\alpha'})$, where $\alpha' = a - b\sqrt{c}$.
(3) Either $\alpha\alpha' = a^2 - cb^2 \in k^2$ or $c\alpha\alpha' \in k^2$.
Show that when these conditions are satisfied, then E is cyclic over k of degree 4 if and only if $c\alpha\alpha' \in k^2$.

5. Let k be a field of characteristic $\neq 2, 3$. Let $f(X)$, $g(X) = X^2 - c$ be irreducible polynomials over k, of degree 3 and 2 respectively. Let D be the discriminant of f. Assume that
$$[k(D^{1/2}) : k] = 2 \quad \text{and} \quad k(D^{1/2}) \neq k(c^{1/2}).$$
Let α be a root of f and β a root of g in an algebraic closure. Prove:
(a) The splitting field of fg over k has degree 12.
(b) Let $\gamma = \alpha + \beta$. Then $[k(\gamma) : k] = 6$.

6. (a) Let K be cyclic over k of degree 4, and of characteristic $\neq 2$. Let $G_{K/k} = \langle\sigma\rangle$. Let E be the unique subfield of K of degree 2 over k. Since $[K : E] = 2$, there exists $\alpha \in K$ such that $\alpha^2 = \gamma \in E$ and $K = E(\alpha)$. Prove that there exists $z \in E$ such that
$$z\sigma z = -1, \quad \sigma\alpha = z\alpha, \quad z^2 = \sigma\gamma/\gamma.$$

(b) Conversely, let E be a quadratic extension of k and let $G_{E/k} = \langle\tau\rangle$. Let $z \in E$ be an element such that $z\tau z = -1$. Prove that there exists $\gamma \in E$ such that $z^2 = \tau\gamma/\gamma$. Then $E = k(\gamma)$. Let $\alpha^2 = \gamma$, and let $K = k(\alpha)$. Show that K is Galois, cyclic of degree 4 over k. Let σ be an extension of τ to K. Show that σ is an automorphism of K which generates $G_{K/k}$, satisfying $\sigma^2\alpha = -\alpha$ and $\sigma\alpha = \pm z\alpha$. Replacing z by $-z$ originally if necessary, one can then have $\sigma\alpha = z\alpha$.

7. (a) Let $K = \mathbf{Q}(\sqrt{a})$ where $a \in \mathbf{Z}$, $a < 0$. Show that K cannot be embedded in a cyclic extension whose degree over $\mathbf{Q}$ is divisible by 4.
   (b) Let $f(X) = X^4 + 30X^2 + 45$. Let α be a root of F. Prove that $\mathbf{Q}(\alpha)$ is cyclic of degree 4 over $\mathbf{Q}$.
   (c) Let $f(X) = X^4 + 4x^2 + 2$. Prove that f is irreducible over $\mathbf{Q}$ and that the Galois group is cyclic.

8. Let $f(X) = X^4 + aX^2 + b$ be an irreducible polynomial over $\mathbf{Q}$, with roots $\pm\alpha, \pm\beta$, and splitting field K.
   (a) Show that $\mathrm{Gal}(K/\mathbf{Q})$ is isomorphic to a subgroup of D_8 (the non-abelian group of order 8 other than the quaternion group), and thus is isomorphic to one of the following:
   (i) $\mathbf{Z}/4\mathbf{Z}$ (ii) $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (iii) D_8.
   (b) Show that the first case happens if and only if
   $$\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbf{Q}.$$
   Case (ii) happens if and only if $\alpha\beta \in \mathbf{Q}$ or $\alpha^2 - \beta^2 \in \mathbf{Q}$. Case (iii) happens otherwise. (Actually, in (ii), the case $\alpha^2 - \beta^2 \in \mathbf{Q}$ cannot occur. It corresponds to a subgroup $D_8 \subset S_4$ which is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, but is not transitive on $\{1, 2, 3, 4\}$).
   (c) Find the splitting field K in $\mathbf{C}$ of the polynomial
   $$X^4 - 4X^2 - 1.$$
   Determine the Galois group of this splitting field over $\mathbf{Q}$, and describe fully the lattices of subfields and of subgroups of the Galois group.

9. Let K be a finite separable extension of a field k, of prime degree p. Let $\theta \in K$ be such that $K = k(\theta)$, and let $\theta_1, \ldots, \theta_p$ be the conjugates of θ over k in some algebraic closure. Let $\theta = \theta_1$. If $\theta_2 \in k(\theta)$, show that K is Galois and in fact cyclic over k.

10. Let $f(X) \in \mathbf{Q}[X]$ be a polynomial of degree n, and let K be a splitting field of f over $\mathbf{Q}$. Suppose that $\mathrm{Gal}(K/\mathbf{Q})$ is the symmetric group S_n with $n > 2$.
   (a) Show that f is irreducible over $\mathbf{Q}$.
   (b) If α is a root of f, show that the only automorphism of $\mathbf{Q}(\alpha)$ is the identity.
   (c) If $n \geqq 4$, show that $\alpha^n \notin \mathbf{Q}$.

11. A polynomial $f(X)$ is said to be **reciprocal** if whenever α is a root, then $1/\alpha$ is also a root. We suppose that f has coefficients in a real subfield k of the complex numbers. If f is irreducible over k, and has a nonreal root of absolute value 1, show that f is reciprocal of even degree.

12. What is the Galois group over the rationals of $X^5 - 4X + 2$?

13. What is the Galois group over the rationals of the following polynomials:
   (a) $X^4 + 2X^2 + X + 3$
   (b) $X^4 + 3X^3 - 3X - 2$
   (c) $X^6 + 22X^5 - 9X^4 + 12X^3 - 37X^2 - 29X - 15$
   [*Hint*: Reduce mod 2, 3, 5.]

14. Prove that given a symmetric group S_n, there exists a polynomial $f(X) \in \mathbf{Z}[X]$ with leading coefficient 1 whose Galois group over $\mathbf{Q}$ is S_n. [*Hint*: Reducing mod 2, 3, 5, show that there exists a polynomial whose reductions are such that the Galois group

contains enough cycles to generate S_n. Use the Chinese remainder theorem, also to be able to apply Eisenstein's criterion.]

15. Let K/k be a Galois extension, and let F be an intermediate field between k and K. Let H be the subgroup of $\mathrm{Gal}(K/k)$ mapping F into itself. Show that H is the normalizer of $\mathrm{Gal}(K/F)$ in $\mathrm{Gal}(K/k)$.

16. Let K/k be a finite Galois extension with group G. Let $\alpha \in K$ be such that $\{\sigma\alpha\}_{\sigma\in G}$ is a normal basis. For each subset S of G let $S(\alpha) = \sum_{\sigma\in S}\sigma\alpha$. Let H be a subgroup of G and let F be the fixed field of H. Show that there exists a basis of F over k consisting of elements of the form $S(\alpha)$.

Cyclotomic fields

17. (a) Let k be a field of characteristic $\not| 2n$, for some odd integer $n \geqq 1$, and let ζ be a primitive n-th root of unity, in k. Show that k also contains a primitive $2n$-th root of unity.
    (b) Let k be a finite extension of the rationals. Show that there is only a finite number of roots of unity in k.

18. (a) Determine which roots of unity lie in the following fields: $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{-5})$.
    (b) For which integers m does a primitive m-th root of unity have degree 2 over $\mathbf{Q}$?

19. Let ζ be a primitive n-th root of unity. Let $K = \mathbf{Q}(\zeta)$.
    (a) If $n = p^r$ ($r \geqq 1$) is a prime power, show that $N_{K/\mathbf{Q}}(1 - \zeta) = p$.
    (b) If n is composite (divisible by at least two primes) then $N_{K/\mathbf{Q}}(1 - \zeta) = 1$.

20. Let $f(X) \in \mathbf{Z}[X]$ be a non-constant polynomial with integer coefficients. Show that the values $f(a)$ with $a \in \mathbf{Z}^+$ are divisible by infinitely many primes.

    [*Note*: This is trivial. A much deeper question is whether there are infinitely many a such that $f(a)$ is prime. There are three necessary conditions:
    The leading coefficient of f is positive.
    The polynomial is irreducible.
    The set of values $f(\mathbf{Z}^+)$ has no common divisor > 1.

    A conjecture of Bouniakowski [Bo 1854] states that these conditions are sufficient. The conjecture was rediscovered later and generalized to several polynomials by Schinzel [Sch 58]. A special case is the conjecture that $X^2 + 1$ represents infinitely many primes. For a discussion of the general conjecture and a quantitative version giving a conjectured asymptotic estimate, see Bateman and Horn [BaH 62]. Also see the comments in [HaR 74]. More precisely, let $f_1, \ldots, f_r$ be polynomials with integer coefficients satisfying the first two conditions (positive leading coefficient, irreducible). Let

$$f = f_1 \cdots f_r$$

be their product, and assume that f satisfies the third condition. Define:

$\pi_{(f)}(x)$ = number of positive integers $n \leqq x$ such that $f_1(n), \ldots, f_r(n)$ are all primes.

(We ignore the finite number of values of n for which some $f_i(n)$ is negative.) The

Bateman-Horn conjecture is that

$$\pi_{(f)}(x) \sim (d_1 \cdots d_r)^{-1} C(f) \int_0^x \frac{1}{(\log t)^r}\, dt,$$

where

$$C(f) = \prod_p \left\{ \left(1 - \frac{1}{p}\right)^{-r} \left(1 - \frac{N_f(p)}{p}\right) \right\},$$

the product being taken over all primes p, and $N_f(p)$ is the number of solutions of the congruence

$$f(n) \equiv 0 \bmod p.$$

Bateman and Horn show that the product converges absolutely. When $r = 1$ and $f(n) = an + b$ with a, b relatively prime integers, $a > 0$, then one gets Dirichlet's theorem that there are infinitely many primes in an arithmetic progression, together with the Dirichlet density of such primes.

[BaH 62] P. T. BATEMAN and R. HORN, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962) pp. 363-367

[Bo 1854] V. BOUNIAKOWSKY, Sur les diviseurs numériques invariables des fonctions rationnelles entières, *Mémoires sc. math. et phys. T. VI* (1854-1855) pp. 307-329

[HaR 74] H. HALBERSTAM and H.-E. RICHERT, *Sieve methods*, Academic Press, 1974

[Sch 58] A. SCHINZEL and W. SIERPINSKI, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958) pp. 185-208

21. (a) Let a be a non-zero integer, p a prime, n a positive integer, and $p \nmid n$. Prove that $p \mid \Phi_n(a)$ if and only if a has period n in $(\mathbf{Z}/p\mathbf{Z})^*$.
    (b) Again assume $p \nmid n$ Prove that $p \mid \Phi_n(a)$ for some $a \in \mathbf{Z}$ if and only if $p \equiv 1 \bmod n$. Deduce from this that there are infinitely many primes $\equiv 1 \bmod n$, a special case of Dirichlet's theorem for the existence of primes in an arithmetic progression.

22. Let $F = \mathbf{F}_p$ be the prime field of characteristic p. Let K be the field obtained from F by adjoining all primitive l-th roots of unity, for all prime numbers $l \neq p$. Prove that K is algebraically closed. [*Hint*: Show that if q is a prime number, and r an integer $\geqq 1$, there exists a prime l such that the period of p mod l is q^r, by using the following old trick of Van der Waerden: Let l be a prime dividing the number

$$b = \frac{p^{q^r} - 1}{p^{q^{r-1}} - 1} = (p^{q^{r-1}} - 1)^{q-1} + q(p^{q^{r-1}} - 1)^{q-2} + \cdots + q.$$

If l does not divide $p^{q^{r-1}} - 1$, we are done. Otherwise, $l = q$. But in that case q^2 does not divide b, and hence there exists a prime $l \neq q$ such that l divides b. Then the degree of $F(\zeta_l)$ over F is q^r, so K contains subfields of arbitrary degree over F.]

23. (a) Let G be a finite *abelian* group. Prove that there exists an abelian extension of $\mathbf{Q}$ whose Galois group is G.

(b) Let k be a finite extension of $\mathbf{Q}$, and let G be a finite abelian group. Prove that there exist infinitely many abelian extensions of k whose Galois group is G.

24. Prove that there are infinitely many non-zero integers a, $b \neq 0$ such that $-4a^3 - 27b^2$ is a square in $\mathbf{Z}$.

25. Let k be a field such that every finite extension is cyclic. Show that there exists an automorphism σ of k^a over k such that k is the fixed field of σ.

26. Let $\mathbf{Q}^a$ be a fixed algebraic closure of $\mathbf{Q}$. Let E be a maximal subfield of $\mathbf{Q}^a$ not containing $\sqrt{2}$ (such a subfield exists by Zorn's lemma). Show that every finite extension of E is cyclic. (Your proof should work taking any algebraic irrational number instead of $\sqrt{2}$.)

27. Let k be a field, k^a an algebraic closure, and σ an automorphism of k^a leaving k fixed. Let F be the fixed field of σ. Show that every finite extension of F is cyclic. (The above two problems are examples of Artin, showing how to dig holes in an algebraically closed field.)

28. Let E be an algebraic extension of k such that every non-constant polynomial $f(X)$ in $k[X]$ has at least one root in E. Prove that E is algebraically closed. [*Hint*: Discuss the separable and purely inseparable cases separately, and use the primitive element theorem.]

29. (a) Let K be a cyclic extension of a field F, with Galois group G generated by σ. Assume that the characteristic is p, and that $[K:F] = p^{m-1}$ for some integer $m \geqq 2$. Let β be an element of K such that $\mathrm{Tr}_F^K(\beta) = 1$. Show that there exists an element α in K such that

$$\sigma\alpha - \alpha = \beta^p - \beta.$$

(b) Prove that the polynomial $X^p - X - \alpha$ is irreducible in $K[X]$.

(c) If θ is a root of this polynomial, prove that $F(\theta)$ is a Galois, cyclic extension of degree p^m of F, and that its Galois group is generated by an extension σ^* of σ such that

$$\sigma^*(\theta) = \theta + \beta.$$

30. Let A be an abelian group and let G be a finite cyclic group operating on A [by means of a homomorphism $G \to \mathrm{Aut}(A)$]. Let σ be a generator of G. We define the trace $\mathrm{Tr}_G = \mathrm{Tr}$ on A by $\mathrm{Tr}(x) = \sum_{\tau \in G} \tau x$. Let A_{Tr} denote the kernel of the trace, and let $(1 - \sigma)A$ denote the subgroup of A consisting of all elements of type $y - \sigma y$. Show that $H^1(G, A) \approx A_{\mathrm{Tr}}/(1 - \sigma)A$.

31. Let F be a finite field and K a finite extension of F. Show that the norm N_F^K and the trace Tr_F^K are surjective (as maps from K into F).

32. Let E be a finite separable extension of k, of degree n. Let $W = (w_1, \ldots, w_n)$ be elements of E. Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of E in k^a over k. Define the **discriminant** of W to be

$$D_{E/k}(W) = \det(\sigma_i w_j)^2.$$

Prove:

(a) If $V = (v_1, \ldots, v_n)$ is another set of elements of E and $C = (c_{ij})$ is a matrix of elements of k such that $w_i = \sum c_{ij} v_j$, then

$$D_{E/k}(W) = \det(C)^2 D_{E/k}(V).$$

(b) The discriminant is an element of k.

(c) Let $E = k(\alpha)$ and let $f(X) = \operatorname{Irr}(\alpha, k, X)$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f and say $\alpha = \alpha_1$. Then

$$f'(\alpha) = \prod_{j=2}^{n} (\alpha - \alpha_j).$$

Show that

$$D_{E/k}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_k^E(f'(\alpha)).$$

(d) Let the notation be as in (a). Show that $\det(\operatorname{Tr}(w_i w_j)) = (\det(\sigma_i w_j))^2$. [*Hint*: Let A be the matrix $(\sigma_i w_j)$. Show that ${}^tAA$ is the matrix $(\operatorname{Tr}(w_i w_j))$.]

Rational functions

33. Let $K = \mathbf{C}(x)$ where x is transcendental over $\mathbf{C}$, and let ζ be a primitive cube root of unity in $\mathbf{C}$. Let σ be the automorphism of K over $\mathbf{C}$ such that $\sigma x = \zeta x$. Let τ be the automorphism of K over $\mathbf{C}$ such that $\tau x = x^{-1}$. Show that

$$\sigma^3 = 1 = \tau^2 \quad \text{and} \quad \tau\sigma = \sigma^{-1}\tau.$$

Show that the group of automorphisms G generated by σ and τ has order 6 and the subfield F of K fixed by G is the field $\mathbf{C}(y)$ where $y = x^3 + x^{-3}$.

34. Give an example of a field K which is of degree 2 over two distinct subfields E and F respectively, but such that K is not algebraic over $E \cap F$.

35. Let k be a field and X a variable over k. Let

$$\varphi(X) = \frac{f(X)}{g(X)}$$

be a rational function in $k(X)$, expressed as a quotient of two polynomials f, g which are relatively prime. Define the degree of φ to be $\max(\deg f, \deg g)$. Let $Y = \varphi(X)$. (a) Show that the degree of φ is equal to the degree of the field extension $k(X)$ over $k(Y)$ (assuming $Y \notin k$). (b) Show that every automorphism of $k(X)$ over k can be represented by a rational function φ of degree 1, and is therefore induced by a map

$$X \mapsto \frac{aX + b}{cX + d}$$

with $a, b, c, d \in k$ and $ad - bc \neq 0$. (c) Let G be the group of automorphisms of $k(X)$ over k. Show that G is generated by the following automorphisms:

$$\tau_b : X \mapsto X + b, \qquad \sigma_a : X \mapsto aX \quad (a \neq 0), \qquad X \mapsto X^{-1}$$

with $a, b \in k$.

36. Let k be a finite field with q elements. Let $K = k(X)$ be the rational field in one variable. Let G be the group of automorphisms of K obtained by the mappings

$$X \mapsto \frac{aX + b}{cX + d}$$

with a, b, c, d in k and $ad - bc \neq 0$. Prove the following statements:

(a) The order of G is $q^3 - q$.

(b) The fixed field of G is equal to $k(Y)$ where

$$Y = \frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}}.$$

(c) Let H_1 be the subgroup of G consisting of the mappings $X \mapsto aX + b$ with $a \neq 0$. The fixed field of H_1 is $k(T)$ where $T = (X^q - X)^{q-1}$.

(d) Let H_2 be the subgroup of H_1 consisting of the mappings $X \to X + b$ with $b \in k$. The fixed field of H_2 is equal to $k(Z)$ where $Z = X^q - X$.

Some aspects of Kummer theory

37. Let k be a field of characteristic 0. Assume that for each finite extension E of k, the index $(E^* : E^{*n})$ is finite for every positive integer n. Show that for each positive integer n, there exists only a finite number of abelian extensions of k of degree n.

38. Let $a \neq 0, \neq \pm 1$ be a square-free integer. For each prime number p, let K_p be the splitting field of the polynomial $X^p - a$ over $\mathbf{Q}$. Show that $[K_p : \mathbf{Q}] = p(p-1)$. For each square-free integer $m > 0$, let

$$K_m = \prod_{p \mid m} K_p$$

be the compositum of all fields K_p for $p \mid m$. Let $d_m = [K_m : \mathbf{Q}]$ be the degree of K_m over $\mathbf{Q}$. Show that if m is odd then $d_m = \prod_{p \mid m} d_p$, and if m is even, $m = 2n$ then $d_{2n} = d_n$ or $2d_n$ according as $\sqrt{a}$ is or is not in the field of m-th roots of unity $\mathbf{Q}(\zeta_m)$.

39. Let K be a field of characteristic 0 for simplicity. Let Γ be a finitely generated subgroup of K^*. Let N be an *odd* positive integer. Assume that for each prime $p \mid N$ we have

$$\Gamma = \Gamma^{1/p} \cap K,$$

and also that $\mathrm{Gal}(K(\mu_N)/K) \approx \mathbf{Z}(N)^*$. Prove the following.

(a) $\Gamma/\Gamma^N \approx \Gamma/(\Gamma \cap K^{*N}) \approx \Gamma K^{*N}/K^{*N}$.

(b) Let $K_N = K(\mu_N)$. Then

$$\Gamma \cap K_N^{*N} = \Gamma^N.$$

[*Hint*: If these two groups are not equal, then for some prime $p \mid N$ there exists an element $a \in \Gamma$ such that

$$a = b^p \quad \text{with} \quad b \in K_N \quad \text{but} \quad b \notin K.$$

In other words, a is not a p-th power in K but becomes a p-th power in K_N. The equation $x^p - a$ is irreducible over K. Show that b has degree p over $K(\mu_p)$, and that $K(\mu_p, a^{1/p})$ is not abelian over K, so $a^{1/p}$ has degree p over $K(\mu_p)$. Finish the proof yourself.]

(c) Conclude that the natural Kummer map

$$\Gamma/\Gamma^N \to \mathrm{Hom}(H_\Gamma(N), \mu_N)$$

is an isomorphism.

(d) Let $G_\Gamma(N) = \mathrm{Gal}(K(\Gamma^{1/N}, \mu_N)/K)$. Then the commutator subgroup of $G_\Gamma(N)$ is $H_\Gamma(N)$, and in particular $\mathrm{Gal}(K_N/K)$ is the maximal abelian quotient of $G_\Gamma(N)$.

40. Let K be a field and p a prime number not equal to the characteristic of K. Let Γ be a finitely generated subgroup of K^*, and assume that Γ is equal to its own p-division group in K, that is if $z \in K$ and $z^p \in \Gamma$, then $z \in \Gamma$. If p is odd, assume that $\mu_p \subset K$, and if $p = 2$, assume that $\mu_4 \subset K$. Let

$$(\Gamma : \Gamma^p) = p^{r+1}.$$

Show that $\Gamma^{1/p}$ is its own p-division group in $K(\Gamma^{1/p})$, and

$$[K(\Gamma^{1/p^m}) : K] = p^{m(r+1)}$$

for all positive integers m.

41. **Relative invariants (Sato).** Let k be a field and K an extension of k. Let G be a group of automorphisms of K over k, and assume that k is the fixed field of G. (We do not assume that K is algebraic over k.) By a **relative invariant** of G in K we shall mean an element $P \in K$, $P \neq 0$, such that for each $\sigma \in G$ there exists an element $\chi(\sigma) \in k$ for which $P^\sigma = \chi(\sigma)P$. Since σ is an automorphism, we have $\chi(\sigma) \in k^*$. We say that the map $\chi : G \to k^*$ **belongs** to P, and call it a **character**. Prove the following statements:

(a) The map χ above is a homomorphism.

(b) If the same character χ belongs to relative invariants P and Q then there exists $c \in k^*$ such that $P = cQ$.

(c) The relative invariants form a multiplicative group, which we denote by I. Elements $P_1, \ldots, P_m$ of I are called multiplicatively independent mod k^* if their images in the factor group I/k^* are multiplicatively independent, i.e. if given integers $v_1, \ldots, v_m$ such that

$$P_1^{v_1} \cdots P_m^{v_m} = c \in k^*,$$

then $v_1 = \cdots = v_m = 0$.

(d) If $P_1, \ldots, P_m$ are multiplicatively independent mod k^* prove that they are algebraically independent over k. [*Hint*: Use Artin's theorem on characters.]

(e) Assume that $K = k(X_1, \ldots, X_n)$ is the quotient field of the polynomial ring $k[X_1, \ldots, X_n] = k[X]$, and assume that G induces an automorphism of the polynomial ring. Prove: If $F_1(X)$ and $F_2(X)$ are relative invariant polynomials, then their g.c.d. is relative invariant. If $P(X) = F_1(X)/F_2(X)$ is a relative invariant, and is the quotient of two relatively prime polynomials, then $F_1(X)$ and $F_2(X)$ are relative invariants. Prove that the relative invariant polynomials generate I/k^*. Let S be the set of relative invariant polynomials which cannot be factored into a product of two relative invariant polynomials of degrees $\geqq 1$. Show that the elements of S/k^* are multiplicatively independent, and hence that I/k^* is a free abelian group. [If you know about transcendence degree, then using (d) you can conclude that this group is finitely generated.]

42. Let $f(z)$ be a rational function with coefficients in a finite extension of the rationals. Assume that there are infinitely many roots of unity ζ such that $f(\zeta)$ is a root of unity. Show that there exists an integer n such that $f(z) = cz^n$ for some constant c (which is in fact a root of unity).

This exercise can be generalized as follows: Let Γ_0 be a finitely generated multiplicative group of complex numbers. Let Γ be the group of all complex numbers γ such that γ^m lies in Γ_0 for some integer $m \neq 0$. Let $f(z)$ be a rational function with complex coefficients such that there exist infinitely many $\gamma \in \Gamma$ for which $f(\gamma)$ lies in Γ. Then again, $f(z) = cz^n$ for some c and n. (Cf. *Fundamentals of Diophantine Geometry.*)

43. Let K/k be a Galois extension. We define the **Krull topology** on the group $G(K/k) = G$ by defining a base for open sets to consist of all sets σH where $\sigma \in G$ and $H = G(K/F)$ for some finite extension F of k contained in K.
    (a) Show that if one takes only those sets σH for which F is finite Galois over k then one obtains another base for the same topology.
    (b) The projective limit $\varprojlim G/H$ is embedded in the direct product
    $$\varprojlim_H G/H \to \prod_H G/H.$$
    Give the direct product the product topology. By Tychonoff's theorem in elementary point set topology, the direct product is compact because it is a direct product of finite groups, which are compact (and of course also discrete). Show that the inverse limit $\varprojlim G/H$ is closed in the product, and is therefore compact.
    (c) Conclude that $G(K/k)$ is compact.
    (d) Show that every closed subgroup of finite index in $G(K/k)$ is open.
    (e) Show that the closed subgroups of $G(K/k)$ are precisely those subgroups which are of the form $G(K/F)$ for some extension F of k contained in K.
    (f) Let H be an arbitrary subgroup of G and let F be the fixed field of H. Show that $G(K/F)$ is the closure of H in G.

44. Let k be a field such that every finite extension is cyclic, and having one extension of degree n for each integer n. Show that the Galois group $G = G(k^a/k)$ is the inverse limit $\lim \mathbf{Z}/m\mathbf{Z}$, as $m\mathbf{Z}$ ranges over all ideals of $\mathbf{Z}$, ordered by inclusion. Show that this limit is isomorphic to the direct product of the limits
$$\prod_p \lim_{n\to\infty} \mathbf{Z}/p^n\mathbf{Z} = \prod_p \mathbf{Z}_p$$
taken over all prime numbers p, in other words, it is isomorphic to the product of all p-adic integers.

45. Let k be a perfect field and k^a its algebraic closure. Let $\sigma \in G(k^a/k)$ be an element of infinite order, and suppose k is the fixed field of σ. For each prime p, let K_p be the composite of all cyclic extensions of k of degree a power of p.
    (a) Prove that k^a is the composite of all extensions K_p.
    (b) Prove that either $K_p = k$, or K_p is infinite cyclic over k. In other words, K_p cannot be finite cyclic over k and $\neq k$.
    (c) Suppose $k^a = K_p$ for some prime p, so k^a is an infinite cyclic tower of p-extensions. Let u be a p-adic unit, $u \in \mathbf{Z}_p^*$ such that u does not represent a rational number. Define σ^u, and prove that σ, σ^u are linearly independent

over $\mathbf{Z}$, i.e. the group generated by σ and σ^u is free abelian of rank 2. In particular $\{\sigma\}$ and $\{\sigma, \sigma^u\}$ have the same fixed field k.

Witt vectors

46. Let $x_1, x_2, \ldots$ be a sequence of algebraically independent elements over the integers $\mathbf{Z}$. For each integer $n \geqq 1$ define

$$x^{(n)} = \sum_{d \mid n} d x_d^{n/d}.$$

Show that x_n can be expressed in terms of $x^{(d)}$ for $d \mid n$, with rational coefficients.

Using vector notation, we call $(x_1, x_2, \ldots)$ the Witt components of the vector x, and call $(x^{(1)}, x^{(2)}, \ldots)$ its **ghost** components. We call x a **Witt vector**.

Define the power series

$$f_x(t) = \prod_{n \geqq 1} (1 - x_n t^n).$$

Show that

$$-t \frac{d}{dt} \log f_x(t) = \sum_{n \geqq 1} x^{(n)} t^n.$$

[By $\frac{d}{dt} \log f(t)$ we mean $f'(t)/f(t)$ if $f(t)$ is a power series, and the derivative $f'(t)$ is taken formally.]

If x, y are two Witt vectors, define their sum and product componentwise *with respect to the ghost components*, i.e.

$$(x \dotplus y)^{(n)} = x^{(n)} \dotplus y^{(n)}.$$

What is $(x + y)_n$? Well, show that

$$f_x(t) f_y(t) = \prod (1 + (x + y)_n t^n) = f_{x+y}(t).$$

Hence $(x + y)_n$ is a polynomial with integer coefficients in $x_1, y_1, \ldots, x_n, y_n$. Also show that

$$f_{xy}(t) = \prod_{d, e \geqq 1} (1 - x_d^{m/d} y_e^{m/e} t^m)^{de/m}$$

where m is the least common multiple of d, e and d, e range over all integers $\geqq 1$. Thus $(xy)_n$ is also a polynomial in $x_1, y_1 \ldots, x_n, y_n$ with integer coefficients. The above arguments are due to Witt (oral communication) and differ from those of his original paper.

If A is a commutative ring, then taking a homomorphic image of the polynomial ring over $\mathbf{Z}$ into A, we see that we can define addition and multiplication of Witt vectors with components in A, and that these Witt vectors form a ring $W(A)$. Show that W is a functor, i.e. that any ring homomorphism φ of A into a commutative ring A' induces a homomorphism $W(\varphi): W(A) \to W(A')$.

47. Let p be a prime number, and consider the projection of $W(A)$ on vectors whose components are indexed by a power of p. Now use the log to the base p to index these components, so that we write x_n instead of x_{p^n}. For instance, x_0 now denotes what was x_1 previously. For a Witt vector $x = (x_0, x_1, \ldots, x_n, \ldots)$ define

$$Vx = (0, x_0, x_1, \ldots) \quad \text{and} \quad Fx = (x_0^p, x_1^p, \ldots).$$

Thus V is a shifting operator. We have $V \circ F = F \circ V$. Show that

$$(Vx)^{(n)} = px^{(n-1)} \quad \text{and} \quad x^{(n)} = (Fx)^{(n-1)} + p^n x_n.$$

Also from the definition, we have

$$x^{(n)} = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n.$$

48. Let k be a field of characteristic p, and consider $W(k)$. Then V is an additive endomorphism of $W(k)$, and F is a ring homomorphism of $W(k)$ into itself. Furthermore, if $x \in W(k)$ then

$$px = VFx.$$

If $x, y \in W(k)$, then $(V^i x)(V^j y) = V^{i+j}(F^{p^j} x \cdot F^{p^i} y)$. For $a \in k$ denote by $\{a\}$ the Witt vector $(a, 0, 0, \ldots)$. Then we can write symbolically

$$x = \sum_{i=0}^{\infty} V^i \{x_i\}.$$

Show that if $x \in W(k)$ and $x_0 \neq 0$ then x is a unit in $W(k)$. *Hint*: One has

$$1 - x\{x_0^{-1}\} = Vy$$

and then

$$x\{x_0^{-1}\} \sum_0^{\infty} (Vy)^i = (1 - Vy) \sum_0^{\infty} (Vy)^i = 1.$$

49. Let n be an integer $\geqq 1$ and p a prime number again. Let k be a field of characteristic p. Let $W_n(k)$ be the ring of truncated Witt vectors $(x_0, \ldots, x_{n-1})$ with components in k. We view $W_n(k)$ as an additive group. If $x \in W_n(k)$, define $\wp(x) = Fx - x$. Then $\wp$ is a homomorphism. If K is a Galois extension of k, and $\sigma \in G(K/k)$, and $x \in W_n(K)$ we can define σx to have component $(\sigma x_0, \ldots, \sigma x_{n-1})$. Prove the analogue of Hilbert's Theorem 90 for Witt vectors, and prove that the first cohomology group is trivial. (One takes a vector whose trace is not 0, and finds a coboundary the same way as in the proof of Theorem 10.1).

50. If $x \in W_n(k)$, show that there exists $\xi \in W_n(\bar{k})$ such that $\wp(\xi) = x$. Do this inductively, solving first for the first component, and then showing that a vector $(0, \alpha_1, \ldots, \alpha_{n-1})$ is in the image of $\wp$ if and only if $(\alpha_1, \ldots, \alpha_{n-1})$ is in the image of $\wp$. Prove inductively that if $\xi, \xi' \in W_n(k')$ for some extension k' of k and if $\wp\xi = \wp\xi'$ then $\xi - \xi'$ is a vector with components in the prime field. Hence the solutions of $\wp\xi = x$ for given $x \in W_n(k)$ all differ by the vectors with components in the prime field, and there are p^n such vectors. We define

$$k(\xi) = k(\xi_0, \ldots, \xi_{n-1}),$$

or symbolically,

$$k(\wp^{-1}x).$$

Prove that it is a Galois extension of k, and show that the cyclic extensions of k, of degree p^n, are precisely those of type $k(\wp^{-1}x)$ with a vector x such that $x_0 \notin \wp k$.

51. Develop the Kummer theory for abelian extensions of k of exponent p^n by using $W_n(k)$. In other words, show that there is a bijection between subgroups B of $W_n(k)$ containing $\wp W_n(k)$ and abelian extensions as above, given by

$$B \mapsto K_B$$

where $K_B = k(\wp^{-1}B)$. All of this is due to Witt, cf. the references at the end of §8, especially [Wi 37]. The proofs are the same, *mutatis mutandis*, as those given for the Kummer theory in the text.

Further Progress and directions

Major progress was made in the 90s concerning some problems mentioned in the chapter. Foremost was Wiles's proof of enough of the Shimura-Taniyama conjecture to imply Fermat's Last Theorem [Wil 95], [TaW 95].

[TaW 95] R. TAYLOR and A. WILES, Ring-theoretic properties or certain Hecke algebras, *Annals of Math.* **141** (1995) pp. 553–572

[Wil 95] A. WILES, Modular elliptic curves and Fermat's last theorem, *Annals. of Math.* **141** (1995) pp. 443–551

Then a proof of the complete Shimura-Taniyama conjecture was given in [BrCDT 01].

[BrCDT 01] C. BREUIL, B. CONRAD, F. DIAMOND, R. TAYLOR, On the modularity of elliptic curves over **Q**: Wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001) pp. 843–839

In a quite different direction, Neukirch started the characterization of number fields by their absolute Galois groups [Ne 68], [Ne 69a], [Ne 69b], and proved it for Galois extensions of **Q**. His results were extended and his subsequent conjectures were proved by Ikeda and Uchida [Ik 77], [Uch 77], [Uch 79], [Uch 81]. These results were extended to finitely generated extensions of **Q** (function fields) by Pop [Pop 94], who has a more extensive bibliography on these and related questions of algebraic geometry. For these references, see the bibliography at the end of the book.