Lectures on the
Algebraic Theory of Fields

By

K.G. Ramanathan

Tata Institute of Fundamental Research, Bombay
1956

Lectures on the
Algebraic Theory of Fields

By

K.G. Ramanathan

Tata Institute of Fundamental Research, Bombay
1954

Introduction

There are notes of course of lectures on Field theory aimed at providing the beginner with an introduction to algebraic extensions, algebraic function fields, formally real fields and valuated fields. These lectures were preceded by an elementary course on group theory, vector spaces and ideal theory of rings—especially of Noetherian rings. A knowledge of these is presupposed in these notes. In addition, we assume a familiarity with the elementary topology of topological groups and of the real and complex number fields.

Most of the material of these notes is to be found in the notes of Artin and the books of Artin, Bourbaki, Pickert and Van-der-Waerden.

My thanks are due to Mr. S. Raghavan for his help in the writing of these notes.

K.G. Ramanathan

Contents

Chapter 1

General extension fields

1 Extensions

A field has characteristic either zero or a prime number p. 1

Let K and k be two fields such that $K \supset k$. We shall say that K is an *extension field* of k and k a *subfield* of K. Any field T such that $K \supset T \supset k$ is called an *intermediary* field, intermediate between K and k.

If K and K' are two fields, then any homomorphism of K into K' is either trivial or it is an isomorphism. This stems from the fact that only ideals in K are (o) and K. Let K have characteristic $p \neq o$. Then the mapping $a \to a^p$ of K into itself is an isomorphism. For,

$$\begin{aligned}(a \pm b)^p &= a^p \pm b^p\\ (ab)^p &= a^p \cdot b^p\end{aligned}$$

and $a^p = b^p \Longrightarrow (a-b)^p = o \Longrightarrow a = b$. In fact for any integer $e \geq 1$, $a \to a^{p^e}$ is also an isomorphism of K into itself.

Let now Z be the ring of rational integers and K a field whose unit element we denote by e. The mapping $m \to$ me of Z into K obviously a homomorphism of the ring Z into K. The kernel of the homomorphism is the set of m is Z such that $me = 0$ in K. This is an ideal in Z and as Z is a principal ideal domain, this ideal is generated by integer say p. Now p is either zero or else is a prime. In the first case it means that K contains

a subring isomorphic to Z and K has characteristic zero. Therefore K contains a subfield isomorphic to the field of rational numbers. In the
2 second case K has characteristic p and since $Z/(p)$ is a finite field of p elements, K contains a subfield isomorphic to $Z/(p)$. Hence the

Theorem 1. *A field of characteristic zero has a subfield isomorphic to the field of rational numbers and a field of characteristic $p > o$ has a subfield isomorphic to the finite of p residue classes of Z modulo p.*

The rational number filed and the finite field of p elements are called *prime fields*. We shall denote them by Γ. When necessary we shall denote the finite field of p elements by Γp.

Let K/k be an extension field of k. We shall identity the elements of K and k and denote the common unit element by 1. Similarly for the zero element. K has over k the structure of a vector space. For, $\alpha, \beta \in K$, $\lambda \in k \Longrightarrow \alpha + \beta \in K$, $\lambda\alpha \in K$. Therefore K δ has over k a base $\{\alpha_\lambda\}$ in the sense that every $\alpha \in K$ can be uniquely written in the form

$$\alpha = \sum_\lambda a_\lambda \alpha_\lambda \quad a_\lambda \in k$$

and $a_\lambda = 0$ for almost all λ. If the base $\{\alpha_\lambda\}$ consists only of a finite number of elements we say that K has a finite base over k. The extension K/k is called a *finite* or *infinite extension* of k according as K has over k a finite or an infinite base. The number of basis elements we call the *degree* of K over k and denote it by $(K : k)$. If $(K : k) = n$ then there exist n elements $\omega, \ldots \omega_n$ in K which are linearly independent over k and every $n + 1$ elements of K linearly dependent over k.

Let K be a finite field of q elements. Obviously K has characteristic $p \neq o$. Therefore K contains a subfield isomorphic to Γ_p. Call it also Γ_p. K is a finite dimensional vector space over Γ_p. Let $(K : \Gamma_p) = n$
3 Then obviously K has p^n elements. Thus

Theorem 2. *The number of elements q in a finite field is a power of the characteristic.*

Let $K \supset T \supset k$ be a tower of fields. K/T has a base $\{\alpha_\lambda\}$ and T/K has a base $\{\beta_\nu\}$. This means that for $\alpha \in K$

$$\alpha = \sum_\lambda t_\lambda \alpha_\lambda$$

$t_\lambda \in T$ and $t_\lambda = 0$ for almost all λ. Also t_λ being in T we have

$$t_\lambda = \sum_\mu a_{\lambda\mu}\beta_\mu$$

$a_{\lambda\mu} = 0$ for almost all μ. Thus

$$\alpha = \sum_{\lambda\mu} a_{\lambda\mu}(\alpha_\lambda\beta_\mu)$$

Thus every element α of K can be expressed linearly in terms of $\{\alpha_\lambda\beta_\mu\}$. On the other hand let

$$\sum_{\lambda\mu}(\alpha_\lambda\beta_\mu) = 0$$

$a_{\lambda\mu} \in k$ and $a_{\lambda\mu} = 0$ for almost all λ, μ. Then

$$0 = \sum_\lambda(\sum_\mu a_{\lambda\mu}\beta_\mu)\alpha_\lambda$$

But $\sum_\mu a_{\lambda\mu}\beta_\mu \in T$ and since the $\{\alpha_\lambda\}$ from a base of K/T we have

$$\sum_\lambda a_{\lambda\mu}\beta_\mu = 0 \text{ for all } \lambda.$$

But $\{\beta_\mu\}$ form a base of T/k so that $a_{\lambda\mu} = 0$ for all λ, μ. We have thus proved that $\{\alpha_\lambda\beta_\mu\}$ is a base of K/k. In particular if $(K : k)$ is finite then $(K : T)$ and $(T : k)$ are finite and

$$(K : k) = (K : T)(T : k)$$

As special cases, $(K : k) = (T : k) \Longrightarrow K = T$ (T is an intermediary field of K and k). $(K : k) = (K : T) \Longrightarrow T = k$.

2 Adjunctions

Let K/k be an extension filed and K_α a family of intermediary extension fields. Then $\bigcap\limits_\alpha K_\alpha$ is again an intermediary field but, in general, $\bigcup\limits_\alpha K_\alpha$ 4 is not a field. We shall define for *any subset* S of K/k the field $k(S)$ is called the *field generated by*S over k. It is trivial to see that

$$k(S) = \bigcap_{T \supset S} T$$

i.e., it is the intersection of all intermediary fields T containing S. $k(S)$ is said to be got from k by *adjunction* of S to k. If S contains a finite number of elements, the adjunction is said to be *finite* otherwise *infinite*. In the former case $k(S)$ is said to be finitely generated over k. If $(K : k) < \infty$ then obviously K is finitely generated over k but the converse is not true.

Obviously $k(S US') = k(S)(S')$ because a rational function of $S US'$ is a rational function of S' over $k(S)$.

Let K/k be an extension field and $\alpha \in K$. Consider the ring $k[x]$ of polynomials in x over k. For any $f(x) \in k[x]$, $f(x)$ is an element of K. Consider the set $\mathscr{G}$ of polynomials $f(x) \in k[x]$ for which $f(\alpha) = o$. $\mathscr{G}$ is obviously a prime ideal. There are now two possibilities, $\mathscr{G} = (0)$, $\mathscr{G} \neq (o)$. In the former case the infinite set of elements $1, \alpha, \alpha^2, \ldots$ are all linearly independent over k. We call such an element α of K, *transcendental* over k. In the second case $\mathscr{G} \neq (o)$ and so $\mathscr{G}$ is a principal ideal generated by an irreducible polynomial $\varphi(x)$. Thus $1, \alpha, \alpha^2, \ldots$ are linearly dependent. We call an element α of this type *algebraic* over k. We make therefore the

Definition. *Let K/k be an extension field. $\alpha \in K$ is said to be algebraic over k if α is root of a non zero polynomial in $k[x]$. Otherwise it is said to be transcendental.*

5 *If α is algebraic, the ideal $\mathscr{G}$ defined above is called the ideal of α over k and the irreducible polynomial $\varphi(x)$ which is a generator of $\mathscr{G}$ is called the irreducible polynomial of α over k. $\varphi(x)$ may be made by multiplying by a suitable element of k. This monic polynomial we shall call the minimum polynomial of α.*

3 Algebraic extensions

Suppose $\alpha \in K$ is algebraic over k and $\varphi(x)$ its minimum polynomial over k. Let $f(x) \in k[x]$ and $f(\alpha) \neq o$. $f(x)$ and $\varphi(x)$ are then coprime and so there exist polynomials $g(x)$, $h(x)$ in $k[x]$ such that

$$f(x)g(x) = 1 + \varphi(x)h(x)$$

which means that $(f(\alpha))^{-1} = g(\alpha) \in k[\alpha]$. Thus $k[\alpha] = k(\alpha)$. On the other hand suppose $\alpha \in K$ such that $k[\alpha] = k(\alpha)$ then there is a $g(\alpha)$ in $k[\alpha]$ such that $\alpha g(\alpha) = 1$ or that α satisfies $xg(x) - 1$ in $k[x]$ so that α is algebraic. Hence

1) *$\alpha \in K$ algebraic over $k \Longleftrightarrow k[\alpha]$ is a field.*

   We now define an extension K/k to be algebraic over k if every of K is algebraic over k. In the contrary case K is said to be transcendental extension of k

   We deduce immediately

2) *K/k algebraic $\Longleftrightarrow$ every ring R with $k \subset R \subset K$ is a field*

   If R is a ring and α in R then $k[\alpha] \subset R$ then $k[\alpha] \subset R$. But α is algebraic so that $\alpha^{-1} \in k[\alpha] \subset R$ so that R is a field. The converse follows from (1).

3) $(K : k) < \infty \Longrightarrow K/k$ *algebraic.*

   For let $(K : k) = n$ then for any for $\alpha \in K$, the $n + 1$ elements $1, \alpha, \alpha^2, \ldots \alpha^n$ are linearly dependant over k so that α is algebraic. 6

   The converse is not true

   Let K/k be an extension field and $\alpha \in K$ algebraic over k. Let $\varphi(x)$ be the minimum polynomial of α over k and let degree of $\varphi(x)$ be n. Then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent over k so that

$$(k(\alpha) : k) \geq n.$$

   On the other hand any β in $k(\alpha)$ is a polynomial in α over k. Let $\beta = b_o + b_1\alpha + \cdots + b_m\alpha^m$. Put $\psi(x) = b_o + b_1 x + \cdots + b_m x^m$.

Then

$$\psi(x) = \varphi(x)h(x) + R(x)$$

where $R(x) = 0$ or deg $R(x) < n$. Hence $\psi(\alpha) = \beta = R(\alpha)$ and so every β cab be expressed linearly in terms of $1, \alpha, \ldots, \alpha^{n-1}$.

Thus

$$\Big(k(\alpha) : k\Big) \leq n.$$

We have hence

4) *If $\alpha \in K$ is algebraic over $K, k(\alpha)/k$ is an algebraic extension of degree equal to the degree of the minimum polynomial of α over k.*

We shall call $\Big(k(\alpha) : k\Big)$ *the degree of α over k*

5) *If α is algebraic over k then for any $L, k \subset L \subset K, \alpha$ is algebraic over L.*

For, the ideal of α over k (which is $\neq (0)$ since α is algebraic) is contained in the ideal of α in $L[X] \supset k[x]$.

Therefore

$$\Big(k(\alpha) : k\Big) \geq (L(\alpha) : L)$$

7 Note that the converse is not true. For let z be transcendental over k and consider the field $k(z)$ of rational functions of z.$\Big(k(z) : k\Big)$ is not finite. But $\Big(k(z) : k(z^2)\Big)$ is finite as z is a root of $x^2 - z^2$ over $k(z^2)$.

6) *If $\alpha_1, \ldots, \alpha_n$ in K are algebraic over k then $k(\alpha_1, \ldots, \alpha_n)$ is algebraic over k.*

For, put $K_o = k$, $K_i = k(\alpha_1, \ldots, \alpha_i)$,

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

Then K_i/K_{i-1} is algebraic and is a finite extension. Now

$$(K_n : k) = \pi_i(K_i : K_{i-1})$$

which is also finite. Hence K_n is algebraic over k.

We deduce immediately

7) *K/T algebraic, T/k algebraic $\Longrightarrow K/k$ algebraic.*

For if $\alpha \in K$, α is a root of $\varphi(x) = X^n + a_1 x^{n+1} + \cdots + a_n$ in $T[x]$. Thus α is algebraic over $k(a_1 \ldots, a_n)$. Hence

$$(k(a_1, a_2, \ldots a_n, \alpha) : k(a_1, a_2, \ldots, a_n)) < \infty.$$
$$(k(a_1, a_2, \ldots, a_n) : k) < \infty$$
$$(k(a_1, a_2, \ldots, a_n, \alpha) : k) < \infty$$

which proves the contention.

If follows that if K/k is any extension, then the set L of elements α of K algebraic over k is a field L which is algebraic over k. L is called the *algebraic closure of k in K*

We shall now show how it is possible to construct algebraic extensions of a field.

If k is a field and $\varphi(x)$ a polynomial in $k[x]$, an element α of an extension field K is said to be *root* of $\varphi(x)$ if $\varphi(\alpha) = o$. It then follows that $\varphi(x)$, has in K at most n roots, n being degree of $\varphi(x)$. 8

Let $f(x)$ be an irreducible polynomial in $k[x]$

The ideal generated by $f(x)$ in $k[x]$ is a maximal ideal since $f(x)$ is irreducible. Therefore the residue class ring K of $k[x]/(f(x))$ is a field. Let σ denote the natural homomorphism of $k[x]$ onto K. σ then maps k onto a subfield of K. We shall identify this subfield with k itself (note that $k[x]$ and $(f(x))$ are vector spaces over k). Let ξ in K be the element into which $\underline{x}$ goes by σ

$$\xi = \sigma x$$

Then $K = k(\xi)$. In the first place $k(\xi) \subset K$. Any element in K is the image, by σ, of an element say $\varphi(x)$ in $k[x]$. But

$$\varphi(x) = h(x) f(x) + \psi(x)$$

So $\varphi(\xi) \in K$ and $\varphi(\xi) = \psi(\xi)$. But $\psi(x)$ above has degree $\leq$ degree of f. Thus

$$k(\xi) \subset K \subset k[\xi] \subset k(\xi)$$

This shows that $K = k(\xi)$ and that $(K : k)$ is equal to the degree of $f(x)$. Also ξ in K satisfies $f(\xi) = o$. We have thus proved that for every irreducible polynomial $f(x)$ in $k[x]$ there exists an extension field in which $f(x)$ has a root.

Let now $g(x)$ be any polynomial in $k[x]$ and $f(x)$ an irreducible factor of $g(x)$ in $k[x]$. Let K be an extension of k in which $f(x)$ has a root ξ. Let in K

$$g(x) = (x - \xi)^{\lambda}\psi(x).$$

Then $\psi(x) \in k[x]$. We again take an irreducible factor of $\psi(x)$ and construct K' in which $\psi(x)$ has a root. After finite number of steps we arrive at a field L which is an extension of k and in which $g(x)$ splits
9 completely into linear factors. Let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of $g(x)$ in L. We call $k(\alpha_1, \ldots, \alpha_n)$ *the splitting field of* $g(x)$ *in* L.

Obviously $(k(\alpha_1, \ldots, \alpha_n) : k) \leq n!$

We have therefore the important

Theorem 3. *If k is a field and $f(x) \in k[x]$ then $f(x)$ has a splitting field K and $(K : k) \leq n!, n$ being degree of $f(x)$.*

It must be noted however that a polynomial might have several splitting fields. For instance if D is the quaternion algebra over the rational number field Γ, generated by $1, i, j, k$ then $\Gamma(i)$, $\Gamma(j)$, $\Gamma(f)$, $\Gamma(k)$ are all splitting fields of $x^2 + 1$ in $\Gamma[x]$. These splitting fields are all distinct.

Suppose k and k' are two fields which are isomorphic by means of an isomorphism σ. Then σ can be extended into an isomorphism $\bar{\sigma}$ of $k[x]$ on $k'[x]$ by the following prescription

$$\bar{\sigma}(\sum a_i x^i) = \sum(\sigma a_i)x^i \quad a_i \in k \quad \sigma a_i \in k'$$

Let now $f(x)$ be a polynomial in $k[x]$ which is irreducible. Denote by $f^{\bar{\sigma}}(x)$, its image in $k'[x]$ by means of the isomorphism $\bar{\sigma}$. Then $f^{\bar{\sigma}}(x)$ is again irreducible in $k'[x]$; for if not one can by means of $\bar{\sigma}^{-1}$ obtain a nontrivial factorization of $f(x)$ in $k[x]$.

Let now α be a root of $f(x)$ over k and β a root of $f^{\bar{\sigma}}(x)$ over k'. Then

$$k(\alpha) \simeq k[x]/(f(x)), k'(\beta) \simeq k'[x]/(f^{\bar{\sigma}}(x))$$

Let τ be the natural homomorphism of $k'[x]$ on $k'[x]/(f^{\overline{\sigma}}(x))$. Consider the mapping $\tau \cdot \overline{\sigma}$ on $k[x]$. Since $\overline{\sigma}$ is an isomorphism, it follows that $\tau \cdot \overline{\sigma}$ is a homomorphism of $k[x]$ on $k'[x]/(F^{\overline{\sigma}}(x))$. The kernel of the homomorphism is the set of $\varphi(x)$ in $k[x]$ such that

$$\varphi^{\overline{\sigma}}(x) \in \left(f^{\overline{\sigma}}(x)\right).$$

10

This set is precisely $(f(x))$. Thus

$$k[x]/(f(x)) \simeq k'[x]/(f^{\bar{\sigma}}(x))$$

By our identification, the above fields contain k and k' respectively as subfields so that there is an isomorphism μ of $k(\alpha)$ on $k'(\beta)$ and the restriction of μ to k is σ.

In particular if $k = k'$, then $k(\alpha)$ and $k(\beta)$ are $k-$ isomorphic i.e., they are isomorphic by means of an isomorphism which is identity on k. We have therefore

Theorem 4. *If $f(x) \in k[x]$ is irreducible and α and β are two roots of it (either in the same extension field of k or in different extension fields), $k(\alpha)$ and $k(\beta)$ are $k-$ isomorphic.*

Note that the above theorem is false if $f(x)$ is not irreducible in $k[x]$.

4 Algebraic Closure

We have proved that every polynomial over k has a splitting field. For a given polynomial this field might very well coincide with k itself. Suppose k has the property that every polynomial in k has a root in k. Then it follows that the only irreducible polynomials over k are linear polynomials. We make now the

Definition. *A field Ω is algebraically closed if the only irreducible polynomials in $\Omega[x]$ are linear polynomials.*

We had already defined the algebraic closure of a field k contained in a field K. Let us now make the

Definition. *A field Ω/k is said to be an algebraic closure of k if*

1) Ω *is algebraically closed*

2) Ω/k *is algebraic.* 11

We now prove the important

Theorem 5. *Every field k admits, upto k-isomorphism, one and only one algebraic closure.*

Proof. 1) *Existence.* Let M be the family of algebraic extensions K_α of k. Partially order M by inclusion. Let $\{K_\alpha\}$ be a totally ordered subfamily of M. Put $K = \bigcup\limits_{\alpha} K_\alpha$ for K_α in this totally ordered family. Now K is a field; for $\beta_1 \in K, \beta_2 \in K$ means $\beta_1 \in K_\alpha$ for some α and $\beta_2 \in K_\beta$ for some β. Therefore β_1, β_2 in K_α or K_β whichever is larger so that $\beta_1 + \beta_2 \in K$. Similarly $\beta_1\beta_2^{-1} \in K$. Now K/k is algebraic since every $\lambda \in K$ is in some K_α and so algebraic over k. Thus $K \in M$ and so we can apply Zorn's lemma. This proves that M has a maximal element $\Omega.\Omega$ is algebraically closed; for if not let $f(x)$ be an irreducible polynomial in $\Omega[x]$ and ρ a root of $f(x)$ in an extension $\Omega(\rho)$ of Ω. Then since Ω/k is algebraic. $\Omega(\rho)$ is an element of M. This contradicts maximality of Ω. Thus Ω is an algebraic closure of k.

2) *Uniqueness*. Let k and k' be two fields which are isomorphic by means of an isomorphism σ. Consider the family M of triplets $\{(K, K', \sigma)_\alpha\}$ with the property 1) K_α is an algebraic extension of k, K'_α of k', 2) σ_α is an isomorphism of K_α on K'_α extending σ. By theorem 4, M is not empty. We partially order M in the following manner

□

$$(K, K', \sigma)_\alpha < (K, K', \sigma)_\beta$$

If 1) $K_\alpha \subset K_\beta, K'_\alpha \subset K'_\beta$, 2) σ_β is an extension of σ_α. Let $\{K, K', \sigma)_\alpha\}$ be a simply ordered subfamily. Put $K = \bigcup\limits_{\alpha} K_\alpha, K' = \bigcup\limits_{\alpha} K'_\alpha$,

These are then algebraic over k and k' respectively.

12 Define $\bar{\sigma}$ on K by

$$\bar{\sigma}x = \sigma_\alpha x$$

where $x \in K_\alpha$. (Note that every $x \in K$ is in some K_α in the simply ordered subfamily). It is easy to see that $\bar{\sigma}$ is well - defined. Suppose $x \in K_\beta$ and $K_\beta \subset K_\alpha$ then σ_α is an extension of σ_ρ and so $\sigma_\alpha x = \sigma_\beta x$. This proves that $\bar{\sigma}$ is an isomorphism of K on K' and extends σ. Thus the triplet $(K, K', \bar{\sigma})$ is in M and is an upper bound of the subfamily. By Zorn's lemma there exists a maximal triplet (Ω, Ω', τ). We assert that Ω is algebraically closed; for if not let ρ be a root of an irreducible polynomial $f(x) \in \Omega[x]$. Then $f^{\zeta}(x) \in \Omega'[x]$ is also irreducible. Let ρ' be a root of $f^{\tau}(x)$. Then τ can be extended to an isomorphism $\bar{\tau}$ of $\Omega(\rho)$ on $\Omega'(\rho)$. Now $(\Omega(\rho), \bar{\tau}$ is in M and hence leads to a contradiction. Thus Ω is an algebraic closure of k, Ω' of k' and τ an isomorphism of Ω on Ω' extending σ.

In particular if $k = k'$ and σ the identity isomorphism, then Ω and Ω' are two algebraic closures of k and τ is then a k-isomorphism.

Out theorem is completely demonstrated.

Let $f(X)$ be a polynomial in $k[x]$ and $K = k(\alpha_1, \ldots, \alpha_n$, a splitting field of $f(x)$, so that $\alpha_1, \ldots, \alpha_n$ are the distinct roots of $f(x)$ in K. Let K' be any other splitting field and $\beta_1, \ldots \beta_m$ the distinct roots of $f(x)$ in K'. Let Ω be an algebraic closure of K and Ω' of K'. Then Ω and Ω' are two algebraic closures of k. There exists therefore an isomorphism σ of Ω on Ω' which is identity on k. Let $\sigma K = K_1$. Then $K_1 = k(\sigma_{\alpha_1}, \ldots, \sigma_{\alpha_n})$. Since $\alpha_1, \ldots \alpha_n$ are distinct $\sigma\alpha_1 \ldots, \sigma\alpha_n$ are distinct and are roots of $f(x)$. Thus K_1 is a splitting field of $f(x)$ in Ω'. This proves that 13

$$K' = K_1.$$

$\beta_1, \ldots, \beta_m$ are distinct and are roots of $f(x)$ in Ω'. We have $m = n$ and $\beta_i = \sigma\alpha_2$ in some order. Therefore the restriction of σ to K is an isomorphism of K on K'. We have

Theorem 6. *Any two splitting fields K, K' of a polynomial $f(x)$ in $k[x]$ are $k-$ isomorphic.*

Let K be a finite field of q elements. Then $q = P^n$ where n is an integer ≥ 1 and p is the characteristic of K. Also $n = (K : \Gamma)$, Γ being the prime field. Let K^* denote the abelian group of non-zero elements of K. Then K^* being a finite group of order $q-1$,

$$\alpha^{q-1} = 1$$

for all $\alpha \in K^*$. Thus K is the splitting field of the polynomial

$$x^q - x$$

in $\Gamma[x]$. It therefore follows

Theorem 7. *Any two finite fields with the same number of elements are isomorphic.*

A finite field cannot be algebraically closed; for if K is a finite field of q elements and $\underline{a} \in K^*$ the polynomial

$$f(x) = x \prod_{b \in K^*} (X - b) + a$$

is in $K[x]$ and has no root in K.

5 Transcendental extensions

We had already defined a transcendental extension as one which contains at least on transcendental element.

Let K/k be a transcendental extension and $Z_1, \ldots, Z_n$ any n elements of K. Consider the ring $R = k[x_1, \ldots x_n]$ of polynomials over k in n
14 variables. Let $\mathscr{Y}$ be the subset of R consisting of those polynomials $f(x_1, \ldots x_n)$ for which

$$f(Z_1, \ldots Z_n) = 0.$$

$\mathscr{Y}$ is obviously an ideal of R. If $\mathscr{Y} = (o)$ we say that $Z_1, \ldots Z_n$ are *algebraically independent* over k. If $\mathscr{Y} \neq (o)$, they are said to be algebraically dependent. Any element of K which is algebraic over $k(Z_1, \ldots, Z_n)$ is therefore algebraically dependent on $Z_1, \ldots Z_n$.

We now define a subset S of K to be algebraically independent over k if every finite subset of S is algebraically independent over k. If K/k is transcendental there is at least one such non empty set S.

Let K/k be a transcendental extension and let S, S' be two subset of K with the properties

i) S algebraically independent over k

ii) S' algebraically independent over $k(s)$

Then S and S' are disjoint subsets of K and SUS' are algebraically independent over k. That S and S' are disjoint is trivially seen. Let now $Z_1, \ldots Z_m \in S$ and $Z'_1, \ldots Z'_n \in S'$ be algebraically dependent. This will mean that there is a polynomial f,

$$f = f(x_1, \ldots, x_{m+n})$$

in $m + n$ variables with coefficients in k, such that

$$f(Z_1, \ldots, Z_m, Z'_1, \ldots Z'_n) = 0.$$

Now f can be regarded as a polynomial in $x_{m+1}, \ldots, x_{m+n}$ with coefficients in $k(x_1, \ldots, x_m)$. If all these coefficients are zero then $Z_1, \ldots Z_m$, $Z'_1, \ldots Z'_n$ are algebraically independent over k. If some coefficient is $\neq 0$, then $f(Z_1, \ldots Z_m,\ x_{m+1}, \ldots, x_{m+n})$ is a non zero polynomial over $k(S)$ which vanishes for $x_{m+1} = Z'_1, \ldots x_{m+n} = Z'_n$ which contradicts the fact that S' is algebraically independent over $k(S)$. Thus $f = o$ identically and our contention is proved. **15**

The converse of the above statement is easily proved.

An extension field K/k is said to be generated by a subset M of K if $K/k(M)$ is algebraic. Obviously K itself is a set of generators. A subset B of K is said to be a *transcendence base* of K if

1) B is a set of generators of K/k

2) B algebraically independent over k.

If K/k is transcendental, then, it contains algebraically independent elements. We shall prove that K has a transcendence base. Actually much more can be proved as in

Theorem 8. *Let K/k be a transcendental extension generated by S and A a set of algebraically independent elements contained in S. Then there is a transcendence base B of K with*

$$A \subset B \subset S$$

Proof. Since S is a set of generators of K, $K/k(S)$ is algebraic. Let M be the family of subsets A_α of K with

1) $A \subset A_\alpha \subset S$

2) A_α algebraically independent over k.

□

The set M is not empty since A is in M. Partially order M by inclusion. Let $\{A_\alpha\}$ be a totally ordered subfamily. Put $B_0 = \bigcup\limits_\alpha A_\alpha$. Then $B_o \subset S$. Any finite subset of B_o will be in some A_α for large α and so B_o satisfies 2) also. Thus using Zorn's lemma there exists a maximal element B in M. Every element x of S depends algebraically on B for otherwise BUx will be in M and will be larger than B. Thus $k(S)/k(B)$ is algebraic. Since $K/k(S)$ is algebraic, it follows that B satisfies the conditions of the theorem.

16 The importance of the theorem is two fold; firstly that every set of elements algebraically independent can be completed into a transcendence base of K and further more every set of generators contains a base.

We make the following simple observation. Let K/k be an extension, $Z_1, \ldots Z_m, m$ elements of K which have the property that $K/k(Z_1, \ldots Z_m)$ is algebraic, i.e., that $Z_1, \ldots, Z_m$ is a set of generators. If $Z \in K$ then Z depends algebraically on $Z_1, \ldots, Z_m$ i.e., $k(Z, Z_1, \ldots, Z_m)/k(Z_1, \ldots, Z_m)$ is algebraic. We may also remark that if in the algebraic relation connecting $Z, Z_1, \ldots Z_m, Z_1$ occurs then we can say that

$$k(Z, Z_1, \ldots Z_m)/k(Z, Z_2, \ldots, Z_m)$$

is algebraic which means that $Z, Z_2, \ldots Z_m$ is again a set of generators.

We now prove the

Theorem 9. *If K/k has a transcendence base consisting of a finite number n of elements, every transcendence base has n elements.*

Proof. Let $Z_1, \ldots, Z_n$ and $Z'_1, \ldots, Z'_m$ be two transcendence bases consisting of n and m elements respectively. If $n \neq m$ let $n < m$. Now $K/k(Z_1, \ldots, Z_n)$ is algebraic. Z'_1 is transcendental over k and depends algebraically on $Z_1, \ldots, Z_n$ so that if Z_1 appears in the algebraic relation, by the remark above, $Z'_1, Z_2, \ldots, Z_n$ is again a set of generators, Z'_2 depends algebraically on $Z'_1, \ldots, Z_n$. In this algebraic relation at least one of $Z_2, \ldots, Z_n$ has to appear since Z'_1, Z'_2, are algebraically independent. If Z_2 appears then $Z'_2, Z'_1, Z_3, \ldots, Z'_n$ is a set of generators. We repeat this process n times, and find, that $Z'_1, Z'_2, Z'_3, \ldots, Z'_n$ is a set of generators which means that $Z'_{n+1}, \ldots, Z'_m$ depend algebraically on $Z'_1, \ldots, Z'_n$. This 17 is a contradiction. So $n \geq m$. We interchange n and m and repeat the argument and get $n \leq m$. This proves that $n = m$.

The unique integer $\underline{n}$ will be called the *dimension* of K/k.

$$n = \dim_k K$$

□

It is also called the *transcendence degree*.

A similar theorem is true even if K has infinite transcendence base but we don't prove it.

Let $k \subset L \subset K$ be a tower of extensions and let B_1 be a transcendence base of L/k and B_2 that over K/L. We assert that $B_1 U B_2$ is a transcendence base of K/k. In the first place $B_1 U B_2$ is algebraically independent over k. Now $k(B_1 U B_2)$ is a subfield of $L(B_2)$. Every element in $L(B_2)$ is a ratio of two polynomials in B_2 with coefficients in L. The elements of L are algebraic over $K(B_1)$. Thus $L(B_2)$ is algebraic over $k(B_1 U B_2)$. But $K/L(B_2)$ is algebraic. Thus $K/k(B_1 U B_2)$ is algebraic. This proves our assertion. In particular it proves

Theorem 10. *If $k \subset L \subset K$ then*

$$\dim_k K = \dim_k L + \dim_L K.$$

A transcendental extension K/k is said to be *purely transcendental* if there exists a base B with $K = k(B)$. Note that this does not mean that every base has this property. For instance if $k(x)$ is the field of rational functions of x then x^2 is also transcendental over x but $k(x^2)$ is a proper subfield of $k(x)$.

Let $K = k(x_1, \ldots x_n)$ and $K' = k(x'_1, \ldots x'_n)$ be two purely transcendental
18 extensions of dimension n. Consider the homomorphism σ defined by

$$\sigma f(x_1, \ldots x_n) = f(x'_1, \ldots, x'_n)$$

Where $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$. It is then easy to see that this is an isomorphism of K on K'. This proves

Theorem 11. *Two purely transcendental extensions of the same dimension n over k k-isomorphic.*

This theorem is true even if the dimension is infinite.

Chapter 2

Algebraic extension fields

1 Conjugate elements

Let Ω be an algebraic closure of k and K an intermediary field. Let Ω' **19** be an algebraic closure of K and so of k. Then there is an isomorphism τ of Ω' on Ω which is trivial on k. The restriction of this isomorphism to K gives a field τK in Ω which is k-isomorphic to K. Conversely suppose K and K' are two subfields of Ω which are k-isomorphic. Since Ω is a common algebraic closure of K and K', there exists an automorphism of Ω which extends the k-isomorphism of K and K'. Thus

1) *Two subfields K, K' of Ω/k are k-isomorphic if and only if there exists a k-automorphism σ of Ω such that $\sigma K = K'$.*

   We call two such fields K and K' *conjugate fields over k.*

   We define two elements ω, ω' of Ω/k, to be *conjugate* over k if there exists a k-automorphism σ of Ω such that

$$\sigma\omega = \omega'$$

   The automorphisms of Ω which are trivial on k form a group and so the above relation of conjugacy is an equivalence relation. We can therefore put elements of Ω into classes of conjugate elements over k. We then have

2) *Each class of conjugate elements over k contains only a finite number of elements.*

20 *Proof.* Let C be a class of conjugate elements and $\omega \in C$. Let $f(x)$ be the minimum polynomial of ω in $k[x]$. Let σ be an automorphism of Ω/k. Then $\sigma\omega \in C$. But $\sigma\omega$ is a root of $f^{\sigma}(x) = f(x)$. Also if $\omega' \in C$ then $\omega' = \sigma\omega$ for some automorphism σ of Ω/k. In that case $\sigma\omega = \omega'$ is again a root of $f(x)$. Thus the elements in C are all roots of the irreducible polynomial $f(x)$. Our contention follows. □

Notice that if α, β are any two roots, lying in Ω, of the irreducible polynomial $f(x)$, then $k(\alpha)$ and $k(\beta)$ are k-isomorphic. This isomorphism can be extended into an automorphism of Ω. Thus

Theorem 1. *To each class of conjugate elements of Ω there is associated an irreducible polynomial in $k[x]$ whose distinct roots are all the elements of this class.*

If $\alpha \in \Omega$ we shall denote by C_α the class of α. C_α is a finite set.

2 Normal extensions

Suppose K is a subfield of Ω/k and σ an automorphism of Ω/k. Let $\sigma K \subset K$. We assert that $\sigma K = K$. For let $\alpha \in K$ and denote by $\overline{C}_\alpha$ the set

$$C_\alpha \cap K$$

Since $\sigma K \subset K$ we have $\sigma\alpha \in K$ so $\sigma\alpha \in \overline{C}_\alpha$. Thus

$$\sigma\overline{C}_\alpha \subset_\alpha$$

$\overline{C}_\alpha$ is a finite set and σ is an isomorphism of K into itself.

Thus

$$\sigma\overline{C}_\alpha = \overline{C}_\alpha$$

21 which means $\alpha \in \sigma K$. Thus $K = \sigma K$.

We shall now study a class of fields $K \subset \Omega/k$ which have the property

$$\sigma K \subset K,$$

for all automorphisms σ of Ω/k. We shall call such fields, *normal extensions* of k in Ω.

Let K/k be a normal extension of k and Ω algebraic closure of k containing K. Let $\alpha \in K$ and C_α the class of α. We assert that $C_\alpha \subset K$. For if β is an element of C_α, there is an automorphism σ of Ω/k for which $\beta = \sigma\alpha$. Since $\sigma K \subset K$, it follows that $\beta \in K$. Now any element α in K is a root of an irreducible polynomial in $k[x]$. Since all the elements of C_α are roots of this polynomial, it follows that if $f(x)$ is an irreducible polynomial with one root in K, then all roots of $f(x)$ lie in K.

Conversely let K be a subfield of Ω/k with this property. Let σ be an automorphism of Ω/k and α/K. Let σ be an automorphism of Ω/k and $\alpha \in K$. Let C_α be the class of α. Since $C_\alpha \subset K, \sigma\alpha \in K$. But α is arbitrary in K. Therefore

$$\sigma K \subset K$$

and K is normal. Thus the

Theorem 2. *Let $k \subset K \subset \Omega$. Then $\sigma K = K$ for all automorphisms σ of $\Omega/k \Longleftrightarrow$ every irreducible polynomial $f(x) \in k[x]$ which has one root in K has all roots in K.*

Let $f(x)$ be a polynomial in $k[x]$ and K its splitting field. Let Ω be an algebraic closure of K. Let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of $f(x)$ in 22
Ω. Then

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

Let σ be an automorphism of Ω/k. $\sigma\alpha_j = \alpha_j$ for some j. Thus σ takes the set $\alpha_1, \ldots, \alpha_n$ onto itself. Since every element of K is a rational function of $\alpha_1, \ldots, \alpha_n$, it follows that $\sigma K \subset K$. Thus

i) *The splitting field of a polynomial in $k[x]$ is a normal extension of* k.

Let $\{K_\alpha\}$ be a family of normal subfields of Ω/k. Then $\bigcap\limits_\alpha K_\alpha$ is trivially normal. Consider $k(\bigcup\limits_\alpha K_\alpha)$. This again is normal since for any automorphism σ of Ω/k.

$$\sigma k\left(\bigcup_\alpha K_\alpha\right) \subset k\left(\bigcup_\alpha \sigma K_\alpha\right) \subset k\left(\bigcup_\alpha K_\alpha\right)$$

Let now $\{f_\alpha(x)\}$ be a set of polynomials in $k[x]$ and K_α their splitting fields, then $K(\bigcup\limits_\alpha K_\alpha)$ is normal. Also it is easy to see that

$$L = k\left(\bigcup_\alpha K_\alpha\right)$$

is the intersection of all subfields of Ω/k in which every one of the polynomials $f_\alpha(x)$ splits completely. Thus

ii) *if $\{f_\alpha(x)\}$ is a set of polynomials in $k[x]$, the subfield of Ω generated by all the roots of $\{f_\alpha(x)\}$ is normal.*

We also have

iii) *If K/k is normal and $k \subset L \subset K$ then K/L is also normal.*

23 For if σ is an L- automorphism of Ω, then σ is also a k-automorphism of Ω and so $\sigma K \subset K$.

The $k-$automorphisms of Ω form a group $G(\Omega/k)$. From what we have seen above, it follows that a subfield K of Ω/k is normal if and only if $\sigma K = K$ for every $\sigma \in G(\Omega/k)$. Now a $k-$ automorphism of K can be be extended into an automorphism of Ω/k, because every such automorphism is an isomorphism of K in Ω. It therefore follows

iv) *K/k is normal if and only if every isomorphism of K in Ω/k is an automorphism of K over k.*

As an example, let Γ be the field of rational numbers and $f(x) = x^3 - 2$. Then $f(x)$ is irreducible in $\Gamma[x]$. Let $\alpha = \sqrt[3]{2}$ be one of its roots. $\Gamma(\alpha)$ is of degree 3 over Γ and is not normal since it does not contain ρ where $\rho = \frac{-1+\sqrt{-3}}{2}$. However the field $\Gamma(\alpha, \rho)$ of degree 6 over Γ is normal and is the splitting field of $x^3 - 2$.

If K is the field of complex numbers, consider $K(z)$ the field of rational function of 2 over K. Consider the polynomial $x^3 - z$ in $K(z)[x]$. This is irreducible. Let $\omega = z^{\frac{1}{3}}$ be a root of this polynomial. Then $K(z)(\omega)$ is of degree 3 $K(z)$ and is the splitting field of the polynomial $x^3 - z$.

3 Isomorphisms of fields

Let K/k be an algebraic extension of k and W *any* extension of K and so of k. A mapping σ of K into W is said to be $k-$ *linear* if for $\alpha, \beta \in K$ 24

$$\sigma(\alpha+\beta) = \sigma\alpha + \sigma\beta$$

$\sigma\alpha \in W$ and if $\lambda \in k, \sigma(\lambda\alpha) = \lambda\sigma\alpha$. If σ is a $k-$linear map of K into W we define $\alpha\sigma$ for α in W by

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

for $\beta \in K$. This again is a $k-$linear map and so the $k-$linear maps of K into W form a vector space V over W.

A $k-$isomorphism σ of K into W is obviously a $k-$linear map and so $\sigma \in V$. We shall say, two isomorphisms σ, τ of K into W (trivial on k) are *distinct* if there exists at least one $\omega \in K, \omega \neq 0$ such that

$$\sigma\omega \neq \tau\omega$$

Let S be the set of mutually distinct isomorphisms of K into W. We then have

Theorem 3. *S is a set of linearly independent elements of V over W.*

Proof. We have naturally to show that every finite subset of S is linearly independent over W. Let on the contrary $\sigma_1, \ldots, \sigma_n$ be a finite subset of S satisfying a non trivial linear relation

$$\sum_i \alpha_i\sigma_i = 0$$

$\alpha_i \in W$. We may clearly assume that no proper subset of $\sigma_1, \ldots, \sigma_n$ is linearly dependent. Then in the above expression all α_i are different from zero. Let ω be any element of K. Then

$$\sum_i \alpha_i\sigma_i\omega = 0$$

□

If we replace ω by $\omega\omega'$ we get, since $\sigma_i{}'s$ are isomorphisms, 25

$$\sum_i \alpha_i \sigma_i \omega' . \sigma_i \omega = o$$

for every $\omega \in K$. This means that $\sigma_i, \ldots, \sigma_n$ satisfy another linear relation

$$\sum_i \alpha_i \sigma_i \omega' . \sigma_i \omega = o$$

Since the isomorphisms are mutually distinct, we can choose ω' in K in such a way that

$$\sigma_1 \omega' \neq \sigma_n \omega'$$

We then get from the two linear relations, the expression

$$\sum_{i=1}^{n-1} \left(\frac{\alpha_i}{\alpha n} - \frac{\sigma_i \omega' \alpha_i}{\sigma_n \omega' \alpha_i} \right) \sigma_i = o.$$

This relation is non trivial since the coefficient of σ_1 is different from zero. This leads to a contradiction and our theorem is proved.

Suppose $\dim V < \infty$ then it would mean that S is a finite set. But the converse is false. We have however the

Theorem 4. *If $(K : k) < \infty$, then dim $V = (K : k)$*

Proof. Let $(K : k) = n$ and $\omega_1, \ldots, \omega_n$ a basis of K/k. □

Consider the k-linear mappings $\sigma_1, \ldots, \sigma_n$ defined by

$$\begin{cases} \sigma_i(\omega_j) & = o \qquad i \neq j \\ & = 1 \qquad i \neq j \end{cases}$$

Then $\sigma_1, \ldots, \sigma_n$ are linearly independent elements of V over W. For, let $\sum_i \alpha_i \sigma_i = o$, $\alpha_i \in W$. Then

$$\left(\sum_i \alpha_i \sigma_i \right) \omega_i = o$$

26 for $j = 1, \ldots, n$. This proves that $\alpha_j = o$. Now let σ be any k-linear

mapping. It is uniquely determined by its effects on $\omega_1, \ldots, \omega_n$. Put $\alpha_i = \sigma\omega_i$ and let τ be given by

$$\tau = \sigma - \sum_i \alpha_i \sigma_i$$

Then $\tau(\omega_j) = \sigma\omega_j \sum_i \alpha_i \sigma_i(\omega_j) = o$ so that $\tau = o$. Our contention is established.

From this we obtain the very important

Corollary. *If $(K : k) < \infty$ then K has in Ω/k at most $(K : k)$ distinct k-isomorphisms.*

Let $\alpha \in \Omega$. Consider the field $k(\alpha)/k$. Let $\alpha^{(1)}(= \alpha), \ldots, \alpha^{(n)}$ be the distinct conjugates of α over k. An isomorphism σ of $k(\alpha)/k$ is determined completely by its effect on α. Since every isomorphism comes from an automorphism of Ω/k, it follows that $k(\alpha^{(i)})$ are all the distinct isomorphic images of $k(\alpha)$. Thus

1) *Number of distinct k-isomorphisms of $k(\alpha)$ in Ω is equal to the number of distinct roots in Ω of the minimum polynomial of α.*

Let K/k be an algebraic extension and Ω an algebraic closure of k containing K. Let K have the property that K/k has only finitely many distinct k-isomorphisms in Ω. Let $K^{(1)}(= K), K^{(2)}, \ldots, K^{(n)}$ be the distinct isomorphic fields. Let $\alpha \in \Omega$ and let α have over K exactly m distinct conjugates $\alpha^{(1)}(= \alpha), \ldots, \alpha^{(m)}$. This means that if $f(x)$ is the minimum polynomial of α over K, then $f(x)$ has in Ω, m distinct roots. We claim that $K(\alpha)$ has over k exactly mn distinct isomorphisms in Ω. **27**

For, let $\sigma_i (i = 1, \ldots, n)$ be the k-isomorphisms defined by

$$\sigma_i K^{(1)} = K^{(i)}$$

Let $f^{\sigma_i}(x)$ be the image of the polynomial $f(x)$ in $K[x]$ by means of the above isomorphism. Let the roots of $f^{\sigma_i}(x)$ by $\alpha^{(i_1)}, \ldots, \alpha^{(i_n)}$ these being the distinct ones. There exists then an isomorphism $\sigma_{ij}(j = 1, \ldots, m)$ extending σ_i of $K^{(1)}(\alpha^{(1)})$ on $K^{(i)}(\alpha^{(ij)})$. Since i has n values, it follows that there are at least mn distinct isomorphisms of $K(\alpha)$ over k.

Let now σ be any automorphism of Ω/k. Let $\sigma K = K^{(i)}$. Then it takes $\alpha^{(1)}$ into a root $\alpha^{(ij)}$ of $f^{\sigma}(x) = f^{\sigma_i}(x)$ where σ_i is the isomorphism which coincides with σ on K. Thus since every isomorphism of $K(\alpha)$ over k comes from an automorphism of Ω/k, our contention is established.

Let now $K = k(\omega_1, \ldots, \omega_n)$ and $K_i = k(\omega_1, \ldots, \omega_i)$ so that $K_o = k$ and $K_n = K$. Let K_i have over K_{i-1} exactly P_i distinct K_{i-1}-isomorphisms. Then K/k has exactly $p_1 \cdots p_n$ distinct k-isomorphisms in Ω. Hence

2) *If $K \supset L \supset k$ be a tower of finite extensions and K has ever L, n distinct L-isomorphisms in Ω and L has over k, m distinct k-isomorphisms then K has over k precisely mn distinct k-isomorphisms.*

28 In particular let $(K : k) < \infty$ and let K have in Ω exactly $(K : k)$ distinct isomorphisms. Let L be any intermediary field. Let $\underline{a}$ be the number of distinct L-isomorphisms of K and $\underline{b}$ the number of distinct k-isomorphisms of L.

Then

$$(K : k) = ab \leq (K : L)(L : k) = (K : k)$$

But $a \leq (K : L), b \leq (L : k)$. Thus $a = (K : L)$ and $b = (L : k)$.

4 Separability

Let Ω be an algebraic closure of k and $\omega \in \Omega$. Let $\phi(x)$ be the minimum polynomial of ω in k. Suppose $k(\omega)/k$ has exactly $(k(\omega) : k)$ distinct k-isomorphisms in Ω. Then from the last article it follows that all the roots of $\phi(x)$ are distinct. Conversely let the irreducible polynomial $\phi(x)$ be of degree n and all its n roots distinct. Then $k(\omega)/k$ has n distinct k-isomorphisms ω being a root of $\phi(x)$. But it can have no more.

Let us therefore make the

Definition. *An element $\omega \in \Omega$ is said to be separably algebraic or separable over k if its minimum polynomial has all roots distinct. Otherwise it is said to be inseparable.*

1) *Let W/k be any extension field and $\omega \in W$ separable over k. Let L be an intermediary field. Then ω is separable over L.*

For, the minimum polynomial of ω over L divides that over k.

2) *$\omega \in \Omega$ separable over $k \Leftrightarrow k(\omega)/k$ has in $\Omega(k(\omega) : k)$ distinct k-isomorphisms.* 29

Let now $K = k(\omega_1, \ldots, \omega_n)$ and let $\omega_1, \ldots \omega_n$ be all separable over k. Put $K_i = k(\omega_1, \ldots, \omega)$ so that $K_o = k$ and $K_n = K$. Now $K_{i-1}(\omega_i)$ and ω_i is separable over K_{i-1} so that K_i over K_{i-1} has exactly $(K_i : K_{i-1})$ distinct K_{i-1}- isomorphisms. This proves that K has over k

$$(K_n : K_{n-1}) \ldots (K_1 : K_o) = (K_n : K_o) = (K : k)$$

distinct k-isomorphisms. If therefore $\omega \in K$, Then by previous article $k(\omega)$ has exactly $(k(\omega) : k)$ distinct isomorphisms and hence ω is separable over k. Conversely if K/k is finite and every element of K is separable over k, then K/k has exactly $(K : k)$ distinct k-isomorphisms. Hence

3) *$(K : k) < \infty$, K/k has $(K : k)$ distinct k-isomorphisms $\Leftrightarrow$ every element of K is separable over k.*

Let us now make the

Definition. *A subfield K of Ω/k is said to be separable over k if every element of K is separable over k.*

From 3) and the definition, it follows that

4) *K/k is separable $\Leftrightarrow$ for every subfield L of K with $(L : K) < \infty, L$ has exactly $(L : K)$ distinct isomorphisms over k.*

5) $K/L, L/k$ separably algebraic $\Leftrightarrow K/k$ separable.

For, let $\omega \in K$. Then ω is separable over L. Let $\omega_1, \ldots, \omega_n$ be the coefficients in the irreducible polynomial satisfied by ω over L. 30
Then ω has over $K_1 = k(\omega_1, \ldots, \omega_n)$ exactly $(K_1(\omega) : K_1)$ distinct K_1-isomorphisms. Also K_1/k is finite separable. Thus $K_1(\omega)$ has over k exactly $(K_1(\omega) : k)$ distinct isomorphisms which proves that ω is separable over k. The converse follows from 2).

6) *If $\{K_\alpha\}$ is a family of separable subfields of Ω then*

2) $\bigcap\limits_{\alpha} K_\alpha$ *and* $b)k(\bigcup\limits_{\alpha} K_\alpha)$ *are separable.*

a) follows easily because every element of K_α is separable over k. b) follows since every element of $k(\bigcup\limits_{\alpha} K_\alpha)$ is a rational function of a finite number of elements and as each of these is separable the result follows from 3).

7) *Let K/k* be any extension-not necessarily algebraic. *The set L of elements of k separably algebraic over K is a field.*

This is evident. We call L the *separable closure* of k in K.

We had already defined an algebraic element ω to be inseparable if its minimum polynomial has repeated roots. Let us study the nature of irreducible polynomials.

Let $f(x) = a_o + a_1 x + \cdots + a_n x^n$ be an irreducible polynomial in $k[x]$. If it has a root $\omega \in \Omega$ which is repeated, then ω is a root of

$$f^1(x) = a_1 + 2a_2 x + \cdots + na_n x^{n-1}.$$

Thus $f(x)|f^1(x)$ which can happen only if

$$ia_i = o, i = 1, \ldots, n.$$

31 Let k have characteristic zero. Then $ia_i = o \Rightarrow a_i = 0$ that is $f(x)$ is a constant polynomial. Thus

8) *Over a field of characteristic zero, every non constant irreducible polynomial has all roots distinct.*

Let now k have characteristic $p \neq o$. if $p\chi i$ then $ia_i = o \Rightarrow a_i = o$. Thus for $f^1(x)$ to be identically zero we must have $a_i = o$ for $p\chi i$. In this case

$$f(x) = a_o + a_p x^p + \cdots$$

or that $f(x) \in k[x^p]$. Let e be the largest integer such that $f(x) \in k[x^p]$ but not in $k[x^{p^{e+1}}]$. Consider the polynomial $\phi(y)$ with $\phi(x^{p^e}) =$

$f(x)$. Then $\phi(y)$ is irreducible in $k[y]$ and $\phi(y)$ has *no repeated roots*. Let $\beta_1, \ldots, \beta_t$ be the roots of $\phi(y)$ in Ω. Then

$$f(x) = (x^{p^e} - \beta_1) \cdots (x^{p^e} - \beta_t).$$

Thus $n = t \cdot p^e$. The polynomial $x^{P^e} - \beta_i$ has in Ω all roots identical to one of them say α_i. Then

$$x^{P^e} - \beta_i = x^{P^e} - \Delta\alpha_i^{p^e} = (x - \alpha_i)^{p^e}$$

Thus

$$f(x) = \{(x - \alpha_1) \cdots (x - \alpha_t)\}^{p^e}$$

Moreover since $\beta_1 \ldots \beta_t$ are distinct, $\alpha_1, \ldots, \alpha_t$ are also distinct. Hence

9) *Over a field of characteristic $p \neq o$, the roots of an irreducible polynomial are repeated equally often, the multiplicity of a* root being p^e, $e \geq o$.

It is important to note that $(x - \alpha_1) \ldots (x - \alpha_t)$ is *not* a polynomial in $k[x]$ and t is *not* necessarily prime to p. **32**

We call t the *reduced degree* of $f(x)$ (or of any of its roots) and p^e, *its degree of inseparability*. Thus

Degree of: Reduced degree X-degree of inseparability

If $\omega \in \Omega$ then we had seen earlier that $k(\omega)/k$ has as many distinct isomorphisms in Ω as there are distinct roots in Ω of the minimum polynomial of ω over k. If we call the reduced degree of $\dfrac{k(\omega)}{k}$ as the *reduced degree of ω* we have

10) *Reduced degree of ω = Number of distinct roots of the minimum polynomial of ω over k.*

We may now call a polynomial *separable* if and only if every root of it in Ω is separable. In particular if $f(x) \in k[x]$ is irreducible then $f(x)$ is separable if one root of it is separable.

Let $\omega \in \Omega$ and $f(x)$ the minimum polynomial of ω in $k[x]$. If $t =$ reduced degree of ω, then

$$f(x) = \{(x - \omega_1) \ldots (x - \omega_t)\}^{p^e}$$

$n = t - p^e$. Let $\omega_1 = \omega$. Consider $\omega_1^{p^e} = \beta_1$. Then

$$f(x) = (x^{p^e} - \beta_1) \cdots (x^{p^e} - \beta_t)$$

and $\beta_1, \ldots \beta_t$ are separable over k. Consider the field $k(\beta_1)$ which is a subfield of $k(\omega).\beta$ being of degree t over $k, (k(\beta_1) : k) = t$. This means that

$$(k(\omega) : k(\beta)) = p^e.$$

But the interesting fact to note is that $k(\omega)$ has over $k(\beta)$ only the identity isomorphism or that $k(\omega)$ is fixed by every $k(\beta)$-automorphism of $\Omega/k(\beta)$. 33

Also since every element of $k(\omega)$ is a rational function of ω over $k(\beta)$, it follows that

$$\lambda^{p^e} \in k(\beta)$$

for every $\lambda \in k(\omega)$. Thus the integer e has the property that for every $\lambda \in k(\omega), \lambda^{p^e} \in k(\beta)$ and there is at least one λ (for instance ω) for which $\lambda^{p^e} \notin k(\beta)$. $\underline{e}$ is called the *exponent* of ω, equivalently of $k(\omega)$. We define the exponent of an algebraic element α over k to be the integer $e \geq o$ such that α^{p^e} is separable but not $\alpha^{p^{e-1}}$. Hence

11) *Exponent of α* is zero $\Leftrightarrow$ *α is separable over k.*

We shall now extend this notion of exponent and reduced degree to any finite extension.

Let K/k be finite so that $K = k(\omega_1, \ldots, \omega_n)$. Put as before $K_o = k$, $K_i = k(\omega_1, \ldots, \omega_i)$ so that $K_n = K$. Let ω_i have reduced degree d_i and exponent e_i over K_{i-1}. Then

$$(K_i : K_{i-1}) = d_i p^{e_i}$$

From the definition of d_i, it follows that the number of distinct k-isomorphisms of K/k is $d_1 \ldots d_n$. We put

$$d = d_1 \cdots d_n$$

and call it the *reduced degree* of K/k. Then

$$(K : k) = d. \ldots p^f$$

where $f = e_1 + \cdots + e_n$. We call p^f the degree of *inseparability* of K/k.

In order to be able to give another interpretation to the integer $\underline{d}$ we make the following considerations. 34

Let $\Omega \supset K \supset k$ and let K/k have the property that every k automorphism of Ω/k acts like identity on K. Thus if $\sigma \in G(\Omega/k)$ and $\omega \in K$, then

$$\sigma\omega = \omega$$

All elements of k have this property. Let $\omega \in K$, $\omega \notin k$. Then by definition, ω has in Ω only one conjugate. The irreducible polynomial of ω has all roots equal. Thus the minimum polynomial of ω is

$$x^{p^m} - a$$

where $\underline{a} \in k$. i.e., $\omega^{p^m} \in k$. On the other hand let K be an extension of k in Ω with the property that for every $\omega \in K$

$$\omega^{p^m} \in k$$

for some integer $m \geq o$. Let σ be an automorphism of Ω/k. Then $\sigma\omega^{p^m} = \omega^{p^m}$. But

$$o = \sigma\omega^{p^m} - \omega^{p^m} = (\sigma\omega - \omega)^{p^m}$$

which shows that $\sigma\omega = \omega$. ω being arbitrary in K, it follows that every element of $G(\Omega/k)$ is identity on K.

Hence for $\omega \in \Omega$ the following three statements are equivalent

1) $\sigma\omega = \omega$ for all $\sigma \in G(\Omega/k)$

2) $\omega^{p^m} \in k$ for some $m \geq o$ depending on ω

3) The irreducible polynomial of ω over k is of the form $x^{p^m} - a, a \in k$.

We call an element $\omega \in \Omega$ which satisfies any one of the above conditions, a *purely inseparable algebraic element over k.* 35

Let us make the

Definition. *A subfield K/k of Ω/k is said to be purely inseparable if element ω of K is purely inseparable.*

From what we have seen above, it follows that K/k is purely inseparable is equivalent to the fact that every k-automorphism of Ω is identity on K.

Let K/k be an algebraic extension and L the maximal separable subfield of K/k. For every $\omega \in K, \omega^{p^e}$ is separable for some $e \geq o$ which means that $\omega^{p^e} \in L$. Thus K/L is a purely inseparable extension field. This means that every k-isomorphism of L/k can be extended uniquely to a k-isomorphism of K/k.

Let, in particular, K/k be a finite extension and L the maximal separable subfield of K. Then K/L is purely inseparable and K/L has no L-isomorphism other than the identity. Thus the number of distinct isomorphism other than the identity. Thus the number of distinct isomorphisms of K/k equals $(L : k)$. But from what has gone before

$$(K : L) = p^f, (L : k) = d.$$

For this reason we shall call $\underline{d}$ also the *degree of separability* of K/k and denote it by $[K : k]$. We shall denote the degree of inseparability, p^f, by $\{K : k\}$. Then

$$(K : k) = [K : k]\{K : k\}.$$

Note. In case k has characteristic zero, every algebraic element over k is separable.

36 If Ω is the algebraic closure of k and L the maximal separable subfield of Ω then Ω/L is purely inseparable. Ω coincides with L in case k

has characteristic zero. But it can happen that L is a proper subfield of Ω.

Let K/k be an algebraic extension and L the maximal separable subfield. Consider the exponents of all elements in K. Let e be the maximum of these if it exists. we call $\underline{e}$ the *exponent* of the extension K/k. It can happen that $\underline{e}$ is finite but K/L is infinite.

If K/k is a finite extension then K/L has degree p^f so that the maximum e of the exponents of elements of K exists. If $\underline{e}$ is the exponent of K/k then

$$e \leq f$$

It can happen that $e < f$. For instance let k have characteristic $p \neq 0$ and let $\alpha \in k$ be not a p^{th} power in k. Then $k(\alpha^{1/p})$ is of degree p over k. Let β in k be not a p^{th} power in k. Then $k(\alpha^{1/p}, \beta^{1/p})$ is of degree p^2 over $k, \beta \notin k(\alpha^{1/p})$ and for every $\lambda \in k(\alpha^{1/p}, \beta^{1/p})$, $\lambda^p \in k$.

We may for instance take $k(x, y)$ to be the field of rational functions of two variables and $K = k(x^{1/p}, y^{1/p})$. Then $(K : k(x, y)) = p^2$ and $\lambda^p \in k(x, y)$ for every $\lambda \in K$.

5 Perfect fields

Let k be a field of characteristic $p > 0$. Let Ω be its algebraic closure. Let $\omega \in k$. Then there is only one element $\omega' \in \Omega$ such that $\omega'^p = \omega$. We can therefore write $\omega^{1/p}$ without any ambiguity. Let $k^{p^{-1}}$ be the field generated in Ω/k by the p^{th} roots of all elements of k. Similarly from 37
$k^{p^{-2}}, \ldots$ Let

$$K = \bigcup_{n \geq 0} k^{p^{-n}}$$

Obviously K is a field; for if $\alpha, \beta \in K$, $\alpha, \beta \in k^{p^{-n}}$ for some large n. We denote K by $k^{p^{-\infty}}$

We shall study $k^{p^{-\infty}}$ in relation to k and Ω . $k^{p^{-\infty}}$ is called the *root field of k*.

Let $\omega \in k^{p^{-\infty}}$. Then $\omega \in k^{p^{-\infty}}$ for some n so that $\omega^{p^{\infty}} \in k$ or ω is purely inseparable. On the other hand let $\omega \in \Omega$ be purely inseparable. Then $\omega^{p^n} \in k$ for some n i.e., $\omega \in k^{p^{-\infty}} \subset k^{p^{-\infty}}$. Thus

1) $k^{p^{-\infty}}$ *is the largest purely inseparable subfield of* Ω/k.

Therefore every automorphism of Ω/k is identity on $k^{p^{-\infty}}$. The set of elements of Ω which are fixed under all the $k-$ automorphisms of Ω/k form a field called the fixed of $G(\Omega/k)$. Since every such element ω, fixed under $G(\Omega/k)$ is purely inseparable, $\Omega \in k^{p^{-\infty}}$. Hence

2) $k^{p^{-\infty}}$ *is the fixed field of the group of* $k-$ *automorphism of* Ω/k.

Let $f(x)$ be an irreducible polynomial in $k^{p^{-\infty}}[x]$. We assert that this is separable. For if not $f(x) \in k^{p^{-\infty}}[x^p]$. Thus $f(x) = a_o + a_1 x^p + \cdots + a_n x^{np}$. Since $a_i \in k^{p^{-\infty}}[X^p]$, it is in some $k^{p^{-t}}$ and so $a_i = b_i^p$ for $b_i \in k^{p^{-\infty}}$. Hence

$$f(x) = (b_o + b_1 x + \cdots + b_n x^n)^p$$

which is contradicts the fact that $f(x)$ is irreducible. Hence

38 3) $\Omega/k^{p^{-\infty}}$ *is a separable extension.*

We now make the

Definition. *A field k is said to be perfect if every algebraic extension of k is separable.*

It follows from the definition that

1) *An algebraically closed field is perfect*

2) *A field of characteristic zero is perfect.*

We shall now prove

3) *A field k of characteristic* $p > 0$ *is perfect if and only if* $k = k^{p^{-\infty}}$.

Let k have no inseparable extension. Then for $a \in k$, $a^{1/p} \in k$ also; for, otherwise $k(a^{1/p})$ is inseparable over k. Thus $k = k^{p^{-1}} = \cdots = k^{p^{-\infty}}$. The converse has already been proved.

We deduce immediately

4) *A finite field is perfect.*

For if k is a finite field of characteristic $p > r$ then $a \to a^p$ is an automorphism of k.

5) *Any algebraic extension of a perfect field is perfect.*

For let K/k be algebraic and k be perfect. If α is inseparable over K, then it is already so over k.

An example of an imperfect field is the field of rational functions of one variable x over a finite field k. For if k has characteristic p, then $x^{1/p} \notin k(x)$ and $k(x^{1/p})$ is a purely inseparable extension over $k(x)$.

Note 1. If $\alpha \in \Omega$ is inseparable over k, it is not true that it is inseparable over every intermediary field, whereas this is true if α is separable. 39

Note 2. If K/k is algebraic and $K \cap k^{p^{-\infty}}$ contains k properly then K is an inseparable extension. But the converse of this is not true, that is, if K/k is an inseparable extension, it can happen that there are no elements in K which are purely inseparable over k. We give to this end the following example due to Bourbaki.

Let k be a field of characteristic $p > 2$ and let $f(x)$ by in irreducible polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

in $k[x]$. If $\alpha_1, \ldots, \alpha_t$ are the distinct roots of $f(x)$ in Ω then

$$f(x) = \Big\{(x - \alpha_1) \ldots (x - \alpha_t)\Big\}^{p^e} e \geq 1.$$

where $n = t. \cdot p^e$. Put $\phi(x) = f(x^p)$. Then

$$\phi(x) = \{(x^p - \alpha_1) \ldots (x^p - \alpha_t)\}^{p^e}$$

If $\beta_i = \alpha_i^{1/p}$ then

$$\phi(x) = \{(x - \beta_1) \ldots (x - \beta_t)\}^{p^{e+1}}$$

and $\beta, \ldots, \beta_t$ are distinct since $\alpha_1 \ldots \alpha_t$ are distinct. Suppose $\phi(x)$ is reducible in $k[x]$ and let $\psi(x)$ be an irreducible factor of $\phi(x)$ in $k[x]$. Then

$$\psi(x) = \Big\{(x - \beta_1) \cdots (x - \beta_t)\Big\}^{p^\mu}$$

for $\mu \geq 0$ and $\ell \leq t$. (This is because roots of $\psi(x)$ occur with the same multiplicity). We can write

$$\psi(x) = \{(x^p - \alpha_1) \ldots (x^p - \alpha_\ell)\}^{p^{\mu-1}}$$

(μ has to be ≥ 1) since otherwise, it will mean that $(x - \alpha_1) \cdots (x - \alpha_t) \in k[x]$). Now this will mean that $\phi(x) = \psi(x)$. $W(x)$ in $k[x^p]$ so that $\ell = t$. Hence

$$\psi(x) = \{(x - \beta_1) \cdots (x - \beta_t)\}^{p^\mu}, \mu \geq 1.$$

40 Since $\psi(x)$ is irreducible and

$$\psi(x) = \{(x^p - \alpha_1) \ldots (x^p - \alpha_t)\}^{p^{\mu-1}}$$

we see that $\mu - 1 = e$ or $\mu = e + 1$. Thus

$$\phi(x) = f(x^p) = \{\psi(x)\}^p$$

Thus if $f(x^p)$ is reducible, it is the p^{th} power of an irreducible polynomial. In this case $a_i = b_i^p, b_i \in k, i = 1, \ldots n$.

Conversely if $a_i = b_i^p, b_i \in k, i = 1, \ldots n$. then $f(x^p)$ is reducible. Hence $f(x^p)$ is reducible $f(x) \in k^p[x]$.

Let k now be a field of characteristic $p > 2$ given by $k = \Gamma(x, y)$, the field of rational functions in two variables x, y over the prime field Γ if p elements. Consider the polynomial

$$f(z) = z^{2p} + xz^p + y,$$

in $k[z]$. Since $x^{1/p}, y^{1/p}$ do not lie in k, $f(z)$ is irreducible in k. Let ϑ be a root of $f(z)$. Then $(k(\vartheta) : k) = 2p$. Let β be in $k(\vartheta)$ and not in k such that $\beta^p \in k$. Then $k(\vartheta) \supset k(\beta) \supset k$. Also $(k(\beta) : k) = p$. In $k(\beta)[x]$ the polynomial $f(z)$ cannot be irreducible, since $(k(\vartheta) : k(\beta)) = 2$. It is reducible and so $k(\beta)$ will contain $x^{1/p}$ and $y^{1/p}$. But then $k(x^{1/p}, y^{1/p}) \supset k(\beta)$.

Thus

$$p^2 = (k(x^{1/p}, y^{1/p}) : k) \leq (k(\beta) : k) \leq (\vartheta) : k) = 2p$$

but this is impossible. Thus there is no element β in $k(\vartheta)$ with $\beta^p \in k$. All the same $k(\vartheta)$ is inseparable.

6) If *k is not perfect then $k^{p^{-\infty}}$ is an infinite extension of k.*

For, if $k^{p^{-\infty}}/k$ is finite then, since $k^{p^{-\infty}} = \bigcup\limits_{n} k^{p^{-n}}$ we have $k^{p^{-n}} = k^{p-(n+1)}$ for some n,

Applying the mapping $a \to a^{a^{p^n}}$ we find $k = k^{p^{-1}}$. But this is false. 41
Thus

$$\left(k^{p^{-(n+1)}} : k^{p^{-n}}\right) > 1$$

which proves our contention.

6 Simple extensions

An algebraic extension K/k is said to be *simple* if there is an $\omega \in K$ such that $K = k(\omega)$. Obviously $(K : k)$ is finite. We call ω a *primitive element* of K. The primitive element is not unique for, $\omega + \lambda$, $\lambda \in k$ also is primitive. We now wish to find conditions when an algebraic extension would be simple. We first prove

Lemma. *Let* k be an infinite field and α, β elements in an algebraic closure Ω *of* k such that α is separable over k. *Then* $k(\alpha, \beta)$ is a simple extension of k.

Proof. Let $f(x)$ and $\phi(x)$ be the irreducible polynomials of α and β respectively in $k[x]$, so that

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$
$$\phi(x) = (x - \beta_1) \cdots (x - \beta_m).$$

□

Since α is separable, $\alpha_1, \ldots \alpha_n$ are all distinct. We shall put $\alpha = \alpha_1$, and $\beta = \beta_1$. Construct the linear polynomials

$$\beta_i + X\alpha_j (i = 1, \ldots, m; j = 1, \ldots, n)$$

These mn polynomials are in Ω, the algebraic closure of k and since k is infinite, there exists an element $\lambda \in k$ such that

$$\beta_i + \lambda\alpha_j \neq \beta_i, +\lambda\alpha_j, \alpha \neq J'$$

Put

$$\gamma = \beta_1 + \lambda\alpha_1 = \beta + \lambda\alpha$$

42 Obviously λ can be chosen so that $\gamma \neq 0$

Now $k(\gamma) \subset k(\alpha,\beta)$. We shall will now show that $\alpha \in k(\gamma)$. From definition of γ, β also will be in $k(\gamma)$ and that will mean

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

In order to do this consider the polynomial $\phi(\gamma - \lambda.x)$in $k(\gamma)[x]$. Also it vanishes for $x = \alpha$. Furthermore by our choice of $\lambda, \phi(\gamma - \lambda\alpha_i) \neq 0$ for $i > 1$. In the algebraic closure Ω, therefore, $f(x)$ and $\phi(\gamma - \lambda x)$ have just $x - \alpha$ as a factor. But $f(x)$ and $\phi(\gamma - \lambda x)$ are both polynomials in $k(\gamma)[x]$. So $x - \alpha$ is the greatest common divisor of $\phi(\gamma - \lambda x)$ and $f(x)$ in $k(\gamma)[x]$. Thus $\alpha \in k(\gamma)$. Our lemma is demonstrated.

We have therefore

Corollary . *If $\alpha_1, \ldots, \alpha_n$ are separably algebraic and $\beta \in \Omega$ then $k(\beta, \alpha, \ldots \alpha_n)$ is a simple extension.*

We deduce immediately

Corollary. *A finite separable extension is simple.*

Let Γ be the field of rational numbers and $\Gamma(\omega,\rho)$ the splitting field of the polynomial $x^3 - 2$ in $\Gamma[x]$. Then $\Gamma(\omega,\rho)$ is simple. A primitive element γ is given by $\omega + \rho = \gamma$. Then $\Gamma(\gamma)$ is of degree 6 over Γ. It is easy to see that γ has over Γ the minimum polynomial

$$(x^3 - 3x - 3)^2 + 3x(x + 1)(x^3 - 3x - 3) + 9x^2(x + 1)^2$$

Let now K/k be a finite extension and L the maximal separable subfield of K/k. Then $(K : L) = p^f$ the degree of inseparability and $(L : k) = d$ the reduced degree. If we consider the exponents of elements of K, these have a maximum e and

$$e \leq f.$$

43 We had given an example of $e < f$. We shall now prove the

Theorem 5. *If e is the exponent and p^f the degree of inseparability of finite extension K of k, then $e = f \iff K/k$ is simple.*

Proof. Let $K = k(\omega)$. Let K_o be the maximal separable subfield of K/k. Now $(K : K_o) = p^f$. But p^f is degree of ω. Thus $e = f$ □

Let now K/k be a finite extension and $e = f$. There exists then a ω in K such that ω^{p^e} is separable and in K_o but for no, $t < e$ ω^{p^t} is in K_o. Thus $K = K_o(\omega)$. K_o being a finite separable extension by our lemma, $K_o = k(\beta)$ for β separable. Thus

$$K = k(\omega, \beta).$$

Using the lemma again, our contention follows.

We now investigate the number of intermediary fields between K and k where K is an algebraic extension of k. Let us first consider a simple extension $K = k(\omega)$. Let $\phi(x)$ be the minimum polynomial of ω in $k[x]$. Let L be any intermediary field. Let $f(x)$ be the minimum polynomial of ω over L. Then $f(x)$ divides $\phi(x)$. Let $f(x)$ have coefficients $a_0, \ldots a_n$ in L. Put L_f the field $k(a_0, \ldots, a_n)$. Then $f(x)$ is minimum polynomial of ω over L_f. Thus

$$(K : L) = (K : L_f)$$

But $L_f \subset L$. This proves that $L = L_f$, and so for every intermediary field there is a unique divisor of $\phi(x)$. Since $\phi(x)$ has in Ω only finitely many factors, K/k has only a finite number of intermediary fields.

We will now prove that the converse is also true. We shall assume k is infinite. 44

Let now K/k be an algebraic extension having only a finite number of intermediary fields. Let $\alpha, \beta \in K$. Consider the elements $\alpha + \lambda\beta$ for $\lambda \in k$. Since k is infinite, the fields $k(\alpha + \lambda\beta)$ are infinite in number and cannot be all distinct. Let for $\lambda = \lambda_1, \lambda_2$ $\lambda_1 \neq \lambda_2$

$$k(\alpha + \lambda_1\beta) = k(\alpha + \lambda_2\beta) = k(\gamma).$$

Then $\alpha + \lambda_1\beta, \alpha + \lambda_2\beta$ are in $k(\gamma)$. Thus $(\lambda_1 - \lambda_2) \in k(\gamma)$. Hence $\beta \in k(\gamma)$ because $\lambda_1 - \lambda_2 \in k$. This means that $\alpha \in k(\gamma)$.

Therefore

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

Hence every subfield of K, generated by 2 and hence by a finite number of elements is simple. Let K be a maximal subfield of K/k which is simple. (This exists since K/k has only finitely many intermediary fields). Let $K_0 = k(\omega)$. Let $\beta \in K$ and $\beta \notin K_0$. Then $k(\gamma) = k(\omega,\beta) \subset K$ and $K_0 \subset k(\gamma)$ contradicting maximality of K_0. Thus $\beta(\gamma) = K$. We have proved

Theorem 6. *K/k is simple $\Longleftrightarrow$ K/k has only finitely many intermediary fields.*

We deduce

Corollary. *If K/k is simple, then every intermediary field is simple.*

Note 1. We have the fact that if K/k is infinite there exist infinitely many intermediary fields.

Note 2. Theorem 6 has been proved on the assumption that k is an infinite
45 field. If k is finite the theorem is still true and we give a proof later.

7 Galois extensions

Let K/k be an algebraic extension and G the group of automorphism of K which are trivial on k. Let L be the subset of all elements of K which are fixed by G. L is then a subfield of K and is called the *fixed field* of G. We shall now consider the class of algebraic extensions K/k which are such that the group $G(K/k)$ of automorphisms of K which are trivial on k, has k as the fixed field. We call such extensions *galois extensions*, the group $G(K/k)$ itself being called the *galois group* of K/k.

We now prove the

Theorem 7. *k is the fixed field of the group of k automorphisms of K $\Longleftrightarrow$ K/k is a normal and separable extension.*

Proof. Let k be the fixed field of the group $G(K/k)$ of k-automorphisms of K. Let $\omega \in K$. Let $\omega_1(= \omega), \ldots \omega_n$ be all the distinct conjugates of ω that lie in K. Consider the polynomial

$$f(x) = (x - \omega_1) \cdots (x - \omega_n)$$

If σ is an element of $G(K/k)$, σ permutes $\omega_1, \ldots, \omega_n$ so that σ leaves the polynomial $f(x)$ unaltered. The coefficients of this polynomial are fixed under all elements of G and hence since k is the fixed field G, $f(x) \in k[x]$. Hence the minimum polynomial roots of the minimum polynomial of ω, since $\omega_1, \ldots \omega_n$ are conjugates. Thus $f(x)/\phi(x)$. Therefore K splitting field of $\phi(x)$, $\phi(x)$ has all roots distinct. Thus K/k is normal and separable. □

46 Suppose now K/k is normal and separable. Consider the group $G(K/k)$ of k-automorphisms of K. Let $\alpha \in K$. Since K/k is separable, all conjugates of α are distinct. Also since K/k is normal K contains all the conjugates. If α is fixed under all $\sigma \in G(K/k)$, then α is a purely inseparable element of K and hence is in k.

Our theorem is thus proved.

We thus see that galois extensions are identical with extension fields which are both normal and separable.

Examples of Galois extensions are the splitting fields of polynomials over perfect fields.

Let k be a field of characteristic $\neq 2$ and let $K = k(\sqrt{\alpha})$ for $\alpha \in k$ and $\sqrt{\alpha} \notin k.(\sqrt{\alpha})^2 = \alpha \in k$. Every element of K is uniquely of the form $a + \sqrt{\alpha} \cdot b$, $a, b \in k$. If σ is an automorphism of K which is trivial on k, then its effect on K is determined by its effect on $\sqrt{\alpha}$. Now

$$\alpha = \sigma \left\{ (\sqrt{\alpha})^2 \right\} = \sigma(\sqrt{\alpha}).\sigma(\sqrt{\alpha})$$

or that $\sigma(\sqrt{\alpha})/\sqrt{\alpha} = \lambda$ is such that $\lambda^2 = 1$. Since $\lambda \in K$, $\lambda = \pm 1$. Thus σ is either th identity or the automorphism

$$\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$$

Thus $G(K/k)$ is a group of order 2. K/k is normal and separable.

We shall obtain some important properties of galois extensions.

1) *If K/k is a galois extension and $k \subset L \subset K$, then K/L is a galois extension also.*

47 For, K/L is clearly separable. We had already seen that it is normal.

If we denote by $G(K/L)$ the galois group of K over L, than $G(K/L)$ is a subgroup of $G(K/k)$.

2) *If $k \subset L_1 \subset L_2 \subset K$* then $G(K/L_2)$ *is a subgroup of* $G(K/L_1)$. This is trivial.

3) If $\{K_\alpha\}$ *is a family of galois extensions of k contained in* Ω then $\bigcap\limits_\alpha K_\alpha$ and $k(\bigcup\limits_\alpha K_\alpha)$ *are galois.*

This follows from the fact that this is already true for normal and also for separable extensions.

4) If *K/k is galois and L* and *L' are two intermediary fields of K/k which are conjugate over k,* then $G(G/L)$ and $G(K/L')$ *are conjugate subgroups of* $G(K/k)$ *and conversely.*

Proof. Since L and L' are conjugate over k let σ be an automorphism of K/k so that $\sigma L = L'$. Let $\tau \in G(K/\sigma L)$. Then for every $\omega \in \sigma L$

$$\tau\omega = \omega$$

But $\omega = \sigma\omega'$ for $\omega' \in L$. Thus

$$\sigma^{-1}\tau\sigma\omega' = \omega'$$

Since this is true for every $\omega' \in L$, it follows that

$$\sigma^{-1}G(K/\sigma L)\sigma \subset G(K/L)$$

In a similar manner one proves that $\sigma G(K/L)\sigma^{-1} \subset G(K/\sigma L)$ which proves our contention. □

Conversely suppose that L and L' are two subfields such that $G(K/L)$ and $G(K/L')$ are conjugate subgroups of $G(K/k)$. Let $G(K/L') = \sigma^{-1}$
48 $G(K/L)\sigma$. Let $\omega \in L'$ and $\tau \in G(K/L)$. Then $\sigma^{-1}\tau\sigma \in G(K/L')$ and so

$$\sigma^{-1}\tau\sigma\omega = \omega$$

or $\tau(\sigma\omega) = \sigma\omega$. This being true for all τ, it follows that $\sigma\omega \in L$ for all ω in L'. Thus $\sigma L' \subset L'$. We can similarly prove that $\sigma^{-1}L \subset L'$ which proves our statement.

In particular let L/k be a normal extension of k which is contained in K. Then $\sigma L = L$ for all $\sigma \in G(K/k)$. This means that $G(K/L)$ is a normal subgroup of $G(K/k)$. On the other hand if L is any subfield such that $G(K/L)$ is a normal subgroup of $G(K/k)$ then by above $\sigma L = L$ for all $\sigma \in G(K/k)$ which proves that L/k is normal. Thus

5) *Let $k \subset L \subset K$.* Then *L/k is normal $\Longleftrightarrow$ $G(K/L)$ is a normal subgroup of $G(K/k)$*

6) If L/k is normal, then $G(K/k) \simeq G(L/k)/G(K/L)$.

Let $\sigma \in G(K/k)$ and $\bar{\sigma}$ the restriction of σ to L. Then $\bar{\sigma}$ is an automorphism of L/k so that $\bar{\sigma} \in G(L/k)$. Now $\sigma \to \bar{\sigma}$ is a homomorphism fo $G(K/k)$ into $G(L/k)$. For
$\overline{\sigma\tau}\omega = \sigma\tau\omega = \sigma(\tau\omega) = \bar{\sigma}\bar{\tau}\omega$ for all $\omega \in L$. Thus $\bar{\sigma}\bar{\tau} = \overline{\sigma\tau}$

The homomorphism is *onto* since every automorphism of L/k can be **49**
extended into an automorphism of K/k. Now $\bar{\sigma}$ is identity if and only if

$$\bar{\sigma}\omega = \omega$$

for all $\omega \in L$. Thus $\sigma \in G(K/L)$. Also every $\sigma \in G(K/L)$ has this property so that the kernel of the homomorphism is $G(K/L)$.

Let K/k be a finite galois extension. Every isomorphism of K/k in Ω is an an automorphism. Also K/k being separable, K/k has exactly $(K : k)$ district isomorphisms. This shows that

$$(K : k) = \text{order of } G.$$

We shall now prove the converse

7) *If G is a finite group of automorphisms of K/k having k as the fixed field then $(K : k)$ = order of G.*

Proof. Let $\sigma_1, \ldots, \sigma_n$ be the n elements of G and $\omega_1, \ldots \omega_{n+1}$ any $n+1$ elements of K. Denote by V_K the vector space over K of n dimensions formed by n- tuples $(\alpha_1, \ldots, \alpha_n)$. Define $n+1$ vectors $\Omega_1, \ldots, \Omega_{n+1}$ by

$$\Omega_i = (\sigma_i(\omega_i), \ldots, \sigma_n(\omega_i)) i = 1, \ldots, n+1$$

Among these vectors there exists $m \leq n$ vectors linearly independent over K. Let $\Omega_1, \ldots, \Omega_m$ be independent. Then

$$\Omega_{m+1} = \sum_{n=1}^{m} a_i \Omega_i \quad a_i \in K$$

This equation gives, for the components of the $\Omega' s$,

$$\sigma_\ell(\omega_{m+1}) = \sum_{1=i}^{m} a_i \sigma_\ell(\omega_i) \alpha = 1, \ldots, n.$$

□

Since $\sigma_1, \ldots, \sigma_n$ form a group then $\sigma_n \sigma_1, \ldots, \sigma_n \sigma_n$ are again the
50 elements $\sigma_1, \ldots, \sigma_n$ in some order. Thus

$$\sigma_h \sigma_\ell(\omega_{m+1}) = \sum_{i=1}^{m} \sigma_h(a_i | \sigma_h \sigma_\ell(\omega_i)$$

which means

$$\sigma_\ell(\omega_{m+1}) = \sum_{i=1}^{m} \sigma_h(a_i) \sigma_\ell(\omega_i) \quad i = 1, \ldots, n$$

subtracting we have

$$\sum_{i=1}^{m} (\sigma_h(a_i) - a_i \sigma_\ell(\omega_i) = 0$$

which means that

$$\sum_{i=1}^{m} (\sigma_h(a_i) - a_i) \Omega_i = 0$$

From linear independence, it follows that $\sigma_h(a_i) = a_i$ for all i. But h is arbitrary. Thus $a_i \in k$. We therefore have by taking σ_1 to be the identity element of G

$$\omega_{m+1} = \sum_{i=1}^{m} a_i \omega_i$$

a_i are in k, not all zero. Hence

$$(K : k) \leq n.$$

But every element of G is an isomorphism of K/k. Thus

$$(K : k) \geq \text{ order of } G = n.$$

Our assertion is established.

Suppose K/k is a galois extension. For every subfield L of K/k, the extension K/L is galois. We denote its galois group by $G(L)$ and this is a subgroup of $G(K/k)$. Suppose g is any subgroup of $G(K/k)$ and let $F(g)$ be its fixed field. Then $F(g)$ is a subfield of K. The galois group $G(F(g))$ of $K/F(g)$ contains g. *In general one has only* **51**

$$g \subset G(F(g))$$

Let now K/k be a *finite* galois extension. Let g be a subgroup of $G(K/k) = G$ and $F(g)$, the fixed field of g. Then by above

$$\Big(K : F(g)\Big) = \text{ order of } g.$$

and so

$$g = G(K/F(g))$$

If g_1 and g_2 are two subgroups of G with $g_1 \subset g_2$ then $F(g_1)$ and $F(g_2)$ are distinct. For if $F(g_1)$ and $F(g_2)$ are identical, then by above $g_1 = G(K/F(g_2)) = g_2$. We thus have the

Main Theorem(of finite galois theory). *Let K/k be a finite galois extension with galois group G. Let M denote the class of all subgroups of G and N the class all subfield of K/k. Let ϕ be the mapping which* *assigns to every subgroup $g \in M$, the fixed field $F(g)$ of g in N. Then ϕ is a mapping of M onto N which is biunivocal.*

In order to restore this property even for infinite extensions, we develop a method due originally to Krull.

Let K/k be a galois extension with galois group $G(K/k)$. For every $\omega \in K$, we denote by G_ω the galois group $G(K/k(\omega))$. This then is a subgroup of $G(K/k)$. We make $G(K/k)$ into a topological group by prescribing the $\{G_\omega\}$ as a fundamental system of neighbourhoods of the identity element $\underline{e} \in G(K/k)$. Obviously $\bigcap\limits_{\alpha} G_\alpha = (e)$. For $\sigma \in \bigcap_\alpha G_\alpha \Rightarrow \sigma\alpha = \alpha$ for all $\alpha \in K$ so that $\sigma = e$. It is easy to verify that $\{G_\alpha\}$ satisfy
52 the axioms for a fundamental system of open sets containing the identity elements $\underline{e}$.

Any open set in G is therefore a union of sets of type $\{\sigma G_\alpha\}$ or a finite intersection of such. Also since G_α are open subgroups they are closed; for, σG_α is open for all σ and hence

$$\bigcup_{\sigma \neq e} \sigma G_\alpha$$

is also open. Therefore G_α is closed. This proves that the topology on G makes it *totally disconnected*. We call the topology on G the *Krull topology*.

If g is a subgroup of G, $\overline{g}$ the closure of g is also a subgroup. We now prove the

Lemma. *Let g be a subgroup of G a and L its fixed field. Then*

$$G(K/L) = \overline{g} \quad \textit{(the closure of } g\textit{)}.$$

Proof. Let ω be an element in K and $f(x)$ its minimum polynomial in k. Consider $f(x)$ as a polynomial over L and let L' be its splitting field over L. Then L'/L is a galois extension. The restriction of elements of g to L' are automorphisms of L' with L as fixed field (by definition of L). By finite galois theory these are all the elements of the galois group of L'/L. This means that every automorphism of L'/L comes from an elements of g. □

Let $\sigma \in G(K/L)$. Let ω be any element in K and G the group $G(K/k(\omega))$. The restriction of σ to L' is an automorphism of L' with L as fixed field. There is thus an element $\tau \in g$, which has on L' the same effect as σ. Hence $\tau^{-1}\sigma$ is identity on L' and since $\omega \in L'$ we get

$$\tau^{-1}\sigma\omega = \omega$$

This means that $\tau^{-1}\sigma \in G_\omega$ by definition of G_ω. Hence $\sigma^{-1}\tau \in G_\omega$ 53
or $\tau \in \sigma G_\omega$. But σG_ω is an open set containing σ. Therefore since $\{\sigma G_\omega\}$ for all G_ω form a fundamental system of neighbourhoods of σ we conclude that

$$\sigma \in \overline{g}.$$

Thus $G(K/L) \subset \overline{g}$

Let now $\sigma \in \overline{g}$. Then σG_ω is a neighbourhood of σ and so intersects g in a non empty set. Let $\omega \in L$. Let $\tau \in \sigma G_\omega \cap g$. Let σ' in G_ω such that

$$\sigma\sigma' = \tau$$

By definition of $\tau, \tau\omega = \omega$. But $\tau\omega = \sigma\sigma'\omega = \omega$. Therefore $\sigma\sigma' \in G_\omega$. But σ' is already is in G_ω. Therefore $\sigma\omega = \omega$. Also ω being arbitrary

$$\sigma L = L$$

which means that $\sigma \in G(K/L)$. Thus

$$\overline{g} \subset G(K/L)$$

and our contention is established.

From the lemma, it follows that if L is an intermediary field, the galois group $G(K/L)$ is a closed subgroup of $G(K/k)$. On the other hand if g is a closed subgroup of G and $F(g)$ its fixed field then

$$G(K/F(g)) = \overline{g} = g.$$

we have hence the fundamental

Theorem 8. *Let K/k be a galois extension and $G(K/k)$ the galois group with the Krull - topology. Let M denote the set of closed subgroups of G and N the set of intermediary fields of K/k. Let ϕ be the mapping which assigns to every $g \in M$, the fixed field $F(g)$ of g in N. Then ϕ is a* 54
biunivocal mapping of M on N.

Suppose now that K/k is a galois extension and L is an intermediary field. Let $G(K/k)$ and $G(K/L)$ be the galois groups. On $G(K/L)$ there are two topologies, one that is induced by the topology on $G(K/k)$ and
55 the other the topology that $G(K/L)$ possesses as a galois extension. If L' is a subfield of K/L so that L'/L is finite, then $G(K/L')$ is an open set in the inherent topology on $G(K/L)$. On the other hand $L' = L(\omega)$ since L'/L is a separable extension.

Thus

$$G(K/L') \subset G_\omega \cap G(K/L)$$

which proves that the two topologies are equivalent. Here we have used the fact that a finite separable extension of L is simple. We gave already seen the truth of this statement if L is infinite. In case L is finite it is proved in the next section. ‘ In a similar manner if K/k is galois and L is a normal extension of k in K, then on $G(L/k)$ there are two topologies, one the inherent one and the other the topology of the quotient group $G(K/k)/G(K/L)$. One can prove that the two topologies are equivalent.

We call an extension K/k *abelian* or *solvable* according as $G(K/k)$ is abelian or a solvable group. If K/k is a galois extension and $G(K/k)$ its galois group with the Krull topology let H denote the closure of the algebraic commutator subgroup of $G(K/k)$. H is called the topological commutator subgroup. If L is its fixed field, then since H is normal, L/k is a galois extension. Its galois group is isomorphic to G/H which is abelian. From the property of the commutator subgroup, it follows that L is the *m*aximal abelian subfield of K/k.

8 Finite fields

Let K be a finite field of q elements, $q = p^n$ where p is the characteristic of K. Let Γ be the prime field of p elements. Then

$$(K : \Gamma) = n$$

K^* the group of non-zero elements of K is an abelian group of order $q - 1$. For $\alpha \in K^*$ we have

$$\alpha^{q-1} = 1$$

1 being the unit element of K. The $q-1$ elements of K^* are roots of $x^{q-1}-1$. Also

$$x^{q-1}-1=\prod_{\alpha\in K^*}(x-\alpha).$$

Let $\alpha\in K^*$. Let $\underline{d}$ be its order as an element of the finite group K^*. Then $\alpha^d=1$. Consider the polynomial x^d-1. It has in K^* at most $\underline{d}$ roots. Also $d/q-1$. But

$$x^{q-1}-1=(x^d-1)(x^{q-1-d}+\cdots)$$

Since x^d-1 and $x^{q-1-d}+\cdots$ both have respectively at most d and $q-1-d$ roots in K^* and they together $q-1$ roots in K^* it follows that for every divisor d of $q-1$, x^d-1 has exactly d roots in K^*. These roots from a group of order $\underline{d}$. If it is cyclic then there is an element of order $\underline{d}$ and there are exactly $\phi(d)$ elements of order $\underline{d}$. Also

$$\sum_{d/q-1}\phi(d)=q-1$$

which proves that for every divisor d of $q-1$ there are $\phi(d)\geq 1$ elements of order $\underline{d}$. Thus **56**

1) *T*he multiplicative group of a finite field is cyclic.

   Let k be a finite of q elements and K a finite extension of k of degree n. Then K has q^n elements. Since K^* is cyclic, let ρ be a generator of K^*. Then

   $$K=k(\rho)$$

   which proves

2) *E*very finite extension of a finite field is simple.

   For a finite field of characteristic p, $a\to a^{p^e}$ is an automorphism of K. Since k has q elements we have

   $$a^q=a$$

   for every $a\in k$.

Now $a \to a^q$ is an automorphism of K/k which fixes elements of k. Call this automorphism σ. σ is determined uniquely by its effect on a generator ρ of K^*. Consider the automorphisms

$$1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$$

These are distinct. For,

$$\sigma^i \rho = \sigma^{i-1}(\sigma\rho) = \sigma^{i-1}(\rho^q) = \rho^{q^i}$$

Hence $\rho^q = 1 \Longleftrightarrow q^i \equiv o(\mod q^n)$ or $i = o$ (Since $i < n$). But K/k being of degree n cannot have more than n automorphisms. We have

3) *T*he galois group of a finite extension of a finite field is cyclic.

The generator σ of this cyclic group, defined by

$$\sigma a = a^q$$

is called the *F*robenius automorphism. It is defined without any reference to a generator of K^*. 57

Let L be an intermediary field of K/k. Then $(L : k)$ is a divisor of $(K : k) = n$. If $d = (L : k)$ then L has q^d elements. Also since K/k has a cyclic galois group, there is one and only one subgroup of a given order $\underline{\text{d}}$. Hence

4) *T*he number of intermediary fields of K/k is equal to the number of divisors of n.

Chapter 3

Algebraic function fields

1 F.K. Schmidt's theorem

Let K/k be an extension field and $x_1, \ldots, x_{n+1}$ any $n+1$ elements of **58**
K. Let $R = k[z_1, \ldots, z_{n+1}]$ be the ring of polynomials in $n+1$ variables over k. Let $\mathscr{Y}$ be the ideal in R of polynomials $f(z_1, \ldots, z_{n+1})$ with the property

$$f(x_1, \ldots, x_{n+1}) = 0.$$

Then clearly $\mathscr{Y}$ is a prime ideal of R. Also since R is a Noetheeian ring, $\mathscr{Y}$ is finitely generated. Note that $\mathscr{Y} = (o)$ if and only if $x_1, \ldots,$ x_{n+1} are algebraically independent over k. $\mathscr{Y}$ is called the *i*deal of the set $x_1, \ldots, x_{n+1}$.

We shall consider the case where the set $x_1, \ldots, x_{n+1}$ has dimension $\underline{\mathrm{n}}$ over k, that is that $k(x_1, \ldots, x_{n+1})$ is of transcendence degree n over k. We prove

Theorem 1. *$\mathscr{Y}$ is a principal ideal generated by an irreducible polynomial.*

Proof. Without loss in generality we may assume that $x_1, \ldots, x_n$ are algebraically independent over k and that x_{n+1} is algebraic over $k(x_1, \ldots, x_n)$, so that $\mathscr{Y} \neq (o)$. □

Consider the degrees of the polynomials $f(z_1, \ldots, z_{n+1})$ (in $\mathscr{Y}$) in the variable z_{n+1}. These degrees have a minimum greater than zero since $\mathscr{Y} \neq (o)$, and $x_1, \ldots, x_n$ are algebraically independent over k. Let φ be a polynomial in $\mathscr{Y}$ of smallest degree in z_{n+1}. Put

$$\varphi = A_o z^{\lambda}_{n+1} + A_1 z^{\lambda-1}_n + \ldots + A_\lambda$$

59 where $A_0, A_1, \ldots, A_\lambda$ are polynomials in $z_1, \ldots z_n$ with coefficients in k. We may assume that $A_0, A_1, \ldots, A_\lambda$ have no common factor in $k[z_1, \ldots, z_n]$. For if $A(z_1, \ldots, z_n)$ is a common factor of $A_0, \ldots, A_\lambda$ then

$$\varphi(z_1, \ldots, z_{n+1}) = A(z_1, \ldots, z_n)\, \varphi_1(z_1, \ldots, z_{n+1})$$

and so, since $x_1, \ldots, x_n$ are algebraically independent,

$$\varphi_1(x_1, \ldots, x_{n+1}) = o$$

and φ_1 will serve our purpose. So we can take φ to be a primitive polynomial in z_{n+1} over $R' = k[z_1, \ldots, z_n]$.

Clearly φ is irreducible in R'. For, if

$$\varphi = g_1(z_1, \ldots, z_{n+1})\; g_2(z_1, \ldots, z_{n+1})$$

then $g_i(x_1, \ldots, x_{n+1}) = 0$ for $i = 1$ or 2, so that either g_1 or g_2 is in $\mathscr{Y}$. Both cannot have a term in z_{n+1} with non zero coefficient. For then the degrees in z_{n+1} of g_1 of g_2 will both be less that of φ in z_{n+1} contradicting the definition of ϕ. So one g_1, g_2 say g_1 is independent of z_{n+1}. But this means that φ is not a primitive polynomial.

Thus we have chosen in $\mathscr{Y}$ a polynomial φ which os irreducible, of the smallest degree in z_{n+1} and primitive in $R'[z_{n+1}]$.

Let $\psi(z_1, \ldots, z_{n+1})$ be any other polynomial in $\mathscr{Y}$.

Since $F = k(z_1, \ldots, z_n)$ is a field, $F[z_{n+1}]$ is a Euclidean ring so that in $F[z_{n+1}]$ we have

$$\psi(z_1, \ldots, z_{n+1}) = A(z_1, \ldots, z_{n+1})\; \varphi(z_1, \ldots, z_{n+1}) + L(z_1, \ldots, z_{n+1})$$

60 where A and L are polynomials in z_{n+1}over F. Here either $L = o$ or degree of L in z_{n+1} is less than that of φ. If $L \neq o$, then we may multiply

both sides of the above equation by a suitable polynomial in $z_1, \ldots, z_n$ over k so that

$$B(z_1, \ldots, z_n)\psi = C(z_1, \ldots, z_{n+1})\varphi(z_1, \ldots, z_{n+1}) + L_1(z_1, \ldots, z_{n+1})$$

L_1 having in z_{n+1} the same degree as L. Since φ and ψ are in $\mathscr{Y}$, it follows that $L_1 \in \mathscr{Y}$. Because of degree of L_1, it follows that

$$L_1 = L = 0.$$

Thus

$$B(z_1, \ldots, z_n)\psi = A(z_1, \ldots, z_{n+1})\varphi(z_1, \ldots, z_{n+1})$$

Since φ is a primitive polynomial, it follows that φ divides ψ and our theorem is proved.

We call φ *the irreducible polynomial of* $x_1, \ldots x_{n+1}$ *over* k.

Note that since $x_1, \ldots x_n$ are algebraically independent over k, the polynomial

$$\varphi_1(z_{n+1}) = \varphi(x_1, \ldots, x_n, z_{n+1})$$

over $k(x_1, \ldots, x_n)$ is irreducible in z_{n+1}.

Let $x_1, \ldots, x_{n+1}$be of dimension n over k and φ the irreducible polynomial of $x_1, \ldots, x_{n+1}$ over k. Let φ be a polynomial in $z_1, \ldots, z_{i+1}$ but not in $z_{i+2}, \ldots, z_{n+1}$, that is it does not involve $z_{i+2}, \ldots, z_{n+1}$ in its expression. Consider the field $L = k(x_1, \ldots, x_{i+1})$. because $x_1, \ldots, x_{i+1}$ are algebraically dependent $(\varphi(x_1, \ldots, x_{i+1}) = 0)$, 61

$$\dim_k L \leq i.$$

But $k(x_1, \ldots, x_{n+1}) = L(x_{i+2}, \ldots, x_{n+1})$ so that

$$\dim_L k(x_1, \ldots, x_{n+1}) \leq n - i.$$

Since dimensions are additive, we have

$$n = \dim_k L + \dim_L k(x_1, \ldots, x_{n+1}) \leq i + n - i = n.$$

Thus L has over k the dimension i. Since φ is a polynomial in $z_1, \ldots, z_{i+1}$ every one of these variables occurring, with non zero coefficients, we get the

Corollary. *If $x_1, \ldots, x_{n+1}$ be $n+1$ elements of K/k and have dimension n, there exist among them $i+1$ elements, $i \leq n$, say $x_1, \ldots, x_{i+1}$ (in some order) such that $k(x_1, \ldots x_{i+1})$ has dimension i over k and every i of them are algebraically independent.*

Let K/k be a transcendental extension with a transcendence base B over k. Then $K/k(B)$ is algebraic. We call K/k an *algebraic function field* if

(1) B is a finite set

(2) $K/k(B)$ is finite algebraic.

Let $\dim_k K = n$. There exist $x_1, \ldots, x_n$ in K which form a transcendence base of K/k. If K is an algebraic function field then $K/k(x_1, \ldots, x_n)$ is finite algebraic. Hence $K = k(x_1, \ldots, x_m), m \geq n$, is finitely generated. This shows that algebraic function fields are identical with finitely generated extensions.

62 An algebraic function field K/k is said to be *separably generated* if there exists a transcendence base $x_1, \ldots, x_n$ of K/k such that $K/k(x_1, \ldots, x_n)$ is a separable algebraic extension of finite degree. $x_1, \ldots, x_n$ is then said to be a *separating base*. Clearly every purely transcendental extension is separably generated. Also, if k has characteristic zero and K is an algebraic function field, it is separably generated. In this case every transcendence base is a separating base. This is no longer true if k has characteristic $p \neq o$.

For example, let $K = k(x, y)$ be a function field of transcendence degree one and let

$$x^2 - y^p = o.$$

Let k have characteristic $p \neq 2$. Obviously x and y are both transcendental over k. But $K/k(x)$ is a simple extension generated by y which is a root of

$$z^p - x^2$$

over $k(x)[z]$ and since k has characteristic p, $K/k(x)$ is purely inseparable. On the other hand $K/k(y)$ is separable since x satisfies over $k(y)$ the polynomial

$$x^2 - y^p.$$

Thus y is separating but not x.

An algebraic function field which is not separably generated is said to be *inseparably generated*. This means that for every base B of K/k. $K/k(B)$ is inseparably algebraic.

63 In algebraic geometry and in algebraic function theory, it is of importance to know when an algebraic function field is separably generated. An important theorem in this regard is theorem 2 due to F.K. Schmidt. We shall first prove a

Lemma . *Let k be a perfect field of characteristic $p \neq o$ and $K = k(x_1, \ldots, x_{n+1})$ an extension field of dimension n. Then K is separably generated.*

Proof. Let φ be the irreducible polynomial of $x_1, \ldots, x_{n+1}$ and let it be a polynomial in $z_1, \ldots, z_{i+1}$ but in $z_{i+2}, \ldots, z_{n+1}$. Then

$$\varphi(x_1, \ldots, z_t, \ldots, x_{i+1})$$

is irreducible over $k(x_1, \ldots, x_{t-1}, x_{t+1}, \ldots, x_{i+1})$ for every $t, 1 \leq t \leq i+1$. At least for one $t, \varphi(z_1, \ldots, z_t, \ldots, z_{i+1})$ is a separable polynomial in z_t over $k(z_1, \ldots, z_{t-1}, \ldots, z_{i+1})$. For, if it is inseparable in every z_t, then

$$\varphi(z_1, \ldots, z_{i+1}) \in k[z_1^p, \ldots, z_{i+1}^p]$$

and since k is perfect, this will mean that $\varphi(z_1, \ldots, z_{i+1})$ is the *pth* power of a polynomial in $k[z_1, \ldots, z_{i+1}]$ which contradicts irreducibility of φ. So, for some z_t, say z_1, we have $\varphi(z_1, x_2, \ldots, x_{i+1})$ is a separable polynomial. Hence x_1 is separable over $k(x_2, \ldots, x_{i+1})$ and so over $k(x_2, \ldots, x_{n+1})$. But $x_2, \ldots, x_{n+1}$ has dimension n and our lemma is proved. □

Corollary . *Under the conditions of the lemma, a separating base of n elements may be chosen from among $x_1, \ldots, x_{n+1}$.*

We are now ready to prove the theorem of *F.K.Schmidt*. 64

Theorem 2. *Every algebraic function field K over a perfect field k is separably generated.*

Proof. Obviously, the theorem is true if k has characteristic zero. So let k have characteristic $p \neq o$. Let $K = k(x_1, \ldots, x_m)$ and let n be the dimension of K/k. Then $m \geq n$. If $m = n$ there is nothing to prove. Let $m = n + q$. If $q = 1$ then lemma 1 proves the theorem. So let us assume theorem proved for $q - 1$ instead of $q > 1$. We may assume, without loss in generality that $x_1, \ldots, x_n$ is a transcendence base of K/k. Consider the fields $L = k(x_1, \ldots, x_n, x_{n+1})$. It satisfies the conditions of the lemma. Hence there exist n elements among $x_1, \ldots, x_{n+1}$ say $x_1, \ldots, x_{t-1}, x_{t+1}, \ldots x_{n+1}$ which from a separating base of L/k. Thus x_t is separable over $k(x_1, \ldots, x_{t-1}, \ldots, x_{n+1})$ and hence over

$$M = k(x_1, \ldots, x_{t-1}, x_{t+1}, x_{t+2}, \ldots, x_m)$$

M/k now satisfies the induction hypothesis and so is separably generated. Since K/M is separable, it follows that K is separably generated. □

We could prove even more if we assume as induction hypothesis the fact that among $x_1, \ldots, x_m$ there exists a separating base.

2 Derivations

Let R be a commutative ring with unit element $\underline{e}$. A mapping D of R into itself is said to be a *derivation* of R if

65 (1) $D(a + b) = Da + Db$

(2) $D(ab) = aDb + bDa$

for $a, b \in R$. It is said to be a derivation *over* a subring R' if for every $a \in R'$, $Da = o$. It then follows that for $a \in R'$ and $x \in R$

$$Dax = aDx$$

The set R_o of $a \in R$ with $Da = o$ is a subring of R and contains $\underline{e}$. For,

$$De = De^2 = De. \quad e + e. \quad De = 2De\,;$$

so $De = o$. If $Da = o$, $Db = o$, then

$$D(a+b) = Da + Db = o$$
$$D(ab) = aDb + bDa = o$$

Thus R_o is a subring. We call R_o the *ring of constants of the derivation D*.

If R is a field, then R_o also is a field. For, if $x \in R_o$ and $x \neq o$, then

$$o = De = Dx.x^{-1} = Dx.x^{-1} + x.Dx^{-1}$$

Thus

$$Dx^{-1} = o$$

so that $x^{-1} \in R_o$.

D is said to be a *non-trivial* derivation of R if there is an $x \in R$ with $Dx \neq o$. It follows from above that

Theorem 3. *A prime field has no non-trivial derivations.*

A Derivation $\bar{D}$ of R is said to be an *extension* of a derivation D of a subring R' of R if $\bar{D}a = Da$ for $a \in R'$. We now prove the 66

Theorem 4. *If K is the quotient field of an integrity domain R, then a derivation D of R can be uniquely extended to K.*

Proof. Every element c in K can be expressed in the form $c = \dfrac{a}{b}$, a, $b \in R$. If an extension $\bar{D}$ of D exists, then

$$\bar{D}a = Da$$

But $a = bc$ so that

$$Da = \bar{D}a = \bar{D}bc = b\bar{D}c + cDb$$

Therefore

$$\bar{D}c = \frac{Da - cDb}{b} = \frac{bDa - aDb}{b^2}$$

If c is expressed in the form $\frac{a'}{b'}$, $a', b' \in R$ then $ab' = ba'$and so

$$Da.b' + a.Db' = Db.a' + bDa'$$

or that

$$\frac{Da' - cDb'}{b'} = \frac{Da - cDb}{b}$$

which proves that $\bar{D}c$ does not depend on the way c is expressed as the ratio of two elements from R. We have therefore only to prove the existence of $\bar{D}$. In order to prove this, put for $c = \frac{a}{b}$

$$\bar{D}c = \frac{bDa - aDb}{b^2};$$

we should verify that it is a derivation, is independent of the way c is expressed as ratio of elements in R and that it coincides with D on R. These are very simple. □

67 Let D_1, D_2 be two deviations of R. Define $D = D_1 + D_2$ by $Da = D_1a + D_2a$ for $a \in R$. Then it is easy to verify that D is a derivation of R. Furthermore if $a \in R$ define aD by

$$(aD)x = a.Dx$$

By this means, the derivations of R from an R module, Suppose $D_1, \ldots, D_r$ from a basis of the module of derivations of R.

Then every derivation D of R is of the form

$$D = \sum_i a_i D_i, \quad a_i \in R.$$

Let R be an integrity domain and $\bar{D}_1, \ldots, \bar{D}_r$ the unique extensions of $D_1, \ldots, D_r$ respectively to K, the quotient, field of R. Then $\bar{D}_1, \ldots, \bar{D}_r$ are linearly independent over K. For, if

$$\sum_i 1_i \bar{D}_i = o, \qquad 1_i \in K$$

then write $1_i = \dfrac{a_i}{b_i}$, $a_i, b_i \in R$. We get

$$\sum_i \frac{ai}{bi}\bar{D}_i = o.$$

Multiplying throughout by $b_1, \ldots, b_r$ which is not zero, we get $(\sum_i \lambda \bar{D}_i)t = o$ for every $t \in R$. Therefore $\sum_i \lambda_i D_i = o$ which implies that $\lambda_i = o$ or $a_i = o$.

Also, since every derivation D of K is an extension of a derivation of R, it follows that the derivations of K from an r-dimensional vector space over K.

Let us now consider the case where $R = k[x_1, \ldots, x_n]$ is the ring of polynomials in n variables $x_1, \ldots, x_n$. The n mappings

$$D_i : \qquad a \to \frac{\partial a}{\partial x_i}, i = 1, \ldots, n$$

are clearly derivations of R over k. They form a base of derivations of 68
R which are trivial on k. For, if

$$\sum_i a_i D_i = o, \qquad a_i \in R$$

then, since $D_i(x_j) = \delta_{ij}$, we get

$$o = (\sum_i a_i D_i)x_j = a_j, j = 1, \ldots, n.$$

Also, if D is any derivation of R which is trivial on k, then let $Dx_i = a_i$. Put

$$\bar{D} = D - \sum_i a_i D_i.$$

Then

$$\bar{D}x_j = Dx_j - (\sum_i a_i D_i)x_j = o$$

which shows that since $x_1, \ldots, x_n$ generate $R, \bar{D} = o$.

Suppose D is any derivation of k and let $\bar{D}$ be an extension of D to R. Let $\bar{D}x_i = a_i$. Let D_o be another extension of D which has the property $D_o x_i = a_i, i = 1, \ldots, n$.

Then $D - D_o$ is a derivation of R which is trivial on k. But since

$$(D - D_o)x_i = o, \quad i = 1, \ldots, n$$

it follows that $D = D_o$. This gives us the

Theorem 5. *The derivations of $K = k(x_1, \ldots, x_n)$, the field of rational functions of n variables over k which are trivial on k from a vector space of dimension n over K. A basis of this space of derivations is given by the n partial derivations*

$$D_i = \frac{\partial}{\partial x_i}, \quad i = 1, \ldots, n.$$

69 *Furthermore if D is any derivation of k, there exists only one extension $\bar{D}$ of D to K for which*

$$\bar{D}x_i = a_i, \quad i = 1, \ldots, n$$

where $a_1, \ldots, a_n$ are any n quantities of K arbitrarily given.

We now consider derivations of algebraic function fields.

Let $K = k(x_1, \ldots, x_m)$ be a finitely generated extension of k. Put $T = k[x_1, \ldots, x_m]$. In order to determine all the derivations of K, it is enough to determine the derivations of T since K is the quotient field of T. Let D be a derivation of k; we wish to find extensions $\bar{D}$ of D to K.

Let R denote the ring of polynomials $k[z_1, \ldots, z_m]$ in m independent variables. For any polynomial $f(x_1, \ldots, x_m)$ in T, denote by $\dfrac{\partial f}{\underline{\partial} x_i}$ the polynomial obtained by substituting $z_i = x_i, i = 1, \ldots, m$ in $\dfrac{\partial \bar{f}}{\partial z_i}$ where $\bar{f} = f(z_1, \ldots, z_m)$ is in R.

If

$$f = \sum_{\lambda} a_{\lambda_1}, \ldots, \lambda_m x_1^{\lambda_1} \cdots x_m^{\lambda_m}$$

$a\lambda_1, \ldots, \lambda_m \in k$, put

$$f^D = \sum_\lambda (Da_{\lambda_1}, \ldots, \lambda_m) x_1^{\lambda_1} \cdot x_m^{\lambda_m}.$$

Obviously f^D is a polynomial in T. If $\bar{D}$ is an extension of the derivation D, then clearly

$$\bar{D}f = f^D + \sum_{i=1}^m \frac{\partial f}{\partial x_i} \bar{D} x_i$$

for any $f \in T$. Also $\bar{D}$ is determined uniquely by its values on $x_1, \ldots, x_m$ 70 which generate T. Now $\bar{D}x_i$ cannot be arbitrary elements of T. For, let $\mathscr{Y}$ be the ideal in R of the set $x_1, \ldots, x_m$.

Then for $f(z_1, \ldots, z_m)$ in $\mathscr{Y}$,

$$f(x_1, \ldots, x_m) = o.$$

Therefore, since $\bar{D}o = 0$, the $\bar{D}x_i$ would have to satisfy the infinity of equations

$$0 = f^D + \sum_{i=1}^m \frac{\partial f}{\partial x_i} \bar{D} x_i$$

for every f in $\mathscr{Y}$.

Conversely, suppose $u_1, \ldots u_m$ are m elements in T satisfying

$$f^D + \sum_{i=1}^m \frac{\partial f}{\partial x_i} u_i = 0$$

for every f in $\mathscr{Y}$. For any φ in T define $\bar{D}$ by

$$\bar{D}\varphi = \varphi^D + f^D + \sum_{i=1}^m \frac{\partial \varphi}{\partial x_i} \bar{D} x_i$$

where $\bar{D}x_i = u_i$. Then clearly $\bar{D}$ is a derivation of T and it coincides with D on k. Furthermore $\bar{D}$ does not depend on the way φ is expressed as a polynomial in $x_1, \ldots, x_m$. For, if $\varphi = a(x_1, \ldots, x_m) = b(x_1, \ldots, x_m)$ then, since $a - b \in \mathscr{Y}$ have

$$a^D - b^D + \sum_i \Big(\frac{\partial a}{\partial x_i} u_i - \frac{\partial b}{\partial x_i} u_i\Big) = o$$

which proves our contention. Hence

71 **Theorem 6.** *Let $K = k(x_1, \ldots, x_m)$ and D a derivation of k. Let $\mathscr{Y}$ be ideal in $k[z_1, \ldots, z_m]$ of the set $x_1, \ldots, x_m$. Let $u_1, \ldots, u_m$ be any elements of K. There exists a derivation $\bar{D}$ and only one satisfying*

$$\bar{D} x_i = u_i, i = 1, \ldots, m$$

and extending the derivation D in k, if and only if, for every $f \in \mathscr{Y}$

$$f^D + \sum_{i=1}^{m} \frac{\partial f}{\partial x_i} u_i = o.$$

and then for every φ in K,

$$\bar{D}\varphi = \varphi^D + \sum_{i=1}^{m} \frac{\partial \varphi}{\partial x_i} u_i.$$

The infinite number of conditions above can be reduced to a finite number in the following manner. Since $R = k[z_1, \ldots, z_m]$ is a noetherian ring, the ideal $\mathscr{Y}$ has a finite set $f_1, \ldots, f_s$ of generators so that $f \in \mathscr{Y}$ may be written

$$f = \sum_{i=1}^{s} A_i f_i, \qquad A_i \in R$$

Suppose $f_1, \ldots, f_s$ satisfy the above conditions, then since

$$f^D(x) = \sum_i A_i^D f_i + \sum_i f_i^D A_i$$

$$\frac{\partial f}{\partial x_i} = \sum_j A_j \frac{\partial f_j}{\partial x_i} + \sum_j f_j \frac{\partial A_j}{\partial x_i},$$

we get

$$f^D(x) + \sum_{i=1}^{m} \frac{\partial f}{\partial x_i} u_i = o.$$

We may therefore replace the above by the finitely many conditions

$$f_i^D + \sum_{j=1}^{m} \frac{\partial f}{\partial x_j} u_j = o, i = 1, \ldots, s.$$

We now consider a few special cases. 72

Let $K = k(x)$ be a simple extension of k. Let D be a derivation of k. We will study extensions $\bar{D}$ of D into K.

(1) First let x be transcendental over k. The ideal of x in $k[z]$ is zero. This means that we can prescribe $\bar{D}x$ arbitrarily. Thus for every $u \in K$ there exists one and only extension $\bar{D}$ with

$$\bar{D}x = u$$

(2) Let now x be algebraic over k. Suppose x is inseparable over k. Let $f(z)$ be the minimum polynomial of x in $k[z]$. Then $f(z)$ generates the ideal of x in $k[z]$. But x being inseparable, $f'(x) = o$. This means that D has to satisfy

$$f^D = o.$$

Also, $\bar{D}$ is uniquely fixed as soon as we assign a value u to $\bar{D}x$. This can be done arbitrarily as can be easily seen. Thus there exist an infinity of extensions $\bar{D}$.

(3) Finally, let X be separable. Then $f(z)$, the irreducible polynomial of x over k is such that

$$f'(x) \neq o.$$

Since $f(z)$ generates $\mathscr{Y}$ we must have

$$f^D(x) + f'(x)\bar{D}x = o,$$

or that $\bar{D}x$ is uniquely fixed by D.

$$-\bar{D}x = \frac{f^D(x)}{f'(x)} \tag{*}$$

There is thus only one extension of D to K and it is given by $(*)$.

73 In particular, K has no derivations, except the trivial one, over k.

We shall now prove

Theorem 7. *In order that a finitely generated extension $K = k(x_1, \ldots, x_n)$ be separably algebraic over k, it is necessary and sufficient that K have no non-trivial derivations over k.*

Proof. If K/k is algebraically separable, then since K is finitely generated over k, it follows that $K = k(x)$ for some x and the last of the considerations above shows that K has no nontrivial derivations over k. □

Suppose now K/k has no-trivial derivations. In case $n = 1$, our considerations above show that K/k is separable. Let now $n > 1$ and assume that theorem is proved for $n - 1$ instead of n.

Put

$$K = K_1(x_n) \qquad K_1 = k(x_1, \ldots, x_{n-1}).$$

Then x_n is separably algebraic over K_1. For, if not, let x_1 be inseparable over K_1 or transcendental over K_1. In both cases the zero derivation in K_1 can be extended into a non-trivial deri-vation of K contradictions hypothesis over K.

Thus x_n is separable over K_1. This implies, since K has no derivations over k that K_1 and our theorem is proved.

Note that in the theorem above, the fact that K/k is finitely generated is essential. For instance, if k is an imperfect field and $K = k^{p^{-\infty}}$ then

74 K/k is infinite. Also if $a \in k$ then $a = b^p$ for some $b \in K$. If D is a derivation of K, then

$$Da = Db^p = pb^{p-1}Db = o$$

This proves, in particular, that a perfect field of characteristic $p \neq o$, has only the trivial derivation.

If we take K to be the algebraic closure of the rational number filed then K has only the trivial derivation.

Let $K = k(x, y)$ be an algebraic function field of one variable. Let us assume that x is a separating variable and $\varphi(X, Y)$ the irreducible polynomial of x, y over k. Then if D is a derivation of K over k,

$$\frac{\partial\varphi}{\partial x}Dx + \frac{\partial\varphi}{\partial y}Dy = o$$

so that if we assume that y is separable over $k(x)$, then $\dfrac{\partial\varphi}{\partial y} \neq o$ and hence

$$Dy = \frac{-\frac{\partial\varphi}{\partial x}}{\frac{\partial\varphi}{\partial y}}Dx$$

This shows that the ratio Dy/Dx is independent of D.

Also, for any rational function $\psi(x, y)$ of x, y

$$D\psi = \frac{\partial\psi}{\partial x}Dx + \frac{\partial\psi}{\partial y}Dy$$

which gives,if $Dx \neq o$

$$\frac{D\psi}{Dx} = \frac{\partial\psi}{\partial x} - \frac{\partial\psi}{\partial y}\left(\frac{\frac{\partial\varphi}{\partial x}}{\frac{\partial\varphi}{\partial y}}\right)$$

which is a well known formula in elementary calculus.

We shall now obtain a generalisation of theorem 7 to algebraic function fields.

Let $K = k(x_1, \ldots, x_m)$ be an algebraic function field of dimension n, so that $o \leq n \leq m$. Let $f_1, \ldots, f_s$ be a system of generators of the 75 ideal $\mathscr{Y}$ of polynomials $f(z_1, \ldots, z_m)$ in $k[x_1, \ldots, x_m]$ which vanish for $x_1, \ldots, x_m$. Let $\dfrac{\partial f}{\partial x_i}$ for f in $k[z_1, \ldots, z_m]$ have the same meaning as before.

Denote by M the matrix

$$M = \left(\frac{\partial f}{\partial x_i}\right) \qquad i = 1, \ldots, m$$

$$j = 1, \ldots, s$$

where i is the row index and j the column index. We denote by $\underline{t}$ the rank of the matrix M which is a matrix over K.

Let $V_K(D)$ denote the vector space of derivations of K which are trivial on k. This is a vector space over K. Denote by l the dimension of $V_K(D)$ over K. We then have

Theorem 8. $\boxed{l+ t =m.}$

Proof. For any integer p, denote by W_p the vector space over K of dimension p, generated by p-tuples $(\beta_1, \ldots, \beta_p), \beta_i \in K$. □

Let σ denote the mapping

$$\sigma D = (Dx_1, \ldots, Dx_m)$$

of $V_k(D)$ into W_m. This is clearly a homomorphism of $V_k(D)$ into W_m. The kernel of the homomorphism is the set of D for which $Dx_i = o; i = 1, \ldots, m$. But since K is generated by $x_1, \ldots, x_m$, this implies that $D = o$. Thus $V_k(D)$ is isomorphic to the subspace of W_m formed the vectors

$$(Dx_1, \ldots, Dx_m).$$

Consider now the vector space W_s and let τ be the mapping
76 $(\tau(\alpha_1, \ldots, \alpha_m) = (\alpha_1, \ldots, \alpha_m)M$ of W_m into W_s. Put

$$\beta_j = \sum_{j=1}^{m} \alpha_j \frac{\partial f_i}{\partial x_j}; i = 1, \ldots, s$$

so that

$$(\beta_1, \ldots, \beta_s) = (\alpha_1, \ldots, \alpha_m)M.$$

The rank of the mapping τ is clearly y equal to the rank t of the matrix M. It is the dimension of the image by τ of W_m into W_s. The kernel of the mapping τ is the set of $(\alpha_1, \ldots, \alpha_m)$with

$$\beta_i = o; i = 1, \ldots, s.$$

which, by theorem 6 is clearly isomorphic to the subspace of W_m formed by vectors $(Dx_1, \ldots, Dx_m)$, $D \in V_K(D)$. This, by previous considerations, proves the theorem.

We shall now prove the

Theorem 9. *With the same notations as before, there exist ℓ elements, say $x_1, \ldots, x_1$ of dimension n over k such that $K/k(x_1, \ldots, x_1)$ is a separably algebraic extension.*

Proof. Since the matrix M has rank t, there exists a submatrix of M of t rows and which is non-singular. Choose notation in such a way, that this matrix is

$$P = \left(\frac{\partial f_j}{\partial x_i}\right), \qquad \begin{array}{c} i = m - t + 1, \ldots, m \\ j = s - t + 1, \ldots, s \end{array}$$

Note that $t \leq$ Min (s, m). Let $L = k(x_1, \ldots, x_1)$. Then $K = L(x_{1+p}, \ldots, x_m)$. Let D be a derivation of K over L. Then since $f_j(x_1, \ldots, x_m) = o$, we must have, by theorem 6

$$\sum_{i=1}^{m} \frac{\partial f_j}{\partial x_i} Dx_i = o.$$

But since D is zero on L, 77

$$Dx_i = o, \quad i = 1, \ldots, l.$$

Thus

$$\sum_{i=l+1}^{m} \frac{\partial f_j}{\partial x_i} Dx_i = o.$$

This means that

$$P \begin{pmatrix} Dx_{l+1} \\ \vdots \\ Dx_m \end{pmatrix} = \begin{pmatrix} o \\ \vdots \\ o \end{pmatrix}$$

But since $|P| \neq o$, it follows that $Dx_{l+1} = o \ldots, Dx_m = o$ which shows that $D = o$

But $K = L(x_{l+1}, \ldots, x_m)$ is finitely generated over L. Using theorem 7, it follows that K/L is algebraic and separable. We get incidentally

$$n \leq 1.$$

We now prove the important □

Theorem 10. *Let $K = k(x_1, \ldots, x_m)$ be of dimension n. Then K is separably generated over k, if and only if* $\dim V_K(D) = n$. *In that case there exists, among $x_1, \ldots, x_m$, a separating base of n elements.*

Proof. If $V_K(D)$ has dimension n then theorem 9 shows that there exist n elements $x_1, \ldots, x_n$ among $x_1, \ldots, x_m$ such $K/k(x_1, \ldots, x_n)$ is separably algebraic. □

Suppose now that K/k is separably generated. Let $y_1, \ldots, y_n$ be a separating base so that $K/k(y_1, \ldots, y_n)$ is separably algebraic. $k(y_1, \ldots, y_n)$ has n linearly independent derivations $D_1, \ldots, D_n$ over k defined by

$$D_i y_j = \begin{cases} o, & \text{if } i \neq j \\ 1, & \text{if } i = j \end{cases}$$

78

Since $K/k(y_1, \ldots, y_n)$ is separably algebraic and finite, it follows that each of $D_1, \ldots, D_n$ has a unique extension $\bar{D}_1, \ldots, \bar{D}_n$ to K. Now $\bar{D}_1, \ldots, \bar{D}_n$ are linearly independent over K. For, if

$$\sum_i a_i \bar{D}_i = o, a_i \in K,$$

then

$$\sum_i a_i \bar{D}_i(y_j) = o \text{ for all } j.$$

Hence $a_j = o$ for $j = 1, \ldots, n$. Let now D be a derivation of K/k and let $Dy_i = a_i$. Put

$$\bar{D} = D - \sum_i a_i \bar{D}_i.$$

Then $\bar{D}y_i = o$ for all i. Therefore since $K/k(y_1, \ldots, y_n)$ is separable, $\bar{D} = o$.This proves that

$$\dim V_K(D) = n.$$

and our theorem is completely established.

Let $K = k(x_1, \ldots, x_n, y)$ where k is of characteristic $p \neq o$ and k is an imperfect field. Let y be algebraic over k and be a root of

$$z^p - t$$

$t \in k$. Then K/k is an inseparably generated extension and

$$\dim V_K(D) = n + 1$$

where n is the dimension of K/k.

3 Rational function fields

79

Let us now consider the field $K = k(x)$ of rational functions of one variable. Let y be any element of K. Hence $y = \dfrac{f(x)}{g(x)}$ where f and g are polynomials in x over k. Also K is the quotient field of the ring $L = k[x]$ of polynomials in x.

Assume that $(f(x), g(x)) = 1$, that is that they have no factor in common. Let n be defined by

$$n = \max(\deg f(x), \deg g(x)).$$

If $n = o$, then clearly $f \in k$, $g \in k$ and so $y \in k$. Let us assume that $n \neq o$ so that at least at least one of f and g is a non-constant polynomial. n is called the degree of y.

Let $F = k(y)$ be the field generated over k by y.

Then x satisfies over F the polynomial

$$\varphi(z) = f(z) - yg(z).$$

$\varphi(z)$ is not a constant polynomial over $k(y)$. For, let

$$\left.\begin{aligned} f(z) &= \sum_{i=o}^{1} a_i z^i \\ g(z) &= \sum_{i=o}^{m} b_i z^i \end{aligned}\right\} a_i, b_i \in k.$$

Then $n = \max(1, m)$. The coefficient of z^n in $\varphi(z)$ is

$$\begin{cases} a_1 & \text{if} \quad 1 > m \\ a_1 - yb_1 & \text{if} \quad 1 = m \\ -yb_m & \text{if} \quad 1 < m \end{cases}$$

In every case, it follows that since y is not in k, $\varphi(z)$ is a non-constant polynomial. Since $\varphi(z)$ has degree n in z, it follows that

$$(K : F) \leq n.$$

80 We assert that $\varphi(z)$ is irreducible over F. For, if it is reducible over $F[z]$, then since $F = k(y)$, it will be reducible over $k[y, z]$. So let $\varphi(z) = \psi_1(y, z)\ \psi_2(y, z)$ in $k[y, z]$. Since $\varphi(z)$ is linear in y it follows that one of $\psi_1$or ψ_2 has to be independent of y. But then since $(f(z), g(z)) = 1$, $\varphi(z)$ is a primitive polynomial in y over $k[z]$. Therefore $\varphi(z)$ is irreducible. This means that

$$(K : F) = n$$

It proves, in particular that y is transcendental over k. Hence

Theorem 11. *k is algebraically closed in $k(x)$.*

We can extend it to the case where $K = k(x_1, \ldots, x_n)$ is a purely transcendental extension of dimension $\underline{n}$. We use induction on $\underline{n}$. Theorem 11 proves that $n = 1$, k is algebraically closed in $k(x)$. Let, for $n - 1$ instead of n, instead of n, it be proved that k is algebraically closed in the purely transcendental extension $k(x_1, \ldots, x_{n-1})$. Let $K = k(x_1, \ldots, x_n)$ be of dimension $\underline{n}$.

Let z in K be algebraic over k. Then $z \in K = K_1(x_n)$, $K_1 = k(x_1, \ldots, x_{n-1})$. Therefore by theorem 11 since z is algebraic over K_1, $z \in K_1$. By induction hypothesis, $z \in k$.

Thus

Corollary. *If $K = k(x_1, \ldots, x_n)$ has dimension n over k, then k is algebraically closed in K*

It is easy to extend this to the case where K is a purely transcendental extension of any transcendence degree.

Since $K = k(x)$, we call x a *generator* of K over k. Let y also be a generator so that $K = k(y)$. Then **81**

$$(k(x) : k(y)) = 1$$

which shows by our considerations leading to theorem 11 that

$$y = \frac{a(x)}{b(x)}$$

where $a(x)$ and $b(x)$ are coprime and have at most the degree 1 in x. Thus

$$y = \frac{\lambda x + \mu}{\nu x + \rho}$$

where λ, μ, ν, ρ are in k and since y is transcendental over k,

$$\lambda\rho - \mu\nu \neq 0.$$

An automorphism of K which is identity on k, is uniquely fixed by its effect on x. If it takes x into y then x and y are related as above. If x and y are related as above, then the mapping which assigns to x the element y is an automorphism.

If we consider the group of two rowed non-singular matrices, with elements in k, then each matrix gives rise to an automorphism of K/k. Obviously two matrices σ and τ give rise to the same automorphism if and only if $\sigma = \lambda\tau$ for some $\lambda \neq o$ in k. Hence

Theorem 12. *The group of automorphisms of $K = k(x)$ over k is isomorphic to the factor group of the group of two rowed matrices over k modulo the group of matrices λE, $\lambda \neq 0 \in k$ and E is the unit matrix of order 2.*

We shall call this group P_2.

82 From theorem 11, it follows that if L is an intermediary field between K and k then L is transcendental over k. But much more is true as in shown by the following theorem of Luroth.

Theorem 13. *If $K = k(x)$ is a simple transcendental extension of k and $k \subset L \subset K$, $L = K(\omega)$ for some $\omega \in K$.*

Proof. We shall assume that $L \neq k$ so that L is transcendental over k and contains an element t, transcendental over k andy by considerations leading to theorem 11, we have $K/k(t)$ is finite algebraic. Since $L \supset k(t)$, it follows that

$$(K : L) < \infty$$

Let x satisfy over L the irreducible polynomial

$$f(z) = z^n + a_1 z^{n-1} + \cdots + a_n$$

where $a_1, \ldots, a_n \in L$ and $n = (K : L)$. At least one a_i is not in k since x is transcendental over k. The $a_i's$ are rational functions of x. So we may write

$b_0(x) f(z) = f(x, z) = b_0(x) z^n + b_1(x) z^{n-1} + \cdots + b_n(x)$ where $b_0(x), \ldots, b_n(x)$ are polynomials in x and $f(x, z)$ is a primitive polynomial in z over $k[x]$. Let m be the maximum of the degrees of $b_0(x)$, $\ldots b_n(x)$. Let a_i be not in k. Then

$$a_i = \frac{b_i(x)}{b_0(x)}$$

so that degree $a_i \leq m$. Since $a_i \in L$ and $L \supset k(a_i)$, it follows that

$$n \leq m$$

Let us write w instead of a_i. Then $w = \dfrac{b_i(x)}{b_0(x)}$. □

83 Let $w = h(x)/g(x)$ where $(h(x), g(x)) = 1$. Then $L \supset k(w)$.

Also x satisfies over $k(w)$ the polynomial

$$h(z) - wg(z)$$

so that since $f(z)$ is irreducible, it follows that $f(z)$ divides $h(z) - wg(z)$, which is a polynomial of degree $\leq m$ in z. Let us therefore write

$$h(z) - wg(z) = \frac{f(x,z)}{b_o(x)} \frac{\varphi(x,z)c_1(x)}{c_o(x)}$$

where $\varphi(x,z)$ is a primitive polynomial in z over $k[x]$. We therefore get on substituting the $w = \dfrac{h(x)}{g(x)}$,

$$h(z)g(x) - g(z)h(x) = \frac{g(x)c_1(x)}{b_o(x)c_o(x)}.f(x,z)\varphi(x,z).$$

The left hand side being a polynomial in x and z, f and φ being primitive polynomials in z over $k[x]$, it follows that

$$h(z)g(x) - g(z)h(x) = f(x,z)\varphi_1(x,z)$$

where $\varphi_1(x,z) \in k[x,z]$. We now compare degrees in x and z on both sides of the above identity. On the right hand side the degree in x is $\geq m$ since one of $b_o(x), \ldots, b_n(x)$ has degree m. Therefore the left side has degree in $x \geq m$. But the degree in x equals degree of $w \leq m$. Thus degree of $w = m$. Since the left side is symmetrical in z and x,it follows that it has degree m in z. Therefore φ_1 has to be independent of x.

Hence $h(z) - wg(z) = f(z)\varphi(z)$, $\varphi(z)$ being independent of x. This can happen only if $\varphi(z)$ is a constant. This proves that

$$n = m.$$

Now $(K : k(w)) = m = (K : L)$ and $L \supset k(w)$. Thus 84

$$L = k(w)$$

and our theorem is proved.

The analogue of Luroth's theorem for $K = k(x_1, \ldots, x_n)$ is not known for $n > 1$.

Let $K = k(x)$ and let G be a finite granite group of automorphism of K/k. If L is the fixed field of G, then K/L is a finite extension of degree equal to order of G. By Luroth's theorem $L = k(y)$ for some y. Thus

$$\text{degree } y = \text{ order of } G.$$

For instance, let G be the finite group of automorphisms of $K = k(x)$ defined by

$$x \to x, x \to 1-x, x \to \frac{1}{x}, x \to 1-\frac{1}{x}, x \to \frac{1}{1-x}, x \to \frac{x}{x-1}$$

This is a group of order 6 and the fixed field will be $k(y)$ where $k(y)$ consists of all rational functions $f(x)$ of x with

$$f(x) = f(1-x) = f(\frac{1}{x}) = f(1-\frac{1}{x}) = f(\frac{1}{1-x}) = f(\frac{x}{1-x}).$$

We have only to find a rational function of degree 6 which satisfies the above conditions. The function

$$f(x) = \frac{(x^2-x+1)^3}{x^2(x-1)^2}$$

satisfies the above conditions and so $y = f(x)$.

Theorem 14. *If G is any finite subgroup of P_2 of linear transformations*

$$x \to \frac{ax+b}{cx+d}$$

85 *$a, b, c, d \in k$, $ad - bc \neq 0$ then there exists a rational function $f(x)$ such that every function $\varphi(x)$ which is invariant under G is a rational function of $f(x)$. $f(x)$ is uniquely determined up to a linear transformation*

$$\frac{\lambda f(x) + \mu}{V f(x) + \rho}$$
$$\lambda, \mu, \nu\rho \in k, \quad \lambda\rho - \mu\nu \neq 0.$$

We now consider the case of a rational function field $K = k(x_1, \ldots x_n)$ of n variables. Let G be a finite group of automorphisms of K which are trivial on k and let L be the fixed field of G. Clearly L has transcendence degree n over k. It is *not known*, except in simple cases, whether L is a purely transcendental extension of k or not. We shall, however, consider the the case where G is the symmetric group on n

symbols. So $G \simeq S_n$. Let G operate on K in the following manner. If σ is an element of S_n, then σ is a permutation

$$\sigma = \begin{pmatrix} 1, 2, 3, \ldots, n \\ \sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n \end{pmatrix}.$$

We define σ on K by

$$\sigma x_i = x_{\sigma_i};\ 1, \ldots, n.$$

We then obtain a faithful representation of S_n on K and we denote this group again by S_n. An element of k which is fixed under S_n and which therefore is in L is called a *symmetric function* of $x_1, \ldots, x_n$. Obviously

$$(K : L) = n!$$

and the galois group of K/L is S_n. **86**

Consider the polynomial

$$f(z) = (z - x_1) \ldots (z - x_n).$$

Since every permutation in S_n leaves $f(z)$ fixed, it follows that $f(z) \in L[z]$. Let us write

$$f(z) = z^n - s_1 z^{n-1} + s_2 z^{n-2} - \cdots + (1)^n s_n$$

where

$$s_i = \sum_{1 \leq t_1 < t_2 < \ldots < t_i \leq n} x_{t_1} \cdots x_{t_i}.$$

The quantities $s_1, \ldots, s_n$ are called the *elementary symmetric functions* of $x_1, \ldots x_n$. Put $L_1 = k(s_1, \ldots, s_n)$. Then $L_1 \subset L$. Also $f(z)$ is a polynomial in $L_1\{z\}$ and is irreducible over it. $f(z)$ is separable and K is the splitting field of $f(z)$ over L_1. Thus K/L_1 is galois. Since $f(z)$ is of degree n

$$(K : L_1) \leq n!$$

Since $L \supset L_1$, it follows that $L = L_1$ and

$$L = k(s_1, \ldots, s_n).$$

We have therefore the

Theorem 15. *Every rational symmetric function of $x_1, \ldots, x_n$ is a rational function over k of the elementary symmetric functions $s_1, \ldots, s_n$.*

Incidentally since L/k has dimension n, the elementary symmetric functions $s_1, \ldots, s_n$ are algebraically independent over k.

Chapter 4

Norm and Trace

1 Norm and trace

87 Let K/k be a finite extension and let $\omega_1, \ldots, \omega_n$ be a base of K/k so that every $\omega \in K$ may be written

$$\omega = \sum_i a_i \omega_i$$

$a_i \in k$. By means of the regular representation

$$\omega \to A_\omega$$

where $A_\omega = (a_{ij})$ is an $n-$ rowed square matrix with

$$\omega\omega_i = \sum_j a_{ij}\omega_j \qquad i = 1, \ldots, n$$

the field K becomes isomorphic to the subalgebra formed by A_ω in the algebra $\mathfrak{m}_n(k)$ of n rowed matrices over k. We denote by $N_{K/k}\omega$, $S_{K/K}\omega$ the *norm* and *trace* respectively of $\omega \in K$ over k and they are defined by

$$\begin{aligned} N_{K/k}\omega &= |A_\omega| \\ S_{K/k}\omega &= \text{trace } A_\omega. \end{aligned}$$

Defined as such, it follows that

$$N_{K/k}\omega\omega' = N_{K/k}\omega \,.\, N_{K/k}\omega'$$
$$S_{K/k}(\omega + \omega') = S_{K/k}\omega + S_{K/k}\omega'$$

for ω, $\omega' \in K$. Obviously $\omega \to N_{K/k}\omega$ is a homomorphism of K^* into K^* and similarly $\omega \to S_{K/k}\omega$ is a homomorphism of K^+, the additive group, into k^+.

Let $\omega'_1, \ldots, \omega'_n$ be any other basis of K/k. Then

$$\begin{pmatrix} \omega'_1 \\ \vdots \\ \omega'_n \end{pmatrix} = P \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}$$

88 where P is a non-singular matrix in $\mathfrak{m}_n(k)$. Since

$$\omega \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A_\omega \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}$$

it follows that

$$\omega \begin{pmatrix} \omega'_1 \\ \vdots \\ \omega'_n \end{pmatrix} = PA'_\omega P^{-1} \begin{pmatrix} \omega'_1 \\ \vdots \\ \omega'_n \end{pmatrix}$$

which shows that by means of the new basis the matrix associated to ω is B_ω where

$$B_\omega = PA_\omega P - 1$$

and then we have

$$| \; B_\omega \; | = |A_\omega|$$
$$\text{Trace } B_\omega = \text{ Trace } A_\omega.$$

This shows that $N_{K/k}\omega$ and $S_{K/k}\omega$ are invariantly defined and do not depend on a basis of K/k.

We write

$$f_{K/k}(x) =\mid xE - A_\omega \mid$$

and call it the *characteristic polynomial* of ω. Obviously $f_{K/k}(0) = (-1)^n \mid A_\omega \mid$ so that

$$N_{K/k}\omega = (-1)^n f_{K/k}(0) = (-1)^n a_n. \tag{1}$$

We also see easily that

$$S_{K/k}\omega = -a_1 \tag{2}$$

where

$$f_{K/k}(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

$a_1, \ldots, a_n \in k$.

Let $k \subset L \subset K$ be a tower of finite extensions. Let $(K : L) = m$ and let $\Omega_1, \ldots, \Omega_m$ be a basis of K/L. Similarly let $(L : k) = n$ and let **89**
$\omega_1, \ldots, \omega_n$ be a base of L/k. Then $(\omega_1\Omega_1, \ldots, \omega_n\Omega_m)$ is a base of K/k. Let $\omega \in L$ and consider the matrix of ω by the regular representation of K/k in terms of the base $(\omega_1\Omega_1, \ldots, \omega_n\Omega_m)$. Call it $\overline{A}_\omega$.

Then it is trivial to see that

$$\overline{A}_\omega = \begin{pmatrix} A_\omega & 0 \\ \multicolumn{2}{c}{\cdots\cdots\cdots} \\ \multicolumn{2}{c}{\cdots\cdots\cdots} \\ 0 & A_\omega \end{pmatrix}$$

a matrix of mn rows and columns. Therefore

$$\begin{aligned} N_{K/k}\omega &=\mid \overline{A}_\omega \mid (N_{K/k}\omega)^{(K:L)} \\ S_{K/k}\omega &= (K : L) S_{K/k}\omega \end{aligned}$$

Also the characteristic polynomials of ω as belonging to L and to K respectively are $f_{L/k}(x)$ and $f_{K/k}(x)$ and they are related by

$$f_{K/k}(x) = (f_{L/k}(x))^{(K:L)}, \tag{3}$$

In particular let $L = k(\omega)$. Then $f_{L/k}(x)$ is the minimum polynomial of ω. We, therefore, have the

Theorem 1. *If K/k is a finite extension and $\omega \in K$, $\varphi(x)$ its minimum polynomial over k and $f(x)$ its characteristic polynomial, then*

$$f(x) = (\varphi(x))^r$$

where $r = (K : k(\omega))$.

From our formulae above, it follows that we can compute the norm and trace of ω in K from a knowledge of its minimum polynomial.

90 Let now K/k be a finite extension and ω an element of K. Let $[K : k(\omega)] = m'$, $[k(\omega) : k] = n'$ be the degrees of separability of K over $k(\omega)$ and $k(\omega)$ over k respectively. Then K/k has $m'n'$ distinct k-isomorphisms in an algebraic closure Ω of k. Let $\left\{\sigma_{ij}\right\},\ {}_{\substack{i=1,\ldots,n'\\ j=1,\ldots,m'}}$, be these isomorphisms and let notation be so chosen that $\sigma_{i1}, \ldots, \sigma_{im}$, have the same the same effect on $k(\omega)$. Then we may take $\sigma_{11}, \sigma_{12}, \ldots, \sigma_{n'1}$ as a complete system of distinct isomorphisms of $k(\omega)/k$ in Ω.

By our considerations above $f_{k(\omega)/k}(x)$ is the polynomial of ω as well as the characteristic polynomial of ω in $k(\omega)/k$. If $f_{K/k}(x)$ is the characteristic polynomial of ω in k, then

$$f_{K/k}(x) = (f_{k(\omega)/k}(x))^{(K:k(\omega))} \tag{4}$$

Now, because of the properties of the isomorphisms σ_{ij}

$$\prod_{i=1}^{n'}\prod_{j=1}^{m'}(x - \sigma_{ij}\omega) = \prod_{i=1}^{n'}(x - \sigma_{i1}\omega)^{m'}. \tag{5}$$

But since $f_{k(\omega)/k}(x)$ is the minimum polynomial of ω, we have

$$f_{k(\omega)/k}(x) = \left\{\prod_{i=1}^{n'}(x - \sigma_{i1}\omega)\right\}^{\{k(\omega):k\}}$$

where $\{k(\omega) : k\}$, as usual, denotes the degree of inseparability of $k(\omega)$ over k. Using (5) we get

$$\left\{\prod_{i,j}(x - \sigma_{ij}(\omega)\right\}^{\{k:k\}} = \left\{\prod_{i=1}^{n'}(x - \sigma_{i1}\omega)\right\}^{m'\{K:k\}}.$$

But $\{K : k\} = \{K : k(\omega)\} \cdot \{k(\omega) : k\}$ so that

$$\left\{\prod_{i,j}(x - \sigma_{ij}\omega)\right\}^{\{K:k\}} = \{f_{k(\omega)/k}(x)\}^{m'\{K:k(\omega)\}}$$

which proves that 91

$$\boxed{f_{K/k}(x) = \left\{\prod_{\sigma}((x - \sigma\omega)\right\}^{\{K:k\}}} \tag{6}$$

where σ runs through all the distinct isomorphisms of $k(\omega)$ in Ω. Using (1) and (2) we get

$$N_{K/k}\omega = \left\{\prod_{\sigma} \omega^{\sigma}\right\}^{\{K:k\}} \tag{7}$$

ω^{σ} is a conjugate of ω. Similarly

$$S_{K/k}\omega = \{K : k\} \sum_{\sigma} \omega^{\sigma}. \tag{8}$$

If K/k is inseparable, then $\{K : k\} = p^t$, $t \geq 1$ so that for every $\omega \in K$

$$S_{K/k}\omega = o.$$

On the other hand, suppose K/k is finite and separable. Let $\sigma_1, \ldots, \sigma_n$ be all the distinct isomorphisms of K/k in Ω, an algebraic closure of K. Then $n = (K : k)$ and since $\sigma_1, \ldots, \sigma_n$ are independent k-linear functions of K/k in Ω, it follows that

$$\sigma = \sigma_1 + \cdots + \sigma_n$$

is a non - trivial $k-$linear function of K/k in Ω. Therefore there exists a $\omega \in K$ such that $\sigma\omega \neq 0$. But by formula (8),

$$\sigma\omega = \omega^{\sigma_1} + \ldots + \omega^{\sigma_n} = S_{K/k}\omega$$

so that we have the

Theorem 2. *A finite extension K/k is separable, if and only if there exist in K an element whose trace over k in not zero.*

In case k has characteristic zero, or k has characteristic $p \nmid n = (K : k)$, the unit element 1 in k has trace $\neq o$. In order to obtain an element ω in K with $S_{K/k}\omega \neq 0$, in every case we proceed thus: 92

Let K/k be separable and $K = k(\alpha)$ for an element α. Let $\varphi(x)$ be its irreducible polynomial over k and

$$\varphi(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

It follows then that

$$\frac{x^{n-1}}{\varphi(x)} = \sum_i \frac{\alpha_i^{n-1}}{\varphi'(\alpha_i)} \frac{1}{x - \alpha_i}.$$

Comparing coefficients of x^{n-1} on both sides we get

$$\sum_i \frac{\alpha_i^{n-1}}{\varphi'(\alpha_i)} = 1.$$

If we put $\omega = \dfrac{\alpha^{n-1}}{\varphi'(\alpha)}$ and observe that $\varphi'(\alpha) \in K$, we get

$$S_{K/K}\omega = 1.$$

Using formula (6), it follows that if $k \subset L \subset K$ is a tower of finite extensions and $\omega \in K$, then

$$N_{K/k}\omega = N_{L/k}(N_{K/L}\omega)$$
$$S_{K/k}\omega = S_{L/k}(S_{K/L}\omega)$$

We now give a simple application of formula (7) to finite fields.

Let k be a finite field of $q = p^a$ elements so that p is the characteristic of k. Let K be a finite extension of k so that $(K : k) = n$. Then K has

q^n elements. The galois group of K/k is cyclic of order n. Let σ be the Frobenius automorphism. Then for $\omega \in K$,

$$\omega^{\sigma} = \omega^{q}.$$

93

The norm of ω is

$$\begin{aligned} N_{K/k}\omega &= \omega \cdot \omega^{\sigma} \cdot \omega^{\sigma^2} \cdots \omega^{\sigma^{n-1}} \\ &= \omega^{\dfrac{q^n-1}{q-1}}. \end{aligned}$$

Since K^* has $q^n - 1$ elements,

$$\alpha^{q^n-1} = 1$$

for all $\alpha \in K^*$. Since K^* is a cyclic group, the number of elements in K^* with

$$\alpha^{\dfrac{q^n-1}{q-1}} = 1$$

is precisely $q^n - 1/q - 1$, since $q - 1$ divides $q^n - 1$.

Now $\omega \to N_{K/k}\omega$ is a homomorphism of K^* into k^* and the kernel of the homomorphism is the set of ω in K^* with

$$1 = N_{K/k}\omega = \omega^{\dfrac{q^n-1}{q-1}}.$$

By the first homomorphism theorem we have, since k^* has only $q-1$ elements, the

Theorem 3. *If K/k is finite and k is a finite field, then every non-zero element of k is the norm of exactly $(K^* : k^*)$ elements of K.*

It is clear that this theorem is not in general true if k is an infinite field.

2 Discriminant

Let K/k be a finite extension and $\omega_1, \ldots, \omega_n$ a basis of K/k. Suppose σ is a k-linear map of K into k, that is 94

$$\begin{aligned} &\sigma(\omega) \in k \\ &\sigma(\omega + \omega') = \sigma\omega + \sigma\omega' \\ &\sigma(\lambda) = \lambda\sigma(\omega) \end{aligned}$$

where $\omega, \omega' \in K$, $\lambda \in K$. Let M^σ denote the matrix

$$M^\sigma = (\sigma(\omega_i \omega j))$$

of n rows and columns. We denote by $D_{K/k}\sigma(\omega_1, \ldots, \omega_n)$ its determinant and call it the σ- *discriminant of the basis* $\omega_1, \ldots, \omega_n$ of K/k. If $\omega'_1, \ldots, \omega'_n$ is another basis, then

$$\begin{pmatrix} \omega'_1 \\ \vdots \\ \omega'_n \end{pmatrix} = P \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}$$

where P is an n rowed non-singular matrix with elements in k.

If $P = (p_{ij})$ then

$$\omega'_i = \sum_j p_{ij}\ \omega_j$$

so that

$$\sigma(\omega'_a \omega'_b) = \sum_{i,j} p_{ai} p_{bj} \sigma(\omega_i \omega_j)$$

which proves that

$$D^\sigma_{K/k}(\omega'_1, \ldots, \omega'_n) = |P|^2 D^\sigma_{K/k}(\omega_1, \ldots, \omega_n).$$

Therefore $D^\sigma_{K/k} = 0$ if it is zero for some basis.

We now prove

Theorem 4. *If $\omega_1, \ldots, \omega_n$ is a basis of K/k and σ a k-linear map of K into k, then*

$$D^{\sigma}_{K/k}(\omega_1, \ldots, \omega_n) = 0$$

95 *if and only if σ is the zero linear mapping.*

Proof. If σ is the zero linear map, that is, one that assigns to every element ω in K, the zero element, then $D^{\sigma}_{K/K} = 0$. Now let $D^{\sigma}_{K/k} = 0$. This means that the matrix M^{σ} with elements in k has determinant zero. Therefore there exist $a_1, \ldots, a_n$ in k, not all zero, such that

$$M^{\sigma}\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

This means that

$$\sum_{j=1}^{n} \sigma(\omega_i\omega_j)a_j = 0; \quad 1 = 1, \ldots, n.$$

If we put $z = \sum\limits_j a_j\omega_j$. then we have

$$\sigma(\omega_i z) = 0, i = 1, \ldots, n.$$

□

Let ω be any element in K. Since $a_1, \ldots, a_n$ are not all zero, $z \neq 0$ and so put

$$\frac{\omega}{z} = b_1\omega_1 + \cdots + b_n\omega_n, b_i \in k.$$

Then $\sigma(\omega) = \sigma\left(\frac{\omega}{z} \cdot z\right) = \sum\limits_i b_i\sigma(\omega_i z) = o$. This proves that σ is the trivial map.

The mapping $\omega \to S_{K/K}\omega$ is also a k-linear map of K into k. For a basis $\omega_1, \ldots, \omega_n$ of K/k we call

$$D_{K/k}(\omega_1, \ldots \omega_n) = |(S_{k/K}(\omega_i\omega_j))|$$

the *discriminant of the basis* $\omega_1, \ldots \omega_n$. Using theorem 2 and theorem 4, we get

Theorem 5. *Discriminant of a base of K/k is not zero if and only if K/k is separable.*

96 Let K/k be finite separable. Let $\sigma_1, \ldots, \sigma_n$ be the distinct k-isomorphisms of K over k in Ω. Then

$$S_{K/k}\omega = \sum_i \omega^{\sigma_i}.$$

Therefore

$$D_{K/k}(\omega_1, \ldots, \omega_n) = \begin{vmatrix} \omega_1^{\sigma_1}, & \omega_1^{\sigma_2}, & \ldots, & \omega_1^{\sigma_n} \\ & \vdots & & \\ \omega_1^{\sigma_1}, & \ldots & \ldots, & \omega_1^{\sigma_n} \end{vmatrix}^2. \tag{9}$$

Since K/k is finite separable, $K = k(\omega)$ for some ω. Also $1, \omega, \omega^2, \ldots, \omega^{n-1}$ form a base of K/k and we have

$$D(1, \omega, \ldots, \omega^{n-1}) = \begin{vmatrix} 1, & \ldots, & 1 \\ \omega^{\sigma_1}, & \ldots, & \omega^{\sigma_1} \\ \cdots & \cdots & \cdots \\ (\omega^{n-1})^{\sigma_1}, & \ldots, & (\omega^{n-1})^{\sigma_n} \end{vmatrix}.$$

Also, $D(1, \omega, \ldots, \omega^{n-1})/D(\omega_1, \ldots, \omega_n)$ is the square of an element of k. The determinant

$$\begin{vmatrix} 1, & \ldots, & 1 \\ \omega^{\sigma_1}, & \ldots, & \omega^{\sigma_n} \\ \cdots & \cdots & \cdots \\ (\omega^{n-1})^{\sigma_n}, & \ldots, & (\omega^{n-1})^{\sigma_n} \end{vmatrix}$$

is the called Van-der-Monde determinant. We call $D(1, \omega, \ldots, \omega^{n-1})$ is the *discriminant* of ω and denote it by $D_{K/k}(\omega)$.

Let $f(x)$ be the minimum polynomial of ω. Then $f(x) = (x - \omega^{\sigma_1}) \ldots (x - \omega^{\sigma_n})$. Since $f'(\omega) \neq 0$, we have

$$f'(\omega) = (\omega^{\sigma_1} - \omega^{\sigma_2})(\omega^{\sigma_1} - \omega^{\sigma_3}). \ldots .(\omega^{\sigma_1} - \omega^{\sigma_n})$$

and is an element of K. We call it the *different* of ω and denote it $d_{K/k}(\omega)$. Also the Vander - monde determinant shows that

$$\boxed{D_{K/k}(\omega) = (-1)^{n(n-1)2} N_{K/k}(d_{K/k}\omega)}$$

97 Suppose K/k is a finite galois extension. Let $\sigma_1, \ldots, \sigma_n$ be the distinct automorphisms of K/k. We shall now prove

Theorem 6. *If k contains sufficiently many elements, then there exists in K an element ω such that $\omega^{\sigma_1}, \ldots, \omega^{\sigma_n}$ form a basis of K over k.*

Proof. It $\omega \in K$ such that

$$D(\omega^{\sigma_1}, \ldots, \omega^{\sigma_n}) \neq o$$

then $\omega^{\sigma_1}, \ldots, \omega^{\sigma_n}$ form a base of K/k. For,if

$$\sum_i a_i \omega^{\sigma_i} = o, \quad a_1, \ldots, a_n \in k$$

not all zero, then since $\sigma_1, \ldots, \sigma_n$ form a group

$$\sum_i a_i \omega^{\sigma_j \sigma_i} = o, \quad j = 1, \ldots, n.$$

Therefore from the expression (9) for $D_{K/k}(\omega^{\sigma_1}, \ldots, \omega^{\sigma_n})$, it follows that

$$(S_{K/k}(\omega^{\sigma_i}\omega^{\sigma_j})) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} o \\ \vdots \\ o \end{pmatrix}$$

or that $D(\omega^{\sigma_1}, \ldots, \omega^{\sigma_n}) = o$ which is a contradiction. We have therefore to find an ω with this property. Put

$$\omega^{\sigma_i} = x_1 \omega_1^{\sigma_i} + \cdots + x_n \omega_n^{\sigma_i}, \quad i = 1, 2, \ldots$$

where $x_1, \ldots, x_n$ are indeterminates and $\omega_1, \ldots, \omega_n$ is a basis of K/k □

Then

$$\begin{aligned} S_{K/k}(\omega^{\sigma_i}\omega^{\sigma_j}) &= \omega^{\sigma_1\sigma_i}\omega^{\sigma_1\sigma_j}, + \cdots + \omega^{\sigma_n\sigma_i}\omega^{\sigma_n\sigma_j} \\ &= \sum_{a,b} S_{K/k}(\omega_a^{\sigma_i}\omega_b^{\sigma_j}) x_a x_b. \end{aligned}$$

Then $D_{K/k}(\omega^{\sigma_1}, \ldots, \omega^{\sigma_n})$ defined as the determinant of the matrix 98 $(S_{K/k}(\omega^{\sigma_i}\omega^{\sigma_j}))$ is a polynomial in $x_1, \ldots, x_n$ with coefficients in k.

In order to prove that $D_{K/k}(\omega^{\sigma_1}, \ldots, \omega^{\sigma_n})$ is non-zero polynomial, notice that by definition,

$$\begin{pmatrix} \omega^{\sigma_1} \\ \vdots \\ \omega^{\sigma_n} \end{pmatrix} = \begin{pmatrix} \omega_1^{\sigma_1}, & \omega_2^{\sigma_1}, & \ldots, & \omega_n^{\sigma_1} \\ \cdots & \cdots & \cdots & \cdots \\ \omega_1^{\sigma_n}, & \omega_2^{\sigma_n}, & \ldots, & \omega_n^{\sigma_n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

so that if $\omega^{\sigma_1} = 1$ and $\omega^{\sigma_i} = o$ for $i > 1$, then $x_1, \ldots, x_n$ are not all zero and for this set of values of $x_1, \ldots, x_n$, the polynomial $D_{K/k}(\omega^{\sigma_1}, \ldots, \omega^{\sigma_n})$ has a value $\neq o$, as can be see from the fact that

$$D_{K/k}(\omega^{\sigma_1}, \ldots, \omega^{\sigma_n}) = \begin{vmatrix} \omega^{\sigma_1}, & \ldots, & \omega^{\sigma_n} \\ \cdots & \cdots & \cdots \\ \omega^{\sigma_n\sigma_i}, & \ldots, & \omega^{\sigma_n\sigma_n} \end{vmatrix}^2$$

Therefore if k has sufficiently many elements, there exist values in k of $x_1, \ldots, x_n$, not all zero, such that $D_{K/k}(\omega^{\sigma_1}, \ldots, \omega^{\sigma_n}) \neq o$.

This proves the theorem

In particular, if k is an infinite field, there exists a base of K/k consisting of an element and its conjugates. Such a base is said to be a *normal base*.

The theorem is also true if k is a finite field.

Chapter 5

Composite extensions

1 Kronecker product of Vector spaces

99 Let V_1 and V_2 be two vector spaces over a field k and $V_1 \times V_2$ their cartesian product. If W is any vector space over k, a bilinear function $f(x, y)$ on $V_1 \times V_2$ is, by definition, a function on $V_1 \times V_2$ into W such that for every $x \in V_1$ the mapping $\lambda_x : y \to f(x, y)$ is a linear function on V_2 into W and for every $y \in V_2$ the function $\mu_y : x \to f(x, y)$ is a linear function on V_1 to W.

A Vector space T over k is said to be a *Kronecker product* or tensor product of V_1 and V_2 over k, if there exists a bilinear function θ on $V_1 \times V_2$ into T such that

1) T is generated by $\theta(V_1 \times V_2)$

2) if V_3 is any vector space over k, then for every bilinear function φ on $V_1 \times V_2$ into V_3 there exists a linear function σ on T into V_3 such that $\sigma\theta = \varphi$.

This is shown by the commutative diagram

$$\begin{tikzcd}
V_1 \times V_2 \arrow[rr, "\varphi"] \arrow[dr, "\theta"'] & & V_3 \\
& T \arrow[ur, "\sigma"'] &
\end{tikzcd}$$

We shall now prove the

Theorem 1. *For any two vector spaces V_1 and V_2 over k there exists one and upto k-isomorphism only one Kronecker product T of V_1 and V_2 over k.*

100 *Proof.* The uniqueness is easy to establish. For, let T_1 and T_2 be two vector spaces satisfying the conditions 1) and 2). Let T_1 be generated by $\theta_1(V_1 \times V_2)$ and T_2 by $\theta_2(V_1 \times V_2)$. Let σ be the linear map of T_1 into T_2 such that $\sigma \cdot \theta_1 = \theta_2$ and τ the linear map of T_2 into T_1 such that $\tau \cdot \theta_2 = \theta_1$. Since $\theta_1(V_1 \times V_2)$ generates T_1 we see that $\tau \cdot \sigma$ is identity on T_1. Similarly $\sigma \cdot \tau$ is identity on T_2. Thus σ and τ are isomorphisms onto. □

We now prove the existence of the space T.

Let V be the vector space formed by finite linear combinations

$$\sum a_{xy}(x,y)$$

$a_{xy} \in k$ and $(x,y) \in V_1 \times V_2$. Every bilinear function f on $V_1 \times V_2$ into V_3 can be extended into a linear function $\overline{f}$ of V into V_3 by the prescription

$$\overline{f}\Big(\sum a_{xy}(x,y)\Big) = \sum a_{x,y} f(x,y)$$

Let W be the subspace of V generated by elements of the type

$$\begin{gathered}(x+x^1,y)-(x,y)-(x^1,y)\\(x,y+y^1)-(x,y)-(x,y^1)\\(ax,y)-a(x,y)\\(x,by)-b(x,y)\end{gathered}$$

where x, $x^1 \in V_1$; y, $y^1 \in V_2$ and a, $b \in k$. W is independent of V_3. Also if f is a bilinear function on $V_1 \times V_2$, its extension $\overline{f}$ on V vanishes on W. Furthermore if f is any linear function on V vanishing on W, 101 its restriction to $V_1 \times V_2$ is a bilinear function. It is then clear that the space of bilinear functions on $V_1 \times V_2$ is isomorphic to the space of linear functions on V which vanish on W. If σ is any linear function on V/W into V_3 and θ the natural homomorphism of V on V/W then $\sigma \cdot \theta$ is a linear function on V vanishing on W. Also $\sigma \to \sigma \cdot \theta$ is an isomorphism of the space of linear functions on V/W into V_3 on the space of linear functions on V vanishing on W. θ is clearly a bilinear function on $V_1 \times V_2$ into $T = V/W$ and furthermore, by definition of V, V/W is generated by $\theta(V_1 \times V_2)$. Thus T is the required space.

By taking k itself as a vector space over k, we have

Theorem 2. *The space of bilinear functions on $V_1 \times V_2$ into k is isomorphic to the dual of the Kronecker product T.*

We denote by $V_1 \otimes_k V_2$ the kronecker product space. When there is no doubt about the field over which the kronecker product is taken we will simply write $V_1 \otimes V_2$.

If $T = V_1 \otimes V_2$ we denote by $x \otimes y$ the element in T which corresponds to (x, y) by the bilinear function θ on $V_1 \times V_2$ into T. Since $\theta(V_1 \times V_2)$ generates T, every element of T is of the form

$$\sum a_{x,y}(x \otimes y) \quad a_{xy} \in k.$$

Clearly

$$\begin{cases} x \otimes o = o \otimes y = o \otimes o \\ (x + x^1) \otimes y = x \otimes y + x^1 \otimes y \\ x \otimes (y + y^1) = x \otimes y + x \otimes y^1 \\ ax \otimes y = a(x \otimes y) \\ x \otimes \text{ by } = b(x \otimes y) \end{cases}$$

with obvious notations. 102

From our considerations it follows that in order to define a linear function on $V_1 \otimes V_2$ it is enough to define it on elements of the type $x \otimes y$. Also for every such linear function, there is a bilinear function on $V_1 \times V_2$.

It is easy to see that the mapping $x \otimes y \to y \otimes x$ of $V_1 \otimes V_2$ to $V_2 \otimes V_1$ is an isomorphism onto.

Suppose now that V_1^* and V_2^* are duals of V_1 and V_2 respectively over k. If $\sigma \in V_1^*$ and $\tau \in V_2^*$ and we define for $(x, y) \in V_1 \times V_2$ the function

$$\sigma.\tau(x, y) = \sigma x.\tau y,$$

then $\sigma.\tau$ is a bilinear function on $V_1 \times V_2$ into k. We shall now prove the

Theorem 3. *If $\{x_\alpha\}$ is a base of V_1 over k and $\{y_\beta\}$ a base of V_2 over k, then $\{x_\alpha \otimes y_\beta\}$ is a base of $V_1 \otimes V_2$ over k.*

Proof. We first prove that $\{x_\alpha \otimes y_\beta\}$ are linearly independent over k. For all $\sum a_{\alpha\beta}(x_\alpha \otimes y_\beta) = o$ for $a_{\alpha\beta} \in k$, $a_{\alpha\beta} = o$ for all but a finite number of α, β. By the method of constructing the tensor product, it follows that $\sum a_{\alpha\beta}(x_\alpha, y_\beta)$ is an element of W. Let σ and τ be elements of V_1^* and V_2^* defined respectively by

$$\begin{aligned} \sigma(x_\alpha) &= 1 \quad \text{if } \alpha = \gamma \\ &= o \quad \text{otherwise} \end{aligned}$$

$$\begin{aligned} \tau(y_\beta) &= 1 \quad \text{if} \quad \beta = \delta \\ &= o \quad \text{otherwise} \end{aligned}$$

103 □

Then $\sigma \cdot \tau$ is a bilinear function on $V_1 \times V_2$ and hence vanishes on W. Thus

$$\sigma.\tau\Big(\sum a_{\alpha\beta}(x_\alpha \otimes y_\beta)\Big) = o.$$

But the left side equals $a_{\gamma\delta}$. Thus all the coefficients $a_{\alpha\beta}$ vanish.

Next any element of $V_1 \otimes V_2$ is a linear combination of elements of the type $x \otimes y$, $x \in V_1$, $y \in V_2$. But then $x = \sum a_\alpha x_\alpha$ and $y = \sum b_\beta y_\beta$ so that

$$x \otimes y = \Big(\sum a_\alpha x_\alpha\Big) \otimes \Big(\sum b_\beta y_\beta\Big)$$

which equals $\sum a_\alpha b_\beta (x_\alpha \otimes y_\beta)$. Our theorem is proved.

We have incidentally the

Corollary. *If V_1 and V_2 are finite dimensional over k then*

$$\dim V_1 \otimes V_2 = \dim V_1 \cdot \dim V_2.$$

Also since the dual of V_1^* is isomorphic in a natural manner with V_1 when $\dim \cdot V_1$ is finite, we get

Corollary. *If V_1 and V_2 are finite dimensional over k then $V_1 \otimes_k V_2$ is isomorphic to the dual of the space of bilinear functions on $V_1 \times V_2$ into k.*

Let now A_1 and A_2 be two associative algebras over a field k. We can form the Kronecker product $A = A_1 \otimes_k A_2$ of the vector spaces A_1 and A_2 over k. We shall now introduce a multiplication into A so as to make it into an associative algebra.

In order to do this, observe that the multiplication defined has to be a bilinear function on $A \times A$ into A. Since A is generated by elements of the type $x \otimes y$, it is enough to define this bilinear function on elements of the type (z, z^1) in $A \times A$ where $z = x \otimes y$ and $z^1 = x^1 \otimes y^1$. Put 104

$$f(z, z^1) = z \cdot z^1 = x \cdot x^1 \otimes y \cdot y^1.$$

Now since $(x, y) \to xx^1 \otimes yy^1$ is a bilinear function on $A_1 \times A_2$ into A, by our previous considerations $z \to z \cdot z^1$ is a linear function on A into A. Similarly $z^1 \to z \cdot z^1$ is a linear function on A. This proves that f is bilinear and that the multiplication so defined distributes addition. That the multiplication is associative is trivial to see.

A is called the *Kronecker product algebra*.

We obtain some very simple consequences from the definition.

α) If e_1 and e_2 are respectively the unit elements of the algebras A_1 and A_2 then $e_1 \otimes e_2$ is the unit element of $A_1 \otimes A_2$.

For, since $A = A_1 \otimes A_2$ is generated by elements $x \otimes y$, it is enough to verify $(x \otimes y)(e_1 \otimes e_2) = (e_1 \otimes e_2)(x \otimes y)$. But this is trivial.

β) If A_1 has $x_1, \ldots, x_m$ as a base over k and A_2 has $y_2, \ldots, y_n$ as a base over k then $(x_i \otimes y_j)$ is a base of $A_1 \otimes A_2$ over k. Furthermore if the multiplication tables for the bases are

$$x_i x_j = \sum_t a_{ij}^{(t)} x_t$$

$$y_i y_j = \sum_{t'} b_{ij}^{(t')} y_{t'}$$

then 105

$$(x_p \otimes y_q)(x_r \otimes y_s) = \sum_{\lambda, \mu} a_{pr}^{(\lambda)} b_{qs}^{(\mu)} (x_\lambda \otimes y_\mu)$$

γ) If A_1 and A_2 have unit elements e_1 and e_2 respectively then the mappings

$$x \to x \otimes e_2$$
$$y \to e_1 \otimes y$$

are isomorphisms of A_1 and A_2 into A. Thus A contains subalgebras isomorphic to A_1 and A_2.

An important special case is the one where one of the algebras is a field. Let A be an algebra over k and K an extension field of k. Let A have unit element e_1 and K the unit element e_2. Form the Kronecker product $A \otimes K$ over k. Then $A \otimes K$ contains subalgebras A_1 and K_1 isomorphic to A and K respectively. For any $x \otimes t$ in $A \otimes K$ we have

$$x \otimes t = x \otimes e_2 . e_1 \otimes t = e_1 \otimes t . x \otimes e_2$$

so that A_1 and K_1 commute. Also every element of $A \otimes K$ is of the form $\sum a_{\alpha\beta}(x_\alpha \otimes t_\beta)$ where $\{x_\alpha\}$ is a base of A over k and $\{t_\beta\}$ a base of K over k. But this expression can be written

$$\sum_\alpha \Big(\sum_\beta a_{\alpha\beta}(e_1 \otimes t_\beta) \Big) (x_\alpha \otimes e_2).$$

This shows that $A \otimes K$ is an algebra over K_1 with the base $\{x_\alpha \otimes e_2\}$. If we identify A_1 with A and K_1 with K then $A \otimes K$ can be considered as an algebra over K, a basis of A over k serving as a base of $A \otimes K$ over K. $A \otimes K$ is then called the *algebra got from A by extending the ground field k to K*. We shall denote it by A_K. 106

It is clear that A_K is commutative if and only if A is a commutative algebra.

Note. Even if A is a field over k, A_K need *not* be a field over K.

Let Γ be the rational number field and $\Gamma o = \Gamma(\sqrt{d})$ the quadratic field over Γ. Let $\overline{\Gamma}$ be the real number field and consider the Kronecker product $A = \Gamma_o \otimes \overline{\Gamma}$ over Γ. Let e_1, e_2 be a basis of Γ_o over Γ with the multiplication table,

$$e_1^2 = e_1, \quad e_1 e_2 = e_2 e_1 = e_2, \quad e_2^2 = de_1.$$

The elements of Γ_o are of the form $ae_1 + be_2$, a, b in Γ. The elements of A are of the form $ae_1 + be_2$ with $a, b \in \overline{\Gamma}$.

Let first $d > o$. Then $\Gamma_o \otimes \overline{\Gamma}$ is not an integrity domain. For,

$$(\sqrt{d}e_1 + e_2)(\sqrt{d}e_1 - e_2) = o.$$

It can however be seen that A is then the direct sum of the two fields $\lambda\overline{\Gamma}$ and $\mu\overline{\Gamma}$ where

$$\lambda = \frac{1}{2}(e_1 + \frac{e_2}{\sqrt{d}}), \quad \mu = \frac{1}{2}(e_1 - \frac{e_2}{\sqrt{d}}).$$

Let $d < o$. Then A is a field. For if $ae_1 + be_2 \neq o$, then $a^2 - db^2 \neq o$. Put $f = \dfrac{a}{a^2 - db^2}$, $g = \dfrac{-b}{a^2 - db^2}$. Then

$$(ae_1 + be_2)(fe_1 + ge_2) = e_1.$$

2 Composite fields

Let K_1 and K_2 be two extension fields of k. Suppose K_1 and K_2 are both contained in an extension field Ω of k. Then the composite of K_1 and K_2 is the field generated over k by K_1 and K_2. In general, given 107
two fields K_1 and K_2 which are extensions of k, there does not exist an extension field Ω containing both. Suppose, however, there is a field Ω/k which contains k-isomorphic images K_1^σ, K_2^τ of K_1 and K_2, then a composite of K_1 and K_2 is defined to be the fields $k(K_1^\sigma \cup K_2^\tau)$. A *composite extension* of K_1 and K_2 is therefore given by a triplet (Ω, σ, τ) consisting of 1) and extension field Ω of k and 2) isomorphisms σ, τ of K_1 and K_2 respectively in Ω which are identity on k. The composite extension is then $k(K_1^\sigma \cup K_2^\tau)$. We wish to study these various composites of K_1 and K_2.

If Ω' is another extension of k and σ', τ' two k-isomorphisms of K_1 and K_2 respectively in Ω' then $k(K_1^{\sigma'} \cup K_2^{\tau'})$ is another composite extension. We say that these two composite extensions are *equivalent* if there exists a k-isomorphism μ of $k(K_1^\sigma \cup K_2^\tau)$ on $k(K_1^{\sigma'} \cup K_2^{\tau'})$ such that

$$\mu\sigma = \sigma', \mu\tau = \tau'.$$

Obviously this is an equivalence relation and we can talk of a class of composite extensions.

If $k(K_1^\sigma \cup K_2^\tau)$ is a composite extension we denote by $R(K_1^\sigma \cup K_2^\tau)$ the ring generated over k by K_1^σ and K_2^τ in Ω. This ring is, in general, different from $k(K_1^\sigma \cup K_2^\tau)$.

Let now $\bar{K} = K_1 \otimes K_2$ be the Kronecker product of K_1 and K_2. $\bar{K}$ contains subfields isomorphic to K_1 and K_2. We shall identify these subfields with K_1 and K_2 respectively. Let now $k(K_1^\sigma \cup K_2^\tau)$ be a
108 composite extension and $R(K_1^\sigma \cup K_2^\tau)$ the ring of the composite extension. Define the mapping φ of $\bar{K}$ into $R(K_1^\sigma \cup K_2^\tau)$ by

$$\varphi\Big(\sum a_{xy}(x \otimes y)\Big) = \sum a_{xy} x^\sigma y^\tau,$$

where $a_{xy} \in k$. Then φ coincides with σ on K_1 and with τ on K_2. Since σ and τ are isomorphisms, it follows that φ is a k-homomorphism of $\bar{K}$ on $R(K_1^\sigma \cup K_2^\tau)$. Since Ω is a field, it follows that kernel of the homomorphism is a prime ideal $\mathscr{Y}$ of $\bar{K}$. Thus

$$\bar{K}/\mathscr{G} \simeq R(K_1^\sigma \cup K_2^\tau).$$

If $k(K_1^{\sigma'} \cup K_2^{\tau'})$ is another composite extension, then μ defined earlier, is an isomorphism of $R(K_1^\sigma \cup K_2^\tau)$ on $R(K_1^{\sigma'} \cup K_2^{\tau'})$. Consider the homomorphism φ defined above. Define $\bar{\varphi}$ on $\bar{K}$ by $\bar{\varphi} = \mu \cdot \varphi$. We have

$$\bar{\varphi}(\sum a_{xy}\Big(x \otimes y)\Big) = \mu\Big(\sum a_{xy} x^\sigma y^\tau\Big) = \sum a_{xy} x^{\sigma'} y^{\tau'}.$$

Then $\bar{\varphi}$ is a homomorphism of $\bar{K}$ on $R(K_1^{\sigma'} \cup K_2^{\tau'})$. But, since μ is an isomorphism, it follows that $\bar{\varphi}$ has $\mathscr{G}$ as the kernel. Thus the prime ideal $\mathscr{G}$ is the same for a class of composite extensions.

Conversely, if two composite extensions correspond to the same prime ideal of $\bar{K}$, it can be seen that they are equivalent.

We have, now, only to prove the existence of a composite extension associated with a prime ideal of $\bar{K}$. Let $\mathscr{G}$ be a prime ideal of $\bar{K}$ and $\mathscr{G} \neq \bar{K}$. Since $\bar{K}$ has a unit element, a prime ideal $\mathscr{G} \neq \bar{K}$ always exists. Let A be the integrity domain

$$A = \bar{K}/\mathscr{G}$$

109 Let φ be the natural homomorphism of $\overline{K}$ on A. Then K_1^φ and K_2^φ are subfields of A. Since $\overline{K}$ is generated by elements of the type $x \otimes y$, K_1^φ and K_2^φ, are different from zero. Clearly $A = R(K_1^\varphi \cup K_2^\varphi)$. Hence the quotient field of A is a composite extension. Hence for every prime ideal $\mathscr{G} \neq \overline{K}$, there exists a composite extension. We have hence proved the

Theorem 4. *The classes of composite extensions of K_1 and K_2 stand in (1,1) correspondence with the prime ideal $\mathscr{G} \neq \overline{K}$ of the Kronecker product $\overline{K}$ of K_1 and K_2 over k.*

Consider now the special case where K_2/k is *algebraic*. Let $k(K_1^\sigma \cup K_2^\tau)$ be a composite extension. Then

$$k(K_1^\sigma \cup K_2^\tau) \supset R(K_1^\sigma \cup K_2^\tau) \supset K_1^\sigma.$$

Since every element of K_2 is algebraic over k, $k(K_1^\sigma \cup K_2^\tau)$ is algebraic over K_1^σ. This means that $R(K_1^\sigma \cup K_2^\tau)$ is a field and so coincides with $k(K_1^\sigma \cup K_2^\tau)$. Thus

Theorem 5. *If K/k is algebraic, then every prime ideal $\mathscr{G} \neq \overline{K}$ of K is a maximal ideal.*

Let K/k be an algebraic extension and L/k any extension. The Kronecker product $\overline{K} = K \otimes_k L$ is the extended algebra $(K)_L$ of K by extending k to L. $\overline{K}$ is thus an algebra (commutative) over L. If $\mathscr{G}$ is a prime of $\overline{K}$, then by above, it is a maximal ideal and $\overline{K}/\mathscr{G}$ gives a composite extension. Since $\overline{K}$ is an algebra over L we may regard $\overline{K}/\mathscr{G}$ as an extension field of L.

Let now $\mathscr{G}_1, \ldots, \mathscr{G}_m$ be m distinct maximal ideals of $\overline{K}$, none of them 110 equal to $\overline{K}$. Let $L_i = \overline{K}/\mathscr{G}_i$ be a composite extension. Form the direct sum algebra

$$\sum_i L_i$$

as a commutative algebra over L. We shall now prove

Theorem 6.

$$\boxed{\sum_i \bar{K}/\mathscr{G}_i \simeq \bar{K}/\bigcap_i \mathscr{G}_i}$$

Proof. We shall construct a homomorphism φ of $\bar{K}$ on $\sum_i L_i$ and show that the kernel is $\bigcap_i \mathscr{G}_i$. □

In order to do this let us denote by σ_i the natural homomorphism of $\bar{K}$ on L_i (this is identity on L), $i = 1, \ldots, m$. If $x \in \bar{K}$, then $\sigma_i x \in L_i$. Define φ on $\bar{K}$ by

$$\varphi(x) = \sum_i \sigma_i x.$$

That this is a homomorphism on $\bar{K}$ is easily seen; for, if $x, y \in \bar{K}$

$$\varphi(x+y) = \sum_i \sigma_i(x+y) = \sum_i \sigma_i x + \sum_i \sigma_i y = \varphi x + \varphi y.$$

$$\varphi(xy) = \sum_i \sigma_i(xy) = \sum_i (\sigma_i x)(\sigma_i y) = (\sum_i \sigma_i x)(\sum_i \sigma_i y) = \varphi x \varphi y.$$

The kernel of the homomorphism is set of x such that $\varphi x = o$. Thus $\sigma_i x = o$ so that $x \in \mathscr{G}_i$ for all i. Hence $x \in \cap_i \mathscr{G}_i$. But every $y \in \cap_i \mathscr{G}_i$ has the property $\varphi y = o$. Thus the kernel is precisely $\bigcap_i \mathscr{G}_i$.

We have only to prove that the homomorphism is *onto*.

111 To this end, notice that for each $i, i = 1, \ldots, m$, there is a $b_i \in \bar{K}$ with

$$b_i \begin{cases} \in \mathscr{G}_j, & j \neq i \\ \notin \mathscr{G}_i \end{cases}$$

For, since $\mathscr{G}_i$ and $\mathscr{G}_j$, $j \neq i$ are distinct, there is $a_j \in \mathscr{G}_j$ which is not in $\mathscr{G}_i$. Put $b_i = \prod_{i \neq j} a_j$. Then b_i satisfies above conditions since $\mathscr{G}_i$ is maximal.

Let now $\sum_i c_i$ be an element in the direct sum, $c_i \in L_i$. By definition of b_i

$$\sigma_j b_i \begin{cases} = o & \text{if } j \neq i \\ \neq o & \text{if } j = i \end{cases}$$

Since L_i is a field, there exists $x_i \neq o$ in L_i such that

$$x_i \sigma_i b_i = o_i.$$

σ_i being a homomorphism of $\overline{K}$ on L_i, let $y_i \in \overline{K}$ with $\sigma_i y_i = x_i$. Put

$$c = \sum_i b_i y_i$$

Then

$$\varphi(c) = \sum_i \sum_j \sigma_j(b_i y_i) = \sum_i c_i$$

which proves the theorem completely.

Suppose in particular K/k is finite. Then $\overline{K_L}$ has over L the degree $(K : k)$. Since, for a maximal ideal, $\mathscr{G} \neq \overline{K}$, $\overline{K}/\mathscr{G}$ has over L at most the degree $(K : k)$, we get

$$1 \leq (\overline{K}/\mathscr{G}_i : L) \leq (K : k) \quad i = 1, \ldots, m.$$

This means that $\overline{K}$ has only finitely many maximal ideals and

$$\overline{K}/\bigcap_{\mathscr{G}} \mathscr{G} \simeq \sum_{\mathscr{G}} \overline{K}/\mathscr{G}$$

the summations running through all maximal ideals of $\overline{K}$. 112

Thus K and L have over k only finitely many inequivalent composite extensions.

3 Applications

Throughout this section Ω will denote an algebraically closed extension of k and K and L will be two intermediary fields between Ω and k. A composite of K and L in Ω will be the field generated over k by K and L. It will be denoted by KL.

Let $\overline{K}$ be the Kronecker product over k of K and L. There is, then, a homomorphism φ of $\overline{K}$ on $R(K \cup L)$ given by

$$\varphi\Big(\sum a_{xy}(x \otimes y)\Big) = \sum a_{xy} x \cdot y.$$

Suppose that this homomorphism is an isomorphism of $\bar{K}$ onto $R(K \cup L)$. This means that

$$\sum a_{xy}(x \otimes y) = o \Longleftrightarrow \sum a_{xy} x \cdot y = o$$

or that every set of elements of K which are linearly independent over k are also so over L. Incidentally, this gives

$$K \cap L = k.$$

Conversely, suppose K and L have the property that every set of elements of K which are linearly independent over k are also so over L. Then the mapping φ is an isomorphism of $\bar{K}$ on $R(K \cup L)$. For, if $\sum a_{xy} xy = o$ we express x and y in terms of a base of L/k and a base of K/k giving

$$\sum b_{\alpha\beta} x_\alpha y_\beta = o$$

113 But this means all $b_{\alpha\beta}$ are zero. Therefore φ is an isomorphism.

It shows that every set of elements of L which are linearly independent over k are also so over K.

We call two such fields L and K *linearly disjoint over k*. Note that $L \cap K = k$. We deduce immediately

1) *If L and K are are linearly disjoint over k then any intermediary field of K/k and any intermediary field of L/k are also linearly disjoint.*

Suppose now that K/k is algebraic. Then every prime ideals of $\bar{K}$ is maximal. Let, in addition, K and L be linearly disjoint over k. Since $\bar{K}$ is isomorphic to $R(K \cup L)$, it follows that (o) is a maximal ideal. Hence $\bar{K}$ is a field. Thus

2) *If K/k is algebraic and K and L are linearly disjoint over k, there exists but one class of composite extensions of K and L over k.*

Let K/k be a finite extension. Then, for some maximal ideal $\mathscr{G}$, $\bar{K}/\mathscr{G}$ is isomorphic to KL. Since $\bar{K}/\mathscr{G}$ may be considered as an extension field of L, we get $(\bar{K}/\mathscr{G} : L) \leq (K : k)$, that is

$$(KL : L) \leq (K : k)$$

Clearly if $\mathscr{G} = (o)$, equality exists, and then K and L are linearly disjoint over k. The converse is true, by above considerations. Hence, in particular,

3) *If* $(K : k) = m$ *and* $(L : k) = n$*, then*

$$(KL : k) \leq mn;$$

equality occurs if and only if K and L are linearly disjoint over k. **114**

We now consider the important case, K/k *galois*. By the considerations above, it follows that KL/k is algebraic over L. Since Ω is a algebraically closed, it contains the algebraic closure of KL. Let σ be an isomorphism of KL in Ω, which is identity on L. Its restriction to K is an isomorphism of K in Ω. But Ω contains the algebraic closure of K and hence $\sigma K = K$. Since KL is generated by K and L, it follows that $\sigma KL \subset KL$. Hence KL/L is a galois extension. (KL/L is already separable since elements of K are separable over k).

$$\begin{tikzcd}
& \Omega \arrow[d, dash] & \\
& KL \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & L \arrow[dl, dash] \\
& K \cap L \arrow[d, dash] & \\
& k &
\end{tikzcd}$$

We now prove the

Theorem 7. *If K/k is a galois extension and L, any extension of k then*

$$G(KL/L) \simeq G(K/K \cap L)$$

Proof. In the first place, we shall prove that K and L are linearly disjoint over $K \cap L$. For this, it is therefore enough to prove that every finite set $y_1, \ldots, y_m$ of elements of L which are linearly independent over $K \cap L$, are also so over K. □

If possible, let $y_1, \ldots, y_m$ be dependent over K so that $\sum x_i y_i = o$, $x_i \in K$. Let us assume that $y_1, \ldots, y_m$ are dependent over K but no proper subset of them is linearly dependent over K. Therefore, all the x_i are different from zero.

We may assume $x_1 = 1$. Let σ be an element of $G(KL/L)$. Then 115

$$0 = \sigma(\sum_i x_i y_i) = \sum_i \sigma x_i \cdot \sigma y_i$$

By subtraction we get, since $\sigma 1 = 1$,

$$0 = \sum_{i \neq 1} (x_i - \sigma x_i) y_i$$

This means that $x_i = \sigma x_i$, $i = 2, \ldots, m$. But, since σ is arbitrary in $G(KL/L)$, it follows that $x_i \in L$. But $x_i \in K$. Thus $y_1, \ldots, y_m$ are linearly dependent on $K \cap L$ which is a contradiction. Hence K and L are linearly disjoint over $K \cap L$.

Therefore, KL is isomorphic to the Kronecker product of K and L over $K \cap L$.

Suppose σ is any L-automorphism of KL. Its restriction to K is an automorphism of K and leaves $K \cap L$ fixed. Consider the mapping $\sigma \to \bar{\sigma}$ of $G(KL/L)$ into $G(K/K \cap L)$. This is clearly a homomorphism. If $\bar{\sigma}$ is identity element of $G(K/K \cap L)$, then σ is identity on K. Since it is already identity on L, it is identity on KL. Thus, $G(KL/L)$ is isomorphic to a subgroup of $G(K/K \cap L)$. To see that this isomorphism is onto $G(K/K \cap L)$, let $\tau \varepsilon G(K/K \cap L)$. Any element of KL may be written (since K and L are linearly disjoint) in the from,

$$\sum_\alpha x_\alpha y_\alpha$$

where x_α are linearly independent elements of K over $K \cap L$ and $y_\alpha \in L$. This expression is unique. Extend τ to $\bar{\tau}$ in $G(KL/L)$ by defining

$$\bar{\tau}\left(\sum_\alpha x_\alpha y_\alpha\right) = \sum_\alpha y_\alpha \tau(x_\alpha).$$

116 This is well defined; for, if $\sum_\alpha y_\alpha \tau(x_\alpha) = 0$, then, since $\{x_\alpha\}$ are linearly independent over $K \cap L$, $\{\tau(x_\alpha)\}$ are also linearly independent

over $K \cap L$ and since K and L are linearly disjoint over $K \cap L$, all y_α are zero. Thus $\bar{\tau}$ is an automorphism of KL/L.

Our theorem is thus proved.

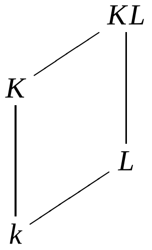
In particular, if K and L are both galois extensions of k and $K \cap L = k$ then, by above,

$$G(KL/L) \simeq G(K/k)$$
$$G(KL/K) \simeq G(L/k)$$

Also, since KL/k is algebraic, let σ be an isomorphism (trivial on k) of KL in Ω. Since its restrictions on K and L are auto morphisms, it follows that KL/k is a galois extension. We now prove

Theorem 8. *$G(KL/k)$ is isomorphic to the direct product of $G(K/k)$ and $G(L/k)$.*

Proof. $G(K/k)$ and $G(KL/L)$ are isomorphic and for every element σ in $G(K/k)$, by the previous theorem, we have the extension $\bar{\sigma}$, an element of $G(KL/L)$ determined uniquely by σ. Similarly, if $\tau \in G(L/k)$, $\bar{\tau}$ denotes its unique extension into an element of $G(KL/k)$.



□

We now consider the mapping

$$(\sigma, \tau) \to \bar{\sigma}\bar{\tau}$$

of the direct product $G(K/k) \cdot G(L/k)$ into $G(KL/k)$.

Suppose λ is an element of $G(KL/k)$. Its restriction λ to K is an 117
element of $G(K/k)$. Consider $\bar{\lambda}_1$. Now $\bar{\lambda}_1^{-1}\lambda$ is identity on K. By the

isomorphism of $G(KL/k)$ and $G(L/k)$, this defines a unique element μ_1 of $G(L/k)$. Hence

$$\lambda = \bar{\lambda}_1 \bar{\mu}_1.$$

Thus the mapping above is a mapping of the direct product $G(K/k) \cdot G(L/k)$ onto $G(KL/k)$. We have only to prove that is a homomorphism to obtain the theorem. It is clearly seen that λ is identity if and only if λ_1 and μ_1 are identity.

Let σ, σ' be two elements of $G(K/k)$ and τ, τ' in $G(L/k)$. Let λ and μ be the unique elements in $G(KL/k)$ defined by

$$\lambda = \bar{\sigma}\bar{\tau}, \quad \mu = \bar{\sigma}', \bar{\tau}'.$$

Consider to element $\lambda\mu$. Its restriction to K is $\sigma\sigma'$ and its restriction to L is $\tau\tau'$. Thus

$$\lambda\mu = \overline{\sigma\sigma'} \cdot \overline{\tau\tau}'$$

which proves that the mapping is a homomorphism.

The theorem is now completely proved.

Chapter 6

Special algebraic extensions

1 Roots of unity

118

Consider the polynomial $x^m - 1$ in $k[k]$, where k is a field. Let k have characteristic p. If $p = o$, then $x^m - 1$ is a separable polynomial over k, whereas if $p \neq o$, the derivative of $x^m - 1$ is mx^{m-1} which is zero, if p divides m. If $p \nmid m$, then $x^m - 1$ is a separable polynomial over k. Therefore, let $m > o$ be an arbitrary positive integer, if k has characteristic zero and m, an integer prime to p, if k has characteristic $p \neq 0$. Then $x^m - 1$ is a separable polynomial over k and it has m roots in Ω, an algebraic closure of k. We call these m roots, the *mth roots of unity*.

If ρ and τ are mth roots of unity then $\rho^m = 1 = \tau^m$. Therefore $(\rho\tau)^m = \rho^m\tau^m = 1$, $(\rho^{-1})^m = (\rho^m)^{-1} = 1$ which shows that the mth roots of unity from a group. This group G_m is abelian and of order m.

Let now d/m. Any root of $x^d - 1$ in Ω is also a root of $x^m - 1$.If ρ is an mth root of unity such that $\rho^d = 1$, then ρ is a root of $x^d - 1$. Since $x^d - 1$ has exactly d roots in Ω, it follows that G_m has the property that for every divisor d of m, the order of G_m, there exist exactly d elements of G_m whose orders divide $\underline{d}$. Such a group G_m is clearly a cyclic group. Hence

The mth roots of unity form a cyclic group G_m of order m. 119

There exists, therefore, a generator ρ of G_m. ρ is called a *primitive mth root of unity*. Clearly, the number of primitive mth roots of unity is

$\varphi(m)$. All the primitive mth roots of unity are given by ρ^a with $1 \leq a < m$, $(a, m) = 1$, ρ a fixed primitive mth roots of unity.

Let Ω be an algebraically closed field. Let m and n be two positive integers which are arbitrary, if Ω has characteristic zero and, prime to p, if Ω has characteristic $p \neq o$. If ρ is an mth root of unity and τ an nth root of unity, then

$$(\rho\tau)^{mn} = \rho^{mn} \cdot \tau^{mn} = 1,$$

so that $\rho\tau$ is an mn th root of unity. This shows that the roots of unity in Ω form a group $H(\Omega)$. We now determine the structure of H.

Theorem 1. *If Ω has characteristic zero, then H is isomorphic to the additive group of rational numbers mod 1, whereas, if Ω has characteristic $p \neq o, H$ is isomorphic to the additive group of rational numbers $\dfrac{a}{b}$, $(a, b) = 1$, $p \nmid b$,* mod 1.

Proof. Let R denote the group (additive) of rational numbers and $\nu_1 < \nu_2 < \nu_3 \cdots$ the sequence of natural numbers, if Ω has characteristic zero, whereas, if Ω has characteristic $p \neq o$, let R denotes the rational numbers $\dfrac{a}{b}$, $(b, a) = 1$, $p \nmid b$ and $\nu_1 < \nu_2 < \nu_3 \cdots$ the sequence of natural numbers prime to p. Put

$$\mu_n = \nu_1 \cdots \nu_n.$$

120

Denote, by H_n, the group of μ_n the roots of unity in Ω. Since every integer $m(p \nmid m$, if Ω has characteristic $p)$ divides some μ_n, if follows that

$$H = \bigcup_n H_n.$$

Since H_n is cyclic, we can choose a generator ρ_n of H_n is such a way that

$$\rho_n = \rho'^{\nu_{n+1}}_{n+1}.$$

□

Any x in R may be written as $\dfrac{a}{\mu_n}$ where $\underline{a}$ is an integer. Define the mapping σ as follows

$$\sigma x = \rho_n^a,$$

so that σ is a function on R with values in H. The mapping is well defined: for if $x = \dfrac{b}{\mu_m}$, then $\mu_m a = \mu_n b$. Suppose $m > n$; then

$$b = a\nu_{n+1} \cdots \nu_m$$

so that $\rho_m^b = \rho_m^{a\nu_{n+1}\cdots\nu_m} = \rho_n^a$ by choice of ρ_n. We now verify that σ is a homomorphism of R on H. If $x\dfrac{a}{\mu_n}$, $y = \dfrac{b}{\mu_m}$ are in R and $m \geq n$, then

$$\sigma(x + y) = \sigma(\frac{a\nu_{n+1} \cdots \nu_m + b}{\mu_m}) = \rho_m^{a\nu_{n+1}\cdots\nu_m+b}$$

which equals $\rho_n^a \cdot \rho_m^b = \sigma x \cdot \sigma y$. Also, since any root of unity is in some H_n, it is of the form ρ_n^a so that, for $x = \dfrac{a}{\mu_n}$, $\sigma x = \rho_n^a$. We have, therefore, to determine the kernel of the homomorphism. It is the set of x in R such that

$$\sigma x = 1.$$

If $x = \dfrac{a}{\mu_n}$, then $1 = \sigma x = \rho_n^a$ so that $|\mu_n|a$ and so x is an integer. The converse being trivial, it follows that the kernel is precisely the additive group of integers and our theorem is established. 121

2 Cyclotomic extensions

Let k be a field and $x^m - 1$ a separable polynomial in $k[x]$. This implies, in case k has characteristic $p \neq o$, that p does not divide m. Let ρ be a primitive mth root of unity in Ω, an algebraic closure of k. Then $K = k(\rho)$ is the splitting field of $x^m - 1$ in Ω. Therefore, K/k is a separable, normal extension. Let G be its galois group. If $\sigma \in G$, σ is determined by its effect on ρ. Since ρ is a primitive mth root of unity, so is $\sigma\rho$. For,

$$(\sigma\rho)^m = \sigma(\rho^m) = 1;$$

so $\sigma\rho$ is a root of unity. Also, if $(\sigma\rho)^t = 1$, then $\sigma(\rho^t) = 1$. Since σ is an automorphism, it follows that $\rho^t = 1$ or m/t. Thus

$$\sigma\rho = \rho^\nu, (\nu, m) = 1.$$

If σ, τ are in G, let $\sigma\rho = \rho^\nu$, $(\nu, m) = 1$ and $\tau\rho = \rho^\mu$ $(\mu, m) = 1$. Then

$$\sigma\tau(\rho) = \sigma(\tau\rho) = \sigma(\rho^\mu) = \rho^{\mu\nu}$$

which shows that $\sigma\tau = \tau\sigma$ or that G is abelian.

Consider now the mapping

$$g : \sigma \to \nu$$

where $\sigma\rho = \rho^\nu$, $(\nu, m) = 1$. This is clearly a homomorphism of G into the multiplicative group prime residue classes $\mod m$. The kernel of the mapping g is set of σ with $\sigma\rho = \rho$.

122 But then $\sigma t = t$ for all $t \in K$, so that by, galois theory, σ is the identity.

Let us call extension $K = k(\rho)$ a *cyclotomic extension* of k. We then have proved the

Theorem 2. *The Cyclotomic extension $k(\rho)/k$ is an abelian extension whose galois is isomorphic to a subgroup of the group of prime residue classes* $\mod m$ *where* $\rho^m = 1$ *and ρ is a primitive mth root of unity.*

Let Γ be the prime field contained in k. Then $\Gamma(\rho)$ is a subfield of $k(\rho) = K$. Let G be the galois group K/k.

$$\begin{tikzcd}
& K = k(\rho) \arrow[dl, dash] \arrow[dd, dash] \\
k \arrow[dd, dash] & \\
& \Gamma(\rho) \arrow[dl, dash] \\
\Gamma &
\end{tikzcd}$$

Let σ be in G and $\bar{\sigma}$ the restriction of σ to $\Gamma(\rho)$. Since σ is identity on k and $\sigma\rho$ is again a primitive root of unity, it follows that $\bar{\sigma}$ is an automorphism of $\Gamma(\rho)/\Gamma$. It is easy to see that the mapping $\sigma \to \bar{\sigma}$ is an isomorphism of G into the galois group of $\Gamma(\rho)/\Gamma$.

We shall therefore confine ourselves to studying the galois group of $\Gamma(\rho)/\Gamma$.

First, let Γ be the rational number field and ρ a primitive *mth* root of unity. Let $\Gamma(\rho)$ be the cyclotomic extension. Let $f(x)$ be the primitive integral polynomial which is irreducible in $\Gamma[x]$ an which ρ satisfies. Then $f(x)$ is a monic polynomial. For, since $f(x)$ divides x^{m-1},

$$x^m - 1 = f(x)\psi(x).$$

$\psi(x)$ has rational coefficients and so $\psi(x) = \frac{a}{b}\psi_1(x)$ where $\psi_1(x)$ is a primitive integral polynomial and a and b are integers. From the the theorem of Gauss on primitive polynomials it follows that $f(x)$ is monic. 123

Let p be a prime not dividing m. Let $\varphi(x)$ be the minimum polynomial (which is monic and integral) of ρ^p. We assert that $f(x) = \varphi(x)$. For, if not, $f(x)$ and $\varphi(x)$ are coprime and so

$$x^m - 1 = f(x) \cdot \varphi(x) \cdot h(x).$$

for some monic integral polynomials $h(x)$.

Consider the polynomial $\varphi(x^p)$. It has φ as a root and so $f(x)$ divides $\varphi(x^p)$. Hence

$$\varphi(x^p) = f(x)g(x),$$

$g(x)$, again, a monic and integral polynomial. Considering the above mod p we get

$$f(x)g(x) \equiv \varphi(x^p) \equiv (\varphi(x))^p (\text{mod } p)$$

so that $f(x)$ divides $(\varphi(x))^p(\mod p)$. If $t(x)$ is a common factor of $f(x)$ and $(\varphi(p)(\mod p)$ then $(t(x))^2$ divides $x^m - 1 \mod p$, which is impossible, since $p \nmid m$ and $x^m - 1$ does not have x as a factor. Thus our assumption $f(x) \neq \varphi(x)$ is false.

This means that, for every prime $p \nmid m$, ρ^p is a root of $f(x)$. If $(\nu, m) = 1$, then $\nu = p_1 p_2 \cdots p_1$ where $p_1, \ldots, p_1$ are primes not dividing

m. By using the above fact successively, we see that, for every $\nu, (\nu, m) = 1, \rho^\nu$ is a root of $f(x)$. Therefore

$$\rho_m(x) = \prod_{(\nu,m)=1} (x - \rho^\nu) \tag{1}$$

124 divides $f(x)$. But $\varphi_m(x)$ is fixed under all automorphisms of $\Gamma(\rho)/_\Gamma$ so that $f(x) = \varphi_m(x)$. We have proved the

Theorem 3. *If Γ is the field of rational numbers and ρ is a primitive mth root of unity, then the galois group of the cyclotomic extension $\Gamma(\rho)/\Gamma$ is isomorphic to the group of prime residue classes* mod m. *The irreducible polynomial $\varphi_m(x)$ of ρ is given by* (1).

$\varphi_m(x)$ is called the *cyclotomic polynomial* of order m. Its degree is $\varphi(m)$. In order to be able to obtain an expression for $\varphi_m(x)$ in terms of polynomials over Γ, we proceed thus.

We introduce the Mobius function defined as follows:

It is a function $\mu(n)$ defined for all positive integers n such that

1) $\mu(1) = 1$

2) $\mu(p_1 \cdots p_t) = (-1)^t$ where $p_1, \ldots, p_t$ are distinct primes.

3) $\mu(m) = o$ if p^2/m, p being a prime.

From this, one deduces easily

4) $\mu(m) \cdot \mu(n) = \mu(mn)$ for $(m, n) = 1$.

For, one has to verify it only for $m = p_1 \cdots p_t$, $n = q_1 \cdots q_1$ where $p's$ and $q's$ are all distinct primes. Then $\mu(m) = (-1)^t$, $\mu(n) = (-1)^1$ and $\mu(mn) = (-1)^{t+1}$.

We now prove the following simple formula

5)

$$\sum_{d|m} \mu(d) = o \text{ if } m > 1$$
$$= 1 \text{ if } m = 1$$

125 the summation running through all divisors d of m.

If $m = 1$, the formula reduces to (1). So, let $m > 1$. Let $m = p_1^{a_1} \cdots p_t^{a_t}$ be the prime factor decomposition of m. Any divisor d of m is of the form $p_1^{b_1} \cdots p_t^{b_t}$ where $o \leq b_i \leq a_i$, $i = 1, \ldots, t$. In view of (3), it is enough to consider divisors d of m for which $o \leq b_i \leq 1$. In that case,

$$\sum_{d|m} \mu(d) = \sum_{i=o}^{t} \binom{t}{i} (-1)^i = o.$$

Let now $f(n)$ be a function defined on positive integers, with values in a multiplicative abelian group. Let $g(n)$ also be such a function. We then have the Möbius inversion formula,

$$\boxed{\prod_{d|n} f(d) = g(n) \Longleftrightarrow f(n) = \prod_{d|n} (g(d))^{\mu(\frac{n}{d})}}$$

Suppose $\prod\limits_{d|n} f(d) = g(n)$. Then

$$\prod_{d|n} (g(d))^{\mu(\frac{n}{g})} = \prod_{d|n} \Bigg(\prod_{d_i|\frac{n}{d}} f(d_1) \Bigg)^{\mu(d)}.$$

Changing the order products, we get

$$\prod_{d_1|n} (f(d_1)) \sum_{d|\frac{n}{d_1}} \mu(d);$$

using formula (5), we obtain the inversion formula. The converse follows in the same way.

Consider now the integers mod m. Divide them into classes in the following manner. Two integers a, b are in the same class if and only if

$$(a, m) = (b, m).$$

Let d/m and C_d, the class of integers a (mod m) with $(a, m) = d$. **126** Then a is of the form $d\lambda$ where $(\lambda, \dfrac{m}{d}) = 1$. Thus C_d has $\varphi(\dfrac{m}{d})$ elements. The classes C_d, for $d|m$, exhaust the set of integers mod m. If ρ is a primitive mth root of unity, then

$$x^m - 1 = \prod_{t=1}^{m} (x - \rho^t).$$

In view of the above remarks, we can write

$$x^m - 1 = \prod_{d|m} \Big(\prod_{t \in C_d} (x - \rho^t) \Big).$$

But if $t \in C_d$, $\rho^t = \rho^{d\lambda}$, $(\lambda, \frac{m}{d}) = 1$ and so ρ^t is a primitive $\frac{m}{d}$ th root of unity. Using the definition of $\varphi_m(x)$, if follows that

$$x^m - 1 = \prod_{d|m} \varphi_d(x)$$

By the inversion formula we get

$$\boxed{\varphi_m(x) = \prod_{d|m} (x^d - 1)^{\mu(\frac{m}{d})}}$$

Comparison of degrees on both sides gives the formula

$$\varphi(m) = \sum_{d|m} d\mu(\frac{m}{d}) = m \sum_{d|m} \frac{\mu(d)}{d}.$$

We may compute $\varphi_m(x)$ for a few special values of m. Let $m = p$, a prime number. Then

$$\varphi_p(x) \frac{x^p - 1}{x - 1} = x^p - 1 + \cdots + x + 1.$$

If $m = pq$, the product of two distinct primes, then

$$\varphi_{pq}(x) = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}.$$

Let us now consider the case when Γ is the prime filed of p elements. 127 Obviously, $\Gamma(\rho)/\Gamma$ is a cyclic extension. If we define the cyclotomic polynomial as before, it is no longer irreducible over $\Gamma[x]$. For instance, let $p = 5$ and $m = 12$. Then

$$\varphi_{12}(x) = \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = x^4 - x^2 + 1.$$

Also

$$x^4 - x^2 + 1 = (x^2 - 2x - 1)(x^2 + 2x - 1) \pmod 5.$$

Therefore, $\Gamma(\rho)/\Gamma$ has degree $< \varphi(m)$. It is obvious since $\Gamma(\rho)/\Gamma$ is cyclic, that, for $\varphi_m(x)$ to be irreducible, the group of prime residue classes $\mod m$ should be cyclic. We shall prove

Theorem 4. *If Γ is the prime filed of characteristic $p \neq o$ and $p \nmid m$,the cyclotomic polynomial $\varphi_m(x)$ is irreducible, if and only if the group of prime residue classes mod m is cyclic and p is a generator of this cyclic group.*

Proof. We already know that $\Gamma(\rho)/\Gamma$ is cyclic. If $\varphi_m(x)$ is irreducible, then $\Gamma(\rho)/\Gamma$ has order $\varphi(m)$. Let σ be the Frobenius automorphism of $\Gamma(\rho)/\Gamma$. Then

$$\rho^\sigma = \rho^p,$$

p being the number of elements in Γ. The $\varphi(m)$ automorphisms $1, \sigma, \sigma^2, \ldots, \sigma^{\varphi(m)-1}$ are distinct. Hence

$$\rho, \rho^p, \rho^{p^2}, \ldots, \rho^{p^{\varphi(m)-1}}$$

are all distinct, which means $1, p, p^2, \ldots, p^{\varphi(m)-1}$ are distinct mod m. Therefore, p is a generator of the multiplicative group of prime residue classes $\mod m$. □

The converse is trivial.

The theorem is true, if, instead of Γ being the prime filed of p elements, Γ is a finite filed of q elements. Then q has to be a generator of the group of prime residue classes $\mod m$. **128**

If R_m denotes the group of prime residue classes $\mod m$, then R_m is cyclic, if and only if

$$m = 2^a, a = 1, 2 \quad \text{or} \quad m = q^b \quad \text{or} \quad 2q^b,$$

where q is a prime. Thus m has necessarily to have one of these forms.

We now use the irreducibility of $\varphi_m(x)$ over the rational number field to prove a theorem of *Wedderburn*.

Theorem 5. *A division ring with a finite number of elements is a filed.*

Proof. Let D be the division ring and k its centre. Then k is a field. D being finite, let k have q elements. If D is of rank n over k, then D has q^n elements. We shall prove that $n = 1$. □

Let D_1 be a subalgebra of D over k. Let D_1 have rank m over k. Then D_1 has q^m elements. But D_1^* is a sub group of D^* so that $q^m - 1$ divides $q^n - 1$. This means that $m|n$. For, if $n = tm + \mu$, $o \leq \mu < m$; then

$$q^n - 1 = q^\mu (q^{tm} - 1) + (q^\mu - 1)$$

so that $q^m - 1|q^\mu - 1$ which cannot happen unless $\mu = 0$. Thus every subalgebra of D has rank d dividing n.

129 Let $x \in D$. Consider the $y \in D$ such that $xy = yx$. They form a subalgebra over k. Therefore, the number of y in D^* which commute with x form a group of order $q^d - 1$, for some d dividing n. This group is the normaliser of x. Hence, the number of distinct conjugates (in the sense of group theory) of x in D^* is

$$q^n - 1|q^d - 1.$$

For the finite group D^*, we have

$$D^* = k^* + \sum_x D_x^*,$$

where D_x^* is the set of all conjugates of x. Comparing number of elements on both sides

$$q^n - 1 = q - 1 + \sum_d q^n - 1/q^d - 1$$

for some divisors d of n.

Since $\varphi_n(x)|x^n - 1$, we see that $\varphi_n(q)$, which is an integer, divides $q^n - 1$. Also $\varphi^n(x)$ divides $x^n - 1|x^d - 1$ for any $d|n$, $d \neq n$. Therefore, $\varphi_n(q)$ divides $q - 1$. But

$$\varphi_n(q) > (q - 1)^{\varphi(n)}$$

which shows that $n \not> 1$.

This proof is due to *Ernst Witt*.

3 Cohomology

Let G be a finite group and A an abelian group on which G acts as a group of left operators. Let A be a multiplicative group. We denote elements of G by $\sigma, \tau, \rho, \ldots$, and elements of A by $a, b, c, \ldots$. We denotes by a^σ the effect of σ on a. Then

$$\begin{aligned}(ab)^\sigma &= a^\sigma b^\sigma\\ (a^\tau)^\sigma &= a^{\sigma\tau}\end{aligned}$$

130

Let 1 be the unit element of A. Denote by G^n, $n \geq 1$ the Cartesian product of G with itself n times.

A function on G^n with values in A is said to be an *n dimensional Cochain* or, simply, an n cochain. This function $f(x_1, \ldots, x_n)$ has values in A. We denote by a $\sigma_1, \ldots, \sigma_n$ the element in A which is the value taken by the n cochain for values $\sigma_1, \ldots, \sigma_n$ of its variables. We denote the function also, by $a\sigma_1, \ldots, \sigma_n$. If $a\sigma_1, \ldots, \sigma_n$ and $b\sigma_1, \ldots, \sigma_n$ are two functions, we define their product by

$$o_{\sigma_1,\ldots,\sigma_n} = a_{\sigma_1,\ldots,\sigma_n} \cdot b_{\sigma_1,\ldots,\sigma_n}.$$

Similarly

$$o_{\sigma_1,\ldots,\sigma_n} = (a_{\sigma_1,\ldots,\sigma_n})^{-1}$$

is called the inverse of $a_{\sigma_1,\ldots,\sigma_n}$. With these definitions, the n cochains form a group $C^n(G, A)$ or simply C^n.

We define $C^o(G, A)$, the zero dimensional cochains, to be the group of functions with constant values, that is functions a_σ on G such that

$$a_\sigma = a$$

is the same for all $\sigma \in G$. It is then clear that C^o is isomorphic to A.

We now introduce a coboundary operator ∂ in the following manner. $\partial(= \partial_n)$ is a homomorphism of C^n into C^{n+1} defined by

$$a_{\sigma_1,\ldots,\sigma_{n+1}} = \partial a_{\sigma_1,\ldots,\sigma_n}$$

$$= a^{\sigma_1}_{\sigma_2,\ldots,\sigma_{n+1}} \prod_{n=1}^{n} (a_{\sigma_1,\ldots,\sigma_{i-1},\sigma_i\sigma_{i+1},\ldots,\sigma_{n+1}})^{(-1)^i} (a_{\sigma_1,\ldots,\sigma_n})^{(-1)^{n+1}}.$$

131

For $n \geq o$, we define the groups $Z^n(G, A)$ and $B^{n+1}(G, A)$ in the following manner. $Z^n(G, A)$ is the kernel of the homomorphism $C^n \xrightarrow{\partial n} C^{n+1}$ and $B^{n+1}(G, A)$ is the homomorphic image. The elements of $Z^n(G, A)$ are called *n dimensional cocycles* or *n*-cocycles and the elements of $B^{n+1}(G, A)$ are $n + 1$-*dimensional coboundaries* or $n + 1$ coboundaries. The homomorphism ∂ has the property

$$\partial\partial = \text{ identity} \tag{2}$$

which proves that $B^{n+1}(G, A)$ is a subgroup of $Z^{n+1}(G, A)$ and we can form for every $n > o$ the factor group $H^n(G, A)$ the *n-dimensional cohomology group*. We verify (2) only in case $n = o$ and 1 which are the ones of use in our work.

The coboundary of a zero cochain is a one cochain given by

$$\partial a = a_\sigma = \frac{a^\sigma}{a}. \tag{3}$$

Its coboundary, by definition is

$$\partial\partial a = a_{\sigma,\tau} = \frac{a_\sigma \cdot a^\sigma_\tau}{a_{\sigma\tau}}.$$

Substituting from (3), we get $a_{\sigma,\tau} = 1$ which verifies (2) for $n = o$.

We define the zero coboundary, that is the elements in $B^o(G, A)$, to be the function with value 1 on all $\sigma \in G$. Thus $B^o(G, A)$ consists only of the identity. An element in $Z^o(G, A)$ will be the constant function a with

$$a^\sigma = a$$

for all σ. Hence

132 *$H^o(G, A)$ is isomorphic with the set of $a \in A$ with the property $a^\sigma = a$ for all $\sigma \in G$.*

A one dimensional cocycle is a function a_σ for which $\partial a_\sigma = 1$. But

$$\partial a_\sigma = \frac{a_\sigma \cdot a^\sigma_\tau}{a_{\sigma\tau}}.$$

Therefore, the elements in $Z'(G, A)$ are functions a_σ with

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

A one coboundary is, already, a function a_σ of the form a^σ/a. It is, certainly, a one cocycle.

For our purposes, we shall need also the *additive cohomology*, instead of the multiplicative cohomology above. We regard now A^+ as an additive, instead of a multiplicative, group. Then $C^n(G, A^+)$ is an additive abelian group. We define the coboundary operator as

$$\begin{aligned} a_{\sigma_1,\ldots,\sigma_{n+1}} &= \partial a_{\sigma_1,\ldots,\sigma_n} \\ &= a^{\sigma_1}_{\sigma_2,\ldots,\sigma_{n+1}} + \sum_{i=1}^{n} (-1)^i a_{\sigma_i,\ldots,\sigma_{i-1},\sigma_i,\tau\sigma_{i+1},\ldots,\sigma_{n+1}} + (-1)^{n+1} a_{\sigma_i,\ldots,\sigma_n}. \end{aligned}$$

As before, a zero cochain is a constant function on G and its coboundary a_σ is

$$\partial a = a_\sigma = a^\sigma - a.$$

A one cochain a_σ is a cocycle if

$$\partial a_\sigma = 0$$

which is the same thing as

$$a_\sigma + a_\tau^\sigma = a_{\sigma\tau}.$$

Exactly as before, we see that $H^o(G, A)$, the zero dimensional additive cohomology group is isomorphic to the set of elements $\underline{a}$ in A^+ with 133 $a^\sigma = a$ for all σ.

We now consider the case when G is a cyclic group. Let σ be a generator of G so that $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are all the elements of G. Taking multiplicative cohomology, if a_σ is a one cocycle, then

$$a_{\tau\mu} = a_\tau a_\mu^\tau$$

or $a_\mu^\tau = a_{\tau\mu}/a_\tau$. Substituting for τ successively $1, \sigma, \ldots, \sigma^{n-1}$ we get

$$a_\mu^{1+\sigma+\cdots+\sigma^{n-1}} = 1.$$

We denote $a_\mu^{1+\sigma+\cdots+\sigma^{n-1}}$ by Na_μ and call it the *norm of* a_μ. Thus, if a_μ is a cocycle, then,

$$Na_\mu = 1.$$

Conversely, suppose a is an element in A with

$$Na = a^{1+\sigma+..+\sigma^{n-1}=1} = 1.$$

We can define a cocycle a_μ such that $a_\sigma = a$. For let $\mu = \sigma^\nu$, for some ν. Put

$$a_\mu = a^{1+\sigma+\cdots+\sigma^{\nu-1}}.$$

Obviously, $a_\sigma = a$. Also, a_σ is a cocycle. For, if $\tau = \sigma^{\nu'}$.

$$\begin{aligned} a_\mu a_\tau^\mu &= a^{1+\sigma+\cdots+\sigma^{\nu-1}}(a^{1+\sigma+\cdots+\sigma^{\nu'-1}})^{\sigma^\nu} \\ &= a^{1+\sigma+\cdots+\sigma^{\nu-1}+\sigma^\nu+\cdots+\sigma^{\nu+\nu'-1}} \\ &= a_{\mu\tau}. \end{aligned}$$

In a similar manner, for additive cohomology, we have $a_{\tau\mu} = a_\tau + a_\mu^\tau$
134 where a_μ is a cocycle. If G is cyclic, on substituting $1, \sigma, \ldots, \sigma^{n-1}$ for τ, we get

$$S a_\mu = a_\mu + a_\mu^\sigma + \cdots + a_\mu^{\sigma^{n-1}} = o.$$

We call $S a_\mu$ the *spur or trace* of a_μ. If a is any element of A, with trace $S a = a + a^\sigma + \cdots + a^{\sigma^{n-1}} = o$, then the cocycle

$$a_\mu = a + a^\sigma + \cdots + a^{\sigma^{\nu-1}}$$

where $\mu = \sigma^\nu$, has the property

$$a_\sigma = a.$$

We now apply the considerations above, in the following situation. K/k is a finite galois extension with galois group G. Then G acts on K^* and also the additive group K^+ as a group of operators. We might, therefore, consider the cohomology groups $H^o(G, K^*)$, $H^1(G, K^*), \ldots$ and $H^o(G, K^+), H^1(G, K^+) \ldots$ etc. As before, $H^o(G, K^*)$ and $H^o(G, K^+)$ are isomorphic to subgroups of K^* and K^+ with $a^\sigma = a$ for all σ. This, by galois theory, shows

Theorem 6. *$H^o(G, K^*)$ is isomorphic to k^* and $H^o(G, K^+)$ is isomorphic to k^+.*

But what we are interested in, is the following important theorem due to *Artin*.

Theorem 7. *The group $H^1(G, K^*)$ and $H^1(G, K^+)$ are trivial.*

Proof. Let us first consider multiplicative cohomology. If a_σ is a cocycle, we have to prove that it is a coboundary. The elements $\sigma, \tau, \ldots$ of G are independent k-linear mappings of K into Ω, the algebraic closure. Hence, if (a_σ) are elements of K^*,

$$\sum_\sigma a_\sigma \cdot \sigma$$

is a non-trivial k-linear map of K into Ω. Therefore, there exists a $\theta \neq o$ in K such that 135

$$\sum_\sigma a_\sigma \theta^\sigma \neq o.$$

□

Put $b^{-1} = \sum\limits_\sigma a_\sigma \theta^\sigma = \sum\limits_\tau a_\tau \theta^\tau$. Then

$$(b^{-1})^\sigma = \sum_\tau a_\tau^\sigma \theta^{\sigma\tau}.$$

Therefore

$$\frac{a_\sigma}{b^\sigma} = \sum_\tau a_\sigma a_\tau^\sigma \theta^{\sigma\tau}.$$

Since (a_σ) is a cocycle, we get

$$\frac{a_\sigma}{b^\sigma} = \sum_\tau a_{\sigma\tau} \theta^{\sigma\tau} = \sum_\tau a_\tau \theta^\tau = b^{-1}.$$

Thus

$$a_\sigma = \frac{b^\sigma}{b} = b^{\sigma - 1}$$

which is a coboundary.

Consider now the additive cohomology. K/k being finite and separable, there exists $a\theta \in K$ such that

$$\sum_\sigma \theta^\sigma = S_{K/k}\theta = 1.$$

Put now

$$-b = \sum_\sigma a_\sigma \theta^\sigma$$

a_σ being an additive cocycle. Then

$$-b^\sigma = \sum_\tau a^\sigma_\tau \theta^{\sigma\tau}.$$

But $a_\sigma = a_\sigma \cdot 1 = \sum_\tau a_\sigma \cdot \theta^\tau$ so that

$$a_\sigma - b^\sigma = \sum_\tau (a_\sigma + a^\sigma_\tau)\theta^{\sigma\tau} = \sum_\tau a_{\sigma\tau}\theta^{\sigma\tau} = -b$$

which proves that $a_\sigma = b^\sigma - b$ is a coboundary.

Our theorem is completely proved.

136 We apply the theorem in the special case where G is cyclic. Let σ be a generator of G. If a_σ is a cocycle then, in multiplicative theory

$$a_\sigma^{1+\sigma+\cdots+\sigma^{n-1}} = 1$$

or $N_{K/k}a_\sigma = 1$. Similarly in additive cohomology,

$$a_\sigma + a^\sigma_\sigma + \cdots + a^{\sigma^{n-1}}_\sigma = o$$

or $S_{K/k}a_\sigma = o$.

Using theorem 7, we obtain 'theorem 90' of *Hilbert*.

Theorem 8. *If K/k is a finite cyclic extension, σ, a generator of the galois group of K/k and a and b two elements of K with $N_{K/k}a = 1$ and $S_{K/k}b = 0$ respectively, then*

$$a = c^{1-\sigma}$$
$$b = d^\sigma - d$$

for two elements c, d in K.

4 Cyclic extensions

Let K/k be a cyclic extension of degree m. Put $m = np^a$, $(n, p) = 1$ if p is the characteristic of k; otherwise, let $m = n$.

Let G be the galois group of K/k. It has only one sub-group of order p^a. Let L be its fixed field. Then K/L is cyclic of degree p^a and L/k is cyclic of degree n prime to p. Let ρ be a primitive *nth* root of unity and $k(\rho)$ the cyclotomic extension. The composite $F = Lk(\rho)$ is cyclic over $k(\rho)$ and of degree prime to p. We shall see that K over L and F over $k(\rho)$ can be described in a simple manner.

We shall, therefore, consider the following case, first.

K/k is a cyclic extension of degree m and $p \nmid m$, if k has characteristic $p \neq o$; otherwise, m is an arbitrary integer. Also, k contains all the *mth* roots of unity. We then have the theorem of *Lagrange*. **137**

Theorem 9. *$K = k(w)$ where $w^m \in k$.*

Proof. Let ρ be a primitive *mth* root of unity. ρ is in k. □

Hence, since K/k has degree m,

$$N_{K/k}\rho = \rho^m = 1.$$

By Hilbert's theorem, therefore, if σ is a generator of the galois group of K/k, then there is an $\omega \in K$ such that

$$\omega^{1-\sigma} = \rho.$$

Since ρ is a primitive *mth* root of unity, $\omega, \omega^\sigma, \omega^{\sigma^2}, \ldots$ are all distinct and are conjugates of ω. Hence our theorem.

ω satisfies a polynomial $x^m - a$, $a \in k$. If $K = k(\omega')$, where ω' also satisfies a polynomial $x^m - b$, $b \in k$,then

$$\omega'^\sigma = \omega' \cdot \rho^+,$$

where ρ^t is a primitive *mth* root of unity and so $(t, m) = 1$.

Now

$$\left(\frac{\omega'}{\omega^t}\right)^\sigma = \frac{\omega' \cdot \rho^t}{\omega^t \cdot \rho^t} = \frac{\omega'}{\omega^t}$$

which shows that

$$\omega' = \omega^t \cdot c, \quad c \in k.$$

We shall call $x^m - a$ a *normed polynomial*. We have, then, the

Corollary. *If $k(\omega) = K = k(\omega')$, where ω and ω' are roots of normed polynomials, then*

$$\omega' = \omega^t \cdot c,$$

138 *where $(t, m) = 1$ and $c \in k$.*

We consider the special case, $m = q$, a prime number. Let K/k be a cyclic extension of degree q. Let $K = k(\alpha)$ and let $\alpha_1 = (\alpha), \alpha_2, \ldots, \alpha_q$ be the irreducible polynomial of α over k. Suppose σ is a generator of the galois group of K/k.

Let notation be so chosen that

$$\alpha_1^\sigma = \alpha_2, \alpha_2^\sigma = \alpha_3, \ldots, \alpha_{q-1}^\sigma = \alpha_q, \alpha_q^\sigma = \alpha_1.$$

Since k contains the *qth* roots of unity and every *qth* root of unity $\rho \neq 1$ is primitive, we construct the *Lagrange Resolvent*.

$$\omega = \omega(\alpha, \rho) = \alpha_1 + \rho\alpha_2 + \cdots + \rho^{q-1}\alpha_q.$$

Then

$$\omega^\sigma = \alpha_2 + \rho\alpha_3 + \cdots + \rho^{q-2}\alpha_q + \rho^{q-1}\alpha_1$$

which shows that $\omega^\sigma = \rho^{-1}\omega$. Hence $K = k(\omega)$. Also,

$$(\omega^q)^\sigma = \omega^q$$

which proves that $\omega^q \in k$ and ω satisfies a normed polynomial.

In particular, if k has characteristic $\neq 2$, and K/k has degree 2, then

$$K = k(\sqrt{d})$$

for $d \in k$.

The polynomial $x^q - a$ for $a \in k$ is, thus, either irreducible and, then, a root of it generates a cyclic extension, or else, $x^q - a$ is a product of linear factors in k.

We study the corresponding situation when K has characteristic $p \neq o$ and K/k is a cyclic extension of degree p^t, $t \geq 1$.

139 We first consider cyclic extensions of degree p.

Let K/k be a cyclic extension of degree p and σ, a generator of the galois group of K/k. Let μ be a generic element of the prime field Γ contained in k.

Introduce the operator $\mathscr{P}x = x^p - x$. Then

$$\mathscr{P}(x + \mu) = \mathscr{P}x.$$

Also, the only α in k satisfying $\mathscr{P}\alpha = o$ are the elements of Γ and these are all the roots of $\mathscr{P}x = o$.

The element 1 in k has the property

$$S_{K/k}\, 1 = o,$$

so that by Hilbert's theorem, there is an $\omega \in K$ such that

$$1 = \omega^\sigma - \omega.$$

Therefore, since K/k has degree p,

$$K = k(\omega).$$

In order to determine the polynomial of which ω is a root, consider $\mathscr{P}\omega$.

$$(\mathscr{P}\omega)^\sigma = \mathscr{P}\omega^\sigma = \mathscr{P}(\omega + 1) = \mathscr{P}\omega$$

which shows that $\mathscr{P}\omega \in k$. If we put $\mathscr{P}\omega = \alpha$, then ω is a root the irreducible polynomial

$$x^p - x - \alpha$$

in $k[x]$. ω is a root of the polynomial and $\omega^\sigma = \omega + 1$. Since σ is a generator of the galois group of K/k, the roots of $x^p - x - \alpha$ are $\omega, \omega + 1, \ldots, \omega + p - 1$.

A polynomial of the type $x^p - x - \alpha$, $\alpha \in k$ is called a *normed polynomial.*

Suppose $K = k(\omega')$ where ω' also satisfies a normed polynomial. 140

Then $\omega', \omega'+1, \ldots, \omega'+p-1$ are the roots of this normed polynomial. So

$$\omega'^{\sigma} = \omega' + h, \quad o < h \leq p-1.$$

Now $\omega' - h\omega$ satisfies

$$(\omega' - h\omega)^{\sigma} = \omega'^{\sigma} - h\omega^{\sigma} = \omega' + h - h\omega - h = \omega' - h\omega$$

which shows that $\omega' - h\omega \in k$. We have, hence, the

Theorem 10. *If K/k is cyclic of degree p and σ, a generator of the galois group of K/k, then $K = k(\omega)$ where ω satisfies a normed polynomial $x^p - x - \alpha$ in $k[x]$ and $\omega^{\sigma} = \omega + 1$. If $K = k(\omega')$ and ω' also satisfies a normed polynomial, then*

$$\omega' = \mu\omega + a,$$

$\mu \in \Gamma$ *and $a \in k$.*

In order to be able to construct ω, we proceed thus. Let α be an element in K with

$$S_{K/k}\alpha = 1.$$

Let $\alpha_1 (= \alpha), \ldots, \alpha_p$ be the roots of the irreducible polynomial which α satisfies over k. Construct the resolvent

$$-\omega = \alpha_1 + 2\alpha_2 + \cdots + (p-1)\alpha_{p-1} + p\alpha_p.$$

Let notation be so chosen that

$$\alpha_1^{\sigma} = \alpha_2, \alpha_2^{\sigma} = \alpha_3, \ldots, \alpha_{p-1}^{\sigma} = \alpha_p, \alpha_p^{\sigma} = \alpha_1.$$

Then

$$-\omega^{\sigma} = \alpha_2 + 2\alpha_3 + \cdots + (p-1)\alpha_p$$

and so $\omega^{\sigma} - \omega = \alpha_1 + \alpha_2 + \cdots + \alpha_p = 1$. Therefore $\omega^p - \omega = t$ for some t in k. This gives the normed polynomial.

141 It should be noticed that, here, we use additive cohomology whereas, in case K/k has degree m prime to p, we used multiplicative cohomology. Furthermore, in the second case, when K/k is of degree p, the

elements of Γ serve the same purpose as the roots of unity in the first case.

If k has characteristic 2 and K/k is a separable extension of degree 2, then

$$K = k(\omega)$$

where $\omega^2 - \omega \in k$.

Observe, also, that any polynomial $x^p - x - \alpha$, for $\alpha \in k$, is either irreducible over k and so generates a cyclic extension over k, or splits completely into linear factors in k. For, if ω is a root of $x^p - x - \alpha$ then, for $\mu \in \Gamma$, $\omega + \mu$ is also a root.

Just as we denote a root of $x^m - \alpha$ by $\sqrt[m]{\alpha}$, we shall denote, for $\alpha \in k$, by $\dfrac{\alpha}{\mathscr{P}}$, a root of $x^p - x - \alpha$. It is obvious that $\dfrac{\alpha}{\mathscr{P}}$ is p valued and if ω is one value of $\dfrac{\alpha}{\mathscr{P}}$, all the values are

$$\omega, \omega + 1, \ldots, \omega + p - 1.$$

We now study the case of cyclic extension of degree p^n, $n \geq 1$.

Let K/k be a cyclic extension of degree p^n and σ, a generator of the galois group G of K/k. Since G is cyclic of order p^n, it has only one subgroup of order p and hence, there exists a unique subfield L of K such that K/L is cyclic of degree p and L/k is cyclic of degree $p^{n-1} = m$. Let us assume that $n \geq 2$.

σ^m is of order p and hence is a generator of the galois group of K/L. **142**
Thus $K = L(\omega)$ where

$$\sigma^m \omega = \omega + 1$$

and ω satisfies $\mathscr{P}\omega = \alpha \in L$.

Put $\sigma\omega - \omega = \beta$. Then $\sigma^m \beta = \sigma(\sigma^m \omega) - \sigma^m \omega = \beta$ which shows that $\beta \in L$. Also,

$$S_{L/k}\beta = \beta + \beta^{\sigma} + \cdots + \beta^{\sigma^{m-1}}.$$

Substituting the value of β, we get

$$\begin{aligned} S_{L/k}\beta &= (\sigma\omega - \omega) + (\sigma^2\omega - \sigma\omega) + \cdots + (\sigma^m\omega - \sigma^{m-1}\omega) \\ &= \sigma^m\omega - \omega = 1. \end{aligned}$$

Hence β has the property

$$S_{L/k}\beta = 1.$$

It is easy to see that α is not k. For,

$$\mathscr{P}\beta = \sigma(\mathscr{P}\omega) - \mathscr{P}\omega = \sigma\alpha - \alpha$$

and α in k would mean $\mathscr{P}\beta = o$ or $\beta \in \Gamma$. This means that $S_{L/k}\beta = o$.

We now proceed in the opposite direction. Let L be cyclic of degree $p^{n-1} > 1$ over k. We shall construct an extension K which is cyclic *over* k and contains L as a proper subfield. Let σ be a generator of the galois group of L/k.

Let us choose $\beta \in L$, such that

$$S_{L/k}\beta = 1.$$

Now $S_{L/k}(\mathscr{P}\beta) = \mathscr{P}(S_{L/k}\beta) = o$ which shows that

$$\mathscr{P}\beta = \sigma\alpha - \alpha$$

143 for some α in L. Also, α is not in k. We claim that for $\lambda \in k$,

$$x^p - x - \alpha - \lambda \tag{4}$$

is irreducible over $L[x]$. For, if it is not irreducible, it is completely reducible in L. Let ω be a root of $x^p - x - \alpha - \lambda$ in L. Then

$$\omega^p - \omega = \alpha + \lambda.$$

This means that

$$\mathscr{P}(\sigma\omega - \omega) = \sigma(\mathscr{P}\omega) - \mathscr{P}\omega = \sigma\alpha - \alpha = \mathscr{P}\beta.$$

Thus

$$\mathscr{P}(\sigma\omega - \omega - \beta) = o$$

or $\sigma\omega - \omega - \beta = \mu$. Since $S_{L/k}(\sigma\omega - \omega) = o$ and $S_{L/k}\mu = o$, it follows that $S_{L/k}\beta = o$, which is a contradiction. Thus for $\lambda \in k$, (4) is irreducible in $L[x]$. Let ω be a root of this irreducible polynomial for some λ. Then $K = L(\omega)/L$ is cyclic of degree p.

Let $\bar{\sigma}$ denote an extension of σ to an isomorphism of K/k in Ω, the algebraic closure of k. Then $\bar{\sigma}$ is not identity on L. Since $\mathscr{P}\omega = \alpha + \lambda$ and $\lambda \in k$, we get

$$\bar{\sigma}(\mathscr{P}\omega) = \sigma\alpha + \lambda.$$

Now

$$\mathscr{P}(\bar{\sigma}\omega - \omega) = \bar{\sigma}(\mathscr{P}\omega) - \mathscr{P}\omega = \sigma\alpha - \alpha = \mathscr{P}\beta$$

and, again, we have

$$\mathscr{P}(\bar{\sigma}\omega - \omega - \beta) = o$$

or that $\bar{\sigma}\omega = \omega + \beta + \mu$ which shows that $\bar{\sigma}$ is an automorphism of K/k. If t is any integer,

$$\bar{\sigma}^t\omega = \omega + \beta + \beta^{\sigma} + \cdots + \beta^{\sigma^{t-1}} + t\mu.$$

144

This shows that 1, $\bar{\sigma}, \bar{\sigma}^2, \ldots, \bar{\sigma}^{p^{n-1}}$ have all different effects on ω, so that they are distinct automorphisms of K/k. But, since K/k has degree p^n, it follows that K/k is cyclic of degree p^n. We have, hence, the important

Theorem 11. *If k is a field of characteristic p and admits a cyclic extension K of k containing L and of degree p^m, $m > n$, for every m.*

In fact, if k is an infinite field, we may very λ over k and obtain an infinity of extensions K over k with the said property. It follows theorem 10.

Corollary. *If k is a field of characteristic p and admits a cyclic extension of degree p^n for some $n \geq 1$, then its algebraic closure is of infinite degree over it.*

5 Artin-Schreier theorem

We had obtained, in the previous section, a sufficient condition on a field so that its algebraic closure may be of infinite degree over it. We would like to know if there are fields K which are such that their algebraic closures are finite over them. The complete answer to this question is given by the following beautiful theorem due to *Artin* and *Schreier*.

Theorem 12. *If Ω it an algebraically closed field and K is a subfield such that*

$$1 < (\Omega : K) < \infty$$

145 *then K has characteristic zero and $\Omega = K(i)$, where i is a root of $x^2 + 1$.*

Proof. The proof is as follows:-

1) K is a perfect field. For if not $K^{p^{-\infty}} \subset \Omega$ and $K^{p^{-\infty}}$ is of infinite degree over K. This shows that Ω/K is a finite separable extension. Since it is is trivially normal, it is galois extension. Let n be the order of the galois group G of Ω/K.

2) If p is the characteristic of K, then $p \nmid n$ (if $p \neq o$). For, if p/n, then G has a subgroup of order p generated by an element σ. Let L be the fixed field of this subgroup. Then Ω/L is a cyclic extension of degree p. By corollary of theorem 11 it follows that Ω/L has infinite degree. This is a contradiction.

   Therefore, the order n of G is prime to the characteristic of K, if different from zero.

3) Let q be a prime dividing n. Then $q \neq p$. Let L now be the fixed field of a cyclic subgroup of G, of order q.

   Then Ω/L is cyclic, of order q. Now L contains the primitive qth root ρ of unity. For, if not since ρ satisfies an irreducible polynomial of degree $q - 1$, it follows that $L(\rho)/L$ has degree $q - 1$. But

$$(L(\rho) : L) | (\Omega : L)$$

   which means that $L(\rho) = L$. By theorem 9, therefore

$$\Omega = L(\omega_1)$$

where $\omega_1^q = \omega \in L$.

4) Any irreducible polynomial over L is either linear or of degree q. 146 For, if t is its degree and α, a root of it then $t = (L(\alpha) : L)$ divides q. Thus, every polynomial in $L[x]$ splits in L into product of linear factors and of factors of degree q.

Consider, in particular, the polynomial $x^{q^2} - \omega$. In Ω, we can write

$$x^{q^2} - \omega = \pi_\mu (x - \mu \sqrt[q^2]{\omega}) \tag{5}$$

where μ runs through all q^2 th roots of unity. Since $(\Omega : L) > 1$, the polynomial $x^{q^2} - \omega$ has, in $L[x]$, an irreducible factor of degree q. Since this factor is formed by q of the linear factors on the right of (5), this factor is of the form

$$x^q + \cdots + \varepsilon \sqrt[\varepsilon]{\omega},$$

ε being a q^2th root of unity. We assert that this is a primitive q^2th root of unity. For if not, it is either 1 or a primitive qth root of unity. Since $\varepsilon \sqrt[q]{\omega} \in L$, it would then follow that $\sqrt[q]{\omega} \in L$. Therefore we get

$$\Omega = L(\varepsilon).$$

5) Let Γ be the prime field contained in L. Consider the field $\Gamma(\varepsilon)$. Let $\Gamma(\varepsilon)$ contain the q^νth but not $q^{\nu+1}$ roots of unity. This integer certainly exists. For, if L has characteristic zero $\nu = 2$. If L has characteristic p (and this is different from q, from (2)), then $\Gamma(\varepsilon)$ contains p^f elements where f is the smallest positive integer with $p^f \equiv 1(\mod q^2)$. If q^ν is the largest power of q dividing $p^f - 1$ then $\Gamma(\varepsilon)$ contains the q^νth, but not the $q^{\nu+1}$ the roots of unity. 147

Let ρ be a primitive $q^{\nu+1}$th root of unity. Then ρ satisfies a polynomial of degree q(irreducible) over L. Thus $\Gamma(\rho)$ is of degree q over $\Gamma(\rho) \cap L$. Now, ρ being a primitive $q^{\nu+1}$th root of unity ρ^q is a q^νth root of unity and so is contained in $\Gamma(\varepsilon)$. But all the roots of $x^q - \rho^q$ are $q^{\nu+1}$th roots of unity. Thus $x^q - \rho^q$ is the irreducible polynomial of ρ over $\Gamma(\varepsilon)$. Hence

$$\begin{tikzcd}
 & \Gamma(\rho) \arrow[dl, dash] \arrow[dr, dash] & \\
\Gamma(\varepsilon) \arrow[dr, dash] & & \Gamma(\rho) \cap L \arrow[dl, dash] \\
 & \Gamma &
\end{tikzcd}$$

and $(\Gamma(\rho) : \Gamma(\varepsilon)) = q = (\Gamma(\rho) : (\Gamma(\rho) \cap L)$.

If Γ is a finite field, then $(\Gamma(\rho)/\Gamma$ is cyclic and it cannot have two distinct subfields $\Gamma(\varepsilon)$ and $\Gamma(\rho) \cap L$ over which it has the same degree. Since $\varepsilon \notin L$, it follows that $\Gamma(\varepsilon)$ and $\Gamma(\rho) \cap L$ are distinct and so, Γ has characteristic zero. In this case, if q is odd, $\Gamma(\rho)/\Gamma$ is cyclic and the same thing holds. Thus $q = 2$. We know, then that $\nu = 2$. If i denotes a fourth root of unity, then

$$\Omega = L(i).$$

6) Form above, it follows that $n = 2^t$ for some t and K does not contain the 4th root of unity. Now $t = 1$, for if not, let $t > 1$. Let M be a subfield of L such that $(L : M) = 2$. Then $(\Omega : M(i)) = 2$ and, by above considerations, $M(i)$ cannot contain 1 which is a contradiction. So

$$K(i) = \Omega.$$

148 We shall make use of this theorem in the next chapter. □

6 Kummer extensions

We now study the structure of finite abelian extensions of a field k. We use the following notation:-

k is a field of characteristic p, not necessarily $> o$.

n is a positive integer not divisible by p if $p \neq o$, otherwise arbitrary.

α, the group of non-zero elements of k. A generic element of α will also be denoted, following Hasse and Witt, by α.

α^n is the group of nth powers of elements of α.
ω, a subgroup of α containing α^n and such that

$$(\omega : \alpha^n) < \infty. \tag{6}$$

Let k contain the nth roots of unity. We shall establish $a(1, 1)$ correspondence between abelian extensions of k of exponent dividing n and subgroups ω of α satisfying (6).

Let K be an extension field obtained from k by adjoining to k the nth roots of all the elements of ω. We shall obtain some properties of K.

Since ω/α^n is a finite group, let $\lambda_1, \ldots, \lambda_t$ in ω, form a system of generators of ω mod α^n. Then any $\omega \in \omega$ is of the form

$$\omega = \lambda_1^{a1}, \ldots, \lambda_t^{ai} \alpha^n$$

where $a_1, \ldots, a_t$ are integers. Put $\Lambda_i = \lambda_i^{1/n}, i = 1, \ldots, t$. Then Λ_i is uniquely determined up to multiplication by an nth root of unity, which is already in k. This means that

$$K = k(\Lambda_1, \ldots, \Lambda_t).$$

149

Therefore

1) *K/k is a finite extension*.

Each Λ_i is a root of a polynomial of the form $x^n - \lambda_i$. This polynomial, by the condition on n, is separable over k. Also, $x^n - \lambda_i$ splits completely in K. Thus

2) *K/k is a finite galois extension and is the splitting field of the polynomial*

$$f(x) = \prod_{i=1}^{t} (x^n - \lambda_i)$$

over $k[x]$.

Let us denote by Λ the group generated by $\Lambda_1, \ldots, \Lambda_t$ and α. Let G denote the galois group of K/k. In the first place,

3) $\Lambda_{/\alpha} \simeq \omega_{/\alpha}n$. *(These are isomorphic groups).*

Consider the homomorphism $\Lambda \to \Lambda^n$ of Λ into itself. It takes α into α^n. The kernels in Λ and α are both the same. Since Λ is taken to ω by this homomorphism, it follows that $\Lambda/\alpha \simeq \omega/\alpha^n$. Incidentally, therefore, Λ/α is a finite group.

We shall now prove the important property,

4) *G is isomorphic to ω/α^n.*

(This proves that K/k is a finite abelian extension.)

In order to prove this, consider the 'pairing', (τ, Λ) of G and Λ, given by

$$(\sigma, \Lambda) = \Lambda^{1-\sigma}, \tag{7}$$

150 $\sigma \in G$, $\Lambda \in \Lambda$. Because of definition of Λ,

$$(\sigma, \Lambda)^n = \frac{\Lambda^n}{(\Lambda^n)^\sigma} = 1.$$

Thus (σ, Λ) is an nth root of unity. Also,

$$(\sigma\tau, \Lambda) = \frac{\Lambda}{\Lambda^{\sigma\tau}} = \frac{\Lambda}{\Lambda^\sigma} = \left(\frac{\Lambda}{\Lambda^\tau}\right)^\sigma = \frac{\Lambda}{\Lambda^\sigma} \cdot \frac{\Lambda}{\Lambda^\tau} = (\sigma, \Lambda) \cdot (\tau, \Lambda).$$

Furthermore,

$$(\sigma, \Lambda\Lambda') = \frac{\Lambda'\Lambda'}{(\Lambda'\Lambda)^\sigma} = \frac{\Lambda}{\Lambda^\sigma}, \frac{\Lambda'}{\Lambda^\sigma} = (\sigma, \Lambda)(\sigma, \Lambda').$$

Thus (σ, Λ) defined by (7) is a pairing.

Let G_o be the subgroup of G consisting of all σ with $(\sigma, \Lambda) = 1$, for all Λ. Since Λ is generated by $\Lambda_1, \Lambda_2, \ldots, \Lambda_t, \alpha$ we get

$$\Lambda_i = \Lambda_i^\sigma.$$

But $\Lambda_1, \ldots, \Lambda_t$ generate K. Therefore,$\beta = \beta^\sigma$ for all $\beta \in K$.

By galois theory, $\sigma = 1$. Thus $G_o = (1)$.

Let Λ_o be the subgroup of all Λ with $(\sigma, \Lambda) = 1$, for all σ. For the same reason as before, $\Lambda_o = \alpha$. Thus, by theorem on pairing, G is isomorphic to $\Lambda/_\alpha$. (4) is thus proved.

Observe, now, that since $\Lambda^n \subset \alpha$, it follows the G is an abelian group whose exponent divides n.

We will denote K symbolically by $K = k(\sqrt[\tau]{\omega})$.

We shall now prove

Theorem 13. *Let K/k be a finite extension with abelian galois group G of exponent dividing n, then $K = k(\sqrt[n]{\omega})$ for a sub group $\omega \subset \alpha$ with $\omega_{/\alpha}n$ finite.*

Proof. Let $\overline{\Lambda}$ denote the group of non-zero elements of K with the property $\Lambda^n \in \alpha$ for $\Lambda \in \overline{\Lambda}$. Then, by considering the homomorphism $\Lambda \to \Lambda^n$, it follows that 151

$$\overline{\Lambda}_{/\alpha} \simeq \omega_{/\alpha}n,$$

where $\omega = \overline{\Lambda}^n$. We shall prove that $K = k(\sqrt[n]{\overline{\omega}})$. In order to prove this, it suffices to prove that

$$G \simeq \omega_{/\alpha}n. \tag{8}$$

□

For, in that case, construct the field $k(\sqrt[n]{\omega})$. Because of the properties of K, it follows that $K \supset k(\sqrt[n]{\overline{\omega}})$. But, by the previous results, $(k(\sqrt[n]{\omega}) : k)$ = order of $\omega_{/\alpha}n$ = order of G.

Hence

$$K = k(\sqrt[n]{\omega}).$$

We shall, therefore, prove (8).

Let $G*$ denote the dual of G. For every Λ in $\overline{\Lambda}$, define the function

$$\chi_\Lambda(\sigma) = \Lambda^{1-\sigma}$$

on G into $\overline{\Lambda}$. Since $\Lambda^n \in \alpha$, it follows that $\chi_\Lambda(\sigma)$ is an *nth* root of unity. Also,

$$\chi_\Lambda(\sigma\tau) = \frac{\Lambda}{\Lambda^{\sigma\tau}} = \frac{\Lambda}{\Lambda^{\sigma}}\left(\frac{\Lambda}{\Lambda^{\tau}}\right)^{\sigma} = \frac{\Lambda}{\Lambda^{\sigma}} \cdot \frac{\Lambda}{\Lambda^{\tau}} = \chi_\Lambda(\sigma)\cdot\chi_\Lambda(\tau)$$

so that χ_Λ is a character of G.

Let χ be any character of G. Since the exponent of G divides n, $\chi^n(\sigma) = 1$ for all σ. Therefore, $\chi(\sigma)$ is an nth root of unity and hence is an element of k. Also, since χ is a character of G,

$$\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$$

152 which equals $\chi(\sigma) \cdot (\chi(\tau))^{\sigma}$. Thus $\chi(\sigma)$ is a one cocycle and, by theorem 7,

$$\chi(\sigma) = \beta^{1-\sigma}$$

for $\beta \in K$. But $(\chi(\sigma))^n = 1$ so that

$$\beta^n = (\beta^n)^{\sigma}$$

for all σ or $\beta^n \in \alpha$. This means, by definition of $\bar{\Lambda}$ that $\beta \in \bar{\Lambda}$.

Consider the mapping $\omega \to \chi_{\Lambda}$ of $\bar{\Lambda}$ into G^*. This is, trivially a homomorphism. By above, it is a homomorphism onto. The kernel of the homomorphism is set of Λ for which $\chi_{\Lambda}(\sigma) = 1$ for all σ. That is

$$\Lambda = \Lambda^{\sigma}$$

for all σ. By galois theory $\Lambda \in \alpha$. But every element in α satisfies this condition. Thus α is precisely the kernel, and

$$\bar{\Lambda}_{/\alpha} \simeq G^*.$$

Since G is a finite abelian group, $G \simeq G^*$ and our theorem is completely proved.

We call a finite abelian extension K/k, a *Kummer extension* if

1) k contains the nth roots of unity, $p \nmid n$, if $p(\neq o)$ is characteristic of k,

2) K/k has a galois Galois group of exponent dividing n.What we have then proved is

Theorem 14. *The Kummer extensions of k stand in $(1, 1)$ correspondence with subgroups ω of α with $\omega_{/\alpha}n$ finite.*

7 Abelian extensions of exponent p

153 We had introduced earlier the operator $\mathscr{P}$ which is defined by

$$\mathscr{P}x = x^p - x.$$

Let k be a field of characteristic p and denote by k^+ the additive group of k. Then $\alpha \to \mathscr{P}\alpha$ is a homomorphism of k^+ into itself. The kernel of the homomorphism is precisely the set of elements in Λ, the prime field of characteristic p, contained in k.

If $\alpha \in k$, we denote by $\dfrac{\alpha}{\mathscr{P}}$, a root of the polynomial $x^p - x - \alpha$. Obviously $\dfrac{\alpha}{\mathscr{P}}$ is p valued. Also,

$$\frac{\alpha+\beta}{\mathscr{P}} = \frac{\alpha}{\mathscr{P}} + \frac{\beta}{\mathscr{P}}. \tag{9}$$

Let us denote by $\mathscr{P}k^+$, the subgroup of k^+ formed by elements $\mathscr{P}\alpha$, $\alpha \in k^+$. Let ω be a subgroup of k^+ with the properties,

$$k^+ \supset \omega \supset \mathscr{P}k^+$$

$$\omega/_{\mathscr{P}k^+} \text{ is finite.}$$

Let K be the extension field of k, formed by adjoining to k all the elements $\dfrac{\alpha}{\mathscr{P}}$, fro $\alpha \in \omega$. We denote

$$K = k(\frac{\omega}{\mathscr{P}}).$$

We then obtain in exactly the same way as before

1) K/k is a finite abelian extension.

2) The galois group G of K/k is isomorphic with $\omega/_{\mathscr{P}k^+}$.

3) G is an abelian group of exponent p. For the proofs, we have to use additive, instead of multiplicative, pairing and the property (9).

Suppose, now, on the other hand, K/k is a finite abelian extension of exponent p, where p is the characteristic of k. 154

Then

$$K = k(\frac{\omega}{\mathscr{P}}),$$

where ω is a subgroup of k^+ with $\omega/\mathscr{P}k^+$ finite. For the proof of this, we have to use additive instead of multiplicative, cohomology. For, let G be the galois group of K/k and G^* its character group. Denote, by $\overline{\Lambda}$, the additive subgroup of K^+ formed by elements Λ with $\mathscr{P}\Lambda \in k^+$. Denote, by ω, the group $\mathscr{P}\overline{\Lambda}$. Then

$$\overline{\Lambda}_{/k^+} \simeq \omega_{/\mathscr{P}k^+}$$

Define $\chi_\Lambda(\sigma)$ by

$$\chi_\Lambda(\sigma) = \Lambda - \Lambda^\sigma.$$

Then

$$\mathscr{P}(\chi_\Lambda(\sigma)) = \mathscr{P}\Lambda - (\mathscr{P}\Lambda)^\sigma).$$

But, $\mathscr{P}\Lambda \in k^+$ by definition. Hence, $\mathscr{P}(\chi_\Lambda(\sigma)) = o$.

Therefore, $\chi_\Lambda(\sigma)$ is an element of Γ. The rest of the proof goes through in the same way and we have the

Theorem 15. *If k has characteristic $p \neq o$, the finite abelian extensions K/k of exponent p stand in a$(1,1)$ correspondence with subgroups ω of k^+ such that $\omega/\mathscr{P}k^+$ is finite, and then $K = k(\frac{\omega}{\mathscr{P}})$.*

8 Solvable extensions

We propose to study now the main problem of the theory of algebraic equations, namely the 'solution' of algebraic equations by radicals

155 k will denote a field of characteristic p,$(p = o$ or $p \neq o)$, Ω will be its algebraic closure and $n, n_1, n_2, \ldots$ integers $> o$ which are prime to p, if k has characteristic $p \neq o$, otherwise arbitrary. An element $\omega \in \Omega$ will be said to be a *simple radical* over k if $\omega^n \in k$, for some integer n. $k(\omega)/k$ is then said to be a *simple radical extension*. $k(\omega)/k$ is clearly separable. If ω is a root of $x^p - x - a$, for a $\in k, \omega$ is called a *simple pseudo radical*

over $k.k(\omega)/k$ is a *pseudo radical extension* and is separable. In fact, it is a cyclic extension over k. This situation occurs, only if $p \neq o$.

An extension field K/k is said to be a *generalized radical extension* if it is a finite tower

$$k = K_o \subset K_1 \subset K_2 \subset \cdots \subset K_m = K$$

where K_i/K_{i-1} is either a simple radical or a simple pseudo radical extension. Every element it K is called a *generalized radical*. A typical element would be

$$\sqrt[n_1]{a_1 + \sqrt[n_2]{a_2 + \frac{a_3}{\mathscr{P}} + ..}}$$

Clearly, K/k is a separable extension. A generalized radical extension is called a *radical extension* if K_i/K_{i-1} is a simple radical extension for every i. A typical element of K would, then be

$$\sqrt[n_1]{a_1 + \sqrt[n_2]{a_2 + \cdots}}.$$

Let $f(x)$ be a polynomial in $k[x]$ and let it be separable. Let K be its splitting field. Then K/k is a galois extension. The galois group G of K/k is called the *group of the polynomial* $f(x)$. The polynomial $f(x)$ is said to be *solvable by generalized radicals*, if K is a subfield **156** of a generalized radical extension. It is, then, clear that the roots of $f(x)$ are generalized radicals. In order to prove the main theorem about solvability of a polynomial by generalized radicals, we first prove some lemmas.

Lemma 1. *Every generalized radical extension is a subfield of a generalized radical extension which is galois, with a solvable galois group.*

Proof. Let K/k be a generalized radical extension so that

$$k = K_o \subset K_1 \subset \cdots \subset K_m = K,$$

where K_i/K_{i-1} is a simple radical or simple pseudo radical extension. Let $K_i = K_{i-1}(\omega_i)$. Then either $\omega_i^n \in K_{i-1}$ for some n_i or $\mathscr{P}\omega_i \in K_{i-1}$. Let $(K : k) = n$. Put $N = n$, if k has characteristic zero; otherwise, let

$$n = N \cdot p^a,$$

$a \geq o, (p, N) = 1$. Let ρ be a primitive Nth root of unity. □

Let $L_1 = K_o(\rho)$. The L_1/K_o is a simple radical extension. Since $K_1 = K_o(\omega_1)$, put $L_2 = K_o(\rho, \omega_1)$. Then L_2 is the splitting field of the polynomial $(x^N - 1)(x^{n1} - a_1)$ or $(x^N - 1)(\mathscr{P}x - a_1)$ depending on whether ω_1 is a simple radical or a simple pseudo radical. In any case, $L_2/K_o$is a galois extension. Furthermore

$$L_2 = L_1(\omega_1)$$

so that L_2/L_1 is cyclic, since, when ω_1 is a simple radical, L_1 contains 157 the requisite roots of unity. Let $\sigma_1, \ldots, \sigma_\ell$ be the distinct automorphisms of L_2/K_o. Put

$$f(x) = \prod_{i=1}^{\ell} (x^{n2} - a_2^{\sigma i}),$$

if ω_2 is a simple radical with $\omega_2^{n_2} = a_2$, and

$$f(x) = \prod_{i=1}^{\ell} (\mathscr{P}x - a_2^{\sigma_i}),$$

if ω_2 is a simple pseudo radical with $\mathscr{P}\omega_2 = a_2$.

Then $f(x)$ is a polynomial in $k[x]$. Let L_3 be its splitting field. Then L_3 is galois over k. Also, L_3 is splitting field of $f(x)$ over L_3 so that L_3/L_2 is either a Kummer extension or else, an abelian extension of exponent p. In this way, one constructs a galois extension T of k such that

$$L_o = k \subset L_1 \subset L_2 \subset L_3 \subset \cdots \subset L_{m-1} \subset T = L_m,$$

where L_i/L_{i-1} is either a kummer extension or an abelian extension of exponent p. Clearly, L_i/L_{i-1} and, hence, T/k is a generalized radical extension. Let $G_i, i = o, 1, 2, \ldots, m$ be the galois group of T/L_i. Then

$$G = G_o \supset G_1 \supset \ldots\ldots \supset G_m = (e)$$

is a normal series. Further, by our construction, G_{i-1}/G_i is the galois group of L_i/L_{i-1} and hence, abelian. Thus, G is a solvable group. The lemma is thus proved.

Lemma 2. *If K/k is a finite solvable extension, then K is a subfield of a generalized extension over k.*

Proof. Let G be the galois group of K/k and G solvable. Let n be the order of G and put

$$n = p^a N$$

with the same connotation, as before. Let ρ be a primitive Nth root of 158
unity and $L = k(\rho)$. Then L/k is a simple radical extension. Let M be a composite of K and L. Then M/L is a galois extension with a galois group which is isomorphic to a subgroup of G and hence, solvable. Let G_o be the galois group of M/L and let it have a composition series

$$G_o \supset G_1 \supset \cdots \supset G_m = (e).$$

□

Then G_i/G_{i+1} is a cyclic group of prime degree. Let $L_o = L$, $L_1, \ldots L_m = M$ be the fixed fields of $G_o, G_1, \ldots, G_m$ respectively. Then L_i/L_{i-1} is a cyclic extension of prime degree. Since L_{i-1} contains the requisite roots of unity, L_i is a simple radical or a simple pseudo radical extension of L_{i-1}. Then M/k is a generalized radical extension and our lemma is proved.

We are, now, ready to prove

Theorem 16. *A separable polynomial $f(x) \in k[x]$ is solvable by generalized radicals if and only if its group is solvable.*

Proof. Let K be the splitting field of $f(x)$ and G the galois group of K/k. Suppose $f(x)$ is solvable by generalized radicals. Then $K \subset L$ where L/k is galois and by lemma 1, has solvable galois group H. Let G_o be the galois group of L/K Then H/G_o is isomorphic to G and so G is solvable. □

Let, conversely, G be solvable. Then, by lemma 2, K is contained in a generalized radical extension and so $f(x)$ is solvable by generalized radicals.

We can easily prove 159

Corollary. *A separable polynomial $f(x) \in k[x]$ is solvable by radicals if and only if its splitting field has a solvable galois group of order prime to the characteristic of k, if different from zero.*

Let k be a field. The polynomial

$$f(x) = x^m - x_1 x^{m-1} + x_2 x^{m-2} \cdots + (-1)^m x_m,$$

where $x_1, \ldots, x_m$ are algebraically independent over k, is said to be the *general polynomial* of the mth degree over k. It is so called, because every monic polynomial of degree m over k is obtained by specializing the values of $x_1, \ldots, x_m$ to be in k. Let $L = k(x_1, \ldots, x_m)$. Let $y_1, \ldots, y_m$ be roots of $f(x)$ over L. Then

$$f(x) = (x - y_1) \cdots (x - y_m)$$

and $y_1, \ldots, y_m$ are distinct. The splitting field $k(y_1, \ldots, y_m)$ of $f(x)$ over L is a galois extension whose galois group is isomorphic to S_m. Hence, the general polynomial of the mth degree over k has a group isomorphic to the symmetric group on m symbols.

But,S_m is not solvable, if $m > 4$, so that in virtue of theorem 16, we have the theorem of *Abel*.

Theorem 17. *The group of the general polynomial $f(x)$ of the mth degree is isomorphic to the symmetric group S_m on m symbols and hence, for m > 4, $f(x)$ is not solvable by generalized radicals.*

We shall now explicitly show how to obtain the roots of a polynomial of degree ≤ 4 in terms of generalized radicals.

160 Let $f(x)$ be a general polynomial of degree m over k and let K be the splitting field. K/k has the group S_m. Let $y_1, \ldots, y_m$ be the roots of $f(x)$. Put

$$D = \prod_{i<j} (y_i - y_j)^2.$$

Then D is fixed under all permutations in S_m and, hence, $D \in k$. If we assume that the characteristic of k is $\neq 2$, then $k(\sqrt{D})$ is a galois extension of k and $K/k(\sqrt{D})$ has the galois group isomorphic to the alternating group on m symbols. D called the *discriminant of the polynomial* $f(x)$.

Let us, first, consider the general polynomial of the second degree

$$f(x) = (x - y_1)(x - y_2) = x^2 - x_1 x + x_2.$$

Then

$$y_1 + y_2 = x_1, y_1 y_2 = x_2.$$

Suppose, now, that k has characteristic $\neq 2$. Then

$$D = (y_1 - y_2)^2 = (y_1 + y_2)^2 - 4y_1 y_2 = x_1^2 - 4x_2.$$

Also, $y_1 + y_2 = x_1, y_1 - y_2 = \pm\sqrt{D}$ so that

$$y_1 = \frac{x_1 + \sqrt{D}}{2}, y_2 = \frac{x_1 - \sqrt{D}}{2}$$

and $K = k(\sqrt{D})$ is the splitting field of $f(x)$ and is a radical extension.

Let, now, k have characteristic 2. Then $x_1 \neq o$, since $f(x)$ is separable. Put $x_1 x$ instead of x. Then the polynomial $x^2 - x + \frac{x_2}{x_1^2}$ has roots $\frac{y_1}{x_1}$ and $\frac{y_2}{x_1}$. But this is a normal polynomial so that if $\lambda = \frac{x_2}{{x_1}^2}$, then 161

$$y_1 = x_1 \frac{\lambda}{\mathscr{P}}, y_2 = x_1 \frac{\lambda}{\mathscr{P}} + x_1$$

and thus $k(\frac{\lambda}{\mathscr{P}})$ is a pseudo radical extension and is splitting field of $f(x)$.

We shall now study cubic and biquadratic polynomials.

Let, first, *k have characteristic* $\neq 2$ or 3. Let $m = 3$ or 4 and

$$f(x) = x^m - x_1 x^{m-1} + \cdots + (-1)^m x_m$$

be the polynomial of the mth degree whose roots are $y_1, \ldots, y_m$.

If we put $x + \frac{x_1}{m}$ instead of x, we get a polynomial whose roots are $y_1 - \frac{x_1}{m}, \ldots, y_m - \frac{x_1}{m}$ and which lacks the terms in x^{m-1}.

We shall, therefore, take the polynomial $f(x)$ in the form

$$f(x) = x^m + x_2 x^{m-2} + \ldots + (-1)^m x_m.$$

If $y_1, \ldots, y_m$ are the roots, then

$$y_1 + y_2 + \ldots + y_m = o.$$

Also , $D_m = \prod\limits_{i<j} (y_i - y_j)^2$. A simple computation shown that

$$D_3 = -4x_2^3 - 27x_3^2$$

and

$$D_4 = 16x_2^4 x_4 - 4x_2^3 x_3^2 - 128x_2^2 x_4^2 + 144x_2 x_3^2 x_4 \\ -27x_3^4 + 256x_4^3.$$

If K is the splitting field of $f(x)$ over $L = k(x_1, \ldots, x_m)$ then $L(\sqrt{D})$ is the fixed field of the alternating group A_m and $L(\sqrt{D})/L$ is a radical extension. In order to study the extension $K/L(\sqrt{D})$, let us, first, take the case $m = 3$. The symmetric group on 3 symbols, S_3, has the composition series

$$S_3 \supset A_3 \supset (e).$$

162 $K/L(\sqrt{D})$ is thus a cyclic extension of degree 3. Let ρ be a primitive cube root of unity and let $M = L(\sqrt{D}, \rho)$. Let $N = KM$ be a composite of K and M. Then KM/M has degree 1 or 3, according as ρ is in K or not. In the first case, $M = K$. In the second case, KM/M is a cyclic extension of degree 3 over K and M contains the cube roots of unity. Thus $KM = M(\sqrt[3]{\omega})$, for some $\omega \in M$. In order of determine this ω, we use Lagrange's method.

KM is the splitting field over M of the polynomial $x^3 + x_2 x - x_3$. Let y_1, y_2, y_3 be roots of this polynomial. Put

$$\omega = y_1 + \rho y_2 + \rho^2 y_3$$
$$\omega' = y_1 + \rho^2 y_2 + \rho y_3.$$

Then $\omega^3 = \dfrac{27}{2}x_3 + 3\sqrt{D}(\rho - \frac{1}{2})$. Changing ρ into ρ^2 we get ω'^3. Hence

$$\omega = \rho^a \sqrt[3]{\frac{27}{2}x_3 + 3\sqrt{D}(\rho - \frac{1}{2})}$$

and we have a similar expression for ω'. Here $a \geq o$. In order to determine $\underline{a}$, we use the fact that $\omega\omega' = -3x_2$ and so, choosing the root of unity ρ^a for ω arbitrarily, the root of unity in the expression for ω' is uniquely determine. Now

$$\begin{aligned} y_1 + y_2 + y_3 &= o \\ y_1 + \rho y_2 + \rho^2 y_3 &= \omega \\ y_1 + \rho^2 y_2 + \rho y_3 &= \omega' \end{aligned}$$

and since the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \rho & \rho^2 \\ 1 & \rho^2 & \rho \end{pmatrix}$$

is non-singular, the values of y_1, y_2, y_3 are uniquely determined $K \cdot M$ is a radical of L and contains K. **163**

Consider, now, the polynomial of the fourth degree

$$f(x) = x^4 + x_2x^2 - x_3x + x_4$$

whose roots are y_1, y_2, y_3, y_4 with $y_1 + y_2 + y_3 + y_4 = o$. The galois group of the splitting field K/k is S_4. This has the composition series

$$S_4 \supset A_4 \supset B_4 \supset C_4 \supset (e).$$

Let K_1, K_b, K_c be the fixed fields of A_4, B_4 and C_4 respectively. Now A_4 is the alternating group, B_4 the group consisting of the permutations

$$(1), (12)(34), (13)(24), (14)(23)$$

and C_4 is the group of order 2 formed by

$$(1), (12)(34).$$

$K_a = k(\sqrt{D})$ and is of degree 2 over k. Now K_b/K_a is of degree 3 and is cyclic. Hence $K_b = K_a(\theta)$ where $\theta \in K$ is an element fixed by B_4 but not by A_4. Such as elements, for instance, is

$$\theta_1 = (y_1 + y_2)(y_3 + y_4).$$

θ_1 has 3 conjugates θ_1, θ_2, θ_3 obtained from θ_1 by operating on θ_1, by representatives of cosets of A_4/B_4. Thus

$$\theta_2 = (y_1 + y_3)(y_2 + y_4)$$
$$\theta_3 = (y_1 + y_4)(y_2 + y_3).$$

164 Consider the polynomial

$$\varphi(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3).$$

It is fixed under A_4 and so, its coefficients are in K_a. A simple computation shows that

$$\varphi(x) = x^3 - 2x_2x^2 + (x_2^2 - 4x_4)x + x_3^2.$$

$\varphi(x)$ is called the *reducing cubic* or the *cubic resolvent*. By the method adopted for the solution of the cubic, if ρ is a primitive cube root of unity and $M = K_a(\rho)$, then K_bM, the composite, is a radical extension of k in which θ_1, θ_2, θ_3 lie.

K_c/K_b is of degree 2 and so $K_c = K_b(\alpha)$ where α is fixed under B_4, but not by C_4. such as element is

$$\alpha = y_1 + y_2.$$

Now $\alpha^2 = (y_1 + y_2)^2 = -(y_1 + y_2)(y_3 + y_4) = -\theta_1$. Thus $K_c = K_b(\sqrt{-\theta_1})$. Hence, if $K_bM = K_d$, then $K_d(\alpha)$ is a radical extension of k containing α. Put now

$$T = K_d(\alpha, \beta)$$

where $\beta = y_1 + y_3 = \sqrt{-\theta_3}$. Then T is a radical extension of k containing K. The indeterminacy signs in taking the square roots of $-\theta_1$ and $-\theta_3$ can be fixed by observing that

$$(y_1 + y_2)(y_1 + y_3)(y_1 + y_4) = x_3.$$

we now have

$$y_1 + y_2 = \sqrt{-\theta_1}, y_3 + y_4 = -\sqrt{-\theta_1}$$
$$y_1 + y_3 = \sqrt{-\theta_2}, y_2 + y_4 = -\sqrt{-\theta_2}$$
$$y_1 + y_4 = \sqrt{-\theta_3}, y_2 + y_3 = -\sqrt{-\theta_3}.$$

for which y_1, y_2, y_3, y_4 can be obtained. We have, hence, proved **165**

Theorem 18. *If K has characteristic $\neq 2$ or 3, then the cubic and biquadratic polynomials over k can be radicals.*

Let us, now, assume that *k has characteristic* 3. Let $x^3 + x_1x^2 + x_2x + x_3$ be a cubic polynomial and K, its splitting field. K/k has the galois group S_3. Let L be the fixed field. K/k has the galois group S_3. Let L be the fixed field of A_3. Then

$$L = k(\sqrt{D})$$

where

$$D = (y_1 - y_2)^2(y_2 - y_3)^2(y_3 - y_1)^2.$$

K/L is now a cyclic extension of degree 3 and since k has characteristic 3, $K = L(\omega)$, where

$$\omega^3 - \omega - \alpha = o$$

for some $\alpha \in L$. Thus K is a generalized radical extension. We shall now determine ω and α and therefrom, y_1, y_2 and y_3.

In order to do this, we have to consider two cases, $x_1 = o$, and $x_1 \neq o$.

Let, first, $x_1 = o$. Then $y_1 + y_2 + y_3 = o$. Let σ be a generator of the galois group fo K/L and let notation be so chosen that

$$y_1^\sigma = y_2, y_2^\sigma = y_3, y_3^\sigma = y_1.$$

Since $S_{K/L}y_1 = y_1 + y_1^\sigma + y_1^{\sigma^2} = o$, by Hilbert's theorem, there is a λ in K such that

$$y_1 = \lambda^\sigma - \lambda.$$

Also 166

$$x_2 = y_1y_2 + y_2y_3 + y_3y_1 = \sum_{\sigma}(\lambda^\sigma - \lambda)(\lambda^{\sigma^2} - \lambda^\sigma) = -(\lambda + \lambda^\sigma + \lambda^{\sigma^2})^2.$$

Since $x_2 \neq o$ (otherwise, polynomials is not separable), we see that $x_2 = -t^2$, for some $t \in L$. The polynomial, therefore, has the form

$$x^3 - t^2x + x_3.$$

Put now tx for x. Then the polynomial $x^3 - x + x_3/t^3$ has roots $\frac{y_1}{t}$, $\frac{y_2}{t}$, $\frac{y_3}{t}$. Let $\omega = x_3/t^3$. Then

$$y_1 = t\frac{\omega}{\mathscr{P}}, \quad y_2 = t\frac{\omega}{\mathscr{P}} + t, \quad y_3 = t\frac{\omega}{\mathscr{P}} + 2t$$

and thus the roots are all obtained.

The indeterminacy in the sign of t does not cause any difficulty; for, if we use $(-t)$ instead of t, then, observing that $-\frac{\omega}{\mathscr{P}} = \frac{-\omega}{\mathscr{P}}$, we see that

$$y_1 = -t\frac{-\omega}{\mathscr{P}}, y_3 = -t\frac{-\omega}{\mathscr{P}} - t, y_2 = -t\frac{-\omega}{\mathscr{P}} + t$$

so that y_2 and y_3 get interchanged.

We now consider the case $x_1 \neq o$.

Put $x + a$ instead of x. Then the new polynomial is

$$x^3 + x_1x^2 + x(x_2 + 2x_1a) + x_3 + x_2a + a^2 + a^3.$$

Choose $\underline{a}$ so that $x_2 + 2x_1a = o$. For this value of $\underline{a}$, $\mu = x_3 + x_2a + a^2 + a^3 \neq o$; for, otherwise, the polynomial will be reducible and the roots are $o, o, -x_1$. The roots of this new polynomial are $y_1 - a, y_2 - a, y_3 - a$.

Let now $\frac{1}{x}$ be written for x, then the polynomial is reduced to $x^3 + \frac{x_1}{\mu}x + \frac{1}{\mu}$. We are in the previous case. The roots, now, are $\frac{1}{y_1 - a}$, $\frac{1}{y_2 - a}$,
167 $\frac{1}{y_3 - a}$. If $-t^2 = \frac{x_1}{\mu}, t \in L$ and $\nu = \frac{1}{\mu t^3}$, then $K = L(\frac{\nu}{\mathscr{P}})$ and the roots

y_1, y_2, y_3 are given by

$$y_1 = a + \frac{1}{t\frac{\nu}{\mathscr{P}}}, y_2 = a + \frac{1}{t + t\frac{\nu}{\mathscr{P}}}, y_3 = a + \frac{1}{2t + t\frac{\nu}{\mathscr{P}}}$$

Since the characteristic is 3, the biquadratic polynomial can be taken in the form

$$x^4 + x_2x^2 + x_3x + x_4.$$

The proof is similar to the old one except that K_b/K_a is a cyclic extension of degree 3 and so $K_b = K_a\left(\frac{\omega}{\mathscr{P}}\right)$ for a suitable ω in K_a. To find ω, we use the foregoing method. One finds that K is a generalized radical extension.

We now consider the case where *k has characteristic* 2. In this case, the cubic polynomial cab be taken in the form, $x^3 + x_2x + x_3$. Let y_1, y_2, y_3 be the roots. Then

$$y_1 + y_2 + y_3 = o$$

and therefore $y_1^2 + y_2^2 = y_3^2$ and so on. Put

$$\omega = \frac{y_1}{y_2} + \frac{y_2}{y_3} + \frac{y_3}{y_1},$$
$$\omega' = \frac{y_2}{y_1} + \frac{y_3}{y_2} + \frac{y_1}{y_3}.$$

Then

$$\omega + \omega' = \frac{y_1(y_2^2 + y_3^2) + y_2(y_3^2 + y_1^2) + y_2(y_1^2 + y_2^2)}{y_1y_2y_3} = 1,$$

which shows that $\omega \notin k$, because ,then, it will be symmetric and equal to ω'. Thus $k(\omega)$ is a quadratic subfield of K. A simple computation shows that ω and $\omega' = \omega + 1$ are roots of

$$x^2 - x + x_2^3.$$

$K/k(\omega)$ is cyclic of degree 3 and one uses the method of Lagrange **168**
to obtain a generalized radical extension.

Suppose now that $f(x)$ is a polynomial of degree 4. Let $f(x) = x^4 + x_1x^3 + x_2x^2 + x_3x + x_4$. We have to consider two cases. Let, first, $x_1 = o$. Then the roots y_1, y_2, y_3, y_4 satisfy

$$y_1 + y_2 + y_3 + y_4 = o.$$

As before, put

$$\theta_1 = (y_1 + y_2)(y_3 + y_4), \quad \theta_2 = \ldots, \theta_3 = \cdots$$

The reducing cubic is then

$$\varphi(x) = x^3 + x_2^2x + x_3.$$

Furthermore $\theta_1 + \theta_2 + \theta_3 = o$. Put now

$$\omega = \frac{\theta_1}{\theta_2} + \frac{\theta_2}{\theta_3} + \frac{\theta_3}{\theta_1}.$$

Then ω is fixed under A_4 but not under S_4. Also $K_a = k(\omega)$ is a simple pseudo radical extension.

Now K_b/K_a is a cyclic extension of degree 3 and has to be solved by Lagrange's methods. Further, K_c/K_b is of degree 2. Put now

$$\omega_1 = \frac{y_3}{y_1y_2y_4}, \quad \omega_1' = \frac{y_4}{y_1y_2y_3}.$$

Then

$$\omega_1 + \omega_1' = \frac{y_3^2 + y_4^2}{y_1y_2y_3y_4} = \frac{(y_1 + y_2)(y_3 + y_4)}{y_1y_2y_3y_4} = \frac{\theta_1}{x_4}.$$

We assume $x_3 \neq o$. Then $\theta_1 \neq o$. If we put

$$\omega_2 = \frac{x_4\omega_1}{\theta_1}, \quad \omega_1' = \frac{x_4\omega_1'}{\theta_1},$$

169 then $\omega_2 + \omega_2' = 1$ and $K_c = K_b(\omega_2)$.

In similar manner, $K = K_c(\omega_3)$ where

$$\omega_3 = \frac{x_4}{\theta_2}, \quad \frac{y_1}{y_2y_3y_4}.$$

Suppose, now, that $x_1 \neq o$. Then, as before, we construct the field K_b. In order to exhibit K_c as a pseudo radical extension of K_b, observe that $y_1 + y_2$ is fixed under C_4 but not under B_4. Also

$$(y_1 + y_2)^2 = (y_1 + y_2)(y_3 + y_4 + x_1) = \theta_1 + x_1(y_1 + y_2)$$

which shows that

$$K_c = K_b \left(\frac{y_1 + y_2}{x_1} \right).$$

Similarly, $K = K_c \left(\dfrac{y_1 + y_3}{x_1} \right)$.

Our contentions are completely established.

Chapter 7

Formally real fields

1 Ordered rings

170 A commutative ring R is said to be *ordered* if there is an ordering relation $>$ (greater than) such that

(1) for every $a \in R$, $a > o$, $a = o$ or $-a > o$.

(1) $a, b \in R, a > o, b > o \Rightarrow a + b > o, ab > o$.

We may then define $a > b$ by $a - b > o$. If $a > b$, then, for any c in R, $a + c > b + c$ and if $c > o$, $ac > bc$.

If $-a > o$, we shall say a is *negative* and if $a > o$, a said to be *positive*. We denote “$\underline{a}$ is negative” by $a < o$.

Let us denote, by P, the set of elements $a \in R$ with $a \geq o$. Then, from the definition or ordered ring, we have

$$A_1) P + P \subset P$$
$$A_2) P \cdot P \subset P$$
$$A_3) P \cap (-P) = (o)$$
$$A_4) P \cup (-P) = R,$$

where $P + P$ denotes the set of elements of R of the form $a + b$, $a, b \in P$; $-P$ denotes the set of elements $-a$, $a \in P \cdot P$ shall be called the set of *non-negative elements of* R. The only element which is both positive and negative is zero. Clearly, if R is a any subset P of R satisfying the four conditions above again determine an order on R.

Two elements $a, b \in R$, $a \neq o \neq b$ are said to have the *same* or *opposite signs* according as $ab > o$ or $ab < o$.

171 Let now R be an ordered ring with unit element 1. Let $a \in R$, $a \neq o$. Then $a^2 = a \cdot a = (-a) \cdot (-a)$, so that $a^2 > o$ for $a \neq o$ in R. More generally, every finite sum of squares of elements of R is positive. These elements will be contained in the set of non-negative elements in every order of R.

Since R has a unit element 1 and $1^2 = 1$, we have $1 > o$. Also, $n \cdot 1 = 1 + 1 \cdots + 1$, n times so $n > o$. This proves

1) *An ordered ring with unit element has characteristic o.*

   Let $a \neq o$, $b \neq o$ be elements of R. Then a or $-a$ is positive. Similarly b or $-b$ is positive. Hence ab or $-ab$ is positive which proves that $ab \neq o$. Therefore

2) *An order ring is an integrity domain*.

   We define an ordered field to be an ordered ring whose non-zero elements form a multiplicative commutative group. We have

3) *If k is an ordered field, its positive elements form a multiplicative group*.

   For, if $x \in k$, $x > o$; then $xx^{-1} > o$. If $-x^{-1} > o$, then $-xx^{-1} > o$ which contradicts $x^{-1}x > o$. Thus $x^{-1} > o$ and (3) is proved. Suppose R and R' are two rings, $R \subset R'$. If R' is ordered, clearly R is ordered by means of the induced order. If however, R is ordered, it may not be possible, in all cases, to extend this order to R'. However, in case, it is always possible, namely

4) *If K is the quotient field of an ordered ring R then the order in R can be uniquely extended to K*.

172 *Proof.* Let R have an order. It is an integrity domain. Any elements $x \in K$ is of the form $x = \frac{a}{b}$, $a, b \in R$, $b \neq o$. Let $x \neq o$. Then $a \neq o$.

define $x > o$ by $ab > o$. Then this defines an order in K. In the first place, the definition does not depend on the way x is expressed in the form $\frac{a}{b}$. Suppose $x = \frac{a'}{b'}$. Then $ab' = a'b$. Since $b' \neq o$, multiplying both sides of this equality by bb', we have

$$ab \cdot b'^2 = a'b' \cdot b^2.$$

□

Since $ab > o$, $b'^2 > o$, $b^2 > o$, it follows that $a'b' > o$, that is $\frac{a'}{b'} > o$.

In order to prove that $A_1, \ldots, A_4$ are satisfies, let $x = \frac{a}{b} > o$ and $y = \frac{a'}{b'} > o$. Then $ab > o$ and $a'b' > o$.

$$x + y = \frac{ab' + a'b}{bb'}$$

Now $(ab' + a'b)bb' = ab \cdot b'^2 + a'b' \cdot b^2$. Since $ab > o$, $a'b' > o$, $b^2 > o$, $b'^2 > o$, it follows that $(ab' + a'b)bb' > o$ or $x + y > o$. In similar manner, $xy > o$.

Suppose $x \geq o$ and $y \geq o$ and $x + y = o$; then $x = o$, $y = o$. For, if $x = \frac{a}{b}$, $y = \frac{c}{d}$, then $ab \geq o$, $cd \geq o$ and $x + y = \frac{ad + bc}{bd} = o$, so that $ad + bc = o$. Thus $abd^2 + cdb^2 = o$, which means that since all elements are in R, $ab = o$, $cd = o$, i.e. $a = o = c$.

If $x \in R$, than $x = \frac{ab}{a}$. If $x = o$, then $ba^2 = o$ or $b = o$, so that the order coincides on R with the given order in R.

That the extension is unique can be, trivially, seen.

Since every ordered field has characteristic zero, it contains a sub- **173**
field isomorphic to Γ, the rational number field Γ has thus induced order. We shall now prove

(5) Γ *can be ordered in one way only.*

For, if Z denotes the set of integers, then Γ is the quotient field of Z. On Z, there is only one order since $1 > o$ and hence $n = 1+1+\cdots+1 > o$. Thus, all natural integers have to be positive.

2 Extensions of orders

Hereafter, we consider ordered fields k. Our main task will be the study of extensions of orders in k to extension fields K of k. For this purpose, we introduce the notion of a *positive form* on k.

Let k be an ordered field. A polynomial $\sum\limits_{i=1}^{m} a_i x_i^2$, $a_i \in k$, is said to be an *m-ary form* over k. It is said to be *positive* if $a_i > o, i = 1, \ldots m$. An m-ary form is said to represent $\underline{a} \in k$, if there exist $\alpha_1, \ldots, \alpha_m$ in k such that

$$\sum_i a_i \alpha_i^2 = a.$$

Clearly a positive form represents zero, only if $\alpha_1, \ldots, \alpha_m = o$. Let k be an ordered field and K/k, an extension field. We shall prove

Theorem 1. *K has an order extending the order in k, if and only if, every positive form over k is still positive in K.*

174 *Proof.* We have only to prove the sufficient. To this end, consider the family M of subsets $\{M_\alpha\}$ of K having the following properties. Denote, by S, the set of elements in K of the form

$$\sum_i a_i \alpha_i^2,$$

$a_i \in k$ and $a_i > o$ and $\alpha_i \in K$. (α_i can be all zero also). □

Then

$$1)\quad M_\alpha \supset S \qquad 2)\quad M_\alpha + M_\alpha \subset M_\alpha$$
$$3)\quad M_\alpha M_\alpha \subset M_\alpha \qquad 4)\quad M_\alpha \cap (-M_\alpha) = (o).$$

This family is not empty, since S satisfies this condition. In the usual way, we make M a partially ordered set and obtain a maximal set P. We have now to show that

$$P \cup (-P) = K$$

and then P will determine an order. Let $x \neq o$ be an elements of K which is not in P. Define

$$Q = P - xP$$

as the set of elements of the form $a - xb$, $a, b \in P$. Obviously Q satisfies (1). To see that Q satisfies (2), observe that if $a - xb$, $c - xd$ are in Q then

$$(a - xb) + (c - xd) = (a + c) - x(b + d);$$

but a, b, c, d being in P which is an element of M, $a + c$, $b + d$ are in P. In a similar way Q satisfies (3). That Q satisfies (4) can be seen as follows: Let $a - xb$ and $c - xd$ be in Q with a, b, c, d, in P. Let $(a + c) - x(b + d) = o$. Then $b + d = o$. For, if $b + d \neq o$, then

$$x = \frac{a + c}{b + d} = (a + c)(b + d)\frac{1}{(b + d)^2}$$

and so is an element of P, which is a contradiction. Hence $b + d = 0$ 175 and, therefore, $a + c = 0$. Since a, b, c, d are all in P, it follows that $a = b = c = d = 0$. Thus $Q \in M$. But $Q \supset P$ so that, by maximality of P, $Q = P$. This means that $-x \in P$ or $x \in -P$. The theorem is therefore proved.

If Γ is the field of rational numbers and n is a positive integer, then $n = 1 + 1 + \cdots + 1$. If $r = \dfrac{a}{b}$ is a positive rational number, then

$$\frac{a}{b} = \frac{ab}{b^2} = \frac{1 + 1 \cdots + 1}{b^2},$$

so that every positive rational number is a sum of squares. This shows that every positive form over Γ can be put in the form $x_1^2 + \cdots + x_n^2$.

If k is an ordered field then $\sum\limits_i \alpha_i^2 = 0$, $\alpha_i \in k$ implies that $\alpha_i = 0$, $i = 1, \ldots$. On the other hand, if k has the property that $\sum \alpha_i^2 = 0$, $\alpha_i \in k$ implies $\alpha_i = 0$, then $n = 1+1+\cdots+1 \neq 0$ so that k has characteristic zero. Since every positive form over Γ is essentially of the type $x_1^2 + \cdots + x_n^2$, we have the

Theorem 2. *k is ordered if and only if* $\sum\limits_i \alpha_i^2 = 0$, $\alpha_i = k$ *implies* $\alpha_i = 0$, $i = 1, 2, \ldots$.

It is obvious that, if, in a field k, $\sum\limits_i \alpha_i^2 = 0$, with $\alpha_1, \alpha_2, \ldots$ not all zero, then

$$-1 = \sum_i \beta_i 2,$$

176 $\beta_i \in k$. A field in which -1 is not a sum of squares is called a *formally real field*. From theorem 2, it follows that formally real fields are identical with ordered fields.

We shall, now, prove the following application of theorem 1.

Theorem 3. *Let k be a formally real field with a given order and $f(x)$, an irreducible polynomial in $k[x]$. Let a, b be two elements in k such that $f(a)f(b) < 0$. Suppose α is a root of $f(x)$ in Ω, an algebraic closure of k. Then $K = k(\alpha)$ is ordered with an order which is an extension of the given order in k.*

Proof. Let $f(x)$ be of degree n. Then every element in $k(\alpha)$ is a polynomial in α of degree $n-1$ with coefficients in k. If $k(\alpha)$ is not ordered with an order extending that in k, then there is a positive form in k which represents -1. That is,

$$-1 = \sum_i a_i\{\varphi_i(\alpha)\}^2,$$

$a_i > 0$ in k. This means that, in $k[x]$,

$$1 + \sum_i a_i\{\varphi_i(x)\}^2 = f(x)\psi(x).$$

Since $f(x)$ has degree n and left side has degree $\leq 2n-2$, $\psi(x)$ has, at most, the degree $n-2$. □

We now use induction on n. If $n = 1$, these is nothing to prove. Assume theorem proved for $n-1$ instead of n. Let $g(x)$ be in irreducible factor of $\psi(x)$. Then $g(x)$ has degree $\leq n-2$. Now

$$0 < 1 + \sum_i a_i\{\varphi_i(a)\}^2 = f(a)\psi(a)$$
$$0 < 1 + \sum_i a_i\{\varphi_i(b)\}^2 = f(b)\psi(b).$$

177 Since $f(a)f(b) < 0$, it follows that $\psi(a)\psi(b) < 0$. Therefore, at least one irreducible factor, say $g(x)$, of $\psi(x)$ has the property $g(a)g(b) < 0$.

If β is a root of $g(x)$ in Ω, then $g(\beta) = f(\beta) = 0$. But by induction hypothesis, $k(\beta)$ has an order extending the given order in k. Hence

$$0 = 1 + \sum_i a_i\{\varphi_i(\beta)\}^2 > 0,$$

which is a contradiction. Thus our theorem is completely proved.

Suppose k is an ordered field, let us denote, by $|a|$, the *absolute value* of $a \in k$ by

$$|a| = \begin{cases} 0 & \text{if } a = 0 \\ a & \text{if } a > 0 \\ -a & \text{if } a < 0. \end{cases}$$

It is then easy to prove that

$$|ab| = |a|\,|b|,$$
$$|a + b| \leq |a| + |b|.$$

Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ be a polynomial in $k[x]$. Put $M = \max(1, |a_1| + \cdots + |a_n|)$. If $t \neq 0 \in k$ and $|t| > M$, then

$$t^{-n}f(t) = 1 + a_1t^{-1} + \cdots + a_nt^{-n} > 0$$

which shows that t^n and $f(t)$ have the same sign.

Suppose now $f(x)$ is irreducible and of odd degree. Then, if M is defined as above,

$$f(M)f(-M) < 0.$$

Therefore, by theorem 3, if β is a root of $f(x)$ in an algebraic closure of k, then $k(\beta)$ has an order extending that in k.

If $a \in k$ and $a > 0$, then the polynomial $x^2 - a$ changes sign in k. **178**
For, $(a + 1)^2 > a$ and $-a < 0$. Thus

$$((a + 1)^2 - a)(0 - a) < 0.$$

Therefore, $k(\sqrt{a})$ has an order extending the given order in k.

3 Real closed fields

We had seen above that, under certain circumstances, an order in a field k can be extended to a finite algebraic extension of k. We shall consider, now, a class of fields called *real closed* fields defined as follows: k is said to be real closed, if

1) k is ordered

2) k has no proper algebraic extension K with an order extending that in k.

Before we establish the existence of such fields, we shall obtain some of their properties. We first prove

Theorem 4. *For a formally real field k, the following properties are equivalent:*

1) $k(i)$ is algebraically closed, i being a root of $x^2 + 1$.

2) k is real closed.

3) Every polynomial of odd degree over k has a root in k and every positive element of k is a square in k.

Proof. $1 \Rightarrow 2$. $k(i)$ being of degree 2 over k, there are no intermediary fields, so that, k being ordered, and $k(i)$ being algebraically closed, k has no ordered algebraic extension.

179 $2 \Rightarrow 3$. Suppose $f(x)$ is a polynomial of odd degree. Then it changes sign in k. Hence an irreducible factor of $f(x)$, also of odd degree, changes sign in k. If α is a root of this irreducible factor, then $k(\alpha)$ is ordered with an order extending that in k. Hence $\alpha \in k$. If $a > 0$ in k, then $x^2 - a$ changes sign in k. Thus $\sqrt{a} \in k$.

$3 \Rightarrow 1$. The poof of this part consists of three steps. Firstly, every element of $K = k(i)$ is a square. For, let $a + bi$ be an element of K, a, $b \in k$. Put

$$a + ib = (c + id)^2$$

where c and d have to be determined in k. Since $1, i$ form a base of K/k we get

$$c^2 - d^2 = a, \quad 2cd = b.$$

Therefore, $(c^2 + d^2)^2 = a^2 + b^2$. But $a^2 + b^2 > 0$ in k and, since every positive element is a square, there is a $\lambda > 0$ in k such that

$$c^2 + d^2 = \lambda.$$

Solving for c^2 and d^2, we have

$$c^2 = \frac{\lambda + a}{2}, \quad d^2 = \frac{\lambda - a}{2}.$$

But, since $\lambda^2 = a^2 + b^2$, it follows that $\lambda \geq |a|$, $\lambda \geq |b|$. Therefore $\frac{\lambda + a}{2} \geq 0$, $\frac{\lambda - a}{2} \geq 0$. Therefore

$$c = \pm\sqrt{\frac{\lambda + a}{2}}, \quad d = \pm\sqrt{\frac{\lambda - a}{2}}$$

exist in k. The arbitrariness in the signs of c and d can be fixed from the fact that 2 $cd = b$. □

This proves that every quadratic polynomial over k has a root in K. For, if $ax^2 + bx + c \in k[x]$, then, in an algebraic closure of K, $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ are its roots ($a \neq 0$). But $\sqrt{b^2 - 4ac} \in K$. 180

The second step consists in showing that every polynomial in $k[x]$ has a root in K. Let $f(x)$ be in $k[x]$ and let N be its degree $N = 2^n \cdot q$, q odd. We shall use induction on n. If $n = 0$, then $N = q$, and so whatever odd number q be, $f(x)$ has a root already in k. Let us, therefore, assume proved that every polynomial of degree $2^{n-1}q'$, where q' is odd, with coefficients in k has a root in K. Let $f(x)$ be of degree $N = 2^n \cdot q$, q odd. Let $\alpha_1, \ldots, \alpha_t$ be the distinct roots of $f(x)$ in an algebraic closure of K. Let $\mu \in k$ be an element to be suitably chosen later. Put

$$\lambda_{ij}(\mu) = \lambda_{ij} = \alpha_i + \alpha_j + \mu\alpha_i\alpha_j i, \, j = 1, \ldots, t, i \neq j.$$

Consider now the polynomial

$$\varphi_\mu(x) = \prod_{i \neq j} (x - \lambda_{ij}).$$

This has degree $\dfrac{N(N-1)}{2} = 2^{n-1} \cdot q', q'$ odd. Also, by every permutation of the symbols $1, \ldots, t$, the polynomial goes over into itself. Thus $\varphi_\mu(x) \in k[x]$. Since its degree satisfies the induction hypothesis, for every $\mu \in k$, there is an i and $a j$ such that $\lambda_{ij}(\mu) \in K$. Since k is an infinite field, there exist μ, μ', $\mu \neq \mu'$ and both in k such that $\lambda_{ij}(\mu)$ and $\lambda_{ij}(\mu')$ for two integers i and j are in K. This means that $\alpha_i \alpha_j$ and, **181** hence, $\alpha_i + \alpha_j$ are in K. The polynomial $x^2 - x(\alpha_i + \alpha_j) + \alpha_i \alpha_j$ is a polynomial in $K[x]$. By what we proved above, both its roots are in K. Thus our contention is proved.

The third step consists in proving that every polynomial in $K[x]$, has a root in K. For, let $f(x)$ be a polynomial in $K[x]$. Let σ be the generating automorphism of K/k. It is of order 2. Denote by $f^\sigma(x)$ the polynomial obtained from f by applying σ on the coefficients of f. Then $\varphi = f(x) f^\sigma(x)$ is a polynomial in $k[x]$. The second step shows that φ has a root α in K. Furthermore if α is a root of φ, α^σ is also a root of φ, so that either α is a root of $f(x)$ or α^σ is a root of $f(x)$.

We have thus proved theorem 4 completely.

We deduce from this an important corollary due to *Artin* and *Schreier*.

Corollary 1. *If* Ω *is an algebraically closed field and* K *a subfield such that* $1 < (\Omega : K) < \infty$, *then* K *is real closed.*

Proof. We had already proved that $K(i) = \Omega$ and that K has characteristic zero. By virtue of theorem 4, it is enough to prove that K is formally real. Every element of Ω is of the form $a + ib$, $a, b \in K$. Also

$$a + ib = (c + id)^2,$$

for c, d in K, since Ω is algebraically closed. Thus

$$a^2 + b^2 = (c^2 + d^2)^2.$$

Hence every sum of two squares and, hence, of any number of squares is a square. Therefore

$$-1 = \sum_i a_i^2$$

is impossible in K. By theorem 2, therefore, K is formally real. □ 182

This proves that the real closed fields are those and only those which are such that their algebraic closures are finite over them.

We have again

Corollary 2. *A real closed field has only one order.*

For, the set of positive elements coincides with the set of squares of the elements of the field.

This shows that, if on ordered field has two distinct orders, it has algebraic extensions which are ordered. It must be remembered that if a field has only one order, it is not necessarily real closed. The rational number field, for example, has only one order.

Suppose k is a real closed field. Then every irreducible polynomial in $k[x]$ is of degree one or two. Suppose $f(x)$ is a polynomial in $k[x]$ and a, b in k such that

$$f(a)f(b) < 0.$$

Then one of the irreducible factors $\varphi(x)$ of $f(x)$ must have the property that $\varphi(a)\varphi(b) < 0$. If α is a root of $\varphi(x)$, then $k(\alpha)$ is ordered. But, k being real closed, $\alpha \in k$. $\varphi(x)$ must be a linear polynomial. Thus $\varphi(x) = x - \alpha$ and

$$(a - \alpha)(b - \alpha) < 0$$

which means that α lies between a and b. Hence the

Theorem 5. *If k is a real closed field, $f(x)$ a polynomial in $k[x]$, a, b in k such that $f(a)f(b) < 0$, then there is a root α of $f(x)$ in k between a and b.*

183 Furthermore, we had seen that there is an M in k depending only on the coefficients of $f(x)$ such that $f(a)$ has the same sign as a^n, $n = \deg f(x)$, if $|a| > M$. This shows

All the roots of $f(x)$ that lie in k lie between $\pm M$.

Let k be a real closed field and $f(x)$ a polynomial in $k[x]$. Let $f'(x)$ be its derivative. Put $\varphi_0 = f$, $\varphi_1 = f'$. Since $k[x]$ is a Euclidean ring, define, by the Euclidean algorithm, the polynomials

$$\begin{aligned}
\varphi_0 &= A_1 \quad \varphi_1 - -\varphi_2\\
\varphi_1 &= A_2 \quad \varphi_2 - -\varphi_3\\
&\ldots \quad \ldots\\
\varphi_{r-1} &= A_r \quad \varphi_r.
\end{aligned}$$

It is then well-known that $\varphi_r(x)$ is the greatest common divisor of φ_0 and φ_1. The sequence $\varphi_0, \varphi_1, \ldots, \varphi_r$ of polynomials in $k[x]$, is known as the *Sturmian polynomial sequence*.

Let $a \in k$ be such that $\varphi_0(a) \neq 0$. Then $\phi_r(a) \neq 0$. Consider the set of elements $\varphi_0(a)$, $\varphi_1(a), \ldots, \varphi_r(a)$ in k. The non-zero ones among them have a sign. Denote, by $\omega(a)$, the number of changes of sign in the sequence of elements,

$$\varphi_0(a), \varphi_1(a), \ldots, \varphi_r(a),$$

in this order, taking only the non-zero elements. A very important theorem due to *Sturm* is

Theorem 6. *Let b and c be two elements of k, $b < c$ and $\varphi_0(b) \neq 0$,* 184 *$\varphi_0(c) \neq 0$. Let $\omega(b)$ and $\omega(c)$ denote the number of changes of sign in the Sturmian sequence for the values b and c. Then $f(x)$ has precisely $\omega(b) - \omega(c)$ distinct roots in k between b and c.*

Proof. Since $\varphi_r(b) \neq 0$, $\varphi_r(c) \neq 0$, we may divide all the Sturmian polynomials by $\varphi_r(x)$ and obtain the sequence $\bar{\varphi}_0(x)$, $\bar{\varphi}_1(x), \ldots \bar{\varphi}_{r-1}(x)$, $\bar{\varphi}_r(x)(= 1)$. Now $\bar{\varphi}_0(x)$ has no multiple roots. For, if α is a root of $f(x)$ of multiplicity t, then

$$\begin{aligned}
\varphi_0(x) &= (x-\alpha)^t \psi_1(x), \quad \psi_1(\alpha) \neq 0\\
\varphi_1(x) &= t(x-\alpha)^{t-1}\psi_1(x) + (x-\alpha)^t \psi_1'(x)
\end{aligned}$$

so that $(x-\alpha)^{t-1}$ is the highest power of of $x-\alpha$, that divides $\varphi_1(x)$. Hence

$$\begin{aligned}\bar{\varphi}_0(x) &= (x-\alpha)\psi_2(x)\\ \bar{\varphi}_1(x) &= t\psi_2(x)+(x-\alpha)\psi_3(x),\end{aligned}$$

$\psi_2(x)$ and $\psi_3(x)$ being polynomials over k. Note that $\bar{\varphi}_1(x)$ is *not* the derivative of $\bar{\varphi}_0(x)$. We shall drop the 'bars' on the $\varphi's$ and write them as $\varphi_0,\varphi_1,\ldots,\varphi_{r-1},\varphi_r = 1$ and φ_0 having no multiple roots. Note that $\omega(b)$ or $\omega(c)$ is not altered by doing the above. □

The finite number of polynomials $\varphi_0,\varphi_1,\ldots,\varphi_{r-1}$ have only finitely many roots between b and c. By means of these roots, we shall split the interval (b,c) into finitely many subintervals, the end points of which are these roots. We shall study how the function $\omega(a)$ changes as $\underline{a}$ runs from b to c.

1) No two consecutive functions of the Sturmian series $\varphi_0(x)$, $\varphi_1(x),\ldots,\varphi_{r-1}(x)$ can vanish at one and the same point, inside the interval (b,c). For, suppose $b<a<c$ and $\varphi_i(a)=0=\varphi_{i+1}(a)$, $0<i+1<r$. Then **185**

$$\varphi_i(x) = A_i\varphi_{i+1}(x)-\varphi_{i+2}(x)$$

so that $\varphi_{i+2}(a)=0$, and, so on, finally $\varphi_r(a)=0$. But $\varphi_r(a)=1$.

2) Inside any one of the intervals, each function keeps a constant sign; for, if any function changed sign then, by theorem 5, there would be a zero inside this interval.

Let $\underline{d}$ denote an end point of an interval and L and R the intervals to the left of d and to the right of d, having d as a common end point.

3) Suppose $\underline{d}$ is a zero of φ_1 for $0<1<r$. Then

$$\varphi_{l-1} = A_l\varphi_l-\varphi_{l+1},$$

so that $\varphi_{l-1}(d) = -\varphi_{l+1}(d)$ and none of them is zero by (1). Because of (2), φ_{l-1} has in L the same sign as at d. Similarly in R. The same is true of φ_{l+1}. Thus, whatever sign φ_l might have in L and R, the function $\omega(a)$ remains constant when $\underline{a}$ goes from L to R crossing a zero of φ_l, $0 < 1 < r$.

4) Let now d be a zero of φ_0. Then d is not a zero of φ_1. We have

$$\varphi_0(x) = (x - d)\psi(x)$$
$$\varphi_1(x) = m\psi(x) + (x - d)\psi_1(x),$$

where m is an integer > 0, $\psi(x)$ and $\psi_1(x)$ are polynomials over k, and $\psi(d) \neq 0$. At $\underline{d}$, $\varphi_1(d)$ has the same sign as $\psi(d)$.

186 In L, φ_0 has the sign of $\varphi_0(a) = (a - d)\psi(a)$. But $a - d < 0$, so that φ_0 has the sign of $-\psi(a)$. In L, $\varphi_1(a)$ has the same sign as $\psi(d)$. Also $\psi(x)$ has no zero in L. Hence $\varphi_1(a)$ has the same sign as $\psi(a)$. Therefore in L, φ_0 and φ_1 have opposite signs. In R, exactly the opposite happens, namely $\varphi_0(a) = (a - d)$. $\psi(d)$, $a - d > 0$. Hence φ_0 and φ_1 have the same sign in R. Thus $\omega(a)$ is lessened by 1, whenever $\underline{a}$ crosses a zero of $\varphi_0(x)$ and remains constant in all other cases.

Our theorem is, thus, completely proved.

We make the following remark.

Remark. Suppose k is a formally real field and

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n,$$

a polynomial in $k[x]$. Let, as before, $M = \max(1, |a_1| + \cdots + |a_n|)$. Suppose there exists a real closed algebraic extension K of k with an order which is an extension of the given order in k. $f(x)$ can, then, be considered as a polynomial in $K[x]$ and, as seen earlier, $f(x)$ has no roots in K outside the interval $(-M, M)$. The number of these distinct roots is thus independent of K.

We now prove

Theorem 7. *Let k be an ordered field, Ω its algebraic closure. Suppose there exist two real closed subfields K, K^* of Ω/k with orders extending the given order in k. Then K and K^* are k isomorphic.*

Proof. 1) Let $f(x)$ be a polynomial in $k[x]$ and $\alpha_1, \ldots, \alpha_t$ the distinct roots of $f(x)$ in K. Let $\alpha_1^*, \ldots, \alpha_t^*$ be the distinct roots of $f(x)$ in K^*. Put $L = k(\alpha_1, \ldots, \alpha_t)$ and $L^* = k(\alpha_1^*, \ldots, \alpha_t^*)$. Since L/k is finite, $L = k(\xi)$ for some ξ in K. Suppose $\varphi(x)$ is the minimum polynomial of ξ in $k[x]$. Let ξ^* be a root of $\varphi(x)$ in K^*. Then $k(\xi)$ and $k(\xi^*)$ are k-isomorphic. If ρ is this isomorphism, then $\rho\xi = \xi^*$. But $k(\xi) = L = k(\alpha_1, \ldots, \alpha_t)$. Hence $\rho\alpha_1, \ldots, \rho\alpha_t$ will be distinct roots of $f(x)$ in K^*. Thus $L^* = k(\xi^*)$. Hence 187

$$L \simeq L^*.$$

2) Suppose $\varphi(x)$ is any polynomial in $k[x]$, $\beta_1, \ldots, \beta_s$ its distinct roots in K. Let $\beta_1^*, \ldots, \beta_s^*$ be the corresponding roots in K^*. Consider all the positive quantities among $\beta_i - \beta_j$, $i \neq j$. Their square roots exist in K. Let $\psi(x)$ be a polynomial in $k[x]$, among whose roots are these square roots and let $\delta_1, \ldots, \delta_g$ be the roots of $\psi(x)$ in K, $\delta_1^*, \ldots, \delta_g^*$ the corresponding roots in K^*. Then, from above,

$$\begin{aligned} F = k(\beta_1, \ldots, \beta_s, \quad \delta_1, \ldots, \delta_g) \simeq \\ \simeq k(\beta_1^*, \ldots, \beta_s^*, \quad \delta_1^*, \ldots, \delta_g^*) = F^*. \end{aligned}$$

Let τ be this isomorphism. Let notation be such that

$$\begin{aligned} \tau(\beta_i) &= \beta_i^* \\ \tau(\delta_i) &= \delta_i^*. \end{aligned}$$

Suppose $\beta_i > \beta_j$. Then $\beta_i - \beta_j > 0$ so that $\beta_i - \beta_j = \delta_t^2$, for some t. Also, $\tau(\beta_i - \beta_j) = \beta_i^* - \beta_j^*$. But

$$\tau(\beta_i - \beta_j) = \tau(\delta_t^2) = \delta_t^{*2}.$$

Hence $\beta_i^* - \beta_j^* = \delta_t^{*^2} > 0$, which proves that

$$\beta_i^* > \beta_j^*.$$

The isomorphism τ between F and F^* preserves order between the roots of $\varphi(x)$ in K. 188

3) In order, now, to construct the isomorphism between K and K^*, we remark that any such isomorphism has to preserve order. For, if σ is this isomorphism and $\alpha > \beta$ in K, then $\alpha - \beta = \delta^2$ so that

$$\sigma(\alpha - \beta) = \sigma(\delta^2) = (\sigma(\delta))^2 > 0$$

so that $\sigma\alpha > \sigma\beta$. We shall, therefore, construct an order preserving map which we shall show to be an isomorphism.

4) Let α be an element in K, $h(x)$ its minimum polynomial over k. Let $\alpha_1, \ldots, \alpha_t$ be the distinct roots of $h(x)$ in K and let notation be so chosen that $\alpha, < \alpha_2 < \ldots < \alpha_t$. Let $\alpha = \alpha_i$. Let $\alpha_1^*, \ldots, \alpha_t^*$ be the distinct roots of $h(x)$ in K^* and, again, let the notation be such that

$$\alpha_1^* < \alpha_2^* < \ldots < \alpha_t^*.$$

Define, now, σ on K by

$$\sigma\alpha = \alpha_i^*.$$

Let α and β be two elements of K and let $f(x)$ be a polynomial in $k[x]$n whose roots in K are $\alpha, \beta, \alpha + \beta, \alpha\beta, \ldots$. Construct the fields F and F^* and the k-isomorphism τ of F on F^*. Since τ preserves order of roots of $f(x)$, it preserves order of roots of the factor of $f(x)$ which has α as its root. Similarly of the factor having β as a root. Hence

$$\tau(\tau) = \sigma(\alpha), \quad \tau(\beta) = \sigma(\beta), \tau(\alpha + \beta) \quad = \sigma(\alpha + \beta), \tau(\alpha\beta) = \sigma(\alpha\beta).$$

189

Hence $\sigma(\alpha + \beta) = \sigma\alpha + \sigma\beta$, $\sigma(\alpha\beta) = \sigma\alpha \cdot \sigma\beta$. Thus σ is an isomorphism of K into K^*. We have similarly an isomorphism σ^* of K^* into K. Thus $\sigma \cdot \sigma^*$ is identity on K^*. Hence K and K^* are k-isomorphic. □

Corollary. *The only automorphism of K over k is the identity.*

We shall now prove the theorem regarding the existence of real closed fields, namely

Theorem 8. *If k is an ordered field with a given order and Ω, its algebraic closure, there exists in Ω, upto k-isomorphism, only one real closed field K with an order extending the given order in k.*

Proof. Let V be the family of formally real subfields of Ω/k which have an order extending that in k. V is not empty, since $k \in V$. We partially order V by inclusion. Let $\{k_\alpha\}$ be a totally ordered subfamily of V. Let $K_0 = \bigcup\limits_{\alpha} k_\alpha$. Then K_0 is a field which is contained in V. This can be easily seen. By Zorn's lemma, there exists a maximal element K in V. K has an order extending the order in k. To prove that K is real closed, let $f(x)$ be a polynomial of odd degree over K. It changes sign. Therefore there is an irreducible factor, also of odd degree, which changes sign in K. This factor must have a root in K. Else, by theorem 3 there exists an algebraic extension with an order extending that in k. This will contradict maximality of K. In a similar way, every positive element of K is a square. By theorem 4, K is real closed. If K and K^* are two real closed subfields with orders extending that in k, then, by theorem 7, they **190** are k-isomorphic. □

Suppose now that k is a perfect field and Ω, its algebraic closure. Let G be the galois group of Ω/K. If G has elements of finite order (not equal to identity), let K be the fixed field of the cyclic group generated by one of them. Then $(\Omega : K)$ is finite and by Artin-Schreier theorem this order has to be two. Thus any element of finite order in G has to have the order two. Furthermore, in this case, k is an ordered field.

On the other hand, if k is an ordered field and Ω, its algebraic closure, there exists, then by theorem 8, a real closed subfield of Ω/k, say K. This means that G has an element of order 2. Moreover no two elements of order 2 commute. For if α, β are of order 2 and commute, then $1, \alpha, \beta, \alpha\beta$ is a group order 4 which must have a fixed field L such that $(\Omega : L) = 4$. This is impossible, by Artin-Schreier theorem. Hence the

Theorem 9. *If k is a perfect field, Ω its algebraic closure and G the galois group of Ω/k then G has elements of finite order if and only if k is formally real. Also, then, all these elements have order 2 and no two of them commute.*

4 Completion under an order

Let k be a formally real field with a given order. We had defined a function $|\,|$ on k with values in k such that

$$|ab| = |a| \cdot |b|,$$
$$|a+b| \leq |a| + |b|.$$

This implies that

$$|a| - |b| \leq |a - b|.$$

191 Also $a \to |a|$ is a homomorphism of k^* into the set of positive elements of k. The function $|\,|$ defines a metric on the field k. We define a *Cauchy sequence* in k to be a sequence $(a_1, \ldots, a_n, .)$ of elements of k such that for *every* $\varepsilon > 0$ in k, there exists n_0, an integer such that

$$| \, a_n - a_m \, |< \varepsilon, n, m > n_0.$$

Obviously, if $m > n_0 + 1$,

$$|a_m| = |a_m - a_{no} - a_{no}| < \varepsilon + |a_{n_0}|,$$

so that all elements of the sequence from n_0 onwards have a value less than a certain positive element of k.

A Cauchy sequence is said to be a *null sequence* if, for every $\varepsilon > 0$ in k, there is an integer $n_0 = n_0(\varepsilon)$ such that

$$| \, a_n \, |< \varepsilon, \quad n > n_0.$$

The sum and product of two Cauchy sequence is defined as follows:-

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots)$$
$$(a_1, a_2, \ldots) - (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots)$$

and it is easy to verify that the Cauchy sequences in k form a ring R and the null sequences, an ideal $\mathscr{Y}$ of R. We assert that $\mathscr{Y}$ is a maximal ideal. For, let $(a_1, \ldots)$ be a Cauchy sequence in k which is not a null sequence. Then there exists a $\lambda > 0$ in k and an integer n such that

$$\mid a_m \mid > \lambda, m > n. \tag{1}$$

For, if not, for every $\varepsilon > 0$ and integer n, there exist an infinity of 192 $m > n$ for which $\mid a_m \mid < \varepsilon$. Since $(a_1, \ldots)$ is a Cauchy sequence, there exists $n_0 = n_0(\varepsilon)$ such that

$$|a_{m_1} - a_{m_2}| < \varepsilon, \quad m_1, m_2 > n_0.$$

Let $m_0 > n_0$ such that $|a_{m_0}| < \varepsilon$. Then, for all $m > m_0$,

$$|a_m| \leq |a_m - a_{m_0} \mid + \mid a_{m_0} < 2\varepsilon$$

which proves that $(a_1, \ldots)$ is a null sequence, contradicting our assumption.

Let 1 be the unit element of k. Then the sequence $(1, 1, \ldots)$ is a Cauchy sequence and is the unit element in R. Let $c = (a_1, \ldots)$ be in R but not in $\mathscr{Y}$. Let m be defined as in (1). Then $c_1 = (0, 0, \ldots 0, a_m^{-1}, a_{m+1}^{-1}, \ldots)$ is also a Cauchy sequence. For, let $\varepsilon > 0$ and n, an integer so that

$$\mid a_{n_1} - a_{n_2} \mid < \varepsilon, \qquad n_1, n_2 > n_0.$$

Then
$$\left|\frac{1}{a_{n_1}} - \frac{1}{a_{n_2}}\right| = \frac{1}{|a_{n_1}||a_{n_2}|}\left|a_{n_2} - a_{n_2}\right| < \frac{\varepsilon}{\lambda^2},$$

if n_1, $n_2 > \max(m, n_0)$. Also $cc_1 = (0, 0, 0, \ldots, 1, 1, \ldots)$ which proves that $cc_1 \equiv (1, 1, 1, \ldots$ $(mod \mathscr{Y})$. This proves that $\mathscr{Y}$ is a maximal ideal and, therefore,

1) *$R/\mathscr{Y}$ is a field $\bar{k}$.*

$\bar{k}$ is called the *completion* of k under the given order. For every $a \in k$, consider the Cauchy sequence $\bar{a} = (a, a, \ldots)$. Then $a \to \bar{a}$ is a non-trivial homomorphism of k into $\bar{k}$.

Since $\bar{k}$ is a field, this is an isomorphism. $\bar{k}$ thus contains a subfield 193 isomorphic to k. We shall identify it with k itself.

(2) *$\overline{k}$ is an extension field of k.*

We shall now make $\overline{k}$ an ordered field with an order which is the extension of the order in k. To this end, define a sequence $c = (a_1, \ldots,)$ of R to be *positive* if there is an $\varepsilon > 0$ and an $n_0 = n_0(\varepsilon)$ such that

$$a_n > \varepsilon, \quad n > n_0.$$

If $b = (b_1, \ldots)$ is a null sequence, then

$$|b_n| < \varepsilon/_2, \quad n > m = m(\varepsilon).$$

If $p > max(m, n_0)$, then

$$a_p + b_p > \varepsilon/2$$

which shows that $a + b$ is also a positive sequence. The definition of positive sequence, therefore, depends only on the residue class mod $\mathscr{Y}$.

Let P denote the set of residue classes containing the positive sequences and the null sequence. We shall show that P determines an order in $\overline{k}$

First, let c_1 and c_2 be two positive sequences. There exist $\varepsilon_1 > 0$, $\varepsilon_2 > 0$ and two integers n_1 and n_2 such that

$$\begin{aligned} a_p &> E_1, & p &> n_1, \\ b_p &> E_2, & p &> n_2; \end{aligned}$$

if $p > \max(n_1, n_2)$, then

$$a_p + b_p > \varepsilon_1 + \varepsilon_2,$$

194 so that $c_1 + c_2$ is a positive sequence or $P + P \subset P$. In a similar manner, $PP \subset P$.

Let now $c = (a_1, \ldots)$ be not a null sequence. Then c and $-c$ cannot both be positive. For then, there exist $\varepsilon, \varepsilon'$ both positive and integers n, n' such that

$$\begin{cases} a_p > \varepsilon, & p > n \\ -a_p > \varepsilon', & p > n. \end{cases}$$

If $p > \max(n, n^1)$, then

$$0 = a_p - a_p > \varepsilon + \varepsilon' > 0,$$

which is absurd. Thus $P \cap (-P) = (0)$.

Suppose now that $c = (a_1, \ldots)$ is not a null sequence. Suppose it is not positive. Then $-c = (-a_1, -a_2, \ldots)$ is a positive sequence. For, otherwise, for every ε and every n,

$$-a_p < \varepsilon, \quad p > n.$$

But, c being not positive, we have

$$a_p < \varepsilon, \quad p > n_1.$$

c being a Cauchy sequence, there exists n_0 with

$$|a_p - a_q| < \varepsilon, \quad p, q > n_0.$$

Hence, if $p > \max(n_0, n_1)$,

$$|a_p| \leq |a_p - a_q| + |a_q| < 2\varepsilon$$

which means that c is a null-sequence. This contradiction proves that

$$P \cup (-P) = \overline{k}.$$

We therefore see that 195

(3) *$\overline{k}$ is an ordered field with an order extending the order in k.*

We shall denote the element $(a_1, \ldots)$ in $\overline{k}$ by $\overline{a}$ and write

$$\overline{a} = \lim_{n \to \infty} a_n.$$

Then, clearly, given any $\varepsilon > 0$, there exists n_0 such that the element $\overline{a} - (a_{n_0})$ in k has all its elements, from some index on, less than ε in absolute value. This justifies our notation. One clearly has

$$\lim a_n + \lim b_n = \lim a_n + b_n.$$

$$\lim a_n . \lim b_n = \lim a_n + b_n .$$
$$\frac{\lim a_n}{\lim b_n} = \lim \frac{a_n}{b_n},$$

if $(b_1, b_2, \ldots)$ is not a null sequence.

If Γ is the rational number field, it is ordered and the completion $\overline{\Gamma}$ under this unique order is called the *real number field*.

This method of construction of the real number field goes back to *Cantor*.

5 Archimedean ordered fields

Ordered fields can be put into two classes.

A field k is said to be *archimedian ordered* if, for every two elements a, b in k, $a > 0$, $b > 0$ there exists an integer n such that

$$nb > a$$

196 and, similarly, there is an integer m with $ma > b$.

We may state equivalently that, for every $a > 0$, there is an integer n with

$$n > a.$$

A field k is said to be *non-archimedian* ordered if there exists $a > 0$ such that

$$a > n$$

for every integer n.

Γ, the rational number field is archimedian ordered. Consider, now, the ring $\Gamma\,[x]$ of polynomials. For

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n, a_0 \neq 0$$

define $f(x) > 0$, if $a_0 > 0$ as a rational number. That this is an order can be verified easily. Also the order is non-archimedian because

$$x^2 + 1 > n,$$

for every integer n. This order can be extended to $\Gamma(x)$.

This examples shows that an archimedian order in k can be extended into a non-archimedian order in an extension field which is transcendental over k. That this is not possible in algebraic extensions is shown by

Theorem 10. *If k is archimedian ordered and K/k is algebraic with an order extending the order in k, the extended order in K is again archimedian.*

Proof. Let α be > 0 in the extended order in K. Let $f(x) = x^n + a_1 x^{n-1} + \cdots a_n$ be the minimum polynomial of α in $k[x]$. Consider the quantities 197
$1 - a_i$, $i = 1, \ldots, n$. They are in k and since k and is archimedian ordered, there exists an integer $t > 0$ such that

$$t > 1 - a_i, i = 1, \ldots, n.$$

We now assert that $\alpha < t$. For if $\alpha \geq t$, then

$$\begin{aligned} 0 = f(\alpha) &= \alpha^n + a_1\alpha^{n-1} + \ldots + a_n \\ &\geq \alpha^n + (\alpha^{n-1} + \ldots +)(1 - t) \\ &\geq \alpha^n + (\alpha^{n-1} + \ldots + 1)(1 - \alpha) = 1, \end{aligned}$$

which is absurd. Our theorem is proved.

We had already introduced the real number field. It is clearly archimedian ordered. In fact, the completion of an archimedian ordered field is archimedian. We can prove even more, as shown by □

Theorem 11. *Every complete archimedian ordered field is isomorphic to the field of real numbers.*

Proof. Let K be an archimedian ordered field. It has a subfield isomorphic to Γ, the field of rational numbers. We shall identify it with Γ it self. Let $\bar{k}$ be the completion of k. Then

$$\bar{k} \supset \bar{\Gamma}.$$

□

In order to prove the inequality the other way round, let R be the ring of Cauchy sequences in k and $\mathscr{Y}$, the maximal ideal formed by null sequences. We shall show that every residue class of $R/\mathscr{Y}$ can be represented by a Cauchy sequence of rational numbers. Therefore, let $c = (a_1, a_2, \ldots)$ be a positive Cauchy sequence in k. Since k is archimedian ordered, there exists, for every n greater than a certain m, an integer 198 λ_n such that

$$\lambda_n < na_n < 1 + \lambda_n$$

which means that

$$\left|a_n - \frac{\lambda_n}{n}\right| < \frac{1}{n}.$$

Let $d = (0, 0, 0, \ldots \dfrac{\lambda_m}{m}, \dfrac{\lambda_{m+1}}{m+1}, \ldots)$ be a sequence of rational numbers. Let $\varepsilon > 0$ be any positive quantity in k. There exists, then, an integer t such that $\varepsilon t > 1$, since k is archimedian ordered. Then, for $n > t$ and m,

$$\left|a_n - \frac{\lambda_n}{n}\right| < \varepsilon$$

which shows that $c - d \in \mathscr{Y}$, which proves that $\bar{k} \subset \bar{\Gamma}$.

We shall now prove the important

Theorem 12. *The real number field $\bar{\Gamma}$ is real closed.*

Proof. We shall show that every polynomial which changes sign in $\bar{\Gamma}$ has a root in $\bar{\Gamma}$. □

Let $b < c$ be two elements of $\bar{\Gamma}$ and $f(x)$ a polynomial in $\bar{\Gamma}[x]$ with $f(b) > 0$ and $f(c) < 0$. We define two sequences of rational numbers $b_0, b_1, b_2, \ldots$ and $c_0, c_1, c_2, \ldots$ in the following way. Define the integers $\lambda_0, \lambda_1, \lambda_2, \ldots$ inductively in the following manner. $\lambda_0 = 0$, and having defined $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}, \lambda_n$ is defined as the largest integer such that

$$f(b + \frac{(c-b)\lambda_n}{2^n}) \geq 0.$$

We shall put $b_n = b + \dfrac{(c-b)\lambda_n}{2^n}$ and since we want b_n to be an increasing sequence, we shall, in addition, require that

$$\frac{\lambda_n}{2} \leq \lambda_{n-1} + 1.$$

199

That such a sequence can be found is easily seen. Put now

$$c_n = b_n + \frac{c-b}{2^n}.$$

Then $c_0, c_1, \ldots$ is a decreasing sequence

$$b \leq b_n \leq b_{n+1} \leq c_{n+1} \leq c_n \leq c.$$

Also (b_n) and (c_n) are Cauchy sequences; for,

$$\mid b_{n+1} - b_n \mid < \frac{c-b}{2^{n+1}}.$$

Furthermore, the sequence $(c_n - b_n)$ is a null sequence. For,

$$c_n = b_n = \frac{c-b}{2^n}$$

There is, therefore, an α between b and c such that

$$\alpha = \lim b_n = \lim c_n.$$

By definition of λ_n, $f(c_n) < 0$ and $f(b_n) \geq o$.

Therefore

$$f(\alpha) = \lim f(b_n) \geq 0, f(\alpha) = \lim f(c_n) < 0.$$

This shows that $f(\alpha) = 0$. Hence $\overline{\Gamma}$ is real closed.

We have the

Corollary. $\overline{\Gamma}(i)$ *is algebraically closed.*

$\overline{\Gamma}(i)$ is the complex number field. We have thus proved the 'fundamental theorem of algebra'.

The algebraic closure of Γ in $\overline{\Gamma}$ is called the field of *real algebraic numbers and is real closed.*

Chapter 8

Valuated fields

1 Valuations

200 Let k be a field. A *valuation* on k is a function $|\,|$ on k with values in the real number field satisfying

(1) $| 0 |= 0$

(2) $| a |> 0$, if $a \neq 0$

(3) $| ab |=| a | \cdot | b |$

(4) $| a + b |\leq| a | + | b |$

where $\underline{a}$ and $\underline{b}$ are elements in k. It follows that $a \to| a |$ is a homomorphisms of k^* into the multiplicative group of positive real numbers. If we denote by 1 the unit element of k, then

$$| 1 |=| 1^2 |=| 1 |^2=| 1 | \cdot | 1 |$$

so that $| 1 |= 1$. If ζ is a root of unity, say an n say an n th root of unity, then

$$1 =| \rho^n |=| \rho |^n$$

and so $| \rho |= 1$. Thus means that $| -1 |= 1$ and so, for $a \in k$,

$$| -a |=| a | .$$

Also, since $a = a - b + b$, we get

$$| a | - | b |\leq a - b | .$$

A valuation is said to be trivial if $| a |= 1$ for all $a \neq 0$.

Two valuations $| |_1$ and $| |_2$ are said to be *equivalent* if for every $a \neq 0$ in k,

$$| a |_1 < 1 \Rightarrow | a |_2 < 1,$$
$$| a |_1 = 1 \Rightarrow | a |_2 = 1.$$

201 It is obvious that the above relation between valuations is an equivalence relation. All valuations equivalent to a given valuation form an equivalence class of valuations.

If $| |$ is a valuation then, for $0 \leq c \leq 1$, $| 1 |^c$ is also a valuation. We shall now prove

Theorem 1. *If* $||_1$ *and* $||_2$ *are equivalent valuations, there exists a real number* $c > 0$ *such that*

$$| a |_1 = | a |_2^c$$

for all $\underline{a} \in k$.

Proof. Let us assume that $||_1$ is non-trivial. Then $||_2$ is also non-trivial. Also, there exists a $b \in k$ such that $| b |_1 > 1$, $| b |_2 > 1$. Let $a \in k$, $a \neq 0$. Then $| a |_1$ and $| b |_1$ being positive real numbers.

$$| a |_1 = | b |_1^\lambda$$

where $\lambda = \dfrac{\log | a |_1}{\log | b |_1}$. □

We approximate to the real number λ from below and from above by means of rational numbers. Let $\dfrac{m}{n} < \lambda$. Then

$$| a |_1 > | b |_1^{m/n}$$

which means that $| \frac{a^n}{b^m} |_1 > 1$. Since $||_1$ and $||_2$ are equivalent, this means that

$$| a |_2 > | b |_2^{m/n} .$$

In a similar manner, if $p/q > \lambda$, then

$$| a |_2 < | b |_2^{p/q} .$$

This means that if $\frac{m}{n} \to \lambda$ and $\frac{p}{q} \to \lambda$,then 202

$$| a |_2 = | b |_2^{\lambda} .$$

Therefore $\lambda = \frac{\log | a |_2}{\log | b |_2}$. This shows that $\frac{\log | a |_1}{\log | a |_2} = \frac{\log | b |_2}{\log | b |_2}$. Putting $c = \frac{\log | b |_1}{\log | b |_2}$ and observing that $c > 0$, our theorem follows.

2 Classification of valuations

A valuation is said to be *archimedian* if for every $a \in k$, there exists an integer $\underline{n} = n(a)$ (that is ne, if e is the unit element of k) such that

$$| a | < | n | .$$

(Compare this with archimedian axiom in ordered fields).

A valuation of k which is not archimedian is said to be *non-archimedian*. We shall deduce a few simple consequences of these definitions.

1) $||$ *is archimedian* $\Longleftrightarrow$ *there exists an integer n in k such that* $| n | > 1$.

Proof. If $||$ is archimedian, there exists $\underline{a} \in k$ with $| a | > 1$ and an integer n with $| n | > | a |$. This means that

$$| n | > 1.$$

□

Let $||$ be a valuation and n, a rational integer so that $| n |> 1$. Let a any element of k. If $| a |\leq 1$, then clearly $| a |< |n |$. Let $| a |> 1$. Since archimedian axiom holds in real number fields, we have an integer m with

$$| a |<| n | \cdot m.$$

203

If $m = 1$, there is nothing to prove. So let $m > 1$. Then $m =| n |^{\lambda}$ $(\lambda = \dfrac{\log m}{\log | n |} > 0)$. Let μ be a positive integer greater than λ. Then $m <| n |^{\mu} =| n^{\mu} |$. Therefore

$$| a |<| n | \cdot m <| n |^{\mu+1}$$

and our assertion is proved.

We deduce

2) $||$ *non-archimedian* $\Longleftrightarrow | n |\leq 1$, *for every integer n in k.*

This shows at once that

3) *All the valuations of a field of characteristic p are non-archimedian.*

We now prove the important property

4) $||$ *is an non-archimedian valuation if and only if for every a, b in k*

$$| a + b |\leq Max(| a |, | b |).$$

Proof. If $||$ is a non-archimedian valuation, then for every integer $n, | n |\leq 1$. Let m be any positive integer. Then

$$(a + b)^m = a^m + \tbinom{m}{1} a^{m-1} b + \ldots + b^m$$

so that

$$\begin{aligned} | a + b |^m &\leq | a |^m + | a |^{m-1} | b | + \ldots + | b |^m \\ &\leq (m + 1) Max(| a |^m, | b |^m). \end{aligned}$$

Taking m th roots and making $m \to \infty$ we get

$$| a + b |\leq Max(| a |, | b |).$$

The converse is trivial, since $| n |=| 1 + \cdots + 1 |\leq 1$. □

We deduce easily **204**

5) *If* $||$ *is non-archimedean and* $| a |\neq| b |$, *then*

$$| a + b |= Max(| a |, | b |).$$

Proof. Let, for instance, $| a |>| b |$. Then

$$| a + b |\leq Max(| a |, | b |) =| a |$$

Also $a = a + b - b$, so that

$$| a |\leq Max(| a + b |, | b |).$$

But, since $| a |>| b |, | a + b |\geq| b |$. Thus $| a |\leq| a + b |$ and our contention is proved. □

More generally, we have, if $| a_1 |>| a_j |$, $j \neq 1$, then

$$| a_1 + a_2 + \ldots a_n |=| a_1 | .$$

In the case of non-archimedean valuations, many times, the so-called *exponential valuation* is used. It is defined thus: If $||_0$ is an non-archimedian valuation, define the function $||$ by

$$| a |= -\log | a |_0, \quad a \neq 0.$$

This has a meaning since $| a |_0> 0$ for $a \neq 0$. We introduce a quantity ∞ which has the property

$$\infty + \infty = \infty$$

$$\infty + a = \infty$$

for any real number a and

$$\frac{a}{\infty} = 0$$

for any real number a. Then $||$ satisfies

1') $| 0 |= \infty$

2') $| a |$ is a real number

3') $| ab |=| a | + | b |$

4') $| a + b |\geq \text{ Min}(| a |, | b |)$.

205 Then $|1| = 0$, $|\rho| = 0$ for a root of unity ρ and the valuation is trivial if $|a| = 0$ for $a \neq 0$. For two valuations $||_1$ and $||_2$ which are equivalent

$$|a|_1 = c|a|_2,$$

$c\rangle 0$ being a real number.

3 Examples

First, let Γ be the finite field of q elements. Every element of Γ^* satisfies the polynomial $x^{q-1} - 1$. Therefore, any valuation $| \, |$ on Γ is trivial.

Let now Γ be the field of rational numbers.

Let $| \, |$ be an archimedian valuation on Γ. It is enough to determine its effect on the set of integers in Γ. There is an integer n such that $|n| > 1$. Let m be any positive integer. Then

$$n = a_0 + a_1 m + \cdots + a_t m^t,$$

where $t \leq \left[\dfrac{\log n}{\log m}\right]$, $0 \leq a_i < m$. Therefore $|a_i| \leq a_i < m$ so that

$$|n| \leq m(t + 1) \max(1, |m|^t).$$

Replace n by n^r, where r is a positive integer. Then again, we have

$$|n| \leq m^{\frac{1}{r}}\left(r\frac{\log n}{\log m}+1\right)^{\frac{1}{r}} \max(1, |m|^t).$$

Making $r \to \infty$, we get

$$|n| \leq \max(1, |m|^{\frac{\log n}{\log m}}).$$

This proves that, since $|n| > 1$,

$$|n| \leq |m|^{\frac{\log n}{\log m}}$$

and $|m| > 1$. 206

Now we can repeat the argument with m and n interchanged and thus obtain

$$|m| \leq |n|^{\frac{\log n}{\log m}}$$

Combining the two inequalities we get

$$\frac{\log |n|}{\log n} = \frac{\log |m|}{\log m}.$$

Since m is arbitrary, it follows that

$$|m| = m^C$$

where $c > 0$ is a constant. Obviously, the valuation is determined by its effect on positive integers. From the definition of equivalence, $||$ is equivalent to the ordinary absolute value induced by the unique order in Γ.

Let now $||$ be a non-trivial non-archimedian valuation. It is enough to determine its effect on Z, the ring of integers.

Since $|\,|$ is non-trivial, consider the set $\mathscr{Y}$ of $\underline{a} \in Z$ with $|a| < 1$. $\mathscr{Y}$ is an ideal. For,

$$|a| < 1, |b| < 1 \Rightarrow |a+b| \leq \operatorname{Max}(|a|, |b|) < 1.$$

Also, if $|a| < 1$ and $b \in Z$, then

$$|ab| = |a|\,|b| < 1.$$

Furthermore, if $ab \in \mathscr{Y}$, then $|ab| < 1$. But $|ab| = |a||b|$ and $|a| \leq 1$, $|b| \leq 1$, since valuation is non-archimedian. Hence $|a| < 1$ which means that $\mathscr{Y}$ is a prime ideal. Thus $g = (p)$ generated by a prime p. Since, by definition of $\mathscr{Y}$, $M < 1 \Leftrightarrow p/n$, we have, if $n = p^{\lambda} \cdot n_1$, $(n_1, p) = 1$,

$$|n| = |p|^{\lambda}.$$

207

If we denote $|p|$ by c, $0 < c < 1$, then for any rational number $\dfrac{a}{b}$, the value is

$$\left|\frac{a}{b}\right| = c^{\lambda}$$

where $\dfrac{a}{b} = p^{\lambda}\dfrac{a'}{b'}$ where $(a', p) = 1 = (b', p)$ and λ a rational integer. This valuations is called the *p-adic valuation*.

Thus with every non-archimedian valuation, there is associated a prime number. Conversely, let p be any prime number and let n be any integer, $n = p^{\lambda} \cdot n_1$, $\lambda \geq 0$, where $(n_1, p) = 1$. Put

$$|n| = |p|^{\lambda} \qquad , 0 < |p| < 1.$$

Then $|\,|$ determines a non-archimedian valuation on Γ. Further, if p and q are distinct primes, then the associated valuations are inequivalent. For, if $|\,|_p$ and $|\,|_q$ are the valuations, then

$$|q|_p = 1, \quad |q|_q < 1.$$

We shall denote the valuation associated with a prime p, by $||_p$. Then we have the

Theorem 2. *The ordinary absolute valuation and the p-adic valuation by means of primes p form a complete system of in-equivalent valuations of the rational number field.*

We shall denote the ordinary absolute valuation by $||_\infty$.

Let us consider the case of a function field K over a ground field k and let L be the algebraic closure of k in K. L is called the *field of constants* of the function field K. The valuations on K that we shall consider shall always be such that 208

$$|a| = o$$

for $a \in k$. (We consider exponential valuation). Hence valuations of function fields are always non-archimedian, since the prime field is contained in k.

Let, now, α be in L. Then α satisfies the equation

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = o$$

where $a_1, \ldots, a_n \in k$. If $||$ is a valuation of K then

$$|\alpha|^n \geq \min(|\alpha|^{n-1}, \ldots, |1|).$$

From this, it follows that $|\alpha| \geq 0$. Also, since $1/\alpha$ is algebraic, $|\alpha| \leq 0$. Hence for all $\alpha \in L$

$$|\alpha| = 0.$$

Thus the valuation is trivial on the field of constants.

We shall consider the simple case where $K = k(x)$, x transcendental over k. Here $L = k$. Let $||$ be a valuation and let $|x| < 0$. Let $f(x) = a_0x^n + \cdots + a_n$ be in $k[x]$. Then

$$f(x) \geq \min(|x|^n, |x|^{n-1}, \ldots, |1|).$$

Therefore

$$f(x) = n|x|.$$

This means that, if $R(x) = \dfrac{g(x)}{h(x)}$ is an element of K, then

$$|R(x)| = (\deg h(x) - \deg g(x))(-|x|).$$

We denote this valuation by $||_\infty$.

Suppose now that $|x| \geq 0$. As in the case of rational integers, consider the subset $\mathscr{Y}$ of $k[x]$ consisting of polynomials $f(x)$ with $|f(x)| > 0$. Then, since for every $\phi(x)$ in $k[x]$, $|\varphi(x)| \geq 0$, it follows that $\mathscr{Y}$ is a maximal ideal generated by an irreducible polynomial $p(x)$. As in the 209 case of the rational number field

$$|R(x)| = \lambda |p(x)|$$

where $R(x) = \{p(x)\}^{\lambda} \dfrac{A(x)}{B(x)}$ where $A(x)$ and $B(x)$ are prime to $p(x)$ and λ is a rational integer. If we denote, by $||_{p(x)}$, this valuation and put $\lambda = ord_{p(x)} R(x)$, then

$$|R(x)| = c \operatorname{ord}_{p(x)} R(x)$$

where $c = |p(x)|_{p(x)} > 0$. Every irreducible polynomial also gives rise to a valuation of this type. Hence

Theorem 3. *A complete system of inequivalent valuations of $k(x)$ is given by the valuations induced by irreducible polynomials in $k[x]$ and the valuation given by the difference of degrees of numerator and denominator of $f(x)$ in $k(x)$.*

4 Complete fields

Let k be a field and $||$ a valuation of it. The valuation function defines on k a metric and one can complete k under this metric. The method is the same as in the previous chapter and we give here the results without proofs.

A sequence $(a_1, a_2, \ldots)$ of elements of k is said to be a Cauchy sequence if for every $\varepsilon > 0$, there exists an integer $n = n(\varepsilon)$ such that

$$|a_{n_1} - a_{n_2}| < \varepsilon \qquad , n_1, n_2 > n.$$

It is a null sequence if for every $\varepsilon > 0$, there is an integer n such that

$$|a_m| < \varepsilon, \qquad m > n.$$

210

The Cauchy sequences form a commutative ring R and the null sequences a maximal ideal $\mathscr{Y}$, therein. The quotient $\bar{k} = R/\mathscr{Y}$ is called the completion of k under $||$. The mapping $a \to (a, a, a, \ldots)$ is an isomorphism of k in $\bar{k}$ and we identify this isomorphic image with k itself.

We extend to $\bar{k}$ the valuation $||$ in k, in the following manner. The real number field $\bar{\Gamma}$ is complete under the valuation induced by the unique order on it. So, if $a \in \bar{k}$, then $a = (a_1, a_2, \ldots)$, a Cauchy sequence of elements of k. Put

$$|a| = \lim_{n\to\infty} |a_n|$$

That this is a valuation follows from the properties of limits in $\bar{\Gamma}$. Also, the extend valuation is archimedian or non-archimedian, according as the valuation in k is archimedian or non-archimedian.

For instance, if $||$ on k is non-archimedian and

$$a = (a_1, a_2, \ldots)$$
$$b = (b_1, b_2, \ldots)$$

are two elements of $\bar{k}$, then

$$a + b = (a_1 + b_1, a_2, +b_2, \ldots)$$

and

$$|a + b| - \text{Max}(|a|, |b|) = \lim_{n\to\infty} (|a_n + b_n| - \text{Max}(|a_n|, |b_n|))$$

which is certainly ≤ 0,

$\bar{k}$ is thus a complete valuated field.

It may also be seen that the elements of k are dense in $\bar{k}$ in the topology induced by the metric. 211

Let $c_1 + c_2 + c_3 + \cdots$ be a series in $\bar{k}$. We denote by S_n the partial sum

$$S_n = c_1 + c_2 + \cdots + c_n.$$

We say that $c_1 + c_2 + \cdots + c_n + \cdots$ is *convergent* if and only if the sequence of partial sums $S_1, S_2, \ldots, S_n, \ldots$ converges. This means that, for every $\varepsilon > 0$, there exists an integer $n = n(\varepsilon)$ such that

$$|S_{m'} - S_m| = |c_{m+1} + \cdots + c_{m'}| < \varepsilon, m, m' > n.$$

Obviously $c_1, c_2, \ldots$ is a null sequence in $\bar{k}$.

In case the valuation is non-archimedian, we have the following property:-

1) *The series $c_1 + c_2 + \cdots + c_n + \cdots$ is convergent if and only if $c_1, c_2, \ldots$ is a null sequence.*

Proof. We have only to prove the sufficiency of the condition. Suppose that $c_n \to 0$; then, for large n and m,

$$\begin{aligned} |S_n - S_m| &= |c_{m+1} + c_{m+2} + \cdots + c_n| \\ &\leq \max(|c_{m+1}|, \ldots, |c_n|) \end{aligned}$$

and so tends to zero. This proves the contention. □

Note that this theorem is false, in case the valuation is archimedian.

Let k be a field and || a valuation on it. $a \to |a|$ is a homomorphism of k^* into multiplicative group of positive real numbers. Let $G(k)$ denote this homomorphic image. This is a group which we call the *value group* of k for the valuation. If $\bar{k}$ is the completion of k by the valuation in k, then $G(\bar{k})$ is value group of $\bar{k}$. 212

Suppose || is an archimedian valuation. Then k has characteristic zero and contains Γ, the rational number field as a subfield. On Γ, || is the ordinary absolute value. Since $\bar{k}$ contains $\bar{\Gamma}$, the field of real numbers, it follows that

1) *$G(\bar{k})$ is the multiplicative group of all positive real numbers.*

Also, because of the definition of the extended valuation, it follows that $G(k)$ is dense in the group $G(\bar{k})$.

We shall now assume that || is a non-archimedian valuation. We consider the exponential valuation. Then $G(k)$ is a subgroup of the additive group of all real numbers. We shall now prove

2) $G(\bar{k}) = G(k)$.

Proof. For, let $0 \neq a \in \bar{k}$. Then $a = (a_1, \ldots)$ is a Cauchy sequence, not a null sequence in k. By definition,

$$|a| = \lim_n |a_n|$$

Now $a_n = a_n - a + a$ so that

$$|a_n| \geq \min(|a_n - a|, |a|).$$

But, for n large, $|a_n - a| > |a|$ so that $|a_n| = |a|$ and our contention is established. □

$G(k)$ being an additive subgroup of the real number field is either dense or discrete. The valuation is then called dense or discrete accordingly. In the second case, there exists π in k with smallest positive value $|\pi| \cdot |\pi|$ is then the generator of the infinite cyclic group $G(k) \cdot \pi$ is called a *uniformising parameter*. It is clear that π is not unique. For, if $u \in k$ with $|u| = 0$, then $|u\pi| = |\pi|$ and $u\pi$ is also a uniformising parameter. 213

Consider in k the set $\mathscr{O}$ of elements a with $|a| \geq o.\mathscr{O}$ is then an integrity domain. For,

$$|a| \geq 0, |b| \geq 0 \Rightarrow |a + b| \geq \text{Min}(|a|, |b|) \geq 0.$$

Also $|ab| = |a| + |b| \geq 0$. We call $\mathscr{O}$ the *ring of integers* of the valuation. Consider the set $\mathscr{Y}$ of elements $a \in k$ with $|a| > 0$. Then $\mathscr{Y}$ is a subset of $\mathscr{O}$ and is a maximal ideal in $\mathscr{O}$. For, if $a \in r$ and $b \in \mathscr{Y}$, then $|ab| = |a| + |b| > 0$. Also, if $a \in r$ but not in $\mathscr{Y}$, then $|a| = 0$ and $|a^{-1}| = 0$ so that if $\mathscr{U}$ is an ideal in $\mathscr{O}$ containing $\mathscr{Y}$, then $\mathscr{U} = \mathscr{Y}$ or $\mathscr{U} = r$. We call $\mathscr{Y}$, the *prime divisor of the valuation*. Since $\mathscr{Y}$ is maximal, $r/\mathscr{Y}$ is a field. We call $\pi/\mathscr{Y}$ *the residue class field*.

Exactly the same notions can be defined for $\bar{k}$. We denote by $\bar{\mathscr{O}}$ the ring of integers of the valuation so that $\bar{\mathscr{O}}$ is the set of $\underline{a} \in \bar{k}$ with $|a| \geq 0.\bar{\mathscr{Y}}$ is the maximal ideal in $\bar{\mathscr{O}}$, hence the set of $\underline{a} \in \bar{k}$ with $|a| > 0$. Also $\bar{\mathscr{O}}/\bar{\mathscr{Y}}$ is the residue class field. Clearly

$$\mathscr{Y} = \bar{\mathscr{Y}} \cap r$$

We now have

2) Every $\underline{a} \in k(\bar{k})$ has the property; $a \in r(\bar{r})$ or $a^{-1} \in \mathscr{Y}(\bar{\mathscr{Y}})$.

   This is evident since if $a \notin \mathscr{O}(\bar{\mathscr{O}})$, $|a| < 0$ so that $|a^{-1}| > 0$ and hence $a^{-1} \in \mathscr{Y}(\bar{\mathscr{Y}})$. 214

3) *$\mathscr{O}(\bar{\mathscr{O}})$ is integrally closed in $k(\bar{k})$.*

   Proof. We should prove that every α in $k(\bar{k})$ which is a root of a polynomial of the type $x^n + a_1 x^{n-1} + \cdots + a_n, a_1, \ldots, a_n \in \mathscr{O}(\bar{\mathscr{O}})$, is already in $\mathscr{O}(\bar{\mathscr{O}})$. For, suppose

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = o$$

   and $\alpha \notin \mathscr{O}(\bar{\mathscr{O}})$. Then $\alpha^{-1} \in \mathscr{Y}(\bar{\mathscr{Y}})$. Therefore

$$1 = -(a_1\alpha^{-1} + a_2\alpha^{-2} + \cdots + a_n\alpha^{-n})$$

   and so

$$o = |1| \geq \min(|a_1\alpha^{-1}|, \ldots |a_n\alpha^{-n}) > o$$

   which is absurd □

4) *Every element in $\bar{\mathscr{O}}$ is the limit of a sequence of elements in $\mathscr{O}$ and conversely.*

   Proof. Let $a = (a_1, \ldots, a_n, \ldots)$ be in $\bar{\mathscr{O}}, a_1, \ldots, a_n, \ldots$ in k. Then, as we saw earlier, for sufficiently large n

$$|a_n| = |a|.$$

   But $|a| \geq 0$ so that $|a_n| \geq 0$. Thus, for sufficiently large n, all $a'_n s$ are in $\mathscr{O}$. Converse is trivial.

   We now prove □

5) *There is a natural isomorphism of $\mathscr{O}/\mathscr{Y}$ on $\bar{\mathscr{O}}/\bar{\mathscr{Y}}$.*

Proof. The elements of $\mathscr{O}/\mathscr{Y}$ are residue classes $a+\mathscr{Y}$, $a \in r$. We now make correspond to $a+\mathscr{Y}$ the residue class $a+\overline{\mathscr{Y}}$. Then $a+\overline{\mathscr{Y}}$ 215 is an element of $\overline{\mathscr{O}}/\overline{\mathscr{Y}}$. The mapping $a+\mathscr{Y} \to a+\overline{\mathscr{Y}}$ is a homomorphism (non-trivial) of $\mathscr{O}/\mathscr{Y}$ into $\overline{\mho}/\overline{\mathscr{Y}}$. Since both are fields, this is an isomorphism into. In order to see that it is an isomorphism of $\mathscr{O}/\mathscr{Y}$ onto $\overline{\mathscr{O}}/\overline{\mathscr{Y}}$, let $\overline{a}+\overline{\mathscr{Y}}$ be any residue class in $\overline{\mathscr{O}}/\overline{\mathscr{Y}}$. By (4) therefore, given any $N > 0$, there exists $a \in \mho$ with

$$|\overline{a}-a| > N > 0$$

or $\overline{a}-a \in \overline{\mathscr{Y}}$. If we then take $a+\mathscr{Y}$, then $\overline{a}+\overline{\mathscr{Y}}$ is the image of $a+\mathscr{Y}$. This proves that the mapping is an isomorphism onto. □

(5) enables us to choose, in k itself, a set of representatives of $\overline{\mho}/\overline{\mathscr{Y}}$, the residue class field. We shall denote this set by $\mathscr{R}$ and assume that it contains the zero element of $\mathscr{O}$. Also it has to be observed that, in general, $\mathscr{R}$ is *not a field*. It is not even an additive group.

We now assume that $|\,|$ is a *discrete valuation*. Let π in $\mathscr{O}$ be a uniformising parameter. Then clearly

$$\overline{\mathscr{Y}} = (\pi)$$

is a principal ideal. Let $a \in \overline{k}$. Then $|a|/|\pi|$ is a rational integer, since $G(k)$ is an infinite cyclic group. Put $|a|/|\pi| = t$. Then $|a\pi^{-t}| = 0$. If we call elements u in $\overline{k}$ with $|u| = 0$, units, then

$$a = \pi^t u$$

where u is a unit.

Let $\mathscr{R}$ be the set defined above and $a \in \overline{\mho}$. Then

$$a \equiv a_0(\quad \mathrm{mod}\ \overline{\mathscr{Y}})$$

with $a_0 \in \mathscr{R}$. This means that $(a-a_0)\pi^{-1}$ is an integer (in $\overline{\Omega}$). 216

$$(a-a_0)\pi^{-1} \equiv a_1(\mathrm{mod}\overline{\mathscr{Y}}),$$

where $a_1 \in \mathscr{R}$. Then

$$a \equiv a_0 + a_1\pi (\text{mod}\overline{\mathscr{Y}}^2)$$

In this way, one proves by induction that

$$a \equiv a_0 + a_1\pi + \cdots + a_m\pi^m (\text{mod})\overline{\mathscr{Y}}^{m+1})$$

where $a_0, a_1, \ldots, a_m \in \mathscr{R}$. Put $b_m = a_0 + a_1\pi + \cdots + a_m\pi^m$.

Then $a \equiv b_m (\text{mod}\overline{\mathscr{Y}}^{m+1})$ which means that

$$|a - b_m| \geq m + 1$$

Consider the series

$$b_0 + (b_1 - b_0) + (b_2 - b_1) + \cdots$$

Then, since $b_{m+1} - b_m = a_{m+1}\pi^{m+1}$, we see that $|b_{m+1} - b_m|$ increases indefinitely. Hence the above series converges. Also, since its elements are integers,

$$b = b_0 + (b_1 - b_0) + (b_2 - b_1) + \cdots$$

is an element of $\overline{\mathscr{O}}$.

Since $b_0 + (b_1 - b_0) + \cdots + (b_m - b_{m-1}) = b_m$, it follows that

$$b = \lim_m b_m.$$

Thus we have

$$a = \lim_{m \to \infty} b_m = a_0 + a_1\pi + a_2\pi^2 + \cdots$$

By the very method of construction this expression for $\underline{a}$ is unique, once we have chosen $\mathscr{R}$ and π.

217 If $a \in \overline{k}$, $a\pi^t \in \overline{\mathscr{O}}$ for some rational integer t. Hence we have

6) *Every element $\underline{a}$ in $\overline{k}$ has the unique expression*

$$a = \sum_{n=-t}^{\infty} a_n \pi^n$$

$a_n \in \mathscr{R}$ and π in $\overline{\mathscr{O}}$ is a generator of $\mathscr{Y}$. t is a rational integer.

If $t > 0$, we shall call

$$h(a) = \sum_{n=-t}^{-1} a_n \pi^n$$

the *principal part* of a. If $t \leq \underline{0}$ we put $h(a) = 0$. Clearly, $h(a)$ is an element in k. Also $a - h(a) \in \overline{\mathscr{O}}$.

We now study the two important examples of the rational number field and the rational function field of one variable.

Let Γ be the field of rational numbers. We shall denote by $||_\infty$ the ordinary absolute value and by $||_p$ the p-adic value for p, a prime. If $\underline{a}$ is an integer, $a = p^\lambda n_1$, $(p, n_1) = 1$.

We put

$$|a|_p = \lambda \log p$$

and

$$|a|_\infty = \text{ absolute value of a.}$$

It is then clear that each of the non-archimedian valuations of Γ is discrete. Let us denote by Γ_∞ the completion of Γ by the archimedian valuation and by Γ_p the completion of Γ by the p-adic valuation. Γ_∞ is clearly the real number field.

If $\mathscr{O}_p$ denotes the set of integers of Γ_p and $\mathscr{Y}$ the prime ideal of the valuation then

$$\mathscr{Y} = (p)$$

A set of representatives of $\mathscr{O}_p \mod \mathscr{Y}$ is given by the integers $0, 1, 2, \ldots, p-1$ as can be easily seen. Hence, by (6), 218

7) *Every $a \in \Gamma_p$ is expressed uniquely in the form*

$$a = \sum_{n=-t}^{\infty} a_n p^n$$

where $a_i = 0, 1, 2, \ldots, p-1$.

The elements of Γ_p are called the *p-adic numbers of Hensel*.

As before, we denote, by $h_p(a)$, the principal part of $\underline{a}$ at p. Clearly $a - h_p(a)$ is a p-adic integer.

Let $\underline{a}$ be a rational number, $a \in \mho_p \Leftrightarrow |a|_p \geq 0$, that is $a = \dfrac{b}{c}$, $(b, c) = 1$ and c is prime to p. Since only finitely many primes divide b and c, it follows that $a \in \mho_p$ for almost all p, that is except for a finite number of p. Hence $h_p(a) = 0$ for all except a finite number of primes. Hence for any $\underline{a}$

$$\sum_p h_p(a)$$

has a meaning. Also, $a - h_p(a)$ is a rational number whose denominator is prime to p. Hence $a - \sum\limits_p h_p(a)$ is a rational number whose denominator is prime to every rational integer. Hence

8) *For every rational number $\underline{a}$*

$$a - \sum_p h_p(a) \equiv 0 (\text{mod} 1).$$

This is the so-called *partial fraction decomposition* of a rational number.

Let now k be an algebraically closed field and $K = k(x)$ the field of rational functions of one variable x. All the valuations are non-archimedean. Every irreducible polynomial of $k[x]$ is linear and of 219 the form $x - a$. With every $a \in k$ there is the valuation $||_a$ associated, which is defined by

$$|f(x)|_a = \lambda,$$

where $f(x) \in k[x]$, $f(x) = (x-a)^{\lambda}\varphi(x)$, $\varphi(a) \neq 0$. If we denote by $||_{\infty}$ the valuation by degree of $f(x)$, then, for $f(x) \in k[x]$,

$$|f(x)|_{\infty} = -\deg f(x)$$

Let K_a and K_{∞} denote the completions, respectively, of K at $||_a$ and $||_{\infty}$. If $\mathscr{O}_a$ and $\mathscr{O}_{\infty}$ are the set of integers of K_a and K_{∞}, $\mathscr{Y}_a$ and $\mathscr{Y}_{\infty}$ the respective prime divisors, then

$$\mathscr{Y}_a = \{x-a\}, \mathscr{Y}_{\infty} = \{\frac{1}{x}\}.$$

It is clear, then, that $\mho_a/\mathscr{Y}_a$ and $\mho_{\infty}/\mathscr{Y}_{\infty}$ are both isomorphic to k and since K contains k, we may take k itself as a set of representatives of the residue class field. Any element f in K_a is uniquely of the form

$$f = \sum_{n=-t}^{\infty} a_n (x-a)^n,$$

$a_n \in k$. Similarly, if $\varphi \in K_{\infty}$,

$$\varphi = \sum_{n=-t}^{\infty} b_n x^{-n}.$$

As before, if we denote by $h_a(f)$ and $h_{\infty}(f)$ the principal parts of $f \in K$ for the two valuations, then

$$\sum_a h_a(f) + h_{\infty}(f)$$

has a meaning since $h_a(f) = 0$ for all but a finite number of $\underline{a}$

If we define $\varphi \in K$ to be regular ar $\underline{a}(\infty)$ if $\varphi \in \mho_a(\mho_{\infty})$, then for $f \in K$, 220

$$f - \sum_a h_a(f)$$

where $\underline{a}$ may be infinity also, is regular at all, $a \in k$ and also for the valuation $||_{\infty}$. Such an element, clearly, is a constant. Hence

9) *If $f \in K$ then*

$$f - \sum_{a} h_a(f) = \text{ constant}$$

Conversely, it is easy to see that there exists, up to an additive constant, only one $f \in K$ which is regular for all $a \in k$ except $a_1, \ldots, a_n$ (one of which may be ∞ also) and with prescribed principal parts at these a_i. 9) gives the partial fraction decomposition of the rational function f.

5 Extension of the valuation of a complete non-archimedian valuated field

We shall study the following problem. Suppose k is compute under a valuation $\|$. Can this valuation be extended, and if so in how many ways, to a finite algebraic extension K of k ?

We prove, first

Lemma 1. *Let k be a field complete under a valuation $\|$, and K a finite algebraic extension of k. Let $\omega_1, \ldots, \omega_n$ be a basis of K/k. Let $\|$ have an extension to K and*

$$\alpha_\nu = \sum_{i=1}^{n} a_{i\nu}\omega_i, a_{i\nu} \in k,$$

221 $\nu = 1, 2, 3, \ldots$ *be a Cauchy sequence in K. Then $a_{i\nu}$ $i = 1, 2, \ldots, n$ are Cauchy sequence in K.*

Proof. We consider the Cauchy sequence $\{\alpha_\nu\}$,

$$\alpha_\nu = \sum_{i=1}^{m} a_{i\nu}\omega_i, a_{i\nu} \in, k$$

$1 \leq m \leq n$ and we shall prove that the $\{a_{i\nu}\}$ are Cauchy sequences in k. We use induction on m. Clearly, if $m = 1$,

$$\alpha_\nu = a_{i\nu}\omega_1$$

and $\{\alpha_\nu\}$ is a Cauchy sequence in K if and only if $\{a_{i\nu}\}$ is a sequence in k. □

Suppose we have proved our statement for $m - 1 \geq 1$, instead of m. Write

$$\alpha_v = \sum_{i=1}^{m-1} a_{iv}\omega_i + a_{mv}\omega_m.$$

If $\{a_{mv}\}$ is a Cauchy in k, then $\{\alpha_v - a_{mv}\omega_m\}$ is a Cauchy sequences in K and induction hypothesis works. Let us assume that a_{mv} is not a Cauchy sequence in k. This means that there exists a $\lambda > 0$ and for every v, an integer μ_v such that

$$\mu_v > v$$

and

$$|a_m\mu_v - a_{mv}| > \lambda.$$

Consider now the sequence $\{\beta_v\}$ in K with

$$\beta_v = \frac{\alpha_{\mu_v} - \alpha_v}{a_{m\mu_v} - a_{mv}}.$$

Because of the above property, we see that $\{\beta_v\}$ is a null sequence in K.

Now

$$\beta_v - \omega_m = \sum_{i=1}^{m-1} \left(\frac{a_i\mu_v - a_{iv}}{a_m\mu_v - a_{mv}} \right) \omega_i$$

and $\{\beta_v - \omega_m\}$ is a Cauchy sequence in K. Induction hypothesis now works and so, if 222

$$\lim_{v\to\infty} \left(\frac{a_{i\mu_v} - a_{iv}}{a_{m\mu_v} - a_{mv}} \right) = b_i,$$

then

$$-\omega_m = \sum_{i=1} b_i\omega_i, \qquad b_i \in k.$$

This is impossible because $\omega_1, \ldots, \omega_m$ are linearly independent over k. Therefore $\{a_{mv}\}$ is a Cauchy sequence and our Lemma is thereby proved.

We shall now prove the following theorem concerning extension of valuation. 223

Theorem 4. *If the valuation $||$ of a complete field k can be extended to a finite extension K, then this extension is unique and K is complete under the extended valuation.*

Proof. That K is complete under the extended valuation is easy to see. For, if $\{\alpha_v\}$ is a Cauchy sequence in K and

$$\alpha_v = \sum_i a_{iv}\omega_i, \quad a_{iv} \in k.,$$

by the lemma, the $\{a_{iv}\}$'s are Cauchy sequences. So, if

$$\lim_{v\to\infty} a_{iv} = b_i \in k,$$

then

$$\lim_{v\to\infty} \alpha_\gamma = \sum_i \omega_1 \lim_{v\to\infty} a_{iv} = \sum_i b_i\omega_i$$

which is again in K. □

We shall now prove that the extended valuation is unique.

From the lemma, it follows that if $\{\alpha_v\}$ is a null sequence in K and $\alpha_v = \sum\limits_i a_{iv}\omega_i$, $a_{iv} \in k$, then the a_{iv}'s are null sequences in k.

In particular, if $\alpha \in K$ and $|\alpha| < 1$ in some extension the valuation $||$ in k, then $\alpha, \alpha^2, \alpha^3, \ldots$ is a null sequence in K. If $\alpha^m = \sum\limits_1 a_1^{(m)}\omega_i$, $a_i^{(m)} \in k$, then $a_i^{(m)}, i = 1, \ldots, n$ are null sequence in k.

If $\alpha = \sum x_i\omega_i$ is a general element of $x_1, \ldots, x_n$. Put

$$\alpha^t = \sum_{i=1} x_i^{(t)}\omega_i;$$

then $N_{K/k}\alpha^t$ is the same polynomial in $x_t^{(t)}$, $i = 1, \ldots, n$ as $N_{K/k}\alpha^t$ is in $x_1, \ldots, x_n$. If now $|\alpha| < 1$, is an extended valuation, then the $\{x_i^(t)\}$ are null sequences. Hence $N\alpha$, $N\alpha^2$ is a null sequences in k, But $N\alpha^t = (N\alpha)^t$ so that $(N\alpha), (N\alpha)^2, \ldots$, is s a null sequence in k. This means that $|N\alpha| < 1$. We have, thus, proved that if α in K is such that $|\alpha| < 1$ is an extended valuation, then $|N\alpha| < 1$ in k.

In a similar manner, if $|\alpha| > 1$, then $|N\alpha| > 1$. Thus we get $|N\alpha| = 1 \Rightarrow |\alpha| = 1$.

Let now β be in K and write $\beta = \dfrac{\alpha^n}{N\alpha}$ where $n = (K : k)$

Then $N\beta = \dfrac{(N\alpha)^n}{(N\alpha)^n}$. Thus

$$|N\beta| = 1.$$

By the above, it means that $|\beta| = 1$ in the valuation. Hence

$$|\alpha| = \sqrt[n]{|N\alpha|}$$

showing that the value of α in the extended valuation is unique fixed. 224

Our theorem is thus completely proved.

In order to prove that an extension of the valuation is possible, we shall consider the case where k is complete under a *discrete* non-archimedian valuation. Let $\mathscr{O}$ be the ring of integers $\mathscr{Y}$, the prime divisor of the valuation and $\mathscr{O}/\mathscr{Y}$, the residue class field. We shall now prove the celebrated lemma due *Hensel*

Lemma 2. *Let $f(x)$ be a polynomial of degree m in $\mathscr{O}[x]$, $g_0(x)$, a monic polynomial of degree $r \geq 1$ and $h_0(x)$, a polynomial of degree $\leq m - r$ both with coefficients in $\mathscr{O}$ such that*

1) $f(x) \equiv g_o(x)h_o(x)\,(\text{mod}\mathscr{Y})$

2) *$g_o(x)$ and $h_o(x)$ are coprime* $\mod \mathscr{Y}$

Then there exists polynomials $g(x)$ and $h(x)$ in $\mathscr{O}[x]$ such that

$$\left.\begin{aligned} g(x) &\equiv g_o(x) \\ h(x) &\equiv h_o(x) \end{aligned}\right\} \quad (\text{mod } \mathscr{Y}),$$

$g(x)$ has the same degree as $g_o(x)$ and $f(x) = g(x) \cdot h(x)$.

Proof. We shall now construct two sequences of polynomials $g_o(x), g_1, (x), \ldots$ and $h_o(x), h_1, (x), \ldots$ satisfying

$$g_n(x) \equiv g_{n-1}(x)(\mod \mathscr{Y}^n)$$

$$h_n(x) \equiv h_{n-1}(x)(\mod \mathscr{Y}^n)$$
$$f_n(x) \equiv g_n(x)h_n(x)(\mod \mathscr{Y}^{n+1})$$

$g_n(x)$ is a monic polynomial of degree r and $h_n(x)$ of degree $\leq m-r$. All the polynomials have coefficients in $\mathscr{O}$. □

225 The polynomials are constructed inductively. For $n = 0$, $g_o(x)$ and $h_o(x)$ are already given and satisfy the conditions. Assume now that $g_o(x), \ldots, g_{n-1}(x)$ and $h_o(x), \ldots, h_{n-1}(x)$ have been constructed so as satisfy the requisite conditions.

Since $g_{n-1}(x) \equiv g_o(x)(\mod \mathscr{Y})$ and $h_{n-1}(x) \equiv h_o(x)(\mod \mathscr{Y})$ and $g_0(x)$ and $h_o(x)$ are coprime $\mod \mathscr{Y}$, there exists, for any polynomial $f_n(x)$ in $\mathscr{O}[x]$, two polynomials $L(x)$ and $M(x)$ with

$$f_n(x) \equiv L(x)g_{n-1}(x) + M(x)h_{n-1}(x) (\mod \mathscr{Y}).$$

$L(x)$ and $M(x)$ are clearly not uniquely determined. We can replace $L(x)$ by $L(x) + \lambda(x)h_{n-1}(x)$ and $M(x)$ by $M(x) + \lambda(x)g_{n-1}(x)$.

Let π be a generator of the principal ideal $\mathscr{Y}$. By induction hypothesis,

$$f_n(x) = \pi^{-n}(f(x) - g_{n-1}(x)h_{n-1}(x))$$

is an integral polynomial, so in $\mathscr{O}[x]$. Since $g_{n-1}(x)$ has degree r and is monic and $h_{n-1}(x)$ degree $\leq m-r$, it is possible to choose $M(x)$ and $L(x)$ so that $M(x)$ has degree $< r$ and $L(x)$ degree $\leq m - r$. Put now

$$g_n(x) = g_{n-1}(x) + \pi^n M(x),$$
$$h_n(x) = h_{n-1}(x) + \pi^n L(x).$$

Then $g_n(x)$ is monic and of degree r, since $M(x)$ has degree $< r.h_n(x)$ has degree $\leq m - r$. Now $f(x) - g_n(x)h_n(x) = f(x) - g_{n-1}(x)h_{n-1}(x) - \pi^n(g_{n-1}(x)L(x) + h_{n-1}(x)M(x))(\mod \mathscr{Y}^{n+1})$ By choice of $L(x)$ and $M(x)$, it follows that

$$f(x) \equiv g_n(x)h_n(x)(\mod \mathscr{Y}^{n+1}).$$

226 We have thus constructed the two sequences of functions. Put now

$$g(x) = g_o(x) + (g_1(x) - g_o(x)) + \cdots + (g_n(x) - g_{n-1}(x)) + \cdots$$
$$h(x) = h_o(x) + (h_1(x) - h_o(x)) + \cdots + (h_n(x) - h_{n-1}(x)) + \cdots$$

Since $g_n(x) - g_{n-1}(x) = 0(\text{mod}\pi^n)$, it follows that the corresponding coefficients of the sequence of polynomials $g_0(x), g_1(x), \ldots$ form Cauchy sequences in $\mathscr{O}$. Since k is complete and

$$g(x) = \lim_{n\to\infty} g_n(x),$$

it follows that $g(x) \in \mho[x]$. It is monic and is of degree r. In a similar way, $b(x) \in \mho[x]$ and has degree $\leq m - r$.

Also since $f(x) - g_n(x)h_n(x) \equiv 0(\text{mod} y^{n+1})$, it follows that the coefficients of $(f(x) - g_n(x)h_n(x))$ form null sequences. Hence

$$f(x) = \lim_n g_n(x)h_n(x) = h_n(x) = g(x)h(x)$$

and our lemma is proved.

We now deduce the following important .

Lemma 3. *Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ be an irreducible polynomial $k[x]$, k satisfying hypothesis of lemma 2. Then $f(x) \in \mathscr{O}[x]$ if and only if $a_n \in \mathscr{O}$.*

Proof. It is clearly enough to prove the sufficiency of the condition. Let $a_n \in \mho$, and if $a_1, \ldots, a_{n-1}$ (some or all of them) are not in $\mho$, then there is a smallest power π^a, $a > 0$, of π such that

$$\pi^a f(x) = b_o x^n + b_1 x^{n-1} + \cdots + b_n$$

is a primitive polynomial in $\mathscr{O}[x]$. Also, now $b_n \equiv 0(\mod \mathscr{Y})$. and 227
at least one of $b_0, \ldots, b_{n-1}$ is not divisible by $\mathscr{Y}$. Let b_r be the first coefficient from the right not divisible by $\mathscr{Y}$. Then

$$\pi^a \equiv (b_0 x^r + \cdots b_r) x^{n-r} (\text{mod}\, \mathscr{Y})$$

Since $b_r \not\equiv 0(\mod \mathscr{Y})$, Hensel's lemma can be applied and we see that $\pi^a f(x)$ is reducible in $\mathscr{O}[x]$. Thus $f(x)$ is reducible in $k[x]$ which contradicts the hypothesis. The lemma is therefore established. □

We are now ready to prove the important theorem concerning extension of discrete non-archimedian valuations, namely

Theorem 5. *Let k be complete under a discrete non-archimedian valuation $||$ and K a finite algebraic extension over k. Then $||$ can be extended uniquely to K and then for any α in K,*

$$|\alpha| = \frac{1}{(K:k)}|N_{K/k}\alpha|.$$

Proof. Because of Theorem 4, it is enough to prove that the function defined on K by

$$|\alpha| = \frac{1}{(K:k)}|N_{K/k}\alpha|$$

is a valuation function. Clearly , $|0| = \infty$; $|\alpha|$ is a real number for $\alpha \neq 0$. Also,

$$|\alpha\beta| = |\alpha| + |\beta|.$$

We shall now prove that

$$|\alpha + \beta| \geq \min(|\alpha|, |\beta|).$$

228 If α or β is zero, then the above is trivial. So let $\alpha \neq 0, \beta \neq 0$. Since $\left|\frac{\alpha}{\beta}\right|$ or $\left|\frac{\beta}{\alpha}\right|$ is ≥ 0, it is enough to prove that if $|\lambda| \geq 0$, $|1+\lambda| \geq 0$. □

Let $f(x) = x^m + a_1x^{m-1} + \cdots + a_m$ be the minimum polynomial of λ in K over k, Then

$$N\lambda = ((-1)^m a_m)^{(K:k(\lambda))}.$$

Also, $N(1+\lambda) = (-1)^n(1 \pm a_1 \pm \cdots + a_m)^{(K:k(\lambda))}$. If $|N\lambda \geq 0|$, then $|a_m| \geq 0$ which , by lemma 3, means that $|a_1|, \ldots, |a_m|$. Hence $|N(1+\lambda)| \geq 0$. Our theorem is proved.

Incidentally it shows that the extended valuation is discrete also.

6 Fields complete under archimedian valuations

Suppose k is complete under an archimedian valuation. Then k has characteristic zero and contains, as a subfield, the completion $\bar{\Gamma}$ of the rational number field. $bar\Gamma(i)$ is, then, the complex number field. Every complex number is to the form $a + ib$, a, $b \in \bar{\Gamma}$. On $\bar{\Gamma}$, we have the ordinary absolute value. Define in $\bar{\Gamma}(i)$ the function

$$|z| = (a^2 + b^2)^{\frac{1}{2}}$$

where $z = a + ib$. It is, then, easy to verify that || is a valuation on $\bar{\Gamma}(i)$ which extends the valuation in $\bar{\Gamma}$. Also, by theorem 4, this is the only extension of the ordinary absolute value. We consider the case $k \supset \bar{\Gamma}(i)$ and prove the theorem of *A. Ostrowski.*

Theorem 6. *Let $k \supset \bar{\Gamma}(i)$ be the complex number field and let k be a field with archimedian valuation and containing $\bar{\Gamma}(i)$. If the valuation in k is an extension of the valuation in $\bar{\Gamma}(i)$, then $k = \bar{\Gamma}(i)$.*

Proof. If $k \neq \bar{\Gamma}(i)$, let $a \in k$ but not in $\bar{\Gamma}(i)$. Denote by || the valuation in **229**
k. Consider $|a - z|$ for all $k = \bar{\Gamma}(i)$. Since $|a - z|1 \geq 0$, we have

$$\rho = g \cdot \frac{1}{2} \cdot b|a - z| \leq 0.$$

There exists, therefore, a sequences $z_1, \ldots, z_n, ..$ of complex numbers such that

$$\lim_{n \to \infty} |a - z_n| = \rho.$$

□

But $z_n = z_n - a + a$ and so $|z_n| \leq |z_n - a| + |a|$ which shows that the $|z_n|$, for large n, are bounded. We may therefore, choose a subsequence $z_{i_1}, z_{i_2}, \ldots$ converging to a limit point z_o such that

$$\rho = \lim_{n \to \infty} |a - z_{i_n}| = |a - z_o|$$

We have thus proved the existence of a z_0 in $\bar{\Gamma}(i)$ such that $b = a - z_0$ has $|b| = \rho$. Since, by assumption, $a \notin \bar{\Gamma}(i)$ we have

$$|b| = \rho > 0.$$

ρ, by definition, being *g.l.b.*, it follows that

$$|b-z| \geq \rho$$

for $z \in \overline{\Gamma}(i)$.

Consider the set of complex numbers z with $|z| < \rho$. Let $n > 0$ be an arbitrary rational integer and ε, a primitive nth root of unity. Then

$$b^n - z^n = (b-z)(b-\varepsilon z)\ldots(b-\varepsilon^{n-1}z).$$

230 Therefore

$$\begin{aligned} |b-z|\rho^{n-1} &\leq |b-z||b-\varepsilon z|\ldots|b-\varepsilon^{n-1}z| = |b^n - z^n| \\ &\leq |b|^n + |z|^n = \rho^n(1+(\frac{|z|}{\rho})^n). \end{aligned}$$

Hence

$$|b-z| \leq \rho\left(1+\frac{|z|^n}{\rho^n}\right).$$

But $|z| < \rho$ and as n is arbitrary, it follows that $|b-z| \leq \rho$.

We therefore have

$$|z| < \rho \Rightarrow |b-z| = \rho.$$

We now prove that for every integer $m > 0$, $|b-mz| = \rho$ if $|z| < \rho$. For, suppose we have proved this for $m-1$ instead of m, then we can carry through the above analysis with $b-(m-1)z$ instead of b, then we can carry through the above analysis with $b-(m-1)z$ instead of b and then we obtain $|b-mz| = \rho$.

Suppose now that z' is *any* complex number. Then there is an integer $m > 0$ such that $|\frac{z'}{m}| < \rho$. Therefore

$$\left|b - m\frac{z'}{m}\right| = |b-z'| = \rho.$$

Now $z' = z' - b + b$ and so

$$|z'| \leq |b-z'| + |b| \leq 2\rho$$

which shows that all complex numbers are bounded in absolute value. This is a contradiction. Hence our assumption that $a \notin \overline{\Gamma}(i)$ is false .

The theorem is thereby proved,

Before proving theorem 7 which gives a complete characterization of all complete fields with archimedean valuation, we shall prove a couple of lemmas.

Lemma 4. *Let k be complete under an archimedean valuation $\|$ and λ in k such that $x^2 + \lambda$ is irreducible in $k[x]$. Then* $|1 + \lambda| \geq 1$. **231**

Proof. If possible, let $|1 + \lambda| < 1$. We construct, by recurrence, the sequence $c_0, c_1, c_2, \ldots$, in k, defined as follows: -

$$c_0 = 1$$
$$c_{n+1} = -2 - \frac{1+\lambda}{c_n} \qquad n = 0, 1, 2, \ldots$$

It, then, follows that $|c_n| \geq 1$. For, if we have proved it upto c_{n-1}, then
$$|c_n| \geq 2 - \frac{|1+\lambda|}{|c_{n-1}|} \geq 1.$$

Thus c_n does not vanish for any n. Also,

$$|c_{n+1} - c_n| = \frac{|1+\lambda||c_n - c_{n-1}|}{|c_n||c_{n-1}|} \leq \rho|c_n - c_{n-1}|$$

where $\rho = |1 + \lambda| < 1$. This means that the series

$$c_0 + (c_1 - c_0) + (c_2 - c_1) + \cdots$$

converges in k. Let it converge to c in k. Then

$$c = \lim_{n\to\infty} c_o + \cdots + (c_n - o_{n-1}) = \lim_{n\to\infty} c_n.$$

Therefore, by definition of c_n, we get $c = -2 - \dfrac{1+\lambda}{c}$. But this means that $-\lambda = c^2 + 2c + 1 = (c + 1)^2$ which contradicts the fact $x^2 + \lambda$ is irreducible in $k[x]$.

We now prove the □

Lemma 5. *If k is complete under an archimedian valuation, $\|$, then this valuation can be extended to $k(i)$.*

Proof. If $i \in k$, there is nothing to prove. Let $i \notin k$. Then every element of $k(i)$ is of the form $a + ib$, $a, b \in k$.

232 The norm from $k(i)$ to k of $\alpha = a + ib$ is

$$N\alpha = a^2 + b^2.$$

By theorem 4, therefore, it is enough to prove that

$$|\alpha| = |(a^2 + b^2)^{\frac{1}{2}}|$$

is a valuation on $k(i)$. By putting $\lambda = \dfrac{b^2}{a^2}$ in the lemma 4, we see that $|a^2 + b^2| \geq a^2$. Therefore

$$\begin{aligned}|(1 + a)^2 + b^2| &\leq 1 + |a^2 + b^2| + 2|a|\\ &\leq 1 + |a^2 + b^2| + 2\sqrt{|a^2 + b^2|}\\ &= (1 + \sqrt{|a^2 + b^2|})^2.\end{aligned}$$

This shows that

$$|1 + \alpha| \leq 1 + |\alpha|$$

and our lemma is proved. □

We now obtain a complete characterization of complete archimedian fields, namely,

Theorem 7. *The only fields complete under an archimedian valuation are the real and complex numbers fields.*

Proof. k has characteristic zero and since it is complete, it contains the field $\overline{\Gamma}$ of real numbers. If k contains $\overline{\Gamma}$ properly, then we assert that k contains i. For, $k(i)$, by lemma 5, is complete and $k(i)$ contains $\overline{\Gamma}(i)$ and, by theorem 6,

$$k(i) = \overline{\Gamma}(i).$$

□

Therefore

$$\overline{\Gamma}(i) = k(i) \supset k \supset \overline{\Gamma}.$$

But $(\overline{\Gamma}(i) : \overline{\Gamma}) = 2$ so that $k = k(i) = \overline{\Gamma}(i)$.

We have thus found all complete fields with archimedian valuation.

7 Extension of valuation of an incomplete field

Suppose k is a complete field under a valuation $||$ and let Ω be its algebraic closure. Then $||$ can be extended to Ω by the prescription 233

$$|\alpha| = |N\alpha|^{\frac{1}{n}},$$

where Norm is takes form $k(\alpha)$ over k and $n = (k(\alpha) : k)$. It is clear that it defines a valuation function. For, of K is a subfields of Ω and K/k is finite and K contains α then, by properties of norms,

$$|\alpha| = |N_{K/k}\alpha|^{\frac{1}{m}},$$

where $m = (K : k)$. So, if α and β are in Ω, we may take for K a field containing α and β and with $(K : k)$ finite.

Furthermore, defined as such, the valuation on Ω is dense because, if $|\alpha| > 1$, then $|\alpha|^{1/n}$ has value as near 1 as one wishes, by increasing n sufficiently. Also, for every n, $\alpha^{1/n}$ is in Ω.

Also, let σ be an automorphism of Ω/k, and α in Ω. Then, by definition of norm,

$$N\alpha = N(\sigma\alpha)$$

so that $|\alpha| = |\sigma\alpha|$. Thus all conjugates of an element have the same value.

We shall now study how one can extend a valuation of an incomplete field to an algebraic extension.

Let k be a field and K a finite algebraic extension of it. Let $||$ be a valuation of k and $\overline{k}$ the completion of k under this valuation. Let $k \neq \overline{k}$. 234

$$\begin{tikzcd}
 & K\bar{k} \arrow[dd, no head] \\
K \arrow[ur, no head] \arrow[dd, no head] & \\
 & \bar{k} \\
k \arrow[ur, no head] &
\end{tikzcd}$$

Suppose it is possible to extend $||$ to K. Let $\bar{K}$ be the completion of K under this extended valuation. Since $\bar{K} \supset K \supset k$, it follows that $\bar{K}$ contains K and $\bar{k}$ and therefore the composite $K\bar{k}$. Thus

$$\bar{K} \supset K\bar{k}.$$

On the other hand, $K\bar{k}/\bar{k}$ is a finite extension, since K/k is finite. Since $\bar{k}$ is complete, $K\bar{k}$ is complete also. $K\bar{k}$ contains K and hence its completion $\bar{K}$ under this extended valuation. Thus

$$\bar{K} = K\bar{k}.$$

Thus if the valuation can be extended, then the completion of K by this extended valuation is a composite extension of K and $\bar{k}$.

Suppose now that Ω is an algebraic closure of $\bar{k}$. Ω, then, contains an algebraic closure of k. We have seen above that the given valuation of k can be extended to Ω. Let σ be an isomorphism of K/k into Ω. The valuation in $\bar{k}$ can be extended to $\sigma K \cdot \bar{k}$ which is a subfield of Ω. Therefore, there is a valuation on σK. Define now, for α in K,

$$|\alpha|_o = |\sigma\alpha|$$

where $||$ is the extension of $||$ on k to $\sigma K \cdot \bar{k}$, which extension is unique. It is now trivial to see that $||_o$ is a valuation on K and extends $||$ on k.

Hence every isomorphism of K into Ω which is trivial on k, gives rise to a valuation of K.

235 We now inverstigate when two isomorphisms give rise to the same valuation on K. Let σ and τ be two isomorphisms of K/k into Ω giving the same valuation on K. σK and τK are subfields of Ω and they have

the same valuation. Thus $\mu = \sigma\tau^{-1}$ is an isomorphism of τK onto σK which preserves the valuation on τK. Now μ is identity on k and so on $\bar{k}$. Since $\sigma K \cdot \bar{k}$ is the completion of σK, it follows that μ is an isomorphism of the composite extensions $\sigma K\bar{k}$ and $\tau K\bar{k}$. Hence, if σ and τ give rise to the same valuation on K, the corresponding composite extensions are equivalent.

Suppose now that σ and τ are isomorphisms of K into Ω such that the composite extensions $\sigma K\bar{k}$ and $\tau K\bar{k}$ are equivalent. There exists then a mapping μ of $\tau K\bar{k}$ on $\sigma K\bar{k}$ which is identity on $\bar{k}$ and such that

$$\mu\tau = \sigma$$

σ induces a valuation $||_1$ on K such that $|\alpha|_1 = |\sigma\alpha|$ and τ induces a valuation $||_2$ on K such that $|\alpha|_2 = |\tau\alpha|$. But μ is such that $\mu\tau\alpha = \sigma\alpha$ or $\sigma\alpha$ and $\tau\alpha$ are conjugates over $\bar{k}$ in Ω. Hence

$$|\sigma\alpha| = |\tau\alpha|$$

or $||_1 = ||_2$ which shows that σ, τ give the same valuation on K.

We have hence the

Theorem 8. *A valuation $||$ of k can be extended to a finite extension K of k only in a finite number of ways. The number of these extensions of* **236** *$||$ to K stand in a (1, 1) correspondence with the classes of composite extensions of K and $\bar{k}$*

From what we have already seen, the number of distinct composite extensions of K and $\bar{k}$ is at most $(K : k)$.

We apply these to the case where $k = \Gamma$, rational number field and K/Γ finite so that K is an algebraic number filed. From theorem 2, it therefore follows that K has at most $(K : \Gamma)$ distinct archimedian valuations and that all the non-archimedian valuations of K, which are countable in number, are discrete.

In a similar manner, if K is an algebraic function field of one variable over a constant filed k, then all the valuations of K are non-archimedian and discrete. This can be seen from the fact that if $x \in K$ is transcendental over k, then $K/k(x)$ is algebraic and one has only to apply theorems 3 and 8.

Appendix

Abelian groups

1 Decomposition theorem

237 All the groups that we deal with here are abelian. Before proving the main decomposition theorem for finite abelian groups we shall prove some lemmas.

Lemma 1. *If a, b are elements in G and have orders m and n respectively and $(m, n) = 1$, then ab has order mn.*

Proof. Clearly if t is the order of ab, $t|mn$, since

$$(ab)^{mn} = (a^m)^n (b^n)^m = e,$$

e being unit element of G. Also $a^t = b^{-t}$. Thus

$$e = a^{tm} = b^{-tm}$$

so that n/t. Similarly $m|t$. Hence $t = mn$. □

Lemma 2. *Let p be a prime number dividing the order n of the group G. Then there is, in G, an element of order p.*

Proof. We use induction on n. Let $\underline{a}$ be an element in G of order m. If $p|m$, then $a^{m/p}$ has order p and we are through. Suppose $p \nmid m$. Let H be the cyclic group generated by $\underline{a} \cdot G/H$ has then order n/m which is divisible by p. Since $\dfrac{n}{m}|n$, induction hypothesis applies, so that there is a coset Hb of order p. If b has order t then $b^t = e$ and so $(Hb)^t = H$ which means that $p|t$ and so $b^{t/p}$ has order p. □

Lemma 3. *Let G be a finite group and λ the maximum of the orders of elements of G. Then*

$$a^{\lambda} = e$$

238 *for all $a \in G$.*

Proof. Let b be an element of order λ. Let $\underline{a}$ be any element in G and let μ be its order. To prove the lemma, it is enough to prove that $\mu|\lambda$. If not, there is a prime p which divides μ to a higher power than it does λ. Let p^r be the highest power of p dividing μ and p^s the highest power dividing λ. Then $r > s$. We will see that this leads to a contradiction. □

Since $\dfrac{\mu}{p^r}$ and p^r are coprime, $a^{\frac{\mu}{p^r}}$ has the order p^r. Similarly b^{p^s} has order $\dfrac{\lambda}{p^s}$. By lemma 1,

$$c = a^{\frac{\mu}{p^r}} \cdot b^{p^s}$$

has order $p^r . \dfrac{\lambda}{p^s} > \lambda$, which contradicts the definition of λ. Hence $\mu|\lambda$.

Lemmas 2 and 3 show that $\lambda|n$ where n is the order of the group and that λ and n have the same prime factors. λ is called the *exponent* of the finite group G.

A set $a_1, \ldots, a_n$ of elements of a finite group G are said to be *independent* if

$$a_1^{x_1} \cdots a_n^{x_n} = e$$

implies $a_i^{x_i} = e$, $i = 1, \ldots, n$.

If G is a finite group and is a direct product of cyclic groups $G_1, \ldots, G_n$ and if $a_i, i = 1, \ldots, n$ is a generator of G_i, then $a_1, \ldots, a_n$ are independent elements of G. They are said to form a *base* of G.

239 We shall now prove

Theorem 1. *Let G be a finite group of order n. Then G is the direct product of cyclic groups $G_1, \ldots, G_l$ of orders $\lambda_1, \ldots, \lambda_l$ such that $\lambda_i | \lambda_{i-1}, i = 2, \ldots, l, \lambda_\ell > 1$.*

Proof. We prove the theorem by induction on the order n of the group G. Let us therefore assume theorem proved for groups of order $< n$. Let

G have order n. Suppose λ_1 is the exponent of G. If $\lambda_1 = n$, then G is cyclic and there and there is nothing to prove. Let therefore $\lambda_1 < n$. There is an element a_1 of order λ_1. Let G_1 be the cyclic group generated by a_1. G/G_1 has order $\dfrac{n}{\lambda_1} < n$. Hence induction hypothesis works on G/G_1. □

G/G_1 is thus the direct product of cyclic groups $W_2, \ldots, W_l$ of order $\lambda_2, \ldots, \lambda_l$ respectively and $\lambda_l | \lambda_{l-1} | \ldots | \lambda_2$. Let H_i be a generator of W_i. Then $H_i = G_l b_i$ for some b_i in the coset H_i. Let the element b_i in G have order t_i. Then $t_i | \lambda_1$ by lemma 3. But

$$H_i^{t_i} = b_i^{t_i} G_1^{t_i} = G_1$$

which proves that $\lambda_i | \lambda_1$. Thus $\lambda_l | \lambda_{l-1} | \ldots | \lambda_1$.

Let now $b_i^{\lambda_i} = a_1^{x_i}$. Put $x_i = y_i \cdot z_i$ where $(y_i, \lambda_1) = 1$ and all the prime factors of z_i divide λ_1. Choose u_i prime to λ_1 such that

$$u_i y_i \equiv 1 (\bmod \lambda_1).$$

Then $b_i^{u_i \lambda_i} = a_1^{z_i}$. Since λ_1 is the exponent of G, 240

$$e = b_i^{u_i \lambda_1} = (a_1^{z_1})^{\lambda_1/\lambda_i}.$$

Since a_1 has order λ_1 this means that $\lambda_i | z_i$, $i = 2, 3, \ldots, l$.

Put now

$$a_i = b_i^{u_i} \quad a_1^{-z_i/\lambda_i}.$$

Since u_i is prime to λ_1 and so to λ_i, the coset $F_i = G_l a_i$ is also a generator of W_i. Thus $G_1 a_2, \ldots, G_1 a_l$ is a base of G/G_1.

Let a_i have order f_i. Then

$$e = a_i^{f_i} = b_i^{u_i f_i} a_i^{-f_i z_i/\lambda_i}.$$

This means that

$$b_i^{u_i f_i} = a_i^{f_i z_i/\lambda_i}.$$

Therefore by definition of $b_i, \lambda_i | u_i f_i$. But $(u_i \lambda_i) = 1$. Hence $\lambda_i | f_i$.

On the other hand

$$a_i^{\lambda_i} = b_i^{u_i\ \lambda_i} a_i^{-z_i} = e.$$

Hence $f_i = \lambda_i$. We have thus elements $a_1, \ldots, a_l$ in G which have orders $\lambda_1, \ldots, \lambda_l$ satisfying $\lambda_l | \lambda_{l-1} | \ldots | \lambda_1$.

We maintain that $a_1, \ldots, a_1$ are independent elements of G. For, if

$$a_1^{v_1} \ldots a_l^{v_l} = e,$$

241 then $a_2^{v_2} \cdot \cdots \cdot a_l^{v_l} = a_1^{-v_1}$ which means that $F_2^{v_2} \ldots F_l^{v_l} = G_1$. But since $F_2, \ldots, F_l$ are independent, $\lambda_i | v_i$, $i = 2, \ldots, l$. But this will mean that $a_1^{v_1} = e$ or $\lambda_1 | v_1$.

Since $\lambda_1 \ldots \lambda_l = n$, if follows that $a_1, \ldots, a_l$ form a base of G and the theorem is proved.

Let G be a group of group of order n and let G be direct product of cyclic groups $G_1, G_2, \ldots, G_l$ of orders $\lambda_1, \ldots, \lambda_l$. We now prove

Lemma 4. *Let μ be a divisor of n. The number $N(\mu)$ of elements $a \in G$ with*

$$a^\mu = e$$

is given by

$$N(\mu) = \prod_{i=1}^{\ell} (\mu, \lambda_i).$$

Proof. Let $a_1, \ldots, a_l$ be a base of G so that a_i is of order λ_i. Any $a \in G$ has the form

$$a = a_1^{x_1} \cdots a_l^{x_l}.$$

If $a^\mu = e$, then $e = a_1^{x_1\mu} \cdots a_l^{x_l\mu}$. Since $a_1, \ldots, a_l$ is a base, this means that $x_i\mu \equiv 0 (\operatorname{mod} \lambda_i)$, $i = 1, \lambda, l$. Hence x_i has precisely (μ, λ_i) possibilities and our lemma is proved.

We can now prove the □

Theorem 2. *If G is the direct product of cyclic groups $G_1, \ldots G_l$, of orders $\lambda_1, \ldots, \lambda_l$ respectively with $\lambda_l | \lambda_{l-1} | \cdots | \lambda_1$ and G is also the direct product of cyclic groups $H_1, \ldots, H_m$ of orders $\mu_1, \ldots, \mu_m$ respectively* 242 *with $\mu_m | \mu_{m-1} | \cdots | \mu_1$, then $m = 1$ and*

$$\lambda_i = \mu_i, i = 1, \ldots, l.$$

Proof. Without loss in generality let $l \geq m$. Let $a_1, \ldots, a_l$ be a base of G in the decomposition $G_1 \times G_2 \times \cdots \times G_1$. Since the number of elements $\underline{a}$ with $a^{\mu} = e$ is independent of the decomposition

$$N(\mu) = \prod_{1=1}^{\ell} (\mu, \lambda_i) = \prod_{j=1}^{m} (\mu, \mu_j)$$

Put now $\mu = \lambda_1$. Then $N(\mu) = \lambda_1^1$. But since $(\mu, \mu_j) \leq \mu$, it follows that $\lambda_\ell^\ell \leq \lambda_\ell^m$, so that $l \leq m$. This proves

$$l = m.$$

□

Also it follows that each factor $(\lambda_1, \mu_j) = \lambda_\ell$ or $\lambda_\ell | \mu_\ell$. Inverting the roles of λ and μ we get

$$\lambda_\ell = \mu_\ell.$$

Suppose now it is proved that $\lambda_{q+1} = \mu_{q+1}, \ldots, \lambda_1 = \mu_1$. Then by putting $\mu = \lambda_q$, we have

$$N(\mu) = \lambda_q^q . \lambda_{q+1} \cdots \lambda_1 = \prod_{j=1}^{q} (\lambda_q, \mu_j) \lambda_{q+1} \cdots \lambda_\ell.$$

By the same reasoning as before, it follows that $\lambda_q = \mu_q$ and we are, therefore, through.

For this reason, the integers $\lambda_1, \ldots, \lambda_l$ are called the *canonical invariants* of G. From theorems 1 and 2 we have the *Corollary Two finite groups G and G′ are isomorphic if and only if they have the same canonical invariants.*

2 Characters and duality

243

Let G be a group, not necessarily abelian and Z a cyclic group. A homomorphism χ of G into Z is called a *character* of G. Thus

$$\chi(a)\chi(b) = \chi(ab).$$

If we denote the unit element of G by e and that of Z by 1, then

$$\chi(e) = 1.$$

The character χ_o defined by $\chi_o(a) = 1$ for all $a \in G$ is called the *Principal character.*

If χ_1 and χ_2 are two characters, we define their product $\chi = \chi_1\chi_2$ by

$$\chi(a) = \chi_1(a)\chi_2(a)$$

and the inverse of χ_1 by

$$\chi_1^{-1}(a) = (\chi_1(a))^{-1}.$$

Under this definition, the characters form a multiplicative abelian group G^* called the *character group* of G.

Since χ is a homomorphism, denote by G_χ the kernel of the homomorphism χ of G into Z. Then G/G_χ is abelian. Denote by H the subgroup of G given by

$$H = \bigcap_\chi G_\chi, \qquad \chi \in G^*.$$

Then clearly G/H is abelian.

We call Z an *admissible group* for G if H consists only of the identity element. This means first that G is abelian and furthermore that given any two elements a, b in G there exists a character χ of G such that, if $a \neq b$, 244

$$\chi(a) \neq \chi(b).$$

If χ is a character of G, then χ can be considered as a character of G/G_o where χ is trivial on G_o, by defining $\chi(G_oa) = \chi(a)$, G_oa being a coset of G modulo G_o. In particular, the elements of G^* can be considered as characters of G/H. Moreover Z is now an admissible group for G/H.

We now prove the

Theorem 3. *If G is a finite abelian group and Z is an admissible group for G, then G^* is finite and G is isomorphic to G^*.*

Proof. In the first place Z is a finite group. For, if $a \in G$, $a \neq e$, there is a character χ such that

$$\chi(a) \neq 1.$$

If G is of order n, then $\chi(a^n) = (\chi(a))^n = 1$ so that $\chi(a)$ in an element of Z of finite order. Since Z is cyclic it follows that Z is finite. □

From this it follows that G^* is finite.

Since $(\chi(a))^n = 1$ for every χ and every $\underline{a}$, there is no loss in generality if we assume that Z is a cyclic group of order n.

In order to prove the theorem let us first assume that G is a cyclic group of order n. Let $\underline{a}$ be a generator of G and $\underline{b}$ a generator of the cyclic group Z of order $\underline{n}$. Define the character χ_1 of G by 245

$$\chi_1(a) = b.$$

Since $\underline{a}$ generates G any character is determined uniquely by its effect on $\underline{a}$. χ_1 is an element of order n in G^*. Let χ be any character of G. Let

$$\chi(a) = b^{\mu}$$

for some integer μ. Consider the character $\tilde{\chi} = \chi \cdot \chi_1^{-\mu}$.

$$\tilde{\chi}(a) = (\chi_1(a))^{-\mu}\chi(a) = b^{-\mu}\ b^{\mu} = 1$$

which shows that $\tilde{\chi} = \chi_o$ is the principal character. Hence G^* is a cyclic group of order n and the mapping

$$a \rightarrow \chi_1$$

establishes an isomorphism of G on G^*.

Let now G be finite non-cyclic abelian of order n. G is then a direct product of cyclic groups $G_1, \ldots, G_l$ of orders $\lambda_1, \ldots, \lambda_l$ respectively. Let a_i be a generator of G_i so that $a_1, \ldots, a_l$ is a base of G. Since $\lambda_1, \ldots, \lambda_l$ divide n, we define l characters $\chi_1, \chi_2, \ldots, \chi_l$ of G by

$$\begin{aligned} \chi_i(a_j) &= 1 \qquad j \neq i \\ \chi_i(a_i) &= b_i \qquad i = 1, \ldots, l, \end{aligned}$$

where b_i is an element in Z of order λ_i. These characters are then independent elements of the abelian group G^*. For, if $\chi_1^{t_1} \cdots \chi_l^{t_l} = \chi_0$, then, for any a $\in G$,

$$\chi_1^{t_1}(a) \ldots \chi_\ell^{t_l}(a) = 1.$$

246 Taking for a successively $a_1, \ldots, a_l$ we see that $\lambda_i | t_i$ and so $\chi_1, \ldots, \chi_l$ are independent.

Let χ be any character of G. Then χ is determined by its effect on $a_1, \ldots, a_l$. Let $\chi(a_i) = s_i$. Since $a_i^{\lambda_i} = e$, $(\chi(a_i))^{\lambda_i} = 1$. But $(\chi(a_i))^{\lambda_i} = s_i^{\lambda_i}$. Thus $s_i^{\lambda_i} = 1$. Z being cyclic, there exists only one subgroup of order λ_i. Thus

$$\chi(a_i) = s_i = b_i^{\mu_i},$$

for some integer $\mu_i(\text{mod } \lambda_i)$. Consider the character $\tilde{\chi} = \chi\chi_1^{-\mu_1} \cdots \chi$. It us clear that $\tilde{\chi}(a_i) = 1$ for all i so that $\tilde{\chi} = \chi_o$ or

$$\chi = \chi_1^{\overset{\mu}{1}} \cdots \chi_\ell^{\overset{\mu}{\ell}}.$$

Thus G^* is the product of cyclic group generated by $\chi_1, \ldots, \chi_1$. By Corollary to theorem 2, it follows that G and G^* are isomorphic.

Corollary. *If G is a finite group and G^* its character group, then whatever may be Z,*

$$Order G^* \leq Order G.$$

Proof. For, if H is the subgroup of G defined earlier, then G/H is abelian and finite, since G is finite. Also Z is admissible for G/H. Furthermore every character of G can be considered as a character of G/H, by definition of H. Hence by theorem 3 □

Order $G^* \leq$ Order $G/H \leq$ Order G.

Let us now go back to the situation where G is finite abelian and Z
247 ia admissible for G. Then $G \simeq G^*$. Let us define on $G \times G^*$ the function

$$(a, \chi) = \chi(a).$$

For a fixed χ, the mapping $a \to (a, \chi)$ is a character of G and so an element of G^*. By definition of product of character, it follows that, for fixed a, the mapping

$$\overline{a} : \chi \to (a, \chi)$$

is a homomorphism of G^* into Z and hence a character of G^*, Let G^{**} denote the character group of G^*. By Corollary above,

$$\text{Order} G^{**} \leq \text{Order} G^* = \text{Order} G.$$

Consider now the mapping

$$\sigma : a \to \bar{a}$$

of G into G^{**}. This is clearly a homomorphism. If $\bar{a}$ is identity, then $(a, \chi) = 1$ for all χ. But since Z is admissible for G, it follows that $a = e$. Hence σ is an isomorphism of G into G^{**}. Therefore we have

Theorem 4. *The mapping $a \to \bar{a}$ is a natural isomorphism of G^* on G^{**}*

Note that the isomorphism of G on G^* is *not natural*.

Under the conditions of theorem 3, we call G^* the dual of G. Then G^{**} is the dual of G^* and theorem 4 shows that the dual of G^* is naturally isomorphic to G. Theorem 4 is called the *duality theorem* for finite abelian groups.

3 Pairing of two groups

Let G and G' be two groups, $\sigma, \sigma', \ldots$, elements of G' and $\tau, \tau', \ldots$, elements of G'. Let Z be a cyclic group. Suppose there is a function 248
(σ, τ) on $G \times G'$ into Z such that for every σ, the mapping

$$\lambda_\sigma : \tau \to (\sigma, \tau)$$

is a homomorphism of G' into Z and for every τ, the mapping

$$\mu_\tau : \sigma \to (\sigma, \tau)$$

is a homomorphism of G into Z, Thus λ_σ and μ_τ are characters of G' and G respectively. We then say that G and G' are *paired* to Z and that (σ, τ) is a pairing.

For every σ, let G'_σ denote the kernel in G' of the homomorphism λ_σ. Put

$$H' = \bigcap_\sigma G'_\sigma$$

for all $\sigma \in G$. Then G'/H' is abelian. Also, H' is the set of τ in G' such that

$$(\sigma, \tau) = 1$$

for all $\sigma \in G$. Define in a similar way the subgroup H of G.

We are going to prove

Theorem 5. *If G/H is finite, then so is G'/H' and both are then isomorphic to each other.*

Proof. From fixed σ, consider the function

$$\chi_\sigma(\tau) = (\sigma, \tau).$$

□

This is clearly a character of G'. By definition of H', it follows that for each σ, χ_σ is a character of G'/H'.

Consider now the mapping

$$\sigma \to \chi_\sigma$$

of G into $(G'/H')^*$. This is again a homomorphism of G into $(G'/H')^*$. The kernel of the homomorphism is the set of σ for which χ_σ is the principal character of G'/H'. By definition of H, it follows that H is the kernel. Hence

$$G/H \simeq \text{ a subgroup of } (G'/H')^*. \tag{1}$$

249

In a similar way

$$(G'/H') \simeq \text{ a subgroup of } (G/H)^*. \tag{2}$$

Let now G/H be finite. Then by Corollary to theorem 3,

$$\text{ord}(G/H)^* \leq \text{ord} G/H.$$

By (2), this means that

$$\text{order}(G'/H') \leq \text{ order } G/H.$$

Reversing the roles of G and G' we see that G/H and G'/H' have the same order. (1) and (2) together with theorem 3 prove the theorem.

If, in particular, we take G^* for G', then $H' = (\chi_o)$ and so we have

Corollary. *If G is any group, G^* its character group and if G/H is finite then*

$$G/H \simeq G^*.$$

Bibliography

[1] A. A Albert Modern Higher Algebra, Chicago, (1937) **250**

[2] E.Artin Galois Theory, Notre Dame, (1944)

[3] E.Artin Algebraic numbers and Algebraic functions, Princeton (1951)

[4] E. Artin and 0.Schreier Eine Kennzeichnung der reell abgeschlossene Korper Hamb, Abhand, Bd 5 (1927) p. 225-231

[5] N. Bourbaki Algebra, Chapters 3-6, paris, 1949

[6] C. Chevalley Introduction to the theory of Algebraic functions, New York, 1951

[7] C. Chevalley Sur la theorie du corps de classes dans les corps finis et les corps locaux Jour. Faculty of Science, Tokyo, Vol, 2, 1933,P. 365-476

[8] M. Deuring Algebren, Ergebn der Math, Vol.4, 1935

[9] S. Eilenberg and S. Maclane Cohomology theory in abstract groups, Annals of Mathematics, Vol.48 (1947), P. 51-78

[10] H. Hasse Zahlentheorie, Berlin, 1949

[11] W. Krull Galoissche theorie der unendlicher erweiterungen Math. Annalen Bd 100 (1928), P.678-698

[12] N. H McCoy Rings and ideals,Carus Mathematical Monographs, No.8 (1948)

251 [13] A. Ostrowski Untersuchugen zur arithmetischen Theorie der Korper Math. Zeit, Bd 39 (1935), P.269-404

[14] G. Pickert Einfuhrung in die Hohere Algebra,Gottingen 1951

[15] B.Steinite Algebraische Theorie der Korper Crelles Jour. Bd 137 (1910), P. 167-309

[16] B.L Van-der-Waerden ModerneAlgebra, Leipzing, 1931

[17] A. Weil Foundations of Algebraic gemetry New York, 1946

[18] E.Witt Uber die commutativitat endlicher Schiefkorper Hamb. Abhand, Vol 8, (1931), P.413

[19] E. Witt Der existenzsatz fur Abelsche Funktionekorper Crelles jour. Bd 173 (1935), P 43-51