PETER ROQUETTE

Analytic theory of elliptic functions over local fields

VANDENHOECK & RUPRECHT IN GÖTTINGEN

Hamburger Mathematische Einzelschriften
Neue Folge · Heft 1

Herausgegeben vom
Mathematischen Seminar der Universität Hamburg

 Gesamtherstellung: Hubert & Co., Göttingen

Contents

§ 1. Introduction

For the purpose of these notes, a *local field* is defined to be a field K, equipped with a non-trivial real-valued valuation $a \to |a|$ such that K is *complete* with respect to this valuation. It is assumed, furthermore, that the valuation of K is *nonarchimedean*, i.e. that the triangle inequality holds in the form

$$|a + b| \leqq \mathrm{Max}\,(|a|, |b|)^{1)}.$$

Although, from the standpoint of number theory, the main interest is concerned with those local fields which are locally compact, we do not make any assumption in this direction.

Our starting point is the observation that for any local field there is an analytic theory of periodic functions which is very much analogous to the classical theory of doubly periodic complex functions. More precisely, the parallelism between these two theories becomes evident if one considers in the complex case the Fourier expansions, usually called q-expansions, of the functions involved. The situation can be described simply by saying that the classical q-expansions, if freed from normalizing constants which have no counterpart in the non-archimedean case, converge universally and thus lead to a theory of periodic functions over an arbitrary local field[2]).

The theory of q-periodic functions over local fields has been developed by Tate. Since no exposition of this theory seems to be available in published form, except a brief remark by Shatz [18], we have included in these notes such an exposition, which will be found in § 2, based on an oral communication by Tate.

For any $q \in K$ with $0 < |q| < 1$, we shall show in § 2 that the q-periodic functions defined over K form an elliptic function field over K, denoted by $F_K(q)$. Once this has been established, the following question arises: Which elliptic function fields $F\,|\,K$ can be analytic-

---

[1]) Much of what we shall say, however, remains true if the valuation of K is archimedean, i. e. if K is the real or the complex number field (a notable exception being the last statement in theorem VII, § 3).

[2]) For the classical theory we refer e. g. to [6]. One should remark that what in the classical theory is usually denoted by q, will be $q^{1/2}$ in our notation.

ally represented by a field $F_K(q)$ of periodic functions? In the classical case, over the complex number field, it is well known that *every* elliptic function field is represented by a field of periodic functions. Over a local field K, the situation is different, even if K is algebraically closed. Namely, we show in § 3 that a necessary condition for $F|K$ to admit such an analytic representation is that its absolute invariant j satisfies $|j| > 1$. If K is algebraically closed, this condition is also sufficient, while for an arbitrary local field there are additional conditions, due to the fact that an elliptic function field need not have a prime divisor of degree 1 and even if it does it is not uniquely determined, up to K-isomorphisms, by its absolute invariant (see § 3).

The condition $|j| > 1$ characterizes those elliptic function fields $F|K$ which do not admit a good reduction modulo the prime of K, not even after applying an algebraic extension of the field of constants. These fields have resisted so far a detailed investigation by "algebraic" methods, and it seems to us a fortunate circumstance that the analytic methods, as developed in these notes, lead to such fields and thus provide us with a handy tool for investigating these fields. This is what we propose to do in these notes which are based on several lectures which we have given at various places, including Columbus (Ohio), Hamburg and Heidelberg, in the past years.

These lectures were directed to an audience which was supposed to have acquired a fair knowledge of the algebraic theory of function fields. Such knowledge will be helpful also for the reader of these notes although he will perceive that only the very rudiments of this theory are required; for these he may consult e.g. [3], [5] or [10]. For the benefit of the reader, we have included an appendix devoted to some aspects of the algebraic theory of elliptic function fields which are used in the text, namely their absolute and Hasse invariants, their Jacobian function fields, and their automorphisms.

We are now going to describe briefly the contents of these notes.

§ 2 contains an exposition of the theory of periodic functions. The necessary facts about the general theory of analytic functions over local fields, which are stated without proof, can be found in [8]. The central theorem of this § 2, and of most of these notes, is the *Abel-Jacobi theorem* which appears in two stages: first in proposition 1 as part of the analytic theory, giving a necessary and sufficient condition for a periodic divisor to be the divisor of a periodic function. Once this has been established, the application of the well known Artin-Whaples theorem exhibits the structure of the field $F_K(q)$ of periodic functions

as an elliptic function field. In the second stage, the Abel-Jacobi theorem then can be interpreted as describing the structure of the group of divisor classes of degree 0 of this elliptic function field by means of a canonical isomorphism Φ_q to the factor group $K^\times/q$ of the multiplicative group of K modulo the cyclic group generated by the fundamental period q. We have here one of the rare occasions that the group of divisor classes of degree 0, which plays a fundamental rôle in the algebraic theory of function fields, can be explicitely described. The isomorphism Φ_q can be regarded as a substitute of the integration procedure which is usually used in the classical case (see e.g. Chevalley [3], p. 172) and $K^\times/q$ is the multiplicative analogue to the parallelogram of periods appearing in the classical theory of doubly periodic functions.

§ 3 contains the investigation of the Weierstraß $\wp$-function which serves to generate $F_K(q)$ together with its derivative. In order to be able to deal also with characteristic 2 and 3 we use a normalization of $\wp$ which differs from the classical one by the summand $\frac{1}{12}$ (up to other normalizing constants which appear in the classical theory from analytic motivations and have no counterpart over local fields).

Also, due to such characteristic considerations, the defining relation of $F_K(q)$ over K does not appear in Weierstraß normal form but in the normal form

$$\wp'^2 + \wp\wp' = \wp^3 + B\wp + C$$

with $B, C \in K$; this can be easily transformed into Weierstraß normal form if char $(K) \neq 2, 3$. The coefficients B, C are explicitely determined as universal power series in the fundamental period q with integral coefficients; this leads to a similar expression of the absolute invariant j which coincides in effect with the classical q-expansion of the modular function. Over local fields, it turns out that j and q determine each other uniquely, contrary to the classical phenomenon that the modular function admits the "modular group". This observation leads to an algebraic description of those elliptic function fields which can be K-isomorphically represented as field of periodic functions, mentioned already earlier in this introduction.

§ 4 is devoted to the description of those elliptic function fields E which admit a field of periodic functions as their Jacobian. It turns out, as a consequence of the Abel-Jacobi theorem, that these fields E can be described by certain characters χ of the Galois group over K, namely those characters for which the fundamental period q is a norm from the cyclic extension K_χ determined by χ. (We have called such a character "q-trivial"). This result can be regarded as a generalization, for the elliptic fields $F_K(q)$, of Tate's cohomological duality theorem [20] which holds only for p-adic ground fields in the usual sense. As a consequence, we prove a remarkable property of the fields E in question concerning their *splitting fields* L, i.e. those fields L for which the constant extension EL has a prime divisor of degree 1. It turns out that *E has a unique minimal algebraic splitting field*, namely the field K_χ. This property is in contrast to the behavior of the fields E with good reduction (for which $|j| \leqq 1$) for we know in the latter case from the work of Lang-Tate [12] that only the ramification of an algebraic extension $L|K$ is responsible for the splitting of E.

§ 5 contains a more detailed description of the fields E mentioned in § 4, by means of their representation as fields of so-called "semi-periodic" functions. We prove the Abel-Jacobi theorem for these fields, and also a remarkable "norm theorem" which can be used to describe the structure of the Brauer group of E although we only prove two preliminary results in this direction: One theorem determines the algebras over K which are split by E, in generalization of our previous results concerning p-adic fields only [16]. A second theorem reduces the Brauer group of E to the Brauer group of the constant extension EK_χ; this result can be regarded as the counterpart of the corresponding result over the real number fields obtained by Witt [22] and Geyer [7].

These results, as well as the minimal splitting property of K_χ mentioned in § 4, seem to be not very well understood from the algebraic point of view; perhaps Néron's theory of minimal models [14] can help to give an algebraic explanation of these facts.

Finally, in § 6 we study the elliptic subfields and the isogenies of the fields $F_K(q)$ and, more generally, of the elliptic fields which admit $F_K(q)$ as Jacobian. For the fields $F_K(q)$, we prove that an isogeny between them exists if and only if the corresponding fundamental periods are commensurable, and we determine all these isogenies. This leads to the statement that $F_K(q)$ does not have complex multiplication, which seems worthwhile to be mentioned since its proof does not use any of the deeper facts usually employed in proving the absence of complex multiplication if the absolute invariant is not absolutely integral. If E is an elliptic field admitting $F_K(q)$ as its Jacobian, we again determine all elliptic subfields of E, proving in particular that E contains a unique maximal subfield which is K-isomorphic to $F_K(q)$ itself. Perhaps this result can be used to obtain, at least in special cases, an explicit description of generators and defining relations for such a field E.

Concluding remarks: The algebraic theory of elliptic function fields has been highly developed during the past decades. It arises the question of the value of an analytic theory as developed in these notes. In our opinion its value rests in the fact that it provides the algebraist with a series of *explicit examples* where algebraic statements can be analytically tested and interpreted. Its shortcoming is, of course, that it yields an analytic representation only for elliptic fields of absolute invariant $|j| > 1$; it would be highly desirable to have a similar theory also for the case $|j| \leqq 1$. The problem is, for any elliptic field $F|K$ with a prime divisor of degree 1, to give an explicit analytic representation of the "universal covering" of its group of divisor classes of degree 0; in the case $|j| > 1$ this is essentially the multiplicative group $K^\times$ and the covering map is given by the residue class map $K^\times \to K^\times/q$. Perhaps the theory of rigid analytic spaces, as initiated by Tate [21] and developed by Grauert, Nastold and others, will provide the analytic background for the solution of this problem.

Another problem is, of course, the generalization to fields of higher genus, thus extending the classical theory of Picard to local fields. Here, one is lead naturally to theta functions of $g > 1$ variables; such a theory has already been developed by Morikawa [13] and it would be a worthwhile enterprise to use this theory in order to establish a generalization of the results of this note to abelian function fields of more than one variable.

Terminology: In these notes, a *function field* $F|K$ is defined to be a finitely generated field extension of K of degree of transcendency 1, such that K is algebraically closed in F.

If the function field $F|K$ has genus 1 then it is called *elliptic*, provided that $F|K$ is *conservative*, i.e. that its genus does not change after applying an extension of the field K of constants[1]).

Let $F|K$ be a function field and L any extension field of K. If the constant extension $FL|L$ has a prime divisor of degree 1 then L is called a *splitting field* of $F|K$, and F is said *to split over* L.

[1]) This conservativity assumption is automatically satisfied if char $(K) \neq 2, 3$ (see [19]).

§ 2. Fields of periodic functions

Let K be a local field. The valuation of K has a unique extension to the algebraic closure Ω of K; this extension will also be denoted by $|\alpha|$ $(\alpha \in \Omega)$. Every finite extension L of K is then complete, hence local. Ω itself is in general not complete.

We consider formal Laurent series

$$f(X) = \sum_{n \in Z} a_n X^n \qquad (a_n \in K)$$

which have the property that $f(\alpha)$ is convergent for every element $\alpha \neq 0$ in Ω. This is equivalent to saying that

$$\lim_{n \in Z} |a_n| \, r^n = 0$$

for every real number $r > 0$. Note that, if this is the case, then $f(\alpha)$ is an element of the complete field $K(\alpha)$.

Every such series $f(X)$ determines a function $\alpha \to f(\alpha)$ from $\Omega^\times$ to Ω and it is uniquely determined by this function. We shall identify $f(X)$ with its corresponding function, and call $f(X)$ a *holomorphic function* on $\Omega^\times$. More precisely, it is a holomorphic function *defined over* K since the coefficients a_n of $f(X)$ are assumed to be in K.

The holomorphic functions on $\Omega^\times$ form an integral domain, containing K as the constant functions. This integral domain is denoted by H_K.

A *meromorphic function* on $\Omega^\times$ is defined to be an element of the quotient field of H_K. This is denoted by M_K.

Now let q be an element in K with

$$0 < |q| < 1.$$

A meromorphic function f is said to admit the *period* q if it satisfies the functional equation

$$f(q^{-1}X) = f(X). \tag{1}$$

These q-periodic functions form a subfield of M_K which contains K and which is denoted by $F_K(q)$.

The first observation is that $F_K(q)$ is *an elliptic function field* over K. To see this, and also to obtain more precise information about this function field, one proceeds as follows:

Let $\alpha \in \Omega^\times$, and let $\varphi_\alpha(X)$ denote the irreducible polynomial of α over K, with highest coefficient 1. Every holomorphic function $0 \neq f(X) \in H_K$ can be written uniquely in the form

$$f(X) = \varphi_\alpha(X)^m \cdot g(X)$$

with $m \geqq 0$, $m \in \mathbf{Z}$, and $g(X) \in H_K$, $g(\alpha) \neq 0$. This can be proved with the help of Hensel's lemma for convergent Laurent series[1]). The exponent m is called the *order* of f at α and is denoted by $w_\alpha(f)$. We put $w_\alpha(0) = +\infty$ and obtain an additive valuation $f \to w_\alpha(f)$ on H_K which extends uniquely to the quotient field M_K of H_K. This is called the *analytic valuation* belonging to α. We have $w_\alpha(f) \geqq 0$ if and only if f can be written in the form

$$f(X) = \frac{g(X)}{h(X)}$$

with $g, h \in H_K$ and $h(\alpha) \neq 0$; if this is the case, we put $f(\alpha) = g(\alpha)/h(\alpha)$ and say that $f \in M_K$ is *finite* at α. Otherwise we put $f(\alpha) = \infty$ and say that f has a *pole* at α. The map $f \to f(\alpha)$ is a place belonging to the valuation w_α; and its residue class field is $K(\alpha)$. We have $w_\alpha = w_\beta$ if and only if α and β are conjugate over K.

If we associate, to every $0 \neq f \in M_K$, the collection of integers $w_\alpha(f)$, then we obtain the *divisor* of f. This is denoted, as usual, by (f). The numbers $w_\alpha(f)$ satisfy the following conditions:

(i) *Finiteness condition:* In every region $0 < r \leqq |\alpha| \leqq r'$ there are only finitely many α with $w_\alpha(f) \neq 0$.

(ii) *Rationality condition:* If α and β are conjugate over K then $w_\alpha(f) = w_\beta(f)$.

Every collection $\mathfrak{m} = \{m_\alpha\}$ $(\alpha \in \Omega^\times)$ of integers $m_\alpha \in \mathbf{Z}$ satisfying these conditions is called a *divisor*[2]). More precisely, these are the divisors *defined over* K because of the condition (ii). These divisors form an additive group, with addition defined componentwise, which is denoted by D_K. This group is partially ordered, the ordering defined componentwise. A divisor $\mathfrak{m} \geqq 0$ is called *integral*.

To every divisor $\mathfrak{m} \in D_K$ there exists a function $0 \neq f \in M_K$ such that $\mathfrak{m} = (f)$. In fact, such a function is given by the Weierstraß product

$$f(X) = \prod_{|\alpha| \leqq 1} (1 - \alpha X^{-1})^{e_\alpha m_\alpha} \prod_{|\alpha| > 1} (1 - \alpha^{-1} X)^{e_\alpha m_\alpha} \tag{2}$$

---

[1]) See e. g. Bourbaki [2], p. 84. For the proofs of general statements about holomorphic functions in the non-archimedean case, see also Güntzer [8].

[2]) m_α is called the "multiplicity" of the divisor $\mathfrak{m}$ at α.

where e_α denotes the degree of inseparability of α over K. The rationality condition (ii) for divisors implies that this function is defined over K; for a given α the partial product taken over the conjugates of α is equal to

$$(X^{-n_\alpha}\varphi_\alpha(X))^{m_\alpha} \quad \text{if} \quad |\alpha| \leqq 1$$

$$(a_0^{-1}\varphi_\alpha(X))^{m_\alpha} \quad \text{if} \quad |\alpha| > 1$$

where $n_\alpha = [K(\alpha):K]$ and $a_0 = N_{K(\alpha)|K}(\alpha)$. The normalizing factors X^{-n_α} and a_0^{-1} render the product (2) convergent; this product is to be understood as the quotient of the partial product taken over those α with $m_\alpha > 0$, by the corresponding product over the α with $m_\alpha < 0$. It is clear by construction that the product function (2) has the divisor $\mathfrak{m}$.

Every function $0 \neq f \in M_K$ is determined by its divisor (f) up to a function of the form cX^d with $c \in K^\times$ and $d \in \mathbf{Z}$; the latter functions are the units of H_K and can be characterized as those meromorphic functions which have no zero and no pole in $\Omega^\times$[1].

If $0 \neq f$ is q-periodic then its divisor (f) is q-periodic too. Here, a divisor $\mathfrak{m} = \{m_\alpha\}$ is called q-periodic if $m_{q\alpha} = m_\alpha$ for every $\alpha \in \Omega^\times$. These q-periodic divisors form a subgroup of D_K which is denoted by $D_K(q)$.

In order to construct q-periodic functions one has to answer the following question: Given a q-periodic divisor $\mathfrak{m}$, under what condition does there exist a q-periodic function admitting this divisor?

Let $f(X)$ be a meromorphic function such that $(f) = \mathfrak{m}$. Since $\mathfrak{m}$ is q-periodic, the function $f(q^{-1}X)$ likewise has the divisor $\mathfrak{m}$. Hence

$$f(q^{-1}X) = a^{-1}(-X)^d f(X) \tag{3}$$

with some integer $d \in \mathbf{Z}$ and some $a \in K^\times$. Functions which satisfy a functional equation of this form are called *theta functions* with respect to q. The exponent d is called the *degree* of f and a is called the *multiplicator* of f.

If $g(X)$ is another function with $(g) = \mathfrak{m}$ then

$$g(X) = cX^k f(X) \tag{4}$$

[1]) See e. g. [8]. The validity of this statement relies on the nonarchimedean property of the valuation of K. If K is the real or complex field, then there are other units in H_K, namely those which are exponentials of holomorphic functions.

with $c \in K^\times$ and $k \in \mathbf{Z}$. Using (3) we see that $g(X)$ satisfies the functional equation

$$g(q^{-1}X) = (aq^k)^{-1}(-X)^d g(X).$$

That is, g is a theta function having the same degree as f, and the multiplicator of g differs from the multiplicator of f by a q-power only. Hence d is uniquely determined by the divisor $\mathfrak{m}$; we shall call d the *degree* of $\mathfrak{m}$ and write

$$d = \deg_q(\mathfrak{m}).$$

The multiplicator a of f is determined by $\mathfrak{m}$ modulo q only; its residue class in the multiplicative factor group $K^\times/q$ is denoted by $\Phi_q(\mathfrak{m})$; so that we can write[1])

$$a \equiv \Phi_q(\mathfrak{m}) \bmod^\times q.$$

We shall call $\Phi_q(\mathfrak{m})$ the *Jacobi image* of the q-periodic divisor $\mathfrak{m}$. Obviously, the map $\Phi_q\colon D_K(q) \to K^\times/q$ thus defined is a homomorphism.

If f is a q-periodic function with $(f) = \mathfrak{m}$ then $a = 1$, $d = 0$ in the functional equation (3); we have therefore

$$\deg_q(\mathfrak{m}) = 0, \quad \Phi_q(\mathfrak{m}) \equiv 1 \bmod^\times q. \tag{5}$$

Conversely, if these conditions are satisfied then for any function $f \in M_K$ with $(f) = \mathfrak{m}$ we have $d = 0$, $a = q^{-k}$ for some $k \in \mathbf{Z}$. The function

$$g(X) = cX^k f(X),$$

defined with this k and an arbitrary factor $c \in K^\times$ is then q-periodic; it is immediate that g is uniquely determined, up to a factor in $K^\times$, as q-periodic function with the divisor $\mathfrak{m}$.

It follows that the conditions (5) are necessary and sufficient for $\mathfrak{m}$ to be the divisor of a q-periodic function. It remains to give an explicit formula for computing the degree and the Jacobi image of a q-periodic divisor $\mathfrak{m}$. This is done by explicitely constructing a theta function for $\mathfrak{m}$.

[1]) Notation: If $a, b \in K^\times$ we write $a \equiv b \bmod^\times q$ if $b = aq^k$ with some $k \in \mathbf{Z}$, i. e. if a and b determine the same element in the multiplicative factor group $K^\times/q$. A similar notation will be used for elements in an extension field L of K; note that $L^\times/q$ contains $K^\times/q$ as a subgroup.

We start with the "fundamental theta function"

(6) $$\Theta(X) = \prod_{n \geqq 0} (1 - q^n X^{-1}) \prod_{n<0} (1 - q^{-n} X).$$

This function is holomorphic, its zeros being the elements $\equiv 1 \bmod^\times q$ with multiplicity 1. Its divisor is therefore q-periodic. By inspection, one verifies that it satisfies the functional equation

(7) $$\Theta(q^{-1}X) = -X\Theta(X).$$

That is, the degree of Θ is 1 and its multiplicator is 1.

For every $\alpha \in \Omega^\times$ we put

(8) $$\Theta_\alpha(X) = \Theta(\alpha^{-1}X).$$

Θ_α is a holomorphic function defined over $K(\alpha)$. Its zeros are the elements $\equiv \alpha \bmod^\times q$ with multiplicity 1; its divisor is therefore q-periodic. From (7) we infer that Θ_α satisfies the functional equation

(9) $$\Theta_\alpha(q^{-1}X) = \alpha^{-1}(-X)\,\Theta_\alpha(X);$$

the degree of Θ_α is 1 and its multiplicator is α.

Now let $\mathfrak{m} = \{m_\alpha\}$ be a q-periodic divisor. We put

(10) $$\Theta_{\mathfrak{m}} = \prod_{|q|<|\alpha|\leqq 1} \Theta_\alpha^{e_\alpha m_\alpha}\,[1].$$

By the finiteness condition (i) for divisors, this is a finite product. By the rationality condition (ii), $\Theta_{\mathfrak{m}}$ is defined over K, i.e. $\Theta_{\mathfrak{m}} \in M_K$. By construction, $w_\alpha(\Theta_{\mathfrak{m}}) = m_\alpha$, i.e. the divisor of $\Theta_{\mathfrak{m}}$ is $\mathfrak{m}$. From (9) we infer that $\Theta_{\mathfrak{m}}$ satisfies the functional equation

$$\Theta_{\mathfrak{m}}(q^{-1}X) = a^{-1}(-X)^d\,\Theta_{\mathfrak{m}}(X)$$

where

(11) $$d = \sum_{|q|<|\alpha|\leqq 1} e_\alpha m_\alpha = \deg_q(\mathfrak{m})$$

$$a = \prod_{|q|<|\alpha|\leqq 1} \alpha^{e_\alpha m_\alpha} \equiv \Phi_q(\mathfrak{m}) \bmod^\times q.$$

From the rationality condition of divisors it is clear that we can write these formulas in the form

(12) $$\deg_q(\mathfrak{m}) = \sum_{|q|<|\alpha|\leqq 1}' [K(\alpha):K]\, m_\alpha$$

$$\Phi_q(\mathfrak{m}) \equiv \prod_{|q|<|\alpha|\leqq 1}' N_{K(\alpha)|K}(\alpha)^{m_\alpha} \bmod^\times q\,[2]$$

[1]) As above, e_α denotes the degree of inseparability of α over K.
[2]) If $L|K$ is a finite algebraic field extension then $N_{L|K}: L \to K$ denotes the norm map from L to K.

where the prime indicates that α ranges over a system of representatives of K-conjugacy classes; note that K-conjugate elements have the same absolute value.

The formulas (12) give an explicit expression of the degree and the Jacobi image of the q-periodic divisor $\mathfrak{m}$. We have proved:

Proposition 1 (Abel-Jacobi theorem): *A q-periodic divisor $\mathfrak{m}$ is the divisor of a q-periodic function f if and only if it satisfies the condition*

$$\deg_q(\mathfrak{m}) = 0, \quad \Phi_q(\mathfrak{m}) \equiv 1 \bmod^\times q$$

where the degree $\deg_q(\mathfrak{m})$ and the Jacobi image $\Phi_q(\mathfrak{m})$ are given by the formulas (12). If this is so, then f is uniquely determined by $\mathfrak{m}$, up to a factor in $K^\times$.

Now it is easy to construct q-periodic functions, namely by constructing q-periodic divisors satisfying the requirements of proposition 1. As an example let us prove:

Corollary: *For every $\alpha \in \Omega^\times$ there exists a q-periodic function f such that $w_\alpha(f) = 1$. If β is not K-conjugate to α (mod$^\times$ q) then f can be chosen such that $w_\beta(f) = 0$.*

Proof. Let $\mathfrak{p}_\alpha$ denote the divisor which has multiplicity 1 at α and at all elements in $\Omega^\times$ which are K-conjugate to α (mod$^\times$ q), and multiplicity 0 elsewhere. Then $\mathfrak{p}_\alpha$ is q-periodic and

$$\deg_q(\mathfrak{p}_\alpha) = [K(\alpha):K], \quad \Phi_q(\mathfrak{p}_\alpha) \equiv N_{K(\alpha)|K}(\alpha) \bmod^\times q.$$

Two cases have to be distinguished:

Case 1: $\alpha \in K^\times$. Then we choose elements $u, v \in K^\times$ such that the elements $\alpha, uv, \alpha u, v$ are all different mod$^\times$ q. The divisor

$$\mathfrak{m} = \mathfrak{p}_\alpha + \mathfrak{p}_{uv} - \mathfrak{p}_{\alpha u} - \mathfrak{p}_v$$

has degree 0 and $\Phi_q(\mathfrak{m}) \equiv \frac{\alpha u v}{\alpha u v} \equiv 1 \bmod^\times q$; hence $\mathfrak{m} = (f)$ with a q-periodic function f. By construction, $\mathfrak{m}$ has multiplicity 1 at α, i.e. $w_\alpha(f) = 1$. We may choose u, v such that $uv, \alpha u, v$ are different also from $\beta \bmod^\times q$, then $\mathfrak{m}$ has multiplicity 0 at β and hence $w_\beta(f) = 0$.

Case 2: $\alpha \notin K^\times$. Let $d = [K(\alpha):K]$ and $a = N_{K(\alpha)|K}(\alpha)$. Let $u \in K^\times$, and put $v = u^{1-d}a$. The divisor

$$\mathfrak{m} = \mathfrak{p}_\alpha - (d-1)\,\mathfrak{p}_u - \mathfrak{p}_v$$

has degree 0 and $\Phi_q(\mathfrak{m}) \equiv \frac{a}{u^{d-1}v} \equiv 1 \bmod^\times q$; hence $\mathfrak{m} = (f)$ with a q-periodic function f. By construction, $\mathfrak{m}$ has multiplicity 1 at α, i.e. $w_\alpha(f) = 1$. We may choose u such that $u, v \not\equiv \beta \bmod^\times q$; then $\mathfrak{m}$ has multiplicity 0 at β and hence $w_\beta(f) = 0$.

QED.

It is now important to answer the Riemann-Roch question: Given a q-periodic divisor $\mathfrak{m}$, what is the K-dimension of the vector space $L_K(q\,|\,\mathfrak{m})$ of q-periodic functions f such that $(f) \geqq -\mathfrak{m}$?

If $\deg_q(\mathfrak{m}) < 0$ then proposition 1 shows that $L_K(q\,|\,\mathfrak{m}) = 0$. If $\deg_q(\mathfrak{m}) = 0$ then, from the same source, we conclude that $L_K(q\,|\,\mathfrak{m}) = 0$ except if $\Phi_q(\mathfrak{m}) \equiv 1 \bmod^\times q$ in which case $\dim L_K(q\,|\,m) = 1$.

Proposition 2 (Riemann-Roch theorem): *If $\mathfrak{m}$ is a q-periodic divisor and* $\deg_q(\mathfrak{m}) > 0$ *then*

$$\dim L_K(q\,|\,\mathfrak{m}) = \deg_q(\mathfrak{m}).$$

Proof.

We supplement the assertion to the effect that it holds also if $\deg_q(\mathfrak{m}) = 0$ provided $\Phi_q(\mathfrak{m}) \not\equiv 1 \bmod^\times q$. This statement being proved by proposition 1, we may assume $d = \deg_q(\mathfrak{m}) > 0$ and use induction. Let $a \in K^\times$ such that $a \equiv \Phi_q(\mathfrak{m}) \bmod^\times q$. We choose an element $b \in K^\times$ such that $\mathfrak{m}$ has multiplicity 0 at b and that $b \not\equiv 1$, $a \bmod^\times q$. The divisor

$$\mathfrak{m}' = \mathfrak{m} - \mathfrak{p}_b$$

has degree $d - 1$ and $\Phi_q(\mathfrak{m}') \equiv \frac{a}{b} \not\equiv 1 \bmod^\times q$. By induction $L_K(q\,|\,\mathfrak{m}')$ has dimension $d - 1$. On the other hand, $L_K(q\,|\,\mathfrak{m}')$ consists of all functions in $L_K(q\,|\,\mathfrak{m})$ which have the value 0 at b, i.e. it is the kernel in $L_K(q\,|\,\mathfrak{m})$ of the map $f \to f(b)$. Hence it remains to show that there exists $f \in L_K(q\,|\,\mathfrak{m})$ with $f(b) \neq 0$. If we write

$$(f) = \mathfrak{z} - \mathfrak{m}$$

then $\mathfrak{z} \geqq 0$ and $\mathfrak{z}$ has multiplicity 0 at b. By proposition 1, we have therefore to show the existence of a q-periodic divisor $\mathfrak{z} \geqq 0$, having the multiplicity 0 at b, such that

$$\deg_q(\mathfrak{z}) = d, \quad \Phi_q(\mathfrak{z}) \equiv a \bmod^\times q.$$

Such a divisor is given by

$$\mathfrak{z} = \mathfrak{p}_a + (d - 1)\,\mathfrak{p}_1$$

in view of the fact that $b \not\equiv 1$, $a \bmod^\times q$.

QED.

Now let us review the situation: We have seen that the field $F_K(q)$ carries certain valuations w_α over K, and that the following statements are true:

1. We have $w_\alpha = w_\beta$ (on $F_K(q)$) if and only if α and β are K-conjugate $\bmod^\times q$.

(This, and the next statement, follows from the corollary to proposition 1.)

2. The value group of w_α (on $F_K(q)$) is **Z**.

3. The residue class field of w_α (on $F_K(q)$) is contained in $K(\alpha)$. In particular, it is a finite algebraic extension of K.

(In fact, the residue class field of w_α (on M_K) is $K(\alpha)$, the corresponding place being $f \to f(\alpha)$.)

4. If $w_\alpha(f) = 0$ for all α then $f \in K$. (From proposition 1, applied to the zero divisor.)

5. For every $f \neq 0$ in $F_K(q)$ there exists only a finite number of the valuations w_α (on $F_K(q)$) such that $w_\alpha(f) \neq 0$. We have the sum formula:

$$\sum_\alpha{}' [K(\alpha) : K] \cdot w_\alpha(f) = 0, \tag{13}$$

the sum being extended over a system of representatives of the classes of K-conjugate elements α in $\Omega^\times \bmod^\times q$.

(This statement is equivalent to saying that the degree of the q-periodic divisor (f) is zero; see proposition 1.)

Statements 1.—5. show that we have precisely the situation of the well known theorem of Artin-Whaples [1] which characterizes fields with those properties as function fields (in the algebraic sense) over K. Applying this theorem, we conclude:

I. *The field $F_K(q)$ is a function field over K in the sense that it is finitely generated of degree of transcendency 1 over K, and K is algebraically closed in $F_K(q)$.*

II. *Every valuation of $F_K(q)$ over K is equivalent to w_α for some suitable α. Thus the prime divisors $\mathfrak{p}$ of $F_K(q)\,|\,K$ (in the algebraic sense) correspond 1—1 to the classes of K-conjugate elements in $\Omega^\times$* mod $q^\times$. *If $\mathfrak{p}$ belongs to α in this correspondence, then w_α is the normalized*[1]) *valuation of $F_K(q)$ belonging to $\mathfrak{p}$.*

1) An additive valuation of a field is said to be normalized if its value group is **Z**.

Moreover, the Artin-Whaples theorem tells us in view of (13) that there exists a constant ϱ, independent of $\mathfrak{p}$, such that

$$\varrho \cdot \deg(\mathfrak{p}) = [K(\alpha) : K];$$

here $\deg(\mathfrak{p})$ denotes the degree of $\mathfrak{p}$ in the algebraic sense. On the other hand, we know from 3. that the residue class field of $\mathfrak{p}$ is contained in $K(\alpha)$ and hence $\deg(\mathfrak{p})$ divides $[K(\alpha) : K]$; thus ϱ is a positive integer. Taking $\alpha = 1$ we have $K(1) = K$ and conclude $\varrho = 1$. Hence:

III. *If $\mathfrak{p}$ belongs to α in the correspondence described in* II, *then the residue class field of $\mathfrak{p}$ is K-isomorphic to $K(\alpha)$. In particular, the degree of $\mathfrak{p}$ (in the algebraic sense) equals $[K(\alpha) : K]$.*

Statement II shows that the prime divisors of $F_K(q)$ in the algebraic sense correspond $1 - 1$ to the q-periodic divisors $\mathfrak{p}_\alpha$ which we have defined above analytically. Henceforth we shall identify $\mathfrak{p}_\alpha$ with the corresponding prime divisors of $F_K(q)$; then the group $D_K(q)$ of q-periodic divisors is identified with the divisor group of $F_K(q)$ in the algebraic sense. Thus, we do not have to distinguish between analytic and algebraic divisors. From III it follows that in this identification, the degree (in the algebraic sense) of a divisor coincides with its degree in the analytic sense which we have defined above and denoted by $\deg_q$.

The K-vector spaces $L_K(q \mid \mathfrak{m})$ as studied in proposition 2 and defined there analytically, now coincide with the corresponding spaces defined in the algebraic theory in connection with the Riemann-Roch theorem.

The genus g of $F_K(q) \mid K$ is algebraically defined by the property that

$$\dim L_K(q \mid \mathfrak{m}) = \deg(\mathfrak{m}) - g + 1$$

if $\deg(\mathfrak{m})$ is sufficiently large. From proposition 2 we conclude therefore that $g = 1$.

In order to show that $F_K(q)$ is elliptic we have still to show that $F_K(q)$ is conservative. Let L be a finite algebraic extension of K. Then L is local too and we may form $F_L(q)$, the field of q-periodic functions defined over L. This has genus 1 by what we have shown. On the other hand, if $u_1, \ldots, u_n$ is a basis of $L \mid K$ then it is also a basis of H_L over H_K and therefore of $M_L \mid M_K$. That is, every meromorphic

function $f \in M_L$ is uniquely representable in the form

$$f = \sum_{1 \leq i \leq n} f_i u_i$$

with $f_i \in M_K$. We conclude: $f(q^{-1}X) = f(X)$ if and only if $f_i(q^{-1}X) = f_i(X)$. Therefore, $u_1, \ldots, u_n$ is a basis of $F_L(q)$ over $F_K(q)$, i. e. $F_L(q) = F_K(q) \cdot L$ is the constant extension of $F_K(q)$ by L. We have shown that the genus of $F_K(q)$ is preserved under arbitrary finite algebraic constant field extensions. Hence $F_K(q)$ is conservative. Thus:

IV. *$F_K(q)$ is an elliptic function field over K. For every finite algebraic extension field L of K, we have $F_L(q) = F_K(q) \cdot L$.*

Let $D_K^0(q)$ denote the subgroup of $D_K(q)$, consisting of the divisors of degree 0. By proposition 1, $D_K^0(q)$ contains the group $P_K(q)$ of principal divisors, i. e. divisors of q-periodic functions. Let us denote by

$$C_K^0(q) = D_K^0(q)/P_K(q)$$

the group of divisor classes of degree 0. By proposition 1, the Jacobi map $\Phi_q : D_K(q) \to K^\times/q$ induces a monomorphism $C_K^0(q) \to K^\times/q$. This is in fact an *isomorphism*. For, if $a \in K^\times$ then $\Phi_q(\mathfrak{p}_a - \mathfrak{p}_1) \equiv a \bmod^\times q$ and $\deg_q(\mathfrak{p}_a - \mathfrak{p}_1) = 0$. Hence the Abel-Jacobi theorem can be restated as follows:

V. *The Jacobi map $\Phi_q : D_K(q) \to K^\times/q$ induces an isomorphism $C_K^0(q) \approx K^\times/q$.*

Thus we have obtained an explicit description of the group $C_K^0(q)$ of divisor classes of degree 0 of $F_K(q)$. This group can be regarded as the group of K-rational points of the Jacobian variety (in the algebraic sense) of $F_K(q)$. As such, it carries naturally the structure of a Lie group over K (see Igusa [11]). It is easily verified that the map $\Phi_q : C_K^0(q) \to K^\times/q$ is an isomorphism of Lie groups, $K^\times/q$ carrying naturally the structure of a 1-dimensional Lie group. This fact, which can be proved independently of proposition 2, shows that the Jacobian variety of $F_K(q)$ has dimension 1 and thus gives another proof of the fact that $F_K(q)$ has genus 1.

There is a corollary of statement V. concerning translation automorphisms, which is worthwhile mentioning. For any $a \in K^\times$, let τ_a denote the automorphism of M_K which is defined by

$$\tau_a : f(X) \to f(a^{-1}X).$$

This is called the *translation automorphism* belonging to a. The q-periodic functions $f \in F_K(q)$ can be described by the property

$$\tau_a f = f.$$

Every translation automorphism τ_a induces in $F_K(q)$ a certain automorphism which is likewise denoted by τ_a. Obviously, if $a \equiv b \bmod^\times q$ then $\tau_a = \tau_b$ on $F_K(q)$. Conversely, if $a \not\equiv b \bmod^\times q$ then (from II.) there exists a q-periodic function f such that $f(a) \neq f(b)$; we have $(\tau_a f)(ab) = f(a^{-1}ab) = f(b) \neq f(a) = f(b^{-1}ab) = (\tau_b f)(ab)$ and hence $\tau_a f \neq \tau_b f$, $\tau_a \neq \tau_b$. We see therefore that $a \to \tau_a$ defines a *monomorphism* of $K^\times/q$ into the group of automorphisms of $F_K(q) \mid K$, its image is called the *translation group* of $F_K(q)$ and is denoted by $T_K(q)$.

Every automorphism τ of $F_K(q)$ acts on the prime divisors $\mathfrak{p}$ of degree 1 of $F_K(q)$ via the formula

$$(\tau f)(\tau \mathfrak{p}) = f(\mathfrak{p}) \qquad (f \in F_K(q));$$

if $\mathfrak{p} = \mathfrak{p}_b$ and $\tau\mathfrak{p} = \mathfrak{p}_{b'}$ then this formula reads

$$(\tau f)(b') = f(b).$$

Now, if $\tau = \tau_a$ then $(\tau_a f)(b') = f(a^{-1}b')$ and we conclude

$$f(a^{-1}b') = f(b).$$

Since f is arbitrary, it follows

$$b' \equiv ab \bmod^\times q$$

which is to say that

$$\tau_a(\mathfrak{p}_b) = \mathfrak{p}_{ab}. \tag{14}$$

This formula describes the action of τ_a on the prime divisors of degree 1 of $F_K(q)$. Since there are infinitely many prime divisors of degree 1, it follows that τ_a is *uniquely determined*, as an automorphism of $F_K(q) \mid K$, by the property (14).

Now, the divisor $\tau_a(\mathfrak{p}_b) - \mathfrak{p}_b = \mathfrak{p}_{ab} - \mathfrak{p}_b$ is of degree 0, and we have

$$\Phi_q(\mathfrak{p}_{ab} - \mathfrak{p}_b) \equiv \frac{ab}{b} \equiv a \bmod^\times q.$$

From V we conclude that the class c_a of $\mathfrak{p}_{ab} - \mathfrak{p}_b$ does not depend on b, and that it is uniquely determined by the property $\Phi_q(c_a) \equiv a \bmod^\times q$. We obtain the

Corollary Va. *Let $a \in K^\times$ and let $\tau_a : f(X) \to f(a^{-1}X)$ be the corresponding translation automorphism of $F_K(q)$. The action of τ_a on the prime divisors $\mathfrak{p}$ of degree 1 of $F_K(q)$ is given by the formula*

$$\tau_a(\mathfrak{p}) \sim \mathfrak{p} + c_a$$

where $c_a \in C_K^0(q)$ is the divisor class which corresponds to a under the Jacobi isomorphism $\Phi_q : C_K^0(q) \to K^\times/q$.

Here, the symbol $\sim$ means divisor equivalence (modulo principal divisors). Note that, by the Riemann-Roch theorem, two equivalent prime divisors of degree 1 are equal. Hence the formula of corollary Va indeed determines the action of τ_a on the primes of degree 1.

There is an *algebraic* notion of translation automorphism τ_c corresponding to a class $c \in C_K^0(q)$; this is the automorphism of $F_K(q)$ which is determined by the formula

$$\tau_c(\mathfrak{p}) \sim \mathfrak{p} + c$$

for every prime divisor $\mathfrak{p}$ of degree 1 of $F_K(q)$. If $c = c_a$ then corollary Va shows that $\tau_c = \tau_a$. Hence:

Corollary Vb. *The translation automorphisms (in the analytic sense) of $F_K(q)$ coincide with the translation automorphisms in the algebraic sense. If $\Phi_q(c) \equiv a \bmod^\times q$ then $\tau_c = \tau_a$.*

Thus we do not have to distinguish between the analytic and the algebraic translation automorphisms.

Additional remarks

1. *Extension of the field of constants:* Let $L \mid K$ be a finite algebraic extension. Any element $\alpha \in \Omega^\times$ defines not only a valuation w_α in M_K and $F_K(q)$, but similarly a valuation in M_L and $F_L(q)$; in order to distinguish these two valuations, we shall employ the notation $w_{\alpha,K}$ and $w_{\alpha,L}$. The irreducible polynomials of α over K and over L will now be denoted by $\varphi_{\alpha,K}(X)$ and $\varphi_{\alpha,L}(X)$. Let

$$\varphi_{\alpha,K}(X) = \prod_{1 \leq i \leq r_\alpha} \varphi_{\alpha_i,L}(X)^{e_i(\alpha)} \tag{15}$$

be the prime decomposition of $\varphi_{\alpha,K}(X)$ over L; the α_i range over a full system of representatives of the L-conjugacy classes into which the K-conjugacy class of α splits.

The exponent $e_i(\alpha)$ is the quotient of the degree of inseparability of α over K, by the degree of inseparability of α_i over L. It is immediate from our definitions that the valuations $w_{\alpha_i, L}$ of M_L are precisely those valuations which induce in M_K a valuation equivalent to $w_{\alpha, K}$; the corresponding ramification index is $e_i(\alpha)$. We have a natural imbedding

$$D_K \subset D_L$$

which identifies every divisor $\mathfrak{m} = \{m_\alpha\}$ of D_K with the divisor $\mathfrak{m}' = \{m'_\alpha\}$ of D_L defined by

$$m'_{\alpha_i} = e_i(\alpha) m_\alpha \qquad (1 \leqq i \leqq r_\alpha).$$

If $\mathfrak{m} \in D_K$ is q-periodic then it is also q-periodic if regarded as a divisor of D_L, i. e. we have

$$D_K(q) \subset D_L(q).$$

By definition, this imbedding is given by the formula

$$\mathfrak{p}_{\alpha, K} = \sum_{1 \leqq i \leqq r_\alpha} e_i(\alpha) \mathfrak{p}_{\alpha_i, L}$$

where we have again employed the subscript K resp. L (in addition to our previous notation) to indicate the ground field which we are referring to. In this formula, the $\mathfrak{p}_{\alpha_i, L}$ are precisely the prime divisors of $F_L(q)$ which extend $\mathfrak{p}_{\alpha, K}$, and $e_i(\alpha)$ is the corresponding ramification index. That is, our imbedding $D_K(q) \subset D_L(q)$, which is defined analytically, coincides with the usual imbedding given by the algebraic theory of function fields.

It is immediate from the definition that the degree of a q-periodic divisor is preserved by this imbedding; hence we are entitled to use the notation $\deg_q$ without reference to any ground field. A similar remark applies to Φ_q.

If $L \mid K$ is separable then $e_i(\alpha) = 1$ for every α, which is to say that $F_L(q)$ is *unramified* over $F_K(q)$.

2. *Galois constant field extensions:* Assume, in addition, that $L \mid K$ is a Galois extension and let G denote its Galois group. G acts on the holomorphic functions in H_L, namely on their coefficients; therefore G acts also on M_L, and M_K is the field of fixed elements of G in M_L. That is, G becomes the Galois group of $M_L \mid M_K$. We have

$$(\sigma f)(\sigma a) = \sigma(f(a)) \qquad (\sigma \in G,\ f \in M_L,\ a \in L^\times).$$

This relation remains true if we replace a by an arbitrary element $\alpha \in \Omega^\times$ provided we extend σ to an automorphism of $\Omega \mid K$ so that $\sigma\alpha$ and $\sigma(f(\alpha))$ are defined.

G also acts naturally on the divisors in D_L such that

$$(\sigma f) = \sigma(f) \qquad (\sigma \in G,\ f \in M_L^\times).$$

The group of fixed elements of G in D_L coincides with D_K.

The q-periodic functions and q-periodic divisors are transformed by G into themselves. It is then evident from (3) that

$$\left.\begin{aligned} \deg_q(\sigma\mathfrak{m}) &= \deg_q(\mathfrak{m}) \\ \Phi_q(\sigma\mathfrak{m}) &\equiv \sigma\Phi_q(\mathfrak{m}) \bmod^\times q \end{aligned}\right. \qquad (\sigma \in G,\ \mathfrak{m} \in D_L^s(q)).$$

That is, the maps

$$\deg_q : D_L(q) \to \mathbf{Z}$$
$$\Phi_q : D_L(q) \to L^\times/q$$

are G-permissible, G acting trivially on $\mathbf{Z}$ and naturally on $L^\times/q$.

It follows that *the Jacobi isomorphism $\Phi_q : C_L^0(q) \to L^\times/q$ is an isomorphism of G-modules.*

3. *Infinite constant field extensions:* For *every* algebraic field extension L of K, finite or infinite, we denote by $F_L(q)$ the union of the fields $F_{L'}(q)$, where L' ranges over the finite subextensions of L. Similarly, $D_L(q)$, $C_L^0(q)$ etc. are defined. The statements I—V and those of remarks 1. and 2. remain true also in this case. Note, however, that L is not complete in the infinite case so that $F_L(q)$ is *not* defined independently without referring to the complete field K over which L is algebraic.

§ 3. The absolute and the Hasse invariant of the fields of periodic functions

Note that $F_K(q)$ has a prime divisor of degree 1, for instance $\mathfrak{p}_1$ in the notation of § 2. Hence $F_K(q)$ can be generated over K by two elements whose defining relation over K is a cubic (see § A 1 of the appendix). We are now going to exhibit explicitely two such functions and compute the coefficients of their defining relation over K.

Let D denote the differential operator of M_K defined by

$$D = X\frac{d}{dX}.$$

Note that D commutes with the translation $f(X) \to f(q^{-1}X)$; in particular, the derivative of a q-periodic function is again q-periodic. As usual, we write $D \log f$ for $\frac{Df}{f}$.

If we define

$$\zeta(X) = D \log \Theta(X)$$

then $\zeta(X)$ satisfies the functional equation

$$\zeta(q^{-1}X) = \zeta(X) + 1$$

as follows from formula (7), § 2. Hence the function

$$\wp(X) = -D\zeta(X)$$

satisfies

$$\wp(q^{-1}X) = \wp(X),$$

i. e. $\wp$ is q-periodic.

From formula (6) in § 2 we see that Θ has its zeros at the points q^n $(n \in Z)$ and that these zeros are of order 1. Hence, ζ has its poles at these points, which are of order 1, and $\wp$ likewise has these points as its poles, but of order 2. That is, the pole divisor of $\wp$ is $2\mathfrak{p}_1$, with the notation of § 2.

From (6) we obtain by differentiation the expansion

$$\wp(X) = \sum_{n \in Z} \frac{q^n X}{(1 - q^n X)^2}. \tag{16}$$

Classically, a second q-periodic function with $3\mathfrak{p}_1$ as its pole divisor is obtained as the derivative $D\wp$; we have from (16)

$$D\wp(X) = \sum_{n \in Z} \frac{q^n X + q^{2n} X^2}{(1 - q^n X)^3}. \tag{17}$$

However, in characteristic 2, the derivative of a function with a pole of order 2 does not have a pole of order 3; in fact we see from (17) that $D\wp = \wp$ if char $(K) = 2$. (The latter statement can be explained by the fact that $\wp = -D\zeta$ is itself the derivative of a meromorphic function, and that in characteristic 2 the operator D is idempotent, due to the fact $D^2(X^n) = n^2 X^n = n X^n = D(X^n)$ since $n^2 \equiv n \bmod 2$.) In any case, we see that $D\wp - \wp$ is formally divisible by 2; hence the function

$$\wp' = \tfrac{1}{2}(D\wp - \wp) \tag{18}$$

is defined for every characteristic; in view of (16) and (17) we have

$$\wp'(X) = \sum_{n \in Z} \frac{q^{2n} X^2}{(1 - q^n X)^3}. \tag{19}$$

From this we see that $\wp'$ has the pole divisor $3\mathfrak{p}_1$. Also, the fact that $\wp'$ is q-periodic is evident from (19).

We have now

$$F_K(q) = K(\wp, \wp')$$

and it remains to determine the defining relation of $\wp, \wp'$ over K.

The *reflection* $f(X) \to f(X^{-1})$ is an automorphism of M_K. It induces in $F_K(q)$ a certain K-automorphism which is denoted by ε. The latter is non-trivial since it acts on the prime divisors $\mathfrak{p}_\alpha$ by means of the rule

$$\varepsilon(\mathfrak{p}_\alpha) = \mathfrak{p}_{\alpha^{-1}}$$

From (16) it is clear that $\varepsilon\wp = \wp$, hence ε is the non-trivial automorphism of the quadratic extension $F_K(q)$ of $K(\wp)$. We conclude that every q-periodic function which is „*even*“ (i. e. which is stable under ε) is contained in $K(\wp)$.

Since D anticommutes with ε, we have

$$\varepsilon(D\wp) = -D\wp, \tag{20}$$

i. e. $D\wp$ is an odd function. From (18),

$$\varepsilon(\wp') = -\wp' - \wp, \tag{21}$$

which can also be verified from (19). It follows that

$$\wp'^2 + \wp\wp' = -\wp' \cdot \varepsilon(\wp') \tag{22}$$

is an even function, hence contained in $K(\wp)$. Since this is a function with no pole except $\mathfrak{p}_1$, it can be written as a *polynomial* in $\wp$ with coefficients in K. The degree of that polynomial is 3 since the function (22) has a pole of order 6 at $\mathfrak{p}_1$. The highest coefficient of that polynomial is 1 since the function

$$\wp'^2 + \wp\wp' - \wp^3 \tag{23}$$

has a pole of order < 6 at $\mathfrak{p}_1$, as follows immediately from (16) and (19); hence the function (23) can be written as a polynomial of degree < 3 in $\wp$.

We conclude:

$$\wp'^2 + \wp\wp' = \wp^3 + A\wp^2 + B\wp + C \tag{24}$$

with $A, B, C \in K$.

It remains to determine the coefficients A, B, C. Let $\mathfrak{P}_1^m$ denote the module of functions $f \in M_K$ with $w_1(f) \geqq m$. We have from (16):

$$\wp(X) \equiv \frac{X}{(1-X)^2} + 2s_1 \mod \mathfrak{P}_1^1 \tag{25}$$

where

$$s_1 = \sum_{n>0} \frac{nq^n}{1-q^n}. \tag{26}$$

Also, from (19):

$$\wp'(X) \equiv \frac{X^2}{(1-X)^3} \mod \mathfrak{P}_1^0. \tag{27}$$

The congruences (25), (27) suffice to determine the functions occurring in (24) modulo $\mathfrak{P}_1^{-3}$. We obtain

$$\frac{X^4}{(1-X)^6} + \frac{X^3}{(1-X)^5} \equiv \frac{X^3}{(1-X)^6} + 3\frac{2s_1X^2}{(1-X)^4} + A\frac{X^2}{(1-X)^4} \mod \mathfrak{P}_1^{-3}$$

which gives:

$$A = -6s_1. \tag{28}$$

At this point it seems advisable to normalize the functions $\wp, \wp'$ by adding suitable constants such that the normalized functions satisfy an equation of the same type (24), but with the coefficient of the quadratic term on the right hand side vanishing. It is immediately verified from (28) that this can be achieved by considering the functions $\wp - 2s_1$, $\wp' + s_1$ instead of $\wp, \wp'$; this is a universal procedure for every characteristic although of course in characteristic 2 or 3 we could well keep our original $\wp, \wp'$ in view of (28).

Rather then introduce new notations, we prefer to change notation and thus give a

New definition of the functions $\wp$ and $\wp'$:

$$\wp(X) = \sum_{n\in Z} \frac{q^nX}{(1-q^nX)^2} - 2s_1, \qquad \wp'(X) = \sum_{n\in Z} \frac{q^{2n}X^2}{(1-q^nX)^3} + s_1. \tag{29}$$

Henceforth, the symbols $\wp, \wp'$ will be used according to this new definition. The reader should observe that the formulas (18), (21), remain valid also for the new functions $\wp, \wp'$. As to (25), this is to be replaced by

$$\wp(X) \equiv \frac{X}{(1-X)^2} \mod \mathfrak{P}_1^1;$$

since $\wp(X^{-1}) = \wp(X)$ it follows easily that this congruence is valid modulo $\mathfrak{P}_1^2$:

$$\wp(X) \equiv \frac{X}{(1-X)^2} \mod \mathfrak{P}_1^2. \tag{30}$$

From this and (18) we obtain

$$\wp'(X) \equiv \frac{X^2}{(1-X)^3} \mod \mathfrak{P}_1^1. \tag{31}$$

As said above, the defining equation for the new $\wp, \wp'$ over K has the form

$$\wp'^2 + \wp\wp' = \wp^3 + B\wp + C \tag{32}$$

with certain new coefficients B, C which may be expressed by the old coefficients in (24) in an obvious manner. It remains to compute the new coefficients B, C. Henceforth, the symbols B, C will be used in the new sense.

In principle, the computation of B, C may be executed by developing $\wp$ and $\wp'$ around the point 1 into a Laurent series with respect to some uniformizing variable, for instance $X - X^{-1}$, then substituting these expansions into (32) and comparing terms. It is clear from this remark that B, C then appear as *universal* power series in q, since the coefficients of the expansions of $\wp, \wp'$ are universal power series in q in view of (29). Here, "universal" means that we obtain the same power series for every characteristic.

This remark may be used to facilitate the computation of B, C, which is now a purely formal affair, by assuming in addition that char $(K) = 0$; by what we have said above the formulas obtained in this case are valid universally. In fact, we may assume that $K = \boldsymbol{Q}((q))$ is the field of formal power series in one indeterminate q over the rational number field $\boldsymbol{Q}$, this field being complete under the power series valuation over $\boldsymbol{Q}$ for which $|q| < 1$.

As a uniformizing variable at 1 we can now introduce the function

$$T = \log X = -\sum_{n>0} \frac{(1-X)^n}{n}$$

which makes sense in characteristic 0. We have

$$X = e^T = \sum_{n\geqq 0} \frac{T^n}{n!}$$

LT

and

$$D = X\frac{d}{dX} = \frac{d}{dT}. \tag{33}$$

This fact, namely that the differential operator D is the differentiation with respect to T, makes computations easier.

From (29),

$$\wp = \frac{e^T}{(1-e^T)^2} + \sum_{m>0} \frac{mq^m}{1-q^m}(e^{mT} + e^{-mT}) - 2s_1$$

which gives the classical expansion

$$(34) \qquad \wp = \frac{1}{T^2} - \sum_{n\geq 0} \frac{B_{n+2}}{n+2} \frac{T^n}{n!} + 2 \sum_{\substack{n>0 \\ n\equiv 0 \bmod 2}} s_{n+1} \frac{T^n}{n!};$$

here, B_n denotes the n-th Bernoulli number:

$$B_0 = 1, \quad B_1 = -\tfrac{1}{2}, \quad B_2 = \tfrac{1}{6}, \quad B_4 = -\tfrac{1}{30}, \quad B_6 = \tfrac{1}{42}$$

and

$$B_n = 0 \quad \text{if} \quad n > 1 \quad \text{and} \quad n \equiv 1 \bmod 2.$$

Furthermore, we have put

$$(35) \qquad s_k = \sum_{m>0} \frac{m^k q^m}{1-q^m}$$

in accordance with (26) for $k = 1$.

Now, the coefficient B is determined from the differential equation

$$(36) \qquad D^2\wp - \wp = 6\wp^2 + 2B$$

which is obtained from (32) by differentiation, using (18). In view of (33) and (34) the computation gives:

$$(37) \qquad B = -5s_3.$$

The coefficient C is determined now by directly substituting (34) into (32) and using (18). One obtains

$$(38) \qquad C = -\tfrac{1}{12}(5s_3 + 7s_5).$$

Note that, for each integer n, we have

$$(38\text{a}) \qquad n^3 \equiv n^5 \bmod 12,$$

hence, in view of (35), we see that the formal denominator 12 in (38) cancels out, so that (38) is in fact a representation of C as an *integral* power series in q.

As said above, the formulas (37), (38) are valid now for arbitrary characteristic.

We collect our results into the following statement:

VI. *The functions $\wp$ and $\wp'$, defined by (29), generate the field $F_K(q)$ of q-periodic functions. $\wp$ has the pole divisor $2\mathfrak{p}_1$, and $\wp'$ has the pole divisor $3\mathfrak{p}_1$. The field $K(\wp)$ is of index 2 in $F_K(q)$, and the non-trivial automorphism of $F_K(q)$ over $K(\wp)$ is given by the reflection $\varepsilon: f(X) \to f(X^{-1})$. The defining relation of $\wp$, $\wp'$ over K has the form*

$$(39) \qquad \wp'^2 + \wp\wp' = \wp^3 + B\wp + C$$

where the coefficients $B, C \in K$ can be expressed as universal power series in q with integral coefficients. Explicitely, these expressions are given by the formulas (35), (37), (38).

Remark:

If char $(K) \neq 2, 3$ then we can use the function $\wp + \frac{1}{12}$ and its derivative $D\wp$ as generators for $F_K(q)$ over K. It is immediately verified that their defining relation is in Weierstraß normal form

$$(40) \qquad (D\wp)^2 = 4(\wp + \tfrac{1}{12})^3 - g_2(\wp + \tfrac{1}{12}) - g_3$$

where the coefficients g_2, g_3 are given by the classical q-expansions

$$(41) \qquad g_2 = \tfrac{1}{12} + 20s_3, \quad g_3 = -\tfrac{1}{216} + \tfrac{7}{3}s_5.$$

Now we turn to the determination of the absolute invariant $j(q)$ of $F_K(q)$. It follows from its definition that $j(q)$ is a certain rational function of the coefficients B, C in (39). According to formulas (39), (40) of the appendix we have explicitely

$$(42) \qquad j(q) = \frac{(1-48B)^3}{\Delta}, \quad \Delta = B^2 - C - 64B^3 + 72BC - 432C^2.$$

If we substitute (37), (38) into these expressions we obtain a universal representation of $j(q)$ as a Laurent series in q with integral coefficients. To investigate this, let us regard for the moment q as an indeterminate so that s_3, s_5 and hence B, C, Δ become elements in the formal power series ring $\mathbf{Z}[[q]]$ over the integers $\mathbf{Z}$. Congruences are to be understood in this power series ring.

From (35) and (38a) we see that

$$(43) \qquad s_3 \equiv s_5 \bmod 12q^2$$

hence

$$5s_3 + 7s_5 \equiv 12s_3 \bmod 12q^2$$

which gives

$$C \equiv -s_3 \equiv -q \mod q^2$$

in view of (38). Moreover, from (37):

$$B \equiv -5q \mod q^2.$$

It follows

$$\Delta \equiv -C \equiv q \mod q^2.$$

We see therefore from (42) that

$$j(q) = \frac{1}{q} \cdot h(q)$$

where $h(q)$ is a quotient of two power series in $\mathbf{Z}[[q]]$ which are $\equiv 1 \mod q$. Therefore, $h(q)$ itself is a power series in $\mathbf{Z}[[q]]$ which is $\equiv 1 \mod q$. We conclude:

$$j(q) = \frac{1}{q} + R(q)$$

where $R(q)$ is a universal power series with integral coefficients.

For the following lemma, the non-archimedean property of the valuation of K is essential.

Lemma 1. *Let*

$$R(X) = c_0 + c_1 X + c_2 X^2 + \cdots$$

be a power series over K, and assume $|c_i| \leqq 1$. Then the function

$$u \to \frac{1}{u} + R(u)$$

defines a bijection of the interior $0 < |u| < 1$ of the unit circle of K onto its exterior $|v| > 1$. We have

$$\left|\frac{1}{u} + R(u)\right| = \frac{1}{|u|} \quad \text{if} \quad 0 < |u| < 1.$$

Proof. Since $|c_i| \leqq 1$ it is clear from the non-archimedean property of K that

$$|R(u)| \leqq 1 \quad \text{if} \quad 0 < |u| < 1$$

and

$$\left|\frac{1}{u} + R(u)\right| = \left|\frac{1}{u}\right| = \frac{1}{|u|}.$$

Also, if

$$\frac{1}{u_1} + R(u_1) = \frac{1}{u_2} + R(u_2)$$

then

$$\left|\frac{1}{u_1} - \frac{1}{u_2}\right| = \left|\sum_{n>0} c_n (u_1^n - u_2^n)\right| \leqq |u_1 - u_2|$$

which implies

$$|u_1 - u_2| \leqq |u_1|\,|u_2|\,|u_1 - u_2|$$

hence $u_1 = u_2$. It remains to show that for every $v \in K$ with $|v| > 1$ there exists an element $u \in K$ with $0 < |u| < 1$ such that $v = \frac{1}{u} + R(u)$.

Such an element u is constructed by the convergent iteration procedure:

$$u_0 = \frac{1}{v}, \quad u_{i+1} = \frac{1}{v}(1 + u_i R(u_i)); \quad u = \lim_i u_i.$$

QED.

Using this lemma, we obtain:

VII. *The absolute invariant $j(q)$ of $F_K(q)$ can be expressed in the form*

$$j(q) = \frac{1}{q} + R(q) \tag{44}$$

where $R(q)$ is a universal power series with integral coefficients. We have

$$|j(q)| = \frac{1}{|q|} > 1.$$

To every element $j \in K$ with $|j| > 1$ there exists one and only one $q \in K$ with $0 < |q| < 1$ such that $j = j(q)$.

Remark 1:

The expansion (44) being of formal nature, it coincides with the classical q-expansion of the modular function $j(\omega)$ if this is regarded as a function of the variable $e^{2\pi i \omega} = q$. For, one knows that $j(\omega)$ is the absolute invariant of the Weierstraß equation (40), (41) if one substitutes $q = e^{2\pi i \omega}$ in these formulas.

The first terms of $R(q)$ are

$$R(q) = 744 + 196884 \cdot q + \cdots$$

Remark 2:

The classically well known product representation

$$\Delta = q \prod_{n>0} (1 - q^n)^{24} \tag{45}$$

holds also in the non-archimedean case for every characteristic. For, both sides in (45) being universal power series in q with integral coefficients, one may regard (45) as an identity in the power series ring $\mathbf{Z}[[q]]$; hence this relation remains true if we substitute for q an element in K with $|q| < 1$.

Note that, from VII, we have

$$j(q) \neq 0,\ 12^3$$

since the valuation of K is non-archimedean. It follows that the *Hasse invariant* of $F_K(q)$, as described in § A1 of the appendix, is defined. Let $\gamma_K(q)$ denote this invariant. If char $(K) \neq 2$ then $\gamma_K(q)$ is an element of $K^\times/K^{\times 2}$, whereas it is an element of $K^+/\pi K^+$ if char $(K) = 2$; here we put

$$\pi(a) = a^2 + a.$$

We have:

VIII. *The Hasse invariant of $F_K(q)$ is*

$$\gamma_K(q) \equiv \begin{cases} 1 \bmod K^{\times 2} & \text{if char } (K) \neq 2 \\ 0 \bmod \pi K^+ & \text{if char } (K) = 2. \end{cases}$$

Proof. If char $(K) = 2$ then $\gamma_K(q) \equiv 0$ since the cubic polynomial on the right hand side of (39) has no quadratic term. If char $(K) \neq 2$ then from (18) and (39) we see that $\wp$, $D\wp$ satisfy the equation

$$(D\wp)^2 = 4\wp^3 + \wp^2 + 4B\wp + 4C \tag{46}$$

If char $(K) = 3$ then we infer from this that $\gamma_K(q) = 1$ since the coefficient of $\wp^2$ in this equation is 1.

Now assume char $(K) \neq 2, 3$. Then we use $\wp + \frac{1}{12}$ and $D\wp$ as generators of $F_K(q)$, whose defining relation over K is in Weierstraß normal form (40). The Hasse invariant is then given by

$$\gamma_K(q) \equiv -\frac{1}{2}\frac{g_2}{g_3} \bmod K^{\times 2}$$

where g_2, g_3 are obtained from (41). Hence

$$\gamma_K(q) \equiv \frac{1 + 240\, s_3}{1 - 504\, s_5} \bmod K^{\times 2}. \tag{47}$$

We are going to show that both numerator and denominator of this formula are squares in K. From (43) we infer that

$$|s_3| = |s_5| = |q| < 1.$$

Hence both numerator and denominator in (47) are of the form

$$v = 1 + 4s \quad \text{with} \quad s \in K,\ |s| < 1.$$

A square root u of such an element can be extracted by means of the convergent iteration procedure:

$$u_0 = 1, \quad u_{i+1} = u_i + \frac{1}{2}\left(\frac{v}{u_i} - u_i\right), \quad u = \lim_i u_i.$$

QED.

The absolute invariant and the Hasse invariant of $F_K(q)$ suffice to characterize $F_K(q)$ as an elliptic function field over K. (See Appendix § A1). Hence we obtain from VII and VIII the following:

VIIIa. *Algebraic description of elliptic function fields $F \mid K$ which can be K-isomorphically represented as a field of q-periodic functions for some $q \in K$ with $0 < |q| < 1$:*
This is the case if and only if the following conditions are satisfied:

(i) *$F \mid K$ has a prime divisor of degree* 1;
(ii) *the absolute invariant j of $F \mid K$ satisfies $|j| > 1$;*
(iii) *the Hasse invariant γ of $F \mid K$ is trivial.*

If this is the case, then from statement VII we see that the element q for which F is K-isomorphic to $F_K(q)$ is uniquely determined. q is called the *period* of F.

§ 4. Elliptic function fields having a periodic Jacobian field

As before, q denotes an element in K with $0 < |q| < 1$ and $F_K(q)$ is the corresponding field of q-periodic functions.

We propose to investigate elliptic function fields $E \mid K$ which admit $F_K(q)$ as their Jacobian field. Here, the notion of "Jacobian field" is to be understood in the algebraic sense as explained in § A2 of the appendix; it means that the absolute and the Hasse invariant of E coincide with the absolute and the Hasse invariant of $F_K(q)$, the latter having been determined in § 3.

If E admits $F_K(q)$ as its Jacobian field, then according to statement VII in § 3 the element q is uniquely determined by this property; it will be called the *period* of E.

Let $L \mid K$ be a Galois extension which splits E, and let G denote its Galois group. According to § A2 of the appendix, E is uniquely determined, up to K-isomorphisms, by its cohomological invariant ζ; this is an element in $H^1(G, T_L(q))$ where $T_L(q)$ denotes the group of translation automorphisms of $F_L(q)$[1])[2]).

We have a canonical G-isomorphism

$$L^\times/q \to T_L(q) \tag{48}$$

which is given by associating to every $a \in L^\times$ its translation automorphism $\tau_a \in T_L(q)$; this follows from corollaries Va and Vb, together with remark 2 of § 2. Hence an isomorphism

$$H^1(G, L^\times/q) \to H^1(G, T_L(q)), \tag{49}$$

so that we may regard ζ as an element in $H^1(G, L^\times/q)$.

If ζ is any given element in $H^1(G, L^\times/q)$ then an elliptic field $E \mid K$ with period q and the cohomological invariant ζ can be obtained in the following way: Choose a 1-cocycle $G \to L^\times/q$ which represents ζ; for simplicity this cocycle is again denoted by ζ. Let σ range over the automorphisms of G, and consider these as automorphisms of $F_L(q)$ over $F_K(q)$ acting on the coefficients of the q-periodic functions.

The map

$$\sigma \to \tau_{\zeta(\sigma)}\sigma$$

is then a monomorphism from G to the automorphism group of $F_L(q)$, and its field E_ζ of fixed elements satisfies our requirements. This follows immediately from the definition of the cohomological invariant as given in § A 2.

First, we are going to describe the structure of the group $H^1(G, L^\times/q)$.

Let exp and log denote the ordinary complex exponential and logarithm. Let us put

$$e_q(a) = \exp\left(2\pi i \frac{\log|a|}{\log|q|}\right) \qquad (a \in L^\times). \tag{50}$$

This defines a homomorphism

$$e_q : L^\times \to \mathbf{W}$$

[1]) $T_L(q)$ being canonically isomorphic to the group $C_L^0(q)$ of divisor classes of degree 0, one may regard ζ as an element in $H^1(G, C_L^0(q))$ if this is convenient.

[2]) Note that ζ is determined by E up to a minus sign only; that is, two cohomology classes ζ_1 and ζ_2 determine K-isomorphic fields E_1, E_2 if and only if $\zeta_1 = \pm\zeta_2$ (see § A 2). This fact should be kept in mind throughout the following discussion.

where $\mathbf{W}$ denotes the multiplicative group of complex numbers of absolute value 1. We have $e_q(q) = 1$ and hence obtain a homomorphism

$$e_q : L^\times/q \to \mathbf{W}.$$

For $\sigma \in G$ we have $|\sigma a| = |a|$ and hence

$$e_q(\sigma a) = e_q(a);$$

this means that the homomorphism (50) is G-permissible, G acting trivially on $\mathbf{W}$. Hence we obtain a cohomology map

$$e_q : H^1(G, L^\times/q) \to H^1(G, \mathbf{W}),$$

where

$$H^1(G, \mathbf{W}) = \mathrm{Hom}\,(G, \mathbf{W}) = \hat{G},$$

the character group of G. We shall see that this is in fact a monomorphism. In order to describe its image, let us make the following definitions: For $\chi \in \hat{G}$ let G_χ denote the kernel of χ in G, and let K_χ be the field of fixed elements of G_χ in L. The field extension $K_\chi \mid K$ is cyclic of degree equal to the order of χ.

Definition. *The character χ of G is called q-trivial if q is the norm of some element Q in K_χ:*

$$q = N_{K_\chi \mid K}(Q).$$

The set of q-trivial characters of G will be denoted by $\hat{G}(q)$. (It follows from lemma 2 that $\hat{G}(q)$ is a subgroup of $\hat{G}$.)

Remark. If K is locally compact and $L \mid K$ finite then $\hat{G}$ can be identified, via the reciprocity law, with the character group of $K^\times/N L^\times$, where $N : L \to K$ is the norm map. After this identification, q-triviality means that $\chi(q) = 1$; this explains our terminology.

We now claim:

Lemma 2. *Let $L \mid K$ be a Galois extension with group G. Then the homomorphism:*

$$e_q : H^1(G, L^\times/q) \to \hat{G} \tag{51}$$

defined by (50) *induces an isomorphism*

$$H^1(G, L^\times/q) \approx \hat{G}(q)$$

where $\hat{G}(q)$ consists of the q-trivial characters of G, as defined above. In particular, $\hat{G}(q)$ is a subgroup of $\hat{G}$.

Proof. (i) First we show that the map (51) is *monomorphic.* We consider the exact and commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & \mathbf{Z} & \xrightarrow[q]{} & L^\times & \to & L^\times/q & \to & 0 \\ & & \| & & \downarrow{\scriptstyle v_q} & & \downarrow{\scriptstyle e_q} & & \\ 0 & \to & \mathbf{Z} & \to & \mathbf{R} & \xrightarrow[\exp]{} & \mathbf{W} & \to & 0 \end{array}$$

where $\mathbf{R}$ denotes the additive group of real numbers. The map denoted by q: $\mathbf{Z} \to L^\times$ is the exponential map

$$k \to q^k \qquad (k \in \mathbf{Z}); \tag{51a}$$

v_q denotes the map

$$v_q(a) = \frac{\log |a|}{\log |q|} \qquad (a \in L^\times)$$

which is an additive valuation equivalent to the valuation $|\ \ |$; finally, exp denotes the exponential map

$$r \to \exp(2\pi i r) \qquad (r \in \mathbf{R}).$$

The vertical double line indicates the identity map. The above diagram leads to an exact and commutative cohomology diagram

$$\begin{array}{ccccccc} H^1(G, L^\times) = 0 & \to & H^1(G, L^\times/q) & \xrightarrow[d_1]{} & H^2(G, \mathbf{Z}) & \xrightarrow[q]{} & H^2(G, L^\times) \\ & & \downarrow{\scriptstyle e_q} & & \| & & \\ H^1(G, \mathbf{R}) = 0 & \to & H^1(G, \mathbf{W}) & \xrightarrow[d_2]{} & H^2(G, \mathbf{Z}) & \to & 0 = H^2(G, \mathbf{R}) \end{array} \tag{52}$$

where d_1, d_2 denote the cohomological connecting operators belonging to the first resp. second row of the former diagram. The fact that $H^1(G, L^\times) = 0$ is known as Hilberts theorem 90. The fact that $H^n(G, \mathbf{R}) = 0$ for $n \geqq 1$ follows from the unique divisibility of $\mathbf{R}$.

From (52) we see that

$$d_1 = d_2 \cdot e_q;$$

moreover, (52) shows that d_1 is monomorphic. It follows that e_q is monomorphic too.

(ii) Before determining the image of the map (51) let us first discuss its behavior under inflation. So let

L_0 be a Galois extension of K contained in L,

G_0 the group of $L_0|K$

S the group of $L|L_0$.

The sequence of groups

$$1 \to S \to G \to G_0 \to 1$$

is exact. For any G-module A, we have a cohomological inflation-restriction sequence

$$0 \to H^1(G_0, A^S) \xrightarrow[\inf]{} H^1(G, A) \xrightarrow[\mathrm{res}]{} H^1(S, A)$$

which is exact; as usual, A^S is the submodule of A consisting of the elements which are fixed under S. This sequence is *functorially covariant* with respect to A.

The map $e_q: L^\times/q \to \mathbf{W}$ thus gives rise to a commutative diagram

$$\begin{array}{cccccc} 0 \to & H^1(G_0, L_0^\times/q) & \xrightarrow[\inf]{} & H^1(G, L^\times/q) & \xrightarrow[\mathrm{res}]{} & H^1(S, L^\times/q) \\ & \downarrow{\scriptstyle e_q} & & \downarrow{\scriptstyle e_q} & & \downarrow{\scriptstyle e_q} \\ 0 \to & H^1(G_0, \mathbf{W}) & \xrightarrow[\inf]{} & H^1(G, \mathbf{W}) & \xrightarrow[\mathrm{res}]{} & H^1(S, \mathbf{W}). \end{array} \tag{53}$$

The second row of this diagram is identical with

$$0 \to \hat{G}_0 \xrightarrow[\inf]{} \hat{G} \xrightarrow[\mathrm{res}]{} \hat{S}$$

where the inflation is obtained by regarding every character of $G_0 = G/S$ as a character of G; as usual we identify $\hat{G}_0 \subset \hat{G}$. For the moment, let $\hat{G}[q]$ denote the image of $e_q: H^1(G, L^\times/q) \to \hat{G}$ and similarly $\hat{G}_0[q]$. Then, *since all three vertical maps of the diagram* (53) *are monomorphic by* (i), we see that

$$\hat{G}_0[q] = \hat{G}[q] \cap \hat{G}_0.$$

In other words: let χ be a character of G which is already a character of G_0, i. e. for which $\chi(S) = 1$. *Then χ is in $\hat{G}[q]$ if and only if χ is in $\hat{G}_0[q]$.*

We also have the relation

$$\hat{G}_0(q) = \hat{G}(q) \cap \hat{G}_0$$

since the property of a character to be q-trivial depends only on K_χ. That is, *χ is in $\hat{G}(q)$ if and only if χ is in $\hat{G}_0(q)$*, provided $\chi(S) = 1$.

Now recall that we want to show $\hat{G}(q) = \hat{G}[q]$. That is, if $\chi \in \hat{G}$ we have to show that χ is in $\hat{G}[q]$ if and only if it is in $\hat{G}(q)$. If $\chi(S) = 1$ then the foregoing arguments show that we may replace G by G_0 and hence L by L_0 without loss of generality.

For a given character $\chi \in \hat{G}$, the largest subgroup of G on which χ is trivial is the kernel G_χ; the corresponding subfield of L being K_χ.

Hence, in order to *prove our assertion for a fixed character* χ, *we may assume that* $L = K_\chi$, i. e. that χ is a faithful character of G.

(iii) So assume that $L|K$ is cyclic and χ is a faithful character of G. We have to show: χ is in the image of the map (51) if and only if χ is q-trivial which now means that q is a norm from L.

Consider once more the diagram (52). Let

$$\psi = d_2(\chi)$$

be the image of χ in $H^2(G, \mathbf{Z})$. From (52) we see that χ is in the image of e_q if and only if ψ is in the image of d_1; this means that ψ is in the kernel of the subsequent map

$$q : H^2(G, \mathbf{Z}) \to H^2(G, L^\times). \tag{54}$$

Now, G and $\hat{G}$ are cyclic and χ generates $\hat{G}$. From (52) we conclude that $H^2(G, \mathbf{Z})$ is cyclic too, being isomorphic to $\hat{G}$ under d_2, and that ψ is a generator of $H^2(G, \mathbf{Z})$. Hence ψ is in the kernel of the map (54) if and only if this is the zero map. We have to show that this is the case if and only if q is a norm from L.

Now, G being cyclic we have for every G-module A an isomorphism

$$H^2(G, A) = H^0(G, A) = A^G/NA$$

where A^G is the submodule of G-stable elements of A and N denotes the norm operator of G on A. This isomorphism is not canonical but depends on the choice of a generator of G; if such a generator is chosen then this isomorphism is functorial with respect to A. We have

$$H^0(G, \mathbf{Z}) = \mathbf{Z}/n, \quad H^0(G, L^\times) = K^\times/NL^\times$$

where $n = [L : K]$. Hence, the map (54) can now be interpreted as the map

$$q : \mathbf{Z}/n \to K^\times/NL^\times$$

which is induced by (51a). This map is the zero map if and only if 1 is mapped onto a norm, i. e. if $q^1 \in NL^\times$.

QED.

In view of lemma 2 and what we have said before we conclude the validity of the following statement:

IX. *Let* $L|K$ *be a Galois extension with group* G. *The classes of* K-*isomorphic elliptic function fields* $E|K$ *of period* q *which are split by* L *correspond* 1 — 1 *to the pairs* χ, χ^{-1} *of mutually inverse* q-*trivial characters of* G.

If E belongs to χ in this correspondence then χ is called the *character invariant* of E. It is determined by E up to the substitution $\chi \to \chi^{-1}$ only.

Two observations have to be added to the statement IX:

1. Let $E|K$ be as in statement IX. *Then the character invariant* χ *of* E *does not depend on the choice of the Galois splitting field* L *of* E. For, assume that E is split already by a subfield L_0 of L which is Galois over K, and let χ_0 be the character invariant of E with respect to L_0. Then

$$\chi = e_q(\zeta), \quad \chi_0 = e_q(\zeta_0)$$

where ζ, ζ_0 are the cohomological invariants of E with respect to L, L_0. If we identify

$$H^1(G_0, L_0^\times/q) \subset H^1(G, L^\times/q)$$

by means of the inflation map, then $\zeta = \pm\zeta_0$ which means that ζ does not depend on the splitting field L; this follows from the general definition of the cohomological invariant as given in the appendix. Using the diagram (53) we conclude that $\chi = \chi_0^{\pm 1}$ in the identification

$$\hat{G}_0 \subset \hat{G}$$

which says that the character invariant too does not depend on the choice of L.

2. The second observation is concerned with the *behavior of the character invariant of* E *under extensions of the field of constants*. Let K' be a finite algebraic field extension of K. Consider the constant field extension EK'. This is an elliptic function field over K' which is split by LK' and has period q. Let χ' be its character invariant; this is a q-trivial character of the Galois group G' of $LK'|K'$. We may identify G' with a subgroup of G according to the following Galois diagram:

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash, "G'"'] & LK' \arrow[d, dash, "G'"] \\
L \cap K' \arrow[r, dash] \arrow[d, dash] & K' \\
K &
\end{tikzcd}$$

The cohomological invariant ζ' of EK' is given as the image of ζ of E under the restriction map

$$\text{res}: H^1(G, L^\times/q) \to H^1(G', (LK')^\times/q).$$

Now it is clear from its definition that the map (51) commutes with the restriction, i. e. that the diagram

$$\begin{array}{ccc} H^1(G, L^\times/q) & \xrightarrow{\text{res}} & H^1(G', (LK')^\times/q) \\ \downarrow{\scriptstyle e_q} & & \downarrow{\scriptstyle e_q} \\ \hat{G} & \xrightarrow{\text{res}} & \hat{G}' \end{array}$$

commutes; here res: $\hat{G} \to \hat{G}'$ is obtained by restricting the range of every character χ of G to the subgroup $G' \subset G$. We conclude: *the character invariant χ' of EK' is obtained from the character invariant χ of E by restricting χ to the subgroup G'.*

There is an interesting consequence of this fact. Namely, we ask: Under what condition is K' a splitting field of E? This is the case if and only if EK' is K'-isomorphic to $F_{K'}(q)$ which is to say that the character invariant χ' of EK' is trivial. By what we have said above this means $\chi(G') = 0$, i. e. $G' \subset G_\chi$, $K_\chi \subset K'$. We obtain:

X. *Let $E|K$ be an elliptic function field of period q and let χ be its character invariant. Then the cyclic extension $K_\chi|K$ can be characterized as the unique minimal algebraic splitting field of E. That is, K_χ splits E and it is contained in every splitting field of E which is algebraic over K.*

Now we ask the following question: Given a q-trivial character χ, how can we explicitely construct an elliptic function field $E \mid K$ of period q which has character invariant χ?

A method of construction is given by following up the various isomorphisms leading to statement IX. First we note that E, the field to be constructed, is split by K_χ. Hence, in the foregoing arguments, we may assume without loss of generality that

$$L = K_\chi.$$

That is, we may assume that χ is a *faithful* character of G. Let

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

There is one and only one generator σ of G which is determined by the condition

$$\chi(\sigma) = \exp\left(\frac{2\pi i}{n}\right) \tag{55}$$

Conversely, if $L|K$ is an arbitrary cyclic extension of degree n and if σ is a given generator of its Galois group G then there is one and only one character χ of G which satisfies (55). This character is q-trivial if and only if there exists $Q \in L$ such that $N\,Q = q$; here and in the following, N denotes the norm map from L to K if nothing is said to the contrary.

So let us change our point of view: Instead of starting with χ, we start with a given triple

$$\mathsf{Q} = (L, \sigma, Q)$$

where

- L is a cyclic extension of K of degree n,
- σ a generator of the Galois group G of L,
- Q an element of L with $N\,Q = q$.

Starting from these data, we shall give an explicit construction of an elliptic function field, called $F_K(\mathsf{Q})$, which has period q and whose character invariant χ is given by the formula (55).

First, we have to look for a 1-cocycle $\zeta: G \to L^\times/q$ which corresponds to χ under the isomorphism e_q of lemma 2. We claim that such a cocycle ζ is given by

$$\zeta(\sigma) \equiv Q \bmod^\times q. \tag{56}$$

For, since $N\,Q = q \equiv 1 \bmod^\times q$ and since σ generates G, it follows that there is one and only one 1-cocycle $\zeta: G \to L^\times/q$ satisfying (56); moreover, we have

$$|q| = |N\,Q| = |Q|^n$$

and therefore in view of (50)

$$e_q(Q) = \exp\left(\frac{2\pi i}{n}\right) \tag{57}$$

which gives

$$e_q\zeta(\sigma) = \chi(\sigma)$$

and hence

$$e_q\zeta = \chi.$$

Secondly, we have to regard ζ as 1-cocycle from G to $T_L(q)$ in view of the isomorphism (48); this gives

$$\zeta(\sigma) = \tau_Q, \tag{58}$$

where τ_Q denotes the translation automorphism of $F_L(q)$ given by

$$\tau_Q : f(X) \to f(Q^{-1}X).$$

Now, $\sigma \to \tau_Q\sigma$ defines a monomorphism of G into the automorphism group of $F_L(q)$ and the field $F_K(\mathsf{Q})$ to be constructed is the field of fixed elements of its image; since G is cyclic it can be described as field of fixed elements of the automorphism $\tau_Q\sigma$. That is, the elements in $F_K(\mathsf{Q})$ are those q-periodic functions f defined over L which satisfy the functional equation

$$\tau_Q\sigma f = f. \tag{59}$$

It is clear from its construction that this field $F_K(\mathsf{Q})$ has period q and that its character invariant χ is given by (55).

Both τ_Q and σ may be considered as operators on the whole field M_L of meromorphic functions over L (and not only on $F_L(q)$). If this is done, we have

$$(\tau_Q\sigma)^i = \tau_{Q_i}\sigma^i, \quad Q_i = Q \cdot (\sigma Q) \cdot (\sigma^2 Q) \cdots (\sigma^{i-1} Q) \tag{60}$$

for $i > 0$; this formula holds also for $i = 0$ if we interpret $Q_0 = 1$. Taking $i = n$ we have

$$(\tau_Q\sigma)^n = \tau_q \tag{61}$$

since $Q_n = N\,Q = q$ and $\sigma^n = 1$. Hence, if $f \in M_L$ satisfies the functional equation (59), then $\tau_q f = f$, i.e. f is contained in $F_L(q)$ and therefore $f \in F_K(\mathsf{Q})$.

Definition. *The function $f \in M_L$ is called semi-periodic with respect to Q if it satisfies the functional equation* (59).

These semi-periodic functions form a subfield $F_K(\mathsf{Q})$ of M_L, and we have proved:

XI. *Consider a triple $\mathsf{Q} = (L, \sigma, Q)$ consisting of a cyclic extension L of K, of a generating automorphism σ of $L|K$ and of an element $Q \in L$ with $N\,Q = q$. Let $F_K(\mathsf{Q})$ denote the field of semi-periodic functions with respect to Q.*

Then $F_K(\mathsf{Q})$ is an elliptic function field over K of period q which is split by L. The character invariant χ of $F_K(\mathsf{Q})$ is given by

$$\chi(\sigma) = \exp\left(\frac{2\pi i}{n}\right), \quad n = [L:K].$$

In particular, $L = K_\chi$ is the minimal algebraic splitting field of $F_K(\mathsf{Q})$.

Every elliptic function field $E|K$ of period q is K-isomorphic to some $F_K(\mathsf{Q})$ with suitable $\mathsf{Q} = (L, \sigma, Q)$. Here, L is uniquely determined by E as its minimal algebraic splitting field, while σ and Q are determined up to the substitutions

$$\sigma \to \sigma^{\pm 1}, \quad Q \to Q\frac{\sigma u}{u} \qquad (u \in L^\times).$$

As to the last sentence, note that the substitution $\sigma \to \sigma^{-1}$ means $\chi \to \chi^{-1}$; fields which have mutually inverse character invariants are K-isomorphic. Also, if $N\,Q = q$, then any other element $Q' \in L^\times$ with $N\,Q' = q$ has the form $Q' = Q\frac{\sigma u}{u}$ with $u \in L^\times$ by Hilberts theorem 90.

§ 5. Properties of semi-periodic function fields

In this section, the properties of the semi-periodic function fields will be studied in more detail. Let us note beforehand that from § 4 we shall essentially use the definition of these fields only; in particular, our arguments will be independent of the algebraic theory of Jacobian fields.

So let us consider a given triple

$$\mathsf{Q} = (L, \sigma, Q)$$

where L is a cyclic extension of K and σ a generator of its Galois group G; furthermore, Q is an element in L with $N\,Q = q$. The degree of $L|K$ will be denoted by n and $N : L \to K$ is the norm function.

As in § 4, $F_K(\mathsf{Q})$ denotes the field of meromorphic functions $f \in M_L$ which satisfy the functional equation (59). From (61) we see that

$$F_K(\mathsf{Q}) \subset F_L(q);$$

we can characterize $F_K(\mathsf{Q})$ as the field of fixed elements in $F_L(q)$ of the automorphism $\tau_Q\sigma$ of order n.

Hence $F_L(q)$ is a cyclic extension of $F_K(\mathsf{Q})$ of degree n, its Galois group G_{Q} being generated by $\tau_Q\sigma$.

Since $\tau_Q\sigma$ induces σ in L which has K as its fixed field, we infer from Galois theory that

$$F_K(\mathsf{Q}) \cap L = K, \quad F_K(\mathsf{Q}) \cdot L = F_L(q)$$

and that $F_K(\mathsf{Q})$ and L are linearly disjoint over K. We know from § 2 that $F_L(q)$ is an algebraic function field over L. It follows that $F_K(\mathsf{Q})$ is an algebraic function field over K and that its constant field extension with L is $F_L(q)$. Since the latter has genus 1 and since the genus does not change under separable constant field extensions, we conclude that $F_K(\mathsf{Q})$ has genus 1. Since $F_L(q)$ is conservative we see that $F_K(\mathsf{Q})$ is conservative too. These arguments show anew that $F_K(\mathsf{Q})$ is an elliptic function field over K.

As a separable constant field extension the field $F_L(q)$ is *unramified* over $F_K(\mathsf{Q})$. It follows that the divisors of $F_K(\mathsf{Q})$ can be characterized as those divisors of $F_L(q)$ which are left fixed by the generating automorphism $\tau_Q\sigma$ of G_{Q}. If $\mathfrak{m}$ is any divisor in D_L (in the analytic sense) which is fixed by $\tau_Q\sigma$ then from (61) we conclude that $\mathfrak{m}$ is q-periodic, i. e. $\mathfrak{m}$ is in the divisor group $D_L(q)$ of $F_L(q)$, and hence $\mathfrak{m}$ is a divisor of $F_K(\mathsf{Q})$.

Accordingly, we define a Q-*semi-periodic divisor* $\mathfrak{m}$ by the condition

$$\tau_Q\sigma\mathfrak{m} = \mathfrak{m}.$$

These divisors form a subgroup $D_K(\mathsf{Q}) \subset D_L$. By what we have said, we have

$$D_K(\mathsf{Q}) \subset D_L(q)$$

and $D_K(\mathsf{Q})$ is the divisor group (in the algebraic sense) of the field $F_K(\mathsf{Q})$.

The degree (in the algebraic sense) of a divisor is invariant under constant field extensions. Hence, by what we have shown in § 2, the degree (in the algebraic sense) of a divisor $\mathfrak{m} \in D_K(\mathsf{Q})$ can be analytically described as $\deg_q(\mathfrak{m})$, if we regard $\mathfrak{m}$ as a q-periodic divisor over L.

In the following, if nothing is said to the contrary, the analytic notions and facts developed in § 2 will be applied to L instead of K as ground field. Accordingly, if $\alpha \in \Omega^\times$ then w_α denotes the analytic valuation of M_L; for simplicity we have dropped the index L as employed in remark 1 of § 2[1]). Hence we have now $w_\alpha = w_\beta$ if and only if α and β are L-conjugate.

According to § 2, every prime divisor of $F_L(q)$ is of the form $\mathfrak{p}_\alpha$, the corresponding normalized valuation of $F_L(q)$ being induced by w_α. We have $\mathfrak{p}_\alpha = \mathfrak{p}_\beta$ if and only if α and β are L-conjugate $\bmod^\times q$.

[1]) In the statements of the propositions and theorems however, we shall again write $w_{\alpha,L}$ and $\mathfrak{p}_{\alpha,L}$ to indicate that we are working over L.

Every prime divisor $\mathfrak{q}$ of $F_K(\mathsf{Q})$ is induced by some prime divisor $\mathfrak{p}$ of $F_L(q)$. If $\mathfrak{p} = \mathfrak{p}_\alpha$ then we write $\mathfrak{q} = \mathfrak{q}_\alpha$. Since $F_L(q)$ is unramified over $F_K(\mathsf{Q})$ the normalized valuation belonging to $\mathfrak{q}_\alpha$ is induced by w_α. To describe the prime divisors of $F_K(\mathsf{Q})$ we have to ask: Under what condition is $\mathfrak{q}_\alpha = \mathfrak{q}_\beta$?

This is the case if and only if the prime divisors $\mathfrak{p}_\alpha$ and $\mathfrak{p}_\beta$ induce the same prime divisor in $F_K(\mathsf{Q})$, i. e. if they are conjugate under the Galois group G_{Q}:

$$\mathfrak{p}_\beta = (\tau_Q\sigma)^i\mathfrak{p}_\alpha \tag{62}$$

for some i with $0 \leqq i < n$. Now, the action of σ on the primes $\mathfrak{p}_\alpha$ is given by the formula

$$\sigma\mathfrak{p}_\alpha = \mathfrak{p}_{\sigma\alpha}\,{}^{1}). \tag{63}$$

The action of τ_Q on $\mathfrak{p}_\alpha$ is given by the formula

$$\tau_Q\mathfrak{p}_\alpha = \mathfrak{p}_{Q\alpha}. \tag{64}$$

Thus formula (62) now reads

$$\mathfrak{p}_\beta = \mathfrak{p}_{(Q\sigma)^i\alpha}$$

where $(Q\sigma)^i$ is to be understood as the i-th power of the permutation $\alpha \to Q\sigma\alpha$ of $\Omega^\times$. This means that the elements β and $(Q\sigma)^i\alpha$ are L-conjugate $\bmod^\times q$, i. e. that there exists an L-conjugate β' of β and an integer k such that

$$\beta' = q^k(Q\sigma)^i\alpha.$$

Since $(Q\sigma)^n = q$ (compare (61)) we may write this in the form

$$\beta' = (Q\sigma)^{nk+i}\alpha.$$

Let us say that two elements $\alpha, \beta \in \Omega^\times$ are L-conjugate $\bmod^\times Q\sigma$ if there exists an L-conjugate β' of β such that

$$\beta' = (Q\sigma)^m\alpha$$

[1]) Strictly speaking, the symbol $\sigma\alpha$ is not defined if α is not contained in L. Hence, to interpret (63), we have to extend σ to an automorphism of Ω; if the extension is again denoted by σ then $\sigma\alpha$ is defined and formula (63) holds. It does not matter which extension we choose since $\mathfrak{p}_\alpha = \mathfrak{p}_\beta$ if α and β are L-conjugate. This is the reason why we prefer not to introduce a new symbol for the extension of σ to an automorphism of Ω. In the following, the symbol $\sigma\alpha$ for $\alpha \in \Omega$ is always meant in this sense, with the understanding that in the respective context it does not matter which extension we choose.

for some $m \in \mathbf{Z}$. Then we have shown:

$\mathfrak{q}_\alpha = \mathfrak{q}_\beta$ *if and only if* α *and* β *are* L*-conjugate* $\bmod^\times Q\sigma$.

At the same time we have seen that the prime divisors of $F_L(q)$ which extend $\mathfrak{q}_\alpha$ are precisely the primes $\mathfrak{p}_{(Q\sigma)^i\alpha}$ for $0 \leqq i < n$. These primes are mutually *distinct*. To see this, one has to verify that the elements

$$(Q\sigma)^i\alpha \qquad (0 \leqq i < n)$$

are mutually non-conjugate over L $\bmod^\times q$. Assume that some L-conjugate of $(Q\sigma)^i\alpha$ is of the form $q^k(Q\sigma)^j\alpha$ $(k \in \mathbf{Z})$. Then

$$|(Q\sigma)^i\alpha| = |q|^k|(Q\sigma)^j\alpha|.$$

Now note that

$$(Q\sigma)^i\alpha = Q_i\sigma^i\alpha$$

where Q_i is as defined in (60); we have $|\sigma^i\alpha| = |\alpha|$ and

$$|Q_i| = |Q|^i = |q|^{\frac{i}{n}}.$$

It follows

$$|q|^{\frac{i}{n}} = |q|^k|q|^{\frac{j}{n}}, \qquad \frac{i}{n} \equiv \frac{j}{n} \bmod \mathbf{Z}, \qquad i = j$$

since $0 \leqq i, j < n$.

We see therefore that every prime $\mathfrak{q}_\alpha$ of $F_K(\mathsf{Q})$ splits into the n distinct primes $\mathfrak{p}_{(Q\sigma)^i\alpha}$ $(0 \leqq i < n)$ of $F_L(q)$. That is, $\mathfrak{q}_\alpha$ *splits completely* in $F_L(q)$. It follows that the residue class field of $\mathfrak{q}_\alpha$ is K-isomorphic to the residue class field of any one of its extensions, for instance of $\mathfrak{p}_\alpha$. The latter residue class field is $L(\alpha)$ according to § 2. In particular, the degree of $\mathfrak{q}_\alpha$ is $[L(\alpha):K] = n \cdot [L(\alpha):L]$.

Let us collect our results into the following statements:

XII. *The field* $F_K(\mathsf{Q})$ *of* Q*-semi-periodic functions is an elliptic function field over* K; *its constant field extension with* L *equals* $F_L(q)$, *the field of* q*-periodic functions over* L.

XIII. *The prime divisors* $\mathfrak{q}$ *of* $F_K(\mathsf{Q})$ *correspond* $1 - 1$ *to the classes of* L*-conjugate elements* $\alpha \in \Omega^\times \bmod^\times Q\sigma$. *If* $\mathfrak{q}$ *belongs to* α *in this correspondence, we write* $\mathfrak{q}_\alpha$. *The normalized valuation of* $\mathfrak{q}_\alpha$ *is induced by the analytic valuation* $w_{\alpha, L}$. *The residue class field of* $\mathfrak{q}_\alpha$ *is* $L(\alpha)$; *in particular, the degree of* $\mathfrak{q}_\alpha$ *is* $n \cdot [L(\alpha):L]$, *hence divisible by* n.

Every prime divisor $\mathfrak{q}_\alpha$ *of* $F_K(\mathsf{Q})$ *splits completely in* $F_L(q)$, *its decomposition being given by the formula*

$$\mathfrak{q}_\alpha = \sum_{0 \leqq i < n} \mathfrak{p}_{(Q\sigma)^i\alpha,\, L} = N_{\mathsf{Q}}(\mathfrak{p}_{\alpha, L})$$

where N_{Q} *denotes the norm operator from* $F_L(q)$ *to* $F_K(\mathsf{Q})$.

XIV. *The divisor group (in the algebraic sense) of* $F_K(\mathsf{Q})$ *can be analytically described as the group* $D_K(\mathsf{Q})$ *of* Q*-semi-periodic divisors. In this description,* $\mathfrak{q}_\alpha$ *is the divisor which has multiplicity* 1 *at the points* β *which are* L*-conjugate to* $\alpha \bmod^\times Q\sigma$, *and multiplicity* 0 *elsewhere. The degree (in the algebraic sense) of a divisor coincides with the analytic degree* $\deg_q$ *as defined in* § 2. *Every divisor of* $D_K(\mathsf{Q})$ *is the* N_{Q}*-norm of a divisor in* $D_L(q)$.

(The last assertion follows from XIII which contains the corresponding statement for *prime* divisors).

Recall that the *index* of an algebraic function field $F|K$ is defined to be the smallest positive integer which is the degree of some divisor of F. From XIII we see that the degree of every prime divisor, hence of every divisor of $F_K(\mathsf{Q})$ is divisible by n. On the other hand, there are prime divisors of degree n, namely $\mathfrak{q}_a$ with $a \in L^\times$ (e. g. $a = 1$). Hence:

Corollary XIIIa. *The function field* $F_K(\mathsf{Q})$ *is of index* n.

It seems noteworthy that the index n thus equals the order of the character invariant χ of $F_K(\mathsf{Q})$ which describes this field according to § 4.

An algebraic field extension K' of K splits $F_K(\mathsf{Q})$ if and only if it contains a K-isomorphic image of the residue class field belonging to some prime divisor $\mathfrak{q}_\alpha$. From XIII we conclude that this is so if and only if K' contains L. Hence we have a new proof of the following statement which is already contained in § 4:

Corollary XIIIb. *The field* L *is characterized as the minimal algebraic splitting field of* $F_K(\mathsf{Q})$.

Now we turn to the description of the divisor class group of degree 0 of $F_K(\mathsf{Q})$ which we denote by $C_K^0(\mathsf{Q})$.

Every divisor of $F_K(\mathsf{Q})$ which becomes principal when regarded as a divisor of $F_L(q)$ is already a principal divisor of $F_K(\mathsf{Q})$. This follows from the general theory of separable constant field extensions; an analytic proof will be obtained later as a side result. Hence the inclusion

$$D_K(\mathbf{Q}) \subset D_L(q)$$

induces an imbedding

$$C_K^0(\mathbf{Q}) \subset C_L^0(q)$$

of the corresponding divisor class groups. It follows that the Abel-Jacobi isomorphism

$$\Phi_q : C_L^0(q) \to L^\times/q$$

induces a *monomorphism* of $C_K^0(\mathbf{Q})$ into $L^\times/q$. To describe the group $C_K^0(\mathbf{Q})$, we ask for its image under Φ_q.

First, we note that the translation τ_Q acts trivially on $C_L^0(q)$. For, by the Riemann-Roch theorem, every $c \in C_L^0(q)$ can be written in the form

$$c \sim \mathfrak{p}_a - \mathfrak{p}_1$$

where $\sim$ means divisor equivalence; here $\mathfrak{p}_a$ is a prime divisor of degree 1 and hence $a \in L^\times$. We have by (64)

$$\tau_Q c \sim \mathfrak{p}_{Qa} - \mathfrak{p}_Q$$

hence

$$\Phi_q(\tau_Q c) \equiv \frac{Qa}{Q} \equiv a \equiv \Phi_q(c) \bmod^\times q$$

and therefore

$$\tau_Q c = c$$

in view of the Abel-Jacobi theorem V (§ 2).

According to § 2 (remark 2) we have therefore

$$\Phi_q(\tau_Q \sigma c) \equiv \Phi_q(\sigma c) \equiv \sigma \Phi_q(c) \bmod^\times q. \tag{65}$$

That is, the map

$$\Phi_q : C_L^0(q) \to L^\times/q$$

is $G_{\mathbf{Q}}$-permissible, if we let $\tau_Q \sigma$ act on $L^\times/q$ in the same way as σ acts on it.

It follows

$$\Phi_q(N_{\mathbf{Q}} c) \equiv N(\Phi_q c) \bmod^\times q. \tag{66}$$

Now, the norm map

$$N_{\mathbf{Q}} : C_L^0(q) \to C_K^0(\mathbf{Q})$$

is *surjective* since we know that every divisor of $F_K(\mathbf{Q})$ is an $N_{\mathbf{Q}}$-norm. From (66) we conclude therefore that the image of $C_K^0(\mathbf{Q})$ under Φ_q consists precisely of the norms. Hence:

XV. *(Abel-Jacobi theorem for semi-periodic functions): The group $C_K^0(\mathbf{Q})$ of divisor classes of degree 0 of $F_K(\mathbf{Q})$ is isomorphic to $NL^\times/q$, this isomorphism being induced by the Jacobi isomorphism Φ_q from $C_L^0(q)$ to $L^\times/q$.*

The group $C_K^0(q)$ is also contained in $C_L^0(q)$ and it is isomorphic, via Φ_q, to $K^\times/q$. Hence we obtain:

Corollary XVa. *$C_K^0(\mathbf{Q})$ is contained in $C_K^0(q)$, and the corresponding factor group is isomorphic to the norm factor group $K^\times/NL^\times$, this isomorphism being induced by Φ_q.*

Examples: Assume that the valuation of K is discrete. If the residue class field of K is algebraically closed then $K^\times = NL^\times$ (see [17], p. 98ff.) and hence $C_K^0(q) = C_K^0(\mathbf{Q})$. If the residue class field of K is finite then $K^\times/NL^\times$ is cyclic of order n, hence the same is true for $C_K^0(q)/C_K^0(\mathbf{Q})$. The same result holds if the residue class field of K is quasi-finite in the sense of Whaples' generalized local class field theory (see [17], p. 200ff.).

Now we are going to prove:

XVI. *(Norm theorem): Every $\mathbf{Q}$-semi-periodic function $0 \neq f \in F_K(\mathbf{Q})$ is the $N_{\mathbf{Q}}$-norm of some q-periodic function $g \in F_L(q)$.*

This statement can also be written as

$$H^0(G_{\mathbf{Q}}, F_L(q)^\times) = 0.$$

In the course of the proof we shall have to compute and to use various other cohomology groups of $G_{\mathbf{Q}}$; our results are contained in the following

List of cohomology groups

A	$H^0(G_{\mathbf{Q}}, A)$	$H^1(G_{\mathbf{Q}}, A)$
$D_L(q)$	0	0
$D_L^0(q)$	0	$\mathbf{Z}/n$
$C_L^0(q)$	$K^\times/NL^\times$	$\mathbf{Z}/n$
$P_L(q)$	0	$K^\times/NL^\times$
$F_L(q)^\times$	0	0

Here, $P_L(q)$ denotes the group of principal divisors of $F_L(q)$.

The last line contains our assertion of the norm theorem. Note that $G_{\mathbf{Q}}$ is cyclic, hence we have for every $G_{\mathbf{Q}}$-module A

$$H^k(G_{\mathbf{Q}}, A) \approx H^{k+2}(G_{\mathbf{Q}}, A) \qquad (k \in \mathbf{Z})$$

so that the list above gives a full cohomological description of the 5 modules in question.

Let us prove the assertions of this list by starting from the first line downwards. To simplify notations, we shall omit, in the course of these proofs, the index L and the bracket (q), so that we will write

$$D,\ D^0,\ C^0,\ P,\ F^\times.$$

The assertion

$$H^0(G_{\mathbf{Q}}, D) = 0$$

says that every $\mathbf{Q}$-semi-periodic divisor is an $N_{\mathbf{Q}}$-norm; this has been proved in XIV already. The assertion

$$H^1(G_{\mathbf{Q}}, D) = 0$$

is generally true for every function field; it is a consequence of the fact that D is the free abelian group generated by its prime divisors which are permuted under $G_{\mathbf{Q}}$ (see e.g. [15].) This shows the validity of the first line of the list, and also that D as a $G_{\mathbf{Q}}$-module is cohomologically trivial.

Now consider the exact sequence

$$(67) \qquad 0 \to D^0 \to D \to \mathbf{Z} \to 0$$

where $D \to \mathbf{Z}$ is the degree map. Since D is cohomologically trivial we conclude that the cohomological connecting operator yields isomorphisms

$$(68) \qquad \begin{aligned} 0 = H^{-1}(G_{\mathbf{Q}}, \mathbf{Z}) &\approx H^0(G_{\mathbf{Q}}, D^0) \\ \mathbf{Z}/n = H^0(G_{\mathbf{Q}}, \mathbf{Z}) &\approx H^1(G_{\mathbf{Q}}, D^0) \end{aligned}$$

which proves the second line of the list.

As to the third line, we use formula (65) which says that the Jacobi isomorphism

$$\Phi_q : C^0 \to L^\times/q$$

is $G_{\mathbf{Q}}$-permissible if we let $\tau_Q\sigma$ act on $L^\times/q$ in the same way as σ acts on it. Hence we have

$$(69) \qquad H^k(G_{\mathbf{Q}}, C^0) = H^k(G, L^\times/q)$$

where G is the group generated by σ.

The exact sequence

$$0 \to \mathbf{Z} \underset{q}{\to} L^\times \to L^\times/q \to 0$$

where the map denoted by q is the exponential map (51a), yields exactly

$$K^\times \to (L^\times/q)^G \to H^1(G, Z) = 0$$

which shows that $(L^\times/q)^G = K^\times/q$, hence

$$H^0(G, L^\times/q) = K^\times/N L^\times$$

since $q \in N L^\times$.

As to $H^1(G, L^\times/q)$, we have seen in Lemma 2 (§ 4) that this is isomorphic to $\hat{G}(q)$; since q is a norm from L and G is cyclic of order n, we have $\hat{G}(q) = \hat{G} \approx \mathbf{Z}/n$. This proves the third line of the list.

Now we show that

$$(70) \qquad H^0(G_{\mathbf{Q}}, P) = 0.$$

Let $\mathfrak{m} \in P$ be a principal divisor which is stable under $G_{\mathbf{Q}}$; we have to show that it is the norm of a principal divisor. In any case, we know from $H^0(G_{\mathbf{Q}}, D^0) = 0$ that $\mathfrak{m}$ is the norm of a divisor $\mathfrak{m}' \in D^0$:

$$\mathfrak{m} = N_{\mathbf{Q}}(\mathfrak{m}').$$

We try to change $\mathfrak{m}'$ by subtracting a divisor of the form

$$\tau_Q\sigma\mathfrak{u} - \mathfrak{u} \qquad (\mathfrak{u} \in D),$$

this will not effect the above norm property of $\mathfrak{m}'$; the divisor $\mathfrak{u}$ should be chosen in such a way that

$$\mathfrak{m}'' = \mathfrak{m}' - (\tau_Q\sigma\mathfrak{u} - \mathfrak{u})$$

is principal. By the Abel-Jacobi theorem, this condition means that

$$\Phi_q(\tau_Q\sigma\mathfrak{u} - \mathfrak{u}) \equiv a' \bmod^\times q$$

where a' is in $L^\times$ such that

$$a' \equiv \Phi_q(\mathfrak{m}') \bmod^\times q.$$

From (66) we infer that

$$N a' \equiv \Phi_q(\mathfrak{m}) \equiv 1 \bmod^\times q$$

since $\mathfrak{m}$ is principal[1]). This means $N a' = q^k = N\, Q^k$ for some integer k, hence

$$a' = Q^k \cdot \frac{\sigma b}{b}$$

with $b \in L^\times$ (by Hilberts theorem 90). Our condition for $\mathfrak{u}$ now reads:

$$\Phi_q(\tau_Q \sigma \mathfrak{u} - \mathfrak{u}) \equiv Q^k \cdot \frac{\sigma b}{b} \bmod^\times q.$$

Accordingly, we put

$$\mathfrak{u} = k \cdot \mathfrak{v} + \mathfrak{w}$$

and look for divisors $\mathfrak{v}$, $\mathfrak{w}$ such that

$$\Phi_q(\tau_Q \sigma \mathfrak{v} - \mathfrak{v}) \equiv Q \bmod^\times q$$

$$\Phi_q(\tau_Q \sigma \mathfrak{w} - \mathfrak{w}) \equiv \frac{\sigma b}{b} \bmod^\times q$$

The first condition is satisfied by $\mathfrak{v} = \mathfrak{p}_1$ since $\tau_Q \sigma \mathfrak{p}_1 = \mathfrak{p}_Q$ and $\Phi_q(\mathfrak{p}_Q - \mathfrak{p}_1) \equiv Q \bmod^\times q$. The second condition is satisfied by $\mathfrak{w} = \mathfrak{p}_b - \mathfrak{p}_1$ in view of (65).

This proves (70)[2]).

Now, the exact sequence

(70a) $$0 \to P \to D^0 \to C^0 \to 0$$

yields a cohomology sequence

$$0 \to H^0(G_{\mathbf{Q}}, C^0) \to H^1(G_{\mathbf{Q}}, P) \to H^1(G_{\mathbf{Q}}, D^0) \to H^1(G_{\mathbf{Q}}, C^0) \to 0$$

since $H^2(G_{\mathbf{Q}}, P) = H^0(G_{\mathbf{Q}}, P) = 0$. The last two groups in this sequence are both isomorphic to $\mathbf{Z}/n$ according to line 2 and 3 of the list; hence the map between them is necessarily an isomorphism and it follows that

$$H^0(G_{\mathbf{Q}}, C^0) \to H^1(G_{\mathbf{Q}}, P)$$

is an isomorphism too. This proves the fourth line of the list.

---

1) Here we use only the fact that $\mathfrak{m}$ becomes principal as a divisor of $F_L(q)$ which already implies that $\Phi_q(\mathfrak{m}) \equiv 1 \bmod^\times q$. Accordingly, our proof yields the following: Every divisor $\mathfrak{m}$ of $D_K(\mathbf{Q})$ which becomes principal in $D_L(q)$ is already principal in $D_K(\mathbf{Q})$ (being the norm of a principal divisor). We have used this result already in the proof of XV.

2) What we have shown in effect is that the map

$$H^{-1}(G_{\mathbf{Q}}, D^0) \to H^{-1}(G_{\mathbf{Q}}, C^0)$$

is epimorphic; this yields (70) in view of the exact sequence (70a) and the triviality of $H^0(G_{\mathbf{Q}}, D^0)$.

As to the last line, the assertion $H^1(G_{\mathbf{Q}}, F^\times) = 0$ is simply Hilberts theorem 90. So we are left with the proof of $H^0(G_{\mathbf{Q}}, F^\times) = 0$ which is in fact the assertion of the norm theorem.

Let $f \in F^\times$ be fixed under $G_{\mathbf{Q}}$. We know already that its principal divisor (f) is the norm of a principal divisor (f'). Hence

$$f = a N_{\mathbf{Q}} f'$$

with a certain constant $a \in K^\times$; it remains to prove that every $a \in K^\times$ is an $N_{\mathbf{Q}}$-norm from $F^\times$.

Consider the meromorphic function

$$g = \frac{\Theta_Q \Theta_a}{\Theta_1 \Theta_{Qa}}$$

where Θ_a is as in § 2. This function is defined over L. Since

$$\tau_q \Theta_a = a^{-1}(-X)\Theta_a$$

we see that

$$\tau_q g = g,$$

i. e.

$$g \in F^\times.$$

Since $a \in K^\times$ is fixed under σ, we may write

$$g = \frac{\tau_Q \sigma \Theta_1}{\Theta_1} \left(\frac{\tau_Q \sigma \Theta_a}{\Theta_a}\right)^{-1}$$

and from (61) we infer that

$$N_{\mathbf{Q}}\left(\frac{\tau_Q \sigma \Theta_a}{\Theta_a}\right) = \frac{\tau_q \Theta_a}{\Theta_a} = a^{-1}(-X)$$

which gives

$$N_{\mathbf{Q}}(g) = \frac{-X}{a^{-1}(-X)} = a\text{ [1]}).$$

QED.

---

1) What we have shown in effect is that the map

$$H^0(G_{\mathbf{Q}}, L^\times) \to H^0(G_{\mathbf{Q}}, F^\times)$$

is the zero map; hence the exact sequence

$$0 \to L^\times \to F^\times \to P \to 0$$

yields

$$0 \to H^0(G_{\mathbf{Q}}, F^\times) \to H^0(G_{\mathbf{Q}}, P)$$

which shows $H^0(G_{\mathbf{Q}}, F^\times) = 0$ in view of the fourth line of the list.

Let us interpret the norm theorem XVI in terms of Brauer groups. For any field K, let $\mathrm{Br}(K)$ denote the Brauer group of K, defined as the group of similarity classes of finite dimensional simple central algebras over K. If L is any overfield of K, we have a natural map $\mathrm{Br}(K) \to \mathrm{Br}(L)$ which associates to every algebra A over K its tensor product $A \underset{K}{\otimes} L$ which is an algebra over L. The kernel of this map is denoted by $\mathrm{Br}(L|K)$; its consists of those algebra classes in $\mathrm{Br}(K)$ which are split by the field L. Thus we have an exact sequence

$$0 \to \mathrm{Br}(L|K) \to \mathrm{Br}(K) \to \mathrm{Br}(L).$$

If $L|K$ is a Galois extension with group G then we have a natural isomorphism

$$\mathrm{Br}(L|K) = H^2(G, L^\times)$$

which is obtained via the theory of crossed products. If in addition $L|K$ is cyclic we have

$$H^2(G, L^\times) = H^0(G, L^\times) = K^\times/NL^\times.$$

Thus the fact that every element in K is a norm from L is equivalent to the fact that the map $\mathrm{Br}(K) \to \mathrm{Br}(L)$ is an injection. We have therefore:

Corollary XVIa. *The natural map* $\mathrm{Br}(F_K(\mathsf{Q})) \to \mathrm{Br}(F_L(q))$ *is injective.*

Now let us consider the commutative diagram

$$\begin{array}{ccc} F_K(\mathsf{Q}) & \to & F_L(q) \\ \uparrow & & \uparrow \\ K & \to & L \end{array}$$

where the maps denote field inclusions. It induces a commutative diagram

$$\begin{array}{ccccc} & & \mathrm{Br}(F_K(\mathsf{Q})) & \to & \mathrm{Br}(F_L(q)) \\ & & \uparrow & & \uparrow \\ 0 \to \mathrm{Br}(L|K) & \to & \mathrm{Br}(K) & \to & \mathrm{Br}(L) \end{array}$$

We know that the upper horizontal map is injective. On the other hand, the right vertical map is injective since $F_L(q)$ has a prime divisor of degree 1 over L (see [15]). It follows that

$$0 \to \mathrm{Br}(L|K) \to \mathrm{Br}(K) \to \mathrm{Br}(F_K(\mathsf{Q}))$$

is exact. Hence:

Corollary XVIb. *An algebra in* $\mathrm{Br}(K)$ *is split by* $F_K(\mathsf{Q})$ *if and only if it is split by* L.

If K is locally compact, local class field theory shows that $\mathrm{Br}(L|K)$ is cyclic of order n; it follows that the group of algebras in $\mathrm{Br}(K)$ which is split by $F_K(\mathsf{Q})$ is cyclic, its order being the index of $F_K(\mathsf{Q})$. This result has been proved, for arbitrary function fields over locally compact fields, in our earlier paper [16].

§ 6. Elliptic subfields and isogenies

We are going to determine the elliptic subfields of the fields of periodic and semi-periodic functions.

We begin with the field $F_K(q)$ of periodic functions. First, we shall exhibit a series of elliptic subfields of $F_K(q)$ and establish their relevant properties. Then we shall prove that our construction yields *all* elliptic subfields of $F_K(q)$.

An element $\bar{q} \in K^\times$ with $0 < |\bar{q}| < 1$ is called *commensurable* with q if there exist integers $d, m \neq 0$ such that

$$\bar{q}^d = q^m. \tag{71}$$

This condition means that $\bar{q}$ has finite order $\bmod^\times q$.

Assume that $\bar{q}$ is commensurable with q and let us fix a pair of integers $d, m \neq 0$ satisfying (71). Consider the map

$$\mu_m : \bar{f}(X) \to \bar{f}(X^m) \qquad (\bar{f} \in F_K(\bar{q})).$$

This is a K-isomorphism of $F_K(\bar{q})$ into the field of meromorphic functions. Its image field is contained in $F_K(q)$. For, every $\bar{f} \in F_K(\bar{q})$ satisfies the functional equation

$$\bar{f}(q^{-m}X) = \bar{f}(X)$$

since q^m is a power of $\bar{q}$. Substituting $X \to X^m$ we obtain

$$\bar{f}(q^{-m}X^m) = \bar{f}(X^m)$$

which says that $\bar{f}(X^m)$ is stable under the translation $X \to q^{-1}X$. That is, $\bar{f}(X^m) \in F_K(q)$.

It will be convenient to use the notation $F_K(q\,|\,X)$ instead of $F_K(q)$ in order to indicate the variable X by which the functions $f(X) \in F_K(q|X)$ are defined[1]).

Then the image field of μ_m is to be denoted by $F_K(\bar{q}\,|\,X^m)$ and *we have proved that*

$$F_K(\bar{q}\,|\,X^m) \subset F_K(q\,|\,X) \tag{72}$$

whenever $\bar{q}$ is commensurable with q and $m \neq 0$ is divisible by the order of q $\bmod^{\times} \bar{q}$.

We have

$$\mu_{-m} = \mu_m \varepsilon \tag{73}$$

where

$$\varepsilon : \bar{f}(X) \to \bar{f}(X^{-1})$$

is the reflection automorphism of $F_K(\bar{q}\,|\,X)$ as defined in § 3. This shows that

$$F_K(\bar{q}\,|\,X^{-m}) = F_K(\bar{q}\,|\,X^m).$$

Hence, in order to study the elliptic fields $F_K(\bar{q}\,|\,X^m)$ we may assume $m > 0$.

XVII. *Let $\bar{q}$ be commensurable with q and let $m > 0$ be a multiple of the order of q $\bmod^{\times} \bar{q}$. Then:*

(i) *The degree of $F_K(q\,|\,X)$ over $F_K(\bar{q}\,|\,X^m)$ is dm, where $d > 0$ is determined by the equation* (71).

(ii) *The degree of inseparability of $F_K(q\,|\,X)$ over $F_K(\bar{q}\,|\,X^m)$ equals the largest power p^r of the characteristic p of K which divides m*[2]). *The maximal separable intermediate field is $F_K(q^{p^r}\,|\,X^{p^r})$.*

(iii) *The automorphism group of $F_K(q\,|\,X)$ over $F_K(\bar{q}\,|\,X^m)$ is isomorphic to the factor group U/q where $U \subset K^{\times}$ consists of all elements $u \in K^{\times}$ with $u^m \equiv 1 \bmod^{\times} \bar{q}$. More precisely, the automorphisms of $F_K(q\,|\,X)$ over $F_K(\bar{q}\,|\,X^m)$ are the translations τ_u with $u \in U$.*

(iv) *The field extension $F_K(q\,|\,X)$ over $F_K(\bar{q}\,|\,X^m)$ is Galois if and only if the following conditions are satisfied:*

$m \not\equiv 0 \bmod p$;
K contains the m-th roots of unity;
$\bar{q}$ is an m-th power in K.

---

[1]) Similarly, $M_K(X)$ now denotes the field of meromorphic functions over K in the variable X.

[2]) If char $(K) = 0$ then we put $p = p^r = 1$.

Proof.

(i) From (72) it follows

$$F_K(\bar{q}\,|\,X^m) \subset F_K(q^m\,|\,X^m) \subset F_K(q\,|\,X). \tag{74}$$

We show that the lower extension has degree d while the upper extension has degree m.

By means of the map $X \to X^m$, the lower extension is isomorphic to the extension

$$F_K(\bar{q}\,|\,X) \subset F_K(q^m\,|\,X). \tag{75}$$

Consider the translation

$$\tau_{\bar{q}} : f(X) \to f(\bar{q}^{-1}X)$$

which, by definition, has $F_K(\bar{q}\,|\,X)$ as its field of fixed elements. As an automorphism of $F_K(q^m\,|\,X)$ the translation $\tau_{\bar{q}}$ has order d since $\bar{q}$ has order d $\bmod^{\times} q^m$ in view of (71). From Galois theory we conclude therefore that

(76) *the extension* (75) *is cyclic of degree d.*

Now we consider the upper extension (74); we shall exhibit explicitely a basis of m elements.

The theta function $\Theta(X)$ defined in § 2 will now be denoted by $\Theta(q\,|\,X)$ in order to indicate the period q by which it is defined. From formula (9) in § 2 we conclude that the functions

$$u_i(q\,|\,X) = X^{-i}\frac{\Theta(q^m\,|\,q^{-i}X^m)}{\Theta(q^m\,|\,X^m)} \qquad (0 \leq i < m) \tag{77}$$

satisfy the functional equation

$$u_i(q\,|\,q^{-1}X) = q^i \frac{-q^{-i}X^m}{-X^m} u_i(q\,|\,X) = u_i(q\,|\,X).$$

That is,

$$u_i(q\,|\,X) \in F_K(q\,|\,X).$$

On the other hand, the u_i form a basis of $M_K(X)$ over $M_K(X^m)$. For, they are obtained from the X^{-i} by multiplication with elements in $M_K(X^m)$, and the X^{-i} $(0 \leq i < m)$ obviously form a basis of $H_K(X)$ over $H_K(X^m)$, hence also of $M_K(X)$ over $M_K(X^m)$.

It follows: every function $f(X) \in M_K(X)$ admits a *unique* representation

$$f(X) = \sum_{0 \leq i < m} f_i(X^m)\, u_i(q \mid X)$$

with coefficients $f_i(X^m) \in M_K(X^m)$. We obtain:

$$f(q^{-1}X) = \sum_{0 \leq i < m} f_i(q^{-m} X^m)\, u_i(q \mid X)$$

and conclude: $f(X) \in F_K(q \mid X)$ if and only if all the coefficients $f_i(X^m) \in F_K(q^m \mid X^m)$. This means that the m functions $u_i(q \mid X)$ indeed form a basis of $F_K(q \mid X)$ over $F_K(q^m \mid X^m)$.

At the same time we have seen that

$$M_K(X^m) \cap F_K(q \mid X) = F_K(q^m \mid X^m). \tag{78}$$

(ii) From (77) we see that the m-th powers of the basic functions $u_i(q \mid X)$ are functions of X^m, hence they are contained in $F_K(q^m \mid X^m)$ in view of (78). Therefore, if $m \not\equiv 0 \bmod p$ we conclude that $F_K(q \mid X)$ is separable over $F_K(q^m \mid X^m)$ while if $m = p^r$ then it is purely inseparable. In general, we infer from (72) that

$$F_K(q^m \mid X^m) \subset F_K(q^{p^r} \mid X^{p^r}) \subset F_K(q \mid X)$$

and from what we have said above, the upper extension is purely inseparable of degree p^r while the lower extension is separable of degree m/p^r. As to the extension

$$F_K(\bar{q} \mid X^m) \subset F_K(q^m \mid X^m),$$

this is separable in view of (76).

(iii) If $u \in U$ then u^m is a power of $\bar{q}$, hence

$$\bar{f}(u^{-m} X^m) = \bar{f}(X^m)$$

if $\bar{f}(X^m) \in F_K(\bar{q} \mid X^m)$. It follows that $\tau_u : X \to u^{-1}X$ leaves the functions in $F_K(\bar{q} \mid X^m)$ fixed. It remains to show that every automorphism of $F_K(q \mid X)$ over $F_K(\bar{q} \mid X^m)$ is such a translation τ_u.

First, assume that K contains the group W_m of m-th roots of unity and also an m-th root $\tilde{q}$ of $\bar{q}$. Then

$$U = \langle \tilde{q} \rangle \times W_m$$

where $\langle \tilde{q} \rangle$ denotes the infinite cyclic group generated by $\tilde{q}$. From (71) it follows

$$q = \tilde{q}^d w$$

with $w \in W_m$. Since W_m has the order m/p^r it follows that U/q has order dm/p^r; this is therefore the order of the group of translations τ_u with $u \in U$. On the other hand, it follows from (i) and (ii) that dm/p^r is the separability degree of $F_K(q \mid X)$ over $F_K(\bar{q} \mid X^m)$. From Galois theory, we conclude that the τ_u with $u \in U$ form the *whole* group of automorphisms of $F_K(q \mid X)$ over $F_K(\bar{q} \mid X^m)$.

In general, let L be a finite algebraic extension of K containing the m-th roots of unity and an m-th root of $\bar{q}$. Every automorphism of $F_K(q \mid X)$ over $F_K(\bar{q} \mid X^m)$ extends uniquely to an automorphism of $F_L(q \mid X)$ over $F_L(\bar{q} \mid X^m)$ and hence is a translation τ_v where $v \in L^\times$ is such that $v^m \equiv 1 \bmod^\times \bar{q}$. From (77) we infer that

$$u_i(q \mid v^{-1}X) = v^i X^{-i} \frac{\Theta(q^m \mid v^{-m} q^{-i} X^m)}{\Theta(q^m \mid v^{-m} X^m)}\,.$$

The left hand side is contained in $F_K(q \mid X)$ since τ_v extends an automorphism of $F_K(q \mid X)$. On the other hand, since v^m is a power of $\bar{q}$, the quotient of theta functions on the right hand side is a meromorphic function defined over K. It follows that $v^i \in K$; taking $i = 1$ we see that $v \in K$, i. e. $v \in U$.

(iv) The condition $m \not\equiv 0 \bmod p$ means that $F_K(q \mid X)$ is separable over $F_K(\bar{q} \mid X^m)$ in view of (ii). Assume this to be the case. Then $F_K(q \mid X)$ is a Galois extension of $F_K(\bar{q} \mid X^m)$ if and only if the order of U/q equals the degree dm; this follows from (iii). From (71), this condition is equivalent to the condition that $U/\bar{q}$ should have order m^2. By definition of U, this means that $\bar{q}$ is an m-th power in K and that the m-th roots of unity are in K. QED.

XVIII. *Every elliptic subfield E of $F_K(q \mid X)$ is of the form $E = F_K(\bar{q} \mid X^m)$ where $\bar{q}$ is commensurable with q and $m > 0$ is a multiple of the order of $q \bmod^\times \bar{q}$. Here, $\bar{q}$ is uniquely determined as the period of E while m is determined as the largest integer such that every function in E can be written as a function in X^m.*

Proof. Let p^r denote the degree of inseparability of $F_K(q \mid X)$ over E and let $E' \mid E$ be the maximal separable subextension. Then $F_K(q \mid X)$ is purely inseparable of degree p^r over E'. On the other hand, $F_K(q \mid X)$ is separably generated over K and hence it contains only one subfield over which it is purely inseparable of degree p^r. From XVII (ii) we conclude therefore

$$E' = F_K(q^{p^r} \mid X^{p^r}).$$

After replacing $F_K(q\,|\,X)$ by $F_K(q^{p^r}\,|\,X^{p^r})$ we may therefore assume that $F_K(q\,|\,X)$ is separable over E.

Consider the algebraic closure Ω of K and the corresponding constant field extensions $F_\Omega(q\,|\,X)$ and $E\Omega$. From the general algebraic theory of elliptic function fields we now use the fact that $F_\Omega(q\,|\,X)$, being separable over its elliptic subfield $E\Omega$, is a Galois extension of $E\Omega$, the Galois group consisting of translations (see e. g. [4], p. 206). Accordingly, let $V \subset \Omega^\times$ be the subgroup containing q such that V/q is isomorphic, by means of $v \to \tau_v$, to the Galois group of $F_\Omega(q\,|\,X)$ over $E\Omega$. Then V/q is finite; hence V is a finitely generated abelian group of rank one and therefore is of the form

$$V = \langle \tilde{q} \rangle \times W_m$$

where $\tilde{q} \in \Omega^\times$ is of infinite order and W_m is the group of roots of unity contained in V, of order m. Since $q \in V$ we have

$$q = \tilde{q}^d w$$

with $w \in W_m$ and $0 \neq d \in \mathbf{Z}$; after replacing $\tilde{q}$ by $\tilde{q}^{-1}$ if necessary we may assume $d > 0$ which implies $0 < |\tilde{q}| < 1$. If we put

$$\overline{q} = \tilde{q}^m$$

then we have

$$q^m = \overline{q}^d$$

which shows that $\overline{q}$ is commensurable with q and that $m > 0$ is a multiple of the order of $q \bmod^\times \overline{q}$.

Let L be a finite algebraic extension of K containing V. Then the translations τ_v $(v \in V)$ are defined over L and their field of fixed elements, within $F_L(q\,|\,X)$, is EL.

On the other hand, we have $\overline{q} \in L$ and hence $F_L(\overline{q}\,|\,X^m)$ is defined. According to XVII (iv), the field $F_L(q\,|\,X)$ is a Galois extension of $F_L(\overline{q}\,|\,X^m)$, the Galois group consisting of the translations τ_v with $v \in V$. We conclude:

$$EL = F_L(\overline{q}\,|\,X^m). \tag{79}$$

In particular, the absolute invariant j_E of E equals the absolute invariant $j(\overline{q})$ of $F_L(\overline{q}\,|\,X^m)$. Since $j_E \in K$ we have therefore $j(\overline{q}) \in K$; from VII (§ 3) we conclude that $\overline{q} \in K$. Hence $F_K(\overline{q}\,|\,X^m)$ is defined and it is a subfield of $F_K(q\,|\,X)$. Intersecting both sides of (79) with $F_K(q\,|\,X)$, we obtain

$$E = F_K(\overline{q}\,|\,X^m).$$

In particular, E is K-isomorphic to $F_K(\overline{q}\,|\,X)$ which shows that $\overline{q}$ is uniquely determined as the period of E (cf. VII, § 3). It remains to prove the uniqueness assertion with respect to m.

So let $k > 0$ be any integer such that $E \subset M_K(X^k)$. From (78) it follows that

$$E \subset F_K(q^k\,|\,X^k) \subset F_K(q\,|\,X).$$

The upper extension has degree k by XVII (i). Hence k is bounded by the degree of $F_K(q\,|\,X)$ over E. Also it is immediate that

$$M_K(X^k) \cap M_K(X^m) = M_K(X^t) \quad \text{where} \quad t = \operatorname{lcm}(k, m).$$

Hence, if k is the *largest* integer such that E is contained in $M_K(X^k)$ then $m\,|\,k$ and

$$E \subset F_K(q^k\,|\,X^k) \subset F_K(q^m\,|\,X^m).$$

We have to show that $k = m$.

We have proved in (76) that $F_K(q^m\,|\,X^m)$ is a cyclic extension of $E = F_K(\overline{q}\,|\,X^m)$ of degree d. Therefore, $F_K(q^k\,|\,X^k)$ is the *unique* intermediate field over which $F_K(q^m\,|\,X^m)$ has degree $\frac{k}{m}$. On the other hand, it follows from (72) and from XVII (i) that

$$F_K(\overline{q}^{\frac{dm}{k}}\,|\,X^m)$$

is another such intermediate field. It follows:

$$F_K(q^k\,|\,X^k) = F_K(\overline{q}^{\frac{dm}{k}}\,|\,X^m)$$

and therefore

$$q^k = \overline{q}^{\frac{dm}{k}} = q^{\frac{m^2}{k}}$$

hence

$$k = \frac{m^2}{k}, \quad k = m.$$

QED.

If $E\,|\,K$ and $F\,|\,K$ are elliptic function fields then an *isogeny* from E to F is defined to be a K-isomorphism μ from E into F; the field degree $[F : \mu E]$ is called the *degree* of μ. If $F = F_K(q)$ then we conclude from XVIII that such an isogeny exists if and only if E is K-isomorphic to $F_K(\bar{q})$ where $\bar{q} \in K^\times$ is commensurable with q. If this is so, i. e. if $E = F_K(\bar{q})$, then the image of any isogeny $\mu : E \to F$ is a field $F_K(\bar{q} \,|\, X^m)$ with $m > 0$ being divisible by the order of $q \bmod^\times \bar{q}$. Hence μ has the same image field as the isogeny μ_m defined by $X \to X^m$. Therefore, $\mu = \mu_m \lambda$ with λ an automorphism of E. If λ is not a translation, then $\lambda = \varepsilon\tau$ where τ is a translation and ε is the reflection automorphism of E, given by $X \to X^{-1}$. (See formula (61) of the appendix.) We have $\mu_m \varepsilon = \mu_{-m}$ according to (73). Hence:

Corollary XVIIIa. *If $E|K$ is any elliptic function field then there exists an isogeny from E to $F_K(q)$ if and only if E is K-isomorphic to $F_K(\bar{q})$ with $\bar{q}$ being commensurable to q.*

If $\bar{q}$ is commensurable with q, then for every integer $m \neq 0$ divisible by the order of $q \bmod^\times \bar{q}$ there exists an isogeny $\mu_m : F_K(\bar{q}) \to F_K(q)$ which is given by $X \to X^m$. The degree of μ_m is dm where d is determined from the equation (71). Every isogeny from $F_K(\bar{q})$ to $F_K(q)$ is of the form $\mu_m \tau$ with m as above, where τ is a translation of $F_K(\bar{q})$.

Every isogeny $\mu : E \to F$ defines by transposition a map $\mu^* : D(F) \to D(E)$ of the respective divisor groups. Explicitely, μ^* is given by the formula

$$\mu^*(\mathfrak{m}) = \mu^{-1} N_\mu(\mathfrak{m}) \qquad (\mathfrak{m} \in D(F))$$

where N_μ stands for the norm operator from F to the image field μE. If $\mathfrak{p}$ is a prime divisor of degree 1 of $F|K$ then $N_\mu(\mathfrak{p})$ is the prime divisor of degree 1 of μE which is induced by $\mathfrak{p}$; thus $\mu^*\mathfrak{p}$ is given by the formula

$$\bar{f}(\mu^*\mathfrak{p}) = (\mu\bar{f})(\mathfrak{p}) \qquad (\bar{f} \in E). \tag{80}$$

The divisor map $\mu^* : D(F) \to D(E)$ preserves the degree of divisors and maps principal divisors onto principal divisors; hence it defines a map

$$\mu^* : C^0(F) \to C^0(E)$$

of the respective divisor class groups of degree 0. This latter map is called the *multiplicator* from $C^0(F)$ to $C^0(E)$ defined by μ.

If $F = F_K(q)$ and $E = F_K(\bar{q})$ with $\bar{q}$ commensurable to q then every multiplicator from $C^0_K(q)$ to $C^0_K(\bar{q})$ is of the form μ_m^* with m as in the above corollary; this is because translations act trivially on

the divisor class group of degree 0. Applying the Jacobian isomorphisms

$$\Phi_q : C^0_K(q) \approx K^\times/q, \quad \Phi_{\bar{q}} : C^0_K(\bar{q}) \approx K^\times/\bar{q}$$

we may regard μ_m^* as a map

$$\mu_m^* : K^\times/q \to K^\times/\bar{q}.$$

As such it can be described as the m-th *power map*

$$\mu_m^*(a) \equiv a^m \bmod^\times \bar{q} \qquad (a \in K^\times \bmod^\times q). \tag{81}$$

To see this, let $a \equiv \Phi_q(c) \bmod^\times q$ with $c \in C^0_K(q)$. Then $c \sim \mathfrak{p}_a - \mathfrak{p}_1$ where $\mathfrak{p}_a, \mathfrak{p}_1$ are prime divisors of degree 1 of $F_K(q)$. Accordingly, if $\mu^*\mathfrak{p}_a = \bar{\mathfrak{p}}_b$[1]) then (80) yields

$$\bar{f}(b) = (\mu_m\bar{f})(a) = \bar{f}(a^m) \qquad (\bar{f} \in F_K(\bar{q})).$$

Hence

$$b \equiv a^m \bmod^\times \bar{q}.$$

It follows

$$\begin{aligned} \mu_m^*(\mathfrak{p}_a) &= \bar{\mathfrak{p}}_{a^m} \\ \mu_m^*(c) &\sim \bar{\mathfrak{p}}_{a^m} - \bar{\mathfrak{p}}_1 \\ \Phi_{\bar{q}}(\mu_m^* c) &\equiv a^m \bmod^\times \bar{q} \end{aligned}$$

which is our contention (81).

Let us apply these considerations to the case $\bar{q} = q$. The multiplicators of $C^0_K(q)$ are then given by $a \to a^m$ $(m \neq 0)$ or, what means the same, by $c \to mc$ $(c \in C^0_K(q))$. That is, they are the *natural multiplicators* of the abelian group $C^0_K(q)$. Here, m ranges over the integers $\neq 0$. Thus the ring $\mathsf{M}_K(q)$ generated by the multiplicators is equal to $\mathbf{Z}$, when considered as natural multiplicators of $C^0_K(q)$.

This statement remains true if we replace K by any finite algebraic field extension L of K.

In general, if $F|K$ is any elliptic function field, the multiplicators of $C^0(F|K)$ generate a ring which is denoted by $\mathsf{M}(F|K)$ and called the *ring of multiplicators* of $F|K$. If $FL|L$ is any constant field extension of $F|K$ then we have a natural imbedding $\mathsf{M}(F|K) \subset \mathsf{M}(FL|L)$; the union of the rings $\mathsf{M}(FL|L)$ is denoted by $\mathsf{M}(F)$ and called the ring of multiplicators of F. It is already the union of the $\mathsf{M}(FL|L)$ where L ranges over the finite algebraic extensions of K.

[1]) $\bar{\mathfrak{p}}_b$ denotes the prime of $F_K(\bar{q})$ belonging to $b \in K^\times$ in the sense of § 2.

If $\mathsf{M}(F) = \mathbf{Z}$ then F is said to have no complex multiplication. We can therefore say:

Corollary XVIIIb. *The field $F_K(q)$ does not have complex multiplication.*

As a consequence, we can prove the following statement:

Let K be an arbitrary field (not necessarily local) and $F|K$ be an elliptic function field over K. If $F|K$ has complex multiplication then its absolute invariant j is absolutely integral; that is, j is a zero of a polynomial whose coefficients are integral multiples of $1 \in K$ and whose highest coefficient is 1.

Proof. Let K_0 be the prime field of K. If j is not absolutely integral then either j is transcendental over K_0 or char $(K) = 0$ and j is an algebraic but not an integral number; in any case, there exists a non-archimedean, discrete valuation of $K_0(j)$ such that $|j| > 1$. This valuation can be extended to a real valued valuation of K. Now note that, in order to show that F has no complex multiplication, we may extend K arbitrarily and replace F by the corresponding constant field extension. After replacing K by its completion with respect to the above valuation we may therefore assume that K is complete. Again, after replacing K by its algebraic closure and then by the completion of it we may assume that K is complete and algebraically closed. Now, since $|j| > 1$, it follows from VIIIa in § 3 that $F = F_K(q)$ for some $q \in K$; hence F has no complex multiplication according to corollary XVIIIb.

QED.

The above statement is of course well known from the general theory of complex multiplication. Our aim was to show that it is an immediate consequence of our general and elementary theory of periodic functions.

Now we turn to the fields of semi-periodic functions. If F is such a field, recall that F is described by its period q and its character invariant χ, according to § 4.

XIX. *Let $F|K$ be an elliptic function field admitting the period q, and let χ denote its character invariant.*

(i) *Every elliptic subfield E of F admits a period $\bar{q} \in K$, and $\bar{q}$ is commensurable with q.*

(ii) *Let $\bar{q} \in K$ with $0 < |\bar{q}| < 1$ be an arbitrary element which is commensurable with q. The elliptic subfields $E \subset F$ with $\bar{q}$ as their period correspond $1 - 1$ to the integers $m > 0$ which are divisible by the order of $q \bmod^{\times} \bar{q}$.*

If E belongs to m in this correspondence, then $[F : E] = dm$ where d is determined from

$$q^m = \bar{q}^d. \tag{81a}$$

The character invariant $\bar{\chi}$ of E is given by

$$\bar{\chi} = \chi^d.$$

The integer m is characterized by the property that E is contained in an elliptic subfield $E' \subset F$ admitting the period q^m, and that m is maximal with this property.

Proof. From XI (§ 4) we know that F is K-isomorphic to a field of semi-periodic functions; we may identify F with such a field. That is, if $L = K_\chi$ is the minimal algebraic splitting field of F, if σ is the generating automorphism of $L|K$ defined by

$$\chi(\sigma) = \exp\left(\frac{2\pi i}{n}\right), \quad n = [L : K], \tag{82}$$

and if $Q \in L$ is a suitable element with

$$N_{L|K}(Q) = q$$

then F is identified with the field of fixed elements in $F_L(q)$ of the automorphism $\tau_Q \sigma$. The constant field extension FL equals $F_L(q)$.

The constant field extension EL is an elliptic subfield of $F_L(q)$. From XVIII (applied to L) we conclude that

$$EL = F_L(\bar{q}\,|\,X^m) \tag{83}$$

where $\bar{q}$ is commensurable with q and $m > 0$ divisible by the order of $q \bmod^{\times} \bar{q}$. In particular, we see that EL admits the period $\bar{q}$. Hence the absolute invariant $j_E = j(\bar{q})$. Since $j_E \in K$ we conclude from § 3 that $\bar{q} \in K$.

It follows that σ induces in $F_L(\bar{q}\,|\,X^m)$ an automorphism, its field of fixed elements being $F_K(\bar{q}\,|\,X^m)$. On the other hand, τ_Q induces in $F_L(\bar{q}\,|\,X^m)$ an automorphism, and this is given by $X^m \to Q^{-m} X^m$. For clarity, we write $Y = X^m$, and see that the automorphism induced by

τ_Q in $F_L(\bar{q}|Y)$ is the translation τ_{Q^m} (with respect to the variable Y). The field of fixed elements of $\tau_{Q^m}\sigma$ in $F_L(\bar{q}|Y)$ is

$$F_L(\bar{q}|Y) \cap F = EL \cap F = E.$$

The characteristic cocycle (in the sense of § 4) of the field E is therefore given by

$$\xi : \sigma \to \tau_{Q^m} \tag{84}$$

Since τ_{Q^m} is a translation, it follows that E admits $F_K(\bar{q}|Y)$ as its Jacobian function field; that is, E has the period $\bar{q}$. This proves (i).

Conversely, let $\bar{q}$ as in (ii) and let $m > 0$ be divisible by the order of $q \bmod^\times \bar{q}$. Then $F_L(\bar{q}|X^m)$ is a subfield of $F_L(q|X)$; let E denote the field of fixed elements in $F_L(\bar{q}|X^m)$ of the automorphism induced by $\tau_Q\sigma$. Then $E \subset F$ and $EL = F_L(\bar{q}|X^m)$; as above it follows that E admits the period $\bar{q}$. We have

$$[F : E] = [FL : EL] = [F_L(q|X) : F_L(\bar{q}|X^m)] = dm$$

according to XVII (i). The character invariant $\bar{\chi}$ of E is obtained by the procedure explained in § 4: First we have to regard the characteristic cocycle ξ of E as a map from the Galois group of $L|K$ to $K^\times/\bar{q}$; in view of (84) this gives

$$\xi(\sigma) \equiv Q^m \bmod^\times \bar{q}. \tag{85}$$

Secondly, we have to apply the map $e_{\bar{q}} : K^\times/\bar{q} \to \mathbf{W}$ defined by formula (50) § 4; this gives the character invariant $\bar{\chi} = e_{\bar{q}}\xi$ and from (85) we obtain

$$\bar{\chi}(\sigma) = \exp\left(2\pi i \frac{\log|Q|^m}{\log|\bar{q}|}\right).$$

Using (81a) and the fact that $|Q|^n = |q|$ we see that

$$\bar{\chi}(\sigma) = \exp\left(2\pi i \frac{d}{n}\right) = \chi(\sigma)^d;$$

hence

$$\bar{\chi} = \chi^d.$$

Finally, if we put

$$E' = F \cap F_L(q^m|X^m)$$

then $E \subset E'$ and the above considerations (applied to E') show that E' admits the period q^m. Conversely, assume that E' is any subfield of F containing E and that E' admits a period q^k which is a power of

q; we have to show that $k \leq m$. Now, $E'L$ is a subfield of $FL = F_L(q|X)$ admitting the period q^k; hence from XVIII we have $E'L = F_L(q^k|X^{ks})$ with $s > 0$; since $EL \subset E'L$ we conclude that the functions in EL can be written as functions of the variable X^{ks}. Now, $EL = F_L(\bar{q}|X^m)$ and therefore we conclude from XVIII that $ks \leq m$, hence $k \leq m$. In fact, we have $ks|m$ and therefore $k|m$. QED.

In the proof we have seen that the elliptic subfields $E \subset F$ correspond $1 - 1$ to those elliptic subfields $EL \subset F_L(q|X)$ which have a period $\bar{q} \in K$. We have not only the degree formula $[F : E] = [FL : EL]$ but the same formula holds also for the degree of inseparability. If τ_u is any automorphism of $FL = F_L(q|X)$ over EL then it induces an automorphism in F if and only if τ_u commutes with $\tau_Q\sigma$; this means that τ_u commutes with σ, i. e. $u \in K$. Hence from XVII we deduce the following.

Corollary XIXa: *Let F be as in* XIX *and let $E \subset F$ be an elliptic subfield, admitting the period $\bar{q}$ and belonging to m in the sense of* XIX. *Then:*

(i) *The degree of inseparability of $F|E$ is p^r, the maximal p-power dividing m.*

(ii) *The group of automorphisms of $F|E$ is isomorphic to U/q, where $U \subset K^\times$ consists of all $u \in K^\times$ such that $u^m \equiv 1 \bmod^\times \bar{q}$.*

(iii) *$F|E$ is a Galois extension if and only if the following conditions are satisfied:*

$m \not\equiv 0 \bmod p$;

K contains the m-th roots of unity;

$\bar{q}$ has an m-th root in K.

Now we ask: which subfields E of F have a prime divisor of degree 1, i. e. split over K? This is the case if and only if $\bar{\chi} = 1$ which by XIX means $\chi^d = 1$, i. e. $d \equiv 0 \bmod n$. Since d is in any case a multiple of the order r of $\bar{q} \bmod^\times q$, we conclude that d is divisible by the least common multiple $d_0 = \operatorname{lcm}(n, r)$.

Let $d = d_0 s$ with $s > 0$. If m_0 is determined from

$$q^{m_0} = \bar{q}^{d_0} \tag{86}$$

then we see that $m = m_0 s$. Thus E splits over K if and only if the integer m belonging to E is divisible by m_0.

In particular, the field $E_0 \subset F$ of period $\bar{q}$ and belonging to m_0 splits over K. From XVIII (applied to $\bar{q}$ instead of q) we infer that

E_0 contains for every integer $s > 0$ one and only one subfield E' which is K-isomorphic to E_0 and such that $[E_0 : E'] = s^2$. Now, E' is a subfield of F of period $\bar{q}$ and $[F : E'] = d_0 m_0 s^2 = dm$; from XIX we conclude that $E' = E$ belongs to $m = m_0 s$. Hence:

Corollary XIXb: *Let F be as in XIX, and let $\bar{q} \in K$ be commensurable with q, $0 < |\bar{q}| < 1$. There exists one and only one maximal elliptic subfield E_0 of F which has period $\bar{q}$ and splits over K. The degree $[F : E_0]$ is $d_0 m_0$ where d_0 is the least common multiple of the order n of the character invariant χ of F, and of the order r of $\bar{q} \bmod^{\times} q$; the integer m_0 is then determined from* (86).

Taking $\bar{q} = q$, we have in particular:

Corollary XIXc: *There is one and only one maximal subfield $F_0 \subset F$ which is K-isomorphic to the Jacobian function field $F_K(q)$ of F. The degree of $F|F_0$ is n^2.*

If in corollary XIXb we try to find subfields E_0 in F with $[F : E_0] = n$ we have to solve $d_0 m_0 = n$ which gives $d = n$ (since $n | d_0$) and $m_0 = 1$, hence $q = \bar{q}^n$ in view of (86). It follows:

Corollary XIXd: *The degree of F over any elliptic subfield which splits over K is divisible by n. There exist such subfields E_0 with $[F : E_0] = n$ if and only if q is an n-th power in K; if this is so then these fields E_0 are in $1 - 1$ correspondence with the n-th roots of q in K which are their respective periods; also, $F | E_0$ is then a cyclic extension.*

The last assertion follows from statement (ii) in corollary XIXa.

Appendix: On the algebraic theory of elliptic function fields

In this appendix, K may be an arbitrary field. § A1 contains the definition of the absolute and the Hasse invariant for an elliptic function field $F|K$ which has a prime divisor of degree 1; for reasons of simplicity we deal with the Hasse invariant in the case $j \neq 0, 12^3$ only which suffices for these notes. In § A2 the absolute and the Hasse invariant (in case $j \neq 0, 12^3$) will be defined for an arbitrary elliptic function field $E|K$ which may not have a prime divisor of degree 1. The notion of *Jacobian field* is introduced and the connection to Galois cohomology is given; in particular the cohomological invariant of an elliptic function field is defined.

§ A1. Fields with a prime divisor of degree 1

Let $F|K$ be an elliptic function field having a prime divisor $\mathfrak{p}$ of degree 1. By the Riemann-Roch theorem, there exists an element $x \in F$ having $2\mathfrak{p}$ as its pole divisor, and an element $y \in F$ having $3\mathfrak{p}$ as its pole divisor. The 7 elements $1, x, y, x^2, xy, x^3, y^2$ are K-linearly dependent since their pole divisors divide $6\mathfrak{p}$. Hence there is a relation of the form

$$y^2 + (ux + v)y = a_0 x^3 + a_1 x^2 + a_2 x + a_3 \tag{1}$$

with coefficients $u, v, \ldots, a_3 \in K$.

The elements x, y are determined by our conditions up to the substitutions

$$\begin{aligned} x &\to \alpha x + \alpha' \\ y &\to \beta y + \beta' x + \beta'' \end{aligned} \tag{2}$$

with coefficients in K and $\alpha, \beta \neq 0$.

Since $a_0 \neq 0$, we may apply the substitution

$$\begin{aligned} x &\to a_0 x \\ y &\to a_0 y \end{aligned}$$

and thus assume that $a_0 = 1$.

If char $(K) \neq 2$ we may apply the substitution

$$\begin{aligned} x &\to x \\ y &\to 2y + (ux + v) \end{aligned}$$

and thus transform the equation (1) into the form

$$y^2 = 4x^3 + b_1x^2 + b_2x + b_3 \tag{3}$$

where

$$\begin{aligned} b_1 &= 4a_1 + u^2 \\ b_2 &= 4a_2 + 2uv \\ b_3 &= 4a_3 + v^2. \end{aligned} \tag{4}$$

If, furthermore, char $(K) \neq 3$ we may apply the substitution

$$\begin{aligned} x &\to x + \tfrac{1}{12}b_1 \\ y &\to y \end{aligned} \tag{5}$$

and thus transform the equation (3) into *Weierstraß normal form*

$$y^2 = 4x^3 - g_2x - g_3 \tag{6}$$

where

$$\begin{aligned} g_2 &= \tfrac{1}{12}b_1^2 - b_2, \\ g_3 &= -\tfrac{1}{216}b_1^3 + \tfrac{1}{12}b_1b_2 - b_3. \end{aligned} \tag{7}$$

In this case, the absolute invariant j is defined by the classical formula

$$j = 12^3 \frac{g_2^3}{\Delta} \tag{8}$$

where

$$\Delta = g_2^3 - 27g_3^2 \neq 0 \tag{9}$$

is essentially the discriminant of the cubic polynomial on the right hand side of (6); if e_1, e_2, e_3 are the roots of that polynomial, we have

$$\Delta = 4^2 \prod_{i<j} (e_i - e_j)^2.$$

The only substitutions (2) preserving the type of normal form (6) are of the form

$$\begin{aligned} x &\to \alpha x \\ y &\to \beta y \end{aligned} \quad \text{with} \quad \alpha^3 = \beta^2; \tag{10}$$

then we have

$$\alpha = \lambda^2, \quad \beta = \lambda^3 \tag{11}$$

with $\lambda \in K$, $\lambda \neq 0$. Under these substitutions, the g_2, g_3 are changed as follows:

$$\begin{aligned} g_2 &\to \lambda^4 g_2 \\ g_3 &\to \lambda^6 g_3 \end{aligned} \tag{12}$$

which shows that j, as defined by (8), remains unchanged. Thus j does not depend on the choice of the generators x, y according to our conditions. It also does not depend on the choice of the prime $\mathfrak{p}$ of degree 1 since it is well known that for any two prime divisors $\mathfrak{p}, \mathfrak{p}'$ of degree 1 of $F|K$ there is an automorphism of F transforming $\mathfrak{p}$ into $\mathfrak{p}'$[1]).

If $j \neq 0$, 12^3, i.e. if $g_2, g_3 \neq 0$ then (12) shows that the element $g_2g_3^{-1} \in K^\times$ is changed by a square in $K^\times$ only, i.e. its class modulo squares is an invariant of $F|K$. This invariant has been introduced by Hasse [9]. In our context it is convenient to normalize the Hasse invariant of $F|K$ by the additional factor $-\frac{1}{2}$. We define:

$$\gamma \equiv -\frac{1}{2}\frac{g_2}{g_3} \bmod K^{\times 2} \quad (\text{char}\,(K) \neq 2, 3;\ j \neq 0, 12^3). \tag{13}$$

The factor $-\frac{1}{2}$ is chosen such that the analytic fields discussed in this paper have Hasse invariant 1. If $j = 0$ or $j = 12^3$ then also a Hasse invariant can be defined, but since this is in general not of quadratic character, and since we will not have use for it in this paper, we shall not discuss this case here.

If an element $\gamma \in K^\times$ representing the Hasse invariant of $F|K$ is given, then the generators x, y of $F|K$ can be chosen in such a way that their defining relation is of Weierstraß normal form (6) with

$$g_2 = -2\gamma g_3; \tag{14}$$

now from (8) we see that

$$g_3 = \frac{-1}{8\gamma^3}\,\frac{27j}{j - 12^3}. \tag{15}$$

This shows that we can find a Weierstraß normal form for $F|K$ in which the coefficients g_2, g_3 are universally expressible in terms of j

[1]) This latter remark applies as well to the cases char $(K) = 2$ or 3 which are discussed below.

and γ. Hence $F|K$ is uniquely determined, up to K-isomorphisms, by its absolute invariant j and its Hasse invariant γ.

Conversely, if $j \neq 0, 12^3$ and $\gamma \neq 0$ are given elements in K, then we define g_2, g_3 by means of (15), (14) and we see that the Weierstraß normal equation (6) defines an elliptic function field $F|K$, which has a prime of degree 1 (namely the pole of x and y), and whose absolute and Hasse invariants are j and γ respectively.

The foregoing definitions of j and γ work only if char $(K) \neq 2, 3$ since otherwise the Weierstraß normal form (6) may not be achieved. If char $(K) \neq 2$ then we may consider the normal form (3) and define j by means of the formula

$$(16) \qquad j = \frac{(b_1^2 - 12 b_2)^3}{\Delta}$$

where

$$(17) \qquad 16\Delta = b_1^2 b_2^2 + 72 b_1 b_2 b_3 - 16 b_2^3 - 4 b_1^3 b_3 - 16 \cdot 27 b_3^2.$$

If char $(K) \neq 2, 3$ we obtain the same j as in (8) in view of the transformation formulas (7). If char $(K) = 3$ then (16) reduces to

$$(18) \qquad j = \frac{b_1^6}{b_1^2 b_2^2 - b_2^3 - b_1^3 b_3}.$$

The only substitutions (2) which preserve the type of normal form (3) are

$$(19) \qquad \begin{aligned} x &\to \alpha x + \alpha' \\ y &\to \beta y \end{aligned} \qquad \text{wit} \quad \alpha^3 = \beta^2;$$

it is clear from our discussion that under the corresponding substitutions of the b_1, b_2, b_3 the rational function on the right hand side of (16) remains unchanged, since this is so in characteristic $\neq 3$ and hence is a universal property of that rational function. That is, also in characteristic 3 the definition (18) of j gives an invariant of $F|K$.

From (18) we see that $j = 0$ in characteristic 3 if and only if $F|K$ can be generated by elements whose defining relation is in Weierstraß normal form. Now assume $j \neq 0$ and char $(K) = 3$. Then the substitution

$$(20) \qquad \begin{aligned} x &\to x - \frac{b_2}{b_1} \\ y &\to y \end{aligned}$$

transforms the equation (3) into the form

$$(21) \qquad y^2 = x^3 + b_1 x^2 + b_3'$$

with

$$(22) \qquad b_3' = \frac{b_2^3}{b_1^3} - \frac{b_2^2}{b_1} + b_3.$$

This may be regarded as a substitute of the Weierstraß normal form for characteristic 3 and $j \neq 0$.

Using this normal form, we have

$$(23) \qquad j = \frac{-b_1^3}{b_3'}.$$

The only substitutions (2) preserving the type of normal form (21) are of the form (10); hence we have (11) and the b_1, b_3' are changed according to the formulas

$$(24) \qquad \begin{aligned} b_1 &\to \lambda^2 b_1 \\ b_3' &\to \lambda^6 b_3'. \end{aligned}$$

In particular, we see that the class of b_1 modulo $K^{\times 2}$ is an invariant, which we define to be the Hasse invariant of $F|K$:

$$(25) \qquad \gamma \equiv b_1 \bmod K^{\times 2} \qquad (\text{char}\,(K) = 3,\ j \neq 0).$$

(we do not define γ if $j = 0$).

By the way, we obtain the same formula if we substitute (7) into (13), clear denominators and reduce modulo 3. Note that this formula depends only on the normal form (3) and does not require the transformation onto normal form (21).

If an element $\gamma \in K^\times$ representing the Hasse invariant of $F|K$ is given, then the generators x, y can be chosen such that $\gamma = b_1$; now we see from (23) that $b_3' = -\gamma^3/j$ which shows that $F|K$ is uniquely determined, up to K-isomorphisms, by its absolute invariant j and its Hasse invariant γ.

Conversely, if $j \neq 0$ and $\gamma \neq 0$ are given elements in K, then we define a function field $F|K$ by the defining equation

$$y^2 = x^3 + \gamma x^2 - \frac{\gamma^3}{j}$$

and obtain an elliptic function field $F = K(x, y)$ which has a prime of degree 1 and whose absolute and Hasse invariants are j and γ respectively.

We have still to discuss the case char $(K) = 2$. In this case, the normal form (3) can never be achieved, since such an equation defines a field of genus 0 over the algebraic closure of K. Hence we have to consider defining relations of type (1).

Let us return for a moment to the case char $(K) \neq 2$, and consider generators x, y of $F|K$ whose defining relation is of type (1) with $a_0 = 1$, i. e.

$$y^2 + (ux + v)y = x^3 + a_1 x^2 + a_2 x + a_3. \tag{26}$$

If we substitute the expressions (4) into (16), then we obtain j as a rational function of u, v, a_1, a_2, a_3. It is easily verified that the denominator 16 which appears formally in view of (17) cancels out so that we have obtained an expression of j as a quotient of two integral polynomials in u, v, a_1, a_2, a_3. The substitutions (2) which preserve the form (26) ($a_0 = 1$) are those for which $\beta^2 = \alpha^3$. It is clear from our discussion that under the corresponding substitutions of u, v, a_1, a_2, a_3 the rational function just described does not change. Since this is a formal property, it holds also in characteristic 2. Hence we may define the absolute invariant *universally for every characteristic* as this rational function in u, v, a_1, a_2, a_3.

If char $(K) = 2$ this reduces to

$$j = \frac{u^{12}}{\Delta} \tag{27}$$

with

$$\Delta = a_2^2 u^4 + a_3 u^6 + a_2 u^5 v + u^3 v^3 + a_1 u^4 v^2 + v^4 \neq 0. \tag{28}$$

Note that, from what we have said above, u, v are not both zero. If $u = 0$ then $j = 0$. If $u \neq 0$ then the substitution

$$\begin{aligned} x &\to u^{-3}(ux + v), \\ y &\to u^{-3} y \end{aligned}$$

transforms (26) into an equation of the form

$$y^2 + xy = x^3 + Ax^2 + Bx + C \tag{29}$$

and we have

$$j = \frac{1}{\Delta} \tag{30}$$

where

$$\Delta = B^2 + C. \tag{31}$$

Now the substitution

$$\begin{aligned} x &\to x \\ y &\to y + B \end{aligned}$$

transforms (29) into an equation of the form

$$y^2 + xy = x^3 + Ax^2 + C' \tag{32}$$

with

$$C' = C + B^2. \tag{33}$$

We may regard (32) as a substitute for the Weierstraß normal form if char $(K) = 2$ and $j \neq 0$.

The only substitutions (2) which preserve this type of normal form are

$$\begin{aligned} x &\to x, \\ y &\to y + \beta' x; \end{aligned} \tag{34}$$

thereby A is changed as follows:

$$A \to A + \beta'^2 + \beta' = A + \pi(\beta') \tag{35}$$

where we put

$$\pi(z) = z^2 + z.$$

This shows that the additive class of A modulo $\pi(K^+)$ is an invariant of K, which we define to be the Hasse invariant:

$$\gamma \equiv A \bmod \pi(K^+) \qquad (\text{char}\,(K) = 2;\ j \neq 0). \tag{36}$$

(We do not define γ if $j = 0$.) Note that this formula depends on the normal form (29) only and does not require the transformation onto (32).

If an element $\gamma \in K^+$ representing the Hasse invariant is given then (35) shows that we can choose x, y in such a way that

$$A = \gamma, \quad C' = \frac{1}{j}$$

so that $F|K$ is uniquely determined, up to K-isomorphisms, by j and γ.

Conversely, if an element $j \neq 0$ in K and $\gamma \in K$ are given, then the equation

$$y^2 + xy = x^3 + \gamma x^2 + \frac{1}{j} \tag{37}$$

defines a function field $F = K(x, y)$ which is elliptic, has a prime of degree 1, and its invariants are j and γ.

We have now defined j and γ (in the case $j \neq 0, 12^3$) *for arbitrary characteristic and shown that $F|K$ is uniquely determined by j and γ.*

Remark 1: If $F|K$ can be generated by elements x, y satisfying an equation of the type

$$y^2 + xy = x^3 + Bx + C \tag{38}$$

then we have for any characteristic:

$$j = \frac{(1-48B)^3}{\Delta} \tag{39}$$

where

$$\Delta = B^2 - C - 64B^3 + 72BC - 432 \cdot C^2. \tag{40}$$

For, in characteristic 2 this reduces to (30), (31); in characteristic $\neq 2$ the substitution

$$\begin{aligned} x &\to x, \\ y &\to 2y + x \end{aligned} \tag{41}$$

transform (38) into

$$y^2 = 4x^3 + x^2 + b_2 x + b_3 \tag{42}$$

where, according to (4):

$$b_2 = 4B, \quad b_3 = 4C; \tag{43}$$

substituting this into (16), (17) we obtain indeed (39), (40).

The formula for the Hasse invariant in the case of an equation (38) is:

$$\begin{aligned} \gamma &\equiv \frac{1-48B}{1-72B+864C} \bmod K^{\times 2} && \text{if char } (K) \neq 2, \\ \gamma &\equiv 0 \bmod \pi(K^+) && \text{if char } (K) = 2. \end{aligned} \tag{44}$$

This is clear if char $(K) = 2$ (viz. (36)); if char $(K) \neq 2$ we use the substitution (41) and see from (43) that our formula is equivalent to

$$\gamma \equiv \frac{1-12b_2}{1-18b_2+216b_3} \bmod K^{\times 2}$$

which is true if char $(K) = 3$ in view of (25); if char $(K) \neq 2, 3$ we use the substitution (5) (with $b_1 = 1$) to transform (42) into Weierstraß normal form (6) and see from (7) that our formula is equivalent to

$$\gamma \equiv \frac{12 g_2}{-216 g_3} \bmod K^{\times 2}$$

which is true in view of (13).

Remark 2: If K is separably algebraically closed, then $K^{\times 2} = K^\times$ (if char $(K) \neq 2$) and $\pi K^+ = K^+$ (if char $(K) = 2$). We conclude that the Hasse invariant of an elliptic function field $F|K$ is always trivial; *hence the absolute invariant j of $F|K$ is sufficient to characterize F up to K-isomorphisms.*

In this statement, we had to assume that $j \neq 0, 12^3$ since otherwise we had not defined the Hasse invariant. However, a more detailed discussion shows in the exceptional cases that $F = K(x, y)$ with the following defining relations:

$$\begin{aligned} y^2 &= 4x^3 - 1 && \text{if char } (K) \neq 2, 3 \text{ and } j = 0, \\ y^2 &= 4x^3 - x && \text{if char } (K) \neq 2 \text{ and } j = 12^3, \\ y^2 + y &= x^3 && \text{if char } (K) = 2 \text{ and } j = 0. \end{aligned} \tag{45}$$

It follows that our statement above remains true also in the exceptional cases.

Remark 3: Let $L|K$ be any extension field with the corresponding constant field extension FL of F. If x, y are generators of $F|K$ then they are also generators of $FL|L$ and their defining relation over L is the same as their defining relation over K. We conclude:

(i) $F|K$ and $FL|L$ have the same absolute invariant;

(ii) The Hasse invariant of $FL|L$ is the image of the Hasse invariant of $F|K$ under the natural map

$$K^\times/K^{\times 2} \to L^\times/L^{\times 2} \text{ resp. } K^+/\pi K^+ \to L^+/\pi L^+.$$

Here, $F|K$ is an elliptic function field with a prime of degree 1; in statement (ii) we have to assume moreover that the absolute invariant j of $F|K$ is $\neq 0, 12^3$. Let $F'|K$ be another such field with absolute invariant j'; if F and F' become isomorphic over L (i. e. if $FL|L$ and $F'L|L$ are L-isomorphic) we conclude from (i) that necassarily $j = j'$. If L is separably closed, then this condition is also sufficient in view of remark 2. For arbitrary L, the necessary and sufficient condition is $j = j'$ and $\gamma\gamma'^{-1} \in L^{\times 2}$ (resp. $\gamma - \gamma' \in \pi L^+$) where γ, γ' are the Hasse invariants of $F|K$ and $F'|K$ respectively.

The latter condition means that L contains the field $K\left(\sqrt{\gamma\gamma'^{-1}}\right)$ $\left(\text{resp. } K\left(\frac{1}{\pi}(\gamma - \gamma')\right)\right)$ which is a separable extension of degree 2 if $\gamma \not\equiv \gamma' \bmod K^{\times 2}$ (resp. $\bmod\ \pi K^+$). We conclude:

If F and F' become isomorphic over some field extension L of K, then $j = j'$. If this is so, then they become isomorphic over the separable *algebraic closure Σ of K. Moreover, among all the field extensions $L|K$ over which F and F' become isomorphic, there is a unique minimal one, namely the field $K(\sqrt{\gamma\gamma'^{-1}})$ (resp. $K\left(\frac{1}{\pi}(\gamma-\gamma')\right)$); this is separable of degree 2 if F and F' are not K-isomorphic.*

In the last sentence, we have of course to assume that $j \neq 0, 12^3$. In fact, this statement does not remain true in the exceptional cases in general.

Remark 4: The consideration of normal forms, as given above, leads to the following

Lemma: *Let $F|K$ be an elliptic function field with a prime $\mathfrak{p}$ of degree 1, and let j be its absolute invariant. If $j \neq 0, 12^3$ then there is only one non-trivial automorphism ε of $F|K$ which leaves $\mathfrak{p}$ fixed.*

Proof. We choose generators x, y of $F|K$ such that x, y have pole divisors $2\mathfrak{p}$, $3\mathfrak{p}$ respectively. We may assume that their defining relation over K is of Weierstraß normal form (6) if char $(K) \neq 2, 3$, of normal form (21) if char $(K) = 3$, of normal form (32) if char $(K) = 2$. In any case, since $\varepsilon(\mathfrak{p}) = \mathfrak{p}$, the elements $\varepsilon(x)$, $\varepsilon(y)$ also have the pole divisors $2\mathfrak{p}$, $3\mathfrak{p}$ respectively and therefore

$$\varepsilon(x) = \alpha x + \alpha',$$
$$\varepsilon(y) = \beta y + \beta' x + \beta''$$

with $\alpha, \beta \neq 0$. Moreover, since ε is an automorphism, the defining relation of $\varepsilon(x)$, $\varepsilon(y)$ over K coincides with that of x, y. In particular, the defining relation of $\varepsilon(x)$, $\varepsilon(y)$ has the same type of normal form as we have chosen for x, y. If char $(K) \neq 2, 3$, we conclude that the substitution

$$x \to \varepsilon(x), \quad y \to \varepsilon(y) \tag{46}$$

is of the form (10), and that according to (12) we have

$$g_2 = \lambda^4 g_2, \quad g_3 = \lambda^6 g_3.$$

Since $j \neq 0, 12^3$ we have $g_2, g_3 \neq 0$ and it follows $\lambda^2 = \alpha = 1$ hence

$$\varepsilon(x) = x. \tag{47}$$

If char $(K) = 3$ we again conclude that the substitution (46) is of the form (10); according to (24) we have

$$b_1 = \lambda^2 b_1$$

and since $b_1 \neq 0$ (because $j \neq 0$) it follows again $\lambda^2 = \alpha = 1$, i. e. (47). If char $(K) = 2$ then the substitution (46) is of the form (34) and we have (47) again.

In any case, we have seen that ε leaves x and hence the field $K(x)$ elementwise fixed. That is, ε is the non-trivial automorphism of the separable quadratic extension $F|K(x)$. By the way, we have

$$\varepsilon(y) = -y \qquad \text{if char } (K) \neq 2,$$
$$\varepsilon(y) = y + x \qquad \text{if char } (K) = 2.$$

If $j = 0$ or $j = 12^3$ then the lemma is false in general.

§ A2. Arbitrary elliptic fields

Now let $E|K$ be an arbitrary elliptic function field; we do not assume that it has a prime divisor of degree 1.

To define the absolute invariant of $E|K$, let L be a splitting field of E. Then EL has a prime divisor of degree 1 over L, and the absolute invariant j_L of $EL|L$ is defined as an element of L, according to § A1. We claim that $j_L \in K$, and that it does not depend on the choice of the splitting field L.

If $L \subset L'$ then $j_L = j_{L'}$ according to remark 3 of § A1. Applying this remark twice, we conclude that $j_L = j_{L'}$ whenever the splitting fields L, L' of E are contained in a common extension field Λ.

Now let E_1 be a field which is K-isomorphic to E. As always, the corresponding constant field extension of E will be denoted by EE_1. More precisely: EE_1 is the quotient field of the tensor product $E \otimes E_1$ over K, where we identify E with the first factor and E_1 with the second.

Every K-isomorphism $\varphi\colon E \to E_1$ extends uniquely to an E_1-homomorphism $E \otimes E_1 \to E_1$ and it is well known that the corresponding local ring is a valuation ring of EE_1. The corresponding prime divisor $\mathfrak{p}_\varphi$ of $EE_1|E_1$ is of degree 1, its residue class field being E_1.

Hence E_1 is a splitting field of E. In particular, $j_{E_1} \in E_1$ is defined.

Given any splitting field L of E, we may imbed E_1 and L into a common overfield Λ in such a way that E_1 and L are linearly disjoint over K; this can be done for instance by defining Λ to be the quotient field of $E_1 \otimes L$ over K, and identifying E_1 with the first and L with the second factor of this tensor product. We then have $j_{E_1} = j_L$ according to the remark above. Hence

$$j_{E_1} = j_L \in E_1 \cap L = K$$

which shows, firstly, that $j_L \in K$ and, secondly, that j_L does not depend on the choice of the splitting field L.

This being shown, we may now write j instead of j_L and define j to be the *absolute invariant* of $E|K$. By definition, the absolute invariant does not change if we apply an arbitrary constant field extension. If $E|K$ has a prime divisor of degree 1 then our definition coincides with that in § A 1.

To define the Hasse invariant of $E|K$, we now assume $j \neq 0, 12^3$ according to our procedure in § A 1. Then, if L is any splitting field of E, the Hasse invariant γ_L of $EL|L$ is defined in § A 1. This is an element in $L^\times/L^{\times 2}$ if char $(K) \neq 2$ and in $L^+/\pi L^+$ if char $(K) = 2$.

We claim that *there exists a unique element $\gamma \in K^\times/K^{\times 2}$ such that γ_L is the image of γ under the canonical map $K^\times/K^{\times 2} \to L^\times/L^{\times 2}$, for every splitting field L of E*; if char $(K) = 2$ one has to replace the multiplicative square factor group by the additive π-factor group in this statement.

In the following proof of this statement, we use the multiplicative notation belonging to the case char $(K) \neq 2$; it is to be understood that the proof remains valid in the case of characteristic 2 after switching from the multiplicative to the additive notation.

Let E_1 be a field which is K-isomorphic to E. We know from above that E_1 splits E, hence γ_{E_1} is defined. Let Ω denote the algebraic closure of K; then Ω splits E too and hence γ_Ω is defined; it is clear that $\gamma_\Omega = 1$ since Ω is algebraically closed.

Both Ω and E_1 are contained in $\Lambda = E_1\Omega$, the field compositum of E_1 with Ω. We know from § A 1 (remark 3) that γ_{E_1} maps onto γ_Λ under the natural map $E_1^\times/E_1^{\times 2} \to \Lambda^\times/\Lambda^{\times 2}$. On the other hand, we know from the same source that γ_Λ is the image of $\gamma_\Omega = 1$ under the natural map $\Omega^\times/\Omega^{\times 2} \to \Lambda^\times/\Lambda^{\times 2}$. We conclude that γ_{E_1} has the image 1 in $\Lambda^\times/\Lambda^{\times 2}$. *From this it follows that γ_{E_1} is the image of some $\gamma \in K^\times/K^{\times 2}$.*

For, consider the field $H = E_1\left(\sqrt{\gamma_{E_1}}\right)$ which we may assume to be of degree 2 over E_1 since otherwise $\gamma_{E_1} = 1$ and we may take $\gamma = 1$. We have

$$H\Omega = E_1\left(\sqrt{\gamma_{E_1}}\right) \cdot \Omega = \Lambda\left(\sqrt{\gamma_{E_1}}\right) = \Lambda = E_1\Omega \tag{48}$$

since γ_{E_1} is a square in Λ. We conclude that H and Ω are *not* linearly disjoint over K, hence H is *not* a regular extension of K[1]).

Since $H|E_1$ is separable and $E_1|K$ is regular, hence separable, it follows that K is *not* algebraically closed in H. Let K' be the algebraic closure of K in H. Then $E_1 \neq E_1K'$, hence $E_1K' = H$. Since $E_1|K$ is regular it follows

$$[K' : K] = [H : E_1] = 2. \tag{49}$$

Moreover, K' is separable over K since $K' \subset H$. Therefore, $K' = K\left(\sqrt{\gamma}\right)$ with some $\gamma \in K^\times/K^{\times 2}$. We now have

$$H = E_1\left(\sqrt{\gamma_{E_1}}\right) = E_1\left(\sqrt{\gamma}\right)$$

which shows that

$$\gamma_{E_1} = \gamma \qquad (\text{in } E_1^\times/E_1^{\times 2}).$$

In other words, *γ_{E_1} is the image of γ under the map $K^\times/K^{\times 2} \to E_1^\times/E_1^{\times 2}$.*

Moreover, γ is *uniquely determined* by this property. For, if γ' also maps onto γ_{E_1} then $\gamma'\gamma^{-1}$ is a square in E_1; since K is algebraically closed in E_1 it follows that it is a square already in K, hence $\gamma' = \gamma$.

Now let L be an *arbitrary splitting field* of E. Consider the independent field compositum E_1L. We know that γ_L and γ_{E_1L} are defined and that γ_L maps onto γ_{E_1L} under the natural map $L^\times/L^{\times 2} \to (E_1L)^\times/(E_1L)^{\times 2}$. Moreover, γ_L is *uniquely determined* by this property; this follows as above from the fact that L is algebraically closed in E_1L.

The commutative field diagram

$$\begin{array}{ccc} E_1 & \longrightarrow & E_1L \\ \uparrow & & \uparrow \\ K & \longrightarrow & L \end{array}$$

leads to a corresponding commutative diagram of the square factor groups. If we chase $\gamma \in K^\times/K^{\times 2}$ through the upper path of the diagram then it first maps onto γ_{E_1} (by definition of γ) which in turn maps onto γ_{E_1L} (by § A 1, remark 3). Hence, if we let γ go through the lower path then it maps first onto some element γ_L' in $L^\times/L^{\times 2}$ which then is mapped onto γ_{E_1L}. From what we have said above, we conclude

$$\gamma_L' = \gamma_L. \tag{50}$$

That is, γ_L is the image of γ.

[1]) A field extension $H|K$ is called *regular* if it is separable and if K is algebraically closed in H. This is equivalent to saying that H is linearly disjoint over K to every algebraic field extension of K.

We have proved:

(51) *Let $E_1|K$ be a field extension isomorphic to E. Then there is a unique element $\gamma \in K^\times/K^{\times 2}$ whose image in $E_1^\times/E_1^{\times 2}$ is the Hasse invariant γ_{E_1}; if $L|K$ is an arbitrary splitting field of E then the image of γ in $L^\times/L^{\times 2}$ is the Hasse invariant γ_L.* (If char $(K) = 2$ one has to replace the multiplicative square factor group by the additive π-factor group in this statement).

Now we define this γ to be the Hasse invariant of $E|K$. By definition, it is an element of $K^\times/K^{\times 2}$ if char $(K) \neq 2$ and of $K^+/\pi K^+$ if char$(K) = 2$. If $L|K$ is an arbitrary extension, then the Hasse invariant of $EL|L$ is the image of the Hasse invariant of $E|K$. If $E|K$ has a prime of degree 1 then our definition coincides with that of § A 1.

Note that we have not defined the Hasse invariant if $j = 0$ or 12^3; these exceptional cases will also be excluded in the following discussion.

Given an elliptic function field $E|K$, with absolute invariant j and Hasse invariant γ, we now define the *Jacobian function field* of E to be the elliptic field $F|K$, having a prime divisor of degree 1, whose absolute and Hasse invariants coincide with those of $E|K$. We have shown in § A 1 that there exists such a field $F|K$, and that it is uniquely determined up to K-isomorphisms. If E itself has a prime divisor of degree 1, then $F = E$.

Using (51), we see that F is uniquely determined by the following condition[1]):

(52) *$F|K$ has a prime divisor of degree 1, and the constant field extensions FE_1 and EE_1 are E_1-isomorphic.*

Also we have:

(53) *For any splitting field L of E, the constant field extensions FL and EL are L-isomorphic.*

If $L|K$ is an arbitrary extension then FL is the Jacobian field of EL. That is, the notion of the „Jacobian field" is preserved by constant field extensions.

[1]) In can be shown that also in the exceptional cases $j = 0$ or 12^3 there exists a unique field $F|K$ having the property (52), and that (53) holds for this field. This field is then defined as the Jacobian function field of E. In fact, this is what is usually done by defining the Jacobian field in the context of "principal homogeneous spaces".

Connection with Galois cohomology

Now let $F|K$ be a given elliptic function field with a prime divisor of degree 1. We want to describe those elliptic function fields $E|K$ which admit $F|K$ as their Jacobian field.

Since $E|K$ is separably generated, it has at least one (and, in fact, infinitely many) prime divisors $\mathfrak{p}$ whose residue class field is separable over K. Let L denote a Galois extension of K containing the residue class field of $\mathfrak{p}$. Then $\mathfrak{p}$ has in $EL|L$ at least one prime divisor of degree 1, as follows from the general theory of constant field extensions. Hence L is a splitting field of E. We see therefore, that E has splitting fields L which are Galois extensions of K.

In the following, let us fix such an L. Of course we could take for L the maximal Galois extension of K, namely the separable algebraic closure Σ of K. However, it seems advisable, in the following considerations, to admit an arbitrary Galois extension L.

If E has F as its Jacobian field, then EL and FL are L-isomorphic; after identifying E with its image under such an isomorphism, we may assume that

$$EL = FL. \tag{54}$$

We now ask: if $E|K$ is any elliptic field with the property (54); under what condition is F the Jacobian field of E, i. e. under what condition do E and F have the same Hasse invariant?

The answer will be given in terms of Galois cohomology.

Let G be the Galois group of $L|K$. Every automorphism $\sigma \in G$ extends uniquely to an automorphism σ_F of $FL|F$. Let us identify $\sigma = \sigma_F$. Thus G becomes the Galois group of $FL|F$.

The same remark may be applied to E instead of F. Thus, σ_E is the automorphism of $FL = EL$ over E inducing σ in L. These automorphisms form the Galois group G_E of $FL|E$.

Let us put

$$\zeta_E(\sigma) = \sigma_E \sigma^{-1} \qquad (\sigma \in G).$$

This is an automorphism of FL inducing in L the identity. Let us denote by A the automorphism group of $FL|L$. Thus we have obtained a map

$$\zeta_E : G \to A;$$

by definition, it satisfies the relation

$$\zeta_E(\sigma\sigma') = \zeta_E(\sigma)\zeta_E(\sigma')^\sigma \qquad (\sigma, \sigma' \in G). \tag{55}$$

Here, G is considered to act on A via the rule

$$\alpha^\sigma = \sigma\alpha\sigma^{-1} \qquad (\sigma \in G, \alpha \in A).$$

The relation (55) says that ζ_E is a 1-cocycle in the sense of group cohomology[1]).

Let us call ζ_E the *characteristic cocycle* of E (with respect to F and L). It is clear that E is already determined by its cocycle, namely as the field of fixed elements of the automorphisms $\zeta_E(\sigma)\sigma$ $(\sigma \in G)$ of FL.

It follows from Galois theory that $E \to \zeta_E$ establishes *a* 1 — 1 *correspondence between the elliptic function fields* $E|K$ *satisfying* (54) *and the set* $Z^1(G, A)$ *of* 1-*dimensional cocycles from* G *to* A[2]).

Two such fields E, E' are K-isomorphic if and only if their corresponding cocycles are *equivalent*, i. e. if their exists an automorphism $\alpha \in A$ such that

$$(56) \qquad \zeta_{E'}(\sigma) = \alpha\zeta_E(\sigma)\alpha^{-\sigma} \qquad (\sigma \in G);$$

such an α then induces a K-isomorphism

$$\alpha : E \to E'.$$

The equivalence classes of 1-cocycles $G \to A$ form the *cohomology set* $H^1(G, A)$. *Thus the elements in* $H^1(G, A)$ *correspond* 1 — 1 *to the classes of* K-*isomorphic elliptic function fields* $E|K$ *with the property* (54). In this correspondence, the class of fields K-isomorphic to F corresponds to the trivial class, consisting of the cocycles of the form

$$\alpha\alpha^{-\sigma} \qquad (\sigma \in G)$$

for some $\alpha \in A$.

As to the structure of A as a G-operator group, this can be described as follows:

Let $\mathfrak{p}_1$ be a fixed prime of degree 1 of $F|K$ which we regard as a prime of degree 1 of $FL|L$. Let A_1 be the group of those automorphisms in A which leave $\mathfrak{p}_1$ fixed. From § A 1 (remark 4) we know that A_1

[1]) Since in general G is not a finite group we have to regard G as a compact topological group in the sense of W. Krull. Accordingly, the definition of a cocycle also contains a continuity condition which says that there is an open subgroup $U \subset G$ such that $\zeta_E(\sigma)$ depends on σ modulo U only.

This condition is satisfied since there exists already a finite subextension L_0 of L such that $EL_0 = FL_0$; one may take U as the Galois group of $L|L_0$.

In the following, we shall omit these more or less trivial continuity discussions.

[2]) See e. g. [16] § 4.

has order 2 since $j \neq 0, 12^3$. Let ε denote the non-trivial automorphism in A_1. Then we have

$$(57) \qquad \sigma\varepsilon\sigma^{-1} = \varepsilon \qquad (\sigma \in G).$$

For, since $\mathfrak{p}_1$ is already a prime of degree 1 of $F|K$ (and not only of $FL|L$) we have

$$(58) \qquad \sigma(\mathfrak{p}_1) = \mathfrak{p}_1 \qquad (\sigma \in G)$$

hence

$$\sigma\varepsilon\sigma^{-1}(\mathfrak{p}_1) = \sigma\varepsilon(\mathfrak{p}_1) = \sigma(\mathfrak{p}_1) = \mathfrak{p}_1$$

and therefore (57) holds.

Formula (57) says that A_1 is a G-permissible subgroup of order 2 of A on which G acts trivially.

According to the general theory of elliptic function fields we have a semi-direct product decomposition

$$(59) \qquad A = A_1 \cdot T$$

where T denotes the normal subgroup of A consisting of the *translation automorphisms* of $FL|L$. This group T is naturally isomorphic to the group C^0 of divisor classes of degree 0 of $FL|L$. If $c \in C^0$, then the corresponding translation automorphism $\tau_c \in T$ has the property

$$(60) \qquad \tau_c(\mathfrak{p}) \sim \mathfrak{p} + c$$

for every prime divisor $\mathfrak{p}$ of degree 1 of $FL|L$ (the symbol $\sim$ denotes equivalence of divisors). The formula (60) describes the action of τ_c on the prime divisors of degree 1 of $FL|L$; if there are infinitely many[1]) such prime divisors then τ_c is uniquely determined, as an automorphism of $FL|L$, by the formula (60). In general, τ_c is uniquely determined by the property that (60) holds not only in $FL|L$ but also after applying an arbitrary constant field extension to $FL|L$.

In follows from (60) that T acts *simply transitive* on the set of prime divisors of degree 1 of $FL|L$. That is, if $\mathfrak{p}$ and $\mathfrak{p}'$ are two such prime divisors, then there is exactly one $c \in C^0$ such that $\mathfrak{p}' = \tau_c(\mathfrak{p})$; one has to take $c \sim \mathfrak{p}' - \mathfrak{p}$. From this we are lead immediately to the semidirect decomposition (59).

The action of ε on C^0 is given by

$$\varepsilon(c) = -c \qquad (c \in C^0)$$

[1]) More precisely: at least 5.

which is easily verified by means of the explicit description of ε in § A1 (remark 4). We conclude from (60) that

$$\varepsilon\tau_c\varepsilon^{-1} = \tau_{-c} = \tau_c^{-1} \qquad (\tau_c \in T); \tag{61}$$

this formula describes the action of A_1 on T. From (60) we see immediately that

$$\sigma\tau_c\sigma^{-1} = \tau_{\sigma c} \qquad (\sigma \in G,\ \tau_c \in T); \tag{62}$$

this formula describes the action of G on T; in particular, we conclude that T is G-permissible.

The statements (59), (61), (57), (62) describe the structure of A as a G-operator group:

A is isomorphic to the semi-direct product of $T \approx C^0$ with the group A_1 of order 2, the non-trivial element ε of A_1 acting as the inverse operator on T and G acting trivially on A_1.

Now we turn to our original question: Given an elliptic field $E|K$ with the property (54); under what condition does $E|K$ have the same Hasse invariant as $F|K$? That is, under what condition is F the Jacobian field of E?

We claim that this is the case *if and only if the characteristic cocycle $\zeta_E: G \to A$ maps G into the translation group T*. That is to say: if and only if ζ_E is in fact a cocycle from G to T.

Proof. If K' is any field extension of K, let us put $L' = K'L$; then $L'|K'$ is a Galois extension whose group G' can be regarded as a subgroup of G, namely as the Galois group of L over $K' \cap L$. Also, the group A of automorphisms of $FL|L$ can be regarded as a subgroup of the group A' of automorphisms of $FL'|L'$; in this way, the translation group $T \subset A$ becomes a subgroup of the translation group $T' \subset A'$ and we have

$$T = T' \cap A \tag{63}$$

which is to say that the notion of „translation automorphism" is preserved under constant field extensions.

After these identifications it is clear from the definitions that the characteristic cocycle $\zeta_{EK'}$ of the constant field extension EK' (with respect to FK' and L') is obtained from ζ_E as the *restriction* from G to its subgroup G'. That is,

$$\zeta_{EK'}(\sigma) = \zeta_E(\sigma) \qquad (\sigma \in G').$$

In particular, if

$$K' \cap L = K \tag{64}$$

then $G' = G$ and we conclude

$$\zeta_{EK'} = \zeta_E,$$

i. e. the characteristic cocycle does not change if we apply a constant field extension, provided (64) holds.

Also, we infer from (63) that $\zeta_E: G \to A$ maps G into T if and only if $\zeta_{EK'}: G \to A'$ maps G into T'.

This being said, let us take $K' = E_1$, a field which is K-isomorphic to E. Then (64) is satisfied, so that the foregoing remarks are applicable. Moreover, we know from (52) that F is the Jacobian field of E if and only if FE_1 is E_1-isomorphic to EE_1. Hence, *in order to prove our assertion, we may extend beforehand our ground field K to the new ground field $K' = E_1$*. We know that $EE_1|E_1$ has a prime divisor of degree 1.

We now change notation, writing again $E|K$ and $EL|L$ instead of $EE_1|E_1$ and $EE_1L|E_1L$, and similarly for F. We shall prove our assertion under the *additional assumption that $E|K$ has a prime divisor $\mathfrak{p}$ of degree* 1.

Under this assumption, to say that F is the Jacobian field of E is equivalent to saying that F is K-isomorphic to E. This in turn means that the characteristic cocycle ζ_E splits, i. e.

$$\zeta_E(\sigma) = \alpha\alpha^{-\sigma} \qquad (\sigma \in G)$$

for some $\alpha \in A$. If α is a translation then $\alpha^{-\sigma}$ is a translation too (by (62)) and therefore $\zeta_E(\sigma)$ is a translation. Otherwise, it follows from (59) that $\alpha = \varepsilon\tau$ with τ a translation; using (57) and (61) we see that

$$\alpha\alpha^{-\sigma} = \varepsilon(\tau\tau^{-\sigma})\varepsilon^{-1} = \tau^{\sigma}\tau^{-1}$$

is a translation, so that again $\zeta_E(\sigma)$ is a translation.

Conversely, assume that $\zeta_E(\sigma)$ is a translation for every $\sigma \in G$. Let $\mathfrak{p}$ be a prime of degree 1 of $E|K$ which exists by assumption; we regard this as a prime of degree 1 of $EL|L$. It is fixed under the automorphisms of $EL|E$:

$$\zeta_E(\sigma)\sigma\mathfrak{p} = \mathfrak{p} \qquad (\sigma \in G).$$

On the other hand, $\mathfrak{p}_1$ is the prime of degree 1 of $F|K$ which leads to the decomposition (59); this is fixed under the automorphisms of $FL|F$:

$$\sigma\mathfrak{p}_1 = \mathfrak{p}_1 \qquad (\sigma \in G).$$

There is one and only one translation $\tau \in T$ which maps $\mathfrak{p}_1$ onto $\mathfrak{p}$:

$$\tau \mathfrak{p}_1 = \mathfrak{p}.$$

By inspection one sees that the automorphism

$$\tau^{-1} \zeta_E(\sigma) \tau^\sigma$$

leaves $\mathfrak{p}_1$ fixed; on the other hand, this is a product of 3 translations and therefore itself a translation; we conclude that this automorphism is the identity. It follows

$$\zeta_E(\sigma) = \tau \tau^{-\sigma} \qquad (\sigma \in G)$$

which shows that the cocycle ζ_E splits. QED.

We have now seen that the elliptic fields $E|K$ with the property (54), which have F as their Jacobian field, correspond 1—1 to the 1-dimensional cocycles $\zeta: G \to T$. Note that the group T is *abelian* (being isomorphic to C^0), hence these cocycles form a *group* $Z^1(G, T)$. If two cocycles $\zeta, \zeta' \in Z^1(G, T)$ determine the same class in $H^1(G, T)$ then the corresponding elliptic fields E, E' are K-isomorphic; moreover, there is a *translation* $\tau \in T$ which maps E onto E' (see (56)); the converse is also true. However, E and E' may be K-isomorphic without being K-isomorphic by a translation; in view of (56) and (61) this means that ζ_E and ζ_E^{-1} determine the same element in $H^1(G, A)$.

Let us collect our results:

Proposition: *Let $F|K$ be an elliptic function field with a prime of degree* 1; *let j and γ denote its absolute and Hasse invariant* ($j \neq 0, 12^3$).

Let $L|K$ be a Galois extension with group G, and let T denote the group of translation automorphisms of $FL|L$, considered as a G-module.

The elliptic function fields $E|K$ which are split by L and have absolute and Hasse invariant j and γ respectively, correspond (up to K-isomorphisms) 1 — 1 *to the pairs $\zeta, -\zeta$ of mutually inverse elements in* $H^1(G, T)$[1]).

In this statement, T may be replaced by the group C^0 of divisor classes of degree 0 *of $FL|L$, which is G-isomorphic to T.*

If ζ belongs to E in this correspondence then we call ζ the *cohomological invariant* of E with the understanding that this is determined by E up to the substitution $\zeta \to -\zeta$ only. (If ζ has order $\leqq 2$ then $-\zeta = \zeta$ and thus ζ is then uniquely determined by E.)

[1]) We have written the group operation in $H^1(G, T)$ additively.

The cohomological invariant ζ is *independent* of the choice of the Galois splitting field L of E in the sense that, if $L'|K$ is a Galois extension containing L, with group G', then $H^1(G, T)$ is identified with a subgroup of $H^1(G', T')$ by means of the cohomological inflation map.

Thus every elliptic field $E|K$ (with $j \neq 0, 12^3$) is completely described by three invariants; its absolute invariant j which is an element in K, its Hasse invariant γ which is an element in $K^\times/K^{\times 2}$ (if char $(K) \neq 2$) and in $K^+/\pi K^+$ (if char $(K) = 2$), *and its cohomological invariant ζ which is an element in $H^1(G, T)$ (or $H^1(G, C^0)$) if L is a Galois splitting field of E with group G.*

Of course, one may take $L = \Sigma$ to be the separable algebraic closure of K.

References

[1] E. Artin - G. Whaples: Axiomatic characterization of fields by the product formula for valuations; Bull. Amer. Math. Soc. **51** (1945) 469—492.

[2] N. Bourbaki: Eléments de Mathématiques, Algèbre commutative, chap. III, fasc. XXVIII, Paris 1961.

[3] C. Chevalley: Introduction to the theory of algebraic functions of one variable. New York 1951.

[4] M. Deuring: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hamburg **14** (1941) 197—272.

[5] M. Eichler: Einführung in die Theorie der algebraischen Zahlen und Funktionen. Basel 1963.

[6] R. Fricke: Die elliptischen Funktionen und ihre Anwendungen I, II. 2. Aufl. Leipzig 1930.

[7] W. D. Geyer: Ein algebraischer Beweis des Satzes von Weichold über reelle algebraische Funktionenkörper; Berichte aus dem Mathematischen Forschungsinstitut Oberwolfach, Heft **2** (Algebraische Zahlentheorie). Mannheim 1966, 83—98.

[8] A. Güntzer: Zur Funktionentheorie einer Veränderlichen über einem vollständigen nichtarchimedischen Grundkörper; Archiv d. Math. **17** (1966) 415—431.

[9] H. Hasse: Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern. Abh. Math. Sem. Hamburg **10** (1934) 325—348.

[10] H. Hasse: Zahlentheorie. 2. Aufl. Berlin 1963.

[11] J. I. Igusa: Analytic groups over complete fields; Proc. Nat. Acad. Sci. **42** (1956) 540—541.

[12] S. Lang - J. Tate: Principal homogeneous spaces over abelian varieties; Amer. Journ. of Math. **80** (1958) 659—684.

[13] H. Morikawa: On theta functions and abelian varieties over valuation fields of rank one; Nagoya Math. Journ. **20** (1962) 1—27; **21** (1962) 231—250.

[14] A. Néron: Modèles minimaux des variétés abéliennes sur les corps locaux et globaux; Publ. Inst. Hautes Et. Sci. no. **21**, Paris 1964.

[15] P. Roquette: On the Galois cohomology of the projective linear group; Math. Annalen **150** (1963) 411—439.

[16] P. Roquette: Splitting of algebras by function fields of one variable; Nagoya Math. Journ. **27** (1966) 625—642.

[17] J. P. Serre: Corps locaux. Paris 1962.

[18] St. S. Shatz: The cohomology of certain elliptic curves over local and quasi-local fields; Illinois Journ. of Math. **11** (1967) 234—241.

[19] J. Tate: Genus change in inseparable extensions of function fields; Proc. Amer. Math. Soc. **3** (1952) 400—406.

[20] J. Tate: *WC*-groups over *p*-adic fields; Séminaire Bourbaki (Dec. 1957), Exposé no. 156.

[21] J. Tate: Rigid analytic spaces; Notes Inst. Hautes Et. Sci. Paris 1962.

[22] E. Witt: Zerlegung reeller algebraischer Funktionen in Quadrate; Schiefkörper über reellem Funktionenkörper; Journ. f. d. r. u. a. Math. **171** (1934) 4—11.

[23] W. Jehne-G. Dankert: *P*-adische Funktionentheorie; Seminar Köln 1966—67 (Mimeographed Notes).

[24] J. P. Serre: Abelian *l*-Adic Representations and Elliptic Curves; New York 1968 (Benjamin).

[25] S. Lichtenbaum: Duality theorems for Curves over *P*-adic Fields; Inventiones Math. **7** (1969) 120—136.

The notes [23] contain the general background of p-adic analysis which we have used.

In [24], appendix A1, the elliptic curves of Tate (as considered here) are described and an isogeny theorem is proved which partly is contained in our theorem XVIII.

The paper [25] ist to be regarded as a complement to [16], mentioned in the introduction and at the end of § 5.

L8