

JOURNAL OF NUMBER THEORY 1, 90–107 (1969)

The Singularities of the Moduli Schemes of Curves*

HERBERT POPP

*Division of Mathematical Sciences,
Purdue University, Lafayette, Indiana 47907*

Communicated by P. Roquette

Received November 17, 1967; revised March 1, 1968

The author gives a characterization of the singularities of the coarse moduli schemes for curves of genus ≥ 3 in terms of the automorphism group of the curves.

INTRODUCTION

For each integer $g \geq 0$ there exists a quasi-projective scheme M_g , defined over the integers \mathbf{Z} , such that for any algebraically closed field k the k -valued points of M_g and the classes of curves of genus g defined over k (the classes with respect to birational equivalence) are in one-to-one correspondence in a functorial way. This is known by Mumford [11] and Grothendieck [7].

Quasi-projective over \mathbf{Z} means in this context that the scheme M_g is an open set of a projective variety, which is defined over the integers \mathbf{Z} .

We prove the following theorem about the singularities of the scheme M_g . k is always an algebraically closed field of arbitrary characteristic.

MAIN THEOREM. (1) *For $g \geq 4$ a k -valued point of M_g is regular if and only if the automorphism group of the corresponding curves is trivial.* (2) *In the case $g = 3$ a k -valued point of M_g is regular if the corresponding curves have only trivial automorphisms. The module points of non-hyperelliptic curves of genus 3 (defined over k) with a nontrivial automorphism group are singular on M_g .*

The results of the theorem are incomplete for genus 3. With our methods we were not able to handle points on the scheme M_3 which correspond to

* This work was supported by the Purdue Research Foundation Grant No. 5009 and by the National Science Foundation under NSF-GP-6388 at Purdue University.

hyperelliptic curves. One may expect that such a hyperelliptic module point of M_3 is regular if and only if the corresponding hyperelliptic curve has only two automorphisms. (For characteristic zero this result was proved by Rauch [13].)

For genus $g = 2$ a complete description of the singularities of the moduli scheme in any characteristic, can be found in Igusa's paper [9]. For $g = 1$ the moduli scheme is the affine line $\text{Spec}(\mathbf{Z}[X])$, see Deuring [16]; for $g = 0$ the moduli scheme is a point. For characteristic zero the theorem was proved by Rauch [13] who uses analytic methods. Our proof is algebraic and is valid for every characteristic.

The following statements describe the essence of the proof for $g > 3$. The proof is based on the existence of the "higher level" moduli schemes $J_{g,n}$ for Jacobians of a fixed dimension g , and the relation of these higher level moduli schemes to M_g . For each natural number $n \geq 1$ one gets a n -level moduli scheme $J_{g,n}$. The scheme $J_{g,n}$ is quasi-projective over $\text{Spec}(\mathbf{Z}) - \cup_{p|n} (p)$. ($\text{Spec}(\mathbf{Z}) - \cup_{p|n} (p)$ denotes the open subscheme of $\text{Spec}(\mathbf{Z})$ which consists of all prime ideals (p) of \mathbf{Z} with $p \nmid n$.) "High level" means that n is sufficiently large. These high level moduli schemes $J_{g,n}$ are nonsingular and ramified Galois coverings of M_g with $\text{GL}(2g, \mathbf{Z}/(n))$ as Galois group. ($\text{GL}(2g, \mathbf{Z}/(n))$ consists of all $2g \times 2g$ -matrices with elements in $\mathbf{Z}/(n)$ and whose determinants are units in $\mathbf{Z}/(n)$.) Using Torelli's theorem one concludes that a k -rational point P of M_g is ramified in such a covering $J_{g,n}$ (n big) if and only if the corresponding curves have nontrivial automorphisms. One even knows that the stabilizer (or inertia group) of a point Q of $J_{g,n}$ with respect to $\text{GL}(2g, \mathbf{Z}/(n))$, which lies over $P \in M_g$, is isomorphic to the automorphism group of the curves corresponding to the point P .

In particular it follows that a k -valued point P of M_g is ramified in the covering, given by a scheme $J_{g,n}$ (n big) if and only if the curves which correspond to P have a nontrivial automorphism group.

Consequently it remains to show that the k -valued points of M_g which correspond to curves with non trivial automorphisms lie in a subset of codimension 2 in M_g provided $g > 3$. (In the case of genus 3 the general hyperelliptic field is in codimension 1, which causes the difficulties.)

If this fact is proved, the theorem follows immediately for $g > 3$, as by the purity of the branch locus, the ramified points of a covering

$$J_{g,n} \rightarrow M_g$$

must be singular, otherwise we would have to have ramification in codimension 1. On the other hand, the nonramified points of M_g are regular, since for large n the scheme $J_{g,n}$ is nonsingular.

We describe in Section 1 the construction of the scheme M_g and the higher level moduli schemes $J_{g,n}$.

In Section 2 and 3 we prove that the k -valued points of M_g , whose corresponding curves have nontrivial automorphisms are in codimension 2 if $g > 3$, and that only the general hyperelliptic curves are in codimension 1 if $g = 3$.

We readily get the following result: Each general curve of genus $g \geq 3$ has a trivial automorphism group. (A general curve is a curve defined over an algebraically closed field k of characteristic $p \geq 0$ such that the corresponding moduli point of M_g is a general point for one of the components of the subscheme $M_g \times \text{Spec}(k_p)$ of M_g . k_p denotes the prime field of the field k . $M_g \times \text{Spec}(k_p)$ is the fibre of the scheme $M_g \rightarrow \text{Spec}(\mathbb{Z})$ over the closed point (p) of $\text{Spec}(\mathbb{Z})$. $M_g \times \text{Spec}(k_p)$ parametrizes the classes of curves of genus g which are defined over algebraically closed fields of characteristic p .)

1. THE MODULI SCHEME FOR CURVES OF GENUS g AND THE MODULI SCHEME OF LEVEL n OF THE JACOBIANS OF DIMENSION g .

This section presents a brief sketch of the construction of the moduli scheme for curves and the moduli scheme for level n -structures of the Jacobians, and the relations of these schemes. All proofs of the theorems we mention here can be found in Mumford's book [11].

We first have to fix terminology and notation.

DEFINITION. Let S be a noetherian scheme. A curve Γ/S of genus g over S is a morphism $\pi: \Gamma \rightarrow S$ which is simple, proper, and whose geometric fibres are irreducible curves of genus g .

We now fix the genus g ($g \geq 2$) and consider the following contravariant functor \mathcal{M}_g from the category of noetherian schemes to the category of sets

$$\mathcal{M}_g: S \rightarrow \left\{ \begin{array}{l} \text{set of curves of genus } g \\ \text{defined over } S \text{ modulo isomorphism} \end{array} \right\}$$

Remark 1. If S and T are noetherian schemes and if $f: T \rightarrow S$ is a morphism, then $\mathcal{M}_g(f): \mathcal{M}_g(S) \rightarrow \mathcal{M}_g(T)$ is defined by taking for a curve $\pi: \Gamma \rightarrow S$ the pullback curve $p_2: \Gamma \times_T S \rightarrow T$ to the scheme T .

Remark 2. For a scheme M the functor $h_M: S \rightarrow \text{Hom}(S, M)$ from the category of noetherian schemes to the category of sets is called the point functor of the scheme M . One also says M represents the functor h_M . In general a functor F from the category of noetherian schemes to the category of sets is called representable, if there exists a scheme M such that F is isomorphic to the point functor h_M of M .

The following definition is important.

DEFINITION. A scheme M_g and a morphism ϕ from the functor \mathcal{M}_g to the functor $h_{M_g}(S) = \text{Hom}(S, M_g)$ is called a coarse moduli scheme if

(a) for all algebraically closed fields k the map $\phi(\text{Spec}(k)) : \mathcal{M}_g(\text{Spec } k) \rightarrow h_{M_g}(\text{Spec } k)$ is an isomorphism, and

(b) h_{M_g} is universal in the following sense: Given any other scheme N and a morphism ψ from \mathcal{M}_g to the representable functor h_N , there is a unique morphism $\chi : h_{M_g} \rightarrow h_N$, such that $\psi = \chi \circ \phi$.

The following theorem can be found in Mumford's book [11], page 143:

THEOREM 1. *There exists a coarse moduli scheme M_g for curves of a fixed genus g ($g \geq 0$) which is quasi-projective over $\text{Spec } (\mathbb{Z})$. Each irreducible component of the closed subscheme $M_g \times \text{Spec}(k_p)$ of M_g is of dimension $3g - 3$ if $g \geq 2$ and of dimension g for $g = 0$ and $g = 1$.*

Remark. The last assertion of Theorem 1 follows from the fact that the fibre $M_g \times \text{Spec}(\mathbb{Q})$ is irreducible and of the described dimension. See Ahlfors [19]. Now the fact that M_g is quasi-projective over \mathbb{Z} together with the construction of M_g as a quotient of a smooth scheme $J_{g,n}$ (see page 7) implies that $M_g \times \text{Spec}(k_p)$ is the specialization of $M_g \times \text{Spec}(\mathbb{Q})$ with respect to the valuation of \mathbb{Q} given by the prime number p . $M_g \times \text{Spec}(k_p)$ is therefore pure dimensional and the dimension of the components are as described. See Mumford [20], chapter 2.

Next we consider polarized Jacobian varieties with level n -structures.

Let $\Gamma \rightarrow S$ be a curve over a locally noetherian scheme S . Let $\text{Pic}^r(\Gamma/S)$ be the divisor classes of Γ/S numerically equivalent to zero. $\text{Pic}^r(\Gamma/S)$ is in a natural way an abelian variety over S (that is, $\text{Pic}^r(\Gamma/S) \rightarrow S$ is a group scheme over S which is simple and proper with connected fibres). Call this scheme $J(\Gamma)$ the Jacobian of the curve Γ/S . The curve Γ can be canonically embedded into $J(\Gamma)$; denote the canonical embedding by

$$\begin{array}{ccc} \alpha : \Gamma & \rightarrow & J(\Gamma) \\ & \searrow & \swarrow \\ & S & \end{array}$$

Let Θ be the canonical divisor class (the Θ -divisor class) of $J(\Gamma)$. This divisor class on $J(\Gamma)$ is ample and defines therefore a polarization, called the canonical polarization of $J(\Gamma)$, that is, a morphism

$$\Theta : J(\Gamma) \rightarrow \mathbf{P}^N \times_S S$$

In the notation of Mumford [11], page 121, the canonical polarization of $J(\Gamma)$ given by Θ is of degree 1. For the notation of the canonical polarization of a Jacobian variety see Matsusaka [17] and Weil [18].

Definition of a level n -structure of an abelian variety.

DEFINITION. Let $\pi: X \rightarrow S$ be an abelian scheme whose fibres have dimension g . Assume that the characteristics of the residue fields of all geometric points $s \in S$ do not divide n . If $n \geq 2$, a level n -structure of X/S consists of $2g$ sections, $\sigma_1, \dots, \sigma_{2g}$ of X over S , such that

- (1) for all geometric points $s \in S$ the images $\sigma_i(s)$ form a base for the group of points of order n on the fibres X_s (X_s denotes the constant field extension of the fibre over s to the algebraic closure of the residue field of s);
- (2) $\psi_n \circ \sigma_i = \varepsilon$, where $\psi_n: X \rightarrow X$ is the morphism which is given by multiplication with n , and ε is the identity morphism.

DEFINITION. X/S without a n -partition point structure is called a level 1 structure.

DEFINITION. Let S be a locally noetherian scheme. $\mathcal{J}_{g,n}(S)$ is the set of triples up to isomorphism, where the triples are given as

- (1) a Jacobian scheme X over S of dimension g ;
- (2) the canonical polarization Θ of X ;
- (3) a level n structure $\sigma_1, \dots, \sigma_{2g}, g$ of X over S .

One checks that $\mathcal{J}_{g,n}$ is a contravariant functor from the category of locally noetherian schemes to the category of sets.

DEFINITION. If the functor $\mathcal{J}_{g,n}$ is represented by a scheme $J_{g,n}$, then this scheme is called a fine moduli scheme of level n for canonical polarized Jacobian varieties of dimension g .

We have also to introduce the notion of a coarse moduli scheme of level n for canonical polarized Jacobian varieties.

DEFINITION. Suppose J is a scheme and ϕ is a morphism from $\mathcal{J}_{g,n}$ to the point functor $h_J(h_J(S) = \text{Hom}(S, J))$, represented by J . Then J is called a coarse moduli scheme if

- (1) for all algebraically closed fields k , $\phi(\text{Spec } k) : \mathcal{J}_{g,n}(\text{Spec } k) \rightarrow h_J(\text{Spec } k)$ is an isomorphism.
- (2) for all morphism ψ from $\mathcal{J}_{g,n}$ to a representable functor h_A there is an unique morphism $\chi : h_J \rightarrow h_A$ such that $\psi = \chi \circ \phi$.

The following is known about the representability of the functor $\mathcal{J}_{g,n}$. See Mumford [11] and Grothendieck* [7].

* Instead of the described functor $\mathcal{J}_{g,n}$ one could also use for the following arguments the functor which Grothendieck calls in [7], Exp. 17, “foncteur Jacobi d’échelon.”

THEOREM 2. (1) *For all g, n there exists a coarse moduli $J_{g,n}$ scheme which is quasi-projective over $\text{Spec}(\mathbf{Z}) - \cup_{p|n} (p)$.*

(2) *If n is big (it is enough to take $n \geq 3$) the functor $\mathcal{J}_{g,n}$ is representable by a scheme $J_{g,n}$ which is quasi-projective over $\text{Spec}(\mathbf{Z}) - \cup_{p|n} (p)$. In other words, for big n a fine moduli scheme $J_{g,n}$ of level n for canonical polarized Jacobian varieties of dimension g exists.*

The proof of the above theorem is in Mumford's book [11]. There, the corresponding theorem is proved for abelian varieties. This proof carries over to the Jacobian functor by the following remark:

By Mumford [11], Proposition 7.3, and by the results of Matsusaka [10] and Hoyt [8], there exists a locally closed subscheme $H'_{g,n}$ of $H_{g,1,n}$ (in the notation of Mumford [11], Proposition 7.3) which represents the following functor $\mathcal{H}'_{g,n}$:

DEFINITION OF $\mathcal{H}'_{g,n}$. For a locally noetherian scheme S let $\mathcal{H}'_{g,n}(S)$ be the set of all linearly rigidified Jacobian schemes X/S with level n -structure and the canonical polarization up to isomorphism. (See for the notion of a linear rigidification Mumford [11], p. 130.) $\mathcal{H}'_{g,n}$ is the functor defined by the sets $\mathcal{H}'_{g,n}(S)$.

Mumford's construction applied to the scheme $H'_{g,n}$ instead of $H_{g,1,n}$ gives the desired result. See also Mumford [12].

We need further information about the scheme $J_{g,n}$. The relation between the schemes $J_{g,1}$ and $J_{g,n}$ is the following:

THEOREM 3. *Let $\Gamma_n = \text{GL}(2g, \mathbf{Z}/n)$ be the group of $2g \times 2g$ -matrices (a_{ij}) where $a_{ij} \in \mathbf{Z}/(n)$ and $\det(a_{ij})$ is a unit in $\mathbf{Z}/(n)$. Then Γ_n acts on the quasi-projective scheme $J_{g,n}$ and the quotient $J_{g,n}/\Gamma_n$ is isomorphic to the scheme $J_{g,1}$. (Γ_n acts in a natural way on the level n -structure $\sigma_1, \dots, \sigma_{2g}$. The action of Γ_n on $J_{g,n}$ comes from this. See Mumford [11], page 141.) This theorem states that the scheme $J_{g,n}$ is a Galois covering of the scheme $J_{g,1}$ with Γ_n as Galois group.*

We will study the covering $J_{g,n} \rightarrow J_{g,1}$ more closely and in particular characterize the ramification points of this covering.

THEOREM 4. *A geometric point P of $J_{g,1}$ is ramified in the covering $J_{g,n} \rightarrow J_{g,1}$ (n big) if and only if the canonical polarized Jacobian varieties which correspond to P have nontrivial automorphisms. Furthermore, if n is big, the stabilizer of a point P^* of $J_{g,n}$ over P is isomorphic to the group of automorphisms of the canonical polarized Jacobian varieties corresponding to P .*

Proof. It suffices to prove the second part of the theorem. For if $\Gamma_n(P^*) = \{\sigma \in \Gamma_n : P^{*\sigma} = P^*\}$ is the stabilizer of P^* one knows that $\Gamma_n(P^*)$ is nontrivial if and only if the point P is ramified in the covering $J_{g,n} \rightarrow J_{g,1}$ (P is a geometric point of $J_{g,1}$). It follows then by the definition of the action of Γ_n on $J_{g,n}$, that there exists a homomorphism of the automorphism group of any canonical polarized Jacobian variety X which has P^* as point on $J_{g,n}$ into the group $\Gamma_n(P^*)$. This homomorphism is onto and has a trivial kernel according to the Rigidy Lemma of Serre [14].

Of further importance for us is the following theorem.

THEOREM 5. *The scheme $J_{g,n} \rightarrow \text{Spec}(\mathbf{Z}) - \cup_{p|n} (p)$ is nonsingular if n is big.*

Proof. We recall the following general notion: A contravariant functor $F: S \rightarrow F(S)$ from the category of locally noetherian Y -schemes S [Y is a fixed scheme, for the functor $\mathcal{J}_{g,n}$ the scheme Y is $\text{Spec}(\mathbf{Z}) - \cup_{p|n} (p)$] into the category of sets is called *nonsingular* over Y , if for all Y -schemes $Y' = \text{Spec}(A)$, where A is an Artinian ring, locally finite over 0_y for all $y \in Y$, and for all closed subschemes Y'_0 of $Y'(Y'_0 \neq \emptyset)$ the canonical map $F(Y') \rightarrow F(Y'_0)$, given by $Y'_0 \rightarrow Y'$, is onto. [see Grothendieck [6] Theorem 3.1 (III).]

Furthermore recall that the point-functor h_M of a Y -scheme M is nonsingular in the above sense if and only if the Y -scheme M is nonsingular. Grothendieck [6] proved that the functor $\mathcal{J}_{g,n}$ for all n is nonsingular over $\text{Spec}(\mathbf{Z}) - \cup_{p|n} (p)$. This fact together with Theorem 2 implies Theorem 5.

Remark. Grothendieck [6] also showed that the functor \mathcal{M}_g is nonsingular over $\text{Spec}(\mathbf{Z})$. This fact together with the main result of this paper implies that the functor \mathcal{M}_g is not representable or which is the same, that a fine moduli scheme for curves of genus g does not exist. To see this a little better assume for a moment that \mathcal{M}_g is representable over \mathbf{Z} by a scheme M_g . Then the scheme M_g would be nonsingular for the functor \mathcal{M}_g is nonsingular. But this is not true as we prove.

It remains to show that the coarse moduli scheme $J_{g,1}$ is also a coarse moduli scheme for curves of genus g . This is proved in Mumford's book [11], page 143.

Remark. Torelli's theorem [15] implies that the automorphism group of a nonsingular curve of genus $g \geq 3$ over a field k and the automorphism group of the canonical polarized Jacobian variety of this curve are canonically isomorphic.

To make this more precise we first note that an automorphism σ of a nonsingular curve C/k (k an algebraic closed field) induces in a natural way an automorphism of the Jacobian $J(C)$ of C . This follows immediately from the following property of the Jacobian of C :

For any field extension K of k there exists a 1-1 correspondence

$$\left\{ \begin{array}{l} \text{points of } J(C) \text{ with} \\ \text{values in } K \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} K\text{-rational divisor} \\ \text{classes of degree 0 on } C \end{array} \right\}$$

Call σ' the automorphism of the Jacobian which is induced by σ . Furthermore σ' preserves the canonical class of the Jacobian. Our construction leads therefore to a homomorphism of the automorphism group of C/k into the automorphism group of the canonical polarized Jacobian variety $J(C)$ of the curve C .

Next Torelli's theorem implies that this homomorphism is an isomorphism onto the automorphism group of the canonical polarized Jacobian $J(C)$. Let σ' be an automorphism of the canonically polarized Jacobian variety $J(C)$. Now examine the diagram

$$(*) \quad \begin{array}{ccc} C & \xrightarrow{\alpha} & J(C) \\ \downarrow \sigma & & \downarrow \sigma' \\ C & \xrightarrow{\alpha'} & J(C) \end{array}$$

Torelli's theorem states there exists an automorphism $\sigma : C \rightarrow C$, such that the diagram (*) is commutative up to a translation of $J(C)$; that is, for all $P \in C$:

$$\alpha\sigma(P) = \sigma'\alpha(P) + a, \quad a \in J(C).$$

σ and a are uniquely defined by α and σ' and one checks that σ' is the automorphism of the Jacobian $J(C)$ which is defined by the automorphism σ of the curve C in the described way.

We can now reformulate Theorem 4.

THEOREM 4a. *Let $\Pi : J_{g,n} \rightarrow J_{g,1}$ be the covering of Theorem 4 (n sufficiently large). If we regard $J_{g,1}$ as a coarse moduli scheme for curves of genus g , the following holds. For each curve $C \rightarrow \text{Spec}(k)$, where k is an algebraically closed field, let P be the corresponding k -rational point of $J_{g,1}$. Then the covering $J_{g,n} \rightarrow J_{g,1}$ is ramified at P if and only if C has a nontrivial automorphism group and furthermore, the automorphism group of C is isomorphic to the decomposition group of any point P^* of $J_{g,n}$ over P .*

2. GEOMETRIC POINTS ON THE MODULI SCHEME M_g FOR WHICH THE CORRESPONDING CURVES HAVE NONTRIVIAL AUTOMORPHISMS.

Let k_p be the prime field of characteristic p and let m be a k -valued point of M_g , where k is some field containing k_p . $k_p(m)$ is the function field of the subscheme of M_g which is generated by m . We assume that the curves which correspond to m have nontrivial automorphisms. Our aim is to estimate the transcendence degree of $k_p(m)/k_p$.

In other words, we want to see in which dimension the points of the moduli scheme M_g are whose corresponding curves have a nontrivial automorphism group. We first remark that for each geometric point m of the moduli scheme M_g there exists a curve C of genus g , which is defined over the algebraic closure $\overline{k_p(m)}$ of $k_p(m)$ with m as module point on M_g . [p is the characteristic of the residue field of m .] On the other hand, if C is a curve of genus g with m for its module point, then each algebraically closed field which is a field of definition of C contains the field $k_p(m)$. This follows immediately from the construction of M_g .

Now let m be a point of M_g and C a curve defined over an algebraic closed field k with m as module point. Let $G \neq 1$ be a cyclic automorphism group of C of prime order q (G does not have to be the whole automorphism group). The fixed curve of the group G shall be denoted by $C^G = C_0$. We have to examine the covering $C \rightarrow C_0$.

We want to construct an algebraic closed field $l (\supseteq k_p)$ over which a curve C is defined, which also has m as module point, such that the transcendence degree of l/k_p is "small" and easy to estimate. Then the inequality $\text{tr}(l/k_p) \geq \text{tr}(k_p(m)/k_p)$ will yield the desired estimate for the transcendental degree of $k_p(m)$.

For the subsequent arguments it is convenient to use the function field of the curves C and C_0 instead of the curves themselves.

Let F/k be the function field of the curve C over the field k .

The fixed field of F for the given cyclic group of automorphisms, $F_0 = F^G$, is the function field of the curve C_0 over k .

The desired field l is obtained by looking for the smallest algebraically closed field in k over which the fields F_0 and the cyclic extension F of F_0 are defined. (As usual the statement that F/F_0 is defined over a subfield l of k means that there exists a function field L_0/l of one variable and a cyclic field extension L/L_0 of degree q such that F_0 is the constant field extension of L_0 to k and F the constant field extension of L to k .) To get the right hold on the field l we have to use some known facts about cyclic field extensions of prime degree of a function field of one variable, due to Deuring [2] and Hasse and Witt [4].

These facts will be formulated next. The indicated nice way of looking at these field extensions I know from Professor Peter Roquette.

3. CHARACTERIZATION OF THE CYCLIC FIELD EXTENSIONS OF PRIME DEGREE OF A FUNCTION FIELD OF ONE VARIABLE.

Let F/k be a function field of one variable with algebraic closed constant field k of characteristic $p \geq 0$. The divisor group of F shall be denoted by D , \mathbb{C} shall denote the divisor class group of degree 0 of F .

For a prime number $q \neq p$ let \mathbb{C}_q be the group of divisor classes in \mathbb{C} annihilated by q . This group has order q^{2g} , $g = \text{genus of } F/k$.

PROPOSITION 1. *The cyclic unramified extensions E/F of degree q are in one to one correspondence with the cyclic subgroups $\langle x \rangle \neq 0$ of \mathbb{C}_q . The relation is the following: Let a be a divisor out of the class x . Further let $a \in F$ be such that $q.a = (a)$, where (a) is the principal divisor of a in F , then the field belonging to the group $\langle x \rangle$ is $E = F(a^{1/q})$.*

The proof is clear by Kummer theory. See Deuring [2].

The group \mathbb{C}_q is not changed if one makes a constant field extension. This fact implies the corollary:

COROLLARY. *Let K/k be any field extension and let F_K be the constant field extension of F to K . Each cyclic unramified extension E'/F_K of degree q is already defined over k . This means that there exists a cyclic unramified extension E/F of degree q such that $E' = E_K$.*

Now let S be a set of prime divisors or primes of the field F/k . The group which is obtained from the group D by allowing rational numbers for the coefficients of the primes in S shall be denoted by D^S . Clearly D^S contains D as a subgroup. We regard the subgroup of D^S of degree 0 and the factor group \mathbb{C}^S of this group modulo the group of principal divisors of F/k . \mathbb{C}_q^S shall be the subgroup of \mathbb{C}^S annihilated by q .

Kummer theory implies:

PROPOSITION 2. *The cyclic extensions E/F of degree q which are ramified at most at the primes of the set S are in one to one correspondence with the cyclic subgroups $\langle x \rangle \neq 0$ of \mathbb{C}_q^S in the same way as it is described in Proposition 1.*

The structure of \mathbb{C}_q^S is determined as follows. We have $\mathbb{C}_q \cong \mathbb{C}_q^S$ and

$$\mathbb{C}_q^S / \mathbb{C}_q = \mathbb{C}_q^S + \mathbb{C} / \mathbb{C} \cong (\mathbb{C}^S / \mathbb{C})_q.$$

Since \mathbb{C} is divisible, we find for $x \in \mathbb{C}^S$ with $q.x \in \mathbb{C}$ that $q.x = q.c$ with $c \in \mathbb{C}$. Therefore $x - c \in \mathbb{C}_q^S$, or $x \in \mathbb{C}_q^S + \mathbb{C}$. This implies $\mathbb{C}_q^S / \mathbb{C}_q = (\mathbb{C}^S / \mathbb{C})_q$

and therefore $\mathfrak{C}_q^S \approx \mathfrak{C}_q \times (\mathfrak{C}^S/\mathfrak{C})_q$. On the other hand we know that

$$\mathfrak{C}^S/\mathfrak{C} \subseteq D^S/D = \sum_S \mathbf{Q}/\mathbf{Z}$$

and that $\mathfrak{C}^S/\mathfrak{C}$ is characterized in D^S/D by degree $(x) = 0$ modulo \mathbf{Z} . Call this subgroup $\sum'_S \mathbf{Q}/\mathbf{Z}$.

We observe in particular that \mathfrak{C}_q^S is not changed if the constant field is extended.

Hence it follows that the corollary to Proposition 1 remains valid if one changes “unramified” to “at most ramified at the places of S ”.

Finally we consider the case $q = p > 0$.

Let V be the k -module of valuation vectors of F/k , and $V(0)$ the k -module of integral valuation vectors.

$D = V/V(0) + F$ (D is dual to the module of differentials of the 1-kind of F/k . The k -dimension of D is $g = \text{genus}(F/k)$.)

Let $\pi(x) = x^p$ be the Frobenius map, and set $\mathfrak{p}(x) = \pi(x) - x$.

The map π and \mathfrak{p} extend naturally to V and D .

Let $D_{\mathfrak{p}}$ be the kernel of \mathfrak{p} in D . By Artin-Schreier theory one knows.

PROPOSITION 3. *The unramified cyclic extensions of degree p are in one to one correspondence to the cyclic subgroups $\langle x \rangle \neq 0$ of $D_{\mathfrak{p}}$ in the following way: if $\mathbf{a} \in V$ is a representative of x and $\mathfrak{p}\mathbf{a} \equiv \mathbf{a}$ modulo $V(0)$ with $a \in F$, then the extension to $\langle x \rangle$ has the form $E = F(b)$ with $\mathfrak{p}(b) = a$.*

Hasse and Witt [4] have shown that D can be written in a unique way in the form

$$D = D_0 \oplus D_1 \quad (\oplus = \text{direct sum})$$

where D_0 consists of the elements of D which are annihilated by a power of π , and where D_1 has a k -base consisting of elements u_1, \dots, u_y which are kept fixed under π . The kernel of the map $\mathfrak{p} = \pi - 1$ in D is therefore the group which is generated by u_1, \dots, u_y over the prime field. This group is elementary abelian of degree p^y ($0 \leq y \leq g$).

Now let K be a field extension of k and F_K the constant field extension of F to K . Let V_K, D_K be the corresponding modules. We have then

$$D_K = D \otimes_k K, \quad (D_K)_0 = D_0 \otimes_k K, \quad (D_K)_1 = D_1 \otimes_k K$$

and therefore $(D_K)_{\mathfrak{p}} = D_{\mathfrak{p}}$.

Consequently the corollary to Proposition 1 also holds for $p = q$.

Now let S be again a set of primes of the field K/k . We will characterize the cyclic field extensions of F of degree p which are ramified at most at the primes of S .

The components of V are the completions \hat{F}_η of F respectively the primes η of F . The field $\hat{F}_\eta = k((t))$ is the power series field over k in one variable t .

Let Ω be the algebraic closure of $k((t))$.

The module V^S shall be the k -module which is obtained from V by taking for the primes $\eta \in S$ components from Ω (instead of $k((t))$). Let $D^S = V^S/V(0) + F$.

The maps π and p are naturally defined on D^S . The kernel of p in D^S shall be denoted by D_p^S . We have therefore

PROPOSITION 4. *The cyclic field extensions E/F of degree p , which are ramified at most at primes of S , are in one-to-one correspondence with the cyclic subgroups $\langle x \rangle \neq 0$ of D_p^S as it is described in Proposition 3.*

Using the divisibility of D by p which comes from the Hasse-Witt factorization of D , one gets as above

$$D_p^S \approx D_p \times (D^S/D)_p = D_p \times \sum_S (\Omega/k((t)))_p.$$

We have also

$$(\Omega/k((t)))_p \approx k((t))/k[[t]] + pk((t)).$$

This result states that each power series in $k((t))$ can be written, modulo p and modulo integral power series, in a unique way in the form

$$(1) \quad \sum_{\substack{\lambda > 0 \\ \lambda \not\equiv 0 \pmod{p}}} a_\lambda t^{-\lambda} \quad (a_\lambda \in k, \text{ only finite many } a_\lambda \text{ appear})$$

For $x \in D_p^S$ we call the power series of the form (1) which is obtained for a prime $\eta \in S$, the normed principal part of x at η .

Now let K be a field extension of k . If $x \in (D_K^S)_p$, we find that the coefficients of the principal parts of x for the primes $\eta \in S$ lie in general in K . (We shall say that they are defined over K .) If these coefficients are already in k , we have $x \in D_p^S$. This means that the field extension E of F_K which corresponds to $\langle x \rangle$ is already defined over k . We have therefore

COROLLARY. *Let K be a field extension of k and E' be a cyclic extension of degree p of the function field F_K which is ramified at most at the primes $\eta \in S$. Let $x \in (D_K^S)_p$ be a generator of the subgroup of $(D_K^S)_p$ which describes E' . Then E' is defined over k if and only if the normed principal parts of x at the primes of S are defined over k .*

This means by construction that $E' = F_K(b)$ with $b^p - b = a$; and we can write the element a for all primes $\eta \in S$ in the form

$$a = \sum_{\lambda > 0} a_\lambda t^{-\lambda} + (u^p - u) + v$$

with $a_\lambda \in k$; $u, v \in F_K$, $v(\eta) \neq \infty$.

We can now describe the field \mathcal{L} .

The case $q \neq p$. In the notation of page 98 let P_1, \dots, P_n be the points of the curve C_0 which are ramified in the covering $C \rightarrow C_0$. Let $S = \{\eta_1, \dots, \eta_n\}$ be the set of primes of F_0/k which correspond to the points P_v . Applying the corollaries to Propositions 1 and 2 to the field extension F/F_0 and the set S , we find immediately that F/F_0 is defined over the algebraic closure \mathcal{L} of the field $k_p(m_0, P_1, \dots, P_n)$. (Here m_0 denotes the module point of C_0 , $k_p(m_0, P_1, \dots, P_n)$ is the smallest field extension of $k_p(m_0)$ in k over which the primes η_1, \dots, η_n are rational. Because C_0 is nonsingular this field is obtained by adjoining the affine coordinates of the Points P_v to the field $k_p(m_0)$. This explains the notation $k_p(m_0, P_v)$ for this field.)

To estimate the transcendence degree of \mathcal{L}/k_p is the same as to estimate the transcendence degree of $k_p(m_0, P_1, \dots, P_n)/k_p$. A boundary for the latter is obviously $\dim(M_{g_0} \times \text{Spec } k_p) + n$ ($g_0 = \text{genus of } C_0$). The subsequent work of this section deals with the comparison of the number $\dim(M_{g_0} \times \text{Spec } k_p) + n$ with the dimension $3g - 3$ of the scheme M_g . To do this we use Hurwitz's genus formula and get

$$g - 1 = q(g_0 - 1) + \frac{n}{2}(q - 1)$$

We have to distinguish several cases.

(1) If $g_0 = 0$ then

$$n = \frac{2(g-1)+2q}{q-1} = \frac{2\left(\frac{g-1}{q}\right)+2}{1-(1/q)} \quad (**)$$

If $q = 2$ then C is hyperelliptic, and we conclude directly from the theory of moduli for hyperelliptic fields that

$$\text{tr}(k_p(m)|k_p) \leq 2g - 1 = \begin{cases} 3g - 4 & \text{if } g = 3 \\ \leqslant 3g - 5 & \text{if } g \geqslant 4 \end{cases}$$

($2g - 1$ is a dimension of the moduli scheme for hyperelliptic fields of genus g ; see Fischer [5].)

If $q > 2$ we get from (**)

$$n \leq \frac{2 \cdot \frac{g-1}{3} + 2}{1 - \frac{1}{3}} = g + 2 \leq \begin{cases} 3g - 4 & \text{if } g = 3 \\ 3g - 5 & \text{if } g > 3 \end{cases}$$

Our calculation shows so far that for $g = 3, g_0 = 0$, and $q = 3$ it may happen that $\text{tr}(k_p(m)|k_p) = 5$. But, if this should be the case, then the ramification points P_1, \dots, P_5 of the covering $C \rightarrow C_0$ are algebraically independent over $k_p(m_0) = k_p$. We have to change the curve C and have

to show that there exists a curve C' of genus 3 birationally equivalent to C over the algebraic closure $\overline{k_p(P_1, \dots, P_n)}$ of $k_p(P_1, \dots, P_n)$ which is defined over a subfield of $\overline{k_p(P_1, \dots, P_n)}$ of transcendence degree < 5 .

For the proof let P'_1, P'_2, P'_3 be 3 different points of the rational curve C_0 with coefficients in the algebraic closure $\overline{k_p}$ of k_p . Let σ be the automorphism of C_0 , such that $P'_1 = P_1^\sigma, P'_2 = P_2^\sigma, P'_3 = P_3^\sigma$. By extending σ to C we get a curve C' which is also a covering of C_0 of degree q and which is ramified at the points P'_1, \dots, P'_5 . The curve C' is defined over the field $\overline{k_p(P_v^\sigma)}$ which has transcendence degree ≤ 2 .

It remains to show that the curves C and C' have the same moduli point. This is clear, for the function field K and K' of the curves C and C' are isomorphic over the algebraic closure of the field $k_p(P_1, \dots, P_n)$ which is a common field of definition for C and C' (or K and K'), and which contains the field $k_p(m)$.

We obtain therefore the following results: $\text{tr}(k_p(m)/k_p) \leq 3g - 5$ if m is the module point of a curve C of genus $g > 3$ with a nontrivial automorphism group of order $q \neq p$; if $g = 3$, the general hyperelliptic module point is in codimension 1 of the scheme M_3 ; all other module points where the corresponding curves have automorphisms of order q unequal to p are in codimension 2.

(2) $g_0 = 1$. We have

$$g - 1 = (n/2)(q - 1)$$

or

$$n = [2(g - 1)]/(q - 1)$$

If $q = 2$, then

$$n = 2(g - 1) = \begin{cases} 3g - 5 & \text{if } g = 3 \\ < 3g - 5 & \text{if } g > 3 \end{cases}$$

If $q > 2$, we have

$$n \leq [2(g - 1)]/2 = g - 1 < 3g - 5 \quad \text{for } g \geq 3$$

Let m_0 again be the module point of C_0 on the scheme M_1 . We get then

$$\text{tr}(k_p(m_0, P_v)|k_p) \leq n + 1 \leq \begin{cases} 3g - 4 & \text{if } g = 3 \text{ ad } q = 2 \\ 3g - 5 & \text{if } g > 3 \text{ or } (g = 3 \text{ and } q > 2) \end{cases}$$

Thus we first have the following estimate

$$\text{tr}(k_p(m)|k_p) \leq \begin{cases} 3g - 4 & \text{if } g = 3 \text{ ad } q = 2 \\ 3g - 5 & \text{if } g > 3 \text{ or } (g = 3 \text{ and } q > 2) \end{cases}$$

We shall prove now that $\text{tr}(k_p(m)/k_p) \leq 3g - 5$ always holds in this case.

Note that, for $g = 3$, $\text{tr}(k_p(m)/k_p) = 3g - 4 = 5$ can only happen, if the ramification points P_1, \dots, P_4 of the covering $C \rightarrow C_0$ are algebraically

independent over $k_p(m_0)$. If this is the case, we change the curve C in essentially the same way as we did before in the case $g_0 = 0$. We show that there exists a curve C' of genus 3 birationally equivalent to C over the algebraic closure of $k_p(m_0)(P_1, \dots, P_4)$, which is defined over a subfield of $k_p(m_0)(P_1, \dots, P_4)$ of transcendence degree ≤ 4 over k_p .

For the proof let P be a point of C_0 which is $k_p(m_0)$ rational. (That is, the coordinates of P are in the algebraic closure of $k_p(m_0)$.) Let σ be an automorphism of the elliptic curve C_0 , defined over $k_p(m_0)(P_1, \dots, P_4)$, such that $P_1^\sigma = P$. Such a σ always exists. See Eichler [2].

By extending σ to C , we get a curve C' as image which is also a covering of C_0 and is ramified exactly at the points $P, P_2^\sigma, P_3^\sigma, P_4^\sigma$. The curve C' is obviously defined over the algebraic closure of $k_p(m_0)(P, P_2, P_3, P_4)$ and this field has transcendence degree ≤ 4 by construction. Furthermore the construction of the curves C and C' yields that they are isomorphic over the algebraic closure of the field $k_p(m_0, P_1, P_2, P_3, P_4)$ which is a common field of definition for C and C' . The curves C and C' have therefore the same moduli point on M_g , and we get in this case the estimate

$$\text{tr}(k_p(m)/k_p) \leq 3g - 5 \quad \text{for } g \geq 3$$

(3) $g_0 > 1$. We have

$$2(g-1) = 2q(g_0-1) + n(q-1)$$

or

$$n = \frac{2(g-1) - 2q(g_0-1)}{q-1}$$

and therefore for all q and $g - n \leq 2(g-1) - 4(g_0-1)$. This inequality implies $3g_0 - 3 + n \leq 2(g-1) - (g_0-1) \leq 3g - 5$, if $g \geq 3$ and therefore the estimate $\text{tr}(k_p(m)/k_p) \leq 3g - 5$.

The case $p = q$. Let P_1, \dots, P_n be the points of C_0 which are ramified for the covering $C \rightarrow C_0$. Let $S = \{\eta_1, \dots, \eta_n\}$ be the set of places of the function field F_0/k which correspond to the points P_1, \dots, P_n . Suppose that $F = F_0(b)$ with $b^p - b = a$ and $a \in F_0$ (for the notation see page 101). For a place $\eta \in S$ let

$$\sum_{\mu=1}^{\lambda_\eta} a_{v\mu} t^{-\mu}$$

be the normed principal part of a . The integers λ_η are ≥ 1 for all $\eta = 1, \dots, n$ because the places η_η are ramified in F .

Applying now the corollary to Proposition 4 we find that the cyclic field extension F/F_0 is defined over the algebraic closure l of the field $k_p(m_0, P_1, \dots, P_n)(a_{11}, \dots, a_{1\lambda_1}, a_{21}, \dots, a_{n\lambda_n})$. The elements $a_{v\mu}$ are those which appear in the principal parts of a at the primes $\eta_v \in S$.

If the covering $C \rightarrow C_0$ is unramified l is just the algebraic closure of the field $k_p(m_0)$. It is now easy to estimate the transcendence degree of l . We get

$$\mathrm{tr}(l|k_p) \leq \mathrm{tr}(k_p(m_0)|k_p) + n + \sum_{v=1}^n \lambda_v = \mathrm{tr}(k_p(m_0)|k_p) + \sum_{v=1}^n (\lambda_v + 1)$$

and from this by a previous remark

$$\mathrm{tr}(k_p(m)|k_p) \leq \mathrm{tr}(k_p(m_0)|k_p) + \sum_{v=1}^n (\lambda_v + 1)$$

Again the numbers

$$\mathrm{tr}(k_p(m_0)|k_p) + \sum_{v=1}^n (\lambda_v + 1)$$

and $3g - 3$ have to be compared. Using Hurwitz formula for the genus of a covering we get

$$(\ast\ast\ast) \quad g - 1 = p(g_0 - 1) + \frac{1}{2} \sum_{v=1}^n (\lambda_v + 1)(p - 1)$$

where $\lambda_v + 1$ is the contribution of the point P_v to the discriminant of the field extension F/F_0 . See Hasse [3].

Equation $(\ast\ast\ast)$ implies

$$\sum_{v=1}^n (\lambda_v + 1) = \frac{2(g - 1) - 2p(g_0 - 1)}{p - 1}$$

Again several cases have to be distinguished.

(1) $g_0 = 0$ We have

$$\sum_{v=1}^n (\lambda_v + 1) = \frac{2(g - 1) + 2p}{p - 1}$$

Now, if $p = 2$, the curve C is hyperelliptic, and we get

$$\mathrm{tr}(k_p(m)|k_p) \leq 2g - 1 \leq \begin{cases} 3g - 4 & \text{if } g = 3 \\ 3g - 5 & \text{if } g > 3 \end{cases}$$

Assume therefore $p \geq 3$. Then the relation $(\ast\ast\ast)$ yields

$$\sum_{v=1}^n (\lambda_v + 1) = \frac{\frac{2(g - 1)}{p} + 2}{\frac{1}{1 - 1/p}} \leq \frac{\frac{2(g - 1)}{3} + 2}{\frac{2}{3}} = g + 2 \leq \begin{cases} 3g - 4 & \text{if } g = 3 \\ 3g - 5 & \text{if } g > 3 \end{cases}$$

Together we get the following estimate:

$$\mathrm{tr}(k_p(m)|k_p) \leq \begin{cases} 3g - 4 & \text{if } g = 3 \\ 3g - 5 & \text{if } g > 3 \end{cases}$$

Using the same procedure as in the tamely ramified case one can always conclude

$$\mathrm{tr}(k_p(m)|k_p) \leq 3g - 5 \quad \text{for } p \geq 3 \text{ and } g \geq 3$$

For in the case $g = 3$ and $p = 3$ the equality $\text{tr}(k_p(m)|k_p) = 3g - 4$ can only hold if all ramification points of the covering F/F_0 are *not* \bar{k}_p -rational (one has one or two ramification points). But then, applying an automorphism σ of F_0 over $\bar{k}_p(P_1, \dots, P_n)$, we can make at least one of the points $P_1^\sigma, \dots, P_n^\sigma$ \bar{k}_p -rational. Denoting F^σ the image of an extension of the automorphism σ to F then the same conclusion as on page 104 gives the desired result.

(2) $g_0 = 1$. We get

$$\sum_{v=1}^n (\lambda_v + 1) = \frac{2(g-1)}{p-1} \leq 2(g-1)$$

and therefore

$$\text{tr}(k_p(m)|k_p) \leq \begin{cases} 3g-4 & \text{if } g = 3 \\ 3g-5 & \text{if } g > 3 \end{cases}$$

Using the same arguments as in the case $g_0 = 1$ and $q \neq$ characteristic p , we find again

$$\text{tr}(k_p(m)|k_p) \leq 3g-5 \quad \text{for } g \geq 3$$

(3) $g_0 > 1$. We get

$$\sum_{v=1}^n (\lambda_v + 1) = \frac{2(g-1)}{p-1} - \frac{2p(g_0-1)}{p-1} \leq 2(g-1) - 4(g_0-1)$$

and therefore

$$\text{tr}(k_p(m)|k_p) \leq 3(g_0-1) + \sum_{v=1}^n (\lambda_v + 1) \leq 2(g-1) - (g_0-1) \leq 3g-5, \text{ if } g \geq 3.$$

The results proved in this chapter can be summarized by the following two theorems

THEOREM. *A general field of genus $g \geq 3$ has no automorphism.*

THEOREM. (1) *If $g > 3$ and F a field defined over an algebraically closed field k of genus g with nontrivial automorphism, then the modulpoint m of F is on M_g in codimension at least 2.*

(2) *If $g = 3$ the module point m of a nonhyperelliptic field F/k of genus 3 with nontrivial automorphism is in codimension at least 2. If the field F is hyperelliptic, then the module point M of F is in codimension 1 if and only if F is the general hyperelliptic field of genus 3.*

Proof of the main theorem. The case $g > 3$ has been handled in the introduction. In the case $g = 3$ it follows that the module points which are unramified in the covering are necessarily regular. If a module point m

corresponds to curves which are nonhyperelliptic and which have non-trivial automorphisms, then this point has to be singular. Otherwise by purity of the branch locus there would exist a point m' of M_3 in codimension 1 which is ramified for the covering $J_{3,n} \rightarrow M_3$ (n big), and such that m is in the closed subscheme, defined by m' . The point m' is then necessarily the general hyperelliptic module point. But then m has to be a hyperelliptic module point too, which is a contradiction.

ACKNOWLEDGMENT

The author wants to thank Professor O. F. G. Schilling for many stimulating conversations.

REFERENCES

1. EICHLER, M. *Einführung in die Theorie der algebraischen Zahlen und Funktionen*. Basel 1963.
2. DEURING, M. Zur arithmetischen Theorie der algebraischen Funktionenkörper. *Math. Ann.* **106**, (1932), 77–106.
3. HASSE, H. Theorie der relativ-zyklischen algebraischen Funktionenkörper insbesondere bei endlichem Konstantenkörper. *J. f.d.r.u.a. Math.* **172** (1934).
4. HASSE, H. UND WITT, E. Zyklische unverzweigte Erweiterungskörper vom Primzahlgrad p über einem algebraischen Funktionenkörper der Charakteristik p . *Monatsh. Math. Phys.* **43** (1936).
5. FISCHER, I. The moduli of hyperelliptic curves. *Trans. Am. Math. Soc.* **82** (1956).
6. GROTHENDIECK, A. Séminaire de géométrie algébrique 1960/61.
7. GROTHENDIECK, A. Séminaire Henri Cartan 1960/61.
8. HOYT, W. L. On products and algebraic families of Jacobian varieties. *Ann. Math.* **77** (1963).
9. IGUSA, J. Arithmetic variety of moduli of genus two. *Ann. Math.* **72** (1960).
10. MATSUSAKA, T. On the characterisation of a Jacobian variety. *Mem. Coll. Sci. Kyoto* **1** (1959).
11. MUMFORD, D. Geometric invariant theory. *Ergebnisse der Mathematik Bd. 34* (1965).
12. MUMFORD, D. An elementary theorem in geometric invariant theory. *Bull. Am. Math. Soc.* **67** (1961).
13. RAUCH, H. E. Singularities of the modulus spaces. *Bull. Am. Math. Soc.* **68** (1962).
14. SERRE, J. P. Séminaire Henri Cartan 1960/61. Nr. 17 Appendix.
15. WEIL, A. Zum Beweis des Torelli'schen Satzes. *Nachr. d. Akad. Wiss. Gott.* 1957.
16. DEURING, M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hamburg*, Bd. **44** (1941), 179–272.
17. MATSUSAKA, T. Polarized varieties. *Am. J. Math.* **80** (1958), 45–82.
18. WEIL, A. "Variétés Abéliennes et Courbes Algébriques." Hermann, Paris 1948.
19. AHLFORS, L. V. The complex analytic structure of the space of closed Riemann surfaces. In "Analytic Functions", pp. 45–66. Princeton University Press, Princeton 1960.
20. MUMFORD, D. Introduction to algebraic geometry. Lecture notes, Harvard University.