COMPOSITIO MATHEMATICA

TSUTOMU SEKIGUCHI

Wild ramification of moduli spaces for curves or for abelian varieties

Compositio Mathematica, tome 54, nº 3 (1985), p. 331-372
<http://www.numdam.org/item?id=CM_1985__54_3_331_0>

Compositio Mathematica 54 (1985) 331–372.

WILD RAMIFICATION OF MODULI SPACES FOR CURVES OR FOR ABELIAN VARIETIES

Dedicated to Professor S. Koizumi on his 60^{th} birthday

Tsutomu Sekiguchi

Introduction

In the present paper, we are concerned only with the field of moduli for a (complete non-singular) curve or a principally polarized abelian variety. The notion of fields of moduli was introduced first by Matsusaka [14] and treated mainly by Shimura. Here the foundation of it follows Koizumi [9]. Due to his definition, a field of moduli is, roughly speaking, the infimum of the fields of definition for the members of a geometric isomorphy class. Shimura [29] showed the fact that in general a field of moduli cannot be a field of definition, that is, in general there is no minimal field of definition. In this paper, we will treat a problem that asks whether or not the field of moduli for a curve or a principally polarized abelian variety coincides with the residue field at the point on the coarse moduli space corresponding to them. In characteristic zero, this problem was affirmatively solved by Baily [1]. Our main purpose is to give some counter examples in positive characteristic. Our results are given as follows:

1. *In characteristic* 2, *the field of moduli for a curve corresponding to the generic point x of the hyperelliptic locus in the moduli space M_g of curves of genus $g \geqslant 3$ coincides neither with the residue field at the point x nor with the field of moduli for its canonically polarized jacobian variety* (cf. Theorem 4.2 and Corollary 4.3).
2. *In characteristic* 3, *there exists a non-hyperelliptic curve of given even genus* ($\geqslant 4$), *for which the problem has a negative answer* (cf. Theorem 5.1).
3. *In characteristic p, for every $g \geqq p-1$, there exists a principally polarized abelian variety of dimension g for which the problem has a negative answer* (cf. Theorem 6.11).

In Section 1, we shall discuss some general theory about the relations between the fields of moduli and the coarse moduli space. In Section 2, for later use, we shall treat cyclic coverings of degree p of $\boldsymbol{P}^1$ in characteristic p. In Section 3, we remark some easy facts about group actions on local rings in positive characteristic. The main results will be given in Sections 4, 5 and 6.

The author would like express his hearty thanks to Professor D. Mumford for very useful conversations. He also thanks Professor T. Miyata and Dr. R. Sasaki for pointing out to him some literature on Theorem 3.4 and for very useful comments on the calculation in the proof of Theorem 2.6.

Notation

Let S be a set, and σ an automorphism of S. Then for an element x of S, sometimes we denote $\sigma(x)=x^{\sigma}$. Moreover we mean by $S^{\langle\sigma\rangle}$ the subset of S consisting of σ-invariant elements of S. Let A be a ring, and M an $A-$ module. We denote by $\mathfrak{N}(A)$ and $\mathfrak{J}(A)$ the nilradical and the Jacobson radical of A, respectively. For a subset N of M, we denote by $\langle N\rangle=\langle N\rangle_A$ the A-submodule of M generated by the elements of N. In particular, if $N=\{x_1, x_2,\dots, x_n\}$, we put $\langle N\rangle=\langle x_1,\dots, x_n\rangle$. For an integral domain A, we denote by f.f.A the field of fractions of A. For a local ring A, we denote by $\mathfrak{M}_A$ the maximal ideal of A and by $\hat{A}$ the completion of A with respect to the $\mathfrak{M}_A$-adic topology. For positive integers g and l, we denote by $A_{g,l}$ the moduli space of principally polarized abelian varieties of dimension g with a level l-structure, and by $M_{g,l}$ the moduli space of curves of genus g with a level l-structure. Throughout the paper, a word "curve" means a complete non-singular curve. In particular, when $l=1$, $A_{g,1}$ and $M_{g,1}$ are abbreviated to A_g and M_g, respectively. We denote by π_n: $A_{g,n}\to A_g$ and π_n: $M_{g,n}\to M_g$ the canonical morphisms. For a prime integer p, we put $A_{g,l}\otimes_{\boldsymbol{Z}}\boldsymbol{F}_p={}^{(p)}A_{g,l}$ and $M_{g,l}\otimes_{\boldsymbol{Z}}\boldsymbol{F}_p={}^{(p)}M_{g,l}$. For a curve C and a polarized abelian variety P, we denote by k_C and k_P the fields of moduli for C and P, respectively. We denote by $P(C)=(J(C),\ \lambda(C))$ the canonically polarized jacobian variety of C.

§1. Fields of moduli

We will start with comparing the definition of fields of moduli for curves or for polarized abelian varieties from Koizumi ([9], Definition 1.1).

Let Ω be a universal domain, and K and K' be subfields of Ω. Let Z and Z' be geometric objects (practically speaking, curves or polarized abelian varieties) over K and K', respectively.

DEFINITION 1.1: We define the *geometric isomorphy* of Z and Z' by the following:

$Z\sim Z'$ if and only if there exist a subfield L of Ω containing both K and K' and an L-isomorphism $Z\otimes_K L \xrightarrow{\sim} Z'\otimes_{K'} L$.

Under these notations, we define the *field of moduli* for Z in the following way.

DEFINITION 1.2: A subfield k_Z of Ω is called a *field of moduli* for Z, if it satisfies the following two conditions:

(1) $k_Z = \bigcap L'$, where L' runs over the set $\{L' \mid \Omega \supset L'$: a subfield; $\exists Z'$ over L' such that $Z' \sim Z\}$.

(2) For any automorphism $\sigma \in \mathrm{Aut}(\Omega)$, $Z \sim Z^\sigma$ if and only if the restriction of σ on k_Z is the identity, where $Z^\sigma = Z \times_{\mathrm{Spec}\,K}$ (Spec K^σ, Spec σ).

In the present paper, we will refer freely to [9] for the foundations concerned with the fields of moduli, for example, the existence of fields of moduli for curves or for polarized abelian varieties in every characteristic, etc.

Next, we will give somewhat general argument over fields of moduli related with the moduli spaces. In this section we give proofs in the case of abelian varieties. In the case of curves the proofs are similar.

Let A and B be noetherian complete local rings with fields of fractions K and L, and residue fields k and l, respectively. We assume that B is a finite and flat extension of A. Let $S' = \mathrm{Spec}\,B \to S = \mathrm{Spec}\,A$ be the canonical morphism, and p_1, p_2: $S'' = S' \times_S S' \rightrightarrows S'$ be the projections to the two factors. Now we shall consider a principally polarized abelian scheme $\mathcal{P}' = (\mathfrak{X}', \Lambda')$ and a curve $\mathcal{C}'$, over S'. Under these notations, we get the following.

LEMMA 1.3: *Assume that* π: $\mathbf{Isom}_{S''}(p_1^*\mathcal{P}', p_2^*\mathcal{P}') \to S''$ *is flat. Moreover, suppose that there exists a principally polarized abelian variety* P *over* k *such that* $\mathcal{P}' \otimes_B l \xrightarrow{\sim} P \otimes_k l$. *Then there exist a principally polarized abelian scheme* $\mathcal{P}$ *over* S, *and isomorphisms* $\mathcal{P} \times_S S' \xrightarrow{\sim} \mathcal{P}'$ *and* $\mathcal{P} \otimes_A k \xrightarrow{\sim} P$, *which induce the given isomorphism* $\mathcal{P}' \otimes_B l \xrightarrow{\sim} P \otimes_k l$.

Similarly we have

LEMMA 1.3′: *Assume that* π: $\mathbf{Isom}_{S''}(p_1^*\mathcal{C}', p_2^*\mathcal{C}') \to S''$ *is flat. Moreover, suppose that there exists a curve* C *over* k *such that* $\mathcal{C}' \otimes_B l \xrightarrow{\sim} C \otimes_k l$. *Then there exist a curve* $\mathcal{C}$ *over* S, *and isomorphisms* $\mathcal{C} \times_S S' \xrightarrow{\sim} \mathcal{C}'$ *and* $\mathcal{C} \otimes_A k \xrightarrow{\sim} C$, *which induce the given isomorphism* $\mathcal{C}' \otimes_B l \xrightarrow{\sim} C \otimes_k l$.

PROOF OF LEMMA 1.3: Obviously, we get the following commutative diagram:

$$\begin{tikzcd}
S_0'' = \mathrm{Spec}(B \otimes_A B / \mathfrak{J}(B \otimes_A B)) \arrow[r, hook] \arrow[dr, hook] & S_s'' = \mathrm{Spec}(B \otimes_A B / \mathfrak{M}_A(B \otimes_A B)) \arrow[r, hook] & S''. \\
& S_*'' = \mathrm{Spec}(B \otimes_A B / \mathfrak{M}_B \otimes B + B \otimes \mathfrak{M}_B) \arrow[u] &
\end{tikzcd}$$

Since π is étale, and $B \otimes_A B$ and $B \otimes_A B/\mathfrak{M}_A(B \otimes_A B)$ are henselian, by using (EGA IV, 18.5.12), we can see that the following canonical maps are bijections:

$$\Gamma(\boldsymbol{Isom}_{S''}(p_1^*\mathscr{P}', p_2^*\mathscr{P}')/S'') \to \Gamma(\boldsymbol{Isom}_{S_0''}(p_1^*\mathscr{P}', p_2^*\mathscr{P}')/S_0'');$$

$$\Gamma(\boldsymbol{Isom}_{S_s''}(p_1^*\mathscr{P}', p_2^*\mathscr{P}')/S_s'') \to \Gamma(\boldsymbol{Isom}_{S_0''}(p_1^*\mathscr{P}', p_2^*\mathscr{P}')/S_0'')$$

and

$$\Gamma(\boldsymbol{Isom}_{S_*''}(p_1^*\mathscr{P}', p_2^*\mathscr{P}')/S_*'') \to \Gamma(\boldsymbol{Isom}_{S_0''}(p_1^*\mathscr{P}', p_2^*\mathscr{P}')/S_0'').$$

Hence, the canonical map

$$\Gamma(\boldsymbol{Isom}_{S''}(p_1^*\mathscr{P}', p_2^*\mathscr{P}')/S'') \to \Gamma(\boldsymbol{Isom}_{S_*''}(p_1^*\mathscr{P}', p_2^*\mathscr{P}')/S_*'')$$

is bijective. On the other hand, by our assumption, there exists a descent datum

$$\phi_* \in \mathrm{Isom}_{S_*''}(p_1^*\mathscr{P}', p_2^*\mathscr{P}')$$

which gives the descent P of $\mathscr{P}' \otimes_B l$. Hence, by the above bijection, there exists a descent datum

$$\phi \in \mathrm{Isom}_{S''}(p_1^*\mathscr{P}', p_2^*\mathscr{P}')$$

corresponding to ϕ_*, and we can descent $\mathscr{P}'$ over S. Q.E.D.

Here we shall state an easy relation between the field of definition and the field of moduli.

LEMMA 1.4: *Let k be a field of characteristic $p(>0)$, and K a purely inseparable extension of k. Let P (resp. C) be a principally polarized abelian variety (resp. a curve) over K. Assume that $k \supset k_P$ (resp. $k \supset k_C$). Then there exists a principally polarized abelian variety P_0 (resp. a curve C_0) over k such that*

$$P_0 \otimes_k K \simeq P \ (\textit{resp. } C_0 \otimes_k K \simeq C.)$$

(cf. [26], Proposition 3.2.)

Let n be an integer larger than 2, and $\mathscr{Q} = (\mathfrak{Z}, \Lambda, \alpha)$ the universal principally polarized abelian scheme with level n-structure over $A_{g,n}$. For an element $\sigma \in G_n = \mathrm{GL}(2g; \boldsymbol{Z}/n\boldsymbol{Z})/\{\pm \mathbf{1}\}$, we denote $\mathscr{Q}^\sigma$ by the fibre product

$$\begin{tikzcd} \mathscr{Q}^{\sigma} = \mathscr{Q} \times_{A_{g,n}} (A_{g,n}, \sigma) \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & A_{g,n} \arrow[d, "\sigma"] \\ \mathscr{Q} \arrow[r] & A_{g,n}. \end{tikzcd}$$

For a point $y \in A_{g,n}$, the automorphism σ induces a local ring homomorphism

$$\sigma^*: \mathscr{O}_{\sigma(y)} \to \mathscr{O}_y,$$

and a homomorphism of the residue fields:

$$\bar{\sigma}^*: \boldsymbol{k}(\sigma(y)) \to \boldsymbol{k}(y).$$

Looking at the composition of fibre products:

$$\begin{tikzcd} \mathscr{Q}^{\sigma}|_{\mathrm{Spec}(\boldsymbol{k}(y))} \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & \mathscr{Q}^{\sigma} \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & \mathscr{Q} \arrow[d] \\ \mathrm{Spec}(\boldsymbol{k}(y)) \arrow[r] \arrow[rr, bend right, "\sigma(y) \circ \mathrm{Spec}(\bar{\sigma}^*)"'] & A_{g,n} \arrow[r, "\sigma"] & A_{g,n}, \end{tikzcd}$$

we get the canonical isomorphism

$$\mathscr{Q}^{\sigma}|_{\mathrm{Spec}(\boldsymbol{k}(y))} \simeq \left(\mathscr{Q}|_{\mathrm{Spec}(\boldsymbol{k}(\sigma(y)))}\right)^{\bar{\sigma}^*}. \tag{1.1}$$

Similarly we obtain the isomorphism

$$\mathscr{Q}^{\sigma}|_{\mathrm{Spec}(\mathscr{O}_y)} \simeq \left(\mathscr{Q}|_{\mathrm{Spec}(\mathscr{O}_{\sigma(y)})}\right)^{\sigma^*}. \tag{1.2}$$

Now let P be the principally polarized abelian variety over $\boldsymbol{k}(y)$ obtained from $\mathscr{Q}|_{\mathrm{Spec}(\boldsymbol{k}(y))}$ by forgetting the level n-structure. We put $x = \pi_n(y) \in A_g$, where π_n: $A_{g,n} \to A_g$ is the canonical morphism. Moreover, we set $S' = \mathrm{Spec}(\boldsymbol{k}(y)) \to S = \mathrm{Spec}(\boldsymbol{k}(x))$ and p_1, p_2: $S'' = S' \times_S S' \rightrightarrows S'$: the projections. Under these notations, we get the following.

LEMMA 1.5: *There exists an isomorphism*

$$\phi\colon\ p_1^* P|_{S''_{\mathrm{red}}} \to p_2^* P|_{S''_{\mathrm{red}}}.$$

PROOF: Since π_n: $A_{g,n} \to A_g$ is a Galois covering with Galois group $G_n = \mathrm{GL}_{2g}(\boldsymbol{Z}/n\boldsymbol{Z})/\{\pm\boldsymbol{1}\}$, the extension $\boldsymbol{k}(y)/\boldsymbol{k}(x)$ is a quasi-Galois extension and the canonical map

$$G_n^Z(y) \to \mathrm{Aut}(\boldsymbol{k}(y)/\boldsymbol{k}(x)) = G$$

is a surjection, where $G_n^Z(y)$ is the decomposition group of y (cf. [3], Chap. 5, §2, no. 2, Théorème 2). Now we take the intermediate field K of $\boldsymbol{k}(y)/\boldsymbol{k}(x)$ such that $\boldsymbol{k}(y)/K$ is separable and $K/\boldsymbol{k}(x)$ is purely inseparable. Then obviously

$$\mathfrak{R}\left(\boldsymbol{k}(y) \otimes_{\boldsymbol{k}(x)} \boldsymbol{k}(y)\right) = (\{t \otimes 1 - 1 \otimes t \mid t \in K\})$$

and

$$\begin{aligned} S''_{\mathrm{red}} &= \mathrm{Spec}\left(\boldsymbol{k}(y) \otimes_{\boldsymbol{k}(x)} \boldsymbol{k}(y)/\mathfrak{R}\left(\boldsymbol{k}(y) \otimes_{\boldsymbol{k}(x)} \boldsymbol{k}(y)\right)\right) \\ &\simeq \mathrm{Spec}\left(\boldsymbol{k}(y) \otimes_K \boldsymbol{k}(y)\right). \end{aligned}$$

Since $\boldsymbol{k}(y)/K$ is a finite Galois extension with Galois group G, the tensor product $\boldsymbol{k}(y) \otimes_K \boldsymbol{k}(y)$ is isomorphic to $\Pi_{\sigma \in G} \boldsymbol{k}(y)$ by the map $\alpha \otimes \beta \mapsto (\alpha\beta^\sigma)_{\sigma \in G}$. If we identify $S''_{\mathrm{red}} = \mathrm{Spec}(\boldsymbol{k}(y) \otimes_K \boldsymbol{k}(y))$ and $\coprod_{\sigma \in G} \mathrm{Spec}(\boldsymbol{k}(y))$ by this isomorphism, then

$$p_1^* P|_{S''_{\mathrm{red}}} = \coprod_\sigma P$$

and

$$p_2^* P|_{S''_{\mathrm{red}}} = \coprod_\sigma P^\sigma.$$

Therefore, noticing the surjectivity of $G_n^Z(y) \to G$ and (1.1), there exist isomorphisms

$$P \simeq P^\sigma \qquad \text{for any} \quad \sigma \in G.$$

Q.E.D.

Now let

$$\begin{array}{ccc} S' = \mathrm{Spec}\, B & \to & A_{g,n} \\ u \downarrow & & \downarrow \pi_n \\ S = \mathrm{Spec}\, A & \to & A_g \end{array} \tag{1.3}$$

be a given commutative diagram with discrete valuation rings A and B and a finite extension u^*: $A \to B$. We put p_1, p_2: $S'' = S' \times_S S' \rightrightarrows S'$: the projections and η the generic point of S. Let $\mathscr{P}$ be the principally polarized abelian scheme obtained from $\mathscr{Q}|_{S'}$ by forgetting the level n-structure. Under these notations, we get the following.

LEMMA 1.6: *Suppose that* $\mathbf{Aut}_{S'}(\mathscr{P}) \to S'$ *and* $\mathbf{Isom}_{S''}(p_1^*\mathscr{P}, p_2^*\mathscr{P})_\eta \to S''_\eta$ *are flat. Then* $\mathbf{Isom}_{S''}(p_1^*\mathscr{P}, p_2^*\mathscr{P}) \to S''$ *is flat, and so étale.*

PROOF: First, we shall show the flatness of

$$\mathbf{Isom}_{S''_{\mathrm{red}}}(p_1^*\mathscr{P}, p_2^*\mathscr{P}) \to S''_{\mathrm{red}}.$$

Let C be any discrete valuation ring, and f: Spec $C \to S''_{\mathrm{red}}$ a given morphism. Put

$$\begin{tikzcd}
 & S' & \\
\mathrm{Spec}\ C \arrow[ur, "p_1'"] \arrow[r, "f"] \arrow[dr, "p_2'"'] & S''_{\mathrm{red}}. \arrow[u, "p_1"'] \arrow[d, "p_2"] \\
 & S' &
\end{tikzcd}$$

Let ξ and η' be the generic points of Spec C and S', respectively. Then $p_1'(\xi) = p_2'(\xi) = \eta'$. In fact, S' is consisting only of two points. Therefore f_ξ factors through $(S''_\eta)_{\mathrm{red}}$:

$$\begin{tikzcd}
(\mathrm{Spec}\ C)_\xi = \mathrm{Spec}(\mathrm{f.f.}C) \arrow[r, "f_\xi"] \arrow[dr] & S''_{\mathrm{red}}. \\
 & (S''_\eta)_{\mathrm{red}} \arrow[u]
\end{tikzcd}$$

By lemma 1.5, $p_1^*\mathscr{P}$ and $p_2^*\mathscr{P}$ are isomorphic over $(S''_\eta)_{\mathrm{red}}$; i.e., there exists a cross-section of

$$\mathbf{Isom}_{\mathrm{Spec}(\mathrm{f.f.}C)}(p_1^*\mathscr{P}, p_2^*\mathscr{P}) \to \mathrm{Spec}(\mathrm{f.f.}C).$$

On the other hand, since the structure morphism

$$\mathbf{Isom}_{\mathrm{Spec}\ C}(p_1^*\mathscr{P}, p_2^*\mathscr{P}) \to \mathrm{Spec}\ C$$

is proper, this cross-section can be extended over Spec C. Hence

$$\mathbf{Isom}_{\mathrm{Spec}\ C}(p_1^*\mathscr{P}, p_2^*\mathscr{P}) \simeq \mathbf{Aut}_{\mathrm{Spec}\ C}(p_1^*\mathscr{P}) \simeq \mathbf{Aut}_{S'}(\mathscr{P}) \times_{S'} \mathrm{Spec}\ C$$

is flat, and so étale, over Spec C by our assumption. This implies that

$$\mathbf{Isom}_{S''_{\mathrm{red}}}(p_1^*\mathscr{P},\ p_2^*\mathscr{P}) \to S''_{\mathrm{red}}$$

is flat by the valuative criterion of flatness. Moreover, by our assumption,

$$\mathbf{Isom}_{S''_\eta}(p_1^*\mathscr{P},\ p_2^*\mathscr{P}) \to S''$$

if flat, and so is

$$\mathbf{Isom}_{\mathrm{Spec}(\mathscr{O}_{z,S''})}(p_1^*\mathscr{P},\ p_2^*\mathscr{P}) \to \mathrm{Spec}(\mathscr{O}_{z,S''})$$

for each associated point z of S''. Therefore, (EGA IV, Corollaire 11.4.9) implies the flatness of

$$\mathbf{Isom}_{S''}(p_1^*\mathscr{P},\ p_2^*\mathscr{P}) \to S''.$$

Q.E.D.

From Lemma 1.5 and the definition of fields of moduli, we can deduce easily the following.

PROPOSITION 1.7: *Let P be a principally polarized abelian variety corresponding to a point $x \in A_g$. Then the field of moduli k_P of P contains $\boldsymbol{k}(x)$ and the extension $k_P/\boldsymbol{k}(x)$ is purely inseparable. In particular, if x is a closed point, $k_P = \boldsymbol{k}(x)$.*

In the rest of this section, we will discuss the conditions of the coincidence of the field of moduli k_P and the corresponding residue field $\boldsymbol{k}(x)$.

The following is a direct consequence of a property of the field of moduli.

PROPOSITION 1.8: *Let p be a prime integer, and x be a point of ${}^{(p)}A_g$. Let P be a principally polarized abelian variety corresponding to x. Then the following conditions are equivalent*:

(i) $k_P = \boldsymbol{k}(x)$.

(ii) *For some integer n with $n \geqslant 3$ and $p \nmid n$, and a point $y \in A_{g,n}$ lying over x, $\boldsymbol{k}(y)$ is separable over $\boldsymbol{k}(x)$.*

(iii) *For any n and y as in* (ii), *$\boldsymbol{k}(y)$ is separable over $\boldsymbol{k}(x)$.*

In fact, there exists a model (X, λ) of P over a separable extension K of k_P (cf. [9], Theorem 2.2). If $p \nmid n$, $X_n \to \mathrm{Spec}\ K$ is étale, and so $K(X_n)$ is separable over K. Moreover, for any n and y as in (ii), $\boldsymbol{k}(y)$ is contained in $K(X_n)$. Hence, if $k_P = \boldsymbol{k}(x)$, $\boldsymbol{k}(y)$ is separable over $\boldsymbol{k}(x)$.

This implies (i) $\Rightarrow$ (iii). On the other hand, the implications (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) are obvious.

The same statement as in Proposition 1.8 is also true for curves.

PROPOSITION 1.8′: *Let p be a prime integer, and x a point of ${}^{(p)}M_g$. Let C be a curve corresponding to x. Then the following conditions are equivalent*:

(i) $k_C = \boldsymbol{k}(x)$.

(ii) *For some integer n with $n \geqslant 3$ and $p \nmid n$, and a point $y \in M_{g,n}$ lying over x, $\boldsymbol{k}(y)$ is separable over $\boldsymbol{k}(x)$.*

(iii) *For any n and y as in* (ii), *$\boldsymbol{k}(y)$ is separable over $\boldsymbol{k}(x)$.*

As in Proposition 1.8, let p be a fixed prime integer, x a point of ${}^{(p)}A_g$, and P a principally polarized abelian variety corresponding to x. For an integer n with $p \nmid n$ and $n \geqslant 3$, let y be a point of ${}^{(p)}A_{g,n}$ lying over x. We put $S' = \mathrm{Spec}(\boldsymbol{k}(y)) \to S = \mathrm{Spec}(\boldsymbol{k}(x))$ and p_1, p_2: $S'' = S' \times_S S' \rightrightarrows S'$. Since ${}^{(p)}A_{g,n}$ is a fine moduli space, we may assume that P is defined over $\boldsymbol{k}(y)$, and we can consider the p_i^*P's. Under these notations, we can continue the equivalent conditions in Proposition 1.8 as follows.

THEOREM 1.9: *The conditions in Proposition* 1.8 *are equivalent to the following mutually equivalent conditions.*

(iii) *For some n and y as above, $p_1^*P \simeq p_2^*P$.*

(iii)′ *For every n and y as above, $p_1^*P \simeq p_2^*P$.*

(iv) *For some n and y as above, $\boldsymbol{Isom}_{S''}(p_1^*P, p_2^*P) \to S''$ is flat, and so étale.*

(iv)′ *For every n and y as above, $\boldsymbol{Isom}_{S''}(p_1^*P, p_2^*P) \to S''$ is flat, and so étale.*

PROOF: By Lemma 1.5, the implication (ii)′ $\Rightarrow$ (iii)′ is obvious. Moreover, the implications (iii)′ $\Rightarrow$ (iii) $\Rightarrow$ (iv)′ $\Rightarrow$ (iv) are trivial, so we have only to deduce (ii) from (iv). We shall prove this by induction on the transcendental degree of $\boldsymbol{k}(x)$ over $\boldsymbol{F}_p$. If tran. deg$(\boldsymbol{x}(x)/\boldsymbol{F}_p) = 0$, $\boldsymbol{x}(x)$ is perfect and our assertion is true by Proposition 1.7. Now we set tran. deg$(\boldsymbol{k}(x)/\boldsymbol{F}_p) = r$ and we assume our assertion is true for any point $x' \in {}^{(p)}A_g$ satisfying the condition (iv) and tran. deg$(\boldsymbol{k}(x')/\boldsymbol{F}_p) = r - 1$. Let

$$T = \overline{\{y\}} \subset {}^{(p)}A_{g,n}$$

and

$$\overline{T} = \overline{\{x\}} \subset {}^{(p)}A_g,$$

endowed with reduced scheme structure. Let

$$\pi = \text{the rest. of } \pi_n \colon T \to \overline{T}.$$

Then π is a finite surjective morphism. By (EGA IV, Théorème 6.9.1), there exists a non-empty open set

$$U \subset \overline{T}$$

such that

$$\pi \colon \pi^{-1}(U) \to U$$

is flat. Moreover, we choose an affine open neighbourhood V at x in $\pi^{-1}(U)$ such that

$$\boldsymbol{Aut}_V(\mathscr{P}|_V) \to V$$

becomes flat, where $\mathscr{P}$ is the universal principally polarized abelian scheme over ${}^{(p)}A_{g,n}$. Let $V'(\subset V)$ be the open subset consisting of all simple points in V. Then since π is flat over U, $\pi(V')$ is open in U. Hence we can choose a simple point x' in $\pi(V')$ of codimension 1 in $\overline{T}$ and $y' \in V'$ lying over x'. Here we put $B = \mathcal{O}_{y',T} \to A = \mathcal{O}_{x',\overline{T}}$. Obviously A and B are discrete valuation rings, and trans. $\deg(\boldsymbol{k}(x')/\boldsymbol{F}_p) = r - 1$. We take the completions:

$$\begin{array}{ccc} \hat{\boldsymbol{k}}(y) = \text{f.f.}\hat{B} & \supset & \hat{B} \\ | & & | \\ \hat{\boldsymbol{k}}(x) = \text{f.f.}\hat{A} & \supset & \hat{A}. \end{array}$$

We denote by k the separable closure of $\hat{\boldsymbol{k}}(x)$ in $\hat{\boldsymbol{k}}(y)$, and put

$$\hat{C} = k \cap \hat{B}.$$

We set $\mathscr{S}' = \operatorname{Spec}(\hat{B}) \to \mathscr{S} = \operatorname{Spec}(\hat{A})$, and $p_1, p_2 \colon \mathscr{S}'' = \mathscr{S}' \times_{\mathscr{S}} \mathscr{S}' \rightrightarrows \mathscr{S}'$. Then by the assumption (iv) and the choice of x' and y', these satisfy the conditions in Lemma 1.6. Hence

$$\boldsymbol{Isom}_{\mathscr{S}''}(p_1^* P', p_2^* P') \to \mathscr{S}'' \tag{1.4}$$

becomes flat, where $\mathscr{P}' = \mathscr{P}|_{S'}$. In particular, this implies that the point x' satisfies the condition (iv). Therefore, by the induction hypothesis, $\boldsymbol{k}(y')$ is separable over $\boldsymbol{k}(x')$, and $\boldsymbol{k}(\hat{C}) = \boldsymbol{k}(y')$. Since $\mathscr{W} = \operatorname{Spec}(\tilde{B} \otimes_{\hat{C}} \hat{B})$

is a closed subscheme of $\mathscr{S}'' = \operatorname{Spec}(\hat{B} \otimes_{\hat{A}} \hat{B})$, (1.4) implies that the morphism

$$\boldsymbol{Isom}_{\mathscr{W}}(p_1^*P', p_2^*P') \to \mathscr{W}$$

is flat. Hence, by Lemma 1.3, $\mathscr{P}'$ can be descended to one on $\hat{C}$. On the other hand, in our case, $\hat{\boldsymbol{k}}(x)$ is separably generated over $\boldsymbol{k}(x)$ (cf. [13], (31.F), Theorem 71). Thus we get our assertion. Q.E.D.

Similarly we can show for curves the same results as in Theorem 1.9. In fact, as in Proposition 1.8′, let p be a fixed prime integer, x a point of ${}^{(p)}M_g$, and C a curve corresponding to x. For an integer n with $p \nmid n$ and $n \geqslant 3$, let y be a point of ${}^{(p)}A_{g,n}$ lying over x. Moreover, we set S, S' and S'' as above. Then we get the following.

THEOREM 1.9′: *The conditions in Proposition* 1.8′ *are equivalent to the following mutually equivalent conditions.*
- (iii) *For some n and y as above, $p_1^*C \simeq p_2^*C$.*
- (iii) *For every n and y as above, $p_1^*C \simeq p_2^*C$.*
- (iv) *For some n and y as above, $\boldsymbol{Isom}_{S''}(p_1^*C, p_2^*C) \to S''$ is flat, and so éatle.*
- (iv)′ *For every n and y as above, $\boldsymbol{Isom}_{S''}(p_1^*C, p_2^*C) \to S''$ is flat, and so ètale.*

Let P be a principally polarized abelian variety of dimension $g(\geqslant 3)$, and C a curve of genus $g \geqslant 4$. Let $x \in {}^{(p)}A_g$ and $y \in {}^{(p)}M_g$ be the corresponding points to P and C, respectively. Then x (resp. y) is a simple point if and only if P (resp. C) has only automorphisms $\pm \mathbf{1}_p$ (resp. $\mathbf{1}_C$). These are results of Popp ([25], Introduction and p. 106, Theorem) for curves and Oort ([21], Theorem 1. AV.) for abelian varieties. Thus we get the following corollary.

COROLLARY 1.10: *Let P be a principally polarized abelian variety of dimension $g(\geqslant 3)$, and C a curve of genus $g(\geqslant 4)$. Let $x \in {}^{(p)}A_g$ and $y \in {}^{(p)}M_g$ be the corresponding points to them, respectively. If x (resp. y) is a simple point of ${}^{(p)}A_g$ (resp. ${}^{(p)}M_g$), then $\boldsymbol{k}(x) = k_P$ (resp. $\boldsymbol{k}(y) = k_C$.)*

Moreover, noticing the facts in the appendix to [28], we get the following.

COROLLARY 1.11: *Let P (resp. C) be a principally polarized abelian variety of dimension g (resp. a curve of genus g) over a field of characteristic p.*
- (i) *If $p > 2g + 1$, then $\boldsymbol{k}(x) = k_P$ (resp. $\boldsymbol{k}(y) = k_C$.)*
- (ii) *If $p > g + 1$, $p \neq 2g + 1$ and P is indecomposable, then $\boldsymbol{k}(x) = k_P$ (resp. $\boldsymbol{k}(y) = k_C$.)*

Lastly, we shall state a remark on the fields of moduli for abelian varieties.

LEMMA 1.12: *Let $\mathscr{P} = (X, \lambda_X)$ and $\mathscr{Q} = (Y, \lambda_Y)$ be two principally polarized abelian varieties over a field k of characteristic p. We assume that $\mathscr{Q}$ is defined over a finite field $\boldsymbol{F}$ contained in $k_{\mathscr{P}}$. Then $k_{\mathscr{P}}$ is separable over $k_{\mathscr{P}\times\mathscr{Q}}$, where $\mathscr{P}\times\mathscr{Q} = (X\times Y, \lambda_X \times \lambda_Y)$.*

PROOF: There exist a separable extension l of $k_{\mathscr{P}\times\mathscr{Q}}$, and a model (Z, λ) over l such that if we take a suitable extension L of l containing k, there exists an isomorphism

$$\phi\colon (\mathscr{P}\times\mathscr{Q}) \otimes_k L \to (Z, \lambda) \otimes_l L.$$

We put

$$\psi = \phi|_{\{0\}\times Y_L}\colon Y_L = Y \otimes_k L \xrightarrow{\sim} \{0\} \times Y_L \to Z_L.$$

Since $\mathscr{Q}$ and (Z, λ) have models over a separable extension l' of l, the morphism ψ is defined over a separable extension l'' of l' (cf. [26], Theorem 3.1). Hence $\psi\colon Y_{l''} \to Z_{l''}$. Then, obviously, $\lambda \otimes_l l''$ can be descended to a principal polarization λ'' of $Z_{l''}/Y_{l''}$ and $(Z_{l''}/Y_{l''}, \lambda'')$ is geometrically isomorphic to $\mathscr{P}$. That is, $\mathscr{P}$ has a model over l'', and we are done. Q.E.D.

§2. Cyclic coverings of $\boldsymbol{P}^1$

In this section, we fix an algebraically closed field k of characteristic $p(>0)$.

Every cyclic covering C of degree p over $\boldsymbol{P}^1$ is given by the normalization of the plane curve defined by the equation:

$$y^p - B(x)y = A(x), \tag{2.1}$$

with

$$A(x) = (x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}\dots(x-\alpha_r)^{e_r}G(x);$$

$$B(x) = (x-\alpha_1)^{n_1(p-1)}(x-\alpha_2)^{n_2(p-1)}\dots(x-\alpha_r)^{n_r(p-1)};$$

$$\deg A(x) = Np;\ x-\alpha_i \nmid G(x),\ 1 \leqslant e_i < p,\ 1 \leqslant n_i$$

$$\text{for each } i = 1, 2, \dots, r;\ \alpha_i \neq \alpha_j \text{ for } i \neq j.$$

Here we put

$$N = \sum_{i=1}^{r} n_i \text{ and } E = \sum_{i=1}^{r} e_i.$$

An automorphism σ of order p of C is given by

$$\sigma(y) = y + (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\dots(x-\alpha_r)^{n_r}. \tag{2.2}$$

For a function f and a differential ω on C, we denote by (f) and (ω) the divisors of them, respectively. Then obviously

$$\begin{aligned}
(x) &= \sum_{j=1}^{p} \mathfrak{Q}_j - \sum_{j=1}^{p} \mathfrak{J}_j,\\
(x-\alpha_i) &= p\mathfrak{P}_i - \sum_{j=1}^{p} \mathfrak{J}_j,\\
(B(x)) &= \sum_{i=1}^{r} p(p-1)n_i\mathfrak{P}_i - \sum_{j=1}^{p}(p-1)N\mathfrak{J}_j,\\
(y) &= \sum_{i=1}^{r} e_i\mathfrak{P}_i + \sum_{j=1}^{pN-E}\mathfrak{R}_j - \sum_{j=1}^{p} N\mathfrak{J}_j,
\end{aligned} \tag{2.3}$$

where $\mathfrak{J}_j$'s and $\mathfrak{Q}_j$'s are the points on C lying over $x=\infty$ and $x=0$, respectively, $\mathfrak{P}_i$ is the point lying over $x=\alpha_i$ for each i, and $\mathfrak{R}_j$'s are the points on C defined by $y=0$ and $G(x)=0$. Moreover, the different $\mathscr{D}$ of $k(C)/k(\boldsymbol{P}^1)$ is given by

$$\mathscr{D} = \sum_{i=1}^{r}(p-1)(pn_i - e_i + 1)\mathfrak{P}_i \tag{2.4}$$

(cf. Hasse [8], p. 42). Therefore, by Hurwitz's theorem,

$$(dx) = \sum_{i=1}^{r}(p-1)(pn_i - e_i + 1)\mathfrak{P}_i - 2\sum_{j=1}^{p}\mathfrak{J}_i \tag{2.5}$$

and the genus g of C is given by

$$g = \tfrac{1}{2}(p-1)(pN - E + r - 2). \tag{2.6}$$

Moreover a basis of differentials of the first kind on C is given as follows.

PROPOSITION 2.1: *A basis of $H^0(C, \Omega_C^1)$ is given by*

$$\prod_{i=1}^{r}(x-\alpha_i)^{l_i}x^m y^n (dx/B) \tag{2.7}$$

with

$$l_i = e_i - 1 - [(n+1)e_i/p];$$

$$n = 0, 1, \ldots, p-2;$$

$$m = 0, 1, \ldots, N(p-n-1) + r - E - 2 + \sum_{i=1}^{r} [(n+1)e_i/p].$$

Here [ ] *means the Gauss symbol.*

PROOF: By (2.3) and (2.5), we get the equality

$$\left(\prod_{i=1}^{r}(x-\alpha_i)^{l_i}x^m y^n (dx/B)\right)$$

$$= \sum_{i=1}^{r}\{pl_i + ne_i - (p-1)(e_i-1)\}\mathfrak{P}_i + \sum_{j=1}^{p} m\mathfrak{Q}_j$$

$$+ \sum_{j=1}^{pN-E} n\mathfrak{R}_j + \sum_{j=1}^{p}\{(p-1)N - m - Nn - L - 2\}\mathfrak{S}_j, \qquad (2.8)$$

where $L = \sum_{j=1}^{r} l_j$. Thus we can see that the differentials given by (2.7) are contained in $H^0(C, \Omega_C^1)$. Next, we shall check the linear independence of differentials given by (2.7). This simple proof is due to Mr. Irokawa.

Since $H^0(C, \Omega_C^1)$ is a subspace of $k(C) \cdot dx$, we have only to check the linear independence of the functions $\prod_{i=1}^{r}(x-\alpha_i)^{l_i}x^m y^n$'s. Moreover, since $k(C)$ is a $k(x)$-vector space with basis $\{1, y, \ldots, y^{p-1}\}$, we can reduce our problem to the linear independence of $\prod_{i=1}^{r}(x-\alpha_i)^{l_i}x^m$ $(m = 0, 1, \ldots, N(p-n-1) + r - E - 2 + \sum_{i=1}^{r}[(n+1)e_i/p])$. But, since l_i's are independent of m, this linear independence is trivial.

On the other hand,

$$\sum_{n=0}^{p-2}[(n+1)e_i/p]$$

$$= \tfrac{1}{2}\left\{\sum_{n=0}^{p-2}[(n+1)e_i/p] + \sum_{n=0}^{p-2}[(p-n-1)e_i/p]\right\}$$

$$= \tfrac{1}{2}\sum_{n=0}^{p-2}(e_i - 1) = \tfrac{1}{2}(p-1)(e_i-1).$$

Therefore, the number of the differentials given by (2.7) is calculated as follows:

$$\sum_{n=0}^{p-2}\left\{N(p-n-1)+r-E-2+\sum_{i=1}^{r}[(n+1)e_i/p]\right\}$$

$$=(p-1)^2N-\tfrac{1}{2}(p-1)(p-2)N+(p-1)(r-E-1)$$

$$+\sum_{i=1}^{r}\sum_{n=0}^{p-2}[(n+1)e_i/p]$$

$$=(p-1)^2N-\tfrac{1}{2}(p-1)(p-2)N+(p-1)(r-E-1)$$

$$+\tfrac{1}{2}\sum_{i=1}^{r}(p-1)(e_i-1)$$

$$=\tfrac{1}{2}(p-1)(pN-E+r-2)=g.$$

This implies our assertion. Q.E.D.

In particular, let C be a curve defined by (2.1) with $n_1=n_2=\ldots=n_r=1$, $e_1=e_2=\ldots=e_r=p-1$ and $r\geqslant 2$. Namely, let

$$C\colon\ y^p-B(x)y=A(x), \tag{2.9}$$

with

$$B(x)=P(x)^{p-1},$$

$$A(x)=P(x)^{p-1}G(x),$$

$$P(x)=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_r),$$

$$\deg G(x)=r.$$

Then by the above proposition, a basis of the differentials of the first kind on this curve becomes as follows.

COROLLARY 2.2: *Let C be a curve defined by* (2.9). *Then a basis of $H^0(C,\Omega_C^1)$ is given by*

$$x^iP^ly^{p-l-2}(dx/B)\ (i=0,1,\ldots,r-2;\ l=0,1,\ldots,p-2). \tag{2.10}$$

Moreover a basis of $H^0(C,\Omega_C^{\otimes 2})$ can be given as follows.

PROPOSITION 2.3: *Let C be a curve defined by* (2.9) *with $p \geqslant 3$ and $r \geqslant 2$. Then a basis of $H^0(C, \Omega_C^{\otimes 2})$ is given by*

$$x^i P^{p-l} y^{p-(4-l)} (dx/B)^2 \quad (l = 1, 2, 3;\ i = 0, 1, \dots, 2r-4), \tag{2.11}$$

$$x^i P^{2p-l-4} y^l (dx/B)^2 \quad (l = 0, 1, \dots, p-4;\ i = 0, 1, \dots, 2r-4), \tag{2.12}$$

$$x^j P^{2p-l-5} G y^l (dx/B)^2 \quad (l = 0, 1, \dots, p-4;\ j = 0, 1, \dots, r-1). \tag{2.13}$$

Here, (2.12) *and* (2.13) *appear only in the case of $p \geqslant 5$.*

PROOF: By (2.3) and (2.5), we can easily see that the members of (2.11), (2.12) and (2.13) are contained in $H^0(C, \Omega_C^{\otimes 2})$. Obviously the number of the members of (2.11), (2.12) and (2.13) is $3g-3$. Moreover, since $H^0(C, \Omega_C^{\otimes 2})$ is contained in $k(C) \cdot (dx/B)^2$, and $\{1, y, \dots, y^{p-1}\}$ is a $k(x)$-basis of $k(C)$, we have only to check the linear independence of the members of (2.12) and (2.13). Since $P(x)$ and $G(x)$ have no common zero, by using Sylvester's resultant, we can see that

$$x^i P,\ x^i G \quad (i = 0, 1, \dots, r-1)$$

are linearly independent. Therefore, the members of (2.12) with $i = 0, 1, \dots, r-1$ and the full members of (2.13) are linearly independent. Hence, looking at the degrees of the rest of (2.12), we see that the full members of (2.12) and (2.13) span a $(3r-3)$-dimensional vector space.

Q.E.D.

By Corollary 2.2 and Proposition 2.3, we can easily see that the canonical map

$$H^0(C, \Omega_C^1) \otimes H^0(C, \Omega_C^1) \to H^0(C, \Omega_C^{\otimes 2})$$

is surjective for $p \geqslant 3$ and $r \geqslant 3$. Therefore, by Noether's theorem, we get the following.

COROLLARY 2.4: *Let C be a curve defined by* (2.9) *with $p \geqslant 3$ and $r \geqslant 3$. Then C is non-hyperelliptic.*

By virtue of the same argument as in the proof of Proposition 2.3, we get the following.

PROPOSITION 2.5: *Let C be a curve defined by* (2.1) *with* $e_1 = e_2 = \dots = e_r = 1$. *Then a basis of* $H^0(C, \Omega_C^{\otimes 2})$ *is given by*

$$x^{i_0}(dx/B)^2, x^{i_1}y(dx/B)^2, \dots, x^{i_{p-1}}y^{p-1}(dx/B)^2, \tag{2.14}$$

where i_j *runs over* $\{0, 1, \dots, N(2p-j-2)-4\}$ *for each* $j = 0, 1, \dots, p-1$.

In the rest of this section, we shall calculate the p-rank of the jacobian varieties of the general members among the curves given by (2.9). For our purpose, we put

$$P(X) = \sum_{i=-\infty}^{\infty} s_i X^i$$

and

$$P(X)^{p-1} = \sum_{i=-\infty}^{\infty} t_i X^i.$$

Of course, $s_i = 0$ and $t_j = 0$ for $i \notin \{0, 1, \dots, r\}$ and $j \notin \{0, 1, \dots, r(p-1)\}$. Then

$$t_j = \sum_{\substack{a_0 + a_1 + \dots + a_r = p-1 \\ a_1 + 2a_2 + \dots + ra_r = j}} \frac{(p-1)!}{a_0! a_1! \dots a_r!} s_0^{a_0} s_1^{a_1} \dots s_r^{a_r}. \tag{2.15}$$

Moreover for each $l = 0, 1, \dots, p-2$, we put

$$W_l = \langle \{ x^i P^l y^{p-l-2}(dx/B) \mid i = 0, 1, \dots, r-2 \} \rangle$$
$$\subset H^0(C, \Omega_C^1).$$

Since $y^p - P^{p-1}y = P^{p-1}G$ and $y = (y^p - P^{p-1}G)/P^{p-1}$, we get the equality

$$\begin{aligned}
&(x^i P^l y^{p-l-2}/B)\,dx \\
&= \left[\left\{ x^i P^l \left(y^p - P^{p-1}G \right)^{p-l-2} \right\} / P^{(p-1)(p-l-1)} \right] dx \\
&= x^i P^{p-1} \left(y^{p-l-2}/P^{p-l-1} \right)^p dx + (\text{lower degree terms in } y^p)\,dx \\
&= \left(t_0 x^i + t_1 x^{i+1} + \dots + t_n x^{i+n} + \dots \right) \left(y^{p-l-2}/P^{p-l-1} \right)^p dx \\
&\quad + (\text{lower degree terms in } y^p)\,dx.
\end{aligned}$$

Therefore the Cartier operator $\check{F}$ acts on the each subspace $W_0 + W_1 + \ldots + W_l$ of $H^0(C, \Omega_C^1)$, and the induced action of $\check{F}$ over $\overline{W_l} = W_0 + W_1 + \ldots + W_l/(W_0 + W_1 + \ldots + W_{l-1})$ is represented by the matrix

$$A = \begin{pmatrix} \sqrt[p]{t_{p-1}} & \sqrt[p]{t_{p-2}} & \cdots & \sqrt[p]{t_{p-r+1}} \\ \sqrt[p]{t_{2p-1}} & \sqrt[p]{t_{2p-2}} & \cdots & \sqrt[p]{t_{2p-r+1}} \\ \vdots & \vdots & & \vdots \\ \sqrt[p]{t_{(r-1)p-1}} & \sqrt[p]{t_{(r-1)p-2}} & \cdots & \sqrt[p]{t_{(r-1)p-r+1}} \end{pmatrix}.$$

Here we put

$$A^{(p)} = \begin{pmatrix} t_{p-1} & t_{p-2} & \cdots & t_{p-r+1} \\ t_{2p-1} & t_{2p-2} & \cdots & t_{2p-r+1} \\ \vdots & \vdots & & \vdots \\ t_{(r-1)p-1} & t_{(r-1)p-2} & \cdots & t_{(r-1)p-r+1} \end{pmatrix}.$$

From the equality (2.15), in the expansion of the determinant of $A^{(p)}$, the term $(s_1 s_2 \ldots s_{r-1})^{p-1}$ occurs only in the term $t_{p-1} t_{2p-2} \cdots t_{(r-1)p-r+1}$. Hence,

$$\det A^{(p)} \not\equiv 0.$$

This implies that if we choose $\alpha_1, \alpha_2, \ldots, \alpha_r$ in a general position, then the representation matrix of $\check{F}$ is non-degenerate. Thus we have obtained the following theorem.

THEOREM 2.6: *Let C be a curve defined by* (2.9), *and $J(C)$ the jacobian variety of C. We put $P(x)^{p-1} = \sum_{i=-\infty}^{\infty} t_i x^i$ and*

$$D = \begin{vmatrix} t_{p-1} & t_{p-2} & \cdots & t_{p-r+1} \\ t_{2p-1} & t_{2p-2} & \cdots & t_{2p-r+1} \\ \vdots & \vdots & & \\ t_{(r-1)p-1} & t_{(r-1)p-2} & \cdots & t_{(r-1)p-r+1} \end{vmatrix}.$$

Then $J(C)$ becomes ordinary if and only if $D \neq 0$. In particular, if we set $\alpha_1, \alpha_2, \ldots, \alpha_r$ in a general position, $J(C)$ becomes ordinary.

§3. Some remarks on group actions

For later use, we shall make some remarks about a linearized group action on a ring in positive characteristic.

LEMMA 3.1: *Let k be a field of characteristic $p(>0)$, V a k-vector space, and σ an automorphism of V of order p. For a vector x in V, the following conditions are equivalent*:

(i) $x+\sigma(x)+\ldots+\sigma^{p-1}(x)\neq 0$.

(ii) *The vectors $x, \sigma(x),\ldots,\sigma^{p-1}(x)$ are linearly independent. Moreover, in this case*

$$\langle x, \sigma(x),\ldots,\sigma^{p-1}(x)\rangle^{\langle\sigma\rangle}=\langle x+\sigma(x)+\ldots+\sigma^{p-1}(x)\rangle.$$

PROOF. Since the implication (ii) $\Rightarrow$ (i) is obvious, we shall prove the converse. We set $V\supset W=\langle x, \sigma(x),\ldots,\sigma^{p-1}(x)\rangle$, and $\dim W=n$. Then W is σ-stable and $1\leqslant n\leqslant p$. So, for simplicity, we identify V and W. We take the Jordan canonical form of σ so that

$$\sigma=\begin{pmatrix} J_1 & & 0\\ & \ddots & \\ 0 & & J_r\end{pmatrix}$$

where $J_i=E_i+T_i\in M(n_i\times n_i;\, k)$ with E_i: the unit matrix; T_i: a torsion matrix of order n_i and $\sum_{i=1}^r n_i=n$. On the other hand, formally,

$$\begin{aligned}&1+(1+t)+(1+t)^2+\ldots+(1+t)^{p-1}\\&=\binom{p}{1}+\binom{p}{2}t+\ldots+\binom{p}{p-1}t^{p-2}+\binom{p}{p}t^{p-1}.\end{aligned}$$

Therefore

$$E_i+J_i+J_i^2+\ldots+J_i^{p-1}=\binom{p}{n_i}T_i^{n_i-1}=\begin{cases}0 & \text{if} \quad n_i<p\\ T_i^{p-1} & \text{if} \quad n_i=p.\end{cases}$$

This implies that if $n_i<p$ for all i, each member e_j of the Jordan canonical basis of V satisfies the equation

$$e_j+\sigma(e_j)+\ldots+\sigma^{p-1}(e_j)=0.$$

But x can be written as a linear combination of e_j's. This contradicts our assumption (i). Hence som n_i must be equal to p, and $n=p$.

The moreover part is a consequence of an easy calculation. Q.E.D.

COROLLARY 3.2: *Let V and σ be as above, and $x_1, x_2,\ldots,x_r$ be vectors of*

V. Assume that

$$\sum_{i=1}^{p-1} \sigma^i(x_j) \quad (j=1,\dots,r)$$

are linearly independent. Then

$$\sigma^i(x_j) \quad (i=1,\dots,p-1; j=1,\dots,r)$$

are linearly independent.

PROOF: We shall prove this assertion by induction on r. For $r=1$, our assertion is contained in the above lemma. So, providing our assertion for $r-1$, we shall prove it for r. For convenience sake, we put $V_i = \langle x_i, \sigma(x_i),\dots,\sigma^{p-1}(x_i)\rangle$ for $i=1,\dots,r$. Then, by induction hypothesis,

$$(V_1 + \dots + V_{r-1})^{\langle\sigma\rangle} = \left\langle \sum_{i=0}^{p-1} \sigma^i(x_1), \sum_{i=0}^{p-1} \sigma^i(x_2),\dots, \sum_{i=0}^{p-1} \sigma^i(x_{r-1}) \right\rangle.$$

If $W=(V_1 + \dots + V_{r-1}) \cap V_r \neq \{0\}$, then W is σ-stable and it contains a non-trivial σ-invariant vector ω. Since ω is contained in both spaces $V_1 + \dots + V_{r-1}$ and V_r, ω can be written as follows:

$$\omega = \lambda_1 \sum_{i=0}^{p-1} \sigma^i(x_1) + \dots + \lambda_{r-1} \sum_{i=0}^{p-1} \sigma^i(x_{r-1}) = \mu \sum_{i=0}^{p-1} \sigma^i(x_r).$$

Hence by our summation, we get

$$\lambda_1 = \lambda_2 = \dots = \lambda_{r-1} = \mu = 0.$$

This contradicts the hypothesis $\omega \neq 0$. Q.E.D.

LEMMA 3.3: *Let k be a field of positive characteristic p, V a finite dimensional k-vector space, and σ an automorphism of V of order p. We denote by $k[[V]]$ the completion at the origin of the symmetric algebra of V. Then there exists a σ-stable prime ideal $\mathfrak{P}$ of $k[[V]]$ such that* f.f.$(k[[V]]/\mathfrak{P})$ *is an inseparable non-trivial extension over* f.f.$(k[[V]]^{\langle\sigma\rangle}/(k[[V]]^{\langle\sigma\rangle} \cap \mathfrak{P}))$.

PROOF: If V is decomposed into a direct sum of two σ-stable subspaces X and Y; i.e., $V = X \oplus Y$, then

$$k[[V]]^{\langle\sigma\rangle}/(Y) \cap k[[V]]^{\langle\sigma\rangle} \simeq k[[X]]^{\langle\sigma\rangle}. \tag{3.1}$$

In fact, we take bases $\{x_1, x_2,\dots,x_r\}$ and $\{y_1, y_2,\dots,y_s\}$ of X and Y, respectively. Then every element F of $k[[V]]$ can be written as follows:

$$F = F_0(x) + G_1(x, y)y_1 + G_2(x, y)y_2 + \ldots + G_s(x, y)y_s.$$

If F is σ-invariant, since X and Y are σ-stable, we can deduce the equality

$$F_0(x)^\sigma = F_0(x).$$

This implies that

$$k[[X]] \simeq k[[V]]/(Y) \supset k[[v]]^{\langle\sigma\rangle}/k[[V]]^{\langle\sigma\rangle} \cap (Y)$$

$$\simeq k[[X]]^{\langle\sigma\rangle}.$$

Therefore, by using the Jordan canonical form of σ and (3.1), we may assume that the action of σ on V is in the following style: There exists a basis $\{x_1, x_2, \ldots, x_n\}$ of V such that

$$x_1^\sigma = x_1 + x_2,\ x_2^\sigma = x_2 + x_3, \ldots, x_{n-1}^\sigma = x_{n-1} + x_n,\ x_n^\sigma = x_n$$

with $2 \leqslant n \leqslant p$. In this case, obviously we have canonical inclusions

$$k[[V]]^{\langle\sigma\rangle}/(x_n) \subset (k[[V]]/(x_n))^{\langle\sigma\rangle} \subset k[[V]]/(x_n).$$

Hence for our purpose we have only to find out a σ-stable prime ideal $\mathfrak{P}$ in $k[[V]]/(x_n)$ so that f.f.$((k[[V]]/(x_n))/\mathfrak{P})$ is an inseparable non-trivial extension over f.f.$((k[[V]]/(x_n))^{\langle\sigma\rangle}/\mathfrak{P} \cap (k[[V]]/(x_n))^{\langle\sigma\rangle})$. Therefore, by induction on n, we can restrict ourselves to the case where $n = 2$; i.e.,

$$V = \langle x, y\rangle \text{ and } x^\sigma = x,\ y^\sigma = y + x.$$

In this case, we can easily see that

$$k[[x, y]]^{\langle\sigma\rangle} = k[[x, N(y)]], \tag{3.2}$$

where

$$N(y) = y(y + x)\ldots(y + (p-1)x) = y^p - yx^{p-1}.$$

Hence if we take the prime ideal (x) as $\mathfrak{P}$, then

$$k[[y]] \simeq k[[x, y]]/(x) \supsetneqq k[[x, y]]^{\langle\sigma\rangle}/(x) = k[[x, N(y)]]/(x)$$

$$\simeq k[[y^p]],$$

and this extension is just our required one.

In fact, the equality (3.2) will be given as follows. The relation $k[[x, y]]^{\langle\sigma\rangle} \supset k[[x, N(y)]]$ is trivial. So, we take an element $F(x, y)$ of $k[[x, y]]^{\langle\sigma\rangle}$. Since the action of σ is a graded ring homomorphism, so we may assume that $F(x, y)$ is a homogeneous polynomial of degree d. Then dividing $F(x, y)$ by $N(y)$, we get

$$F(x, y) = N(y)P(x, y) + Q_0(x)y^{p-1} + Q_1(x)y^{p-2} + \dots + Q_{p-1}(x)$$

where $Q_i(x)$'s are monomials and $P(x, y)$ is a homogeneous polynomial of degree $d-p$. Since $F(x, y)^\sigma = F(x, y)$, we get the equalities

$$P(x, y) = P(x, y+x),$$

and

$$\begin{aligned} &Q_0(x)y^{p-1} + Q_1(x)y^{p-2} + \dots + Q_{p-1}(x) \\ &= Q_0(x)(y+x)^{p-1} + Q_1(x)(y+x)^{p-2} + \dots + Q_{p-1}(x). \end{aligned}$$

From the latter equality, we get

$$\begin{aligned} \binom{p-1}{1}Q_0(x)y^{p-2}x + \binom{p-1}{2}Q_0(x)y^{p-3}x^2 + \dots &+ \binom{p-1}{p-1}Q_0(x)x^{p-1} \\ + \binom{p-2}{1}Q_1(x)y^{p-3}x + \dots &+ \binom{p-1}{p-2}Q_1(x)x^{p-2} \\ &\vdots \\ &+ Q_{p-2}(x)x = 0. \end{aligned}$$

This equality yields that

$$Q_0(x) = Q_1(x) = \dots = Q_{p-2}(x) = 0,$$

that is,

$$F(x, y) = N(y)P(x, y) + Q_{p-1}(x).$$

Therefore by induction on the degree d of $F(x, y)$, we get the fact that $F(x, y) \in k[[x, N(y)]]$. Q.E.D.

Lastly, we state here a well-known theorem about the representation of a cyclic group of prime order p into the group $\mathrm{GL}_n(\boldsymbol{Z}_p)$ of general linear matrices of size n.

THEOREM 3.4: *Let p be a prime integer, and n a given integer. Let A_0 and A_1 be the matrices defined by*

$$A_0 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -1 & -1 & -1 & \dots & -1 \end{pmatrix} \in \mathrm{GL}_{p-1}(\boldsymbol{Z}_p)$$

and

$$A_1 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} \in \mathrm{GL}_p(\boldsymbol{Z}_p),$$

respectively. If $A \in \mathrm{GL}_n(\boldsymbol{Z}_p)$ satisfies the equality

$$A^p = E_n,$$

then A is conjugate to a matrix of the type

$$\begin{pmatrix} A_0 & & & & & & \\ & \ddots & & & 0 & & \\ & & A_0 & & & & \\ & & & A_1 & & & \\ & 0 & & & \ddots & & \\ & & & & & A_1 & \\ & & & & & & E \end{pmatrix},$$

where E means the unit matrix.

In fact, we can easily get this theorem by modifying the proof of ([2], Theorem 74.3.)

§4. Characteristic 2 case (for curves)

By the argument of §2, every hyperelliptic curve of genus g over a field of characteristic 2 is given by

$$C\colon\ y^2 + B(x)y = A(x),$$

with

$$A(x)=(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_r)G(x),$$

$$B(x)=(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\dots(x-\alpha_r)^{n_r},$$

$$G(\alpha_i)\neq 0,\ \deg G=2N-r,\ g=N-1 \text{ and } N=\sum_{i=1}^{r} n_i.$$

In this case, a basis of $H^0(C, \Omega_C^{\otimes 2})$ is given by Proposition 2.5. Since $H^1(C, \check{\Omega}_C^1)$ is dual to $H^0(C, \Omega_C^{\otimes 2})$, we can calculate the action σ^*, of the involution σ of C, on $H^1(C, \check{\Omega}_C^1)$ as follows.

LEMMA 4.1: *There exists a k-basis* $\{a_1, a_2,\dots, a_{g-2}, a_{g-1},\dots, a_{2g-1}, b_1, b_2,\dots, b_{g-1}\}$ *of* $H^1(C, \check{\Omega}_C^1)$ *such that*

$$\sigma^* a_i = a_i \quad (1\leqslant i\leqslant 2g-1)$$

and

$$\sigma^* b_j = b_j + a_j \quad (1\leqslant j\leqslant g-2).$$

(cf. Laudal-Lønsted [10] p. 158 or Oort-Steenbrink [22], p.47).

We choose an odd integer l larger than 2, and a level l-structure α for C. Then (C, α) defines a point $x\in M=M_{g,l}$. By virtue of the above lemma, there exists a complete system of regular parameters

$$\{w_1, w_2,\dots, w_{g+1}, u_1, u_2,\dots, u_{g-2}, v_1, v_2,\dots, v_{g-2}\} \tag{4.1}$$

of $\hat{\mathcal{O}}_{x,M}$ such that

$$\begin{cases} \sigma^* v_i = u_i & (i=1,2,\dots,g-2) \\ \sigma^* w_j \equiv w_j \pmod{\mathfrak{M}_x^2} & (j=1,2,\dots,g+1). \end{cases}$$

Following Oort-Steenbrink ([22], p. 8), let Σ be the involution of $M_{g,l}$ defined by $(E, \beta)\mapsto(E, -\beta)$ for every curve E of genus g with level l-structure β, and $j^{(l)}$: $M_{g,l}\to A_{g,l}$ the Torelli map defined by $(E, \beta)\mapsto (J(E), \lambda(E), \beta)$. In particular, for $l=1$, we put $j^{(1)}=j$. Obviously $j^{(l)}$ induces the morphism ι: $V_{g,l}=M_{g,l}/\Sigma\to A_{g,l}$; i.e., we have a commutative diagram (the notations following loc. cit. [22], p. 8):

$$\begin{tikzcd}
M_{g,l} \arrow[rr, "j^{(l)}"] \arrow[dr, "q"] \arrow[dd, "\phi"'] & & A_{g,l} \arrow[dd, "\psi_2"] \\
& V_{g,l} \arrow[ur, "\iota"'] \arrow[dl, "\psi_1"] \arrow[dr] & \\
M_g \arrow[rr, "j"'] & & A_g .
\end{tikzcd}$$

Under these notations, we shall prove the following.

THEOREM 4.2: *Let z be the generic point of the hyperelliptic locus* (*in the sense of* [10], *Definition* 2) *in* ${}^{(2)}M_g(g \geqslant 3)$, *and D a curve corresponding to z. Then we have $k_D \supsetneqq \boldsymbol{k}(z)$.*

PROOF: First, we remark a result of Lønsted [11], theorem 4.1) and one of Laudal-Lønsted ([10], Theorem 3). The first one asserts the irreducibility of the hyperelliptic locus, and the latter one implies that the hyperelliptic curves with a level l-structure form a regular subscheme in $M_{g,l}(l \geqslant 3)$.

We take a hyperelliptic curve C and choose a point $x \in M_{g,l}$ as above. Then by (4.1),

$$\hat{\mathcal{O}}_x = \hat{\mathcal{O}}_{x,M_{g,l}} \simeq k\big[\big[w_1,\dots,w_{g+1}, u_1,\dots,u_{g-2}, v_1,\dots,v_{g-2}\big]\big],$$

where $k = \boldsymbol{k}(x)$. Let z' be the point on $M_{g,l}$ lying over z, whose locus contains x, and $\mathfrak{P}$ the prime ideal of $\hat{\mathcal{O}}_x$ defining the locus $\overline{\{z'\}}$. Since σ^* acts trivially on

$$\hat{\boldsymbol{k}}(z) = \text{f.f.}\big(k\big[\big[w_1,\dots,w_{g+1}, u_1,\dots,u_{g-2}, v_1,\dots,v_{g-2}\big]\big]/\mathfrak{P}\big),$$

$\mathfrak{P}$ contains the variables

$$u_1 + v_1, u_2 + v_2,\dots,u_{g-2} + v_{g-2}.$$

Since the dimension of the hyperelliptic locus is $2g - 1$, we see that

$$\mathfrak{P} = \big(u_1 + v_1, u_2 + v_2,\dots,u_{g-2} + v_{g-2}\big).$$

Now, $\hat{\mathcal{O}}_x$ is a Galois covering of $\hat{\mathcal{O}}_x^{\langle\sigma^*\rangle}$ with Galois group $G = [\sigma]$, and G is the inertia group of $\mathfrak{P}$. Hence f.f. $(\hat{\mathcal{O}}_x/\mathfrak{P})$ is purely inseparable over f.f.$(\hat{\mathcal{O}}_x^{\langle\sigma^*\rangle}/\mathfrak{P}^{\langle\sigma^*\rangle})$. If f.f.$(\hat{\mathcal{O}}_x/\mathfrak{P}) =$ f.f.$(\hat{\mathcal{O}}_x^{\langle\sigma^*\rangle}/\mathfrak{P}^{\langle\sigma^*\rangle})$, since $\mathfrak{P}^{\langle\sigma^*\rangle}\hat{\mathcal{O}}_x = \mathfrak{P}$, this covering is unramified at $\mathfrak{P}^{\langle\sigma^*\rangle}$ and we get the equality

$$(\hat{\mathcal{O}}_x)_{\mathfrak{P}} = \big(\hat{\mathcal{O}}_x^{\langle\sigma^*\rangle}\big)_{\mathfrak{P}^{\langle\sigma^*\rangle}}.$$

This is absurd, for we assumed $g \geqslant 3$. Hence f.f.$(\hat{\mathcal{O}}/\mathfrak{P})$ is not equal to f.f.$(\hat{\mathcal{O}}_x^{\langle\sigma^*\rangle}/\mathfrak{P}^{\langle\sigma^*\rangle})$. Moreover, in general, let $(A, \mathfrak{M})$ be a local Nagata domain, and $\hat{A}$ the completion of A. Then f.f.$(\hat{A})$ is separably generated over f.f.(A) (cf. Matsumura [13], (31.F), Theorem 71). Therefore, we obtain that $\boldsymbol{k}(z') \supsetneqq \boldsymbol{k}(z)$. Thus we get our assertion by Proposition 1.8′. Q.E.D.

COROLLARY 4.3: *If D is a curve corresponding to the generic point of the hyperelliptic locus in ${}^{(2)}M_g (g \geqslant 3)$, then $k_D \supsetneqq k_{P(D)}$.*

PROOF: Since $P(D)$ has only automorphisms $\pm \mathbf{1}_{P(D)}$ (cf. Matsusaka [15], p. 790, Theorem), the point x of A_g corresponding to $P(D)$ is a simple point (cf. Oort [21], Theorem 1.AV.). Hence, by Corollary 1.10,

$$\boldsymbol{k}(x) = k_{P(D)}.$$

On the other hand, $\boldsymbol{k}(z)$ contains $\boldsymbol{k}(x)$, and by the above theorem, the field of moduli k_D is not equal to $\boldsymbol{k}(z)$, where $z \in M_g$ is the point corresponding to D. Thus we obtain our assertion. Q.E.D.

In the previous paper [28], the author showed that except in characteristic two, the isomorphism scheme of curves is almost isomorphic to that of their principally polarized jacobian schemes. But, in characteristic two, there exists a counter example. In fact, combining Corollary 4.3 with Theorems 1.9 and 1.9′, we can get easily the following.

REMARK 4.4: *Let S be a spectrum of an artin local ring of characteristic two, and C, C' hyperelliptic curves over S. Then, in general the canonical map*

$$\boldsymbol{Isom}_S(C, C') \to \boldsymbol{Isom}_S(P(C'), P(C))$$

is not isomorphic.

§5. Characteristic 3 case (for curves)

Let C be a curve defined by (2.9) over a field of characteristic $p = 3$. That is,

$$C: y^3 - B(x)y = A(x), \tag{5.1}$$

where

$$A(x)=P(x)^2G(x),$$

$$B(x)=P(x)^2,$$

$$P(x)=(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_r) \quad (r\geqslant 2),$$

$$\deg G(x)=r.$$

Let σ be, as in §2, the automorphism of C defined by $y\mapsto y+P$. The genus of C is given by $g=2(r-1)$. By Corollary 2.3, a basis of $H^0(C, \Omega_C^{\otimes 2})$ is given by

$$\begin{aligned} &y^2(dx/B)^2, xy^2(dx/B)^2,\dots,x^{2r-4}y^2(dx/B)^2;\\ &Py(dx/B)^2, xPy(dx/B)^2,\dots,x^{2r-4}Py(dx/B)^2; \qquad (5.2)\\ &P^2(dx/B)^2, xP^2(dx/B)^2,\dots,x^{2r-4}P^2(dx/B)^2. \end{aligned}$$

Therefore

$$\sum_{i=0}^{2}\left(x^ly^2(dx/B)^2\right)^{(\sigma^*)^i}=2x^lP^2(dx/B)^2$$

for $l=0, 1,\dots,2r-4$. Hence, if we choose a level n-structure α of C with $n\geqslant 3$ and $3\nmid n$, and x is the point on $M=M_{g,n}$ corresponding to (C, α), by Corollary 3.2, the action σ on $\hat{\mathcal{O}}_{x,M}$ is linearlized. So, by Lemma 3.3, we get the following.

THEOREM 5.1: *Let g be a given even integer. Then there exists a curve C of genus g over a field of characteristic* 3 *with ordinary jacobian variety so that* $k_C \supsetneqq \boldsymbol{k}(x)$, *where x is the point on* M_g *corresponding to C.*

COROLLARY 5.2: *Let g be as above. Then there exists a principally polarized ordinary abelian variety* $P=(X,\lambda)$ *of dimension g over a field of characteristic* 3 *so that* $k_P\supsetneqq \boldsymbol{k}(y)$, *where y is the point on* A_g *corresponding to P.*

In fact, we take a curve C as in Theorem 5.1. Furthermore, let x and y be the points on M_g and A_g corresponding to C and $P(C)$, respectively. By a result of ([28], Corollary 3.3), $k_C=k_{P(C)}$. On the other hand, by our choice of C, $k_C\supsetneqq \boldsymbol{k}(x)\supset \boldsymbol{k}(y)$. Thus we are done. Q.E.D.

§6. Abelian varieties with automorphisms of order p

In this section, we shall discuss our problem for abelian varieties. Our main tool is Serre-Tate's theorem. So we will start with the theorem. Let p be a prime integer, S a scheme with p locally nilpotent on it, and S_0 a closed subscheme of S defined by a locally nilpotent quasi-coherent ideal $\mathscr{I}$ of $\mathscr{O}_S$. For an abelian scheme X, we denote by $\bar{X}$ the Barsotti-Tate group associated to it. Now we fix an abelian scheme X_0 over S_0 of relative dimension g. We set

$$\mathscr{L}(X_0;\, S_0 \hookrightarrow S) = \left\{\begin{array}{l}\text{isomorphism classes of pairs } (X, i) \text{ such}\\ \text{that } X \to S \text{ is an abelian scheme,}\\ \text{and } i\colon X \times_S S_0 \xrightarrow{\sim} X_0 \text{ an isomorphism}\end{array}\right\}$$

and

$$\mathscr{L}(\bar{X}_0;\, S_0 \hookrightarrow S) = \left\{\begin{array}{l}\text{isomorphism classes of pairs } (B, i) \text{ such}\\ \text{that } B \to S \text{ is a Barsotti-Tate group,}\\ \text{and } i\colon B \times_S S_0 \xrightarrow{\sim} \bar{X}_0 \text{ an isomorphism}\end{array}\right\}$$

Then Serre-Tate's theorem can be stated as follows:

THEOREM 6.1 (Serre-Tate): *The map* $(X, i) \mapsto (\bar{X}, \bar{i})$ *gives a bijection from* $\mathscr{L}(X_0;\, S_0 \hookrightarrow S)$ *to* $\mathscr{L}(\bar{X}_0;\, S_0 \hookrightarrow S)$.
(cf. Messing [16], Chapter V, Theorem 2.3.)

Moreover, let R be a complete local ring with perfect residue field k of characteristic p, and G_0' and G_0'' be ind-étale and toroidal Barsotti-Tate groups on $S_0 = \operatorname{Spec} k$, respectively. Let G' and G'' be the liftings of G_0' and G_0'' to Barsotti-Tate groups on S. Then we get the following.

PROPOSITION 6.2: *There is a bijection from* $\mathscr{L}(G_0' \times G_0'';\, \operatorname{Spec} k \to S)$ *to* $\operatorname{Ext}^1(G', G'')$.
(cf. [16], Appendix, Corollary (2.3).)

Now, we reformulate the argument in (loc. cit., Appendix) for our purpose. We denote by $\boldsymbol{\mu}$ the formal scheme

$$\boldsymbol{\mu} = \varinjlim \mu_{p^n}.$$

Let R be an artin local ring with perfect residue field k of characteristic p.

We consider the inductive system of sheaves on $S = \operatorname{Spec} R$:

$$\boldsymbol{Z}^g \xrightarrow{g} \boldsymbol{Z}^g \xrightarrow{p} \boldsymbol{Z}^g \xrightarrow{p} \cdots.$$

Then we get a canonical exact sequence of sheaves on S:

$$0 \to \boldsymbol{Z}^g \to \varinjlim \boldsymbol{Z}^g \to (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g \to 0.$$

By taking the long exact sequence of this sequence, we get an isomorphism:

PROPOSITION 6.3: *The homomorphism*

$$\delta_R \colon \bigoplus_{i=1}^{r} \boldsymbol{\mu}^g(R_i) \to \operatorname{Ext}^1_R\big((\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g, \boldsymbol{\mu}^g\big)$$

$$\simeq \bigoplus_{i,j} \operatorname{Ext}^1_R\big((\boldsymbol{Q}_p/\boldsymbol{Z}_p)_i, \boldsymbol{\mu}_j\big)$$

is an isomorphism. Here R_i, $(\boldsymbol{Q}_p/\boldsymbol{Z}_p)_i$ and $\boldsymbol{\mu}_j$ are the copies of R, $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ and $\boldsymbol{\mu}$, respectively. Hence we get an isomorphism

$$\delta_R \colon \boldsymbol{\mu}^{g^2}(R) \xrightarrow{\sim} \bigoplus_{i,j} \operatorname{Ext}^1_R\big(\boldsymbol{Q}_p/\boldsymbol{Z}_p, \boldsymbol{\mu}\big).$$

(cf., loc. cit., Appendix, Proposition 2.5.)

Next, let (X_0, λ_0) be an ordinary abelian variety of dimension g over an algebraically closed field k of characteristic p, with a principal polarization $\lambda_0 \colon X_0 \to \hat{X}_0$. Then the Barsotti-Tate group $\overline{X}_0$ associated to X_0 is decomposed into

$$\overline{X}_0 = G_0' \times G_0'',$$

where $G_0' = \overline{X}_0^{\text{ét}}$ and $G_0'' = \overline{X}_0^{\text{tor}}$ are the étale and the toroidal parts of $\overline{X}_0$, respectively. Then the polarization λ_0 induces the isomorphisms:

$$\begin{array}{ccc} \overline{X}_0 & \xrightarrow{\sim} & G_0' \times G_0'' \\ \bar{\lambda}_0 \downarrow & & \downarrow \lambda_1 \times \lambda_2 \\ \hat{\overline{X}}_0 & \xrightarrow{\sim} & \hat{G}_0'' \times \hat{G}_0'. \end{array}$$

Since λ_0 is symmetric, we get the equalities

$$\lambda_1 = \hat{\lambda}_2 \quad \text{and} \quad \lambda_2 = \hat{\lambda}_1.$$

Now we choose an isomorphism

$$r_0 \colon G_0' \xrightarrow{\sim} (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g,$$

and put

$$s_0 = \hat{r}_0^{-1} \circ \lambda_2 \colon G_0'' \xrightarrow{\sim} \boldsymbol{\mu}^g.$$

Using these isomorphisms, we get a commutative diagram:

$$\begin{array}{ccccccccc} 0 \to \boldsymbol{\mu}^g \to & \overline{X}_0 & \to (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g \to 0 \\ \| & \downarrow \overline{\lambda}_0 & \| \\ 0 \to \boldsymbol{\mu}^g \to & \hat{\overline{X}}_0 & \to (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g \to 0. \end{array} \tag{6.1}$$

Let σ_0 be an automorphism of (X_0, λ_0). Then σ_0 induces the isomorphisms:

$$\begin{array}{cccc} \overline{X}_0 & \xrightarrow{\sim} G_0' \times G_0'' & \overset{r_0 \times s_0}{\xrightarrow{\sim}} & (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g \times \boldsymbol{\mu}^g \\ \bar{\sigma}_0 \downarrow & \downarrow \sigma_1 \times \sigma_2 & & \downarrow \sigma_1' \times \sigma_2' \\ \overline{X}_0 & \xrightarrow{\sim} G_0' \times G_0'' & \overset{r_0 \times s_0}{\xrightarrow{\sim}} & (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g \times \boldsymbol{\mu}^g. \end{array} \tag{6.2}$$

Here $\sigma_1' \in \operatorname{Aut}((\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g) = \mathrm{GL}_g(\boldsymbol{Z}_p)$ and $\sigma_2' \in \operatorname{Aut}(\boldsymbol{\mu}^g) = \mathrm{GL}_g(\boldsymbol{Z}_p)$. Since $\lambda_0 = \hat{\sigma}_0 \lambda_0 \sigma_0$, we get the equality

$$\hat{\sigma}_2' = \sigma_1'^{-1},$$

that is,

$${}^t\sigma_2' = \sigma_1'^{-1}, \tag{6.3}$$

where ${}^t\sigma_2'$ means the transposed matrix of $\sigma_2' \in \mathrm{GL}_g(\boldsymbol{Z}_p)$. Let $(R, \mathfrak{M})$ be a complete noetherian local ring with residue field k, and

$$\mathscr{L}((X_0, \lambda_0); \operatorname{Spec} k \to \operatorname{Spec} R)$$

$$= \left\{ \begin{array}{l} \text{isomorphism classes of triplets } (X, \lambda, i) \text{ such} \\ \text{that } X \to \operatorname{Spec} R \text{ is an abelian scheme,} \\ \lambda \colon X \to \hat{X} \text{ a polarization, } i \colon X \otimes_R k \xrightarrow{\sim} X_0, \\ \text{and } \lambda \otimes k = \hat{i} \circ \lambda_0 \circ i \end{array} \right\}.$$

Then summalizing the above discussion, we obtain the following.

THEOREM 6.4: *There is a bijection*

$$\mathscr{L}((X_0, \lambda_0); \operatorname{Spec} k \to \operatorname{Spec} R) \to \mathrm{SM}_g(1 + \mathfrak{M}),$$

where $\mathrm{SM}_g(1 + \mathfrak{M})$ *is the set of symmetric* $g \times g$ *matrices with entries in* $1 + \mathfrak{M}$. *Moreover, for an automorphism* σ_0 *of* (X_0, λ_0), *we define* σ_1' *and* σ_2' *by* (6.2). *Then the action* σ_0 *on* $\mathrm{SM}_g(1 + \mathfrak{M})$ *through the above bijection is given by*

$$A \mapsto {}^{t\sigma_2'}A^{\sigma_2'} = {}^{\sigma_1'^{-1}}A^{t\sigma_1'^{-1}}. \tag{6.4}$$

Here, for $g \times g$ *matrices* $U = (u_{ij})$, $A = (a_{ij})$ *and* $V = (v_{ij})$, *we define* ${}^{U}A$ *and* A^{V} *as follows*:

$$\textit{the } (i, j) \textit{ component of } {}^{U}A = \prod_{l=1}^{g} a_{lj}^{u_{il}};$$

$$\textit{the } (i, j) \textit{ component of } A^{V} = \prod_{l=1}^{g} a_{il}^{v_{lj}}.$$

PROOF: Combining Theorem 6.1 with Propositions 6.2 and 6.3, forgetting the polarization gives an injection

$$\mathscr{L}((X_0, \lambda_0); \operatorname{Spec} k \hookrightarrow \operatorname{Spec} R) \to \boldsymbol{\mu}^{g^2}(R) = M_g(1 + \mathfrak{M}),$$

where $M_g(1 + \mathfrak{M})$ is the set of $g \times g$ matrices with entries in $1 + \mathfrak{M}$. Obviously, by the bijections given in Propositions 6.2 and 6.3, the Cartier dual corresponds to the transposition on $M_g(1 + \mathfrak{M})$. Therefore when $A = (a_{ij}) \in M_g(1 + \mathfrak{M})$ corresponds with a formal lifting X over R of X_0, noticing the commutative diagram (6.1), X admits a lifted polarization λ of λ_0 if and only if $A = {}^{t}A$. Moreover, by the Grothendieck theory (cf. EGA, Chapitre III, Théorème 5.4.5), every proper formal scheme with a lifted polarization is algebraisable. Hence, we get a bijection

$$\mathscr{L}((X_0, \lambda_0); \operatorname{Spec} k \hookrightarrow \operatorname{Spec} R) \xrightarrow{\sim} \mathrm{SM}_g(1 + \mathfrak{M}).$$

Let σ_0 be an automorphism of (X_0, λ_0), σ_1', $\sigma_2' \in \mathrm{GL}_g(\boldsymbol{Z}_p)$ be as above, and $A \in M_g(1 + \mathfrak{M}) \simeq \operatorname{Ext}^1_R((\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g, \boldsymbol{\mu}^g)$ corresponds to an extension of $(\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g$ by $\boldsymbol{\mu}^g$:

$$E\colon 0 \to \boldsymbol{\mu}^g \to G \to (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g \to 0.$$

Then the "pushing out" of E via σ_2': $\boldsymbol{\mu}^g \to \boldsymbol{\mu}^g$ and the "pulling back" of E via σ_1': $(\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g \to (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g$ correspond to the maps of $M_g(1 + \mathfrak{M})$:

$$A \mapsto A^{\sigma_2'}$$

and

$$A \mapsto {}^{\sigma_1'}A,$$

respectively. On the other hand, obviously via the map

$$\mathscr{L}((X_0, \lambda_0); \operatorname{Spec} k \to \operatorname{Spec} R) \to \operatorname{Ext}^1_R\big((\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g, \mu^g\big),$$

the action σ_0 on $\mathscr{L}((X_0, \lambda_0); \operatorname{Spec} k \to \operatorname{Spec} R)$ corresponds to the composition of the "pushing out" via σ_2' and the "pulling back" via σ_1'. Therefore, noticing the equality (6.3), we obtain the assertion of the moreover part in the theorem. Q.E.D.

Hereafter, we fix an algebraically closed field k of characteristic p. Let l be an integer larger than 2 and prime to p. Let $(X_0, \lambda_0, \alpha_0)$ be a principally polarized ordinary abelian variety (X_0, λ_0) of dimension g over k with a level l-structure α_0. Then this triplet defines a point x on $A_{g,l} \otimes k$. Moreover, let σ_0 be an automorphism of (X_0, λ_0) of order p, and σ_1' be the automorphism, induced by σ_0, of the étale part G_0' of the Barsotti-Tate group $\overline{X}_0$ of X_0. Since G_0' is isomorphic to $(\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g$, σ_1' can be seen as an element of order p of $\mathrm{GL}_g(\boldsymbol{Z}_p)$. Therefore, by Theorem 3.4, we can choose an isomorphism

$$r_0 \colon G_0' \xrightarrow{\sim} (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^g$$

so that σ_1' becomes the following style:

$$\sigma_1' = \begin{pmatrix} A_0^{-1} & & & & & & \\ & \ddots & & & 0 & & \\ & & A_0^{-1} & & & & \\ & & & A_1^{-1} & & & \\ & 0 & & & \ddots & & \\ & & & & & A_1^{-1} & \\ & & & & & & E \end{pmatrix}, \tag{6.5}$$

where A_0 and A_1 are as in Theorem 3.4. Here, let a be the number of A_0^{-1}'s in σ_1', and e be the size of E. Under these notation, we get the following theorem:

THEOREM 6.5: *The action of σ_0 over the completion $\hat{\mathcal{O}}_x$ of the local ring $\mathcal{O}_x$ at the point x can be linearized if and only if $ae = 0$.*

PROOF: By Theorem 6.4,

$$\hat{\mathcal{O}}_x \xrightarrow{\sim} k\left[\left[x_{11}-1,\ x_{12}-1,\dots,x_{gg}-1\right]\right]\Big/\left(\left\{\ x_{ij}-x_{ji}\Big|^{i,j}_{=1,2,\dots,g}\right\}\right). \tag{6.6}$$

Of course, we take the variables x_{ij} using the above r_0. Moreover, due to the same theorem, the action of σ_0 on the right hand side of (6.6) is given by

$$(x_{ij}) \mapsto {}^{\sigma_1'^{-1}}(x_{ij})^{{}^t\sigma_1'^{-1}}.$$

Therefore, we can reduce our problem to the posibility of the linearization of the action ρ of $\boldsymbol{Z}/p\boldsymbol{Z}$ over the formal power series ring R in the following 7 cases, and we complete the proof by the following lemmas and corollary.

Case I. $R=k[[\{t_{Ij}|i,\ j=1,\dots,p-1\}]]$ and the action ρ is given by

$$\left(\sigma(x_{ij})\right)={}^{A_0}(x_{ij})^{{}^tA_0}, \tag{6.7}$$

where $x_{ij}=t_{ij}+1$ and $\sigma=\rho(\bar{1})$, and so on.

Case II. $R=k[[\{t_{ij}|i,\ j=1,\dots,p-1\}]]/(\{t_{ij}-t_{ji}|i,\ j=1,\dots,p-1\})$ and the action ρ is given by (6.7).

Case III. $R=k[[\{t_{ij}|i,\ j=1,\dots,p\}]]$ and the action ρ is given by

$$\left(\sigma(x_{ij})\right)={}^{A_1}(x_{ij})^{{}^tA_1}. \tag{6.8}$$

Case IV. $R=k[[\{t_{ij}|i,\ j=1,\dots,p\}]]/(\{t_{ij}-t_{ji}|i,\ j=1,\dots,p\})$ and the action ρ is given by (6.8).

Case V. $R=k[[\{t_{ij}|i=1,\dots,p-1;\ j=1,\dots,p\}]]$ and the action ρ is given by

$$\left(\sigma(x_{ij})\right)={}^{A_0}(x_{ij})^{{}^tA_1}. \tag{6.9}$$

Case VI. $R=k[[t_1,\dots,t_p]]$ and the action ρ is given by

$${}^t\left(\sigma(x_1),\dots,\sigma(x_p)\right)={}^{A_1t}(x_1,\dots,x_p). \tag{6.10}$$

Case VII. $R=k[[t_1,\dots,t_{p-1}]]$ and the action ρ is given by

$${}^t\left(\sigma(x_1),\dots,\sigma(x_{p-1})\right)={}^{A_0t}(x_1,\dots,x_{p-1}). \tag{6.11}$$

Hereafter, in each case, we put $T=\mathfrak{M}_R/\mathfrak{M}_R^2$ and $\bar{t}_{ij}=$ the class represented by t_{ij} in T for each i, j. Of course, in Case VII, we denote by $\bar{t}_i$ the class represented by t_i in T. Moreover, $\bar{\rho}$ denotes the induced action on $\mathfrak{M}_R/\mathfrak{M}_R^2$ of ρ, and we put $\bar{\rho}(\bar{1})=\bar{\sigma}$.

LEMMA 6.6: *In Case I, ρ is linear.*

PROOF: By (6.7),

$$\left(\sigma(x_{ij})\right) = {}^{A_0}(x_{ij})^{{}^tA_0}$$

$$= \begin{pmatrix} x_{22} & x_{23} & \cdots & x_{2,p-1} & \left(\prod_j x_{2j}\right)^{-1} \\ x_{32} & x_{33} & \cdots & x_{3,p-1} & \left(\prod_j x_{3j}\right)^{-1} \\ \vdots & \vdots & & \vdots & \vdots \\ x_{p-1,2} & x_{p-1,3} & \cdots & x_{p-1,p-1} & \left(\prod_j x_{p-1,j}\right)^{-1} \\ \left(\prod_i x_{i2}\right)^{-1} & \left(\prod_i x_{i3}\right)^{-1} & \cdots & \left(\prod_i x_{i,p-1}\right)^{-1} & \left(\prod_{i,j} x_{ij}\right) \end{pmatrix}$$

and

$$\sigma(x_{ij}) = \begin{cases} x_{i+1,j+1} & \text{if} \quad i \leqslant p-2,\ j \leqslant p-2 \\ \prod_{l=1}^{p-1} x_{i+1,l}^{-1} & \text{if} \quad i \leqslant p-2,\ j = p-1 \\ \prod_{k=1}^{p-1} x_{k,j+1}^{-1} & \text{if} \quad i = p-1,\ j \leqslant p-2 \\ \prod_{k,l} x_{kl} & \text{if} \quad i = p-1,\ j = p-1. \end{cases}$$

That is,

$$\bar{\sigma}(\bar{t}_{ij}) = \begin{cases} \bar{t}_{i+1,j+1} & \text{if} \quad i \leqslant p-2, j \leqslant p-2 \\ -\sum_{l=1}^{p-1} \bar{t}_{i+1,l} & \text{if} \quad i \leqslant p-2,\ j = p-1 \\ -\sum_{k=1}^{p-1} \bar{t}_{k,j+1} & \text{if} \quad i = p-1,\ j \leqslant p-2 \\ \sum_{k,l} \bar{t}_{k,l} & \text{if} \quad i = p-1,\ j = p-1. \end{cases}$$

Hence we get

$$\sum_{k=0}^{p-1} \bar{\sigma}^k(\bar{t}_{11}) = \bar{t}_{11} + \bar{t}_{22} + \dots + \bar{t}_{p-1,p-1} + \sum_{i,j} \bar{t}_{ij} \tag{6.12}$$

and

$$\sum_{k=0}^{p-1} \bar{\sigma}^k(\bar{t}_{12}) = \bar{t}_{12} + \bar{t}_{23} + \dots + \bar{t}_{p-2,p-1} - \sum_{l=1}^{p-1} \bar{t}_{p-1,l} - \sum_{k=1}^{p-1} \bar{t}_{k,1}. \tag{6.13}$$

Moreover, for n with $3 \leqslant n \leqslant (p-1)/2$,

$$\begin{aligned}\sum_{k=0}^{p-1} \bar{\sigma}^k(\bar{t}_{1n}) = \bar{t}_{1n} + \bar{t}_{2,n+1} + \dots + \bar{t}_{p-n,p-1} \\ - \sum_{l=1}^{p-1} \bar{t}_{p-n+1,l} + \bar{t}_{p-n+2,1} + \bar{t}_{p-n+3,2} \\ + \dots + \bar{t}_{p-1,p-2} - \sum_{k=1}^{p-1} \bar{t}_{k,n-1}.\end{aligned} \tag{6.14}$$

Compairing the coeffitients of t_{ii}'s, we can easily see that

$$\sum_{k=0}^{p-1} \bar{\sigma}^k(\bar{t}_{in}) \quad \left(n = 1, 2, \dots, \frac{p-1}{2}\right) \tag{6.15}$$

are linearly independent.

Next, we put $T_{ij} = t_{ij} - t_{ji}$ and $\bar{T}_{ij} = \bar{t}_{ij} - \bar{t}_{ji}$ for each i, j. Then

$$\sum_{k=0}^{p-1} \bar{\sigma}^k(\bar{T}_{12}) = \bar{T}_{12} + \bar{T}_{23} + \dots + \bar{T}_{p-2,p-1} + \sum_{i} \bar{T}_{i,p-1} + \sum_{j} \bar{T}_{1j}, \tag{6.16}$$

and for n with $3 \leqslant n \leqslant (p-1)/2$,

$$\sum_{k=0}^{p-1} \bar{\sigma}(\bar{T}_{1n}) = \bar{T}_{1n} + \bar{T}_{2,n+1} + \dots + \bar{T}_{p-n,p-1}$$

$$+\sum_{i=1}^{p-n} \overline{T}_{i,p-n+1} - \sum_{j=p-n+2}^{p-1} \overline{T}_{p-n+1,j}$$

$$-\overline{T}_{1,p-n+2} - \overline{T}_{2,p-n+3} - \dots - \overline{T}_{n-2,p-1}$$

$$-\sum_{i=1}^{n-2} \overline{T}_{i,n-1} + \sum_{j=n}^{p-1} \overline{T}_{n-1,j}. \tag{6.17}$$

Moreover, we put

$$U = \prod_{i=1}^{\frac{p-1}{2}} \prod_{\frac{p+1}{2} \leqslant j \leqslant \frac{p+1}{2}+i-1} \frac{t_{ij}+1}{t_{ji}+1} - 1.$$

Then obviously U is invariant under the action of ρ and

$$\overline{U} = \sum_{i=1}^{\frac{p-1}{2}} \sum_{\frac{p+1}{2} \leqslant j \leqslant \frac{p+1}{2}+i-1} \overline{T}_{ij}. \tag{6.18}$$

Now looking at the coefficients of $\overline{T}_{12}, \overline{T}_{13}, \dots, \overline{T}_{1,(p+1)/2}$ in the expansions of $\sum_{k=0}^{p-1}\bar{\sigma}^k(\overline{T}_{1n})$ $(2 \leqslant n \leqslant (p-1)/2)$ and $\overline{U}$, we get the matrix

$$A = \begin{pmatrix} 2 & 1 & 1 & \dots & 1 & 1 & 1 \\ -1 & 1 & & & & & \\ & & \ddots & \ddots & & & \\ & & & & -1 & 1 & \\ & & & & & & 1 \end{pmatrix}.$$

Here, the i-th row vector of A is made of the coefficients of T_{1j}'s in $\sum_{k=0}^{p-1}\bar{\sigma}^k(\overline{T}_{1,i+1})$ and in $\overline{U}$ if $i = (p-1)/2$. Obviously, det $A \neq 0$, or more precisely det $A = (p-1)/2$. Hnce, we have seen that the $(p-1)/2$ elements

$$\sum_{k=0}^{p-1} \bar{\sigma}^k(\overline{T}_{1n}) \qquad \left(2 \leqslant n \leqslant \frac{p-1}{2}\right) \quad \text{and} \quad \overline{U}$$

are linearly independent. Moreover, the linear independence of these elements and (6.15) is clear. Therefore, by Corollary 3.2.

$$\sigma^k(t_{1n}),\ \sigma^k(T_{1m})\quad\left(k=0,1,\dots,p-1;\ 1\leqslant n\leqslant\frac{p-1}{2};\ 2\leqslant m\leqslant\frac{p-1}{2}\right)$$

and U form a complete system of regular parameters of R, and we know the linearizability of the action ρ in Case I. Q.E.D.

COROLLARY 6.7: *In Case* II, ρ *is linear.*

PROOF: The proof of the linear independence of (6.15) in the proof of the above lemma is also true in this case. Therefore, by Corollary 3.2,

$$\sigma^k(t_{1n})\qquad\left(k=0,1,\dots,p-1;\ j=1,2,\dots,\frac{p-1}{2}\right)$$

form a complete system of regular parameters of R, and we are done. Q.E.D.

LEMMA 6.8: *In Cases* III, IV *and* VI, ρ *is linear.*

In fact,

$$^{A_1}(x_{ij})^{{}^tA_1}=A_1(x_{ij})\,{}^tA_1$$

and

$$^{A_1}{}^t(x_1,\dots,x_p)=A_1{}^t(x_1,\dots,x_p);$$

that is, these are linear.

LEMMA 6.9: *In Case* V, ρ *is linear.*

PROOF: By (6.9),

$$\left(\sigma(x_{ij})\right)={}^{A_0}(x_{ij})^{{}^tA_1}$$

$$=\begin{pmatrix} x_{22} & x_{23} & \cdots & x_{2p} & x_{21}\\ x_{32} & x_{33} & \cdots & x_{3p} & x_{31}\\ \vdots & \vdots & & \vdots & \vdots\\ x_{p-1,2} & x_{p-1,3} & \cdots & x_{p-1,p} & x_{p-1,1}\\ \left(\prod_i x_{i2}\right)^{-1} & \left(\prod_i x_{i3}\right)^{-1} & \cdots & \left(\prod_i x_{ip}\right)^{-1} & \left(\prod_i x_{i1}\right)^{-1}\end{pmatrix}.$$

Hence

$$\sigma(x_{ij}) = \begin{cases} x_{i+1,\overline{j+1}} & \text{if} \quad i \leqslant p-2 \\ \left(\prod_k x_{k,\overline{j+1}}\right)^{-1} & \text{if} \quad i = p-1 \end{cases}$$

and

$$\bar{\sigma}(\bar{t}_{ij}) = \begin{cases} t_{i+1,\overline{j+1}} & \text{if} \quad i \leqslant p-2 \\ -\sum_k \bar{t}_{k,\overline{j+1}} & \text{if} \quad i = p-1, \end{cases}$$

where $\bar{n}$ is the integer defined by $\bar{n} \equiv n \pmod p$ and $1 \leqslant \bar{n} \leqslant p$ for an integer n. Therefore

$$\sum_{k=0}^{p-1} \bar{\sigma}^k(\bar{t}_{1n}) = \sum_{l=1}^{p-1} \bar{t}_{l,\overline{n+l-1}} - \sum_i \bar{t}_{i,\overline{n+l}}$$

for $n = 1, 2, \ldots, p-1$. The coefficients of $\bar{t}_{ii}$'s in these expansions form a non-degenerate matrix of size $p-1$:

$$\begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ -1 & & & & \\ & -1 & & & \\ & & \ddots & & \\ & & & -1 & \end{pmatrix}.$$

Hence, by Corollary 3.2,

$$\sigma^k(t_{1n}) \quad (n = 1, 2, \ldots, p-1)$$

form a complete system of regular parameters of R and we are done.

Q.E.D.

LEMMA 6.10: *In Case* VII, ρ *is not linear.*

PROOF: By (6.11),

$$^t(\sigma(x_1), \ldots, \sigma(d_{p-1})) = {}^{A_0 t}(x_1, \ldots, x_{p-1})$$

$$= {}^t\left(x_2, x_3, \ldots, x_{p-1}, \left(\prod_i x_i\right)^{-1}\right); \qquad (6.19)$$

i.e.,

$$\sigma(t_j) = \begin{cases} t_{j+1} & \text{if } \ j \leqslant p-2 \\ \prod_i (t_i + 1)^{-1} - 1 & \text{if } \ j = p-1. \end{cases}$$

On the other hand, according to a result of Peskin ([24], Chapter II, Theorem 3.12), σ is linear if and only if

$$\iota\colon R^{\langle\sigma\rangle} \to R$$

is ramified in dimension > 0. Moreover, according to (loc. cit., Chapter II, Lemma 2.2), ι is ramified in dimension > 0 if and only if

$$(\sigma - 1)^{p-1} t_1 \big|_{(\sigma-1)t_1 = (\sigma-1)^2 t_1 = \ldots = (\sigma-1)^{p-2} t_1 = 0} = 0.$$

In our case, by (6.19), $(\sigma - 1)^i t_1 = 0$ for $i = 1, 2, \ldots, p-2$ imply $t_1 = t_2 = \ldots = t_{p-1}$, and

$$(\sigma - 1)^{p-1} t_1 = t_1 + \ldots + T_{p-1} + \prod_{i=1}^{p-1} (t_i + 1)^{-1} - 1.$$

Therefore,

$$\begin{aligned} &(\sigma - 1)^{p-1} t_1 \big|_{(\sigma-1)t_1 = (\sigma-1)^2 t_1 = \ldots = (\sigma-1)^{p-2} t_1 = 0} \\ &= (p-1)t_1 + (1/(t_1+1))^{p-1} - 1 \\ &= -t_1^p - t_1^{p+1} + t_1^{2p} + t_1^{2p+1} - t_1^{3p} - t_1^{3p+1} + \ldots \\ &\neq 0. \end{aligned}$$

This implies that ρ can not be linearized. Q.E.D.

Example: Let (X_0, λ_0) be the canonically polarized jacobian variety of the curve C defined by (2.9). According to Theorem 2.6, we can choose C so that X_0 becomes ordinary. Let σ_0 be the automorphism of (X_0, λ_0) corresponding to the automorphism of C defined by $y \mapsto y + P(x)$. Then $H^1(C, \mathcal{O}_C)$ is canonically isomorphic to the tangent space $T_0(X_0)$ of X_0 at the origin, and $T_0(X_0) \simeq T_0((X_0)_p)$. Moreover, $H^1(C, \mathcal{O}_C)$ is dual to $H^0(C, \Omega_C^1)$, and $\overline{X}_0^{\text{ét}}$ is Cartier dual to $\overline{X}_0^{\text{tor}}$ in our case. Therefore, by using the basis of $H^0(C, \Omega_C^1)$ given by Corollary 2.2, we can see that the action σ_1' of σ_0 over $\overline{X}_0^{\text{ét}}$ must be of the type

$$\sigma_1' = \begin{pmatrix} A_0 & & & \\ & A_0 & & \\ & & \ddots & \\ & & & A_0 \end{pmatrix}$$

in a normalized form as (6.5).

THEOREM 6.11: *Let p be an odd prime integer, and g an integer with $g \geqslant p-1$. Then there exists a principally polarized ordinary abelian variety $P = (X, \lambda)$ of dimension g over a field of characteristic p so that $k_P \neq \boldsymbol{k}(x)$, where x is the point on A_g corresponding to P.*

PROOF: Let $Q = (X_0, \lambda_0, \alpha_0)$ be a principally polarized ordinary abelian variety with a level l-structure α_0 corresponding to an $\overline{\boldsymbol{F}}_p$-rational point $y \in A_{g,l} \otimes \overline{\boldsymbol{F}}_p$ ($l \geqslant 3$, $p \nmid l$). We suppose that (X_0, λ_0) has an automorphism α_0 of order p whose action on $\hat{\mathcal{O}}_y$ is linear. Then Lemma 3.3 asserts that there exists a σ_0-stable prime ideal $\mathfrak{P}$ of $\hat{\mathcal{O}}_y$ such that $\boldsymbol{k}(y)$ is a non-trivial inseparable extension over $\hat{\mathcal{O}}_y^{\langle\sigma_0\rangle}/\mathfrak{P} \cap \hat{\mathcal{O}}_y^{\langle\sigma_0\rangle}$. Therefore, if (X, λ, α) is a triplet corresponding to $\mathfrak{P}$, Proposition 1.8 implies that $P = (X, \lambda)$ satisfies our requiring condition. Such principally polarized ordinary abelian variety (X_0, λ_0) with an automorphism σ_0 as above exists for $g = (p-1)(r-1)$, because of the above example and of Theorem 6.5. Thus we get our assertion for g with $(p-1)|g$.

Moreover for any g, we set $g = (p-1)a + r$ with $0 < r \leqslant p-2$. By the above discussion, there exists a principally polarized ordinary abelian variety $P = (X_1, \lambda_1)$ of dimension $(p-1)a$ satisfying the condition of the theorem. We choose an elliptic curve E with p-rank 1 over $\boldsymbol{F}_p$, and denote λ_2 the polarization of E defined by the origin of E. Then by Lemma 1.12, if we put $\Omega = (X_1 \times E^r, \lambda_1 \times (\lambda_2)^r)$, k_P is separable over k_Q. On the other hand, there exists a canonical morphism

$$A_{(p-1)a} \times A_1^r \to A_g.$$

Therefore $\boldsymbol{k}(y) \supset \boldsymbol{k}(x)$, where y and x are the points on $A_{(p-1)a}$ and on A_g corresponding to P and Q, respectively. By the choice of P, the extension $k_P/\boldsymbol{k}(y)$ is a non-trivial inseparable extension, and so is $k_Q/\boldsymbol{k}(x)$. Thus we are done. Q.E.D.

Acknowledgments

The author should express his hearty thanks to the referee and Professor F. Oort for their kind advice on arranging this paper.

Added in proof

The author is grateful to Mr. I. Kuribayashi for pointing out that D. Subro has already given a complete formula of the p-rank of Artin-Schreier curves and has shown that the assertion of Theorem 2.6 was always true for any mutually distinct $\alpha_1, \ldots, \alpha_r$ (cf. D. Subro: The p-rank of Artin-Schreier curves. Manuscripta Math. 16, 169–193(1975).)

References

[1] W. BAILY: On the theory of θ-functions, the moduli of abelian varieties, and the moduli of curves. *Annals of Math.* 75 (1962) 342–381.

[2] C.W. CURTIS and I. REINER: *Representation Theory of Finite Groups and Associative Algebras*. New York: Interscience Publishers (1962).

[3] N. BOURBAKI: Algèbre commutative. *Eléments de Math.* 27, 28, 30, 31. Hermann: Paris (1961–1965).

[4] P. DELIGNE and D. MUMFORD: The irreducibility of the space of curves of given genus. *Publ. Math. IHES* 36 (1969) 75–110.

[5] A. GROTHENDIECK: Fondéments de la géométrie algébrique. *Séminaire Bourbaki 1957–1962.* Secrétariat Math. paris (1962). Refered to as FGA.

[6] A. GROTHENDIECK and J. DIEUDONNÉ: Eléments de géométrie algébrique. *Publ. Math. IHES* 4, 8, 11, 17, 20, 24, 28, 32, 1960–1972. Refered to as EGA.

[7] A. GROTHENDIECK et al.: Séminaire de géométrie algébrique 1. *Lecture Notes in Math.* Vol. 224. Berlin-Heidelberg-New York: Springer (1971). Refered to as SGA 1.

[8] H. HASSE: Theorie der relativ-zyklischen algebraischen Funktionen-Körper, insbesondere bei endlichen Konstanten-Körper. *Journ. reine angew. Math.* (Crelle) 172 (1935) 37–54.

[9] S. KOIZUMI: The fields of moduli for polarized abelian varieties and for curves. *Nagoya Math. J.* 48 (1972) 37–55.

[10] O.A. LAUDAL and K. LØNSTED: Deformations of curves I, moduli for hyperelliptic curves. In: *Algebraic Geometry*. Proceedings Tromso, Norway 1977. *Lecture Notes in Math.* Vol. 687, pp. 150–167. Berlin-Heidelberg-New York: Springer (1978).

[11] K. LØNSTED: The hyperelliptic locus with special reference to characteristic two. *Math. Ann.* 222 (1976) 55–61.

[12] K. LØNSTED and S.L. KLEIMAN: Basics on families of hyperelliptic curves. *Comp. Math.* 38 (1979) 83–111.

[13] H. MATSUMURA: *Commutative Algebra*. New York: W.A. Benjamin (1970).

[14] T. MATSUSAKA: Polarized varieties, fields of moduli, and generalized Kummer varieties of polarized abelian varieties. *Amer. J. Math.* 80 (1958) 45–82.

[15] T. MATSUSAKA: On a theorem of Torelli. *Amer. J. Math.* 80 (1958) 784–800.

[16] W. MESSING: The crystals associated to Barsotti-Tate groups; with applications to abelian schemes. *Lecture Notes in Math.* Vol. 264. Berlin-Heidelberg-New York: Springer (1972).

[17] D. MUMFORD: *Geometric Invariant Theory*. Ergebnisse. Berlin-Heidelberg-New York: Springer (1965).

[18] D. MUMFORD Abelian varieties. *Tata Inst. Studies in Math.* Oxford University Press (1970).

[19] M. NAGATA: Local rings. *Interscience Tracts in Pure & Applied Math.* 13. New York: J. Wiley (1962).

[20] F. OORT: Finite group schemes, local moduli for abelian varieties and lifting problems. In: *Algebraic Geometry*, Oslo (1970) pp. 223–254. Wolters-Noordhoff (1972). Also: *Comp. Math.* 23 (1972) 265–296.

[21] F. Oort: Singularities of coarse moduli schemes. *Sém. Dubreil* 29 (1975/1976). *Lecture Notes in Math*. Vol. 586, pp. 61–76. Berlin-Heidelberg-New York: Springer (1977).
[22] F. Oort and J. Steenbrink: The local Torelli problem for algebraic curves. *J. de Geometrie Algebrique Angers* (1979) A. Beauville editor, Sijthoff & Noordhoff (1980) pp. 157–203.
[23] F. Oort and K. Ueno: Principally polarized abelian varieties of dimension two or three are jacobian varieties. *J. Fac. Sci. Univ. Tokyo*, Section IA, Math. 20 (1973) 377–381.
[24] B.R. Peskin: Quotient-singularities in characteristic p. Thesis, M.I.T. (1980).
[25] H. Popp: The singularities of the moduli scheme of curves. *J. Number Theory* 1 (1969) 90–107.
[26] T. Sekiguchi: On the fields of rationality for curves and for abelian varieties. *Bull. Facult. Sci. & Eng. Chuo Univ.* 23 (1980) 35–41.
[27] T. Sekiguchi: The coincidence of fields of moduli for nonhyperelliptic curves and for their jacobian varieties. *Nagoya Math. J.* 82 (1981) 57–82.
[28] T. Sekiguchi: On the fields of rationality for curves and for their jacobian varieties. *Nagoya Math. J.* 88 (1982) 197–212.
[29] G. Shimura: On the field of rationality for an abelian variety. *Nagoya Math. J.* 45 (1972) 167–178.

(Oblatum 13-XII-1982 & 22-XII-1983)

Department of Mathematics
Faculty of Science and Engineering
Chuo University
Kasuga, Bunkyo-ku
Tokyo
Japan