Frobenius base change of torsors

Mitsui, Kentaro

(Citation)
Journal of Pure and Applied Algebra,223(2):553-570

(Issue Date)
2019-02

(Resource Type)
journal article

(Version)
Accepted Manuscript

(URL)
https://hdl.handle.net/20.500.14094/90005358

FROBENIUS BASE CHANGE OF TORSORS

KENTARO MITSUI

ABSTRACT. We study the Frobenius base change of a torsor under a smooth algebraic group over a field of positive characteristic by relating it to the pushforward of the torsor under the Frobenius homomorphism. As an application, we determine the change of the multiplicity of a closed fiber of an elliptic surface by purely inseparable base changes with respect to the base curve in the case where the generic fiber is supersingular.

1. INTRODUCTION

We study the Frobenius base change of a torsor X under a smooth algebraic group G over a field K of positive characteristic p (i.e., G is a quasi-projective smooth K-group scheme). In the first part (§§2–4), we study the relationship between the Frobenius base change of X and the pushforward of X under the Frobenius homomorphism $G \to G^{(p)}$. In the last part (§§5–6), we apply the result in the first part to the case where X is the generic fiber of an elliptic fibration in order to determine the change of the multiplicity of a closed fiber of an elliptic surface by purely inseparable base changes with respect to the base curve.

Let us give details on the first part. Choose an algebraic closure K^{alg} of K. Take $n \in \mathbb{Z}_{\geq 0}$. Put $q := p^n$, $K_n := K^{\frac{1}{q}} := \{b \in K^{\mathrm{alg}} \mid b^q \in K\}$, and $S := \operatorname{Spec} K$. We denote the n-th iterate of the Frobenius homomorphisms by $F_{G/S,n} \colon G \to G^{(q)}$ (Definition 2.26). We define a K_n-group scheme G_n and a K_n-torsor X_n under G_n as the base changes of G and X via K_n/K, respectively, and a K-torsor $X^{(q)}$ under $G^{(q)}$ as the pushforward of X under $F_{G/S,n}$ (Definition 3.12). Recall that the first Galois cohomology $H^1(K,G)$ of K with coefficients in G may be regarded as the set of isomorphism classes of K-torsors under G (Definition 3.3 and Remark 3.13). We denote the cohomology class corresponding to the isomorphism class of X by $[X]$. We first construct a bijection $\phi^1_{G/S,n}$ such that the diagram

$$(*) \qquad \begin{array}{ccccc} H^1(K,G) & \xrightarrow[F^1_{G/S,n,*}]{} & H^1(K,G^{(q)}) & \xrightarrow[\phi^1_{G/S,n}]{\cong} & H^1(K_n,G_n) \end{array} \qquad \overset{b^1_{G/S,n}}{\overbrace{\qquad\qquad\qquad\qquad}}$$

commutes, where $b^1_{G/S,n}([X]) = [X_n]$ and $F^1_{G/S,n,*}([X]) = [X^{(q)}]$ for any K-torsor X under G (Definition 3.9 and Proposition 3.14). In the case $n = 1$, Diagram $(*)$ relates the Frobenius base change of X to the pushforward of X under the Frobenius homomorphism $G \to G^{(p)}$.

Assume that G is commutative. Then Diagram $(*)$ is a diagram of Abelian groups and homomorphisms (Remark 3.10). We denote the order of $[X_n]$ in $H^1(K_n,G_n)$ by m_n. As an application of Diagram $(*)$, we show the following behavior of $(m_n)_{n\geq 0}$ at the end of §4.

2010 *Mathematics Subject Classification.* Primary 14G17; Secondary 11S25,14J27,14K05.

Theorem 1.1. *Assume that G is a superspecial K-Abelian variety, e.g., a supersingular K-elliptic curve* (*Definition* 4.1)*. Then the following statements hold. If $p \mid m_n$, then one of the following equalities holds*:

(1) $(m_{n+1}, m_{n+2}) = (m_n/p, m_{n+1})$;
(2) $(m_{n+1}, m_{n+2}) = (m_n, m_{n+1}/p)$.

Otherwise, the equality $m_{n+1} = m_n$ holds.

In the proof of the above theorem, we decompose the multiplication of G by p into the two Frobenius homomorphisms and an isomorphism (Proposition 4.3), and apply Diagram $(*)$ for $n = 2$.

In the last part, we prove Theorem 1.2 below. Let $\pi\colon \mathscr{X} \to C$ be a relatively minimal elliptic fibration (Definition 5.3). The *multiplicity* of a closed fiber of π is defined as the greatest common divisor of the multiplicities of the irreducible components of the fiber. If the multiplicity is greater than one, then the fiber is called a *multiple fiber*. We consider the case where K is the function field of C, X is the generic fiber of $\mathscr{X}$, and G is the Jacobian of X. Take the normalization $u_n\colon C_n \to C$ of C in K_n. Let x be a closed point on C. The preimage $u_n^{-1}(x)$ consists of a single closed point on C_n since K_n is purely inseparable over K. We denote this closed point by x_n, the fiber over x_n of the minimal regular C_n-model of X_n by $\mathscr{X}_{x,n}$, and the multiplicity of the fiber $\mathscr{X}_{x,n}$ by $m_{x,n}$.

Theorem 1.2. *Let k be an algebraically closed field of positive characteristic p. Suppose that C is isomorphic to one of the following schemes*: (a) *a smooth k-curve*; (b) *the spectrum of the one-parameter formal power series ring with coefficients in k. Assume that G is supersingular. Then the following statements hold. If $p \mid m_{x,n}$, then one of the following equalities holds*:

(1) $(m_{x,n+1}, m_{x,n+2}) = (m_{x,n}/p, m_{x,n+1})$;
(2) $(m_{x,n+1}, m_{x,n+2}) = (m_{x,n}, m_{x,n+1}/p)$.

Otherwise, the equality $m_{x,n+1} = m_{x,n}$ holds.

We prove the above theorem at the end of §5. In the proof, we reduce the global case (a) to the local case (b) by base change with respect to C. In the local case, it is known that $m_{x,n} = m_n$ for any $n \in \mathbb{Z}_{\geq 0}$ (Theorem 5.7 (1)). Thus, Theorem 1.1 implies Theorem 1.2.

On the other hand, we may determine the type ${}_{m_{x,n}}T_n$ (Kodaira's symbol) of the fiber $\mathscr{X}_{x,n}$ in the following way. We denote the fiber over x_n of the minimal regular C_n-model of G_n by $\mathscr{G}_{x,n}$. Then T_n is equal to the type of $\mathscr{G}_{x,n}$ (Theorem 5.7 (1)), which may be determined from G_n by Tate's algorithm [Tat75]. In conclusion, we may determine T_n by the previously known results (see also Remark 5.9) while Theorem 1.2 provides a method to determine $m_{x,n}$. We remark that it seems to be much more difficult to study the singularities on $\mathscr{X} \times_C C_n$ or its normalization explicitly although its minimal regular C_n-model $\mathscr{X}_n$ can be analyzed as above.

Let us explain Theorem 1.2 in the context of surface theory. We fix an algebraically closed base field of characteristic $p \geq 0$. In the studies on elliptic surfaces, it is important to study multiple fibers since they appear in the canonical bundle formula. Multiple fibers and the canonical bundle formula were studied by Kodaira in the complex analytic case ([Kod63a] and [Kod63b]), and by Bombieri and Mumford in the positive characteristic case [BM77]. In the complex analytic case, any multiple fiber of multiplicity m over a point x may be resolved by the normalization of the base change via a finite covering of the base curve each of whose ramification indices over x is equal to m [Kod63a, pp. 571–572]. Although the resolution of multiple fibers is a fundamental problem, few facts are known

in the case $p > 0$. We denote the type of a multiple fiber over a point x by ${}_mT$ (Kodaira's symbol), and summarize previously known results.

(1) The algebraic case with $p \nmid m$ is same as in the complex analytic case.
(2) The case $T = \mathrm{I}_n$ ($n > 0$) was settled in [LLR04, §8].

In (1) and (2), the multiple fiber is resolved by the normalization of the base change via a separable covering of the base curve, and the induced morphism between elliptic surfaces is étale over an open neighborhood of x. The remaining cases are difficult. In the following, we consider the case $p > 0$. For any type ${}_qT'$ with power q of p, there exists a closed fiber of type ${}_qT'$ (Example 6.5). The base changes via separable coverings and purely inseparable coverings were studied in (3) and (4), where the induced morphisms between elliptic surfaces are étale over an open neighborhood of x or purely inseparable.

(3) In [KU85, §§6–7], the multiple fiber is resolved by successive base changes whenever $T = \mathrm{I}_0$ and no multiple fiber of strange type appears during these procedures (see [KU85, p. 330, Note added in proof] for the definition of *strange type*; in [KU86, §2], the case $T \neq \mathrm{I}_n$ ($n \geq 0$) is reduced to the case $T = \mathrm{I}_n$ ($n \geq 0$) whenever $p \geq 5$).
(4) In [Kaw00, §3] and [Kaw06, §3], the multiple fiber is resolved by successive base changes whenever the given elliptic fibration $\mathscr{X} \to C$ satisfies the following conditions. The generic fiber is supersingular (Definition 5.3), and the equality $q(\mathscr{X}) = g(C) + 1$ holds, where $q(\mathscr{X})$ is the dimension of the Albanese variety of $\mathscr{X}$, and $g(C)$ is the genus of C.

Both (3) and (4) are based on the studies of the Frobenius action on $H^1(\mathscr{X}, \mathscr{O}_{\mathscr{X}})$, which, however, give restrictive results since this action depends on the global geometry of $\mathscr{X}$. On the other hand, our approach is local with respect to the base curve (Remark 5.6), which enables us to study multiple fibers in a systematic way (see, e.g., [Mit15] and [Mit16]). As a result, we obtain Theorem 1.2, which determines the change of the multiplicity by purely inseparable base changes without any additional assumption on p, fibers, or the global geometry of $\mathscr{X}$ (Remark 5.9).

Finally, we remark that the resolutions of (4) are incorrect. In §6, we give counterexamples to the main results in [Kaw00] and [Kaw06] by constructing an elliptic surface over the projective line with trivial second Chern number, supersingular generic fiber, and exactly one singular fiber, of type ${}_{p^n}\mathrm{I}_0$ for any $n \in \mathbb{Z}_{>1}$ (Example 6.9 and Remark 6.10). These elliptic surfaces are interesting in its own right since they give an answer to the question on the existence of such elliptic surfaces in [Tak94, p. 314], [Tak96], and [Kaw06, §1]. Our studies correct these errors, and give a new resolution of multiple fibers by purely inseparable base changes.

2. Frobenius Morphisms

Let K be a field of positive characteristic p. Choose an algebraic closure K^{alg} of K. Take the separable closure $\overline{K}$ of K in K^{alg}. We denote the Galois group of $\overline{K}/K$ equipped with the Krull topology by $\mathfrak{g}_K$. Put $S := \operatorname{Spec} K$ and $\overline{S} := \operatorname{Spec} \overline{K}$.

Definition 2.1. A $\mathfrak{g}_K$-set is a discrete set with continuous left action of $\mathfrak{g}_K$. A $\mathfrak{g}_K$-map is a map between $\mathfrak{g}_K$-sets that is $\mathfrak{g}_K$-equivariant with respect to the equipped actions of $\mathfrak{g}_K$. For a K-scheme Z, we define a $\mathfrak{g}_K$-set $Z(\overline{K})$ as the set of $\overline{K}$-valued points of Z equipped with the action of $\mathfrak{g}_K$ induced by that on $\overline{K}$. For a K-morphism $j\colon Z_1 \to Z_2$ between K-schemes, we define a map

$$j_*\colon Z_1(\overline{K}) \longrightarrow Z_2(\overline{K})$$

by putting $j_*(s) := j \circ s$ for each $(s\colon \overline{S} \to Z_1) \in Z_1(\overline{K})$.

Remark 2.2. The map j_* is a $\mathfrak{g}_K$-map.

Let L be a field extension of K in K^{alg}. Take the separable closure $\overline{L}$ of L in K^{alg}. We denote the Galois group of $\overline{L}/L$ by $\mathfrak{g}_L$. Put $T := \mathrm{Spec}\, L$ and $\overline{T} := \mathrm{Spec}\, \overline{L}$. The field extensions $\overline{L}/L/K$ and $\overline{L}/\overline{K}/K$ induce a diagram with commutative square:

$$\begin{array}{ccc} \overline{T} & \xrightarrow{\overline{u}} & \overline{S} \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \sigma} \\ T & \xrightarrow{u} & S. \end{array}$$

Definition 2.3. Let M be a field extension of K in K^{alg}. Take $n \in \mathbb{Z}_{\geq 0}$. Put $q := p^n$.

(1) Put $M^{\frac{1}{q}} := \{b \in K^{\mathrm{alg}} \mid b^q \in M\}$.
(2) We define a map $l_M^{(q)} : M^{\frac{1}{q}} \to M$ by putting $l_M^{(q)}(b) := b^q$ for each $b \in M^{\frac{1}{q}}$.
(3) For $a \in M$, we denote the unique q-th root of a in $M^{\frac{1}{q}}$ by $a^{\frac{1}{q}}$ (Remark 2.4).
(4) For $\alpha(z) = \sum_{i=0}^N a_i z^i \in M[z]$, we put $\alpha^{(\frac{1}{q})}(z) := \sum_{i=0}^N a_i^{\frac{1}{q}} z^i \in M^{\frac{1}{q}}[z]$.
(5) For $\beta(z) = \sum_{i=0}^N b_i z^i \in M^{\frac{1}{q}}[z]$, we put $\beta^{(q)}(z) := \sum_{i=0}^N b_i^q z^i \in M[z]$.

Remark 2.4. The subset $M^{\frac{1}{q}}$ of K^{alg} is a subfield, and the map $l_M^{(q)}$ is an isomorphism of fields.

Remark 2.5. The equalities $\alpha^{(\frac{1}{q})}(z)^q = \alpha(z^q)$ and $\beta^{(q)}(z^q) = \beta(z)^q$ hold. For the image i of any rational integer in K, the equalities $i^q = i$ and $i^{\frac{1}{q}} = i$ hold. Thus, the equalities

$$\frac{d\alpha^{(\frac{1}{q})}}{dz}(z)^q = \left(\sum_{i=1}^N i a_i^{\frac{1}{q}} z^{i-1}\right)^q = \sum_{i=1}^N i a_i z^{(i-1)q} = \frac{d\alpha}{dz}(z^q)$$

and

$$\frac{d\beta^{(q)}}{dz}(z^q) = \sum_{i=1}^N i b_i^q z^{(i-1)q} = \left(\sum_{i=1}^N i b_i z^{i-1}\right)^q = \frac{d\beta}{dz}(z)^q$$

hold.

Definition 2.6. We define homomorphisms

$$r_K\colon \mathrm{Aut}(K^{\mathrm{alg}}/K) \longrightarrow \mathfrak{g}_K$$

and

$$r_L\colon \mathrm{Aut}(K^{\mathrm{alg}}/L) \longrightarrow \mathfrak{g}_L$$

by the restrictions of the actions to $\overline{K}$ and $\overline{L}$, respectively.

Lemma 2.7. *Both r_K and r_L are bijective.*

Proof. We have only to show the statement for r_L. Let us give the inverse of r_L. Take $g \in \mathfrak{g}_L$. Choose $a \in K^{\mathrm{alg}}$. Since the field extension $K^{\mathrm{alg}}/\overline{L}$ is purely inseparable, we may take a power q of p so that $a^q \in \overline{L}$. Put $a' := g(a^q)^{\frac{1}{q}}$ (Definition 2.3 (3)). Then a' does not depend on the choice of q. The map associating a with a' gives $g' \in \mathrm{Aut}(K^{\mathrm{alg}}/L)$. We define a map $r'_L\colon \mathfrak{g}_L \to \mathrm{Aut}(K^{\mathrm{alg}}/L)$ by putting $r'_L(g) := g'$ for each $g \in \mathfrak{g}_L$. Then r'_L is the inverse of r_L, which concludes the proof. □

Definition 2.8. We define a homomorphism $i_{L/K}\colon \mathrm{Aut}(K^{\mathrm{alg}}/L) \to \mathrm{Aut}(K^{\mathrm{alg}}/K)$ as the canonical inclusion. We define a continuous homomorphism $r_{L/K}\colon \mathfrak{g}_L \to \mathfrak{g}_K$ by putting $r_{L/K} := r_K \circ i_{L/K} \circ r_L^{-1}$ (Lemma 2.7).

Remark 2.9. We may regard a $\mathfrak{g}_K$-set as a $\mathfrak{g}_L$-set by $r_{L/K}$. The groups $\mathfrak{g}_K$ and $\mathfrak{g}_L$ act on $\overline{S}$ and $\overline{T}$, respectively. The group $\mathfrak{g}_L$ acts on $\overline{S}$ via $r_{L/K}$. Then $\overline{u}$ is $\mathfrak{g}_L$-equivariant.

Lemma 2.10. *Assume that the field extension L/K is purely inseparable. Then both $i_{L/K}$ and $r_{L/K}$ are bijective.*

Proof. We have only to show that $i_{L/K}$ is surjective (Lemma 2.7). Take $g \in \mathrm{Aut}(K^{\mathrm{alg}}/K)$. Choose $a \in L$. By assumption, we may take a power q of p so that $a^q \in K$. Since $g(a)^q = g(a^q) = a^q$, the equality $g(a) = a$ holds (Remark 2.4), which implies that $g \in \mathrm{Im}\, i_{L/K}$. Thus, the homomorphism $i_{L/K}$ is surjective, which concludes the proof. □

Lemma 2.11. *Assume that $L = K^{\frac{1}{p}}$. Then $\overline{L} = \overline{K}^{\frac{1}{p}}$.*

Proof. First, we show that $\overline{L} \subset \overline{K}^{\frac{1}{p}}$. Choose $a \in \overline{L}$. Take $\beta(z) \in L[z]$ so that $\beta(a) = 0$ and $\frac{d\beta}{dz}(a) \neq 0$. Then $\beta^{(p)}(a^p) = 0$ and $\frac{d\beta^{(p)}}{dz}(a^p) \neq 0$ (Remark 2.5), which implies that $a^p \in \overline{K}$. Thus, we conclude that $\overline{L} \subset \overline{K}^{\frac{1}{p}}$. Next, we show that $\overline{L} \supset \overline{K}^{\frac{1}{p}}$. Choose $a \in \overline{K}^{\frac{1}{p}}$. Since $a^p \in \overline{K}$, we may take $\alpha(z) \in K[z]$ so that $\alpha(a^p) = 0$ and $\frac{d\alpha}{dz}(a^p) \neq 0$. Then $\alpha^{(\frac{1}{p})}(a) = 0$ and $\frac{d\alpha^{(\frac{1}{p})}}{dz}(a) \neq 0$ (Remark 2.5), which implies that $a \in \overline{L}$. Thus, we conclude that $\overline{L} \supset \overline{K}^{\frac{1}{p}}$. Therefore, the equality $\overline{L} = \overline{K}^{\frac{1}{p}}$ holds. □

Let Y be a K-scheme with structure morphism $f\colon Y \to S$. Take the base change $u_Y\colon Y_T \to Y$ of u via f and the base change $f_T\colon Y_T \to T$ of f via u:

$$\begin{array}{ccc} Y_T & \xrightarrow{u_Y} & Y \\ \downarrow{\scriptstyle f_T} & & \downarrow{\scriptstyle f} \\ T & \xrightarrow{u} & S. \end{array}$$

Take the $\mathfrak{g}_K$-set $Y(\overline{K})$ and the $\mathfrak{g}_L$-set $Y_T(\overline{L})$ (Definition 2.1). We regard $Y(\overline{K})$ as a $\mathfrak{g}_L$-set by $r_{L/K}$ (Remark 2.9).

Definition 2.12. We define a map

$$b_{Y,L/K}\colon Y(\overline{K}) \longrightarrow Y_T(\overline{L})$$

in the following way. Take $(s\colon \overline{S} \to Y) \in Y(\overline{K})$. Then $f \circ s \circ \overline{u} = \sigma \circ \overline{u} = u \circ \tau$. Thus, since $Y_T = Y \times_S T$, there exists a unique $(t\colon \overline{T} \to Y_T) \in Y_T(\overline{L})$ such that $u_Y \circ t = s \circ \overline{u}$. Put $b_{Y,L/K}(s) := t$.

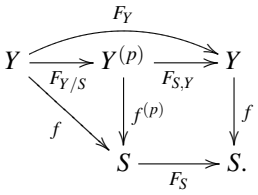
Remark 2.13. The map $b_{Y,L/K}$ is a $\mathfrak{g}_L$-map since $\overline{u}$ is $\mathfrak{g}_L$-equivariant (Remark 2.9).

Definition 2.14. For a K-algebra R, we define the *Frobenius endomorphism* $\phi_R\colon R \to R$ *of* R by putting $\phi_R(a) := a^p$ for each $a \in R$. For an affine open subscheme $U \cong \mathrm{Spec}\, R$ of Y, the endomorphism ϕ_R induces an endomorphism of U. Patching such endomorphisms, we define the *absolute Frobenius morphism* $F_Y\colon Y \to Y$ *of* Y (Remark 2.15). Take the base change $f^{(p)}\colon Y^{(p)} \to S$ of f via F_S and the base change $F_{S,Y}\colon Y^{(p)} \to Y$ of F_S via f. We equip $Y^{(p)}$ with the K-scheme structure by $f^{(p)}$. Then there exists a unique K-morphism

$F_{Y/S}\colon Y \to Y^{(p)}$ such that $F_{S,Y} \circ F_{Y/S} = F_Y$ (Remark 2.16). The K-morphism $F_{Y/S}$ is called the *relative Frobenius morphism of* Y. The relative Frobenius morphism $F_{G/S}$ of a K-group scheme G is called the *Frobenius homomorphism of* G (Remark 2.17).

Remark 2.15. For any K-algebra homomorphism $\psi\colon R_1 \to R_2$ between K-algebras, the equality $\psi \circ \phi_{R_1} = \phi_{R_2} \circ \psi$ holds. For any K-morphism $j\colon Z_1 \to Z_2$ between K-schemes, the equality $j \circ F_{Z_1} = F_{Z_2} \circ j$ holds.

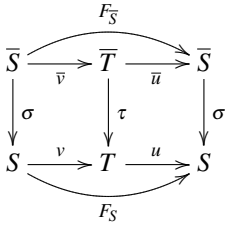
Remark 2.16. The square is Cartesian, and any circle is commutative in the following diagram:



Remark 2.17. Let G be a K-group scheme. We equip $G^{(p)}$ with the K-group scheme structure induced by the base change of G via F_S. Then $F_{G/S}$ is a K-homomorphism.

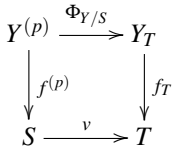
Definition 2.18. Assume that $L = K^{\frac{1}{p}}$. Then $\overline{L} = \overline{K}^{\frac{1}{p}}$ (Lemma 2.11). The isomorphisms $l_K^{(p)}$ and $l_{\overline{K}}^{(p)}$ induce isomorphisms $v\colon S \to T$ and $\overline{v}\colon \overline{S} \to \overline{T}$, respectively (Definition 2.3 (2) and Remark 2.4).

Remark 2.19. Any circle in the diagram



is commutative. The isomorphism $\overline{v}$ is $\mathfrak{g}_L$-equivariant since $l_{\overline{K}}^{(p)}$ is $\mathfrak{g}_L$-equivariant.

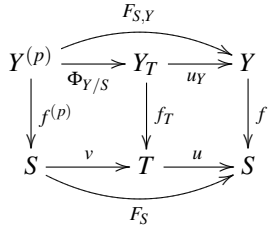
Lemma 2.20. *Assume that* $L = K^{\frac{1}{p}}$. *Then there exists a unique morphism* $\Phi_{Y/S}\colon Y^{(p)} \to Y_T$ *such that* $u_Y \circ \Phi_{Y/S} = F_{S,Y}$ *and* $f_T \circ \Phi_{Y/S} = v \circ f^{(p)}$. *Moreover, the square in the diagram*



is Cartesian, and the morphism $\Phi_{Y/S}$ *is an isomorphism.*

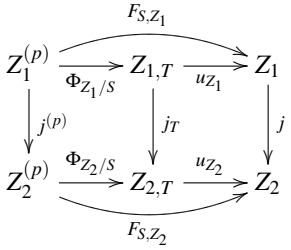
Proof. Since $Y_T = Y \times_S T$, the first statement follows from the equalities $f \circ F_{S,Y} = F_S \circ f^{(p)} = u \circ v \circ f^{(p)}$ (Remark 2.19). Let us show the other statements. Any circle in the

diagram



is commutative. Since the 1×2 rectangle and the right square are Cartesian, the left square is Cartesian. Since v is an isomorphism, the morphism $\Phi_{Y/S}$ is an isomorphism. □

Remark 2.21. The equalities $F_Y = F_{S,Y} \circ F_{Y/S} = u_Y \circ \Phi_{Y/S} \circ F_{Y/S}$ hold. Let $j\colon Z_1 \to Z_2$ be a K-morphism between K-schemes. Then any square in the diagram



is Cartesian, where $j^{(p)}$ and j_T are the base changes of j via F_S and u, respectively.

Definition 2.22. Assume that $L = K^{\frac{1}{p}}$.

(1) Put $b_{Y/S} := b_{Y,L/K}$ (Definition 2.12).
(2) We define a bijection

$$\phi_{Y/S}\colon Y^{(p)}(\overline{K}) \longrightarrow Y_T(\overline{L})$$

by putting $\phi_{Y/S}(r) := \Phi_{Y/S} \circ r \circ (\overline{v})^{-1}$ for each $(r\colon \overline{S} \to Y^{(p)}) \in Y^{(p)}(\overline{K})$ (Definition 2.18 and Lemma 2.20).
(3) We define a map

$$c_{Y/S}\colon Y(\overline{K}) \longrightarrow Y_T(\overline{L})$$

by putting $c_{Y/S} := \phi_{Y/S} \circ F_{Y/S,*}$ (Definition 2.1).

Remark 2.23. For any $s \in Y(\overline{K})$, the equality $c_{Y/S}(s) = \Phi_{Y/S} \circ F_{Y/S} \circ s \circ (\overline{v})^{-1}$ holds. The maps $\phi_{Y/S}$ and $c_{Y/S}$ are $\mathfrak{g}_L$-maps since $F_{Y/S,*}$ and $\overline{v}$ are $\mathfrak{g}_L$-equivariant (Remarks 2.2 and 2.19).

Remark 2.24. We use the notation introduced in Remark 2.21. Then the diagram

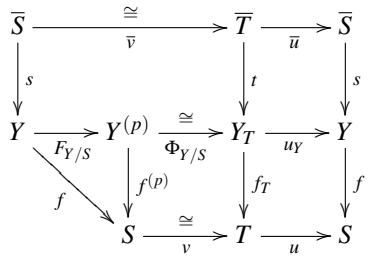
$$\begin{array}{ccc} Z_1^{(p)}(\overline{K}) & \xrightarrow[\phi_{Z_1/S}]{\cong} & Z_{1,T}(\overline{L}) \\ \downarrow{\scriptstyle j_*^{(p)}} & & \downarrow{\scriptstyle j_{T,*}} \\ Z_2^{(p)}(\overline{K}) & \xrightarrow[\phi_{Z_2/S}]{\cong} & Z_{2,T}(\overline{L}) \end{array}$$

commutes (Definition 2.1).

The following lemma plays a key role in the present paper.

Lemma 2.25. *Assume that $L = K^{\frac{1}{p}}$. Then $b_{Y/S} = c_{Y/S}$.*

Proof. Take $s \in Y(\overline{K})$. Put $t := b_{Y/S}(s) \in Y_T(\overline{L})$. Let us show that the upper left rectangle in the diagram



is commutative. Note that any of the squares and triangle is commutative. Since the lower right square is Cartesian, the commutativity of the rectangle follows from the equalities

$$u_Y \circ \Phi_{Y/S} \circ F_{Y/S} \circ s = F_Y \circ s = s \circ F_{\overline{S}} = s \circ \overline{u} \circ \overline{v} = u_Y \circ t \circ \overline{v}$$

(see Remarks 2.21, 2.15, and 2.19 for the first three equalities, respectively) and

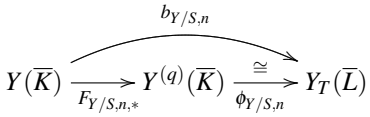
$$f_T \circ \Phi_{Y/S} \circ F_{Y/S} \circ s = v \circ f \circ s = v \circ \sigma = \tau \circ \overline{v} = f_T \circ t \circ \overline{v}$$

(see Remark 2.19 for the third equality). Thus, the equalities

$$b_{Y/S}(s) = t = \Phi_{Y/S} \circ F_{Y/S} \circ s \circ (\overline{v})^{-1} = c_{Y/S}(s)$$

hold (see Remark 2.23 for the last equality), which concludes the proof. □

Definition 2.26. Take $n \in \mathbb{Z}_{\geq 0}$. Put $q := p^n$. Assume that $L = K^{\frac{1}{q}}$. We define a K-morphism $F_{Y/S,n} \colon Y \to Y^{(q)}$, and maps $\phi_{Y/S,n} \colon Y^{(q)}(\overline{K}) \to Y_T(\overline{L})$ and $b_{Y/S,n} \colon Y(\overline{K}) \to Y_T(\overline{L})$ in the following way. We define $F_{Y/S,0}$ as the identity of Y, and $\phi_{Y/S,0}$ and $b_{Y/S,0}$ as the identity of $Y(\overline{K})$. For each $n \in \mathbb{Z}_{>0}$, we inductively put $F_{Y/S,n} := F_{Y^{(p)}/S,n-1} \circ F_{Y/S}$, $\phi_{Y/S,n} := \phi_{Y_U/U,n-1} \circ \phi_{Y^{(r)}/S}$, and $b_{Y/S,n} := b_{Y_U/U,n-1} \circ b_{Y/S}$, where $r := q/p$, $U := \operatorname{Spec} K^{\frac{1}{p}}$, and $Y_U := Y \times_S U$. Finally, we obtain a diagram of $\mathfrak{g}_L$-sets and $\mathfrak{g}_L$-maps

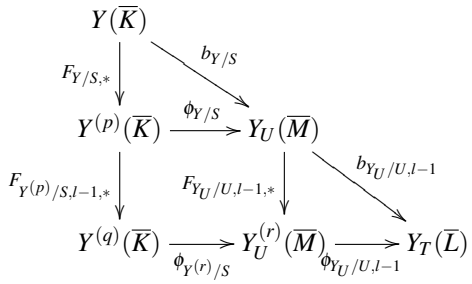


(Remarks 2.2, 2.13, and 2.23).

Lemma 2.27. *The diagram in Definition* 2.26 *commutes.*

Proof. Let us show the statement by the induction on n. The case $n = 0$ is clear. The case $n = 1$ follows from Lemma 2.25. Take $l \in \mathbb{Z}_{>1}$. Assume that the case $n = l - 1$ holds. Let us show the case $n = l$. Put $r := q/p$, $M := K^{\frac{1}{p}}$, $U := \operatorname{Spec} M$, and $Y_U := Y \times_S U$. Take the separable closure $\overline{M}$ of M in K^{alg}. Remark 2.24 and the cases $n = 1$ and $n = l - 1$ imply

that any circle in the diagram



is commutative, which proves the case $n = l$. □

3. Galois Cohomology

We use the notation $K \subset \overline{K} \subset K^{\mathrm{alg}}$, p, and $\mathfrak{g}_K$ introduced in §2. We refer to [Ser02, I.5] for Galois cohomology.

Definition 3.1. A $\mathfrak{g}_K$-*group* is a discrete group $\mathfrak{G}$ with continuous left action of $\mathfrak{g}_K$ satisfying that $g(st) = g(s)g(t)$ for any $g \in \mathfrak{g}_K$, any $s \in \mathfrak{G}$, and any $t \in \mathfrak{G}$. A $\mathfrak{g}_K$-*homomorphism* is a homomorphism between $\mathfrak{g}_K$-groups that is a $\mathfrak{g}_K$-map (Definition 2.1). We denote the first Galois cohomology of K with coefficients in a $\mathfrak{g}_K$-group $\mathfrak{G}$ by $H^1(K,\mathfrak{G})$ [Ser02, I.5.1]. If $\mathfrak{G}$ is commutative, then we denote the order of $\eta \in H^1(K,\mathfrak{G})$ by $\operatorname{ord}\eta$ (Remark 3.2). For a field extension L of K in K^{alg}, we denote the map induced by a $\mathfrak{g}_L$-homomorphism $\lambda\colon \mathfrak{G} \to \mathfrak{H}$ from a $\mathfrak{g}_K$-group (Remark 2.9) to a $\mathfrak{g}_L$-group by

$$\lambda^1\colon H^1(K,\mathfrak{G}) \longrightarrow H^1(L,\mathfrak{H}).$$

Remark 3.2. The group structure of an Abelian $\mathfrak{g}_K$-group $\mathfrak{G}$ induces that of $H^1(K,\mathfrak{G})$, and $H^1(K,\mathfrak{G})$ is commutative [Ser02, I.2.2]. For a field extension L of K in K^{alg}, the map λ^1 induced by a $\mathfrak{g}_L$-homomorphism λ from an Abelian $\mathfrak{g}_K$-group to an Abelian $\mathfrak{g}_L$-group is a homomorphism between Abelian groups [Ser02, I.2.4].

Let G be a smooth K-algebraic group.

Definition 3.3. The *first Galois cohomology* $H^1(K,G)$ *of* K *with coefficients in* G is defined as $H^1(K,G(\overline{K}))$ (Definition 3.1 and Remark 3.4).

Remark 3.4. We equip the $\mathfrak{g}_K$-set $G(\overline{K})$ (Definition 2.1) with the group structure induced by the K-group scheme structure of G. Then $G(\overline{K})$ is a $\mathfrak{g}_K$-group.

Definition 3.5. Take $r \in \mathbb{Z}$. By $r_G\colon G \to G$ we denote the multiplication of G by r.

We use the notation $L \subset \overline{L}$, $\mathfrak{g}_L$, and $u\colon T \to S$ introduced in §2. We define a T-group scheme G_T as the base change of G via u.

Definition 3.6. The $\mathfrak{g}_L$-homomorphism $b_{G,L/K}$ induces a map

$$b^1_{G,L/K}\colon H^1(K,G) \longrightarrow H^1(L,G_T)$$

(Definition 2.12, Remark 2.13, and Definition 3.1).

Remark 3.7. If G is commutative, then $b^1_{G,L/K}$ is a homomorphism between Abelian groups (Remark 3.2).

Proposition 3.8. *Assume that G is commutative. Suppose that L is a finite separable field extension of K of degree d. Take $\eta \in H^1(K,G)$. Put $m := \operatorname{ord} \eta$ and $m' := \operatorname{ord} b^1_{G,L/K}(\eta)$. Assume that m is prime to d. Then $m = m'$.*

Proof. By assumption, the equality $\overline{L} = \overline{K}$ holds, which implies that $r_{L/K} \colon \mathfrak{g}_L \to \mathfrak{g}_K$ (Definition 2.8) is equal to the canonical inclusion, and that $b_{G,L/K} \colon G(\overline{K}) \to G_T(\overline{L})$ (Definition 2.12) is bijective. We denote the restriction homomorphism and corestriction homomorphism by

$$\operatorname{Res}_{L/K} \colon H^1(K,G) \longrightarrow H^1(L,G_T)$$

and

$$\operatorname{Cor}_{L/K} \colon H^1(L,G_T) \longrightarrow H^1(K,G),$$

respectively [Ser02, I.2.4]. Then the equality $b^1_{G,L/K} = \operatorname{Res}_{L/K}$ holds. Therefore, since m is prime to d, and $\operatorname{Cor}_{L/K} \circ \operatorname{Res}_{L/K}$ is equal to the multiplication of $H^1(K,G)$ by d [Ser02, I.2.4], the equality $\operatorname{ord} \operatorname{Cor}_{L/K}(b^1_{G,L/K}(\eta)) = m$ holds, which implies that $m = m'$. □

Definition 3.9. The diagram in Definition 2.26 induces a diagram

$$H^1(K,G) \xrightarrow[F^1_{G/S,n,*}]{} H^1(K,G^{(q)}) \xrightarrow[\phi^1_{G/S,n}]{\cong} H^1(L,G_T), \qquad H^1(K,G) \xrightarrow{b^1_{G/S,n}} H^1(L,G_T)$$

(Definition 3.1 and Lemma 2.10).

Remark 3.10. The above diagram commutes (Lemma 2.27). Assume that G is commutative. Then any of $F^1_{G/S,n,*}$, $\phi^1_{G/S,n}$, and $b^1_{G/S,n}$ is a homomorphism between Abelian groups (Remark 3.2). Since $\phi^1_{G/S,n}$ is an isomorphism, the equality $\operatorname{ord} F^1_{G/S,n,*}(\eta) = \operatorname{ord} b^1_{G/S,n}(\eta)$ holds for any $\eta \in H^1(K,G)$.

Proposition 3.11. *Assume that G is commutative. Take $\eta \in H^1(K,G)$, $n \in \mathbb{Z}_{\geq 0}$, and $r \in \mathbb{Z}$. Put $q := p^n$, $m := \operatorname{ord} \eta$, and $m' := \operatorname{ord} b^1_{G/S,n}(\eta)$. Suppose that there exists a K-isomorphism $\chi \colon G^{(q)} \cong G$ of K-group schemes such that $\chi \circ F_{G/S,n} = r_G$ (Definition 3.5). Then $m' = m/gcd(m,r)$.*

Proof. Since $F_{G/S,n}$, χ, and r_G induce a diagram of Abelian groups and homomorphisms with commutative circle

$$H^1(K,G) \xrightarrow[F^1_{G/S,n,*}]{} H^1(K,G^{(q)}) \xrightarrow[\chi^1_*]{\cong} H^1(K,G), \qquad H^1(K,G) \xrightarrow{r^1_{G,*}} H^1(K,G),$$

the proposition follows from Remark 3.10. □

Let X be a K-torsor under G with right K-action ρ of G [BLR90, 6.4].

Definition 3.12. We denote the cohomology class corresponding to the isomorphism class of X by $[X] \in H^1(K,G)$ (Remark 3.13). Let $j \colon G \to H$ be a K-homomorphism between smooth K-algebraic groups. We define the *pushforward of X under j* as a K-torsor under H whose cohomology class in $H^1(K,H)$ is equal to $j^1_*([X])$ (Remark 2.2 and Definition 3.1).

Remark 3.13. The set $H^1(K,G)$ may be regarded as the set of isomorphism classes of K-torsors under G [Mil80, III.4.8].

Take the base change $\rho_T\colon G_T \times_T X_T \to X_T$ of $\rho\colon G \times_S X \to X$ via u:

$$\begin{array}{ccccc} G_T \times_T X_T & \xrightarrow{\rho_T} & X_T & \longrightarrow & T \\ \downarrow & & \downarrow & & \downarrow u \\ G \times_S X & \xrightarrow{\rho} & X & \longrightarrow & S. \end{array}$$

Then X_T is an L-torsor under G_T with right L-action ρ_T of G_T. We denote the cohomology classes corresponding to the isomorphism classes of X and X_T by $[X] \in H^1(K,G)$ and $[X_T] \in H^1(L,G_T)$, respectively (Definition 3.12).

Proposition 3.14. *The equality $b^1_{G,L/K}([X]) = [X_T]$ holds.*

Proof. The right actions ρ and ρ_T induce right actions ρ_* and $\rho_{T,*}$ of $G(\overline{K})$ and $G_T(\overline{L})$ on $X(\overline{K})$ and $X_T(\overline{L})$, respectively. Then the above diagram induces a diagram of $\mathfrak{g}_L$-sets and $\mathfrak{g}_L$-maps with commutative square

$$\begin{array}{ccc} G(\overline{K}) \times X(\overline{K}) & \xrightarrow{\rho_*} & X(\overline{K}) \\ {\scriptstyle b_{G,L/K} \times b_{X,L/K}}\downarrow & & \downarrow{\scriptstyle b_{X,L/K}} \\ G_T(\overline{L}) \times X_T(\overline{L}) & \xrightarrow{\rho_{T,*}} & X_T(\overline{L}) \end{array}$$

(Remarks 2.2 and 2.13). Let us give a cocycle that represents $[X]$ [Ser02, I.5.2, p. 47]. Choose $s \in X(\overline{K})$. Since X is a K-torsor under G, there exists a unique $s_g \in G(\overline{K})$ such that $g(s) = ss_g$ for any $g \in \mathfrak{g}_K$. Then the cochain $(s_g)_{g\in\mathfrak{g}_K}$ is a cocycle that represents $[X]$. Put $t := b_{X,L/K}(s) \in X_T(\overline{L})$. For each $h \in \mathfrak{g}_L$, we put $t_h := b_{G,L/K}(s_{r_{L/K}(h)}) \in G_T(\overline{L})$ (Definition 2.8). Since the above diagram commutes, the equality $h(t) = tt_h$ holds for any $h \in \mathfrak{g}_L$. Thus, the cochain $(t_h)_{h\in\mathfrak{g}_L}$ is a cocycle that represents $[X_T]$, which implies that $b^1_{G,L/K}([X]) = [X_T]$. □

4. Torsors under Superspecial Abelian Varieties

We use the notation $K \subset K^{\mathrm{alg}}$, p, and S introduced in §2.

Definition 4.1. A K-elliptic curve E is said to be *supersingular* if $E(K^{\mathrm{alg}})$ is p-torsion free. A K-Abelian variety A is said to be *superspecial* if there exist a finite product B of supersingular K^{alg}-elliptic curves and a K^{alg}-isomorphism $A \times_S \operatorname{Spec} K^{\mathrm{alg}} \cong B$ of K^{alg}-group schemes.

Remark 4.2. The above definition does not depend on the choice of K^{alg}.

Proposition 4.3. *Let A be a superspecial K-Abelian variety. Then there exists a K-isomorphism $\chi\colon A^{(p^2)} \to A$ of K-group schemes such that $\chi \circ F_{A/S,2} = p_A$ (Definition 3.5).*

Proof. Take the kernel $i\colon \operatorname{Ker} F_{A/S,2} \to A$ of $F_{A/S,2}$. Put $j := p_A \circ i$. Since $F_{A/S,2}$ and p_A are K-isogenies of same degree, we have only to show that $j = 0$. Since the formation of j commutes with any base change [Gro77, XV.1.2, Proposition 1], we may assume that $K = K^{\mathrm{alg}}$. Since A is superspecial, we may assume that A is a supersingular K-elliptic curve. Then p_A is purely inseparable of degree p^2. Thus, the proposition follows from [Sil09, II.2.12]. □

Corollary 4.4. *Let A be a superspecial K-Abelian variety. Take $\eta \in H^1(K,A)$ and $n \in \mathbb{Z}_{\geq 0}$. Put $m := \operatorname{ord} \eta$ and $m' := \operatorname{ord} b^1_{A/S,2n}(\eta)$. Then $m' = m/gcd(m,p^n)$.*

Proof. The corollary follows from Propositions 3.11 and 4.3. □

Proof of Theorem 1.1. Corollary 4.4 gives the equality $m_{n+2} = m_n/\gcd(m_n,p)$, which concludes the proof. □

5. Multiple Fibers of Elliptic Surfaces

Definition 5.1. For a field k, a *k-curve* is a separated integral k-scheme of finite type of dimension one. Let C be an excellent regular integral scheme of dimension one, and x be a closed point on C. We denote the completion of $\mathscr{O}_{C,x}$ with respect to the maximal ideal by $\widehat{\mathscr{O}}_{C,x}$, and the field of fractions of $\widehat{\mathscr{O}}_{C,x}$ by K_x. A uniformizer of $\widehat{\mathscr{O}}_{C,x}$ is called a *local parameter of C at x*.

Remark 5.2. We use the notation $K \subset K_n \subset K^{\mathrm{alg}}$, p, and C introduced in §1. Suppose that C satisfies the condition in Theorem 1.2. Then C is an excellent regular integral scheme of dimension one, and K_n is equal to the unique purely inseparable field extension of K in K^{alg} of degree p^n for any $n \in \mathbb{Z}_{\geq 0}$.

We refer to [Liu02, §§8–9] for fibered surfaces.

Definition 5.3. A morphism $\pi\colon \mathscr{X} \to C$ between schemes is called an *elliptic fibration* if the following conditions are satisfied:

(1) $\mathscr{X}$ and C are excellent regular integral schemes of dimension two and one, respectively;
(2) π is proper;
(3) the homomorphism $\mathscr{O}_C \to \pi_*\mathscr{O}_{\mathscr{X}}$ associated with π is an isomorphism;
(4) the generic fiber of π is a proper smooth curve of genus one.

An elliptic fibration $\pi\colon \mathscr{X} \to C$ is said to be *relatively minimal* if any closed fiber of π does not contain a (-1)-curve [Liu02, 9.3.1 and 9.3.12]. The generic fiber of π is said to be *supersingular* if its Jacobian is supersingular (Definition 4.1).

Definition 5.4. Let C be an excellent regular integral scheme of dimension one with function field K, and X be a proper smooth geometrically integral K-curve of genus one. A *(minimal) regular C-model of X* is a (relatively minimal) elliptic fibration $\pi\colon \mathscr{X} \to C$ with K-isomorphism between X and the generic fiber of π (Remark 5.5). The *Jacobian fibration of an elliptic fibration* $\pi\colon \mathscr{X} \to C$ is the minimal regular C-model of the Jacobian of the generic fiber of π.

Remark 5.5. Since X is of genus one, a regular C-model of X is relatively minimal if and only if it is minimal [Liu02, 9.3.14 and 9.3.24]. There exists a unique minimal regular C-model of X up to unique C-isomorphism [Mit16, 3.2.5].

Remark 5.6. Let x be a closed point on C, and $\pi\colon \mathscr{X} \to C$ be a relatively minimal elliptic fibration. Put $C_x := \operatorname{Spec} \widehat{\mathscr{O}}_{C,x}$ (Definition 5.1). Then the base change $\pi_x\colon \mathscr{X}_x \to C_x$ of π via the canonical morphism $C_x \to C$ is a relatively minimal elliptic fibration [Liu02, 9.3.28 and 9.3.30]. The closed fiber of π_x is x-isomorphic to the fiber of π over x.

Theorem 5.7 ([LLR04, 6.6, 6.7, and 7.4])**.** *Let C be the spectrum of a complete discrete valuation ring with algebraically closed residue field of characteristic $p \geq 0$ and field of fractions K. Let E be a K-elliptic curve. Take the minimal regular C-model $\theta\colon \mathscr{E} \to C$ of*

E. We denote the type of the closed fiber of θ by T (Kodaira's symbol). Then the following statements hold.

(1) *Let $\pi\colon \mathscr{X} \to C$ be a relatively minimal elliptic fibration with generic fiber X whose Jacobian fibration is given by θ. Put $m := \operatorname{ord}[X]$ (Definition 3.12). Then the closed fiber of π is of type ${}_mT$.*
(2) *Take $m \in \mathbb{Z}_{>0}$. If $T = \mathrm{I}_n$ ($n \geq 0$), then there exists an element of $H^1(K,E)$ of order m. Otherwise, there exists an element of $H^1(K,E)$ of order m if and only if m is a power of p.*

Proof of Theorem 1.2. By Remarks 5.2 and 5.6, we have only to show the local case (b). Thus, the theorem follows from Theorems 1.1 and 5.7 (1). □

Remark 5.8. If the reduction of any closed fiber of π is smooth over k, then the minimal regular C_n-model of X_n is C_n-isomorphic to the normalization of $\mathscr{X}$ in X_n for any $n \in \mathbb{Z}_{\geq 0}$ [Mit16, 5.4.2]. Thus, if the reduction of $\mathscr{X}_{x,0}$ is smooth over k, then there exists a k-morphism $\mathscr{X}_{x,n+1} \to \mathscr{X}_{x,n}$ for any $n \in \mathbb{Z}_{\geq 0}$, which implies that the reduction of $\mathscr{X}_{x,n}$ is k-isomorphic to a k-elliptic curve for any $n \in \mathbb{Z}_{\geq 0}$.

Remark 5.9. We denote the type of $\mathscr{X}_{x,n}$ by ${}_{m_{x,n}}T_n$ (Kodaira's symbol). If $T_0 = \mathrm{I}_0$, then $T_n = T_0$ (Remark 5.8). Otherwise, the equality $T_n = T_0$ does not hold in general ([Kat81, Lemmas 2.1 and 3.1] and [Ohh92, Theorem 2.1]). Nevertheless, the equality $T_{n+2} = T_n$ holds for any $n \in \mathbb{Z}_{\geq 0}$ (Proposition 4.3 and Theorem 5.7 (1)).

6. Examples

Let k be an algebraically closed field of characteristic $p \geq 0$, and C be a proper smooth k-curve with function field K.

Definition 6.1. An elliptic fibration $\pi\colon \mathscr{X} \to C$ is said to be *trivial* if there exist a k-elliptic curve E_k and a C-isomorphism $\mathscr{X} \cong E_k \times_{\operatorname{Spec} k} C$.

Theorem 6.2 ([CD89, Corollary 5.4.6])**.** *Let E be a K-elliptic curve. Take the minimal regular C-model $\theta\colon \mathscr{E} \to C$ of E (Definition 5.4). Assume that θ is non-trivial (Definition 6.1). Then the global-to-local map*

$$\phi_E\colon H^1(K,E) \longrightarrow \bigoplus_{x \in C(k)} H^1(K_x, E_x)$$

is surjective, where E_x is the base change of E via K_x/K (Definition 5.1).

Remark 6.3. Take $x \in C(k)$. We denote the type of $\theta^{-1}(x)$ by T_x (Kodaira's symbol). Let X be a K-torsor under E. Take the base change X_x of X via K_x/K and the minimal regular C-model $\pi\colon \mathscr{X} \to C$ of X. Put $(\eta_y)_{y \in C(k)} := \phi_E([X])$ (Definition 3.12), $m_x := \operatorname{ord} \eta_x$, $C_x := \operatorname{Spec} \widehat{\mathscr{O}}_{C,x}$ (Definition 5.1), $\mathscr{E}_x := \mathscr{E} \times_C C_x$, and $\mathscr{X}_x := \mathscr{X} \times_C C_x$. Then $[X_x] = \eta_x$, $\mathscr{E}_x$ (resp. $\mathscr{X}_x$) is the minimal regular C-model of E_x (resp. X_x), and the special fiber of $\mathscr{E}_x$ (resp. $\mathscr{X}_x$) is x-isomorphic to the fiber of $\mathscr{E}$ (resp. $\mathscr{X}$) over x (Remark 5.6). Thus, the type of $\pi^{-1}(x)$ is equal to ${}_{m_x}T_x$ (Theorem 5.7 (1)).

Remark 6.4. Let K' be a finite field extension of K. Take the normalization $\xi\colon C' \to C$ of C in K'. For $x' \in C'(k)$, we take the composite

$$b_{x'}\colon \bigoplus_{x \in C(k)} H^1(K_x, E_x) \longrightarrow H^1(K_{\xi(x')}, E_{\xi(x')}) \longrightarrow H^1(K_{x'}, E_{x'})$$

of the projection onto the summand at $\xi(x')$ and $b^1_{E_{\xi(x')},K_{x'}/K_{\xi(x')}}$ (Definition 3.6), where $E_{x'}$ is the base change of E via $K_{x'}/K$ (Definition 5.1). Then the diagram

$$\begin{array}{ccc} H^1(K,E) & \xrightarrow{\phi_E} & \bigoplus_{x\in C(k)} H^1(K_x,E_x) \\ \Big\downarrow{\scriptstyle b^1_{E,K'/K}} & & \Big\downarrow{\scriptstyle \left(b_{x'}\right)_{x'\in C'(k)}} \\ H^1(K',E') & \xrightarrow{\phi_{E'}} & \bigoplus_{x'\in C'(k)} H^1(K_{x'},E_{x'}) \end{array}$$

commutes, where E' is the base change of E via K'/K, and ϕ_E and $\phi_{E'}$ are the global-to-local maps for E and E', respectively. We use the notation introduced in Remark 6.3. Choose $x' \in \xi^{-1}(x)$. Take the base change X' of X via K'/K and the minimal regular C'-model $\pi' \colon \mathscr{X}' \to C'$ of X'. Then $b^1_{E,K'/K}([X]) = [X']$ (Proposition 3.14), and the type ${}_{m'_{x'}}T'_{x'}$ of $(\pi')^{-1}(x')$ may be determined in the same way as in Remark 6.3. In particular, if K'/K is a Galois extension whose degree is prime to m_x, then $m'_{x'} = m_x$ (Proposition 3.8).

Example 6.5. We use the notation introduced in Theorem 6.2. Suppose that $p > 0$. Take $(m_x)_{x\in C(k)}$ so that each m_x is a power of p, and only finitely many m_x is greater than 1. Assume that θ is non-trivial. For $x \in C(k)$, we denote the type of $\theta^{-1}(x)$ by T_x (Kodaira's symbol). By means of Theorems 5.7 and 6.2, we may produce a relatively minimal elliptic fibration $\pi \colon \mathscr{X} \to C$ satisfying that the type of $\pi^{-1}(x)$ is equal to ${}_{m_x}T_x$ for any $x \in C(k)$ in the following way. By Theorem 5.7 (2), we may choose $\eta_x \in H^1(K_x,E_x)$ of order m_x for each $x \in C(k)$. By Theorem 6.2, we may take $\eta \in H^1(K,E)$ so that $\phi_E(\eta) = (\eta_x)_{x\in C(k)}$. Choose a K-torsor X under E so that $[X] = \eta$ (Definition 3.12). Take the minimal regular C-model $\pi \colon \mathscr{X} \to C$ of X. Then the type of $\pi^{-1}(x)$ is equal to ${}_{m_x}T_x$ for any $x \in C(k)$ (Remark 6.3).

Definition 6.6. Let $\mathscr{X}$ be a proper smooth integral k-scheme of dimension two. We denote the second Chern number and the ℓ-adic Euler characteristic of $\mathscr{X}$ by $c_2(\mathscr{X})$ and $e(\mathscr{X})$, respectively, where ℓ is a prime number not equal to p.

Proposition 6.7. *Let $\pi \colon \mathscr{X} \to C$ be a relatively minimal elliptic fibration with Jacobian fibration $\theta \colon \mathscr{E} \to C$. For $x \in C(k)$, we denote the valuation of the minimal discriminant of $\mathscr{E}/C$ at x by d_x* [Liu02, 9.4.33]*. Then the equalities and inequality*

$$c_2(\mathscr{X}) = e(\mathscr{X}) = e(\mathscr{E}) = \sum_{x\in C(k)} d_x \geq 0$$

hold. The equality in the last inequality holds if and only if θ is smooth.

Proof. The equalities follow from [Mil80, V.3.12], [CD89, Proposition 5.3.6], and [Ogg67, p. 20], respectively. The last inequality follows from the inequality $d_x \geq 0$ for all $x \in C(k)$. The equality $d_x = 0$ holds if and only if θ is smooth at any point over x. Thus, the last statement holds. □

Lemma 6.8. *Assume that $p \geq 3$ (resp. $p = 2$). Put $d := 2$ and $e := 4$ (resp. $d := 3$ and $e := 3$). Let E_k be a k-elliptic curve with k-automorphism τ of order d fixing the origin. We denote the fixed locus of τ by $\mathscr{R}$. Then $\mathscr{R}$ consists of e points, and there exist a primitive d-th root ζ_d of unity and a local parameter s_y of E_k at all $y \in \mathscr{R}$ such that $\tau s_y = \zeta_d s_y$ for any $y \in \mathscr{R}$ (Definition* 5.1*).*

Proof. Take the quotient $\xi\colon E_k \to F_k$ of the k-action of $\mathbb{Z}/d\mathbb{Z}$ on E_k induced by τ. Then ξ is a k-morphism between smooth k-curves that is a Galois covering with Galois group $\mathbb{Z}/d\mathbb{Z}$. The ramification locus and the branch locus of ξ are equal to $\mathscr{R}$ and $\xi(\mathscr{R})$, respectively, and the k-morphism ξ induces a bijection $\mathscr{R} \to \xi(\mathscr{R})$. Since $p \nmid d$, the Riemann–Hurwitz formula implies that $F_k \cong \mathbb{P}^1_k$ over k, and proves the first statement.

Since $p \nmid d$, the Kummer theory implies that there exists a rational function γ on F_k such that E_k is F_k-isomorphic to the smooth model of the curve defined by the equation $P(z) = 0$, where $P(z) := z^d - \gamma$. Choose a root s of $P(z)$ in the function field of E_k. Put $\zeta := \tau s/s$. Then ζ is a primitive d-th root of unity. The rational function γ defines a principal divisor $\sum_{x\in F_k(k)} n_x[x]$ on F_k, where $n_x \in \mathbb{Z}$, and $[x]$ is the prime divisor on F_k with support x. Put $\mathscr{B} := \{x \in F_k(k) \mid d \nmid n_x\}$. Then there exists $n \in \mathbb{Z}$ such that $n_x \equiv n \bmod d$ for any $x \in \mathscr{B}$ since $\mathscr{B} = \xi(\mathscr{R})$, $(d,e) = (2,4)$ or $(3,3)$, and $\sum_{x\in F_k(k)} n_x = 0$. Put $\zeta_d := \zeta^n$. Then ζ_d is a primitive d-th root of unity since $\gcd(n,d) = 1$.

Take $y \in \mathscr{R}$. Put $x := \xi(y) \in \mathscr{B}$ and $m_x := (nn_x - 1)/d$. Then $m_x \in \mathbb{Z}$ since $nn_x \equiv n^2 \equiv 1 \bmod d$. Choose a local parameter t_x of F_k at x. The k-morphism ξ induces an extension K_y/K_x of valuation fields (Definition 5.1). We may regard s and t_x as elements of K_y. Put $s_y := s^n t_x^{-m_x} \in K_y$. Then s_y is a local parameter of E_k at y since $nn_x - dm_x = 1$. Since $\tau s = \zeta s$ and $\tau t_x = t_x$, the equality $\tau s_y = \zeta_d s_y$ holds, which concludes the proof of the last statement. □

Example 6.9. We use the notation introduced in Lemma 6.8. Put $(T,T') := (\mathrm{I}_0^*, \mathrm{I}_0^*)$ (resp. $(\mathrm{IV}, \mathrm{IV}^*)$). Suppose that $C \cong \mathbb{P}^1_k$ over k. Choose a coordinate function t of $C \setminus \{\infty\} \cong \mathbb{A}^1_k$. Take the smooth model C' of the curve defined by the equation $Q(z) = 0$, where $Q(z) := z^d - t$. Choose a root s of $Q(z)$ in the function field of C' and a generator σ of the Galois group of C'/C, which is isomorphic to $\mathbb{Z}/d\mathbb{Z}$. Put $\mathscr{E}' := E_k \times_{\operatorname{Spec} k} C'$ and $\mu := (\tau, \sigma) \in \operatorname{Aut}(\mathscr{E}'/C)$. Then μ and σ induce C-actions ρ_μ and ρ_σ of $\mathbb{Z}/d\mathbb{Z}$ on $\mathscr{E}'$ and C', respectively. The structure morphism $\theta'\colon \mathscr{E}' \to C'$ is equivariant with respect to ρ_μ and ρ_σ. Take the quotients $\xi_\mu\colon \mathscr{E}' \to \widetilde{\mathscr{E}}$ and $\xi_\sigma\colon C' \to C$ of ρ_μ and ρ_σ, respectively. Then there exists a unique morphism $\widetilde{\theta}$ such that the diagram

$$\begin{array}{ccc} \mathscr{E}' & \xrightarrow{\xi_\mu} & \widetilde{\mathscr{E}} \\ \downarrow{\scriptstyle \theta'} & & \downarrow{\scriptstyle \widetilde{\theta}} \\ C' & \xrightarrow{\xi_\sigma} & C \end{array}$$

commutes. We denote the generic points of C and C' by S and S', respectively, and the generic fibers of $\widetilde{\theta}$ and θ' by E and E', respectively. Then $E' \cong E \times_S S'$ over S'. Since τ fixes the origin of E_k, the morphism $\widetilde{\theta}$ admits a section, which implies that $E(S) \neq \emptyset$.

The singular locus of $\widetilde{\mathscr{E}}$ consists of 4 A_1-singularities over 0 and 4 A_1-singularities over ∞ (resp. 3 contractions of (-3)-curves over 0 and 3 A_2-singularities over ∞, where we replace t by t^{-1} if necessary) (Lemma 6.8 and [Mit16, A.3 and A.6 (2)–(3)]). Take the minimal desingularization $\nu\colon \widehat{\mathscr{E}} \to \widetilde{\mathscr{E}}$ of $\widetilde{\mathscr{E}}$ [Liu02, 9.3.31 and 9.3.32]. Put $\widehat{\theta} := \widetilde{\theta} \circ \nu$. We denote the strict transforms of the fibers of $\widetilde{\theta}$ over 0 and ∞ under ν by D_0 and D_∞, respectively, and the fibers of $\widehat{\theta}$ over 0 and ∞ by $\widehat{D}_0$ and $\widehat{D}_\infty$, respectively. Then the dual graphs of $\widehat{D}_0$ and $\widehat{D}_\infty$ with self-intersection numbers are given by Figure 1, where the self-intersection numbers of D_0 and D_∞ are determined by means of the classification of singular fibers of elliptic fibrations (see, e.g., [Liu02, 10.2.1]). Thus, the minimal regular

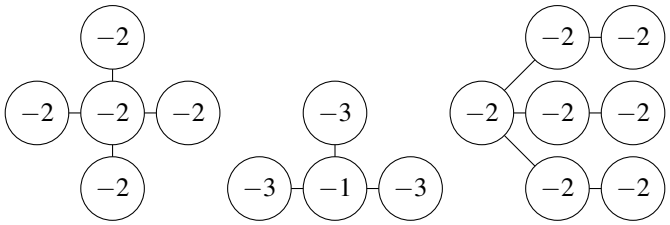


FIGURE 1. The dual graphs of $\widehat{D}_0$ and $\widehat{D}_\infty$ are equal to the left graph (resp. the middle and right graphs, respectively). The integer at the center of a node is the self-intersection number of the corresponding prime divisor. The node connected to 4 edges (resp. 3 edges) corresponds to D_0 or D_∞.

C-model $\theta\colon \mathscr{E} \to C$ of E (Definition 5.4) is given by the C-scheme $\widehat{\mathscr{E}}$ (resp. the blowing-down of $\widehat{\mathscr{E}}$ along the (-1)-curve D_0), which admits exactly two singular fibers, of type T over 0 and of type T' over ∞.

Take $n \in \mathbb{Z}_{>0}$. Put $q := p^n$. Then there exists a relatively minimal elliptic fibration $\pi\colon \mathscr{X} \to C$ satisfying the following conditions (Example 6.5).

(1) The Jacobian fibration of π is given by θ.
(2) The elliptic fibration π admits exactly two singular fibers, of type ${}_qT$ over 0 and of type T' over ∞.

We denote the generic fiber of π by X. Take the base change X' of X via S'/S and the minimal regular C'-model $\pi'\colon \mathscr{X}' \to C'$ of X'. Since $E' \cong E \times_S S'$ over S', the Jacobian of X' is S'-isomorphic to E'. Thus, the following statements hold.

(1') The Jacobian fibration of π' is given by θ' (Remark 5.5).
(2') The elliptic fibration π' admits exactly one singular fiber, of type ${}_q\mathrm{I}_0$ over $\xi_\sigma^{-1}(0)$ (Remark 6.4).
(3') The equality $c_2(\mathscr{X}') = 0$ holds (Proposition 6.7).

Remark 6.10. Example 6.9 for a supersingular k-elliptic curve E_k and $n > 1$ contradicts [Kaw00, Theorem B] and [Kaw06, Theorem 4.1], each of which states that there do not exist such elliptic surfaces. These incorrect results are based on the resolutions of multiple fibers in [Kaw00, Theorem 3.2] and [Kaw06, Theorem 3.1], respectively, both of which contradict Theorem 1.2. Let us explain the errors in the proofs of these resolutions. In [Kaw00, p. 193, l. 2], both domain and codomain of

$$(\phi|_{S_i})^*\colon H^1(E, \mathscr{O}_E) \longrightarrow H^1(S_i, \mathscr{O}_{S_i})$$

are incorrect. Moreover, the assumption that $\phi|_{S_i}\colon S_i \to E$ is a non-separable covering does not imply that $\widehat{\pi}|_{\widehat{S}_i}\colon \widehat{S}_i \to S_i$ is an isomorphism by the following reason.

Let us recall the notation and argument in [Kaw00, pp. 191–193, Proof of Theorem 3.2]. Let k be an algebraically closed field of positive characteristic p, $f\colon X \to \mathbb{P}^1_k$ be a relatively minimal elliptic fibration, and S_i be the reduction of a closed fiber of f whose multiplicity is divisible by p. Take the Albanese map $\phi\colon X \to E$ of X. Assume that E is a supersingular k-elliptic curve. Then S_i is k-isomorphic to a k-elliptic curve. Choose a non-zero element ρ of $H^1(E, \mathscr{O}_E)$. Then $F^*\rho = 0$, where F is the absolute Frobenius morphism of E.

In [Kaw00, p. 191, the second paragraph of Proof of Theorem 3.2], a finite flat morphism $\pi\colon E_1 \to E$ is induced by ρ in the following way. Choose an affine open covering $\mathscr{U} = (U_\lambda)_{\lambda\in\Lambda}$ of E and a Čech 1-cocycle $(\rho_{\lambda,\mu})_{\lambda\in\Lambda,\mu\in\Lambda} \in Z^1(\mathscr{U},\mathscr{O}_E)$ that represents ρ. Since $F^*\rho = 0$, there exists a Čech 0-cochain $(\rho_\lambda)_{\lambda\in\Lambda} \in C^0(\mathscr{U},\mathscr{O}_E)$ such that $\rho_{\lambda,\mu}^p = \rho_\lambda - \rho_\mu$ in $\mathscr{O}_E(U_{\lambda,\mu})$ for any $\lambda\in\Lambda$ and any $\mu\in\Lambda$, where $U_{\lambda,\mu} := U_\lambda \cap U_\mu$. For each $\lambda\in\Lambda$, the finite flat $\mathscr{O}_E(U_\lambda)$-algebra $\mathscr{O}_E(U_\lambda)[z_\lambda]/(z_\lambda^p - \rho_\lambda)$ induces a finite flat morphism $\pi_\lambda : \widetilde{U}_\lambda \to U_\lambda$. For each $\lambda\in\Lambda$ and each $\mu\in\Lambda$, we put $\widetilde{U}_{\lambda,\mu} := \pi_\lambda^{-1}(U_{\lambda,\mu})$. Then the $\mathscr{O}_E(U_{\lambda,\mu})$-isomorphism $\mathscr{O}_{\widetilde{U}_\lambda}(\widetilde{U}_{\lambda,\mu}) \cong \mathscr{O}_{\widetilde{U}_\mu}(\widetilde{U}_{\mu,\lambda})$ defined by $z_\lambda \mapsto z_\mu + \rho_{\lambda,\mu}$ induces a $U_{\lambda,\mu}$-isomorphism $\psi_{\lambda,\mu}\colon \widetilde{U}_{\mu,\lambda} \cong \widetilde{U}_{\lambda,\mu}$. By these isomorphisms $(\psi_{\lambda,\mu})_{\lambda\in\Lambda,\mu\in\Lambda}$, the morphisms $(\pi_\lambda)_{\lambda\in\Lambda}$ glue to a finite flat morphism $\pi\colon E_1 \to E$.

Take the base change $\widetilde{\pi}\colon \widetilde{X} \to X$ of π via ϕ, which is induced by $\phi^*\rho$ in the same way as in the case of π. Take the normalization $\nu\colon \widehat{X} \to \widetilde{X}$ of $\widetilde{X}$. Put $\widehat{\pi} := \widetilde{\pi}\circ\nu\colon \widehat{X} \to X$. Take the base changes $\widetilde{\pi}_i\colon \widetilde{F}_i \to S_i$ and $\widehat{\pi}_i\colon \widehat{F}_i \to S_i$ of $\widetilde{\pi}$ and $\widehat{\pi}$ via the closed immersion $S_i \to X$, respectively, and the reduction $\widehat{S}_i$ of $\widehat{F}_i$. In [Kaw00, p. 193, l. 2], the morphism $\phi|_{S_i}$ is assumed to be a non-separable covering. Then $(\phi|_{S_i})^*\rho = 0$. However, we cannot conclude that $\widehat{\pi}|_{\widehat{S}_i}\colon \widehat{S}_i \to S_i$ is an isomorphism since $\widehat{\pi}_i\colon \widehat{F}_i \to S_i$ is *not* induced by $(\phi|_{S_i})^*\rho$ while $\widetilde{\pi}_i\colon \widetilde{F}_i \to S_i$ is induced by $(\phi|_{S_i})^*\rho$ in the same way as in the case of π.

The same argument appears in [Kaw06, p. 608, the last paragraph].

Acknowledgments. The author thanks the referee for helpful comments. This work was supported by JSPS KAKENHI Grant Numbers JP09J01111, JP12J01432, JP25800018, JP24224001, JP17K14167, JP17H02832, JP17H06127, and the Japan–France Research Cooperative Program of JSPS and CNRS.

REFERENCES

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990.

[BM77] E. Bombieri and D. Mumford, *Enriques' classification of surfaces in char. p, II*, Complex analysis and algebraic geometry, Iwanami Shoten, Tokyo, 1977, pp. 23–42.

[CD89] F. R. Cossec and I. V. Dolgačev, *Enriques surfaces I*, Progress in Mathematics, vol. 76, Birkhäuser Boston Inc., Boston, MA, 1989.

[Gro77] A. Grothendieck, *Cohomologie l-adique et Fonctions L*, Lecture Notes in Mathematics, vol. 589, Springer-Verlag, Berlin, 1977, Séminaire de Géométrie Algébrique du Bois-Marie 1965–1966 (SGA 5), Avec la collaboration de I. Bucur, C. Houzel, L. Illusie, J. P. Jouanolou et J. P. Serre.

[Kat81] T. Katsura, *Unirational elliptic surfaces in characteristic p*, Tôhoku Math. J. (2) **33** (1981), no. 4, 521–553.

[Kaw00] M. Kawazoe, *Multiple fibers on elliptic surfaces in positive characteristic*, J. Math. Kyoto Univ. **40** (2000), no. 1, 185–201.

[Kaw06] ———, *Multiple supersingular elliptic fibers on elliptic surfaces*, J. Pure Appl. Algebra **204** (2006), no. 3, 602–615.

[Kod63a] K. Kodaira, *On compact analytic surfaces: II*, Ann. of Math. (2) **77** (1963), no. 3, 563–626.

[Kod63b] ———, *On compact analytic surfaces, III*, Ann. of Math. (2) **78** (1963), no. 1, 1–40.

[KU85] T. Katsura and K. Ueno, *On elliptic surfaces in characteristic p*, Math. Ann. **272** (1985), no. 3, 291–330.

[KU86] ———, *Multiple singular fibres of type* $\mathbf{G}_a$ *of elliptic surfaces in characteristic p*, Algebraic and topological theories (Kinosaki, 1984), Kinokuniya, Tokyo, 1986, pp. 405–429.

[Liu02] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.

[LLR04] Q. Liu, D. Lorenzini, and M. Raynaud, *Néron models, Lie algebras, and reduction of curves of genus one*, Invent. Math. **157** (2004), no. 3, 455–518.

[Mil80] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.
[Mit15] K. Mitsui, *Homotopy exact sequences and orbifolds*, Algebra Number Theory **9** (2015), no. 5, 1089–1136.
[Mit16] ———, *Canonical bundle formula and base change*, J. Algebraic Geom. **25** (2016), no. 4, 775–814.
[Ogg67] A. P. Ogg, *Elliptic curves and wild ramification*, Amer. J. Math. **89** (1967), no. 1, 1–21.
[Ohh92] M. Ohhira, *Unirational elliptic surfaces in characteristic* 2, J. Math. Soc. Japan **44** (1992), no. 4, 709–738.
[Ser02] J. P. Serre, *Galois cohomology*, English ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author.
[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[Tak94] Y. Takeda, *False hyperelliptic surfaces with section*, Math. Nachr. **167** (1994), no. 1, 313–329.
[Tak96] ———, *Errata to the paper: "False hyperelliptic surfaces with section" [Math. Nachr.* **167** *(1994), 313–329]*, Math. Nachr. **182** (1996), no. 1, 329.
[Tat75] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Mathematics, vol. 476, Springer, Berlin, 1975, pp. 33–52.

DEPARTMENT OF MATHEMATICS, GRADUATE SCHOOL OF SCIENCE, KOBE UNIVERSITY, HYOGO 657-8501, JAPAN

E-mail address: mitsui@math.kobe-u.ac.jp