Ramification of Torsion Points on a Curve with Superspecial Reduction over an Absolutely Unramified Base

Yuichiro Hoshi

June 2021

Abstract. — Let p be a prime number, W an absolutely unramified p-adically complete discrete valuation ring with perfect residue field, and X a curve over the field of fractions of W of genus greater than one. In the present paper, we study the ramification of torsion points on the curve X. A consequence of the main result of the present paper is nonexistence of ramified torsion point on X in the case where p is greater than three, the Jacobian variety J of X has good reduction over W, and the special fiber of the good model of J is superspecial. This consequence generalizes a theorem proved by Coleman.

Contents

Introduction

In the present Introduction, let p be a prime number and k a perfect field of characteristic p. Write W for the ring of Witt vectors with coefficients in k and $K \overset{\text{def}}{=} W[p^{-1}]$ for the field of fractions of W. Let $\overline{K}$ be an algebraic closure of K. Write $\Gamma_K \overset{\text{def}}{=} \mathrm{Gal}(\overline{K}/K)$ for the absolute Galois group of K determined by the algebraic closure $\overline{K}$. Moreover, let $g \geq 2$ be an integer and X a curve over K [i.e., a scheme of dimension one that is projective, smooth, and geometrically connected over K] of genus g. Write J for the Jacobian variety of X. In the present Introduction, suppose that

> the inequality $p > 3$ holds, and, moreover, the abelian variety J over K has *good reduction* over W.

Write, moreover, $X_{\overline{K}} \overset{\text{def}}{=} X \times_K \overline{K}$ (respectively, $J_{\overline{K}} \overset{\text{def}}{=} J \times_K \overline{K}$) and $X^{\mathrm{cl}}_{\overline{K}}$ (respectively, $J^{\mathrm{cl}}_{\overline{K}}$) for the set of closed points of $X_{\overline{K}}$ (respectively, $J_{\overline{K}}$). We shall say that a closed point

2010 Mathematics Subject Classification. — Primary 14H25; Secondary 11G20, 14H40, 14L15.
Key words and phrases. — curve, ramified torsion point, superspecial.

of $J_{\overline{K}}$ is *unramified* if the image, by the natural morphism $J_{\overline{K}} \to J$, of the closed point is a closed point of J whose residue field is unramified over K.

If x_0 is a K-rational point of X, then one may consider the *Albanese embedding* $X \hookrightarrow J$ with respect to $x_0 \in X(K)$, i.e., the closed immersion over K obtained by, roughly speaking, mapping a closed point "x" of X to the point of J corresponding to the divisor "$[x] - [x_0]$" — where we write "$[-]$" for the prime divisor determined by the closed point "$(-)$" — of degree zero, which thus determines an injective map

$$\mathfrak{a}\colon X^{\mathrm{cl}}_{\overline{K}} \hookrightarrow J^{\mathrm{cl}}_{\overline{K}}.$$

In the present paper, we study a *torsion point* on $X_{\overline{K}}$, i.e., a closed point of $X_{\overline{K}}$ whose image, via "$\mathfrak{a}$" with respect to some K-rational point of X, is a torsion point of $J_{\overline{K}}$. More specifically, in the present paper, we study the *ramification of torsion points* on $X_{\overline{K}}$.

In the remainder of the present Introduction, suppose, moreover, that we are in the following situation:

> Let $x_0 \in X(K)$ be a K-rational point of X. By means of the injective map $\mathfrak{a}\colon X^{\mathrm{cl}}_{\overline{K}} \hookrightarrow J^{\mathrm{cl}}_{\overline{K}}$ determined by the Albanese embedding with respect to this K-rational point $x_0 \in X(K)$, we regard $X^{\mathrm{cl}}_{\overline{K}}$ as a subset of $J^{\mathrm{cl}}_{\overline{K}}$. Let $x \in X^{\mathrm{cl}}_{\overline{K}}$ $(\subseteq J^{\mathrm{cl}}_{\overline{K}})$ be a closed point of $X_{\overline{K}}$ such that the closed point $x \in J^{\mathrm{cl}}_{\overline{K}}$ [i.e., $\mathfrak{a}(x) \in J^{\mathrm{cl}}_{\overline{K}}$] of $J_{\overline{K}}$ is *torsion*.

Let us first recall that *Coleman* posed, in [2], a conjecture concerning the ramification of torsion points on a curve that satisfies certain conditions [cf. [2, Conjecture B]]. The following is the statement [of a stronger version] of the conjecture. [Note that the *original* conjecture posed by Coleman is the following conjecture in the case where the pair (X, x_0) arises from a similar pair defined over a *number field contained in* K.]

CONJECTURE A (Coleman). — *Suppose that the curve X over K has* **good reduction** *over W. Then the torsion point $x \in J^{\mathrm{cl}}_{\overline{K}}$ is* **unramified**.

Moreover, Coleman also essentially proved the following result concerning Conjecture A [cf. [2, Corollary 20.2]].

THEOREM B (Coleman). — *Suppose that the curve X over K has* **good reduction** *over W. Suppose, moreover, that one of the following two conditions is satisfied:*

(O) *The special fiber of the good model of J is an* **ordinary** *abelian variety over k.*

(S) *The special fiber of the good model of J is a* **superspecial** *abelian variety over k [i.e., is isomorphic to the fiber product of finitely many* **supersingular** *elliptic curves over k].*

Then the torsion point $x \in J^{\mathrm{cl}}_{\overline{K}}$ is **unramified**.

Next, let us recall that *Tamagawa* gives a refinement of Theorem B in the case where condition (O) is satisfied. More precisely, by this refinement, one may remove the assumption that the curve X over K has *good reduction* over W from the statement of

Theorem B in the case where condition (O) is satisfied [cf. [9, Proposition 2.1] and [9, Theorem 3.6, (ii)]].

THEOREM C (Tamagawa). — *Suppose that the special fiber of the good model of J is an* **ordinary** *abelian variety over k. Then the torsion point $x \in J^{\mathrm{cl}}_{\overline{K}}$ is* **unramified**.

Next, let us also recall that the author of the present paper proved the following result closely related to Conjecture A [cf. [5, Theorem B]].

THEOREM D. — *The torsion point $p \cdot x \in J^{\mathrm{cl}}_{\overline{K}}$ is* **unramified**.

In the present paper, we study the ramification of torsion points on a curve such that the special fiber of the good model of the Jacobian variety of the curve is *superspecial* by means of Theorem D and some classical results in the study of finite flat commutative group schemes. The main result of the present paper [cf. Corollary 3.3] implies the following result, that is a refinement of Theorem B in the case where condition (S) is satisfied. By this refinement, one may remove the assumption that the curve X over K has *good reduction* over W from the statement of Theorem B in the case where condition (S) is satisfied.

THEOREM E. — *Suppose that the special fiber of the good model of J is a* **superspecial** *abelian variety over k. Then the torsion point $x \in J^{\mathrm{cl}}_{\overline{K}}$ is* **unramified**.

A short description of the strategy of the proof of Theorem E is as follows: Suppose that we are in the situation of Theorem E. Let us first observe that, to verify Theorem E, we may assume without loss of generality that k is *algebraically closed*. Then, to verify Theorem E, it suffices to verify that a certain finite Γ_K-stable submodule $M(x, \Gamma_K)$ of $J^{\mathrm{cl}}_{\overline{K}}$ determined by the torsion point $x \in J^{\mathrm{cl}}_{\overline{K}}$ [cf. Definition 2.3, (ii)] is *trivial* [cf. Lemma 2.4]. Assume that $M(x, \Gamma_K)$ is *nontrivial*. Then it follows from some elementary considerations in the theory of algebraic curves that, to obtain a *contradiction*, it suffices to verify that the image of the action of Γ_K on $M(x, \Gamma_K)$ contains *sufficiently many homotheties* [cf. Lemma 2.7, (i), and condition (2C) in the discussion following Lemma 2.5; also Corollary 3.2]. The first important observation to verify the existence of *sufficiently many homotheties* is that

> it follows from [5, Theorem B] that $M(x, \Gamma_K)$ is *annihilated by p* [cf. Lemma 2.5, (ii)].

The second important observation to verify the existence of *sufficiently many homotheties* is that since [we have assumed that] the special fiber of the good model of J is *superspecial*,

> it follows from the main theorem of [6] that there exist g elliptic curves $E_1, \ldots, E_g$ over W such that the special fiber $E_i \times_W k$ is *supersingular* for each $i \in \{1, \ldots, g\}$, and, moreover, the Γ_K-module $J^{\mathrm{cl}}_{\overline{K}}[p]$ of p-torsion elements of $J^{\mathrm{cl}}_{\overline{K}}$ is isomorphic to the Γ_K-module of p-torsion $\overline{K}$-valued points of $E_1 \times_W \cdots \times_W E_g$.

On the other hand, it follows from some classical results in the study of finite flat commutative group schemes that the image of the action of Γ_K on the module of p-torsion $\overline{K}$-valued points of $E_1 \times_W \cdots \times_W E_g$, hence also on the module $M(x, \Gamma_K)$, contains *sufficiently many homotheties* [cf. Lemma 1.9], as desired. This completes the short description of the strategy of the proof of Theorem E.

Here, let us observe that one may think that curves over K subject to Theorem B in the case where condition (S) is satisfied are "*few*" [cf. Remark 3.3.1, (i)]. On the other hand, one may conclude that "*many*" curves over K may be thought to be subject to Theorem E [cf. Remark 3.3.1, (ii)].

The present paper is organized as follows: In §1, we give proofs of some facts concerning a Galois module *of type* G annihilated by p. In §2, we discuss Galois modules that arise from *torsion points* on curves. In §3, we prove the main result of the present paper.

Acknowledgments

The author would like to thank the referee for carefully reading some versions of the present paper. This research was supported by JSPS KAKENHI Grant Number 18K03239 and by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

1. Galois Modules of Type G Annihilated by p

In the present §1, we give proofs of some facts concerning a Galois module *of type* G [cf. Definition 1.4 below] *annihilated by* p.

Definition 1.1. — Let Γ be a group and S a set on which Γ acts. Then we shall write $S^{\Gamma} \subseteq S$ for the subset of S of Γ-invariants, $\Gamma^S \subseteq \Gamma$ for the unique maximal [necessarily normal] subgroup of Γ that acts on S trivially, and $\Gamma[S] \stackrel{\text{def}}{=} \Gamma/\Gamma^S$ for the quotient of Γ by Γ^S.

Remark 1.1.1. — In the situation of Definition 1.1, it is immediate that the action of Γ on S *factors* through the natural surjective homomorphism $\Gamma \twoheadrightarrow \Gamma[S]$, and, moreover, the resulting action of $\Gamma[S]$ on S is *faithful*.

Definition 1.2. — Let A be a finite module.

(i) We shall write $\mathrm{Aut}(A)$ for the [necessarily finite] group of automorphisms of the module A.

(ii) Let n be an integer. Then we shall write $A[n] \stackrel{\text{def}}{=} \{ a \in A \mid na = 0 \} \subseteq A$.

(iii) Let l be a prime number. Then we shall write $A[l^{\infty}] \stackrel{\text{def}}{=} \bigcup_{i \geq 1} A[l^i] \subseteq A$ and $A[l^{\infty}_{\neq}] \subseteq A$ for the submodule of A generated by the elements of the $A[(l')^{\infty}]$'s, where l' ranges over the prime numbers such that $l' \neq l$.

Remark 1.2.1. — In the situation of Definition 1.2, (iii), it is immediate that we have a natural decomposition $A = A[l^\infty] \oplus A[l^\infty_{\neq}]$.

Definition 1.3. — Let Γ be a group, A a Γ-module whose underlying module is finite, and l a prime number.

(i) Suppose that $A[l^\infty] = \{0\}$. Then we shall define the *l-height* of A to be zero.

(ii) Suppose that $A[l^\infty] \neq \{0\}$. Then we shall define the *l-height* of A to be the unique minimal positive integer divisible by $\dim_{\mathbb{F}_l} V$, where V ranges over nonzero simple Γ-modules that arise as Γ-stable subquotients of the Γ-module $A[l^\infty]$.

(iii) Let h be a nonnegative integer. Then we shall say that the Γ-module A is *of strictly l-height h* if $\dim_{\mathbb{F}_l} V = h$ for each simple Γ-module V that arises as a Γ-stable subquotient of the Γ-module $A[l^\infty]$.

Let p be an odd prime number and k a perfect field of characteristic p. Write W for the ring of Witt vectors with coefficients in k and $K \stackrel{\mathrm{def}}{=} W[p^{-1}]$ for the field of fractions of W. Let $\overline{K}$ be an algebraic closure of K. Write $K^{\mathrm{tm}} \subseteq \overline{K}$ for the unique maximal tamely ramified extension of K in $\overline{K}$ and $\Gamma_K^{\mathrm{wd}} \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{K}/K^{\mathrm{tm}}) \subseteq \Gamma_K \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{K}/K)$ for the respective absolute Galois groups of K^{tm}, K determined by the algebraic closure $\overline{K}$. [Thus, it is well-known that if k is *algebraically closed*, then the closed subgroup Γ_K^{wd} of Γ_K is the *unique pro-p-Sylow* subgroup of Γ_K.] Let M be a Γ_K-module whose underlying module is *nonzero* and *finite*.

Definition 1.4. — We shall say that the Γ_K-module M is *of type G* [cf. [5, Definition 2.3, (i)]] if there exist an abelian variety A over K that has good reduction over W and a Γ_K-equivariant injective homomorphism $M \hookrightarrow A(\overline{K})$.

In the remainder of the present §1, suppose that k is *algebraically closed*, and that the following two conditions are satisfied:

(1A) The Γ_K-module M is *of type G*.

(1B) The *equality* $M[p] = M$ holds.

Write h_M ($\neq 0$ — cf. condition (1B)) for the *p-height* of the Γ_K-module M and $q_M \stackrel{\mathrm{def}}{=} p^{h_M}$.

Definition 1.5. — We shall say that the Γ_K-module M is *connected* if the action of Γ_K on every nonzero Γ_K-stable subquotient of M is nontrivial [cf. also [5, Lemma 2.4, (ii)]].

Lemma 1.6. — *Suppose that the Γ_K-module M is* **connected** *and* **semisimple**, *i.e., that there exist a positive integer r and, for each $i \in \{1, \ldots, r\}$, a* **connected** *and* **simple** *Γ_K-module M_i ($\neq \{0\}$) such that the Γ_K-module M is* **isomorphic** *to the Γ_K-module $\bigoplus_{i=1}^r M_i$. For each $i \in \{1, \ldots, r\}$, write $d_i \stackrel{\mathrm{def}}{=} \dim_{\mathbb{F}_p} M_i$ [cf. condition (1B)] and $q_i \stackrel{\mathrm{def}}{=} p^{d_i}$.*

[Thus, one verifies easily that the integer h_M **coincides** *with the least common multiple of the d_i's, where i ranges over the elements of $\{1, \ldots, r\}$.] Then there exist*

(a) *a surjective homomorphism $\mathbb{F}_{q_M}^{\times} \twoheadrightarrow \Gamma_K[M]$ of groups,*

(b) *an isomorphism $M_i \xrightarrow{\sim} \mathbb{F}_{q_i}$ of modules for each $i \in \{1, \ldots, r\}$, and*

(c) *a nonempty subset $I_i \subseteq \{0, 1, \ldots, d_i - 1\}$ for each $i \in \{1, \ldots, r\}$*

such that, for each $i \in \{1, \ldots, r\}$, the following two actions of $\mathbb{F}_{q_M}^{\times}$ on $\mathbb{F}_{q_i}$ **coincide***:*

- *The action*

$$\mathbb{F}_{q_M}^{\times} \twoheadrightarrow \Gamma_K[M] \longrightarrow \mathrm{Aut}(M_i) \xrightarrow{\sim} \mathrm{Aut}(\mathbb{F}_{q_i})$$

obtained by forming the composite of the surjective homomorphism $\mathbb{F}_{q_M}^{\times} \twoheadrightarrow \Gamma_K[M]$ of (a)*, the homomorphism $\Gamma_K[M] \to \mathrm{Aut}(M_i)$ determined by the action of Γ_K on M_i, and the isomorphism $\mathrm{Aut}(M_i) \xrightarrow{\sim} \mathrm{Aut}(\mathbb{F}_{q_i})$ obtained by conjugation by the isomorphism $M_i \xrightarrow{\sim} \mathbb{F}_{q_i}$ of* (b)*.*

- *The action*

$$\mathbb{F}_{q_M}^{\times} \xrightarrow{\mathrm{Norm}_{\mathbb{F}_{q_M}/\mathbb{F}_{q_i}}} \mathbb{F}_{q_i}^{\times} \xrightarrow{a \mapsto a^{\sum_{j \in I_i} p^j}} \mathbb{F}_{q_i}^{\times} \xhookrightarrow{\text{multiplication}} \mathrm{Aut}(\mathbb{F}_{q_i}).$$

PROOF. — This assertion follows immediately, in light of [5, Remark 2.3.1, (iii)], from [8, Théorème 3.3.3] and [8, Corollaire 3.4.4]. □

REMARK 1.6.1. — In the situation of Lemma 1.6, suppose, moreover, that $r = 1$, which thus implies that $q_M = q_1$. Then since the Γ_K-module M is *simple*, it follows immediately from Lemma 1.6 that the image of the homomorphism

$$\mathbb{F}_{q_M}^{\times} \xrightarrow{a \mapsto a^{\sum_{j \in I_1} p^j}} \mathbb{F}_{q_M}^{\times}$$

does *not factor* through any subgroup of $\mathbb{F}_{q_M}^{\times}$ of the form "$\mathbb{F}^{\times} \subseteq \mathbb{F}_{q_M}^{\times}$", where $\mathbb{F} \subseteq \mathbb{F}_{q_M}$ is a *subfield* of $\mathbb{F}_{q_M}$.

REMARK 1.6.2. — In the situation of Lemma 1.6, suppose, moreover, that $d_i = 2$ for each $i \in \{1, \ldots, r\}$ [which thus implies that the Γ_K-module M is *of strictly p-height two*]. Then one verifies easily [cf. also Remark 1.6.1] that the subset $I_i \subseteq \{0, 1\}$ of (c) may be taken to be *of cardinality one* for each $i \in \{1, \ldots, r\}$.

LEMMA 1.7. — *There exist*

(a) *a surjective homomorphism $\mathbb{F}_{q_M}^{\times} \twoheadrightarrow \Gamma_K[M]/\Gamma_K^{\mathrm{wd}}[M]$ of groups,*

(b) *a sequence of Γ_K-stable submodules of M*

$$\{0\} = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M^{\circ} \subseteq M,$$

(c) *an isomorphism $M_i/M_{i-1} \xrightarrow{\sim} \mathbb{F}_{q_i}$ of modules, where we write $d_i \stackrel{\mathrm{def}}{=} \dim_{\mathbb{F}_p}(M_i/M_{i-1})$ [cf. condition* (1B)*], which thus implies that $q_i = p^{d_i}$, for each $i \in \{1, \ldots, r\}$, and*

(d) *a nonempty subset* $I_i \subseteq \{0, 1, \ldots, d_i - 1\}$ *for each* $i \in \{1, \ldots, r\}$

that satisfy the following three conditions:

(1) *The action of* Γ_K *on* M/M° *is* **trivial**. *Moreover, the* Γ_K*-module* M° *is* **connected**.

(2) *For each* $i \in \{1, \ldots, r\}$*, the action of* Γ_K *on* M_i/M_{i-1} **factors** *through the natural surjective homomorphism* $\Gamma_K \twoheadrightarrow \Gamma_K[M]/\Gamma_K^{\mathrm{wd}}[M]$.

(3) *For each* $i \in \{1, \ldots, r\}$*, the following two actions of* $\mathbb{F}_{q_M}^\times$ *on* $\mathbb{F}_{q_i}$ **coincide**:

- *The action*

$$\mathbb{F}_{q_M}^\times \twoheadrightarrow \Gamma_K[M]/\Gamma_K^{\mathrm{wd}}[M] \longrightarrow \mathrm{Aut}(M_i/M_{i-1}) \xrightarrow{\sim} \mathrm{Aut}(\mathbb{F}_{q_i})$$

obtained by forming the composite of the surjective homomorphism $\mathbb{F}_{q_M}^\times \twoheadrightarrow \Gamma_K[M]/\Gamma_K^{\mathrm{wd}}[M]$ *of* (a)*, the homomorphism* $\Gamma_K[M]/\Gamma_K^{\mathrm{wd}}[M] \to \mathrm{Aut}(M_i/M_{i-1})$ *determined* [*cf.* (2)] *by the action of* Γ_K *on* M_i/M_{i-1}*, and the isomorphism* $\mathrm{Aut}(M_i/M_{i-1}) \xrightarrow{\sim} \mathrm{Aut}(\mathbb{F}_{q_i})$ *obtained by conjugation by the isomorphism* $M_i/M_{i-1} \xrightarrow{\sim} \mathbb{F}_{q_i}$ *of* (c).

- *The action*

$$\mathbb{F}_{q_M}^\times \xrightarrow{\mathrm{Norm}_{\mathbb{F}_{q_M}/\mathbb{F}_{q_i}}} \mathbb{F}_{q_i}^\times \xrightarrow{a \mapsto a^{\sum_{j \in I_i} p^j}} \mathbb{F}_{q_i}^\times \xhookrightarrow{\text{multiplication}} \mathrm{Aut}(\mathbb{F}_{q_i}).$$

PROOF. — Let us first observe that it follows from [5, Proposition 2.5, (i)] and condition (1A) that the Γ_K-module M has a *G-part* $M^\circ \subseteq M$ [cf. [5, Definition 2.3, (ii)]]. Now we claim the following assertion:

> Claim 1.7.A: The action of Γ_K on M/M° is *trivial.* Moreover, the Γ_K-module M° is *connected.*

Indeed, the first assertion follows from condition (2) of [5, Definition 2.3, (ii)]. Moreover, the second assertion follows from condition (3) of [5, Definition 2.3, (ii)]. This completes the proof of Claim 1.7.A.

Let $\{0\} = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M^\circ$ be a composition series of the Γ_K-module M°. For each $i \in \{1, \ldots, r\}$, write $V_i \stackrel{\mathrm{def}}{=} M_i/M_{i-1}$. Write, moreover, $M_{\mathrm{ss}}^\circ \stackrel{\mathrm{def}}{=} \bigoplus_{i=1}^r V_i$ and $M_{\mathrm{ss}} \stackrel{\mathrm{def}}{=} (M/M^\circ) \oplus M_{\mathrm{ss}}^\circ$. Now we claim the following assertion:

> Claim 1.7.B: The kernel of the natural surjective homomorphism $\Gamma_K[M] \twoheadrightarrow \Gamma_K[M_{\mathrm{ss}}^\circ]$ is a *p-group.*

To this end, let us first observe that since [one verifies easily that] the group of upper triangular unipotent matrices of a fixed degree with coefficients in $\mathbb{F}_p$ is a *p-group*, it follows from condition (1B) that the kernel of the natural surjective homomorphism $\Gamma_K[M] \twoheadrightarrow \Gamma_K[M_{\mathrm{ss}}]$ is a *p-group.* On the other hand, it follows from the first assertion of Claim 1.7.A that the two quotients $\Gamma_K[M_{\mathrm{ss}}^\circ]$ and $\Gamma_K[M_{\mathrm{ss}}]$ of Γ_K *coincide.* This completes the proof of Claim 1.7.B.

Next, let us observe that it follows from Lemma 1.6 and Claim 1.7.A that there exist

(a′) a surjective homomorphism $\mathbb{F}_{q_M}^\times \twoheadrightarrow \Gamma_K[M_{\mathrm{ss}}^\circ]$ of groups, (b′) an isomorphism $V_i \xrightarrow{\sim} \mathbb{F}_{q_i}$ of modules for each $i \in \{1, \ldots, r\}$, and

(c′) a nonempty subset $I_i \subseteq \{0, 1, \ldots, d_i - 1\}$ for each $i \in \{1, \ldots, r\}$

such that, for each $i \in \{1, \ldots, r\}$, the following two actions of $\mathbb{F}_{q_M}^{\times}$ on $\mathbb{F}_{q_i}$ *coincide*:

- The action

$$\mathbb{F}_{q_M}^{\times} \twoheadrightarrow \Gamma_K[M_{\mathrm{ss}}^{\circ}] \longrightarrow \mathrm{Aut}(V_i) \xrightarrow{\sim} \mathrm{Aut}(\mathbb{F}_{q_i})$$

obtained by forming the composite of the surjective homomorphism $\mathbb{F}_{q_M}^{\times} \twoheadrightarrow \Gamma_K[M_{\mathrm{ss}}^{\circ}]$ of (a′), the homomorphism $\Gamma_K[M_{\mathrm{ss}}^{\circ}] \to \mathrm{Aut}(V_i)$ determined by the action of Γ_K on V_i, and the isomorphism $\mathrm{Aut}(V_i) \xrightarrow{\sim} \mathrm{Aut}(\mathbb{F}_{q_i})$ obtained by conjugation by the isomorphism $V_i \xrightarrow{\sim} \mathbb{F}_{q_i}$ of (b′).

- The action

$$\mathbb{F}_{q_M}^{\times} \xrightarrow{\mathrm{Norm}_{\mathbb{F}_{q_M}/\mathbb{F}_{q_i}}} \mathbb{F}_{q_i}^{\times} \xrightarrow{a \mapsto a^{\sum_{j \in I_i} p^j}} \mathbb{F}_{q_i}^{\times} \xhookrightarrow{\text{multiplication}} \mathrm{Aut}(\mathbb{F}_{q_i}).$$

Thus, we conclude immediately [cf. also Claim 1.7.A] that, to complete the verification of Lemma 1.7, it suffices to verify the following assertion:

> Claim 1.7.C: The two quotients $\Gamma_K[M_{\mathrm{ss}}^{\circ}]$ and $\Gamma_K[M]/\Gamma_K^{\mathrm{wd}}[M]$ of Γ_K *coincide.*

To this end, let us first recall that the natural surjective homomorphism $\Gamma_K \twoheadrightarrow \Gamma_K[M_{\mathrm{ss}}^{\circ}]$ *factors* through the natural surjective homomorphism $\Gamma_K \twoheadrightarrow \Gamma_K[M]$. Thus, to verify Claim 1.7.C, it suffices to verify that the kernel of the resulting surjective homomorphism $\Gamma_K[M] \twoheadrightarrow \Gamma_K[M_{\mathrm{ss}}^{\circ}]$ *coincides* with the normal subgroup $\Gamma_K^{\mathrm{wd}}[M]$ of $\Gamma_K[M]$. On the other hand, the inclusion $\mathrm{Ker}(\Gamma_K[M] \twoheadrightarrow \Gamma_K[M_{\mathrm{ss}}^{\circ}]) \subseteq \Gamma_K^{\mathrm{wd}}[M]$ follows immediately from Claim 1.7.B. Moreover, since the order of the group $\Gamma_K[M_{\mathrm{ss}}^{\circ}]$ is *prime to* p [cf. (a′)], the inclusion $\Gamma_K^{\mathrm{wd}}[M] \subseteq \mathrm{Ker}(\Gamma_K[M] \twoheadrightarrow \Gamma_K[M_{\mathrm{ss}}^{\circ}])$ holds. This completes the proof of Claim 1.7.C, hence also of Lemma 1.7. □

REMARK 1.7.1. — In the situation of Lemma 1.7, suppose, moreover, that the Γ_K-module M is *of strictly* p*-height two.* Then it follows from Remark 1.6.2, together with the proof of Lemma 1.7, that the subset $I_i \subseteq \{0, 1\}$ of (d) may be taken to be *of cardinality one* for each $i \in \{1, \ldots, r\}$.

LEMMA 1.8. — *There exist*

(a) *a finite quotient* $\Gamma_K \twoheadrightarrow Q$ *of* Γ_K*,*

(b) *an injective homomorphism* $\mathbb{F}_p^{\times} \hookrightarrow Q$ *of groups,*

(c) *a* Γ_K*-stable submodule* M° *of* M*, and*

(d) *decompositions* $M = M^{\circ} \oplus M(0)$ *and* $M^{\circ} = \bigoplus_{i=1}^{h_M} M(i)$

that satisfy the following four conditions:

(1) *The action of* Γ_K *on* M **factors** *through the finite quotient* $\Gamma_K \twoheadrightarrow Q$ *of* (a).

(2) *If one writes* $Q^{\mathrm{wd}} \subseteq Q$ *for the normal subgroup of* Q *obtained by forming the image of* $\Gamma_K^{\mathrm{wd}} \subseteq \Gamma_K$ *in* Q*, then the quotient* Q/Q^{wd} *is* **cyclic** *and* **of order** $\boldsymbol{q_M - 1}$.

(3) *The* Γ_K*-module* M° *is* **connected**.

(4) *Let us regard* M *as an* $\mathbb{F}_p^\times$*-module by the action of* $\mathbb{F}_p^\times$ *on* M *obtained by forming the composite*

$$\mathbb{F}_p^\times \hookrightarrow Q \longrightarrow \mathrm{Aut}(M)$$

— where the first arrow is the injective homomorphism of (b)*, and the second arrow is the homomorphism determined by the action of* Γ_K *on* M [*cf.* (1)]*. Then the decompositions* $M = M^\circ \oplus M(0)$ *and* $M^\circ = \bigoplus_{i=1}^{h_M} M(i)$ *of* (d) *are* $\mathbb{F}_{\boldsymbol{p}}^\times$**-stable**. *Moreover, for each* $i \in \{0, 1, \ldots, h_M\}$*, the resulting action of* $\mathbb{F}_p^\times$ *on* $M(i)$ **coincides** *with the action of* $\mathbb{F}_p^\times$ *on* $M(i)$ *obtained by forming the composite*

$$\mathbb{F}_p^\times \xrightarrow{a \mapsto a^i} \mathbb{F}_p^\times \xhookrightarrow{\text{multiplication}} \mathrm{Aut}\big(M(i)\big).$$

PROOF. — Write $H \subseteq \Gamma_K$ for the unique normal open subgroup of Γ_K *of index* $q_M - 1$, $\Gamma_K \twoheadrightarrow Q$ for the [necessarily finite] quotient of Γ_K by the normal open subgroup $\mathrm{Ker}(\Gamma_K \twoheadrightarrow \Gamma_K[M]) \cap H$ of Γ_K, and Q^{wd} for the normal subgroup of Q obtained by forming the image of $\Gamma_K^{\mathrm{wd}} \subseteq \Gamma_K$ in Q. Now we claim the following assertion:

> Claim 1.8.A: The action of Γ_K on M *factors* through the finite quotient $\Gamma_K \twoheadrightarrow Q$.

Indeed, this assertion follows from the definition of the finite quotient $\Gamma_K \twoheadrightarrow Q$.

Next, we claim the following assertion:

> Claim 1.8.B: The quotient Q/Q^{wd} is *cyclic* and *of order* $q_M - 1$.

Indeed, this assertion follows from the existence of (a) in the statement of Lemma 1.7, together with the definition of the finite quotient $\Gamma_K \twoheadrightarrow Q$.

Next, let us observe that since Q^{wd} is a *p-group*, which thus implies [cf. Claim 1.8.B] that Q is *solvable*, it follows from Claim 1.8.B that every prime-to-p Hall subgroup of Q determines a *splitting* of the natural surjective homomorphism $Q \twoheadrightarrow Q/Q^{\mathrm{wd}}$. In particular, an arbitrary prime-to-p Hall subgroup of Q yields a [necessarily injective] *lifting* $\mathbb{F}_{q_M}^\times \hookrightarrow Q$ of a surjective homomorphism $\mathbb{F}_{q_M}^\times \twoheadrightarrow \Gamma_K[M]/\Gamma_K^{\mathrm{wd}}[M]$ as in the existence of (a) in the statement of Lemma 1.7 [i.e., relative to the natural surjective homomorphism $Q \twoheadrightarrow \Gamma_K[M]/\Gamma_K^{\mathrm{wd}}[M]$ — cf. Claim 1.8.A]. Thus, since [it is immediate that] an arbitrary action of $\mathbb{F}_p^\times$ on a finite module annihilated by p is *semisimple*, we conclude immediately, by considering the injective homomorphism $\mathbb{F}_p^\times \hookrightarrow Q$ obtained by forming the composite of the natural inclusion $\mathbb{F}_p^\times \hookrightarrow \mathbb{F}_{q_M}^\times$ and a lifting $\mathbb{F}_{q_M}^\times \hookrightarrow Q$ as above, from Lemma 1.7 that Lemma 1.8 holds. This completes the proof of Lemma 1.8. □

LEMMA 1.9. — *Suppose that the* Γ_K*-module* M *is* **of strictly** $\boldsymbol{p}$**-height two**. *Then the image of the injective* [*cf. Remark* 1.1.1] *homomorphism* $\Gamma_K[M] \hookrightarrow \mathrm{Aut}(M)$ *determined by the action of* Γ_K *on* M **contains** *the subgroup* $\mathbb{F}_p^\times \subseteq \mathrm{Aut}(M)$ *of homotheties.*

PROOF. — Since M is *of strictly p-height two*, it follows immediately from Remark 1.7.1, together with the proof of Lemma 1.8, that the decomposition of (d) of Lemma 1.8 is given by $M = M(1)$. Thus, this assertion follows from condition (4) of Lemma 1.8. □

2. GALOIS MODULES ARISING FROM TORSION POINTS ON CURVES

In the present §2, we discuss Galois modules that arise from *torsion points* on curves. In the present §2, we maintain the notational conventions introduced in the discussion following Definition 1.3. Moreover, let $g \geq 2$ be an integer and X a curve over K [i.e., a scheme of dimension one that is projective, smooth, and geometrically connected over K] of genus g. Write J for the Jacobian variety of X. Write, moreover, $X_{\overline{K}} \stackrel{\text{def}}{=} X \times_K \overline{K}$ (respectively, $J_{\overline{K}} \stackrel{\text{def}}{=} J \times_K \overline{K}$).

DEFINITION 2.1.

(i) We shall write $X^{\text{cl}}_{\overline{K}}$ (respectively, $J^{\text{cl}}_{\overline{K}}$) for the set of closed points of $X_{\overline{K}}$ (respectively, $J_{\overline{K}}$).

(ii) Let $x \in X^{\text{cl}}_{\overline{K}}$ be a closed point of $X_{\overline{K}}$. Then we shall write $[x]$ for the prime divisor on $X_{\overline{K}}$ determined by x.

REMARK 2.1.1.

(i) We have a natural bijective map $X_{\overline{K}}(\overline{K}) \xrightarrow{\sim} X^{\text{cl}}_{\overline{K}}$ (respectively, $J_{\overline{K}}(\overline{K}) \xrightarrow{\sim} J^{\text{cl}}_{\overline{K}}$), which thus determines a natural action of Γ_K on the set $X^{\text{cl}}_{\overline{K}}$ (respectively, $J^{\text{cl}}_{\overline{K}}$).

(ii) We also have a natural injective map $X(K) \hookrightarrow X^{\text{cl}}_{\overline{K}}$ (respectively, $J(K) \hookrightarrow J^{\text{cl}}_{\overline{K}}$), that determines a bijective map $X(K) \xrightarrow{\sim} (X^{\text{cl}}_{\overline{K}})^{\Gamma_K}$ (respectively, $J(K) \xrightarrow{\sim} (J^{\text{cl}}_{\overline{K}})^{\Gamma_K}$) [cf. (i)].

DEFINITION 2.2. — We shall write $\text{Deg}(X_{\overline{K}})$ for the set consisting of the degrees of finite morphisms $X_{\overline{K}} \to \mathbb{P}^1_{\overline{K}}$ over $\overline{K}$.

Let us fix a K-rational point $x_0 \in X(K)$ of X. Write

$$\mathfrak{a} \colon X^{\text{cl}}_{\overline{K}} \hookrightarrow J^{\text{cl}}_{\overline{K}}$$

for the injective map determined by the *Albanese embedding* $X \hookrightarrow J$ with respect to $x_0 \in X(K)$. In particular, for each $x \in X^{\text{cl}}_{\overline{K}}$, the image $\mathfrak{a}(x)$ is the closed point of $J_{\overline{K}}$ that corresponds to the divisor $[x] - [x_0]$ of degree zero. Let x be a closed point of $X_{\overline{K}}$.

In the remainder of the present §2, suppose that k is *algebraically closed*, and that the following two conditions are satisfied:

(2A) The abelian variety J over K has *good reduction* over W.

(2B) The closed point $\mathfrak{a}(x) \in J^{\text{cl}}_{\overline{K}}$ is *torsion*.

Moreover, let $H \subseteq \Gamma_K$ be a normal closed subgroup of Γ_K.

DEFINITION 2.3.

(i) We shall write $M(x)$ for the [necessarily finite — cf. condition (2B)] Γ_K-stable submodule of $J^{\mathrm{cl}}_{\overline{K}}$ generated by $\mathfrak{a}(x)$.

(ii) We shall write $M(x, H) \subseteq M(x)$ for the [necessarily finite and Γ_K-stable] submodule of $M(x)$ generated by $\gamma_1(1-\delta)\gamma_2 \cdot \mathfrak{a}(x) \in M(x)$, where γ_1, γ_2 range over the elements of Γ_K, and δ ranges over the elements of H.

LEMMA 2.4. — *The following three conditions are equivalent:*

(1) *The residue field at the image, by the natural morphism $X_{\overline{K}} \to X$, of the closed point $x \in X^{\mathrm{cl}}_{\overline{K}}$ is* **contained** *in $\overline{K}^H$.*

(2) *The action of H on $M(x)$ is* **trivial**.

(3) *The* **equality** *$M(x, H) = \{0\}$ holds.*

PROOF. — This assertion is immediate. □

LEMMA 2.5. — *The following assertions hold:*

(i) *The Γ_K-module $M(x)$, hence also the Γ_K-module $M(x, \Gamma_K)$, is* **of type G**.

(ii) *The* **equality** *$M(x, H)[p] = M(x, H)$ holds.*

PROOF. — Assertion (i) follows from condition (2A). Assertion (ii) follows, in light of condition (2A), from [5, Theorem B], together with the definition of $M(x, H)$. □

Here, let us observe that it follows from Lemma 2.5 that the Γ_K-module $M(x, \Gamma_K)$ satisfies two conditions (1A), (1B) in the discussion following Definition 1.4.

In the remainder of the present §2, suppose, moreover, that the following condition is satisfied:

(2C) The action of Γ_K on $M(x)$ is *nontrivial*, and, moreover, the image of the injective [cf. Remark 1.1.1] homomorphism $\Gamma_K[M(x, \Gamma_K)] \hookrightarrow \mathrm{Aut}(M(x, \Gamma_K))$ determined by the action of Γ_K on $M(x, \Gamma_K)$ ($\neq \{0\}$ — cf. Lemma 2.4) *contains* the subgroup $\mathbb{F}_p^\times \subseteq \mathrm{Aut}(M(x, \Gamma_K))$ of homotheties [cf. Lemma 2.5, (ii)].

LEMMA 2.6. — *Let a be an element of $\mathbb{F}_p^\times \setminus \{1\}$ and γ_a an element of Γ_K whose action on $M(x, \Gamma_K)$ is given by multiplication by $a \in \mathbb{F}_p^\times$ [cf. condition (2C)]. Then there exists an element γ of Γ_K such that γ_a does* **not fix** *the closed point $\gamma \cdot x \in X^{\mathrm{cl}}_{\overline{K}}$.*

PROOF. — Since the action of γ_a on $M(x, \Gamma_K)$, hence also on $M(x)$, is *nontrivial*, this assertion is immediate. □

LEMMA 2.7. — *The following assertions hold:*

(i) *The* **equality** $p = 3$ *holds.*

(ii) *It holds that* $3 \in \mathrm{Deg}(X_{\overline{K}})$.

PROOF. — Let us begin the proof of Lemma 2.7 with the following claim:

> Claim 2.7.A: If either $p \neq 3$ or $3 \notin \mathrm{Deg}(X_{\overline{K}})$, then $2 \in \mathrm{Deg}(X_{\overline{K}})$, and the closed point $x \in X^{\mathrm{cl}}_{\overline{K}}$ is a *Weierstrass point* of $X_{\overline{K}}$.

Let us first verify Claim 2.7.A in the case where $p \neq 3$. Suppose that $p \neq 3$. Then since $p \neq 3$ [which thus implies that $-2 \neq 1$ in $\mathbb{F}_p$], it follows from condition (2C) and Lemma 2.6 that there exist elements γ_{-2}, γ of Γ_K such that the action of γ_{-2} on $M(x, \Gamma_K)$ is given by multiplication by -2, and, moreover, γ_{-2} does *not fix* the closed point $\gamma \cdot x \in X^{\mathrm{cl}}_{\overline{K}}$, i.e., $\gamma_{-2}\gamma \cdot x \neq \gamma \cdot x$. Then since $(1-\gamma_{-2})\gamma \cdot \mathfrak{a}(x) \in M(x)$ is *contained* in $M(x, \Gamma_K)$, it follows from our choice of $\gamma_{-2} \in \Gamma_K$ that the divisor $(2+\gamma_{-2})(1-\gamma_{-2})\gamma \cdot \mathfrak{a}(x)$ is *principal*, i.e., that the effective divisor $2[\gamma \cdot x]$ is *linearly equivalent* to the effective divisor $[\gamma_{-2}\gamma \cdot x] + [\gamma_{-2}^2\gamma \cdot x]$. Thus, since $\gamma_{-2}\gamma \cdot x \neq \gamma \cdot x$, we conclude that $2 \in \mathrm{Deg}(X_{\overline{K}})$, and the closed point $\gamma \cdot x$, hence also the closed point x, is a *Weierstrass point* of $X_{\overline{K}}$, as desired. This completes the proof of Claim 2.7.A in the case where $p \neq 3$.

Next, let us verify Claim 2.7.A in the case where $3 \notin \mathrm{Deg}(X_{\overline{K}})$. Suppose that $3 \notin \mathrm{Deg}(X_{\overline{K}})$. Let us first recall from condition (2C) that there exists an element $\gamma_2 \in \Gamma_K$ whose action on $M(x, \Gamma_K)$ is given by multiplication by 2. Next, let us observe that it follows from Lemma 2.4 that there exists an element $\delta \in \Gamma_K$ such that $(1-\delta)\cdot\mathfrak{a}(x) \in M(x)$ is *nonzero*, or, equivalently, $x \neq \delta \cdot x$. Then since $(1-\delta) \cdot \mathfrak{a}(x) \in M(x)$ is *contained* in $M(x, \Gamma_K)$, it follows from our choice of $\gamma_2 \in \Gamma_K$ that the divisor $(2-\gamma_2)(1-\delta) \cdot \mathfrak{a}(x)$ is *principal*, i.e., that the effective divisor $2[x] + [\gamma_2\delta \cdot x]$ is *linearly equivalent* to the effective divisor $2[\delta \cdot x] + [\gamma_2 \cdot x]$. Thus, since [we have assumed that] $3 \notin \mathrm{Deg}(X_{\overline{K}})$, and $x \neq \delta \cdot x$, we conclude that either $x = \gamma_2 \cdot x$ or $\gamma_2\delta \cdot x = \delta \cdot x$ holds, which thus implies that either

- the effective divisor $[x] + [\gamma_2\delta \cdot x]$ is *linearly equivalent* to the effective divisor $2[\delta \cdot x]$,

or

- the effective divisor $2[x]$ is *linearly equivalent* to the effective divisor $[\delta \cdot x] + [\gamma_2 \cdot x]$.

In particular, again by the fact that $x \neq \delta \cdot x$, we conclude that $2 \in \mathrm{Deg}(X_{\overline{K}})$, and, moreover, a Γ_K-conjugate of x, hence also x itself, is a *Weierstrass point* of $X_{\overline{K}}$, as desired. This completes the proof of Claim 2.7.A in the case where $3 \notin \mathrm{Deg}(X_{\overline{K}})$.

Assume that $p \neq 3$ or $3 \notin \mathrm{Deg}(X_{\overline{K}})$. Then it follows from Claim 2.7.A and [9, Proposition 3.1, (i)] that the action of Γ_K on $2 \cdot M(x)$ is *trivial*. Thus, since $p \neq 2$, it follows from Lemma 2.5, (i), together with [5, Remark 2.3.1, (ii)], that the action of Γ_K on $M(x)$ is *trivial*, in *contradiction* to condition (2C). This completes the proof of Lemma 2.7. □

LEMMA 2.8. — *Suppose that* $2 \notin \mathrm{Deg}(X_{\overline{K}})$. *Then the* Γ_K*-module* $M(x, \Gamma_K)$ *is* **isomorphic** *to the* Γ_K*-module* $\mathbb{F}_p(1)$*, where "(1)" denotes a Tate twist [i.e., the* Γ_K*-module obtained by forming the group of p-th roots of unity in* $\overline{K}$*].*

PROOF. — Let us first recall from condition (2C) that there exists an element $\gamma_{-1} \in \Gamma_K$ whose action on $M(x, \Gamma_K)$ is given by multiplication by -1.

Let δ be an element of Γ_K such that $\delta \cdot x \neq x$, or, equivalently, $(1-\delta) \cdot \mathfrak{a}(x) \in M(x)$ is *nonzero*. Then since $(1-\delta) \cdot \mathfrak{a}(x) \in M(x)$ is *contained* in $M(x, \Gamma_K)$, it follows from our choice of $\gamma_{-1} \in \Gamma_K$ that the divisor $(1+\gamma_{-1})(1-\delta) \cdot \mathfrak{a}(x)$ is *principal*, i.e., that the effective divisor $[x] + [\gamma_{-1} \cdot x]$ is *linearly equivalent* to the effective divisor $[\delta \cdot x] + [\gamma_{-1}\delta \cdot x]$. Thus, since [we have assumed that] $2 \notin \mathrm{Deg}(X_{\overline{K}})$, and $\delta \cdot x \neq x$, it follows that $\delta \cdot x = \gamma_{-1} \cdot x$. In particular, we conclude that the equality $\Gamma_K \cdot x = \{x, \gamma_{-1} \cdot x\}$ holds. Thus, it follows from the definition of $M(x, \Gamma_K)$ that the module $M(x, \Gamma_K)$ is, as an abstract module, generated by the *single* element $(1-\gamma_{-1}) \cdot \mathfrak{a}(x) \in M(x, \Gamma_K)$. In particular, it follows immediately — in light of Lemma 1.6 — from condition (2C) that the Γ_K-module $M(x, \Gamma_K)$ is *isomorphic* to $\mathbb{F}_p(1)$, as desired. This completes the proof of Lemma 2.8. □

3. Ramified Torsion Points on Curves with Superspecial Reduction

In the present §3, we prove the main result of the present paper [cf. Corollary 3.3 below]. In the present §3, we maintain the notational conventions introduced at the beginning of the preceding §2 and in the discussion following Definition 2.2.

THEOREM 3.1. — *Suppose that k is* **algebraically closed**. *Suppose, moreover, that two conditions* (2A), (2B) *in the discussion following Definition* 2.2 *and condition* (2C) *in the discussion following Lemma* 2.5 *are satisfied. Then the* **equality** $p = 3$ *holds. Moreover, one of the following two conditions is satisfied:*

(a) *The curve X over K is* **of genus two**.

(b) *The Γ_K-module $M(x, \Gamma_K)$ is* **isomorphic** *to the Γ_K-module $\mathbb{F}_p(1)$, where "(1)" denotes a Tate twist.*

PROOF. — Let us first observe that it follows from Lemma 2.7, (i), that $p = 3$. Suppose that condition (b) is *not satisfied*. Then it follows from Lemma 2.7, (ii), and Lemma 2.8 that $\{2, 3\} \subseteq \mathrm{Deg}(X_{\overline{K}})$. In particular, it follows from [1, Chapter I, Exercise D-9] that $g = 2$, as desired. This completes the proof of Theorem 3.1. □

COROLLARY 3.2. — *Suppose that the following four conditions are satisfied:*

(1) *The abelian variety J over K has* **good reduction** *over W.*

(2) *The closed point $\mathfrak{a}(x) \in J^{\mathrm{cl}}_{\overline{K}}$ is* **torsion**.

(3) *The natural action of the inertia subgroup of Γ_K on $J(\overline{K})[p]$ is* **of strictly *p*-height two**.

(4) *Either $p > 3$ or $g > 2$.*

Then the residue field at the image, by the natural morphism $X_{\overline{K}} \to X$, of the closed point $x \in X^{\mathrm{cl}}_{\overline{K}}$ is **unramified** *over K.*

PROOF. — Let us first observe that, to verify Corollary 3.2, we may assume without loss of generality, by replacing K by the p-adic completion of the unique maximal unramified extension of K in $\overline{K}$, that k is *algebraically closed*. Then this assertion follows immediately, in light of Lemma 2.4, from Theorem 3.1, together with Lemma 1.9. $\square$

The main result of the present paper is as follows.

COROLLARY 3.3. — *Suppose that the following two conditions are satisfied:*

(1) *The closed point* $\mathfrak{a}(x) \in J^{\mathrm{cl}}_{\overline{K}}$ *is* **torsion**.

(2) *Either* $p > 3$ *or* $g > 2$.

Suppose, moreover, that one of the following two conditions is satisfied:

(a) *The abelian variety* J *over* K *has* **good reduction** *over* W. *Moreover, the special fiber of the good model of* J *is a* **superspecial** *abelian variety over* k [*i.e., is isomorphic to the fiber product of finitely many* **supersingular** *elliptic curves over* k].

(b) *For each* $i \in \{1, \ldots, g\}$, *there exists an elliptic curve* E_i *over* W *such that* $E_i \times_W k$ *is* **supersingular**, *and, moreover, the abelian variety* J *is* **isogenous** *to* $(E_1 \times_W \cdots \times_W E_g) \times_W K$ *over* K.

Then the residue field at the image, by the natural morphism $X_{\overline{K}} \to X$, *of the closed point* $x \in X^{\mathrm{cl}}_{\overline{K}}$ *is* **unramified** *over* K.

PROOF. — Each of conditions (a) and (b) implies immediately condition (1) in the statement of Corollary 3.2. Condition (1) implies condition (2) in the statement of Corollary 3.2. Condition (2) implies condition (4) in the statement of Corollary 3.2. Thus, it follows from Corollary 3.2 that, to complete the verification of Corollary 3.3, it suffices to verify that each of conditions (a) and (b) implies condition (3) in the statement of Corollary 3.2. On the other hand, it follows immediately — in light of the discussion given in [8, §3.4, Exemple] — from the main theorem of [6] (respectively, the various definitions involved) that condition (a) (respectively, (b)) implies condition (3) in the statement of Corollary 3.2, as desired. This completes the proof of Corollary 3.3. $\square$

REMARK 3.3.1.

(i) Let us recall that it follows from [7, Corollary 1.2], together with the well-known *finiteness* of the set of isomorphism classes of supersingular elliptic curves over k, that the set of isomorphism classes of curves over k of genus g whose Jacobian varieties are *superspecial* is *finite*. Moreover, it follows from [4, §2, Theorem 1.1] that there is *no curve* over k of genus g whose Jacobian variety is *superspecial* whenever $2g > p^2 - p$. Thus, one may conclude that curves over k whose Jacobian varieties are *superspecial* are "*few*". On the other hand, a curve over K subject to Theorem B [i.e., of the Introduction] in the case where condition (S) is satisfied is a curve over K obtained as the generic fiber of [the algebraization of] a deformation to W of such a curve over k. In particular, one may also conclude that curves over K subject to Theorem B in the case where condition (S) is satisfied are "*few*".

(ii) Suppose that $g > 2$. Then one verifies immediately, by considering, for instance, stable curves [cf. [3], Definition 1.1] over k whose dual graphs are *trees* and whose irreducible components are *supersingular elliptic curves* over k, that there are *infinitely many* isomorphism classes of stable curves over k of genus g whose Jacobian varieties are *superspecial abelian varieties* [even if the inequality $2g > p^2 - p$ holds]. Moreover, a curve over K obtained as the generic fiber of [the algebraization of] a generically smooth deformation to W of such a stable curve over k satisfies condition (a) in the statement of Corollary 3.3. In particular, one may conclude that "*many*" curves over K may be thought to be subject to Corollary 3.3.

REFERENCES

[1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris: Geometry of algebraic curves. Vol. I. Grundlehren der Mathematischen Wissenschaften, **267**. *Springer-Verlag, New York*, 1985.

[2] R. F. Coleman: Ramified torsion points on curves. *Duke Math. J.* **54** (1987), no. **2**, 615-640.

[3] P. Deligne and D. Mumford: The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math.* No. **36** (1969), 75-109.

[4] T. Ekedahl: On supersingular curves and abelian varieties. *Math. Scand.* **60** (1987), no. **2**, 151-178.

[5] Y. Hoshi: On ramified torsion points on a curve with stable reduction over an absolutely unramified base. *Osaka J. Math.* **54** (2017), no. **4**, 767-787.

[6] Y. Hoshi: Pseudo-rigid p-torsion finite flat commutative group schemes. to appear in *J. Number Theory*.

[7] M. S. Narasimhan and M. V. Nori: Polarisations on an abelian variety. *Proc. Indian Acad. Sci. Math. Sci.* **90** (1981), no. **2**, 125-128.

[8] M. Raynaud: Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France* **102** (1974), 241-280.

[9] A. Tamagawa: Ramification of torsion points on curves with ordinary semistable Jacobian varieties. *Duke Math. J.* **106** (2001), no. **2**, 281-319.

(Yuichiro Hoshi) RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES, KYOTO UNIVERSITY, KYOTO 606-8502, JAPAN

Email address: `yuichiro@kurims.kyoto-u.ac.jp`