

RIMS-1841

**On Ramified Torsion Points on a Curve with Stable
Reduction over an Absolutely Unramified Base**

By

Yuichiro HOSHI

December 2015



京都大学 数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

ON RAMIFIED TORSION POINTS ON A CURVE WITH STABLE REDUCTION OVER AN ABSOLUTELY UNRAMIFIED BASE

YUICHIRO HOSHI

DECEMBER 2015

ABSTRACT. — Let p be an odd prime number, W an *absolutely unramified* p -adically complete discrete valuation ring with algebraically closed residue field, and X a curve of genus at least two over the field of fractions K of W . In the present paper, we study, under the assumption that X has *stable reduction* over W , *torsion points on X* , i.e., torsion points of the Jacobian variety J of X which lie on the image of the Albanese embedding $X \hookrightarrow J$ with respect to a K -rational point of X . A consequence of the main result of the present paper is that if, moreover, J has good reduction over W , then every torsion point on X is *K -rational after multiplying p* . This result is closely related to a conjecture of *R. Coleman* concerning the ramification of torsion points. For instance, this result leads us to a solution of the conjecture in the case where a given curve is hyperelliptic and of genus at least p .

CONTENTS

INTRODUCTION	1
§0. NOTATIONS AND CONVENTIONS	4
§1. LEVEL AND RAMIFICATION OF FINITE FLAT COMMUTATIVE GROUP SCHEMES	5
§2. GALOIS MODULES OF TYPE S	10
§3. RAMIFIED TORSION POINTS ON CURVES	15
REFERENCES	20

INTRODUCTION

Throughout the present paper, let p be an odd prime number and k an algebraically closed field of characteristic p . Write $W \stackrel{\text{def}}{=} W(k)$ for the ring of Witt vectors with coefficients in k and K for the field of fractions of W . Let \overline{K} be an algebraic closure of K . Write $K^{\text{tm}} \subseteq \overline{K}$ for the maximal tamely ramified extension of K in \overline{K} and $\Gamma_K \stackrel{\text{def}}{=} \text{Gal}(\overline{K}/K)$ for the absolute Galois group of K determined by the algebraic closure \overline{K} . Let $g \geq 2$ be an integer and X a curve over K [i.e., a scheme of dimension one which is projective, smooth, and geometrically connected over K] of genus g . Write J for the Jacobian variety of X . In the present paper, suppose that

2010 MATHEMATICS SUBJECT CLASSIFICATION. — Primary 14H25; Secondary 11G20, 14H40, 14H55, 14L15, 11S15.

KEY WORDS AND PHRASES. — curve, ramified torsion point.

the curve X over K has *stable reduction* over W , which thus implies that the abelian variety J over K has *semistable reduction* over W .

Write, moreover, $X_{\overline{K}} \stackrel{\text{def}}{=} X \times_K \overline{K}$, $J_{\overline{K}} \stackrel{\text{def}}{=} J \times_K \overline{K}$, and $X_{\overline{K}}^{\text{cl}}, J_{\overline{K}}^{\text{cl}}$ for the sets of closed points of $X_{\overline{K}}, J_{\overline{K}}$, respectively. Thus, we have natural bijections $X_{\overline{K}}(\overline{K}) \xrightarrow{\sim} X_{\overline{K}}^{\text{cl}}, J_{\overline{K}}(\overline{K}) \xrightarrow{\sim} J_{\overline{K}}^{\text{cl}}$, which thus determine natural actions of Γ_K on $X_{\overline{K}}^{\text{cl}}, J_{\overline{K}}^{\text{cl}}$, respectively.

Let $x_0 \in X(K)$ be a K -rational point of X . Then we have 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 “ x ” to the invertible sheaf corresponding to the divisor “[x] – [x_0]” — where we write “[$-$]” for the prime divisor determined by “($-$)” — of degree zero. By this embedding, we have an injection

$$\varphi_{x_0}: X_{\overline{K}}^{\text{cl}} \hookrightarrow J_{\overline{K}}^{\text{cl}}.$$

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 φ_{x_0} for some $x_0 \in X(K)$, is a torsion point in $J_{\overline{K}}^{\text{cl}}$. In particular, in the present paper, we study a *ramified torsion point* on $X_{\overline{K}}$, i.e., a non- K -rational torsion point on $X_{\overline{K}}$ [cf. Definition 3.5, (i)].

In Introduction, let us consider the following situation:

(\dagger): Let $x_0 \in X(K)$ be a K -rational point of X . By means of the above injection $\varphi_{x_0}: X_{\overline{K}}^{\text{cl}} \hookrightarrow J_{\overline{K}}^{\text{cl}}$, we regard $X_{\overline{K}}^{\text{cl}}$ as a subset of $J_{\overline{K}}^{\text{cl}}$. Let $x \in X_{\overline{K}}^{\text{cl}}$ ($\subseteq J_{\overline{K}}^{\text{cl}}$) be a closed point of $X_{\overline{K}}$. Suppose that $x \in J_{\overline{K}}^{\text{cl}}$ is *torsion*.

Let us first recall that, in [4], *R. Coleman* stated a conjecture concerning the *ramification of torsion points* on a curve which satisfies certain conditions [cf. [4], Conjecture B]. The following is the statement of a slightly stronger version of the conjecture. Note that the *original* conjecture of Coleman is the following conjecture in the case where the pair (X, x_0) can be descended to a subfield of K which is *finite over the field of rational numbers*.

CONJECTURE (Coleman). — *In the situation (\dagger), suppose, moreover, that the following two conditions are satisfied:*

- (1) *It holds that $p \geq 5$.*
- (2) *The curve X , hence also the abelian variety J , over K has **good reduction** over W .*

*Then $x \in J_{\overline{K}}^{\text{cl}}$ is **K-rational**. In other words, there is **no ramified torsion point** on $X_{\overline{K}}$.*

Moreover, Coleman essentially proved the following result concerning the above conjecture [cf. [4], Corollary 20.2]:

THEOREM (Coleman). — *In the situation of Conjecture, suppose, moreover, that one of the following three conditions is satisfied:*

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

(b) *The special fiber of the good model of J is isomorphic to the direct product of supersingular elliptic curves over k .*

(c) *It holds that $2g < p$.*

*Then $x \in J_K^{\text{cl}}$ is **K-rational**.*

Next, let us recall that *A. Tamagawa* studied, in [13], the ramification of torsion points in the case where the abelian variety-part of the special fiber of the semistable model of J is an *ordinary* abelian variety. Tamagawa proved, for instance, the following result [cf. [13], Theorem 0.1]:

THEOREM (Tamagawa). — *In the situation (\ddagger) , suppose, moreover, that the following three conditions are satisfied:*

(1) *It holds that $p \geq 29$.*

(2) *The abelian variety-part of the special fiber of the semistable model of J is an **ordinary** abelian variety over k .*

(3) *The curve X over K is **not hyperelliptic**.*

*Then $x \in J_K^{\text{cl}}$ is **K-rational**.*

In the present paper, by combining the idea of Tamagawa that was applied in [13] with the study of the Galois representations associated to *finite flat commutative group schemes*, we prove the following result [cf. Theorem 3.4]. This result concerns the ramification of torsion points *after multiplying p* without any assumption on the reduction of J .

THEOREM A. — *In the situation (\ddagger) , it holds that $p \cdot x \in J_K^{\text{cl}}$ is **Ktm-rational**.*

In the case where J has *good reduction* over W , we obtain the following result [cf. Theorem 3.4, (ii)]:

THEOREM B. — *In the situation (\ddagger) , if, moreover, the abelian variety J over K has **good reduction** over W , then $p \cdot x \in J_K^{\text{cl}}$ is **K-rational**.*

In §3 of the present paper, by means of Theorems A and B, we study the geometry of curves which admit *ramified torsion* points. As one of consequences, we prove the following *nonexistence of ramified torsion points* [cf. Corollary 3.6]:

THEOREM C. — *In the situation (\ddagger) , suppose that the following two conditions are satisfied:*

(1) *It holds that $g \geq p$.*

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

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

- (a) The curve $X_{\overline{K}}$ over \overline{K} is **hyperelliptic** [i.e., of gonality 2].
- (b) The curve $X_{\overline{K}}$ over \overline{K} is of gonality $> p$.
- (c) Every **Weierstrass point** of $X_{\overline{K}}$ is **K -rational**.

Then $x \in J_{\overline{K}}^{\text{cl}}$ is **K -rational**. In other words, there is **no ramified torsion point** on $X_{\overline{K}}$.

Note that Theorem C yields some *conditional results* of the above conjecture of Coleman. Indeed, by, for instance, Theorem C in the case where the condition (a) is satisfied, we conclude that the conjecture of Coleman holds if X is *hyperelliptic* and of genus $\geq p$ [cf. also Remark 3.6.1].

The present paper is organized as follows: In §1, we consider the Galois representations associated to finite flat commutative group schemes. In particular, we discuss the relationship between the *level* of a finite flat commutative group scheme over W [cf. Definition 1.2, (i)] and the *ramification* of the Galois representation associated to the finite flat commutative group scheme [cf. Proposition 1.8, Lemma 1.9]. In §2, we consider a *Galois module of type S* [cf. Definition 2.3, (i)], i.e., a Γ_K -module which is isomorphic to a finite Γ_K -submodule of the Γ_K -module obtained by considering torsion points of an abelian variety with semistable model over W . In particular, we prove the *triviality* of the Galois action on a subquotient of a Galois module of type S which satisfies a technical condition [cf. Lemma 2.7]. In §3, we prove the main result of the present paper [cf. Theorem 3.4], which is closely related to the above conjecture due to Coleman [cf. Remark 3.4.1]. Moreover, by means of the main result, we study the geometry of curves which admit *ramified torsion points* [cf. Corollary 3.6, Corollary 3.8, Corollary 3.9].

ACKNOWLEDGMENTS

The author would like to thank *Akio Tamagawa* for comments concerning the content of Remark 1.9.1, (ii), and a refinement of an earlier version of Corollary 3.9, (i) [i.e., the content of the present version of Corollary 3.9, (i)]. This research was supported by JSPS KAKENHI Grant Number 15K04780.

0. NOTATIONS AND CONVENTIONS

GROUPS. — Let G be a group and S a set on which G acts. Then we shall write $S^G \subseteq S$ for the subset of S of G -invariants, $G^S \subseteq G$ for the [necessarily normal and uniquely determined] maximal subgroup of G which acts on S trivially, and $G[S] \stackrel{\text{def}}{=} G/G^S$. Thus, the action of G on S factors through the natural surjection $G \rightarrow G^S$, and, moreover, the resulting action of G^S on S is *faithful*.

MODULES. — Let M be a module, $n \geq 0$ an integer, and l a prime number. Then we shall write $\text{Aut}(M)$ for the group of automorphisms of the module M , $M[n] \subseteq M$ for the submodule of M obtained by forming the kernel of the endomorphism of M given

by multiplication by n , and $M_l \stackrel{\text{def}}{=} \bigcup_{i \geq 1} M[l^i] \subseteq M$. If, moreover, M is *finite*, then we shall write $M_{\neq l} \subseteq M$ for the submodule of M generated by elements of the $M_{l'}$'s, where l' ranges over the prime numbers such that $l' \neq l$. Thus, if M is *finite*, then we have a natural decomposition $M = M_l \oplus M_{\neq l}$.

Let G be a group and M a G -module. Then we shall say that an element $x \in M$ of M is a *weak G -invariant* if, for every $\gamma, \delta \in G$, the following holds: If $(1 - \gamma)^2(\delta \cdot x) = 0$, then $(1 - \gamma)(\delta \cdot x) = 0$. [Thus, if $x \in M$ is a G -invariant, then $x \in M$ is a *weak G -invariant*.]

VARIETIES. — Let k be a field. Then we shall say that a scheme over k is a *variety* over k if the scheme is separated and of finite type over k .

Let V be a variety over k and \bar{k} an algebraic closure of k . Then we shall write $V_{\bar{k}} \stackrel{\text{def}}{=} V \times_k \bar{k}$ for the variety over \bar{k} determined by V and $V_{\bar{k}}^{\text{cl}}$ for the set of closed points of $V_{\bar{k}}$. Thus, if k is *perfect*, then we have a natural bijection $V_{\bar{k}}(\bar{k}) \xrightarrow{\sim} V_{\bar{k}}^{\text{cl}}$, which thus determines a natural action of $\text{Gal}(\bar{k}/k)$ on $V_{\bar{k}}^{\text{cl}}$; moreover, the natural injection $V(k) \hookrightarrow V_{\bar{k}}(\bar{k})$ from the set $V(k)$ of k -rational points of V determines a bijection $V(k) \xrightarrow{\sim} (V_{\bar{k}}^{\text{cl}})^{\text{Gal}(\bar{k}/k)}$.

CURVES. — Let k be a field. Then we shall say that a scheme over k is a *curve* over k if the scheme is of dimension one and, moreover, projective, smooth, and geometrically connected over k . Thus, a curve over k is a variety over k .

Let C be a curve over k and $g \geq 0$ an integer. We shall say that C is of *genus g* if $H^1(C, \mathcal{O}_C)$ is of dimension g over k . We shall say that C is of *gonality g* if the minimum among the degrees of finite morphisms from C to curves of genus zero over k is equal to g .

Suppose that the curve C is of genus $g \geq 2$, and that the field k is of characteristic zero. Let \bar{k} be an algebraic closure of k , $c \in C_{\bar{k}}^{\text{cl}}$, and $n \geq 0$ an integer. We shall say that the integer n is a *Weierstrass non-gap* at $c \in C_{\bar{k}}^{\text{cl}}$ if there exists a section of $\mathcal{O}_{C_{\bar{k}}}$ on $C_{\bar{k}} \setminus \{c\}$ of order $-n$ at c [i.e., the integer n contains the Weierstrass monoid of $C_{\bar{k}}$ at $c \in C_{\bar{k}}^{\text{cl}}$]. We shall say that $c \in C_{\bar{k}}^{\text{cl}}$ is a *Weierstrass point* of $C_{\bar{k}}$ if there exists an integer $1 \leq i \leq g$ such that i is a Weierstrass non-gap at $c \in C_{\bar{k}}^{\text{cl}}$. Note that, as is well-known [cf., e.g., [1], Chapter I, Exercises E-8, (ii), and E-9], if we write N for the number of Weierstrass points of $C_{\bar{k}}$, then it holds that $2g + 2 \leq N \leq g^3 - g$. We shall say that the pair (C, c) is *exceptional* [cf. [13], Definition in the discussion entitled “Weierstrass points on hyperelliptic curves”] if 2 is a Weierstrass non-gap at $c \in C_{\bar{k}}^{\text{cl}}$ [i.e., $C_{\bar{k}}$ is hyperelliptic, and the hyperelliptic involution of $C_{\bar{k}}$ is ramified at $c \in C_{\bar{k}}^{\text{cl}}$].

1. LEVEL AND RAMIFICATION OF FINITE FLAT COMMUTATIVE GROUP SCHEMES

In the present §1, we consider the Galois representations associated to finite flat commutative group schemes. In particular, we discuss the relationship between the *level* of a finite flat commutative group scheme [cf. Definition 1.2, (i), below] and the *ramification* of the Galois representation associated to the finite flat commutative group scheme [cf. Proposition 1.8, Lemma 1.9, below].

In the present §1, let p be an odd prime number and k an algebraically closed field of characteristic p . Write $W \stackrel{\text{def}}{=} W(k)$ for the ring of Witt vectors with coefficients in k

and K for the field of fractions of W . Let \overline{K} be an algebraic closure of K and $L \subseteq \overline{K}$ a(n) [possibly infinite] algebraic extension of K . Write $\Gamma_L \stackrel{\text{def}}{=} \text{Gal}(\overline{K}/L)$ for the absolute Galois group of L determined by the algebraic closure \overline{K} , v_0 for the [uniquely determined] p -adic valuation on \overline{K} such that $v_0(p) = 1$, and $\overline{W} \subseteq \overline{K}$, $V \subseteq L$ for the rings of integers of \overline{K} , L , respectively.

DEFINITION 1.1.

(i) Let M be a V -module which is *annihilated* by a power of p . Then we shall write

$$\text{lv}_V(M) \stackrel{\text{def}}{=} v_0(\text{Ann}_V(M)).$$

(ii) Suppose that $[L : K] < \infty$. Then we shall write

$$\text{lv}^\Omega(L/K) \stackrel{\text{def}}{=} \text{lv}_V(\Omega_{V/W}^1).$$

Thus, it follows that

$$\text{lv}^\Omega(L/K) = v_0(\delta_{L/K})$$

— where we write $\delta_{L/K}$ for the different of the finite extension L/K .

In the remainder of the present §1, let G be a *finite flat commutative group scheme* over W which is *annihilated* by a power of p . Thus, we have an exact sequence of finite flat commutative group schemes over W

$$0 \longrightarrow G^\circ \longrightarrow G \longrightarrow G^{\text{ét}} \longrightarrow 0$$

— where $G^\circ \subseteq G$ is *connected*, and $G^{\text{ét}}$ is *étale* over W . Write $K_G \subseteq \overline{K}$ for the [necessarily finite Galois] extension of K corresponding to the kernel of the natural action of Γ_K on $G(\overline{K})$ — i.e., the finite Galois extension of K corresponding to the quotient $\Gamma_K \twoheadrightarrow \Gamma_K[G(\overline{K})]$ — and $W_G \subseteq K_G$ for the ring of integers of K_G .

DEFINITION 1.2.

(i) We shall write

$$\text{lv}(G) \stackrel{\text{def}}{=} \text{lv}_W(G(\overline{K}) \otimes_{\mathbb{Z}_p} W) \quad (\in \mathbb{Z})$$

and refer to $\text{lv}(G)$ as the *level* of G .

(ii) Let M be a W -module. Then we shall write

$$t_G^*(M) \stackrel{\text{def}}{=} (e_G^* \Omega_{G/W}^1) \otimes_W M$$

— where we write e_G for the identity section of G/W — and

$$t_G(M) \stackrel{\text{def}}{=} \text{Hom}_W(t_G^*(W), M).$$

We shall refer to $t_G^*(M)$ (respectively, $t_G(M)$) as the M -valued *cotangent* (respectively, *tangent*) space of G/W . Note that since G is *étale over* K , it follows that $t_G^*(M)$, hence also $t_G(M)$, is *annihilated* by a power of p .

(iii) We shall write

$$\text{lv}^\Omega(G) \stackrel{\text{def}}{=} \text{lv}_W(t_G^*(W)).$$

(iv) Suppose that L is *Galois* over K , and that $K_G \subseteq L$. [So $G(\overline{W}) = G(V)$]. Then we shall define a homomorphism of \overline{W} -modules

$$\text{ev}_L: G(\overline{W}) \otimes_{\mathbb{Z}_p} \overline{W} = G(V) \otimes_{\mathbb{Z}_p} \overline{W} \longrightarrow t_G(\Omega_{V/W}^1 \otimes_V \overline{W})$$

as follows [cf. [7], §4.7]: Let $x \in G(V)$ be a V -valued point of G . Then, by considering the operation of restricting differential forms on G over W to x , we obtain a homomorphism $t_G^*(W) \rightarrow \Omega_{V/W}^1$, hence also a homomorphism of W -modules

$$e_x: t_G^*(W) \longrightarrow \Omega_{V/W}^1 \otimes_V \overline{W}.$$

Thus, the assignment “ $x \mapsto e_x$ ” determines a map

$$G(V) \longrightarrow t_G(\Omega_{V/W}^1 \otimes_V \overline{W}).$$

Now since [one verifies easily that] this map is a homomorphism of \mathbb{Z}_p -modules, this map determines the homomorphism ev_L as above.

REMARK 1.2.1. — Thus, it holds that $t_G^* \leq \text{lv}^\Omega(G)$ and $t_G^* \not\leq \text{lv}^\Omega(G)$ [cf. [9], Definition 1.3, (ii)]. If, moreover, G is of *p-rectangle-type* [cf. [9], Definition 2.1, (ii)], then $\text{lv}(G)$ of Definition 1.2, (i), *coincides* with $\text{lv}(G)$ of [9], Definition 2.1, (ii).

THEOREM 1.3 (Fontaine). — *The following hold:*

(i) *The \overline{W} -module $\text{Coker}(\text{ev}_{\overline{K}})$ is **annihilated** by a power of p . Moreover, it holds that*

$$\text{lv}_{\overline{W}}(\text{Coker}(\text{ev}_{\overline{K}})) \leq \frac{1}{p-1}.$$

(ii) *It holds that*

$$\text{lv}^\Omega(K_G/K) < \text{lv}(G) + \frac{1}{p-1}.$$

PROOF. — Assertion (i) follows from [7], Corollaire to Théorème 3. Assertion (ii) follows from [8], Corollaire to Théorème A. \square

PROPOSITION 1.4. — *It holds that*

$$\text{lv}^\Omega(G) \leq \text{lv}^\Omega(K_G/K) + \frac{1}{p-1}.$$

PROOF. — Let us first observe that we have a commutative diagram of \overline{W} -modules

$$\begin{array}{ccc} G(K_G) \otimes_{\mathbb{Z}_p} \overline{W} & \xlongequal{\quad} & G(\overline{W}) \otimes_{\mathbb{Z}_p} \overline{W} \\ \text{ev}_{K_G} \downarrow & & \text{ev}_{\overline{K}} \downarrow \\ t_G(\Omega_{W_G/W}^1 \otimes_{W_G} \overline{W}) & \longrightarrow & t_G(\Omega_{\overline{W}/W}^1) \end{array}$$

— where the lower horizontal arrow is *injective* [cf., e.g., [7], Lemma 4]. Thus, it follows from Theorem 1.3, (i), that

$$\text{lv}_{\overline{W}}(\text{Coker}(t_G(\Omega_{W_G/W}^1 \otimes_{W_G} \overline{W}) \hookrightarrow t_G(\Omega_{\overline{W}/W}^1))) \leq \frac{1}{p-1}.$$

In particular, we conclude that

$$\mathrm{lv}_{\overline{W}}(t_G(\Omega_{\overline{W}/W}^1)) \leq \mathrm{lv}^\Omega(K_G/K) + \frac{1}{p-1}.$$

Finally, let us observe that it follows immediately from [7], Corollaire 1, (1), that

$$\mathrm{lv}_{\overline{W}}(t_G(\Omega_{\overline{W}/W}^1)) = \mathrm{lv}^\Omega(G).$$

This completes the proof of Proposition 1.4. \square

THEOREM 1.5 (Raynaud). — *Every homomorphism over K between the generic fibers [i.e., the results of base-changing via $W \hookrightarrow K$] of finite flat commutative group schemes over W **uniquely extends** to a homomorphism between the original finite flat commutative group schemes over W . Moreover, the kernel of the resulting homomorphism between the original finite flat commutative group schemes over W is **flat** over W .*

PROOF. — This follows from [11], Corollaire 3.3.6, (1). \square

LEMMA 1.6. — *Let $n \geq 0$ be an integer. Write $G[p^n] \subseteq G$ for the finite flat commutative group scheme over W obtained by forming the kernel of the endomorphism of G given by multiplication by p^n [cf. Theorem 1.5]. Then the exact sequence of finite flat commutative group schemes over W*

$$0 \longrightarrow G[p^n] \longrightarrow G \longrightarrow G/G[p^n] \longrightarrow 0$$

determines a commutative diagram of W -modules

$$\begin{array}{ccccccc} 0 & \longrightarrow & t_{G/G[p^n]}^*(W) & \longrightarrow & t_G^*(W) & \longrightarrow & t_{G[p^n]}^*(W) & \longrightarrow & 0 \\ & & \wr \downarrow & & \parallel & & \wr \downarrow & & \\ 0 & \longrightarrow & p^n \cdot t_G^*(W) & \longrightarrow & t_G^*(W) & \longrightarrow & t_G^*(W) \otimes_W W/p^n & \longrightarrow & 0 \end{array}$$

— where the horizontal sequences are exact, and the vertical arrows are isomorphisms.

PROOF. — Let us observe that one verifies immediately that the exact sequence of finite flat commutative group schemes over W

$$0 \longrightarrow G[p^n] \longrightarrow G \xrightarrow{p^n} G$$

determines an exact sequence

$$t_G^*(W) \xrightarrow{p^n} t_G^*(W) \longrightarrow t_{G[p^n]}^*(W) \longrightarrow 0,$$

which thus determines an isomorphism

$$t_G^*(W) \otimes_W W/p^n \xrightarrow{\sim} t_{G[p^n]}^*(W).$$

Thus, Lemma 1.6 follows from [9], Lemma 1.6. This completes the proof of Lemma 1.6. \square

PROPOSITION 1.7. — *It holds that*

$$\mathrm{lv}^\Omega(G) = \mathrm{lv}(G^\circ).$$

PROOF. — Write $n \stackrel{\text{def}}{=} \text{lv}(G^\circ)$. Then it follows from a similar conclusion to the conclusion “ $t_G^* \leq \text{lv}(G)$ ” of [9], Lemma 2.3 [cf. also Remark 1.2.1 of the present paper], that, to verify Proposition 1.7, it suffices to verify that $p^{n-1} \cdot t_G^*(W) \neq \{0\}$. To this end, assume that $p^{n-1} \cdot t_G^*(W) = \{0\}$. Then it follows from Lemma 1.6 that $t_{G/G[p^{n-1}]}^*(W) = \{0\}$, which thus implies that $G/G[p^{n-1}]$ is *étale* over W . Thus, the composite $G^\circ \hookrightarrow G \twoheadrightarrow G/G[p^{n-1}]$ is *trivial*, i.e., $G^\circ \subseteq G[p^{n-1}]$ — which *contradicts* our assumption that $\text{lv}(G^\circ) = n$. This completes the proof of Proposition 1.7. \square

PROPOSITION 1.8. — *It holds that*

$$\text{lv}(G^\circ) - \frac{1}{p-1} \leq \text{lv}^\Omega(K_G/K) < \text{lv}(G) + \frac{1}{p-1}.$$

PROOF. — This follows from Theorem 1.3, (ii); Proposition 1.4, together with Proposition 1.7. \square

The following result is the main result of the present §1:

LEMMA 1.9. — *Let H be a finite flat commutative group scheme over W . Suppose that $K_H \subseteq K_G$ [cf. the notation introduced in the discussion preceding Definition 1.2]. Then it holds that*

$$\text{lv}(H^\circ) \leq \text{lv}(G).$$

PROOF. — It follows from Proposition 1.8, together with our assumption, that

$$\text{lv}(H^\circ) - \frac{1}{p-1} \leq \text{lv}^\Omega(K_H/K) \leq \text{lv}^\Omega(K_G/K) < \text{lv}(G) + \frac{1}{p-1}.$$

Thus, since [we have assumed that] $p \geq 3$, it holds that $\text{lv}(H^\circ) \leq \text{lv}(G)$. This completes the proof of Lemma 1.9. \square

REMARK 1.9.1.

(i) One verifies immediately that even if $p = 2$, one may apply the various arguments given in the present §1. In particular, even if $p = 2$, one may prove Proposition 1.8, as well as a similar assertion to Lemma 1.9 [i.e., the assertion obtained by replacing the “ $\text{lv}(G)$ ” of the display of Lemma 1.9 by “ $\text{lv}(G) + 1$ ”]. We leave the routine details to the interested reader.

(ii) One verifies immediately from Theorem 1.5 that the exact sequence $0 \rightarrow G^\circ(\overline{K}) \rightarrow G(\overline{K}) \rightarrow G^{\text{ét}}(\overline{K}) \rightarrow 0$ of [not Γ_K -modules but abstract] modules is *split*. One also verifies immediately that the action of $\Gamma_{K_{G^\circ}} (\supseteq \Gamma_{K_G})$ on $G(\overline{K})$ determines and is determined by a homomorphism $\Gamma_{K_{G^\circ}} \rightarrow \text{Hom}_{\mathbb{Z}_p}(G^{\text{ét}}(\overline{K}), G^\circ(\overline{K}))$. By means of these observations, one verifies easily that one may replace the respective “ $\text{lv}(G)$ ” of the right-hand sides of the displays of Proposition 1.8 and Lemma 1.9 by “ $\text{lv}(G^\circ)$ ”. We leave the routine details to the interested reader.

(iii) Let us recall that we have worked in a situation of *absolute ramification index one*, i.e., a situation where the base discrete valuation field is of *absolute ramification*

index one. Now let us observe that Theorem 1.5 may be applied in a situation of *absolute ramification index* $< p - 1$ [cf. [11], Corollaire 3.3.6, (1)]. In particular, even if we are in a situation of *absolute ramification index* $< p - 1$, one may obtain a similar result to Proposition 1.8, as well as a similar result to Lemma 1.9. We leave the routine details to the interested reader.

2. GALOIS MODULES OF TYPE S

In the present §2, we consider a *Galois module of type S* [cf. Definition 2.3, (i), below], i.e., a Γ_K -module which is isomorphic to a finite Γ_K -submodule of the Γ_K -module obtained by considering torsion points of an abelian variety with semistable model over W . In particular, we prove the *triviality* of the Galois action on a subquotient of a Galois module of type S which satisfies a technical condition [cf. Lemma 2.7 below].

In the present §2, we maintain the notation introduced at the beginning of §1. Write, moreover, $K^{\text{tm}} \subseteq \overline{K}$ for the maximal tamely ramified extension of K in \overline{K} .

LEMMA 2.1. — *Let M be a finite module, $\Gamma \subseteq \text{Aut}(M)$ a subgroup of $\text{Aut}(M)$, and $x \in M$ an element of M . Write $x = x_p + x_{\neq p}$ for the representation of $x \in M$ with respect to the natural direct decomposition $M = M_p \oplus M_{\neq p}$ and $S_x \subseteq M$ for the subset of M consisting of the elements $y \in M$ which satisfy one of the following three conditions:*

- (1) *There exist elements $\gamma_1, \gamma_2 \in \Gamma$ of Γ and an integer $i \geq 0$ such that $y = p^i(\gamma_1 - \gamma_2)x \in M$.*
- (2) *There exist elements $\gamma_1, \gamma_2 \in \Gamma$ of Γ and an integer $i \geq 0$ such that $y = p^i(\gamma_1 - \gamma_2)x_p \in M$.*
- (3) *There exist elements $\gamma_1, \gamma_2, \gamma_3, \gamma_4 \in \Gamma$ of Γ and an integer $i \geq 0$ such that $y = p^i(\gamma_1 - \gamma_2)(\gamma_3 - \gamma_4)x \in M$.*

*Note that one verifies immediately that the subset $S_x \subseteq M$, hence also the subset $S_x[p] \stackrel{\text{def}}{=} S_x \cap M[p]$, of M is **stable** under the action of Γ on M . Suppose that the following two conditions are satisfied:*

- (a) *The element $x \in M$ is a **weak Γ -invariant**.*
- (b) *For every $\gamma \in \Gamma$, it holds that $(1 - \gamma)^2 M_{\neq p} = \{0\}$.*

Then the following hold:

- (i) *It holds that $x_p \in M^{\Gamma^{S_x[p]}}$.*
- (ii) *Suppose, moreover, that the following condition is satisfied:*
- (c) *The Γ -module M is **generated** by $x \in M$.*

Then it holds that $\Gamma^{S_x[p]} = \{1\}$.

PROOF. — To verify assertion (i), assume that $x_p \notin M^{\Gamma^{S_x[p]}}$. Write n for the smallest [necessarily positive] integer such that $p^n x_p \in M^{\Gamma^{S_x[p]}}$. Now since $p^{n-1} x_p \notin M^{\Gamma^{S_x[p]}}$, there exists a(n) [necessarily nontrivial] element $\gamma \in \Gamma^{S_x[p]}$ of $\Gamma^{S_x[p]}$ such that $p^{n-1}(1 - \gamma)x_p \neq 0$.

For $1 \leq i \leq n$, write

$$y_i \stackrel{\text{def}}{=} p^{n-i}(1 - \gamma^{p^{i-1}})x_p \in M.$$

Now I claim that the following assertion holds:

Claim 2.1.A: It holds that $y_1 \in S_x[p] \setminus \{0\}$.

Indeed, the fact that $y_1 (= p^{n-1}(1 - \gamma)x_p) \neq 0$ has already been verified. It follows from (2), together with the definition of y_i , that $y_i \in S_x$. Moreover, since $p^n x_p \in M^{\Gamma^{S_x[p]}}$, and $\gamma \in \Gamma^{S_x[p]}$, it holds that $py_1 = p^n(1 - \gamma)x_p = 0$, i.e., that $y_1 \in M[p]$. This completes the proof of Claim 2.1.A.

Next, I claim that the following assertion holds:

Claim 2.1.B: It holds that $y_i = y_1$ for every $1 \leq i \leq n$.

We prove Claim 2.1.B by *induction on i* . Suppose that, for $1 \leq i \leq n-1$, it holds that $y_i = y_1$. Then it follows from Claim 2.1.A, together with the induction hypothesis, that $p^2 \cdot p^{n-i-1}(1 - \gamma^{p^{i-1}})x_p = py_i = py_1 = 0$, which thus implies that $p \cdot p^{n-i-1}(1 - \gamma^{p^{i-1}})x_p \in S_x[p]$ [cf. (2)]. In particular, since $\gamma \in \Gamma^{S_x[p]}$, it holds that

$$(*) \quad p \cdot p^{n-i-1}(1 - \gamma^{p^{i-1}})^2 x_p = 0.$$

Thus, since $(1 - \gamma^{p^{i-1}})^2 x_{\neq p} = 0$ [cf. (b)], it holds that $p \cdot p^{n-i-1}(1 - \gamma^{p^{i-1}})^2 x = 0$, which thus implies that $p^{n-i-1}(1 - \gamma^{p^{i-1}})^2 x_p = p^{n-i-1}(1 - \gamma^{p^{i-1}})^2 x \in S_x[p]$ [cf. (3)]. Thus, since $\gamma \in \Gamma^{S_x[p]}$, it holds that

$$(**) \quad p^{n-i-1}(1 - \gamma^{p^{i-1}})^3 x_p = 0.$$

It follows from (*), (**), together with Lemma 2.2 below, that

$$(1 - (\gamma^{p^{i-1}})^p)p^{n-i-1}x_p = p(1 - \gamma^{p^{i-1}})p^{n-i-1}x_p,$$

i.e., that $y_{i+1} = y_i$, as desired. This completes the proof of Claim 2.1.B.

Next, let us observe that it follows from Claim 2.1.A and Claim 2.1.B that

$$(1 - \gamma^{p^{n-1}})x_p = y_n = y_1 \in S_x[p] \setminus \{0\}.$$

Thus, since $\gamma^{p^{n-1}} \in \Gamma^{S_x[p]}$, and $(1 - \gamma^{p^{n-1}})^2 x_{\neq p} = 0$ [cf. (b)], it holds that

$$(1 - \gamma^{p^{n-1}})^2 x = (1 - \gamma^{p^{n-1}})^2 x_p = (1 - \gamma^{p^{n-1}})y_n = 0,$$

which thus implies [cf. (a)] that $(1 - \gamma^{p^{n-1}})x = 0$. In particular, we conclude that

$$y_n = (1 - \gamma^{p^{n-1}})x_p = 0$$

— which *contradicts* Claim 2.1.A and Claim 2.1.B. This completes the proof of assertion (i).

Finally, we verify assertion (ii). Let $\gamma \in \Gamma^{S_x[p]}$ be an element of $\Gamma^{S_x[p]}$. Then since $x_p \in M^{\Gamma^{S_x[p]}}$ [cf. assertion (i)], and $\Gamma^{S_x[p]} \subseteq \Gamma$ is *normal*, it holds that $\delta \cdot x_p \in M^{\Gamma^{S_x[p]}}$ for every $\delta \in \Gamma$. Thus, it holds that $(1 - \gamma)(\delta \cdot x) = (1 - \gamma)(\delta \cdot x_{\neq p})$, which thus implies that $(1 - \gamma)^2(\delta \cdot x) = (1 - \gamma)^2(\delta \cdot x_{\neq p}) = 0$ [cf. (b)]. In particular, it follows from (a) that $(1 - \gamma)(\delta \cdot x) = 0$. Thus, it follows from (c) that the action of γ on M is *trivial*. This completes the proof of assertion (ii), hence also of Lemma 2.1. \square

LEMMA 2.2. — *In the ring $\mathbb{Z}[T]$ of polynomials in T with coefficients in \mathbb{Z} , the congruence*

$$1 - T^p \equiv p(1 - T) \pmod{(p(1 - T)^2, (1 - T)^3)}$$

holds.

PROOF. — By “mod $(1 - T)^3$ ”, we obtain that

$$\begin{aligned} 1 - T^p &= 1 - (1 - (1 - T))^p \equiv 1 - (1 - p(1 - T) + p(p - 1)(1 - T)^2/2) \\ &= p(1 - T) - p(p - 1)(1 - T)^2/2. \end{aligned}$$

Thus, since [we have assumed that] $p \neq 2$, Lemma 2.2 holds. This completes the proof of Lemma 2.2. \square

DEFINITION 2.3. — Let M be a finite module equipped with an action of Γ_K .

(i) We shall say that the Γ_K -module M is *of type G* (respectively, *of type S*) if there exist an abelian variety A over K which has good (respectively, semistable) reduction over W and a Γ_K -equivariant injection $M \hookrightarrow A(\overline{K})$.

(ii) We shall say that a Γ_K -submodule $N \subseteq M$ of M is a *G -part* of M if the following three conditions are satisfied:

(1) The Γ_K -module N is of type G [which thus implies that the action of Γ_K on $N_{\neq p}$ is trivial — cf. Remark 2.3.1, (i), (ii), below].

(2) The action of Γ_K on M/N is trivial.

(3) The action of Γ_K on every nontrivial Γ_K -stable subquotient of N_p is nontrivial [cf. Lemma 2.4, (ii), below].

(iii) We shall say that the action of Γ_K on M is *tame* if the [necessarily finite] quotient $\Gamma_K[M]$ of Γ_K is of order prime to p , i.e., the natural surjection $\Gamma_K \rightarrow \Gamma_K[M]$ factors through the quotient of Γ_K corresponding to the Galois extension $K^{\text{tm}} (\subseteq \overline{K})$ of K .

REMARK 2.3.1.

(i) One verifies immediately from the various definitions involved that a Γ_K -module obtained by forming a subquotient of a finite Γ_K -module *of type G* (respectively, *of type S*) is *of type G* (respectively, *of type S*).

(ii) Let M be a finite Γ_K -module *of type G* such that $M = M_{\neq p}$. Then one verifies immediately that the action of Γ_K on M is *trivial* [cf., e.g., Lemma 2.4, (i), below].

(iii) It is well-known [cf., e.g., [10], Appendix A, Theorem A.6] that, for a finite Γ_K -module M , it holds that M is *of type G* if and only if there exist a finite flat commutative group scheme G over W and a Γ_K -equivariant isomorphism $M \xrightarrow{\sim} G(\overline{K})$.

LEMMA 2.4. — *Let M be a finite Γ_K -module of type G . Thus, by Remark 2.3.1, (iii), there exist a finite flat commutative group scheme G over W and a Γ_K -equivariant isomorphism $M \xrightarrow{\sim} G(\overline{K})$. Then the following hold:*

- (i) The action of Γ_K on M is **trivial** if and only if G is **étale** over W .
- (ii) The action of Γ_K on every nontrivial Γ_K -stable subquotient of M is **nontrivial** if and only if G is **connected**.

PROOF. — These assertions follow immediately from Theorem 1.5. \square

Now let us recall the following *well-known* lemma:

PROPOSITION 2.5. — *Let M be a finite Γ_K -module of type **S**. Then the following hold:*

- (i) The Γ_K -module M has a **G-part**.
- (ii) If $M = M_{\neq p}$, then the action of Γ_K on M is **tame**.

PROOF. — Assertion (ii) follows immediately from assertion (i), together with conditions (1) and (2) of Definition 2.3, (ii). Thus, to complete the verification of Proposition 2.5, it suffices to verify assertion (i). On the other hand, assertion (i) follows from basic facts concerning Galois actions on torsion points of semi-abelian schemes [cf., e.g., [6], Chapter III, or [10], Appendix C, the discussion entitled “The Raynaud group”] as follows.

To verify assertion (i), let us first review some consequences of the discussions of [6], Chapter III. Let A be an abelian variety over K which has *semistable reduction* over W and n an integer such that $M \subseteq A(\overline{K})[n]$. Write A^D for the dual abelian variety of A . Then it follows from the discussions of [6], Chapter III, that there exist semi-abelian schemes \tilde{A}, \tilde{A}_D over W ; abelian schemes B, B_D over W ; split tori T, T_D over W ; free \mathbb{Z}/n -modules P, P_D of finite rank equipped with the trivial actions of Γ_K which satisfy the following three conditions:

- (a) The semi-abelian scheme \tilde{A} (respectively, \tilde{A}_D) is an extension of B (respectively, B_D) by T (respectively, T_D). In particular, we have exact sequences of Γ_K -modules

$$\begin{aligned} 0 &\longrightarrow T(\overline{K})[n] \longrightarrow \tilde{A}(\overline{K})[n] \longrightarrow B(\overline{K})[n] \longrightarrow 0, \\ 0 &\longrightarrow T_D(\overline{K})[n] \longrightarrow \tilde{A}_D(\overline{K})[n] \longrightarrow B_D(\overline{K})[n] \longrightarrow 0. \end{aligned}$$

- (b) The Γ_K -modules of n -torsion points of $A, \tilde{A}, A^D, \tilde{A}_D$ fit into exact sequences of Γ_K -modules

$$\begin{aligned} 0 &\longrightarrow \tilde{A}(\overline{K})[n] \longrightarrow A(\overline{K})[n] \longrightarrow P \longrightarrow 0, \\ 0 &\longrightarrow \tilde{A}_D(\overline{K})[n] \longrightarrow A^D(\overline{K})[n] \longrightarrow P_D \longrightarrow 0. \end{aligned}$$

- (c) The natural pairing $A(\overline{K})[n] \times A^D(\overline{K})[n] \rightarrow \mu_n(\overline{K})$ — where we write $\mu_n(\overline{K}) \subseteq \overline{K}^\times$ for the group of n -th roots of unity in \overline{K} — determines a Γ_K -equivariant isomorphism [cf. [6], Chapter III, Corollary 7.4]

$$A(\overline{K})[n]/T(\overline{K})[n] \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\tilde{A}_D(\overline{K})[n], \mu_n(\overline{K})).$$

Moreover, by (a), the quasi-finite flat commutative group schemes $G \stackrel{\mathrm{def}}{=} \tilde{A}[n], \tilde{A}_D[n]$ over W obtained by forming the respective kernels of the endomorphisms of \tilde{A}, \tilde{A}_D given by multiplication by n is in fact *finite* over W . Thus, it follows from Remark 2.3.1, (iii), that the following holds:

(d) The finite Γ_K -modules $\tilde{A}(\overline{K})[n]$, $\tilde{A}_D(\overline{K})[n]$ are of type G . In particular, by (c), the finite Γ_K -module $A(\overline{K})[n]/T(\overline{K})[n]$ is of type G .

If $M = M_{\neq p}$, then it follows immediately — in light of Remark 2.3.1, (ii) — from (d), together with the various definitions involved, that the Γ_K -submodule of M determined by $T(\overline{K})[n] \subseteq A(\overline{K})[n]$ in the above discussion is a G -part. Thus, to complete the verification of assertion (i), we may assume without loss of generality that $M = M_p$, and that n is a power of p .

Since $G = \tilde{A}[n]$ is a finite flat commutative group scheme over W [cf. the discussion preceding (d)], we have an exact sequence of finite flat commutative group schemes over W

$$0 \longrightarrow G^\circ \longrightarrow G \longrightarrow G^{\text{ét}} \longrightarrow 0$$

— where $G^\circ \subseteq G$ is connected, and $G^{\text{ét}}$ is étale over W . Now I claim that the following assertion holds:

Claim 2.5.A: The finite Γ_K -module $A(\overline{K})[n]/G^\circ(\overline{K})$ is of type G .

Indeed, by (d), to verify Claim 2.5.A, it suffices to verify that the inclusion $T(\overline{K})[n] \subseteq G^\circ(\overline{K})$ holds. On the other hand, this follows from the [easily verified] fact that the action of Γ_K on every nontrivial Γ_K -stable subquotient of $T(\overline{K})[n]$ is nontrivial. This completes the proof of Claim 2.5.A.

Next, I claim that the following assertion holds:

Claim 2.5.B: The Γ_K -submodule $N \subseteq M$ of M determined by $G^\circ(\overline{K}) \subseteq A(\overline{K})$ is a G -part.

Indeed, it follows from the various definitions involved, together with Lemma 2.4, (ii), that N satisfies conditions (1) and (3) of Definition 2.3, (ii). Next, to verify the assertion that N satisfies condition (2) of Definition 2.3, (ii), let us consider the following exact sequence of Γ_K -modules [which arises from the first exact sequence of (b)]

$$0 \longrightarrow G^{\text{ét}}(\overline{K}) \longrightarrow A(\overline{K})[n]/G^\circ(\overline{K}) \longrightarrow P \longrightarrow 0.$$

Since the actions of Γ_K on $G^{\text{ét}}(\overline{K})$ and P are trivial, it follows immediately from Claim 2.5.A [cf. also Remark 2.3.1, (iii)] that the action of Γ_K on $A(\overline{K})[n]/G^\circ(\overline{K})$ is trivial. Thus, since M/N is a Γ_K -submodule of $A(\overline{K})[n]/G^\circ(\overline{K})$, it follows that N satisfies condition (2) of Definition 2.3, (ii). This completes the proof of Claim 2.5.B, hence also of assertion (i). \square

LEMMA 2.6. — Let M be a finite Γ_K -module of type **S**. Suppose that there exists a weak Γ_K -invariant $x \in M$ of M such that the Γ_K -module M is generated by $x \in M$. Then there exists a Γ_K -submodule $N \subseteq M$ of M which satisfies the following two conditions:

- (1) The Γ_K -module N is of type **G** and annihilated by p .
- (2) The natural surjection $\Gamma_K[M] \twoheadrightarrow \Gamma_K[N]$ is an isomorphism.

PROOF. — Let $F \subseteq M$ be a G -part of M [cf. Proposition 2.5, (i)]. Write $S_x[p] \subseteq M$ for the “ $S_x[p]$ ” of Lemma 2.1 in the case where we take the “ (M, Γ, x) ” of Lemma 2.1 to be

$(M, \Gamma_K[M], x)$. Then it follows from condition (2) of Definition 2.3, (ii), together with the definition of S_x , that $S_x[p] \subseteq F[p]$. Write $N \subseteq (F[p] \subseteq) M$ for the Γ_K -submodule of M generated by $S_x[p]$. Then it follows immediately from condition (1) of Definition 2.3, (ii), that N satisfies condition (1) of Lemma 2.6. Moreover, since [it follows from conditions (1) and (2) of Definition 2.3, (ii) that] (b) of Lemma 2.1 [in the case where we take the “ (M, Γ, x) ” of Lemma 2.1 to be $(M, \Gamma_K[M], x)$] holds, it follows from Lemma 2.1, (ii), that N satisfies condition (2) of Lemma 2.6. This completes the proof of Lemma 2.6. \square

The following result is the main result of the present §2:

LEMMA 2.7. — *Let M be a finite Γ_K -module of type **S**. Suppose that there exists a weak Γ_K -invariant of M which generates the Γ_K -module M . Then the action of Γ_K on $p \cdot M_p$ is trivial.*

PROOF. — Let $F \subseteq M$ be a G -part of M [cf. Proposition 2.5, (i)] and $N \subseteq M$ a Γ_K -submodule of M which satisfies two conditions (1), (2) of Lemma 2.6. Then let us observe that since $F_p \subseteq M$, it follows from condition (2) of Lemma 2.6 that the natural surjection $\Gamma_K \twoheadrightarrow \Gamma_K[F_p]$ factors through $\Gamma_K \twoheadrightarrow \Gamma_K[N]$. Thus, since both F_p and N are of type G , it follows — in light of Remark 2.3.1, (iii), and Lemma 2.4, (ii) — from Lemma 1.9, together with the fact that $p \cdot N = \{0\}$ [cf. condition (1) of Lemma 2.6], that $p \cdot F_p = \{0\}$. In particular, it follows from condition (2) of Definition 2.3, (ii), that the action of Γ_K on $p \cdot M_p$ is trivial. This completes the proof of Lemma 2.7. \square

3. RAMIFIED TORSION POINTS ON CURVES

In the present §3, we prove the main result of the present paper [cf. Theorem 3.4 below], which is closely related to a conjecture due to *R. Coleman* concerning the *ramification of torsion points* [cf. Remark 3.4.1 below]. Moreover, by means of the main result, we study the geometry of curves which admit *ramified torsion points* [cf. Corollary 3.6, Corollary 3.8, Corollary 3.9 below].

In the present §3, we maintain the notation of §2. Let $g \geq 2$ be an integer and X a curve of genus g over K which has *stable reduction* over W . Write J for the Jacobian variety of X .

Let us first recall the following *well-known* result:

PROPOSITION 3.1. — *The abelian variety J over K has semistable reduction over W . Moreover, it holds that the abelian variety J over K has good reduction over W if and only if the dual graph of the special fiber of the stable model of X over W is a tree.*

PROOF. — This follows from, for instance, [3], §9.2, Example 8, and [3], §9.7, Corollary 2. \square

DEFINITION 3.2. — Let $x \in X_{\overline{K}}^{\text{cl}}$ be a closed point of $X_{\overline{K}}$. Then we shall write $\varphi_x: X_{\overline{K}}^{\text{cl}} \hookrightarrow J_{\overline{K}}^{\text{cl}}$ for the injection between the sets of closed points determined by the Albanese embedding of X with respect to $x \in X_{\overline{K}}^{\text{cl}}$.

LEMMA 3.3. — *Let $x_0 \in X(K)$ be a K -rational point of X and $x \in X_{\bar{K}}^{\text{cl}}$ a closed point of $X_{\bar{K}}$. Suppose that $\varphi_{x_0}(x) \in J_{\bar{K}}^{\text{cl}}$ is **torsion**. Write $M \subseteq J_{\bar{K}}^{\text{cl}}$ for the [necessarily finite] Γ_K -submodule of $J_{\bar{K}}^{\text{cl}}$ generated by $\varphi_{x_0}(x) \in J_{\bar{K}}^{\text{cl}}$. Then the following hold:*

(i) *The Γ_K -module M is of type **S**. If, moreover, the abelian variety J over K has **good reduction** over W , then the Γ_K -module M is of type **G**.*

(ii) *If (X, x) is **not exceptional**, then the element $\varphi_{x_0}(x) \in M$ is a **weak Γ_K -invariant**.*

(iii) *The action of Γ_K on $p \cdot M_p$ is **trivial**.*

PROOF. — Assertion (i) follows from Proposition 3.1, together with the various definitions involved. Next, we verify assertion (ii). Let $\gamma, \delta \in \Gamma_K$ be such that $(1-\gamma)^2 \delta \cdot \varphi_{x_0}(x) = 0$. Then since x_0 is K -rational, our assumption $(1-\gamma)^2 \delta \cdot \varphi_{x_0}(x) = 0$ implies that $[\delta \cdot x] + [\gamma^2 \cdot \delta \cdot x] = 2[\gamma \cdot \delta \cdot x]$, where we write “[$-$]” for the prime divisor determined by “[$-$]”. In particular, since (X, x) , hence also $(X, \delta \cdot x)$, is *not exceptional*, it holds that $\delta \cdot x = \gamma \cdot \delta \cdot x$, i.e., that $(1-\gamma)\delta \cdot \varphi_{x_0}(x) = 0$. This completes the proof of assertion (ii).

Finally, we verify assertion (iii). If (X, x) is *not exceptional*, then assertion (iii) follows from Lemma 2.7, together with assertions (i), (ii). If (X, x) is *exceptional*, then it follows from [13], Proposition 3.1, (i), that the action of Γ_K on $2 \cdot M$ is *trivial*. Thus, the action of Γ_K on $M_p \subseteq 2 \cdot M$, hence also on $p \cdot M_p$, is *trivial*. This completes the proof of assertion (iii), hence also of Lemma 3.3. \square

The following result is the main result of the present paper:

THEOREM 3.4. — *In the notation introduced at the beginning of §3, let $x_0 \in X(K)$ be a K -rational point of X and $x \in X_{\bar{K}}^{\text{cl}}$ a closed point of $X_{\bar{K}}$. Suppose that $\varphi_{x_0}(x) \in J_{\bar{K}}^{\text{cl}}$ is **torsion**. Then the following hold:*

(i) *The residue field of J at $p \cdot \varphi_{x_0}(x) \in J_{\bar{K}}^{\text{cl}}$ is **at most tamely ramified** over K .*

(ii) *Suppose, moreover, that one of the following two conditions is satisfied:*

(a) *There exists an integer $n \geq 1$ such that $p^n \cdot \varphi_{x_0}(x) \in J_{\bar{K}}^{\text{cl}}$ is **K -rational**.*

(b) *The abelian variety J over K has **good reduction** over W [cf. Proposition 3.1].*

*Then $p \cdot \varphi_{x_0}(x) \in J_{\bar{K}}^{\text{cl}}$ is **K -rational**.*

PROOF. — Assertion (i) follows immediately from Lemma 3.3, (i), (iii), together with Proposition 2.5, (ii). Assertion (ii) in the case where the condition (a) is satisfied follows immediately from Lemma 3.3, (iii). Assertion (ii) in the case where the condition (b) is satisfied follows immediately from Lemma 3.3, (i), (iii), together with Remark 2.3.1, (ii). This completes the proof of Theorem 3.4. \square

REMARK 3.4.1.

(i) *R. Coleman* stated, in [4], a conjecture concerning the *ramification of torsion points* on a curve which satisfies certain conditions. Let us recall the statement of [a slightly stronger version of] the conjecture as follows [cf. [4], Conjecture B]:

In the notation introduced at the beginning of §3, let $x_0 \in X(K)$ be a K -rational point of X and $x \in X_{\overline{K}}^{\text{cl}}$ a closed point of $X_{\overline{K}}$. Suppose that $\varphi_{x_0}(x) \in J_{\overline{K}}^{\text{cl}}$ is *torsion*. Suppose, moreover, that the following two conditions are satisfied:

- (1) It holds that $p \geq 5$.
- (2) The curve X , hence also the abelian variety J , over K has *good reduction* over W .

Then $\varphi_{x_0}(x) \in J_{\overline{K}}^{\text{cl}}$ is K -rational.

As we discussed in Introduction of the present paper, Coleman himself proved the conjecture in the case where the given curve X satisfies a further assumption.

(ii) Observe that we conclude from Theorem 3.4 that, in the situation of the conjecture of (i), it holds that

at least $p \cdot \varphi_{x_0}(x) \in J_{\overline{K}}^{\text{cl}}$ is K -rational

[cf. Theorem 3.4, (ii), in the case where the condition (b) is satisfied]. Unfortunately, however, at the time of this writing, the author cannot derive a solution of the conjecture of (i) from Theorem 3.4.

REMARK 3.4.2. — Note that the proof of the main result of the present paper may be regarded as a *refinement* [in the *absolutely unramified* case] of an argument of [12] given by *D. Rössler*.

DEFINITION 3.5.

(i) We shall say that a closed point $x \in X_{\overline{K}}^{\text{cl}}$ of $X_{\overline{K}}$ is a *ramified torsion point* (respectively, *wildly ramified torsion point*) if the closed point $x \in X_{\overline{K}}^{\text{cl}}$ is not K -rational (respectively, not K^{tm} -rational), and, moreover, there exists a K -rational point $x_0 \in X(K)$ of X such that $\varphi_{x_0}(x) \in J_{\overline{K}}^{\text{cl}}$ is torsion.

(ii) We shall refer to an equivalence class with respect to the following equivalence relation “ \sim ” on $X_{\overline{K}}^{\text{cl}}$ as a *torsion packet* on X : For $x, y \in X_{\overline{K}}^{\text{cl}}$, write $x \sim y$ if $\varphi_x(y)$ ($= -\varphi_y(x)$) $\in J_{\overline{K}}^{\text{cl}}$ is torsion.

(iii) We shall say that a torsion packet is a *ramified torsion packet* (respectively, *wildly ramified torsion packet*) if the torsion packet contains a ramified (respectively, wildly ramified) torsion point.

REMARK 3.5.1. — Thus, the conjecture of Coleman discussed in Remark 3.4.1, (i), is *equivalent* to the following assertion:

In the notation introduced at the beginning of §3, suppose that the following two conditions are satisfied:

- (1) It holds that $p \geq 5$.

(2) The curve X , hence also the abelian variety J , over K has *good reduction* over W .

Then there is *no ramified torsion point* [cf. Definition 3.5, (i)] on $X_{\overline{K}}$, or, equivalently, there is *no ramified torsion packet* [cf. Definition 3.5, (iii)] on X .

COROLLARY 3.6. — *In the notation introduced at the beginning of §3, let $x \in X_{\overline{K}}^{\text{cl}}$ be a **ramified torsion point** on $X_{\overline{K}}$. Suppose that one of the following two conditions is satisfied:*

- (1) *The abelian variety J over K has **good reduction** over W .*
- (2) *The closed point $x \in X_{\overline{K}}^{\text{cl}}$ is a **wildly ramified torsion point**.*

Then the following hold:

- (i) *Suppose that condition (1) (respectively, (2)) is satisfied. Let γ be an element of Γ_K (respectively, of the uniquely determined p -Sylow subgroup of Γ_K). Then it holds that $p \cdot \varphi_{\gamma \cdot x}(x) = 0$.*
- (ii) *The prime number p is a **Weierstrass non-gap** at $x \in X_{\overline{K}}^{\text{cl}}$. In particular, if $g \geq p$, then $x \in X_{\overline{K}}^{\text{cl}}$ is a **Weierstrass point** of $X_{\overline{K}}$.*
- (iii) *There is a finite morphism $X_{\overline{K}} \rightarrow \mathbb{P}_{\overline{K}}^1$ of degree p over \overline{K} which is **totally ramified** at $x \in X_{\overline{K}}^{\text{cl}}$. In particular, the curve $X_{\overline{K}}$ over \overline{K} is of **gonality** $\leq p$.*
- (iv) *If $g \geq p$, then the curve $X_{\overline{K}}$ over \overline{K} is **not hyperelliptic**.*

PROOF. — First, we verify assertion (i). It follows immediately from the various definitions involved that there exists a K -rational point $x_0 \in X(K)$ of X such that $\varphi_{x_0}(x) \in J_{\overline{K}}^{\text{cl}}$ is *torsion*. Thus, since [one verifies immediately that] $(1 - \gamma)\varphi_{x_0}(x) = \varphi_{\gamma \cdot x}(x)$, assertion (i) follows from Theorem 3.4. This completes the proof of assertion (i).

Next, we verify assertion (ii). Suppose that condition (1) (respectively, (2)) is satisfied. Then it follows immediately from the various definitions involved that there exists an element γ of Γ_K (respectively, of the uniquely determined p -Sylow subgroup of Γ_K) such that $\varphi_{\gamma \cdot x}(x) \neq 0$, which thus implies [cf. assertion (i)] that $\varphi_{\gamma \cdot x}(x)$ is of order p . Thus, we conclude immediately from the various definitions involved that p is a *Weierstrass non-gap* at $x \in X_{\overline{K}}^{\text{cl}}$. This completes the proof of assertion (ii). Assertion (iii) follows immediately from assertion (ii).

Finally, we verify assertion (iv). It follows from assertion (iii) that there exists a finite morphism $X_{\overline{K}} \rightarrow \mathbb{P}_{\overline{K}}^1$ of degree p over \overline{K} . Thus, since [we have assumed that] $g \geq p \geq 3$, it follows from Lemma 3.7, (i), below that there is *no* finite morphism $X_{\overline{K}} \rightarrow \mathbb{P}_{\overline{K}}^1$ of degree 2 over \overline{K} . This completes the proof of assertion (iv), hence also of Corollary 3.6. \square

REMARK 3.6.1. — Note that, in Corollary 3.6, (iv), one cannot remove the hypothesis “ $g \geq p$ ”. Indeed, if $p = 3$, then the *hyperelliptic* modular curve “ $X_1(13)$ ” [of genus 2] over K has *good reduction* over W and admits a *ramified torsion point* [cf. [2], Appendix, the discussion following Conjecture 6.4].

LEMMA 3.7. — *Let $d \geq 1$ be an integer and $\phi, \psi: X_{\overline{K}} \rightarrow \mathbb{P}_{\overline{K}}^1$ finite morphisms over \overline{K} . Suppose that ϕ is of degree p , that ψ is of degree d , and that $g > (p-1)(d-1)$. Then the following hold:*

(i) *It holds that $d \in p\mathbb{Z}$, which thus implies that $d \geq p$.*

(ii) *Suppose that $d = p$. Then the invertible sheaf $\phi^*\mathcal{O}_{\mathbb{P}_{\overline{K}}^1}(1)$ on $X_{\overline{K}}$ is **isomorphic** to the invertible sheaf $\psi^*\mathcal{O}_{\mathbb{P}_{\overline{K}}^1}(1)$ on $X_{\overline{K}}$.*

PROOF. — These assertions follow immediately from the *Castelnuovo-Severi inequality* [cf., e.g., [1], Chapter VIII, Exercise C-1]. \square

COROLLARY 3.8. — *In the situation of Corollary 3.6, suppose, moreover, that $g > (p-1)^2$. Then the following hold:*

(i) *The curve $X_{\overline{K}}$ over \overline{K} is of gonality p .*

(ii) *Let $\phi: X_{\overline{K}} \rightarrow \mathbb{P}_{\overline{K}}^1$ be a finite morphism of degree p over \overline{K} [cf. (i)]. Then ϕ is **totally ramified** at $x \in X_{\overline{K}}^{\text{cl}}$.*

(iii) *If condition (1) (respectively, (2)) in the statement of Corollary 3.6 is satisfied, then the curve X has **exactly one ramified** (respectively, **wildly ramified**) torsion packet.*

PROOF. — Assertion (i) (respectively, (ii)) follows immediately from Corollary 3.6, (iii), together with Lemma 3.7, (i) (respectively, (ii)). Assertion (iii) follows immediately from assertions (i), (ii). This completes the proof of Corollary 3.8. \square

COROLLARY 3.9. — *In the situation of Corollary 3.6, let us suppose that condition (1) (respectively, (2)) in the statement of Corollary 3.6 is satisfied. Write $d_x (> 1)$ for the extension degree over K of the residue field of X at $x \in X_{\overline{K}}^{\text{cl}}$, $d_{x,p}$ for the “ p -part” of d_x , i.e., $d_{x,p} \stackrel{\text{def}}{=} \#(\mathbb{Z}_p/d_x)$, and $D_x \stackrel{\text{def}}{=} d_x$ (respectively, $\stackrel{\text{def}}{=} d_{x,p}$). Then the following hold:*

(i) *It holds that $D_x \leq g(p-1)^2$.*

(ii) *Suppose, moreover, that $g > (p-1)^2$. If condition (1) (respectively, (2)) in the statement of Corollary 3.6 is satisfied, then the number of **ramified** (respectively, **wildly ramified**) torsion points on $X_{\overline{K}}$ is $\leq 2 + 2g/(p-1)$. In particular, it holds that $D_x \leq 2 + 2g/(p-1)$.*

PROOF. — First, we verify assertion (i). Write $(x \in) \{x_1, x_2, \dots, x_{D_x}\} \subseteq X_{\overline{K}}^{\text{cl}}$ for the orbit of $x \in X_{\overline{K}}^{\text{cl}}$ by the action of Γ_K (respectively, the uniquely determined p -Sylow subgroup of Γ_K). Then it follows from Corollary 3.6, (i), that, for every $i \in \{2, \dots, D_x\}$, it holds that $\varphi_{x_1}(x_i) \in J_{\overline{K}}^{\text{cl}}$ is of order p , which thus implies that $(1-p) \cdot \varphi_{x_1}(x_i) = \varphi_{x_1}(x_i)$. In particular, we conclude that

$$\{\varphi_{x_1}(x_1), \varphi_{x_1}(x_2), \dots, \varphi_{x_1}(x_{D_x})\} \subseteq \varphi_{x_1}(X) \cap (1-p) \cdot \varphi_{x_1}(X).$$

Thus, it follows from [5], Lemma 4.1, that $D_x \leq g(1-p)^2$. This completes the proof of assertion (i).

Next, we verify assertion (ii). If condition (1) (respectively, (2)) in the statement of Corollary 3.6 is satisfied, then write N for the number of *ramified* (respectively, *wildly ramified*) *torsion* points on $X_{\overline{K}}$. Let $\phi: X_{\overline{K}} \rightarrow \mathbb{P}_{\overline{K}}^1$ be a finite morphism of degree p over \overline{K} [cf. Corollary 3.8, (i)]. Then, by applying Corollary 3.8, (ii), and the *Riemann-Hurwitz formula* to ϕ , we conclude that $2g - 2 \geq -2p + (p - 1)N$, which thus implies that $N \leq 2 + 2g/(p - 1)$. This completes the proof of Corollary 3.9. \square

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] M. Baker, *Torsion points on modular curves*, Ph.D. thesis, University of California, Berkeley, 1999.
- [3] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (**3**), **21**. Springer-Verlag, Berlin, 1990.
- [4] R. F. Coleman, Ramified torsion points on curves, *Duke Math. J.* **54** (1987), no. **2**, 615–640.
- [5] R. F. Coleman, B. Kaskel, and K. A. Ribet, Torsion points on $X_0(N)$, *Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996)*, 27–49, Proc. Sympos. Pure Math., **66**, Part **1**, Amer. Math. Soc., Providence, RI, 1999.
- [6] G. Faltings and C.-L. Chai, *Degeneration of abelian varieties. With an appendix by David Mumford*, Ergebnisse der Mathematik und ihrer Grenzgebiete (**3**), **22**. Springer-Verlag, Berlin, 1990.
- [7] J.-M. Fontaine, Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux, *Invent. Math.* **65** (1981/82), no. **3**, 379–409.
- [8] J.-M. Fontaine, Il n’y a pas de variété abélienne sur \mathbb{Z} , *Invent. Math.* **81** (1985), no. **3**, 515–538.
- [9] Y. Hoshi, Tame-blind extension of morphisms of truncated Barsotti-Tate group schemes, *J. Math. Sci. Univ. Tokyo* **16** (2009), no. **1**, 23–54.
- [10] J. S. Milne, *Arithmetic duality theorems*, Second edition. BookSurge, LLC, Charleston, SC, 2006.
- [11] M. Raynaud, Schémas en groupes de type (p, \dots, p) , *Bull. Soc. Math. France* **102** (1974), 241–280.
- [12] D. Rössler, A note on the ramification of torsion points lying on curves of genus at least two, *J. Théor. Nombres Bordeaux* **22** (2010), no. **2**, 475–481.
- [13] 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

E-mail address: yuichiro@kurims.kyoto-u.ac.jp