

A note on the ramification of torsion points lying on curves of genus at least two

Damian RÖSSLER*

Abstract

Let C be a curve of genus $g \geq 2$ defined over the fraction field K of a complete discrete valuation ring R with algebraically closed residue field. Suppose that $\text{char}(K) = 0$ and that the characteristic of the residue field is not 2. Suppose that the Jacobian $\text{Jac}(C)$ has semi-stable reduction over R . Embed C in $\text{Jac}(C)$ using a K -rational point. We show that the coordinates of the torsion points lying on C lie in the unique tamely ramified quadratic extension of the field generated over K by the coordinates of the p -torsion points on $\text{Jac}(C)$.

1 Introduction

Let R be a complete discrete valuation ring. Suppose that the residue field k of R is algebraically closed and of characteristic $p \geq 0$. Suppose that $p \neq 2$. Let K be the fraction field of R and suppose that $\text{char}(K) = 0$. Let C be a curve of genus $g \geq 2$ defined over K . Let $j : C \rightarrow \text{Jac}(C)$ be the closed immersion of C into its Jacobian defined by a K -rational point. Let $A := \text{Jac}(C)$. Let \mathcal{A} be the Néron model of A over R .

Let $L := K(A[p](\bar{K}))$ be the extension of K generated by the coordinates of the p -torsion points of $A(\bar{K})$. In particular, $L = K$ if $p = 0$. Let L' be the unique tamely ramified quadratic extension of L .

Finally, let $K_1 \subseteq \bar{K}$ be the field generated over K by the coordinates of the elements of $\text{Tor}(A(\bar{K})) \cap C(\bar{K})$. Here $\text{Tor}(A(\bar{K}))$ is the subgroup of $A(\bar{K})$ consisting of elements of finite order.

*Département de Mathématiques, Bâtiment 425, Faculté des Sciences d'Orsay, Université Paris-Sud, 91405 Orsay Cedex, FRANCE, E-mail: damian.rossler@math.u-psud.fr, Homepage: <http://www.math.u-psud.fr/~rossler>

The aim of this note is to prove the following statement :

Theorem 1.1. *Suppose that the connected component of the special fiber \mathcal{A}_k of \mathcal{A} is a semi-abelian variety (i.e. A has semi-stable reduction over R). Then we have*

- (a) $K_1 \subseteq L'$;
- (b) if C is not hyperelliptic then we have $K_1 \subseteq L$.

Corollary 1.2. *If $p > 3$, the inequality*

$$[K_1 : K] \leq 2 \cdot \#\mathrm{GL}_{2g}(\mathbb{Z}/3\mathbb{Z}) \cdot \#\mathrm{GL}_{2g}(\mathbb{Z}/p\mathbb{Z})$$

is verified.

Corollary 1.2 is an immediate consequence of Theorem 1.1 and of Raynaud's criterion of semi-stable reduction. Recall that according to this criterion, A will have semi-stable reduction over K if the l -torsion points of A are K -rational, for some prime number l such that $l \neq p$ and $l > 2$ (see [6, IX]).

For the convenience of the reader, we recall the formula

$$\#\mathrm{GL}_{2g}(\mathbb{Z}/l\mathbb{Z}) = (l^{2g} - 1) \cdot (l^{2g} - l) \cdots (l^{2g} - l^{2g-1}),$$

which is valid for any prime number l .

Theorem 1.1 should be understood as a complement to some results of Tamagawa (see [10]), Baker-Ribet (see [2]) and Coleman (see [5]).

For instance, with the present notation, suppose that $p > 0$, that R is the maximal unramified extension of \mathbb{Q}_p and that the abelian part of the connected component of \mathcal{A}_k is an ordinary abelian variety. Tamagawa then proves that K_1 is contained in the extension of K generated by the p -th roots of unity (see [10] or [2, Th. 4.1]). Another example is the following result of Coleman : if $p > \max(2g, 5)$, R is the maximal unramified extension of \mathbb{Q}_p and \mathcal{A}_k is an abelian variety, then $K_1 \subseteq K$ (see [5, Conj. B]).

All these results restrict the size of K_1 under various hypotheses on the special fiber \mathcal{A}_k and on the order of absolute ramification of K . The interest of Theorem 1.1 and its corollary is that they provide a limit for the size of K_1 with no assumption on the absolute ramification of K and little or no assumptions on the special fiber \mathcal{A}_k .

Remark. (1) The avoidance of the prime $p = 2$ is critical. It appears in both Lemma 2.4 and Lemma 2.6 and this is exploited at the end of the proof of Theorem 1.1. It would be interesting to extend the method used in this note to the case $p = 2$.

(2) A closer examination of the proof of Theorem 1.1 (b) shows that the following statement holds. Let $x \in \text{Tor}(A(\bar{K})) \cap C(\bar{K})$. Suppose that C is hyperelliptic. If x is not a fixed point of the uniquely defined hyperelliptic involution of C , then the field generated over K by the coordinates of x is included in L .

Notations. If l is a prime number and G is an abelian group, we write $\text{Tor}^l(G)$ for the set of elements of $\text{Tor}(G)$ whose order is prime to l and $\text{Tor}_l(G)$ for the set of elements of $\text{Tor}(G)$ whose order is a power of l . The expression $\text{Tor}^0(G)$ will stand for $\text{Tor}(G)$. We shall denote by $+$ the group law on $A(\bar{L})$. We shall write divisors on $C_{\bar{L}}$ in the form

$$n_1 P_1 \oplus n_2 P_2 \oplus \cdots \oplus n_r P_R$$

where $n_i \in \mathbb{Z}$. The symbol \sim will be used to denote linear equivalence of divisors.

Acknowledgments. I am grateful to M. Baker and J. Boxall for their feedback and for some useful comments.

2 Proof of Theorem 1.1

Let L^t be the maximal tamely ramified extension of L . Let $I := \text{Gal}(\bar{L}|L)$, $I^w := \text{Gal}(\bar{L}|L^t)$ and $I^t := \text{Gal}(L^t|L)$. Recall that $I^w = 0$ if $\text{char}(k) = 0$ and that there is a non-canonical isomorphism $I^t \simeq \bigoplus_{l \neq p, l \text{ prime}} \mathbb{Z}_l$ (see [9, chap. IV]). Furthermore, the group I^w is a pro- p -group if $p > 0$.

We shall need the following five results.

Theorem 2.1 (monodromy theorem). *For any $x \in \text{Tor}^p(A(\bar{L}))$ and any $\sigma \in I$, the equation $\sigma^2(x) - 2\sigma(x) + x = 0$ is satisfied.*

Proof. See [6, IX, 5.12.2] \square

Lemma 2.2. *The action of I^w on $\text{Tor}^p(A(\bar{L}))$ is trivial.*

Proof. This is a direct consequence of Theorem 2.1. See for instance [2, Appendix, Lemma A.1]. \square

Lemma 2.3. *The action of I^t on $\text{Tor}_p(A(L^t))$ is trivial.*

Proof. We may restrict ourselves to the case where $p > 0$. Let $T \subseteq \text{Tor}_p(A(L^t))$ be a finite I^t -invariant subgroup. We have to show that the action of I^t on T is trivial. The action

of I^t on T preserves the order of elements, hence T is an inner direct sum of G^t -invariants subgroups of the form $(\mathbb{Z}/p^r)^s$. Hence we might suppose without loss of generality that $T \simeq (\mathbb{Z}/p^r)^s$ for some $r, s \leq 1$. Let T_p be the subgroup of p -torsion elements of T . The fact that the p -torsion points in $A(\bar{L})$ are L -rational implies that the action of G^t on T_p is trivial. Hence the image of G^t in $\text{Aut}(T)$ lies in the kernel of the natural group map

$$\text{Aut}(T) \rightarrow \text{Aut}(T_p)$$

Under the above isomorphism $T \simeq (\mathbb{Z}/p^r)^s$, this corresponds to $s \times s$ -matrices of the form $\text{Id} + pM$, where M is an $s \times s$ -matrices with coefficients in $\mathbb{Z}/p^r\mathbb{Z}$. This last fact is a consequence of the fact that multiplication by p^{r-1} induces an I^t -equivariant isomorphism $T/pT \rightarrow T_p$. The calculation $(\text{Id} + pM)^{p^{r-1}} = \text{Id}$ now shows that the image of I^t in $\text{Aut}(T)$ is a p -group. On the other hand, I^t is a direct sum of pro- l -groups, with $l \neq p$. The order of the image of I^t is thus prime to p . This image is thus trivial. \square

Lemma 2.4 (Boxall). *Let B be an abelian variety over a field F of characteristic 0. Let $l > 2$ be a prime number and let $L := F(B[l])$ be the extension of K generated by the l -torsion points of B . Let $P \in \text{Tor}_l(B(\bar{L}))$ and suppose that $P \notin B(L)$. Then there exists $\sigma \in \text{Gal}(\bar{L}|L)$ such that $\sigma(P) - P \in B[l](\bar{L}) \setminus \{0\}$.*

Proof. See [4, Lemme 1] or [8, Prop. 3]. \square

Lemma 2.5. *Let $P \oplus Q$ and $P' \oplus Q'$ be two divisors of degree 2 on $C_{\bar{L}}$. Suppose that $P \oplus Q$ and $P' \oplus Q'$ are linearly equivalent.*

If C is not hyperelliptic, then the two divisors coincide.

If C is hyperelliptic, then either the two divisors coincide or we have $Q = \iota(P)$ and $Q' = \iota(P')$.

Here $\iota : C \rightarrow C$ is the uniquely defined hyperelliptic involution.

Proof. See [7, IV, Prop. 5.3]. \square

Lemma 2.6. *Let $x \in A(\bar{L})$ and suppose that $x \neq 0$. The inequality*

$$\#(C(\bar{L}) \cap (C(\bar{L}) + x)) \leq 2 \tag{1}$$

is then verified. If C is not hyperelliptic, we even have

$$\#(C(\bar{L}) \cap (C(\bar{L}) + x)) \leq 1. \tag{2}$$

This Lemma is a consequence of [1, Prop. 4]. For the convenience of the reader, we provide the following proof.

Proof. We shall write O for the K -rational point on C , which is used to embed C in A .

Let $a_1, \dots, a_r \in C(\bar{L})$ be pairwise distinct points such that $a_1 + x, a_2 + x, \dots, a_r + x \in C(\bar{L})$. Let $b_i := a_i + x$ ($i = 1, \dots, r$).

Suppose first that $r > 1$ and that C is not hyperelliptic. We then have a linear equivalence

$$b_1 \oplus a_2 \sim b_2 \oplus a_1 \quad (3)$$

Hence either $b_1 = b_2$ or $b_1 = a_1$, either of which are ruled out. So we conclude that if C is not hyperelliptic, then $r \leq 1$. This proves the inequality (2).

Now suppose that C is hyperelliptic and that $r > 2$. Let $\iota : C \rightarrow C$ be the corresponding hyperelliptic involution. On top of (3), we then have the further linear equivalence

$$b_2 \oplus a_3 \sim a_2 \oplus b_3$$

Lemma 2.5 now implies that $a_2 = \iota(b_1)$ and $a_2 = \iota(b_3)$. Hence $b_1 = b_3$, which is impossible. Thus we conclude that $r \leq 2$, if C is hyperelliptic. This proves the first inequality (1). \square

We can now start with the proof of Theorem 1.1.

The monodromy theorem 2.1 says that for any $x \in \text{Tor}^p(A(\bar{L}))$ and any $\sigma \in I$ the equation $(\sigma - \text{Id})^2(x) = 0$ is satisfied (remember that $\text{Tor}^p(\cdot) = \text{Tor}(\cdot)$ if $p = 0$). On the other hand, Lemma 2.2 says that $\text{Tor}^p(A(\bar{L})) \subseteq \text{Tor}^p(A(L^t))$ and Lemma 2.3 implies that $\sigma(x) = x$ for any $x \in \text{Tor}_p(A(L^t))$ and any $\sigma \in I^t$. Hence the equation

$$(\sigma - \text{Id})^2(x) = 0 \quad (4)$$

is verified for any $x \in \text{Tor}(A(L^t))$ and any $\sigma \in I^t$. Let $x \in \text{Tor}(A(L^t)) \cap C(\bar{L})$ and $\sigma \in I^t$. The equation (4) implies the linear equivalence

$$\sigma^2(x) \oplus x \sim 2\sigma(x) \quad (5)$$

of divisors of degree 2 on $C_{\bar{L}}$.

First suppose that C is not hyperelliptic; then any two linearly equivalent divisors of degree 2 on $C_{\bar{L}}$ coincide (see Lemma 2.5) and the relation (5) thus implies that $x = \sigma(x)$.¹

Summing up, there is an inclusion

$$\text{Tor}(A(L^t)) \cap C(\bar{L}) \subseteq A(L)$$

¹This calculation is partly the motivation for Ribet's definition of an "almost rational point" (see [2, Lemma 2.7]) and is the starting point of Tamagawa's article [10] (see Prop. 0.2 in that reference).

if C is not hyperelliptic.

Now suppose that C is hyperelliptic and let $\iota : C \rightarrow C$ be the uniquely defined hyperelliptic involution. Lemma 2.5 then implies that either $x = \sigma(x)$ as above or that the equations $\iota(\sigma(x)) = \sigma(x)$ and $\iota(x) = \sigma^2(x)$ hold. Suppose the latter. Since ι is defined over L , the equation $\iota(\sigma(x)) = \sigma(x)$ implies that $\iota(x) = x$. This together with the equation $\iota(x) = \sigma^2(x)$ implies that $\sigma^2(x) = x$.

Now notice that since the group I^t is abelian, the set $(I^t)^2$ of squares of elements is a normal subgroup of I^t . Let J' be the Galois extension of L defined by $(I^t)^2$. Since $I^t \simeq \bigoplus_{l \neq p, l \text{ prime}} \mathbb{Z}_l$, we see that $[J' : L] = 2$. In the last paragraph, we showed that $\text{Tor}(A(L^t)) \cap C(\bar{L})$ is fixed by $(I^t)^2$. In other words, we have shown that $\text{Tor}(A(L^t)) \cap C(\bar{L}) \subseteq A(J')$ where J' is the unique tamely ramified quadratic extension of L . In the notation of the introduction, $J' = L'$.

Summing up, we see that

$$\text{Tor}(A(L^t)) \cap C(\bar{L}) \subseteq A(L')$$

if C is hyperelliptic.

If $p = 0$, then $L^t = \bar{K}$ so this completes the proof of Theorem 1.1 in that case.

Now let $x \in \text{Tor}(A(\bar{L})) \cap C(\bar{L}) \setminus C(L^t)$. Let $x = x^p + x_p$ be the decomposition of x into its components of prime-to- p torsion and p -primary torsion, respectively. Lemma 2.3 implies that $x_p \in A(\bar{L}) \setminus A(L^t)$. Also, using Boxall's lemma 2.4 and the fact that L contains the coordinates of the p -torsion points, we see that there exists $\sigma_x \in I^w$ such that $\sigma_x(x) - x = \sigma_x(x_p) - x_p \in A[p](L) \setminus \{0\}$. Hence

$$\sigma_x(x) \in \bigcup_{\tau \in A[p](L) \setminus \{0\}} C(\bar{L}) \cap (C(\bar{L}) + \tau). \quad (6)$$

Lemma 2.6 now implies that

$$\#(C(\bar{L}) \cap (C(\bar{L}) + \tau)) \leq 2 \quad (7)$$

for all $\tau \in A[p](L) \setminus \{0\}$. Notice that if $\sigma_x(x) \in C(\bar{L}) \cap (C(\bar{L}) + \tau_0)$ for a particular $\tau_0 \in A[p](L) \setminus \{0\}$, then we have

$$\{\sigma_x(x), \sigma_x^2(x), \dots, \sigma_x^p(x)\} \subseteq C(\bar{L}) \cap (C(\bar{L}) + \tau_0)$$

(remember that by construction τ_0 is fixed by I^w). On the other hand

$$\{\sigma_x(x), \sigma_x^2(x), \dots, \sigma_x^p(x)\} = \{x + \tau_0, x + 2\tau_0, \dots, x + p\tau_0 = x\}.$$

Since $p > 2$ and τ_0 has exact order p in $A(\bar{K})$, this leads to a contradiction. Thus we have

$$\mathrm{Tor}(A(\bar{L})) \cap C(\bar{L}) \subseteq A(L^t).$$

Now remember that we have shown above (see the italicized sentences) that $\mathrm{Tor}(A(L^t)) \cap C(\bar{L}) \subseteq A(L)$ if C is not hyperelliptic and that $\mathrm{Tor}(A(L^t)) \cap C(\bar{L}) \subseteq A(L')$ if C is hyperelliptic. This concludes the proof of (a) and (b).

References

- [1] Matthew Baker and Bjorn Poonen, *Torsion packets on curves*, Compositio Math. **127** (2001), no. 1, 109–116.
- [2] Matthew H. Baker and Kenneth A. Ribet, *Galois theory and torsion points on curves*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 11–32 (English, with English and French summaries). Les XXIIèmes Journées Arithmétiques (Lille, 2001).
- [3] John Boxall, *Autour d'un problème de Coleman*, C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), no. 10, 1063–1066 (French, with English and French summaries).
- [4] ———, *Sous-variétés algébriques de variétés semi-abéliennes sur un corps fini*, Number theory (Paris, 1992), London Math. Soc. Lecture Note Ser., vol. 215, Cambridge Univ. Press, Cambridge, 1995, pp. 69–80 (French, with English and French summaries).
- [5] Robert F. Coleman, *Ramified torsion points on curves*, Duke Math. J. **54** (1987), no. 2, 615–640.
- [6] *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin, 1972 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I); Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim.
- [7] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.
- [8] Damian Rössler, *A note on the Manin-Mumford conjecture*, Number fields and function fields—two parallel worlds, Progr. Math., vol. 239, Birkhäuser Boston, Boston, MA, 2005, pp. 311–318.
- [9] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.
- [10] Akio Tamagawa, *Ramification of torsion points on curves with ordinary semistable Jacobian varieties*, Duke Math. J. **106** (2001), no. 2, 281–319.