

# Torsion Points of Abelian Varieties with Values in Infinite Extensions over a $p$ -adic Field

By

Yoshiyasu OZEKI\*

## Abstract

Let  $A$  be an abelian variety over a  $p$ -adic field  $K$  and  $L$  an algebraic infinite extension over  $K$ . We consider the finiteness of the torsion part of the group of rational points  $A(L)$  under some assumptions. In 1975, Hideo Imai proved that such a group is finite if  $A$  has good reduction and  $L$  is the cyclotomic  $\mathbb{Z}_p$ -extension of  $K$ . In this paper, first we show a generalization of Imai's result in the case where  $A$  has good ordinary reduction. Next we give some finiteness results when  $A$  is an elliptic curve and  $L$  is the field generated by the  $p$ -th power torsion of an elliptic curve.

## §1. Introduction

Let  $K$  be a finite extension of the  $p$ -adic number field  $\mathbb{Q}_p$  with residue field  $k$  and fix an algebraic closure  $\bar{K}$  of  $K$ . Let  $A$  be an abelian variety over  $K$ . If  $L \subset \bar{K}$  is a finite extension over  $K$ , it is well-known that the torsion part of the  $L$ -rational points  $A(L)$  is finite (cf. [5], Thm. 7). On the other hand, in general, much less is known whether the torsion part of  $A(L)$  is finite or infinite if  $L \subset \bar{K}$  is an infinite algebraic extension over  $K$ . We are interested in understanding whether the torsion part of  $A(L)$  is finite or infinite. As one of the known results, Imai ([4]) proved that the torsion part of  $A(K(\mu_{p^\infty}))$  is finite if  $A$  has potential good reduction, where  $K(\mu_{p^\infty})$  is the smallest field containing  $K$  and all  $p$ -th power roots of unity. In this connection we first prove the following:

---

Communicated by A. Tamagawa. Received November 26, 2008. Revised April 23, 2009.  
2000 Mathematics Subject Classification(s): 11G10, 11G07, 11S99, 22E50.

Key words: abelian variety, Galois representation,  $p$ -adic Lie group.

Supported by the JSPS Fellowships for Young Scientists.

\*Graduate School of Mathematics, Kyushu University, Fukuoka 812-8581, Japan.

e-mail: y-ozeki@math.kyushu-u.ac.jp

**Theorem 1.1.** *Let  $A$  be an abelian variety over  $K$  which has potential good ordinary reduction. Let  $L$  be an algebraic extension of  $K$  with residue field  $k_L$ .*

- (1) *Assume that the residue field of  $L(\mu_{p^\infty})$  is a potential prime-to- $p$  extension of  $k$  (in the sense of Def. 2.1). Then  $A(L)[p^\infty]$  is finite.*
- (2) *If  $L$  contains  $K(A[p])$  and  $K(\mu_{p^\infty})$ , then  $k_L$  is a potential prime-to- $p$  extension of  $k$  if and only if  $A(L)[p^\infty]$  is finite.*
- (3) *Assume that  $L(\mu_{p^\infty})$  is a Galois extension of  $K$  whose residue field is finite. Then the torsion part of  $A(L)$  is finite.*

Here we denote by  $K(A[p])$  the field generated by the coordinates of all  $p$ -torsion points of  $A$ . The proof of the above Theorem is given in Theorem 2.1 and Corollary 2.1. This theorem is a generalization of Imai's theorem under the hypothesis that  $A$  has good ordinary reduction. We can also obtain the global case of this theorem, see Section 2.4. As an easy consequence of Theorem 1.1 (2), we see that the group  $A(K(\mu_\infty))[p^\infty]$  is infinite for an abelian variety  $A$  as in the theorem if we replace  $K$  with its suitable finite extension (here we denote by  $K(\mu_\infty)$  the field obtained by adjoining all roots of unity to  $K$ ). We shall point out that such a group must be finite *in the global case* by a result of Ribet ([7]).

Next we consider the finiteness of the torsion part of  $A(L)$  for  $L = K_{B,p} := K(B[p^\infty])$ , the field generated by the coordinates of all  $p$ -th power torsion points of a semiabelian variety  $B$ . For example,  $K_{\mathbb{G}_m,p}$  is the cyclotomic field  $K(\mu_{p^\infty})$ , where  $\mathbb{G}_m$  is the multiplicative group over  $K$ . Hence Imai's theorem is a result on the torsion part of  $A(K_{\mathbb{G}_m,p})$ . From such a point of view, we raise the following question:

**Question.** Let the notation be as above. Then is the torsion part of  $A(K_{B,p})$  finite?

The torsion part of  $A(K_{B,p})$  is finite if and only if  $A(K_{B,p})[\ell^\infty]$  is finite for all primes  $\ell$  and  $A(K_{B,p})[\ell^\infty] = 0$  for almost all primes  $\ell$ . For any prime  $\ell \neq p$ , it is easy to see that the  $\ell$ -part of  $A(K_{B,p})$  is finite (cf. Prop. 3.1). Hence we are interested in the finiteness of the  $p$ -part of  $A(K_{B,p})$ . If  $A = E_1$  and  $B = E_2$  are elliptic curves, we can gain various results by distinguishing the reduction types of  $E_1$  and  $E_2$ , see the table below.

**Theorem 1.2.** *The finiteness of  $E_1(K_{E_2,p})[p^\infty]$  is as follows:*

| $E_1$          |         | $E_2$ |         | $\sharp E_1(K_{E_2,p})[p^\infty]$ | statement  |
|----------------|---------|-------|---------|-----------------------------------|------------|
| ord            |         | ord   |         | “ $\infty$ ” $^{*_1}$             | Prop. 3.4  |
|                |         | ss    |         | finite                            | Cor. 3.2   |
|                |         | mult  |         | finite                            | Cor. 3.2   |
| ss             | FCM     | ord   | CM      | finite $^{*_2}$                   | Prop. 3.6  |
|                |         |       | non-CM  | finite                            | Prop. 3.6  |
|                |         | ss    | FCM     | “finite”                          | Prop. 3.7  |
|                |         |       | non-FCM | finite                            | Prop. 3.6  |
|                | non-FCM | ord   | CM      | finite                            | Prop. 3.6  |
|                |         |       | non-CM  | finite                            | Prop. 3.6  |
|                |         | ss    | FCM     | finite                            | Prop. 3.6  |
|                |         |       | non-FCM | finite or $\infty^{*_3}$          | Prop. 3.8  |
| split mult     |         | any   |         | $\infty$                          | Prop. 3.9  |
| non-split mult |         | any   |         | “finite”                          | Prop. 3.10 |

Here "ord", "ss", "mult", "CM" and "FCM" in the above table stand for ordinary, supersingular, multiplicative, complex multiplication and formal complex multiplication, respectively. The definition of "formal complex multiplication" is given in Section 3.2. The symbols  $*_1$ ,  $*_2$  and  $*_3$  in the table imply the followings:

$*_1 \cdots E_1, E_2$  : good ordinary reduction

$\Rightarrow E_1(K_{E_2,p})[p^\infty]$  is infinite in many cases.

$*_2 \cdots E_1$  : good supersingular reduction with formal complex multiplication

$E_2$  : good ordinary reduction with complex multiplication

$\Rightarrow E_1(K_{E_2,p})[p^\infty]$  is finite in all cases.

$*_3 \cdots E_1, E_2$  : good supersingular reduction without formal complex multiplication

$\Rightarrow E_1(K_{E_2,p})[p^\infty]$  may be finite or infinite (case by case).

For more precise information of Theorem 1.2, see the corresponding statements of the table.

## §2. Finiteness Theorems for Abelian Varieties

In this section, we prove Theorem 1.1 given in the Introduction and consider the global case for this theorem.

Let  $p$  be a prime number. Let  $A$  be an abelian variety over a field  $F$  of dimension  $d$  and  $A^\vee$  the dual abelian variety of  $A$ . Fix an algebraic closure

$\bar{F}$  of  $F$  and a separable closure  $F^{\text{sep}}$  of  $F$  in  $\bar{F}$ . Put  $G_F := \text{Gal}(F^{\text{sep}}/F)$ , the absolute Galois group of  $F$ . For any algebraic extension  $L$  over  $F$  and any integer  $n > 0$ , We denote by  $A(L)[p^n]$  the kernel of the multiplication-by- $p^n$  map of the  $L$ -rational points  $A(L)$  of  $A$  and put  $A(L)[p^\infty] := \bigcup_{n>0} A(L)[p^n]$ . We denote by  $F_{A[p^n]} = F(A[p^n])$  the field generated by the coordinates of  $A(F^{\text{sep}})[p^n] = A(\bar{F})[p^n]$ . Put  $F_{A,p} = F(A[p^\infty]) := \bigcup_{n>0} F_{A[p^n]}$ . Then the field  $F_{A,p}$  contains  $F(\mu_{p^\infty})$ , the field adjoining all  $p$ -th power roots of unity to  $F$ . The natural continuous representation associated to the Tate module  $T_p(A)$  of  $A$  is denoted by

$$\rho_{A,p} : G_F \rightarrow GL(T_p(A)) \simeq GL_h(\mathbb{Z}_p)$$

for some  $h \geq 0$  and denote its residual representation by

$$\bar{\rho}_{A,p} : G_F \xrightarrow{\rho_{A,p}} GL_h(\mathbb{Z}_p) \xrightarrow{\text{mod } p} GL_h(\mathbb{F}_p) (\simeq GL(A(F^{\text{sep}})[p])).$$

By abuse of notation, we shall consider  $\rho_{A,p}$  as the representation of  $V_p(A) = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ . We note that the definition field of the representation  $\rho_{A,p}$  (resp.  $\bar{\rho}_{A,p}$ ) is the field  $F_{A,p}$  (resp.  $F_{A[p]}$ ).

## §2.1. Some properties of torsion points

In this subsection, we collect some (in-)finiteness properties of the torsion part of abelian varieties which are easy to prove.

First we note the following proposition, which plays an important role throughout this paper:

**Proposition 2.1.**  *$A(L)[p^\infty]$  is finite if and only if the fixed subgroup  $T_p(A)^{G_L}$  of  $T_p(A)$  by the absolute Galois group  $G_L$  of  $L$  is 0.*

*Proof.* This immediately follows from the definition of Tate module and the fact that each  $A(L)[p^n]$  is finite.  $\square$

The field  $F(A[p])$  is a finite Galois extension of  $F$  whose Galois group  $\text{Gal}(F(A[p])/F)$  is a subgroup of  $GL_h(\mathbb{F}_p)$  for the integer  $h \geq 0$  such that  $A(\bar{F})[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus h}$ . Put  $g_{h,p} := (p^h - 1)(p^h - p) \cdots (p^h - p^{h-1})$ , the order of  $GL_h(\mathbb{F}_p)$ .

**Proposition 2.2.** (1) *If the absolute Galois group  $G_F$  of  $F$  is an inverse limit of finite groups of order prime to  $p$ , then*

$$A(F_{A[p]})[p^\infty] = A(F^{\text{sep}})[p^\infty].$$

(2) If the absolute Galois group  $G_F$  of  $F$  is an inverse limit of finite groups of order prime to  $g_{h,p}$ , then

$$A(F)[p^\infty] = A(F^{\text{sep}})[p^\infty].$$

*Proof.* (1) If the group  $A(F^{\text{sep}})[p^\infty]$  is 0, there is nothing to prove and hence we may assume that  $A(F^{\text{sep}})[p^\infty] \neq 0$ . Hence, for some  $h > 0$ ,  $\rho_{A,p}|_{G_{F_{A[p]}}}$  has values in the kernel of the reduction map  $GL_h(\mathbb{Z}_p) \rightarrow GL_h(\mathbb{F}_p)$ , which is a pro- $p$  group. Since  $G_{F_{A[p]}}$  is an inverse limit of finite groups of order prime to  $p$ , the representation  $\rho_{A,p}|_{G_{F_{A[p]}}}$  is trivial and thus we have

$$A(\bar{F})[p^\infty] = A(\bar{F})[p^\infty]^{\ker \rho_{A,p}} \subset A(\bar{F})[p^\infty]^{G_{F_{A[p]}}} = A(F_{A,p})[p^\infty].$$

This completes the proof of (1).

(2) We use the same argument as (1) except only that we do not need to consider  $F_{A[p]}$  since  $\rho_{A,p}|_{G_F}$  is already trivial.  $\square$

If there is a Galois equivariant homomorphism among two Tate modules of abelian varieties, we can see some infiniteness properties about torsion points of abelian varieties.

**Proposition 2.3.** *Let  $A$  and  $B$  be abelian varieties over  $F$ . If*

$$\text{Hom}_{\mathbb{Z}_p[G_F]}(T_p(B), T_p(A)) \neq 0,$$

*then  $A(F_{B,p})[p^\infty]$  is infinite.*

*Proof.* Take  $f$  to be a non-trivial element of  $\text{Hom}_{\mathbb{Z}_p[G_F]}(T_p(B), T_p(A))$ . Then  $T_p(B)/\ker(f)$  is a non-zero subspace of  $T_p(A)$  with trivial  $G_{F_{B,p}}$ -action. This implies the desired statement.  $\square$

**Definition 2.1.** Let  $L$  be an algebraic extension of  $F$ .

(1) We say that  $L$  is a *prime-to- $p$  extension* of  $F$  if  $L$  is a union of finite extensions over  $F$  of degree prime-to- $p$ .

(2) We say that  $L$  is a *potential prime-to- $p$  extension* of  $F$  if  $L$  is a prime-to- $p$  extension over some finite extension field of  $F$ .

**Proposition 2.4.** *Assume that  $A$  has the following property: for any finite Galois extension  $F'$  of  $F$ , the torsion part of  $A(F')$  is finite. Then  $A(L)[p^\infty]$  is finite for any potential prime-to- $p$  Galois extension  $L$  of  $F$ .*

*Proof.* The assertion follows from the facts that

$$A(L)[p^\infty] = A(L \cap F_{A,p})[p^\infty]$$

and  $L \cap F_{A,p}$  is a finite Galois extension of  $F$ .  $\square$

Note that we can apply Proposition 2.4 if  $F$  is one of the following fields:

- (i) a finitely generated field over a prime field,
- (ii) a finite extension of  $\mathbb{Q}_p$ .

**Proposition 2.5.** *Let  $F$  be a finite field of characteristic  $p > 0$  and  $F_p$  the maximal pro- $p$ -extension of  $F$  in  $\bar{F}$ . Assume that  $A(\bar{F})[p]$  is not trivial.*

*(1) Suppose that  $A(\bar{F})[p]$  is rational over  $F$ . Then  $A(L)[p^\infty]$  is finite if and only if  $L$  is a potential prime-to- $p$  extension over  $F$ . Furthermore in the other case,  $A(L)[p^\infty] = A(\bar{F})[p^\infty]$ .*

*(2)  $F_{A,p} = F_p(A[p])$ .*

*Proof.* (1) First we note that  $F_p = F_{A,p}$  because  $A(\bar{F})[p] \neq 0$  and  $F$  is a finite field of characteristic  $p$ . If  $L$  is a potential prime-to- $p$  extension over  $F$ , Prop. 2.4 implies that  $A(L)[p^\infty]$  is finite. In the other case,  $L$  contains  $F_p$  and hence  $A(L)[p^\infty]$  is infinite.

(2) If we put  $F' := F(A[p])$ , we see that  $F_{A,p}$  coincides with  $F'_p$ , the maximal pro- $p$ -extension of  $F'$ . Since  $F'_p = F_p(A[p])$ , we have done.  $\square$

## §2.2. Finiteness theorems for abelian varieties with good ordinary reduction

Let  $K$  be a finite extension of  $\mathbb{Q}_p$  with integer ring  $\mathcal{O}_K$  and residue field  $k$ . Let  $I_K$  be the inertia subgroup of  $G_K$ . If an abelian variety  $A$  over  $K$  has good reduction, we denote by  $\tilde{A}$  the reduction of  $A$  over  $k$ . For any  $p$ -divisible group  $G$  over  $\mathcal{O}_K$ , we denote its Tate module, Tate comodule, connected component and maximal étale quotient by  $T_p(G)$ ,  $\Phi_p(G)$ ,  $G^0$  and  $G^{\text{ét}}$ , respectively and put  $V_p(G) := T_p(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ .

Before proving Theorem 1.1 given in the Introduction, we shall show the proposition related with the matrix of the representation attached to abelian varieties by an analogous proof due to Conrad ([1], Thm. 1.1).

**Proposition 2.6.** *Let  $A$  be an abelian variety over  $K$  of dimension  $d$  which has good reduction.*

(1) The representation  $\rho_{A,p}$  has the form

$$\begin{pmatrix} S_A & U_A \\ 0 & T_A \end{pmatrix}$$

with respect to a suitable basis of  $T_p(A)$ . Here, for some integer  $0 \leq f \leq d$ ,

- (i)  $S_A : G_K \rightarrow GL_{2d-f}(\mathbb{Z}_p)$  is a continuous homomorphism,
  - (ii)  $T_A : G_K \rightarrow GL_f(\mathbb{Z}_p)$  is an unramified continuous homomorphism and
  - (iii)  $U_A : G_K \rightarrow M_{2d-f,f}(\mathbb{Z}_p)$  is a map.
- (2) If  $A$  has good ordinary reduction over  $K$ , then  $f = d$  and  $S_A|_{I_K}$  is conjugate with the direct sum of the  $p$ -adic cyclotomic characters  $\varepsilon^{\oplus d}$ .
- (3) If  $A$  has good ordinary reduction over  $K$ , the map  $S_A$  is conjugate with the map  $\varepsilon \cdot ({}^tT_{A^\vee})^{-1}$ .

Here, explicitly, the map  $\varepsilon^{\oplus d} : G_K \rightarrow GL_d(\mathbb{Z}_p)$  is given by the equation

$$\varepsilon^{\oplus d}(\sigma) = \text{diag}(\varepsilon(\sigma)) \in GL_d(\mathbb{Z}_p),$$

the diagonal matrix with coefficients  $\varepsilon(\sigma)$  for all  $\sigma \in G_K$ , and for any map  $T : G_K \rightarrow GL_d(\mathbb{Z}_p)$ , we denote by  ${}^tT$  the map  $G_K \rightarrow GL_d(\mathbb{Z}_p)$  defined by

$${}^tT(\sigma) := {}^t(T(\sigma)) \in GL_d(\mathbb{Z}_p)$$

for all  $\sigma \in G_K$ , where  ${}^t(T(\sigma))$  is the transposed matrix of  $T(\sigma)$ .

*Proof of Proposition 2.6.* (1) Let  $\mathcal{A}$  be the Néron model of  $A$  over  $\mathcal{O}_K$  and  $\mathcal{A}(p)$  the  $p$ -divisible group associated to  $\mathcal{A}$ . The connected-étale sequence of  $\mathcal{A}(p)$  induces the exact sequence

$$0 \rightarrow V_p(\mathcal{A}(p)^0) \rightarrow V_p(\mathcal{A}(p)) \rightarrow V_p(\mathcal{A}(p)^{\text{ét}}) \rightarrow 0$$

of  $\mathbb{Q}_p[G_K]$ -modules. The desired decomposition of  $\rho_{A,p}$  can be obtained by this sequence.

(2) Assume the reduction type of  $\mathcal{A}$  over  $\mathcal{O}_K$  is ordinary. Let  $K^{\hat{u}r}$  be the completion of the maximal unramified extension  $K^{ur}$  over  $K$  and  $\mathcal{O}_{K^{\hat{u}r}}$  the integer ring of  $K^{\hat{u}r}$ . Then  $\hat{\mathcal{A}}_{\mathcal{O}_{K^{\hat{u}r}}} := \hat{\mathcal{A}} \times_{\mathcal{O}_K} \text{Spf}(\mathcal{O}_{K^{\hat{u}r}})$  is isomorphic to  $\hat{\mathbb{G}}_m^{\oplus d}$  over  $\mathcal{O}_{K^{\hat{u}r}}$ , where  $\hat{\mathcal{A}}$  is the formal completion of  $\mathcal{A}$  along its zero section and  $\hat{\mathbb{G}}_m$  is the formal multiplicative group over  $\mathcal{O}_{K^{\hat{u}r}}$  (cf. [6], Lem. 4.26 and Lem. 4.27). This implies the assertion (2).

(3) Consider the following two exact sequences as  $G_K$ -modules;

$$\begin{aligned} 0 \rightarrow V_p(\mathcal{A}(p)^{\text{ét}})^\vee &\rightarrow V_p(\mathcal{A}(p))^\vee \rightarrow V_p(\mathcal{A}(p)^0)^\vee \rightarrow 0, \\ 0 \rightarrow V_p(\mathcal{A}^\vee(p)^0)(-1) &\rightarrow V_p(\mathcal{A}^\vee(p))(-1) \rightarrow V_p(\mathcal{A}^\vee(p)^{\text{ét}})(-1) \rightarrow 0, \end{aligned}$$

where  $M^\vee = \operatorname{Hom}_{\mathbb{Q}_p}(M, \mathbb{Q}_p)$  is the dual of a  $\mathbb{Q}_p[G_K]$ -module  $M$  and  $M(i)$  is the  $i$ -th Tate twist of  $M$ . Note that  $V_p(\mathcal{A}(p))^\vee \simeq V_p(\mathcal{A}^\vee(p))(-1)$  as  $G_K$ -modules. By taking the functor  $H^0(I_K, -)$  of the above exact sequences and using the assertion (2), we can see that

$$V_p(\mathcal{A}(p)^{\text{ét}})^\vee \simeq (V_p(\mathcal{A}(p))^\vee)^{I_K} \simeq (V_p(\mathcal{A}^\vee(p))(-1))^{I_K} \simeq V_p(\mathcal{A}^\vee(p)^0)(-1)$$

as  $G_K$ -modules, since  $I_K$  acts on  $V_p(\mathcal{A}(p)^{\text{ét}})^\vee$  and  $V_p(\mathcal{A}^\vee(p)^0)(-1)$  trivially, and  $I_K$  acts on  $V_p(\mathcal{A}(p)^0)^\vee$  and  $V_p(\mathcal{A}^\vee(p)^{\text{ét}})(-1)$  by  $(\varepsilon^{\oplus d})^{-1}$ . We know that the group  $G_K$  acts on  $V_p(\mathcal{A}(p)^{\text{ét}})^\vee(1)$  by  $\varepsilon \cdot ({}^tT_A)^{-1}$  and also acts on  $V_p(\mathcal{A}^\vee(p)^0)$  by  $S_{A^\vee}$ . Therefore, we see that  $\varepsilon \cdot ({}^tT_A)^{-1}$  is conjugate with  $S_{A^\vee}$  and thus we finish the proof of the assertion (3) after replacing  $A$  with  $A^\vee$ .  $\square$

*Remark.*

(1) The integer  $f$  is equal to the dimension of  $V_p(\tilde{A})$  and the map  $S_A$  is the natural continuous homomorphism

$$G_K \rightarrow GL(T_p(\mathcal{A}(p)^0)) \simeq GL_{2d-f}(\mathbb{Z}_p)$$

and the map  $T_A$  is the natural continuous homomorphism

$$G_K \rightarrow GL(T_p(\tilde{A})) \simeq GL_f(\mathbb{Z}_p).$$

(2) Suppose that  $A$  has good ordinary reduction over  $K$ . We denote the semi-simplification of  $\rho_{A,p}$  by  $\rho_{A,p}^{ss}$ . By Proposition 2.6, the representation  $\rho_{A,p}^{ss}|_{G_L}$  factors through  $G_{k_L}$  for any algebraic extension  $L$  of  $K$  such that  $L$  contains all  $p$ -th power roots of unity.

Now we can show our main finiteness theorem which is given in the Introduction.

**Theorem 2.1.** *Let  $A$  be an abelian variety over  $K$  which has potential good ordinary reduction. Let  $L$  be an algebraic extension of  $K$ .*

- (1) *Assume that the residue field of  $L(\mu_{p^\infty})$  is a potential prime-to- $p$  extension of  $k$ . Then  $A(L)[p^\infty]$  is finite.*
- (2) *Assume that  $L(\mu_{p^\infty})$  is a Galois extension of  $K$  whose residue field is finite. Then the torsion part of  $A(L)$  is finite.*

*Proof.* (1) By extending  $K$  and  $L$ , we may assume that  $A$  has good ordinary reduction over  $K$  and  $L$  contains  $K(\mu_{p^\infty})$ . Put  $d := \dim(A)$  and denote

by  $k_L$  the residue field of  $L$ . We have the following form of the representation  $\rho_{A,p}$  for a suitable basis of the  $\mathbb{Z}_p$ -module  $T_p(A)$ :

$$\begin{pmatrix} S_A & U_A \\ 0 & T_A \end{pmatrix},$$

with certain  $S_A = \varepsilon \cdot ({}^tT_{A^\vee})^{-1} : G_K \rightarrow GL_d(\mathbb{Z}_p)$ ,  $T_A : G_K \rightarrow GL_d(\mathbb{Z}_p)$  and  $U_A : G_K \rightarrow M_d(\mathbb{Z}_p)$  as in Proposition 2.6. In this proof, we shall fix the above basis and identify  $V_p(A)$  with  $\mathbb{Q}_p^{\oplus 2d} = M_{2d,1}(\mathbb{Q}_p)$ . Since  $L$  contains all  $p$ -th power roots of unity, we know that the maps  $S_A|_{G_L}$  and  $T_A|_{G_L}$  factor through the absolute Galois group  $G_{k_L} := \text{Gal}(k^{\text{sep}}/k_L)$  of  $k_L$ . Thus the maps  $S_A|_{G_L}$  and  $T_A|_{G_L}$  are determined by a topological generator  $\sigma_L$  of  $G_{k_L}$ . To prove  $V_p(A)^{G_L} = 0$ , it suffices to show that the matrices  $S_A(\sigma_L)$  and  $T_A(\sigma_L)$  do not have eigenvalue 1. First we assume that this assertion about  $T_A(\sigma_L)$  is false. Then the Tate module  $V_p(\tilde{A})^{G_L}$  is not zero and hence  $\tilde{A}(k_L)[p^\infty]$  is infinite. By Proposition 2.4, this contradicts the assumption that the field  $k_L$  is potential prime-to- $p$  extension of  $k$ . Next we show that  $S_A(\sigma_L)$  does not have eigenvalue 1. Since  $L$  contains  $K(\mu_{p^\infty})$  and  $A$  has good ordinary reduction, the map  $S_A|_{G_L}$  coincides with  $({}^tT_{A^\vee}|_{G_L})^{-1}$ . Hence if we assume  $S_A(\sigma_L)$  has eigenvalue 1, then  $T_{A^\vee}(\sigma_L)$  also has eigenvalue 1. But this induces a contradiction by the same argument as the above.

(2) The criterion of Néron-Ogg-Shafarevich implies that

$$A(L)' \subset A(L(\mu_{p^\infty}))' = A(L(\mu_{p^\infty}) \cap K^{\text{ur}})',$$

where the symbol  $'$  means the prime-to- $p$  part, and thus  $A(L)'$  is finite because  $L(\mu_{p^\infty})$  has a finite residue field. Note that the above equality  $A(L(\mu_{p^\infty}))' = A(L(\mu_{p^\infty}) \cap K^{\text{ur}})'$  comes from the assumption that  $L(\mu_{p^\infty})$  is a Galois extension of  $K$ . Therefore, the assertion (1) implies that the torsion points of  $A(L)$  is finite.  $\square$

**Corollary 2.1.** *Let  $A$  be an abelian variety over  $K$  which has good ordinary reduction. Let  $L$  be a Galois extension of  $K$  with residue field  $k_L$ . Assume that  $L$  contains  $K(\mu_{p^\infty})$  and  $K(A[p])$ . Then the followings are equivalent:*

- (1)  $A(L)[p^\infty]$  is finite,
- (2)  $A^\vee(L)[p^\infty]$  is finite,
- (3)  $\tilde{A}(k_L)[p^\infty]$  is finite,
- (4)  $\tilde{A}^\vee(k_L)[p^\infty]$  is finite,
- (5)  $k_L$  is a potential prime-to- $p$  extension over  $k$ .

Note that the Weil-paring implies that  $L$  contains  $K(\mu_{p^\infty})$  and  $K(A[p])$  if and only if  $L$  contains  $K(\mu_{p^\infty})$  and  $K(A^\vee[p])$ .

*Proof.* The equivalence of assertions (3), (4) and (5) follows from Proposition 2.5, thus it is enough to show that (1) is equivalent to (3), (4) and (5). By Theorem 2.1 (1), the condition (5) implies the condition (1).

Let us assume that the condition (4) is not satisfied. Then we know that  $T_{A^\vee}(\sigma_L)$  has eigenvalue 1, where  $T_{A^\vee}$  is a natural unramified homomorphism  $G_K \rightarrow GL(T_p(\tilde{A}^\vee))$  and  $\sigma_L$  is a topological generator of  $G_{k_L}$ . Hence  $\varepsilon \cdot ({}^tT_{A^\vee})^{-1}(\sigma_L)$  has also eigenvalue 1. By using this fact and Proposition 2.6, we can see that  $T_p(A)^{G_L}$  is not trivial. Therefore, the group  $A(L)[p^\infty]$  is infinite.  $\square$

### §2.3. $K^{\text{ur}}$ -rational points

We continue to use the same notation  $p$ ,  $K$ ,  $k$ ,  $A$  and  $d$  as in the previous subsection. In this subsection, we consider some relations of  $\rho_{A,p} : G_K \rightarrow GL(V_p(A)) \simeq GL_{2d}(\mathbb{Q}_p)$  with  $A(K^{\text{ur}})[p^\infty]$ . Our goal in this subsection is to prove that

**Theorem 2.2.** *Let  $E$  be an elliptic curve over  $K$  which has good ordinary reduction. Then the followings are equivalent;*

- (1)  $\rho_{E,p}$  is abelian,
- (2)  $\rho_{E,p}|_{I_K}$  is abelian,
- (3)  $E(K^{\text{ur}})[p^\infty]$  is infinite.

Note that it is known that the condition (1) is equivalent to the condition (4)  $E$  has complex multiplication over  $K$ .

See [9], A.2.4 for more information.

Now we start with an argument by proving the fact below;

**Proposition 2.7.** *Let  $A$  be an abelian variety over  $K$  which has good ordinary reduction. If  $\rho_{A,p}|_{I_K}$  is abelian, then  $A(K^{\text{ur}})[p^\infty]$  is infinite.*

*Proof.* By Proposition 2.6, we have the following form of the representation  $\rho_{A,p}|_{I_K}$  for a suitable basis of the  $\mathbb{Q}_p$ -module  $V_p(A)$ :

$$\begin{pmatrix} \varepsilon^{\oplus d} & U \\ 0 & I_d \end{pmatrix},$$

where  $U$  is a map  $I_K \rightarrow M_d(\mathbb{Q}_p)$  and  $I_d$  is the unit matrix of  $d \times d$ . Since  $\rho_{A,p}|_{I_K}$  is abelian, we see that  $U = (\varepsilon^{\oplus d} - I_d)U_0$  for some  $U_0 \in M_d(\mathbb{Q}_p)$ . Then,

on  $I_K$ ,

$$\begin{pmatrix} \varepsilon^{\oplus d} & U \\ 0 & I_d \end{pmatrix} \begin{pmatrix} U_0 1_d \\ 1_d \end{pmatrix} = \begin{pmatrix} U_0 1_d \\ 1_d \end{pmatrix},$$

where  $1_d = {}^t(1, 1, \dots, 1) \in M_{d,1}(\mathbb{Q}_p)$ . Consequently, we know that  $V_p(A)^{I_K} \neq 0$  and this implies the desired result.  $\square$

In the rest of this subsection we always assume that  $A$  has good ordinary reduction over  $K$ . Let  $K^{\text{ab}}$  be the maximal abelian extension of  $K$  in  $\bar{K}$ . The exact sequence

$$0 \rightarrow \ker(r) \rightarrow V_p(A) \xrightarrow{r} V_p(\tilde{A}) \rightarrow 0$$

gives the exact sequence

$$0 \rightarrow \ker(r) \rightarrow V_p(A)^{G_{K^{\text{ab}}}} \xrightarrow{r} V_p(\tilde{A}) \quad (*)$$

of  $\mathbb{Q}_p[\text{Gal}(K^{\text{ab}}/K)]$ -modules. Here we remark that  $G_{K^{\text{ab}}}$  acts trivially on  $\ker(r)$  and  $V_p(\tilde{A})$ . We define the representation  $\rho_{A,p}^{\text{ur}}$  by the natural action of  $\text{Gal}(K^{\text{ab}}/K^{\text{ur}})$  on  $V_p(A)^{G_{K^{\text{ab}}}} = V_p(A(K^{\text{ab}}))$ ;

$$\rho_{A,p}^{\text{ur}} : \text{Gal}(K^{\text{ab}}/K^{\text{ur}}) \rightarrow GL(V_p(A)^{G_{K^{\text{ab}}}}) = GL(V_p(A(K^{\text{ab}}))).$$

Now we define the integer  $e(A)$  to be  $e(A) := \dim_{\mathbb{Q}_p} V_p(A(K^{\text{ab}})) - \dim_{\mathbb{Q}_p} \ker(r) = \dim_{\mathbb{Q}_p} V_p(A(K^{\text{ab}})) - d$ . Then  $\rho_{A,p}^{\text{ur}}$  is a  $p$ -adic representation of dimension  $d + e(A)$ . Clearly  $0 \leq e(A) \leq d$ . Furthermore, the above sequence  $(*)$  implies that  $\rho_{A,p}^{\text{ur}}$  has the following shape for a suitable basis of the  $\mathbb{Q}_p$ -module  $V_p(A(K^{\text{ab}}))$ :

$$\rho_{A,p}^{\text{ur}} \simeq \begin{pmatrix} \varepsilon^{\oplus d} & U \\ 0 & I_{e(A)} \end{pmatrix},$$

where  $U$  is a map  $\text{Gal}(K^{\text{ab}}/K^{\text{ur}}) \rightarrow M_{d,e(A)}(\mathbb{Q}_p)$  and  $I_{e(A)}$  is the unit matrix of  $e(A) \times e(A)$ .

(I) The case  $e(A) \neq 0$ .

In this case, we see that  $U = (\varepsilon^{\oplus d} - I_d)U_0$  for some  $U_0 \in M_{d,e(A)}(\mathbb{Q}_p)$  since  $\rho_{A,p}^{\text{ur}}$  is abelian. Then, on  $\text{Gal}(K^{\text{ab}}/K^{\text{ur}})$ ,

$$\begin{pmatrix} \varepsilon^{\oplus d} & U \\ 0 & I_{e(A)} \end{pmatrix} \begin{pmatrix} U_0 1_{e(A)} \\ 1_{e(A)} \end{pmatrix} = \begin{pmatrix} U_0 1_{e(A)} \\ 1_{e(A)} \end{pmatrix},$$

where  $1_{e(A)} = {}^t(1, 1, \dots, 1) \in M_{e(A),1}(\mathbb{Q}_p)$ . This equation shows the fact that  $V_p(A(K^{\text{ab}}))^{\text{Gal}(K^{\text{ab}}/K^{\text{ur}})} \neq 0$ , that is,  $A(K^{\text{ur}})[p^\infty]$  is infinite.

(II) The case  $e(A) = 0$ .

In this case, we have  $\rho_{A,p}^{\text{ur}} = \varepsilon^{\oplus d}$  and hence  $V_p(A(K^{\text{ab}}))^{\text{Gal}(K^{\text{ab}}/K^{\text{ur}})} = 0$ , that is,  $A(K^{\text{ur}})[p^\infty]$  is finite.

Consequently we obtained the following lemma:

**Lemma 2.1.** *Let the notation be as above. Then  $e(A) = 0$  if and only if  $A(K^{\text{ur}})[p^\infty]$  is finite.*

Now we can finish the proof of Theorem 2.2.

*Proof of Theorem 2.2.* Since  $E$  is an elliptic curve, by combining Proposition 2.7 with Lemma 2.1, we can show the desired statement by the following way:  $e(E) \neq 0 \Leftrightarrow e(E) = 1 \Leftrightarrow \dim_{\mathbb{Q}_p} V_p(E(K^{\text{ab}})) = 2 \Leftrightarrow V_p(E(K^{\text{ab}})) = V_p(E) \Leftrightarrow G_{K^{\text{ab}}} \subset G_{K_{E,p}} \Leftrightarrow \rho_{E,p}$  is abelian.  $\square$

## §2.4. Global cases

Consider “global cases” of Theorem 2.1. Let  $A$  be an abelian variety over a number field  $K$ . It is well-known that the group  $A(L)$  is a finitely generated commutative group for a finite extension field  $L$  of  $K$  by the theorem of Mordell-Weil-Néron-Lang. In particular its torsion subgroup is finite. In the case where  $L$  is any algebraic extension of  $K$ , there are many results on the finiteness of torsion points of  $A(L)$ .

Let  $v$  be a finite place of  $K$ . For any finite extension  $K'$  of  $K$  and any finite place  $v'$  of  $K'$  above  $v$ , we denote the completion of  $K'$  at  $v'$  by  $K'_{v'}$ . More generally, for any algebraic extension  $L$  and any place  $w$  above  $v$ , we denote

$$L_w := \bigcup_{K'} K'_{v'},$$

where  $K'$  runs through all the finite extensions of  $K$  in  $L$  and  $v'$  is the unique place of  $K'$  under  $w$ . Note that the residue field  $k_{L_w}$  of  $L_w$  is  $\bigcup_{K'} k_{K'_{v'}}$ .

As corollaries of Theorem 2.1, we can see the “global cases” below immediately.

**Corollary 2.2.** *Let  $K, L, A$  be as above. Assume that there exist places  $v$  of  $K$  above  $p$  and  $w_\infty$  of  $L(\mu_{p^\infty})$  above  $v$  satisfying the following properties:*

- (i) *The residue field  $k_{w_\infty}$  of  $L(\mu_{p^\infty})$  at  $w_\infty$  is a potential prime-to- $p$  extension of the residue field  $k_v$  of  $K$  at  $v$ .*
- (ii)  *$A$  has potential good ordinary reduction at  $v$ .*

*Then  $A(L)[p^\infty]$  is finite.*

**Corollary 2.3.** *Let  $K, L, A$  be as above. Assume that  $L(\mu_{p^\infty})$  is a Galois extension of  $K$ , and there exist places  $v$  of  $K$  above  $p$  and  $w_\infty$  of  $L(\mu_{p^\infty})$  above  $v$  satisfying the following properties:*

- (i) *The residue field  $k_{w_\infty}$  of  $L(\mu_{p^\infty})$  at  $w_\infty$  is finite.*
- (ii)  *$A$  has potential good ordinary reduction at  $v$ .*

*Then the torsion part of  $A(L)$  is finite.*

If we always assume that  $L$  contains all  $p$ -th power roots of unity, these corollaries are generalizations of a result of Greenberg. See [3], Prop. 1.2 (ii).

### §3. Finiteness of Torsion Points for Elliptic Curves

We use the same notations as defined at the beginning of the previous section (soon we will suppose  $K$  to be a finite extension of  $\mathbb{Q}_p$ ). In particular  $A$  is an abelian variety over a field  $K$ . In this section, we give results on the Question which is proposed in the Introduction. At the beginning, we shall remark the following proposition related with “a torsion problem of two abelian varieties”.

**Proposition 3.1.** *Let  $A$  and  $B$  be abelian varieties over a field  $K$ . Assume that  $K$  has the following property: the torsion part of  $A(K')$  is finite for any finite Galois extension  $K'$  of  $K$ . Then, for two different prime numbers  $\ell_1$  and  $\ell_2$ , the group  $A(K_{B,\ell_2})[\ell_1^\infty]$  is finite.*

*Proof.* This follows immediately from Proposition 2.4. □

In view of the above proposition, we will be interested in the finiteness of  $A(K_{B,\ell_2})[\ell_1^\infty]$  with  $\ell_1 = \ell_2$ .

From now on, throughout this Section, we always denote by  $K$  a finite extension of  $\mathbb{Q}_p$ . Some of results on such the (in-)finiteness properties can be checked immediately, by using the results given in the previous section, as follows.

**Proposition 3.2.** *Let  $E$  be elliptic curves over  $K$  which has potential multiplicative reduction or potential good supersingular reduction. We assume that  $A$  has potential good ordinary reduction over  $K$ . Then the torsion part of  $A(K_{E,p})$  is finite.*

*Proof.* The two Lie groups  $\rho_{E,p}(G_K)$  and  $\rho_{E,p}(I_K)$  have the same Lie algebras (cf. [8]) and hence the residue field of  $K_{E,p}$  is a finite field. Therefore, the residue field of  $K_{E,p}$  is also finite. Consequently we finish the proof by Theorem 2.1 (2). □

**Proposition 3.3.** *Let  $A$  and  $B$  be abelian varieties over  $K$  which have good ordinary reductions. Assume that  $A(\bar{K})[p]$  is rational over  $K$ . Then  $A(K_{B,p})$  is infinite.*

*Proof.* Since  $B(K_{B,p})[p^\infty]$  is infinite, the residue field  $k_{B,p}$  of  $K_{B,p}$  is not a potential prime-to- $p$  extension of  $k$  by Theorem 2.1. Because  $A(\bar{K})[p]$  is rational over  $K$ , Corollary 2.1 shows that  $A(K_{B,p})[p^\infty]$  is infinite.  $\square$

In the rest of this section, we discuss the following question:

**Question.** Let  $A$  and  $B$  be abelian varieties over  $K$ . When is  $A(K_{B,p})[p^\infty]$  finite?

Now we are interested in the case where  $A$  (and  $B$ ) are elliptic curves. Let us consider the above Question by distinguishing the reduction type of  $A$ .

### §3.1. Good ordinary reduction case

Let  $A = E_1$  and  $B = E_2$  be two elliptic curves over  $K$ . We have already proved in Corollary 3.2 that the torsion part of  $E_1(K_{E_2,p})[p^\infty]$  is finite if  $E_1$  has good ordinary reduction over  $K$  and  $E_2$  has good supersingular reduction or multiplicative reduction over  $K$ . We consider the infiniteness of  $E_1(K_{E_2,p})[p^\infty]$  under the condition that  $E_1$  and  $E_2$  have good ordinary reduction over  $K$ . One of the result for the infiniteness of  $E_1(K_{E_2,p})[p^\infty]$  has given in Proposition 3.3. However, in this 1-dimensional case, we will show more precise criterion in Theorem 3.4 and Corollary 3.1.

We shall give some notation that we need. In the rest of this subsection we always assume that  $E_1$  and  $E_2$  have good ordinary reduction over  $K$ . Let  $\tilde{E}_1$  and  $\tilde{E}_2$  be the reduction of  $E_1$  and  $E_2$  over  $k$ , respectively. For each elliptic curves  $E_i$ , Put

$$\chi_i = \rho_{\tilde{E}_i,p} : G_K \rightarrow GL(T_p(\tilde{E}_i)) \simeq GL_1(\mathbb{Z}_p) = \mathbb{Z}_p^\times,$$

and

$$\bar{\chi}_i = \bar{\rho}_{\tilde{E}_i,p} : G_K \rightarrow GL(\tilde{E}_i(k^{\text{sep}})[p]) \simeq GL_1(\mathbb{F}_p) = \mathbb{F}_p^\times.$$

Clearly  $\chi_i$  and  $\bar{\chi}_i$  are unramified characters by their definitions. It can be checked that each  $\chi_i$  is of infinite order. We know that each  $\rho_{E_i,p}$  has the form

$$\begin{pmatrix} \varepsilon \chi_i^{-1} & u_i \\ 0 & \chi_i \end{pmatrix}$$

with respect to a suitable basis of  $T_p(E_i)$ . We fix such a basis and identify  $T_p(E_i)$  with  $\mathbb{Z}_p^{\oplus 2}$ .

**Proposition 3.4.** *Let the notations be as above and  $p \geq 3$ . Consider the following four conditions:*

- (a) *The group  $E_1(K_{E_2,p})[p^\infty]$  is infinite.*
- (b)  $G_{K_{E_2,p}} \subset \ker(\chi_1)$ .
- (c)  $\ker(\chi_2) \subset \ker(\chi_1)$ .
- (d)  $\text{Im}(\bar{\chi}_1) \subset \text{Im}(\bar{\chi}_2)$ .

*Then there is the following relation: (a)  $\Leftrightarrow$  (b)  $\Leftarrow$  (c)  $\Leftrightarrow$  (d).*

*Proof.* If we assume that the condition (a) is satisfied, there is a 1-dimensional  $G_{K_{E_2,p}}$ -invariant subspace  $W$  of  $V_p(E_1) = M_{2,1}(\mathbb{Q}_p)$ . Take any non-zero element  $\begin{pmatrix} x \\ y \end{pmatrix}$  in  $W$ . Since  $x$  or  $y$  is a non-zero element which is invariant under the multiplication by  $\chi_1(\sigma)$  for all  $\sigma \in G_{K_{E_2,p}}$ , we see that  $V_p(\tilde{E}_1)^{G_{K_{E_2,p}}}$  has non-trivial subspace and hence  $V_p(\tilde{E}_1)^{G_{K_{E_2,p}}} = V_p(\tilde{E}_1)$ . This implies the condition (b). Conversely we assume that the condition (b) is satisfied. Then the condition (a) follows from the fact that

$$\rho_{E_1,p}|_{G_{K_{E_2,p}}} = \begin{pmatrix} \varepsilon\chi_1^{-1} & u_1 \\ 0 & \chi_1 \end{pmatrix} = \begin{pmatrix} 1 & u_1 \\ 0 & 1 \end{pmatrix}.$$

Because  $G_{K_{E_2,p}} \subset \ker(\chi_2)$ , the condition (c) implies (b). Finally let us show that conditions (c) and (d) are equivalent. Since  $\chi_1$  and  $\chi_2$  are unramified, we may consider each character  $\chi_i$  as a character

$$G_k \xrightarrow{\chi_i} \mathbb{Z}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p,$$

where  $G_k$  is an absolute Galois group of  $k$ . By  $\text{pr}_1 : \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \rightarrow \mathbb{Z}/(p-1)\mathbb{Z}$  and  $\text{pr}_2 : \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ , we denote natural projections. Furthermore we denote by  $k_{\chi_i}, k_{\bar{\chi}_i}$  and  $k_p$  the corresponding field over  $k$  of  $\chi_i, \bar{\chi}_i = \text{pr}_1 \circ \chi_i$  and  $\text{pr}_2 \circ \chi_i$  on  $G_k$ , respectively. Then we have  $k_{\chi_i} = k_{\bar{\chi}_i}k_p$ . Since the extension degree of  $k_{\bar{\chi}_i}$  over  $k$  is prime-to- $p$ , we see that  $\ker(\chi_2) \subset \ker(\chi_1)$  if and only if  $k_{\bar{\chi}_1} \subset k_{\bar{\chi}_2}$ , which implies the condition (d). □

Let  $k_{\tilde{E}_i[p]}$  be the smallest field extension of  $k$  over which the elements of  $\tilde{E}_i(k^{\text{sep}})[p]$  is rational.

**Corollary 3.1.** *Let  $E_1$  and  $E_2$  be elliptic curves over  $K$  which have good ordinary reduction. Assume that  $p \geq 3$ .*

- (1) *If  $k_{\tilde{E}_1[p]} \subset k_{\tilde{E}_2[p]}$ , then  $E_1(K_{E_2,p})[p^\infty]$  is infinite.*
- (2) *If the map  $\bar{\chi}_1$  is trivial, then  $E_1(K_{E_2,p})[p^\infty]$  is infinite.*
- (3) *If the map  $\bar{\chi}_2$  is surjective, then  $E_1(K_{E_2,p})[p^\infty]$  is infinite.*

*Proof.* All statements will immediately follow from Proposition 3.4.  $\square$

### §3.2. Good supersingular reduction case

Let  $A = E_1$  and  $B = E_2$  be elliptic curves over  $K$ . In this subsection we consider the case where  $E_1$  has (potential) good supersingular reduction over  $K$ . We recall the structure of the Lie algebra associated to an elliptic curve (cf. [9], Appendix of Chapter 4).

**Proposition 3.5.** *Let  $E$  be an elliptic curve over  $K$ . Put  $\mathfrak{g} := \text{Lie}(\rho_{E,p}(G_K))$  and  $\mathfrak{i} := \text{Lie}(\rho_{E,p}(I_K))$  (these are Lie subalgebras of  $\text{End}_{\mathbb{Q}_p}(V_p(E))$ ).*

- (1) *If  $E$  has good ordinary reduction with complex multiplication, then  $\mathfrak{g}$  is a split Cartan subalgebra of  $\text{End}_{\mathbb{Q}_p}(V_p(E))$  and  $\mathfrak{i}$  is a 1-dimensional subspace of  $\mathfrak{g}$ .*
- (2) *If  $E$  has good ordinary reduction without complex multiplication, then  $\mathfrak{g}$  is the Borel subalgebra of  $\text{End}_{\mathbb{Q}_p}(V_p(E))$  corresponding to the kernel of the natural reduction map  $V_p(E) \rightarrow V_p(\bar{E})$  and  $\mathfrak{i}$  is a 2-dimensional subspace of  $\mathfrak{g}$  with  $\dim(\mathfrak{i}/[\mathfrak{i}, \mathfrak{i}]) = 1$ .*
- (3) *If  $E$  has good supersingular reduction with formal complex multiplication, then  $\mathfrak{g}$  is a non-split Cartan subalgebra of  $\text{End}_{\mathbb{Q}_p}(V_p(E))$  and  $\mathfrak{i} = \mathfrak{g}$ .*
- (4) *If  $E$  has good supersingular reduction without formal complex multiplication, then  $\mathfrak{g} = \text{End}_{\mathbb{Q}_p}(V_p(E))$  and  $\mathfrak{i} = \mathfrak{g}$ .*
- (5) *If the  $j$ -invariant of  $E$  has negative  $p$ -adic valuation, then  $\mathfrak{g}$  coincides with  $\mathfrak{n}_X$  for some 1-dimensional subspace  $X$  of  $V_p(E)$  and  $\mathfrak{i} = \mathfrak{g}$ . Here  $\mathfrak{n}_X$  is the subspace of  $\text{End}_{\mathbb{Q}_p}(V_p(E))$  generated by all  $u \in \text{End}_{\mathbb{Q}_p}(V_p(E))$  satisfying that  $u(V_p(E)) \subset X$ .*

Here, for any elliptic curve  $E$  over  $K$  which has good supersingular reduction, we say that  $E$  has *formal complex multiplication* over  $K$  if an endomorphism ring of the  $p$ -divisible group  $\mathcal{E}(p)$  over  $\mathcal{O}_K$  has rank 2 as a  $\mathbb{Z}_p$ -module, where  $\mathcal{E}(p)$  is the  $p$ -divisible group associated with the Néron model  $\mathcal{E}$  of  $E$  over  $\mathcal{O}_K$ . We also say that  $E$  has *formal complex multiplication* if  $E \times_K K'$  has formal complex multiplication defined over some algebraic extension  $K'$  of  $K$ . Then the quadratic field  $\text{End}_{\mathcal{O}_{K'}}(\mathcal{E}(p)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$  is called the field of formal complex multiplication. We can take  $K'$  for at most degree 2 extension of  $K$ .

Our first result in this subsection is:

**Proposition 3.6.** *Let  $E_1$  and  $E_2$  be elliptic curves over  $K$ . Suppose that  $E_1$  has potential good supersingular reduction over  $K$ . Then  $E_1(K_{E_2,p})[p^\infty]$  is finite if one of the following conditions is satisfied:*

- (1) The elliptic curve  $E_2$  has potential good ordinary reduction.
- (2) The elliptic curve  $E_2$  has potential good supersingular reduction. Furthermore, one of the following conditions is satisfied:
  - (i)  $E_1$  has formal complex multiplication but  $E_2$  does not have.
  - (ii)  $E_2$  has formal complex multiplication but  $E_1$  does not have.
- (3) The  $j$ -invariant of  $E_2$  has negative  $p$ -adic value.

To prove this proposition, we need the following important lemma, which is easy to prove, but we often make use of this lemma in this subsection.

**Lemma 3.1.** *Let  $E$  be an elliptic curve over  $K$  which has good supersingular reduction over  $K$ . Let  $L$  be a Galois extension of  $K$ . Then the group  $E(L)[p^\infty]$  is finite if and only if  $K_{E,p}$  is not contained in  $L$ .*

*Proof.* Let us assume that  $K_{E,p}$  is not contained in  $L$ . Then we have  $V_p(E)^{G_L} \subsetneq V_p(E)$ . By the assumption that  $L$  is a Galois extension of  $K$ , we see that  $V_p(E)^{G_L}$  is a  $G_K$ -submodule of  $V_p(E)$ . In addition, since  $E$  has good supersingular reduction,  $V_p(E)$  is an irreducible  $G_K$ -module (cf. [9], Thm. of A.2.2). Hence we see that  $V_p(E)^{G_L}$  is vanished and this implies the fact that  $E(L)[p^\infty]$  is finite.

The converse is obvious. □

*Proof of Proposition 3.6.* First we note that the Lie algebras  $\mathfrak{g}_i := \text{Lie}(\rho_{E_i,p}(G_K))$  and  $\mathfrak{i}_i := \text{Lie}(\rho_{E_i,p}(I_K))$  are subspaces of  $\text{End}(V_p(E_i))$  for  $i = 1, 2$ . By extending  $K$  finitely, we may assume that  $E_1$  has good reduction over  $K$ . By Lemma 3.1, it suffices to show that  $K_{E_1,p}$  is not contained in  $K_{E_2,p}$ . Let us assume that  $K_{E_1,p}$  is contained in  $K_{E_2,p}$ . Then there is a natural surjection  $\text{Gal}(K_{E_2,p}/K) \rightarrow \text{Gal}(K_{E_1,p}/K)$  and hence we obtain the surjections of Lie algebras  $\mathfrak{g}_2 \rightarrow \mathfrak{g}_1$  and  $\mathfrak{i}_2 \rightarrow \mathfrak{i}_1$ . Hence we see that  $\dim_{\mathbb{Q}_p} \mathfrak{g}_2 \geq \dim_{\mathbb{Q}_p} \mathfrak{g}_1$  and  $\dim_{\mathbb{Q}_p} \mathfrak{i}_2 \geq \dim_{\mathbb{Q}_p} \mathfrak{i}_1$ . If  $\mathfrak{g}_1$  (resp.  $\mathfrak{i}_1$ ) is abelian, we can also obtain the inequality  $\dim_{\mathbb{Q}_p}(\mathfrak{g}_2/[\mathfrak{g}_2, \mathfrak{g}_2]) \geq \dim_{\mathbb{Q}_p} \mathfrak{g}_1$  (resp.  $\dim_{\mathbb{Q}_p}(\mathfrak{i}_2/[\mathfrak{i}_2, \mathfrak{i}_2]) \geq \dim_{\mathbb{Q}_p} \mathfrak{i}_1$ ). But Proposition 3.5 implies that at least one of the above inequalities is not satisfied. □

In the rest of this section, we consider about the case where  $E_2$  has good supersingular reduction. First we prove an elementary result of the algebraic number theory.

**Lemma 3.2.** *Suppose  $F_1$  and  $F_2$  are quadratic subfields in  $K$ . Denote by  $\text{Nr}_{K/F_i}$  the norm map  $K^\times \rightarrow F_i^\times$  for  $i = 1, 2$ . Then the followings are equivalent:*

- (a)  $F_1 \neq F_2$ ,
- (b)  $\ker(\mathrm{Nr}_{K/F_2}) \not\subset \ker(\mathrm{Nr}_{K/F_1})$ ,
- (c)  $\ker(\mathrm{Nr}_{K/F_1}) \not\subset \ker(\mathrm{Nr}_{K/F_2})$ .

*Proof.* Let  $\alpha_i$  be a  $p$ -adic integer satisfying that  $F_i = \mathbb{Q}_p(\alpha_i)$  and  $\alpha_i^2 \in \mathbb{Z}_p$  for  $i = 1, 2$ . Assume that  $F_1 \neq F_2$ . Then

$$\mathrm{Nr}_{K/F_2}(x + y\alpha_1) = (x^2 - y^2\alpha_1^2)^d, \quad \mathrm{Nr}_{K/F_1}(x + y\alpha_1) = (x + y\alpha_1)^{2d},$$

where  $d$  is the extension degree of  $K/F_1F_2$  and  $x, y \in \mathbb{Z}_p$ . By the elementary field theory,  $\ker(\mathrm{Nr}_{K/F_1}|_{F_1^\times})$  has order at most  $2d$ . Thus, to obtain the desired result, it is enough to show that the following claim:

**Claim.** *The group  $\ker(\mathrm{Nr}_{K/F_2}|_{F_1^\times})$  has an infinite order.*

If we suppose  $p \geq 3$ , then the polynomial  $T^2 - y^2\alpha_1^2 - 1$  has roots in  $\mathbb{Z}_p$  for all  $y \in p\mathbb{Z}_p$  by Hensel's lemma and thus the claim is true. Suppose  $p = 2$ . To prove the claim, it suffices to show that  $x^2 - y^2\alpha_1^2$  is equal to 1 for infinitely many  $x, y \in \mathbb{Z}_p$ . Take any integer  $k \geq 0$  and suppose  $y = 4kx$ . In this case  $x^2 - y^2\alpha_1^2 = (1 - 16k^2\alpha_1^2)x^2$  and we see  $(1 - 16k^2\alpha_1^2) \in (\mathbb{Z}_p^\times)^2$  since it can be checked that the polynomial  $(1 + 2T)^2 - (1 - 16k^2\alpha_1^2) \in \mathbb{Z}_p[T]$  has roots in  $\mathbb{Z}_p$  by Hensel's lemma. This completes the proof of the claim.  $\square$

**Proposition 3.7.** *Let  $E_1$  and  $E_2$  be elliptic curves over  $K$  which have good supersingular reduction with formal complex multiplication. Let  $F_i \subset K$  be the field of formal complex multiplication for each  $E_i$ . Then  $E_1(K_{E_2,p})[p^\infty]$  is finite if  $F_1 \neq F_2$ .*

*Proof.* By extending  $K$  finitely, we may assume that  $E_1$  and  $E_2$  have formal complex multiplication over  $K$ . Then the representation  $\rho_{E_i,p} : G_K \rightarrow GL(V_p(E))$  has values in  $\mathcal{O}_{F_i}^\times$  and hence  $\rho_{E_i,p}$  induces the representation

$$\Psi_i : \mathcal{O}_K^\times \simeq I(K^{\mathrm{ab}}/K) \rightarrow \mathcal{O}_{F_i}^\times,$$

where  $I(K^{\mathrm{ab}}/K)$  is the inertia subgroup of  $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ . It is known that  $\Psi_i(x) = \mathrm{Nr}_{K/F_i}(x^{-1})$  for any  $x \in \mathcal{O}_K^\times$  (see [9], A.2.2). Lemma 3.1 implies that if  $E_1(K_{E_2,p})[p^\infty]$  is infinite, then  $K^{\mathrm{ur}}(E_1(\bar{K})[p^\infty]) \subset K^{\mathrm{ur}}(E_2(\bar{K})[p^\infty])$ . Because  $K^{\mathrm{ur}}(E_i(\bar{K})[p^\infty])$  is the definition field of the representation  $\rho_{E_i,p}|_{I_K}$  and  $\ker(\mathrm{Nr}_{K/F_2}|_{\mathcal{O}_K^\times}) = \ker(\mathrm{Nr}_{K/F_2})$  (resp.  $\ker(\mathrm{Nr}_{K/F_1}|_{\mathcal{O}_K^\times}) = \ker(\mathrm{Nr}_{K/F_1})$ ), we see that if  $E_1(K_{E_2,p})[p^\infty]$  is infinite, then  $\ker(\mathrm{Nr}_{K/F_2}) \subset \ker(\mathrm{Nr}_{K/F_1})$ . Combining this fact and Lemma 3.2, we obtain the desired result.  $\square$

For any elliptic curve  $E$  over  $K$ , we denote by  $\hat{E}$  the formal group associated with  $E$ .

**Proposition 3.8.** *Let  $E_1$  and  $E_2$  be elliptic curves over  $K$  which have good supersingular reduction without formal complex multiplication.*

- (1) *If there is a non-trivial homomorphism of formal groups  $\hat{E}_2 \rightarrow \hat{E}_1$  over  $\mathcal{O}_K$ , then  $E_1(K_{E_2,p})[p^\infty]$  is infinite.*
- (2) *If  $E_1(K_{E_2,p})[p^\infty]$  is infinite, then there is a non-trivial homomorphism of formal groups  $\hat{E}_2 \rightarrow \hat{E}_1$  over  $\mathcal{O}_{K'}$  for some finite extension  $K'$  of  $K$ .*

*Proof.* (1) Since each  $E_i$  has good supersingular reduction, there is a non-trivial  $G_K$ -homomorphism  $T_p(E_2) \rightarrow T_p(E_1)$  by a theorem of Tate (cf. [11], Cor. 1 of Thm. 4). Hence Proposition 2.3 implies that  $E_1(K_{E_2,p})[p^\infty]$  is infinite.

(2) By Lemma 3.1, we know that  $K_{E_1,p} \subset K_{E_2,p}$ . Furthermore this is a finite field extension because the Lie groups  $\text{Gal}(K_{E_1,p}/K)$  and  $\text{Gal}(K_{E_2,p}/K)$  have same Lie algebras. Hence we may assume that  $K_{E_1,p}$  coincides with  $K_{E_2,p}$  by replacing  $K$  with a finite extension. Put  $G := \text{Gal}(K_{E_1,p}/K) = \text{Gal}(K_{E_2,p}/K)$  and  $\mathfrak{g} := \text{Lie}(G)$ . Then the Lie algebra homomorphism  $\text{Lie}(\rho_{E_i,p}) : \mathfrak{g} \rightarrow \mathfrak{gl}_2(\mathbb{Q}_p)$  corresponding to  $\rho_{E_i,p} : G \rightarrow GL(T_p(E_i)) \simeq GL_2(\mathbb{Z}_p)$  is an isomorphism by our assumptions of  $E_i$  for  $i = 1, 2$ .

**Claim.**  $\text{Lie}(\rho_{E_1,p})$  is conjugate with  $\text{Lie}(\rho_{E_2,p})$ .

If we finish the proof of this claim, we know that  $\rho_{E_1,p}$  is conjugate with  $\rho_{E_2,p}$  on  $G_{K'}$  for some finite extension  $K'$  of  $K$  (this fact follows from [2], Thm. 9.11). Thus there is a non-trivial  $G_{K'}$ -homomorphism  $T_p(E_2) \rightarrow T_p(E_1)$ . By using the theorem of Tate again, we see that there is a desired non-trivial homomorphism of formal groups  $\hat{E}_2 \rightarrow \hat{E}_1$  over  $\mathcal{O}_{K'}$ .

Let us prove the above claim. We denote by  $Z(G)$  (resp.  $Z_1, Z_2$ ) the center of  $G$  (resp.  $\text{Im}(\rho_{E_1,p}), \text{Im}(\rho_{E_2,p})$ ) and put  $\mathfrak{s} := \text{Lie}(\text{Gal}(K_{E_1,p}/K(\mu_{p^\infty}))) = \text{Lie}(\text{Gal}(K_{E_2,p}/K(\mu_{p^\infty})))$ . We see that the homomorphisms  $\text{Lie}(\rho_{E_1,p})$  and  $\text{Lie}(\rho_{E_2,p})$  induce isomorphisms  $\text{Lie}(Z(G)) \simeq \text{Lie}(Z_1) = \mathbb{Q}_p \cdot I_2$  and  $\text{Lie}(Z(G)) \simeq \text{Lie}(Z_2) = \mathbb{Q}_p \cdot I_2$ , respectively. Here  $I_2$  is the unit matrix of  $2 \times 2$ . We shall remark that  $\text{Lie}(Z(G))$  and  $\mathfrak{s}$  generate  $\mathfrak{g}$ . This can be checked from the facts that  $\dim_{\mathbb{Q}_p} \text{Lie}(Z(G)) = 1$ ,  $\dim_{\mathbb{Q}_p} \mathfrak{s} = 3$  and

$$\begin{aligned} \text{Lie}(\rho_{E_1,p})(\text{Lie}(Z(G)) \cap \mathfrak{s}) &= \text{Lie}(\rho_{E_1,p})(\text{Lie}(Z(G))) \cap \text{Lie}(\rho_{E_1,p})(\mathfrak{s}) \\ &= \mathbb{Q}_p \cdot I_2 \cap \mathfrak{sl}_2(\mathbb{Q}_p) = 0. \end{aligned}$$

Since  $\det(\rho_{E_1,p})$  and  $\det(\rho_{E_2,p})$  coincide with the  $p$ -adic cyclotomic character, we have the equality that  $\text{Lie}(\rho_{E_1,p}) = \text{Lie}(\rho_{E_2,p})$  on  $\text{Lie}(Z(G))$ . On the other hand, up to inner automorphisms, there exists the unique Lie algebra injection

from  $\mathfrak{s}$  to  $\mathfrak{gl}_2(\mathbb{Q}_p)$  because  $\mathfrak{s}$  is isomorphic to  $\mathfrak{sl}_2(\mathbb{Q}_p)$ . This fact is followed from the highest weight theory (cf. [10], the remark of the end of Subsection 7.4). Thus  $\mathrm{Lie}(\rho_{E_1,p})$  is conjugate with  $\mathrm{Lie}(\rho_{E_2,p})$  on  $\mathfrak{s}$ . Thus we have proved the assertion of the claim.  $\square$

### §3.3. Multiplicative reduction case

Finally we give some results on the finiteness of  $A(K_{B,p})[p^\infty]$  for an elliptic curve  $A = E$  over  $K$  with multiplicative reduction and an abelian variety  $B$  over  $K$ . We always suppose this assumption to the end of this subsection. Since  $E$  has multiplicative reduction, we may choose a suitable basis of  $T_p(E)$  such that the corresponding matrix of  $\rho_{E,p}$  has the form

$$\begin{pmatrix} \varepsilon\chi^{-1} & u \\ 0 & \chi \end{pmatrix},$$

where  $\chi : G_K \rightarrow \mathbb{Z}_p^\times$  is a character which has an image of order at most 2 (cf. [1], Thm. 1.1). Moreover  $\chi$  is trivial if and only if  $E$  has split multiplicative reduction over  $K$ . We identify  $T_p(E)$  as  $\mathbb{Z}_p^{\oplus 2}$  with respect to the above basis.

**Proposition 3.9.** *Let  $E$  be an elliptic curve which has split multiplicative reduction over  $K$ . Let  $K(\mu_{p^\infty})$  be an algebraic extension of  $K$  adjoining all  $p$ -th power roots of unity. Then  $E(K(\mu_{p^\infty}))[p^\infty]$  is infinite. In particular,  $E(K_{B,p})[p^\infty]$  is infinite for any abelian varieties  $B$  over  $K$ .*

*Proof.* By the theory of Tate curve, we have a  $G_K$ -isomorphism

$$E(\bar{K})[p^\infty] \simeq \bar{K}^\times / q^\mathbb{Z}$$

for some element  $q$  in the maximal ideal of  $\mathcal{O}_K$  and hence we have the desired result.  $\square$

Finally we consider the case where  $E$  has non-split multiplicative reduction, equivalently,  $\chi \neq 1$ .

**Proposition 3.10.** *Suppose that  $E$  has non-split multiplicative reduction over  $K$ .*

- (1) *Let  $L$  be an algebraic extension of  $K$  which contains all  $p$ -th power roots of unity. Then  $E(L)[p^\infty]$  is finite if and only if  $\chi$  is not trivial on  $G_L$ .*
- (2) *If  $L$  is a prime-to-2 algebraic extension of  $K$  which contains all  $p$ -th power roots of unity and  $p \neq 2$ , then  $E(L)[p^\infty]$  is finite. In particular, if  $B$  is an abelian variety such that  $B(\bar{K})[p]$  is rational over  $K$ , then  $E(K_{B,p})[p^\infty]$  is finite.*

*Proof.* The assertion (2) is a special case of (1) and hence it is enough to show the assertion (1). Since the field  $L$  contains all  $p$ -th power roots of unity, the matrix  $\begin{pmatrix} x \\ y \end{pmatrix} \in T_p(E)$  is contained in  $T_p(E)^{G_L}$  if and only if

$$\chi(\sigma)^{-1}x + u(\sigma)y = x, \quad \chi(\sigma)y = y$$

for all  $\sigma \in G_L$ . The assertion immediately follows from this fact.  $\square$

### Acknowledgements

The author would like to express his sincere gratitude to Professor Yuichiro Taguchi who proposed the theme of this paper to him and gave him useful advices, especially the proof of Proposition 3.8. The author also would like to thank Akio Tamagawa for pointing out a mistake of Theorem 1.1.

### References

- [1] B. Conrad, The flat deformation functor, in *Modular forms and Fermat's last theorem* (Boston, MA, 1995), 373–420, Springer, New York, 1997.
- [2] J. D. Dixon M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro- $p$  groups*, Second edition, Cambridge Studies in Advanced Mathematics, 61, Cambridge Univ. Press, Cambridge, 1999.
- [3] R. Greenberg, Galois theory for the Selmer group of an abelian variety, *Compositio Math.* **136** (2003), no. 3, 255–297.
- [4] H. Imai, A remark on the rational points of abelian varieties with values in cyclotomic  $\mathbb{Z}_p$ -extensions, *Proc. Japan Acad.* **51** (1975), 12–16.
- [5] A. Mattuck, Abelian varieties over  $p$ -adic ground fields, *Ann. of Math. (2)* **62** (1955), 92–119.
- [6] B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* **18** (1972), 183–266.
- [7] N. M. Katz and S. Lang, Finiteness theorems in geometric classfield theory, With an appendix by Kenneth A. Ribet, *Enseign. Math. (2)* **27** (1981), no. 3–4, 285–319 (1982).
- [8] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), no. 4, 259–331.
- [9] ———, *Abelian  $l$ -adic representations and elliptic curves*, Second edition. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. With the collaboration of Willem Kuyk and John Labute.
- [10] ———, *Lie algebras and Lie groups*, Lecture Notes in Mathematics, vol. 1500, Springer-Verlag, Berlin, 2006, 1964 lectures given at Harvard University, Corrected fifth printing of the second edition, 1992.
- [11] J. T. Tate,  $p$ -divisible groups., in *Proc. Conf. Local Fields (Driebergen, 1966)*, 158–183, Springer, Berlin, 1967.