On the vanishing of cohomologies of p-adic Galois representations associated with elliptic curves

Jerome T. Dimabayao (Kyushu University)

Abstract

We present generalizations of some results of Coates, Sujatha and Wintenberger on the vanishing of certain Galois cohomology groups of large Galois extensions with values in the p-adic representation associated with an elliptic curve.

The author thanks Yuichiro Taguchi who suggested the topic of this work and the organizers of the 8th Fukuoka Number Theory Symposium for giving him the opportunity to participate in the symposium.

1 Introduction

The determination of the vanishing of cohomology groups of p-adic representations of compact p-adic Lie groups was motivated by the study of Euler characteristics of such representations. The interest for these Euler characteristics arose from a paper by Coates-Howson [3], where the authors proposed the idea to develop the Iwasawa theory for elliptic curves defined over number fields, over the infinite p-adic Lie extension obtained by adjoining the coordinates of all p-power torsion points of the elliptic curve. Iwasawa theory relates Euler characteristics of p-adic representations of elliptic curves for certain p-adic Lie groups to special values of L-functions. An important hypothesis towards generalization of their methods to larger Galois extensions is the vanishing of the cohomology groups associated with p-adic Galois representations defined by elliptic curves (cf. [4], [15]).

This note aims to discuss the results of [5] on the vanishing of cohomology groups with values in a geometric p-adic Galois representation with respect to some Galois extensions which contain all the p-power roots of unity. In particular, we consider the extensions of a p-adic field obtained by adjoining the coordinates of p-power torsion points on an elliptic curve.

Let p be a prime number and K a finite extension of $\mathbb{Q}_p$. Fix a separable closure K^{sep} of K. Put $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$, the absolute Galois group of K. Let X be a proper smooth variety defined over K. For each integer $i \geq 0$, we let

$$V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) = \varprojlim H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/p^n\mathbb{Z}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

denote the ith étale cohomology group of $X_{\overline{K}}$ having coefficients in $\mathbb{Q}_p$, which is a finite-dimensional vector space over $\mathbb{Q}_p$. We denote by

$$\rho : G_K \longrightarrow \mathrm{GL}(V)$$

the homomorphism giving the action of G_K on the vector space V.

If E is an elliptic curve over K, the Tate-module $T_p(E) := \varprojlim E_{p^n}(K^{\mathrm{sep}})$ of E is a free $\mathbb{Z}_p$-module of rank 2. Set $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then $V_p(E)$ is a 2-dimensional p-adic Galois representation and we denote by ρ_E the continuous homomorphism attached to $V_p(E)$. Its dual $V_p(E)^\vee = \mathrm{Hom}(V_p(E), \mathbb{Q}_p(1))$ is canonically isomorphic to $H^1_{\text{ét}}(E_{\bar{K}}, \mathbb{Q}_p)$. Here, $\mathbb{Q}_p(r)$ denotes the rth twist by the p-adic cyclotomic character, where $r \in \mathbb{Z}$. If $E^\vee$ is the dual of E then the Weil pairing implies that we may identify $V_p(E)$ canonically with $V_p(E^\vee)^\vee$. Thus $V_p(E)$ is canonically isomorphic to $H^1_{\text{ét}}(E^\vee_{\bar{K}}, \mathbb{Q}_p)$.

For a general finite-dimensional vector space V over $\mathbb{Q}_p$ and a compact subgroup G of $\mathrm{End}(V)$, we write $H^i(G, V)$ $(i = 0, 1, \ldots)$ for the cohomology groups of G acting on V defined by continuous cochains, where V is endowed with the p-adic topology.

Definition 1.1. The vector space V has *vanishing G-cohomology* if the cohomology groups $H^n(G, V)$ are trivial for all $n \geq 0$.

For a Galois representation (ρ, V) as given above, we denote by $K(V)$ the fixed field in K^{sep} of the kernel of ρ. If $V = V_p(E)$ is given by an elliptic curve E over K, the field $K(V_p(E))$ is the Galois extension obtained by adjoining the coordinates of p-power division points of E. We use the notation $K(E_\infty)$ instead of $K(V_p(E))$ in this case. For a subfield L of K^{sep}, let G_L denote the subgroup of G_K corresponding to L. Let $K(\mu_{p^\infty})$ be the smallest field extension of K which contains all the roots of unity of order a power of p. Denote by G_V (resp. H_V) the image of G_K (resp. $G_{K(\mu_{p^\infty})}$) under ρ. As G_K (resp. $G_{K(\mu_{p^\infty})}$) is a profinite group, the group G_V (resp. H_V) is a compact p-adic Lie group contained in $\mathrm{GL}_d(\mathbb{Z}_p)$, where $d = \dim V$. The group G_V (resp. H_V) can be realised as the Galois group of $K(V)$ over K (resp. $K(\mu_{p^\infty})$). In their study of Euler characteristics of p-adic Galois representations, Coates, Sujatha and Wintenberger proved the following result:

Theorem 1.2 ([4], Theorems 1.1 and 1.5)**.** *Let X be a proper smooth variety defined over K with potential good reduction. Let $i > 0$ be an odd integer and $V = H^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)$. Then V has vanishing G_V-cohomology and vanishing H_V-cohomology.*

Remark 1. Note that the hypothesis of potential good reduction is necessary. For instance, if $V = V_p(E)$ where E is an elliptic curve with split multiplicative reduction, then the theory of Tate curves shows that in this case we have $H^0(G_{K(\mu_{p^\infty})}, V) = V_p(\mu)$, provided K contains the pth-roots of unity if p is odd or the 4th-roots of unity if $p = 2$. Here, $V_p(\mu)$ is the $\mathbb{Q}_p$-vector space given by the action of G_K on the p-power roots of unity. It is likewise necessary to assume that i be odd. If $i \neq 2j$ is even and X is defined over an algebraic number field contained in K, then (part of) the Tate conjecture implies that $H^0(G_L, V)$ is nontrivial if L contains $K(\mu_{p^\infty})$.

It is then natural to ask whether a similar result can be obtained if the field $K(\mu_{p^\infty})$ is replaced by a larger field L. Consider a Galois extension L/K which contains the field $K(\mu_{p^\infty})$. Put $J_V = \rho(G_L)$. We ask

Question. When does the vector space V have vanishing J_V-cohomology?

2 Vanishing of $H^0(J_V, V)$

In this section we line up some known results about the vanishing of the group $H^0(J_V, V)$. For a p-adic Galois representation V as in the previous section, let T be a G_K-stable $\mathbb{Z}_p$-lattice. It is of great importance to determine whether the group $H^0(J_V, V/T)$ is finite or not. Establishing the finiteness of this group for J_V given by arbitrary p-adic Lie extension allows us to weaken hypothesis of many theorems in Iwasawa theory (cf. [9], Section 6). The finiteness of the group $H^0(J_V, V/T)$ is equivalent to the vanishing of the group $H^0(J_V, V)$ (cf. e.g. *op. cit.*, Lemma 2.1). Although the results that we will discuss in this subsection were originally stated in terms of $H^0(G_L, V/T)$, we will restate them in terms of $H^0(J_V, V)$ via the aforementioned equivalence statement.

The first related result was obtained by Imai [7]. Theorem 1.2, as well as the succeeding results that we will mention provide generalizations of this theorem.

Theorem 2.1. *Let A be an abelian variety over K with potential good reduction and consider the vector space $V = V_p(A)$ given by the Tate module of A and let $L = K(\mu_{p^\infty})$. Then the group $A(L)[p^\infty]$ is finite. That is, the group $H^0(J_V, V)$ vanishes.*

In [11], Ozeki considered the case when the field L is obtained by adjoining to K the coordinates of p-power torsion points of an abelian variety. Suppose A/K is an abelian variety with potential good *ordinary* reduction and consider $V = V_p(A)$. In this case Ozeki determined, under suitable conditions, a necessary and sufficient condition for the vanishing of $H^0(J_V, V)$. Let L be a Galois extension of K. Following *op. cit.*, we say that the residue field k_L of L is a *potential prime-to-p extension* if the p-part of the degree of k_L over k is finite. Then we have the following result

Theorem 2.2 ([11], Theorem 1.1 (2))**.** *Suppose A is an abelian variety with potential good ordinary reduction over K. Assume L contains $K(A[p])$ and $K(\mu_{p^\infty})$. Then $H^0(J_V, V)$ vanishes if and only if k_L is not a potential prime-to-p extension of k.*

In the case where $V = V_p(E)$ and $L = K(E'_\infty)$ are given by elliptic curves E/K and E'/K such that E has potential good reduction, Ozeki further proved the following

Theorem 2.3 ([11], Theorem 1.2)**.** *The group $H^0(J_V, V)$ vanishes in the following cases*:

E	E'
ordinary	*supersingular*
	multiplicative
supersingular with FCM	*ordinary*
	*supersingular with FCM**
	supersingular without FCM
	multiplicative
supersingular without FCM	*ordinary*
	supersingular with FCM
	*supersingular without FCM**
	multiplicative

In the table above, FCM means formal complex multiplication. An elliptic curve E over K with good supersingular reduction is said to have *formal complex multiplication over K* if the endomorphism ring of the p-divisible group $\mathcal{E}(p)$ associated with the Néron model $\mathcal{E}$ of E over $\mathcal{O}_K$ is a $\mathbb{Z}_p$-module of rank 2. The symbol * means that the vanishing holds under some suitable condition. The reader is encouraged to consult [11], particularly Propositions 3.10 and 3.11 for more details. The results that we will present provide an extension of the above theorem.

In a recent paper [9], Kubo and Taguchi studied the vanishing of $H^0(J_V, V)$ in the general setting where K is a complete discrete valuation field of mixed characteristic $(0, p)$. This includes the possibility that the residue field k of K is imperfect. For this setting, let M be the Kummer extension obtained by adjoining all p-power roots of all elements of $K^\times$.

Theorem 2.4 ([9], Theorem 1.2 (i))**.** *Let K be a complete discrete valuation field of mixed characteristic $(0, p)$. Assume X is a proper smooth variety over K with potential good reduction and i an odd integer ≥ 1. Put $V = H^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)$. Then the group $H^0(J_V, V)$ vanishes for any subfield L of M.*

Remark 2. Theorem 2.4 is just the p-part of the main result of Kubo and Taguchi. In fact, they also considered the l-adic cohomologies (cf. *op. cit.* Theorem 1.2 (ii)). With the notation and hypothesis in the theorem above, assume in addition that the residue field k of K is an algebraic extension of finite separable degree over a purely transcendental extension of a prime field (*essentially of finite type* in the language of [9]). Let $l \neq p$ be a prime. Then they proved that for the $\mathbb{Q}_l$-vector space $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_l)$, the group of G_L-fixed points $H^0(G_L, V)$ vanishes for any subfield L of M.

3 Preliminaries

3.1 Vanishing of Lie algebra cohomology

Let F be a field of characteristic 0 and U a finite dimensional vector space over F. Let $\mathfrak{G}$ be a finite dimensional Lie algebra over K. Suppose we have representation of Lie algebras

$$\tau : \mathfrak{G} \to \mathrm{End}(U)$$

We write $H^n(\mathfrak{G}, U)$ for the Lie algebra cohomology groups of U. These cohomology groups are vector spaces over F.

Definition 3.1. The vector space U has vanishing $\mathfrak{G}$-cohomology if the Lie algebra cohomology groups $H^n(\mathfrak{G}, U)$ are trivial for all $n \geq 0$.

If Z is an element of $\mathfrak{G}$, we write $A(Z)$ for the set of distinct eigenvalues of $\tau(Z)$ in an algebraic closure of F.

Definition 3.2. Assume τ is faithful. We say that τ satisfies the *strong Serre criterion* if there exists an element Z of $\mathfrak{G}$ with the following property: for every nonnegative integer k, and for each choice $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k, \beta_{k+1}$ of $2k+1$ not necessarily distinct elements of $A(Z)$, we have the following relation

$$\alpha_1 + \cdots + \alpha_k \neq \beta_1 + \cdots + \beta_{k+1}$$

(when $k = 0$, this is interpreted as meaning that every eigenvalue of $\tau(Z)$ is nonzero).

Lemma 3.3. *If τ satisfies the strong Serre criterion, then U has vanishing $\mathfrak{G}$-cohomology.*

3.2 Vanishing of H_V-cohomology

In this subsection, we recall how the vanishing of H_V-cohomology was proved. Recall our vector space $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$, where X is a proper smooth variety with potential good reduction over the p-adic local field K and i is an odd positive integer. Replacing K with a finite extension, we may assume that X has good reduction over K. Then V is a crystalline Galois representation. Let K_0 denote the maximal unramified extension of $\mathbb{Q}_p$ contained in K. We recall that V is said to be *crystalline* if

$$D_{\text{crys}}(V) = (\mathrm{B}_{\text{crys}} \otimes_{\mathbb{Q}_p} V)^{G_K}$$

has dimension d over K_0, where $d = \dim_{\mathbb{Q}_p} V$; here B_{crys} is Fontaine's ring for crystalline representations. The vector space $D_{\text{crys}}(V)$ is a filtered φ-module. This means $D_{\text{crys}}(V)$ is endowed with a filtration $(\mathrm{Fil}^i\, D_K)_{i\in\mathbb{Z}}$ indexed by $\mathbb{Z}$ on $D_K := K \otimes_{K_0} D_{\text{crys}}(V)$ that is decreasing ($\mathrm{Fil}^{i+1}\, D_K \subset \mathrm{Fil}^i\, D_K$), exhaustive ($\cup_{i\in\mathbb{Z}}\mathrm{Fil}^i\, D_K = D_K$) and separated ($\cap_{i\in\mathbb{Z}}\mathrm{Fil}^i\, D_K = 0$), and σ-linear map $\varphi : D_{\text{crys}}(V) \to D_{\text{crys}}(V)$, in the sense that

$\varphi(av) = \sigma(a)\varphi(v)$ for a in K_0 and v in $D_{\text{crys}}(V)$; here σ denotes the arithmetic Frobenius in the Galois group of K_0 over $\mathbb{Q}_p$. Let k denote the residue field of K and suppose it has cardinality $q = p^f$. Then

$$\Phi = \varphi^f$$

is a K_0-linear automorphism of $D_{\text{crys}}(V)$. Let $\lambda_1, \ldots, \lambda_d$ be the eigenvalues of Φ in $\overline{\mathbb{Q}}_p$. Since crystalline cohomology is a Weil cohomology theory, the purity results in crystalline cohomology (cf. [2]) implies that the eigenvalues $\lambda_1, \ldots, \lambda_d$ are q-Weil numbers of (odd) weight i (an algebraic number α is called a *q-Weil number of weight w* if $|\iota(\alpha)| = q^{w/2}$ for every embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$).

In addition to above, a deep result of Faltings shows that the vector space V is a Hodge-Tate representation, whose definition we now recall. For any vector space W over $\mathbb{Q}_p$ and a field extension $F/\mathbb{Q}_p$, put $W_F := W \otimes_{\mathbb{Q}_p} F$. Let C be the completion of $\overline{\mathbb{Q}}_p$. The Galois group G_K acts on C. The action of G_K on V can be extended to the C-vector space V_C by

$$\sigma(\sum_i (v_i \otimes c_i)) = \sum_i (\sigma(v_i) \otimes \sigma(c_i)), \qquad v_i \in V, c_i \in C, \sigma \in G_K.$$

Let $\chi : G_K \to \mathbb{Z}_p^\times$ denote the p-adic cyclotomic character. For $m \in \mathbb{Z}$, we define the set $V_C\{m\}$ to be the set of $v \in V_C$ such that

$$\sigma(v) = \chi(\sigma)^m v, \qquad \sigma \in G_K, v \in V.$$

The set $V_C\{m\}$ is in fact a K-vector subspace of V_C. That the representation V is *Hodge-Tate* means that the natural C-linear G_K-equivariant map

$$\xi : \bigoplus_{m \in \mathbb{Z}} (V_C\{m\} \otimes_K C) \to V_C$$

is an isomorphism. In particular, $V_C\{m\} \otimes_K C = 0$ for all but finitely many m. The nonzero integers m which occur in the above direct sum decomposition of V_C are called the *Hodge-Tate weights* of V.

Using Fontaine's theory of unramified Galois representations and Tannakian formalisms, Coates, Sujatha and Wintenberger constructed a special element of the Lie algebra $\mathfrak{H}_{\overline{\mathbb{Q}}_p}$, where $\mathfrak{H}$ is the Lie algebra of H_V.

Theorem 3.4 ([4], Theorem 3.2)**.** *There exists an element Z in the Lie algebra $\mathfrak{H}_{\overline{\mathbb{Q}}_p}$ such that for a suitable ordering of $\lambda_1, \ldots, \lambda_d$, the eigenvalues of Z on $V_{\overline{\mathbb{Q}}_p}$ are*

$$\log_\pi(\lambda_1 q^{t_1}), \ldots, \log_\pi(\lambda_d q^{t_d}),$$

where $q = p^f$ and $t_1, \ldots, t_d$ denote the Hodge-Tate weights of V.

Here, the logarithm $\log_\pi(\cdot)$ is the extension of the p-adic logarithm to the multiplicative group of $\overline{\mathbb{Q}}_p$ for some fixed non-zero element π of $\overline{\mathbb{Q}}_p$ whose absolute value is less than one. For the proof of Theorem 1.2, the element π may be chosen to be transcendental over $\mathbb{Q}$. The above theorem shows that for every family $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_{k+1}$ of $2k + 1$ elements of $A(Z)$, we have

$$S = (\alpha_1 + \cdots + \alpha_k) - (\beta_1 + \cdots + \beta_{k+1}) = \log_\pi(\kappa),$$

where κ is a q-Weil number of weight $m/2$, with m an odd integer. In particular, $S \neq 0$ and hence the strong Serre criterion is satisfied for the Lie algebra representation

$$\mathfrak{H}_{\overline{\mathbb{Q}}_p} \to \text{End}(V_{\overline{\mathbb{Q}}_p})$$

By Lemma 3.3, $V_{\overline{\mathbb{Q}}_p}$ has vanishing $\mathfrak{H}_{\overline{\mathbb{Q}}_p}$-cohomology. This implies that V has vanishing $\mathfrak{H}$-cohomology. Finally, by a result of Lazard (cf. [10], Theorem 2.4.10), the cohomology group $H^n(H_V, V)$ is a $\mathbb{Q}_p$-vector subspace of $H^n(\mathfrak{H}, V)$, for all $n \geq 0$. Thus, $H^n(H_V, V)$ are trivial for all $n \geq 0$, which completes the proof that V has vanishing H_V-cohomology.

3.3 Good ordinary reduction

In this subsection, we recall the notion of good ordinary reduction for proper smooth varieties as defined by Bloch-Kato (cf. [1], Definition 7.2) and an important consequence on the characterization of the étale cohomology groups of such varieties which was proved by Illusie [6]. This characterization allows us to obtain an idea on how the inertia subgroup of G_K acts on these cohomology groups.

Definition 3.5. Let X be a proper smooth variety over K. We say that X has *good ordinary reduction* over K if there exists a proper smooth model $\mathfrak{X}$ over $\mathcal{O}_K$ with special fiber $\mathcal{Y}$ such that the de Rham-Witt cohomology spaces $H^r(\mathcal{Y}, d\Omega^s_{\mathcal{Y}})$ are trivial for all r and all s. Here, $d\Omega^s_{\mathcal{Y}}$ is the sheaf of exact differentials on $\mathcal{Y}$.

Equivalent statements for this definition are given in Proposition 7.3 of *op. cit.* When X is an abelian variety of dimension g, this definition coincides with the property that the group of $\bar{k}$-points of $\mathcal{Y}$ killed by p is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^g$, which is the classical definition of an abelian variety with good ordinary reduction.

Definition 3.6. Let W be a p-adic Galois representation. We say that W is *ordinary* if there is a filtration $(\mathrm{Fil}^i\, W)_{i\in\mathbb{Z}}$ by G_K-stable subspaces $\mathrm{Fil}^i\, W$ that is decreasing ($\mathrm{Fil}^{i+1}\, W \subset \mathrm{Fil}^i\, W$), exhaustive ($\cup_{i\in\mathbb{Z}}\mathrm{Fil}^i\, W = V$) and separated ($\cap_{i\in\mathbb{Z}}\mathrm{Fil}^i\, W = 0$) such that the inertia subgroup I_K of G_K acts on the graded quotients $\mathrm{gr}^r\, W = \mathrm{Fil}^r\, W/\mathrm{Fil}^{r+1}\, W$ by χ^r, where χ is the p-adic cyclotomic character.

By working on the results of Bloch-Kato and Hyodo, Illusie proved the following characterization of the étale cohomology groups of X with good ordinary reduction.

Theorem 3.7 ([6], Corollary 2.7)**.** *Let X be a proper smooth variety over K. If X has good ordinary reduction, then the étale cohomology groups $H^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)$ are ordinary in the sense of Definition* 3.6*.*

Suppose X is a proper smooth variety over K with good ordinary reduction. The result above implies in particular that for the p-adic Galois representation $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$, the image by ρ of the inertia subgroup I_K is representable by upper triangular matrices

$$\begin{pmatrix} * & * & \dots & * \\ & * & \dots & * \\ & & \ddots & \vdots \\ & & & * \end{pmatrix},$$

whose diagonal entries are images by integral powers of the p-adic cyclotomic character.

4 Results

We now present our main results and give a sketch of their proofs. For a p-adic Galois representation V, recall that ρ denotes the continuous homomorphism given by the action of G_K. When $V = V_p(E)$ is given by an elliptic curve E, we denote ρ by ρ_E.

4.1 Statement of Results

Theorem 4.1. *Let X be a proper smooth variety over K with potential good ordinary reduction* (*in the sense of Definition* 3.5) *and $i > 0$ an odd integer. Consider an elliptic curve E/K with potential good supersingular reduction.*
(*a*) *Let $V = H^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)$ and $L = K(E_\infty)$. Then V has vanishing J_V-cohomology, where $J_V = \rho(G_L)$;*
(*b*) *Let $V' = V_p(E)$ and $L' = K(V)$, where V is the $\mathbb{Q}_p$-vector space in* (*a*). *Then V' has vanishing $J_{V'}$-cohomology, where $J_{V'} = \rho_E(G_{L'})$.*

Suppose E is an elliptic curve with potential good reduction over K and assume $L = K(E'_\infty)$ is given by another elliptic curve E'. By distinguishing the reduction types of E and E', we obtain the following result on the vanishing of J_V-cohomology of $V = V_p(E)$, where $J_V = \rho_E(G_L)$. It also involves the case where E' has potential multiplicative reduction. This extends some of the results obtained in [11].

Theorem 4.2. *Let E, E' and J_V be as given above. The vanishing of J_V-cohomology of $V = V_p(E)$ is given by the following table*:

E	*E'*	*J_V-cohomology vanish*
ordinary	*ordinary*	*No*
	supersingular	*Yes*
	multiplicative	*Yes*
supersingular with FCM	*ordinary*	*Yes*
	supersingular with FCM	*Yes**
	supersingular without FCM	*Yes*
	multiplicative	*Yes*
supersingular without FCM	*ordinary*	*Yes*
	supersingular with FCM	*Yes*
	supersingular without FCM	*Yes**
	multiplicative	*Yes*

The symbol $*$ means conditional vanishing. The vanishing in such cases hold under the additional assumption that the group $E(L)[p^\infty]$ of L-rational points of E of p-power order is finite. We see that for these cases the vanishing of all cohomology groups is determined by the vanishing of the group $H^0(J_V, V)$.

Remark 3. When the elliptic curve E in Theorem 4.1 has potential good ordinary reduction, the vanishing result may not hold because $H^0(J_V, V)$ may be nontrivial. This is easily observed by taking $V = V_p(E)$ and $E' = E$. In fact this observation is valid in a more general setting (cf. Theorem 2.2).

4.2 Sketch of Proofs

We outline the ideas used in the proofs of Theorems 4.1 and 4.2. The theorem follows from Theorem 1.2 if we prove that $J_V \simeq \mathrm{Gal}(K(V)/K(V) \cap L)$ is an open subgroup of $H_V \simeq \mathrm{Gal}(K(V)/K(V) \cap K(\mu_{p^\infty}))$. This is equivalent to the finiteness of the degree of the field extension $K(V) \cap L$ over $K(V) \cap K(\mu_{p^\infty})$. Since Theorem 1.2 holds for any finite extension of $\mathbb{Q}_p$, it does no harm to replace the base field with a finite extension in our proofs.

The proofs make use of the following description of the Lie algebra $\mathfrak{g} \subset \mathrm{End}(V_p(E))$ associated with an elliptic curve E over K (cf. [13], Appendix of Chapter IV):

Reduction of E		$\mathfrak{g}$
good supersingular	FCM	split Cartan subalgebra
	non-FCM	$\mathrm{End}(V_p(E))$
good ordinary	CM	nonsplit Cartan subalgebra
	non-CM	Borel subalgebra
multiplicative		half-Borel subalgebra

By a half-Borel subalgebra, we mean the algebra of 2×2-matrices with zero entries on the second row.

Proof of Theorem 4.1. Replacing K with a finite extension, we may assume that X has good ordinary reduction, E has good supersingular reduction over K and that $K(V)$ contains the field $K(\mu_{p^\infty})$. Let K^{ur} be the maximal unramified extension of K in K^{sep} and put $N_\infty = K(V) \cap K^{\mathrm{ur}}(\mu_{p^\infty})$. The assumption on X implies that the Galois group $\mathrm{Gal}(K(V)/N_\infty) \simeq \rho(I_K \cap G_{K(\mu_{p^\infty})})$ consists of unipotent matrices. Thus, its Lie algebra is nilpotent.

On the other hand, since E has good supersingular reduction, the Lie algebra $\mathfrak{h}$ of the p-adic Lie group $\mathrm{Gal}(L/K(\mu_{p^\infty}))$ is given by

$$\mathfrak{h} = \begin{cases} \text{Cartan subalgebra of } \mathfrak{sl}_2(\mathbb{Q}_p), & \text{if } E \text{ has FCM,} \\ \mathfrak{sl}_2(\mathbb{Q}_p), & \text{if } E \text{ has no FCM.} \end{cases}$$

We obtain the finiteness of $[M : K(\mu_{p^\infty})]$, where $M = K(V) \cap L$, from these observations. □

Proof of Theorem 4.2. After replacing K by a finite extension, we may assume that the elliptic curves E has good reduction over K and that E' has good reduction or multiplicative reduction over K depending on the hypothesis about E'. We consider the following cases:

(Case 1) Assume that E has good ordinary reduction and E' has good supersingular reduction, or vice versa. This case is a special case of Theorem 4.1.

(Case 2) Suppose E has good supersingular reduction and E' has good supersingular reduction or multiplicative reduction. Then we compare the p-adic Lie groups $H = \mathrm{Gal}(K(E_\infty)/K(\mu_{p^\infty}))$ and $H' = \mathrm{Gal}(K(E'_\infty)/K(\mu_{p^\infty}))$ or their Lie algebras. Ozeki proved that in this case, the group $E(K(E'_\infty))[p^\infty]$ is finite if and only if the field $K(E_\infty)$ does not contain the field $K(E'_\infty)$. This finiteness result and the description of the Lie algebras of H and H' allow us to deduce the finiteness of $[K(E_\infty) \cap K(E'_\infty) : K(\mu_{p^\infty})]$.

(Case 3) Assume E has good ordinary reduction and E' has multiplicative reduction over K. Then by the theory of Tate curves (cf. [14]), we can express the field $K(E'_\infty)$ in the following form:

$$K(E'_\infty) = K'(\mu_{p^\infty}, \alpha^{p^{-\infty}}),$$

where $[K' : K] \leq 2$ and $v_p(\alpha) = -v_p(j_{E'}) > 0$. On the other hand Serre-Tate theory (cf. [8]) allows us to express the field $K(E_\infty)$ in the form:

$$K(E_\infty) = H_\infty(\mu_{p^\infty}, q_E^{p^{-\infty}}),$$

for some unit element q_E in $H_\infty = K(E_\infty) \cap K^{\mathrm{ur}}$. Note that q_E is a root of unity if and only if E has complex multiplication over K. The finiteness of the degree of the field $K(E_\infty) \cap K(E'_\infty)$ over $K(\mu_{p^\infty})$ follows from Kummer theory. □

References

[1] S. Bloch and K. Kato, *p-adic étale cohomology*, Inst. Hautes Etudes Sci. Publ. Math. **63** (1986), 107–152.

[2] B. Chiarellotto and B. Le Stum, *Sur la pureté de la cohomologie cristalline*, C. R. Acad. Sci. Paris Ser. I Math. **326** (1998), 961–963.

[3] J. Coates and S. Howson, *Euler Characteristics and elliptic curves. II*, J. Math. Soc. Japan **53** (2001), 175–235.

[4] J. Coates, R. Sujatha and J-P. Wintenberger, *On Euler-Poincaré characteristics of finite dimensional p-adic Galois representations*, Inst. Hautes Études Sci. Publ. Math. **51** (2001), 107–143.

[5] J. Dimabayao, *On the vanishing of cohomologies of p-adic Galois representations associated with elliptic curves*, preprint, 2013, arXiv:1309.7240v1.

[6] L. Illusie, *Réduction semi-stable ordinaire, cohomologie étale p-adique et Cohomologie de de Rham, d'apres Bloch-Kato et Hyodo*, In: Périodes p-adiques, Seminaire de Bures, 1988, (J-M Fontaine ed.), 209–220, Astérisque, 223, Soc. Math. France, Montrouge, 1994.

[7] 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.

[8] N. Katz and B. Mazur, Arithmetic Moduli of Elliptic Curves, Annals of Mathematics Studies, 108, Princeton University Press, Princeton, NJ, 1985.

[9] Y. Kubo and Y. Taguchi, *A generalization of a theorem of Imai and its applications to Iwasawa theory*, Mathematische Zeitschrift **275** (2013), 1181–1195.

[10] M. Lazard, *Groupes analytiques p-adiques*, Inst. Hautes Études Sci. Publ. Math. **26** (1965), 389–603.

[11] Y. Ozeki, *Torsion Points of Abelian Varieties with Values in Infinite Extensions over a p-adic Field*, Publ. Res. Inst. Math. Sci. **45** (2009), 1011–1031.

[12] B. Perrin-Riou, *Représentations p-adiques ordinaires*, In: Périodes p-adiques, Seminaire de Bures, 1988, (J-M Fontaine ed.), 185–208, Astérisque, 223, Soc. Math. France, Montrouge, 1994.

[13] J-P. Serre, Abelian l-adic Representations and Elliptic Curves, With the collaboration of Willem Kuyk and John Labute. Second Edition, Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[14] J. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Math, 151, Springer-Verlag, New York, 1994.

[15] S. L. Zerbes, *Generalised Euler characteristics of Selmer groups*, Proc. London Math. Soc. (3) **98** (2009), 775–796.