On the cohomological coprimality of Galois representations associated with elliptic curves

By Jerome Tomagan DIMABAYAO

Institute of Mathematics, University of the Philippines, C.P. Garcia St., U.P. Campus Diliman, 1101 Quezon City, Philippines

(Communicated by Heisuke HIRONAKA, M.J.A., Nov. 12, 2015)

Abstract: Let E and E' be elliptic curves over an algebraic number field. We show that systems of ℓ-adic representations associated with E and E' are cohomologically coprime, in the sense that the Galois cohomology groups corresponding to respective fields of division points are all trivial. This provides a generalization of some known results about the vanishing of the cohomology groups associated with the ℓ-adic Tate module of an elliptic curve.

Key words: Galois representations; elliptic curves.

1. Introduction. Let G be a topological group. Given two continuous representations V and V' of G, we are interested in determining up to what extent they are "independent". There can be several notions of "independence", the simplest being non-isomorphism. Another notion is the "independence" among representations in a given system of representations of a profinite group (see §2) which was studied in [12]. Motivated by results of [1] and [2], we introduce in this note another notion of "independence" between representations of a topological group and prove that under some suitable conditions, representations of the absolute Galois group of a number field associated with two elliptic curves are "independent" in this sense.

Let F be an algebraic number field and we fix a separable closure $\overline{F}$ of F. For a subextension L of $\overline{F}$, we put $G_L = \mathrm{Gal}(\overline{F}/L)$. Let ℓ be a prime number. Denote by $F(\mu_{\ell^\infty})$ the field extension obtained by adjoining to F all the roots of unity of ℓ-power order. Let E be an elliptic curve over F. The action of G_F on the division points of E with order a power of ℓ defines a continuous homomorphism

$$\rho_{\ell,E} : G_F \to \mathrm{GL}(T_\ell(E)) \simeq \mathrm{GL}_2(\mathbf{Z}_\ell),$$

where $T_\ell(E)$ denotes the ℓ-adic Tate module of E. We write $V_\ell(E) = T_\ell(E) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. We denote by $F(E_{\ell^\infty})$ the field extension obtained by adjoining to F the coordinates of all ℓ-power division points of E. Note that $F(E_{\ell^\infty})$ is the fixed subfield of $\overline{F}$ by the kernel of $\rho_{\ell,E}$. Moreover, the Weil pairing shows that $F(E_{\ell^\infty})$ contains $F(\mu_{\ell^\infty})$. Put $G_{\ell,E} = \rho_{\ell,E}(G_F)$ and $H_{\ell,E} = \rho_{\ell,E}(G_{F(\mu_{\ell^\infty})})$. We may identify $G_{\ell,E}$ with the Galois group $\mathrm{Gal}(F(E_{\ell^\infty})/F)$ and H_ℓ with $\mathrm{Gal}(F(E_{\ell^\infty})/F(\mu_{\ell^\infty}))$. We have the following variant of results of Serre [10] and Coates-Sujatha [1].

Theorem 1.1. *Let ℓ be a prime number. Let U be an open normal subgroup of $G_{\ell,E}$ or of $H_{\ell,E}$. Then $V_\ell(E)$ has vanishing U-cohomology.*

Here, a topological module V over a topological ring R is said to have *vanishing U-cohomology*, where U is a topological group which acts continuously and faithfully on V, if the cohomology groups $H^n(U,V)$ defined by continuous cochains are trivial for all $n = 0, 1, \ldots$.

Proof. If U is an open normal subgroup of $G_{\ell,E}$ then we have an equality $\mathrm{Lie}(U) = \mathrm{Lie}(G_{\ell,E})$ of Lie algebras. By a theorem of Lazard ([7], Chap. V, Théorème 2.4.10), we may identify $H^n(U, V_\ell(E))$ with a $\mathbf{Q}_\ell$-vector subspace of $H^n(\mathrm{Lie}(G_{\ell,E}), V_\ell(E))$. The statement follows directly from Théorème 2 of [10]. We assume henceforth that U is an open normal subgroup of $H_{\ell,E}$. Lemma 4 of [1] shows the existence of a closed normal subgroup J of $G_{\ell,E}$ such that $H_{\ell,E}$ is an open subgroup of J and having the following property: If $\mathfrak{J}$ is the Lie algebra of J, then $H^n(\mathfrak{J}, V_\ell(E)) = 0$ for all $n \geq 0$. Note that the Lie algebras $\mathrm{Lie}(U)$ and $\mathfrak{J}$ coincide by the hypothesis. Arguing in a similar manner as above, we obtain our desired result. □

It is interesting to identify the field extensions of F with respect to which the corresponding cohomology groups vanish as in Theorem 1.1. In

2000 Mathematics Subject Classification. Primary 11F80, 11G05.

doi: 10.3792/pjaa.91.141

particular, we are interested in the case where the field extension corresponds to the kernel of another representation of G_F. This motivates the following

Definition 1.2. Let G be a topological group and R and R' be topological rings. Let $\rho : G \to \mathrm{GL}_R(V)$ and $\rho' : G \to \mathrm{GL}_{R'}(V')$ be two continuous linear representations of G on a topological R-module V and a topological R'-module V', respectively. Put $\mathcal{G} = \rho(\operatorname{Ker}\rho')$ and $\mathcal{G}' = \rho'(\operatorname{Ker}\rho)$. We say that V and V' are *cohomologically coprime* if V has vanishing $\mathcal{G}$-cohomology and V' has vanishing $\mathcal{G}'$-cohomology.

Let Λ be the set of all primes and S be a subset of Λ. For an elliptic curve E over F, the system of representations $(\rho_{\ell,E})_{\ell\in S}$ of G_F associated with E defines a continuous representation

$$\rho_{S,E} = \left(\prod_{\ell\in S}\rho_{\ell,E}\right) : G_F \to \prod_{\ell\in S}\mathrm{GL}(T_\ell(E)) \simeq \prod_{\ell\in S}\mathrm{GL}_2(\mathbf{Z}_\ell),$$

where the products in the right-hand side are endowed with the product topology. Put $V_S(E) = \bigoplus_{\ell\in S} V_\ell(E)$. We prove the following

Theorem 1.3. *Let S and S' be sets of primes. Let E and E' be elliptic curves over F.*
(i) *Assume that E and E' are not isogenous over $\overline{F}$. Then $V_S(E)$ and $V_{S'}(E')$ are cohomologically coprime.*
(ii) *If $S \cap S' = \emptyset$, then $V_S(E)$ and $V_{S'}(E')$ are cohomologically coprime.*

In fact, statement (ii) of Theorem 1.3 holds for general abelian varieties. On the other hand, an analogue of statement (i) does not hold for general abelian varieties. If A is an abelian variety over F which is a product of non-trivial abelian varieties A_1 and A_2 over F, then it can be verified that the p-adic representations $V_p(A)$ and $V_p(A_1)$ are not cohomologically coprime. We may then ask whether the statement (i) of Theorem 1.3 holds in the case of simple abelian varieties and not just elliptic curves. The crucial ingredient in the proof of Theorem 1.3 is the finiteness of the degree of $F(E_{\Lambda^\infty}) \cap F(E'_{\Lambda^\infty})$ over F^{cyc}; and an extension of this finiteness result for the case of simple abelian varieties will give the desired analogue of our main theorem. Here, $F(E_{\Lambda^\infty})$ denotes the fixed subfield of $\overline{F}$ by the kernel of $\rho_{\Lambda,E}$ and F^{cyc} is the field extension obtained by adjoining to F all roots of unity.

The Isogeny Theorem due to Faltings ([4], §5 Korollar 2) implies that

E and E' are isogenous over F
$\Leftrightarrow V_\ell(E) \simeq V_\ell(E')$ as G_F-modules for some prime ℓ
$\Leftrightarrow V_\ell(E) \simeq V_\ell(E')$ as G_F-modules for all primes ℓ.

Hence we have the following

Corollary 1.4. *Let E and E' be elliptic curves over F. The following statements are equivalent:*
(i) *E and E' are not isogenous over $\overline{F}$;*
(ii) *$V_S(E)|_{G_{F'}}$ and $V_{S'}(E')|_{G_{F'}}$ are cohomologically coprime for any S and S' and for every finite extension F' of F;*
(iii) *$V_\ell(E)|_{G_{F'}}$ $(= V_{\{\ell\}}(E)|_{G_{F'}})$ and $V_\ell(E')|_{G_{F'}}$ $(= V_{\{\ell\}}(E')|_{G_{F'}})$ are cohomologically coprime for some prime number ℓ and for every finite extension F' of F.*

Proof. The implication (i) $\Rightarrow$ (ii) is given by Theorem 1.3-(i) and clearly (ii) $\Rightarrow$ (iii). We show (iii) $\Rightarrow$ (i). If E and E' are isogenous over $\overline{F}$, then they are isogenous over some finite extension F' of F. Then the Isogeny Theorem implies that $V_\ell(E)$ and $V_\ell(E')$ are isomorphic as $G_{F'}$-modules for any prime ℓ. Since kernels of isomorphic representations coincide, $V_\ell(E)$ and $V_\ell(E')$ are not cohomologically coprime over F'. $\square$

We refer the reader to §6 of [3] for some partial results in a similar but more general setting.

Details of this paper were presented in the Algebraic Number Theory and Related Topics Workshop at RIMS, Kyoto University in December 2014 and a report will appear in its proceedings.

2. Almost independence of systems of representations. Let G be a profinite group and $(\varrho_i : G \to G_i)_{i\in I}$ be a system of continuous homomorphisms of G into a locally compact group G_i. This system defines a continuous homomorphism $\varrho = (\varrho_i)_{i\in I} : G \to \prod_{i\in I} G_i$ where the product is endowed with the product topology. Following [12], we make the following

Definition 2.1. The system $(\varrho_i)_{i\in I}$ is said to be *independent* if $\varrho(G) = \prod_{i\in I}\varrho_i(G)$. We say that it is *almost independent* if there exists an open subgroup Γ in G such that $\varrho(\Gamma) = \prod_{i\in I}\varrho_i(\Gamma)$.

Remark 2.2. (1) Let φ_1 and φ_2 be continuous representations of a profinite group G. Consider the continuous homomorphism $\varphi = (\varphi_1, \varphi_2) : G \to \varphi_1(G) \times \varphi_2(G)$. We have projections $\pi_1 : \varphi(G) \twoheadrightarrow \varphi_1(G)$ and $\pi_2 : \varphi(G) \twoheadrightarrow \varphi_2(G)$. Let $N_1 = \operatorname{Ker}\pi_2$ and

$N_2 = \operatorname{Ker}\pi_1$. Then $N_1 = \varphi(G) \cap (\varphi_1(G) \times \{1\})$ and $N_2 = \varphi(G) \cap (\{1\} \times \varphi_2(G))$. Thus we may identify N_i with a normal subgroup of $\varphi_i(G)$ for $i = 1, 2$. Goursat's lemma (cf. e.g. [9], Lemma 5.2.1) implies that

$$\varphi(G) = \varphi_1(G) \times_C \varphi_2(G),$$

where C in the fiber product is $\varphi(G)/(N_1N_2) \simeq \varphi_1(G)/N_1 \simeq \varphi_2(G)/N_2$. Then the following statements are equivalent:
(i) (φ_1, φ_2) is almost independent;
(ii) $\varphi(G)$ is an open subgroup of $\varphi_1(G) \times \varphi_2(G)$;
(iii) C is finite.
We clearly have (ii) $\Leftrightarrow$ (iii) as the cardinality of C equals the index of $\varphi(G)$ in $\varphi_1(G) \times \varphi_2(G)$. The implication (ii) $\Rightarrow$ (i) is a special case of the implication (RO) $\Rightarrow$ (PR) in [12], §1. We verify (i) $\Rightarrow$ (ii). Assume (i). Let Γ be an open subgroup of G such that $(\varphi_1|_\Gamma, \varphi_2|_\Gamma)$ is independent. Since $\varphi_1(\Gamma)$ (resp. $\varphi_2(\Gamma)$) is an open subgroup of $\varphi_1(G)$ (resp. $\varphi_2(G)$), it follows that $\varphi(\Gamma)$ is an open subgroup of $\varphi_1(G) \times \varphi_2(G)$. We obtain (ii) from the inclusion:

$$\varphi(\Gamma) \subseteq \varphi(G) \subseteq \varphi_1(G) \times \varphi_2(G).$$

(2) Let $(\varrho_i)_{i\in I}$ be a system of continuous homomorphisms of a profinite group G into a locally compact group G_i and ϱ be the continuous homomorphism defined by their product as in the definition above. Let S be a subset of I and put $S' = I \smallsetminus S$. We consider the subsystem $(\varrho_i)_{i\in\bullet}$ and the homomorphism $\varrho_\bullet$ given by the product, where $\bullet = S, S'$. If $(\varrho_i)_{i\in I}$ is independent, then $(\varrho_S, \varrho_{S'})$ is independent. Indeed, since subsystems of an independent system are independent (cf. [12], §1), the systems $(\varrho_i)_{i\in\bullet}$ are independent (where $\bullet = S, S'$). Then the equalities $\varrho(G) = \prod_{i\in S}\varrho_i(G) \times \prod_{i\in S'}\varrho_i(G) = \varrho_S(G) \times \varrho_{S'}(G)$ imply the surjectivity of $\varphi = \varrho_S \times \varrho_{S'} : G \to \varrho_S(G) \times \varrho_{S'}(G)$.
(3) Applying (1) to the situation of (2), we see that if $(\varrho_i)_{i\in I}$ is almost independent, then the group C in the fiber product $\varrho_S(G) \times_C \varrho_{S'}(G)$ is finite.

We aim to show that the independence of a system is inherited by the system of representations obtained by restriction to a normal subgroup (resp. by passing to a quotient) of G. Consider a system $(\varrho_i)_{i\in I}$ as above. Let H be a closed normal subgroup of G. For each $i \in I$, we define the continuous homomorphism $\pi_i : \varrho_i(G) \to \bar{G}_i := \varrho_i(G)/\varrho_i(H)$ of compact groups. Then we obtain new systems of representations:

$$(\varrho_i|_H : H \to G_i)_{i\in I}$$

obtained by restriction of the ϱ_i's ($i \in I$) to H and

$$(\bar{\varrho}_i : G \xrightarrow{\varrho_i} \varrho_i(G) \xrightarrow{\pi_i} \bar{G}_i)_{i\in I}.$$

Write $\bar{\varrho} = \prod_{i\in I}\bar{\varrho}_i$.

Lemma 2.3. *Let $(\varrho_i)_{i\in I}$ be a system of representations of a profinite group G. Let H be a closed normal subgroup of G. Then $(\varrho_i)_{i\in I}$ is independent if and only if the systems $(\varrho_i|_H)_{i\in I}$ and $(\bar{\varrho}_i)_{i\in I}$ are independent.*

Proof. By definition of $\bar{\varrho}$, we have the following commutative diagram of (compact) topological groups with exact rows

$$\begin{tikzcd}
1 \arrow[r] & \varrho(H) \arrow[r] \arrow[d, "\alpha"] & \varrho(G) \arrow[r] \arrow[d, "\beta"] & \bar{\varrho}(G) \arrow[r] \arrow[d, "\gamma"] & 1 \\
1 \arrow[r] & \prod_{i\in I}\varrho_i(H) \arrow[r] & \prod_{i\in I}\varrho_i(G) \arrow[r, "\prod_{i\in I}\pi_i"] & \prod_{i\in I}\bar{\varrho}_i(G) \arrow[r] & 1
\end{tikzcd} \tag{1}$$

where the maps α, β and γ are injective by definition. The five lemmas show that the independence of the systems $(\varrho_i|_H)_{i\in I}$ and $(\bar{\varrho}_i)_{i\in I}$ implies the independence of $(\varrho_i)_{i\in I}$. Conversely if $(\varrho_i)_{i\in I}$ is independent; that is, β is an isomorphism, then the five lemmas applied to the commutative diagram obtained by taking the first four terms of diagram (1) and adding trivial groups on the left end implies that the system $(\varrho_i|_H)_{i\in I}$ is independent. Applying the same argument to the commutative diagram obtained by taking the last four terms of diagram (1) and adding trivial groups on the right end implies that the system $(\bar{\varrho}_i)_{i\in I}$ is independent. $\square$

Now let us consider the case where the profinite group G in the definition above is the absolute Galois group G_F of a number field F and the index set I is the set Λ of all primes. Consider a system of continuous representations $(\varrho_\ell)_{\ell\in\Lambda} = (\varrho_\ell : G_F \to G_\ell)_{\ell\in\Lambda}$ of G_F into a locally compact ℓ-adic Lie group G_ℓ (e.g., $G_\ell = \mathrm{GL}_n(\mathbf{Q}_\ell)$). For each $\ell \in \Lambda$, let F_ℓ be the fixed subfield of $\overline{F}$ by the kernel of ϱ_ℓ. We write $\varrho_\Lambda = \prod_{\ell\in\Lambda}\varrho_\ell$ and F_Λ for the compositum of all F_ℓ as ℓ runs over the elements of Λ. The field F_Λ is the fixed subfield of $\overline{F}$ by the kernel of ϱ_Λ. We let F^{cyc} be the field extension obtained by adjoining to F all roots of unity.

Lemma 2.4. *Let $(\varrho_\ell)_{\ell\in\Lambda}$ be a system as above. Assume the following condition:*

$$F_\ell \supset F(\mu_{\ell^\infty}) \quad \textit{for each} \quad \ell \in \Lambda. \tag{2}$$

For $\ell \in \Lambda$, let $N_\ell = F_\ell \cap F^{\mathrm{cyc}}$. Then
(i) *if the system $(\varrho_\ell)_{\ell\in\Lambda}$ is independent then $N_\ell = F(\mu_{\ell^\infty})$ for each $\ell \in \Lambda$;*
(ii) *if the system $(\varrho_\ell)_{\ell\in\Lambda}$ is almost independent then $N_\ell/F(\mu_{\ell^\infty})$ is a finite extension for each $\ell \in \Lambda$.*

Note that the condition (2) implies that F_Λ contains the field F^{cyc}.

Proof. Statement (ii) follows from (i) after replacing F by a suitable finite extension. For the proof of (i), we apply Lemma 2.3 to the system $(\rho_\ell)_{\ell\in\Lambda}$ with $H = G_{F^{\mathrm{cyc}}}$. Then we may identify diagram (1) with the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{A} & \longrightarrow & \mathcal{B} & \longrightarrow & \mathcal{C} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \prod_{\ell\in\Lambda} \mathcal{A}_\ell & \longrightarrow & \prod_{\ell\in\Lambda} \mathcal{B}_\ell & \longrightarrow & \prod_{\ell\in\Lambda} \mathcal{C}_\ell & \longrightarrow & 1 \end{array} \tag{3}$$

where $\mathcal{A} = \mathrm{Gal}(F_\Lambda/F^{\mathrm{cyc}})$, $\mathcal{B} = \mathrm{Gal}(F_\Lambda/F)$, $\mathcal{C} = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$, $\mathcal{A}_\ell = \mathrm{Gal}(F_\ell/N_\ell)$, $\mathcal{B}_\ell = \mathrm{Gal}(F_\ell/F)$, and $\mathcal{C}_\ell = \mathrm{Gal}(N_\ell/F)$. By the hypothesis and Lemma 2.3, diagram (3) gives an isomorphism $\mathrm{Gal}(F^{\mathrm{cyc}}/F) \simeq \prod_{\ell\in\Lambda} \mathrm{Gal}(N_\ell/F)$. From this we get an isomorphism $\prod_{\ell\in\Lambda} \mathrm{Gal}(F(\mu_{\ell^\infty})/F) \simeq \prod_{\ell\in\Lambda} \mathrm{Gal}(N_\ell/F)$. Taking the projection to the ℓth component, we obtain an isomorphism $\mathrm{Gal}(F(\mu_{\ell^\infty})/F) \simeq \mathrm{Gal}(N_\ell/F)$ for each $\ell \in \Lambda$. This completes the proof of Lemma 2.4. $\square$

3. The elliptic curve setting. Let S be a set of primes. Given an elliptic curve E over F, we consider the system $(\rho_{\ell,E})_{\ell\in S}$ of G_F associated with E and the continuous representation $\rho_{S,E}$ as defined in §1. The Weil pairing shows that $F(\mu_{\ell^\infty})$ is contained in $F(E_{\ell^\infty})$ for each prime ℓ. The following lemma is a special case of Theorem 1 of [12].

Lemma 3.1. *Let S be a set of primes. Then the system $(\rho_{\ell,E})_{\ell\in S}$ is almost independent.*

Remark 3.2. In general, we need a finite extension F' of F so that the system $(\rho_{\ell,E}|_{G_{F'}})$ is independent. This is observed in the case where $S = \Lambda$ and E has complex multiplication over $\overline{F}$ with CM field $\mathbf{Q}(\sqrt{d})$ such that $\sqrt{d} \notin F$. Also note that there are examples of elliptic curves without complex multiplication such that $\rho_{\ell,E}$ is surjective for all prime ℓ but $\rho_{\Lambda,E}$ is not (so the system $(\rho_{\ell,E})_{\ell\in\Lambda}$ is not independent). This is illustrated by the following example.

Example 3.3. Consider the system $(\rho_{\ell,E} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_\ell))_{\ell\in\Lambda}$ associated with the elliptic curve E over $\mathbf{Q}$ of conductor 1728 with minimal Weierstrass model $y^2 = x^3 + 6x - 2$. It has no complex multiplication and its discriminant is $\Delta = -2^6 3^5$. This curve was considered in §5.9.2 of [11], where it was verified that the mod ℓ representation $\overline{\rho}_{\ell,E}$ associated with E is surjective for all ℓ. A group-theoretic result (cf. e.g. [5], Corollary 2.13-(iii)) implies that $\rho_{\ell,E}$ is surjective for all $\ell \geq 5$. The proof for the surjectivity of $\rho_{\ell,E}$ for $\ell = 2, 3$ was carried out in §I-7 of [6]. Hence $\rho_{\ell,E}$ is surjective for all ℓ. But $\sqrt{\Delta} \in \mathbf{Q}^{\mathrm{ab}} = \mathbf{Q}^{\mathrm{cyc}}$, where $\mathbf{Q}^{\mathrm{ab}}$ is the maximal abelian extension of $\mathbf{Q}$. Therefore, $\rho_{\Lambda,E}$ is not surjective by Theorem 1.2 of [5]. This shows that the system $(\rho_{\ell,E})_{\ell\in\Lambda}$ is not independent.

Lemma 3.4. *Let V be a finitely generated topological module over a topological ring R. Let G be a profinite group which acts continuously and faithfully on V and let N be a closed normal subgroup of G. If V has vanishing N-cohomology, then V has vanishing G-cohomology.*

Proof. Under the given assumption we have the Hochschild-Serre spectral sequence (cf. [8], Chap. II, §4, Theorem 2.4.1):

$$E_2^{rs} = H^r(G/N, H^s(N, V)) \Rightarrow H^{r+s}(G, V).$$

From this we immediately see that V has vanishing G-cohomology if V has vanishing N-cohomology. $\square$

Lemma 3.5. *Let S be a set of primes and L be a Galois extension of F. Assume that $F(E_{\ell^\infty}) \cap L$ is a finite extension of F or of $F(\mu_{\ell^\infty})$ for each $\ell \in S$. Put $J_{S,E} = \rho_{S,E}(G_L)$. Then $V_S(E)$ has vanishing $J_{S,E}$-cohomology.*

Proof. By Lemma 3.1, there exists a finite extension F'/F such that $(\rho_{\ell,E}|_{G_{F'}})_{\ell\in S}$ is an independent system. Let L' be the compositum of L and F'. It is a Galois extension of F'. Thus, Lemma 2.3 implies that $(\rho_{\ell,E}|_{G_{L'}})_{\ell\in S}$ is an independent system. Let L'' be the Galois closure of L'/L. This is of finite degree over L. Put $J'_{S,E} = \rho_{S,E}(G_{L''})$. Then $J'_{S,E}$ is an open normal subgroup of $J_{S,E}$ and applying Lemma 2.3 to the system $(\varrho_{\ell,E}|_{G_{F'}})$ with $H = G_{L''}$, we have $J'_{S,E} = \prod_{\ell\in S} \rho_{\ell,E}(G_{L''})$. It suffices to show that $V_S(E)$ has vanishing $J'_{S,E}$-cohomology by Lemma 3.4. As cohomology commutes with direct sums, we have

$$H^r(J'_{S,E}, V_S(E)) = \bigoplus_{\ell\in S} H^r(J'_{S,E}, V_\ell(E))$$

for $r \geq 0$. Thus, it is enough to show that the cohomology groups $H^r(J'_{S,E}, V_\ell(E))$ vanish for each

$\ell \in S$. For $\ell \in S$, let us write $J'_{\ell,E} = \rho_{\ell,E}(G_{L''})$. We identify $G_{\ell,E} = \rho_{\ell,E}(G_F)$ (resp. $H_{\ell,E} = \rho_{\ell,E}(G_{F(\mu_{\ell^\infty})})$) with the Galois group $\mathrm{Gal}(F(E_{\ell^\infty})/F)$ (resp. $\mathrm{Gal}(F(E_{\ell^\infty})/F(\mu_{\ell^\infty}))$). Then we may identify $J'_{\ell,E}$ with $\mathrm{Gal}(F(E_{\ell^\infty})/F(E_{\ell^\infty}) \cap L'')$. As $[F(E_{\ell^\infty}) \cap L'' : F(E_{\ell^\infty}) \cap L] \le [L'' : L] < \infty$, our hypothesis implies that $J'_{\ell,E}$ is an open subgroup of $G_{\ell,E}$ or of $H_{\ell,E}$. Thus $V_\ell(E)$ has vanishing $J'_{\ell,E}$-cohomology by Theorem 1.1. Applying Lemma 3.4 with $G = J'_{S,E}$ and $N = J'_{\ell,E}$, it follows that $V_\ell(E)$ has vanishing $J'_{S,E}$-cohomology. $\square$

The above lemmas allow us to obtain the S-adic version of Theorem 1.1:

Theorem 3.6. *Let S be a set of primes. Write $G_{S,E} = \rho_{S,E}(G_F)$ and $H_{S,E} = \rho_{S,E}(G_{F^{\mathrm{cyc}}})$. Let U be an open normal subgroup of $G_{S,E}$ or of $H_{S,E}$. Then $V_S(E)$ has vanishing U-cohomology.*

Proof. Let F' be a finite extension of F such that $U = \rho_{S,E}(G_{F'})$ or $U = \rho_{S,E}(G_{F'^{\mathrm{cyc}}})$. The statement of the theorem follows from Lemma 3.5 applied to $L = F'$ and $L = F'^{\mathrm{cyc}}$. The hypothesis of the said lemma clearly holds if $L = F'$. If $L = F'^{\mathrm{cyc}}$, the required hypothesis is true because of Lemmas 3.1 and 2.4. $\square$

4. Proof of Theorem 1.3. For sets S and S' of primes, we write $F(E_{S^\infty})$ (resp. $F(E'_{S'^\infty})$) for the compositum of all the $F(E_{\ell^\infty})$ (resp. $F(E'_{\ell^\infty})$) as ℓ runs over the elements of S (resp. S'). We put $J_{S,E} := \rho_{S,E}(G_{F(E'_{S'^\infty})})$ and $J_{S',E'} := \rho_{S',E'}(G_{F(E_{S^\infty})})$.

Proof of (i). To prove this, we must show that $V_S(E)$ has vanishing $J_{S,E}$-cohomology and $V_{S'}(E')$ has vanishing $J_{S',E'}$-cohomology. We prove the former. First, we observe that if S'' is a subset of S' then $J_{S,E}$ is a closed normal subgroup of $\mathcal{J}_{S,E} = \rho_{S,E}(G_{F(E'_{S''^\infty})})$. We see that the vanishing of $J_{S,E}$-cohomology implies the vanishing of $\mathcal{J}_{S,E}$-cohomology by applying Lemma 3.4. Thus, we may assume that $S' = \Lambda$. We verify the hypothesis of Lemma 3.5 with $L = F(E'_{\Lambda^\infty})$; that is, we show that $M_\ell := F(E_{\ell^\infty}) \cap L$ is a finite extension of $F(\mu_{\ell^\infty})$ for each $\ell \in S$. We let $M = F(E_{\Lambda^\infty}) \cap L$. It is known that M is a finite extension of F^{cyc} (cf. [11], Théorèmes $6''$ and 7). We also let

$$\begin{aligned} M_S &= F(E_{S^\infty}) \cap L = F(E_{S^\infty}) \cap M, \\ N_S &= F(E_{S^\infty}) \cap F^{\mathrm{cyc}}, \quad \text{and} \\ N_\ell &= F(E_{\ell^\infty}) \cap F^{\mathrm{cyc}} = F(E_{\ell^\infty}) \cap N_S. \end{aligned}$$

Note further that $M_\ell = F(E_{\ell^\infty}) \cap M = F(E_{\ell^\infty}) \cap M_S$ for each $\ell \in S$. We have the following diagram of fields.

$$\begin{tikzcd}[column sep=tiny]
 & & F(E_{\Lambda^\infty}) \arrow[dl, dash] \arrow[ddrr, dash] & & & & L = F(E'_{\Lambda^\infty}) \arrow[ddll, dash] \\
 & F(E_{S^\infty}) \arrow[dl, dash] \arrow[ddrr, dash] & & & & & \\
F(E_{\ell^\infty}) \arrow[ddrr, dash] & & & & M \arrow[dl, dash] \arrow[dr, dash] \arrow[dr, bend left, dash, "< \infty"] & & \\
 & & & M_S \arrow[dl, dash] \arrow[dr, dash] & & F^{\mathrm{cyc}} \arrow[dl, dash] & \\
 & & M_\ell \arrow[dr, dash] & & N_S \arrow[dl, dash] & & \\
 & & & N_\ell \arrow[d, dash] & & & \\
 & & & F(\mu_{\ell^\infty}) & & &
\end{tikzcd}$$

The extension M_ℓ/N_ℓ is of finite degree since $\mathrm{Gal}(M_\ell/N_\ell)$ is isomorphic to a quotient of the finite group $\mathrm{Gal}(M/F^{\mathrm{cyc}})$. Moreover N_ℓ is a finite extension of $F(\mu_{\ell^\infty})$ by Lemma 2.4. Thus the hypothesis of Lemma 3.5 holds. Therefore $V_S(E)$ has vanishing $J_{S,E}$-cohomology. Similarly, $V_{S'}(E')$ has vanishing $J_{S',E'}$-cohomology. This completes the proof of (i). $\square$

Proof of (ii). This is a special case of (i) if E and E' are not isogenous over $\overline{F}$. Suppose that E and E' are isogenous over $\overline{F}$. Then they are isogenous over some finite extension of F. Let F' be the Galois closure of this finite extension. Then the Isogeny Theorem (see §1) implies that $V_\ell(E) \simeq V_\ell(E')$ as $G_{F'}$-modules for each $\ell \in S'$. We identify $\rho_{S,E}(G_{F'})$ (resp. $\rho_{S',E}(G_{F'})$) with the Galois group $\mathrm{Gal}(F'(E_{S^\infty})/F')$ (resp. $\mathrm{Gal}(F'(E_{S'^\infty})/F')$). As S and S' are disjoint, applying Remark 2.2-(3) to the system $(\rho_{\ell,E}|_{G_{F'}}, \rho_{\ell',E'}|_{G_{F'}})_{\ell \in S, \ell' \in S'} = (\rho_{\ell,E}|_{G_{F'}})_{\ell \in S \cup S'}$ shows that $[F'(E_{\ell^\infty}) \cap F'(E_{S'^\infty}) : F'] \le [F'(E_{S^\infty}) \cap F'(E_{S'^\infty}) : F'] < \infty$ for each $\ell \in S$. Therefore $V_S(E)$ has vanishing $\mathcal{J}_{S,E}$-cohomology by Lemma 3.5, where $\mathcal{J}_{S,E} = \rho_{S,E}(G_{F'(E_{S'^\infty})})$. Then $V_S(E)$ has vanishing $J_{S,E}$-cohomology by Lemma 3.4 with $G = J_{S,E}$ and $N = \mathcal{J}_{S,E}$. In the same manner, we see that $V_{S'}(E')$ has vanishing $J_{S',E'}$-cohomology. This ends the proof of Theorem 1.3. $\square$

Acknowledgements. The author is greatly indebted to Prof. Yuichiro Taguchi for his guidance, advice and encouragement in the course of this work. He is also grateful to the anonymous referee for his/her thorough reading of this work and for helpful comments and suggestions. This work was done while the author was a student at

Kyushu University, Japan. He would also like to thank the Ministry of Education, Culture, Sports, Science and Technology of Japan for its support.

References

[1] J. Coates and R. Sujatha, Euler-Poincaré characteristics of abelian varieties, C. R. Acad. Sci. Paris Sér. I Math. **329** (1999), no. 4, 309–313.

[2] J. Coates, R. Sujatha and J.-P. Wintenberger, On the Euler-Poincaré characteristics of finite dimensional p-adic Galois representations, Publ. Math. Inst. Hautes Études Sci. **93** (2001), 107–143.

[3] J. T. Dimabayao, On the vanishing of cohomologies of p-adic Galois representations associated with elliptic curves, Kyushu J. Math. **69** (2015), no. 2, 367–386.

[4] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), no. 3, 349–366.

[5] A. Greicius, Elliptic curves with surjective adelic Galois representations, Experiment. Math. **19** (2010), no. 4, 495–507.

[6] S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics, 504, Springer, Berlin, 1976.

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

[8] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften, 323, Springer, Berlin, 2008.

[9] K. A. Ribet, Galois action on division points of Abelian varieties with real multiplications, Amer. J. Math. **98** (1976), no. 3, 751–804.

[10] J.-P. Serre, Sur les groupes de congruence des variétés abéliennes. II, Izv. Akad. Nauk SSSR Ser. Mat. **35** (1971), 731–737.

[11] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), no. 4, 259–331.

[12] J.-P. Serre, Un critère d'indépendance pour une famille de représentations ℓ-adiques, Comment. Math. Helv. **88** (2013), no. 3, 541–554.