FINE SELMER GROUPS AND ISOGENY INVARIANCE

R. SUJATHA AND M. WITTE

ABSTRACT. We investigate fine Selmer groups for elliptic curves and for Galois representations over a number field. More specifically, we discuss Conjecture A, which states that the fine Selmer group of an elliptic curve over the cyclotomic extension is a finitely generated $\mathbb{Z}_p$-module. The relationship between this conjecture and Iwasawa's classical $\mu = 0$ conjecture is clarified. We also present some partial results towards the question whether Conjecture A is invariant under isogenies.

1. INTRODUCTION

The fine Selmer group is a subgroup of the Selmer group of elliptic curves which plays an important role in Iwasawa theory. More generally, it can be defined for any Galois representation over a number field. It has been widely studied by many authors [Bil86], [PR00, App. B], [Gre11], [Wut07], [CS05]. In the last reference, the authors conjecture that the fine Selmer group of an elliptic curve over the cyclotomic extension is a finitely generated $\mathbb{Z}_p$-module (Conjecture A in *loc. cit.*). There is ample numerical evidence in support of this conjecture [Wut07], [Cha14]. It is further stated (rather optimistically) in [CS05] that Conjecture A should be invariant under isogeny. The results in this article indicate that the extent of optimism expressed towards isogeny invariance is not commensurate with what one can concretely prove. The relationship between Conjecture A and Iwasawa's classical $\mu = 0$ conjecture is already touched upon in [CS05] and [Gre11]. Our results in this paper demonstrate the depth of this relationship. In particular, the results seem to indicate that even the seemingly weaker isogeny invariance conjecture is potentially as difficult as the $\mu = 0$ conjecture.

This article has six sections. In Section 2, we introduce notation that is used subsequently throughout the paper. In Section 3, we discuss the fine Selmer group and its relation to other cohomological modules. Several assertions that are equivalent to Conjecture A are discussed in Section 4. In Section 5, we investigate the isogeny invariance of Conjecture A for elliptic curves. In particular, we prove isogeny invariance for a large class of CM elliptic curves. In the final Section 6, we point towards a connection of isogeny invariance and cup products in cohomology.

We would like to thank Karl Rubin, Christian Wuthrich, and Benedict Gross for helpful conversations on CM elliptic curves. We also thank Zheng Li for helpful insights into this problem.

---

2. Notation

Throughout the text, we will use the following notation. For any field F, we let G_F denote its absolute Galois group. The letter p will always denote an odd prime. If K is a number field, a *prime* of K will always refer to a non-archimedean place of K. If S is a finite set of primes of K, we will write K_S for the maximal extension of K which is unramified outside S and the archimedean places of K. We will always assume that S contains all primes of K above p. For any subextension L/K of K_S/K we let $G_S(L)$ denote the Galois group of K_S/L and S_L the primes of L above S. If v is a prime of L, we write L_v for the completion of L at v and $k(v)$ for its residue field. For any profinite group G, we write $\mathrm{cd}_p G$ for its p-cohomological dimension. For any compact or discrete G-module M, we write $\mathrm{H}^i(G, M)$ for the i-th continuous cohomology group of M and $M^\vee$ for its Pontryagin dual. For any compact or discrete $G_S(K)$-module M and any integer n, we write $M(n)$ for its n-th Tate twist.

We write K_{cyc} for the cyclotomic $\mathbb{Z}_p$-extension of K and let Γ denote the Galois group of K_{cyc}/K. The profinite group rings of Γ over $\mathbb{Z}_p$ and $\mathbb{F}_p$ will be denoted by

$$\Lambda = \mathbb{Z}_p[[\Gamma]], \qquad \Omega = \mathbb{F}_p[[\Gamma]],$$

respectively. We will write Q for the quotient field of Ω.

More generally, let $\mathcal{L}/K$ be any Galois subextension of K_S/K such that for some finite extension K'/K inside $\mathcal{L}$, the extension $\mathcal{L}/K'$ is pro-p. In particular, since the maximal pro-p-quotient of $G_S(K')$ is topologically finitely generated [NSW00, Thm. 10.7.12, Prop. 3.9.1], the Galois group $\mathcal{G} = G(\mathcal{L}/K)$ is topologically finitely generated, as well. The profinite group ring $\mathbb{Z}_p[[\mathcal{G}]]$ is then an *adic ring* in the sense that it is compact for the topology defined by the powers of its Jacobson radical $\mathfrak{J}_{\mathbb{Z}_p[[\mathcal{G}]]}$ [Wit14, Prop. 3.2]. We may equip $\mathbb{Z}_p[[\mathcal{G}]]$ with a continuous $G_S(K)$-action by letting $g \in G_S(K)$ act as multiplication by the inverse of its image in $\mathcal{G}$. Let $\mathbb{Z}_p[[\mathcal{G}]]^\sharp$ denote the corresponding $G_S(K)$-module.

Suppose that M is a compact $\mathbb{Z}_p$-module with a continuous $G_S(K)$-action such that $M^\vee$ is a countable set. In other words, M has a presentation

$$M = \varprojlim_{n \in \mathbb{N}} M_n$$

with M_n finite. We set

(2.1)
$$M_{\mathcal{L}} = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}_p[[\mathcal{G}]]^\sharp / \mathfrak{J}_{\mathbb{Z}_p[[\mathcal{G}]]}^n \otimes_{\mathbb{Z}_p} M_n$$

so that $M_{\mathcal{L}}$ is the completed tensor product over $\mathbb{Z}_p$ of $\mathbb{Z}_p[[\mathcal{G}]]^\sharp$ and M.

Let v be a prime of K. We then have

(2.2)
$$\mathrm{H}^i(G_S(K), M_{\mathcal{L}}) = \varprojlim_{K \subset L \subset \mathcal{L}} \mathrm{H}^i(G_S(L), M),$$

$$\mathrm{H}^i(G_{K_v}, M_{\mathcal{L}}) = \varprojlim_{K \subset L \subset \mathcal{L}} \bigoplus_{w | v} \mathrm{H}^i(G_{L_w}, M)$$

where the limit is taken over all finite subextensions L/K of $\mathcal{L}/K$ with respect to the corestriction map [NSW00, Cor. 2.7.6]. In particular, $\mathrm{H}^i(G_S(K), M_{\mathcal{L}})$ agrees with the group denoted by $\mathcal{Z}^i(M/\mathcal{L})$ in [CS05].

For any integral domain R with quotient field $Q(R)$ and any finitely generated R-module T, we will write $\mathrm{rk}_R T$ for the dimension of the vector space $Q(R) \otimes_R T$

over $Q(R)$. If M is a G_K-representation on a finite-dimensional vector space over $\mathbb{F}_p$, we set

$$r_M = \operatorname{rk}_{\mathbb{F}_p} \bigoplus_{v|\infty} H^0(K_v, M^\vee(1))$$

$$= -\operatorname{rk}_{\mathbb{F}_p} H^0(G_S(K), M) + \operatorname{rk}_{\mathbb{F}_p} H^1(G_S(K), M) - \operatorname{rk}_{\mathbb{F}_p} H^2(G_S(K), M),$$

where S is any finite set of primes of K containing the primes above p such that M is unramified outside S. In other words, r_M is the negative of the Euler characteristic of M as considered in [NSW00, 8.7.4]. We will write M^{ss} for the semisimplification of M.

For any elliptic curve E over K, we let $E[n]$ denote its n-torsion points considered as a G_K-module. We write

$$T_p E = \varprojlim_n E[p^n]$$

for the p-adic Tate module and

$$E[p^\infty] = \varinjlim_n E[p^n]$$

for the p-power division points of E.

3. The Fine Selmer Group and some Useful Exact Sequences

Let us recall the definition of the fine Selmer group from [CS05]. Let K be a number field, p an odd prime number, and S a finite set of primes of K containing the primes above p. Assume that $\mathcal{L}/K$ is any subextension of K_S/K.

Definition 3.1. For any discrete $G_S(\mathcal{L})$-module M, the *fine Selmer group* of M is given by

$$R_S(M/\mathcal{L}) = \varinjlim_{L/K} \ker\left(H^1(G_S(L), M) \to \bigoplus_{v \in S_L} H^1(G_{L_v}, M)\right),$$

with L/K running through the finite subextensions of $\mathcal{L}/K$. We write

$$Y_S(M/\mathcal{L}) = R_S(M/\mathcal{L})^\vee$$

for the Pontryagin dual of the fine Selmer group of M.

In general, $R_S(M/\mathcal{L})$ and $Y_S(M/\mathcal{L})$ do depend on the choice of S. However, if we assume that $\mathcal{L}$ contains the cyclotomic $\mathbb{Z}_p$-extension K_{cyc}, then the groups do not change if we enlarge S. In this case, we drop the S from the notation.

The justification is given as follows. As

$$R_S(M/\mathcal{L}) = \varinjlim_{L/K} R_S(M/L_{\mathrm{cyc}}),$$

with L/K running through the finite subextensions of $\mathcal{L}/K$, we may as well assume that $\mathcal{L} = K_{\mathrm{cyc}}$.

Let v be a prime of K_{cyc}. Write $I_v \subset G_{(K_{\mathrm{cyc}})_v}$ for the inertia group of v and let $k(v)$ be the residue field. The Hochschild-Serre spectral sequence gives an exact sequence

(3.1) $0 \to H^1(G_{k(v)}, M^{I_v}) \to H^1(G_{(K_{\mathrm{cyc}})_v}, M) \to H^0(G_{k(v)}, H^1(I_v, M)) \to 0.$

and an isomorphism

$$H^2(G_{(K_{\mathrm{cyc}})_v}, M) \cong H^1(G_{k(v)}, H^1(I_v, M)).$$

For any prime v of K_{cyc} not dividing p, $\mathrm{G}_{k(v)}$ is of order prime to p and the exact sequence (3.1) reduces to an isomorphism

$$(3.2) \qquad \mathrm{H}^1(\mathrm{G}_{(K_{\mathrm{cyc}})_v}, M) \cong \mathrm{H}^0(\mathrm{G}_{k(v)}, \mathrm{H}^1(I_v, M)),$$

while

$$\mathrm{H}^1(\mathrm{G}_{k(v)}, \mathrm{H}^1(I_v, M)) = 0.$$

Furthermore, if v is not contained in $S_{K_{\mathrm{cyc}}}$, then

$$\mathrm{H}^1(I_v, M) \cong M(-1)$$

as $\mathrm{G}_{k(v)}$-modules.

If T is any finite set of primes of K containing S, we thus obtain a long exact Gysin sequence

(3.3)
$$0 \to \mathrm{H}^1(\mathrm{G}_S(K_{\mathrm{cyc}}), M) \to \mathrm{H}^1(\mathrm{G}_T(K_{\mathrm{cyc}}), M) \to \bigoplus_{v \in (T-S)_{K_{\mathrm{cyc}}}} \mathrm{H}^0(\mathrm{G}_{k(v)}, M(-1))$$

$$\to \mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), M) \to \mathrm{H}^2(\mathrm{G}_T(K_{\mathrm{cyc}}), M) \to 0.$$

Note that every prime of K splits into only finitely many primes of K_{cyc}, so that $(T - S)_{K_{\mathrm{cyc}}}$ is still a finite set.

Hence,

(3.4)
$$R_T(M/K_{\mathrm{cyc}})$$

$$= \ker\left(\mathrm{H}^1(\mathrm{G}_T(K_{\mathrm{cyc}}), M) \to \bigoplus_{v \in (T-S)_{K_{\mathrm{cyc}}}} \mathrm{H}^0(\mathrm{G}_{k(v)}, M(-1)) \oplus \bigoplus_{v \in S_{K_{\mathrm{cyc}}}} \mathrm{H}^1(\mathrm{G}_{(K_{\mathrm{cyc}})_v}, M)\right)$$

$$= \ker\left(\mathrm{H}^1(\mathrm{G}_S(K_{\mathrm{cyc}}), M) \to \bigoplus_{v \in S_{K_{\mathrm{cyc}}}} \mathrm{H}^1(\mathrm{G}_{(K_{\mathrm{cyc}})_v}, M)\right)$$

$$= R_S(M/K_{\mathrm{cyc}}).$$

We also obtain isomorphisms

$$R(M/K_{\mathrm{cyc}}) \cong \ker\left(\mathrm{H}^1(\mathrm{G}_{K_{\mathrm{cyc}}}, M) \to \bigoplus_v \mathrm{H}^1(\mathrm{G}_{(K_{\mathrm{cyc}})_v}, M)\right)$$

$$\cong \ker\left(\mathrm{H}^1(\mathrm{G}_{K_{\mathrm{cyc}}}, M) \to \bigoplus_{v \nmid p} \mathrm{H}^1(I_v, M) \oplus \bigoplus_{v \mid p} \mathrm{H}^1(\mathrm{G}_{K_{\mathrm{cyc}}}, M)\right),$$

with v running through all primes of K_{cyc}. For the first isomorphism, we note that

$$\mathrm{G}_{K_{\mathrm{cyc}}} = \varprojlim_T \mathrm{G}_T(K_{\mathrm{cyc}}),$$

where T runs through all finite sets of primes of K containing S and then pass to the direct limit over all such T in equation (3.4). For the second isomorphism, we note from (3.2) that

$$\mathrm{H}^1(\mathrm{G}_{(K_{\mathrm{cyc}})_v}, M) \to \mathrm{H}^1(I_v, M)$$

is injective for all primes v of K_{cyc} not lying over p.

We digress briefly to express $R(M/K_{\mathrm{cyc}})$ in terms of étale cohomology as follows. Consider M as an étale sheaf on $\operatorname{Spec} K_{\mathrm{cyc}}$. Write $\mathcal{O}_{\mathrm{cyc}}$ for its ring of integers and

$$\eta \colon \operatorname{Spec} K_{\mathrm{cyc}} \to \operatorname{Spec} \mathcal{O}_{\mathrm{cyc}}$$

for the inclusion of the generic point. Then it follows easily from [Mil06, Prop. II.2.9] that

$$\mathrm{H}^1_{\text{ét}}(\operatorname{Spec}\mathcal{O}_{\text{cyc}},\eta_*M) \cong \ker\left(\mathrm{H}^1(\mathrm{G}_S(K_{\text{cyc}}),M) \to \bigoplus_{v \in S_{K_{\text{cyc}}}} \mathrm{H}^0(\mathrm{G}_{k(v)},\mathrm{H}^1(I_v,M))\right)$$

and

$$R(M/K_{\text{cyc}}) \cong \operatorname{im}\left(\mathrm{H}^1_c(\operatorname{Spec}\mathcal{O}_{\text{cyc}}[\tfrac{1}{p}],\eta_*M) \to \mathrm{H}^1_{\text{ét}}(\operatorname{Spec}\mathcal{O}_{\text{cyc}},\eta_*M)\right)$$

$$\cong \ker\left(\mathrm{H}^1_{\text{ét}}(\operatorname{Spec}\mathcal{O}_{\text{cyc}},\eta_*M) \to \bigoplus_{v|p} \mathrm{H}^1(\mathrm{G}_{k(v)},M^{I_v})\right).$$

Under the assumption that $\mathrm{H}^0(\mathrm{G}_{k(v)},M^{I_v}) = 0$ for all primes v of K_{cyc} dividing p, we also have

$$\mathrm{H}^1(\mathrm{G}_{k(v)},M^{I_v}) = 0$$

and hence,

$$R(M/K_{\text{cyc}}) \cong \mathrm{H}^1_{\text{ét}}(\operatorname{Spec}\mathcal{O}_{\text{cyc}},\eta_*M).$$

Assume that M is countable as a set. Recall from [CS05, Prop. 2.1] that

$$\mathrm{H}^0(\mathrm{G}_S(K),(M^\vee)_{K_{\text{cyc}}}(1)) = 0,$$

$$\left(\bigoplus_{w \in S} \mathrm{H}^0(\mathrm{G}_{K_w},(M^\vee)_{K_{\text{cyc}}}(1))\right)^\vee = \bigoplus_{v \in S_{K_{\text{cyc}}}} \mathrm{H}^2(\mathrm{G}_{(K_{\text{cyc}})_v},M) = 0,$$

where $M^\vee_{K_{\text{cyc}}}$ is defined as in (2.1). By passing to the direct limit over all finite subsets of M and all finite subextensions of K_{cyc}/K, we obtain from the Poitou-Tate sequence an exact sequence of discrete $\mathbb{Z}_p$-modules

(3.5)

$$0 \to \mathrm{H}^0(\mathrm{G}_S(K_{\text{cyc}}),M) \to \bigoplus_{v \in S_{K_{\text{cyc}}}} \mathrm{H}^0(\mathrm{G}_{(K_{\text{cyc}})_v},M)$$

$$\to \mathrm{H}^2(\mathrm{G}_S(K),(M^\vee)_{K_{\text{cyc}}}(1))^\vee \to \mathrm{H}^1(\mathrm{G}_S(K_{\text{cyc}}),M) \to \bigoplus_{v \in S_{K_{\text{cyc}}}} \mathrm{H}^1(\mathrm{G}_{(K_{\text{cyc}})_v},M)$$

$$\to \mathrm{H}^1(\mathrm{G}_S(K),(M^\vee)_{K_{\text{cyc}}}(1))^\vee \to \mathrm{H}^2(\mathrm{G}_S(K_{\text{cyc}}),M) \to 0$$

Again, we use that $S_{K_{\text{cyc}}}$ is a finite set.

Taking the dual, we also obtain an exact sequence of compact $\mathbb{Z}_p$-modules

(3.6)

$$0 \to \mathrm{H}^2(\mathrm{G}_S(K_{\text{cyc}}),M)^\vee \to \mathrm{H}^1(\mathrm{G}_S(K),(M^\vee)_{K_{\text{cyc}}}(1)) \to \bigoplus_{v \in S} \mathrm{H}^1(\mathrm{G}_{K_v},(M^\vee)_{K_{\text{cyc}}}(1))$$

$$\to \mathrm{H}^1(\mathrm{G}_S(K_{\text{cyc}}),M)^\vee \to \mathrm{H}^2(\mathrm{G}_S(K),(M^\vee)_{K_{\text{cyc}}}(1)) \to \bigoplus_{v \in S} \mathrm{H}^2(\mathrm{G}_{K_v},(M^\vee)_{K_{\text{cyc}}}(1))$$

$$\to \mathrm{H}^0(\mathrm{G}_S(K_{\text{cyc}}),M)^\vee \to 0.$$

We will derive yet another useful exact sequence. Recall that Q denotes the quotient field of Ω.

Lemma 3.2. *Assume that S is a finite set of primes of K containing the primes above p. For any $\mathrm{G}_S(K)$-representation M on a finite-dimensional vector space over $\mathbb{F}_p$, there is an exact sequence*

$$0 \to \mathrm{H}^0(\mathrm{G}_S(K_{\mathrm{cyc}}), M)$$

$$\to \mathrm{H}^1(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) \to Q \otimes_\Omega \mathrm{H}^1(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) \to \mathrm{H}^1(\mathrm{G}_S(K_{\mathrm{cyc}}), M)$$

$$\to \mathrm{H}^2(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) \to Q \otimes_\Omega \mathrm{H}^2(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) \to \mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), M) \to 0$$

Proof. Choose a topological generator γ of Γ and set $t = \gamma - 1$. Write K_n for the intermediate field of K_{cyc}/K of degree p^n over K. We then have

$$Q/\Omega = \varinjlim_{n \in \mathbb{N}} \frac{1}{t^{p^n}} \Omega/\Omega$$

Moreover, we have an isomorphism

$$\frac{1}{t^{p^n}} \Omega/\Omega \xrightarrow{\cong} \Omega/t^{p^n}\Omega = \mathbb{F}_p[\mathrm{G}(K_n/K)],$$

$$\frac{a}{t^{p^n}} + \Omega \mapsto a + t^{p^n}\Omega.$$

For any compact $\mathrm{G}_S(K)$-module N, write $C^\bullet(\mathrm{G}_S(K), N)$ for the continuous homogenous cochain complex. Clearly, $M_{K_{\mathrm{cyc}}}$ is finitely generated and free as Ω-module. Hence, there is an isomorphism

$$\frac{1}{t^{p^n}} \Omega/\Omega \otimes_\Omega^{\mathbb{L}} C^\bullet(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) \cong C^\bullet(\mathrm{G}_S(K_n), M)$$

in the derived category of complexes of Ω-modules [FK06, Prop. 1.6.5] and one checks that the map induced from the inclusion

$$\frac{1}{t^{p^n}} \Omega/\Omega \subset \frac{1}{t^{p^{n+1}}} \Omega/\Omega$$

agrees with the restriction map

$$C^\bullet(\mathrm{G}_S(K_n), M) \to C^\bullet(\mathrm{G}_S(K_{n+1}), M).$$

Therefore, we obtain an isomorphism

$$Q/\Omega \otimes_\Omega^{\mathbb{L}} C^\bullet(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) \cong C^\bullet(\mathrm{G}_S(K_{\mathrm{cyc}}), M)$$

in the derived category of complexes of Ω-modules. We take the derived tensor product over Ω of the exact sequence

$$0 \to \Omega \to Q \to Q/\Omega \to 0$$

with $C^\bullet(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}})$ and consider the associated long exact cohomology sequence of the resulting distinguished triangle. Since Q is a flat Ω-module, we conclude

$$Q \otimes_\Omega \mathrm{H}^n(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) = \mathrm{H}^n(Q \otimes_\Omega^{\mathbb{L}} C^\bullet(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}})).$$

Finally, we recall that

$$\mathrm{H}^0(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) = 0.$$

$\square$

4. Conjecture A and Equivalent Formulations

Let E be an elliptic curve over the number field K and S a finite set of primes of K containing the primes dividing p and the primes of bad reduction of E. Recall [CS05, Conjecture A] for the group $\mathrm{H}^2(\mathrm{G}_S(K), (\mathrm{T}_p E)_{K_{\mathrm{cyc}}})$:

Conjecture $A(K, E[p])$. *The group $\mathrm{H}^2(\mathrm{G}_S(K), (\mathrm{T}_p E)_{K_{\mathrm{cyc}}})$ is finitely generated as a $\mathbb{Z}_p$-module. Equivalently, the Pontryagin dual $Y(E[p^\infty]/K_{\mathrm{cyc}})$ of the fine Selmer group $R(E[p^\infty]/K_{\mathrm{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module.*

In fact, as Greenberg points out in [Gre11, Prop. 4.1.6], Conjecture $A(K, E[p])$ is also equivalent to the vanishing of $\mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), E[p])$. In this form, it admits the following sensible generalisation for any G_K-representation M on a finite-dimensional vector space over $\mathbb{F}_p$:

Conjecture $A(K, M)$. *Let S be any finite set of primes of K containing the primes above p and the primes where M is ramified. Then*

$$\mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), M) = 0.$$

We compile a list of equivalent reformulations.

Theorem 4.1. *Let K be a number field and M be a G_K-representation on a finite-dimensional vector space over $\mathbb{F}_p$. Assume that S is a finite set of primes of K containing the primes above p and the primes where M is ramified. The following statements are equivalent:*

(1) $\mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), M) = 0$.
(2) $\mathrm{H}^2(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}})$ *is finite.*
(3) $\mathrm{rk}_\Omega \mathrm{H}^1(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) = r_M$.
(4) $\mathrm{rk}_\Omega \mathrm{H}^1(\mathrm{G}_S(K_{\mathrm{cyc}}), M)^\vee = r_M$.
(5) $\mathrm{H}^1(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}^\vee(1)) \to \bigoplus_{v \in S} \mathrm{H}^1(\mathrm{G}_{K_v}, M_{K_{\mathrm{cyc}}}^\vee(1))$ *is injective.*
(6) *The fine Selmer group $R(M^\vee(1)/K_{\mathrm{cyc}})$ is finite.*
(7) *The inflation map $\mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), M) \to \mathrm{H}^2(\mathrm{G}_T(K_{\mathrm{cyc}}), M)$ is injective for every finite set of primes T containing S.*
(8) *The Gysin map $\mathrm{H}^1(\mathrm{G}_{K_{\mathrm{cyc}}}, M) \to \bigoplus_{v \notin S_{K_{\mathrm{cyc}}}} \mathrm{H}^0(\mathrm{G}_{k(v)}, M(-1))$ is surjective.*

Proof. The equivalence of (1), (2), (3), (4) is an immediate consequence of the sequence in Lemma 3.2 and the Euler characteristic formula

$$\mathrm{rk}_\Omega \mathrm{H}^1(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) - \mathrm{rk}_\Omega \mathrm{H}^2(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) = r_M.$$

The equivalence of (1) and (5) follows easily from the Poitou-Tate sequence (3.6). Similarly, we may consider the Poitou-Tate sequence (3.5), with M replaced by $M^\vee(1)$. Since the first two terms are finite groups, the equivalence of (2) and (6) is immediate.

The equivalence of (1), (7), and (8) can be seen as follows. Recall that

$$\mathrm{H}^k(\mathrm{G}_{K_{\mathrm{cyc}}}, M) = \varinjlim_T \mathrm{H}^k(\mathrm{G}_T(K_{\mathrm{cyc}}), M)$$

where T runs through all finite sets of primes of K containing S. Moreover,

$$\mathrm{H}^2(\mathrm{G}_{K_{\mathrm{cyc}}}, M) = 0$$

by [NSW00, Cor. 8.1.18]. Trivially, (1) implies (7). If we assume (7), then $\mathrm{H}^2(G_S(K_{\mathrm{cyc}}), M)$ injects into $\mathrm{H}^2(\mathrm{G}_{K_{\mathrm{cyc}}}, M)$ and is therefore the trivial group. So, (1) and (7) are equivalent.

Passing to the direct limit over T of the Gysin sequences (3.3) we obtain the exact sequence

$$0 \to \mathrm{H}^1(\mathrm{G}_S(K_{\mathrm{cyc}}), M) \to \mathrm{H}^1(\mathrm{G}_{K_{\mathrm{cyc}}}, M) \to \bigoplus_{v \notin S_{K_{\mathrm{cyc}}}} \mathrm{H}^0(\mathrm{G}_{k(v)}, M(-1))$$

$$\to \mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), M) \to 0$$

From this sequence, we can easily read off the equivalence of (1) and (8). $\qquad\square$

Remark 4.2. As $R(M^\vee(1)/K_{\mathrm{cyc}})$ does not depend on S, we also see that Conjecture $A(K, M)$ is independent of the particular choice of S.

Recall that M^{ss} denotes the semisimplification of M.

Lemma 4.3. *Let M be a representation of G_K on a finite-dimensional vector space over $\mathbb{F}_p$ and $N \subset M$ be a subrepresentation.*
  (1) *$A(K, M)$ implies $A(K, M/N)$.*
  (2) *The conjunction of $A(K, N)$ and $A(K, M/N)$ imply $A(K, M)$.*
  (3) *$A(K, M^{\mathrm{ss}})$ implies $A(K, M)$.*

Proof. The first two assertions follow easily from the long exact cohomology sequence associated to the short exact sequence

$$0 \to N \to M \to M/N \to 0$$

and the fact that the p-cohomological dimension of $\mathrm{G}_S(K_{\mathrm{cyc}})$ is at most 2. The third assertion follows from the second by induction over the filtration steps of a Jordan-Hölder series for M. $\qquad\square$

Corollary 4.4. *Assume that E/K has a p-torsion point defined over K. Then the conjunction of $A(K, \mu_p)$ and $A(K, \mathbb{F}_p)$ implies $A(K, E[p])$ and $A(K, E[p])$ implies $A(K, \mu_p)$. If in addition K contains μ_p, then $A(K, \mu_p)$, $A(K, \mathbb{F}_p)$, and $A(K, E[p])$ are equivalent.*

Proof. The p-torsion point generates a submodule T of $E[p]$ of dimension 1 over $\mathbb{F}_p$ with trivial G_K-action. Moreover, the Weil pairing on $E[p]$ implies that $E[p]/T \cong \mu_p$. Hence, we have an exact sequence of G_K-modules

$$0 \to \mathbb{F}_p \to E[p] \to \mu_p \to 0.$$

The claim now follows from Lemma 4.3. $\qquad\square$

Remark 4.5. We will explain in Proposition 4.10 the relation of $A(K, \mu_p)$ and $A(K, \mathbb{F}_p)$ with Iwasawa's conjecture on the vanishing of the μ-invariant.

We investigate how Conjecture $A(K, M)$ behaves under field extensions.

Lemma 4.6. *Let L/K be a finite field extension and M a G_K-representation on a finite-dimensional vector space over $\mathbb{F}_p$.*
  (1) *If Conjecture $A(L, M)$ is true, then so is $A(K, M)$.*
  (2) *If M is the induced representation of a G_L-representation N, then Conjecture $A(K, M)$ is true if and only if $A(L, N)$ is true.*
  (3) *If L/K is Galois with Galois group Δ, then $A(L, M)$ is true if and only if $A(K, \rho \otimes_{\mathbb{F}_p} M)$ is true for every finite-dimensional (every simple) $\mathbb{F}_p$-representation ρ of Δ.*
  (4) *If L/K is a Galois extension of order a power of p, then $A(L, M)$ is true if and only if $A(K, M)$ is true.*

Proof. Choose S large enough such that L/K and M are unramified outside S. Since the p-cohomological dimension of $\mathrm{G}_S(K_{\mathrm{cyc}})$ is less or equal to 2, the corestriction map

$$\mathrm{H}^2(\mathrm{G}_S(L_{\mathrm{cyc}}), M) \to \mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), M)$$

is surjective [NSW00, Prop. 3.3.11]. This proves (1).

Let n be the degree of $L \cap K_{\mathrm{cyc}}/K$ and assume that M is induced by the G_L-representation N. Let M' be the $\mathrm{G}_{K_{\mathrm{cyc}}}$-representation induced by the $\mathrm{G}_{L_{\mathrm{cyc}}}$-representation N. Then $M = (M')^n$ as $\mathrm{G}_{K_{\mathrm{cyc}}}$-representations. By Shapiro's Lemma we have

$$\mathrm{H}^2(\mathrm{G}_S(L_{\mathrm{cyc}}), N^n) = \mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), (M')^n)$$

Hence $A(K, M)$ is equivalent to $A(L, N^n)$, which is clearly equivalent to $A(L, N)$. This proves (2).

We prove (3). Let L/K be Galois with Galois group Δ and ρ a $\mathbb{F}_p$-representation of Δ of dimension k over $\mathbb{F}_p$. Then ρ is trivial as a $\mathrm{G}_S(L_{\mathrm{cyc}})$-representation. In particular,

$$\mathrm{H}^2(\mathrm{G}_S(L_{\mathrm{cyc}}), \rho \otimes_{\mathbb{F}_p} M) = \mathrm{H}^2(\mathrm{G}_S(L_{\mathrm{cyc}}), M)^k$$

and Conjecture $A(L, M)$ is true if and only if Conjecture $A(L, \rho \otimes_{\mathbb{F}_p} M)$ is true. Combining this with (1), we see that $A(L, M)$ implies $A(K, M \otimes_{\mathbb{F}_p} \rho)$.

Suppose that $A(K, M \otimes_{\mathbb{F}_p} \rho)$ is true for every simple $\mathbb{F}_p$-representation of Δ. The induced G_K-representation of the restriction of M to G_L is $\mathbb{F}_p[\Delta]^{\sharp} \otimes_{\mathbb{F}_p} M$. By induction on the length of a Jordan-Hölder series of $\mathbb{F}_p[\Delta]$ we see that $A(K, \mathbb{F}_p[\Delta]^{\sharp} \otimes_{\mathbb{F}_p} M)$ is true. Hence, $A(L, M)$ is also true by (2).

For the proof of (4) it remains to note that $\mathbb{F}_p$ is the only simple Δ-representation if the order of Δ is a power of p. $\qquad\qquad\square$

The following proposition is essentially well-known, see for example [Sch85, Lem. 8].

Proposition 4.7. *The following are equivalent:*

(1) *Conjecture $A(K, M)$ holds for all number fields K and all G_K-representations M.*

(2) *Conjecture $A(K, M)$ holds for a fixed field K and all simple G_K-representations M.*

(3) *Conjecture $A(L, M)$ holds for all finite extensions L/K for a fixed field K and a fixed G_K-representation M.*

(4) *The p-cohomological dimension of $\mathrm{G}_S(K_{\mathrm{cyc}})$ is 1 for some number field K and some finite set S of primes containing the primes above p.*

(5) *The p-cohomological dimension of $\mathrm{G}_S(K_{\mathrm{cyc}})$ is 1 for every number field K and every finite set S of primes containing the primes above p.*

Proof. The implications

$$(5) \Rightarrow (4) \Rightarrow (1) \Rightarrow (2)$$

are trivial.

Assume (2). Then Conjecture $A(K, M)$ holds for all G_K-representations M by Lemma 4.3.(3). Let L/K be a finite extension and M a fixed G_K-representation. Let N be the G_K-representation which is induced from the restriction of M to G_L, so that $A(K, N)$. Assertion (3) now follows from Lemma 4.6.(2).

Assume (3) for a fixed number field K' and a fixed $\mathrm{G}_{K'}$-representation M and let L be a finite extension of K' such that the restriction of M to L is trivial.

Then $A(L, M)$ implies $A(L, \mathbb{F}_p)$ by Lemma 4.3.(3). By Lemma 4.6.(1), this implies $A(L', \mathbb{F}_p)$ for all subfields L' of L. In particular, we have $A(K', \mathbb{F}_p)$ for every number field K'. Fix a number field K and let $\mathcal{L} \subset K_S$ be the field fixed by a p-Sylow subgroup of $\mathrm{G}_S(K_{\mathrm{cyc}})$. Then

$$\mathrm{H}^2(\mathrm{G}_S(\mathcal{L}), \mathbb{F}_p) = \varinjlim_{L/K} \mathrm{H}^2(\mathrm{G}_S(L_{\mathrm{cyc}}), \mathbb{F}_p) = 0,$$

with L/K running through the finite subextensions of $\mathcal{L}/K$. Since $\mathrm{G}_S(\mathcal{L})$ is a pro-p group of p-cohomological dimension at most 2, we conclude

$$\mathrm{cd}_p \mathrm{G}_S(\mathcal{L}) \leq 1.$$

Note that the p-cohomological dimensions of $\mathrm{G}_S(K_{\mathrm{cyc}})$ and any of its p-Sylow subgroups are the same. On the other hand, we cannot have $\mathrm{cd}_p \mathrm{G}_S(K_{\mathrm{cyc}}) = 0$, as we know that $\mathrm{cd}_p \mathrm{G}_S(K) = 2$ and that

$$\mathrm{cd}_p \mathrm{G}_S(K) \leq \mathrm{cd}_p \mathrm{G}_S(K_{\mathrm{cyc}}) + \mathrm{cd}_p \Gamma = \mathrm{cd}_p \mathrm{G}_S(K_{\mathrm{cyc}}) + 1$$

[NSW00, Prop. 10.11.3, Prop. 3.3.8]. We have thus proved the remaining implication $(3) \Rightarrow (5)$. $\qquad\square$

Conjecture A has been generalised in various other directions, for example by allowing more general coefficient rings [Lim13] or by considering Hida deformations and 'admissible' p-adic Lie extensions [JS11], [Jha12]. In the end, however, these generalisations turn out to be equivalent to Conjecture $A(K, M)$ for suitable M, as the following result shows.

Proposition 4.8. *Let R be a possibly non-commutative adic $\mathbb{Z}_p$-algebra, i. e. compact for the topology defined by the powers of the Jacobson radical $\mathfrak{J}_R \subset R$, and let M be a finitely generated, compact left R-module with a continuous, R-linear action of G_K which is unramified outside a finite set S of primes of K containing the primes above p. Assume that $\mathcal{L}/K$ is a Galois extension inside K_S/K with Galois group $\mathcal{G} = \mathrm{G}(\mathcal{L}/K)$ such that*

(1) $K_{\mathrm{cyc}} \subset \mathcal{L}$,
(2) $\mathcal{H} = \mathrm{G}(\mathcal{L}/K_{\mathrm{cyc}})$ *is a topologically finitely generated pro-p-group.*

Then $\mathrm{H}^2(\mathrm{G}_S(K), M_{\mathcal{L}})$ is finitely generated over the profinite group ring $R[[\mathcal{H}]]$ if and only if $A(K, M/\mathfrak{J}_R M)$ holds. If in addition, $R[[\mathcal{H}]]$ is Noetherian, then $Y(M^{\vee}(1)/\mathcal{L})$ is finitely generated over $R[[\mathcal{H}]]$ if and only if $A(K, M/\mathfrak{J}_R M)$ holds.

Proof. Under our assumptions on $\mathcal{H}$, both $\mathcal{G}$ and $\mathcal{H}$ are topologically finitely generated pro-p groups. Hence, both $R[[\mathcal{H}]]$ and $R[[\mathcal{G}]]$ are adic $\mathbb{Z}_p$-algebras [Wit14, Prop 3.2]. The Jacobson radical of $R[[\mathcal{H}]]$ is given by

$$\mathfrak{J}_{R[[\mathcal{H}]]} = \ker\left(R[[\mathcal{H}]] \to R/\mathfrak{J}_R\right).$$

Since

$$\mathfrak{J}_{R[[\mathcal{H}]]}/\mathfrak{J}^2_{R[[\mathcal{H}]]} \subset R[[\mathcal{H}]]/\mathfrak{J}^2_{R[[\mathcal{H}]]}$$

is finite, the Jacobson radical is finitely generated as a left or right $R[[\mathcal{H}]]$-module by the topological Nakayama lemma. Hence,

$$\mathfrak{J}_{R[[\mathcal{H}]]} R[[\mathcal{G}]] = \ker\left(R[[\mathcal{G}]] \to R/\mathfrak{J}_R[[\Gamma]]\right)$$

is also finitely generated as a left or right $R[[\mathcal{G}]]$-module. In particular,

$$R/\mathfrak{J}_R[[\Gamma]] = R/\mathfrak{J}_R \otimes_{R[[\mathcal{H}]]} R[[\mathcal{G}]]$$

is finitely presented as a right $R[[\mathcal{G}]]$-module. Since $\mathrm{H}^2(\mathrm{G}_S(K), -)$ is a right exact functor that commutes with finite products, we conclude from the choice of a finite free presentation that

$$\begin{aligned} R/\mathfrak{J}_R \otimes_{R[[\mathcal{H}]]} \mathrm{H}^2(\mathrm{G}_S(K), M_{\mathcal{L}}) &= R/\mathfrak{J}_R[[\Gamma]] \otimes_{R[[\mathcal{G}]]} \mathrm{H}^2(\mathrm{G}_S(K), M_{\mathcal{L}}) \\ &= \mathrm{H}^2(\mathrm{G}_S(K), R/\mathfrak{J}_R[[\Gamma]] \otimes_{R[[\mathcal{G}]]} \otimes_{R[[\mathcal{G}]]} M_{\mathcal{L}}) \\ &= \mathrm{H}^2(\mathrm{G}_S(K), (M/\mathfrak{J}_R M)_{\mathcal{K}_{\mathrm{cyc}}}) \end{aligned}$$

The topological Nakayama lemma then implies that the compact $R[[\mathcal{H}]]$-module $\mathrm{H}^2(\mathrm{G}_S(K), M_{\mathcal{L}})$ is finitely generated precisely if $\mathrm{H}^2(\mathrm{G}_S(K), (M/\mathfrak{J}_R M)_{\mathcal{K}_{\mathrm{cyc}}})$ is finite. The latter is equivalent to Conjecture $A(K, M/\mathfrak{J}_R M)$ by Theorem 4.1.

Now assume that $R[[\mathcal{H}]]$ is Noetherian and note that

$$Y(M^\vee(1)/\mathcal{L}) = \ker\left(\mathrm{H}^2(\mathrm{G}_S(K), M_{\mathcal{L}}) \to \bigoplus_{v \in S} \mathrm{H}^2(\mathrm{G}_{K_v}, M_{\mathcal{L}})\right).$$

In particular, if $\mathrm{H}^2(\mathrm{G}_S(K), M_{\mathcal{L}})$ is finitely generated over $R[[\mathcal{H}]]$, then so is its submodule $Y(M^\vee(1)/\mathcal{L})$. Conversely, assume $Y(M^\vee(1)/\mathcal{L})$ is finitely generated over $R[[\mathcal{H}]]$. In order to imply that $\mathrm{H}^2(\mathrm{G}_S(K), M_{\mathcal{L}})$ is finitely generated over $R[[\mathcal{H}]]$, it is then sufficient to prove that $\mathrm{H}^2(\mathrm{G}_{K_v}, M_{\mathcal{L}})$ is finitely generated over $R[[\mathcal{H}]]$ for each prime v of K.

By the same argument as before, this will follow if we show that the group $\mathrm{H}^2(\mathrm{G}_{K_v}, (M/\mathfrak{J}_R M)_{K_{\mathrm{cyc}}})$ is finite. But this is true, since by local duality,

$$\mathrm{H}^2(\mathrm{G}_{K_v}, (M/\mathfrak{J}_R M)_{K_{\mathrm{cyc}}})^\vee = \bigoplus_{w|v} \mathrm{H}^0(\mathrm{G}_{(K_{\mathrm{cyc}})_w}, M/\mathfrak{J}_R M^\vee(1))$$

and since in K_{cyc}/K, every prime splits into finitely many primes. $\qquad\square$

Remark 4.9.
  (1) The ring $R[[\mathcal{H}]]$ is Noetherian if R is a commutative adic $\mathbb{Z}_p$-algebra and $\mathcal{H}$ is a compact p-adic Lie group [Wit13, Cor. 3.4].
  (2) In general, $Y(M^\vee(1)/\mathcal{L})$ is expected to be rather small. If $\mathcal{G}$ is a compact p-adic Lie group of dimension greater than 1, then it is conjectured that $Y(E[p^\infty]/\mathcal{L})$ is in fact a finitely generated torsion module over $\mathbb{Z}_p[[\mathcal{H}]]$ [CS05, Conjecture B].
  (3) One may also conjecture that $\mathrm{H}^2(\mathrm{G}_S(\mathcal{L}), M) = 0$ for a G_K-representation M on a finite-dimensional vector space over $\mathbb{F}_p$ and with $\mathcal{L}$ as in the above proposition. This is clearly implied by Conjecture $A(K, M)$, but it seems to be considerably weaker than $A(K, M)$ if $\mathcal{L}/K_{\mathrm{cyc}}$ is of infinite degree.

Conjecture $A(K, M)$ is closely related to Iwasawa's classical conjecture on the vanishing of the μ-invariant for the cyclotomic extension of any number field K. The precise relationship is as follows: We consider the Iwasawa modules

$$\begin{aligned} X_{\mathrm{nr}}(K) &= \varprojlim_{K \subset L \subset K_{\mathrm{cyc}}} \mathrm{Cl}(L) \otimes_{\mathbb{Z}} \mathbb{Z}_p, \\ X_{\mathrm{cs}}(K) &= \varprojlim_{K \subset L \subset K_{\mathrm{cyc}}} \mathrm{Cl}_p(L) \otimes_{\mathbb{Z}} \mathbb{Z}_p, \\ X_S(K) &= \mathrm{G}(K_S(p)/K)^{\mathrm{ab}}, \end{aligned}$$

where $\mathrm{Cl}_p(L)$ is the Picard group of the ring of integers $\mathcal{O}_L[\frac{1}{p}]$ of L with p inverted and $K_S(p)$ is the maximal pro-p-Galois extension of K unramified outside the finite set S of primes containing the primes above p. It is known that $X_{\mathrm{nr}}(K)$, $X_{\mathrm{cs}}(K)$ and $X_S(K)$ are finitely generated Λ-modules. While $X_{\mathrm{nr}}(K)$ and $X_{\mathrm{cs}}(K)$ are Λ-torsion, the Λ-rank of $X_S(K)$ is given by the number r_2 of complex places of K [NSW00, Prop. 11.1.4, Prop. 11.3.1, Cor. 11.3.15]. For any finitely generated Λ-module M, we write $\mu(M)$ for the μ-invariant of M. We then have

$$\mu(X_{\mathrm{nr}}(K)) = \mu(X_{\mathrm{cs}}(K))$$

and if the p-th roots of unity μ_p are contained in K, we also have

$$\mu(X_S(K)) = \mu(X_{\mathrm{nr}}(K))$$

[NSW00, Cor. 11.3.16, 11.3.17]. Iwasawa's classical conjecture on the μ-invariant amounts to

$$\mu(X_{\mathrm{nr}}(K)) = 0$$

for all number fields K.

Proposition 4.10. *Let K be a number field.*
 (1) *Conjecture $A(K, \mu_p)$ holds if and only if $\mu(X_{\mathrm{nr}}(K)) = 0$.*
 (2) *Conjecture $A(K, \mathbb{F}_p)$ holds if and only if $\mu(X_S(K)) = 0$ for some finite S containing the primes above p.*

In particular, Iwasawa's conjecture on the μ-invariant holds for all number fields K precisely if Conjecture $A(K, M)$ holds for all K and M.

Proof. We prove (1). Let Σ be the set of primes of K above p. Then class field theory in combination with local duality and the Poitou-Tate sequence implies

$$\mathrm{Cl}_p(K) \otimes_{\mathbb{Z}} \mathbb{Z}/(p^n) = \mathrm{coker}\left(\bigoplus_{v \in \Sigma} \mathrm{G}_{K_v}^{\mathrm{ab}} \otimes_{\mathbb{Z}} \mathbb{Z}/(p^n) \to \mathrm{G}_\Sigma(K)^{\mathrm{ab}} \otimes_{\mathbb{Z}} \mathbb{Z}/(p^n)\right)$$

$$= \mathrm{coker}\left(\bigoplus_{v \in \Sigma} \mathrm{H}^1(\mathrm{G}_{K_v}, \mu_{p^n}) \to \mathrm{H}^1(\mathrm{G}_S(K), \mathbb{Z}/(p^n))^\vee\right)$$

$$= \ker\left(\mathrm{H}^2(\mathrm{G}_\Sigma(K), \mu_{p^n}) \to \bigoplus_{v \in \Sigma} \mathrm{H}^2(\mathrm{G}_{K_v}, \mu_{p^n})\right).$$

Passing to the inverse limit over $n \in N$ and all finite subextensions of K_{cyc}/K we conclude

$$X_{\mathrm{cs}}(K) = Y((\mathbb{Q}_p/\mathbb{Z}_p)/K_{\mathrm{cyc}}).$$

Since $X_{\mathrm{cs}}(K)$ is Λ-torsion, we have $\mu(X_{\mathrm{nr}}(K)) = \mu(X_{\mathrm{cs}}(K)) = 0$ precisely if $X_{\mathrm{cs}}(K)$ is finitely generated over $\mathbb{Z}_p$. The equivalence of $A(K, \mu_p)$ with $\mu(X_{\mathrm{nr}}(K)) = 0$ then follows from Proposition 4.8 with $R = \mathbb{Z}_p$, $\mathcal{L} = K_{\mathrm{cyc}}$ and $M = \mathbb{Z}_p(1)$.

For (2), we use that $\mu(X_S(K)) = 0$ is equivalent to the maximal pro-p-quotient $\mathrm{G}_S(K_{\mathrm{cyc}})(p)$ of $\mathrm{G}_S(K_{\mathrm{cyc}})$ being a free pro-p-group, which is in turn equivalent to

$$\mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}})(p), \mathbb{F}_p) = 0.$$

Moreover,

$$\mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}})(p), \mathbb{F}_p) = \mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), \mathbb{F}_p)$$

[NSW00, Thm. 11.3.7, Prop. 3.9.5, Cor. 10.4.8]. $\qquad\square$

Remark 4.11. Assume that T is a representation of G_K on a finitely generated free $\mathbb{Z}_p$-module which is unramified outside a finite set of primes S. The weak Leopoldt conjecture for T over K_{cyc} states that

$$\mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), T^\vee(1)) = 0,$$

see [Gre97] and the references given therein. We note that this conjecture is implied by $A(K, (T/pT)^\vee(1))$. Indeed, assuming $A(K, (T/pT)^\vee(1))$, the long exact cohomology sequence for the short exact sequence

$$0 \to (T/pT)^\vee(1) \to T^\vee(1) \xrightarrow{\cdot p} T^\vee(1) \to 0$$

shows that the group $\mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), T^\vee(1))$ is uniquely p-divisible and p-torsion, and hence trivial.

To view Conjecture $A(K, M)$ in this framework, see also [Suj10].

5. The Isogeny Invariance Conjecture

In [CS05], the authors express their belief that Conjecture $A(K, E[p])$ is isogeny invariant in the following sense:

Conjecture $I(K, E)$. *Let E be a fixed elliptic curve over K. For every nontrivial isogeny $f \colon E \to E'$ to an elliptic curve E', with both f and E' defined over K, $A(K, E[p])$ holds if and only if $A(K, E'[p])$ holds.*

In this section, we will discuss this conjecture. Let us first recall the following fact on isogenies.

Proposition 5.1. *Let E/K and E'/K be elliptic curves which are isogenous over K. Then precisely one of the following holds true:*

(a) *E has no G_K-submodule of order p, $E[p]$ is a simple G_K-module and there exists a G_K-isomorphism $E'[p] \cong E[p]$.*

(b) *E has a G_K-submodule $T \cong T^\vee(1)$ of order p and both $E[p]$ and $E'[p]$ are extensions of T by T.*

(c) *E has complex multiplication over K by an imaginary quadratic extension of $\mathbb{Q}$ in which p splits completely and $\mathrm{T}_p E \cong \chi \oplus \chi^{-1}(1) \cong \mathrm{T}_p E'$ for some character $\chi \colon \mathrm{G}_K \to \mathbb{Z}_p^\times$ such that the residual representation of $\chi^{-2}(1)$ is nontrivial.*

(d) *E has a G_K-submodule $T \not\cong T^\vee(1)$ of order p and there exists an elliptic curve E_0/K isogenous to E over K with a unique finite maximal cyclic G_K-submodule $C \subset E_0$ of p-power order. Set $E_1 = E_0/C$. Then there exist non-split exact sequences*

$$\begin{array}{ccccccc} 0 & \to & T & \to & E_0[p] & \to & T^\vee(1) & \to & 0, \\ 0 & \to & T^\vee(1) & \to & E_1[p] & \to & T & \to & 0. \end{array}$$

Moreover, $E'[p]$ is either isomorphic to $E_0[p]$, to $E_1[p] \not\cong E_0[p]$, or to $T \oplus T^\vee(1)$. The last possibility can occur if and only if the order of C is greater than p.

Proof. Since E and E' are isogenous over K, the group of continuous G_K-homomorphisms $\mathrm{Hom}_{\mathrm{G}_K}(\mathrm{T}_p E, \mathrm{T}_p E')$ is nontrivial [Sil09, Thm. 7.4]. Moreover, the $\mathbb{Z}_p$-module $\mathrm{Hom}_{\mathrm{G}_K}(\mathrm{T}_p E, \mathrm{T}_p E')$ is a finitely generated and free. The long exact $\mathrm{Ext}_{\mathrm{G}_K}$-sequence for the short exact sequence

$$0 \to \mathrm{T}_p E' \xrightarrow{\cdot p} \mathrm{T}_p E' \to E'[p] \to 0$$

gives us a left exact sequence

$$0 \to \mathrm{Hom}_{\mathrm{G}_K}(\mathrm{T}_p\,E, \mathrm{T}_p\,E') \xrightarrow{\cdot p} \mathrm{Hom}_{\mathrm{G}_K}(\mathrm{T}_p\,E, \mathrm{T}_p\,E') \to \mathrm{Hom}_{\mathrm{G}_K}(\mathrm{T}_p\,E, E'[p]).$$

The corresponding short exact sequence for $\mathrm{T}_p\,E$ gives us an isomorphism

$$\mathrm{Hom}_{\mathrm{G}_K}(\mathrm{T}_p\,E, E'[p]) \cong \mathrm{Hom}_{\mathrm{G}_K}(E[p], E'[p]).$$

In particular, $\mathrm{Hom}_{\mathrm{G}_K}(E[p], E'[p])$ is nontrivial. Since $E[p]$ and $E'[p]$ are groups of the same order p^2, there exists either an G_K-equivariant isomorphism $E[p] \cong E'[p]$ or a G_K-equivariant homomorphism

$$f \colon E[p] \to E'[p]$$

with kernel $\ker(f)$ of order p. In the latter case, the nondegenerate, alternating Weil pairings on $E[p]$ and $E'[p]$ imply the existence of a G_K-equivariant homomorphism $f^\vee \colon E'[p] \to E[p]$ with kernel isomorphic to $\ker(f)^\vee(1)$. Moreover, we have

$$\ker(f^\vee) \cong \mathrm{im}(f) \cong \ker(f)^\vee(1),$$
$$\ker(f) \cong \mathrm{im}(f^\vee) \cong \ker(f^\vee)^\vee(1).$$

In any case, we conclude that $E[p]^{\mathrm{ss}} = E'[p]^{\mathrm{ss}}$.

If E has no finite G_K-submodule of order p, $E[p]$ must be a simple G_K module. Hence, an isogeny f as above cannot exist. In particular, $E[p] \cong E'[p]$.

Henceforth, we may assume that $E[p]$ has a finite submodule T of order p. If $T \cong T^\vee(1)$, then $E[p]^{\mathrm{ss}} = T^2$. In particular, both $E[p]$ and $E'[p]$ are extensions of T by itself. So, we may assume that $T \not\cong T^\vee(1)$.

Assume that $\mathrm{T}_p\,E$ contains a G_K-stable submodule X of rank 1 over $\mathbb{Z}_p$. Then $V = \mathbb{Q}_p \otimes_{\mathbb{Z}} \mathbb{Z}_p$ splits into two one-dimensional representations and necessarily, the image of G_K in the automorphism group of $\mathrm{T}_p\,E$ is abelian. Then E must have complex multiplication over K by an order $\mathcal{O}$ in an imaginary quadratic number field L. Indeed, the $\mathbb{Z}_p$-module $\mathrm{End}_{\mathrm{G}_K}(\mathrm{T}_p\,E)$ of G_K-equivariant endomorphisms of $\mathrm{T}_p\,E$, i.e. those endomorphisms that commute with elements in the image of G_K, is strictly greater than the centre of $\mathrm{End}_{\mathbb{Z}_p}(\mathrm{T}_p\,E)$, since it contains the centre and the image of G_K. (If the image of G_K were contained in the centre, which is not possible, then $\mathrm{End}_{\mathrm{G}_K}(\mathrm{T}_p\,E) = \mathrm{End}_{\mathbb{Z}_p}(\mathrm{T}_p\,E)$.) By a celebrated theorem of Faltings [Sil09, Thm. 7.7], this implies that the endomorphism ring of E must be larger than $\mathbb{Z}$, as well. In particular, V is a module of rank 1 over $\mathbb{Q}_p \otimes_{\mathbb{Q}} L$ and $\mathrm{G}(\mathcal{L}/K)$ may be identified with an open subgroup of $(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O})^\times$. But then, X can only exist if $\mathbb{Q}_p \otimes_{\mathbb{Q}} L$ is not a field. So, p must split in L. In this case, $\mathrm{T}_p\,E \cong \chi \oplus \chi^{-1}(1)$ for a 1-dimensional representation χ. The residual representation of $\chi^{-2}(1)$ cannot be trivial by our assumption that $T \not\cong T^\vee(1)$. Moreover, the same decomposition also holds for $\mathrm{T}_p\,E'$.

Henceforth, we may assume that $\mathrm{T}_p\,E$ contains no G_K-stable submodule of rank 1 over $\mathbb{Z}_p$. In particular, maximal cyclic G_K-submodules of order a power of p exist in E and all E' isogenous to E. If E contains a further submodule T' of order p besides T, then necessarily $T' \cong T^\vee(1)$ and there exists a maximal cyclic submodule $C' \subset E$ of p-power order that contains T'. Consider the isogeny $\pi \colon E \to E/C' = E_0$. The preimage of any submodule T_0 of E_0 of order p under π cannot be cyclic because of the maximality of C'. Hence,

$$\pi^{-1}(T_0) = E[p] + C'$$

and T_0 is the unique submodule of order p. Since π restricted to T is injective, we conclude that $T_0 = \pi(T)$. Hence, $E_0[p]$ is a nontrivial extension of $T^\vee(1)$ by T. If T is the only submodule of E of order p, we may simply set $E_0 = E$.

There exists a unique maximal cyclic G_K-submodule C of E_0 of order a power of p. Indeed, if $D \neq C$ is a second submodule with the same property, then $C + D$ cannot be cyclic. Hence, $C + D$ must contain $E_0[p]$ and $(C + D)^{\mathrm{ss}}$ contains $T^\vee(1)$ as a submodule. But both C and D are cyclic and contain T as a submodule. Hence, C^{ss}, D^{ss} and $(C + D)^{\mathrm{ss}}$ are powers of T. This contradicts our assumption that $T \neq T^\vee(1)$.

Consider $E_1 = E_0/C$. Arguing as before, we see that E_1 contains a unique submodule T_1 of order p. Let p^n be the order of C. The composition of the maps

$$E_0[p] \subset E_0[p^n] \twoheadrightarrow E_0[p^n]/C \subset E_1[p^n]$$

shows that $T_1 = E_0[p]/T_0 \cong T^\vee(1)$. Hence, $E_1[p]$ is a nontrivial extension of T by $T^\vee(1)$. Since T is a submodule of $E_0[p]$, but not of $E_1[p]$, we have $E_0[p] \not\cong E_1[p]$.

Assume now that $E'[p]$ is not isomorphic to $E_0[p]$ or to $E_1[p]$. Because the group $\mathrm{Hom}_{G_K}(E'[p], E_0[p])$ is nontrivial, we find a G_K-equivariant homomorphism

$$f \colon E'[p] \to E_0[p]$$

with kernel isomorphic to $T^\vee(1)$. Replacing E_0 by E_1, we see that T is also a submodule of $E'[p]$. Hence, $E'[p] \cong T \oplus T^\vee(1)$.

If the order of C is larger than p, then it is easy to check that $(E_0/T)[p] \cong T \oplus T^\vee(1)$. Conversely, assume that E' has two distinct submodules

$$T_1 \cong T, \qquad T_2 \cong T^\vee(1)$$

of order p. Note that

$$\mathrm{Hom}_{G_K}(E_0[p], E'[p]) = \mathrm{Hom}_{G_K}(T^\vee(1), T^\vee(1)) = \mathbb{F}_p$$

such that every element $E_0[p] \to E'[p]$ may be lifted to an isogeny $E_0 \to E'$. In particular, there exists an isogeny $\phi \colon E_0 \to E'$ whose restriction to $E_0[p]$ has kernel T_0. This implies that the p-primary component of $\ker \phi$ is cyclic and hence, it is contained in C. The p-primary component of $\phi^{-1}(T_1)$ is then also cyclic and contained in C. We conclude that C must have an order of at least p^2. $\square$

Corollary 5.2. *Let E/K be a fixed elliptic curve. If E satisfies (a), (b), or (c) of Proposition 5.1, then Conjecture $I(K, E)$ holds.*

If E satisfies (d), then the following are equivalent:

(1) *Conjecture $I(K, E)$ holds.*
(2) *$A(K, E_0[p])$ holds if and only if $A(K, E_1[p])$ holds.*
(3) *Let $T \subset E_0[p]$ be the submodule of order p. Then $A(K, E_0[p])$ implies $A(K, T)$ and $A(K, E_1[p])$ implies $A(K, T^\vee(1))$.*

Proof. If E satisfies (a), then $I(K, E)$ is trivial, since $E[p] \cong E'[p]$ for every E' isogenous to E. If E satisfies (b), then for every E' isogenous to E, $A(K, E')$ holds if and only if $A(K, T)$ holds. If E satisfies (c), then $E'[p]$ is semisimple for all E' and $A(K, E')$ holds if and only if $A(K, T)$ and $A(K, T^\vee(1))$ holds. In both cases, either $A(K, E')$ holds for all E' or for none.

Assume E satisfies (d) and that $C \subset E_0$ is the unique maximal cyclic G_K-submodule C of p-power order. Clearly, (1) implies (2). Assume (2) and that $A(K, E_0[p])$ or $A(K, E_1[p])$ holds. Then the respective other holds as well. Since

T is a quotient of $E_1[p]$ and $T^\vee(1)$ a quotient of $E_0[p]$, we conclude from Lemma 4.3 that $A(K,T)$ and $A(K,E_1[p])$ hold. Hence, (3) is true. Finally, assume (3) and that $A(K,E'[p])$ holds for some E' isogenous to E. If $E'[p]$ is semisimple, then both T and $T^\vee(1)$ are quotients of $E'[p]$. Otherwise, $E'[p]$ is either isomorphic to $E_0[p]$ or to $E_1[p]$. In any case, we may deduce that $A(K,T)$ and $A(K,T^\vee(1))$ hold, either from (3) or from Lemma 4.3. Lemma 4.3 then also implies that $A(K,E')$ holds for every E' isogenous to E. Hence, Conjecture $I(K,E)$ is true.   □

Remark 5.3. In the case (d) of the above proposition, note that both $E_0[p]$ and $E_1[p]$ are quotients of the G_K-representation $E[p^{n+1}]$ with p^n denoting the order of the maximal cyclic G_K-submodule C of p-power order of E_0. Let $K(E[p^{n+1}])$ denote the minimal extension trivialising the Galois representation $E[p^{n+1}]$. Then both $E_0[p]$ and $E_1[p]$ may be viewed as specific extensions of one dimensional representations of $G(K(E[p^{n+1}])/K)$ over $\mathbb{F}_p$. In particular, the isogeny conjecture in this case boils down to understanding the relationship between these two extensions.

Let us now discuss Conjecture $I(K,E)$ for CM elliptic curves. Let $\mathcal{O}$ be an order in an imaginary quadratic field L. Then $\mathcal{O}$ is of the form

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_L,$$

with $f \in \mathbb{N}$ the conductor of $\mathcal{O}$ and $\mathcal{O}_L$ the maximal order of L. Recall that the discriminant of $\mathcal{O}$ is given by

$$d_\mathcal{O} = f^2 d_L,$$

with d_L denoting the discriminant of L. Recall that an elliptic curve E/K is a CM elliptic curve if the endomorphism ring of E over the algebraic closure $\overline{K}$ of K is strictly larger than $\mathbb{Z}$. Let us first assume that E/K is an elliptic curve which has complex multiplication by $\mathcal{O}$ over K so that all endomorphisms over $\overline{K}$ are already defined over K. In this case, $E[p]$ is a free $\mathcal{O}/p\mathcal{O}$-module of rank 1 [Par89, Lem. 1] and the action of G_K on $E[p]$ is given by a character

$$\psi\colon G_K \to (\mathcal{O}/p\mathcal{O})^\times.$$

Corollary 5.4. *Assume that E/K has complex multiplication by $\mathcal{O}$ over K. Then Conjecture $I(K,E)$ holds.*

Proof. Write g for the image of G_K in the automorphism group of $E[p]$. By Corollary 5.2 we may assume that $E[p]$ has a non-trivial g-subrepresentation T of rank 1 over $\mathbb{F}_p$ such that $E[p]$ is a non-trivial extension of $T^\vee(1)$ by T and such that $T \not\cong T^\vee(1)$. Consider the g-representation

$$A = T \otimes_{\mathbb{F}_p} T(-1)$$

of rank 1 over $\mathbb{F}_p$. Then $E[p]$ represents a nontrivial class in

$$\mathrm{Ext}^1_g(T^\vee(1), T) = \mathrm{H}^1(g, A).$$

If E has complex multiplication over K, then g is abelian. Let $h \subset g$ be the maximal subgroup of order prime to p. By our assumption that $T \not\cong T^\vee(1)$, h acts non-trivially on A, so that $A^h = 0$. The Hochschild-Serre spectral sequence then implies

$$\mathrm{H}^1(g, A) = \mathrm{H}^0(g/h, \mathrm{H}^1(h, A)) = 0$$

in contradiction to our assumption that the class of $E[p]$ is nontrivial.   □

Let us now consider the case when E/K does not have complex multiplication over K, but does so over the larger field KL.

Lemma 5.5. *Let E/K be an elliptic curve such that*

  (i) *E has complex multiplication by $\mathcal{O}$ over $KL \ne K$,*
  (ii) *there exists a G_K-submodule $T \subset E[p]$ of rank 1 over $\mathbb{F}_p$,*
  (iii) *$T \not\cong T^\vee(1)$ as G_K-modules,*
  (iv) *$E[p]$ is a non-trivial extension of $T^\vee(1)$ by T.*

Then p divides the discriminant $d_{\mathcal{O}}$ and $T \cong T^\vee(1)$ as G_{LK}-modules. If $p \equiv 3$ mod 4 and $\sqrt{-p} \in K$, then such a curve cannot exist.

Proof. We write g' for the image of G_K in the automorphism group of $E[p]$ and set $A = T \otimes_{\mathbb{F}_p} T(-1)$ as before. Then g' is an extension of the group

$$z = \mathrm{G}(KL/K)$$

of order 2 by an abelian group g. Since we assume $p \ne 2$, the restriction map

$$\mathrm{H}^1(g', A) \to \mathrm{H}^1(g, A)$$

is injective. Since $E[p]$ represents a non-trivial class in $\mathrm{H}^1(g', A)$, we conclude that $\mathrm{H}^1(g, A) \ne 0$. By the same argument as in Corollary 5.4, this can only be true if the action of g on A is trivial. In particular, T and $T^\vee(1)$ are isomorphic as G_{LK}-modules. Moreover, g must contain a non-trivial subgroup of order p. This can only happen if p divides the discriminant $d_{\mathcal{O}}$. Indeed, if this were not the case, then the primes of $\mathcal{O}$ above p are regular in the sense of [Neu99, § 12] and unramified in $L/\mathbb{Q}$. If p is inert in L, then $E[p]$ is a vector space of dimension 1 over the residue field k of p in L with an faithful action of g' by k-linear automorphisms. In particular, the order of g' is prime to p. If p splits in L, then the restriction of $E[p]$ to G_{LK} is split. In both cases, $E[p]$ represents the trivial class in $\mathrm{H}^1(g', A)$, in contradiction to our assumptions.

Now, assume that $p \equiv 3$ mod 4 and that $\sqrt{-p} \in K$. Let $\sigma \in g$ be an element which is not contained in g'. Since $\frac{p-1}{2}$ is an odd integer, the element $\sigma' = \sigma^{\frac{p-1}{2}}$ is also not contained in g'. However, since $\sqrt{-p} \in K$, the element σ' fixes $K(\mu_p)$. Moreover, σ' acts trivially on $T \otimes_{\mathbb{F}_p} T$. Hence, σ' acts trivially on A, so that A is in fact a trivial g'-module, in contradiction to assumption (iii). $\square$

Corollary 5.6. *Assume that $p \equiv 3$ mod 4 and that $\sqrt{-p} \in K$. Then $I(K, E)$ holds for all CM elliptic curves E/K.*

Proof. Let E/K be any CM elliptic curve. By Corollary 5.4 we may assume that E does not have CM over K. By Lemma 5.5, case (d) of Proposition 5.1 can never occur. Hence, $I(K, E)$ holds by Corollary 5.2. $\square$

6. Closing Remarks

In the light of (3) of Corollary 5.2, we may formulate the following conjecture for arbitrary G_K-representations M on finite-dimensional vector spaces over $\mathbb{F}_p$.

Conjecture *$Sub(K, M)$.* *For every subrepresentation $N \subset M$, $A(K, M)$ implies $A(K, N)$.*

In particular, for an elliptic curve E/K, $I(K, E)$ is equivalent to the conjunction of $Sub(K, E'[p])$ for every E' which is K-isogenous to E. Moreover, note that

$Sub(K, M)$ holds if every subrepresentation of M also appears as a quotient representation of M. In particular, $Sub(K, M)$ holds if the semisimplification of M is a power of a simple G_K-module. This can always be achieved by passing to a finite extension K' of K. We also note the following.

Lemma 6.1. *Let L/K be a Galois extension of order a power of p and M be a G_K-representations on a finite-dimensional vector space over $\mathbb{F}_p$. Then $Sub(L, M)$ implies $Sub(K, M)$.*

Proof. This is an immediate consequence of Lemma 4.6.(4). $\qquad\square$

However, beware that in general, $Sub(K, M)$ does not imply $Sub(L, M)$, since the set of G_L-subrepresentations of M might be strictly larger than the set of G_K-subrepresentations.

Corollary 6.2. *Let M be a G_K-representations on a finite-dimensional vector space over $\mathbb{F}_p$ unramified outside of S. Then there exists a finite subextension K'/K of K_S/K of degree prime to p such that $Sub(K', M)$ holds. Likewise, if E/K is an elliptic curve with good reduction outside of S, then there exists a finite subextension K'/K of K_S/K of degree prime to p such that $I(K', E)$ holds.*

Proof. Choose L/K to be a Galois subextension of K_S/K trivialising the G_K-representations M and $E[p]$, respectively. In particular, E/L satisfies case (b) of Proposition 5.1, so that $I(L, E)$ holds by Corollary 5.2. Conjecture $Sub(L, M)$ is obviously true.

Now choose $K' \subset L$ to be the fixed field of a p-Sylow subgroup of $G(L/K)$. Then $Sub(K', M)$ and $I(K', E)$ hold by Lemma 6.1. $\qquad\square$

If L/K is Galois of order prime to p, it is in general not possible to infer $Sub(K, M)$ from $Sub(L, M)$. To overcome this deficiency, it might be worthwhile to study the following strengthening of $Sub(K, M)$. As before, we let S denote a finite set of primes of K containing the primes above p and those primes where M is ramified.

Conjecture $C(K, M)$**.** *For every G_K-subrepresentation $N \subset M$,*

$$Q \otimes_\Omega \mathrm{H}^2(G_S(K), N_{K_{\mathrm{cyc}}}) \to Q \otimes_\Omega \mathrm{H}^2(G_S(K), M_{K_{\mathrm{cyc}}})$$

is injective.

Lemma 6.3. *Let M be a G_K-representation which is unramified outside of S. Then the following are equivalent:*
  (1) *Conjecture $C(K, M)$ holds,*
  (2) *for every G_K-subrepresentation $N \subset M$,*

$$\ker(\mathrm{H}^2(G_S(K_{\mathrm{cyc}}), N) \to \mathrm{H}^2(G_S(K_{\mathrm{cyc}}), M))$$

   is finite,
  (3) *for every G_K-subrepresentation $N \subset M$,*

$$\ker(\mathrm{H}^2(G_S(K), N_{K_{\mathrm{cyc}}}) \to \mathrm{H}^2(G_S(K), M_{K_{\mathrm{cyc}}}))$$

   is finite,
  (4) *for every G_K-subrepresentation $N \subset M$,*

$$Q \otimes_\Omega \mathrm{H}^1(G_S(K), M_{K_{\mathrm{cyc}}}) \to Q \otimes_\Omega \mathrm{H}^1(G_S(K), (M/N)_{K_{\mathrm{cyc}}})$$

   is surjective,

(5) *for every* G_K-*subrepresentation* $N \subset M$,

$$\mathrm{coker}(\mathrm{H}^1(\mathrm{G}_S(K_{\mathrm{cyc}}), M) \to \mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), M/N))$$

   is finite,

(6) *for every* G_K-*subrepresentation* $N \subset M$,

$$\mathrm{coker}(\mathrm{H}^1(\mathrm{G}_S(K), M_{K_{\mathrm{cyc}}}) \to \mathrm{H}^1(\mathrm{G}_S(K), (M/N)_{K_{\mathrm{cyc}}}))$$

   is finite,

(7) *Conjecture* $C(K, M^\vee(1))$ *holds.*

Proof. The equivalences (1)–(6) follow easily from the exact sequence in Lemma 3.2. To show that (7) implies (2), we compare the Poitou-Tate sequences (3.6) for M and N. The same argument with M replaced with $M^\vee(1)$ together with the equivalence of (1) and (2) applied to $M^\vee(1)$ shows that (1) implies (7). $\quad\square$

Lemma 6.4. *Conjecture* $C(K, M)$ *does not depend on the finite set of primes* S.

Proof. Let T be a finite set of prime containing S and note that $\mathrm{H}^0(\mathrm{G}_{k(v)}, M(-1))$ is a finite group for every $v \in (T - S)_{K_{\mathrm{cyc}}}$. The claim of the lemma then follows from the Gysin sequence (3.3). $\quad\square$

Lemma 6.5. *Let* L/K *be a finite extension of degree prime to* p *and* M *a* G_K-*representation on a finite-dimensional vector space over* $\mathbb{F}_p$. *Then* $C(L, M)$ *implies* $C(K, M)$.

Proof. The restriction map $\mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), M) \to \mathrm{H}^2(\mathrm{G}_S(L_{\mathrm{cyc}}), M)$ is split injective, as its composition with the corestriction map is the multiplication by the degree of L/K. Hence, if $N \subset M$ is a G_K-subrepresentation such that the group $\ker(\mathrm{H}^2(\mathrm{G}_S(L_{\mathrm{cyc}}), N) \to \mathrm{H}^2(\mathrm{G}_S(L_{\mathrm{cyc}}), M))$ is finite, then $\ker(\mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), N) \to \mathrm{H}^2(\mathrm{G}_S(K_{\mathrm{cyc}}), M))$ is also finite. $\quad\square$

Conjecture $C(K, M)$ is connected with the isogeny conjecture $I(K, E)$ for elliptic curves in the case when M is a 2-dimensional reducible representation over $\mathbb{F}_p$. We then have an exact sequence

$$0 \to N \to M \to N' \to 0$$

with one-dimensional representations N and N'. Passing to an extension of degree prime to p and using Lemma 6.5, we can further reduce to the case that N and N' are trivial representations. In this case, M represents a class ξ in $\mathrm{H}^1(\mathrm{G}_S(K), \mathbb{F}_p)$ and the connecting homomorphism

$$Q \otimes_\Omega \mathrm{H}^1(\mathrm{G}_S(K), (\mathbb{F}_p)_{K_{\mathrm{cyc}}}) \to Q \otimes_\Omega \mathrm{H}^2(\mathrm{G}_S(K), (\mathbb{F}_p)_{K_{\mathrm{cyc}}})$$

is given by the cup product with ξ. So, in essence, Conjecture $C(K, M)$ for reducible two-dimensional representations M boils down to the vanishing of cup products. We plan to investigate this further in subsequent work.

References

[Bil86] P. Billot, *Quelques aspects de la descente sur une courbe elliptique dans le cas de réduction supersingulière*, Compositio Math. **58** (1986), no. 3, 341–369.

[Cha14] A. Chandrakant, *On the μ-invariant of fine Selmer groups*, J. Number Theory **135** (2014), 284–300.

[CS05] J. Coates and R. Sujatha, *Fine Selmer groups for elliptic curves with complex multiplication*, Algebra and number theory, Hindustan Book Agency, Delhi, 2005, pp. 327–337.

[FK06]   T. Fukaya and K. Kato, *A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory*, Proceedings of the St. Petersburg Mathematical Society (Providence, RI), vol. XII, Amer. Math. Soc. Transl. Ser. 2, no. 219, American Math. Soc., 2006, pp. 1–85.

[Gre97] R. Greenberg, *The structure of Selmer groups*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), no. 21, 11125–11128, Elliptic curves and modular forms (Washington, DC, 1996).

[Gre11] _____ , *Iwasawa theory, projective modules, and modular representations*, Mem. Amer. Math. Soc. **211** (2011), no. 992, vi+185.

[Jha12] S. Jha, *Fine Selmer group of Hida deformations over non-commutative p-adic Lie extensions*, Asian J. Math. **16** (2012), no. 2, 353–365.

[JS11]   S. Jha and R. Sujatha, *On the Hida deformations of fine Selmer groups*, J. Algebra **338** (2011), 180–196.

[Lim13] M. F. Lim, *Notes on fine Selmer groups*, preprint, arXiv:1306.2047v3, 2013.

[Mil06] J. S. Milne, *Arithmetic duality theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006. MR 2261462 (2007e:14029)

[Neu99] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NSW00] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren der mathematischen Wissenschaften, no. 323, Springer Verlag, Berlin Heidelberg, 2000.

[Par89] J. L. Parish, *Rational torsion in complex-multiplication elliptic curves*, J. Number Theory **33** (1989), no. 2, 257–265.

[PR00]   B. Perrin-Riou, *p-adic L-functions and p-adic representations*, SMF/AMS Texts and Monographs, vol. 3, American Mathematical Society, Providence, RI; Société Mathématique de France, Paris, 2000, Translated from the 1995 French original by Leila Schneps and revised by the author.

[Sch85] P. Schneider, *p-adic height pairings. II*, Invent. Math. **79** (1985), no. 2, 329–374.

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Suj10] R. Sujatha, *Elliptic curves and Iwasawa's $\mu = 0$ conjecture*, Quadratic forms, linear algebraic groups, and cohomology, Dev. Math., vol. 18, Springer, New York, 2010, pp. 125–135. MR 2648723

[Wit13] M. Witte, *On a localisation sequence for the K-theory of skew power series rings*, J. K-Theory **11** (2013), no. 1, 125–154.

[Wit14] _____ , *On a noncommutative Iwasawa main conjecture for varieties over finite fields*, J. Eur. Math. Soc. (JEMS) **16** (2014), no. 2, 289–325.

[Wut07] C. Wuthrich, *Iwasawa theory of the fine Selmer group*, J. Algebraic Geom. **16** (2007), no. 1, 83–108.

R. Sujatha
Department of Mathematics,
University of British Columbia,
Vancouver,
Canada V6T1Z2
    E-mail address: sujatha@math.ubc.ca

M. Witte
Universität Heidelberg,
Mathematisches Institut,
Im Neuenheimer Feld 205,
D-69120 Heidelberg
    E-mail address: witte@mathi.uni-heidelberg.de