Math. Proc. Camb. Phil. Soc. (2025), **179**, 449–501
doi:10.1017/S0305004125000325
First published online 24 June 2025

On the $\mathfrak{M}_H(G)$-property

BY SÖREN KLEINE
Institut für Anwendungssicherheit, Fakultät für Informatik, Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, D-85579 Neubiberg, Germany.
e-mail: soeren.kleine@unibw.de

AHMED MATAR
Department of Mathematics, University of Bahrain, P.O. Box 32038, Sukhair, Bahrain.
e-mail: amatar@uob.edu.bh

AND SUJATHA RAMDORAI
Department of Mathematics, 1984, Mathematics Road, University of British Columbia, Vancouver, V6T1Z2, Canada.
e-mail: sujatha@math.ubc.ca

(*Received* 11 *May* 2023*; revised* 11 *December* 2024)

Abstract

Let E be an elliptic curve defined over $\mathbb{Q}$ which has good ordinary reduction at the prime p. Let K be a number field with at least one complex prime which we assume to be totally imaginary if $p = 2$. We prove several equivalent criteria for the validity of the $\mathfrak{M}_H(G)$-property for $\mathbb{Z}_p$-extensions other than the cyclotomic extension inside a fixed $\mathbb{Z}_p^2$-extension K_∞/K. The equivalent conditions involve the growth of μ-invariants of the Selmer groups over intermediate shifted $\mathbb{Z}_p$-extensions in K_∞, and the boundedness of λ-invariants as one runs over $\mathbb{Z}_p$-extensions of K inside of K_∞.

Using these criteria we also derive several applications. For example, we can bound the number of $\mathbb{Z}_p$-extensions of K inside K_∞ over which the Mordell–Weil rank of E is not bounded, thereby proving special cases of a conjecture of Mazur. Moreover, we show that the validity of the $\mathfrak{M}_H(G)$-property sometimes can be shifted to a larger base field K'.

2020 Mathematics Subject Classification: 11R23 (Primary)

1. *Introduction*

Let p be a rational prime, and let E be an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at p. Let K be a number field with at least one complex prime which we assume to be totally imaginary if $p = 2$. Denote by K_∞ a $\mathbb{Z}_p^2$-extension of K. In this paper we study a property of the Selmer group of E over K_∞ with respect to varying $\mathbb{Z}_p$-subextensions. In order to be more precise, we introduce some notation.

Let S be a finite set of nonarchimedean primes of K containing all the primes dividing p and all the primes where E has bad reduction. We let K_S be the maximal extension of

Dedicated to the memory of John H. Coates

© The Author(s), 2025. Published by Cambridge University Press on behalf of Cambridge Philosophical Society.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

K unramified outside S. Suppose now that L is a field with $K \subseteq L \subseteq K_S$. We let $G_S(L) = \mathrm{Gal}(K_S/L)$ and for $v \in S$ we define $J_v(E/L) = \varinjlim \bigoplus_{w|v} H^1(F_w, E)[p^\infty]$ where the direct limit runs over finite extensions F of K contained in L (see [9]). We define the p^∞-Selmer group of E/L as

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/L) \longrightarrow H^1(G_S(L), E[p^\infty]) \longrightarrow \bigoplus_{v \in S} J_v(E/L).$$

Let $G := \mathrm{Gal}(K_\infty/K)$. We denote the Iwasawa algebra $\Lambda(G) = \mathbb{Z}_p[[G]]$ by Λ_2. If σ and τ are topological generators of G, then $\Lambda_2 \cong \mathbb{Z}_p[[T, U]]$ via the map sending $\sigma - 1$ to U and $\tau - 1$ to T.

Consider the set $\mathbb{P}^1(\mathbb{Z}_p) = \{(a, b) \in \mathbb{Z}_p^2 \mid p \text{ does not divide both } a \text{ and } b\}/\sim$ where $(a_1, b_1) \sim (a_2, b_2)$ if there exists $t \in \mathbb{Z}_p^\times$ with $a_1 = ta_2$ and $b_1 = tb_2$. Then the $\mathbb{Z}_p$-extensions of K which are contained in K_∞ are in bijection with the elements of $\mathbb{P}^1(\mathbb{Z}_p)$: every element $[(a, b)] \in \mathbb{P}^1(\mathbb{Z}_p)$ maps to the $\mathbb{Z}_p$-extension being the fixed field of K_∞ of the closed subgroup generated by $\sigma^a \tau^b$.

Let $\mathcal{E}$ be the set of all $\mathbb{Z}_p$-extensions of K. Greenberg [18] introduced the following topology on $\mathcal{E}$ (which we call Greenberg's topology). For $L \in \mathcal{E}$ and n a positive integer we define $\mathcal{E}(L, n) := \{L' \in \mathcal{E} \mid [L' \cap L : K] \geq p^n\}$. This means $\mathcal{E}(L, n)$ consists of all $\mathbb{Z}_p$-extensions of K which coincide with L at least up to level n. Taking $\mathcal{E}(L, n)$ as a base of neighbourhoods of L gives us a topology on $\mathcal{E}$. Now let $\mathcal{E}^{\subseteq K_\infty}(K)$ be the subset of $\mathcal{E}$ which contains the $\mathbb{Z}_p$-extensions of K that are contained in the fixed $\mathbb{Z}_p^2$-extension K_∞ of K. With the above topology the bijection $\mathbb{P}^1(\mathbb{Z}_p) \leftrightarrow \mathcal{E}^{\subseteq K_\infty}(K)$ becomes a homeomorphism. Indeed, if two $\mathbb{Z}_p$-extensions $L, L' \in \mathcal{E}^{\subseteq K_\infty}(K)$ of K correspond to $[(a, b)], [(a', b')] \in \mathbb{P}^1(\mathbb{Z}_p)$, respectively, then $L' \in \mathcal{E}(L, n)$ if and only if $a \equiv a' \pmod{p^n}$ and $b \equiv b' \pmod{p^n}$. This means that the above bijection maps the open sets of $\mathbb{P}^1(\mathbb{Z}_p)$ to the open sets of $\mathcal{E}^{\subseteq K_\infty}(K)$.

We let $X(E/K_\infty)$ be the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$. Also if $L \in \mathcal{E}^{\subseteq K_\infty}(K)$, then we let $X(E/L)$ be the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/L)$, and we denote the Iwasawa algebra $\mathbb{Z}_p[[\mathrm{Gal}(L/K)]]$ by $\Lambda_{\mathrm{Gal}(L/K)}$ or when it is clear from context simply by Λ.

For any subgroup H of G we denote its fixed field by K_∞^H. We now define a certain subset $\mathcal{H}$ of subgroups H of G. In view of the bijection $\mathbb{P}^1(\mathbb{Z}_p) \leftrightarrow \mathcal{E}^{\subseteq K_\infty}(K)$, $\mathcal{H}$ will correspond to a subset of $\mathbb{Z}_p$-extensions of K which have certain properties.

Definition 1·1. Let $\mathcal{H}$ be the subset of all subgroups $H = \overline{\langle \sigma^a \tau^b \rangle}$ of $G = \mathrm{Gal}(K_\infty/K)$ which are topologically generated by $\sigma^a \tau^b$ for some $[(a, b)] \in \mathbb{P}^1(\mathbb{Z}_p)$ such that:

(a) No prime in S splits completely in K_∞^H/K;

(b) Every prime of K above p ramifies in K_∞^H/K;

(c) $X(E/K_\infty^H)$ is a torsion $\Lambda_{G/H}$-module.

In all that follows we will always assume that $\mathcal{H}$ is not empty. We shall show that in this case $\overline{\langle \sigma^a \tau^b \rangle} \in \mathcal{H}$ for all but finitely many $[(a, b)] \in \mathbb{P}^1(\mathbb{Z}_p)$ (Proposition 2·5). Moreover, if K_∞ contains the cyclotomic $\mathbb{Z}_p$-extension K_{cyc} of K and $K/\mathbb{Q}$ is an abelian extension, then $H_{cyc} := \mathrm{Gal}(K_\infty/K_{cyc}) \in \mathcal{H}$ (Proposition 2·6), i.e. in this case $\mathcal{H}$ will be automatically non-empty.

For $H \in \mathcal{H}$ we define $H_n := H^{p^n}$. For every n, we fix a finite extension $K_{H,n}/K$ of degree p^n such that $K_\infty^{H_n} = K_{H,n} K_\infty^H$. Then $K_\infty^{H_n}/K_{H,n}$ is a $\mathbb{Z}_p$-extension. We will sometimes

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

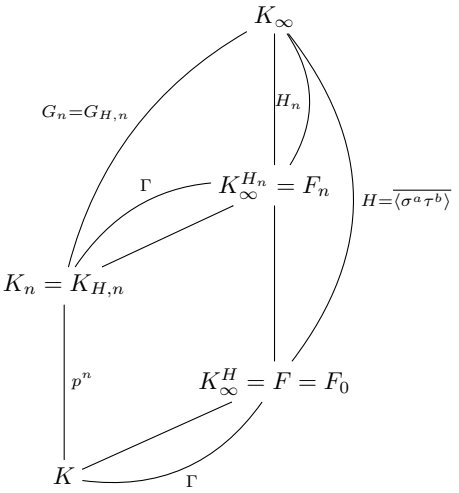


Fig. 1. Overview of the intermediate fields and Galois groups.

abbreviate $K_\infty^{H_n}$ to F_n and write $F_0 = F$ in this paper. We summarise all these subfields and the corresponding Galois groups in the field diagram given in Figure 1. The Galois groups $\mathrm{Gal}(F/K) \cong \mathrm{Gal}(F_n/K_{H,n})$ are isomorphic to $\mathbb{Z}_p$ and are abbreviated to Γ in this diagram.

We define $\Lambda_{H,K_{H,n}} := \mathbb{Z}_p[[\mathrm{Gal}(K_\infty^{H_n}/K_{H,n})]]$. For every n, we let $G_{H,n} = \mathrm{Gal}(K_\infty/K_{H,n})$ and we write $\mu_{G_{H,n}/H_n}(X(E/K_\infty^{H_n}))$ for the μ-invariant of $X(E/K_\infty^{H_n})$ as a $\Lambda_{H,K_{H,n}}$-module. When we are working with a fixed $H \in \mathcal{H}$, then, to ease notation, we will sometimes drop the subscript H from all the symbols in this paragraph.

We define $X(E/K_\infty)_f := X(E/K_\infty)/X(E/K_\infty)[p^\infty]$ (this group was denoted $Y(E/K_\infty)$ in [**10**]). We similarly define $X(E/K_\infty^{H_n})_f$ for any $H \in \mathcal{H}$ and any $n \geq 0$. For any $H \in \mathcal{H}$ one may ask whether $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H) := \mathbb{Z}_p[[H]]$.

Definition 1·2. For $H \in \mathcal{H}$ we say that $X(E/K_\infty)$ satisfies the $\mathfrak{M}_H(G)$-property if $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$.

For $H = H_{cyc}$ this is conjectured to be true if p is odd (see [**10**]) and is known as the $\mathfrak{M}_H(G)$-conjecture. For instance, this conjecture holds true if $X(E/K_{cyc})$ is $\mathbb{Z}_p[[T]]$-torsion and has μ-invariant zero. In this case it is known that there exists a Greenberg neighbourhood U of K_{cyc} such that the Selmer group is cotorsion with μ-invariant zero for each $L \in U$. It is natural to ask whether a similar fact is true for the $\mathfrak{M}_H(G)$-property, i.e. whether the following question can be answered affirmatively: Given that the $\mathfrak{M}_H(G)$-property is satisfied for some $H \in \mathcal{H}$, can one find a neighbourhood U of K_∞^H such that the $\mathfrak{M}_H(G)$-property is satisfied for each $\mathbb{Z}_p$-extension in U? We will prove that this is indeed the case. The major ingredient of our argument is a new criterion for the validity of the $\mathfrak{M}_H(G)$-property, which is part of our first main result.

Suppose that $X(E/K_\infty)$ is a torsion $\Lambda_{\mathrm{Gal}(K_\infty/K)}$-module, and let f_∞ be the characteristic power series of $X(E/K_\infty)$. If $f_\infty \neq 0$, write $f_\infty = p^m g_\infty$ where $m = \mu_G(X(E/K_\infty))$ so

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

that $p \nmid g_\infty$. When $f_\infty = 0$, we set $g_\infty = 0$. If $H \in \mathcal{H}$, we let λ_H be the lambda-invariant of $X(E/K_\infty^H)$. The first main result of this paper is the following

THEOREM 1·3. *Let $\mathcal{H}$ be as in Definition 1·1, and suppose that $\mathcal{H}$ is not empty. Then $X(E/K_\infty)$ is Λ_2-torsion, and for any $H = \overline{\langle \sigma^a \tau^b \rangle} \in \mathcal{H}$ the following are equivalent*:

(*a*) *$X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$;*

(*b*) *$\mu_G(X(E/K_\infty)) = \mu_{G/H}(X(E/K_\infty^H))$;*

(*c*) *for all n, $X(E/K_\infty^{H_n})$ is a torsion $\Lambda_{H,K_{H,n}}$-module and*

$$p^n \mu_G(X(E/K_\infty)) = \mu_{G_n/H_n}(X(E/K_\infty^{H_n}));$$

(*d*) *either $g_\infty = 0$, or $g_\infty \neq 0$ and the image of g_∞ in $\Lambda_2/p\Lambda_2$ is not divisible by the coset of $(1+U)^a(1+T)^b - 1$ (here $U = \sigma - 1$ and $T = \tau - 1$);*

(*e*) *$\lambda(X(E/L))$ is bounded as L varies through the elements in a neighbourhood of K_∞^H. If $E(K_\infty)[p^\infty]$ is finite, the above are equivalent to:*

(*f*) *we have an injective $\Lambda(H)$-homomorphism*

$$X(E/K_\infty)_f \hookrightarrow \Lambda(H)^{\lambda_H}$$

with finite cokernel and a Λ_2-exact sequence

$$0 \to A \to X(E/K_\infty) \to \bigoplus_{i=1}^{s} \Lambda_2/f_i^{n_i} \oplus \bigoplus_{j=1}^{t} \Lambda_2/p^{m_j} \to B \to 0,$$

where $s \leq \lambda_H$, A and B are pseudo-null Λ_2-modules with A annihilated by some power of p, $f_i \in \Lambda_2 \setminus \Lambda(H)$ are irreducible power series and $\mu_G(X(E/K_\infty)) = \sum_{j=1}^{t} m_t$.

If $E(K)[p] = 0$, then $X(E/K_\infty)$ has no nontrivial pseudo-null Λ_2-submodules and so $A = 0$ in (f).

The equivalences of (*a*), (*b*) and (*c*) above for $H_{cyc} = \mathrm{Gal}(K_\infty/K_{cyc})$ are proven using methods from [**10**]. For H_{cyc}, the single implication (*a*) $\Rightarrow$ (*b*) is also proven in special cases in [**8, 42**]. Our proofs of the equivalences of (*a*), (*b*) and (*c*) for any $H \in \mathcal{H}$ will follow similar lines.

The main novelty of our approach is that it relates statements (*d*), (*e*) and (*f*) to the $\mathfrak{M}_H(G)$-property. As far as we know this has not been realised in the literature before. We will be able to derive several interesting consequences for the $\mathfrak{M}_H(G)$-property by using these conditions. For example, it is clear from (*e*) that the validity of the $\mathfrak{M}_H(G)$-property for some $H \in \mathcal{H}$, automatically guarantees the validity of the $\mathfrak{M}_H(G)$-property for each $\mathbb{Z}_p$-extension of K which is contained in some small neighbourhood of K_∞^H.

Moreover, as an easy consequence of part (*d*) above, we will show the following result which provides strong heuristic evidence in favor of the $\mathfrak{M}_H(G)$-conjecture.

PROPOSITION 1·4. *Assume as before that $\mathcal{H}$ is not empty. For all but finitely many $H \in \mathcal{H}$, $X(E/K_\infty)_f$ is a finitely generated $\Lambda(H)$-module.*

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

We say a few words on the proof of the conditions (d), (e) and (f) from Theorem 1·3. The result stated in (f) is similar to Theorem 3·1 in the paper of Hachimori and Venjakob [**25**]; the latter was proven in the setup of a $\mathbb{Z}_p \rtimes \mathbb{Z}_p$-extension containing K_{cyc} under the additional condition that $\mu(X(E/K_{cyc})) = 0$, whereas we make no assumption on the vanishing of the μ-invariant but work in a $\mathbb{Z}_p^2$-extension. The main tools used to prove $(a) \Rightarrow (f)$ are a control theorem $(X(E/K_\infty)_f)_{H_n} \to X(E/K_\infty^{H_n})_f$ (see Proposition 4·2) and Theorem 8·1.

The implication $(d) \Rightarrow (a)$ can be shown via purely module-theoretic arguments (see Proposition 7·1). In order to obtain the reverse implication, we prove an asymptotic growth formula for the $\mu_{G_n/H_n}(X(E/K_\infty^{H_n}))$ which is an analog of a similar formula for class numbers due to Cuoco [**12**]. Finally, the equivalence of (d) and (e) is proven using the work of Monsky [**47**].

The condition in (f) that $E(K_\infty)[p^\infty]$ is finite is imposed in order to bound the order of the maximal finite $\Lambda_{H,K_{H,n}}$- submodule of $X(E/K_\infty^{H_n})$ as n varies. Such a bound is proven using the work of Hachimori and Matsuno [**23**]. This condition is mild as we will show in Lemma 3·5.

Remark. If $E(K)[p^\infty] = 0$, then $E(K_\infty)[p^\infty] = 0$ since K_∞/K is a pro-p-extension (recall that this condition is used in the last assertion of Theorem 1·3).

A well-known result of Iwasawa (see [**28**, Theorem 2]) states that the vanishing of the Iwasawa μ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of a number field K implies that also the μ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of any finite p-extension K' of K vanishes. In the good ordinary case the analog of this statement for Selmer groups is shown in [**22**, corollary 3·4]. Using the equivalent conditions from our main result, we can derive a similar result on the shifting of the $\mathfrak{M}_H(G)$-property (see Theorem 11·9 in Section 11). In particular, this result can be used in order to deduce from the validity of the $\mathfrak{M}_H(G)$-conjecture for K the validity of the $\mathfrak{M}_H(G)$-conjecture for the larger base field K'. The shifting of the $\mathfrak{M}_H(G)$-property seems to be a very hard problem. We were able to prove its shifting invariance only under certain additional assumptions (see Theorem 11·9 for the details). We describe a natural setting where some of the additional hypothesis hold at the end of the paper.

Now we describe further applications of our main results. We now specialise to an imaginary quadratic base field K, i.e. the $\mathbb{Z}_p^2$-extension K_∞ of K is now just the composite of all $\mathbb{Z}_p$-extensions of K. It contains the cyclotomic $\mathbb{Z}_p$-extension K_{cyc} of K, and also the anticyclotomic $\mathbb{Z}_p$-extension K_{ac}. We mention an application of Theorem 1·3 to the number of $L \in \mathcal{E} = \mathcal{E}^{\subseteq K_\infty}(K)$ where the rank of E stays bounded. As a first observation, it follows from Proposition 2·3, Proposition 2·6 and Lemma 9·1 that the rank of E stays bounded in all but finitely many $\mathbb{Z}_p$-extensions $L \in \mathcal{E}$. The precise number of $\mathbb{Z}_p$-extensions where the rank of E stays bounded is predicted by Mazur's growth number conjecture ([**45**, section 18]).

CONJECTURE (Mazur). *The Mordell–Weil rank of E stays bounded along any $\mathbb{Z}_p$-extension of the imaginary quadratic field K, unless the extension is anticyclotomic and the root number of E/K is -1.*

It seems striking to us that the $\mathfrak{M}_H(G)$-property has relations to Mazur's conjecture. Let Σ be the set of all $H \in \mathcal{H}$ such that $X(E/K_\infty)_f$ is a finitely generated $\Lambda(H)$-module. In relation

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

to Mazur's conjecture, using a slightly weaker version of Theorem 1·3(f) and a technique of Bloom and Gerth [4], we will show

THEOREM 1·5. *Let t be the number of $\mathbb{Z}_p$-extensions of an imaginary quadratic field K, where the rank of E does not stay bounded. Then $t \leq \min\{\lambda_H \mid H \in \Sigma\}$.*

In particular, if $\lambda_H = 0$ for *any* $H \in \Sigma$ (respectively, $\lambda_H = 1$ if the root number of the L-function is -1), then Mazur's Conjecture holds true. We provide explicit examples in Section 9 where this happens, thus deriving sufficient criteria for the validity of Mazur's Conjecture, and we illustrate our results with numerical examples.

We now recall the following conjecture of Greenberg (see [19, conjecture 1·11]).

CONJECTURE (Greenberg). *Let E be an elliptic curve which is defined over $\mathbb{Q}$. If $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{cyc})$ is Λ-cotorsion, then there exists a $\mathbb{Q}$-isogenous elliptic curve E' such that $\mathrm{Sel}_{p^\infty}(E'/\mathbb{Q}_{cyc})$ has μ-invariant zero.*

In particular, if $E[p]$ is an irreducible $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$-module, then $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{cyc})$ has μ-invariant zero.

Let us mention one final application. As mentioned above, when p is odd, it is conjectured that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H_{cyc})$. Assuming this, we use our main theorem and a result of Pollack and Weston [50] on the vanishing of the μ-invariant of $X(E/K_{ac})$ to prove a result (see Theorem 10·8), which establishes an interesting connection between the $\mathfrak{M}_H(G)$-conjecture and the above conjecture of Greenberg.

This paper consists of 11 sections, including this introduction. Sections 2-8 are devoted to the proofs of the equivalent conditions in our main theorem (in particular, we derive the connection to the boundedness of λ-invariants through analogues of results of Cuoco and Monsky in Sections 6 and 7). In Section 9 and Section 10 we prove the applications concerning the conjectures of Mazur and Greenberg. The final section is devoted to a study of the shifting invariance of the $\mathfrak{M}_H(G)$-property.

The $\mathfrak{M}_H(G)$-conjecture plays a crucial role and in fact is an assumption in the formulation of the noncommutative main conjecture (see [6, 17, 57]). John Coates strongly believed that the $\mathfrak{M}_H(G)$-conjecture should be true and viewed the statement as a natural generalisation of the celebrated conjecture of Mazur [19, Conjecture 1·3]. The Akashi series in [8] was developed as a tool towards tackling the $\mathfrak{M}_H(G)$-conjecture. The authors therefore dedicate this paper to the memory of John Coates and his contributions to Iwasawa theory.

2. *Results on $\mathrm{Sel}_{p^\infty}(E/L)$ for $L = K_\infty$ and $L \in \mathcal{E}^{\subseteq K_\infty}(K)$*

This section is preliminary in nature and collects several auxiliary results, the most important of which is our control theorem (Proposition 2·8) which works for non-cyclotomic $\mathbb{Z}_p$-extensions.

Let K be as in Theorem 1·3. The following well-known result is easy to prove:

LEMMA 2·1. *Let R be a Noetherian UFD of dimension at least two. Let $W = \bigoplus_{i=1}^{t} R/\mathfrak{p}_i^{n_i}$ where, for all i, $\mathfrak{p}_i$ is a prime ideal of height one. Then W has no nontrivial pseudo-null R-submodules.*

Proof. Assume that M is a pseudo-null submodule of W. Then, by the very definition of what it means to be pseudo-null, we have that $M_\mathfrak{p} = 0$ for all prime ideals $\mathfrak{p}$ of R of height

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

less than or equal to one. We now show that for any prime ideal $\mathfrak{p}$ of R of height one and any $n > 0$ the natural map $\psi : R/\mathfrak{p}^n \to S^{-1}(R/\mathfrak{p}^n)$ where $S = R \setminus \mathfrak{p}$ is an injection. Applying this to the prime ideals $\mathfrak{p}_i$ appearing in the decomposition of W shows that we must have $M = 0$.

To show the claim, assume that for some $x \in R$ we have $\psi(x + \mathfrak{p}^n) = 0$. Then for some $s \in S$ we have $sx \in \mathfrak{p}^n$. Since R is a UFD, therefore $\mathfrak{p} = \langle y \rangle$ for some $y \in R$ (see [**43**, Theorem 20·1]). The element y is necessarily an irreducible(=prime) element of R. So $y^n \mid sx$. Since $y \nmid s$ and R is a UFD, therefore $y^n \mid x$ which shows that $x \in \mathfrak{p}^n$. □

Recall that there exists a bijection $\mathbb{P}^1(\mathbb{Z}_p) \leftrightarrow \mathcal{E}^{\subseteq K_\infty}(K)$, i.e. each element $[(a, b)] \in \mathbb{P}^1(\mathbb{Z}_p)$ uniquely determines a $\mathbb{Z}_p$-extension of K inside K_∞, via the subgroup H of $\mathrm{Gal}(K_\infty/K)$ fixing it. We need the following

LEMMA 2·2. *Let $[(a, b)] \in \mathbb{P}^1(\mathbb{Z}_p)$ and let $H = \overline{\langle \sigma^a \tau^b \rangle}$ and $\Upsilon = (1 + U)^a(1 + T)^b - 1$. If $f_\infty \neq 0$, then we have that $X(E/K_\infty)_H$ is a torsion Λ_2/Υ-module if and only if f_∞ and Υ are relatively prime.*

Proof. To simplify notation, we will denote $X(E/K_\infty)$ by simply X_∞. Assume that $f_\infty \neq 0$. Taking into account Lemmas 2·9 and 2·1, we have by [**5**, chapter VII, section 4·4 Theorem 5], that there exist irreducible power series $f_j \in \mathbb{Z}_p[[T, U]]$, integers m_i, n_j and an exact sequence

$$0 \to W \to X_\infty \to B \to 0,$$

where $W = \bigoplus_{i=1}^{s} \Lambda_2/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda_2/f_j^{n_j}$ and B is a pseudo-null Λ_2-module. From this exact sequence, we get another exact sequence

$$B^{\Upsilon=0} \to W/\Upsilon \to X_\infty/\Upsilon \to B/\Upsilon \to 0. \tag{1}$$

Since B is a pseudo-null Λ_2-module, therefore it has Krull dimension at most one. So the Λ_2/Υ-modules B/Υ and $B^{\Upsilon=0}$ also have Krull dimension at most one and hence they are Λ_2/Υ-torsion.

Therefore, it follows from the sequence (1) that X_∞/Υ and W/Υ have the same Λ_2/Υ-rank. Hence we must show that W/Υ is Λ_2/Υ-torsion if and only if f_∞ and Υ are relatively prime. Clearly if $D = \Lambda_2/p^{m_i}$, then D/Υ is a torsion Λ_2/Υ-module. So we see that W/Υ has positive Λ_2/Υ-rank if and only if $\Lambda_2/\langle f_j^{n_j}, \Upsilon \rangle$ has positive Λ_2/Υ-rank for some j and this is the case, if and only if, for some j, f_j divides Υ (see [**43**, Theorem 17·4]). □

In the following, for $L \in \mathcal{E}$, we will abbreviate the Iwasawa algebra $\Lambda(\mathrm{Gal}(K_\infty/L))$ to Λ. Recall the definition of $\mathcal{H}$ from Definition 1·1.

PROPOSITION 2·3. *Suppose that $\mathcal{H}$ is not empty. Then $X(E/L)$ is a torsion Λ-module for all but finitely many $L \in \mathcal{E}^{\subseteq K_\infty}(K)$.*

Proof. If $L \in \mathcal{E}^{\subseteq K_\infty}(K)$, consider the map (induced by restriction)

$$s : \mathrm{Sel}_{p^\infty}(E/L) \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{Gal}(K_\infty/L)}.$$

We have that $\ker s$ injects into

$$H^1(\mathrm{Gal}(K_\infty/L), E(K_\infty)[p^\infty]) = \ker\left(H^1(G_S(L), E[p^\infty]) \to H^1(G_S(K_\infty), E[p^\infty])\right).$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Since $H^1(\mathrm{Gal}(K_\infty/L), E(K_\infty)[p^\infty])$ is clearly cofinitely generated over $\mathbb{Z}_p$, so is $\ker s$. Therefore by considering the dual of the map s, we see that $X(E/L)$ will be a torsion Λ-module if this is the case for $X(E/K_\infty)_{\mathrm{Gal}(K_\infty/L)}$.

If $f_\infty = 0$, then $X(E/K_\infty)$ is a pseudo-null Λ_2-module. Hence it has Krull dimension at most one. Therefore for any $L \in \mathcal{E}^{\subseteq K_\infty}(K)$, we have that $X(E/K_\infty)_{\mathrm{Gal}(K_\infty/L)}$ has Krull dimension at most one and hence is a torsion $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/L)]]$-module. Therefore in this case for all $L \in \mathcal{E}^{\subseteq K_\infty}(K)$, $X(E/L)$ is a torsion Λ-module.

Now assume that $f_\infty \neq 0$. From Lemma 2·2 (and since Λ_2 is a UFD), we see that the desired result follows from the following lemma. □

LEMMA 2·4. *If [(a,b)] and [(c,d)] are two distinct elements of $\mathbb{P}^1(\mathbb{Z}_p)$, then $\sigma^a\tau^b - 1$ and $\sigma^c\tau^d - 1$ are relatively prime elements of $\Lambda(G)$.*

Proof. Let $\tilde{G}$ be the subgroup topologically generated by $\sigma^a\tau^b$ and $\sigma^c\tau^d$. Then $\tilde{G}$ has finite index in G. Let $I_{\tilde{G}}$ (resp. I_G) be the ideal of $\Lambda(\tilde{G})$ (resp. $\Lambda(G)$) generated by $\sigma^a\tau^b - 1, \sigma^c\tau^d - 1$ and p. Since $\tilde{G}$ is topologically generated by $\sigma^a\tau^b$ and $\sigma^c\tau^d$, therefore $I_{\tilde{G}}$ has finite index in $\Lambda(\tilde{G})$. As $\tilde{G}$ has finite index in G therefore $\Lambda(G)$ is a finitely generated $\Lambda(\tilde{G})$-module. These two facts imply that I_G has finite index in $\Lambda(G)$. By [43, Theorem 17·4], this in turn implies that the sequence $\sigma^a\tau^b - 1, \sigma^c\tau^d - 1, p$ is regular. In particular $\sigma^a\tau^b - 1$ and $\sigma^c\tau^d - 1$ are relatively prime. □

The next proposition establishes the result mentioned in the introduction.

PROPOSITION 2·5. *Suppose that $\mathcal{H}$ is non-empty. Then for all but finitely many $L \in \mathcal{E}^{\subseteq K_\infty}(K)$ we have*:

(*a*) *no prime in S splits completely in L/K;*
(*b*) *every prime of K above p ramifies in L/K;*
(*c*) *$X(E/L)$ is a torsion Λ-module.*

Proof. Let $F = K_\infty^H$ with $H \in \mathcal{H}$, and let L be given. Suppose $v \in S$ splits completely in L/K. Since v does not split completely in F/K, therefore we see that the decomposition group D_v for a prime of K_∞ over v has $\mathbb{Z}_p$-rank one. It follows from this that v does not split completely for any $L' \in \mathcal{E}^{\subseteq K_\infty}(K)$ with $L' \neq L$. Since the set S is finite, (*a*) excludes finitely many $L \in \mathcal{E}^{\subseteq K_\infty}(K)$. Now let $\mathfrak{p}$ be a prime of K above p. Since $\mathfrak{p}$ ramifies in F/K, therefore the inertia group $I_\mathfrak{p}$ of a prime of K_∞ above $\mathfrak{p}$ must have $\mathbb{Z}_p$-rank greater than or equal to one. It follows from this that (*b*) excludes at most finitely many $\mathbb{Z}_p$-extensions. Proposition 2·3 shows that (*c*) excludes finitely many extensions. Putting all these results together gives the proposition. □

PROPOSITION 2·6. *Suppose that K_{cyc} is contained in K_∞ and $K/\mathbb{Q}$ is an abelian extension. Then $H_{cyc} \in \mathcal{H}$.*

Proof. We must show that:

(a) no prime in S splits completely in K_{cyc}/K;
(b) every prime of K above p ramifies in K_{cyc}/K;

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

(c) $X(E/K_{cyc})$ is a torsion Λ-module. □

(a) and (b) certainly hold. (c) holds from results of Kato [32] and Rohrlich [52].

We need the following lemma for the proof of the next proposition.

LEMMA 2·7. *Let $H \in \mathcal{H}$. Then for any $n \geq 0$, we have that $E(K_\infty^{H_n})[p^\infty]$ is finite.*

Proof. This follows from [20, proposition 3·2(ii)]. □

PROPOSITION 2·8. *Let $H \in \mathcal{H}$. The natural maps (induced by restriction):*

$$s_n : \mathrm{Sel}_{p^\infty}(E/K_\infty^{H_n}) \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n}$$

have finite kernel and cokernel and their orders are bounded independently of n.

Proof. For simplicity, let $F_n = K_\infty^{H_n}$ and $F = F_0$. For any n we have a commutative diagram with vertical maps induced by restriction:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n} & \longrightarrow & H^1(G_S(K_\infty), E[p^\infty])^{H_n} & \longrightarrow & \bigoplus_{v\in S} J_v(E/K_\infty)^{H_n} \\
 & & \uparrow{\scriptstyle s_n} & & \uparrow{\scriptstyle g_n} & & \uparrow{\scriptstyle h_n} \\
0 & \longrightarrow & \mathrm{Sel}_{p^\infty}(E/F_n) & \longrightarrow & H^1(G_S(F_n), E[p^\infty]) & \xrightarrow{\theta_n} & \bigoplus_{v\in S} J_v(E/F_n)
\end{array}$$

By the snake lemma we have an exact sequence

$$0 \to \ker s_n \to \ker g_n \to \ker h_n \cap \mathrm{img}\ \theta_n \to \mathrm{coker}\ s_n \to \mathrm{coker}\ g_n.$$

From this exact sequence we see that $\ker s_n$ (resp. $\mathrm{coker}\ s_n$) will be finite and bounded independently of n if we show that $\ker g_n$ (resp. $\mathrm{coker}\ g_n$ and $\ker h_n$) is finite and bounded independently of n.

Let S_n be all the primes of F_n above those in S and $S_{p,n}$ be the primes of S_n above p. We define the following groups:

(1) $A_n := H^1(H_n, E(K_\infty)[p^\infty])$;
(2) $B_n := H^2(H_n, E(K_\infty)[p^\infty])$;
(3) $C_n := \prod_{w\in S_n\setminus S_{p,n}} H^1(H_{n,w}, E(K_{\infty,w})[p^\infty])$;
(4) $D_n := \prod_{w\in S_{p,n}} H^1(H_{n,w}, \tilde{E}(k_{\infty,w})[p^\infty])$.

In (3) and (4) we have also written w for a fixed prime of K_∞ above w and $H_{n,w}$ is the decomposition group. $k_{\infty,w}$ is the residue field and $\tilde{E}$ is the reduction of E over the residue field.

Since all primes of K above p ramify in F (because $H \in \mathcal{H}$), the results of [7] allow us to write

$$\bigoplus_{v\in S} J_v(E/F_n) = \prod_{w\in S_n\setminus S_{p,n}} H^1(F_{n,w}, E[p^\infty]) \times \prod_{w\in S_{p,n}} H^1(F_{n,w}, \tilde{E}[p^\infty]).$$

Here $\tilde{E}$ denotes the reduction of the elliptic curve over the residue field. We can similarly do the same for $\oplus_{v\in S} J_v(E/K_\infty)$.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

From this and Shapiro's lemma we can write $\ker h_n = C_n \times D_n$. Also, we have $\ker g_n = A_n$ and $\operatorname{coker} g_n$ injects into B_n. Therefore, we only need to show that the groups A_n, B_n, C_n and D_n are all finite and bounded independently of n.

First we deal with A_n : Let $W = E(K_\infty)[p^\infty]$. If γ is a topological generator of H, then $A_n = W/(\gamma^{p^n} - 1)W$. The kernel of $\gamma^{p^n} - 1$ acting on W is $E(F_n)[p^\infty]$. This is a finite group by Lemma 2·7.

Let W_{div} be the maximal divisible subgroup of W. Since W_{div} has finite $\mathbb{Z}_p$-corank and the kernel of $\gamma^{p^n} - 1$ acting on W is finite, it follows that $(\gamma^{p^n} - 1)W_{\mathrm{div}} = W_{\mathrm{div}}$. Therefore we see that $H^1(H_n, W)$ has order bounded by $[W : W_{\mathrm{div}}]$. This takes care of the group A_n. As for B_n, this group is zero for all n because $cd_p(H_n) = 1$.

Now we deal with C_n: let $w \in S_n \setminus S_{p,n}$. As primes in S do not split completely in F/K (because $H \in \mathcal{H}$), $F_{n,w}/(K_{H,n})_w$ is a $\mathbb{Z}_p$-extension. This together with the fact that $(K_{H,n})_w$ has no $\mathbb{Z}_p^2$-extension implies that $H_{n,w} = 0$. Therefore $C_n = 0$ for all n.

Finally we deal with D_n: Let $w \in S_{p,n}$. Suppose first that the decomposition group of a prime of K_∞ above w is an open subgroup of $\mathrm{Gal}(K_\infty/K)$ so $H_{n,w}$ is isomorphic to $\mathbb{Z}_p$. Since primes of K above p ramify in F/K, we see that the $H_{n,w}$-invariants of $\tilde{E}(k_{\infty,w})[p^\infty]$ are finite. Therefore, as in the proof for A_n, we see that $H^1(H_{n,w}, \tilde{E}(k_{\infty,w})[p^\infty])$ is finite and bounded independently of n. Now let $w \in S_{p,n}$ be a prime such that the decomposition subgroup of any prime of K_∞ above w is not open in $\mathrm{Gal}(K_\infty/K)$. Since $\mathcal{H}$ is non-empty, the decomposition group will have $\mathbb{Z}_p$-rank one. As there are only finitely many primes in F_n above v (because $H \in \mathcal{H}$), w splits completely in the $\mathbb{Z}_p$-extension K_∞/F_n, and thus $H_{n,w} = 0$. □

LEMMA 2·9. *If $\mathcal{H}$ is non-empty, then $X(E/K_\infty)$ is a torsion Λ_2-module.*

Proof. Choose some $H \in \mathcal{H}$, and recall that $X(E/K_\infty^H)$ is a torsion Λ-module. In view of Proposition 2·8, it follows that $X(E/K_\infty)_H$ is Λ-torsion. Therefore the intended result follows from [**41**, lemma 4·7]. □

Recall that for $H \in \mathcal{H}$ and $n \in \mathbb{N}$ we abbreviate the Iwasawa algebra $\Lambda(\mathrm{Gal}(K_\infty^{H_n}/K_{H,n}))$ to Λ_{K_n} (these fields have been defined in the introduction, just below the large field diagram).

LEMMA 2·10. *Let $H \in \mathcal{H}$. For any n, consider the sequence*

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/K_\infty^{H_n}) \longrightarrow H^1(G_S(K_\infty^{H_n}), E[p^\infty]) \longrightarrow \bigoplus_{v \in S} J_v(E/K_\infty^{H_n}) \longrightarrow 0.$$

This sequence is exact for $n = 0$ and $H^2(G_S(K_\infty^H), E[p^\infty]) = 0$. Furthermore, if $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, then for all n:

(1) *$X(E/K_\infty^{H_n})$ is a torsion Λ_{K_n}-module;*
(2) *the sequence is exact;*
(3) *$H^2(G_S(K_\infty^{H_n}), E[p^\infty]) = 0$.*

Proof. By Lemma 2·7 we have that $E(K_\infty^{H_n})[p^\infty]$ is finite for all n. Taking this into account, we have that if $X(E/K_\infty^{H_n})$ is a torsion Λ_{K_n}-module, then from [**25**, Theorem 7·2] we get that the sequence in the statement of the lemma is exact and also $H^2(G_S(K_\infty^{H_n}), E[p^\infty]) = 0$ (note that loc. cit. Theorem 7·2 requires p to be odd. However as K was assumed to be totally

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

imaginary if $p = 2$, the proof also works for $p = 2$). Since for $H \in \mathcal{H}$ we have that $X(E/K_\infty^H)$ is a torsion Λ-module, we get the desired result for $n = 0$.

Suppose that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$. To complete the proof, from what we just observed, it will suffice to show that $X(E/K_\infty^{H_n})$ is a torsion Λ_{K_n}-module. To prove this, we can proceed as in [**10**, proposition 2·5]. Consider the following commutative diagram with exact rows

$$\begin{array}{ccccc} X(E/K_\infty)_{H_n} & \longrightarrow & (X(E/K_\infty)_f)_{H_n} & \longrightarrow & 0 \\ \downarrow{\scriptstyle \hat{s}_n} & & \downarrow{\scriptstyle \theta_n} & & \\ X(E/K_\infty^{H_n}) & \longrightarrow & X(E/K_\infty^{H_n})_f & \longrightarrow & 0 \end{array}$$

The map $\hat{s}_n$ is the dual of the map s_n in Proposition 2·8 and θ_n is induced by $\hat{s}_n$. By Proposition 2·8, coker $\hat{s}_n$ is finite and hence so is coker θ_n. Since $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$ and H_n has finite index in H, therefore $(X(E/K_\infty)_f)_{H_n}$ is finitely generated over $\mathbb{Z}_p$. Thus we get that $X(E/K_\infty^{H_n})_f$ is finitely generated over $\mathbb{Z}_p$. This implies that $X(E/K_\infty^{H_n})$ is a torsion Λ_{K_n}-module which completes our proof. □

LEMMA 2·11. *Let $H \in \mathcal{H}$. For any n, consider the sequence*

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n} \longrightarrow H^1(G_S(K_\infty), E[p^\infty])^{H_n} \longrightarrow \bigoplus_{v \in S} J_v(E/K_\infty)^{H_n} \longrightarrow 0.$$

This sequence is exact for $n = 0$. If $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, then the sequence is exact for all n.

Proof. Now proceed as in [**8**, lemma 2·3]. Let $H \in \mathcal{H}$ and $n \geq 0$. For simplicity, let $F_n = K_\infty^{H_n}$. Let S_n be the set of all the primes of F_n above those in S and $S_{p,n}$ be the primes of S_n above p.

Consider the map induced by restriction

$$h_n : \bigoplus_{v \in S} J_v(E/F_n) \to \bigoplus_{v \in S} J_v(E/K_\infty)^{H_n}.$$

We claim that h_n is surjective. By the same arguments as in the proof of Proposition 2·8, we have that coker h_n is a submodule of

$$M_n := \prod_{w \in S_n \setminus S_{p,n}} H^2(H_{n,w}, E(K_{\infty,w})[p^\infty]) \times \prod_{w \in S_{p,n}} H^2(H_{n,w}, \tilde{E}(k_{\infty,w})[p^\infty]).$$

In each factor above, we have also written w for a fixed prime of K_∞ above w and $H_{n,w}$ is the decomposition group. $k_{\infty,w}$ is the residue field and $\tilde{E}$ is the reduction of the elliptic curve. Since $cd_p(H_{n,w}) \leq 1$, we therefore see that $M_n = \{0\}$, whence h_n is surjective.

Consider the commutative diagram

$$\begin{array}{ccc} H^1(G_S(K_\infty), E[p^\infty])^{H_n} & \xrightarrow{\rho_n} & \bigoplus_{v \in S} J_v(E/K_\infty)^{H_n} \\ \uparrow & & \uparrow{\scriptstyle h_n} \\ H^1(G_S(F_n), E[p^\infty]) & \xrightarrow{\lambda_n} & \bigoplus_{v \in S} J_v(E/F_n) \end{array}$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

The exactness of the sequence in the statement of the lemma is equivalent to the surjectivity of ρ_n. Since h_n is surjective, the commutative diagram shows that the surjectivity of ρ_n will follow if λ_n is surjective. Therefore, the desired result follows from Lemma 2·10. □

LEMMA 2·12. *Suppose that $\mathcal{H}$ is non-empty. Then $H^2(G_S(K_\infty), E[p^\infty]) = 0$.*

Proof. Let $F = K_\infty^H$ for some $H \in \mathcal{H}$. From Lemma 2·10, it follows that $H^2(G_S(F), E[p^\infty]) = 0$. As $cd_p(H) = 1$, the Hochschild-Serre spectral sequence implies that we have a surjection $H^2(G_S(F), E[p^\infty]) \twoheadrightarrow H^2(G_S(K_\infty), E[p^\infty])^H$. This implies $H^2(G_S(K_\infty), E[p^\infty]) = 0$. □

The above lemma will allow us to show:

LEMMA 2·13. *For any $H \in \mathcal{H}$ we have $H^i(H, H^1(G_S(K_\infty), E[p^\infty])) = 0$ for all $i \geq 1$. Furthermore, if $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, then for any n we have $H^i(H_n, H^1(G_S(K_\infty), E[p^\infty])) = 0$ for all $i \geq 1$.*

Proof. We proceed as in [**8**, lemma 2·4]. Combining [48, proposition 8·3·18] and the previous lemma, we get that

$$H^m(G_S(K_\infty), E[p^\infty]) = 0, \quad m \geq 2.$$

In view of this result, the Hochschild–Serre spectral sequence (see [**48**, lemma 2·1·3]) implies that for any $i \geq 1$ we have an exact sequence

$$H^{i+1}(G_S(K_\infty^{H_n}), E[p^\infty]) \to H^i(H_n, H^1(G_S(K_\infty), E[p^\infty])) \to H^{i+2}(H_n, E(K_\infty^H)[p^\infty]). \quad (1)$$

The group on the right vanishes because $cd_p(H_n) = 1$. For $i \geq 2$ the group on the left vanishes by [**48**, proposition 8·3·18]. By Lemma 2·10, for $i = 1$ the group on the left vanishes for $n = 0$ and assuming that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$ it vanishes for all n. This implies the result. □

LEMMA 2·14. *Let $H \in \mathcal{H}$. We have $H^1(H, \mathrm{Sel}_{p^\infty}(E/K_\infty)) = 0$. If $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, then $H^1(H_n, \mathrm{Sel}_{p^\infty}(E/K_\infty)) = 0$ for all $n \geq 0$.*

Proof. We proceed as in [**8**, lemma 2·6]. Let $n \geq 0$ and assume that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$ if $n > 0$. Now consider the sequence

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n} \longrightarrow H^1(G_S(K_\infty), E[p^\infty])^{H_n} \longrightarrow \bigoplus_{v \in S} J_v(E/K_\infty)^{H_n} \longrightarrow 0. \quad (2)$$

We will show that $H^1(H_n, \mathrm{Sel}_{p^\infty}(E/K_\infty)) = 0$ if the sequence (2) is exact. Therefore, the lemma will follow from Lemma 2·11.

Assume that (2) is exact. Let

$$A_\infty = \mathrm{img}\,(H^1(G_S(K_\infty), E[p^\infty]) \to \bigoplus_{v \in S} J_v(E/K_\infty)),$$

i.e. we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/K_\infty) \longrightarrow H^1(G_S(K_\infty), E[p^\infty]) \longrightarrow A_\infty \longrightarrow 0.$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

This exact sequence and Lemma 2·13 imply that we have an exact sequence

$$0 \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n} \to H^1(G_S(K_\infty), E[p^\infty])^{H_n} \to A_\infty^{H_n} \to H^1(H_n, \mathrm{Sel}_p(E/K_\infty)) \to 0.$$

The exactness of the sequence (2) implies that

$$A_\infty^{H_n} = \bigoplus_{v \in S} J_v(E/K_\infty)^{H_n},$$

whence it is clear that $H^1(H_n, \mathrm{Sel}_p(E/K_\infty)) = 0$, as required. □

The final result in this section is:

PROPOSITION 2·15. *Suppose that $\mathcal{H}$ is not empty. We have an exact sequence*

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/K_\infty) \longrightarrow H^1(G_S(K_\infty), E[p^\infty]) \xrightarrow{\lambda_\infty} \bigoplus_{v \in S} J_v(E/K_\infty) \longrightarrow 0.$$

Proof. We proceed as in [**8**, proposition 2·9]. Let

$$A_\infty = \mathrm{img}\,(\lambda_\infty : H^1(G_S(K_\infty), E[p^\infty]) \to \oplus_{v \in S} J_v(E/K_\infty))$$

i.e. we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/K_\infty) \longrightarrow H^1(G_S(K_\infty), E[p^\infty]) \longrightarrow A_\infty \longrightarrow 0.$$

Choose an element $H \in \mathcal{H}$, and let $F = K_\infty^H$. It then follows from the above sequence and from Lemma 2·13 that

$$H^1(H, A_\infty) \cong H^2(H, \mathrm{Sel}_{p^\infty}(E/K_\infty)),$$

whence $H^1(H, A_\infty) = 0$ because $cd_p(H) = 1$.

Now let $B_\infty = \mathrm{coker}\ \lambda_\infty$. Taking the H_{cyc}-cohomology of the sequence

$$0 \to A_\infty \to \bigoplus_{v \in S} J_v(E/K_\infty) \to B_\infty \to 0$$

and using Lemma 2·11, we get that B_∞^H injects into $H^1(H, A_\infty) = 0$. Therefore, $B_\infty = 0$. This implies that λ_∞ is surjective. □

3. *The maximal finite submodule of $X(E/K_\infty^{H_n})$*

In this section we will use the work of Hachimori and Matsuno [**23**] to bound the order of the maximal finite submodule of $X(E/K_\infty^{H_n})$. This is used for the proof of Proposition 4·3 in the next section which in turn is a key tool used in the proof of the implication $(a) \Rightarrow (f)$ in Theorem 1·3. Moreover, we prove Lemma 3·5, which shows that the additional hypothesis in part (f) of Theorem 1·3 is rather mild.

If A is an abelian group, let A_{div} be the maximal divisible subgroup of A. First we need

LEMMA 3·1. *Let L be a number field, L_∞/L be a $\mathbb{Z}_p$-extension with tower fields L_n, E an elliptic curve defined over L and p a rational prime. Let $s_n : \mathrm{Sel}_{p^\infty}(E/L_n) \to \mathrm{Sel}_{p^\infty}(E/L_\infty)^{\Gamma_n}$ be the map induced by restriction (here, $\Gamma = \mathrm{Gal}(L_\infty/L)$ and $\Gamma_n = \Gamma^{p^n}$). Then, for any n,* $\ker s_n$ *is finite of order at most* $[E(L_\infty)[p^\infty] : E(L_\infty)[p^\infty]_{div}]$.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Proof. This follows from a similar argument to the one used in the proof of Proposition 2·8. □

We now have the following important theorem.

THEOREM 3·2 (Hachimori–Matsuno [23]). *We retain the setup and notation of the previous lemma and assume that the Pontryagin dual of* $\mathrm{Sel}_{p^\infty}(E/L_\infty)$*, denoted* $X(E/L_\infty)$*, is* $\mathbb{Z}_p[[\Gamma]]$*-torsion. Then the maximal finite* $\mathbb{Z}_p[[\Gamma]]$*-submodule of* $X(E/L_\infty)$ *is isomorphic to* $\varprojlim \ker s_n$ *where the inverse limit is with respect to the corestriction maps.*

The following lemma is easy to prove. We leave the proof for the reader.

LEMMA 3·3. *Let* $M > 0$ *be an integer. Then there exists* $C > 0$ *satisfying the following: If* (B_i, φ_{ij})*,* $i \in \mathbb{N}$ *is a projective system and for all* $i \in \mathbb{N}$ B_i *is finite of order at most* M*, then* $\varprojlim B_i$ *is finite of order at most* C*.*

Now we return to our setup and show:

THEOREM 3·4. *Suppose that* $E(K_\infty)[p^\infty]$ *is finite. Then there exists* $C > 0$ *satisfying the following: Assume* $H \in \mathcal{H}$ *and* $n \geq 0$*. If* $X(E/K_\infty^{H_n})$ *is* Λ_{K_n}*-torsion, then the maximal finite* Λ_{K_n}*-submodule of* $X(E/K_\infty^{H_n})$ *has order at most* C*.*

Proof. Suppose that $E(K_\infty)[p^\infty]$ is finite. Assume $H \in \mathcal{H}$ and $n \geq 0$. Denote $K_\infty^{H_n}$ by L_∞ and $K_{H,n}$ by L. Then L_∞/L is a $\mathbb{Z}_p$-extension with tower fields L_n. Let $s_n : \mathrm{Sel}_{p^\infty}(E/L_n) \to \mathrm{Sel}_{p^\infty}(E/L_\infty)^{\Gamma_n}$ be the map induced by restriction. Since $E(L_\infty)[p^\infty]$ is finite with $\#E(L_\infty)[p^\infty] \leq \#E(K_\infty)[p^\infty]$, we get from Lemma 3·1 that $\ker s_n$ is finite of order at most $\#E(K_\infty)[p^\infty]$. From this we see that the desired result follows from Theorem 3·2 and Lemma 3·3. □

LEMMA 3·5. $E(K_\infty)[p^\infty]$ *is finite if either:*

(1) *E does not have complex multiplication;*

(2) *E has complex multiplication by the ring of integers of a quadratic imaginary field L,* $[K : \mathbb{Q}] \leq 8$ *and* $p \geq 5$*. In this case we have* $E(K_\infty)[p^\infty] = 0$*.*

Proof. (1) follows from Zarhin's Theorem [58]. For (2) assume that E has complex multiplication by the ring of integers $\mathcal{O}_L$ of a quadratic imaginary field L, $[K : \mathbb{Q}] \leq 8$ and $p \geq 5$. To prove the desired result it will suffice to show that $E(LK_\infty)[p^\infty] = 0$.

We now use an idea similar to the proof of [59, lemma 3·5]. Let $\Delta := \mathrm{Gal}(L(E[p])/L)$. According to [53, Corollary 5·20(ii)] we have an isomorphism $\Delta \cong (\mathcal{O}_L/p\mathcal{O}_L)^\times$. As E has ordinary reduction at p, p splits in $L/\mathbb{Q}$. Whence we have $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$. Since $p \geq 5$, this implies that $\#\Delta \geq 16$. Combining this with the fact that $[K : \mathbb{Q}] \leq 8$ gives that $\Delta' := \mathrm{Gal}(LK(E[p])/LK)$ is a nontrivial group whose order is prime to p. As K_∞/K is pro-p, we may identify $\mathrm{Gal}(LK_\infty(E[p])/LK_\infty)$ with Δ'.

Now assume that $E(LK_\infty)[p^\infty] \neq 0$. Then by an appropriate choice of a $\mathbb{F}_p$-basis of $E[p]$ we have an injection from $\mathrm{Gal}(LK_\infty(E[p])/LK_\infty)$ to the subgroup of $GL_2(\mathbb{F}_p)$ consisting of

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

matrices of the form $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, where $\alpha \in \mathbb{F}_p$. But if $\alpha \neq 0$, then $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ generates a group of order p. It follows that $\mathrm{Gal}(LK_\infty(E[p])/LK_\infty) \cong \Delta'$ is trivial. This is a contradiction since Δ' is nontrivial of order prime to p by the above. □

4. *A control theorem for* $(X(E/K_\infty)_f)_{H_n} \to X(E/K_\infty^{H_n})_f$

In this section, for $H \in \mathcal{H}$, we study the kernels and cokernels of the maps $\theta_n : (X(E/K_\infty)_f)_{H_n} \to X(E/K_\infty^{H_n})_f$. The proof of a control theorem for this map is technically quite delicate.

First, we need:

PROPOSITION 4·1. *Let $H \in \mathcal{H}$ and let $n, m \geq 0$ be arbitrary integers. The maps (induced by the maps s_n in Proposition 2·8)*:

$$s'_{n,m} : \mathrm{Sel}_{p^\infty}(E/K_\infty^{H_n})/p^m \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n}/p^m$$

have finite kernel and cokernel and their orders are bounded independently of n and m.

Proof. For simplicity, let $S_n = \mathrm{Sel}_{p^\infty}(E/K_\infty^{H_n})$ and $S_\infty = \mathrm{Sel}_{p^\infty}(E/K_\infty)$. Moreover, we let $m \geq 0$ be arbitrary but fixed, and we abbreviate $s'_{n,m}$ to s'_n for convenience. Consider the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & p^m(S_\infty^{H_n}) & \longrightarrow & S_\infty^{H_n} & \longrightarrow & S_\infty^{H_n}/p^m & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \tilde{s}_n} & & \uparrow{\scriptstyle s_n} & & \uparrow{\scriptstyle s'_n} & & \\ 0 & \longrightarrow & p^m S_n & \longrightarrow & S_n & \longrightarrow & S_n/p^m & \longrightarrow & 0 \end{array}$$

By Proposition 2·8, coker s_n is finite and bounded independently of n. Since we have a surjection coker $s_n \twoheadrightarrow$ coker s'_n, therefore the same is true for coker s'_n.

By the snake lemma, we have an exact sequence $\ker s_n \to \ker s'_n \to \mathrm{coker}\, \tilde{s}_n$. Since $\ker s_n$ is finite and bounded independently of n by Proposition 2·8, therefore to show that $\ker s'_n$ is finite and bounded independently of n, we only need to show that coker $\tilde{s}_n$ is finite and bounded independently of n. To this end, note that $\mathrm{img}\, \tilde{s}_n = p^m \,\mathrm{img}\, s_n$. Therefore the multiplication by p^m map induces a surjection from coker s_n onto coker $\tilde{s}_n$. This implies that coker $\tilde{s}_n$ is finite and the order is bounded independently of n, because this property is true for coker s_n by Proposition 2·8. □

For $H \in \mathcal{H}$, we study the kernels and cokernels of the maps $\theta_n : (X(E/K_\infty)_f)_{H_n} \to X(E/K_\infty^{H_n})_f$. We want to show that $\ker \theta_n$ and coker θ_n are finite and bounded independently of n. In order to prove this, we require the following condition.

Condition $\mathcal{C}_{H,m}$: There is an $m > 0$ such that $X(E/K_\infty)[p^\infty] = X(E/K_\infty)[p^m]$ and that $X(E/K_\infty^{H_n})[p^\infty] = X(E/K_\infty^{H_n})[p^m]$ for all n.

At the end of this section, we shall show that this condition is met if $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$ and $E(K_\infty)[p^\infty]$ is finite.

PROPOSITION 4·2. *Let $H \in \mathcal{H}$. Assume that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$. Then the maps (induced by the dual of the maps s_n in Proposition 2·8)*

$$\theta_n : (X(E/K_\infty)_f)_{H_n} \to X(E/K_\infty^{H_n})_f$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

have finite kernels and cokernels. Furthermore, if condition $\mathcal{C}_{H,m}$ is met then the orders of these kernels and cokernels are bounded independently of n.

Proof. Assume that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$. For simplicity, let $F_n = K_\infty^{H_n}$. Fix $n \in \mathbb{N}$ and let $m > 0$ be such that $X(E/K_\infty)[p^\infty] = X(E/K_\infty)[p^m]$ and $X(E/F_n)[p^\infty] = X(E/F_n)[p^m]$. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} & & X(E/K_\infty)[p^m]_{H_n} & \longrightarrow & X(E/K_\infty)_{H_n} & \longrightarrow & (X(E/K_\infty)_f)_{H_n} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_n} & & \downarrow{\scriptstyle \hat{s}_n} & & \downarrow{\scriptstyle \theta_n} & & \\ 0 & \longrightarrow & X(E/F_n)[p^m] & \longrightarrow & X(E/F_n) & \longrightarrow & X(E/F_n)_f & \longrightarrow & 0 \end{array}$$

From the snake lemma applied to this diagram, we get an exact sequence

$$\ker \phi_n \to \ker \hat{s}_n \to \ker \theta_n \to \operatorname{coker} \phi_n \to \operatorname{coker} \hat{s}_n \to \operatorname{coker} \theta_n \to 0. \tag{3}$$

By Proposition 2·8, both $\ker \hat{s}_n$ and $\operatorname{coker} \hat{s}_n$ are finite. This, together with the exact sequence (3), implies that $\operatorname{coker} \theta_n$ is finite. Also since $\ker \hat{s}_n$ is finite, the exact sequence (3) shows that in order to show that $\ker \theta_n$ is finite it will suffice to show that $\operatorname{coker} \phi_n$ is finite. We now proceed to show this.

Since $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$ and H_n has finite index in H, therefore $(X(E/K_\infty)_f)_{H_n}$ is finitely generated over $\mathbb{Z}_p$. Therefore $\ker \theta_n$ is finitely generated over $\mathbb{Z}_p$. From this fact and the fact that $\operatorname{coker} \hat{s}_n$ is finite, we see from the exact sequence (3) that $\operatorname{coker} \phi_n$ is actually finite (it is finitely generated over $\mathbb{Z}_p$ and annihilated by p^m).

From now on suppose that condition $\mathcal{C}_{H,m}$ is met, and choose m accordingly. We want to show that the orders of $\ker \theta_n$ and $\operatorname{coker} \theta_n$ are bounded independently of n. By Proposition 2·8, the cardinalities of $\ker \hat{s}_n$ and $\operatorname{coker} \hat{s}_n$ are bounded independently of n. Therefore the exact sequence (3), implies that the order of $\operatorname{coker} \theta_n$ is bounded independently of n. Also since $\ker \hat{s}_n$ is finite and bounded independently of n, the exact sequence (3) shows that in order to show that the order of $\ker \theta_n$ is bounded independently of n, it will suffice to show that the order of $\operatorname{coker} \phi_n$ is bounded independently of n.

Dualising ϕ_n, we get

$$\hat{\phi}_n : \mathrm{Sel}_{p^\infty}(E/F_n)/p^m \to (\mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m)^{H_n}.$$

We will show that the order of $\ker \hat{\phi}_n$ is bounded independently of n. Consider the exact sequence:

$$0 \to p^m \mathrm{Sel}_{p^\infty}(E/K_\infty) \to \mathrm{Sel}_{p^\infty}(E/K_\infty) \to \mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m \to 0.$$

For any n, this sequence gives us an exact sequence

$$0 \to (p^m \mathrm{Sel}_{p^\infty}(E/K_\infty))^{H_n} \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n} \to (\mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m)^{H_n}.$$

Therefore we have an injection

$$\varphi_n : \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n}/(p^m \mathrm{Sel}_{p^\infty}(E/K_\infty))^{H_n} \hookrightarrow (\mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m)^{H_n}.$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

We define the map

$$\psi_n : \mathrm{Sel}_{p^\infty}(E/F_n)/p^m \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n}/(p^m \mathrm{Sel}_{p^\infty}(E/K_\infty))^{H_n}.$$

Since φ_n is an injection, therefore $\ker \psi_n = \ker(\varphi_n \circ \psi_n) = \ker \hat{\phi}_n$. So we see that we need to show that the order of $\ker \psi_n$ is bounded independently of n. Consider the exact sequence

$$0 \to \mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m] \to \mathrm{Sel}_{p^\infty}(E/K_\infty) \xrightarrow{\times p^m} p^m \mathrm{Sel}_{p^\infty}(E/K_\infty) \to 0.$$

This sequence induces an exact sequence

$$0 \to p^m(\mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n}) \to (p^m \mathrm{Sel}_{p^\infty}(E/K_\infty))^{H_n} \to H^1(H_n, \mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m]) \to 0.$$

We have a zero on the right because $H^1(H_n, \mathrm{Sel}_{p^\infty}(E/K_\infty)) = 0$ from Lemma 2·14. This exact sequence gives us an exact sequence

$$0 \to H^1(H_n, \mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m]) \to \frac{\mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n}}{p^m} \xrightarrow{\pi_n} \frac{\mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n}}{(p^m \mathrm{Sel}_{p^\infty}(E/K_\infty))^{H_n}} \to 0. \quad (4)$$

Let $s_n' : \mathrm{Sel}_{p^\infty}(E/F_n)/p^m \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n}/p^m$ be the map in Proposition 4·1. Then $\psi_n = \pi_n \circ s_n'$. It is easy to see that we have an exact sequence

$$0 \to \ker s_n' \to \ker \psi_n \to \ker \pi_n \to \mathrm{coker}\, s_n'.$$

Taking the exact sequence (4) into account, the above exact sequence becomes

$$0 \to \ker s_n' \to \ker \psi_n \to H^1(H_n, \mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m]) \to \mathrm{coker}\, s_n'.$$

Recall that $\ker \psi_n$ is finite for all n. We need to show its order is bounded. According to Proposition 4·1, both $\ker s_n'$ and $\mathrm{coker}\, s_n'$ are finite and bounded independently of n. Therefore by the above exact sequence, $H^1(H_n, \mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m])$ is finite for all n and we need to show that its order is bounded independently of n. The Pontryagin dual of $H^1(H_n, \mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m])$ is $(X(E/K_\infty)/p^m)^{H_n}$. Since $X(E/K_\infty)$ is finitely generated over the Noetherian ring Λ_2, therefore it follows that $X(E/K_\infty)/p^m$ is a Noetherian Λ_2-module. The Λ_2-submodules $(X(E/K_\infty)/p^m)^{H_n}$ form an increasing nested chain, the chain must stabilise and so the orders are bounded. This completes the proof. □

We now show;

PROPOSITION 4·3. *Let $H \in \mathcal{H}$. Assume that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$ and $E(K_\infty)[p^\infty]$ is finite. Then condition $\mathcal{C}_{H,m}$ is met.*

Proof. Let $H \in \mathcal{H}$ and assume that the hypotheses in the statement of the proposition are true. As usual, let $F_n = K_\infty^{H_n}$. From Lemma 2·10 we get that $X(E/F_n)$ is a torsion Λ_{K_n}-module for all n. From Theorem 3·4 it follows that there exists $t > 0$ such that for all n the maximal finite Λ_{K_n}-submodule of $X(E/F_n)$ is annihilated by p^t. Also since $X(E/K_\infty)$ is finitely generated over the Noetherian ring Λ_2, therefore $X(E/K_\infty)[p^\infty] = X(E/K_\infty)[p^m]$ for some $m \geq t$. We will show that $X(E/F_n)[p^\infty] = X(E/F_n)[p^{2m}]$ for all n.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

For any $n \geq 0$, let $Y(E/F_n) = X(E/F_n)/X(E/F_n)[p^m]$. Then we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X(E/K_\infty)[p^m]_{H_n} & \longrightarrow & X(E/K_\infty)_{H_n} & \longrightarrow & (X(E/K_\infty)_f)_{H_n} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_n} & & \downarrow{\scriptstyle \hat{s}_n} & & \downarrow{\scriptstyle \theta_n} & & \\ 0 & \longrightarrow & X(E/F_n)[p^m] & \longrightarrow & X(E/F_n) & \longrightarrow & Y(E/F_n) & \longrightarrow & 0 \end{array}$$

To see that the first map on the top row is an injection, we first note that since $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$ we have by Lemma 2·14 that $H_1(H_n, X(E/K_\infty)) = 0$. But $X(E/K_\infty)_f \cong p^m X(E/K_\infty)$ which is a submodule of $X(E/K_\infty)$. It follows that $H_1(H_n, X(E/K_\infty)_f) = 0$ because $cd_p(H_n) = 1$. This shows that the first map on the top row is in fact an injection. From the snake lemma applied to above diagram, we get an exact sequence

$$0 \to \ker \phi_n \to \ker \hat{s}_n \to \ker \theta_n \to \operatorname{coker} \phi_n \to \operatorname{coker} \hat{s}_n \to \operatorname{coker} \theta_n \to 0. \tag{5}$$

By Proposition 2·8, $\ker \hat{s}_n$ is finite. This, together with the exact sequence (5), implies that $\ker \phi_n$ is finite. Since $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$ and H_n has finite index in H, therefore $(X(E/K_\infty)_f)_{H_n}$ is finitely generated over $\mathbb{Z}_p$. Therefore, for all n, $\ker \theta_n$ is finitely generated over $\mathbb{Z}_p$. Combining this with the fact that $\operatorname{coker} \hat{s}_n$ is finite by Proposition 2·8, the exact sequence (5) shows that $\operatorname{coker} \phi_n$ is finitely generated over $\mathbb{Z}_p$ and hence is finite since the target group is annihilated by p^m.

So we have shown that the map

$$\phi_n : X(E/K_\infty)[p^m]_{H_n} \to X(E/F_n)[p^m]$$

has finite kernel and cokernel. In an identical way we can show that the map

$$\phi_n' : X(E/K_\infty)[p^\infty]_{H_n} \to X(E/F_n)[p^\infty]$$

has finite kernel and cokernel. Combining this with the fact that $X(E/K_\infty)[p^\infty] = X(E/K_\infty)[p^m]$, we get that $\mu_{G_n/H_n}(X(E/F_n)[p^\infty]) = \mu_{G_n/H_n}(X(E/F_n)[p^m])$.

Taking Lemma 2·1 into account, we have an exact sequence

$$0 \to \bigoplus_{i=1}^{s} \Lambda(G_n/H_n)/p^{m_i'} \to X(E/F_n)[p^\infty] \to B \to 0, \tag{6}$$

where B is finite. This exact sequence induces the sequence

$$0 \to \bigoplus_{i=1}^{s} (\Lambda(G_n/H_n)/p^{m_i'})[p^m] \to X(E/F_n)[p^m] \to B[p^m]. \tag{7}$$

Since we have $\mu_{G_n/H_n}(X(E/F_n)[p^\infty]) = \mu_{G_n/H_n}(X(E/F_n)[p^m])$ we see from the exact sequences (6) and (7) that we must have $m_i' \leq m$ for $i = 1, ..., s$.

The exact sequence (6) induces an exact sequence

$$0 \to A' \to X(E/F_n)[p^\infty] \to \bigoplus_{i=1}^{s} \Lambda(G_n/H_n)/p^{m_i'} \to B' \to 0, \tag{8}$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

where A' and B' are finite. By assumption, p^t annihilates A' and $m \geq t$. Also $m_i' \leq m$ for $i = 1, ..., s$. Therefore it follows that p^{2m} annihilates $X(E/F_n)[p^\infty]$, i.e. $X(E/F_n)[p^\infty] = X(E/F_n)[p^{2m}]$. This completes the proof. □

5. *μ-invariants and the $\mathfrak{M}_H(G)$-property*

In this section, we prove results that will help to establish the equivalences $(a) \Leftrightarrow (b) \Leftrightarrow (c)$ of Theorem 1·3. The first two results below are proven for H_{cyc} in [**10**] and our proofs will be very similar.

THEOREM 5·1. *For any $H \in \mathcal{H}$ we have*

$$\mu_G(X(E/K_\infty)) = \mu_{G/H}(X(E/K_\infty^H)) - \mu_{G/H}(H_0(H, X(E/K_\infty)_f)).$$

Also, if $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, then for all $n \geq 0$ we have

$$\mu_{G_n}(X(E/K_\infty)) = \mu_{G_n/H_n}(X(E/K_\infty^{H_n})).$$

Proof. We follow the proof of [**8**, proposition 2·12] closely. For simplicity, let $F_n = K_\infty^{H_n}$ with $F = F_0$. Also let $X_\infty = X(E/K_\infty)$. First, recall from [**27**, corollary 1·7] that if M is a finitely generated $\Lambda(G)$-module, then

$$p^{\mu_G(M)} = \prod_{i \geq 0} \#H_i(G, M[p^\infty])^{(-1)^i} = \chi(G, M[p^\infty]).$$

We have a similar formula when M is a finitely generated $\Lambda(G/H)$-module. From the Hochschild–Serre spectral sequence it is easy to prove that

$$\chi(G, X_\infty[p^\infty]) = \prod_{i=0,1} \chi(G/H, H_i(H, X_\infty[p^\infty]))^{(-1)^i}.$$

From this we get

$$\mu_G(X_\infty) = \mu_{G/H}(H_0(H, X_\infty[p^\infty])) - \mu_{G/H}(H_1(H, X_\infty[p^\infty])). \tag{9}$$

Consider the exact sequence

$$0 \to X_\infty[p^\infty] \to X_\infty \to X_{\infty,f} \to 0. \tag{10}$$

Since $cd_p(H) = 1$, therefore the functor $H_1(H, -)$ is left exact. On the other hand, one has that $X[p^\infty] \subseteq X_\infty$ and $X_{\infty,f} \cong p^t X_\infty \subseteq X_\infty$ for some big enough t. Therefore, combining the above observations with Lemma 2·14, we have that $H_1(H, X_\infty[p^\infty]) = H_1(H, X_{\infty,f}) = 0$. This fact implies that we have a short exact sequence

$$0 \to H_0(H, X_\infty[p^\infty]) \to H_0(H, X_\infty) \to H_0(H, X_{\infty,f}) \to 0. \tag{11}$$

Taking (9) into account, we obtain

$$\mu_G(X_\infty) = \mu_{G/H}(H_0(H, X_\infty)) - \mu_{G/H}(H_0(H, X_{\infty,f})). \tag{12}$$

But the quantity $\mu_{G/H}(H_0(H, X_\infty))$ is precisely $\mu_{G/H}(X(E/F))$ by virtue of the dual descent map $(X_\infty)_H \to X(E/F)$ having finite kernel and cokernel (cf. Proposition 2·8). Therefore we get the desired formula for $n = 0$.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Now assume that $X_{\infty,f}$ is finitely generated over $\Lambda(H)$. Then from Lemma 2·14 we get that $H_1(H_n, X_\infty) = 0$. Also, Lemma 2·10 gives that $X(E/F_n)$ is a torsion $\Lambda(G_n/H_n)$-module. Therefore, the same proof above may be adapted to show that for any $n \geq 0$ that

$$\mu_{G_n}(X_\infty) = \mu_{G_n/H_n}(X(E/F_n)) - \mu_{G_n/H_n}(H_0(H_n, X_{\infty,f})). \tag{13}$$

But since $X_{\infty,f}$ is finitely generated over $\Lambda(H)$ and H_n has finite index in H, therefore $(X_{\infty,f})_{H_n}$ is finitely generated over $\mathbb{Z}_p$. In particular, this quotient is a torsion $\Lambda(G_n/H_n)$-module and has μ_{G_n/H_n}-invariant zero. We see from this that the formula (13) becomes

$$\mu_{G_n}(X_\infty) = \mu_{G_n/H_n}(X(E/F_n)).$$

We also have kind of a converse to Theorem 5·1. □

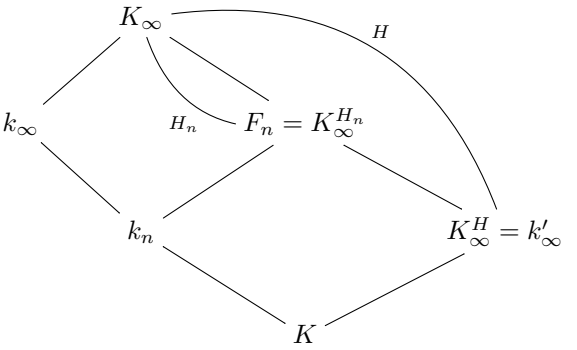
COROLLARY 5·2. *Let $H \in \mathcal{H}$. If $\mu_G(X(E/K_\infty)) = \mu_{G/H}(X(E/K_\infty^H))$, then $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$.*

Proof. According to the previous theorem, this equality implies that $\mu_{G/H}((X(E/K_\infty)_f)_H) = 0$. According to Proposition 2·8, the map $\alpha : X(E/K_\infty)_H \to X(E/K_\infty^H)$ has finite kernel and cokernel. Since by definition of $\mathcal{H}$, $X(E/K_\infty^H)$ is a torsion $\Lambda(G/H)$-module, we get that $X(E/K_\infty)_H$ is also a torsion $\Lambda(G/H)$-module. It follows that $(X(E/K_\infty)_f)_H$ is also a torsion $\Lambda(G/H)$-module. Therefore, since $\mu_{G/H}((X(E/K_\infty)_f)_H) = 0$, we get that $(X(E/K_\infty)_f)_H$ is finitely generated over $\mathbb{Z}_p$. This implies that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$. □

6. *Asymptotic growth of Iwasawa invariants*

In this section, we prove analogues of results of Cuoco on the asymptotic growth of Iwasawa invariants in $\mathbb{Z}_p^2$-extensions. These results are interesting in their own right, but they are also related to parts (*b*) and (*c*) of Theorem 1·3. We will use the main results of this section in the proof of Proposition 7·1.

First, we describe the basic setting from [**12**]. We choose two independent $\mathbb{Z}_p$-extensions k_∞ and k'_∞ of K (i.e., $k_\infty \cap k'_\infty = K$) such that $K_\infty = k_\infty \cdot k'_\infty$. Let k_n, $n \in \mathbb{N}$, be the unique subfield of k_∞ of degree p^n over K. Then we consider the sequence of $\mathbb{Z}_p$-extensions F_n/k_n, where we let $F_n = k'_\infty \cdot k_n$ for every $n \in \mathbb{N}$. In the notation of the introduction, $k_n = K_{H,n}$ and $F_n = K_\infty^{H_n}$, where $H_n = H^{p^n}$ and $H = \mathrm{Gal}(K_\infty/k'_\infty)$, and we have the following diagram of fields:



https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

The classical Iwasawa–Greenberg module attached to F_n (i.e., the projective limit of the ideal class groups of the intermediate number fields of the $\mathbb{Z}_p$-extension F_n/k_n), which will be denoted C_n for the moment, is a finitely generated and torsion $\Lambda_{K_{H,n}}$-module, where $\Lambda_{K_{H,n}} = \mathbb{Z}_p[[\mathrm{Gal}(F_n/k_n)]]$, as in the introduction. Therefore it makes sense to define μ- and λ-invariants for each C_n.

The main result of [12] describes the asymptotic growth of the μ- and the λ-invariants of the C_n:

THEOREM 6·1 (Cuoco). *In the above setting (in particular, $k'_\infty = K_\infty^H$), there exist constants l, m_0, m_1, c_1 and c_2 which are independent of n such that for all sufficiently large n,*

$$\mu(C_n) = m_0 p^n + m_1 n + c_1$$

and

$$\lambda(C_n) = l p^n + c_2.$$

Note that the base fields grow in the $\mathbb{Z}_p$-extensions F_n/k_n, and that these fields, and therefore also the Iwasawa invariants $\mu(C_n)$ and $\lambda(C_n)$, depend crucially on the fixed choice of the subgroup H of $G = \mathrm{Gal}(K_\infty/K)$.

In subsequent work, Cuoco was able to describe the arithmetic meaning of the constants m_0, m_1 and l, as follows. Let $C = C(K_\infty)$ be the projective limit of the ideal class groups of all intermediate number fields contained in the $\mathbb{Z}_p^2$-extension K_∞ of K. Then C is a finitely generated torsion Λ_2-module, and one defines the *generalised Iwasawa invariants* of C as follows (cf. [13, definitions 1·1 and 1·2]). Let $f_C \in \Lambda_2$ be the characteristic power series of C, and write $f_C = p^{m_0} \cdot g_C$, where g_C is not divisible by p. Then m_0 is nothing but the invariant $\mu_G(C)$, where $G = \mathrm{Gal}(K_\infty/K)$. Moreover, we consider the image $\overline{g_C}$ of g_C in the quotient Iwasawa algebra $\Omega_2 = \Lambda_2/p$. Then we let

$$l_0(C) = \sum_{\mathcal{P}} v_{\mathcal{P}}(\overline{g_C}),$$

where the sum runs over the prime ideals of the form $\mathcal{P} = (\overline{\sigma - 1}) \subseteq \Lambda_2$ for elements $\sigma \in G \setminus G^p$. Note that this is a finite sum, since the ring Ω_2 is a Noetherian UFD.

PROPOSITION 6·2 (Cuoco). *Let C be as above, and consider the constants from Theorem 6·1. Then*

$$m_0 = \mu_G(C), \quad l_0(C) = \sum_{H \subseteq G} m_1(H),$$

where $H \subseteq G$ runs over the subgroups of dimension 1 and $m_1(H)$ is the constant from Theorem 6·1, applied to $H = \mathrm{Gal}(K_\infty/k'_\infty)$. In particular, Cuoco has shown that $m_1(H)$ is zero for all but finitely many H.

If $C_f := C/C[p^\infty]$ is finitely generated over $\Lambda(H)$, then moreover the constant l from the second growth formula in Theorem 6·1 satisfies

$$l = \mathrm{rank}_{\Lambda(H)}(C_f).$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

In this section, we prove analogues of these results for Selmer groups. Recall the notion $\mathcal{H}$ from Definition 1·1. It will turn out that the validity of the $\mathfrak{M}_H(G)$-property for some $H \in \mathcal{H}$, i.e. the quotient $X(E/K_\infty)_f$ being finitely generated over $\Lambda(H)$, is equivalent to having a particularly uniform growth of the μ-invariants (see the remark after Theorem 8·1 below). In all what follows, we abbreviate $X(E/K_\infty)$ to X.

THEOREM 6·3. *Let E be an elliptic curve defined over K with good ordinary reduction at p, let K_∞ be a $\mathbb{Z}_p^2$-extension of K, and let $H \subseteq G$ be a subgroup of dimension* 1. *We let X_n be the Pontryagin dual of the Selmer group of E over the $\mathbb{Z}_p$-extension F_n/k_n, where k_n has degree p^n over K, $F_n = K_\infty^{H_n}$ and $F_n = k_n \cdot K_\infty^H$ for every n, as in the introduction.*

We assume that each X_n is a finitely generated torsion $\Lambda_n := \mathbb{Z}_p[[\mathrm{Gal}(F_n/k_n)]]$-module, and we identify each of these group rings with $\Lambda_1 = \mathbb{Z}_p[[T]]$. Then we can define μ- and λ-invariants of the X_n, which we will denote by μ_n and λ_n. Suppose that either of the following conditions hold:

(1) *$H \in \mathcal{H}$;*

(2) *$\mathcal{H} \neq \emptyset$ and the decomposition group $D_v \subseteq G$ of each of the primes v of K above p has $\mathbb{Z}_p$-rank two.*

Then the following assertions hold.

(*a*) *We have*

$$\mu_n = \mu_G(X)p^n + m_1 n + O(1) \tag{14}$$

and

$$\lambda_n = lp^n + O(1) \tag{15}$$

for suitable constants m_1 and l.

(*b*) *The parameter $m_1 = m_1(H)$ is zero for all but finitely many choices of H, and*

$$\sum_{H \subseteq G} m_1(H) = l_0(X),$$

where l_0 is defined as above and H runs over all dimension 1 subgroups of $G = \mathrm{Gal}(K_\infty/K)$, as in Proposition 6·2.

(*c*) *If X_f is finitely generated as a $\Lambda(H)$-module, then moreover*

$$l = \mathrm{rank}_{\Lambda(H)}(X_f).$$

Remark.

(1) We stress that the sum in (*b*) is taken over all $H \subseteq G$ of dimension 1, not only over $H \in \mathcal{H}$. This is one of two main reasons for us to prove the asymptotic formulas (14) and (15) also for $H \notin \mathcal{H}$ (under the assumption 2), although this will require to prove a stronger control theorem (see Proposition 6·8 below). The second motivation to study

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

also the case $H \notin \mathcal{H}$ comes from Section 10 below: we will apply Theorem 6·3 to the anticyclotomic $\mathbb{Z}_p$-extension K_{ac} of an imaginary quadratic number field. However, we cannot ensure that the corresponding subgroup H of G, fixing K_{ac}, is contained in $\mathcal{H}$, because some of the primes in S might split completely in K_{ac}. Therefore it will be very useful to have Theorem 6·3(a) available also for $H \notin \mathcal{H}$.

(2) If X_f is finitely generated as a $\Lambda(H)$-module, as in part (c) of the theorem, then the general hypothesis that each X_n is finitely generated and torsion over Λ_n is automatically satisfied, by Lemma 2·10.

(3) Suppose that $H \in \mathcal{H}$ and that X_f is finitely generated over $\Lambda(H)$. Then Theorem 5·1 implies that actually $\mu_n = \mu_G(X)p^n$, and in particular $m_1 = 0$, in equation (14). Moreover, we will show in Theorem 8·1 below that in this case $\lambda_n = lp^n$ in equation (15).

COROLLARY 6·4. *In the setting of Theorem 6·3, suppose that K_∞ contains only finitely many primes above p. If the λ-invariants of the $X(E/L)$, L running over all the $\mathbb{Z}_p$-extensions of K, are bounded, then $m_1(H) = 0$ for each $H \subseteq G$ of dimension* 1.

We will break up the proof of Theorem 6·3 and Corollary 6·4 into several lemmas. Fix the $\mathbb{Z}_p$-extensions $k_\infty = \bigcup k_n$ and $k'_\infty = K_\infty^H$, and suppose that the topological generators σ and τ of $G \cong \mathbb{Z}_p^2$ are chosen such that $H = \mathrm{Gal}(K_\infty/k'_\infty)$ is generated topologically by σ and $\mathrm{Gal}(K_\infty/k_\infty)$ is generated topologically by τ. Then $\Lambda(G) = \Lambda_2$ can be identified with the ring of formal power series $\mathbb{Z}_p[[T, U]]$ in two variables, where $U = \sigma - 1$ and $T = \tau - 1$.

The following two module-theoretic results are taken without changes from [**12**]. We must, however, warn the reader that Cuoco's notation differs from ours: in the current section (as in the whole paper) the subgroup H denotes the subgroup of $G = \mathrm{Gal}(K_\infty/K)$ which fixes k'_∞. In Cuoco's paper, H corresponds to the quotient group $\mathrm{Gal}(k'_\infty/K)$ instead.

We will use the following notation: for any $n \in \mathbb{N}$, we let

$$\eta_n = (U+1)^{p^n} - 1. \tag{16}$$

For two integers n and m with $n > m$, we define

$$\alpha_{n,m} = \frac{\eta_n}{\eta_m} = 1 + (U+1)^{p^m} + (U+1)^{p^{m+1}} + \cdots + (U+1)^{p^n}. \tag{17}$$

If m is fixed, then $\alpha_{n,m}$ is abbreviated to α_n.

LEMMA 6·5. *Let V be a finitely generated torsion Λ_2-module, and let N be a pseudo-null submodule. Suppose that $(V_n)_{n\in\mathbb{N}}$ is a family of submodules of V and that there exists an integer $n_0 \in \mathbb{N}$ such that the following hold for each integer $n \geq n_0$:*

(1) $V_n = \alpha_{n,n_0} \cdot V_{n_0}$, *and*

(2) $\eta_n \cdot V \subseteq V_n$.

Then $(N + V_n)/V_n$ is a finitely generated and torsion $\Lambda(G/H)$-module for each $n > n_0$, and the invariants $\mu_{G/H}((N+V_n)/V_n)$ and $\lambda_{G/H}((N+V_n)/V_n)$ become constant for sufficiently large n.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Proof. This is [**12**, lemma 2·8]. □

LEMMA 6·6. *Let W be a finitely generated and torsion Λ_2-module, and suppose that there exists an integer n_0 such that the quotient $W/\alpha_n W$ is a finitely generated and torsion $\Lambda(G/H)$-module for each $n > n_0$. Then there exist constants l, m_0, m_1, c_1 and c_2, independent of n, such that*

$$\mu_{G/H}(W/\alpha_n W) = m_0 p^n + m_1 n + c_1$$

and

$$\lambda_{G/H}(W/\alpha_n W) = l p^n + c_2$$

for each sufficiently large $n \in \mathbb{N}$. Here $m_0 = \mu_G(W)$ denotes the largest power of p which divides the characteristic power series of W in Λ_2.

Proof. This follows from [**12**, proposition 2·1 and remark on p. 430]. □

Now we prove the first part of Theorem 6·3, namely the existence of the asymptotic formulas in (*a*).

LEMMA 6·7. *There exist constants such that equations (14) and (15) hold.*

Proof. Fix a pseudo-isomorphism $\varphi : X \longrightarrow M$, where M is an elementary torsion Λ_2-module. We let N and R denote the kernel and the image of φ. Then N and M/R are pseudo-null Λ_2-modules.

Recall the definitions (16) and (17) of η_n and $\alpha_{n,0} = \eta_n/U$. Now we define $Y_n = \eta_n \cdot X$ for every $n \in \mathbb{N}$, and we let $W_n = \varphi(Y_n)$, $n \in \mathbb{N}$. Then

$$W_n = \alpha_{n,0} \cdot W_0$$

for each $n \in \mathbb{N}$, since φ is a Λ_2-module homomorphism. The map φ induces surjections

$$\overline{\varphi_n} : X/Y_n \twoheadrightarrow R/W_n$$

with kernel $(N + Y_n)/Y_n$ for each $n \in \mathbb{N}$.

We will prove a control theorem below (see Proposition 6·8) which is independent from the results of Cuoco and which implies that the kernels and the cokernels of the canonical maps

$$X/Y_n = X/\eta_n X \longrightarrow X(E/F_n) = X_n$$

are torsion $\mathbb{Z}_p[[T]]$-modules, where we recall that $X(E/F_n)$ denotes the Pontryagin dual of the Selmer group of E over $F_n = K_\infty^{H_n}$ (when $H \in \mathcal{H}$ it follows from Proposition 2·8 that the kernels and cokernels are even finite and of bounded order). In particular, since $X(E/F_n)$ is a torsion $\mathbb{Z}_p[[T]]$-module by assumption, the same holds true for the quotient X/Y_n, $n \in \mathbb{N}$. Therefore also R/W_n and $(N + Y_n)/Y_n$ (i.e. the kernel and the image of $\overline{\varphi_n}$) are torsion $\mathbb{Z}_p[[T]]$-modules. Moreover, the additivity of μ- and λ-invariants on short exact sequences of finitely generated torsion $\mathbb{Z}_p[[T]]$-modules imply that

$$\mu(X/Y_n) = \mu(R/W_n) + \mu((N + Y_n)/Y_n)$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

and

$$\lambda(X/Y_n) = \lambda(R/W_n) + \lambda((N + Y_n)/Y_n).$$

Now we can apply Lemma 6·5 in order to conclude that the μ-and λ-invariants of the quotients $(N + Y_n)/Y_n$ stabilise. Moreover,

$$\mu(R/W_n) = \mu(R/W_0) + \mu(W_0/\alpha_n W_0)$$

for every $n > 0$, and a similar equation holds for the λ-invariants.

Note that $W_0 \subseteq M$ is a finitely generated and torsion Λ_2-module, and $W_0/\alpha_n W_0 \subseteq R/W_n$ is a finitely generated and torsion $\mathbb{Z}_p[[T]]$-module for each $n > 0$. Therefore by Lemma 6·6 and the above we conclude that for sufficiently large n we have

$$\mu(X/Y_n) = \mu_G(X)p^n + m_1 n + c_1$$

and

$$\lambda(X/Y_n) = lp^n + c_2$$

for suitable constants m_1, l, c_1 and c_2.

By Proposition 6·8 we have that

$$|\lambda(X/Y_n) - \lambda(X_n)|$$

and

$$|\mu(X/Y_n) - \mu(X_n)|$$

are both bounded independently of n. Combining this fact with the equations for $\mu(X/Y_n)$ and $\lambda(X/Y_n)$ above, we get equations (14) and (15). □

The next result is a control theorem which works also if $H \notin \mathcal{H}$. For any n we let η_n be defined as in (16) and $\phi_n : X/\eta_n X \longrightarrow X_n$ to be the dual of the map (induced by restriction) $s_n : \mathrm{Sel}_{p^\infty}(E/F_n) \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{H_n}$.

PROPOSITION 6·8. *Suppose that the hypotheses from Theorem 6·3 hold. Then for any $n \geq 0$ the kernel and cokernel of the map $\phi_n : X/\eta_n X \longrightarrow X_n$ are finitely generated torsion $\mathbb{Z}_p[[T]]$-modules whose μ- and λ-invariants are bounded as n varies.*

Proof. If $H \in \mathcal{H}$, we get the desired result from Proposition 2·8. Otherwise if $H \notin \mathcal{H}$, we assume that $\mathcal{H} \neq \emptyset$ and that the decomposition group of any prime of K_∞ above p is an open subgroup of $\mathrm{Gal}(K_\infty/K)$. In this more general setting the only concern is that one has to take more care to prove that C_n and D_n (using the notation in the proof of Proposition 2·8) are finite when primes in $S_n \setminus S_{p,n}$ split completely in F_n/k_n and when not all primes in $S_{p,n}$ ramify in F_n/k_n.

Now consider the map

$$h_n : \bigoplus_{v \in S} J_v(E/F_n) \to \bigoplus_{v \in S} J_v(E/K_\infty).$$

By the proof of Proposition 2·8 we see that:

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

(1) the Pontryagin dual of $H^1(\mathrm{Gal}(K_\infty/F_n), E(K_\infty)[p^\infty])$ surjects onto coker ϕ_n;

(2) $\ker \phi_n$ injects into a quotient of the Pontryagin dual of $\ker h_n$.

Let γ be a topological generator of $\mathrm{Gal}(K_\infty/F_n)$. We have $H^1(\mathrm{Gal}(K_\infty/F_n), E(K_\infty)[p^\infty]) = E(K_\infty)[p^\infty]/(\gamma-1)E(K_\infty)[p^\infty]$. Therefore $\mathrm{corank}_{\mathbb{Z}_p}(H^1(\mathrm{Gal}(K_\infty/F_n), E(K_\infty)[p^\infty])) \leq 2$. It then follows from (1) above that coker ϕ_n is a torsion $\mathbb{Z}_p[[T]]$-module with $\mu = 0$ and $\lambda \leq 2$.

Now we may write $\ker h_n = \bigoplus_{v\in S} \ker h_{n,v}$. We now prove that $\ker \phi_n$ is a torsion $\mathbb{Z}_p[[T]]$-module whose μ- and λ-invariants are bounded as n varies. From (2) above it will suffice to show that for each $v \in S$ the Pontryagin dual of $\ker h_{n,v}$ is a torsion $\mathbb{Z}_p[[T]]$-module whose μ- and λ-invariants are bounded as n varies.

First, consider a prime $v \in S$ that does not divide p. Assume that v does not split completely in F/k. Then for any sufficiently large n, no prime of k_n above v splits completely in F_n/k_n. It follows then by the same argument as in Proposition 2·8 that we have that $\ker h_{n,v} = 0$.

Now assume that v splits completely in F/k. Let $n \geq 0$. We have that every prime of k_n above v splits completely in F_n/k_n. Recall from the introduction that we defined $J_v(E/F_n)$ as $J_v(E/F_n) = \varinjlim \bigoplus_{w|v} H^1(L_w, E)[p^\infty]$ where the direct limit runs over finite extensions L of k_n contained in F_n. Had there been a finite number of primes of F_n above v, we could then write $J_v(E/F_n) = \oplus_{w|v} H^1(F_{n,w}, E)[p^\infty]$, where the sum runs over all primes w of F_n above v. This was the case in the proof of Proposition 2·8 and so as in the proof we were able to express $\ker h_{n,v}$ as a finite direct sum of cohomology groups. However as v splits completely in F_n/k_n we cannot write $J_v(E/F_n)$ as a direct sum. This will make the expression of $\ker h_{n,v}$ more complicated. Let l be the rational prime below v. If L is a finite extension of $\mathbb{Q}_l$, then by Mattuck's theorem $E(L) \cong \mathbb{Z}_l^{[L:\mathbb{Q}_l]} \times T$ where T is a finite group. Since $l \neq p$, we get from this that $E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. Therefore we have an isomorphism $H^1(L, E)[p^\infty] \cong H^1(L, E[p^\infty])$. By taking direct limits, we have such an isomorphism for any algebraic extension L of $\mathbb{Q}_l$. Now let $\{F_{n,m}\}_{m\in\mathbb{N}}$ be the layers of the $\mathbb{Z}_p$-extension F_n/k_n. Using the isomorphism just mentioned as well as Shapiro's lemma we can write

$$\ker h_{n,v} = \varinjlim_m \bigoplus_{w_m|v} H^1(\mathrm{Gal}(K_{\infty,w_m}/(F_{n,m})_{w_m}), E(K_{\infty,w_m})[p^\infty]), \tag{18}$$

where the direct sum runs over the primes w_m of $F_{n,m}$ above v. In the above we have also written w_m for a fixed place of K_∞ above w_m. Now let $\{w_1', w_2', ..., w_c'\}$ be the set of primes of $F_{n,0} = k_n$ above v. Let $1 \leq i \leq c$. Since $k_{n,w_i'}$ is a finite extension of $\mathbb{Q}_l$ we have that $E(k_{n,w_i'})[p^\infty]$ is finite. So it follows by the same argument as in the proof of Proposition 2·8 that $H^1(\mathrm{Gal}(K_{\infty,w_i'}/k_{n,w_i'}), E(K_{\infty,w_i'})[p^\infty])$ is finite. We can write

$$H^1(\mathrm{Gal}(K_{\infty,w_i'}/k_{n,w_i'}), E(K_{\infty,w_i'})[p^\infty]) \cong \bigoplus_{j=1}^{t_i} \mathbb{Z}/p^{m_{i,j}}\mathbb{Z}. \tag{19}$$

For any $m \in \mathbb{N}$ and $w_m|w_0|v$, $H^1(\mathrm{Gal}(K_{\infty,w_m}/(F_{n,m})_{w_m}), E(K_{\infty,w_m})[p^\infty])$ is isomorphic to $H^1(\mathrm{Gal}(K_{\infty,w_0}/(F_{n,0})_{w_0}), E(K_{\infty,w_0})[p^\infty])$. Letting $U_{n,v}$ be the Pontryagin dual of $\ker h_{n,v}$ we therefore see that from (18), (19) and [**37**, corollary A·8] that we have an isomorphism

$$U_{n,v} \cong \bigoplus_{i=1}^{c} \Big(\bigoplus_{j=1}^{t_i} \mathbb{Z}_p[[T]]/p^{m_{i,j}} \Big).$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

We see from this that $U_{n,v}$ is a torsion $\mathbb{Z}_p[[T]]$-module with λ-invariant $\lambda_{n,v} = 0$ and μ-invariant $\mu_{n,v} = \sum_w \mathrm{ord}_p(\#H^1(\mathrm{Gal}(K_{\infty,w}/F_{n,w}), E(K_{\infty,w})[p^\infty]))$, where the sum runs over all the primes w of k_n dividing v (for any such w we have also written w for a fixed place of K_∞ (and F_n) above w). Since $\mathcal{H} \neq \emptyset$, therefore it follows that the decomposition group of a prime v of K_∞ in $\mathrm{Gal}(K_\infty/K)$ has $\mathbb{Z}_p$-rank at least one. So as v splits completely in F/k, it follows that the number of primes of k_n above v is bounded independently of n. Therefore we see from this that $\mu_{n,v}$ is bounded independently of n.

Now let $v \in S$ be a prime above p. By hypothesis, the decomposition group of any prime of K_∞ above p is an open subgroup of $\mathrm{Gal}(K_\infty/K)$. Therefore we can write $\ker h_{n,v} = \oplus_{w|v} \ker h_{n,w}$ where $h_{n,w} : H^1(F_{n,w}, E)[p^\infty] \to H^1(K_{\infty,w}, E)[p^\infty]$ is the restriction map (as above, we have also written w for a fixed place of K_∞ above w). We now determine the structure of $\ker h_{n,w}$ as a $\mathbb{Z}_p$-module for any such w above v. Let

$$\kappa_{n,w} : E(F_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(F_{n,w}, E[p^\infty]),$$
$$\kappa_w : E(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(K_{\infty,w}, E[p^\infty])$$

be the Kummer maps. Then the map $h_{n,w}$ is

$$h_{n,w} : H^1(F_{n,w}, E[p^\infty])/\mathrm{img}\ \kappa_{n,w} \to H^1(K_{\infty,w}, E[p^\infty])/\mathrm{img}\ \kappa_w.$$

Now let $C_w = \mathcal{F}(\bar{\mathfrak{m}})[p^\infty]$ where $\bar{\mathfrak{m}}$ is the maximal ideal of $\bar{K}_v$ and $\mathcal{F}$ is the formal group of E. The inclusion $C_w \subseteq E[p^\infty]$ induces maps

$$\lambda_{n,w} : H^1(F_{n,w}, C_w) \to H^1(F_{n,w}, E[p^\infty]),$$
$$\lambda_w : H^1(K_{\infty,w}, C_w) \to H^1(K_{\infty,w}, E[p^\infty]).$$

As $\mathcal{H} \neq \emptyset$, it follows from [7, Theorem 2·13] that the extension $K_{\infty,w}/K_v$ is deeply ramified in the sense of [7]. Therefore by [7, proposition 4·3] and the discussion proceeding it we have $\mathrm{img}\ \kappa_w = \mathrm{img}\ \lambda_w$ and $\mathrm{img}\ \kappa_{n,w} \subseteq \mathrm{img}\ \lambda_{n,w}$. Therefore $h_{n,w}$ can be viewed as the composition of the following maps:

$$a_{n,w} : H^1(F_{n,w}, E[p^\infty])/\mathrm{img}\ \kappa_{n,w} \to H^1(F_{n,w}, E[p^\infty])/\mathrm{img}\ \lambda_{n,w},$$
$$b_{n,w} : H^1(F_{n,w}, E[p^\infty])/\mathrm{img}\ \lambda_{n,w} \to H^1(K_{\infty,w}, E[p^\infty])/\mathrm{img}\ \lambda_w.$$

We will now show that $\ker a_{n,w}$ and $\ker b_{n,w}$ are both cofinitely generated over $\mathbb{Z}_p$.

First we deal with $\ker b_{n,w}$. Let $\tilde{E}$ be the reduction of E over the residue field of $\bar{K}_w$. The exact sequence

$$0 \to C_w \to E[p^\infty] \to \tilde{E}[p^\infty] \to 0$$

induces an exact sequence

$$0 \to \mathrm{img}\ \lambda_{n,w} \to H^1(F_{n,w}, E[p^\infty]) \to H^1(F_{n,w}, \tilde{E}[p^\infty]) \to 0.$$

The last map is surjective because $cd_p(F_{n,w}) \leq 1$ (see [48, Theorem 7·1·8(i)]). Similarly, we have an exact sequence

$$0 \to \mathrm{img}\ \lambda_w \to H^1(K_{\infty,w}, E[p^\infty]) \to H^1(K_{\infty,w}, \tilde{E}[p^\infty]) \to 0.$$

It follows that $\ker b_{n,w}$ is isomorphic to $H^1(\mathrm{Gal}(K_{\infty,w}/F_{n,w}), \tilde{E}[p^\infty])$ which is clearly cofinitely generated over $\mathbb{Z}_p$ with $\mathrm{corank}_{\mathbb{Z}_p}(\ker b_{n,w}) \leq 1$.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Now we deal with $\ker a_{n,w}$. Let L be a finite extension of K_v contained in $F_{n,w}$. First we note that Tate local duality [48, Theorem 7·2·6] together with the Weil pairing yields a non-degenerate pairing

$$\langle\ ,\ \rangle : H^2(L, T_p(C_w)) \times H^0(L, \tilde{E}[p^\infty]) \to \mathbb{Q}_p/\mathbb{Z}_p,$$

where $T_p(C_w)$ is the p-adic Tate module of C_w. If L'/L is a finite extension, let $\mathrm{res} : H^2(L, T_p(C_w)) \to H^2(L', T_p(C_w))$ be the restriction map and $\mathrm{cor} : H^0(L', \tilde{E}[p^\infty]) \to H^0(L, \tilde{E}[p^\infty])$ be the corestriction (norm) map. For $a \in H^2(L, T_p(C_w))$ and $b \in H^0(L', \tilde{E}[p^\infty])$ a property of Tate local duality gives $\langle \mathrm{res}\, a, b\rangle = \langle a, \mathrm{cor}\, b\rangle$. As above, we have maps

$$\kappa_L : E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(L, E[p^\infty]),$$
$$\lambda_L : H^1(L, C_w) \to H^1(L, E[p^\infty]).$$

For any Hausdorff abelian locally compact topological group A, let $\hat{A}$ denote its Pontryagin dual. Taking into account [7, proposition 4·5], the proof of [7, proposition 4·6] shows that we have an isomorphism $\theta_L : \mathrm{img}\, \lambda_L/\mathrm{img}\, \kappa_L \xrightarrow{\sim} \widehat{\tilde{E}(k_L)[p^\infty]}$ where k_L is the residue field of L. Taking into account the property of Tate local duality above and the description of the map θ_L we have an isomorphism

$$\mathrm{img}\, \lambda_{n,w}/\mathrm{img}\, \kappa_{n,w} \cong \varinjlim \mathrm{img}\, \lambda_L/\mathrm{img}\, \kappa_L \cong \varprojlim \widehat{\tilde{E}(k_L)[p^\infty]}.$$

The limits are taken over all finite extensions L/K_v inside $F_{n,w}/K_v$; the direct limits are taken with respect to restriction and inverse limits are taken with respect to corestriction. As $\varprojlim \tilde{E}(k_L)[p^\infty]$ is a pro-p procyclic group, it is a quotient of $\mathbb{Z}_p$ (see [51, proposition 2·7·1]). Therefore it follows from the isomorphism above that $\ker a_{n,w} = \mathrm{img}\, \lambda_{n,w}/\mathrm{img}\, \kappa_{n,w}$ is cofinitely generated over $\mathbb{Z}_p$ with $\mathrm{corank}_{\mathbb{Z}_p}(\ker a_{n,w}) \le 1$.

We get from the above that the kernel of $h_{n,w} = b_{n,w} \circ a_{n,w}$ is cofinitely generated over $\mathbb{Z}_p$ with $\mathrm{corank}_{\mathbb{Z}_p}(\ker h_{n,w}) \le 2$. By hypothesis, the decomposition group of any prime of K_∞ above p is an open subgroup of $\mathrm{Gal}(K_\infty/K)$. It follows that the number of primes w of F_n above v is finite and bounded by an integer $M > 0$. Therefore $\ker h_{n,v} = \bigoplus_{w|v} \ker h_{n,w}$ is cofinitely generated over $\mathbb{Z}_p$ with $\mathrm{corank}_{\mathbb{Z}_p}(\ker h_{n,v}) \le 2M$. We see from this that the Pontryagin dual of $h_{n,v}$ is a torsion $\mathbb{Z}_p[[T]]$-module with μ-invariant zero and λ-invariant at most $2M$. This completes the proof. □

In order to finish the proof of Theorem 6·3, it remains to prove the following

LEMMA 6·9. *The constants from Lemma 6·6 have the following arithmetic meaning:*

(*a*) *$m_1 = m_1(H)$ is zero for all but finitely many choices of the dimension 1 subgroup H of G, and the sum of the m_1-invariants equals $l_0(X)$;*

(*b*) *if X_f is finitely generated over $\Lambda(H)$, then $l = \mathrm{rank}_{\Lambda(H)}(X_f)$.*

Proof. Going through the proof of [15, Theorem 2·4], one sees that $m_1(H)$ can be described in a module-theoretic way, as follows: write the characteristic power series $f_X \in \Lambda_2$ of X as $f_\infty = p^{\mu_G(X)} \cdot g_\infty$, where $p \nmid g_\infty$, and consider the class $\overline{g_\infty}$ of g_∞ in $\Omega_2 = \Lambda_2/(p)$. Then we

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

let

$$l_H(X) = \sum_{\mathcal{P}} v_{\mathcal{P}}(\overline{g_\infty}),$$

where $\mathcal{P}$ runs over the primes of Ω_2 of the form $\mathcal{P} = (\overline{\sigma - 1})$, $\sigma \in H \setminus H^p$ (if $\overline{g_\infty} = \overline{0}$, then we define $l_H(X) = 0$). It has been shown in [**15**, Theorem 2·4] that

$$m_1(H) = l_H(X).$$

Assertion (*a*) now follows from [**14**, lemma 1].

In order to prove assertion (*b*), we assume that X is finitely generated over $\Lambda(H)$, and we recall that $H_n = H^{p^n}$ for each $n \in \mathbb{N}$. By a result of Harris (see [**26**]), we have the asymptotic formula

$$\operatorname{rank}_{\mathbb{Z}_p}((X_f)_{H_n}) = \operatorname{rank}_{\Lambda(H)}(X_f) \cdot p^n + O(1).$$

On the other hand, we have shown above that

$$\operatorname{rank}_{\mathbb{Z}_p}((X_f)_{H_n}) = \lambda(X_{H_n}) = \lambda(X/Y_n)$$

satisfies the growth formula (15). Comparing coefficients proves that $l = \operatorname{rank}_{\Lambda(H)}(X)$. □

This also concludes the *proof of Theorem 6·3*, since $W_0 \subseteq M$ is pseudo-isomorphic to X. Indeed, $W_0 = \varphi(Y_0)$ is pseudo-isomorphic to Y_0, and the latter is pseudo-isomorphic to X because the quotient X/Y_0 is a finitely generated torsion $\Lambda(G/H)$-module by the above, and thus is pseudo-null as a Λ_2-module.

Proof of Corollary 6·4. Following the proof of Monsky in [**47**], one can prove that the hypothesis from the corollary is equivalent to saying that $l_0(X) = 0$. The assertion therefore follows from Lemma 6·9(*a*). □

7. *Characteristic power series and λ-invariants*

The following short section is purely algebraic in nature. At the end of the section we apply results of Monsky to our setting. We begin the section with the following proposition that establishes a connection between parts (*a*) and (*d*) of Theorem 1·3. Let $X = X(E/K_\infty)$, and recall that $f_\infty = p^m \cdot g_\infty \in \Lambda(G)$ denotes the characteristic power series of X (and $p \nmid g_\infty$). We also recall that $\Lambda(G) \cong \mathbb{Z}_p[[T, U]]$, where the two topological generators $\sigma, \tau \in G$ correspond to $U + 1$ and $T + 1$.

PROPOSITION 7·1. *For any $H = \overline{\langle \sigma^a \tau^b \rangle} \in \mathcal{H}$, $X(E/K_\infty)_f$ is finitely generated as a $\Lambda(H)$-module if and only if either $g_\infty = 0$ or $g_\infty \neq 0$ and the image of g_∞ in Λ_2/p is not divisible by the coset of $\Upsilon := (1 + U)^a(1 + T)^b - 1$.*

Proof. Suppose first that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$ and $g_\infty \neq 0$. Then Theorem 5·1 implies that

$$\mu_{G_n}(X(E/K_\infty)) = \mu_{G_n/H_n}(X(E/K_\infty^{H_n}))$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

for every $n \geq 0$. It follows from Theorem 6·3 that $m_1(H) = 0$. As we have seen in the proof of Lemma 6·9(a), this means that the image of g_∞ in $\Omega_2 = \Lambda_2/p$ is not divisible by the coset of Υ.

On the other hand, suppose that the cosets of g_∞ and Υ in Ω_2 are relatively prime. If $g_\infty = 0$, then $X = X(E/K_\infty)$ is pseudo-null as a Λ_2-module. Therefore the quotient X_f of X is also pseudo-null, i.e. it has Krull dimension at most 1. Moreover, multiplication by p is injective on X_f by definition. Therefore X_f/p is finite by [**1**, corollary 11·9], i.e. in this case X_f is a finitely generated free $\mathbb{Z}_p$-module, and therefore in particular it is finitely generated as a $\Lambda(H)$-module.

Now we consider the case $g_\infty \neq 0$. Let W be an elementary torsion Λ_2-module attached to X_f. Then we have an exact sequence

$$0 \longrightarrow A \longrightarrow X_f \longrightarrow W, \tag{20}$$

where $A \subseteq X_f$ denotes the maximal pseudo-null submodule. Since multiplication by p is injective on $A \subseteq X_f$, it follows as in the first case that A is finitely generated over $\Lambda(H)$. On the other hand, Lemma 2·2 implies that X_f/Υ is a torsion $\Lambda(G/H)$-module, and we have seen in the proof of that lemma that the same follows for W/Υ. Since the coset of g_∞ in Ω_2 is not divisible by Υ, it is immediate that $\mu_{G/H}(W/\Upsilon) = 0$. Since W/Υ is a finitely generated and torsion $\Lambda(G/H)$-module, it follows from the general structure theory that W/Υ is a finitely generated $\mathbb{Z}_p$-module. Therefore W is finitely generated over $\Lambda(H)$, and it follows from the exact sequence (20) that the same holds true for X_f. □

For any $\alpha = [(a, b)] \in \mathbb{P}^1(\mathbb{Z}_p)$, we define $\Upsilon_\alpha = (1+U)^a(1+T)^b - 1$. With this definition, if M is a finitely generated torsion Λ_2-torsion module, we let $M_\alpha = M/\Upsilon_\alpha$. So M_α is a $\Lambda_2/\Upsilon_\alpha$-module. Let f_M be the characteristic power series of M. If $f_M \neq 0$, write $f_M = p^m g_M$ with $p \nmid g_M$. We have the following theorem of Monsky.

THEOREM 7·2. *Assume that $f_M \neq 0$. Let $\alpha \in \mathbb{P}^1(\mathbb{Z}_p)$ and assume that M_α is a torsion $\Lambda_2/\Upsilon_\alpha$-module. Then the following statements are equivalent*:

(*a*) *$\lambda(M_\beta)$ is unbounded as β runs over a neighbourhood of α;*

(*b*) *the image of g_M in Λ_2/p is divisible by the coset of Υ_α.*

Proof. See [**47**, Theorem 3·3]. □

From this theorem, we can easily show

PROPOSITION 7·3. *Assume that $f_\infty \neq 0$. Let $H = \overline{\langle \sigma^a \tau^b \rangle} \in \mathcal{H}$. Then $\lambda(X(E/L))$ is bounded in a neighbourhood of K_∞^H if and only if the image of g_∞ in Λ_2/p is not divisible by the coset of $(1+U)^a(1+T)^b - 1$.*

Proof. Let $H' \in \mathcal{H}$. According to Proposition 2·8, the kernel and cokernel of the map $X(E/K_\infty)_{H'} \to X(E/K_\infty^{H'})$ are finite. Therefore, considering both the domain and codomain as $\Lambda(G/H')$-modules, we see that their λ-invariants are the same. Taking Proposition 2·5 into account, the desired result follows from the previous theorem. □

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

8. *The $\Lambda(H)$-structure of $X(E/K_\infty)_f$ and proof of Theorem 1·3*

Let $H \in \mathcal{H}$. In this section, assuming that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, we determine its structure as a $\Lambda(H)$-module. Moreover, we glue together the results from the preceding sections to a proof of our main result.

The two key ingredients we need are Theorem 8·1 below and Proposition 4·2.

THEOREM 8·1. *Let $H \in \mathcal{H}$ and assume that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$. Then for any $n \geq 1$ we have*

$$\operatorname{rank}_{\mathbb{Z}_p}(X(E/K_\infty^{H_n})_f) = p^n \operatorname{rank}_{\mathbb{Z}_p}(X(E/K_\infty^{H})_f).$$

Proof. For simplicity, let $F_n = K_\infty^{H_n}$ with $F = F_0$. Note that since $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, therefore by Lemma 2·10, for any $n \geq 0$, $X(E/F_n)$ is a torsion Λ_{K_n}-module so $X(E/F_n)_f$ is a finitely generated $\mathbb{Z}_p$-module. This makes sense of the statement in the theorem. For any $n \geq 0$ the dual of the map s_n in Proposition 2·8 induces a map $\theta_n : (X(E/K_\infty)_f)_{H_n} \to X(E/F_n)_f$. As $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, Proposition 4·2 shows that $\ker \theta_n$ and $\operatorname{coker} \theta_n$ are finite. Therefore

$$\operatorname{rank}_{\mathbb{Z}_p}(X(E/F_n)_f) = \operatorname{rank}_{\mathbb{Z}_p}((X(E/K_\infty)_f)_{H_n}). \tag{21}$$

Since $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, it is finitely generated over $\Lambda(H_n)$ and from Lemma 2·14 we get that $H_1(H_n, X(E/K_\infty)) = 0$. Now, $X(E/K_\infty)_f \cong p^m X(E/K_\infty)$ for some $m > 0$ and so $X(E/K_\infty)_f$ is a submodule of $X(E/K_\infty)$. Therefore, $H_1(H_n, X(E/K_\infty)_f) = 0$ since $H_1(H_n, X(E/K_\infty)) = 0$ and $cd_p(H) = 1$. It then easily follows from this and the structure theorem of $X(E/K_\infty)_f$ as a $\Lambda(H_n)$-modules that

$$\operatorname{rank}_{\Lambda(H_n)}(X(E/K_\infty)_f) = \operatorname{rank}_{\mathbb{Z}_p}((X(E/K_\infty)_f)_{H_n}). \tag{22}$$

The theorem now follows from (21) and (22) because for any n we have

$$\operatorname{rank}_{\Lambda(H_n)}(X(E/K_\infty)_f) = p^n \operatorname{rank}_{\Lambda(H)}(X(E/K_\infty)_f). \qquad \square$$

Remark. Suppose that $H \in \mathcal{H}$ and that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, as in Theorem 8·1. Then Lemma 2·10 implies that $X(E/K_\infty^{H_n})$ is a torsion Λ_{K_n}-module for every $n \in \mathbb{N}$. Therefore it follows from Theorem 6·3 that

$$\operatorname{rank}_{\mathbb{Z}_p}(X(E/K_\infty^{H_n})_f) = p^n \cdot \operatorname{rank}_{\Lambda(H)}(X(E/K_\infty)_f) + O(1)$$

for every $n \in \mathbb{N}$. Theorem 8·1 provides a stronger statement, namely we get rid off the O(1) error term. This follows by combining the statement of the theorem with equations (21) and (22), both applied with $n = 0$.

In the introduction, we defined λ_H to be the λ-invariant of the $\Lambda(G/H)$-module $X(E/K_\infty^H)$. Note: If $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, it follows from Theorem 6·3(c) and Theorem 8·1 (alternatively, from the proof of Proposition 4·2) that

$$\lambda_H = \operatorname{rank}_{\Lambda(H)}(X(E/K_\infty)_f),$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

provided that the latter is finite. We can now prove the following:

THEOREM 8·2. *Assume that $E(K_\infty)[p^\infty]$ is finite and $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, then we have an injective $\Lambda(H)$-homomorphism*

$$X(E/K_\infty)_f \hookrightarrow \Lambda(H)^{\lambda_H}$$

with finite cokernel and a Λ_2-exact sequence

$$0 \to A \to X(E/K_\infty) \to \bigoplus_{i=1}^{s} \Lambda_2/f_i^{n_i} \oplus \bigoplus_{j=1}^{t} \Lambda_2/p^{m_j} \to B \to 0,$$

where $s \leq \lambda_H$, A and B are pseudo-null Λ_2-modules with A annihilated by some power of p, $f_i \in \Lambda_2 \setminus \Lambda(H)$ are irreducible power series and $\mu_G(X(E/K_\infty)) = \sum_{j=1}^{t} m_t$.

Proof. Assume that $E(K_\infty)[p^\infty]$ is finite and that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$. By Proposition 4·3 and Proposition 4·2 we get that the maps

$$\theta_n : (X(E/K_\infty)_f)_{H_n} \to X(E/K_\infty^{H_n})_f$$

have finite kernel and cokernel and their orders are bounded independently of n.

Recall that λ_H is the same as $\operatorname{rank}_{\mathbb{Z}_p}(X(E/K_\infty^H)_f)$. Taking into account Theorem 8·1, from the control theorem above we get that $(X(E/K_\infty)_f)_{H_n} \cong (\mathbb{Z}_p)^{p^n \lambda_H} \times C_n$ where C_n is finite. Because $\ker \theta_n$ has bounded order and $X(E/K_\infty^{H_n})_f$ is $\mathbb{Z}_p$-torsion-free, it follows that the order of C_n is bounded independently of n.

From the structure theorem of modules over $\Lambda(H)(\cong \mathbb{Z}_p[[X]])$, we see that $X(E/K_\infty)_f$ is pseudo-isomorphic to $\Lambda(H)^{\lambda_H}$. Since $X(E/K_\infty)_f$ is $\mathbb{Z}_p$-torsion-free, it cannot have any non-trivial finite submodules. So we have a $\Lambda(H)$-exact sequence

$$0 \to X(E/K_\infty)_f \to \Lambda(H)^{\lambda_H} \to C, \tag{23}$$

where C is finite. This proves the first statement.

Now we prove the second statement. First we note that $X(E/K_\infty)_f$ has no nonzero pseudo-null Λ_2-submodules. To see this, assume that G is a pseudo-null Λ_2-submodule of $X(E/K_\infty)_f$. Then G has Krull dimension at most one. Since multiplication by p is injective on $G \subseteq X(E/K_\infty)_f$, therefore by [**1**, Corollary 11·9] G/p is finite i.e. G is finitely generated over $\mathbb{Z}_p$. So G is torsion as a $\Lambda(H)$-module. The exact sequence (23) shows that $X(E/K_\infty)_f$ is $\Lambda(H)$-torsion free. Therefore $G = 0$.

Now we determine the structure of $X(E/K_\infty)_f$ as a Λ_2-module. Taking into account Lemmas 2·9 and 2·1, we have by [**5**, chapter VII, section 4·4 Theorem 5], that there exist irreducible power series $f_j \in \Lambda_2 \cong \mathbb{Z}_p[[T, U]]$, integers m_i, n_j and a Λ_2-exact sequence

$$0 \to W \to X(E/K_\infty)_f \to D \to 0,$$

where $W = \bigoplus_{i=1}^{s} \Lambda_2/f_i^{n_i}$ and D is a pseudo-null Λ_2-module. From the exact sequence (23) we have that $X(E/K_\infty)_f$ is $\Lambda(H)$-torsion free. This implies that for all i we have $f_i \notin \Lambda(H)$. Furthermore, the exact sequence (23) shows that $\operatorname{rank}_{\Lambda(H)}(X(E/K_\infty)_f) = \lambda_H$. Since for any i we have $\operatorname{rank}_{\Lambda(H)}(\Lambda_2/f_i^{n_i}) \geq 1$, therefore we see that $s \leq \lambda_H$.

Since both $X(E/K_\infty)_f$ and W are torsion Λ_2-modules and taking into account the fact shown above that $X(E/K_\infty)_f$ has no nonzero pseudo-null Λ_2-submodules, we also have a

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Λ_2-exact sequence

$$0 \to X(E/K_\infty)_f \to W \to D' \to 0, \tag{24}$$

where D' is a pseudo-null Λ_2-module.

The prime ideals of height one in the support of $X(E/K_\infty)[p^\infty]$ (which is only $\langle p\rangle$) are disjoint from the prime ideals of height one in the support of $X(E/K_\infty)_f$. Therefore as explained in [**48**, remark 2, p. 271] we have a Λ_2-pseudo-isomorphism $X(E/K_\infty) \sim X(E/K_\infty)[p^\infty] \oplus X(E/K_\infty)_f$. From this we see that the second statement of the theorem follows from the exact sequence (24). The fact that the pseudo-null Λ_2-module A is annihilated by a power of p can be seen as follows: Let $\pi(A)$ be the image of A under the projection map $\pi : X(E/K_\infty) \to X(E/K_\infty)_f$. Then $\pi(A)$ is a pseudo-null submodule of $X(E/K_\infty)_f$. Since as shown above $X(E/K_\infty)_f$ has no nonzero pseudo-null Λ_2-submodules, therefore $\pi(A) = 0$. This implies that the group A in the second statement is contained in $X(E/K_\infty)[p^\infty]$ and hence is annihilated by a power of p. □

We need one last result:

THEOREM 8·3. *Assume that $\mathcal{H}$ is not empty. If $E(K)[p] = 0$, then $X(E/K_\infty)$ has no nontrivial pseudo-null Λ_2-submodules.*

Proof. This theorem follows from the work of Greenberg [**21**]. See [**38**, proposition 6·1] for details. □

Proof of Theorem 1·3. $X(E/K_\infty)$ is Λ_2-torsion by Lemma 2·9.

$(a) \Rightarrow (b)$ and (c) Lemma 2·10 and Theorem 5·1, noting that, since $\Lambda(G)$ is a free $\Lambda(G_n)$-module of rank p^n, we have $p^n \mu_G(X(E/K_\infty)) = \mu_{G_n}(X(E/K_\infty))$.

$(b) \Rightarrow (a)$ Corollary 5·2

$(c) \Rightarrow (b)$ Clear

$(f) \Rightarrow (a)$ Clear.

$(a) \Leftrightarrow (d)$ Proposition 7·1.

$(d) \Leftrightarrow (e)$ If $f_\infty = g_\infty \neq 0$ use Proposition 7·3. If $f_\infty = 0$, then $X(E/K_\infty)$ is a pseudo-null Λ_2-module. As in the proof of Proposition 7·1, this implies that $X(E/K_\infty)_f \subseteq X(E/K_\infty)$ is a finitely generated free $\mathbb{Z}_p$-module; we let r denote its rank. For any $H \in \mathcal{H}$ we have that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$. Proposition 4·2 implies that the restriction map $\theta_0 : (X(E/K_\infty)_f)_H \longrightarrow X(E/K_\infty^H)_f$ has finite kernel and cokernel. In particular, $\operatorname{rank}_{\mathbb{Z}_p}(X(E/K_\infty^H)_f) = r$ for each $H \in \mathcal{H}$. Taking Proposition 2·5 into account, we get (e).

Assuming that $E(K_\infty)[p^\infty]$ is finite we get

$(a) \Rightarrow (f)$ Theorem 8·2.

The statement about pseudo-null submodules is Theorem 8·3. □

Proof of Proposition 1·4. Let $\Omega_2 = \Lambda_2/p\Lambda_2 (\cong \mathbb{F}_p[[T, U]])$. This is a UFD, so by Theorem 1·3(d), we only need to prove the following statement: if $[(a,b)]$ and $[(c,d)]$ are two distinct elements of $\mathbb{P}^1(\mathbb{Z}_p)$, then $\sigma^a\tau^b - 1$ and $\sigma^c\tau^d - 1$ are relatively prime elements of Ω_2. This can be proven in the same way as Lemma 2·4. □

9. *Bounding ranks*

In the next two sections, we derive the applications of our main theorem which we announced in the introduction. We consider an imaginary quadratic base field K, so that

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

the $\mathbb{Z}_p^2$-extension K_∞/K is just the composite of all $\mathbb{Z}_p$-extensions of K. In this section we prove Theorem 1·5 on Mazur's Conjecture. First we need

LEMMA 9·1. *If L/K is a $\mathbb{Z}_p$-extension with $X(E/L)$ a torsion Λ-module, then the rank of E is bounded in L/K.*

Proof. Let L_n be a tower field of the extension L/K with corresponding subgroup Γ_n. Since $\mathrm{rank}_{\mathbb{Z}_p}(X(E/L)_{\Gamma_n})$ is bounded independently of n and we have an injection $E(L_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathrm{Sel}_{p^\infty}(E/L_n)$, it suffices to show that the map $s_n : \mathrm{Sel}_{p^\infty}(E/L_n) \to \mathrm{Sel}_p(E/L)^{\Gamma_n}$ has finite kernel. $\ker s_n$ is contained in the kernel of the map $g_n : H^1(L_n, E[p^\infty]) \to H^1(L, E[p^\infty])^{\Gamma_n}$. We have

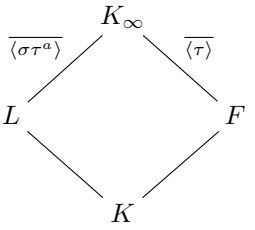
$$\ker g_n = H^1(\Gamma_n, E(L)[p^\infty]) = \mathrm{coker}\,(E(L)[p^\infty] \xrightarrow{\gamma-1} E(L)[p^\infty]),$$

where γ is a topological generator of Γ_n. This group is finite because $\ker\,(E(L)[p^\infty] \xrightarrow{\gamma-1} E(L)[p^\infty]) = E(K)[p^\infty]$ is finite. □

Proof of Theorem 1·5. The proof uses a technique from the paper of Bloom and Gerth [**4**]. Let $H \in \Sigma$ and denote K_∞^H by F. We must show that $t \le \lambda_H$. First we note that the rank of E stays bounded in F. This follows from Lemma 9·1 since $X(E/F)$ is a torsion Λ-module (because $H \in \mathcal{H}$). Now we make the following claim: It suffices to show that the number of $\mathbb{Z}_p$-extensions disjoint from F where the rank of E does not stay bounded is at most λ_H. To see this, suppose that we have $\lambda_H + 1$ $\mathbb{Z}_p$-extensions of K $L_1, L_2, ..., L_{\lambda_H+1}$, where the rank of E does not stay bounded. By what we just mentioned, none of these extensions equals F. Therefore $\bigcup_{i=1}^{\lambda_H+1}(F \cap L_i) = K_m$ where K_m is a finite extension of K. Now for each $i = 1, ..., \lambda_H + 1$ let $L_i' = L_i K_m$. Then the fields L_i' are $\lambda_H + 1$ $\mathbb{Z}_p$-extensions of K_m that are disjoint from F/K_m and the rank of E does not stay bounded in each L_i'. However, the proof below can easily be adapted replacing K by K_m to show that the number of $\mathbb{Z}_p$-extension of K_m inside K_∞ disjoint from F/K_m where the rank of E does not stay bounded is at most λ_H. This proves the claim.

By the claim above and Lemma 9·1, we only need to show that the number of $\mathbb{Z}_p$-extensions L/K disjoint from F where $\mathrm{rank}_\Lambda(X(E/L)) > 0$ is at most λ_H. Choose σ and τ to be topological generators of $G = \mathrm{Gal}(K_\infty/K)$ such that $H = \mathrm{Gal}(K_\infty/F)$ is topologically generated by τ. Then the $\mathbb{Z}_p$-extensions of K disjoint from F are the fixed fields of $\overline{\langle \sigma\tau^a\rangle}$ for $a \in \mathbb{Z}_p$. The Iwasawa algebra $\Lambda(G)$ is isomorphic to $\mathbb{Z}_p[[T, U]]$ via an isomorphism that takes σ to $U + 1$ and τ to $T + 1$.

Let L/K be a $\mathbb{Z}_p$-extension disjoint from F with $\mathrm{rank}_\Lambda(X(E/L)) > 0$. L is the fixed field of $\overline{\langle \sigma\tau^a\rangle}$ for $a \in \mathbb{Z}_p$:



https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Consider the map $s : \mathrm{Sel}_{p^\infty}(E/L) \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{\overline{\langle \sigma\tau^a \rangle}}$. We have that $\ker s$ is contained in

$$H^1(\mathrm{Gal}(K_\infty/L), E(K_\infty)[p^\infty]) = \ker\left(H^1(L, E[p^\infty]) \to H^1(K_\infty, E[p^\infty])\right).$$

As $H^1(\mathrm{Gal}(K_\infty/L), E(K_\infty)[p^\infty]))$ is clearly cofinitely generated over $\mathbb{Z}_p$, it follows that $\ker s$ is also cofinitely generated over $\mathbb{Z}_p$. Dualising everything, we get that the cokernel of the map $\hat{s} : X(E/K_\infty)/(\sigma\tau^a - 1)X(E/K_\infty) \to X(E/L)$ is finitely generated over $\mathbb{Z}_p$. Since $\mathrm{rank}_\Lambda(X(E/L)) > 0$, therefore the $\mathbb{Q}_p$-vector space $X(E/L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ has infinite dimension so

$$(X(E/K_\infty)_f/(\sigma\tau^a - 1)X(E/K_\infty)_f) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong (X(E/K_\infty)/(\sigma\tau^a - 1)X(E/K_\infty)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

has infinite dimension as well.

Since $H \in \Sigma$, therefore $X(E/K_\infty)_f/(\sigma\tau^a - 1)X(E/K_\infty)_f$ is a finitely generated $\Lambda(H)$-module and by the above we see that it must have positive $\Lambda(H)$-rank. Let $Q(\Lambda(H))$ be the field of fractions of $\Lambda(H)$ and $V(E/K_\infty) = X(E/K_\infty)_f \otimes_{\Lambda(H)} Q(\Lambda(H))$. So we see that there must be nonzero $z \in V(E/K_\infty)$ such that

$$0 = (\sigma\tau^a - 1)z = [(1+U)(1+T)^a - 1]z.$$

This implies

$$Uz = [(1+T)^{-a} - 1]z.$$

Thus $(1+T)^{-a} - 1$ is an eigenvalue of the endomorphism U of the $Q(\Lambda(H))$-vector space $V(E/K_\infty)$. So if L is the fixed field of $\overline{\langle \sigma\tau^a \rangle}$ and $\mathrm{rank}_\Lambda(X(E/L)) > 0$, then $(1+T)^{-a} - 1$ is an eigenvalue of the endomorphism U of $V(E/K_\infty)$. The number of eigenvalues is at most $\dim_{Q(\Lambda(H))}(V(E/K_\infty))$ and so to complete the proof it will suffices to show that $\dim_{Q(\Lambda(H))}(V(E/K_\infty)) \leq \lambda_H$. Under the assumption that $E(K_\infty)[p^\infty]$ is finite, this would follow from Theorem 1·3(f). However the condition that $E(K_\infty)[p^\infty]$ is finite is not needed, since Proposition 4·2 shows that the map $\theta : (X(E/K_\infty)_f)_H \to X(E/K_\infty^H)_f$ has finite kernel. Therefore, $\mathrm{rank}_{\Lambda(H)}(X(E/K_\infty)_f) \leq \lambda_H$. This completes the proof. □

We end this section by making some observations about Mazur's conjecture (listed in the introduction) in the cases when $\mathrm{rank}(E(K)) = 0, 1$. First, we list a few useful relations that we will need. Let $E^{(K)}$ be the quadratic twist of E by K. From [**49**, lemma 3·1] we have

$$\mathrm{rank}(E(K)) = \mathrm{rank}(E(\mathbb{Q})) + \mathrm{rank}(E^{(K)}(\mathbb{Q})). \tag{25}$$

If p is odd, we have

$$\mathrm{Sel}_{p^\infty}(E/K) \cong \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \oplus \mathrm{Sel}_{p^\infty}(E^{(K)}/\mathbb{Q}), \tag{26}$$

$$Ш(E/K)[p^\infty] \cong Ш(E/\mathbb{Q})[p^\infty] \oplus Ш(E^{(K)}/\mathbb{Q})[p^\infty]. \tag{27}$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

If p is odd and $\mathbb{Q}_{cyc}$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, then the extensions $\mathbb{Q}_{cyc}/\mathbb{Q}$ and $K/\mathbb{Q}$ are disjoint. Therefore we may identify the Galois groups $\mathrm{Gal}(\mathbb{Q}_{cyc}/\mathbb{Q}) = \mathrm{Gal}(K_{cyc}/K) = \Gamma_{cyc}$. Similar to (26), we get from loc. cit. the following

LEMMA 9·2. *Assume that p is odd. Then we have an isomorphism of Γ_{cyc}-modules*

$$\mathrm{Sel}_{p^\infty}(E/K_{cyc}) \cong \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{cyc}) \times \mathrm{Sel}_{p^\infty}(E^{(K)}/\mathbb{Q}_{cyc}).$$

Also, we have the following relationship between L-functions

$$L(E_K, s) = L(E, s)L(E^{(K)}, s). \tag{28}$$

If $\mathrm{Sel}_{p^\infty}(E/K)$ is finite, then the above relations together with the proven parity conjecture ([16]) allow us to deduce that the root number of $L(E_K, s)$ is 1 as follows: First, by (26) both $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ and $\mathrm{Sel}_{p^\infty}(E^{(K)}/\mathbb{Q})$ are finite. Then from [16, Theorem 1·4] we have that the root numbers of $L(E,s)$ and $L(E^{(K)}, s)$ are both 1. It then follows from (28) that the root number of $L(E_K, s)$ is also 1.

We will continue to assume that E has good ordinary reduction at p. In the $\mathrm{rank}(E(K)) = 0$ case we have the following theorem.

THEOREM 9·3. *Assume that p is odd. If $\mathrm{rank}(E(K)) = 0$ and $Ш(E/K)[p^\infty]$ is finite, then Mazur's conjecture is true.*

Proof. We have that $\mathrm{Sel}_{p^\infty}(E/K)$ is finite. As explained above this implies that the root number of $L(E_K, s)$ is 1. So Mazur's conjecture predicts that in this case the rank of E stays bounded along every $\mathbb{Z}_p$-extension of K.

We now show this. Let L be a $\mathbb{Z}_p$-extension of K with $\Gamma = \mathrm{Gal}(L/K)$. By Mazur's control theorem ([44] or [19, Theorem 1·2]) the map (induced by restriction)

$$\mathrm{Sel}_{p^\infty}(E/K) \to \mathrm{Sel}_{p^\infty}(E/L)^\Gamma$$

has finite kernel and cokernel. Therefore, as $\mathrm{Sel}_{p^\infty}(E/K)$ is finite, it follows that $\mathrm{Sel}_{p^\infty}(E/L)^\Gamma$ is finite. This implies by the structure theorem for $X(E/L)$ as a Λ-module that $X(E/L)$ is a torsion Λ-module. The desired result then follows from Lemma 9·1. □

Now we deal with the case $\mathrm{rank}(E(K)) = 1$. In this case, we combine results of Kundu–Ray [39] together with Theorem 1·5 to prove Mazur's conjecture under various assumptions. Let us first fix some notation. For an elliptic curve $E'/\mathbb{Q}$, let $R_p(E'/\mathbb{Q})$ be the p-adic regulator. Recall that if $\mathrm{rank}(E'(\mathbb{Q})) = 0$, then $R_p(E'/\mathbb{Q}) = 1$. Also, for any rational prime l we let $c_l(E')$ be the Tamagawa number of E' at l. Let N be the conductor of E. The result in this case is

THEOREM 9·4. *Assume that p is odd and unramified in $K/\mathbb{Q}$. Also assume that $\mathrm{rank}(E(K)) = 1$, $Ш(E/K)[p^\infty] = 0$, $v_p(R_p(E/\mathbb{Q})R_p(E^{(K)}/\mathbb{Q})) \leq 1$ and all the primes dividing N split in $K/\mathbb{Q}$. Furthermore, suppose that p does not divide any of the following:*

(1) $\prod_l c_l(E) \cdot c_l(E^{(K)})$;
(2) $\#\tilde{E}(\mathbb{F}_p) \cdot \#\tilde{E}^{(K)}(\mathbb{F}_p)$.

Then Mazur's conjecture is true.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Proof. Note that $\text{rank}(E(K)) = 1$ implies by (25) that $\text{rank}(E'(\mathbb{Q})) = 1$ for precisely one of $E' = E$ or $E^{(K)}$. Therefore $v_p(R_p(E/\mathbb{Q})R_p(E^{(K)}/\mathbb{Q})) \leq 1$ is the same as saying that $v_p(R_p(E'/\mathbb{Q})) \leq 1$.

Since all the primes dividing N split in $K/\mathbb{Q}$, therefore the root number of $L(E_K, s)$ is -1. So Mazur's conjecture predicts that in this case the rank of E stays bounded along every $\mathbb{Z}_p$-extension of K except the anticyclotomic one. Let K_{ac} be the anticyclotomic $\mathbb{Z}_p$-extension of K with tower fields $K_{ac,n}$. Using Theorem 1·4 of [**56**] together with the main result of [**3**] it follows that $\text{rank}(E(K_{ac,n})) = p^n + O(1)$, so the rank of E is in fact unbounded along the anticyclotomic $\mathbb{Z}_p$-extension of K.

Let $E_1, E_2 \in \{E, E^{(K)}\}$ with $\text{rank}(E_1(\mathbb{Q})) = 1$ and $\text{rank}(E_2(\mathbb{Q})) = 0$. Taking (27) into account, the conditions of the theorem together with [**39**, theorems 3·7 and 3·13] imply that $\text{Sel}_{p^\infty}(E_2/\mathbb{Q}_{cyc}) = 0$ and the Pontryagin dual of $\text{Sel}_{p^\infty}(E_1/\mathbb{Q}_{cyc})$ has μ-invariant zero and λ-invariant one. Therefore by Lemma 9·2 $\mu(X(E/K_{cyc})) = 0$ and $\lambda(X(E/K_{cyc})) = 1$. The fact that $\mu(X(E/K_{cyc})) = 0$ implies by Proposition 2·8 that $X(E/K_\infty)_{H_{cyc}}$ is finitely generated over $\mathbb{Z}_p$. So $X(E/K_\infty)$ is finitely generated over $\Lambda(H_{cyc})$ whence also $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H_{cyc})$. Therefore by Theorem 1·5 the number of $\mathbb{Z}_p$-extensions of K where the rank of E does not stay bounded is at most $\lambda(X(E/K_{cyc})) = 1$. This completes the proof. □

We now list some examples satisfying Theorem 9·4. The following computations were done in SAGE [**54**].

(1) Let $E = 43a1$ (Cremona labeling [**11**]) and $K = \mathbb{Q}(\sqrt{-3})$. One can choose $p = 11, 13, 17, 19$.
(2) Let $E = 58a1$ and $K = \mathbb{Q}(\sqrt{-7})$. One can choose $p = 5, 11, 13, 17$.
(3) Let $E = 61a1$ and $K = \mathbb{Q}(i)$. One can choose $p = 5, 11, 17, 19$.

10. *Deriving the triviality of the μ-invariant for the cyclotomic $\mathbb{Z}_p$-extension from the vanishing of the μ-invariant for the anticyclotomic one*

In this section we let K_∞ be the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field K. Recall that $K_{cyc}, K_{ac} \subseteq K_\infty$ denote the cyclotomic and anticyclotomic $\mathbb{Z}_p$-extensions of K. The main goal of this section is to prove Theorem 10·8, which establishes a connection between the $\mathfrak{M}_H(G)$-conjecture and Greenberg's Conjecture from the introduction.

We begin this section by recalling the definition of the component group and Tamagawa number of an abelian variety (at a prime).

Definition 10·1 Let A be an abelian variety defined over L, a finite extension of $\mathbb{Q}_p$ (p a prime), let $\mathcal{A}$ be the Néron model of A over the ring of integers of L and let k be the residue field of L. Let $\mathcal{A}_k$ be the special fiber of $\mathcal{A}$ and $\mathcal{A}_k^0$ its connected component of the identity. The group $\Phi_A = \mathcal{A}_k/\mathcal{A}_k^0$ of connected components is a finite étale group scheme over k. This group scheme is called the *component group* of A, and the *Tamagawa number* of A is $c_A = \#\Phi_A(k)$.

Now suppose that A is an abelian variety over a number field L, then for any non-archimedean prime v of L the Tamagawa number of A at v, denoted $c_{A,v}$ or simply c_v, is the Tamagawa number of A_{L_v}, where L_v is the completion of L at v.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

PROPOSITION 10·2. *Let A be an abelian variety defined over L, a finite extension of $\mathbb{Q}_p$ (p some prime). If L'/L is an unramified extension, k' the residue field of L' and $G = \mathrm{Gal}(L'/L)$, then: $H^1(G, A(L')) = H^1(G, \Phi_A(k'))$.*

Proof. See [44, proposition 4·3]. □

Let $H_{cyc} = \mathrm{Gal}(K_\infty/K_{cyc})$, $H_{ac} = \mathrm{Gal}(K_\infty/K_{ac})$, $\Gamma_{cyc} = \mathrm{Gal}(K_{cyc}/K)$ and $\Gamma_{ac} = \mathrm{Gal}(K_{ac}/K)$. We denote the Iwasawa algebras of Γ_{cyc} and Γ_{ac} by Λ_{cyc} and Λ_{ac}, respectively. Let $X(E/K_{ac})$ be the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/K_{ac})$ and let N be the conductor of E. We say that (E, p) satisfies $(\star)$ if N is relatively prime to the discriminant of K and for any prime v of K lying above a rational prime q dividing N that is inert in $K/\mathbb{Q}$ we have $p \nmid c_v$.

PROPOSITION 10·3. *Assume that (E, p) satisfies $(\star)$ and that $X(E/K_{ac})$ is a torsion Λ_{ac}-module. Then $\mu_{\Gamma_{ac}}(X(E/K_{ac})) = 0$ implies that $\mu_G(X(E/K_\infty)) = 0$.*

Proof. Assume that (E, p) satisfies $(\star)$, $X(E/K_{ac})$ is a torsion Λ_{ac}-module and $\mu_{\Gamma_{ac}}(X(E/K_{ac})) = 0$. Let L/K be a finite subextension of K_∞/K disjoint from K_{ac}/K. We define $L_{ac} := LK_{ac}$ and identify Γ_{ac} with $\mathrm{Gal}(L_{ac}/L)$. Let $H = \mathrm{Gal}(L_{ac}/K_{ac})$. By a similar line of proof as [22, corollary 3·4] we now show that $X(E/L_{ac})$ is a torsion Λ_{ac}-module with $\mu = 0$. We claim that the map $\phi : \mathrm{Sel}_{p^\infty}(E/K_{ac}) \to \mathrm{Sel}_{p^\infty}(E/L_{ac})^H$ has finite kernel and cokernel.

For this proof we fix S to be the set of all primes of K dividing Np. We first note that since all primes of K above p ramify in K_{ac}/K, there are a finite number of primes of K_{ac} above p. Also by [2, Theorem 2] there are a finite number of primes of K_{ac} above any prime l dividing N that splits in $K/\mathbb{Q}$. However any prime v of K lying over a prime l dividing N that is inert in $K/\mathbb{Q}$ will split completely in K_{ac}/K. Let $\{K_{ac,m}\}_{m\in\mathbb{N}}$ be the tower fields of the $\mathbb{Z}_p$-extension K_{ac}/K and let S'_m be the set of primes of $K_{ac,m}$ lying above a prime l dividing N that is inert in $K/\mathbb{Q}$. From the previous observations it follows as in the proof of Proposition 2·8 (see also the case when a prime v of k splits completely in F/k in the proof of Proposition 6·8), that to prove the claim, it will suffice to show that for any $m \in \mathbb{N}$ and any prime $w \in S'_m$ we have that $H^1(\mathrm{Gal}(L_{ac,w}/(K_{ac,m})_w), E(L_{ac,w})[p^\infty]) = 0$, where we have also written w for a fixed prime of L_{ac} above w.

Let $m \in \mathbb{N}$ and $w \in S'_m$. By [7, proposition 4·1] it follows that

$$H^1(\mathrm{Gal}(L_{ac,w}/(K_{ac,m})_w), E(L_{ac,w})[p^\infty]) = H^1(\mathrm{Gal}(L_{ac,w}/(K_{ac,m})_w), E(L_{ac,w})).$$

By Proposition 10·2,

$$\begin{aligned} H^1(\mathrm{Gal}(L_{ac,w}/(K_{ac,m})_w), E(L_{ac,w})) &= H^1(\mathrm{Gal}(L_{ac,w}/(K_{ac,m})_w), \Phi_E(l_w)) \\ &= H^1(\mathrm{Gal}(L_{ac,w}/(K_{ac,m})_w), \Phi_E(l_w)[p^\infty]), \end{aligned}$$

where l_w is the residue field. The last equality follows from the fact that $\mathrm{Gal}(L_{ac,w}/(K_{ac,m})_w)$ is pro-p. Since (E, p) satisfies $(\star)$, therefore $\Phi_E(l_w)[p^\infty]^{\mathrm{Gal}(L_{ac,w}/K_w)} = \Phi_E(k_w)[p^\infty] = 0$ (k_w be the residue field of K_w). Therefore $\Phi_E(l_w)[p^\infty] = 0$ and so $H^1(\mathrm{Gal}(L_{ac,w}/(K_{ac,m})_w), E(L_{ac,w})[p^\infty]) = H^1(\mathrm{Gal}(L_{ac,w}/(K_{ac,m})_w), \Phi_E(l_w)[p^\infty]) = 0$ as desired. Thus we have now shown that $\ker\phi$ and $\mathrm{coker}\,\phi$ are finite.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Since $X(E/K_{ac})$ is a torsion Λ_{ac}-module with $\mu = 0$, therefore it is a finitely generated $\mathbb{Z}_p$-module. So since coker ϕ is finite, this implies that the H-coinvariants of $X(E/L_{ac})$ are finitely generated over $\mathbb{Z}_p$. Therefore by Nakayama's lemma $X(E/L_{ac})$ is finitely generated over $\mathbb{Z}_p[H]$. In particular, $X(E/L_{ac})$ is finitely generated over $\mathbb{Z}_p$. This implies that $X(E/L_{ac})$ is a torsion Λ_{ac}-module with $\mu = 0$.

As K_∞ contains K_{cyc}, therefore by Proposition 2·6 it follows that $\mathcal{H} \neq \emptyset$. Also by [**46**, lemma 3·1], the decomposition group of any prime w of K_∞ above p is an open subgroup of $\mathrm{Gal}(K_\infty/K)$. These facts allow us to apply Theorem 6·3. In the notation of Theorem 6·3 what we proved above gives that $\mu_n = 0$ for all n. Therefore by equation (14) we can conclude that $\mu_G(X(E/K_\infty)) = 0$ as desired. □

We now need the following important theorem on the vanishing of the μ-invariant of $X(E/K_{ac})$ which is due to Pollack and Weston.

THEOREM 10·4. *Let $p \geq 5$ be a prime where E has good ordinary reduction and assume that the discriminant of K is relatively prime to pN. Write $N = N^+N^-$ where all the prime divisors of N^+ (respectively N^-) are split (respectively inert) in $K/\mathbb{Q}$. Assume that N^- is a squarefree product of an odd number of primes. Furthermore, suppose that*

(1) If $p \geq 7$, then $E[p]$ is an irreducible $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$-module and if $p = 5$, then $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$.

(2) If $q \mid N^-$ and $q \equiv \pm 1 \pmod p$, then q ramifies in $\mathbb{Q}(E[p])/\mathbb{Q}$.

(3) $a_p \not\equiv \pm 1 \pmod p$.

Then $X(E/K_{ac})$ is a torsion Λ_{ac}-module with μ-invariant zero.

Proof. See [**50**, Theorem 1·1] and [**31**, corollary 2·3]. □

LEMMA 10·5. *Assume that $p \geq 5$. Let q be a rational prime dividing N that is unramified in $K/\mathbb{Q}$. The following are equivalent:*

(a) The Kodaira type of E at q is I_n with $p \mid n$;

(b) q does not ramify in $\mathbb{Q}(E[p])/\mathbb{Q}$;

(c) $p \mid c_v$ for any prime v of K above q.

Proof. From [**29**, Theorem 1·1] we get the equivalence of (a) and (b). By [**55**, p. 448] we have that $p \mid c_v$ if and only if the Kodaira type of E and v is I_m with $p \mid m$. Therefore the equivalence of (a) and (c) follows from [**30**, table 1 on p. 556-557]. □

From Theorem 10·4 and Lemma 10·5 we get

COROLLARY 10·6 *Let $p \geq 5$ be a prime where E has good ordinary reduction and assume that the discriminant of K is relatively prime to pN. Write $N = N^+N^-$ where all the prime divisors of N^+ (respectively N^-) are split (respectively inert) in $K/\mathbb{Q}$. Assume that N^- is a squarefree product of an odd number of primes. Furthermore, suppose that*

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

(1) If $p \geq 7$, then $E[p]$ is an irreducible $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$*-module and if $p = 5$, then* $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$*;*

(2) N^- is the product of all primes q dividing N such that the Kodaira type of E at q is I_n with $p \nmid n$;

(3) $a_p \not\equiv \pm 1 \pmod p$.

Then $X(E/K_{ac})$ is a torsion Λ_{ac}-module with μ-invariant zero. Moreover, (E, p) satisfies $(\star)$, i.e. for any prime v of K dividing N^- we have $p \nmid c_v$.

Combining the above corollary with Proposition 10·3 and Theorem 1·3, we get:

THEOREM 10·7 *Suppose the assumptions of Corollary* 10·6 *are met, and further assume that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H_{cyc})$. Then $\mu_{\Gamma_{cyc}}(X(E/K_{cyc})) = 0$.*

We can now prove the following result, which we alluded to in the introduction.

THEOREM 10·8. *Assume that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H_{cyc})$ for all quadratic imaginary fields K, all elliptic curves $E/\mathbb{Q}$ and all primes $p \geq 5$. Under this assumption, let $p \geq 5$ be a prime and $E/\mathbb{Q}$ an elliptic curve with conductor N having good ordinary reduction at p. Suppose that*

(1) If $p \geq 7$, then $E[p]$ is an irreducible $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$*-module and if $p = 5$, then* $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$

(2) The number of primes q dividing N, such that the Kodaira type of E at q is I_n with $p \nmid n$ is odd

(3) $a_p \not\equiv \pm 1 \pmod p$

Then $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{cyc})$ is Λ-cotorsion with μ-invariant zero. Here, $\mathbb{Q}_{cyc}$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Proof. $X(E/\mathbb{Q}_{cyc})$ is a torsion Λ_{cyc}-module by the results of Kato [**32**] and Rohrlich [**52**]. Under the assumptions in the statement of the theorem, let N^- be the product of all primes q dividing N such that the Kodaira type of E at q is I_n with $p \nmid n$. Let $N^+ = N/N^-$. We may apply the Chinese remainder theorem to obtain an imaginary quadratic field K such that all the prime divisors of N^+ (respectively N^-) are split (respectively inert) in $K/\mathbb{Q}$. The desired result now follows from Theorem 10·7 and Lemma 9·2. □

11. *Shifting the $\mathfrak{M}_H(G)$-property*

In this final section we prove a result on the shifting of the $\mathfrak{M}_H(G)$-conjecture. Let K_∞ be a $\mathbb{Z}_p^2$-extension of a number field K, and let E be an elliptic curve defined over K. If $p = 2$, then we will always assume K to be totally imaginary. In this section, we want to derive from the $\mathfrak{M}_H(G)$-property for E over K (i.e. the condition that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$, $H = \mathrm{Gal}(K_\infty/K_{cyc})$) that the same property holds for each suitable finite p-extension K' of K such that $K' \cap K_\infty = K$ (for the hypotheses which have to be satisfied we refer to Theorem 11·9 below).

The main result of this section is Theorem 11·9 where we consider, more generally, arbitrary groups $H \in \mathcal{H}$ instead of $H = \mathrm{Gal}(K_\infty/K_{cyc})$ (here $\mathcal{H}$ is defined as in the introduction),

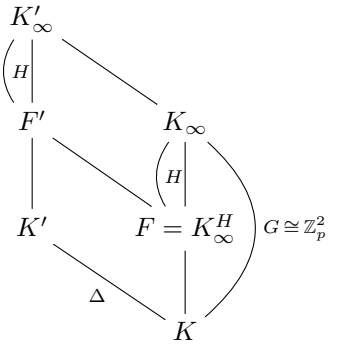
https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

i.e. we do not assume that K_∞ contains K_{cyc}. To this end, we use the equivalent formulations of the $\mathfrak{M}_H(G)$-property from Theorem 1·3, and in particular parts (b) and (e): under the hypothesis that the λ-invariants of the Pontryagin duals $X(E/L)$ are bounded as L runs over the $\mathbb{Z}_p$-extensions of K which are contained in K_∞ and coincide with $F = K_\infty^H$ up to at least a certain layer, we want to prove that a similar statements holds true for the shifted $\mathbb{Z}_p$-extensions L'/K', where $L' = L \cdot K'$. Alternatively, under the assumption that $\mu_G(X(E/K_\infty)) = \mu(X(E/F))$, we prove that an analogous equality holds for $F' \subseteq K'_\infty$.

The task of shifting the $\mathfrak{M}_H(G)$-property turned out to be much more involved than we would have thought at first glance. We cannot prove this result without assuming that several additional hypotheses are satisfied. In the course of the proof we will explain where these hypotheses are used.

In the following, we denote by Δ the Galois group of K' over K, which is a finite p-group. As in the introduction, we denote by $\mathcal{E}^{\subseteq K_\infty}(K)$ the set of all $\mathbb{Z}_p$-extensions of K which are contained in K_∞.

We summarise the fields under consideration in the following diagram.



We start with the following lemma.

LEMMA 11·1. *Suppose that Δ is a finite p-group. There exists a neighbourhood $U \subseteq \mathcal{E}^{\subseteq K_\infty}(K)$ of F such that the kernel and the cokernel of the natural map*

$$s_L : \mathrm{Sel}_{p^\infty}(E/L) \longrightarrow \mathrm{Sel}_{p^\infty}(E/L')^\Delta$$

are finite and of bounded order as L runs over the elements in U.

Proof. Since $H \in \mathcal{H}$, we know that no prime of S splits completely in F/K and that every prime of K above p ramifies in F/K. We therefore can pick a layer F_n $(n > 0)$ such that the primes of F_n above S do not split at all in F/F_n and that every prime of K above p ramifies in F_n/K. Let U contain only the $\mathbb{Z}_p$-extensions $L \subseteq K_\infty$ of K which coincide with F at least up to layer $n+1$. Then for any $L \in U$ we have:

(1) the number of primes of L above S is finite and bounded on U;

(2) every prime of K above p ramifies in L/K.

Taking into account the properties (1) and (2) above, we see by arguments similar to those used in the proof of Proposition 2·8, using the snake lemma, that it suffices to bound the cohomology groups $H^i(\Delta, E(L')[p^\infty])$ for $i = 1, 2$, and the local cohomology groups

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

$H^1(L'_w/L_v, A)$ where $w \mid v$ runs over the primes of L' and L above S, $A = E(L'_w)[p^\infty]$ if w does not lie above p and $A = \tilde{E}(l'_w)[p^\infty]$ if w does lie above p; here l'_w is the residue field of L'_w.

Now each of the groups $E(L')[p^\infty]$ is cofinitely generated over $\mathbb{Z}_p$ of rank at most two. Since all the cohomology groups $H^i(\Delta, E(L')[p^\infty])$ are annihilated by $|\Delta|$, it follows that each of these cohomology groups is actually finite, and that their orders are bounded as L runs over the elements from U. A similar argument shows that $H^1(L'_w/L_v, A)$ is finite of bounded order. □

Dualising, we obtain the following:

COROLLARY 11·2. *Let $m \in \mathbb{N}$, and let U be as in Lemma 11·1. Then the kernels and the cokernels of the maps*

$$\varphi_L : X(E/L')_\Delta \longrightarrow X(E/L)$$

are finite and of bounded order as L runs over the elements in U.

In what follows, we will repeatedly use the following auxiliary result. The main reason for hypothesis (3) in Theorem 11·9 is that we cannot prove the following technical result without posing additional assumptions on Z, and condition (3) seems the most natural condition under which this result holds true (cf. also the remark after Lemma 11·3).

LEMMA 11·3. *Let Z be a $\mathbb{Z}_p[\Delta]$-module such that $pZ = 0$, and write $|\Delta| = p^r$. Assume that Z_Δ is finite. Then Z is finite and*

$$v_p(|Z|) \leq p^r v_p(|Z_\Delta|). \tag{29}$$

Proof. Choose $x_1, x_2, ..., x_n \in Z$ such that their images in Z_Δ form an $\mathbb{F}_p$-basis of Z_Δ. Then by Nakayama's lemma $x_1, x_2, ..., x_n$ generate Z as an $\mathbb{F}_p[\Delta]$-module. Since $|\Delta| = p^r$, the result follows. □

Remark. If $pZ \neq 0$, then the statement of Lemma 11·3 is wrong in general. In fact, the cardinality of Z can be arbitrarily large even if we fix the cardinality of Z_Δ, by the following example.[1]

Suppose that $|\Delta| = p$, let σ be a generator of Δ, and write

$$N = \sigma^{p-1} + \sigma^{p-2} + \cdots + \sigma + 1$$

for the norm element in the group ring $\mathbb{Z}_p[\Delta]$. Now let $t \in \mathbb{N}$ be arbitrary but fixed, and define

$$Z := \mathbb{Z}_p[\Delta]/(p^t, N).$$

Since $\mathbb{Z}_p[\Delta]/(N)$ is a free $\mathbb{Z}_p$-module of rank $p-1$, the cardinality of Z is equal to $p^{t(p-1)}$, i.e. $|Z| \to \infty$ as $t \to \infty$. On the other hand, we have

$$Z_\Delta = \mathbb{Z}_p[\Delta]/(p^t, \sigma - 1, N) = \mathbb{Z}_p[\Delta]/(p^t, \sigma - 1, p)$$

[1] We are grateful to Cornelius Greither for explaining this example to us.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

for any t, since $N \equiv p (\mathrm{mod}\ \sigma - 1)$. This shows that the cardinality of the quotient of coinvariants is equal to p for any t.

In other words, although the cardinality of Z_Δ is fixed, the cardinality of Z can be arbitrarily large without further information on the action of Δ on Z. This is why we stick to the $pZ = 0$ case in all what follows.

Using the arguments from Proposition 4·1, we immediately derive from Corollary 11·2 the following special case of the main result of this section.

THEOREM 11·4 *Let K'/K and K_∞/K be as above (in particular, we assume that $H = \mathrm{Gal}(K_\infty/F)$ is contained in $\mathcal{H}$), and suppose that $\mu(X(E/F)) = 0$. Recall that E has good and ordinary reduction at the primes above p. For any $\mathbb{Z}_p$-extension $L \in U$ of K, we write $L' = LK'$.*

Then $X(E/L')$ is Λ-torsion and $\mu(X(E/L'))$ vanishes for each $L \in U$, and there exists some constant $C \in \mathbb{N}$ such that

$$\lambda(X(E/L')) \leq C$$

for each $L \in U$.

Proof. Write

$$\mathrm{rank}_p(N) = \dim_{\mathbb{F}_p}(N/pN)$$

for every abelian group N such that the quotient N/p is finite. It follows from Corollary 11·2 that the kernels and the cokernels of the maps

$$\overline{\varphi_L} : (X(E/L')_\Delta)/p \longrightarrow X(E/L)/p$$

are bounded as L runs over the elements from U. Since $X(E/F)$ is Λ-torsion and $E(F)[p^\infty]$ is finite because $H \in \mathcal{H}$, it follows from [**34**, Theorem 4·5] that there exist constants $C_1, C_2 \in \mathbb{N}$ such that the cardinalities of the kernels and cokernels of the natural maps

$$s_{L,n} : \mathrm{Sel}_{p^\infty}(E/L^{H_{L,n}}) \longrightarrow \mathrm{Sel}_{p^\infty}(E/L)^{H_{L,n}}$$

are bounded by C_1 and C_2 for each $n \in \mathbb{N}$ and for every $L \in U$, where we denote by $H_{L,n}$ the Galois group $\mathrm{Gal}(L/K)^{p^n} = \mathrm{Gal}(L/L_n)$ over the n-th intermediate layer, respectively. In [**34**, Theorem 4·5] this is phrased in terms of so-called *Fukuda modules*. For the purpose of this paper it suffices to think of a Fukuda module as a collection of Iwasawa modules along a $\mathbb{Z}_p$-extension (e.g. the Pontryagin duals of the Selmer groups of E along the layers of a $\mathbb{Z}_p$-extension L/K) for a which a control theorem holds.

If $U = \mathcal{E}(K_\infty, m)$ and $n \leq m$, then $L_n = F_n$ equals the n-th intermediate layer of the $\mathbb{Z}_p$-extension F/K, and therefore

$$\mathrm{rank}_p(X(E/L_n)) = \mathrm{rank}_p(X(E/F_n)) \leq \mathrm{rank}_p(X(E/F)) + C_3$$

for each $L \in U$ and some fixed constant C_3. Now we use [**34**, Corollary 3·8] (applied to $A = X(E/L)$ and $I = (p) \subseteq \Lambda$, respectively) in order to deduce that $\mathrm{rank}_p(X(E/L))$ is finite and bounded for each $L \in U$, provided that this neighbourhood is sufficiently small. Therefore $X(E/L)$ is Λ-torsion and $\mu(X(E/L)) = 0$ for each $L \in U$. Moreover, since

$$(X(E/L')_\Delta)/p = (X(E/L')/p)_\Delta,$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

it follows from Corollary 11·2 and Lemma 11·3 that $\mathrm{rank}_p(X(E/L'))$ is bounded as L runs over the elements from U. This implies that $X(E/L')$ is Λ-torsion and $\mu(X(E/L'))=0$ for each of these L, and that $\lambda(X(E/L'))$ remains bounded. Indeed, if Z denotes any finitely generated and torsion Λ-module such that $\mathrm{rank}_p(Z)$ is finite, and if E_Z denotes an elementary Λ-module attached to Z, then $\mathrm{rank}_p(E_Z)$ is also finite, and

$$\mathrm{rank}_p(E_Z) \leq \mathrm{rank}_p(Z)$$

(see [**33**, proposition 3·4]). Note that $\mathrm{rank}_p(E_Z)$ is finite if and only if $\mu(Z)=0$, and in this case we have $\mathrm{rank}_p(E_Z)=\lambda(Z)$. □

We want to prove a similar result which also holds in situations where the μ-invariant of $X(E/F)$ is not trivial. In this case we cannot consider p-ranks because the quotient $X(E/F)/p$ will not longer be finite. However, we can exploit the Galois module structure of our Iwasawa modules. Recall that $K' \cap K_\infty = K$. Therefore the extension K'_∞/K is abelian with Galois group isomorphic to

$$G \times \Delta,$$

where $G = \mathrm{Gal}(K'_\infty/K')$ can be identified with $\mathrm{Gal}(K_\infty/K)$. Similarly,

$$\mathrm{Gal}(L'/K) \cong \Gamma_L \times \Delta$$

for each $L \in U$, where $\Gamma_L = \mathrm{Gal}(L/K) \cong \mathbb{Z}_p$. This implies that the map φ_L from Corollary 11·2 is a homomorphism of Λ-modules (the action of Δ commutes with the G-action). As in Proposition 4·1, we may thus derive the following

COROLLARY 11·5. *Let $m \in \mathbb{N}$, let $\nu \in \Lambda$ be an arbitrary element, and let U be as in Lemma 11·1. Then the kernels and the cokernels of the maps*

$$\overline{\varphi_L} : (X(E/L')_\Delta)/\nu \longrightarrow X(E/L)/\nu$$

are finite and of bounded order as L runs over the elements in U. The upper bounds for the cardinalities do not depend on the choice of ν.

We are now ready to prove the main ingredient of our shifting result.

THEOREM 11·6. *Let K'/K and K_∞/K be as above (in particular, we recall that $\Delta = \mathrm{Gal}(K'/K)$ has order p^r), and let E be an elliptic curve defined over K. For any $\mathbb{Z}_p$-extension L of K, we write $L' = L \cdot K'$. We assume that E has good ordinary reduction at the primes above p, and that $F = K_\infty^H$ is a $\mathbb{Z}_p$-extension of K inside K_∞. Suppose that $H \in \mathcal{H}$, and that $X(E/F')$ is Λ-torsion.*

We assume that

$$X(E/K_\infty)[p^\infty] = X(E/K_\infty)[p] \quad \text{and} \quad X(E/K'_\infty)[p^\infty] = X(E/K'_\infty)[p].$$

Then there exists a neighbourhood $U \subseteq \mathcal{E}^{\subseteq K_\infty}(K)$ of F such that

$$\mu(X(E/L')) \leq p^r \cdot \mu(X(E/L))$$

for all but finitely many $L \in U$.

If moreover $X(E/F')[p^\infty] = X(E/F')[p]$, then

$$\mu(X(E/F')) \leq p^r \cdot \mu(X(E/F)).$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Proof. We will use Corollary 11·5 with the choice

$$\nu = \nu_{m,n}(T) = \frac{(T+1)^{p^m}-1}{(T+1)^{p^n}-1} \in \mathbb{Z}_p[T] \subseteq \Lambda$$

for suitable integers $m \geq n$. Since $X(E/F')$ and $X(E/F)$ are both Λ-torsion in view of our hypotheses, the quotients $X(E/F)/\nu$ and $X(E/F')/\nu$ are finite for all sufficiently large m and n (the polynomials $\nu_{n+1,n}(T)$ are pairwise coprime as n runs over the natural numbers, and therefore the $\nu_{m,n}$ will be coprime with the characteristic power series of $X(E/F)$ and $X(E/F')$ for sufficiently large m and n). Fix m and n for the moment (a more concrete choice will be made below), and let $I \subseteq \Lambda$ be the ideal generated by p and $\nu_{n,m}$. As in the proof of Theorem 11·4 it follows from [**34**, Theorem 4·5 and Corollary 3·8] that U can be made small enough to ensure that, for some constant $\tilde{C}$, we have

$$v_p(|X(E/L)/I|) \leq v_p(|X(E/F)/I|) + \tilde{C} \tag{30}$$

for each $L \in U$. These results can be applied because $X(E/F)$ is Λ-torsion, E has good ordinary reduction at the primes above p and $E(F)[p^\infty]$ is finite (because $H \in \mathcal{H}$, see Lemma 2·7). Note that the constant $\tilde{C}$ is independent from m and n. Indeed, according to [**34**, corollary 3·8] the choice of $\tilde{C}$ depends only on the number of generating elements of the ideal I, which is two for any choice of n and m.

Corollary 11·5 implies that there exists a constant $C \in \mathbb{N}$ such that

$$v_p(|(X(E/L')_\Delta)/(p, \nu_{m,n})|) \leq v_p(|X(E/L)/(p, \nu_{m,n})|) + C \tag{31}$$

for each $L \in U$. Recall from Lemma 11·3 that for any finite $\mathbb{Z}_p[\Delta]$-module Z which is annihilated by p, we have

$$v_p(|Z|) \leq p^r \cdot v_p(|Z_\Delta|).$$

We apply this to the module $Z = X(E/L')/(p, \nu_{m,n})$ in order to conclude that, for a suitable constant C', we have

$$v_p(|X(E/L')/(p, \nu_{m,n})|) \leq p^r \cdot v_p(|X(E/L)/(p, \nu_{m,n})|) + C' \tag{32}$$

for each $L \in U$. Indeed, let $\Delta = \{\sigma_1, \ldots, \sigma_{p^r}\}$. Then

$$\begin{aligned}(X(E/L')_\Delta)/(p, \nu_{m,n}) &= X(E/L')/(\sigma_1 - 1, \ldots, \sigma_{p^r} - 1, p, \nu_{m,n}) \\ &= (X(E/L')/(p, \nu_{m,n}))_\Delta,\end{aligned}$$

since Δ and Γ commute. Therefore we can combine equations (29) (with $Z = X(E/L')/(p, \nu_{m,n})$) and (31) in order to obtain the desired inequality.

Now we need two auxiliary lemmas.

LEMMA 11·7 *Let $L = K_\infty^{H_L}$. Then it follows from the assumptions of Theorem 11·6 that*

$$\mu(X(E/L)) = \mu(X(E/L)/p)$$

holds as soon as $H_L \in \mathcal{H}$ and $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H_L)$.

Therefore this equation holds for all but finitely many $L \in \mathcal{E}^{\subseteq K_\infty}(K)$.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Similarly,

$$\mu(X(E/L')) = \mu(X(E/L')/p)$$

holds for all but finitely many L' under the assumptions of Theorem 11·6.

Proof. Suppose that $L = K_\infty^{H_L}$ for some $H_L \in \mathcal{H}$, let $m \geq 2$ be arbitrary, and consider the map

$$\phi_0 : X(E/K_\infty)[p^m]_{H_L} \longrightarrow X(E/L)[p^m].$$

If $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H_L)$, then it follows from Proposition 4·2 that the cokernel of ϕ_0 is finite. Since $X(E/K_\infty)[p^m] = X(E/K_\infty)[p]$, it follows that

$$X(E/L)[p^m] \setminus X(E/L)[p]$$

is finite. The first part of the lemma now follows from the general structure theory of Λ-modules.

We already know from Proposition 1·4 that the $\mathfrak{M}_H(G)$-property holds for all but finitely many $H \in \mathcal{E}$, provided that $\mathcal{H}$ is non-empty. The latter holds for both $\mathbb{Z}_p^2$-extensions K_∞/K and K'_∞/K' in view of the hypotheses from Theorem 11·6. The last assertion of the lemma thus can be proved analogously. □

LEMMA 11·8 *Let Z be any finitely generated torsion Λ-module such that $Z[p^\infty] = Z[p]$. For each $m, n \in \mathbb{N}$ such that $\nu_{m,n}$ is coprime with the characteristic power series of Z, we have*

$$\mu(Z) \cdot (p^m - p^n) \leq \nu_p(|Z/(p, \nu_{m,n})|).$$

Proof. Let E_Z be an elementary torsion Λ-module attached to Z, and write

$$E_Z = E_1 \oplus E_2,$$

where $p \cdot E_2 = \{0\}$, and where multiplication by p is injective on E_1. Then [**35**, lemma 3·7] implies that

$$\nu_p(|Z/(p, \nu_{m,n})|) \geq \nu_p(|E_2/(p, \nu_{m,n})|).$$

Since $Z[p^\infty] = Z[p]$ and therefore $p \cdot E_2 = \{0\}$, the right hand side of this inequality equals

$$\mu(Z) \cdot \deg(\nu_{m,n}) = \mu(Z) \cdot (p^m - p^n).$$

Now suppose that $L \in U$ is such that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H_L)$, and let $M = \bigoplus_{i=1}^s \Lambda/(p) \oplus \bigoplus_{j=1}^t \Lambda/(f_j)$ be an elementary Λ-module attached to $X(E/L)$ (here we use Lemma 11·7). We choose n large enough to ensure that

$$\lambda(X(E/L)) < p^{n+1} - p^n,$$

and we let $m = 2n$. Then

$$\Lambda/(p, \nu_{m,n}, f_j) = \Lambda/(p, T^{\deg(f_j)})$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

for each j, and therefore

$$v_p(|M/(p,\nu_{m,n})|) = \mu(X(E/L)) \cdot (p^{2n} - p^n) + \lambda(X(E/L)).$$

Let $\varphi : X(E/L) \longrightarrow M$ be a pseudo-isomorphism. Then the kernel and the cokernel of φ are finite, and it follows from [**35**, lemma 3·8] that there exists a fixed constant D such that

$$|v_p(|M/(p,\nu_{m,n})|) - v_p(|X(E/L)/(p,\nu_{m,n})|)| \leq D$$

for each m,n.

Using equation (32), it follows from the above that there exists some constant C'' such that

$$v_p(|X(E/L')/(p,\nu_{m,n})|) \leq p^r \cdot \Big(\mu(X(E/L)) \cdot (p^{2n} - p^n) + \lambda(X(E/L))\Big) + C''$$

for every $n \in \mathbb{N}$. We enlarge n if necessary to ensure that

$$p^r \cdot \lambda(X(E/L)) + C'' < p^{n+1} - p^n.$$

Now consider an elementary Λ-module

$$N = \bigoplus_{i=1}^{r} \Lambda/(p^{n_i}) \oplus \bigoplus_{j=1}^{w} \Lambda/(g_j)$$

attached to $X(E/L')$. In view of Lemma 11·7, for all but finitely many $L \in U$, we may assume that $n_i = 1$ for each i. Recall that $\mu(X(E/L')) \cdot (p^{2n} - p^n) \leq v_p(|X(E/L')/(p,\nu_{m,n})|)$ by Lemma 11·8. The first statement of the theorem is now immediate from our choice of n.

The proof of the second statement is analogous – if $X(E/F')[p^\infty]$ is annihilated by p, then the assertion $\mu(X(E/F')) = \mu(X(E/F')/p)$ from Lemma 11·7 clearly holds for F' even although we do not know whether $X(E/K'_\infty)_f$ is finitely generated over $\Lambda(\mathrm{Gal}(K'_\infty/F'))$. (This is important since our major goal is to *prove* the $\mathfrak{M}_H(G)$-property for F'). □

We now prove the main result of this section.

THEOREM 11·9 *Let K_∞/K, $F = K_\infty^H$, K'/K and the neighbourhood U be as in Theorem 11·6. In particular, we assume that $H \in \mathcal{H}$ and that $X(E/F')$ is Λ-torsion. Suppose that:*

(1) $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$;

(2) $\mu_G(X(E/K'_\infty)) = [K' : K] \cdot \mu_G(X(E/K_\infty))$; and that

(3) $X(E/K_\infty)[p^\infty]$, $X(E/F')[p^\infty]$ and $X(E/K'_\infty)[p^\infty]$ are annihilated by p.

Then $X(E/K'_\infty)_f$ is finitely generated over $\Lambda(H)$ (here we identify $\mathrm{Gal}(K'_\infty/F')$ with H).

Proof. We will actually give two arguments, using Theorem 1·3, and in particular the equivalence of (a) with (b) and (e), respectively.

First recall from Theorem 5·1, Corollary 5·2 and Theorem 1·3 that

$$\mu(X(E/L)) \geq \mu_G(X(E/K_\infty))$$

for each $L = K_\infty^{H_L}$, $H_L \in \mathcal{H}$, with equality iff $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H_L)$. A similar fact holds for the $\mathbb{Z}_p$-subextensions L' of K'_∞. Now choose a neighbourhood U of F

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

as in Theorem 11·6. In view of hypothesis (1) and Proposition 1·4, we may and will assume that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(\mathrm{Gal}(K_\infty/L))$ for each $L \in U$. For all but finitely many of these L (including F by (3)), we thus have

$$\begin{aligned}\mu_G(X(E/K'_\infty)) &\overset{5\cdot1}{\leq} \mu(X(E/L')) \\ &\overset{11\cdot6}{\leq} [K' : K] \cdot \mu(X(E/L)) \\ &\overset{1\cdot3}{=} [K' : K] \cdot \mu_G(X(E/K_\infty)) \\ &\overset{(2)}{=} \mu_G(X(E/K'_\infty)).\end{aligned}$$

First approach to prove the theorem: in fact, it follows from this chain of inequalities that we must have equality everywhere. Looking at the first line, the case $L = F$ yields the first proof of the theorem.

Second approach to prove the theorem: now we consider the $\mathbb{Z}_p$-extensions in the neighbourhood U of F. We will study the boundedness of λ-invariants. To this purpose, we will show that, if U is sufficiently small, then

$$\lambda(X(E/L')) \leq C$$

for each $L \in U$, for some fixed constant C. Then the statement of the theorem will follow from the implication $(e) \Longrightarrow (a)$ of Theorem 1·3.

Recall from the above that

$$\mu(X(E/L')) = \mu_G(X(E/K'_\infty))$$

for all but finitely many $L \in U$, including $L = F$. Since $H \in \mathcal{H}$, it follows from Lemma 2·7 that $E(F')[p^\infty]$ is finite. Moreover, $X(E/F')$ is Λ-torsion by assumption. Therefore [**34**, Theorem 4·11] implies that in a possibly smaller neighbourhood $U' \subseteq U$ of F', we have that

$$\lambda(X(E/L')) \leq \lambda(X(E/F'))$$

for all but finitely many L'. This proves that the λ-invariant of $X(E/L')$ is bounded on U. □

In the remainder of this section, we want to describe a natural setting where the second condition from Theorem 11·9 is satisfied. We restrict to the case $[K' : K] = p$. The idea is to kind of use Theorem 1·3 for a vertical' second $\mathbb{Z}_p^2$-extension of K which contains F and K'.

LEMMA 11·10 *Let K_∞, K', F and F' be as in Theorem 11·6, and suppose that $[K' : K] = p$ and that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(H)$. We assume that K' is contained in a $\mathbb{Z}_p$-extension M of K, and we let $\mathbb{K}_\infty = K_\infty M$ (this is a $\mathbb{Z}_p^3$-extension of K). Write $\mathbb{G} = \mathrm{Gal}(\mathbb{K}_\infty/K)$ and $G' = \mathrm{Gal}(FM/M)$.*

Suppose that:

(a) $X(E/FM)_f$ is finitely generated over $\Lambda(\mathrm{Gal}(FM/F))$, and

(b) $\mu_{\mathbb{G}}(X(E/\mathbb{K}_\infty)) = \mu_{G'}(X(E/FM))$.

Then

$$\mu_G(X(E/K'_\infty)) = p \cdot \mu_G(X(E/K_\infty)).$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Before we start with the proof of the lemma, we would like to make plausible that such auxiliary 'vertical' $\mathbb{Z}_p^2$-extensions do exist naturally. Let K_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of K. We assume that K_{cyc} is contained in the 'vertical' $\mathbb{Z}_p^2$-extension FM of K. Then it is plausible in view of Proposition 1·4 that F can be chosen such that hypothesis (a) from the lemma is satisfied. Moreover, suppose that $\operatorname{rank}_\Lambda(X(E/K_{cyc})) = \mu(X(E/K_{cyc})) = 0$ (or that the analogous properties hold for any other $\mathbb{Z}_p$-extension FM^H, $H \in \mathcal{H}$, of K contained in FM). Then it follows from Theorem 5·1 that

$$\mu_{G'}(X(E/FM)) = 0.$$

Analogously, one can show (by using [**36**, corollary 3·15(a) and (b)] for example) that $\mu_{\mathbb{G}}(X(E/\mathbb{K}_\infty)) = 0$. Therefore hypothesis (b) from Lemma 11·10 is satisfied.

Proof of Lemma 11·10. The main part of the proof will focus on the following auxiliary statement: we show that there exists a neighbourhood $U = \mathcal{E}(F, n) \cap \mathcal{E}^{\subseteq K_\infty}(K)$ of F such that:

(1) $\operatorname{Gal}(K_\infty/L) \in \mathcal{H}$;

(2) $\operatorname{Gal}(K'_\infty/L') \in \mathcal{H}$ and

(3) $\mu(X(E/L')) = p \cdot \mu(X(E/L))$

for each $L \in U$.

This statement will imply the assertion of the lemma. Indeed, we recall that the equivalent conditions from Theorem 1·3 hold for all but finitely many $L \in \mathcal{E}^{\subseteq K_\infty}(K)$ and for all but finitely many $L' \in \mathcal{E}^{\subseteq K'_\infty}(K')$ (cf. Proposition 1·4). Therefore Theorem 1·3,(b) and the last assertion of the auxiliary result yield the lemma.

It follows from Proposition 2·5 and our hypotheses on F and F' that the first two conditions of the auxiliary result are satisfied in each sufficiently small neighbourhood of F.

Since $X(E/FM)_f$ is finitely generated over $\Lambda(\operatorname{Gal}(FM/F))$ and as K' corresponds to the first layer of the $\mathbb{Z}_p$-extension M/K, it follows from the implication $(a) \Longrightarrow (c)$ of Theorem 1·3 that

$$\mu(X(E/F')) = p \cdot \mu(X(E/F)).$$

We will now show that for each L which is contained in some sufficiently small neighbourhood U of F, $X(E/LM)_f$ is finitely generated over $\Lambda(LM/L)$; by the above, this will conclude the proof of the lemma.

To this purpose, we consider the $\mathbb{Z}_p^3$-extension $\mathbb{K}_\infty = K_\infty \cdot M$ of K (recall that $K' \cap K_\infty = K$). Choose topological generators σ, τ and ρ of $\operatorname{Gal}(\mathbb{K}_\infty/K) \cong \mathbb{Z}_p^3$ such that

$$K_\infty = \mathbb{K}_\infty^{\langle\rho\rangle}, \quad M = \mathbb{K}_\infty^{\langle\sigma,\tau\rangle}.$$

Moreover, we can assume that $H = \langle\tau\rangle$, i.e. $F = K_\infty^{\langle\tau\rangle}$. For any intermediate field Z of the $\mathbb{Z}_p^3$-extension $\mathbb{K}_\infty/K$, we denote by $\operatorname{Fix}(Z) \subseteq \langle\sigma, \tau, \rho\rangle$ the subgroup such that $Z = \mathbb{K}_\infty^{\operatorname{Fix}(Z)}$. Then

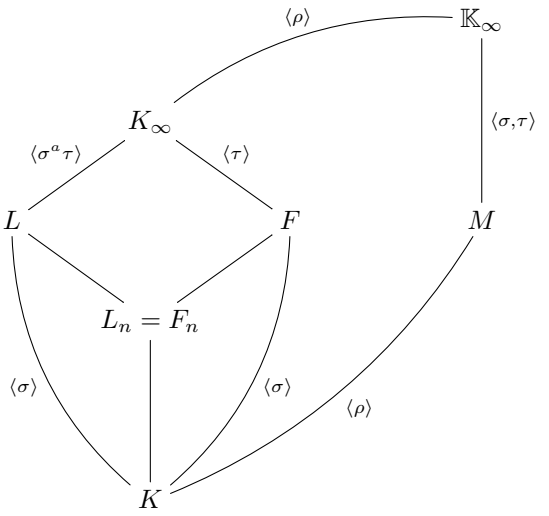
$$\operatorname{Fix}(F \cdot M) = \operatorname{Fix}(F) \cap \operatorname{Fix}(M) = \langle\tau, \rho\rangle \cap \langle\sigma, \tau\rangle = \langle\tau\rangle.$$

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

Suppose that $U = \mathcal{E}(F,n) \cap \mathcal{E}^{\subseteq K_\infty}(K)$. Then any $\mathbb{Z}_p$-extension $L \in U$ of K is a subfield of K_∞ which is fixed by an element of the form $\sigma^a\tau$, $a \in p^n\mathbb{Z}_p$. Therefore

$$\mathrm{Fix}(L \cdot M) = \mathrm{Fix}(L) \cap \mathrm{Fix}(M) = \langle \sigma^a\tau, \rho\rangle \cap \langle \sigma, \tau\rangle = \langle \sigma^a\tau\rangle.$$

We summarise the fields in the following diagram.



Now fix $L \in U$, $L = K_\infty^{\langle\sigma^a\tau\rangle}$. We have that $\mathrm{Gal}(K_\infty/L) \in \mathcal{H}$. This allows us to replace K_∞ with $L\,M$ in Lemma 2·12 and Proposition 2·15 to show that $H^2(G_S(LM), E[p^\infty]) = 0$ and that we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/LM) \longrightarrow H^1(G_S(LM), E[p^\infty]) \xrightarrow{\lambda_\infty} \bigoplus_{v\in S} J_v(E/LM) \longrightarrow 0.$$

Therefore [**40**, proposition 4·8] can be applied to the $\mathbb{Z}_p$-extension $\mathbb{K}_\infty/LM$ in order to deduce that

$$\mu_{\mathbb{G}}(X(E/\mathbb{K}_\infty)) = \mu_{\mathrm{Gal}(LM/K)}(X(E/LM)) - \mu_{\mathrm{Gal}(LM/K)}((X(E/\mathbb{K}_\infty)_f)_{\langle\sigma^a\tau\rangle})$$

(note that both $\mathbb{K}_\infty$ and LM are 'admissible' extensions in the sense of [**40**] although they might not contain the cyclotomic $\mathbb{Z}_p$-extension of K, since they contain $L = K_\infty^{H_L}$ with $H_L \in \mathcal{H}$; also note that Lim assumes p to be odd, but as K is assumed to be totally imaginary if $p = 2$ his proof also works for $p = 2$).

It therefore follows that

$$\mu_{\mathbb{G}}(X(E/\mathbb{K}_\infty)) \leq \mu_{\mathrm{Gal}(LM/K)}(X(E/LM)) \tag{33}$$

with equality iff $\mu_{\mathrm{Gal}(LM/K)}((X(E/\mathbb{K}_\infty)_f)_{\langle\sigma^a\tau\rangle}) = 0$.

In the following chain of equations, we will, by abuse of notation, denote any two-variable Iwasawa algebra by Λ_2 and any one-variable Iwasawa algebra by Λ_1. Moreover, we will repeatedly use the equivalence $(a) \Leftrightarrow (b)$ from Theorem 1·3, which will be abbreviated by the symbol $(\star)$. Recall that $X(E/K_\infty)_f$ is finitely generated over $\Lambda(\mathrm{Gal}(K_\infty/F))$ by assumption and that it follows from Theorem 1·3, $(a) \Leftrightarrow (e)$ that the same holds true for each $L \in U$, provided that U has been chosen small enough. On the other hand, $X(E/FM)_f$ is finitely

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

generated over $\Lambda(\mathrm{Gal}(FM/F))$ in view of hypothesis (a). Therefore

$$\begin{aligned}\mu_{\Lambda_2}(X(E/FM)) &\overset{(\star)}{=} \mu_{\Lambda_1}(X(E/F))\\ &\overset{(\star)}{=} \mu_{\Lambda_2}(X(E/K_\infty))\\ &\overset{(\star)}{=} \mu_{\Lambda_1}(X(E/L))\\ &\overset{5\cdot1}{\geq} \mu_{\Lambda_2}(X(E/LM))\\ &\overset{(33)}{\geq} \mu_{\mathbb{G}}(X(E/\mathbb{K}_\infty))\\ &\overset{(b)}{=} \mu_{\Lambda_2}(X(E/FM)).\end{aligned}$$

It follows that we have equality everywhere. In particular,

$$\mu_{\Lambda_2}(X(E/LM)) = \mu_{\Lambda_1}(X(E/L))$$

for each $L \in U$ (provided that U has been chosen small enough), and therefore, for each such L, Theorem 1·3 implies that $X(E/LM)_f$ is finitely generated over $\Lambda(\mathrm{Gal}(LM/L))$. This concludes the proof of the auxiliary statement and therefore also the proof of Lemma 11·10. □

Acknowledgements. The authors would like to thank Chandrakant Aribam, Cornelius Greither, Somnath Jha, Chan-Ho Kim, Robert Pollack, Karl Rubin, Florian Sprung, Oliver Thomas and Jeanine Van Order for helpful discussions. We thank the anonymous referee for the detailed report which led to considerable improvements in the exposition.

REFERENCES

[1] M. Atiyah and I. Macdonald. *Introduction to Commutative Algebra* (Adison-Wesley, 1969).
[2] D. Brink. Prime decomposition in the anti-cyclotomic extensions, *Math. Comp.*, **76**(260) (2007), 2127-2138.
[3] M. Bertolini and H. Darmon. Kolyvagin's descent and Mordell–Weil groups over ring class fields, *J. Reine Angew. Math.* **412** (1990), 63–74.
[4] J. Bloom and F. Gerth III. The Iwasawa invariant μ in the composite of two $\mathbb{Z}_p$-extensions, *J. Number Theory* **13** (1981), 262–267.
[5] N. Bourbaki. *Commutative Algebra*, (Hermann, Paris, 1972).
[6] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob. The GL_2 main conjecture for elliptic curves without complex multiplication, *Publ. Math. Inst. Hautes Études Sci.* (2005), no. **101**, 163–208.
[7] J. Coates and R. Greenberg. Kummer theory for Abelian varieties over local fields, *Invent. Math.* **124** (1996), 129–174.
[8] J. Coates, P. Schneider and R. Sujatha. Links between cyclotomic and GL_2 Iwasawa theory, *Doc. Math.* (2003), extra vol., 187–215.
[9] J. Coates and R. Sujatha. *Galois Cohomology of Elliptic Curves*, 2nd. ed., Tata Institute of Fundamental Research Lectures on Mathematics, 88 (Published by Narosa Publishing House, New Delhi; for the Tata Institute of Fundamental Research, Mumbai, 2010)
[10] J. Coates and R. Sujatha On the $\mathfrak{M}_H(G)$-conjecture, *Non-abelian Fundamental Groups and Iwasawa Theory*. London Math. Soc. Lecture Note Ser. 393 (Cambridge University Press, Cambridge, 2012). 132–161.
[11] J. E. Cremona. *Algorithms for modular elliptic curves*, 2nd ed. (Cambridge University Press, Cambridge, 1997).
[12] A. Cuoco. The growth of Iwasawa invariants in a family. *Compos. Math.* **41**(3) (1980), 415–437.
[13] A. Cuoco, P. Monsky. Class numbers in $\mathbb{Z}_p^d$-*extensions*, *Math. Ann.* **255** (1981), 235–258.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

[14] A. CUOCO. Relations between invariants in $\mathbb{Z}_p^2$-extensions, *Math. Z.* **181**(2) (1982), 197–200.
[15] A. CUOCO. Generalized Iwasawa invariants in a family, *Compos. Math*. **51**(1) (1984), 89–103.
[16] T. DOKCHITSER, V. DOKCHITSER. On the Birch-Swinnerton-Dyer quotients modulo squares, *Ann. of Math.* 172(1) (2010), 567–596.
[17] T. FUKAYA, K. KATO. A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory. *Proc. St. Petersburg Math. Soc. Vol. XII, Amer. Math. Soc. Transl. Ser. 2 219* (Amer. Math. Soc., 2006), 1–85.
[18] R. GREENBERG. The Iwasawa invariants of Γ-extensions of a fixed number field, *Amer. J. Math.* **95** (1973), 204–214.
[19] R. GREENBERG. *Iwasawa theory for elliptic curves*. Lecture Notes in Math. 1716 (Springer, New York 1999), pp.51-144.
[20] R. GREENBERG. Galois theory for the Selmer group of an abelian variety, *Compos. Math.* **136** (2003), 255–297.
[21] R. GREENBERG. *On the structure of Selmer groups*. In Elliptic Curves, Modular Forms and Iwasawa Theory (in honour of John H. Coates' 70th birthday; eds. D. LOEFFLER, S.L. ZERBES), Springer Proc. in Math. and Stat. 188 (Springer, 2016), pp. 225-252.
[22] Y. HACHIMORI, K. MATSUNO. An analogue of Kida's formula for the Selmer groups of elliptic curves, *J. Algebraic Geometry* **8** (1999), 581–601.
[23] Y. HACHIMORI, K. MATSUNO. On finite Λ-submodules of Selmer groups of elliptic curves, *Proc. Amer. Math. Soc*. **128** (9) (2000), 2539–2541.
[24] Y. HACHIMORI, T. OCHIAI. Notes on non-commutative Iwasawa theory, *Asian J. Math.* **14** (1) (2010), 11–18.
[25] Y. HACHIMORI, O. VENJAKOB. Completely faithful Selmer groups over Kummer extensions, *Doc. Math*. 2003, Extra Vol., 443–478.
[26] M. HARRIS. Correction to: "p-adic representations arising from descent on abelian varieties", *Compos. Math*. **121** (1) (2000), 105–108.
[27] S. HOWSON. Euler characteristics as invariants of Iwasawa modules, *Proc. Lond. Math. Soc*. **85** (3), (2002) 634–658.
[28] K. IWASAWA. *On the* μ-invariants of $\mathbb{Z}_l$*-extensions*. In *Number Theory, Algebraic Geometry and Commutative Algebra (in honor of Yasuo Akizuki)*, (Kinokuniya, Tokyo, 1973) pp. 1-11.
[29] M. KIDA. Ramification in the division fields of an elliptic curve, *Abh. Math. Sem. Univ. Hamburg* 73 (2003), 195–207.
[30] M. KIDA. Variation of the reduction type of elliptic curves under small base change with wild ramification, *Cent. Eur. J. Math.* **1** (4) (2003), 510–560.
[31] C.-H. KIM, R. POLLACK and T. WESTON. On the freeness of anticyclotomic Selmer groups of modular forms, *Int. J. Number Theory*, **13** (6) (2017), 1443–1455.
[32] K. KATO. *p-adic Hodge theory and values of zeta functions of modular forms*. In Cohomologies p-adique et Applications Arithmetiques III. Astérisque 295 (2004), 117–290.
[33] S. KLEINE. Local behavior of Iwasawa's invariants, *Int. J. Number Theory*, **13** (4) (2017), 1013-1036.
[34] S. KLEINE. Bounding the Iwasawa invariants of Selmer groups, Canad. *J. Math.* **73** (5) (2021), 1390–1422.
[35] S. KLEINE. On the Iwasawa invariants of non-cotorsion Selmer groups, *Asian J. Math.*, **26** (3) (2022), 373–406.
[36] S. KLEINE and A. MATAR. Boundedness of Iwasawa Invariants of fine Selmer Groups and Selmer groups, *Results Math.*, **78** (4) (2023), paper no. 148.
[37] K. KIDWELL. On the structure of Selmer groups of p-ordinary modular forms over $\mathbb{Z}_p$-extensions. *J. Number Theory*, **187** (2018), 296–331.
[38] D. KUNDU, A. LEI, A. RAY. Arithmetic statistics and noncommutative Iwasawa theory, Doc. *Math.* **27** (2022), 89–149.
[39] D. KUNDU and A. RAY. Statistics for Iwasawa invariants of elliptic curves, *Trans. Amer. Math. Soc.* **374** (2021), 7945–7965.
[40] M.F. LIM. A remark on the $\mathfrak{M}_H(G)$-conjecture and Akashi series, *Int. J. Number Theory* **11** (1) (2015), 269–297.
[41] M.F. LIM. Notes on the fine Selmer groups, *Asian J. Math.* **21** (2) (2017), 337-362.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press

[42] M. F. LIM. Some remarks on Kida's formula when $\mu \neq 0$, *The Ramanujan Journal* **55** (3) (2021), 1127-1144.
[43] H. MATSUMURA. *Commutative Ring Theory* (Cambridge University Press, 1989).
[44] B. MAZUR. Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* **18** (1972), 183–266.
[45] B. MAZUR. *Modular Curves and Arithmetic*, Proc. Internat. Congress Math., Vols. 1, 2 (Warsaw, 1983), PWN, Warsaw, 1984, pp. 185–211.
[46] J. MINARDI. Iwasawa Modules for $\mathbb{Z}_p^d$-Extensions of Algebraic Number Fields, PhD. thesis. University of Washington (1986).
[47] P. MONSKY. Some invariants of $\mathbb{Z}_p^d$-extensions, *Math. Ann.* **255** 229–233, 1981.
[48] J. NEUKIRCH, A. SCHMIDT, K. WINGBERG. *Cohomology of Number Fields*, 2nd ed. Grundlehren Math. Wiss. 323, (Springer, 2008), xvi+825.
[49] K. ONO, M. PAPANIKOLAS. *Quadratic twists of modular forms and elliptic curves*, Number Theory for the Millennium III (Urbana, IL, 2000), A. K. Peters, 2002, pp. 73-85.
[50] R. POLLACK and T. WESTON. On anticyclotomic μ-invariants of modular forms, *Compositio. Math.* **147** (5) (2011), 1353–1381.
[51] L. RIBES and P. ZALESSKII. Profinite Groups. *Ergeb. der Math.* **40** (Springer-Verlag, 2000).
[52] D. ROHRLICH. On L-functions of elliptic curves and cyclotomic towers, *Invent. Math.* **75** (1984), 409–423.
[53] K. RUBIN. *Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer*. Lecture Notes in Math. 1716 (Springer, New York 1999), pp.167-234.
[54] *SageMath, the Sage Mathematics Software System (Version* 8.9*)*. The Sage Developers (2019), http://www.sagemath.org.
[55] J. SILVERMAN. *The Arithmetic of Elliptic Curves*. Graduate Texts in Math. **106** (Springer-Verlag, 2009).
[56] V. VATSAL. Special values of anticyclotomic L-functions, *Duke Math. J.* **116** (2003), 219–261.
[57] O. VENJAKOB. Characteristic elements in non-commutative Iwasawa theory, *J. Reine Angew. Math.* **583** (2005), 193–236.
[58] Y. ZARHIN. Endomorphisms and torsion of abelian varieties, *Duke Math. J.* **54**(1) (1987), 131–145.
[59] S. ZERBES. Generalised Euler characteristics of Selmer groups, *Proc. London Math. Soc.* **98**(3) (2008), 775–796.

https://doi.org/10.1017/S0305004125000325 Published online by Cambridge University Press