Nagoya Math. J., **248** (2022), 922–938
DOI 10.1017/nmj.2022.14

SELMER GROUPS OF ELLIPTIC CURVES OVER THE $PGL(2)$ EXTENSION

JISHNU RAY AND R. SUJATHA

Abstract. Iwasawa theory of elliptic curves over noncommutative $GL(2)$ extension has been a fruitful area of research. Over such a noncommutative p-adic Lie extension, there exists a structure theorem providing the structure of the dual Selmer groups for elliptic curves in terms of reflexive ideals in the Iwasawa algebra. The central object of this article is to study Iwasawa theory over the $PGL(2)$ extension and connect it with Iwasawa theory over the $GL(2)$ extension, deriving consequences to the structure theorem when the reflexive ideal is the augmentation ideal of the center. We also show how the dual Selmer group over the $GL(2)$ extension being torsion is related with that of the $PGL(2)$ extension.

§1. Introduction

Let $p \geq 5$ be a prime, which is our assumption throughout the article. Let G be a compact noncommutative torsion-free p-adic analytic group. Let $\Lambda(G) = \mathbb{Z}_p[[G]]$ be the Iwasawa algebra of G. An ideal J of $\Lambda(G)$ is called left reflexive ideal if the natural map

$$J \to \mathrm{Hom}_{\Lambda(G)^{\mathrm{op}}}\big(\mathrm{Hom}_{\Lambda(G)}(J, \Lambda(G)), \Lambda(G)\big)$$

is an isomorphism as $\Lambda(G)$-modules. We can also define a right reflexive ideal in a similar fashion. A two-sided ideal is called reflexive if it is both right and left reflexive. In [A], Ardakov showed that if $G \cong H \times C$ where H is a torsion-free pro-p group with split semisimple Lie algebra and $C \cong \mathbb{Z}_p$, the *two-sided* reflexive ideals of G are of the form $J = f\Lambda(G)$, where f is a distinguished polynomial in $\Lambda(C)$ (see [A, Cor. 4.8]).

Reflexive ideals occur naturally in the study of Selmer groups of elliptic curves with good ordinary reduction at p over noncommutative p-adic Lie towers. More precisely, let E be an elliptic curve over a number field F such that E has good ordinary reduction at all the primes of F lying over an odd prime p. Let $F_\infty = F[E_{p^\infty}]$ be the noncommutative p-adic Lie extension with Galois group $G = \mathrm{Gal}(F_\infty/F)$ having center C. Since $p \geq 5$, G is p-torsion-free compact p-adic Lie group (cf. Lemma 2.1). We also assume throughout our article that G is a pro-p group. Therefore, $\Lambda(G)$ is an Auslander regular local ring [V, Th. 3.26]. Let $\widehat{\mathrm{Sel}(E/F_\infty)}$ be the Pontryagin dual of the Selmer group over F_∞; it is easily seen to be a finitely generated module over the Iwasawa algebra $\Lambda(G)$. In [CFK+], the authors study Iwasawa theory over this noncommutative extension F_∞. If $\widehat{\mathrm{Sel}(E/F_\infty)}$ is torsion (see

Received November 17, 2020. Revised January 31, 2022. Accepted April 30, 2022.
2020 Mathematics subject classification: Primary 11R23; Secondary 11G05, 11R34.
This work started with the Pacific Institute for the Mathematical Sciences and the Centre National de la Recherche Scientifique research funding received by Jishnu Ray. Later on, he also received funding from the Tata Institute of Fundamental Research and the Institute for Advancing Intelligence, The Chatterjee Group—Centres for Research and Education in Science and Technology in writing the revised versions. R. Sujatha gratefully acknowledges support from the Natural Sciences and Engineering Research Council of Canada Discovery grant 2019-03987.

Theorem 2.4), we have the following (weak) structure theorem:

$$\widehat{\mathrm{Sel}(E/F_\infty)} \sim \oplus_{i=1}^{m} \Lambda(G)/J_i, \tag{1.1}$$

where J_i are nonzero left reflexive ideals in $\Lambda(G)$ and $\sim$ is a pseudoisomorphism of left $\Lambda(G)$-modules [CSS, p. 74]. Note that Ardakov's result mentioned above only applies to two-sided reflexive ideals. However, there can be ideals in the structure theorem which are left reflexive but not right reflexive. Note also that Ardakov's result does not give us whether a particular two-sided reflexive ideal actually appears in the structure theorem for Selmer groups in (1.1). Therefore, in order to better understand the structure of the Selmer groups, it is crucial to classify all the reflexive (left) ideals that can occur in the decomposition in (1.1).

Our point of interest in this article is to understand when the augmentation ideal $I(C)$ can occur in the decomposition in (1.1). We show that this question is crucially related with the question of understanding whether the dual Selmer group for the $PGL(2)$ extension is torsion over the corresponding Iwasawa algebra. In the following, we discuss the main result in our article.

Let K_∞ be the fixed field of F_∞ under the center C. Let $\mathrm{Sel}(E/K_\infty)$ be the Selmer group over K_∞; its dual is again a finitely generated module over the Iwasawa algebra $\Lambda(\mathrm{PG}) = \Lambda(G/C)$. As $p \geq 5$, one easily obtains that PG has no p-torsion (cf. Lemma 2.1). Since Iwasawa algebras of compact, p-torsion-free, p-adic Lie groups are Auslander regular [V, Th. 3.26], $\Lambda(\mathrm{PG})$ is also an Auslander regular local ring. By using our main theorem (see Theorem 1.1), we can classify when $\mathrm{Sel}(E/K_\infty)$ is cotorsion as a $\Lambda(\mathrm{PG})$-module in terms of the ideals J_i. We can prove that all the ideals J_i cannot be the augmentation ideal $I(C)$ (because the center cannot act trivially on $\mathrm{Sel}(E/F_\infty)$; see Proposition 3.8). Now, on the one hand, if any of these ideals is $I(C)$, then $\mathrm{Sel}(E/K_\infty)$ is *not* a cotorsion $\Lambda(\mathrm{PG})$-module. On the other hand, if none of the ideals are contained in $I(C)$, then $\mathrm{Sel}(E/K_\infty)$ is a cotorsion $\Lambda(\mathrm{PG})$-module (see Theorem 3.6 and Remark 3.7). This gives a complete classification of when $\widehat{\mathrm{Sel}(E/K_\infty)}$ can be a torsion $\Lambda(\mathrm{PG})$-module.

Under suitable hypotheses, Coates showed that the dual Selmer group over the $GL(2)$ extension is torsion over $\Lambda(G)$ (cf. [Co1, Th. 4.5]). In particular, in [Co1, Th. 4.5], it was shown that if the dual Selmer group of the elliptic curve over the cyclotomic extension is torsion and has μ-invariant zero, then the dual Selmer group of the elliptic curve over the $GL(2)$ extension is $\Lambda(G)$-torsion. As a consequence of our main result in this article, we can show that if the dual Selmer group of the elliptic curve over the PGL(2) extension is torsion, this implies that the dual Selmer group over the $GL(2)$ extension is also torsion. Hence, our result gives an alternative criterion under which the dual Selmer group of the elliptic curve over the $GL(2)$ extension is torsion.

Our main result can be summarized as follows (see Theorems 3.1 and 3.5).

THEOREM 1.1. *Let $p \geq 5$, and let G be a pro-p compact p-adic Lie group.*

1. *As $\Lambda(\mathrm{PG})$-modules, the Selmer group $\mathrm{Sel}(E/K_\infty)$ is isomorphic to the Selmer group $\mathrm{Sel}(E/F_\infty)$ invariant by the center C.*
2. *The dual Selmer group $\widehat{\mathrm{Sel}(E/K_\infty)}$ is a torsion $\Lambda(\mathrm{PG})$-module if and only if $\widehat{\mathrm{Sel}(E/F_\infty)}$ is a torsion $\Lambda(G)$-module and $H_1(C, \widehat{\mathrm{Sel}(E/F_\infty)}) = 0$.*

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

Furthermore, any of the following conditions are sufficient to conclude that $\widehat{\mathrm{Sel}(E/K_\infty)}$ *is a torsion* $\Lambda(\mathrm{PG})$*-module.*

- *The Selmer group* $\mathrm{Sel}(E/F)$ *is finite and* $H_2(\mathrm{PG}, \widehat{\mathrm{Sel}(E/K_\infty)})$ *is finite.*
- *The Selmer group* $\mathrm{Sel}(E/F)$ *is finite,* $\widehat{\mathrm{Sel}(E/F_\infty)}$ *is a torsion* $\Lambda(G)$*-module, and* $H_0(\mathrm{PG}, H_1(C, \widehat{\mathrm{Sel}(E/F_\infty)}))$ *is finite.*

Note that part (1) of the theorem above gives an isomorphism and not just a pseudo-isomorphism, whereas the natural map

$$\mathrm{Sel}(E/F) \to \mathrm{Sel}(E/K_\infty)^{\mathrm{PG}}$$

has finite kernel and cokernel (see Theorem 4.2). We could prove part (2) only because of the interesting isomorphism in part (1). In the context of Iwasawa theory over a noncommutative p-adic Lie extension, one mainly considers admissible p-adic Lie extensions. We define a Galois extension M_∞ of F to be an admissible p-adic Lie extension of F if (i) $\mathrm{Gal}(M_\infty/F)$ is a p-adic Lie group, (ii) M_∞/F is unramified outside a finite set of primes of F, and (iii) M_∞ contains the cyclotomic $\mathbb{Z}_p$-extension of F [CS2, §2]. Results from cyclotomic Iwasawa theory are then used to obtain results in noncommutative Iwasawa theory. In this article, an attempt is made to rephrase the question of whether the two-sided reflexive ideal $I(C)$ can occur in the structure theorem of $\mathrm{Sel}(E/F_\infty)$ in terms of whether $\mathrm{Sel}(E/K_\infty)$ is cotorsion over $\Lambda(\mathrm{PG})$. For this, we adopt a descent approach, since the $PGL(2)$ extension does not contain the cyclotomic extension. For our descent argument, we use $GL(2)$ Iwasawa theory to try and gain insights into $PGL(2)$ Iwasawa theory. Moreover, we also ascend the Iwasawa theoretic tower from the $PGL(2)$ extension to the $GL(2)$ extension and derive conditions when the dual Selmer group over the $GL(2)$ extension is torsion.

Another reason to consider the $PGL(2)$ extension is the following. The Lie algebra of $PGL(2)$ is a simple (noncommutative) Lie algebra. Unlike $SL(2)$, the $PGL(2)$ extension occurs naturally as a p-adic Lie extension of the number field F in Iwasawa theory of elliptic curves. Over the $GL(2)$ extension, $\widehat{\mathrm{Sel}(E/F_\infty)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is an infinite dimensional $\mathbb{Q}_p$-representation [Co1, Th. 1.5]. Therefore, it is interesting to explore if the corresponding result holds for $PGL(2)$ extension. One can also enquire if the Lie algebra representation theory of $PGL(2)$ enables us to study the module structure of the dual Selmer group $\widehat{\mathrm{Sel}(E/K_\infty)}$, and thus giving us more insight into the arithmetic theory of elliptic curves.

This article consists of four sections including the introduction. In §2, we set up notation and collect the preliminary results that are needed. In §3, the defining exact sequences for the Selmer groups are used to compare the Selmer groups over the $GL(2)$ extension and the $PGL(2)$ extension (see Theorem 3.1). Furthermore, using a descent approach from the Selmer group over the $GL(2)$ extension, we prove various equivalent conditions that are sufficient to ensure that the dual Selmer over the $PGL(2)$ extension is a cotorsion module over the corresponding Iwasawa algebra (see Theorems 3.5 and 3.6). As applications, §4 deals with regular growth of ranks of Selmer groups as we descend from the $GL(2)$ extension to the $PGL(2)$ extension (see Proposition 4.1). Moreover, we study the relation between the Selmer group over the base field F and the Selmer group over the $PGL(2)$ extension (see Theorem 4.2).

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

Under the assumption that the dual Selmer group over the $PGL(2)$ extension is torsion, its Euler characteristic and the nonexistence of its nontrivial pseudonull submodules have been shown in §4. These questions have been dealt in Howson's dissertation [Ho1, Th. 5.34] and Zerbes' dissertation [Z, Chaps. 8 and 9], but our proofs are different and much simpler.

It is clear that our methods in this article are extendable to a broader class of Galois representations. Our case of representations arising from elliptic curves should be seen as a first step.

§2. Preliminaries

LEMMA 2.1. *For $p > n+1$, there are no elements of p-power order in $GL_n(\mathbb{Z}_p)$ and $PGL_n(\mathbb{Z}_p)$.*

Proof. First, consider the case for $GL_n(\mathbb{Z}_p)$. Suppose $X \in GL_n(\mathbb{Z}_p)$ and $X^p = 1$. Since $X^p - 1 = (X-1)(X^{p-1} + \cdots + 1)$ and $(X^{p-1} + \cdots + 1)$ is irreducible over $\mathbb{Z}_p$, we deduce that the minimal polynomial of X is of degree $p-1$. We know that the characteristic polynomial of X is of degree n. Hence, $n \geq p-1$, which is a contradiction.

Next, consider the case for $PGL_n(\mathbb{Z}_p)$. Suppose $X \in PGL_n(\mathbb{Z}_p)$ and $X^p = 1$. Let Z be a lift of X in $GL(n, \mathbb{Z}_p)$. Then $Z^p = cI_n$ for some $c \in \mathbb{Z}_p$ (c is actually in $\mathbb{Z}_p^\times$) and I_n is the identity matrix. Suppose c is not a pth power. Then the polynomial $T^p - c$ is irreducible. (This follows from a general fact that if F is a field, p is a prime, and $c \in F$, then $x^p - c$ is irreducible in $F[x]$ if and only if $x^p - c$ does not have any root in F.) Hence, $n \geq p$, which is a contradiction.

Suppose $c = k^p$ where $k \in \mathbb{Z}_p^\times$, then $Z^p - cI_n = 0$ is the same as $(k^{-1}Z)^p - I_n = 0$. But then we can invoke the fact from $GL_n(\mathbb{Z}_p)$ and deduce that $k^{-1}Z = I_n$ which gives that $Z = kI_n$ and hence Z belongs to the center. □

Suppose $p \geq 5$ and G is a pro-p, compact open subgroup of $GL_2(\mathbb{Z}_p)$ with center C. Let PG be the quotient G/C. Then G and PG are p-torsion-free, and hence their Iwasawa algebras are Auslander regular local rings (cf. [V, Th. 3.26]) and so we have a dimension theory. Furthermore, the usual notion of rank of a module over these Iwasawa algebras (cf. [V, Def. 1.2]) coincides with the homological rank (see [Ho2]). The module is torsion if and only if its rank over the corresponding Iwasawa algebra is zero. Finally, note that the p-cohomological dimensions of G and PG are 4 and 3, respectively.

Now, suppose G is not necessarily pro-p (still assuming $p > 3$). Let G' be a compact open pro-p subgroup of G. Both $\Lambda(G)$ and $\Lambda(G')$ are Auslander regular integral domains. (This result does not need the pro-p assumption (see [V, Th. 3.36]).) Suppose M is a finitely generated $\Lambda(G)$-module. Then M is $\Lambda(G)$-torsion if and only if

$$M^+ := \mathrm{E}^0_{\Lambda(G)}(M) = \mathrm{Hom}_{\Lambda(G)}(M, \Lambda(G)) = 0.$$

Given a finitely generated $\Lambda(G)$-module M, there is an exact sequence

$$0 \to \mathrm{E}^1_{\Lambda(G)} DM \to M \to (M^+)^+ \to \mathrm{E}^2_{\Lambda(G)} DM \to 0$$

(see [V, Prop. 2.5]). This submodule $\mathrm{E}^1_{\Lambda(G)} DM$ is the $\Lambda(G)$-torsion submodule of M (see [V, Def. 2.6]). Hence, the module M is said to be $\Lambda(G)$-torsion if and only if

$$\mathrm{E}^1_{\Lambda(G)} DM = M.$$

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

It is easy to see that if G' is an open pro-p subgroup, then there are natural isomorphisms

$$\mathrm{E}^0_{\Lambda(G)}(M) \cong \mathrm{E}^0_{\Lambda(G')}(M) \quad \text{and} \quad \mathrm{E}^1_{\Lambda(G)}DM \cong \mathrm{E}^1_{\Lambda(G')}DM$$

(see [V, Prop. 2.7(ii)] and the discussion after Definition 2.6 of [V]). Consequently, M is torsion as a $\Lambda(G)$-module if and only if M is torsion as a $\Lambda(G')$-module. Thus, in order to show that M is a torsion $\Lambda(G)$-module, it suffices to show that the homological rank of M as a $\Lambda(G')$-module is zero. Since any compact p-adic analytic group contains an open characteristic subgroup which is uniform and extrapowerful pro-p group, one may study modules over $\Lambda(G')$ by restriction of scalars (see [V, Rem. 3.23]).

Let E be an elliptic curve over a number field F without complex multiplication, and let $p \geq 5$. Let us suppose that E has good ordinary reduction at the primes of F above p. Let S be a finite set of primes of F including those above $\{p, \infty\}$ and the primes where E has bad reduction. Suppose F_S is the maximal extension of F unramified outside S. Assume that H_∞ is an infinite Galois extension of F, contained in F_S, whose Galois group $\mathrm{Gal}(H_\infty/F)$ is a pro-p, compact, p-torsion-free, p-adic Lie group of positive dimension.

For such a p-adic Lie extension H_∞ of F, we can define the Selmer group of E over H_∞ as a kernel of a natural global to local cohomological map defined by the following sequence:

$$0 \to \mathrm{Sel}(E/H_\infty) \to H^1(F_S/H_\infty, E_{p^\infty}) \xrightarrow{\lambda_{H_\infty}} \oplus_{v \in S} J_v(H_\infty). \tag{2.1}$$

Here, $J_v(H_\infty)$'s are local cohomology groups defined as follows (cf. [Co1, §3.1]). Let H_∞ be the union of an increasing tower of finite extensions H_n of F. Let $v \in S$, and for each n, denote by H_{n,ω_n} the completion of H_n with respect to a prime ω_n of H_n such that ω_n divides v and such that ω_n form a compatible sequence of primes $\omega_{n+1} \mid \omega_n$. Then

$$J_v(H_\infty) := \varinjlim_{n \to \infty} \oplus_{\omega_n | v} H^1(H_{n,\omega_n}, E)(p),$$

where the limit is taken with respect to the restriction maps.

The Selmer group encodes several p-adic arithmetic information about the elliptic curve. It follows immediately from Kummer theory of E over H_∞ that we have the following exact sequence:

$$0 \to E(H_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}(E/H_\infty) \to Ш(E/H_\infty)(p) \to 0,$$

where $Ш(E/H_\infty)$ is the Tate–Shafarevich group (cf. [CS1, p. 15]).

It is easy to see that the dual Selmer group is a finitely generated module over the Iwasawa algebra

$$\Lambda(\Omega) = \varprojlim_{W} \mathbb{Z}_p[\Omega/W],$$

where W runs over all open normal subgroups of $\Omega = \mathrm{Gal}(H_\infty/F)$. In the rest of the text, H_∞ is either the cyclotomic $\mathbb{Z}_p$-extension of F, or a pro-p noncommutative $GL(2)$ extension of F, or a pro-p noncommutative $PGL(2)$ extension of F (see below). Since we are assuming $p \geq 5$, the corresponding Galois groups are p-torsion-free, pro-p, compact p-adic Lie groups. It is natural to study the structure of this Selmer group. In the classical case, when the group $\Omega = \mathrm{Gal}(F_{\mathrm{cyc}}/F) \cong \mathbb{Z}_p$ is commutative, the Iwasawa algebra $\Lambda(\Omega)$ is a commutative local ring. One may then use the well-known structure theorem of finitely generated modules over

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

$\Lambda(\mathrm{Gal}(F_{\mathrm{cyc}}/F))$ in this setting [Bo, Chap. VII, §4]. In the noncommutative cases, when Ω is a compact pro-p, p-adic analytic group without p-torsion, the Iwasawa algebra $\Lambda(\Omega)$ is an Auslander regular local ring [V, Th. 3.26], and hence there is a dimension theory for modules in this setting. Suppose M is a finitely generated module over a noncommutative Iwasawa algebra $\Lambda(\Omega)$. Then M is a torsion $\Lambda(\Omega)$-module if $\dim M \leq \dim \Lambda(\Omega) - 1$. The module M is pseudonull if $\dim M \leq \dim \Lambda(\Omega) - 2$ (see [V, §3]). There is also a weak structure theorem [CSS].

Set

$$F_n = F(E_{p^{n+1}}), \qquad F_\infty = F(E_{p^\infty}),$$

and write

$$G_n = \mathrm{Gal}(F_\infty/F_n), \qquad G = \mathrm{Gal}(F_\infty/F).$$

By a well-known result of Serre [S], G is open in $GL_2(\mathbb{Z}_p)$ for all primes and $G = GL_2(\mathbb{Z}_p)$ for all but a finite number of primes. Note that F_∞ contains F_{cyc}, the cyclotomic $\mathbb{Z}_p$-extension over F with Galois group Γ, a p-adic Lie group of dimension 1.

A deep conjecture of [Ma] asserts the following conjecture.

CONJECTURE 2.2. *$\mathrm{Sel}(E/F_{\mathrm{cyc}})$ is a finitely generated cotorsion $\Lambda(\Gamma)$-module.*

This conjecture is known to hold in some cases (e.g., when $F = \mathbb{Q}$), thanks to a celebrated result of Kato [K]. Coates and Howson in [CH1], [CH2], developed Iwasawa theory over the $GL(2)$ extension F_∞ and provided conditions under which the Selmer group $\mathrm{Sel}(E/F_\infty)$ is cotorsion as a module over the noncommutative Iwasawa algebra $\Lambda(G)$. In particular, they showed the following results (cf. Lemmas 4.7 and 4.8, Proposition 4.3, and Theorem 4.5 of [Co1]).

THEOREM 2.3. *If $\mathrm{Sel}(E/F)$ is finite, then $H^i(G, \mathrm{Sel}(E/F_\infty))$ is finite for $i = 0, 1$. Additionally, if $\mathrm{Sel}(E/F_\infty)$ is $\Lambda(G)$-cotorsion, then $H^i(G, \mathrm{Sel}(E/F_\infty))$ is 0 for $i = 2, 3, 4$.*

THEOREM 2.4. *If $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ is a cotorsion $\Lambda(\Gamma)$-module and has μ-invariant 0, then $\mathrm{Sel}(E/F_\infty)$ is a cotorsion $\Lambda(G)$-module.*

Coates and Howson have also calculated an explicit formula for the Euler characteristic $\chi(G, \mathrm{Sel}(E/F_\infty))$ (cf. [CH2, Th. 1.1]) under the assumption that $\mathrm{Sel}(E/F_\infty)$ is cotorsion as a $\Lambda(G)$-module. Their point of view was to understand how Iwasawa theory over the cyclotomic extension F_{cyc} influences the Iwasawa theory when one climbs up the tower to F_∞.

Let N be a module endowed with the discrete topology and a continuous action of a profinite group G. Let H be a closed normal subgroup of G. Recall the Hochschild–Serre spectral sequence

$$H^r(G/H, H^s(H, N)) \implies H^{r+s}(G, N). \tag{2.2}$$

We shall make repeated use of this sequence with $H = C$, the center of G.

§3. Descent from $GL(2)$ Iwasawa theory to $PGL(2)$ Iwasawa theory

Let us make the following assumptions throughout the rest of this article. Assume that G is a pro-p group. Since $p \geq 5$, we note that the compact p-adic pro-p Lie groups G, C, and PG are all p-torsion-free and hence have p-cohomological dimensions 4, 1, and 3,

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

respectively. Hence, their Iwasawa algebras are all Auslander regular local rings by [V, Th. 3.26].

From the Hochschild–Serre spectral sequence (see (2.2)) with $G = \mathrm{Gal}(F_\infty/F)$, $H = C$, and $G/H = \mathrm{PG}$, it is easy to see that we obtain the commutative diagram (3.1) with exact rows.

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}(E/F_\infty)^C & \longrightarrow & H^1(F_S/F_\infty, E_{p^\infty})^C & \longrightarrow & \left(\oplus_{v\in S} J_v(F_\infty)\right)^C \\ & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \gamma} \\ 0 & \longrightarrow & \mathrm{Sel}(E/K_\infty) & \longrightarrow & H^1(F_S/K_\infty, E_{p^\infty}) & \xrightarrow{\lambda_{K_\infty}} & \oplus_{v\in S} J_v(K_\infty) \end{array} \tag{3.1}$$

The vertical maps are given by restriction maps. Our first objective is to prove the following theorem.

THEOREM 3.1. *The vertical maps α, β, γ in the fundamental diagram (3.1) are all isomorphisms. In particular,*

$$\mathrm{Sel}(E/K_\infty) \cong \mathrm{Sel}(E/F_\infty)^C$$

as $\Lambda(\mathrm{PG})$-modules.

Proof. From the Hochschild–Serre spectral sequence, we have the following exact sequence:

$$0 \to H^1(C, E_{p^\infty}) \to H^1(F_S/K_\infty, E_{p^\infty}) \xrightarrow{\beta} H^1(F_S/F_\infty, E_{p^\infty})^C \to H^2(C, E_{p^\infty}).$$

Since the p-cohomological dimension of C is 1, $H^2(C, E_{p^\infty}) = 0$, and hence the cokernel of the map β is zero. By applying Shapiro's lemma (cf. the proof of [Co1, Lem. 3.1]), we have the following exact sequence:

$$0 \to H^1(\Theta_w^C, E(F_{\infty,w}))(p) \to J_v(K_\infty) \xrightarrow{\gamma_v} \left(J_v(F_\infty)\right)^C \to H^2(\Theta_w^C, E(F_{\infty,w}))(p), \tag{3.2}$$

where w is a prime of F_∞ above v and Θ_w^C is the decomposition group of C at w (see also [CH2, (19), (133), and (134)] for the corresponding exact sequence when K_∞ is replaced by F_{cyc}). As Θ_w^C is a closed subgroup of C which is of dimension 1 as a p-adic Lie group, $H^2(\Theta_w^C, E(F_{\infty,w}))(p) = 0$, which proves that the cokernel of γ_v is zero.

The following argument shows that $\ker(\beta) = H^1(C, E_{p^\infty})$ is zero. The congruence subgroups of $GL_2(\mathbb{Z}_p)$ form a base of neighborhood for its topology, and thus C must contain a scalar matrix

$$x = \begin{pmatrix} 1+p^n & 0 \\ 0 & 1+p^n \end{pmatrix}$$

for n sufficiently large. However, x lies in C, so $x-1$ annihilates $H^1(C, E_{p^\infty})$ (see [Mi, Chap. I, Lem. 6.21]). Therefore, $p^n H^1(C, E_{p^\infty}) = 0$. Now, consider the short exact sequence

$$0 \to E_{p^n} \to E_{p^\infty} \xrightarrow{\times p^n} E_{p^\infty} \to 0. \tag{3.3}$$

As $p^n H^1(C, E_{p^\infty}) = 0$, the long exact sequence corresponding to (3.3) gives rise to the following short exact sequence:

$$0 \to H^1(C, E_{p^\infty}) \to H^2(C, E_{p^n}) \to H^2(C, E_{p^\infty}) \to 0. \tag{3.4}$$

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

Now, C has p-cohomological dimension 1, and hence $H^2(C, E_{p^n}) = 0$. Therefore, $H^1(C, E_{p^\infty}) = 0$ by (3.4). This shows that the map β is injective.

Writing $\gamma = \oplus_{v \in S}\gamma_v$, (3.2) gives

$$\mathrm{Ker}(\gamma_v) = H^1(\Theta_w^C, E(F_{\infty,w}))(p), \tag{3.5}$$

where w is a prime of F_∞ above v and Θ_w^C is the decomposition group of C at w. In the following, it is shown that

$$H^1(\Theta_w^C, E_{p^\infty}) = 0. \tag{3.6}$$

The decomposition subgroup Θ_w^C is a subgroup of C which is pro-p. Therefore, Θ_w^C is a subgroup of $1 + p\mathbb{Z}_p$ and hence a procyclic group. Choose σ to be a topological generator of Θ_w^C; for instance, $\sigma = 1 + p^n$ for some n. By [NS, Prop. 1.7.7],

$$H^1(\Theta_w^C, E_{p^\infty}) = E_{p^\infty}/(\sigma - 1)E_{p^\infty} = E_{p^\infty}/p^n E_{p^\infty}.$$

As E_{p^∞} is a p-divisible group, $E_{p^\infty}/p^n E_{p^\infty} = 0$, giving us $H^1(\Theta_w^C, E_{p^\infty}) = 0$.

If $v \nmid p$, by Kummer theory [G, §2], $H^1(\Theta_w^C, E(F_{\infty,w}))(p) = H^1(\Theta_w^C, E_{p^\infty})$, which vanishes by (3.6). This proves that $\mathrm{Ker}(\gamma_v) = 0$ when $v \nmid p$.

Now, suppose that $v \mid p$. Let u be the prime of K_∞ such that $w \mid u$ and $u \mid v$, and let I_u be the inertia subgroup of K_∞ over F at the prime u. Since I_u is infinite, $K_{\infty,u}$ is deeply ramified (see [CG]). It is also well known that $F_{\infty,w}$ is deeply ramified.

Hence, [CG, Prop. 4.8 and Th. 2.13] gives

$$H^1(K_{\infty,u}, D) \cong H^1(K_{\infty,u}, E)(p), \tag{3.7}$$

$$H^1(F_{\infty,w}, D) \cong H^1(F_{\infty,w}, E)(p), \tag{3.8}$$

where D can be identified with $\tilde{E}_{v,p^\infty}$, the p-primary subgroup of the reduction of E modulo v. Note that E has good ordinary reduction at primes of F above p. By [CG], the module D also satisfies the following exact sequence:

$$0 \to C' \to E_{p^\infty} \to D \to 0, \tag{3.9}$$

where C' is divisible and D is the maximal quotient of E_{p^∞} by a divisible subgroup such that I_v acts on D via a finite quotient. Note that the following sequence is exact:

$$0 \to H^1(\Theta_w^C, D) \to H^1(K_{\infty,u}, D) \to H^1(F_{\infty,w}, D)^{\Theta_w^C}.$$

Hence, using (3.7) and (3.8) into the above exact sequence, it is easy to see that

$$\ker(\gamma_v) = H^1(\Theta_w^C, E(F_{\infty,w}))(p) \cong H^1(\Theta_w^C, D).$$

The exact sequence (3.9) gives that the following sequence

$$H^1(\Theta_w^C, E_{p^\infty}) \to H^1(\Theta_w^C, D) \to H^2(\Theta_w^C, C)$$

is exact. By (3.6), we know that $H^1(\Theta_w^C, E_{p^\infty}) = 0$, and since Θ_w^C is a subgroup of C which has p-cohomological dimension 1, we have $H^2(\Theta_w^C, C) = 0$. Therefore, it is clear that $H^1(\Theta_w^C, D) = 0$, which shows that $\ker(\gamma_v) = 0$ for $v \mid p$.

Thus, the maps β and γ are isomorphisms. The theorem now follows from the snake lemma applied to the fundamental diagram (3.1). □

COROLLARY 3.2. *If $H^1(G, \mathrm{Sel}(E/F_\infty))$ is finite, then $H^1(\mathrm{PG}, \mathrm{Sel}(E/K_\infty))$ is also finite.*

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

Proof. The assertion follows from the natural injection

$$H^1\Big(PG, \big(\mathrm{Sel}(E/F_\infty)\big)^C\Big) \hookrightarrow H^1(G, \mathrm{Sel}(E/F_\infty))$$

and Theorem 3.1. □

The reader is referred to Theorem 2.3 in §2 for cases where $H^1(G, \mathrm{Sel}(E/F_\infty))$ is known to be finite.

3.3 Conditions when the Selmer over PGL(2) extension is cotorsion

The following theorems give several conditions when $\widehat{\mathrm{Sel}(E/K_\infty)}$ is torsion as a $\Lambda(\mathrm{PG})$-module.

THEOREM 3.4. *Assume weak Leopoldt's conjecture at K_∞, that is, $H^2(F_S/K_\infty, E_{p^\infty}) = 0$. Then the dual Selmer group $\widehat{\mathrm{Sel}(E/K_\infty)}$ is $\Lambda(\mathrm{PG})$-torsion if and only if the map λ_{K_∞} in (3.1) is surjective.*

Proof. The proof follows from [SS, Th. 7.2]. □

THEOREM 3.5. *The dual Selmer group $\widehat{\mathrm{Sel}(E/K_\infty)}$ is a torsion $\Lambda(\mathrm{PG})$-module if any of the following conditions hold:*

1. *The Selmer group $\mathrm{Sel}(E/F)$ is finite and $H_2(\mathrm{PG}, \widehat{\mathrm{Sel}(E/K_\infty)})$ is finite.*
2. *The Selmer group $\mathrm{Sel}(E/F)$ is finite, $\widehat{\mathrm{Sel}(E/F_\infty)}$ is a torsion $\Lambda(G)$-module, and $H_0(\mathrm{PG}, H_1(C, \widehat{\mathrm{Sel}(E/F_\infty)}))$ is finite.*
3. *$\widehat{\mathrm{Sel}(E/F_\infty)}$ is a torsion $\Lambda(G)$-module and $H_1(C, \widehat{\mathrm{Sel}(E/F_\infty)}) = 0$.*

Conversely, if $\widehat{\mathrm{Sel}(E/K_\infty)}$ is a torsion $\Lambda(\mathrm{PG})$-module, then (3) holds.

Proof. Let $M = \widehat{\mathrm{Sel}(E/F_\infty)}$. We have $M_G \cong H_0(\mathrm{PG}, M_C)$ and $M_C \cong \widehat{\mathrm{Sel}(E/K_\infty)}$. Now, since $\mathrm{Sel}(E/F)$ is finite, by Theorem 2.3, it follows that $H_0(\mathrm{PG}, M_C)$ is finite. By assumption, $H_2(\mathrm{PG}, M_C)$ is also finite. Since

$$\mathrm{rank}_{\Lambda(\mathrm{PG})} M_C = \sum_{k\geq 0}^{3} (-1)^k \mathrm{rank}_{\mathbb{Z}_p} H_k(\mathrm{PG}, M_C)$$

(see [Ho2, Th. 1.1]), we obtain $\mathrm{rank}_{\Lambda(\mathrm{PG})} M_C = 0$ and hence M_C is $\Lambda(\mathrm{PG})$-torsion. This shows that $\widehat{\mathrm{Sel}(E/K_\infty)}$ is a torsion as a $\Lambda(\mathrm{PG})$-module and hence proves that the condition (1) is sufficient.

To show that the condition in (2) is also sufficient, note that if M is $\Lambda(G)$-torsion and $\mathrm{Sel}(E/F)$ is finite, then $H_1(G, M)$ is finite and $H_2(G, M) = 0$ (see Theorem 2.3). By Hochschild–Serre spectral sequence, we conclude that $H_0(\mathrm{PG}, H_1(C, M))$ is finite if and only if $H_2(\mathrm{PG}, M_C)$ is finite, and hence (2) follows from (1).

For (3), note that it follows from [Ho2, Th. 1.1] the Hochschild–Serre spectral sequence (use (2.2) with $H = C$ and $N = H_l(C, M)$) that

$$\mathrm{rank}_{\Lambda(G)} M = \sum_{k\geq 0} (-1)^k \mathrm{rank}_{\mathbb{Z}_p} H_k(G, M) \tag{3.10}$$

$$= \sum_{k,l\geq 0} (-1)^{k+l} \mathrm{rank}_{\mathbb{Z}_p} H_k(\mathrm{PG}, H_l(C, M)) \tag{3.11}$$

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

$$= \sum_{l\geq 0}(-1)^l \mathrm{rank}_{\Lambda(\mathrm{PG})} H_l(C,M) \tag{3.12}$$

$$= \mathrm{rank}_{\Lambda(\mathrm{PG})} M_C - \mathrm{rank}_{\Lambda(\mathrm{PG})} H_1(C,M). \tag{3.13}$$

Suppose (3) holds. Since $H_1(C,M)$ is precisely the $\Lambda(G)$-submodule of M consisting of the elements in M annihilated by the augmentation ideal $I(C)=\langle c-1\rangle$, we have $H_1(C,M)=0$. Hence, the conclusion follows from (3.13) and Theorem 3.1.

Finally, suppose if $M_C \cong \widehat{\mathrm{Sel}(E/K_\infty)}$ is a torsion $\Lambda(\mathrm{PG})$-module. Then it follows from (3.13) that M is torsion as a $\Lambda(G)$-module and $H_1(C,M)$ is torsion as a $\Lambda(\mathrm{PG})$-module. Then $H_1(C,M)$ is pseudonull as a $\Lambda(G)$-module. However, M has no nonzero pseudonull submodules (see [OV, Th. 5.1]), and therefore $H_1(C,M)=0$. □

The following theorem gives a restatement of condition (3) in Theorem 3.5 using the structure theorem of dual Selmer groups over noncommutative Iwasawa algebras [CSS]. By [CSS], there is an injection of $\Lambda(G)$-modules

$$\oplus_{i=1}^m \Lambda(G)/J_i \hookrightarrow M/M_0$$

with pseudonull cokernel. Here, J_i's are reflexive ideals in $\Lambda(G)$ which are pure of grade 1, and M_0 is the maximal pseudonull submodule of M. Recall that $M=\widehat{\mathrm{Sel}(E/F_\infty)}$; hence, M has no nontrivial pseudonull submodule and therefore $M_0=0$. This gives the exact sequence

$$0 \to \oplus_{i=1}^m \Lambda(G)/J_i \to M \to N \to 0, \tag{3.14}$$

where N is a pseudonull $\Lambda(G)$-module.

THEOREM 3.6. *The Selmer group* $\mathrm{Sel}(E/K_\infty)$ *is a cotorsion* $\Lambda(\mathrm{PG})$*-module if and only if* $\mathrm{Sel}(E/F_\infty)$ *is a cotorsion* $\Lambda(G)$*-module and* $H_1(C,\oplus_{i=1}^m \Lambda(G)/J_i)=0$.

Proof. Since the center C has p-cohomological dimension 1, the sequence (3.14) gives the following exact sequence of $\Lambda(\mathrm{PG})$-modules:

$$0 \to H_1(C,\oplus_{i=1}^m \Lambda(G)/J_i) \to H_1(C,M) \to H_1(C,N) \tag{3.15}$$

$$\to (\oplus_{i=1}^m \Lambda(G)/J_i)_C \to M_C \to N_C \to 0. \tag{3.16}$$

Let $\overline{J_i}$ be the image of J_i under the natural projection $\Lambda(G)\to\Lambda(G/C)=\Lambda(G)/I(C)$. Since $H_1(C,\Lambda(G)/J_i)=0$ for each $i=[1,m]$ by assumption, then $J_i \nsubseteq I(C)$ and hence $\overline{J_i}$ is nonzero. Therefore, we have

$$\dim_{\Lambda(\mathrm{PG})}(\Lambda(G)/J_i)_C = \dim_{\Lambda(\mathrm{PG})}(\Lambda(G/C)/\overline{J_i}) < \dim \Lambda(\mathrm{PG}) = 4, \tag{3.17}$$

which implies that $(\Lambda(G)/J_i)_C$ is $\Lambda(\mathrm{PG})$-torsion. Now, as N is a pseudonull $\Lambda(G)$-module,

$$\dim_{\Lambda(G)} N \leq \dim \Lambda(G) - 2 = \dim \Lambda(\mathrm{PG}) - 1.$$

This implies that N_C is a torsion $\Lambda(\mathrm{PG})$-module, and the same holds for the module M_C from (3.17) and (3.16).

Conversely, suppose that $M_C \cong \widehat{\mathrm{Sel}(E/K_\infty)}$ is torsion as a $\Lambda(\mathrm{PG})$-module. Then, by Theorem 3.5, M is torsion as a $\Lambda(G)$-module and $H_1(C,M)=0$ whence $H_1(C,\oplus_{i=1}^m \Lambda(G)/J_i)=0$ by (3.15). □

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

REMARK 3.7. We note that the ideals J_i cannot be $I(C)$ for all $i \geq 1$ because the center C cannot act trivially on the Selmer group at F_∞ (see Proposition 3.8).

Suppose none of the ideals J_i are contained in $I(C)$. Then $\widehat{\mathrm{Sel}(E/K_\infty)}$ is torsion as a $\Lambda(\mathrm{PG})$-module. On the other hand, if $J_i = I(C)$ for some i, then $\widehat{\mathrm{Sel}(E/K_\infty)}$ cannot be torsion as a $\Lambda(\mathrm{PG})$-module (see Theorem 3.6).

Suppose $\mathrm{Sel}(E/F_\infty)$ is cotorsion as a $\Lambda(G)$-module, and $\mathrm{Sel}(E/F)$ and $H_1(G,N)$ are finite. Then none of the ideals J_i can be contained in $I(C)$. This is because, from (3.14), we obtain the exact sequence

$$H_1(G,N) \to (\oplus_{i=1}^m \Lambda(G)/J_i)_G \to M_G,$$

whose first and last terms are finite. In this case, $\widehat{\mathrm{Sel}(E/K_\infty)}$ is torsion as a $\Lambda(\mathrm{PG})$-module.

In [CSS, Prop. 8.10], for the elliptic curve $E = X_1(11) : y^2 + y = x^3 - x^2$ of conductor 11 and prime $p = 5$, the authors show that the center C cannot act trivially on $\mathrm{Sel}(E/F_\infty)$. The following proposition generalizes this for any elliptic curve without complex multiplication and with good ordinary reduction for the primes above p.

PROPOSITION 3.8. *Suppose $G \cong C \times \mathrm{PG}$, and $\mathrm{Sel}(E/F)$ is finite. Then the center C cannot act trivially on $\mathrm{Sel}(E/F_\infty)$.*

Proof. If C acts trivially on $\mathrm{Sel}(E/F_\infty)$, then

$$\mathrm{Sel}(E/F_\infty) = \mathrm{Sel}(E/F_\infty)^C \cong \mathrm{Sel}(E/K_\infty).$$

Hoewever, $\mathrm{Sel}(E/K_\infty)$ is cofinitely generated over $\Lambda(\mathrm{PG})$ and so with the above identification, $\mathrm{Sel}(E/F_\infty)$ is cotorsion over $\Lambda(G)$. As $\mathrm{Sel}(E/F_\infty)$ is $\Lambda(G)$-cotorsion and $\mathrm{Sel}(E/F)$ is finite, the cohomology groups $H^i(G, \mathrm{Sel}(E/F_\infty))$ are finite for all i. The degeneration of the Hochschild–Serre spectral sequence (see [NS, Prop. 2.4.5]) gives an injection

$$H^i(\mathrm{PG}, \mathrm{Sel}(E/K_\infty)) \hookrightarrow H^i(G, \mathrm{Sel}(E/F_\infty)).$$

This implies that the cohomology groups $H^i(\mathrm{PG}, \mathrm{Sel}(E/K_\infty))$ are finite for all i. Hence,

$$\mathrm{rank}_{\Lambda(\mathrm{PG})} \widehat{\mathrm{Sel}(E/K_\infty)} = \sum_{i \geq 0} (-1)^i \mathrm{rank}_{\mathbb{Z}_p} H_i(\mathrm{PG}, \widehat{\mathrm{Sel}(E/K_\infty)}) = 0,$$

whereby $\mathrm{Sel}(E/K_\infty)$ is $\Lambda(\mathrm{PG})$-cotorsion. We deduce that

$$\dim_{\Lambda(G)} \widehat{\mathrm{Sel}(E/F_\infty)} \leq \dim \Lambda(\mathrm{PG}) - 1 = \dim \Lambda(G) - 2.$$

This would imply that $\widehat{\mathrm{Sel}(E/F_\infty)}$ is a pseudonull $\Lambda(G)$-module. However, $\widehat{\mathrm{Sel}(E/F_\infty)}$ has no nonzero pseudonull submodules. Hence, $\widehat{\mathrm{Sel}(E/F_\infty)} = 0$. On the other hand, it is known that $\widehat{\mathrm{Sel}(E/F_\infty)}$ is infinite dimensional as a $\mathbb{Q}_p$-vector space (see [Co1, Th. 1.5]). This gives us a contradiction. □

EXAMPLES 3.9. Here are some examples of elliptic curves E such that $G = \mathrm{Gal}(F_\infty/F)$ is a direct product of its center C and PG. We follow the nomenclature from Cremona tables [Cr].

1. Let E be the elliptic curve $X_1(11)$, namely E is the curve $y^2 + y = x^3 - x^2$ and prime $p = 5$. This is a curve of conductor 11 defined over $\mathbb{Q}$, but we consider it over $F = \mathbb{Q}(\mu_5)$.

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

Put $F_\infty = F(E_{5^\infty})$. Then $G = \mathrm{Gal}(F_\infty/F)$ has the form $G = C \times PG$ [CSS, Exam. 8.7, p. 104].

2. Let E be the elliptic curve $X_0(11)$, namely E is the curve $y^2 + y = x^3 - x^2 - 10x - 20$ and $p = 5$. This is a curve of conductor 11 defined over $\mathbb{Q}$, but we consider it over $F = \mathbb{Q}(\mu_5)$. Put $F_\infty = F(E_{5^\infty})$. Then the Galois group $G = \mathrm{Gal}(F_\infty/F)$ is a subgroup of the first congruence kernel of $GL_2(\mathbb{Z}_5)$ [F, (3), p. 586]. Hence, G is of the form $C \times \mathrm{PG}$.
3. For any general elliptic curve E over F without complex multiplication and with good ordinary reduction for the primes above p, we can always find an integer k large enough such that, over the base field $F[E_{p^k}]$, the Galois group $G = \mathrm{Gal}(F_\infty/F[E_{p^k}])$ lies inside the first congruence kernel of $GL_2(\mathbb{Z}_p)$ and hence can be written in the form $C \times \mathrm{PG}$. The center C can be identified with a subgroup of diagonal matrices of a certain form (see [V, Rem. 4.11]).

§4. Applications

Suppose $G \cong \mathrm{PG} \times C$. Let $C_n = C^{p^n}$ and $G_n = \mathrm{PG} \times C_n$. Note that $G_n \neq G^{p^n}$. Let $M = \widehat{\mathrm{Sel}(E/F_\infty)}$.

PROPOSITION 4.1. *Suppose that M is a torsion $\Lambda(G)$-module. Then, for all large n, $\mathrm{rank}_{\Lambda(\mathrm{PG})} M_{C_n}$ is a constant, independent of n.*

Proof. As G_n is of finite index in G, M is also a finitely generated module over $\Lambda(G_n)$. As $C_n \cong \mathbb{Z}_p$, we can identify M^{C_n} with $H_1(C_n, M)$ and then they both are finitely generated over $\Lambda(\mathrm{PG})$. The Hochschild–Serre spectral sequence $H^r(\mathrm{PG}, H^s(C_n, M)) \Longrightarrow H^{r+s}(G, M)$ and the argument as in (3.10)–(3.13) give

$$\mathrm{rank}_{\Lambda(G_n)} M = \mathrm{rank}_{\Lambda(\mathrm{PG})} M_{C_n} - \mathrm{rank}_{\Lambda(\mathrm{PG})} H_1(C_n, M).$$

Identifying M^{C_n} with $H_1(C_n, M)$, we deduce

$$\begin{aligned} \mathrm{rank}_{\Lambda(\mathrm{PG})} M_{C_n} &= \mathrm{rank}_{\Lambda(G_n)} M + \mathrm{rank}_{\Lambda(\mathrm{PG})} M^{C_n} \\ &= p^n \mathrm{rank}_{\Lambda(G)} M + \mathrm{rank}_{\Lambda(\mathrm{PG})} M^{C_n} \\ &= \mathrm{rank}_{\Lambda(\mathrm{PG})} M^{C_n}. \end{aligned}$$

(The second equality follows since G_n is of index p^n in G, and the third equality follows as M is a torsion $\Lambda(G)$-module by assumption.) Note that C_n is in the center, and hence abelian, and therefore M^{C_n} is a $\Lambda(G)$-submodule of M. However, M is a finitely generated module over $\Lambda(G)$, and hence M is a Noetherian module and satisfies the ascending chain condition on its submodules. Hence, the chain

$$M^{C_0 = C} \subset M^{C_1} \subset \cdots M^{C_n} \cdots$$

stabilizes and so $\mathrm{rank}_{\Lambda(\mathrm{PG})} M^{C_n}$ is a constant independent of n, for all sufficiently large n. ∎

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

Consider the following fundamental diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}(E/K_\infty)^{\mathrm{PG}} & \longrightarrow & H^1(F_S/K_\infty, E_{p^\infty})^{\mathrm{PG}} & \xrightarrow{\lambda_{K_\infty}^{\mathrm{PG}}} & \left(\oplus_{v\in S} J_v(K_\infty)\right)^{\mathrm{PG}} \\ & & \uparrow f & & \uparrow g & & \uparrow h \\ 0 & \longrightarrow & \mathrm{Sel}(E/F) & \longrightarrow & H^1(F_S/F, E_{p^\infty}) & \xrightarrow{\lambda_F} & \oplus_{v\in S} H^1(F_v, E)(p). \end{array} \tag{4.1}$$

Let $\mathrm{Coker}(\lambda_{K_\infty}^{\mathrm{PG}})$ be the cokernel of the map $\lambda_{K_\infty}^{\mathrm{PG}}$ in (4.1).

THEOREM 4.2. *The vertical maps f, g, h in the fundamental diagram (4.1) have finite kernels and cokernels. Furthermore, if* $\mathrm{Sel}(E/F)$ *is finite, then* $\mathrm{Coker}(\lambda_{K_\infty}^{\mathrm{PG}})$ *is finite.*

Proof. Since $H^1(C, E_{p^\infty}) = 0$, using Hochschild–Serre spectral sequence and noting that the cohomology groups

$$H^i(\mathrm{PG}, E_{p^\infty}(K_\infty)) = H^i(G, E_{p^\infty})$$

are finite for $i \geq 1$, it is easy to see that the kernel and the cokernel of g are finite.

Next, we decompose h into local components $h = \oplus_{v\in S} h_v$ and analyze the kernel of cokernel of the map h_v.

Let w be a prime of F_∞ above $v \in S$, and let u be a prime of K_∞ below w. If one denotes Θ_u (resp., Δ_w) the decomposition group of PG at u (resp., the decomposition group of G at w), then one has an isomorphism $\Theta_u = \Delta_w/C \cap \Delta_w$.

By Shapiro's lemma, $H^i(\mathrm{PG}, J_v(K_\infty)) \cong H^i(\Theta_u, H^1(K_{\infty,u}, E)(p))$.

By Hochschild–Serre spectral sequence, the following sequence is exact:

$$\begin{aligned} 0 \to H^1(\Theta_u, E(K_{\infty,u}))(p) \to H^1(F_v, E)(p) \xrightarrow{h_v} H^1(K_{\infty,u}, E)(p)^{\Theta_u} \\ \to H^2(\Theta_u, E(K_{\infty,u}))(p). \end{aligned}$$

Therefore, to prove that $\ker(h_v)$ and $\mathrm{cokernel}(h_v)$ are finite, it is sufficient to show that

1. $H^1(\Theta_u, E(K_{\infty,u}))(p)$ is finite, and
2. $H^2(\Theta_u, E(K_{\infty,u}))(p)$ is finite.

Consider the following exact sequence:

$$0 \to H^1(\Theta_u, E(K_{\infty,u}))(p) \to H^1(\Delta_w, E(F_{\infty,w}))(p) \to H^1(C \cap \Delta_w, E(F_{\infty,w}))(p)^{\Theta_u} \tag{4.2}$$

$$\to H^2(\Theta_u, E(K_{\infty,u}))(p) \to H^2(\Delta_w, E(F_{\infty,w}))(p). \tag{4.3}$$

With $\Theta_w^C = C \cap \Delta_w$, the third term of the above exact sequence is

$$H^1(C \cap \Delta_w, E(F_{\infty,w}))(p)^{\Theta_u} = H^1(\Theta_w^C, E(F_{\infty,w}))(p)^{\Theta_u} = \mathrm{Ker}(\gamma_v)^{\Theta_u}.$$

The last equality is due to (3.5), which is zero by Theorem 3.1.

Therefore, by the exact sequence (4.2), it suffices to show that

1. $H^1(\Delta_w, E(F_{\infty,w}))(p)$ is finite, and
2. $H^2(\Delta_w, E(F_{\infty,w}))(p)$ is finite.

However, $H^1(\Delta_w, E(F_{\infty,w}))(p)$ and $H^2(\Delta_w, E(F_{\infty,w}))(p)$ are the kernel and cokernel of the map δ_v, the local map of the following fundamental diagram which is known to be

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

finite by the work of Coates and Howson (cf. proof of [CH2, Prop. 3.3] or Proposition 5.21 of [Ho1]):

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}(E/F_\infty)^G & \longrightarrow & H^1(F_S/F_\infty, E_{p^\infty})^G & \longrightarrow & \left(\oplus_{v\in S} J_v(F_\infty)\right)^G \\ & & \uparrow & & \uparrow & & \uparrow{\scriptstyle \oplus_{v\in S}\delta_v} \\ 0 & \longrightarrow & \mathrm{Sel}(E/F) & \longrightarrow & H^1(F_S/F, E_{p^\infty}) & \longrightarrow & \oplus_{v\in S} H^1(F_v, E)(p). \end{array} \tag{4.4}$$

Therefore, the kernel and cokernel of h are finite. By the snake lemma, we deduce that the same is true for f.

If $\mathrm{Sel}(E/F)$ is finite, $\mathrm{Coker}(\lambda_F)$ is finite (cf. [CS1, p. 35]). This implies that $\mathrm{Coker}(h\circ\lambda_F)$ is finite. However, $\mathrm{Coker}(h\circ\lambda_F) = \mathrm{Coker}(\lambda_{K_\infty}^{\mathrm{PG}}\circ g)$, and hence $\mathrm{Coker}(\lambda_{K_\infty}^{\mathrm{PG}})$ is finite. □

Let $\mathcal{M}$ be the category of all finitely generated $\Lambda(G)$-modules, let $\mathcal{C}$ be the full subcategory of all pseudonull modules in $\mathcal{M}$, and let $q:\mathcal{M}\to\mathcal{M}/\mathcal{C}$ denote the quotient functor. From [A, §1.3], recall that an object $q(M)$ in the quotient category $\mathcal{M}/\mathcal{C}$ is said to be *completely faithful* if $\mathrm{Ann}(N)=0$ for any $N\in\mathcal{M}$ such that $q(N)$ is isomorphic to a nonzero subquotient of $q(M)$.

LEMMA 4.3. *(see [Co2, Lem. 9][1]) Suppose* $q(\widehat{\mathrm{Sel}(E/F_\infty)})$ *is completely faithful. Then* $\mathrm{Sel}(E/K_\infty)$ *is* $\Lambda(\mathrm{PG})$*-cotorsion.*

REMARK 4.4. In [BZ, §7], the authors consider an elliptic curve E over a number field and study the dual Selmer group of E over a PG-extension that arises from the trivializing extension of the Galois representation associated with *another* elliptic curve A. The example in [BZ, §7] combined with the method of the proof of [Co2, Lem. 9] extend to give an example of the dual Selmer group of E which is cotorsion over the PG-extension arising from the trivializing extension defined by the elliptic curve A. However, we are primarily interested in studying the cotorsion property of the dual Selmer group over the PG-extension of the number field contained in the trivializing extension of the *same* elliptic curve. A detailed study is currently underway in a broader context.

The Euler characteristic of the Selmer group of the $PGL(2)$ extension has been computed in Zerbes' dissertation [Z, Chap. 8] and Howson's dissertation [Ho1, Th. 5.34], but we include a simpler proof here.

Let $\chi(\mathrm{PG},\mathrm{Sel}(E/K_\infty))$ be the Euler characteristic of Selmer group of the PGL(2) extension, and let

$$\xi_p(E/F) = \rho_p(E/F)\times\prod_{v\in B}(1/L_v(E,1))^{(p)} \tag{4.5}$$

be defined as in [CS1, §3.14].

THEOREM 4.5. *Suppose* $\mathrm{Sel}(E/K_\infty)$ *is* $\Lambda(\mathrm{PG})$*-cotorsion and* $\mathrm{Sel}(E/F)$ *is finite. Then* $\mathrm{Sel}(E/K_\infty)$ *has finite Euler characteristic given by*

$$\chi(\mathrm{PG},\mathrm{Sel}(E/K_\infty)) = \chi(G,\mathrm{Sel}(E/F_\infty)) = \xi_p(E/F), \tag{4.6}$$

where $\xi_p(E/F)$ *is as in (4.5).*

[1] We thank the referee for reminding us about this reference.

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

Proof. Since $\mathrm{Sel}(E/K_\infty)$ is $\Lambda(\mathrm{PG})$-cotorsion, it implies that $\mathrm{Sel}(E/F_\infty)$ is $\Lambda(G)$-torsion and $H^1(C,\mathrm{Sel}(E/F_\infty))=0$ (cf. Theorems 3.5 and 3.6). The Hochschild–Serre spectral sequence

$$H^i(\mathrm{PG},H^j(C,\mathrm{Sel}(E/F_\infty)))\implies H^{i+j}(G,\mathrm{Sel}(E/F_\infty))$$

gives

$$\chi(G,\mathrm{Sel}(E/F_\infty))=\sum_{i\geq 0}(-1)^i\chi(\mathrm{PG},H^i(C,\mathrm{Sel}(E/F_\infty)))=\chi(\mathrm{PG},\mathrm{Sel}(E/K_\infty)).$$

Under the assumption that $\mathrm{Sel}(E/F)$ is finite, $\chi(G,\mathrm{Sel}(E/F_\infty))$ equals $\xi_p(E/F)$ by [CS1, Th. 3.16]. □

The quantity $\xi_p(E/F)$ in (4.5) is related to the exact formula of the p-part of Birch and Swinnerton-Dyer conjecture, which in turn gives the value of the p-part of the leading coefficient of the complex L-value at 1.

Suppose that $\widehat{\mathrm{Sel}(E/F_{\mathrm{cyc}})}$ is $\Lambda(\Gamma)$-torsion (e.g., $F=\mathbb{Q}$) and $\mathrm{Sel}(E/F)$ is finite. It is well known that $\chi(\Gamma,\mathrm{Sel}(E/F_{\mathrm{cyc}}))=\rho_p(E/F)$ (cf. [CS1, Th. 3.3]). From (4.5) and (4.6), we obtain

$$\chi(\mathrm{PG},\mathrm{Sel}(E/K_\infty))=\chi(G,\mathrm{Sel}(E/F_\infty))=\chi(\Gamma,\mathrm{Sel}(E/F_{\mathrm{cyc}}))\times\prod_{v\in B}(1/L_v(E,1))^{(p)}.$$

Then the Iwasawa Main Conjecture predicts that the characteristic ideal of $\widehat{\mathrm{Sel}(E/F_{\mathrm{cyc}})}$ is generated by a p-adic L-function $f_E(T)\in\Lambda(\Gamma)$. Since $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-cotorsion, we deduce that the leading term of $f_E(T)$ is nonzero and

$$f_E(0)\sim\chi(\Gamma,\mathrm{Sel}(E/F_{\mathrm{cyc}})).$$

Here, $a\sim b$ means that a and b both have the same p-adic valuation (cf. [G, Lem. 4.2]). This gives a conjectural connection of $f_E(T)$ with the value of the Hasse–Weil complex L-function $L(E/F,s)$ at $s=1$. This is based on the Birch and Swinnerton-Dyer conjecture for E over F. The conjecture then asserts that $L(E/F,1)\neq 0$, and for a suitably defined period $\Omega(E/F)$, the value $L(E/F,1)/\Omega(E/F)$ is rational. One would then expect

$$f_E(0)\sim\Big(\prod_{v|p}(1-\beta_v N(v)^{-1})^2\Big)L(E/F,1)/\Omega(E/F),$$

where $(1-\beta_v N(v)^{-1})^2$ is a certain Euler factor as in [G, p. 91].

The nonexistence of nontrivial pseudonull submodules of $\widehat{\mathrm{Sel}(E/K_\infty)}$ has been dealt with in Zerbes' dissertation [Z, Chap. 9, §3]. The referee suggested that we include a proof of this assertion. This is done in the following theorem. Our proof is different to that of [Z, Chap. 9, §3]. The proof uses a standard result from Iwasawa theory and is originally due to Greenberg for commutative Iwasawa algebras.

THEOREM 4.6. *Assume weak Leopoldt's conjecture at K_∞, that is, $H^2(F_S/K_\infty,E_{p^\infty})=0$. Suppose $\mathrm{Sel}(E/K_\infty)$ is $\Lambda(\mathrm{PG})$-cotorsion. Then $\widehat{\mathrm{Sel}(E/K_\infty)}$ has no nontrivial pseudonull submodule.*

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

Proof. Let S_p be the set of places of S above the prime p. As $\mathrm{Sel}(E/K_\infty)$ is $\Lambda(\mathrm{PG})$-cotorsion, Theorem 3.4 gives the exact sequence

$$0 \to \bigoplus_{v\in S_p} \widehat{J_v(K_\infty)} \bigoplus \bigoplus_{v\in S\setminus S_p} \widehat{J_v(K_\infty)} \to H^1(F_S\widehat{/K_\infty}, E_{p^\infty}) \to \widehat{\mathrm{Sel}(E/K_\infty)} \to 0. \tag{4.7}$$

By Theorem 3.1, $\widehat{J_v(K_\infty)} = \widehat{J_v(F_\infty)}_C$ for all $v \in S$.

For $v \in S_p$, the corresponding decomposition subgroup of the Galois group of the trivializing extension F_∞ is of dimension 3 (see [CH2, Lem. 5.1]). Hence, $\widehat{J_v(F_\infty)}$ is free as a $\Lambda(G)$-module (see [OV, Lem. 5.4(i)]), whence $\widehat{J_v(K_\infty)}$ is free as a $\Lambda(\mathrm{PG})$-module.

For $v \in S\setminus S_p$, $J_v(F_\infty) = 0$ (see [CH2, Lem. 5.4]), and hence $J_v(K_\infty) = 0$.

Since $H^2(F_S/K_\infty, E_{p^\infty}) = 0$, [OV, Th. 4.7] allows us to conclude that $H^1(F_S\widehat{/K_\infty}, E_{p^\infty})$ has no nonzero pseudonull submodule.

Now, (4.7) gives an exact sequence where the first term is $\Lambda(\mathrm{PG})$-free, and the middle term has no nonzero pseudonull submodule. An analogue of the argument by Greenberg referred to above (see [HO, Prop. 3.5]) allows us to conclude that $\widehat{\mathrm{Sel}(E/K_\infty)}$ has no nontrivial pseudonull submodule. □

It seems to us that the full strength of the structure theorem has not been exploited. Specifically, the ideals in the summands are reflexive and pure of grade 1. It might be possible to use this effectively to study the homology groups $H_j(\mathrm{PG}, \Lambda(G)/J_i)$. This would then yield finer results on the structure of the dual Selmer group. We hope to return to this line of investigation later.

Acknowledgments. The authors would like to thank Konstantin Ardakov, Srikanth B. Iyengar, Antonio Lei, and Dipendra Prasad for helpful discussions. Jishnu Ray would also like to thank the organizers of "Iwasawa 2019" conference (June 2019, Bordeaux) for invitation to speak. Theorem 3.1 in this article was announced in that conference. Jishnu Ray is very grateful to Sarah Zerbes for sending him a copy of her Ph.D. dissertation on Selmer groups over p-adic Lie extensions. Finally, the authors thank the referees for their careful reading of the article and suggestions, which helped improve the exposition.

References

[A] K. Ardakov, *Centres of skewfields and completely faithful Iwasawa modules*, J. Inst. Math. Jussieu **7** (2008), 457–468.

[BZ] T. Backhausz and G. Zábrádi, *Algebraic functional equations and completely faithful Selmer groups*, Int. J. Number Theory **11** (2015), 1233–1257.

[Bo] N. Bourbaki, *Commutative Algebra. Chapters 1–7*, Elem. Math. (Berlin), Springer, Berlin, 1998, translated from the French, reprint of the 1989 English translation.

[Co1] J. Coates, "Fragments of the GL_2 Iwasawa theory of elliptic curves without complex multiplication" in *Arithmetic Theory of Elliptic Curves (Cetraro, 1997)*, Lecture Notes in Math. **1716**, Springer, Berlin, 1999, 1–50.

[Co2] J. Coates, "Elliptic Curves — The Crossroads of Theory and Computation" In: Fieker, C., Kohel, D.R. (eds) Algorithmic Number Theory. ANTS 2002. Lecture Notes in Computer Science, vol 2369. Springer, Berlin, Heidelberg.

[CFK+] 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. **101** (2005), 163–208.

[CG] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), 129–174.

[CH1] J. Coates and S. Howson, *Euler characteristics and elliptic curves*, *Proc. Natl. Acad. Sci. USA* **94** (1997), 11115–11117, elliptic curves and modular forms (Washington, DC, 1996).

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press

[CH2] J. Coates and S. Howson, *Euler characteristics and elliptic curves II*, *J. Math. Soc. Japan* **53** (2001), 175–235.
[CSS] J. Coates, P. Schneider, and R. Sujatha, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2** (2003), 73–108.
[CS1] J. Coates and R. Sujatha, *Galois Cohomology of Elliptic Curves*, 2nd ed., Narosa, New Delhi, 2010, for the Tata Institute of Fundamental Research, Mumbai.
[CS2] J. Coates and R. Sujatha, "On the $M_H(G)$-conjecture" in *Non-Abelian Fundamental Groups and Iwasawa Theory*, London Math. Soc. Lecture Note Ser. **393**, Cambridge Univ. Press, Cambridge, 2012, 132–161.
[Cr] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.
[F] T. Fisher, *Descent calculations for the elliptic curves of conductor 11*, Proc. Lond. Math. Soc. **86** (2003), 583–606.
[G] R. Greenberg, "Iwasawa theory for elliptic curves" in *Arithmetic Theory of Elliptic Curves (Cetraro, 1997)*, Lecture Notes in Math. **1716**, Springer, Berlin, 1999, 51–144.
[HO] Y. Hachimori and T. Ochiai, *Notes on non-commutative Iwasawa theory*, Asian J. Math. **14** (2010), 11–18.
[Ho1] S. Howson, *Iwasawa theory of elliptic curves for p-adic Lie extensions*, Ph.D. dissertation, University of Cambridge, Cambridge, 1998.
[Ho2] S. Howson, *Euler characteristics as invariants of Iwasawa modules*, Proc. Lond. Math. Soc. **85** (2002), 634–658.
[K] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, *Astérisque* **295** (2004), 117–290, cohomologies p-adiques et applications arithmétiques. III.
[Ma] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.
[Mi] J. S. Milne, *Arithmetic duality theorems*, Perspect. Math. **1**, Academic Press, Boston, MA, 1986.
[NS] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren Math. Wiss. [Fund. Principles Math. Sci.] **323**, Springer, Berlin, 2008.
[OV] Y. Ochi and O. Venjakob, *On the structure of Selmer groups over p-adic Lie extensions*, J. Algebraic Geom. **11** (2002), 547–580.
[S] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
[SS] S. Shekhar and R. Sujatha, *On the structure of Selmer groups of Λ-adic deformations over p-adic Lie extensions*, Doc. Math. **17** (2012), 573–606.
[V] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. (JEMS) **4** (2002), 271–311.
[Z] S. Zerbes, *Selmer groups over p-adic Lie extensions*, Ph.D. dissertation, University of Cambridge, Cambridge, 2005.

Jishnu Ray
Institute for Advancing Intelligence
TCG Centres for Research and Education in Science and Technology
1st Floor, Tower 1, Bengal Eco Intelligent Park (Techna Building)
Block EM, Plot No 3, Sector V, Salt Lake
Kolkata 700091, India
jishnu.ray@tcgcrest.org,jishnuray1992@gmail.com

R. Sujatha
Department of Mathematics
The University of British Columbia
Room 121, 1984 Mathematics Road
Vancouver, BC V6T 1Z2, Canada
sujatha@math.ubc.ca

https://doi.org/10.1017/nmj.2022.14 Published online by Cambridge University Press