Proceedings of the London Mathematical Society Advance Access published June 2, 2010

Proc. London Math. Soc. Page 1 of 38 © 2010 London Mathematical Society
doi:10.1112/plms/pdq015

Pairings and functional equations over the GL_2-extension[†]

Gergely Zábrádi

Abstract

We construct a pairing on the dual Selmer group over the GL_2-extension $\mathbb{Q}(E[p^\infty])$ of an elliptic curve without complex multiplication and with good ordinary reduction at a prime $p \geqslant 5$ whenever it satisfies certain, conjectured, torsion properties. This gives a functional equation of the characteristic element which is compatible with the conjectural functional equation of the p-adic L-function. As an application we reduce the parity conjecture for the p-Selmer rank and the analytic root number for the twists of elliptic curves with self-dual Artin representation to the case when the Artin representation factors through the quotient of $\mathrm{Gal}(\mathbb{Q}(E[p^\infty])/\mathbb{Q})$ by its maximal pro-p normal subgroup. This gives a new proof of the parity conjecture whenever the elliptic curve E has a p-isogeny over the rationals.

1. *Introduction*

The main conjectures of Iwasawa theory usually state that (i) there exists a p-adic L-function attached to the elliptic curve over a p-adic Lie extension of $\mathbb{Q}$, which interpolates the special values of the complex L-functions of the elliptic curve twisted by Artin representations of the Galois group and (ii) this p-adic L-function is a characteristic element for the dual of the Selmer group. These are the only tools known at present for studying the mysterious relationship between the arithmetic properties of elliptic curves and the special values of their complex L-functions, especially for attacking the conjectures of Birch and Swinnerton-Dyer. The p-adic L-function in the GL_2-case (and also in the false Tate curve case) lies in the algebraic K_1-group of $\Lambda(G)_{S^*}$, the Iwasawa algebra of the Galois group localized by a canonical Ore set defined in [7].

The aim of this paper is to investigate the conjectural functional equation of the p-adic L-function from both the algebraic and analytic side. The heuristics for the existence of this functional equation is the following. The p-adic L-function $\mathcal{L}_E$ conjecturally interpolates a certain modification (see Conjecture 1 for precise terms) of the special values $L(E,\tau,1)$ of the complex L-functions of the elliptic curve twisted by Artin representations τ by taking its value $\mathcal{L}_E(\tau^*)$ at the contragredient representation τ^* of τ. Moreover, we have a conjectural functional equation of the complex L-function relating the L-values $L(E,\tau,s)$ and $L(E,\tau^*,2-s)$ (see Subsection 2.4 for precise statements). As $\mathcal{L}_E(\tau^*)$ and $\mathcal{L}_E(\tau)$ approximate the modification of $L(E,\tau,1)$ and $L(E,\tau^*,1)$, respectively, we can relate $\mathcal{L}_E(\tau^*)$ and $\mathcal{L}_E(\tau)$. Now if we define $\mathcal{L}_E^\#$ to be the element we get from $\mathcal{L}_E$ by replacing elements of G with their inverses, then $\mathcal{L}_E(\tau) = \mathcal{L}_E^\#(\tau^*)$ is a tautology. Thus we get an equation involving the values of $\mathcal{L}_E$ and $\mathcal{L}_E^\#$ at arbitrary Artin representations τ^*. This can actually be thought of as the functional equation of the *values* of the p-adic L-function, and therefore we can also predict a functional equation for the p-adic L-function itself. Now the Main Conjecture of Iwasawa theory states that the p-adic L-function is a characteristic element for the dual of the Selmer group over the false

Received 5 February 2008; revised 4 February 2010.

2000 *Mathematics Subject Classification* 11R23 (primary), 11G05, 11G40, 19A31, 20C07, 16E30 (secondary).

[†]During this research the author was holding an External Research Studentship of Trinity College (Cambridge) under the title Prince of Wales.

Tate curve extension. This means that we also expect a 'functional equation' on the stage of modules in the category $\mathfrak{M}_H(G)$ (see Subsection 3.2 for the definition) relating the dual Selmer $X(E/F_\infty)$ and its opposite module $X(E/F_\infty)^\#$. This can actually be proved without using the Main Conjecture or the functional equation of the p-adic L-function. More precisely, in Section 5 we construct a pairing over the GL_2-extension associated to elliptic curves on the dual of the p-Selmer group whenever the elliptic curve has good ordinary reduction at the prime $p \geqslant 5$ and the dual Selmer $X(E/F_\infty)$ is in the category $\mathfrak{M}_H(G)$. This pairing is actually a map from $X(E/F_\infty)$ to the first extension group of $X(E/F_\infty)^\#$ with the Iwasawa algebra $\Lambda(G)$. The methods build on earlier work by Perrin-Riou [25] and the author [37]. We take the projective limit of maps defined by the Cassels–Tate pairing. As a corollary we prove an algebraic functional equation for the characteristic element that coincides with the conjectural functional equation of the p-adic L-function (see Section 6 for details). This is a good evidence for both the Main Conjecture and the conjectural functional equation of the p-adic L-function.

In Subsection 7.2 we investigate the consequences of the functional equation of the characteristic element to the parity conjecture. We prove that if the rank of the twisted dual Selmer group $X(\mathrm{tw}_\tau(E)/\mathbb{Q}^{\mathrm{cyc}})$ for all self-dual Artin representations τ factoring through the image of G modulo its maximal pro-p normal subgroup (that is, it factors through $\mathrm{GL}_2(\mathbb{F}_p)$ if $G = \mathrm{GL}_2(\mathbb{Z}_p)$) is the same as what the analytic root number would suggest, then the similar statement holds for any self-dual Artin representation of G. The parity conjecture is an immediate consequence of this whenever E has a p-isogeny over $\mathbb{Q}$. The proof relies on the fact that we can relate these parities from both the algebraic and analytic side to the sign in the functional equation of the characteristic element of the dual Selmer group of E over F_∞.

Finally we present the example of the curve $X_1(11)$ to illustrate our results. We provide a potential characteristic element for the dual Selmer satisfying all the so far known properties.

Throughout the paper all modules are assumed to be left modules, unless otherwise stated. However, when we take the extension functors of modules with the Iwasawa algebra, to try to avoid confusion we do not invert the group action and so these extension functors of left (right) modules will be right (left) modules.

2. *Analytic preliminaries and notations*

2.1. *The* GL_2*-extension associated to elliptic curves without complex multiplication*

Let $p \geqslant 5$ be a fixed prime number. If F is a finite extension of $\mathbb{Q}$, then we write F^{cyc} for the cyclotomic $\mathbb{Z}_p$-extension of F. Let E be an elliptic curve defined over $\mathbb{Q}$ and without complex multiplication, and $E[p^\infty]$ be the group of all p-power division points on E. We define

$$F_\infty := \mathbb{Q}(E[p^\infty]). \tag{2.1}$$

By the Weil pairing this field contains all the p-power roots of unity. Hence $\mathbb{Q}^{\mathrm{cyc}} \subset F_\infty$ and we put

$$G = \mathrm{Gal}(F_\infty/\mathbb{Q}), \quad H = \mathrm{Gal}(F_\infty/\mathbb{Q}^{\mathrm{cyc}}), \quad \Gamma = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}). \tag{2.2}$$

By a classical result of Serre [31], G can be identified with an open subgroup of

$$\mathrm{GL}_2(\mathbb{Z}_p) = \mathrm{Aut}(E[p^\infty]) \tag{2.3}$$

as E does not admit complex multiplication. Moreover, let G_0 and H_0 be the maximal pro-p normal subgroup of G and H, respectively, that is, the intersection of all the pro-p-Sylow subgroups. If q is any prime in $\mathbb{Q}$, then define G_q and H_q to be the decomposition subgroups of G and H, respectively, corresponding to some fixed embedding $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}_q}$.

2.2. *Systems of l-adic representations*

If E is an elliptic curve defined over $\mathbb{Q}$ and $\tau : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{Q}})$ is an Artin representation, then both of them determine a compatible system of l-adic representations for primes l of $\mathbb{Q}$. In the case of τ the l-adic representation is $M_l(\tau) := \tau \otimes \overline{\mathbb{Q}_l}$. The l-adic representation of the elliptic curve is $M_l(E) := H^1_{\mathrm{et}}(E, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}_l}$ or, equivalently, the dual of the l-adic Tate module $T_l(E)$ with scalars extended to $\overline{\mathbb{Q}}_l$. Further, we define the system of l-adic representations of the elliptic curve twisted by the Artin representations

$$M_l(E, \tau) := M_l(E) \otimes_{\overline{\mathbb{Q}_l}} M_l(\tau). \tag{2.4}$$

2.3. *L-functions*

To a system M of l-adic representations M_l we associate an L-function $L(M, s)$ as follows. For a prime q of $\mathbb{Q}$ the local polynomials of $L(M, s)$ are

$$P_q(M, T) := \det(1 - \mathrm{Frob}_q^{-1} T \mid M_l^{I_q}) \tag{2.5}$$

for any prime $l \neq q$. We define the local L-factor

$$L_q(M, s) := P_q(M, q^{-s})^{-1} \tag{2.6}$$

and the global L-function as a Euler-product

$$L(M, s) := \prod_v L_q(M, s). \tag{2.7}$$

We write

$$L(E, s) := L(M(E), s), \quad L(\tau, s) := L(M(\tau), s), \quad L(E, \tau, s) := L(M(E, \tau), s). \tag{2.8}$$

The L-series $L(\tau, s)$ converges to an analytic function on the half-plane $\Re s > 1$. The L-series $L(E, s)$ and $L(E, \tau, s)$ define analytic functions in the half-plane $\Re s > 3/2$ and are conjectured to have an entire continuation to the whole complex plane. We define

$$g_{E,\tau} = \mathrm{rk}_{\mathbb{Z}}(E(\overline{\mathbb{Q}}) \otimes \tau), \quad r_{E,\tau} = \mathrm{ord}_{s=1}(L(E, \tau, s)). \tag{2.9}$$

The generalized Birch–Swinnerton-Dyer conjecture predicts that $g_{E,\tau} = r_{E,\tau}$ always holds.

Let us recall that the L-functions are multiplicative in the sense that

$$L(E, \tau_1 \oplus \tau_2) = L(E, \tau_1) L(E, \tau_2). \tag{2.10}$$

2.4. *Functional equations of complex L-functions*

The twisted L-functions $L(E, \tau, s)$ conjecturally satisfy a functional equation of the following form. Let

$$\hat{L}(E, \tau, s) := \left(\frac{N(E, \tau)}{\pi^{2 \dim \tau}}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{\dim \tau} \Gamma\left(\frac{s+1}{2}\right)^{\dim \tau} L(E, \tau, s). \tag{2.11}$$

Then, conjecturally,

$$\hat{L}(E, \tau, s) = w(E, \tau) \hat{L}(E, \tau^*, 2 - s), \tag{2.12}$$

where τ^* denotes the contragredient representation of τ and $w(E, \tau)$ is an algebraic number of complex absolute value 1. If $\tau \cong \tau^*$, then $w(E, \tau) = \pm 1$ and we call it the sign in the functional equation.

3. *Algebraic preliminaries and notations*

3.1. *The dual Selmer and the Iwasawa algebra*

If $L \subseteq F_\infty$ is any Galois extension of $\mathbb{Q}$ (later usually $L = k^{\mathrm{cyc}}$, or $L = k$, where k is a number field, or $L = F_\infty$), then we define $X(E/L)$ as the Pontryagin dual of the Selmer group

$$X(E/L) = \mathrm{Sel}_{p^\infty}(E/L)^{\mathrm{v}} = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/L), \mathbb{Q}_p/\mathbb{Z}_p). \tag{3.1}$$

If k is a number field, then $t_{E/k,p}$ denotes the $\mathbb{Z}_p$-rank of $X(E/k)$. Let $Y(E/L)$ be the factor of $X(E/L)$ by its p-primary part. Then $X(E/F_\infty)$, and also $Y(E/F_\infty)$, is a finitely generated compact (left) module over the Iwasawa algebra $\Lambda(G) = \Lambda(\mathrm{Gal}(F_\infty/\mathbb{Q}))$, where, for any profinite group $\mathcal{G}$, the Iwasawa algebra of $\mathcal{G}$ is

$$\Lambda(\mathcal{G}) = \varprojlim_{N \lhd_o \mathcal{G}} \mathbb{Z}_p[\mathcal{G}/N]. \tag{3.2}$$

We denote the $\mathbb{F}_p$-Iwasawa algebra, the epimorphic image of the previous one modulo p, by

$$\Omega(\mathcal{G}) = \varprojlim_{N \lhd_o \mathcal{G}} \mathbb{F}_p[\mathcal{G}/N]. \tag{3.3}$$

For the Galois group $\mathrm{Gal}(L/k)$ of a Galois extension L of the number field k and a prime v of k we write $\mathrm{Gal}(L/k)_v$ for the decomposition subgroup of v. Here we fix once and for all an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_q}$ for each rational prime q.

3.2. *K-theory and localization*

Let S be the set of all f in $\Lambda(G)$ such that $\Lambda(G)/\Lambda(G)f$ is a finitely generated $\Lambda(H)$-module and

$$S^* = \bigcup_{n \geqslant 0} p^n S. \tag{3.4}$$

These are multiplicatively closed (left and right) Ore sets of $\Lambda(G)$ (Theorem 2.4 in [7]), and so we can define $\Lambda(G)_S$ and $\Lambda(G)_{S^*}$ as the localizations of $\Lambda(G)$ at S and S^*, respectively. We write $\mathfrak{M}_H(G)$ for the category of all finitely generated $\Lambda(G)$-modules that are S^*-torsion. A finitely generated left module M is in $\mathfrak{M}_H(G)$ if and only if $M/M(p)$ is finitely generated over $\Lambda(H)$ (see [7, Proposition 2.3, the definition of S^* on p. 7]). It is conjectured that $X(E/F_\infty)$ always lies in this category. For a module M in $\mathfrak{M}_H(G)$ one can define a characteristic element in the first K-group $K_1(\Lambda(G)_{S^*})$ (see [7, Proposition 3.4]). It is a pre-image of the class of M under the connecting homomorphism

$$\partial_G : K_1(\Lambda(G)_{S^*}) \longrightarrow K_0(\mathfrak{M}_H(G)) \tag{3.5}$$

in the long exact sequence of localization in K-theory

$$\cdots \longrightarrow K_1(\Lambda(G)) \longrightarrow K_1(\Lambda(G)_{S^*}) \xrightarrow{\partial_G} K_0(\mathfrak{M}_H(G)) \longrightarrow K_0(\Lambda(G)) \longrightarrow K_0(\Lambda(G)_{S^*}) \longrightarrow 0, \tag{3.6}$$

where $K_0(\mathfrak{M}_H(G))$ denotes the Grothendieck group of the category $\mathfrak{M}_H(G)$. This definition makes sense because the connecting homomorphism ∂_G is surjective (see [7, Proposition 3.4]). Further, if we denote by $\mathfrak{N}_H(G)$ the category of $\Lambda(G)$-modules that are finitely generated over $\Lambda(H)$, then we get a similar exact sequence

$$\cdots \longrightarrow K_1(\Lambda(G)) \longrightarrow K_1(\Lambda(G)_S) \xrightarrow{\partial_G} K_0(\mathfrak{N}_H(G)) \longrightarrow K_0(\Lambda(G)) \longrightarrow K_0(\Lambda(G)_S) \longrightarrow 0. \tag{3.7}$$

As defined in [6] there is a C_2-action, that is, the group of order 2, on the localized K_1-group induced by the anti-isomorphism $\#$ of $\Lambda(G)$ and its opposite ring $\Lambda(G)^{\#}$, which sends the elements of G to their inverse. Recall that this action on an $[A] \in K_1(\Lambda(G)_{S^*})$ represented by a matrix $A \in \mathrm{GL}_n(\Lambda(G)_{S^*})$ (for some positive integer n) is defined by applying # on each of the entries of the matrix A and transposing the matrix in order to get a homomorphism from $\mathrm{GL}_n(\Lambda(G)_{S^*})$ to its opposite group. This definition makes sense and is well defined on $K_1(\Lambda(G)_{S^*})$, since the sets S and S^* are invariant under the action of # on $\Lambda(G)$.

Further, if M is a left $\Lambda(G)$-module, then by $M^{\#}$ we denote the right module defined on the same underlying set with the action of $\Lambda(G)$ via the map #, that is, for an m element in M and g in G, and the right action is defined by $mg := g^{-1}m$. By extending the right multiplication linearly to the whole Iwasawa algebra, we get $mx = x^{\#}m$.

We also define the similar notions for G replaced by G_0 or G_q and H by H_0 or H_q, respectively.

3.3. *Dimension filtration of Iwasawa modules*

Let $\mathcal{G}$ be a p-adic Lie group without elements of order p. Following [10] the *grade* of a left or right $\Lambda(\mathcal{G})$-module M is defined to be the smallest non-negative integer $j(M) = j_{\Lambda(\mathcal{G})}(M)$ such that $\mathrm{Ext}^{j(M)}_{\Lambda(\mathcal{G})}(M, \Lambda(\mathcal{G})) \neq 0$ (we let $j(\{0\}) = \infty$). For any finitely generated $M \neq 0$, the grade $j(M)$ is bounded above by the projective dimension of M. We say that M satisfies the *Auslander condition* if, for each $k \geqslant 0$ and any submodule N of $\mathrm{Ext}^k_{\Lambda(\mathcal{G})}(M, \Lambda(\mathcal{G}))$, we have $j(N) \geqslant k$ (note that if M is a right (left) $\Lambda(\mathcal{G})$-module, then the right (left) multiplication on $\Lambda(\mathcal{G})$ makes $\mathrm{Ext}^k_{\Lambda(\mathcal{G})}(M, \Lambda(\mathcal{G}))$ into a right (left) $\Lambda(\mathcal{G})$-module). The Iwasawa algebra $\Lambda(\mathcal{G})$ of $\mathcal{G}$ is an *Auslander regular* ring [34, 35], and so every finitely generated left or right $\Lambda(\mathcal{G})$-module satisfies the Auslander condition.

Let

$$0 \longrightarrow \Lambda(\mathcal{G}) \xrightarrow{\mu_0} E_0 \xrightarrow{\mu_1} E_1 \xrightarrow{\mu_2} \cdots \xrightarrow{\mu_i} E_i \xrightarrow{\mu_{i+1}} \tag{3.8}$$

be the minimal injective resolution of $\Lambda(\mathcal{G})$, where E_{i+1} is the injective hull (see [32, Definition 1.5.1]) of the cokernel of μ_i for any $i \geqslant 0$. Moreover, let

$$\mathcal{C}^n_{\Lambda(\mathcal{G})} = \mathcal{C}^n := \text{full subcategory of all modules } M \text{ such that } \mathrm{Hom}_{\Lambda(\mathcal{G})}(M, E_0 \oplus \ldots \oplus E_n) = 0.$$

This subcategory $\mathcal{C}^n$ is 'localizing' in the sense that it satisfies the following conditions.

(i) In any short exact sequence $0 \to M' \to M \to M'' \to 0$ of $\Lambda(\mathcal{G})$-modules, M' and M'' lie in $\mathcal{C}^n$ if and only if so does M.

(ii) Any $\Lambda(\mathcal{G})$-module has a unique largest submodule contained in $\mathcal{C}^n$.

It is called the *hereditary torsion theory* cogenerated by the injective module $E_0 \oplus \ldots \oplus E_n$ (see [32, Chapter VI]).

We say that a module M is *pure* if $\mathrm{Ext}^i_{\Lambda(\mathcal{G})}(\mathrm{Ext}^i_{\Lambda(\mathcal{G})}(M, \Lambda(\mathcal{G})), \Lambda(\mathcal{G})) = 0$ for any $i \neq j(M)$. Suppose that the $\Lambda(\mathcal{G})$-module M is finitely generated and its projective dimension is d. Then M carries [3, 10] a natural filtration, called the *dimension filtration*, by submodules

$$M = \Delta^0(M) \supseteq \Delta^1(M) \supseteq \ldots \subseteq \Delta^{d+1}(M) = 0, \tag{3.9}$$

where the numbering corresponds to codimension as in [10]. This filtration is characterized by the property that a submodule $N \subseteq M$ has grade $j(N) \geqslant p$ if and only if $N \subseteq \Delta^p(M)$. In addition, one has the following:

(i) $j(M) = \max\{p \geqslant 0 \mid \Delta^p(M) = M\}$;

(ii) if M is pure, then $M = \Delta^{j(M)}(M) \supset \Delta^{j(M)+1}(M) = 0$;

(iii) $\Delta^p(M)/\Delta^{p+1}(M)$ is zero or pure of grade p.

Moreover, since $\Lambda(\mathcal{G})$ is Auslander regular, we have the following lemma.

Lemma 3.1 [10, Lemma 2.4]. *A finitely generated $\Lambda(G)$-module M lies in the category $\mathcal{C}^n$ if and only if $j(M) > n$.*

This above lemma shows that the pseudo-null modules are exactly those lying in $\mathcal{C}^1$. Throughout the paper we are going to use the notation

$$a^i_{\Lambda(\mathcal{G})}(M) := \mathrm{Ext}^i_{\Lambda(\mathcal{G})}(M, \Lambda(\mathcal{G})). \tag{3.10}$$

3.4. *Galois representations and twists*

As in [7], let O denote the ring of integers of some finite extension L of $\mathbb{Q}_p$ and let us assume that we are given a continuous homomorphism

$$\rho : G \longrightarrow \mathrm{GL}_n(O), \tag{3.11}$$

where $n \geqslant 1$ is an integer. If M is a finitely generated $\Lambda(G)$-module, then put $M_O = M \otimes_{\mathbb{Z}_p} O$, and define the twist of M with ρ by

$$\mathrm{tw}_\rho(M) = M_O \otimes_O O^n. \tag{3.12}$$

We endow $\mathrm{tw}_\rho(M)$ with the diagonal action of G, that is, if g is in G, then $g(m \otimes z) = (gm) \otimes (gz)$, where it is understood that G acts on O^n on the left via the homomorphism ρ. By compactness, this left action of G extends to an action of the whole Iwasawa algebra $\Lambda(G)$.

As explained in [7], we see that ρ induces a homomorphism

$$\Phi'_\rho : K_1(\Lambda(G)_{S^*}) \longrightarrow K_1(M_n(Q_O(\Gamma))) = Q_O(\Gamma)^\times, \tag{3.13}$$

where $Q_O(\Gamma)$ denotes the field of fractions of $\Lambda_O(\Gamma) = \Lambda(\Gamma) \otimes_{\mathbb{Z}_p} O$. Let $\varphi : \Lambda_O(\Gamma) \to O$ denote the augmentation map, and write $\mathfrak{p} = \mathrm{Ker}(\varphi)$. Writing $\Lambda_O(\Gamma)_\mathfrak{p} \subset Q_O(\Gamma)$ for the localization of $\Lambda_O(\Gamma)$ at $\mathfrak{p}$, we find that φ extends to a homomorphism

$$\varphi : \Lambda_O(\Gamma)_\mathfrak{p} \longrightarrow L, \tag{3.14}$$

and for $\xi \in K_1(\mathfrak{M}_H(G))$ we define $\xi(\rho) = \varphi(\Phi'_\rho(\xi))$ if $\Phi'_\rho(\xi)$ belongs to $\Lambda_O(\Gamma)_\mathfrak{p}$, and $\xi(\rho) = \infty$ otherwise.

4. *Finitely generated $\mathbb{Z}_p$-modules*

Our goal in this section is to prove that the modules, which are finitely generated over $\mathbb{Z}_p$, represent the trivial element in the Grothendieck group of the category $\mathfrak{M}_H(G)$. Our key lemma is a consequence of the work of Ardakov and Wadsley [2].

Lemma 4.1. *All finite $\Omega(H)$-modules represent the trivial element in the category $K_0(\Omega(H))$.*

Proof. First note that, as we assume $p \geqslant 5$ throughout the paper, the group H does not contain any element of order p and hence $\Omega(H)$ has finite global dimension. This means that any finitely generated $\Omega(H)$-module really has a class in $K_0(\Omega(H))$.

The statement follows from [2, Theorem B] as all the p-regular elements (that is, elements of finite order prime to p) have centralizers of dimension at least 1 in H. Indeed, the dimension of the centralizer in H is the same as the dimension of the centralizer in the Lie algebra of H over an algebraically closed field. This Lie algebra is isomorphic to $\mathfrak{sl}_2 = \mathrm{Lie}(\mathrm{SL}_2(\mathbb{Z}_p))$ as H has a finite index subgroup isomorphic to a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$. However, over an algebraically closed field the matrix of any p-regular element is diagonalizable and so it clearly has a centralizer as acting by conjugation on $\mathfrak{sl}_2$. □

Now we can state the main result of this section.

Proposition 4.2. *If M is a $\Lambda(G)$-module and it is finitely generated over $\mathbb{Z}_p$, then it represents the trivial element in the Grothendieck group $K_0(\mathfrak{M}_H(G))$.*

Proof. We may assume that M is p-torsion free because its p-power torsion part is finite and so represents the trivial element in $K_0(\mathfrak{M}_H(G))$. Indeed, the finite p-torsion modules even have trivial class in $K_0(\Omega(G))$. This can be seen using a similar Lie-theoretical argument together with [2, Theorem B] as in the proof of Lemma 4.1, but here the Lie algebra is isomorphic to $\mathfrak{gl}_2$ and hence the p-regular elements have centralizer of dimension even at least 2. On the other hand, we have a natural homomorphism $K_0(\Omega(G)) \to K_0(\mathfrak{M}_H(G))$. The statement for p-power torsion modules follows by induction.

Hence from now on we assume that M has no p-torsion and put

$$\hat{H} := \{A \in \mathrm{GL}_2(\mathbb{Z}_p) \mid \det(A)^{p-1} = 1\} \quad \text{and} \quad \hat{G} := \mathrm{GL}_2(\mathbb{Z}_p). \tag{4.1}$$

The group H can be identified with a finite index subgroup of $\hat{H}$ by construction. First note that $K_0(\Lambda(\hat{H})) \cong K_0(\Omega(\hat{H}))$ since the ideal generated by p is contained in the Jacobson radical of $\Lambda(\hat{H})$. The isomorphism is given by the natural map sending the class of a projective $\Lambda(\hat{H})$-module P to the class of P/pP. As $p \geqslant 5$, $\hat{G}$ (hence $\hat{H}$) does not contain any element of order p, that is, $K_0(\Lambda(\hat{H})) \cong K_0(\Lambda(\hat{H})\text{-mod})$. There is an exact functor $\phi\colon \Lambda(\hat{H})\text{-mod} \to \mathfrak{M}_{\hat{H}}(\hat{G})$ by extending the $\hat{H}$-action to a $\hat{G}$-action, by taking the trivial action for $\hat{\Gamma} := \hat{G}/\hat{H}$. This works because we have $\hat{G} \cong \hat{\Gamma} \times \hat{H}$. Note that we do not have $G \cong H \times \Gamma$ in general. Indeed, we always have that G is a semidirect product $H \rtimes \Gamma$, but Γ might not map into $\hat{\Gamma}$ inside $\hat{G}$ and therefore need not act trivially on H, only via a finite quotient. This is why we first need to consider $\mathrm{GL}_2(\mathbb{Z}_p)$-modules. However, we may take the exact forgetful functor $\mathfrak{M}_{\hat{H}}(\hat{G}) \to \mathfrak{M}_H(G)$ since G and H are open subgroups of $\hat{G}$ and $\hat{H}$, respectively. Also, the tensoring $\cdot \otimes_{\mathbb{Z}_p} M$ with M and endowing the tensor product with the diagonal G-action gives rise to another exact functor $\mathfrak{M}_H(G) \to \mathfrak{M}_H(G)$. All together we obtain a canonical map

$$\begin{tikzcd}
K_0(\Omega(\hat{H})) \cong K_0(\Lambda(\hat{H})) \arrow[r, "\phi_*"] & K_0(\mathfrak{M}_{\hat{H}}(\hat{G})) \arrow[r, "\text{forget}"] & K_0(\mathfrak{M}_H(G)) \arrow[r, "\cdot\otimes_{\mathbb{Z}_p} M"] & K_0(\mathfrak{M}_H(G)), \\
{[\mathbb{F}_p] \mapsto [\mathbb{Z}_p]} \arrow[r, mapsto] & {[\mathbb{Z}_p]} \arrow[r, mapsto] & {[\mathbb{Z}_p]} \arrow[r, mapsto] & M.
\end{tikzcd} \tag{4.2}$$

The claim follows because $[\mathbb{F}_p] = 0$ by Lemma 4.1. □

5. *Pairings*

Following the ideas of [25, 37] in this section we construct a generalized Cassels–Tate pairing for the dual Selmer group over the GL_2-extension. Let E be an elliptic curve with good ordinary reduction at the prime $p \geqslant 5$. Moreover, let us assume that the dual of the Selmer group, $X(E/F_\infty)$ lies in the category $\mathfrak{M}_H(G)$. The strategy is that we take the projective limit of the homomorphisms

$$X(E/L^{\mathrm{cyc}}) \longrightarrow a^1_{\Lambda(\Gamma)}(X(E/L^{\mathrm{cyc}})^{\#}) \tag{5.1}$$

constructed by Perrin-Riou [25] with respect to the intermediate number fields $\mathbb{Q} \subseteq L \subset F_\infty$ to get a map

$$X(E/F_\infty) \longrightarrow a^1_{\Lambda(G)}(X(E/F_\infty)^{\#}). \tag{5.2}$$

We shall show that this homomorphism is a pseudo-isomorphism, and describe the kernel and the cokernel. This provides us with a functional equation of the characteristic element of $X(E/F_\infty)$.

Perrin-Riou's [25] main idea was that she wrote the Cassels–Tate pairing as an isomorphism

$$C_F : \ X(E/L)(p) \longrightarrow \mathrm{Sel}(E/L)/\mathrm{div}(\mathrm{Sel}(E/L)) \tag{5.3}$$

over a number field L, where $\mathrm{Sel}(E/L)$ is the p-Selmer group of the elliptic curve E, $X(E/L)$ is its Pontryagin dual, and $\mathrm{div}(\cdot)$ denotes the divisible part of an abelian group. Moreover, a special case of a theorem of Flach [17] is that there also is an isomorphism

$$C_F:\ X(\mathrm{tw}_\tau(E)/L)(p) \longrightarrow \mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/L)/\mathrm{div}(\mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/L)) \tag{5.4}$$

for any (not necessarily Artin) character τ of the Galois group $\mathrm{Gal}(L^{\mathrm{cyc}}/L)$ with values in $\mathbb{Z}_p^\times$. Thus we have the choice of the character τ and it is easy to see that it can be chosen so that it is *admissible*, that is, $\mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/M)$ is finite for any subextension $L \subseteq M \subset L^{\mathrm{cyc}}$. Indeed, since $X(E/L^{\mathrm{cyc}})$ is a torsion $\Lambda(\mathrm{Gal}(L^{\mathrm{cyc}}/L))$-module (which is a consequence of $X(E/F_\infty)$ lying in $\mathfrak{M}_H(G)$), we can take any character τ not appearing in the representation space $X(E/L^{\mathrm{cyc}}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ for $\mathrm{Gal}(L^{\mathrm{cyc}}/L)$. Now, whenever $\mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/M)$ is finite, its divisible part is trivial, and so the pairing is in fact on the Selmer group itself.

On the other hand, whenever $X(E/L^{\mathrm{cyc}})$ is a torsion $\Lambda(\mathrm{Gal}(L^{\mathrm{cyc}}/L))$-module, we also have the restriction map

$$\mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/M) \longrightarrow \mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/L^{\mathrm{cyc}})^{\mathrm{Gal}(L^{\mathrm{cyc}}/M)} \tag{5.5}$$

for any intermediate field $L \subseteq M \subset L^{\mathrm{cyc}}$. By composing the two maps and taking the projective limit, we get another map

$$X(\mathrm{tw}_\tau(E)/L^{\mathrm{cyc}}) \longrightarrow \varprojlim_{L\subseteq M\subset L^{\mathrm{cyc}}} \mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/L^{\mathrm{cyc}})^{\mathrm{Gal}(L^{\mathrm{cyc}}/M)}. \tag{5.6}$$

Moreover, we have an isomorphism [25]

$$\varprojlim_{L\subseteq M\subset L^{\mathrm{cyc}}} \mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/L^{\mathrm{cyc}})^{\mathrm{Gal}(L^{\mathrm{cyc}}/M)} \cong \mathrm{Ext}^1_\Lambda(X(\mathrm{tw}_{\tau^{-1}}(E)/L^{\mathrm{cyc}})^\#, \Lambda), \tag{5.7}$$

where Λ temporarily denotes $\Lambda(\mathrm{Gal}(L^{\mathrm{cyc}}/L))$. Therefore we get a map

$$\begin{tikzcd} X(\mathrm{tw}_\tau(E)/L^{\mathrm{cyc}}) \arrow[r] \arrow[d, phantom, "\|"] & \mathrm{Ext}^1_\Lambda(X(\mathrm{tw}_{\tau^{-1}}(E)/L^{\mathrm{cyc}})^\#, \Lambda) \arrow[d, phantom, "\|"] \\ X(E/L^{\mathrm{cyc}}) \otimes \tau & \mathrm{Ext}^1_\Lambda(X(E/L^{\mathrm{cyc}})^\#, \Lambda) \otimes \tau. \end{tikzcd} \tag{5.8}$$

Thus, by taking the tensor product with τ^{-1}, we obtain a map from $X(E/L^{\mathrm{cyc}})$ to its first extension group with the Iwasawa algebra which is in fact independent of the choice of the admissible representation τ.

Investigating the kernel and cokernel of the map

$$X(E/L^{\mathrm{cyc}}) \longrightarrow \mathrm{Ext}^1_{\Lambda(\mathrm{Gal}(L^{\mathrm{cyc}}/L))}(X(E/L^{\mathrm{cyc}})^\#, \Lambda(\mathrm{Gal}(L^{\mathrm{cyc}}/L))) \tag{5.9}$$

is equivalent to describing the kernels and cokernels of the restriction maps (5.5). This can be done using the usual diagrams

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Sel}(E/M) \arrow[r] \arrow[d, "r_M"] & H^1(F_R/M, E[p^\infty]) \arrow[r] \arrow[d, "g_M"] & \bigoplus_{u\in R} J_u(M) \arrow[r] \arrow[d, "\oplus h_{M,u}"] & 0 \\ 0 \arrow[r] & \mathrm{Sel}(E/L^{\mathrm{cyc}})^{\Gamma_M} \arrow[r] & H^1(F_R/L^{\mathrm{cyc}}, E[p^\infty])^{\Gamma_M} \arrow[r] & \bigoplus_{u\in R} J_u(L^{\mathrm{cyc}})^{\Gamma_M}, & \end{tikzcd} \tag{5.10}$$

where $\Gamma_M = \mathrm{Gal}(L^{\mathrm{cyc}}/M)$, R is the finite set of primes in L containing those at which E does not have good reduction and the primes above p, F_R is the maximal Galois extension of L unramified outside the primes in R,

$$J_u(M) := \mathrm{Ker}(H^1(M, E[p^\infty]) \longrightarrow \bigoplus_{u\in R} H^1(M_u, E[p^\infty])/\mathrm{Im}(\kappa_u)), \tag{5.11}$$

$$J_u(L^{\mathrm{cyc}}) := \bigoplus_{u_L|u} H^1(L_{u_L}, E(\overline{L_{u_L}}))[p^\infty], \tag{5.12}$$

and κ_u is the local Kummer map.

For our purposes we will need the following lemma which is a slight generalization of [25, Proposition 1.3.1] to this non-commutative situation.

Lemma 5.1. *If the $\Lambda(G)$-module M lies in $\mathfrak{M}_H(G)$, then we have*

$$\operatorname{Ext}^1_{\Lambda(G)}(M,\Lambda(G)) \cong \varprojlim_L \operatorname{Ext}^1_{\Lambda(\Gamma_L)}(M_{H_L},\Lambda(\Gamma_L)) \tag{5.13}$$

where L runs through the finite Galois subextensions of F_∞, $H_L = \mathrm{Gal}(F_\infty/L^{\mathrm{cyc}})$, and $\Gamma_L = \mathrm{Gal}(L^{\mathrm{cyc}}/L)$. We implicitly claim that there is a natural $\Lambda(G)$-action on the right-hand side, as well.

Proof. It is a theorem of Jannsen [24] that since Γ_L is a finite index subgroup of $\Gamma_L^* := \mathrm{Gal}(L^{\mathrm{cyc}}/\mathbb{Q})$, we have the $\Lambda(\Gamma_L)$-isomorphism for any $\Lambda(\Gamma_L^*)$-module N

$$\operatorname{Ext}^i_{\Lambda(\Gamma_L)}(N,\Lambda(\Gamma_L)) \cong \operatorname{Ext}^i_{\Lambda(\Gamma_L^*)}(N,\Lambda(\Gamma_L^*)). \tag{5.14}$$

Now by taking $N = M_{H_L}$, we may equip the right-hand side of (5.13) with a $\Lambda(G)$-action using this isomorphism and noting that any $\Lambda(\Gamma_L^*)$-module is also a $\Lambda(G)$-module via the natural surjection $\Lambda(G) \to \Lambda(\Gamma_L^*)$ of algebras.

We clearly have $\Lambda(G) = \varprojlim_L \Lambda(\Gamma_L^*)$. Hence the functors $\operatorname{Hom}_{\Lambda(G)}(\cdot,\Lambda(G))$ and $\varprojlim_L \operatorname{Hom}_{\Lambda(G)}(\cdot,\Lambda(\Gamma_L^*))$ coincide by the definition of the projective limit. Moreover, the projective limit functor is exact on compact spaces, in particular on finitely generated $\Lambda(G)$-modules. Therefore the derived functors of $\varprojlim_L \operatorname{Hom}_{\Lambda(G)}(\cdot,\Lambda(\Gamma_L^*))$ are $\varprojlim_L \operatorname{Ext}^i_{\Lambda(G)}(\cdot,\Lambda(\Gamma_L^*))$ and, in particular, we obtain

$$\operatorname{Ext}^1_{\Lambda(G)}(M,\Lambda(G)) \cong \varprojlim_L \operatorname{Ext}^1_{\Lambda(G)}(M,\Lambda(\Gamma_L^*)). \tag{5.15}$$

On the other hand let P be the $\Lambda(G)$-projective cover of M with the short exact sequences

$$0 \longrightarrow M_1 \longrightarrow P \longrightarrow M \longrightarrow 0 \tag{5.16}$$

and

$$0 \longrightarrow M_2 \longrightarrow P_{H_L} \longrightarrow M_{H_L} \longrightarrow 0. \tag{5.17}$$

Then, by definition of M_2, we have a short exact sequence

$$0 \longrightarrow H_1(H_L,M) \longrightarrow {M_1}_{H_L} \longrightarrow M_2 \longrightarrow 0. \tag{5.18}$$

Note that if N is any $\Lambda(G)$-module, then we have a natural identification

$$\operatorname{Hom}_{\Lambda(G)}(N,\Lambda(\Gamma_L^*)) = \operatorname{Hom}_{\Lambda(\Gamma_L^*)}(N_{H_L},\Lambda(\Gamma_L^*)). \tag{5.19}$$

Thus we have the following commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & & & 0 \arrow[d] & & \\
0 \arrow[r] & a^0_{\Lambda(\Gamma_L^*)}(M_{H_L}) \arrow[r] \arrow[d, equal] & a^0_{\Lambda(\Gamma_L^*)}(P_{H_L}) \arrow[r] \arrow[d, equal] & a^0_{\Lambda(\Gamma_L^*)}(M_2) \arrow[r] \arrow[d] & a^1_{\Lambda(\Gamma_L^*)}(M_{H_L}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Hom}_G(M,\Lambda(\Gamma_L^*)) \arrow[r] & \operatorname{Hom}_G(P,\Lambda(\Gamma_L^*)) \arrow[r] & \operatorname{Hom}_G(M_1,\Lambda(\Gamma_L^*)) \arrow[r] \arrow[d] & \operatorname{Ext}^1_G(M,\Lambda(\Gamma_L^*)) \arrow[r] & 0 \\
 & & & a^0_{\Lambda(\Gamma_L^*)}(H_1(H_L,M)), & &
\end{tikzcd} \tag{5.20}$$

where for the sake of simplicity Hom_G and Ext_G denote $\operatorname{Hom}_{\Lambda(G)}$ and $\operatorname{Ext}_{\Lambda(G)}$, respectively. Now since M is in $\mathfrak{M}_H(G)$, it follows that $H_1(H_L,M)$ is a torsion $\Lambda(\Gamma_L)$-module and so its

a^0 vanishes. This means that in (5.20) all the modules corresponding to each other in the two rows are isomorphic and so we have

$$a^1_{\Lambda(\Gamma_L^*)}(M_{H_L}) \cong \mathrm{Ext}^1_{\Lambda(G)}(M, \Lambda(\Gamma_L^*)). \tag{5.21}$$

The result follows from the isomorphism (5.15). □

Our main theorem is the following. It is a generalisation of the pairings constructed by Greenberg [**20**] over the cyclotomic extension, by Perrin–Riou [**25**] over more general $\mathbb{Z}_p$- and $\mathbb{Z}_p^2$-extensions, and by the author [**37**] over the false Tate curve extension.

Theorem 5.2. *Let E be an elliptic curve without complex multiplication and with good ordinary reduction at the prime $p \geqslant 5$. Then there is a map*

$$\varphi : X(E/F_\infty) \longrightarrow \mathrm{Ext}^1(X(E/F_\infty)^\#, \Lambda(G)) \tag{5.22}$$

such that $\mathrm{Ker}(\varphi)$ is finitely generated over $\mathbb{Z}_p$ (so it represents the trivial element in $K_0(\mathfrak{M}_H(G))$) and $\mathrm{Coker}(\varphi)$ represents the same element in $K_0(\mathfrak{M}_H(G))$ as

$$\bigoplus_{q \mid v_q(j_E)<0} \Lambda(G) \otimes_{\Lambda(G_q)} T_p(E)^*. \tag{5.23}$$

Proof. As explained earlier we are going to take the projective limit of the maps

$$X(E/L^{\mathrm{cyc}}) \xrightarrow{\varphi_{2,L}} a^1_{\Lambda(\Gamma_L)}(X(E/L^{\mathrm{cyc}})^\#) \xrightarrow{\varphi_{1,L}} a^1_{\Lambda(\Gamma_L)}(X(E/F_\infty)^\#_{H_L}) \tag{5.24}$$

(where φ_2 has been defined by Perrin-Riou [**25**]) with respect to finite Galois subextensions $L \subset F_\infty$, where $H_L := \mathrm{Gal}(F_\infty/L^{\mathrm{cyc}})$ and $\Gamma_L := \mathrm{Gal}(L^{\mathrm{cyc}}/L)$. Since

$$\varprojlim_L X(E/L^{\mathrm{cyc}}) = X(E/F_\infty) \tag{5.25}$$

and by Lemma 5.1

$$\varprojlim_L a^1_{\Lambda(\Gamma_L)}(X(E/F_\infty)^\#_{H_L}) = a^1_{\Lambda(G)}(X(E/F_\infty)^\#), \tag{5.26}$$

we certainly get a map

$$X(E/F_\infty) \xrightarrow{\varphi} a^1_{\Lambda(G)}(X(E/F_\infty)^\#), \tag{5.27}$$

where $\varphi = \lim_L(\varphi_{1,L} \circ \varphi_{2,L})$ and we only need to describe its kernel and cokernel.

We shall begin with the investigation of $\varphi_{1,L}$. Let R denote the set of primes with potential multiplicative reduction for E together with the prime p and let

$$J_u(L^{\mathrm{cyc}}) := \bigoplus_{u_L \mid u} H^1(L_{u_L}, E(\overline{L_{u_L}}))[p^\infty] \tag{5.28}$$

and

$$J_u(F_\infty) := \varinjlim_L J_u(L^{\mathrm{cyc}}). \tag{5.29}$$

We use the following fundamental diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}(E/L^{\mathrm{cyc}}) \arrow[r] \arrow[d, "r_L"] & H^1(F_R/L^{\mathrm{cyc}}, E[p^\infty]) \arrow[r] \arrow[d, "g_L"] & \bigoplus_{u \in R(L^{\mathrm{cyc}})} J_u(L^{\mathrm{cyc}}) \arrow[r] \arrow[d, "\oplus h_{L,u}"] & 0 \\
0 \arrow[r] & \mathrm{Sel}(E/F_\infty)^{H_L} \arrow[r] & H^1(F_R/F_\infty, E[p^\infty])^{H_L} \arrow[r] & \bigoplus_{u \in R(L^{\mathrm{cyc}})} J_u(F_\infty)^{H_L} &
\end{tikzcd} \tag{5.30}$$

to analyse the kernel and cokernel of the map $X(E/F_\infty)^{\#}_{H_L} \to X(E/L^{\mathrm{cyc}})^{\#}$. Here $R(L^{\mathrm{cyc}})$ denotes the set of primes in L^{cyc} above those in R. The 0 in the top right corner of (5.30) is proved, for instance, in [**23**, § 7] (see also [**9**, Lemma 2.1]). By (5.30) and the snake lemma we have an exact sequence

$$0 \longrightarrow \mathrm{Ker}(r_L) \longrightarrow \mathrm{Ker}(g_L) \longrightarrow \bigoplus_{u\in R(L^{\mathrm{cyc}})} \mathrm{Ker}(h_{L,u}) \longrightarrow \mathrm{Coker}(r_L) \longrightarrow \mathrm{Coker}(g_L). \tag{5.31}$$

On the other hand, by the inflation–restriction exact sequence we have

$$\mathrm{Ker}(g_L) \cong H^1(H_L, E[p^\infty]) \quad \text{and} \quad \mathrm{Coker}(g_L) \hookrightarrow H^2(H_L, E[p^\infty]). \tag{5.32}$$

These cohomology groups are finite (see the paragraph after Theorem 4.2 in [**8**]), and we claim the following lemma.

Lemma 5.3. *Whenever the field L contains $\mathbb{Q}(E[p])$, the number of generators of the finite p-groups $H^1(H_L, E[p^\infty])$ and $H^2(H_L, E[p^\infty])$ is at most 6.*

Proof. Since these cohomology groups are finite (abelian) p-groups, their number of generators can be computed as the dimension of $H^i(H_L, E[p^\infty])/pH^i(H_L, E[p^\infty])$ $(i = 1, 2)$ as an $\mathbb{F}_p$-vector space. By Kummer theory we have the long exact sequence

$$\cdots \longrightarrow H^i(H_L, E[p]) \longrightarrow H^i(H_L, E[p^\infty]) \xrightarrow{p\cdot} H^i(H_L, E[p^\infty]) \longrightarrow H^{i+1}(H_L, E[p]) \longrightarrow \cdots . \tag{5.33}$$

Hence it suffices to show that $\dim_{\mathbb{F}_p} H^i(H_L, E[p]) \leqslant 6$. Moreover, since L contains $\mathbb{Q}(E[p])$, the group H_L acts trivially on $E[p]$. Therefore as an H_L-module $E[p]$ is isomorphic to $\mathbb{F}_p^2$. Finally, we have $\dim_{\mathbb{F}_p} H^0(H_L, \mathbb{F}_p) = \dim_{\mathbb{F}_p} H^3(H_L, \mathbb{F}_p) = 1$ and $\dim_{\mathbb{F}_p} H^2(H_L, \mathbb{F}_p) = \dim_{\mathbb{F}_p} H^1(H_L, \mathbb{F}_p) = \dim H_L = 3$ because H_L is a 3-dimensional uniform pro-p group (and hence we have duality between H^i and H^{3-i}). Let us remark that in fact we obtain that $H^2(H_L, E[p^\infty])$ is generated by at most 2 elements over $\mathbb{Z}_p$. □

Thus the projective limits of the Pontryagin dual of the kernel and cokernel of g_L are finitely generated over $\mathbb{Z}_p$ and so represent the trivial element in $K_0(\mathfrak{M}_H(G))$ by Proposition 4.2. Now we have a quasi-exact sequence (up to finite modules with bounded number of generators)

$$0 \longrightarrow \bigoplus_{u\in R(L^{\mathrm{cyc}})} \mathrm{Ker}(h_{L,u})^{\vee\#} \longrightarrow X(E/F_\infty)^{\#}_{H_L} \longrightarrow X(E/L^{\mathrm{cyc}})^{\#} \longrightarrow 0. \tag{5.34}$$

On the other hand, we claim that $\mathrm{Ext}^2_{\Lambda(\Gamma_L)}(X(E/L^{\mathrm{cyc}})^{\#})$ is finite with bounded number of generators. Indeed, by Auslander regularity of $\Lambda(\Gamma_L)$ we have

$$\mathrm{Ext}^2_{\Lambda(\Gamma_L)}(X(E/L^{\mathrm{cyc}})^{\#}) \cong \mathrm{Ext}^2_{\Lambda(\Gamma_L)}(F), \tag{5.35}$$

where F is the maximal finite submodule of $X(E/L^{\mathrm{cyc}})^{\#}$ as the finite modules are exactly the pseudo-null modules for $\Lambda(\Gamma_L)$. Moreover, by [**22**], we see that F is the projective limit of the kernels X_n of the restriction homomorphisms

$$\mathrm{Sel}(E/L_n) \longrightarrow \mathrm{Sel}(E/L^{\mathrm{cyc}})^{\Gamma_n}. \tag{5.36}$$

Here Γ_n is a subgroup of Γ_L of index p^n and L_n is its fixed field. Now by the proof of Mazur's Control Theorem (see, for instance, [**21**, Lemma 4.2]) the kernel of (5.36) is contained in the finite module $H^1(\Gamma_n, E(L^{\mathrm{cyc}})[p^\infty]) = E(L^{\mathrm{cyc}})[p^\infty]/(\gamma_L^{p^n} - 1)E(L^{\mathrm{cyc}})[p^\infty]$ for n big enough. Since $E(L^{\mathrm{cyc}})[p^\infty]$ is cogenerated by at most two elements, our claim follows.

Thus we get another quasi-exact sequence

$$0 \longrightarrow a^1_{\Lambda(\Gamma_L)}(X(E/L^{\mathrm{cyc}})^{\#}) \longrightarrow a^1_{\Lambda(\Gamma_L)}(X(E/F_\infty)^{\#}_{H_L}) \longrightarrow, \tag{5.37}$$

$$\longrightarrow \bigoplus_{u\in R(L^{\mathrm{cyc}})} a^1_{\Lambda(\Gamma_L)}(\mathrm{Ker}(h_{L,u})^{\vee\#}) \longrightarrow 0. \tag{5.38}$$

If u does not divide p, then, by Shapiro's lemma, we get

$$\mathrm{Ker}(h_{L,u}) = \bigoplus_{u_L|u} H^1(H_{L,w}, E(F_{\infty,w}))[p^\infty] \tag{5.39}$$

and by a standard argument, using Kummer theory [8, 23], we have that if w does not divide p, then

$$H^1(H_{L,w}, E(F_{\infty,w}))[p^\infty] \cong H^1(H_{L,w}, E(F_{\infty,w})[p^\infty]). \tag{5.40}$$

Moreover, E has potential multiplicative reduction at the primes in R not dividing p, and for some finite subextension L_0 of $F_\infty/\mathbb{Q}$ it becomes split multiplicative [8]. Further, as we are taking inverse limit, we may assume that L contains L_0, and so we have a short exact sequence

$$0 \longrightarrow A \longrightarrow E[p^\infty] \longrightarrow B \longrightarrow 0, \tag{5.41}$$

where as $\mathrm{Gal}(F_\infty/L)_w$-modules A is isomorphic to μ_{p^∞} and B is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. However, they have an additional action of the group $\mathrm{Gal}(F_\infty/\mathbb{Q})_u$ which is slightly bigger than $\mathrm{Gal}(F_\infty/L)_w$. Note that since the reduction of E at the prime w is split multiplicative, $H_{L,w}$ is isomorphic to $\mathbb{Z}_p$ by the theory of the Tate curve. By taking $H_{L,w}$-homology for L sufficiently large, we get the exact sequence

$$0 \longrightarrow B \longrightarrow H^1(H_{L,w}, A) \longrightarrow H^1(H_{L,w}, E[p^\infty]) \longrightarrow H^1(H_{L,w}, B) \longrightarrow 0, \tag{5.42}$$

and noting that $H^1(H_{L,w}, \mu_{p^\infty}) \cong \mathbb{Q}_p/\mathbb{Z}_p$ as $\mathrm{Gal}(F_\infty/L)_w$-modules, we obtain

$$H^1(H_{L,w}, E[p^\infty]) \cong H^1(H_{L,w}, B) \cong \mathrm{Hom}(H_{L,w}, B). \tag{5.43}$$

Moreover, since $\mathrm{Gal}(F_\infty/\mathbb{Q})_u$ acts on $H_{L,w}$ via the cyclotomic character, we have

$$\mathrm{Hom}(H_{L,w}, B) \cong B(-1), \tag{5.44}$$

where $M(-1)$ denotes the (-1)st Tate twist of the Galois module M. On the other hand if u divides p, then $\mathrm{Ker}(h_{L,u})$ is finite and has bounded order [8, 23], and so it is negligible. Therefore from (5.38) we get the quasi-exact sequence

$$0 \longrightarrow a^1_{\Lambda(\Gamma_L)}(X(E/L^{\mathrm{cyc}})^{\#}) \longrightarrow a^1_{\Lambda(\Gamma_L)}(X(E/F_\infty)^{\#}_{H_L}) \longrightarrow \bigoplus_{u\in R(L^{\mathrm{cyc}})\setminus S_p(L^{\mathrm{cyc}})} B^\vee(-1) \longrightarrow 0 \tag{5.45}$$

(where $S_p(L^{\mathrm{cyc}})$ denotes the set of primes in L^{cyc} lying above p and $-^\vee$ stands for the Pontryagin dual) as

$$a^1_{\Lambda(\Gamma_{L,u})}(\mathrm{Hom}(H^1(H_{L,w}, B), \mathbb{Q}_p/\mathbb{Z}_p)^{\#}) \cong a^1_{\Lambda(\Gamma_{L,u})}((H_1(H_{L,w}, B^\vee))^{\#}) \cong B^\vee(-1). \tag{5.46}$$

Recall (see the proof of Lemma 5.1) that the connecting maps for the intermediate fields $L_1 \supseteq L_2$ between $a^1_{\Lambda(\Gamma_{L_1})}(X(E/F_\infty)^{\#}_{H_{L_1}})$ and $a^1_{\Lambda(\Gamma_{L_2})}(X(E/F_\infty)^{\#}_{H_{L_2}})$ are induced by the surjection $\Lambda(\Gamma^*_{L_1}) \twoheadrightarrow \Lambda(\Gamma^*_{L_2})$ noting that any $\Lambda(G)$-homomorphism from a $\Lambda(G)$-module M to $\Lambda(\Gamma^*_{L_2})$ factors through $M_{H_{L_2}}$. We claim the following lemma.

Lemma 5.4. *The induced connecting homomorphism*

$$\begin{tikzcd} a^1_{\Lambda(\Gamma^*_{L_{1,u_1}})}(H_1(H_{L_{1,w}}, B^\vee)^{\#}) \arrow[r] \arrow[d, equal] & a^1_{\Lambda(\Gamma^*_{L_{2,u_2}})}(H_1(H_{L_{2,w}}, B^\vee)^{\#}) \arrow[d, equal] \\ B^\vee(-1) & B^\vee(-1) \end{tikzcd} \tag{5.47}$$

is surjective (hence an isomorphism) for primes $u_1 \mid u_2$ in L_1 and L_2, respectively.

Proof of the lemma. We may assume using induction that $[L^{\mathrm{cyc}}_{1,u_1} : L^{\mathrm{cyc}}_{2,u_2}] = p$, whence we have

$$\mathrm{Gal}(L^{\mathrm{cyc}}_{1,u_1}/L_{2,u_2}) = \Gamma_{L_{1,u_1}} \times H_{21} \tag{5.48}$$

as the group $\Gamma_{L_{1,u_1}} \cong \mathbb{Z}_p$ can only act trivially on the finite group $H_{21} := H_{L_{2,w}}/H_{L_{1,w}}$ of order p (by Nakayama's lemma). Moreover, a theorem of Jannsen [24] provides us with the $\Lambda(\mathrm{Gal}(L^{\mathrm{cyc}}_{1,u_1}/L_{2,u_2}))$-isomorphism $a^1_{\Lambda(\Gamma^*_{L_{1,u_1}})}(M) \cong a^1_{\Lambda(\mathrm{Gal}(L^{\mathrm{cyc}}_{1,u_1}/L_{2,u_2}))}(M)$ for any $\Lambda(\Gamma^*_{L_{1,u_1}})$-module M, and also with the $\Lambda(\Gamma_{L_{2,u_2}})$-isomorphism $a^1_{\Lambda(\Gamma^*_{L_{2,u_2}})}(N) \cong a^1_{\Lambda(\Gamma_{L_{2,u_2}})}(N)$ for $\Lambda(\Gamma^*_{L_{2,u_2}})$-modules N. Hence the map (5.47) is induced by the surjection $\mathrm{Gal}(L^{\mathrm{cyc}}_{1,u_1}/L_{2,u_2}) \twoheadrightarrow \Gamma_{L_{2,u_2}}$. On the other hand, by the same argument as in (5.20), we obtain

$$\mathrm{Ext}^1_{\Lambda(\Gamma_{L_{1,u_1}}\times H_{21})}(H_1(H_{L_{1,w}}, B^{\vee})^{\#}, \Lambda(\Gamma_{L_{2,u_2}})) \cong a^1_{\Lambda(\Gamma_{L_{2,u_2}})}(H_1(H_{L_{1,w}}, B^{\vee})^{\#}_{H_{21}}) \tag{5.49}$$

since we have $a^0_{\Lambda(\Gamma_{L_{2,u_2}})}(H_1(H_{21}, H_1(H_{L_{1,w}}, B^{\vee})^{\#})) = 0$. Now by the spectral sequence

$$E^2_{pq} = H_p(H_{21}, H_q(H_{L_{1,w}}, \cdot)) \Longrightarrow H_{p+q}(H_{L_{2,w}}, \cdot) \tag{5.50}$$

we get a short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & H_1(H_{L_{1,w}}, B^{\vee})^{\#}_{H_{21}} \arrow[r, "(1)"] \arrow[d, equal, "\wr"] & H_1(H_{L_{2,w}}, B^{\vee})^{\#} \arrow[r] \arrow[d, equal, "\wr"] & H_1(H_{21}, B^{\vee}_{H_{L_{1,w}}})^{\#} \arrow[r] \arrow[d, equal, "\wr"] & 0. \\
& \mathbb{Z}_p & \mathbb{Z}_p & \mathbb{F}_p &
\end{tikzcd} \tag{5.51}$$

Here note that the map (1) has to be injective as otherwise it could not have finite cokernel. Hence, by the long exact sequence of $a_{\Lambda(\Gamma_{L_{2,u_2}})}(\cdot)$ we deduce that $a^1_{\Lambda(\Gamma_{L_{2,u_2}})}(H_1(H_{L_{2,w}}, B^{\vee})^{\#})$ is naturally a submodule of $a^1_{\Lambda(\Gamma_{L_{2,u_2}})}(H_1(H_{L_{1,w}}, B^{\vee})^{\#}_{H_{21}})$ of index p as $a^1_{\Lambda(\Gamma_{L_{2,u_2}})}(\mathbb{F}_p) = 0$ and $a^2_{\Lambda(\Gamma_{L_{2,u_2}})}(\mathbb{F}_p) \cong \mathbb{F}_p$. Hence by (5.49) it suffices to show that the natural map

$$a^1_{\Lambda(\Gamma_{L_{1,u_1}}\times H_{21})}(H_1(H_{L_{1,w}}, B^{\vee})^{\#}) \longrightarrow \mathrm{Ext}^1_{\Lambda(\Gamma_{L_{1,u_1}}\times H_{21})}(H_1(H_{L_{1,w}}, B^{\vee})^{\#}, \Lambda(\Gamma_{L_{2,u_2}})) \tag{5.52}$$

also has cokernel $\mathbb{F}_p$ (and hence is surjective onto $a^1_{\Lambda(\Gamma_{L_{2,u_2}})}(H_1(H_{L_{2,w}}, B^{\vee})^{\#})$). However, since $H_1(H_{L_{1,w}}, B^{\vee})^{\#} \cong \mathbb{Z}_p$ as $\Lambda(\Gamma_{L_{1,u_1}} \times H_{21})$-modules, the above map (5.52) fits into the long exact sequence of $\mathrm{Ext}_{\Lambda(\Gamma_{L_{1,u_1}}\times H_{21})}(\mathbb{Z}_p, \cdot)$. Therefore the cokernel of (5.52) is isomorphic to $\mathrm{Ext}^2_{\Lambda(\Gamma_{L_{1,u_1}}\times H_{21})}(\mathbb{Z}_p, I_{21})$, where I_{21} is the kernel of the surjection $\Lambda(\Gamma_{L_{1,u_1}} \times H_{21}) \twoheadrightarrow \Lambda(\Gamma_{L_{2,u_2}})$. (Here note that $a^2_{\Lambda(\Gamma_{L_{1,u_1}}\times H_{21})}(\mathbb{Z}_p) = 0$.) By writing down an explicit $\Lambda(\Gamma_{L_{1,u_1}} \times H_{21})$-projective resolution of $\mathbb{Z}_p$ it is easy to compute that $\mathrm{Ext}^2_{\Lambda(\Gamma_{L_{1,u_1}}\times H_{21})}(\mathbb{Z}_p, I_{21}) \cong \mathbb{F}_p$ and the statement follows. □

This above lemma shows that the connecting homomorphisms

$$\bigoplus_{u\in R(L_1^{\mathrm{cyc}})\setminus S_p(L_1^{\mathrm{cyc}})} B^{\vee}(-1) \longrightarrow \bigoplus_{u\in R(L_2^{\mathrm{cyc}})\setminus S_p(L_2^{\mathrm{cyc}})} B^{\vee}(-1) \tag{5.53}$$

are surjective.

Now we turn to the investigation of $\varphi_{2,L}$. The kernel of $\varphi_{2,L}$ is finite and bounded by $\mathrm{Hom}(H^1(L, E[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p)$; thus its projective limit is finitely generated over $\mathbb{Z}_p$ and hence trivial in $K_0(\mathfrak{M}_H(G))$. However, the cokernel of $\varphi_{2,L}$ is [21, 25]

$$\left(\varinjlim_{k\longrightarrow\infty} \bigoplus_{u\in R(L^{\mathrm{cyc}})\setminus S_p(L^{\mathrm{cyc}})} \bigoplus_{u_L|u} H^1(\Gamma_k, E(L^{\mathrm{cyc}}_{u_L})[p^\infty]) \right)^{\vee} \tag{5.54}$$

up to finite modules bounded by $H^i(L, E[p^\infty])^\vee$ for $(i = 1, 2)$. Now for L large enough (so that all potentially multiplicative primes become split multiplicative) we have the exact sequence

$$0 \longrightarrow B(1) \longrightarrow E(L_{u_L}^{\mathrm{cyc}})[p^\infty] \longrightarrow B[p^{r_L}] \longrightarrow 0 \tag{5.55}$$

for some non-negative integer r_L. By the long exact sequence of Γ_k-cohomology we get that $H^1(\Gamma_k, E(L_{u_L}^{\mathrm{cyc}}))$ is isomorphic to $B[p^{r_L}](\cong p^{-r_L}\mathbb{Z}_p/\mathbb{Z}_p)$ independently of k, where r_L tends to infinity as the field L grows since F_∞ contains the whole $E[p^\infty]$. Now we claim that the connecting homomorphisms between $\mathrm{Coker}(\varphi_{2,L_1})$ and $\mathrm{Coker}(\varphi_{2,L_2})$ for the intermediate fields $L_1 \supseteq L_2$ induce surjections from $B[p^{r_{L_1}}]$ to $B[p^{r_{L_2}}]$. Indeed, we have the long exact sequence of Γ_k-cohomology

$$\begin{aligned}0 \longrightarrow H^0(\Gamma_k, E(L_{2,u_{L_2}}^{\mathrm{cyc}})[p^\infty]) \longrightarrow H^0(\Gamma_k, E(L_{1,u_{L_1}}^{\mathrm{cyc}})[p^\infty]) \xrightarrow{(1)} H^0(\Gamma_k, \mathbb{Z}/p^{r_{L_1}-r_{L_2}}\mathbb{Z})\\ \longrightarrow H^1(\Gamma_k, E(L_{2,u_{L_2}}^{\mathrm{cyc}})[p^\infty]) \xrightarrow{(2)} H^1(\Gamma_k, E(L_{1,u_{L_1}}^{\mathrm{cyc}})[p^\infty]) \longrightarrow H^1(\Gamma_k, \mathbb{Z}/p^{r_{L_1}-r_{L_2}}\mathbb{Z}) \longrightarrow \cdots\end{aligned} \tag{5.56}$$

with the surjective map (1) as the Γ_k-action is semisimple on $E(L_{i,u_{L_i}}^{\mathrm{cyc}})[p^\infty]$, and hence

$$H^0(\Gamma_k, E(L_{i,u_{L_i}}^{\mathrm{cyc}})[p^\infty]) \cong H^0(\Gamma_k, B(1)) \oplus B[p^{r_{L_i}}] \tag{5.57}$$

for $i = 1, 2$. Therefore the map (2) is injective, and so its Pontryagin dual is surjective from $B[p^{r_{L_1}}]$ to $B[p^{r_{L_2}}]$. This means that the projective limit of each local factor in (5.54) is $T_p(B) \cong B^\vee$.

We saw that the cokernel of $\varprojlim_L \varphi_{1,L}$ is the direct sum of local terms that are isomorphic to $B^\vee(-1)$ and the cokernel of $\varprojlim_L \varphi_{2,L}$ is the sum of the local $B^\vee$ up to modules finitely generated over $\mathbb{Z}_p$. The kernels of both are finitely generated over $\mathbb{Z}_p$. Thus the statement follows by the exact sequence

$$0 \longrightarrow B^\vee \longrightarrow T_p(E)^* \longrightarrow B^\vee(-1) \longrightarrow 0 \tag{5.58}$$

of $\Lambda(G_q)$-modules as G permutes the primes above a prime q. □

6. *The functional equation of the characteristic element*

In this section we are going to investigate the consequences of Theorem 5.2 on the characteristic element of the dual Selmer group $X(E/F_\infty)$. What one would expect is a functional equation relating the characteristic element $\xi_{X(E/F_\infty)}$ and $\xi^{\#}_{X(E/F_\infty)}$. For this we would require that the characteristic elements of $X(E/F_\infty)^{\#}$ and $a^1(X(E/F_\infty)^{\#})$ be the same. (Note that $X(E/F_\infty)^{\#}$ is a *right* module and $a^1(X(E/F_\infty)^{\#})$ is a *left* module over $\Lambda(G)$.) This was more or less trivial in the false Tate curve case [**37**], however, in the GL_2-case one has to be a bit more careful.

6.1. *The vanishing of the characteristic elements of higher extension groups*

The following general proposition is the first step towards proving that $a^1(X(E/F_\infty)^{\#})$ and $X(E/F_\infty)^{\#}$ have the same characteristic element. The proposition relies on the observation that $a^1(\Lambda(G)/\Lambda(G)s) \cong \Lambda(G)/s\Lambda(G)$ whenever s is in the Ore set S. In other words in this case s is a characteristic element for both $\Lambda(G)/\Lambda(G)s$ and its first extension group. Note that we are comparing characteristic elements of left and right modules without applying # (otherwise the characteristic element would change to $s^{\#}$). In fact, we have two different categories with the name $\mathfrak{M}_H(G)$: one (say $\mathfrak{M}_H(G)_{\mathrm{left}}$) for left modules and the other (say $\mathfrak{M}_H(G)_{\mathrm{right}}$) for right modules. Moreover, we have two different isomorphisms between their K_0. One is induced by the map # and the other is the somewhat less natural

$$\phi\colon [M_{\mathrm{left}}] \mapsto \xi_{M_{\mathrm{left}}} \in K_1(\Lambda(G)_{S^*})/K_1(\Lambda(G)) \mapsto \partial(\xi_{M_{\mathrm{left}}}) \in K_0(\mathfrak{M}_H(G)_{\mathrm{right}}). \tag{6.1}$$

However, the advantage of ϕ is that it preserves characteristic elements. The functional equations actually come from the non-trivial comparison between ϕ and $\#$ in the case of dual Selmer groups. By a certain abuse of notation we keep using $\mathfrak{M}_H(G)$ for both left and right modules.

Proposition 6.1. *Let M be in the category $\mathfrak{M}_H(G)$. Let ξ_M and $\xi_{a^i(M)}$ be characteristic elements of M and of $a^i(M)$ for $1 \leqslant i \leqslant 5$, respectively. Then we have that*

$$\xi_M^{-1} \prod_{i=1}^{5} \xi_{a^i(M)}^{(-1)^{i+1}} \tag{6.2}$$

lies in the image of $K_1(\Lambda(G))$ in $K_1(\Lambda(G)_{S^*})$.

Proof. First of all we need to verify that whenever M is in $\mathfrak{M}_H(G)$, then so is $a^i(M)$ for any $i \geqslant 1$. Because of the long exact sequence of $\operatorname{Ext}_{\Lambda(G)}(\cdot, \Lambda(G))$, it is enough to prove both this and the statement of the proposition separately for p-torsion modules and modules finitely generated over $\Lambda(H)$.

For p-torsion modules the extension groups $a^i(M)$ are also p-torsion and hence lie in $\mathfrak{M}_H(G)$. On the other hand, it suffices to show the statement of the proposition for projective $\Omega(G)$-modules. Indeed, as G does not have any element of order p (we assume $p \geqslant 5$), the Iwasawa algebra $\Omega(G)$ has finite global dimension and we can apply once again the long exact sequence of $\operatorname{Ext}_{\Lambda(G)}(\cdot, \Lambda(G))$. For projective modules we only have first extension groups. Furthermore, if M is a projective $\Omega(G)$-module, then $a^1(M) \cong \operatorname{Hom}(M, \Omega(G))$ and so have the same characteristic element as M using the formula for the characteristic element of p-torsion modules [1].

Now if M is finitely generated over $\Lambda(H)$, then by [29, Theorem 3.1], we see that $a^i(M)$ is isomorphic to $\operatorname{Ext}^{i-1}(M, \Lambda(H))$ up to a twist, and in particular $a^i(M)$ is also finitely generated over $\Lambda(H)$ (hence lies in $\mathfrak{M}_H(G)$). On the other hand, the characteristic element for M in this case is in the image of the composed map [7, 33]

$$\Lambda(G)_S^\times \twoheadrightarrow K_1(\Lambda(G)_S) \longrightarrow K_1(\Lambda(G)_{S^*}). \tag{6.3}$$

Moreover, any element in $\Lambda(G)_S$ can be written in the form $x_1 x_2^{-1}$ with x_1, x_2 in $\Lambda(G)$. Now it can be easily seen that

$$a^1(\Lambda(G)/\Lambda(G)x_i) \cong \Lambda(G)/x_i\Lambda(G) \quad \text{for } i = 1, 2 \tag{6.4}$$

and their higher extension groups vanish as these modules have a projective resolution of length 1. Hence (6.2) is true for modules M_i with characteristic elements x_i and therefore it is also true for M with characteristic element $x_1 x_2^{-1}$ as both sides of (6.2) are multiplicative with respect to short exact sequences. □

This above lemma shows that we only need to prove the vanishing of the characteristic elements of $a^i(X(E/F_\infty)^\#)$ for $i \geqslant 2$ which is equivalent to the fact that they represent the trivial element in $K_0(\mathfrak{M}_H(G))$. The key observation is that since we have a map

$$\varphi^\# : X(E/F_\infty)^\# \longrightarrow \operatorname{Ext}^1(X(E/F_\infty), \Lambda(G)) \tag{6.5}$$

constructed in Theorem 5.2, we can relate the extension functors of $\operatorname{Ext}^1(X(E/F_\infty), \Lambda(G))$ and $X(E/F_\infty)^\#$. This is why the following lemma is of interest to us.

Lemma 6.2. *For any module M in $\mathfrak{M}_H(G)$ the extension group $\operatorname{Ext}^i(\operatorname{Ext}^1(M, \Lambda(G)), \Lambda(G))$ is in the category $\mathcal{C}^3$ for $i \geqslant 2$.*

Proof. Let

$$0 \longrightarrow P_5 \longrightarrow \ldots \longrightarrow P_0 \longrightarrow M \longrightarrow 0 \tag{6.6}$$

be the projective resolution of M as a $\Lambda(G)$-module (it has length 5 at most as G has dimension 4 as a p-adic Lie group). For the sake of simplicity let us introduce the notation

$$a^i(N) := \mathrm{Ext}^i_{\Lambda(G)}(N, \Lambda(G)) \quad \text{and} \quad N^* := \mathrm{Hom}_{\Lambda(G)}(N, \Lambda(G)) \tag{6.7}$$

for any finitely generated $\Lambda(G)$-module N. Moreover, let M_i be the image of the map from P_{i+1} to P_i for $i = 0, \ldots, 4$. Now since M has trivial Ext^0, we have a short exact sequence

$$0 \longrightarrow P_0^* \longrightarrow M_0^* \longrightarrow a^1(M) \longrightarrow 0. \tag{6.8}$$

By taking the long exact sequence of $\mathrm{Ext}(\cdot, \Lambda(G))$ and noting that P_0^* is a projective module, we obtain $a^i(a^1(M)) \cong a^i(M_0^*)$ for $i \geqslant 2$. By using the short exact sequence

$$0 \longrightarrow M_1 \longrightarrow P_1 \longrightarrow M_0 \longrightarrow 0, \tag{6.9}$$

we get an exact sequence

$$0 \longrightarrow M_0^* \longrightarrow P_1^* \longrightarrow M_1^* \longrightarrow a^2(M) \longrightarrow 0 \tag{6.10}$$

that we can split up into two short exact sequences

$$0 \longrightarrow M_0^* \longrightarrow P_1^* \longrightarrow A \longrightarrow 0$$

and

$$0 \longrightarrow A \longrightarrow M_1^* \longrightarrow a^2(M) \longrightarrow 0 \tag{6.11}$$

with some $\Lambda(G)$-module A. From the first exact sequence in (6.11) and since P_1^* is a projective module, we get

$$a^i(a^1(M)) \cong a^i(M_0^*) \cong a^{i+1}(A), \tag{6.12}$$

and from the second exact row we get a long exact sequence

$$\ldots \longrightarrow a^{i+1}(M_1^*) \longrightarrow a^{i+1}(A) \longrightarrow a^{i+2}(a^2(M)) \longrightarrow \cdots . \tag{6.13}$$

Since $a^{i+2}(N) \in \mathcal{C}^3$ for $i \geqslant 2$ and any finitely generated $\Lambda(G)$-module N by Auslander regularity, by (6.12) one only has to show that $a^{i+1}(M_1^*)$ is in $\mathcal{C}^3$ for $i \geqslant 2$, by Auslander regularity again. However, similarly to (6.10) and (6.11) we have two short exact sequences

$$0 \longrightarrow M_1^* \longrightarrow P_2^* \longrightarrow B \longrightarrow 0$$

and

$$0 \longrightarrow B \longrightarrow M_2^* \longrightarrow a^3(M) \longrightarrow 0 \tag{6.14}$$

with some $\Lambda(G)$-module B. Thus by the same trick $a^{i+1}(M_1^*) \cong a^{i+2}(B)$ (with $i \geqslant 1$, although we only need it for $i \geqslant 2$) and hence lies in $\mathcal{C}^3$ for $i \geqslant 2$, and we are done. □

The following is a slight generalization of Lemma 4.1. When a p-adic Lie group is commutative, pseudo-null Iwasawa modules have trivial characteristic elements. However, one of the biggest difficulties of non-commutative Iwasawa theory is that pseudo-null modules (those lying in $\mathcal{C}^1$) no longer represent trivial elements in the Grothendieck group of the category $\mathfrak{M}_H(G)$. Contrarily, for this GL_2-case we do have a positive statement in this direction.

Lemma 6.3. *Any element in the category $\mathfrak{M}_H(G) \cap \mathcal{C}^3$ represents the trivial element in the Grothendieck group $K_0(\mathfrak{M}_H(G))$.*

Proof. At first we prove the statement for p-torsion modules with the same property. By the formula for the characteristic element of p-torsion modules (see [1, § 1.5, Theorem]) we only need to prove that, for such modules, their G-Euler characteristics vanish. These modules have dimension at most 1 as $\Omega(G)$-modules (as their dimension is at most 1 as $\Lambda(G)$-modules and these dimensions are equal by [2, § 5.2]) and so their Euler characteristics is 1 because in $\mathrm{GL}_2(\mathbb{Z}_p)$ every p-regular element has at least a 2-dimensional centralizer in $\mathrm{GL}_2(\mathbb{Z}_p)$ and it has been proved by Ardakov and Wadsley [2, Theorem A] that if the dimension of the centralizer of all p-regular elements in a group is bigger than the dimension of a module, then the module has trivial Euler characteristics.

Hence it remains to prove the statement for modules M without p-torsion. We are going to prove that these modules are finitely generated over $\mathbb{Z}_p$. Indeed, their image in $K_0(\Omega(G))$ under the map sending projective modules P to P/pP is on the one hand equal to M/pM (since it has no p-torsion) and on the other hand this is a 0-dimensional $\Omega(G)$-module (as its a^i vanishes for $0 \leqslant i \leqslant 3$) and so finite because both conditions are equivalent to the Poincaré series of M being a polynomial (see [2, § 5.2]). Now M/pM is finite, which means that M is finitely generated over $\mathbb{Z}_p$ and so it has trivial characteristic element by Proposition 4.2. □

The above lemma leaves open the following natural question.

PROBLEM 1. Is there a module in the category $\mathfrak{M}_H(G) \cap \mathcal{C}^2$ which represents a non-trivial element in the Grothendieck group $K_0(\mathfrak{M}_H(G))$?

Now we have established the necessary tools to our main goal in this section.

PROPOSITION 6.4. *Let E be an elliptic curve without complex multiplication and with good ordinary reduction at the prime $p \geqslant 5$. Then the characteristic element of $\mathrm{Ext}^1(X(E/F_\infty)^\#, \Lambda(G))$ is the same as the characteristic element of $X(E/F_\infty)^\#$ modulo the image of $K_1(\Lambda(G))$ in $K_1(\Lambda(G)_{S^*})$.*

Proof. By Proposition 6.1 we only need to check that $\mathrm{Ext}^i(X(E/F_\infty)^\#, \Lambda(G))$ has trivial characteristic element for any $i \geqslant 2$. By Theorem 5.2 (and taking inverted action) we have a map

$$\varphi^\# : X(E/F_\infty)^\# \longrightarrow \mathrm{Ext}^1(X(E/F_\infty), \Lambda(G)) \tag{6.15}$$

such that its kernel is in $\mathcal{C}^3$ and its cokernel is

$$\bigoplus_{q|v_q(j_E)<0} \left(\Lambda(G) \otimes_{\Lambda(G_q)} C_q\right)^\# \tag{6.16}$$

modulo $\mathcal{C}^3$ for some $\Lambda(G_q)$-module C_q which is free of rank 2 over $\mathbb{Z}_p$ and represents the same element in $K_0(\mathfrak{M}_{H_q}(G_q)$ as $T_p(E)^*$. Note that this is not a formal consequence of Theorem 5.2, but in the proof the modifying factors are actually finitely generated $\mathbb{Z}_p$-modules and therefore lie in $\mathcal{C}^3$. Now $\Lambda(G)$ is a flat $\Lambda(G_q)$-module, and so

$$\left(\Lambda(G) \otimes_{\Lambda(G_q)} C_q\right)^\# \tag{6.17}$$

only has a non-trivial Ext^2 and its higher and lower Ext functors are trivial, since C_q is a pseudo-null $\Lambda(G_q)$-module of projective dimension 2. Indeed, G_q is a 2-dimensional p-adic Lie group and the module C_q has no p-torsion. Since $\mathcal{C}^3$ is closed with respect to the functors $\mathrm{Ext}^i_{\Lambda(G)}(\cdot, \Lambda(G))$ by Auslander regularity, the statement follows from Lemmas 6.2 and 6.3, and the long exact sequence of $\mathrm{Ext}(\cdot, \Lambda(G))$. □

6.2. *The functional equation*

To prove a functional equation for the characteristic element of $X(E/F_\infty)$, we need to construct the characteristic elements of the modules

$$\Lambda(G) \otimes_{\Lambda(G_q)} T_p(E)^* \tag{6.18}$$

for each prime q in $\mathbb{Q}$ with potentially multiplicative reduction for E. It can be easily seen that the characteristic element of (6.18) is the same as the image of the characteristic element of $T_p(E)^*$ under the natural map

$$K_1(\Lambda(G_q)_{S_q}) \longrightarrow K_1(\Lambda(G)_S), \tag{6.19}$$

where S_q is the canonical Ore set in the Iwasawa algebra $\Lambda(G_q)$ (see Subsection 3.2). Indeed, by the flatness of $\Lambda(G)$ as a $\Lambda(G_q)$-module for any matrix A in $\mathrm{GL}_n(\Lambda(G_q)_{S_q}) \cap M_n(\Lambda(G_q))$ for some positive integer n we have

$$\Lambda(G) \otimes_{\Lambda(G_q)} (\Lambda(G_q)^n/\Lambda(G_q)^n A) \cong \Lambda(G)^n/\Lambda(G)^n A. \tag{6.20}$$

On the other hand, the characteristic element of the right-hand side of (6.20) is by definition of the boundary map ∂ the class of $A \in \mathrm{GL}_n(\Lambda(G_q)_{S_q}) \subset \mathrm{GL}_n(\Lambda(G)_S)$ in $K_1(\Lambda(G)_S)$. Moreover, any element in $\mathrm{GL}_n(\Lambda(G_q)_{S_q})$ can be written in the form AB^{-1} for some A and B in $\mathrm{GL}_n(\Lambda(G_q)_{S_q}) \cap M_n(\Lambda(G_q))$ (just collect all the denominators into one element b of S_q and define B as a scalar matrix $b\mathrm{Id}$). Hence we obtain a commutative diagram

$$\begin{tikzcd}
K_1(\Lambda(G_q)_{S_q}) \arrow[r] \arrow[d] & K_1(\Lambda(G)_S) \arrow[d] \\
K_0(\mathfrak{M}_{H_q}(G_q)) \arrow[r, "\cdot\otimes_{\Lambda(G_q)}\Lambda(G)"] & K_0(\mathfrak{M}_H(G)).
\end{tikzcd} \tag{6.21}$$

Thus from now on we focus on determining the characteristic element of $T_p(E)^*$ as a $\Lambda(G_q)$-module for each q potentially multiplicative prime for E. The reduction type becomes split multiplicative over a finite subextension of F_∞ (see [8]), and hence there exists an open subgroup $I_q^{(1)} \leqslant_o I_q$ of the inertia subgroup such that we have an exact sequence of $\Lambda(G_q)$-modules

$$0 \longrightarrow A_q \longrightarrow T_p(E)^* \longrightarrow B_q \longrightarrow 0, \tag{6.22}$$

where both A_q and B_q are free $\mathbb{Z}_p$-modules of rank 1 and $I_q^{(1)}$ acts trivially on them. Indeed, $I_q^{(1)}$ can be chosen to equal the (unique) pro-p-Sylow subgroup of I_q and $A_q := H^0(I_q^{(1)}, T_p(E)^*)$ is a $\Lambda(G_q)$-submodule of $T_p(E)^*$ since $I_q^{(1)}$ is normal in G_q as it is a characteristic subgroup of the normal subgroup I_q. In fact by the theory of the Tate curve we have the following conditions.

(i) If E has multiplicative reduction at q, then $I_q = I_q^{(1)}$.

(ii) If E has additive (but potentially multiplicative) reduction at q, then $I_q/I_q^{(1)} = 2$.

Moreover, because of the Tate duality of the Galois-representation $T_p(E)^*$, we have the isomorphism of $\Lambda(G_q)$-modules $A_q \cong B_q(1)$, $B_q(2) \cong \mathrm{Hom}(B_q, \mathbb{Z}_p)$, and $A_q \cong \mathrm{Hom}(A_q, \mathbb{Z}_p)$, where $M(i)$ denotes the ith Tate twist of a Galois-module M. We define the module C_q by the exact sequence of $\Lambda(G_q)$-modules

$$0 \longrightarrow X_q \left(A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)})\right) \longrightarrow X_q^{-1} \left(A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)})\right) \longrightarrow C_q \longrightarrow 0, \tag{6.23}$$

where $X_q = i_q - 1$ and i_q is a topological generator of the group $I_q^{(1)} \cong \mathbb{Z}_p$. Then C_q represents the same element in the Grothendieck group $K_0(\mathfrak{M}_H(G))$ as $T_p(E)^*$ since we have an exact sequence

$$0 \longrightarrow A_q \longrightarrow C_q \longrightarrow B_q \longrightarrow 0 \tag{6.24}$$

similar to (6.22) as A_q and B_q by the above properties satisfy the exact sequences

$$0 \longrightarrow X_q\left(A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)})\right) \longrightarrow A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)}) \longrightarrow A_q \longrightarrow 0, \tag{6.25}$$

$$0 \longrightarrow A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)}) \longrightarrow X_q^{-1}\left(A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)})\right) \longrightarrow B_q \longrightarrow 0. \tag{6.26}$$

Now $A_q \cong \mathrm{Hom}_{\mathbb{Z}_p}(A_q, \mathbb{Z}_p)$ and hence we have

$$A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)}) \cong \mathrm{Hom}_{\Lambda(I_q)}(A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)}), \Lambda(I_q^{(1)})). \tag{6.27}$$

This means that the characteristic element β_q of $A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)})$ satisfies the functional equation $\beta_q^{\#} = \varepsilon_q \beta_q$ with an $\varepsilon_q \in K_1(\Lambda(G_q))$. Moreover, we have the following lemma.

Lemma 6.5. *The characteristic element of the $\Lambda(G_q)$-module $A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)})$ is*

$$\beta_q = \begin{cases} 1 + e_q \mathrm{Frob}_q & \text{if } E \text{ has non-split multiplicative reduction at } q, \\ 1 - e_q \mathrm{Frob}_q & \text{otherwise,} \end{cases} \tag{6.28}$$

where e_q is the central idempotent element in $\Lambda(I_q) \subset \Lambda(G_q)$ corresponding to the projective module

$$P_q := \Lambda(G_q) \otimes_{\Lambda(I_q)} (A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)})). \tag{6.29}$$

Moreover, $e_q^{\#} = e_q$.

Proof. By the flatness of $\Lambda(G_q)$ over $\Lambda(I_q)$ the idempotent in $\Lambda(G_q)$ corresponding to P_q is the image of the idempotent corresponding to $A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)})$ under the inclusion $\Lambda(I_q) \hookrightarrow \Lambda(G_q)$, and hence it is determined by how the group $I_q/I_q^{(1)}$ of order at most 2 acts on A_q. We have $e_q = 1$ in case the reduction is multiplicative ($I_q = I_q^{(1)}$), and $e_q = (1-t)/2$ for some central element t of order 2 in $I_q^{(1)} \leqslant G_q$ if the reduction is additive. Indeed, this central element t acts by -1 on the whole Tate module in the case of additive, but potentially multiplicative reduction and the summand of $\Lambda(I_q)$ on which t acts by -1 is exactly $\Lambda(I_q)((1-t)/2)$. The second statement ($e_q^{\#} = e_q$) already follows from this observation.

For the first statement note that in any case e_q is central in the Iwasawa algebra $\Lambda(G_q)$, and by definition of e_q we have $P_q = \Lambda(G_q)e_q \cong \Lambda(G_q)/\Lambda(G_q)(1-e_q)$. Therefore the left ideal in $\Lambda(G_q)$ generated by $1 - e_q$ and $1 \pm \mathrm{Frob}_q$ is the same as the left ideal generated by the single element $1 \pm e_q\mathrm{Frob}_q$. The latter fact follows from the identities

$$\begin{aligned} 1 \pm e_q\mathrm{Frob}_q &= (1-e_q) + e_q(1 \pm \mathrm{Frob}_q) \\ 1 - e_q &= (1 \pm e_q\mathrm{Frob}_q) - e_q(1 \pm e_q\mathrm{Frob}_q) \\ 1 \pm \mathrm{Frob}_q &= 1 \pm e_q\mathrm{Frob}_q \pm \mathrm{Frob}_q(1-e_q). \end{aligned} \tag{6.30}$$

Hence we have

$$\begin{aligned} &\Lambda(G_q)/\Lambda(G_q)(1 \pm e_q\mathrm{Frob}_q) \\ &\quad\cong \Lambda(G_q)/\Lambda(G_q)(1-e_q, 1 \pm \mathrm{Frob}_q) \\ &\quad\cong (\Lambda(G_q)/\Lambda(G_q)(1-e_q)) \,/\, (\Lambda(G_q)/\Lambda(G_q)(1-e_q))\,(1 \pm \mathrm{Frob}_q) \cong P_q/P_q(1 \pm \mathrm{Frob}_q) \\ &\quad\cong \Lambda(G_q) \otimes_{\Lambda(I_q)} (A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)}))/\Lambda(G_q) \otimes_{\Lambda(I_q)} (A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)}))\,((1 \pm \mathrm{Frob}_q) \otimes 1 \otimes 1) \\ &\quad\cong A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)}) \end{aligned} \tag{6.31}$$

The last isomorphism follows by comparing the $\Lambda(I_q^{(1)})$-rank of the two sides (both have rank 1) and noting that Frob_q acts on A_q trivially if the reduction is split multiplicative or additive, and by -1 if the reduction is non-split multiplicative. Indeed, we have a natural homomorphism

$$\Lambda(G_q)\otimes_{\Lambda(I_q)}(A_q\otimes_{\mathbb{Z}_p}\Lambda(I_q^{(1)}))\longrightarrow A_q\otimes_{\mathbb{Z}_p}\Lambda(I_q^{(1)}), \tag{6.32}$$

$$\lambda\otimes(x\otimes y)\mapsto\lambda x\otimes y \tag{6.33}$$

with kernel generated by $(1\pm\mathrm{Frob}_q)\otimes 1\otimes 1$. Hence the first statement of the result. □

Remark 1. It can be easily seen that

$$\varepsilon_q=1+e_q(\mathrm{Frob}_q^{-1}-1)\quad\text{if }\beta_q=1+e_q\mathrm{Frob}_q \tag{6.34}$$

and

$$\varepsilon_q=1-e_q(\mathrm{Frob}_q^{-1}+1)\quad\text{if }\beta_q=1-e_q\mathrm{Frob}_q. \tag{6.35}$$

On the other hand the characteristic element of

$$X_q^{\pm1}\left(A_q\otimes_{\mathbb{Z}_p}\Lambda(I_q^{(1)})\right) \tag{6.36}$$

is $X_q^{\pm}\beta_qX_q^{\mp}$. Moreover, as # reverses the order of multiplication,

$$\left(X_q\beta_qX_q^{-1}\right)^{\#}=\frac{1}{1/(X_q+1)-1}\beta_q^{\#}\left(\frac{1}{X_q+1}-1\right)=\frac{X_q+1}{X_q}\varepsilon_q\beta_q\frac{X_q}{X_q+1} \tag{6.37}$$

is also a characteristic element for the module

$$X_q^{-1}\left(A_q\otimes_{\mathbb{Z}_p}\Lambda(I_q^{(1)})\right) \tag{6.38}$$

because ε_q and X_q+1 are in $K_1(\Lambda(G_q))$ and so they map to the trivial element in $K_0(\mathfrak{M}_H(G))$. Putting

$$\alpha_q:=\frac{\left(X_q\beta_qX_q^{-1}\right)^{\#}}{X_q\beta_qX_q^{-1}} \tag{6.39}$$

and denoting its image under the map

$$K_1(\Lambda(G_q)_{S_q^*})\longrightarrow K_1(\Lambda(G)_{S^*}) \tag{6.40}$$

by the same letter we get the following corollary.

Corollary 6.6. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and with good ordinary reduction at the prime $p\geqslant 5$ and assume that the dual Selmer $X(E/F_\infty)$ over the GL_2-extension $F_\infty=\mathbb{Q}(E[p^\infty])$ is in the category $\mathfrak{M}_H(G)$. Then the characteristic element $\xi_{X(E/F_\infty)}$ of the $\Lambda(G)$-module $X(E/F_\infty)$ in the group $K_1(\Lambda(G)_{S^*})$ satisfies the functional equation*

$$\xi^{\#}_{X(E/F_\infty)}=\xi_{X(E/F_\infty)}\varepsilon_0(X(E/F_\infty))\prod_{q\in R}\alpha_q \tag{6.41}$$

for some $\varepsilon_0(X(E/F_\infty))$ in $K_1(\Lambda(G))$. Here the modifying factors α_q are defined in (6.39), and R is the set of rational primes at which the elliptic curve has potentially multiplicative reduction. Moreover, we have $\alpha_q\alpha_q^{\#}=1$ for each q in R.

Proof. We use Theorem 5.2 and the fact that two elements in $K_1(\Lambda(G)_{S^*})$ define the same class in the Grothendieck group $K_0(\mathfrak{M}_H(G))$ if and only if they differ by an element in $K_1(\Lambda(G))$. The characteristic element of $\Lambda(G) \otimes_{\Lambda(G_q)} T_p(E)^*$ is α_q, and

$$\alpha_q \alpha_q^{\#} = \frac{\left(X_q \beta_q X_q^{-1}\right)^{\#}}{X_q \beta_q X_q^{-1}} \left(\frac{\left(X_q \beta_q X_q^{-1}\right)^{\#}}{X_q \beta_q X_q^{-1}} \right)^{\#} = 1. \tag{6.42}$$

□

Remark 2. Fukaya and Kato [18, Theorem 4.4.7] also showed the functional equation of the p-adic L-function in a more general situation. They even give a more precise description of the modifying factor $\varepsilon_0(X(E/F_\infty))$. However, their result uses the (local and global) non-commutative Tamagawa number conjecture. Thus in some sense our result can be thought of further evidence for these conjectures, as well. In their notation $s(v, F_\infty/F)$ is our α_q up to an element in $K_1(\Lambda(G))$. Indeed, they map to the same class in $K_0(\mathfrak{M}_H(G))$ by [18, Proposition 4.4.6] and by our definition of α_q.

7. *Connections to the analytic side*

In this section we investigate the compatibility of Corollary 6.6 with the GL_2 Main Conjecture [7] for elliptic curves without complex multiplication and the conjectural functional equation of the p-adic L-function. We also investigate its consequences towards the parity conjecture.

7.1. *Compatibility up to p-adic units*

Let us recall at first the Main Conjecture over the GL_2-extension. Fix a global minimal Weierstra equation for E over $\mathbb{Z}$. We denote by $\Omega_\pm(E)$ the periods of E, defined by integrating the Néron differential of this Weierstra equation over the ± 1 eigenspaces $H_1(E(\mathbb{C}), \mathbb{Z})^\pm$ of complex conjugation. As usual, Ω_- is chosen to lie in $i\mathbb{R}$. Moreover, for any Artin representation τ of the absolute Galois group of $\mathbb{Q}$ let $d^+(\tau)$ and $d^-(\tau)$ denote the dimension of the subspace of the vector space of τ on which complex conjugation acts by $+1$ and -1, respectively. Deligne's period conjecture [15] asserts that

$$\frac{L(E, \tau, 1)}{\Omega_+(E)^{d^+(\tau)} \Omega_-(E)^{d^-(\tau)}} \in \overline{\mathbb{Q}}. \tag{7.1}$$

Let R denote the set of rational primes at which E has potentially multiplicative reduction. We define the modified L-function

$$L_R(E, \tau, s) := \prod_{q \notin R} P_q(E, \tau, q^{-s})^{-1} \tag{7.2}$$

by removing the Euler factors at primes in R. Finally, since E has good ordinary reduction at p, we have

$$P_p(E, T) = 1 - a_p T + p T^2 = (1 - b_p T)(1 - c_p T), \quad b_p \in \mathbb{Z}_p^\times, \tag{7.3}$$

where $p + 1 - a_p = \#(\tilde{E}_p(\mathbb{F}_p))$ is the number of points on the curve reduced modulo p.

Conjecture 1 [7, Conjecture 5.7]. Assume that $p \geqslant 5$ and that E has good ordinary reduction at p. Then there exists $\mathfrak{L}_E$ in $K_1(\Lambda(G)_{S^*})$ such that, for all Artin representations τ of G, we have $\mathfrak{L}_E(\tau) \neq \infty$, and

$$\mathfrak{L}_E(\tau^*) = \frac{L_R(E, \tau, 1)}{\Omega_+(E)^{d^+(\tau)} \Omega_-(E)^{d^-(\tau)}} \cdot \varepsilon_p(\tau) \cdot \frac{P_p(\tau^*, b_p^{-1})}{P_p(\tau, c_p^{-1})} \cdot b_p^{-f_\tau}, \tag{7.4}$$

where $\varepsilon_p(\tau)$ denotes the local ε-factor at p attached to τ, and p^{f_τ} is the p-part of the conductor of τ.

The Main Conjecture of the Iwasawa theory for elliptic curves without complex multiplication over the GL_2-extension is the following.

Conjecture 2 [7, Conjecture 5.8]. Assume that $p \geqslant 5$, E has good ordinary reduction at p, and $X(E/F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$. Granted Conjecture 1, the p-adic L-function $\mathfrak{L}_E$ in $K_1(\Lambda(G)_{S^*})$ is a characteristic element of $X(E/F_\infty)$.

Remark 3. Recently Bouganis and Venjakob [4] managed to prove the Main Conjecture (Conjecture 2) for curves with complex multiplication using the two-variable Main Conjecture by Yager [36], and Rubin [28] assuming that the dual Selmer lies in the category $\mathfrak{M}_H(G)$. Moreover, Coates and Sujatha [12] have made some progress towards eliminating this assumption for CM curves.

To investigate the connections between Corollary 6.6 and Conjecture 2, we need the values of the local factors α_q at Artin representations.

Proposition 7.1. *Let τ be an Artin representation of the Galois group $G = \mathrm{Gal}(F_\infty/\mathbb{Q})$. Then we have*

$$\alpha_q(\tau) = \varepsilon_q(\tau_{G_q}^{(1)}) \frac{P_q(E,\tau,q^{-1})}{P_q(E,\tau^*,q^{-1})}, \tag{7.5}$$

where $\tau_{G_q}^{(1)}$ is the maximal subrepresentation of the restriction of τ to the decomposition subgroup G_q of G on which the eigenvalues of the generator i_q of $I_q^{(1)}$ are not equal to 1.

Proof. As both sides of (7.5) depend only on τ_{G_q} and are multiplicative with respect to the direct sum of Artin representations, we only need to prove the statement separately for Artin representations τ_{G_q} with eigenvalues of $\tau_{G_q}(i_q)$ being 1 and different from 1.

If 1 is not an eigenvalue of $\tau_{G_q}(i_q)$, then the image of $X_q = i_q - 1$ under τ_{G_q} is invertible. This means that τ_{G_q} maps β_q and $X_q\beta_q X_q^{-1}$ to conjugate matrices and so

$$\alpha_q(\tau_{G_q}) = \frac{(X_q\beta_q X_q^{-1})^{\#}(\tau_{G_q})}{(X_q\beta_q X_q^{-1})(\tau_{G_q})} = \frac{\beta_q^{\#}(\tau_{G_q})}{\beta_q(\tau_{G_q})} = \varepsilon_q(\tau_{G_q}). \tag{7.6}$$

On the other hand, in this case $P_q(E,\tau,q^{-1}) = P_q(E,\tau^*,q^{-1}) = 1$ as $(T_p(E)^* \otimes \tau)^{I_q}$ is trivial. Therefore the statement is true whenever 1 is not an eigenvalue of $\tau_{G_q}(i_q)$.

Now let $\tau_{G_q}(i_q)$ be equal to the identity matrix as this is the case when all its eigenvalues are equal to 1. It is enough to prove that

$$(X_q\beta_q X_q^{-1})^{\#}(\tau_{G_q}) = \left(\frac{X_q+1}{X_q}\beta_q^{\#}\frac{X_q}{X_q+1}\right)(\tau_{G_q}) = P_q(E,\tau,q^{-1}) \tag{7.7}$$

since $(X_q\beta_q X_q^{-1})(\tau_{G_q}) = (X_q\beta_q X_q^{-1})^{\#}(\tau_{G_q}^*)$. We compute

$$\begin{aligned}\left(\frac{X_q+1}{X_q}\beta_q^{\#}\frac{X_q}{X_q+1}\right)(\tau_{G_q}) &= \left(\frac{X_q+1}{X_q}(1\pm e_q\mathrm{Frob}_q^{-1})\frac{X_q}{X_q+1}\right)(\tau_{G_q}) \overset{(1)}{=}\\ &= \left(1\pm e_q\frac{X_q+1}{X_q}\mathrm{Frob}_q^{-1}\frac{X_q}{X_q+1}\right)(\tau_{G_q}) \overset{(2)}{=}\\ &= \left(1\pm e_q\frac{(X_q+1)^{1/q}-1}{X_q(X_q+1)^{1/q-1}}\mathrm{Frob}_q^{-1}\right)(\tau_{G_q}) \overset{(3)}{=}\\ &= \det\left(\tau_{G_q}\left(1\pm e_q\frac{(X_q+1)^{1/q}-1}{X_q(X_q+1)^{1/q-1}}\mathrm{Frob}_q^{-1}\right)\right) \overset{(4)}{=}\\ &= \det\left(1\pm\tau_{G_q}(e_q)q^{-1}\tau_{G_q}(\mathrm{Frob}_q^{-1})\right). \end{aligned} \tag{7.8}$$

Indeed, we have the following:

(1) e_q is central by Lemma 6.5;

(2) Frob_q^{-1} acts on (X_q+1) by conjugation via the cyclotomic character $\chi_{cyc}(\mathrm{Frob}_q^{-1}) = 1/q$;

(3) By definition (see [7, pp. 9–10]) noting that

$$1\pm e_q\frac{(X_q+1)^{1/q}-1}{X_q(X_q+1)^{1/q-1}}\mathrm{Frob}_q^{-1}$$

lies in $\Lambda(G_q)$.

(4) $\tau_{G_q}(X_q) = 0$ by assumption.

Moreover, e_q is an idempotent element in $\Lambda(I_q) \subset \Lambda(G_q)$ which corresponds to the projective cover of A_q. This means that, using a suitable basis, $\tau_{G_q}(e_q)$ is a diagonal matrix with entries 0 or 1 and the entries 1 correspond to the generators of the subspace $W'_{\tau_{G_q}}$ of $W_{\tau_{G_q}}$ on which $I_q/I_q^{(1)}$ acts the same way as on $A_q = T_p(E)^{I_q^{(1)}}$. Now by the self-duality of the Galois representation A_q this space is spanned by the vectors occurring in $(T_p(E)^*\otimes W_{\tau_{G_q}})^{I_q}$. Hence we have

$$\begin{aligned}\det(1\pm\tau_{G_q}(e_q)q^{-1}\tau_{G_q}(\mathrm{Frob}_q^{-1})) &= \det(1\pm q^{-1}\tau_{G_q}(\mathrm{Frob}_q^{-1}) \mid W'_{\tau_{G_q}})\\ &= \det(1-q^{-1}\mathrm{Frob}_q^{-1} \mid (T_p(E)^*\otimes W_{\tau_{G_q}})^{I_q}) = P_q(E,\tau,q^{-1})\end{aligned} \tag{7.9}$$

because we have the equality

$$(T_p(E)^*\otimes W_{\tau_{G_q}})^{I_q} = (T_p(E)^{*I_q^{(1)}}\otimes W_{\tau_{G_q}}^{I_q^{(1)}})^{I_q/I_q^{(1)}} \tag{7.10}$$

and Frob_q^{-1} acts on $T_p(E)^{*I_q^{(1)}}$ by ∓1. The statement follows. □

Remark 4. (i) It is easy to see that the part of the statement of [37, Proposition 7.3] dealing with the primes of split multiplicative reduction is a special case of this above proposition. However, the (potentially) good primes, the other case of [37, Proposition 7.3], do not ramify infinitely in this GL_2-extension, and that is why we do not deal with them in this paper.

(ii) This above proposition is analogous to the more general Proposition 4.4.6 in [18]. However, there the non-commutative Tamagawa number conjectures are assumed.

Since $\mathfrak{L}_E^{\#}(\tau) = \mathfrak{L}_E(\tau^*)$ for any Artin representation τ of G, by this above proposition we conclude the following proposition.

Proposition 7.2. *The functional equation of the characteristic element of $X(E/F_\infty)$ is compatible with the Main Conjecture up to p-adic units. By this we mean that the values*

$\mathfrak{L}_E(\tau)$ and $\mathfrak{L}_E(\tau^*)$ prescribed by Conjecture 1 differ by the same value (up to p-adic units) as the value we get from the functional equation (6.41) using Conjecture 2.

Proof. Indeed, by Conjecture 1 we have

$$\mathfrak{L}_E(\tau^*) = \frac{L_R(E,\tau,1)}{\Omega_+(E)^{d^+(\tau)}\Omega_-(E)^{d^-(\tau)}} \cdot \varepsilon_p(\tau) \cdot \frac{P_p(\tau^*, b_p^{-1})}{P_p(\tau, c_p^{-1})} \cdot b_p^{-f_\tau} \tag{7.11}$$

and

$$\mathfrak{L}_E^{\#}(\tau^*) = \mathfrak{L}_E(\tau) = \frac{L_R(E,\tau^*,1)}{\Omega_+(E)^{d^+(\tau^*)}\Omega_-(E)^{d^-(\tau^*)}} \cdot \varepsilon_p(\tau^*) \cdot \frac{P_p(\tau, b_p^{-1})}{P_p(\tau^*, c_p^{-1})} \cdot b_p^{-f_{\tau^*}}.$$

Moreover, the functional equation of the complex L-function is

$$\hat{L}(E,\tau,s) = w(E,\tau)\hat{L}(E,\tau^*,2-s), \tag{7.12}$$

where

$$\hat{L}(E,\tau,s) := \left(\frac{N(E,\tau)}{\pi^{2\dim\tau}}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{\dim\tau} \Gamma\left(\frac{s+1}{2}\right)^{\dim\tau} L(E,\tau,s). \tag{7.13}$$

From this we obtain

$$L(E,\tau,1) = w(E,\tau)L(E,\tau^*,1) \tag{7.14}$$

as the modifying factors are the same for τ and τ^* at $s=1$ since τ and τ^* have both the same dimension and conductor. Moreover, $d^{\pm}(\tau^*) = d^{\pm}(\tau)$ and the local factors at p cancel each other as they do in the functional equation over the cyclotomic extension, and so by combining (7.11) and (7.14) we get that

$$\frac{\mathcal{L}_E(\tau^*)}{\prod_{q\in R\setminus\{p\}} P_q(E,\tau,q^{-1})} \quad \text{and} \quad \frac{\mathcal{L}_E^{\#}(\tau^*)}{\prod_{q\in R\setminus\{p\}} P_q(E,\tau^*,q^{-1})} \tag{7.15}$$

are equal up to p-adic units. Thus Proposition 7.1 shows that the functional equation of the characteristic element of the dual Selmer is compatible with the conjectural functional equation of the p-adic L-function up to p-adic units. □

7.2. *Root numbers*

In this section we are going to investigate the sign in the functional equation of the characteristic element when we substitute a self-dual Artin representation τ. We assume that τ is realized over $\mathcal{O}$, the ring of integers of a finite extension L of $\mathbb{Q}_p$ with maximal ideal $\mathcal{M}$. Moreover, let W_τ be the $\mathcal{O}$-representation space of τ. We define

(i) $r_E(\tau)$ as the multiplicity of τ in $E(F)\otimes L$, where τ factors through $\mathrm{Gal}(F/\mathbb{Q})$;

(ii) $s_E(\tau)$ as the $\mathcal{O}$-corank of $\mathrm{Sel}(\mathrm{tw}_\tau(E)/\mathbb{Q})$ which is by definition the Selmer group associated to the Galois representation $T_p(E)\otimes_{\mathbb{Z}_p} W_\tau$;

(iii) $\lambda_E(\tau)$ as the $\mathcal{O}$-rank of the dual Selmer $X(\mathrm{tw}_\tau(E)/\mathbb{Q}^{\mathrm{cyc}})$;

(iv) $w_E(\tau)$ as the analytic root number associated to the complex L-function $L(E,\tau,s)$.

The parity conjecture, which is a consequence of the generalized Birch–Swinnerton-Dyer conjecture, asserts that

$$(-1)^{r_E(\tau)} = (-1)^{s_E(\tau)} = (-1)^{\lambda_E(\tau)} = w_E(\tau) \tag{7.16}$$

for all irreducible self-dual Artin representations τ.

Our main goal in this section is to prove some special cases of this conjecture when τ factors through the GL_2-extension associated to the elliptic curve E. The strategy is to relate the sign in the functional equation of the characteristic element of $X(E/F_\infty)$ to these quantities. We substitute the self-dual Artin representation τ into (6.41) in order to get a functional equation of the twisted Akashi series of $X(E/F_\infty)$ by τ. Whenever we have a functional equation

$$f(1/(T+1)-1)=\varepsilon_f(T)f(T) \tag{7.17}$$

in the ring $\mathbb{Q}_p\otimes\mathcal{O}[\![T]\!]$ with ε_f in $\mathcal{O}[\![T]\!]^\times$, we can define its sign by the reduction of $\varepsilon_f(0)$ modulo the maximal ideal $\mathcal{M}$. Moreover, it is easy to see that this sign is equal to $(-1)^{\deg(g)}$ when we decompose f by the Weierstraß-preparation theorem in the form $f(T)=p^k u(T)g(T)$, where k is an integer, $u(T)$ is in $\mathcal{O}[\![T]\!]^\times$, and $g(T)$ is a distinguished polynomial of degree $\deg(g)$. Further, the roots of $g(T)$ are in pairs $(z,1/(z+1)-1)$ except for the root $T=0$ and so $\deg(g)$ has the same parity as its order of vanishing at $T=0$.

Note that any irreducible self-dual Artin representation admits a non-degenerate pairing on its representation space. This pairing can either be orthogonal or symplectic and then we call the representation itself orthogonal or symplectic, respectively. The following theorem of Greenberg makes orthogonal representations easier to handle. We shall use this later on.

THEOREM 7.3 Greenberg [19]. *Let τ be an orthogonal Artin representation of the group G. Then the order of vanishing of the characteristic power series of the module $X(\mathrm{tw}_\tau(E)/\mathbb{Q}^{\mathrm{cyc}})$ has the same parity as the rank of the dual Selmer $X(\mathrm{tw}_\tau(E)/\mathbb{Q})$.*

The following proposition shows that the sign in the functional equation of the characteristic element of the dual Selmer $X(E/F_\infty)$ naturally contains all the information about the signs in the residue functional equations of the characteristic elements of the twisted dual Selmers over the cyclotomic extension.

PROPOSITION 7.4. *Let τ be a self-dual Artin representation of the group G. Then we have*

$$\varepsilon_0(X(E/F_\infty))(\tau)\prod_{q\in R}\alpha_q(\tau)\equiv(-1)^{\mathrm{ord}_{T=0}\xi_{X(\mathrm{tw}_\tau(E)/\mathbb{Q}^{\mathrm{cyc}})}}=(-1)^{\lambda_E(\tau)}\pmod{\mathcal{M}}, \tag{7.18}$$

where $\xi_{X(\mathrm{tw}_\tau(E)/\mathbb{Q}^{\mathrm{cyc}})}$ is the characteristic power series (in $\mathcal{O}[\![T]\!]$) of the Pontryagin dual of the Selmer group $\mathrm{Sel}(\mathrm{tw}_\tau(E)/\mathbb{Q}^{\mathrm{cyc}})$. This is the sign in the functional equation we get when we substitute τ into the functional equation of $\xi_{X(E/F_\infty)}$.

Proof. The proof is similar to the proof of [37, Proposition 5.5]. The sign in the functional equation of $\xi_{X(E/F_\infty)}(\tau)$ is by definition the reduction of the left-hand side of equation (7.18) modulo the maximal ideal $\mathcal{M}$ of $\mathcal{O}$. Hence it suffices to prove the first statement.

The value of an element ξ in $K_1(\Lambda(G)_{S^*})$ at the Artin representation τ is by definition

$$\varphi(\Phi'_\tau(\xi))\in\mathcal{O} \tag{7.19}$$

whenever it is defined, and ∞ otherwise (see Subsection 3.4). Moreover, by [7, Lemma 3.7], we have that $\Phi'_\tau(\xi_{X(E/F_\infty)})$ is the Akashi series of the module $X(E/F_\infty)\otimes W_\tau$ which is isomorphic to the module $X(\mathrm{tw}_{\tau^*}(E)/F_\infty)=X(\mathrm{tw}_\tau(E)/F_\infty)$ by [6, Lemma 3.4]. As the higher homology groups $H_i(H,X(\mathrm{tw}_\tau(E)/F_\infty))$ for $i\geqslant 1$ are p-torsion by [7, Lemmas 3.9 and 5.3], this Akashi series actually lies in $\mathcal{O}[\![T]\!][1/p]$. The sign in question is

$$(-1)^{\mathrm{ord}_{T=0}\mathrm{Ak}_{\mathcal{O}}(X(\mathrm{tw}_\tau(E)/F_\infty))}. \tag{7.20}$$

Indeed, the sign in a functional equation satisfied by an element $f(T)$ in $\mathcal{O}[\![T]\!][1/p]$ relating $f(T)$, and $f(1/(T+1)-1)$ equals -1 to the order of vanishing of the power series at $T=0$ as all the other roots of the power series are in pairs $(z,1/(z+1)-1)$.

Since the characteristic elements for p-torsion modules are powers of p and these do not vanish at $T=0$, the order of vanishing of the Akashi series of $X(\mathrm{tw}_\tau(E)/F_\infty)$ equals the order of vanishing of the characteristic power series of $X(\mathrm{tw}_\tau(E)/F_\infty)_H$ at $T=0$. On the other hand we have the restriction homomorphism

$$X(\mathrm{tw}_\tau(E)/F_\infty)_H \longrightarrow X(\mathrm{tw}_\tau(E)/\mathbb{Q}^{\mathrm{cyc}}) \tag{7.21}$$

with finite cokernel. Its kernel equals up to finite modules

$$\bigoplus_{q\in R} H^0(\mathrm{Gal}(\overline{\mathbb{Q}_q}/\mathbb{Q}_q^{\mathrm{cyc}}), T_p(E)\otimes W_\tau) \tag{7.22}$$

by [**6**, Theorem 3.5 and Lemma 3.6] (see also the arguments (5.30)–(5.40) for trivial τ). It suffices to show that the characteristic power series of (7.22) does not vanish at $T=0$. Since τ is an Artin representation, an element $\sum_i x_i\otimes y_i$ can only lie in the summand at q in (7.22) if a finite index subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}_q}/\mathbb{Q}_q^{\mathrm{cyc}})$ fixes all the x_i. On the other hand, by the theory of the Tate curve we have a short exact sequence

$$0\longrightarrow A_q(1)\longrightarrow T_p(E)\longrightarrow A_q\longrightarrow 0, \tag{7.23}$$

where A_q is a (free of rank 1 over $\mathbb{Z}_p$) Galois module on which $\mathrm{Gal}(\overline{\mathbb{Q}_q}/\mathbb{Q}_q^{\mathrm{cyc}})$ acts via a quadratic character if the reduction at q is additive, and trivially otherwise. Moreover, Frob_q acts on A_q by -1 if the reduction is split multiplicative, and trivially otherwise. Moreover, $A_q(1)$ is the maximal submodule of $T_p(E)$ on which $\mathrm{Gal}(\overline{\mathbb{Q}_q}/\mathbb{Q}_q^{\mathrm{cyc}})$ acts via a finite quotient. Further, $\mathrm{Gal}(\mathbb{Q}_q^{\mathrm{cyc}}/\mathbb{Q}_q)$ does not act via a finite quotient on $A_q(1)$ (as Frob_q acts via the cyclotomic character), and hence nor on

$$H^0(\mathrm{Gal}(\overline{\mathbb{Q}_q}/\mathbb{Q}_q^{\mathrm{cyc}}), T_p(E)\otimes W_\tau). \tag{7.24}$$

Indeed, otherwise $\tau(\mathrm{Frob}_q)$ would not have finite order for some q, which is impossible. The result follows noting that $\mathrm{Gal}(\mathbb{Q}_q^{\mathrm{cyc}}/\mathbb{Q}_q)$ cannot fix any element of (7.24), and so its characteristic power series does not vanish at $T=0$. □

Now we turn to the description of $\varepsilon_0(X(E/F_\infty))$. Let $\{P_i \mid 1\leqslant i\leqslant r\}$ be the set of indecomposable projective $\Lambda(H)$-modules. These projective modules correspond to the irreducible finite-dimensional modular representations of H in characteristic p. Further, we choose orthogonal idempotents e_{P_i} in $\Lambda(H)$ such that $P_i=\Lambda(H)e_{P_i}$. These are lifts of orthogonal idempotents of the semisimple Artinian ring $\Lambda(H)/\mathrm{Jac}(\Lambda(H))$, where $\mathrm{Jac}(\Lambda(H))$ is the Jacobson radical of the Iwasawa algebra $\Lambda(H)$. These lifts exist by [**14**, Volume I, Theorem 6.7] as $\Lambda(H)$ is complete with respect to its $\mathrm{Jac}(\Lambda(H))$-adic filtration, in other words it is a complete semilocal ring.

Proposition 7.5. *Let $[X(E/F_\infty)/X(E/F_\infty)(p)]=\sum_{i=1}^r n_i[P_i]$ be the decomposition of the class of $X(E/F_\infty)/X(E/F_\infty)(p)$ in the Grothendieck group $K_0(\Lambda(H))$, where $n_i\in\mathbb{Z}$. Then, for each self-dual Artin representation τ of G over $\mathcal{O}$, the ring of integers of a finite extension of $\mathbb{Q}_p$ we have*

$$\varepsilon_0(X(E/F_\infty))(\tau)\equiv\prod_{i=1}^r(1-2e_{P_i})(\tau)^{n_i}\prod_{q\in R}\varepsilon_q(\chi_{q,\mathrm{cyc}}\tau) \pmod{\mathcal{M}} \tag{7.25}$$

where $\chi_{q,\mathrm{cyc}}$ is the character of H_q acting on μ_{p^∞} and $\mathcal{M}$ is the maximal ideal of $\mathcal{O}$.

Proof. By Corollary 6.6 we obtain

$$\xi^{\#}_{X(E/F_\infty)}=\xi_{X(E/F_\infty)}\varepsilon_0(X(E/F_\infty))\prod_{q\in R}\alpha_q, \tag{7.26}$$

so

$$\left(\xi_{X(E/F_\infty)}\prod_{q\in R}(X_q\beta_qX_q^{-1})^{\#}\right)^{\#}=\varepsilon_0(X(E/F_\infty))\left(\xi_{X(E/F_\infty)}\prod_{q\in R}(X_q\beta_qX_q^{-1})^{\#}\right). \tag{7.27}$$

Now, for each self-dual representation τ of G, we define a homomorphism

$$\mathrm{sign}_\tau\colon K_0(\Lambda(H))\longrightarrow\{\pm 1\}, \tag{7.28}$$

$$[M]\mapsto(-1)^{\sum_{i=0}^{\infty}(-1)^i\mathrm{rk}_{\mathcal{O}}(H_i(H,\mathrm{tw}_{\tau_{|H}}(M)))}. \tag{7.29}$$

Note that the summation is always finite in (7.29). It is easy to see that this a well-defined homomorphism as the right-hand side is multiplicative with respect to short exact sequences. Moreover, let M be a module in the category $\mathfrak{M}_H(G)$ with characteristic element ξ_M in $K_1(\Lambda(G)_{S^*})$ satisfying a functional equation $\xi_M^{\#}=\varepsilon_M\xi_M$ with ε_M in $K_1(\Lambda(G)$. Then we have

$$\varepsilon_M(\tau)\equiv\mathrm{sign}_\tau([M/M(p)])\ (\mathrm{mod}\ \mathcal{M}) \tag{7.30}$$

because both are the sign in the functional equation of the Akashi series of $\mathrm{tw}_\tau(M)$ as the Akashi series of p-torsion modules are powers of p and so they do not influence the sign of the functional equation. Note that this means that the $\Lambda(H)$-structure of M already determines the sign in the functional equation.

Now we can apply (7.30) on

$$\partial_G\left(\xi_{X(E/F_\infty)}\prod_{q\in R}(X_q\beta_qX_q^{-1})^{\#}\right). \tag{7.31}$$

On the other hand, we have

$$\mathrm{sign}_\tau(P_i)=(1-2e_{P_i})(\tau). \tag{7.32}$$

Indeed, $\tau(e_{P_i})$ is an idempotent matrix in $M_{\dim\tau}(\mathcal{O})$ because e_{P_i} is an idempotent in $\Lambda(G)$. Hence, in a suitable basis $\tau(e_{P_i})$ is a diagonal matrix with entries 0 or 1 in the diagonal. Moreover, its rank is $m_i(\tau)$, the number of copies of τ in the representation space $(\mathcal{O}\otimes P_i)_{\mathrm{Ker}(\tau)\cap H}$. Thus it equals the $\mathcal{O}$-rank of $(\mathrm{tw}_\tau(P_i))_H$ (by Frobenius reciprocity) and

$$(1-2e_{P_i})(\tau)=\det(\tau(1-2e_{P_i}))=(-1)^{m_i(\tau)}=\mathrm{sign}_\tau(P_i). \tag{7.33}$$

Hence it remains to show that, for $q\in R$, we have

$$\mathrm{sign}_\tau(\partial_G(X_q\beta_qX_q^{-1}))\equiv\varepsilon_q(\chi_{q,\mathrm{cyc}}\tau)\ (\mathrm{mod}\ \mathcal{M}). \tag{7.34}$$

For this let us note that

$$\partial_G(X_q\beta_qX_q^{-1})\cong\Lambda(G)\otimes_{\Lambda(G_q)}\partial_{G_q}(X_q\beta_qX_q^{-1}) \tag{7.35}$$

since $X_q\beta_qX_q^{-1}$ lies in $\Lambda(G_q)$, and so we can work over $\Lambda(G_q)$. Moreover, as $\Lambda(H_q)$-modules we have the isomorphisms

$$\partial_{G_q}(X_q\beta_qX_q^{-1})\cong\chi_{q,\mathrm{cyc}}\otimes\partial_{G_q}(\beta_q) \tag{7.36}$$

and so

$$\tau\otimes\partial_{G_q}(X_q\beta_qX_q^{-1})\cong(\chi_{q,\mathrm{cyc}}\tau)\otimes\partial_{G_q}(\beta_q). \tag{7.37}$$

Indeed, by the definition of ∂_{G_q} we have $\partial_{G_q}(\beta_q)=\Lambda(G_q)/\Lambda(G_q)\beta_q$, which has rank 1 over $\mathbb{Z}_p[[X_q]]$ by the construction of β_q. Moreover, the map

$$\begin{aligned}\partial_{G_q}(X_q\beta_qX_q^{-1})=\Lambda(G_q)/\Lambda(G_q)(X_q\beta_qX_q^{-1})&\longrightarrow\Lambda(G_q)X_q/(\Lambda(G_q)X_q\cap\Lambda(G_q)X_q\beta_q)\\ 1+\Lambda(G_q)(X_q\beta_qX_q^{-1})&\mapsto X_q+(\Lambda(G_q)X_q\cap\Lambda(G_q)X_q\beta_q)\end{aligned} \tag{7.38}$$

is an isomorphism of $\Lambda(G_q)$-modules because it is clearly surjective and both sides have rank 1 over $\mathbb{Z}_p[[X_q]]$. Now note that $I_q^{(1)} = \langle 1 + X_q \rangle$ is a finite (prime to p) index subgroup of H_q on which H_q acts by conjugation via the cyclotomic character $\chi_{q,\mathrm{cyc}}$. On the other hand, both $\partial_{G_q}(\beta_q)$ and $\partial_{G_q}(X_q\beta_q X_q^{-1})$ are projective $\Lambda(H_q)$-modules (both are free of rank 1 over $\Lambda(I_q^{(1)})$) and the projective modules over this ring are determined by the $H_q/I_q^{(1)}$-action on their 0th $I_q^{(1)}$-homology. However, for the homology groups we have

$$H_0(I_q^{(1)}, \partial_{G_q}(X_q\beta_q X_q^{-1})) = \chi_{q,\mathrm{cyc}} \otimes H_0(I_q^{(1)}, \partial_{G_q}(\beta_q)) \tag{7.39}$$

as $H_q/I_q^{(1)}$-modules since $H_q/I_q^{(1)}$ acts on X_q via $\chi_{q,\mathrm{cyc}}$ modulo X_q^2. Therefore we have

$$\partial_{G_q}(X_q\beta_q X_q^{-1}) \cong \chi_{q,\mathrm{cyc}} \otimes \partial_{G_q}(\beta_q) \tag{7.40}$$

as $\Lambda(H_q)$-modules because both sides are projective and have the same action of $H_q/I_q^{(1)}$ on their 0th $I_q^{(1)}$-homology.

Thus we obtain

$$\mathrm{sign}_\tau(\partial_G(X_q\beta_q X_q^{-1})) \equiv \mathrm{sign}_{\chi_{q,\mathrm{cyc}}\tau}(\partial_G(\beta_q)) \equiv \varepsilon_q(\chi_{q,\mathrm{cyc}}\tau) \pmod{\mathcal{M}} \tag{7.41}$$

as $\beta_q^{\#} = \varepsilon_q\beta_q$. □

For each prime q in R we define the character χ_q of G_q with $\chi_q^2 = 1$ as follows. If E has split multiplicative reduction at q, then $\chi_q := 1$; if E does not have split multiplicative reduction, then χ_q is the non-trivial character of the Galois group of the quadratic extension of $\mathbb{Q}_q$ over which E achieves split multiplicative reduction. Note that χ_q can indeed be viewed as a character of G_q as E always achieves split multiplicative reduction over $\mathbb{Q}_q(E[p^\infty])$. Combining Propositions 7.1, 7.4, and 7.5 we get the following theorem.

Theorem 7.6. *If τ is any self-dual Artin representation of G, then we have*

$$(-1)^{\lambda_E(\tau)} = \prod_{i=1}^{r}(1 - 2e_{P_i})(\tau)^{n_i} \prod_{q\in R}(-1)^{\langle \chi_q\chi_{q,\mathrm{cyc}}^{-1}, \tau_{G_q}\rangle} \tag{7.42}$$

where $\langle \chi_q\chi_{q,\mathrm{cyc}}^{-1}, \tau_{G_q}\rangle$ is the multiplicity of the character $\chi_q\chi_{q,\mathrm{cyc}}^{-1}$ in the representation τ_{G_q}.

Proof. First of all note that both sides of (7.42) are *a priori* ±1 by equation (7.33). Since τ is self-dual, by Proposition 7.1 we have

$$\alpha_q(\tau) = \varepsilon_q(\tau_{G_q}^{(1)})\frac{P_q(E,\tau,q^{-1})}{P_q(E,\tau^*,q^{-1})} = \varepsilon_q(\tau_{G_q}^{(1)}) = (X_q\varepsilon_q X_q^{-1})(\tau_{G_q}^{(1)}). \tag{7.43}$$

as $\tau(X_q)$ is invertible in this case. Hence we only need to verify that, for any q in R,

$$(-1)^{\langle \chi_q\chi_{q,\mathrm{cyc}}^{-1}, \tau_{G_q}\rangle} \equiv (X_q\varepsilon_q X_q^{-1})(\tau_{G_q}^{(2)}) = \varepsilon_q(\chi_{q,\mathrm{cyc}}\tau_{G_q}^{(2)}) \pmod{\mathcal{M}}, \tag{7.44}$$

where $\tau_{G_q}^{(2)}$ is the maximal subrepresentation of τ_{G_q} on which the generator i_q of $I_q^{(1)}$ acts trivially. Indeed, τ_{G_q} clearly equals $\tau_{G_q}^{(1)} \oplus \tau_{G_q}^{(2)}$. For the proof of (7.44) we apply our remark after Lemma 6.5,

$$\varepsilon_q = 1 + e_q(\mathrm{Frob}_q^{-1} - 1) \quad \text{if } E \text{ has non-split multiplicative reduction at } q, \tag{7.45}$$

$$\varepsilon_q = 1 - e_q(\mathrm{Frob}_q^{-1} + 1) \quad \text{otherwise.} \tag{7.46}$$

Moreover, recall that e_q is the idempotent element in $\Lambda(I_q)$ corresponding to the projective $\Lambda(I_q)$-module $T_p(E)^{I_q^{(1)}} \otimes \Lambda(I_q^{(1)})$. Now we distinguish three cases.

Case 1: E has split multiplicative reduction at q. Then $I_q = I_q^{(1)}$, and so $e_q = 1$, $\chi_q = 1$, and

$$\varepsilon_q(\chi_{q,\mathrm{cyc}}\tau^{(2)}_{G_q}) = -\mathrm{Frob}_q^{-1}(\chi_{q,\mathrm{cyc}}\tau^{(2)}_{G_q}) = (-1)^{\langle \chi_{q,\mathrm{cyc}}^{-1}, \tau_{G_q}\rangle} \tag{7.47}$$

because both sides are equal to (-1) to the dimension of the subrepresentation of τ on which I_q acts trivially and Frob_q via $\chi_{q,\mathrm{cyc}}^{-1}$.

Case 2: E has split multiplicative reduction at q. Then $I_q = I_q^{(1)}$, and so $e_q = 1$, $\chi_q(\mathrm{Frob}_q) = -1$, and $\varepsilon_q = \mathrm{Frob}_q^{-1}$. Thus

$$\varepsilon_q(\chi_{q,\mathrm{cyc}}\tau^{(2)}_{G_q}) = \mathrm{Frob}_q^{-1}(\chi_{q,\mathrm{cyc}}\tau^{(2)}_{G_q}) = (-1)^{\langle \chi_q\chi_{q,\mathrm{cyc}}^{-1}, \tau_{G_q}\rangle} \tag{7.48}$$

because both sides are equal to (-1) to the multiplicity of the eigenvalue $-\chi_{q,\mathrm{cyc}}(\mathrm{Frob}_q)$ of $\tau^{(2)}_{G_q}(\mathrm{Frob}_q)$.

Case 3: E has additive (but potentially multiplicative) reduction at q. Then we have

$$\varepsilon_q(\chi_{q,\mathrm{cyc}}\tau^{(2)}_{G_q}) = \det(\chi_{q,\mathrm{cyc}}\tau^{(2)}_{G_q}(1 - e_q(\mathrm{Frob}_q^{-1}+1))) = \det(-\mathrm{Frob}_q^{-1} \mid W), \tag{7.49}$$

where W is the subrepresentation of $\chi_{q,\mathrm{cyc}}\tau_{G_q}$ on which I_q acts via the character χ_q because $\chi_{q,\mathrm{cyc}}\tau^{(2)}_{G_q}(e_q)$ is the projection onto this space. Now this is (-1) to the dimension of the subspace of τ on which G_q acts via $\chi_q\chi_{q,\mathrm{cyc}}^{-1}$ as this is exactly the tensor product of $\chi_{q,\mathrm{cyc}}^{-1}$ and the subspace of W on which Frob_q acts trivially.

So the result follows in each case. □

We also have the following version of the above theorem as a corollary.

Corollary 7.7. *Let τ be a self-dual representation of G which does not factor through the maximal pro-p normal subgroup G_0 of G. We get*

$$(-1)^{\lambda_E(\tau)} = \prod_{i=1}^{r}(1-2e_{P_i})(\tau)^{n_i}\prod_{q\in R}(-1)^{\langle \chi_q, \tau_{G_q}\rangle}. \tag{7.50}$$

Proof. This is a consequence of [6, Lemma 6.18]. We only need to verify that if τ does not factor through the maximal pro-p normal subgroup G_0 of G, then, for all q in R, we have

$$\langle \chi_q, \tau_{G_q}\rangle = \langle \chi_q\chi_{q,\mathrm{cyc}}^{-1}, \tau_{G_q}\rangle = (\langle \chi_q\chi_{q,\mathrm{cyc}}^{-1}, \tau_{G_q}\rangle + \langle \chi_q\chi_{q,\mathrm{cyc}}, \tau_{G_q}\rangle)/2. \tag{7.51}$$

Since $G_q \subset G$ is always contained in an Iwahori subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$, we may restrict τ to the Iwahori subgroup containing G_q and decompose the restriction into irreducible representations. If all these irreducible components have dimension at least 2, then the statement follows from [6, Lemma 6.18]. Note that we may assume that these irreducible subrepresentations of the restriction to the Iwahori subgroup are also self-dual as otherwise we would have their contragredient representation as a constitute too, and we could just cancel both of them by the second equality of (7.51). Moreover, if we have a self-dual irreducible 1-dimensional representation of the Iwahori subgroup, then it has to be trivial on its pro-p-Sylow subgroup (which is the same as the pro-p-Sylow of G) as these elements cannot map to -1. Now the statement follows noting that if τ does not satisfy (7.51), then its representation space has to have a 1-dimensional subspace on which the maximal pro-p normal subgroup acts trivially and the subspace on which a normal subgroup acts trivially is a subrepresentation, and so it has to be the whole τ as τ is irreducible. □

Now we can state our main result in this section.

Theorem 7.8. *Let us assume that E is an elliptic curve defined over $\mathbb{Q}$, without complex multiplication, with good ordinary reduction at the prime p and good or potentially multiplicative reduction at the primes 2 and 3. Moreover, assume that $X(E/F_\infty)$ is in the category $\mathfrak{M}_H(G)$. Then if*

$$(-1)^{\lambda_E(\tau)} = w_E(\tau) \tag{7.52}$$

holds for all self-dual representations τ of G/G_0, then it is also true for any self-dual representation τ of G. Here G_0 denotes the maximal pro-p normal subgroup of G.

Proof. Let τ be an Artin representation of G that does not factor through G/G_0. We would like to prove that the product of the two sides of (7.52) depend only on the semisimplification $\widetilde{\tau}^{ss}$ of the reduction $\widetilde{\tau}$ of τ modulo the maximal ideal $\mathcal{M}$ of $\mathcal{O}$. From this the statement follows by noting that the irreducible modular representations of G in characteristic p factor through G/G_0 and it is a theorem of Brauer (see [30, Part III, Theorem 1]) that we have a surjection

$$K_0(\mathrm{Rep}(G/G_0)) \longrightarrow K_0(\mathrm{Rep}_{\text{mod-}p}(G/G_0)) \tag{7.53}$$

from the Grothendieck group of the finite-dimensional representations of G/G_0 in characteristic zero to Grothendieck group of finite-dimensional modular representations of G/G_0. This surjection is in fact the reduction map modulo the maximal ideal $\mathcal{M}$ of $\mathcal{O}$. Moreover, Greenberg [19, Propositions 10.2.1 and 11.2.1] (see also [26]) showed that the product of the analytic root number and the terms $\langle \chi_q \chi_{q,\mathrm{cyc}}^{-1}, \tau_{G_q}\rangle$ only depends on the image of τ in $K_0(\mathrm{Rep}_{\text{mod-}p}(G/G_0))$. Hence it remains to show the same for the terms $(1-2e_{P_i})(\tau)$. Indeed, by definition for each indecomposable projective module P_i of $\Lambda(H)$ we have

$$(1-2e_{P_i})(\tau) = (-1)^{m_i(\tau)}, \tag{7.54}$$

where $m_i(\tau)$ equals the inner product of the character of the modular H-representation corresponding to the projective module P_i with the character of the modular representation $\widetilde{\tau}^{\mathrm{ss}}$ and by nature depends only on $\widetilde{\tau}^{\mathrm{ss}}$. This latter fact is a basic result in modular representation theory and can be found in both [19, § 2 of Section 1.1; 30]. The result follows. □

Remark 5. (i) The theorem above is closely related to [19, Proposition 11.3]. However, Greenberg's assumptions are a bit different. He does not investigate the Selmer group over F_∞, but he works always over a finite extension of $\mathbb{Q}^{\mathrm{cyc}}$. Moreover, we do not need the finiteness of the p-Selmer group over any finite extension of $\mathbb{Q}^{\mathrm{cyc}}$. However, we do need the assumption that $X(E/F_\infty)$ is in $\mathfrak{M}_H(G)$ and that E has good ordinary reduction at p.

(ii) The assumptions on the reduction type of E at 2 and 3 should be unnecessary, but the formulas of Rohrlich [26] for the local root numbers do not cover all the cases. For example, if G is contained in the Iwahori subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ (or in other words E has a p-isogeny over $\mathbb{Q}$), then these assumptions are removable.

We end this section by proving a purely group theoretical statement and its consequences when G is contained in the Iwahori subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$.

Proposition 7.9. *Let A be an open subgroup of the Iwahori subgroup*

$$B = \left\{ M \in \mathrm{GL}_2(\mathbb{Z}_p) \mid M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{p} \right\} \tag{7.55}$$

of $\mathrm{GL}_2(\mathbb{Z}_p)$ such that the determinant map

$$\det\colon \tilde{A} \longrightarrow \mathbb{F}_p^\times \tag{7.56}$$

is surjective on the image $\tilde{A}$ of A in $\mathrm{GL}_2(\mathbb{F}_p)$ under the natural reduction map $\mathrm{GL}_2(\mathbb{Z}_p) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$. Then A does not have any irreducible symplectic Artin representation (in characteristic zero).

Proof. We prove the statement indirectly. Let us assume that

$$\tau\colon A \longrightarrow \mathrm{GL}_k(\overline{\mathbb{Q}}) \tag{7.57}$$

is an irreducible symplectic Artin representation. Now write $A_0 := A/\mathrm{Ker}(\tau)$. Since τ is Artin, it follows that A_0 is a finite group. Moreover, note that the centre $Z(A_0)$ of A_0 has order at most 2 because by Schur's lemma central elements map to diagonal matrices under irreducible representations and the entries in these diagonal matrices must equal ± 1 as τ is self-dual. Now τ is faithful on A_0 by construction and the centre of the image has order at most 2. Further, we have the following lemma.

Lemma 7.10. *We have that A_0 is either abelian or can be written in the form*

$$(P \rtimes S) \times C, \tag{7.58}$$

where $P \neq 1$ is a finite p-group, C is cyclic of order at most 2, and S is also cyclic of order dividing $p-1$.

Proof. As the normalizer of the pro-p-Sylow subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ is exactly the Iwahori subgroup, we immediately get that the p-Sylow subgroup P of A_0 is normal in A_0. Moreover, the p-Sylow subgroup has a complement in A_0, which is a factor of a subgroup of the diagonal matrices in $\mathrm{GL}_2(\mathbb{F}_p)$. Thus this complement is generated by two elements both of order dividing $p-1$ as this diagonal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ is isomorphic to $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$. We may assume without loss of generality that $P \neq 1$ because otherwise A_0 would be abelian. Now let $n \geqslant 1$ be the smallest integer such that $\mathrm{Ker}(\tau)$ contains the intersection of A with the nth congruent subgroup

$$I_n := \{M \in \mathrm{GL}_2(\mathbb{Z}_p) \mid M \equiv \mathrm{id} \pmod{p^n}\}. \tag{7.59}$$

Let us denote by I_0 the pro-p-Sylow subgroup of B. By the construction the image of $A \cap I_{n-1}$ is a non-trivial normal p-subgroup in A_0 and so has a non-trivial intersection with the centre of P. Let us denote this intersection by $P_0 = Z(P) \cap \mathrm{Im}(A \cap I_{n-1})$. Now A_0/P does not act trivially on any non-trivial subgroup of P_0 because otherwise that subgroup would be in the centre of A_0, which contradicts the fact that it has odd order by our remark before the Lemma 7.10. It also follows that $\mathrm{Ker}(\tau)$ cannot contain an element x of order dividing $p-1$, which is not a scalar matrix. Indeed, this would mean that $\mathrm{Ker}(\tau)$ contained a non-trivial element in P_0, namely the commutator of x and an arbitrary non-trivial element in P_0. Now $A/(A \cap I_0)$ is generated by two elements g_1 and g_2 and we may assume that g_2 is (the image of) a scalar matrix of order dividing $p-1$. On the other hand, since the determinant map is surjective on $\tilde{A}$, it follows that g_1 has to be the image of a diagonal matrix $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \beta\end{smallmatrix}\right)$ such that one of α and β has to be a quadratic residue modulo p and the other one a quadratic non-residue as otherwise the image of the determinant map would only contain quadratic residues. It is easy to see from this that if a power of g_1 is a diagonal matrix, then this power has to have odd order. This means that the intersection of the subgroups generated by the image of g_1 and g_2 in A_0/P is just the trivial element; moreover, the image of g_2 has at most order 2 as it is in the centre of A_0. The lemma follows by putting S and C to be the image of the group generated by g_1 and g_2, respectively. □

Now the proof of the proposition is as follows. Abelian groups have only 1-dimensional irreducible representations and these cannot be symplectic since those have even dimension. Thus we may assume that A_0 is in the form (7.58). The restriction of τ to $P \rtimes S$ is also irreducible and symplectic as C maps to scalar matrices under τ. Now as in the proof of the Lemma 7.10, we see that S acts faithfully on P_0. Moreover, P_0 is an abelian group of exponent p and so it can be viewed as a vector space over $\mathbb{F}_p$; thus we can pick up a non-trivial eigenvector $v \in P_0$ of the S-action (S is cyclic). This means that the subgroup generated by v is normal in $P \rtimes S$ and so the eigenvalues of $\tau(v)$ are different from 1 because otherwise v would either be in the kernel of τ or the subspace on which $\tau(v)$ acts trivially would be a non-trivial invariant subspace of the underlying vector space of τ. Now S permutes regularly the eigenspaces of v because S acts faithfully on the subgroup generated by v. In other words τ is induced from P. Now since τ is self-dual, the eigenvalues of τ are in pairs (ζ, ζ^{-1}), where ζ is a primitive pth root of unity, and so there must be an element s of order 2 in S such that $svs^{-1} = v^{-1}$. This means that in a suitable basis, $\tau(s)$ is in the block matrix form

$$\begin{pmatrix} 0 & \mathrm{id} & 0 & 0 & \dots & 0 & 0 \\ \mathrm{id} & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \mathrm{id} & \dots & 0 & 0 \\ 0 & 0 & \mathrm{id} & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & \mathrm{id} \\ 0 & 0 & 0 & 0 & \dots & \mathrm{id} & 0 \end{pmatrix}. \tag{7.60}$$

This means that the matrix of the invariant bilinear symplectic form also has to be in the form

$$\begin{pmatrix} 0 & X_1 & 0 & 0 & \dots & 0 & 0 \\ X_1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & X_2 & \dots & 0 & 0 \\ 0 & 0 & X_2 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & X_l \\ 0 & 0 & 0 & 0 & \dots & X_l & 0 \end{pmatrix} \tag{7.61}$$

because if u is an eigenvector of v with eigenvalue ζ, and if its inner product with w is non-zero, then w has to be an eigenvector with eigenvalue ζ^{-1} and the matrix of the invariant symplectic form commutes with $\tau(s)$. Now this form is symplectic if and only if $X_i = -X_i^{\mathrm{T}}$ for each $1 \leqslant i \leqslant l$, where $\cdot^{\mathrm{T}}$ denotes the transpose matrix. This is a contradiction because X_i has p-power dimension because its dimension is equal to the degree of an irreducible representation of P. □

Remark 6. (i) The statement of Proposition 7.9 remains true if we replace the assumption of the surjectivity of the determinant map with the weaker assumption that there exists a quadratic non-residue in the image. Moreover, if p is congruent to 3 modulo 4, then we do not even need this assumption. We omit the proof of these as they are similar to the proof of Proposition 7.9.

(ii) On the other hand the following example shows that the statement fails to be true if we drop both the conditions in the previous remark. Let A be the subgroup of the Iwahori subgroup generated by the pro-p-Sylow subgroup and the element

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \tag{7.62}$$

of order 4, where i is an element of $\mathbb{Z}_p$ with $i^2 = -1$. There is such an element if p is congruent to 1 (mod 4). Now let σ be the 2-dimensional representation of A, which is trivial on the congruent subgroup

$$\sigma\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right) = \begin{pmatrix}\xi & 0\\ 0 & \xi^{-1}\end{pmatrix} \quad\text{and}\quad \sigma\left(\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}\right) = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \tag{7.63}$$

where ξ is a primitive pth root of unity. This is clearly an irreducible representation admitting the symplectic pairing with matrix $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$.

Our next corollary has essentially been proved independently by Coates, Fukaya, Kato and Sujatha [6] too. Their method was completely different.

Corollary 7.11. *Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at the prime p. Let us assume that $X(E/F_\infty)$ is in the category $\mathfrak{M}_H(G)$ and that E has a p-isogeny over $\mathbb{Q}$. Then, for any self-dual Artin representation τ, we have*

$$(-1)^{s_E(\tau)} = w_E(\tau). \tag{7.64}$$

Proof. Since E has a p-isogeny over $\mathbb{Q}$, the group G is contained in an Iwahori subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. We may assume without loss of generality that this Iwahori subgroup is the standard upper Iwahori subgroup B. By the Weil pairing the determinant map on the reduction of G to $\mathrm{GL}_2(\mathbb{F}_p)$ is surjective onto $\mathbb{F}_p^\times$, and so by Proposition 7.9 we conclude that G does not have symplectic representations and thus τ is orthogonal. For orthogonal representations the statement follows from Greenberg's Theorem (Theorem 7.3) and Theorem 7.8 (see also [6, Theorem 6.2]) by noting that if τ factors through G/G_0, then τ is actually a 1-dimensional character and in this latter case the parity conjecture has already been proved [16]. Indeed, since τ is self-dual, it has to be a quadratic character. Moreover, for quadratic characters both the analytic and arithmetic root numbers are the quotients of the root numbers over the quadratic field defined by τ and over the rational numbers. Formally our corollary only follows when we assume that the reduction of E is either semistable or potentially multiplicative at the primes 2 and 3, but we only need to check that the local analytic root numbers at 2 and 3 only depend on the semisimplification $\widetilde{\tau}^{\mathrm{ss}}$ of the reduction of τ modulo the maximal ideal $\mathcal{M}$ in $\mathcal{O}$. By [27, Proposition 3], it follows that if E has potentially multiplicative reduction at the prime q, then the local root number at q is

$$\det \tau_{G_q}(-1)\chi_q(-1)^{\dim \tau}, \tag{7.65}$$

where χ_q is a certain fixed character of $\mathrm{Gal}(\overline{\mathbb{Q}_q}/\mathbb{Q}_q)$ associated to E. Now since -1 has order prime to p, we have that $\det \tau_{G_q}(-1)$ depends only on $\widetilde{\tau}^{ss}$ and the other term only depends on $\dim \tau = \dim \widetilde{\tau}^{\mathrm{ss}}$ and we are done. □

8. *An example*

We end this paper by giving an example of an elliptic curve illustrating our results. Let E be the elliptic curve 11A3 in Cremona's tables [13], of conductor 11. It has a minimal Weiestraß equation

$$E:\ y^2 + y = x^3 - x^2 \tag{8.1}$$

and is also denoted by $X_1(11)$. It does not admit complex multiplication and thus is relevant to us. Let $p = 5$ at which $X_1(11)$ has good ordinary reduction. Moreover, it has a rational point of order 5, and hence we have

$$E[5] \cong \mathbb{Z}/5\mathbb{Z} \oplus \mu_5. \tag{8.2}$$

Now it is easy to see [8] that in this case $\mathrm{Gal}(F_\infty/\mathbb{Q})$ can be identified with the subgroup G of $\mathrm{GL}_2(\mathbb{Z}_p)$ consisting of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c \equiv 0 \pmod{5^2}$ and $a \equiv 1 \pmod 5$. This means that the Galois group $\mathrm{Gal}(F_\infty/\mathbb{Q}(\mu_5))$ is pro-p. Now the only bad prime for E is 11 and the reduction type is split multiplicative. So $X(E/F_\infty)$ has rank 4 over the Iwasawa algebra

$$\Lambda(H_K) := \Lambda(\mathrm{Gal}(F_\infty/\mathbb{Q}(\mu_{5^\infty}))) \tag{8.3}$$

as the prime 11 splits completely in the field $\mathbb{Q}(\mu_5)$ and $X(E/\mathbb{Q}(\mu_{5^\infty})) = 0$ (see [11]), so $X(E/F_\infty)$ is in $\mathfrak{M}_H(G)$. Moreover, the corestriction map

$$X(E/F_\infty)_{H_K} \longrightarrow X(E/\mathbb{Q}(\mu_{5^\infty})) = 0 \tag{8.4}$$

has kernel of $\mathbb{Z}_p$-rank 4. Four elements of this kernel, which are $\mathbb{Z}_p$-independent, correspond to the four primes v_i $(i = 1, 2, 3, 4)$ above 11 in $\mathbb{Q}(\mu_5)$ as they are the images of the generators of

$$\mathrm{Hom}(H^1(H_{K,v_i}, E[5^\infty]), \mathbb{Q}_p/\mathbb{Z}_p) \tag{8.5}$$

for $i = 1, 2, 3, 4$. Therefore the element of order 4 in G acts regularly on these elements. Now let ξ be a characteristic element of $X(E/F_\infty)$ in $K_1(\Lambda(G)_{S^*})$. Further, $\mathrm{Frob}_{11} = \left(\begin{smallmatrix} 11 & 0 \\ -50 & 1 \end{smallmatrix}\right)$ is a topological generator of the group G/H. Now we can apply Corollary 6.6. The functional equation of the characteristic element is in the form

$$\xi^\# = \xi\varepsilon_0 \frac{(X_{11}(1 - \mathrm{Frob}_{11})X_{11}^{-1})^\#}{X_{11}(1 - \mathrm{Frob}_{11})X_{11}^{-1}}, \tag{8.6}$$

where $X_{11} = \left(\begin{smallmatrix} 6 & 1 \\ -25 & -4 \end{smallmatrix}\right) - 1$ as an element of $\Lambda(H)$. As

$$X_{11}(1 - \mathrm{Frob}_{11})X_{11}^{-1} = 1 - \frac{X_{11}}{(X_{11}+1)^{11} - 1}\mathrm{Frob}_{11}, \tag{8.7}$$

the simplest example for ξ would be $\mathrm{Frob}_{11} - ((X_{11}+1)^{11} - 1)/X_{11}$ because it certainly satisfies a functional equation in the form (8.6). However, this element is in the image of $K_1(\Lambda(G_{11})_{S_{11}})$ and so it would give the same characteristic power series of $X(E/L_1^{\mathrm{cyc}})$ and $X(E/L_2^{\mathrm{cyc}})$, where $L_1 = \mathbb{Q}(E[p])$, $L_2 = \mathbb{Q}(\mu_{11})^+(\mu_5)$, and $\mathbb{Q}(\mu_{11})^+$ denotes the maximal real subfield of $\mathbb{Q}(\mu_{11})$. (Note that L_2 is contained in F_∞.) Indeed, the completions $L_{1,11}$ and $L_{2,11}$ at primes above 11 are isomorphic and so the $\mathrm{Gal}(F_\infty/L_1)$- and $\mathrm{Gal}(F_\infty/L_2)$-Akashi series of $X(E/F_\infty)$ would be the same in this case. This would contradict to the Birch–Swinnerton-Dyer conjecture as the complex L-function of the curve over $L_1(\mu_{5^n})$ does not vanish for any n and the order of vanishing of the complex L-function over $L_2(\mu_{5^2})$ is exactly 4 by a result of Matsuno (see the end of [5] for details). Now let

$$\gamma := \begin{pmatrix} \sqrt{11} & 0 \\ 0 & \sqrt{11} \end{pmatrix}, \tag{8.8}$$

$$\alpha := \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}, \tag{8.9}$$

$$\delta := \gamma \mathrm{Frob}_{11}^{-1}\left((1 + X_{11})^3 + X_{11}^2(\alpha + 1)X_{11}\right), \tag{8.10}$$

$$\xi_0 := \gamma^2 - \delta(\delta^\#)^{-1}, \tag{8.11}$$

$$\xi_* := \gamma^2 - X_{11}\delta(\delta^\#)^{-1}X_{11}^{-1}, \tag{8.12}$$

where $\sqrt{11}$ and i are fixed elements in $\mathbb{Z}_5$ with $\sqrt{11}^2 = 11$ and $i^2 = -1$.

We are going to prove that ξ_* satisfies all the conjectural properties of the characteristic element of $X(E/F_\infty)$ known so far. The first step is that it satisfies the required functional equation.

Proposition 8.1. *The element ξ_* in $K_1(\Lambda(G)_{S^*})$ satisfies the functional equation*

$$\xi_*^{\#} = \xi_* \varepsilon_* \frac{(X_{11}(1 - \mathrm{Frob}_{11})X_{11}^{-1})^{\#}}{X_{11}(1 - \mathrm{Frob}_{11})X_{11}^{-1}} \tag{8.13}$$

with some element ε_* in $K_1(\Lambda(G))$.

Proof. At first note that ξ_0 satisfies a functional equation without a modifying term outside $K_1(\Lambda(G))$. Indeed, we have

$$\xi_0^{\#} = -\gamma^4 \delta \xi_0 (\delta^{\#})^{-1} \tag{8.14}$$

as γ is in the centre of $\Lambda(G)$. Moreover, it is easy to see that $\delta(\delta^{\#})^{-1}$ lies in the set $\gamma^2 \mathrm{Frob}_{11}^{-2} + \Lambda(H)X_{11}$. This means that the modules

$$\partial_G(\xi_0/\xi_*) = (\Lambda(G)/\Lambda(G)\xi_0) \,/\, (\Lambda(G)X_{11}/(\Lambda(G)\xi_0 \cap \Lambda(G)X_{11})) \tag{8.15}$$

and

$$\partial_G \left((\mathrm{Frob}_{11} - 1) \left(\mathrm{Frob}_{11} - \frac{(X_{11}+1)^{11} - 1}{X_{11}} \right)^{-1} \right) \tag{8.16}$$

$$= (\Lambda(G)/\Lambda(G)(\mathrm{Frob}_{11} - 1)) \,/\, (\Lambda(G)X_{11}/(\Lambda(G)(\mathrm{Frob}_{11} - 1) \cap \Lambda(G)X_{11})) \tag{8.17}$$

are isomorphic since they are trivially isomorphic as $\Lambda(H)$-modules, and γ acts the same way on them. Now ξ_0 and $\mathrm{Frob}_{11} - 1$ satisfy functional equations of the same type, and therefore so do ξ_* and $\mathrm{Frob}_{11} - ((X_{11}+1)^{11} - 1)/X_{11}$. □

Let us remark that satisfying the above type of functional equation is equivalent to a condition on the characteristic elements of the kernels of the corestriction maps

$$X(E/F_\infty)_{H_n} \longrightarrow X(E/F_n^{\mathrm{cyc}}). \tag{8.18}$$

Apart from the functional equation the characteristic element has to satisfy, we also know some information about the behaviour of the curve E over the following three Galois extensions of degree 20 of $\mathbb{Q}$:

$$L_1 = \mathbb{Q}(E[5]), \quad L_2 = \mathbb{Q}(\mu_{11})^+(\mu_5), \quad L_3 = \mathbb{Q}(E'[5]), \tag{8.19}$$

where E' is the unique elliptic curve which is 5-isogenous to E. These Galois extensions all contain $\mathbb{Q}(\mu_5)$. Let us denote by P the unique pro-p-Sylow subgroup of H. It is easy to see that as an abstract group P/P^5 is isomorphic to $\mathbb{F}_5^3$. It has three generators, namely $a_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \pmod{P^5}$, $a_2 = \left(\begin{smallmatrix} 6 & 0 \\ 0 & 1/6 \end{smallmatrix}\right) \pmod{P^5}$, and $a_3 = \left(\begin{smallmatrix} 1 & 0 \\ 25 & 1 \end{smallmatrix}\right) \pmod{P^5}$. These are all eigenvectors of the generator of $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ corresponding to different eigenvalues. Moreover, the image of a_i is trivial in L_j if and only if $i \neq j$.

The next step is that ξ_* gives the required [5] Mordell–Weil rank over the fields contained in L_2^{cyc}.

Proposition 8.2. *Assume that $\partial_G(\xi_*) = X(E/F_\infty)$. Then the order of vanishing of the characteristic power series of $X(E/L_2^{\mathrm{cyc}})$ is zero at $T = 0$ and 1 at $T = \zeta_5 - 1$, where ζ_5 is any fixed primitive fifth root of unity. In other words this would conjecturally imply that the Mordell–Weil rank is zero over L_2 but 4 over $L_2(\mu_{5^2})$.*

Proof. The Galois group $\mathrm{Gal}(L_2/\mathbb{Q})$ is cyclic of order 20. It can be easily seen that the image of α in this Galois group is an element of order 4 and the images of $X_{11} + 1$ and $\gamma \mathrm{Frob}_{11}^{-1}$ are elements of order 5 (and are in fact each other's reciprocal). The characters of $\mathrm{Gal}(L_2/\mathbb{Q})$ of order dividing 4 correspond to the kernel of the restriction map

$$X(E/F_\infty)_{H_{L_2}} \longrightarrow X(E/L_2^{\mathrm{cyc}}) \tag{8.20}$$

and so they do not give any zero at $T = 0$ or $T = \zeta_5 - 1$. Now consider a fixed character χ which takes $X_{11} + 1$ to ζ_5^3 and α to some power of i. Then we have

$$\xi_*(\chi) = (T+1)^2 - \zeta_5^{-1}\left(\zeta_5^{-1} + (\chi(\alpha)+1)(\zeta_5^{-1} - 1)^3\right)\left(\zeta_5 + (\chi(\alpha)+1)(\zeta_5 - 1)^3\right)^{-1}. \tag{8.21}$$

This power series does not have a root at $T = 0$ and has a root of multiplicity 1 at $T = \zeta_5 - 1$ if and only if $\chi(\alpha) = -1$. The result follows. □

Finally we prove that if the characteristic element of $X(E/F_\infty)$ was ξ_*, then there would be no points over the fields $\mathbb{Q}(E[5])^{\mathrm{cyc}}$ and $\mathbb{Q}(E'[5])^{\mathrm{cyc}}$, where E' is the elliptic curve with conductor 11 and no 5-torsion point over $\mathbb{Q}$, which result is compatible with the previously known facts about this curve [5]. Note that this latter field is also contained in F_∞ as E and E' are 5-isogenous.

Proposition 8.3. *Assume that $\partial_G(\xi_*) = X(E/F_\infty)$. Then the characteristic power series of $X(E/L_i^{\mathrm{cyc}})$ $(i = 1, 3)$ do not vanish at $T = \zeta - 1$, where ζ is any root of unity of 5-power order, $L_3 = \mathbb{Q}(E'[5])$, and E' is the unique elliptic curve with the isogeny $E \to E'$ of degree 5. In other words this would conjecturally imply that the Mordell–Weil rank is zero over L_1^{cyc} and L_3^{cyc}.*

Proof. The Galois groups $\mathrm{Gal}(L_1/\mathbb{Q}) \cong \mathrm{Gal}(L_3/\mathbb{Q})$ are isomorphic to the group $(\mathbb{Z}/5\mathbb{Z}) \rtimes (\mathbb{Z}/5\mathbb{Z})^\times$.

Let us begin with the description of $\mathrm{Gal}(L_1/\mathbb{Q})$. The images of α, $X_{11} + 1$, and $\gamma\mathrm{Frob}_{11}^{-1}$ are an element of order 4, an element of order 5, and trivial, respectively. The group $(\mathbb{Z}/5\mathbb{Z}) \rtimes (\mathbb{Z}/5\mathbb{Z})^\times$ has four 1-dimensional characters and one irreducible representation ρ of dimension 4. The 1-dimensional representations correspond to the kernel of the restriction maps

$$X(E/F_\infty)_{H_{L_i}} \longrightarrow X(E/L_i^{\mathrm{cyc}}) \quad i = 1, 3 \tag{8.22}$$

again. Hence it remains to prove that the characteristic power series we get by substituting the irreducible 4-dimensional representation into ξ_* does not vanish at $T = \zeta - 1$ for any ζ 5-power root of unity. As $\rho(X_{11})$ is invertible, $\rho(\xi_0)$ equals $\rho(\xi_*)$. Moreover,

$$\begin{aligned}\rho(\xi_0) &= \det\left((T+1)\mathrm{id} - A(A^*)^{-1}\right) \qquad \text{where} \\ A &= \begin{pmatrix} \zeta_5^3 + (\zeta_5 - 1)^3 & (\zeta_5 - 1)^2(\zeta_5^2 - 1) & 0 & 0 \\ 0 & \zeta_5 + (\zeta_5^2 - 1)^3 & (\zeta_5^2 - 1)^2(\zeta_5^4 - 1) & 0 \\ 0 & 0 & \zeta_5^2 + (\zeta_5^4 - 1)^3 & (\zeta_5^4 - 1)^2(\zeta_5^3 - 1) \\ (\zeta_5^3 - 1)^2(\zeta_5 - 1) & 0 & 0 & \zeta_5^4 + (\zeta_5^3 - 1)^3 \end{pmatrix}\end{aligned} \tag{8.23}$$

and A^* denotes 'the complex conjugate' (the unique Galois-automorphism of the extension $\mathbb{Q}_5(\mu_5)/\mathbb{Q}_5$ which takes ζ_5 to ζ_5^{-1}) of the transpose matrix of A. It is easy to see that if the order of ζ is at least 25, then the polynomial $\rho(\xi_0)$ does not vanish at $T = \zeta - 1$ as its degree is 4 and ζ is not contained in any extension of $\mathbb{Q}_5(\mu_5)$ of degree 4. In order to prove that $\rho(\xi_0)$ does not vanish at $T = 0$, note that the entries in the diagonal of the matrix $A^* - A$ have $\zeta_5 - 1$-valuation 1 and all the other entries have bigger valuations. This means that the determinant of $A^* - A$ has valuation 4 and, in particular, it is not equal to zero. It follows that 1 is not an eigenvalue of the matrix $A(A^*)^{-1}$ and the polynomial in question does not vanish at $T = 0$. Hence it remains to show that $\zeta - 1$ is not a root of $\rho(\xi_0)$, where ζ is a fifth root of unity or equivalently that $\det(\zeta A^* - A) \neq 0$. For any fifth root of unity ζ the entries of the matrix $\zeta A^* - A$ have valuations at least 3 except for three of the four diagonal elements which have valuation 1. Moreover, the remaining element in the diagonal has valuation exactly 3. This means that the valuation of the determinant of this matrix is exactly 6 as all but one of the terms in its expansion have valuation bigger than 6 and the term coming from the diagonal has valuation exactly 6. In particular this determinant is non-zero.

The case of $\mathrm{Gal}(L_3/\mathbb{Q})$ is quite similar. The only difference is that the image of $\gamma\mathrm{Frob}_{11}^{-1}$ is not trivial in this group but the third power of the image of $X_{11}+1$. Thus the matrix A has the form

$$A = \begin{pmatrix} \zeta_5 + \zeta_5^3(\zeta_5 - 1)^3 & \zeta_5^3(\zeta_5 - 1)^2(\zeta_5^2 - 1) & 0 & 0 \\ 0 & \zeta_5^2 + \zeta_5(\zeta_5^2 - 1)^3 & \zeta_5(\zeta_5^2 - 1)^2(\zeta_5^4 - 1) & 0 \\ 0 & 0 & \zeta_5^4 + \zeta_5^2(\zeta_5^4 - 1)^3 & \zeta_5^2(\zeta_5^4 - 1)^2(\zeta_5^3 - 1) \\ \zeta_5^4(\zeta_5^3 - 1)^2(\zeta_5 - 1) & 0 & 0 & \zeta_5^3 + \zeta_5^4(\zeta_5^3 - 1)^3 \end{pmatrix} \tag{8.24}$$

in this case. The result follows similarly as above. □

Remark 7. The characteristic element ξ_* described above is by far not the only one satisfying all the requirements. The proofs of the Propositions 8.1–8.3 show that we had a lot of freedom in choosing this particular ξ_*. This still leaves the following question open.

Problem 2. What is the asymptotic rank of $X_1(11)$ inside the GL_2-extension? Is it finite or infinite?

Acknowledgements. I would like to express my gratitude to my research supervisor, John Coates, for suggesting the problem and for his constant encouragement. I would like to thank Konstantin Ardakov, Tim Dokchitser, Ralph Greenberg, and Simon Wadsley for valuable discussions and comments.

References

1. K. Ardakov and S. Wadsley, 'Characteristic elements for p-torsion Iwasawa modules', *J. Algebraic Geom.* 15 (2006) 339–377.

2. K. Ardakov and S. Wadsley, 'K_0 and the dimension filtration for p-torsion Iwasawa modules', *Proc. London Math. Soc.* 97 (2008) 31–59.

3. J.-E. Björk, 'Filtered Noetherian rings', *Noetherian rings and their applications*, Mathematical Survey Monographs 24 (American Mathematical Society, Providence, RI, 1987) 59–97.

4. Th. Bouganis and O. Venjakob, 'On the noncommutative Iwasawa Main Conjecture for CM-elliptic curves', Preprint, 2009, http://www.newton.ac.uk/programmes/NAG/seminars/072711301.html.

5. J. Coates, 'Iwasawa algebras and arithmetic', *Astérisque* 29 (2003).

6. J. Coates, T. Fukaya, K. Kato and R. Sujatha, 'Root numbers, Selmer groups, and non-commutative Iwasawa theory', *J. Algebraic Geom.* 19 (2010) 19–97.

7. 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.

8. J. Coates and S. Howson, 'Euler characteristics and elliptic curves II', *J. Math. Soc. Japan* 53 (2001) 175–235.

9. J. Coates, P. Schneider and R. Sujatha, 'Links between cyclotomic and GL_2 Iwasawa theory', *Doc. Math.*, Extra Volume: Kazuya Kato's Fiftieth Birthday (2003) 187–215.

10. J. Coates, P. Schneider and R. Sujatha, 'Modules over Iwasawa algebras', *J. Inst. Math. Jussieu* (2003) 73–108.

11. J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research 88 (Narosa, New Delhi, 2000).

12. J. Coates and R. Sujatha, 'Iwasawa theory of elliptic curves with complex multiplication', Preprint, 2009, http://www.newton.ac.uk/programmes/NAG/seminars/072810001.html.

13. J. Cremona, 'Elliptic curves data', Preprint, http://www.warwick.ac.uk/staff/J.E.Cremona//ftp/data/.

14. C.W. Curtis and I. Reiner, *Methods of representation theory*', (Wiley, New York, 1981).

15. P. Deligne, *Valeur de fonctions L et périodes d'intégrales*, Proceedings of Symposia in Pure Mathematics 33 (American Mathematical Society, Providence, RI, 1979) 313–346.

16. T. Dokchitser and V. Dokchitser, 'Self-duality of Selmer groups', *Math. Proc. Cambridge Philos. Soc.* 146 (2009), 257–267.

17. M. Flach, 'A generalisation of the Cassels–Tate pairing', *J. reine angew. Math.* 412 (1990) 113–127.

18. T. Fukaya and K. Kato, 'A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory', *Proceedings of the St. Petersburg Mathematical Society*, vol. XII, American Mathematical Society Translations Series 2 219 (American Mathematical Society, Providence, RI, 2006) 1–85.

19. R. Greenberg, 'Iwasawa theory, projective modules, and modular representations', *Mem. Amer. Math. Soc.*, to appear.

20. R. Greenberg, 'Iwasawa theory for p-adic representations', *Adv. Stud. Pure Math.* 17 (1989) 97–137.

21. R. Greenberg, 'Introduction to Iwasawa theory for elliptic curves', *Arithmetic algebraic geometry* (American Mathematical Society, Providence, RI, 2009) 407–464.

22. Y. Hachimori and K. Matsuno, 'On finite Λ-submodules of Selmer groups of elliptic curves, *Proc. Amer. Math. Soc.* 128 (2000) 2539–2541.

23. Y. Hachimori and O. Venjakob, 'Completely faithful Selmer groups over Kummer extensions', *Doc. Math.*, Extra Volume: Kazuya Kato's Fiftieth Birthday (2003) 443–478.

24. U. Jannsen, 'Iwasawa modules up to isomorphism', *Adv. Stud. Pure Math.* 17 (1989) 171–207.

25. B. Perrin-Riou, 'Groupes de Selmer et accouplements; Cas particulier des courbes elliptiques', *Doc. Math.*, Extra Volume: Kazuya Kato's Fiftieth Birthday (2003) 725–760.

26. D. E. Rohrlich, 'Galois theory, elliptic curves, and root numbers', *Compos. Math.* 100 (1996) 311–349.

27. D. E. Rohrlich, 'Scarcity and abundance of trivial zeros in division towers', *Journal of Algebraic Geom.* 17 (2008) 643–675.

28. K. Rubin, 'The "main conjectures" of Iwasawa theory for imaginary quadratic fields', *Invent. Math.* 103 (1991) 25–68.

29. P. Schneider and O. Venjakob, 'On the codimension of modules over skew power series rings with applications to Iwasawa algebras', *J. Pure Appl. Algebra* 204 (2005) 349–367.

30. J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics (Springer, London, 1977).

31. J.-P. Serre, 'Properiètés Galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* 15 (1972) 259–331.

32. B. Stenström, *Rings of quotients* (Springer, Berlin, 1975).

33. L. N. Vaserstein, 'On the Whitehead determinant for semi-local rings', *J. Algebra* 283 (2005) 690–699.

34. O. Venjakob, 'Iwasawa theory of p-adic Lie extensions', PhD Thesis, University of Heidelberg, 2000.

35. O. Venjakob, 'On the structure of Iwasawa algebra of a p-adic Lie group', *J. Eur. Math. Soc.* 4 (2002) 272–311.

36. R. I. Yager, 'On two variable p-adic L-functions', *Ann. of Math.* (2) 115 (1982) 153–191.

37. G. Zábrádi, 'Characteristic elements, pairings, and functional equations over the false Tate curve extension', *Math. Proc. Cambridge Philos. Soc.* 144 (2008) 535–574.

Gergely Zábrádi
Max-Planck-Institut fr Mathematik
Vivatsgasse 7
53111 Bonn
Germany

zger@cs.elte.hu