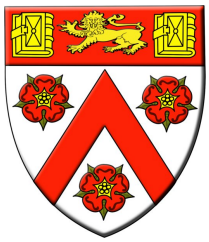
Characteristic elements, pairings, and functional equations in non-commutative Iwasawa theory

GERGELY ZÁBRÁDI

Trinity College



This dissertation is submitted for the degree of Doctor of Philosophy.

Research Supervisor: Prof John H Coates

16th April 2008

Summary

This dissertation deals with the conjectural functional equation of the p-adic L-function attached to elliptic curves over p-adic Lie extensions of the rationals unramified outside a finite set of primes. From arithmetic viewpoint one of the most interesting p-adic Lie extensions is the GL_2-extension defined by adjoining all the p-power division points on the elliptic curve E. In this case we implicitly assume that E has no complex multiplication so that the Galois group is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. Another interesting example of p-adic Lie extensions is the false Tate tower which is the extension of $\mathbb{Q}$ by adjoining all p-power roots of unity and all the p-power roots of a given integer m. In both cases we construct a pairing over the tower extension F_∞ on the dual Selmer group of the elliptic curve E with good ordinary reduction at a prime p whenever the dual Selmer satisfies certain—conjectured—torsion properties. This gives a functional equation of the characteristic element under the anti-involution of the Galois group $\mathrm{Gal}(F_\infty/\mathbb{Q})$ sending elements to their inverses. This functional equation is compatible with the—conjectural—functional equation of the p-adic L-function which would be, by the Main Conjecture, a characteristic element for the dual Selmer.

As an application we reduce the parity conjecture inside the GL_2-extension for the p-Selmer rank and the analytic root number for Artin twists of elliptic curves to the case when the Artin representation factors through the finite group $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. In particular this gives a new proof of the parity conjecture in this case whenever the elliptic curve E has a p-isogeny over the rationals.

Over the false Tate curve extension, however, much more is known. For example, we can compute the characteristic elements of those modules—arising naturally in Iwasawa-theory—which have rank 1 over the Iwasawa algebra of the subgroup of the Galois group fixing the cyclotomic extension of the ground field. There are no such examples known in the GL_2-case.

Preface

This dissertation has been written for the PhD degree at the University of Cambridge. It is my original work. The results dealing with the false Tate curve extension (chapter 2) have already been accepted for publication at the Mathematical Proceedings of the Cambridge Philosophical Society [42]. The results concerning the GL_2-extension (chapter 3) have also been submitted for publication to the London Mathematical Society and are under consideration. I have done this research on my own and whenever I have used any results of other people, an explicit citation has been made. I gratefully acknowledge the encouragement and support of my research supervisor, Prof. J. H. Coates. During this research I was holding an External Research Studentship of Trinity College, Cambridge, under the title Prince of Wales.

Contents

Chapter 1

Introduction

The main conjectures of Iwasawa theory usually state that (i) there exists a p-adic L-function attached to the elliptic curve E over a p-adic Lie extension of $\mathbb{Q}$ which interpolates the special values of the complex L-functions of E 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 conjecture of Birch and Swinnerton-Dyer. From arithmetic viewpoint one of the most interesting p-adic Lie extensions is the GL_2-extension defined by adjoining all the p-power division points on the elliptic curve E. In this case we will assume that E has no complex multiplication so that the Galois group is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. Another interesting example of p-adic Lie extensions is the false Tate tower which is the extension of $\mathbb{Q}$ by adjoining all p-power roots of unity and all the p-power roots of a given integer m. This seemingly much less natural extension is easier to understand as its Galois group is only 2-dimensional—being isomorphic to the semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$—and at certain primes q locally this tower is the extension of $\mathbb{Q}_q$ with the p-division points on the curve E. Moreover, the decomposition subgroup of the prime above q is an open subgroup of the global Galois group of the tower. This latter fact makes the behaviour of the curve E in this tower similar to its local

behaviour. In both cases the p-adic L-function 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] (also see section 1.2.2). In this thesis we will investigate the Main Conjecture mostly from its algebraic side, however, in sections 2.4 and 3.4 we will see the compatibility of the results with the analytic theory. In section 1.3 we formulate the conjectural functional equation of the p-adic L-function over any p-adic Lie extension unramified outside a finite set of primes and containing all the p-power roots of unities. In the second chapter we deal with the false Tate curve extension, and in the third we generalize some of the results to the GL_2-extension.

In section 2.1.2 we investigate the integrality properties of characteristic elements over the false Tate curve extension. In section 2.1.3 we construct canonical characteristic elements for pseudo-null $\Lambda(G)$-modules. These canonical characteristic elements are 'positive' in the sense they reduce to $1 \in \mathbb{F}_p$ modulo the Jacobson radical of the Iwasawa algebra and so they do not influence the sign in any functional equation in $K_1(\Lambda(G)_{S^*})$ involving them. This fact allows us to prove a formula for the sign in the algebraic functional equation of an arbitrary element in the K_1-group of the localized Iwasawa algebra $\Lambda(G)_{S^*}$ in terms of the $\Lambda(H)$-rank of the defined module whenever such an equation exists.

The aim of the following sections is to investigate the conjectural functional equation of the p-adic L-function from both the algebraic and analytic side over the false Tate curve extension. 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 2.4.1 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 when we substitute the contragredient representation τ^* into it. 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 section 1.1.3 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. So 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, 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. This means that we also expect a 'functional equation' on the stage of modules in $\mathfrak{M}_H(G)$ 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 2.2 we construct a pairing over the false Tate curve extension on the dual of the p-Selmer group whenever the elliptic curve has good ordinary reduction at the prime $p \geq 5$ 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 used are similar to Perrin-Riou's [29]. 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 which coincides with the conjectural functional equation of the p-adic L-function (see section 2.4 for details). This is a good evidence for both the Main Conjecture and the conjectural functional equation of the p-adic L-function.

In the next part of this thesis we compute the characteristic elements of some modules in the category $\mathfrak{M}_H(G)$ (see definition in section 1.2.2) arising naturally in Iwasawa theory for elliptic curves [17], [6] over the false Tate curve extension. In section 2.5 the Heegner-like cases are the first examples of elliptic curves whose characteristic elements in $K_1(\Lambda(G)_{S^*})$ can be determined. We call the two cases in Proposition 2.5.2 Heegner-like because the upper bound for the algebraic rank of the elliptic curve in the finite subfields of the false Tate curve extension is the same as the lower bound for the analytic rank which fact makes these cases similar to the ones when Heegner points can be constructed. In fact, Darmon and Tian [14] have some results towards constructing Heegner points in this case, as well.

As an application of the investigations of rank-1 Iwasawa-modules, in

section 2.6 we show that the example of a non-principal reflexive left ideal of the Iwasawa algebra does not rule out the possibility that all torsion $\Lambda(G)$-modules are pseudo-isomorphic to the direct sum of quotients of $\Lambda(G)$ by principal ideals.

In the remaining part of this dissertation we generalize some of the results to the GL_2-extension $\mathbb{Q}(E[p^\infty])$ associated to elliptic curves without complex multiplication. The problem is somewhat easier and has been discussed previously whenever the curve admits complex multiplication. Indeed, in this case the Main Conjecture is true provided that $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$. This fact can be deduced from the proof by Yager [41] and Rubin [32] of what is called the two variable main conjecture (recall that in this case G is a p-adic Lie group of dimension 2). In section 3.2 we construct a pairing on the dual Selmer $X(E/F_\infty)$ similar to the one in section 2.2. One interesting phenomenon is that while over the false Tate curve extension finitely generated $\mathbb{Z}_p$-modules have nontrivial characteristic elements unless they are finite, in the GL_2-case these modules represent the trivial element in the Grothendieck group $K_0(\mathfrak{M}_H(G))$. This fact—which is quite reasonable as G is much bigger in this case—will be needed when we prove the negligibility of the 'global' part of the modifying factors in the 'functional equation' of the dual Selmer. By this we obtain a functional equation of the characteristic element in section 3.3.

In section 3.4 we investigate the connections of our results to the analytic side of the picture. First, we prove that the functional equation of the characteristic element of the dual Selmer group is compatible with the Main Conjecture up to p-adic units. Then in section 3.4.2 we investigate the consequences of the 'algebraic' functional equation to the parity conjecture. We prove that if the corank of the twisted Selmer group $\mathrm{Sel}(\mathrm{tw}_\tau(E)/\mathbb{Q})$ is the same as what the analytic root number would suggest for all self-dual Artin representations τ factoring through the maximal pro-p normal subgroup of G (in other words whenever τ is a representation of $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$) 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 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.

The assumption we made for the whole thesis that the dual of the Selmer group $X(E/F_\infty)$ always lies in $\mathfrak{M}_H(G)$ is also conjectured [7] if the elliptic curve E has good ordinary reduction at the prime $p \geq 5$. In fact if the dual Selmer $X(E/K^{cyc})$ is finitely generated over $\mathbb{Z}_p$ for some number field $K \subset F_\infty$ such that the group $\mathrm{Gal}(F_\infty/K)$ is pro-p then we do know that $X(E/F_\infty)$ is in $\mathfrak{M}_H(G)$, moreover its p-torsion part is trivial [25]. This assumption is equivalent to that the μ-invariant of $X(E/K^{cyc})$ vanishes.

Throughout the thesis 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. So these extension functors of left (right) modules will be right (left) modules, respectively.

1.1 Analytic preliminaries and notations

Let $p \geq 5$ be a prime and let F_∞/k be a p-adic Lie extension (ie. it is Galois and its Galois group is a p-adic Lie group) of a number field k containing the cyclotomic $\mathbb{Z}_p$-extension k^{cyc} of k. We are going to use the following notations.

$$G := \mathrm{Gal}(F_\infty/k), \quad H := \mathrm{Gal}(F_\infty/k^{cyc}), \quad \Gamma := \mathrm{Gal}(k^{cyc}/k).$$

Now it is easy to see that $\Gamma \cong \mathbb{Z}_p$ and $G \cong H \rtimes \Gamma$. Later usually k will be $\mathbb{Q}$ and F_∞ will be either the false Tate curve extension or the GL_2-extension (see the beginning of chapters 2 and 3 for definitions) associated to elliptic curves. Moreover, we also assume for the whole of the thesis that G has no element of order p.

If v is a prime in the ground field L_2 of a Galois extension then we denote by $\mathrm{Gal}(L_1/L_2)_v$ the decomposition subgroup of v (we choose once and for all fixed embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ and $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$). $I(L_1/L_2)_v$ is the inertia subgroup and Frob_v is the arithmetic Frobenius element.

For an abelian group A we denote by $A(p)$ the p-primary part of A.

1.1.1 Systems of l-adic representations

If E/k is an elliptic curve defined over a number field k and $\tau : \mathrm{Gal}(\overline{\mathbb{Q}}/k) \to \mathrm{GL}_n(\overline{\mathbb{Q}})$ is an Artin representation then both of them determine a compatible system of l-adic representations for primes l of $\mathbb{Q}$. In 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 $M_l(E) := H^1_{et}(E, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}_l}$ 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 M of the elliptic curve twisted by the Artin representations

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

1.1.2 L-functions

To a system of l-adic representations and a number field k we associate an L-function $L(M, k, s)$ as follows. For a prime v of k the local polynomials of $L(M, k, s)$ are

$$P_v(M, T) := \det(1 - \mathrm{Frob}_v^{-1} T \mid M_l^{I_v}) \tag{1.1}$$

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

$$L_v(M, s) := P_v(M, N_{k/\mathbb{Q}}(v)^{-s})^{-1} \tag{1.2}$$

and the global L-function as an Euler-product

$$L(M, s) := \prod_v L_v(M, s). \tag{1.3}$$

We write

$$\begin{aligned} L(E/k,s) &:= L(M(E),k,s), \\ L(\tau,s) &:= L(M(\tau),k,s), \\ L(E,\tau,s) &:= L(M(E,\tau),k,s). \end{aligned} \tag{1.4}$$

The L-series $L(\tau,s)$ converges to an analytic function on the half plane $\Re s > 1$. The L-series $L(E/k,s)$ 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

$$g_{E/k} = \mathrm{rk}_{\mathbb{Z}}(E(k)), \qquad r_{E/k} = \mathrm{ord}_{s=1}(L(E/k,s)).$$

The conjecture of Birch and Swinnerton-Dyer predicts that $g_{E/k} = r_{E/k}$ always holds.

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

$$L(E,\tau_1 \oplus \tau_2) = L(E,\tau_1)L(E,\tau_2).$$

1.1.3 Functional equations of complex L-functions

For the sake of simplicity let $k = \mathbb{Q}$. The twisted L-functions $L(E,\tau,s)$ conjecturally satisfy a functional equation of the following form. Let

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

where $N(E,\tau)$ is the conductor of the curve E twisted by τ. Then, conjecturally,

$$\hat{L}(E,\tau,s) = w(E,\tau)\hat{L}(E,\tau^*,2-s), \tag{1.5}$$

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.

1.2 Algebraic preliminaries and notations

1.2.1 The dual Selmer and the Iwasawa algebra

If $L \subseteq F_\infty$ is any Galois extension of $\mathbb{Q}$ then we define $X(E/L)$ as the Pontryagin dual of the Selmer group,

$$X(E/L) = \mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/L), \mathbb{Q}_p/\mathbb{Z}_p). \tag{1.6}$$

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 $\Lambda(G)$, where for any profinite group $\mathcal{G}$ the Iwasawa algebra of $\mathcal{G}$ with coefficients in $\mathbb{Z}_p$ is

$$\Lambda(\mathcal{G}) = \varprojlim_{N \lhd_o \mathcal{G}} \mathbb{Z}_p[\mathcal{G}/N]. \tag{1.7}$$

We denote the Iwasawa algebra with coefficients in $\mathbb{F}_p$—an epimorphic image of the previous one—by

$$\Omega(\mathcal{G}) = \varprojlim_{N \lhd_o \mathcal{G}} \mathbb{F}_p[\mathcal{G}/N]. \tag{1.8}$$

1.2.2 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

$$S^* = \bigcup_{n \geq 0} p^n S.$$

These are multiplicatively closed (left and right) Ore sets of $\Lambda(G)$ [7], so we can define $\Lambda(G)_S$, $\Lambda(G)_{S^*}$ as the localizations of $\Lambda(G)$ at S and S^*. We write $\mathfrak{M}_H(G)$ for the category of all finitely generated $\Lambda(G)$-modules, which 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 $\Lambda(H)$ [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 $K_1(\Lambda(G)_{S^*})$ [7]. It is a pre-image of the class of M under the connecting homomorphism

$$\partial_G \ : \ K_1(\Lambda(G)_{S^*}) \to K_0(\mathfrak{M}_H(G)) \tag{1.9}$$

in the long exact sequence of localization in K-theory

$$\begin{aligned} \cdots \to K_1(\Lambda(G)) \to K_1(\Lambda(G)_{S^*}) &\stackrel{\partial_G}{\to} K_0(\mathfrak{M}_H(G)) \\ &\to K_0(\Lambda(G)) \to K_0(\Lambda(G)_{S^*}) \to 0, \end{aligned} \tag{1.10}$$

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 [7]. Further, if we denote by $\mathfrak{N}_H(G)$ the category of $\Lambda(G)$-modules which are finitely generated over $\Lambda(H)$, then we get a similar exact sequence

$$\begin{aligned} \cdots \to K_1(\Lambda(G)) \to K_1(\Lambda(G)_S) &\stackrel{\partial_G}{\to} K_0(\mathfrak{N}_H(G)) \\ &\to K_0(\Lambda(G)) \to K_0(\Lambda(G)_S) \to 0. \end{aligned} \tag{1.11}$$

As defined in [6] there is a C_2-action, ie. 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 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 $\#$, i. e. 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 $mx = x^{\#}m$.

1.2.3 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 $k \geq 0$ and any submodule N of $\mathrm{Ext}^k_{\Lambda(\mathcal{G})}(M, \Lambda(\mathcal{G}))$ we have $j(N) \geq k$ (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 [37, 38], so every finitely generated left or right $\Lambda(\mathcal{G})$-module satisfies the Auslander condition.

Let

$$0 \to \Lambda(\mathcal{G}) \stackrel{\mu_0}{\to} E_0 \stackrel{\mu_1}{\to} E_1 \stackrel{\mu_2}{\to} \ldots \stackrel{\mu_i}{\to} E_i \stackrel{\mu_{i+1}}{\to}$$

the minimal injective resolution of $\Lambda(\mathcal{G})$, where E_{i+1} is the injective hull ([35], Definition 1.5.1) of the cokernel of μ_i for any $i \geq 0$. Moreover, we define the full subcategory

$$\mathcal{C}^n_{\Lambda(\mathcal{G})} = \mathcal{C}^n := \{M \mid \mathrm{Hom}_{\Lambda(\mathcal{G})}(M, E_0 \oplus \cdots \oplus E_n) = 0\}. \tag{1.12}$$

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 $E_0 \oplus \cdots \oplus E_n$ (see [35], 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

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

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

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

(*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 1.2.1 (Lemma 2.4 in [10])**.** *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 thesis we are going to use the notation

$$a^i_{\Lambda(\mathcal{G})}(M) := \mathrm{Ext}^i_{\Lambda(\mathcal{G})}(M, \Lambda(\mathcal{G})). \tag{1.13}$$

1.2.4 Galois representations and twists

As in [7], let $\mathcal{O}$ 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

$$\rho \,:\, G \to \mathrm{GL}_n(\mathcal{O}) \tag{1.14}$$

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

$$\mathrm{tw}_\rho(M) = M_{\mathcal{O}} \otimes_{\mathcal{O}} \mathcal{O}^n.$$

We endow $\mathrm{tw}_\rho(M)$ with the diagonal action of G, ie. if g is in G, $g(m \otimes z) = (gm) \otimes (gz)$, where it is understood that G acts on $\mathcal{O}^n$ 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] ρ induces a homomorphism

$$\Phi'_\rho \,:\, K_1(\Lambda(G)_{S^*}) \to K_1(M_n(Q_{\mathcal{O}}(\Gamma))) = Q_{\mathcal{O}}(\Gamma)^\times, \tag{1.15}$$

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

$$\varphi \,:\, \Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}} \to L,$$

and for $\xi \in K_1(\Lambda(G)_{S^*})$ we define $\xi(\rho) = \varphi(\Phi'_\rho(\xi))$ if $\Phi'_\rho(\xi)$ belongs to $\Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}}$, and $\xi(\rho) = \infty$ otherwise.

1.3 Conjectural functional equation of the p-adic L-function

In this section we formulate the conjectural functional equation of the p-adic L-function attached to elliptic curves E over p-adic Lie extensions F_∞ of the rationals unramified outside a finite set of primes and containing all the p-power roots of unity. For the sake of brevity we will also assume that E is defined over $\mathbb{Q}$. However, the conjecture could be generalized to any number field and possibly to any motive other than elliptic curves.

Let us denote by Z the (finite) set of primes in $\mathbb{Q}$ that *ramify infinitely* in the p-adic Lie extension F_∞ and are not equal to the fixed prime $p \geq 5$. Let us denote by G the Galois group $\mathrm{Gal}(F_\infty/\mathbb{Q})$ and by G_0 the maximal normal pro-p subgroup of G, that is the intersection of all the pro-p Sylow subgroups of G. As in section 1.2.2 we also define H as the Galois group $\mathrm{Gal}(F_\infty/\mathbb{Q}^{cyc})$ and the canonical Ore-sets S and S^* with respect to the subalgebra $\Lambda(H)$ of $\Lambda(G)$. Further, let K be the fixed field of G_0—this is a finite extension of $\mathbb{Q}$. Let us define the following subsets of Z.

$$\begin{aligned} R_1 &:= \{q \in Z \mid E \text{ has split multiplicative reduction at } u_q\} \qquad (1.16)\\ R_2 &:= \{q \in Z \mid E \text{ has good reduction at } u_q \text{ and } E[p^\infty](K_{u_q}^{cyc}) \neq 0\}, \end{aligned}$$

where u_q is any prime in $K^{cyc} = K(\mu_{p^\infty})$ above q. Put

$$R_0 := R_1 \cup R_2, \qquad \text{and} \qquad R = R_0 \cup \{p\}. \qquad (1.17)$$

Proposition 1.3.1. *The set of primes R_0 defined above is exactly the set of primes $q \neq p$ satisfying the following two conditions:*

(*i*) *q ramifies infinitely in $F_\infty/\mathbb{Q}$;*

(*ii*) *$\mathbb{Q}_q(E[p^\infty])$ is contained in the completion F_{∞,v_q} at any prime v_q of F_∞ above q.*

Moreover, for any prime q in $Z \setminus R_0$ the group of p-division points on E is finite over the completion of F_∞ at any prime above q.

Proof. For potentially multiplicative primes q the statement follows from the theory of the Tate curve noting that $F_{v_q}/K_{u_q}^{cyc}$ is the unique infinite pro-p-extension of $K_{u_q}^{cyc}$ as it is infinite since q is in Z and pro-p by the construction of K.

For potentially good primes q note that if the reduction type of E over $K_{u_q}^{cyc}$ is additive then the group of p-division points must be finite over this field. Now if the reduction type of E at u_q is good and $E[p^\infty](K_{u_q}^{cyc}) = 0$ then by the Nakayama lemma it also follows that $E[p^\infty](F_{\infty,v_q}) = 0$ as $\mathrm{Gal}(F_{\infty,v_q}/K_{u_q}^{cyc})$ is pro-p. On the other hand if $E[p^\infty](K_{u_q}^{cyc}) \neq 0$ then $\mathbb{Q}_q(E[p^\infty])$ is contained in $K_{u_q}^{cyc}$ as the latter field contains all the p-power roots of unities. □

This above Proposition motivates how one should formulate the Main Conjecture of Iwasawa theory for elliptic curves over this p-adic Lie extension.

Fix a global minimal Weierstraß equation for E over $\mathbb{Z}$. We denote by $\Omega_\pm(E)$ the periods of E, defined by integrating the Néron differential of

this Weierstraß 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 $d^+(\tau)$ (resp. $d^-(\tau)$) denote the dimension of the subspace of the vector space of ρ on which complex conjugation acts by $+1$ (resp. -1). Deligne's period conjecture [15]—which has already been proved [4] in the case when τ factors through the false Tate curve extension—asserts that

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

We define the modified L-function

$$L_R(E,\tau,s) := \prod_{q\notin R} P_q(E,\tau,q^{-s})^{-1} \tag{1.18}$$

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

$$P_p(E,T) = 1 - a_pT + pT^2 = (1-b_pT)(1-c_pT), \quad b_p \in \mathbb{Z}_p^\times, \tag{1.19}$$

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

Conjecture 1.3.2. *Assume that $p \geq 5$ 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*

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

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.

This above conjecture is parallel to the one in the GL_2-case (Conjecture 5.7 in [7]), however, there R consists of those primes q in $\mathbb{Q}$ besides p for which $\mathrm{ord}_q(j_E) < 0$, where j_E is the j-invariant of the elliptic curve. Proposition

1.3.1 shows that the set defined in (1.17) is the right generalization of this set to arbitrary p-adic Lie extensions.

Now we can state the main conjecture of Iwasawa theory for elliptic curves over p-adic Lie extensions which is a generalization of Conjecture 5.8 in [7].

Conjecture 1.3.3 (The main conjecture)**.** *Assume that $p \geq 5$, E has good ordinary reduction at p, and $X(E/F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$. Granted Conjecture* 1.3.2*, the p-adic L-function $\mathfrak{L}_E$ in $K_1(\Lambda(G)_{S^*})$ is a characteristic element of $X(E/F_\infty)$.*

Now we can state the conjectural functional equation of the p-adic L-function.

Conjecture 1.3.4. *Let E be an elliptic curve with good ordinary reduction at $p \geq 5$. Then the p-adic L-function $\mathfrak{L}_E$ in $K_1(\Lambda(G)_{S^*})$ satisfies the functional equation*

$$\mathfrak{L}_E^{\#} = \mathfrak{L}_E \varepsilon_0 \prod_{q \in R_0} \gamma_q,$$

where ε_0 lies in $K_1(\Lambda(G))$ and the local factors γ_q are in the image of the natural map from $K_1(\Lambda(G_q)_{S_q})$ to $K_1(\Lambda(G)_{S^*})$. Moreover, the modifying factors satisfy the following interpolation properties for any Artin representation τ of G.

$$\varepsilon_0(\tau) = \prod_{q \notin R} \varepsilon_q(\tau, E) \text{ and}$$
$$\gamma_q(\tau) = \varepsilon_q(\tau, E) \frac{P_q(E, \tau, q^{-1})}{P_q(E, \tau^*, q^{-1})}$$

where $\varepsilon_q(\tau, E)$ denotes the local epsilon factor attached to the twist of curve E by the Artin representation τ at the prime q.

Chapter 2

The false Tate curve extension

In this chapter we deal with the false Tate curve extension associated to elliptic curves. Let $p \geq 5$ be a prime and m be a p-power free integer, ie. not divisible by the pth power of any integer. Let E denote an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p and such that E does not have additive reduction at any prime q dividing m. Furthermore, let us denote by

(*i*) $K = \mathbb{Q}(\mu_p)$,

(*ii*) $K_n = \mathbb{Q}(\mu_{p^n})$,

(*iii*) $F_n = \mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{m})$

the finite layers of the false Tate curve extension $F_\infty = \bigcup_{n=1}^{\infty} F_n$. We denote the Galois group of the following extensions by

(*i*) $G = \mathrm{Gal}(F_\infty/K) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$,

(*ii*) $G_0 = \mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$,

(*iii*) $\Gamma = \mathrm{Gal}(K^{cyc}/K) \cong \mathbb{Z}_p$,

(*iv*) $\Gamma_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) \cong \mathbb{Z}_p$,

(*v*) $\Gamma_0 = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$,

(*vi*) $H = \mathrm{Gal}(F_\infty/K^{cyc}) \cong \mathbb{Z}_p$,

(*vii*) $H_0 = \mathrm{Gal}(F_\infty/\mathbb{Q}^{cyc}) \cong \mathbb{Z}_p \rtimes \mathbb{F}_p^\times$,

(*viii*) $G_n = \mathrm{Gal}(F_\infty/F_n)$,

(*ix*) $\Gamma_n = \mathrm{Gal}(F_n^{cyc}/F_n)$,

(*x*) $H_n = \mathrm{Gal}(F_\infty/F_n^{cyc})$.

Now the Iwasawa algebra $\Lambda(G)$ has a nice well-described structure. For a fixed topological generator γ of Γ we choose a lift $\tilde{\gamma} \in G$, put $Y = \tilde{\gamma} - 1$, $X = h - 1$ if h is a fixed topological generator of H and identify $\Lambda(G)$ with the skew power series ring [39]

$$\Lambda(G) \cong \mathbb{Z}_p[\![X]\!][\![Y; \sigma, \delta]\!], \tag{2.1}$$

where σ is the ring automorphism induced by

$$X \mapsto (X+1)^{\chi(\gamma)} - 1, \tag{2.2}$$

$\delta = \sigma - 1$ a σ-derivation, and χ is the cyclotomic character. We also identify $\Lambda(\Gamma)$ with $\mathbb{Z}_p[\![T]\!]$ where the natural surjection from $\Lambda(G)$ to $\Lambda(\Gamma)$ sends Y to T.

Moreover, there is a nice description of elements in the canonical Ore-set S (see section 1.2.2 for the definition) in this case. An element of $\Lambda(G)$ is in S in this case if and only if it is a distinguished skew polynomial in the variable Y up to a unit. We call a (skew) polynomial *distinguished* if its leading coefficient is a unit and all the other coefficients are in the maximal ideal of the coefficient ring.

2.1 Iwasawa-modules

2.1.1 Further localizations

We are going to define another action on the characteristic elements of Iwasawa modules in $\mathfrak{N}_H(G)$, the category of left $\Lambda(G)$-modules that are finitely generated over $\Lambda(H)$. Let R be the set of formal power series in

$\mathbb{Z}_p[\![X]\!] = \Lambda(H)$ which are invariant under the action of γ up to multiplication by units, ie.

$$R = \{r(X) \in \mathbb{Z}_p[\![X]\!] \mid r(X)^{1-\gamma} \in \mathbb{Z}_p[\![X]\!]^\times\}. \tag{2.3}$$

Lemma 2.1.1. *R is a canonical (left and right) Ore set in $\Lambda(G)_S$ as well as in $\Lambda(H)$.*

Proof. The statement is trivial for the ring $\Lambda(H)$. So it suffices to prove that for elements $r(X) \in R$, and $s \in \Lambda(G)_S$ we have that sr is divisible by r from the left, as well. Indeed, since this assumption is true for $s = \gamma$ by the definition of R, it is also true for any element s in $\Lambda(G)$ by linearity and continuicity of sr in the variable s. Now if we have $s^{-1}r$ with s in S then similarly we can choose an x in $\Lambda(G)$ such that $rx = sr$. Moreover, x will in fact be in S. This follows from the description of elements in S, namely that a skew power series in $\Lambda(G)$ lies in S if and only if it is a distinguished skew polynomial in the variable Y up to an invertible element. So we may assume that s is a distinguished polynomial. Now the leading coefficient of x is a unit times the leading coefficient of s and all the other coefficients differ by elements of the maximal ideal of $\Lambda(H)$ because of the formula

$$r^{-1}Yr = r^{\gamma-1}Y + r^{\gamma-1} - 1.$$

Therefore x is in S and $s^{-1}r = rx^{-1}$ makes sense in the localized ring $\Lambda(G)_S$, so the Lemma follows. □

Because of the above lemma we can localize by R and get rings $\Lambda(G)_{S,R}$, and $\Lambda(H)_R$. Now there is a canonical inclusion of the multiplicative groups

$$\begin{aligned} (\Lambda(G)_S)^\times &\hookrightarrow (\Lambda(G)_{S,R})^\times, \text{ and} \\ (\Lambda(H)_R)^\times &\hookrightarrow (\Lambda(G)_{S,R})^\times. \end{aligned}$$

The elements in the image of $(\Lambda(H)_R)^\times$ are contained in the normalizer of the subgroup $(\Lambda(G)_S)^\times$ by the definition of R. Moreover, $K_1(\Lambda(G)_S)$ is the abelianization of the latter subgroup [36], so there is an action of $(\Lambda(H)_R)^\times$

on the K_1-group, since the commutator is a characteristic subgroup. We will see in section 2.1.3 that the conjugation of the characteristic element by an element in $(\Lambda(H)_R)^\times$ corresponds to a pseudo-isomorphism of modules as the quotient of the characteristic elements is a commutator and by Proposition 2.1.8 these commutators correspond to pseudo-null modules. Since [27]

$$K_0(\mathfrak{M}_H(G)) = K_0(\mathfrak{N}_H(G)) \oplus \mathbb{Z},$$

we can extend this action on the characteristic elements to $K_1(\Lambda(G)_{S^*})$ by acting trivially on the p-part of the characteristic elements so that the action still corresponds to pseudo-isomorphism of modules.

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

2.1.2 Integrality properties of characteristic elements

We will see in section 2.5 that the characteristic element of $X(E/F_\infty)$ is integral in the sense that it is in the image of the natural morphism

$$\Lambda(G) \cap (\Lambda(G)_{S^*})^\times \to K_1(\Lambda(G)_{S^*}) \tag{2.4}$$

in those Heegner-like cases and in fact this is true for all $\Lambda(H)$-torsion free modules of rank 1 (compare to Conjecture 4.8. in [7]). Since the map

$$(\Lambda(G)_S)^\times / [(\Lambda(G)_S)^\times, (\Lambda(G)_S)^\times] \to K_1(\Lambda(G)_S)$$

is an isomorphism [36], and the characteristic element can be induced from $K_1(\Lambda(G)_S)$ when the module has no p-torsion, one would expect that (2.4) was true in general. A slightly weaker statement can be proved in general for modules $X(E/F_\infty)$ with $\Lambda(H)$-rank greater than 1, if the μ-invariant of $X(E/K^{cyc})$ vanishes.

Lemma 2.1.2. *If M is a left $\Lambda(G)$-module and a finite index submodule of $\Lambda(H)^d$ as a $\Lambda(H)$-module then the action of G can be extended from M to $\Lambda(H)^d$. In other words M is a finite index $\Lambda(G)$-submodule of a module*

which is isomorphic to $\Lambda(H)^d$ *as a* $\Lambda(H)$*-module.*

Proof. Let $\tilde{\gamma}$ be a lift of the topological generator $\gamma \in \Gamma$. Note that it is sufficient to extend the action of $\tilde{\gamma}$. Let us identify $\Lambda(H)$ with $\mathbb{Z}_p[\![X]\!]$ and let $\{e_j\}_{j=1}^d$ be a $\Lambda(H)$-base of $\Lambda(H)^d$. As M is a finite index submodule, for all $1 \leq j \leq d$ there exist l_j's for which $p^{l_j}e_j$ is in $M \leq \Lambda(H)^d$. So we can define a matrix $A = (a_{ij})_{i,j=1}^d$ with entries in $p^{-\max(l_1,l_2,\ldots,l_d)}\mathbb{Z}_p[\![X]\!]$ by the equations

$$p^{-l_j}\tilde{\gamma}(p^{l_j}e_j) = \sum_{i=1}^{d} a_{ij}e_i.$$

This matrix A determines the action of $\tilde{\gamma}$ on M, namely if

$$\begin{pmatrix} f_1(X) \\ f_2(X) \\ \vdots \\ f_d(X) \end{pmatrix} \in M \leq \mathbb{Z}_p[\![X]\!]^d \text{ then}$$

$$\tilde{\gamma}\begin{pmatrix} f_1(X) \\ f_2(X) \\ \vdots \\ f_d(X) \end{pmatrix} = A\begin{pmatrix} \tilde{\gamma}f_1(X)\tilde{\gamma}^{-1} \\ \tilde{\gamma}f_2(X)\tilde{\gamma}^{-1} \\ \vdots \\ \tilde{\gamma}f_d(X)\tilde{\gamma}^{-1} \end{pmatrix}. \tag{2.5}$$

Since M is a finite index submodule of $\mathbb{Z}_p[\![X]\!]^d$, there are distinct positive integers $k_1 > k_2$ such that $X^{k_1} - X^{k_2}$ is in M. Taking $f_j(X) = X^{k_1} - X^{k_2}$, $f_{j'}(X) \equiv 0$ if $j' \neq j$ for varying $1 \leq j \leq d$ and noting that $\mathbb{Z}_p[\![X]\!]$ is a unique factorization domain, we conclude that the entries of the matrix A are in $\mathbb{Z}_p[\![X]\!]$ because $\tilde{\gamma}(X^{k_1} - X^{k_2})\tilde{\gamma}^{-1}$ has a unit leading coefficient, so it is not divisible by any positive integer power of p. Now the action of $\tilde{\gamma}$ can be extended to the whole $\Lambda(H)$-module $\Lambda(H)^d$ by the formula (2.5) and we are done. □

Remarks. 1. In fact the matrix A cannot be arbitrary. The action of $\tilde{\gamma}$ is continuous provided that $A^{p^n} \to I$ as $n \to \infty$ or equivalently A has p-power order modulo the maximal ideal of $\Lambda(H)$.

2. The matrix A is determined by a $\Lambda(G)$-module which is free as a $\Lambda(H)$-module up to conjugacy in the sense that A is equivalent to $BA\gamma B^{-1}\gamma^{-1}$ for any B matrix in $\mathrm{GL}_d(\Lambda(H))$. This gives a one-to-one correspondence between the equivalency class of matrices and the isomorphism class of these modules. An easy consequence of Lemma 2.1.2 that for modules of $\Lambda(H)$-rank 1 the characteristic elements are also in one-to-one correspondence with the isomorphism classes of modules if we know a priori that the module is free over $\Lambda(H)$. This is not true for modules of higher rank. For example

$$(Y+1)I - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } (Y+1)I - \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$$

represent the same element in $K_1(\Lambda(G)_{S^*})$ (their Whitehead determinant is the same), but the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$$

define non-isomorphic $\Lambda(G)$-modules.

Proposition 2.1.3. *If M is in the category $\mathfrak{N}_H(G)$ with no nontrivial pseudo-null submodule then there exist a positive integer d and a matrix A in the ring $\mathbb{Z}_p[\![X]\!]^{d\times d}$ such that M is a finite index submodule of the $\Lambda(G)$-module*

$$\Lambda(G)^d/\Lambda(G)^d((Y+1)I - A),$$

where I is the identity matrix and the $\Lambda(G)$-submodule $\Lambda(G)^d((Y+1)I-A)$ is defined by

$$\Lambda(G)^d((Y+1)I-A) := \{(x^t((Y+1)I-A)^t)^t \mid x \in \Lambda(G)^d \text{ a column vector}\}.$$

In particular the characteristic element of M is the image of $(Y+1)I - A$ under the natural map

$$M_d(\Lambda(G)) \cap \mathrm{GL}_d(\Lambda(G)_{S^*}) \hookrightarrow \mathrm{GL}_d(\Lambda(G)_{S^*}) \to K_1(\Lambda(G)_{S^*}).$$

Proof. From Lemma 2.1.2 we get that the action of G can be extended to $\Lambda(H)^d$ with a matrix A in $\Lambda(H)^{d\times d}$ for which

$$\tilde{\gamma}\begin{pmatrix} f_1(X) \\ f_2(X) \\ \vdots \\ f_d(X) \end{pmatrix} = A\begin{pmatrix} \tilde{\gamma}f_1(X)\tilde{\gamma}^{-1} \\ \tilde{\gamma}f_2(X)\tilde{\gamma}^{-1} \\ \vdots \\ \tilde{\gamma}f_d(X)\tilde{\gamma}^{-1} \end{pmatrix}.$$

Now the natural embedding $\Lambda(H)^d \hookrightarrow \Lambda(G)^d$ induces a $\Lambda(G)$-isomorphism between $\Lambda(H)^d$ endowed with the above action of $\tilde{\gamma}$ and the factor module $\Lambda(G)^d/\Lambda(G)^d((Y+1)I - A)$. □

The following slightly more general theory of $\Lambda(G)$-modules gives another application of Lemma 2.1.2.

Lemma 2.1.4. *There exists a $\Lambda(H)$-projective resolution of $\Lambda(G)$-modules which are finitely generated as $\Lambda(H)$-modules such that the resolution can be endowed with a compatible $\Lambda(G)$-action, so the modules are $\Lambda(G)$-modules and the morphisms are $\Lambda(G)$-morphisms.*

Proof. It is enough to prove that if M is a $\Lambda(G)$-module with minimal generating system $a_1, a_2, \ldots, a_d \in M$ over $\Lambda(H)$ and

$$\varphi: \ \Lambda(H)^d \to M$$

is the corresponding surjection then $\Lambda(H)^d$ can be endowed with a $\Lambda(G)$-action such that φ becomes a $\Lambda(G)$-homomorphism. We can pull back the action of $\tilde{\gamma}$ from M to the base of $\Lambda(H)^d$ by choosing any lift and since the kernel of φ is contained in the d-th direct power of the maximal ideal of $\Lambda(H)$ (it was a minimal resolution), the action can be extended continuously to the whole $\Lambda(H)^d$. Indeed, any lift works because the action of Y^n converges to 0 if and only if for some n the image of Y^n is contained in the maximal ideal of $\Lambda(H)$. This means that we need the matrix of Y to be nilpotent when reducing it modulo (p, X). On the other hand the action of Y is continuous on the factor module M and so it is continuous if we factor out with $(p, X)M$,

so it represents a nilpotent matrix on the $\mathbb{F}_p$ vector space $M/(p,X)M$ and we are done because $M/(p,X)M \cong \Lambda(H)^d/(p,X)\Lambda(H)^d$ as the kernel of φ is contained in $(p,X)\Lambda(H)^d$. □

Proposition 2.1.5. *If M is in the category $\mathfrak{M}_H(G)$ and has no p-torsion then the following are equivalent.*

(*i*) *M has no nonzero pseudo-null submodule.*

(*ii*) *M is $\Lambda(H)$-torsion free.*

(*iii*) *M is a finite index submodule of another $\Lambda(G)$-module which is free as a $\Lambda(H)$-module.*

(*iv*) *The homology groups $H_i(H', M)$ are trivial for all $H' \leq H$ open subgroups, and $i \geq 1$.*

Proof. The first three statements are certainly equivalent by applying Lemma 2.1.2 and the general theory for $\Lambda(H)$-modules. To prove the direction $(iii) \Rightarrow (iv)$ it is easy to see that the third assertion holds for any free $\Lambda(H)$-module. Moreover, it is hereditary with respect to submodules because of the long exact sequence of homology.

The only direction for which we need the $\Lambda(G)$-structure of the module M is $(iv) \Rightarrow (ii)$. Let us assume indirectly that $H_i(H', M) = 0$ for all $H' \leq H$ open subgroups, and $i \geq 1$ and M does have a nontrivial $\Lambda(H)$-torsion submodule. We may suppose without loss of generality that M itself is $\Lambda(H)$-torsion because the assumption remains true for any submodule of M. Now it is easy to see that each minimal projective resolution of M as a $\Lambda(H)$-module has length 1 and the maps in it are $\Lambda(G)$-homomorphisms by Lemma 2.1.4. So it is in the form

$$0 \longrightarrow \Lambda(H)^d \xrightarrow{A} \Lambda(H)^d \longrightarrow M \longrightarrow 0,$$

where $A \in \Lambda(H)^{d\times d} \cong \mathbb{Z}_p[\![X]\!]^{d\times d}$ is a matrix. Since $H_1(H^{p^n}, M) = 0$ for all $n \geq 0$ we get that A has nonzero determinant modulo the ideal generated by $(X+1)^{p^n} - 1$. On the other hand since M is nontrivial, this determinant is

not a unit in $\mathbb{Z}_p[\![X]\!]$, so it must have a root (in some finite extension of $\mathbb{Q}_p$) which is not in the form $\zeta - 1$ where ζ is any root of unity of p-power order. This means, however, that the ideal in $\mathbb{Z}_p[\![X]\!]$ generated by the determinant is not invariant under the action of $\tilde{\gamma}$ by conjugation because the roots are mapped by $\tilde{\gamma}$ as

$$z \mapsto (z+1)^{\chi(\tilde{\gamma}^{-1})} - 1$$

because $f(z) = 0$ if and only if

$$f\left(\left(\left((z+1)^{\chi(\tilde{\gamma}^{-1})} - 1\right) + 1\right)^{\chi(\tilde{\gamma})} - 1\right) = 0.$$

This contradicts to the fact that the map A is a $\Lambda(G)$-homomorphism between some $\Lambda(G)$-modules, since $\tilde{\gamma}$ maps a generating system over $\Lambda(H)$ to another one and the determinant is independent of the choice of this system. □

Corollary 2.1.6. *Assume that a $\Lambda(G)$-module M is finitely generated over $\Lambda(H)$ and $H_i(H', M)$ vanishes for all $H' \leq H$ open subgroups, and $i \geq 1$. Then its characteristic element is in the form $\xi = (Y+1)I - A$ for some $A \in \Lambda(H)^{d \times d}$, where d is the rank of M. Moreover, for all continuous representations of the form (1.14), $\xi(\rho)$ is finite and in $\mathcal{O}$, and $\Phi'_\rho(\xi)$ is in $\Lambda_{\mathcal{O}}(\Gamma)$.*

2.1.3 The sign in the functional equation

In section 2.2 we will see that the characteristic element of the dual Selmer $X(E/F_\infty)$ satisfies an algebraic functional equation in the group $K_1(\Lambda(G)_{S^*})$. In this section we prove that whenever such a functional equation exists for an element of the K_1-group of the localized Iwasawa algebra then the sign is determined by the $\Lambda(H)$-rank of the module associated to the element in $K_1(\Lambda(G)_{S^*})$.

Lemma 2.1.7. *An element $r(X) \in \mathbb{Z}_p[\![X]\!]$ is in the Ore-set R if and only if its zeros are in the form $\zeta - 1$ where ζ is any root of unity of p-power order.*

Proof. By definition $r(X)$ is in R if and only if its zeros are permuted by $\tilde{\gamma}$, which means that z is a root of r exactly when so is $(z+1)^{\chi(\tilde{\gamma}^{-1})}-1$. Now the orbit of an element in the ring of integers of $\overline{\mathbb{Q}_p}$ is finite under this action if and only if the element is a root of unity minus 1. Moreover, the value of a formal power series is only defined at elements of the maximal ideal of the ring of integers, so the root of unity must be of p-power order. □

Proposition 2.1.8. *M is a pseudo-null $\Lambda(G)$-module in the category $\mathfrak{M}_H(G)$ if and only if its characteristic element is a product of commutators of the form $[f,r]=frf^{-1}r^{-1}$ considered as elements of $K_1(\Lambda(G)_{S^*})$, where r is in R and f is an invertible element of $\Lambda(G)_S$.*

Proof. Since pseudo-null p-torsion modules have trivial characteristic elements [1], we may assume without loss of generality that M has trivial p-torsion. So M is a finitely generated torsion $\Lambda(H)$-module with $\Lambda(H)$-characteristic power series $r_0(X)$ in R, since it acquires an action of $\tilde{\gamma}$. By Lemma 2.1.7, $r_0(X)$ is in the form

$$r_0(X)=\prod_{i=0}^{n}\Phi_{p^i}(X)^{l_i}$$

where Φ_{p^i} is the p^ith cyclotomic polynomial. Since these cyclotomic polynomials are in the Ore-set R, the $\Lambda(H)$-submodule of M annihilated by one particular irreducible factor of r_0 is a $\Lambda(G)$ submodule of M. Therefore—by induction—it is enough to prove the statement when the generator $r_1 \mid r_0$ of the annihilator ideal is irreducible. So let $r_1(X):=\Phi_{p^i}(X)$ for some $i\geq 0$. Now M is isomorphic to

$$\bigoplus_{j=1}^{n}\left(\mathbb{Z}_p[\![X]\!]/\Phi_{p^i}(X)\right)_j$$

as a $\Lambda(H)$-module for some n, since $\mathbb{Z}_p[\![X]\!]/\Phi_{p^i}(X)$ is a principal ideal domain. This means that as a $\Lambda(G)$-module it is isomorphic to $N/\Phi_{p^i}(X)N$ for some $\Lambda(G)$-module N which is finitely generated and free over $\Lambda(H)$ (see Lemma 2.1.4). This gives the required expression for the characteristic ele-

ment of M as the characteristic element of $\Phi_{p^i}(X)N$ is the conjugate of the characteristic element of N by $\Phi_{p^i}(X)$. □

Corollary 2.1.9. *If M is in $\mathfrak{M}_H(G)$ then its characteristic element can be written in the form $p^{\mu_G(M)}\xi_1\xi_2^{-1}$, where ξ_1 and ξ_2 are skew-polynomials over $\mathbb{Z}_p[\![X]\!]$ of degree $\deg(\xi_1)$ and $\deg(\xi_2)$ satisfying*

$$\deg(\xi_1) - \deg(\xi_2) = \operatorname{rank}_{\Lambda(H)}(M/M(p))$$

in the variable Y.

Proof. The characteristic element of the p-torsion part equals $p^{\mu_G(M)}$ by definition [1]. For pseudo-null modules the statement follows from Proposition 2.1.8. So we may assume that M has trivial p-torsion and no nontrivial pseudo-null submodule. The statement follows from 2.1.3 by taking the Whitehead determinant of the characteristic element. □

For the sake of simplicity for any ring R and (left or right) R-module M put

$$a_R^i(M) := \operatorname{Ext}_R^i(M, R) \quad (i \geq 0). \tag{2.6}$$

Proposition 2.1.10. *Let M be in the category $\mathfrak{M}_H(G)$. Then we have the following relation connecting the characteristic element ξ_M of M and the characteristic elements $\xi_{a^i_{\Lambda(G)}(M)}$ of $a^i_{\Lambda(G)}(M)$ for $1 \leq i \leq 3$.*

$$\xi_M = \prod_{i=1}^{3} \xi_{a^i_{\Lambda(G)}(M)}^{(-1)^{i+1}}. \tag{2.7}$$

Proof. Because of the long exact sequence of $\operatorname{Ext}_{\Lambda(G)}(\cdot, \Lambda(G))$ it is enough to prove the statement separately for p-torsion modules and modules finitely generated over $\Lambda(H)$.

For p-torsion modules it suffices to show the statement for projective $\Omega(G)$-modules. For these modules we only have first extension groups. Furthermore, if M is a projective $\Omega(G)$-module then $a^1_{\Lambda(G)}(M) \cong \operatorname{Hom}(M, \Omega(G))$ and so have the same characteristic element as M using the formula for the

characteristic element of p-torsion modules [1] (the characteristic element is p^d in this case where d is the rank of this projective $\Omega(G)$-module).

For modules finitely generated over $\Lambda(H)$ it suffices to prove the statement for $\Lambda(H)$-projective modules by Lemma 2.1.4. The $\Lambda(G)$-modules which are projective as $\Lambda(H)$-modules are by Proposition 2.1.3 in the form

$$\Lambda(G)^d/\Lambda(G)^d((Y+1)I-A),$$

where d is the $\Lambda(H)$-rank of the module, I is the identity matrix, and A is a matrix in $\Lambda(H)^{d\times d}$. Moreover,

$$a^1_{\Lambda(G)}\left(\Lambda(G)^d/\Lambda(G)^d((Y+1)I-A)\right) \cong \Lambda(G)^d/((Y+1)I-A)\Lambda(G)^d$$

and the higher extension groups vanish as this module has a projective $\Lambda(G)$-resolution of length 1. The result follows. □

Theorem 2.1.11. *Let us assume that M is in the category $\mathfrak{M}_H(G)$ and M is pseudo-isomorphic to $a^1_{\Lambda(G)}(M^\#)$. Then its characteristic element ξ_M in $K_1(\Lambda(G)_{S^*})$ satisfies a functional equation of the form*

$$\xi_M^\# = \varepsilon(M)\xi_M \prod_{i=1}^{n}[f_i, r_i]^{k_i}, \tag{2.8}$$

where $\varepsilon(M)$ is an element coming from $\Lambda(G)^\times$, f_i is in $K_1(\Lambda(G)_S)$, r_i is in the Ore-set R, and the k_i's are (possibly negative) integers. Moreover if we reduce $\varepsilon(M)$ modulo the Jacobson radical of $\Lambda(G)$ we get an element $\overline{\varepsilon(M)}$ in $\mathbb{F}_p$ ("the sign of the functional equation") which is -1 if the $\Lambda(H)$-rank of M is odd, and $+1$ if the rank is even.

Proof. It is enough to prove the statement for modules in $K_0(\mathfrak{N}_H(G))$ since p-torsion modules' characteristic elements are powers of p and they are fixed by the action of $\#$.

The existence of the functional equation follows from the fact that two elements of $K_1(\Lambda(G)_S)$ map to the same element in $K_0(\mathfrak{N}_H(G))$ if and only if they differ by an element in the image of $K_1(\Lambda(G))$. Moreover, $a^1_{\Lambda(G)}(M^\#)$

is pseudo-isomorphic to M, and by Proposition 2.1.10 we have

$$\xi_M^{\#} = \xi_{M^{\#}} = \prod_{i=1}^{3} \xi_{a^i_{\Lambda(G)}(M^{\#})}^{(-1)^{i+1}}.$$

Now $a^2_{\Lambda(G)}(M^{\#})$ and $a^3_{\Lambda(G)}(M^{\#})$ are pseudo-null and pseudo-null modules' characteristic elements are products of commutators by Proposition 2.1.8.

For proving the statement on the sign of the functional equation we may choose ξ_M in the form $\xi_1\xi_2^{-1}$ as in Corollary 2.1.9. Since the degree of $\xi_1\xi_2^{\#}$ has the same parity as the rank of M and it satisfies the same functional equation, it is enough to prove the statement when ξ_M is integral. Now we can multiply the both sides of equation (2.8) by the "denominators" of the commutators and get an equation of the form

$$\xi_M^{\#} \prod_{i=1}^{n_1} (r_{i,1}^{l_{i,1}} f_{i,1}^{k_{i,1}} r_{i,1}^{-l_{i,1}}) \prod_{j=1}^{n_2} f_{j,2}^{k_{j,2}} = \varepsilon(M)\xi_M \prod_{i=1}^{n_1} f_{i,1}^{k_{i,1}} \prod_{j=1}^{n_2} (r_{j,2}^{l_{j,2}} f_{j,2}^{k_{j,2}} r_{j,2}^{-l_{j,2}}), \quad (2.9)$$

where $k_{i,1}$'s and $k_{j,2}$'s are positive integers, $l_{i,1}$'s and $l_{j,2}$'s are $+1$ or -1, so all factors on both sides are integral in the sense that they are in the image of $\Lambda(G) \cap \Lambda(G)_S^{\times}$ in $K_1(\Lambda(G)_S)$. Now we can reduce (2.9) modulo the ideal generated by X and p and get an equation in $K_1(\mathbb{F}_p((Y))) = \mathbb{F}_p((Y))^{\times}$. Moreover, it is easy to see that

$$\begin{aligned} (r_{i,1}^{l_{i,1}} f_{i,1}^{k_{i,1}} r_{i,1}^{-l_{i,1}}) &\equiv f_{i,1}^{k_{i,1}} \mod (X,p) \\ (r_{j,2}^{l_{j,2}} f_{j,2}^{k_{j,2}} r_{j,2}^{-l_{j,2}}) &\equiv f_{j,2}^{k_{j,2}} \mod (X,p), \text{ and} \\ \xi_M &\equiv Y^{\mathrm{rank}_{\Lambda(H)}(M)} \mod (X,p). \end{aligned}$$

So the reduced functional equation is in the form

$$\left(\frac{1}{1+Y} - 1\right)^{\mathrm{rank}_{\Lambda(H)}(M)} = \widetilde{\varepsilon(M)} Y^{\mathrm{rank}_{\Lambda(H)}(M)}.$$

Now if we divide both sides by $Y^{\mathrm{rank}_{\Lambda(H)}(M)}$ and reduce the equation modulo Y we obtain $\overline{\varepsilon(M)} = (-1)^{\mathrm{rank}_{\Lambda(H)}(M)}$. □

2.2 Pairings

Following the ideas of Perrin-Riou [29] in this section we construct a generalized Cassels-Tate pairing for the dual Selmer group over the false Tate curve extension. Let E be an elliptic curve with good ordinary reduction at the prime $p \geq 5$. 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

$$X(E/F_n^{cyc}) \to a^1_{\Lambda(\Gamma)}(X(E/F_n^{cyc})^\#)$$

constructed by Perrin-Riou [29] to get a map

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

We will 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 [29] main idea was that she wrote the Cassels-Tate pairing as an isomorphism

$$C_F : \ X(E/L)(p) \to \mathrm{Sel}(E/L)/\mathrm{div}(\mathrm{Sel}(E/L)) \tag{2.10}$$

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 [19] is that there also is an isomorphism

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

for any (not necessarily Artin) character τ of the Galois group $\mathrm{Gal}(L^{cyc}/L)$ with values in $\mathbb{Z}_p^\times$. So we have the choice of the character τ and it is easy to see that it can be chosen so that it is *admissible*, ie. $\mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/M)$ is finite for any subextension $L \subseteq M \subset L^{cyc}$. The reason why we need these

admissible representations is that in this case we have

$$\begin{aligned} \mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/L)/\mathrm{div}(\mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/L)) &= \mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/L), \text{ and} \\ X(\mathrm{tw}_{\tau}(E)/L) &= X(\mathrm{tw}_{\tau}(E)/L)(p), \end{aligned}$$

so we have a pairing on the Selmer group itself.

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

$$\mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/M) \to \mathrm{Sel}(\mathrm{tw}_{\tau^{-1}}(E)/L^{cyc})^{\mathrm{Gal}(L^{cyc}/M)} \tag{2.11}$$

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

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

Moreover, we have an isomorphism [29]

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

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

$$\begin{aligned} X(E/L^{cyc}) \otimes \tau = X(\mathrm{tw}_{\tau}(E)/L^{cyc}) \to \\ \to \mathrm{Ext}^1_{\Lambda}(X(\mathrm{tw}_{\tau^{-1}}(E)/L^{cyc})^{\#}, \Lambda) = \mathrm{Ext}^1_{\Lambda}(X(E/L^{cyc})^{\#}, \Lambda) \otimes \tau. \end{aligned}$$

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

To investigate the kernel and cokernel of the map

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

is equivalent to the description of the kernels and cokernels of the restriction

maps (2.11). This can be done using the usual diagrams

$$\begin{array}{ccccccc} 0 \to & \mathrm{Sel}(E/M) & \to H^1(F_R/M, E[p^\infty]) & \to \bigoplus_{u\in R} J_u(M) & \to 0 \\ & \downarrow r_M & \downarrow g_M & \downarrow \oplus\, h_{M,u} & \\ 0 \to & \mathrm{Sel}(E/L^{cyc})^{\Gamma_M} & \to H^1(F_R/L^{cyc}, E[p^\infty])^{\Gamma_M} & \to \bigoplus_{u\in R} J_u(L^{cyc})^{\Gamma_M}, & \end{array} \tag{2.12}$$

where $\Gamma_M = \mathrm{Gal}(L^{cyc}/M)$, R is the set of 'bad primes', F_R is the maximal Galois extension of L unramified outside the primes in R,

$$\begin{aligned} J_u(M) &:= \mathrm{Ker}(H^1(M, E[p^\infty]) \to \bigoplus_{u\in R} H^1(M_u, E[p^\infty])/\mathrm{Im}(\kappa_u)), \\ J_u(L^{cyc}) &:= \bigoplus_{u_L|u} H^1(L_{u_L}, E(\overline{L_{u_L}}))[p^\infty], \end{aligned}$$

and κ_u is the local Kummer map.

In this section we generalize this above idea from the commutative to the noncommutative Iwasawa theory.

2.2.1 Control Theorems

In this section we put together the already known [25], [29] facts about the kernels and cokernels of the homomorphisms

$$H_0(X(E/F_\infty), H_n) \longrightarrow X(E/F_n^{cyc}), \qquad \text{and} \tag{2.13}$$

$$X(E/F_n^{cyc}) \longrightarrow a^1_{\Lambda(\Gamma)}(X(E/F_n^{cyc})^\#). \tag{2.14}$$

As in [25] we define the following sets of primes. Let $P_0 = P_0(F_\infty/K^{cyc})$ the set of all primes of K^{cyc} which are not lying above p and ramified for F_∞/K^{cyc} (literally the primes dividing m and not dividing p). Further,

$$\begin{aligned} P_1 &:= \{u \in P_0 \mid E/K^{cyc} \text{ has split multiplicative reduction at } u\} \quad (2.15) \\ P_2 &:= \{u \in P_0 \mid E \text{ has good reduction at } u \text{ and } E[p^\infty](K_u^{cyc}) \neq 0\}, \end{aligned}$$

and we denote by $P_1^{(n)}$, $P_2^{(n)}$, $P_1(K)$, and $P_2(K)$ the corresponding sets of primes in F_n^{cyc} and K, respectively.

The cokernel of the homomorphism (2.13) and the kernel of (2.14) are bounded by $|E[p^\infty](F_\infty)|$, which is finite ([25] Lemma 3.12).

The kernel of (2.13) equals the Pontryagin dual of

$$\bigoplus_{u \in P_1 \cup P_2,\ u|w} H^1(H_{n,w}, E[p^\infty](F_{\infty,w}))$$

modulo finite modules which are bounded by $|E[p^\infty](F_\infty)|$ [25]. Moreover, as $\mathrm{Gal}(F_n^{cyc}/K)_v$-modules

$$H^1(H_{n,w}, E[p^\infty](F_{\infty,w})) \cong \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p(-1) \text{ if } w \text{ corresponds to a prime } v \in P_1, \\ E[p^\infty](-1) \text{ if } w \text{ corresponds to a prime } v \in P_2, \end{cases}$$

where $M(-1)$ denotes the -1st Tate twist of the Galois module M. Indeed, if v is in P_1 there is an exact sequence of modules

$$0 \to \mu_{p^\infty} \to E[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p \to 0 \tag{2.16}$$

and by taking its long exact sequence of $H_{n,w}$-cohomologies we get

$$0 \to \mathbb{Q}_p/\mathbb{Z}_p \to H^1(H_{n,w}, \mu_{p^\infty}) \to H^1(H_{n,w}, E[p^\infty]) \to H^1(H_{n,w}, \mathbb{Q}_p/\mathbb{Z}_p) \to 0,$$

and as abelian groups all of them in the sequence are isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$, however, as $\mathrm{Gal}(F_n^{cyc}/K)_v$-modules

$$\begin{aligned} H^1(H_{n,w}, \mu_{p^\infty}) &\cong \mathbb{Q}_p/\mathbb{Z}_p, \qquad \text{and} \\ H^1(H_{n,w}, E[p^\infty]) &\cong H^1(H_{n,w}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Q}_p/\mathbb{Z}_p(-1). \end{aligned}$$

When v is in P_2 then the statement follows from the fact that $H_{n,w}$ acts trivially on $E[p^\infty]$.

On the other hand, the cokernel of (2.14) equals the following modulo

finite modules with order bounded by $|E[p^\infty](F_\infty)|$ [23, 29]

$$\mathrm{Hom}\left(\varinjlim_{k\to\infty}\bigoplus_{u\in P_1^{(n)}} H^1(\Gamma_k, E[p^\infty](F_{n,u}^{cyc})), \mathbb{Q}_p/\mathbb{Z}_p\right).$$

Now since $E[p^\infty](F_{\infty,w}) = E[p^\infty]$ for any prime w above a prime in P_1 [25, 24] (because F_∞ is the maximal tame p-extension), we have the exact sequence

$$0 \to \mu_{p^\infty} \to E[p^\infty](F_{n,u}^{cyc}) \to \mathbb{Z}/p^{r_n}\mathbb{Z} \to 0$$

with some $r_n \geq 0$ integer, so $H^1(\Gamma_k, E[p^\infty](F_{n,u}^{cyc})) = \mathbb{Z}/p^{r_n}\mathbb{Z}$ is finite and independent of k, Γ acts trivially on it, and its order is not bounded when n tends to infinity. The unboundedness is true because $E(F_{\infty,w})$ contains all the p-division points on the curve.

Now we can state the following

Proposition 2.2.1. *There exists a map*

$$X(E/F_n^{cyc}) \left(\to a^1_{\Lambda(\Gamma)}(X(E/F_n^{cyc})^\#)\right) \to a^1_{\Lambda(\Gamma)}(H_0(H_n, X(E/F_\infty)^\#))$$

with finite and bounded kernel for varying n. The cokernel differs from

$$\bigoplus_{u\in P_2^{(n)}} T_p(E[p^\infty](F_{n,u}^{cyc}))^{\mathrm{v}} \oplus \bigoplus_{u\in P_1^{(n)}} M_u^{(n)}$$

by a finite module with bounded order for varying n, where $M_u^{(n)}$ fits into a short exact sequence

$$0 \to \mathbb{Z}_p/p^{r_n}\mathbb{Z}_p \to M_u^{(n)} \to \mathbb{Z}_p(-1) \to 0, \tag{2.17}$$

where $T_p(\cdot)$ denotes the p-adic Tate module of a module and the superscript $^{\mathrm{v}}$ denotes the dual $\mathrm{Hom}(\cdot, \mathbb{Z}_p)$.

Proof. The quasi-exact sequence

$$0 \to \bigoplus_{u \in P_1^{(n)} \cup P_2^{(n)},\ u|w} \mathrm{Hom}(H^1(H_{n,w}, E[p^\infty](F_{\infty,w})), \mathbb{Q}_p/\mathbb{Z}_p)^\# \to$$
$$\to H_0(H_n, X(E/F_\infty)^\#) \to X(E/F_n^{cyc})^\# \to 0$$

defines a quasi-exact sequence of extension functors

$$0 \to a^1_{\Lambda(\Gamma)}(X(E/F_n^{cyc})^\#) \to a^1_{\Lambda(\Gamma)}(H_0(H_n, X(E/F_\infty)^\#)) \to$$
$$\to \bigoplus_{u \in P_1^{(n)} \cup P_2^{(n)},\ u|w} a^1_{\Lambda(\Gamma)}(\mathrm{Hom}(H^1(H_{n,w}, E[p^\infty](F_{\infty,w})), \mathbb{Q}_p/\mathbb{Z}_p)^\#) \to 0,$$

since $\mathrm{Ext}^2_{\Lambda(\Gamma)}(X(E/F_n^{cyc})^\#, \Lambda(\Gamma))$ is trivial.

Now if u is in $P_2^{(n)}$ then

$$H^1(H_{n,w}, E[p^\infty](F_{\infty,w})) = E[p^\infty](-1)$$

and therefore

$$a^1_{\Lambda(\Gamma)}(\mathrm{Hom}(H^1(H_{n,w}, E[p^\infty](F_{\infty,w})), \mathbb{Q}_p/\mathbb{Z}_p)^\#) \cong T_p(E[p^\infty])^\vee.$$

Moreover, in this case there is no u-part of the cokernel of the map

$$X(E/F_n^{cyc}) \to a^1_{\Lambda(\Gamma)}(X(E/F_n^{cyc})^\#).$$

On the other hand, if u is in P_1 then

$$H^1(H_{n,w}, E[p^\infty](F_{\infty,w})) = \mathbb{Q}_p/\mathbb{Z}_p(-1)$$

and therefore

$$a^1_{\Lambda(\Gamma)}(\mathrm{Hom}(H^1(H_{n,w}, E[p^\infty](F_{\infty,w})), \mathbb{Q}_p/\mathbb{Z}_p)^\#) \cong \mathbb{Z}_p(-1).$$

Further, $H^1(H_{n,w}, E[p^\infty](F_{\infty,w}) = \mu_{p^\infty}$ and the u-part of the cokernel of the

morphism

$$X(E/F_n^{cyc}) \to a^1_{\Lambda(\Gamma)}(X(E/F_n^{cyc})^{\#}).$$

differs from $\mathbb{Z}/p^{r_n}\mathbb{Z}$ with trivial Γ-action by a finite module of bounded order for varying n. □

2.2.2 Main theorem

The following theorem is a generalization of pairings to non-commutative Iwasawa theory. There are previous results for the cyclotomic, anticyclotomic or $\mathbb{Z}_p^2$-case [22, 29]. Moreover, it is compatible with the main conjecture for the false Tate curve extension, and the conjectural functional equation of the p-adic L-function [6, 7, 20].

Theorem 2.2.2. *If E has good ordinary reduction at the prime $p \geq 5$ and $X(E/F_\infty)$ lies in the category $\mathfrak{M}_H(G)$ then there is an exact sequence*

$$0 \to X(E/F_\infty) \xrightarrow{\varphi} a^1_{\Lambda(G)}(X(E/F_\infty)^{\#}) \to \mathrm{Coker}(\varphi) \to 0,$$

where $\mathrm{Coker}(\varphi)$ *represents the same element in* $K_0(\mathfrak{M}_H(G))$ *as*

$$\bigoplus_{v \in P_1(K) \cup P_2(K)} \Lambda(G) \otimes_{\Lambda(G_v)} T_p(E[p^\infty](F_{\infty,w}))^{\mathrm{v}},$$

where w is a (fixed) prime in F_∞ above v.

Proof. First of all let us remark that each component of the above expression for the cokernel is isomorphic to

$$\Lambda(G) \otimes_{\Lambda(G_v)} T_p(E[p^\infty](F_{\infty,w}))^{\mathrm{v}} \cong \bigoplus_{u \in P_1 \cup P_2,\ v|u|w} T_p(E[p^\infty](F_{\infty,w}))^{\mathrm{v}} \qquad (2.18)$$

as $\Lambda(G)$-modules with the natural action of $\Lambda(G)$ on the right hand side (G permutes the primes above a fixed prime v in K) since the primes in $P_1 \cup P_2$ ramify totally in the extension F_∞/K^{cyc}. So it is enough to prove that the cokernel in the theorem is isomorphic to the direct sum of the modules on the right hand side of (2.18).

We would like to take the projective limit of homomorphisms in Proposition 2.2.1

$$X(E/F_n^{cyc}) \to a^1_{\Lambda(\Gamma)}(H_0(H_n, X(E/F_\infty)^\#)).$$

For this we first remark that there is a canonical identification

$$a^1_{\Lambda(\Gamma)}(H_0(H_n, X(E/F_\infty)^\#)) \cong a^1_{\Lambda(\mathrm{Gal}(F_n^{cyc}/K))}(H_0(H_n, X(E/F_\infty)^\#))$$

as $\Lambda(\Gamma)$-modules [26]. Moreover the norm map from F_{n+1}^{cyc} to F_n^{cyc} induces a natural homomorphism

$$a^1_{\Lambda(\mathrm{Gal}(F_{n+1}^{cyc}/K))}(X(E/F_\infty)^\#_{H_{n+1}}) \to a^1_{\Lambda(\mathrm{Gal}(F_n^{cyc}/K))}(X(E/F_\infty)^\#_{H_n}),$$

so we can take the projective limit of these modules with the connecting maps above. It is easy to see that the limit is $a^1_{\Lambda(G)}(X(E/F_\infty)^\#)$ so we get a map from $X(E/F_\infty)$ to this module. The kernel of this homomorphism is the limit of the finite and bounded kernels and so is finite. However, $X(E/F_\infty)$ has no nontrivial pseudo-null submodule and finite modules are obviously pseudo-null, so the morphism we got is injective. Note that $X(E/F_\infty)$ has the same $\Lambda(H)$-rank as $a^1_{\Lambda(G)}(X(E/F_\infty)^\#)$, so this map is automatically a pseudo-isomorphism. The cokernel is the limit of the cokernels in the finite layers and so it equals

$$\bigoplus_{u\in P_2,\ u|w} T_p(E[p^\infty](F_{\infty,w}))^\vee \oplus \bigoplus_{u\in P_1} \varprojlim M_u^{(n)}$$

up to finite modules. Because of (2.17) and the fact that $r_n \to \infty$ the projective limit of the modules $M_u^{(n)}$ fits into the exact sequence

$$0 \to \mathbb{Z}_p \to \varprojlim M_u^{(n)} \to \mathbb{Z}_p(-1) \to 0.$$

So does $T_p(E[p^\infty](F_{\infty,w}))^\vee$ and therefore they represent the same element in $K_0(\mathfrak{M}_H(G))$. □

Remarks. 1. For any w above a prime in P_1

$$T_p(E[p^\infty](F_{\infty,w}))^\vee$$

represents the same element in $K_0(\mathfrak{M}_{H_v}(G_v))$ as

$$\mathbb{Z}_p \oplus \mathbb{Z}_p(-1)$$

because it fits into the exact sequence of $\Lambda(G_v)$-modules

$$0 \to \mathbb{Z}_p \to T_p(E[p^\infty](F_{\infty,w}))^\vee \to \mathbb{Z}_p(-1) \to 0.$$

However, this exact sequence does not split.

2. If we define $P_1(\mathbb{Q})$ and $P_2(\mathbb{Q})$ to be the set of primes q in $\mathbb{Q}$ such that all primes in K above q are in $P_1(K)$ and $P_2(K)$, respectively then we can investigate the $\Lambda(G_0)$-structure of the above cokernel. Since the reduction type of the elliptic curve at two primes in K over the same prime in $\mathbb{Q}$ are the same, the $\Lambda(G_0)$ structure is the following

$$\bigoplus_{q \in P_1(\mathbb{Q}) \cup P_2(\mathbb{Q})} \Lambda(G_0) \otimes_{\Lambda(G_q)} T_p(E[p^\infty](F_{\infty,w}))^\vee,$$

where w is a prime in F_∞ above q.

2.3 Functional equations

2.3.1 Functional equation of the characteristic element

We are going to apply Theorems 2.2.2 and 2.1.11. Note that by Lemma 2.1.10 the characteristic element of

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

is $\xi^\#_{X(E/F_\infty)}$ as the higher extension groups of $X(E/F_\infty)^\#$ are finite since $X(E/F_\infty)$ has no nontrivial pseudo-null submodule [25]. We get the following

corollary on the characteristic element.

Corollary 2.3.1. *If E has good ordinary reduction at the prime $p \geq 5$ and $X(E/F_\infty)$ is in $\mathfrak{M}_H(G)$ then the characteristic element $\xi_{X(E/F_\infty)}$ of $X(E/F_\infty)$ in $K_1(\Lambda(G)_{S^*})$ satisfies a functional equation of the following form*

$$\xi^{\#}_{X(E/F_\infty)} = \xi_{X(E/F_\infty)}\varepsilon_0(X(E/F_\infty)) \prod_{v \in P_1(K) \cup P_2(K)} \alpha_v,$$

where $\varepsilon_0(X(E/F_\infty))$ is in $K_1(\Lambda(G))$, and

$$\alpha_v = \frac{\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-N_{K/\mathbb{Q}}v}-1}{\frac{1}{X+1}-1}}{\mathrm{Frob}_v - \frac{(X+1)^{N_{K/\mathbb{Q}}v}-1}{X}} \qquad \text{if } v \text{ is in } P_1(K), \text{ and}$$

$$\alpha_v = \frac{\left(\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-b_v}-1}{\frac{1}{X+1}-1}\right)\left(\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-N_{K/\mathbb{Q}}v}-1}{\frac{1}{(X+1)^{b_v}}-1}\right)}{\left(\mathrm{Frob}_v - \frac{(X+1)^{b_v}-1}{X}\right)\left(\mathrm{Frob}_v - \frac{(X+1)^{N_{K/\mathbb{Q}}v}-1}{(X+1)^{b_v}-1}\right)} \text{ if } v \text{ is in } P_2(K),$$

where Frob_v *is the arithmetic Frobenius, and b_v is a root of the polynomial*

$$x^2 - (N_{K/\mathbb{Q}}v + 1 - \#\tilde{E}(\mathbb{F}_v))x + N_{K/\mathbb{Q}}v$$

in $\mathbb{Z}_p$, and $\#\tilde{E}(\mathbb{F}_v))$ is the number of points on the curve reduced modulo v. Moreover, if we reduce $\varepsilon_0(X(E/F_\infty))$ modulo the Jacobson radical of $\Lambda(G)$ we get an element in $\mathbb{F}_p$ that equals $(-1)^{\mathrm{rank}_{\mathbb{Z}_p}(X(E/K^{cyc}))}$.

Proof. Since $H = H_v$ for all v's in question (it is a totally ramified extension), the characteristic element of a module in $\mathfrak{M}_H(G)$ of the form

$$\Lambda(G) \otimes_{\Lambda(G_v)} M$$

with M in $\mathfrak{M}_{H_v}(G_v)$ is the image of the characteristic element of M in $K_1(\Lambda(G)_S)$. So in view of the first remark after Theorem 2.2.2, we only have to verify the following statements. Firstly, there exists an element b_v in $\mathbb{Z}_p$ with

$$b_v^2 - (N_{K/\mathbb{Q}}v + 1 - \#\tilde{E}(\mathbb{F}_v))b_v + N_{K/\mathbb{Q}}v = 0$$

because the above is the characteristic polynomial of Frob_v^{-1} acting on the Tate module and Frob_v^{-1} has p-power order when reducing modulo p, so its eigenvalues are in $\mathbb{F}_p$ and can be lifted to $\mathbb{Z}_p$.

Secondly, that for $v \in P_2(K)$ the characteristic element of the dual of the Tate module $T_p(E[p^\infty](F_{\infty,w}))^\vee$ is

$$\frac{\left(\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-b_v}-1}{\frac{1}{X+1}-1}\right)\left(\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-N_{K/\mathbb{Q}^v}}-1}{\frac{1}{(X+1)^{b_v}}-1}\right)}{\left(\mathrm{Frob}_v - \frac{(X+1)^{b_v}-1}{X}\right)\left(\mathrm{Frob}_v - \frac{(X+1)^{N_{K/\mathbb{Q}^v}}-1}{(X+1)^{b_v}-1}\right)} \tag{2.19}$$

as a $\Lambda(G_v)$-module. This is true because H acts trivially on $T_p(E[p^\infty](F_{\infty,w}))^\vee$ and we have an exact sequence of $\Lambda(G_v)$-modules

$$0 \to X(T_p(E[p^\infty])^\vee \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!]) \to T_p(E[p^\infty])^\vee \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!] \to T_p(E[p^\infty]) \to 0.$$

Moreover, the numerator of (2.19) reduces to the characteristic polynomial of Frob_v^{-1} modulo X so it is a characteristic element to

$$T_p(E[p^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!].$$

Now we have an isomorphism $T_p(E[p^\infty])^\vee(1) \cong T_p(E[p^\infty])$ and

$$X(T_p(E[p^\infty])^\vee \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!]) \cong T_p(E[p^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!],$$

so the denominator

$$\left(\mathrm{Frob}_v - \frac{(X+1)^{b_v}-1}{X}\right)\left(\mathrm{Frob}_v - \frac{(X+1)^{N_{K/\mathbb{Q}^v}}-1}{(X+1)^{b_v}-1}\right) =$$
$$\left(\left(\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-b_v}-1}{\frac{1}{X+1}-1}\right)\left(\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-N_{K/\mathbb{Q}^v}}-1}{\frac{1}{(X+1)^{b_v}}-1}\right)\right)^\#$$

is a characteristic element to

$$X(T_p(E[p^\infty])^\vee \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!]).$$

Finally, the characteristic element of $\mathbb{Z}_p \oplus \mathbb{Z}_p(-1)$ is

$$\frac{\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-N_{K/\mathbb{Q}^v}}-1}{\frac{1}{X+1}-1}}{\mathrm{Frob}_v - \frac{(X+1)^{N_{K/\mathbb{Q}^v}}-1}{X}}$$

as a $\Lambda(G_v)$-module when $v \in P_1(K)$. Indeed, since

$$\mathrm{Frob}_v(X+1)\mathrm{Frob}_v^{-1} = (X+1)^{N_{K/\mathbb{Q}^v}}$$

it is easy to see that the following sequences are exact

$$0 \to \Lambda(G_v)/\left(\mathrm{Frob}_v - \frac{(X+1)^{N_{K/\mathbb{Q}^v}}-1}{X}\right) \\ \to \Lambda(G)/(\mathrm{Frob}_v - 1) \to \mathbb{Z}_p \to 0,$$

$$0 \to \Lambda(G)/(\mathrm{Frob}_v - 1) \\ \to \Lambda(G)/\left(\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-N_{K/\mathbb{Q}^v}}-1}{\frac{1}{X+1}-1}\right) \to \mathbb{Z}_p(-1) \to 0.$$

The first statement follows immediately from the fact that the characteristic element of a module which is the factor of $\Lambda(G)$ modulo a principal (left) ideal is the generator of the ideal. The sign in this functional equation follows from Theorem 2.1.11 and the formula [25]

$$\mathrm{rank}_{\Lambda(H)}(X(E/F_\infty)) = \mathrm{rank}_{\mathbb{Z}_p}(X(E/K^{cyc})) + |P_1(K)| + 2|P_2(K)|,$$

because the v-part of the characteristic element of the cokernel reduces to -1 modulo the Jacobson radical of $\Lambda(G)$ if v is $P_1(K)$ and to $+1$ if it is in $P_2(K)$. □

Remarks. 1. The following functional equation of the characteristic element $\xi_{\mathbb{Q},X(E/F_\infty)}$ of $X(E/F_\infty)$ in $K_1(\Lambda(G_0)_{S_\mathbb{Q}^*})$ can be proved similarly

$$\xi^{\#}_{\mathbb{Q},X(E/F_\infty)} = \xi_{\mathbb{Q},X(E/F_\infty)}\varepsilon_0(\mathbb{Q}, X(E/F_\infty)) \prod_{q \in P_1(\mathbb{Q}) \cup P_2(\mathbb{Q})} \alpha_q.$$

Here $\varepsilon_0(\mathbb{Q}, X(E/F_\infty))$ is in $K_1(\Lambda(G_0))$, and

$$\alpha_q = \frac{\mathrm{Frob}_q^{-1} - \frac{(X+1)^{-q}-1}{\frac{1}{X+1}-1}}{\mathrm{Frob}_q - \frac{(X+1)^q-1}{X}} \qquad \text{if } q \text{ is in } P_1(\mathbb{Q}), \text{ and}$$

$$\alpha_q = \frac{\left(\mathrm{Frob}_q^{-1} - \frac{(X+1)^{-b_q}-1}{\frac{1}{X+1}-1}\right)\left(\mathrm{Frob}_q^{-1} - \frac{(X+1)^{-q}-1}{\frac{1}{(X+1)^{b_q}}-1}\right)}{\left(\mathrm{Frob}_q - \frac{(X+1)^{b_q}-1}{X}\right)\left(\mathrm{Frob}_q - \frac{(X+1)^q-1}{(X+1)^{b_q}-1}\right)} \text{ if } q \text{ is in } P_2(\mathbb{Q}),$$

where Frob_q is the arithmetic Frobenius, and b_q is a root of the polynomial

$$x^2 - (q + 1 - \#\tilde{E}(\mathbb{F}_q))x + q$$

in $\mathbb{Z}_p$, and $\#\tilde{E}(\mathbb{F}_q))$ is the number of points on the curve reduced modulo q.

2. We chose a different normalization of the characteristic element of the cokernel in the above theorem from the one in section 2.1.3 because it fits more into the analytic theory in the following section. Moreover, for each v and q, we have $\alpha_v \alpha_v^{\#} = 1$, and $\alpha_q \alpha_q^{\#} = 1$.

2.4 Connections to the analytic side

In this section we compare the algebraic functional equation we obtained in the previous section for the characteristic element of the dual Selmer group and the conjectural functional equation of the p-adic L-function.

2.4.1 The Main Conjecture

Let R denote the following set of rational primes

$$R := \{p\} \cup \{q \in \mathbb{Q} \text{ prime } : q \mid m \text{ and } E[p^\infty] \subseteq F_{\infty,w} \text{ for a } w \in F_\infty \text{ above } q\}. \tag{2.20}$$

When we specialize Conjecture 1.3.2 to the false Tate curve case we obtain the following

Conjecture 2.4.1. *Assume that $p \geq 5$ and that E has good ordinary reduction at p. Then there exists $\mathfrak{L}_E$ in $K_1(\Lambda(G_0)_{S^*_{\mathbb{Q}}})$ such that, for all Artin representations τ of G_0, we have $\mathfrak{L}_E(\tau) \neq \infty$, and*

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

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.

Let us also recall the main conjecture of Iwasawa theory for elliptic curves over the false Tate tower which is a special case of Conjecture 1.3.3.

Conjecture 2.4.2 (The main conjecture)**.** *Assume that $p \geq 5$, E has good ordinary reduction at p, and $X(E/F_\infty)$ belongs to the category $\mathfrak{M}_{H_0}(G_0)$. Granted Conjecture* 2.4.1*, the p-adic L-function $\mathfrak{L}_E$ in $K_1(\Lambda(G_0)_{S^*_{\mathbb{Q}}})$ is a characteristic element of $X(E/F_\infty)$.*

2.4.2 Compatibility of the functional equations

We begin this section with investigating the values of the modifying factors α_q of the algebraic functional equation at the irreducible Artin representations of G_0. The irreducible Artin representations of G_0 are in the form $\rho_n\chi$ or χ, where ρ_n is a representation of $\mathrm{Gal}(F_n/\mathbb{Q})$ induced by any character of $\mathrm{Gal}(F_n/\mathbb{Q}(\mu_{p^n}))$ of exact order p^n, and χ is a 1-dimensional character of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$. It is enough to deal with irreducible representations because both the modified L-values and the values of elements in $K_1(\Lambda(G_0)_{S^*_{\mathbb{Q}}})$ are multiplicative with respect to direct sums of representations.

Proposition 2.4.3. *The values of α_q at irreducible Artin representations of G_0 are as follows.*

$$\begin{aligned}
\alpha_q(\chi) &= \frac{P_q(E,\chi,q^{-1})}{P_q(E,\overline{\chi},q^{-1})}, \text{ and} \\
\alpha_q(\rho_n\chi) &= \begin{cases} \left(\frac{q}{p}\right)\frac{P_q(E,\rho_n\chi,q^{-1})}{P_q(E,\rho_n\overline{\chi},q^{-1})}\chi(\mathrm{Frob}_q^{-1})^{p^{n-1}(p-1)}, & \text{if } q \in P_1(\mathbb{Q}) \\ \frac{P_q(E,\rho_n\chi,q^{-1})}{P_q(E,\rho_n\overline{\chi},q^{-1})}, & \text{if } q \in P_2(\mathbb{Q}), \end{cases}
\end{aligned}$$

Where $\left(\frac{q}{p}\right)$ *denotes the Legendre symbol.*

Proof. This is a simple computation using that $\det \rho_n(\mathrm{Frob}_q) = \left(\frac{q}{p}\right)$. □

Since $\mathfrak{L}_E^{\#}(\tau) = \mathfrak{L}_E(\tau^*)$ for any Artin representation τ of G_0, this above proposition shows that the functional equation of the characteristic element of $X(E/F_\infty)$ is compatible with the Main Conjecture up to p-adic units because they modify the same way when changing τ to τ^*. Indeed, by conjecture 2.4.1 we have

$$\begin{aligned} \mathfrak{L}_E(\tau^*) &= \frac{L_R(E,\tau,1)}{\Omega_+(E)^{d^+(\tau)}\Omega_-(E)^{d^-(\tau)}} \cdot \varepsilon_p(\tau) \cdot \frac{P_p(\tau^*, b_p^{-1})}{P_p(\tau, c_p^{-1})} \cdot b_p^{-f_\tau}, \text{ and} \qquad (2.21) \\ \mathfrak{L}_E^{\#}(\tau^*) &= \mathfrak{L}_E(\tau) = \frac{L_R(E,\tau^*,1)}{\Omega_+(E)^{d^+(\tau^*)}\Omega_-(E)^{d^-(\tau^*)}} \cdot \varepsilon_p(\tau^*) \cdot \frac{P_p(\tau, b_p^{-1})}{P_p(\tau^*, c_p^{-1})} \cdot b_p^{-f_{\tau^*}}. \end{aligned}$$

Moreover, the functional equation of the complex L is

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

where

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

From this we obtain

$$L(E,\tau,1) = w(E,\tau)L(E,\tau^*,1) \qquad (2.22)$$

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, so by combining (2.21) and (2.22) we obtain

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

are equal up to p-adic units. So Proposition 2.4.3 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.

In the following proposition we prove that for any *self-dual* Artin representation τ the signs in the algebraic and analytic functional equations coincide, as well. This is also a good evidence for both the Main Conjecture and the conjectural functional equation of the p-adic L-function.

Proposition 2.4.4. *The signs when substituting self-dual Artin representations of G_0 into the the functional equation of the characteristic element $\xi_{\mathbb{Q},X(E/F_\infty)}$ of the dual Selmer group $X(E/F_\infty)$ are as follows. All of them are equal to the signs of the functional equations of the twisted L-functions of the elliptic curve with the Artin representations in question.*

$$w_{\mathrm{alg}}(E,\tau) = \begin{cases} (-1)^{t_{E/\mathbb{Q},p}} & \text{if } \tau \text{ is the trivial representation,} \\ (-1)^{t_{E/\mathbb{Q},p}+t_{E/K,p}} & \text{if } \tau \text{ is the real character of order 2,} \\ (-1)^{t_{E/K,p}} \prod_{q\in P_1(\mathbb{Q})} \left(\frac{q}{p}\right) & \text{if } \tau = \rho_n \text{ for some } n, \\ 1 & \text{if } \tau = \chi \oplus \overline{\chi} \text{ or } \rho_n \otimes (\chi \oplus \overline{\chi}) \text{ for some } n \text{ and} \\ & \quad \chi \text{ character of } \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}), \end{cases}$$

where $t_{E/k,p}$ is the $\mathbb{Z}_p$-rank of the dual Selmer $X(E/k)$ for any number field k.

Proof. It is enough to prove that modulo squares in $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]^\times$ the factor $\varepsilon_0(\mathbb{Q}, X(E/F_\infty))$ reduces to $(-1)^{t_{E/\mathbb{Q},p}}\tilde{\gamma}_0^{t_{E/K,p}}$ because then the statement follows by substituting the Artin representations into this epsilon factor and applying Proposition 2.4.3. The statement regarding the sign in the analytic functional equation follows from the formulae for the root numbers [16], and from the fact that the parity conjectures $t_{E/\mathbb{Q},p} \equiv r_{E/\mathbb{Q}}$ and $t_{E/K,p} \equiv r_{E/K}$ are true due to Nekovář [28]. For this let us reduce the equation

$$\xi^{\#}_{\mathbb{Q},X(E/F_\infty)} = \xi_{\mathbb{Q},X(E/F_\infty)}\varepsilon_0(\mathbb{Q}, X(E/F_\infty)) \prod_{q\in P_1(\mathbb{Q})\cup P_2(\mathbb{Q})} \alpha_q$$

modulo X. After multiplying by the denominators we get the following

$$\tilde{\xi}^{\#} \prod_{q \in P_1(\mathbb{Q})} (\mathrm{Frob}_q - q) \prod_{q \in P_2(\mathbb{Q})} (\mathrm{Frob}_q - b_q)(\mathrm{Frob}_q - q/b_q) = \tag{2.23}$$

$$= \tilde{\xi}\tilde{\varepsilon}_0 \prod_{q \in P_1(\mathbb{Q})} (\mathrm{Frob}_q^{-1} - q) \prod_{q \in P_2(\mathbb{Q})} (\mathrm{Frob}_q^{-1} - b_q)(\mathrm{Frob}_q^{-1} - q/b_q),$$

where $\tilde{\xi}$ and $\tilde{\varepsilon}_0$ denote the reduction of $\xi_{\mathbb{Q},X(E/F_\infty)}$ and $\varepsilon_0(\mathbb{Q}, X(E/F_\infty))$ modulo X, respectively. Now $\tilde{\xi}$ is a polynomial in the variable $\tilde{\gamma}_0$—which is the generator of the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$—of degree $\mathrm{rank}_{\Lambda(H)}(X(E/F_\infty))$ and Frob_q equals $\tilde{\gamma}_0$ to some even power if $\left(\frac{q}{p}\right) = 1$ and to some odd power if $\left(\frac{q}{p}\right) = -1$. Since

$$(-1)^{t_{E/K,p}} = (-1)^{\mathrm{rank}_{\Lambda(H)}(X(E/F_\infty))} \prod_{q \in P_1(\mathbb{Q})} \left(\frac{q}{p}\right),$$

on the right hand side of the equation (2.23) there is a polynomial in $\tilde{\gamma}_0$ of degree the same parity as $t_{E/K,p}$. Moreover, the roots of this polynomial are in pairs, except when they are ± 1 because if a (p-adic) number is a root of this polynomial then so is its reciprocal. We get a -1 in the functional equation for each multiplicity of the root 1 and this number is exactly $t_{E/\mathbb{Q},p}$. We also get a $\tilde{\gamma}_0$ to the power of the degree in the functional equation and we are done. □

2.5 Heegner-like cases

Throughout this section we shall need the following hypotheses on p and the elliptic curve E imposed in [6].

Hypothesis 1. *E has good ordinary reduction at p.*

Hypothesis 2. *$X(E/F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$.*

Recall that a finitely generated module M over the Iwasawa algebra of the cyclotomic $\mathbb{Z}_p$-extension is always pseudo-isomorphic to a module of the

form

$$\bigoplus_i \mathbb{Z}_p[[T]]/p^{\mu_i} \oplus \bigoplus_j \mathbb{Z}_p[[T]]/f_j^{m_j},$$

where the f_j's are distinguished polynomials. Its characteristic power series is defined to be

$$f_M = \prod_i p^{\mu_i} \prod_j f_j^{m_j}$$

and its μ-invariant is $\mu(M) = \sum_i \mu_i$. If L is any number field and E an elliptic curve satisfying the above hypotheses, let us denote by $\mu_{E/L}$ the μ-invariant of $X(E/L^{cyc})$. Note that Hypothesis 2 is automatic if $\mu_{E/K} = 0$ [25].

Since G is a pro-p group without p-torsion, the pseudo-null p-primary finitely generated $\Lambda(G)$-modules are exactly those whose classes are trivial in the Grothendieck group $K_0(\mathfrak{M}_H(G))$, or equivalently if its characteristic element vanishes [1]. It also follows that if M is a p-primary module in the category $\mathfrak{M}_H(G)$ then its characteristic element is the image of

$$p^{\mathrm{rank}_{\Omega(G)}\mathrm{gr}_p(M)}$$

in the group $K_1(\Lambda(G)_{S^*})$, where $\mathrm{gr}_p(M)$ denotes the graded module of M with respect to the p-adic filtration of M [1]. Moreover, by definition the rank of the graded module is equal to the μ-invariant $\mu_G(M)$ of the $\Lambda(G)$-module M.

Proposition 2.5.1. *If E is an elliptic curve and $p \geq 5$ is a prime satisfying Hypotheses 1 and 2 then the characteristic element of $X(E/F_\infty)(p)$ is the image of $p^{\mu_{E/K}}$ in the group $K_1(\Lambda(G)_{S^*})$. Moreover, if $K \leq L \leq F_\infty$ is an intermediate number field then $\mu_{E/L} = p^{[L:K]}\mu_{E/K}$.*

Proof. The first statement immediately follows from the fact that

$$\mu_G(X(E/F_\infty)) = \mu_{E/K}$$

whenever we assume Hypotheses 1 and 2 [9]. We can obtain the second statement by applying the first one for the extension F_∞/L and comparing

the rank of the module $\mathrm{gr}_p(X(E/F_\infty)(p))$ over $\Lambda(G)$ and $\Lambda(\mathrm{Gal}(F_\infty/L))$. $\square$

If v is a prime in K, we write k_v for the residue class field of K at v. Further, $\tilde{E}_v$ denotes the reduction of E mod v. Recall our standing hypothesis that m is p-power free and not divisible by any rational prime q such that E has additive reduction at q. Consider the following sets of rational primes:

$$\begin{aligned} P_1 &= \{q \mid \text{split multiplicative reduction at all primes } v \text{ of } K \text{ above } q\} \\ P_2 &= \{q \mid q \neq p, \text{ good reduction at } q, \tilde{E}_v(k_v)(p) \neq 0 \text{ for a } v \in K \text{ above } q.\} \end{aligned} \tag{2.24}$$

The following proposition can be found in [6].

Proposition 2.5.2. *Assume Hypotheses 1 and 2. Then $X(E/F_\infty)$ has $\Lambda(H)$-rank 1 if and only if m has no prime divisor in the set P_2 and either (i) $X(E/K^{cyc})$ has $\mathbb{Z}_p$-rank zero and m has precisely one prime divisor q in P_1 which is inert in K^{cyc} or (ii) $X(E/K^{cyc})$ has $\mathbb{Z}_p$-rank 1 and m has no prime divisor in P_1.*

The following sections deal with these two cases.

2.5.1 The classical case

In this section let us assume the second case of Proposition 2.5.2. Therefore we have $g_{E/F_n} \leq p^n \leq r_{E/F_n}$ for any positive integer n (see the Appendix A of [17]). Moreover, the characteristic power series for $Y(E/F_n^{cyc})$ is T^{p^n} and the p^∞-Selmer rank $t_{E/F_n,p} = p^n$ for all $n \geq 1$ [6]. Since there is an injective $\Lambda(H)$-homomorphism

$$Y(E/F_\infty) \hookrightarrow \Lambda(H)$$

with finite cokernel [25], we can investigate the action of G on this finite index submodule of $\Lambda(H)$. Let us at first identify the Iwasawa algebra $\Lambda(H)$ with the ring of formal power series $\mathbb{Z}_p[\![X]\!]$ so that a topological generator $h \in H$ is mapped to the power series $1 + X$. Now we can consider $Y(E/F_\infty)$

as a finite index submodule of $\mathbb{Z}_p[\![X]\!]$, hence it contains a constant power series p^l for some $l \in \mathbb{N}$. Since $Y(E/F_\infty)$ admits an action of G, we can define a power series $f(X) \in p^{-l}\mathbb{Z}_p[\![X]\!]$ as $f(X) = p^{-l}\tilde{\gamma}p^l$ where $\tilde{\gamma} \in G$ is a lift of the topological generator $\gamma \in \Gamma$ to G such that it fixes the subfield $\mathbb{Q}(\mu_p, \sqrt[p^\infty]{m})$. We are going to show that in fact $f(X)$ is in $\mathbb{Z}_p[\![X]\!]$ and satisfies some functional equation. This will be the image of $1 \in \Lambda(H)$ when we extend the action of γ to the whole $\mathbb{Z}_p[\![X]\!]$.

Lemma 2.5.3. *Under the Hypotheses 1 and 2 and the second case of Proposition 2.5.2 we have the following functional equation for the power series $f(X)$:*

$$\begin{aligned} \prod_{j=0}^{p^{n-1}-1} f(\zeta_{p^n}^{1+jp} - 1) &= 1, \text{ and} \\ f(0) &= 1 \end{aligned} \tag{2.25}$$

where ζ_{p^n} is an arbitrary primitive p^nth root of unity ($n \geq 1$ integer). In particular $f(0) = f(\zeta_p - 1) = 1$.

Proof. First of all let us remark that in fact $f(X)$ determines the action of G on $Y(E/F_\infty)$ because if $f_1(X) \in Y(E/F_\infty) \leq \mathbb{Z}_p[\![X]\!]$ then $\tilde{\gamma}f_1(X) = \tilde{\gamma}f_1(X)\tilde{\gamma}^{-1}\tilde{\gamma}1 = (\tilde{\gamma}f_1(X)\tilde{\gamma}^{-1})f(X)$ where $\tilde{\gamma}f_1(X)\tilde{\gamma}^{-1}$ is the conjugation by $\tilde{\gamma}$ on the group ring $\Lambda(H)$. Since the kernel and the cokernel of the restriction homomorphism

$$Y(E/F_\infty)_{H_n} \to Y(E/F_n^{cyc})$$

are finite [25] and the characteristic element of $Y(E/F_n^{cyc})$ is T^{p^n}, the Akashi series (ie. the characteristic element of $Y(E/F_\infty)_{H_n}$ as a Γ_n-module since the higher homology groups of $Y(E/F_\infty)$ are finite because $Y(E/F_\infty)$ is a finite index submodule of a free $\Lambda(H)$-module) of $Y(E/F_\infty)$ is also T^{p^n}, namely $\tilde{\gamma}^{p^{n-1}}$ (and $\tilde{\gamma}$ when $n = 0$) has the unique eigenvalue 1 when acting on

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \left(Y(E/F_\infty) / \left((X+1)^{p^n} - 1 \right) Y(E/F_\infty) \right).$$

and we immediately get $f(0) = 1$ when $n = 0$. However, the latter action

can be computed in a different way. For any $f_1(X) \in Y(E/F_\infty)$ we have

$$\tilde{\gamma}^{p^{n-1}} f_1(X) = \tilde{\gamma}^{p^{n-1}} f_1(X) \tilde{\gamma}^{-p^{n-1}} \prod_{j=0}^{p^{n-1}-1} \tilde{\gamma}^j f(X) \tilde{\gamma}^{-j}.$$

Since the commutator $[\tilde{\gamma}^{p^{n-1}}, H]$ is equal to H_n, we have

$$\prod_{j=0}^{p^{n-1}-1} f(\zeta_{p^n}^{\tilde{\gamma}^{-j}} - 1) = \prod_{j=0}^{p^{n-1}-1} f(\zeta_{p^n}^{1+jp} - 1)$$

is an eigenvalue of $\tilde{\gamma}^{p^{n-1}}|_{Y(E/F_\infty)_{H_n} \otimes \mathbb{Q}_p}$ and we are done. □

Remark. This condition on $f(X)$ actually means that the relative norm of $f(\zeta_{p^n} - 1)$ is 1 in the extension $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_p)$.

Let ρ_n be the Artin representation of G obtained by inducing any character of exact order p^n of $\mathrm{Gal}(F_n/\mathbb{Q}(\mu_{p^n}))$ to $\mathrm{Gal}(F_n/K)$.

Proposition 2.5.4. *Under the Hypotheses 1 and 2 and the second case of Proposition 2.5.2, the Akashi series of the twisted module* $\mathrm{tw}_{\rho_n}(Y(E/F_\infty))$ *is* $(T+1)^{p^{n-1}} - 1$.

Proof. Since in the standard basis of ρ_n

$$\rho_n(\tilde{\gamma}) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & 0 & \ddots & \vdots \\ 0 & \vdots & \vdots & \ddots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad \rho_n(h) = \begin{pmatrix} \zeta & 0 & 0 & \cdots & 0 \\ 0 & \zeta^{\tilde{\gamma}} & 0 & \cdots & 0 \\ \vdots & 0 & \zeta^{\tilde{\gamma}^2} & \ddots & \vdots \\ 0 & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & \zeta^{\tilde{\gamma}^{p^{n-1}-1}} \end{pmatrix},$$

where ζ is a primitive p^nth root of unity, we have that the matrix of $\tilde{\gamma}$ is

$$\begin{pmatrix} 0 & f(\zeta^{-1} - 1) & 0 & \cdots & 0 \\ 0 & 0 & f(\zeta^{-\tilde{\gamma}} - 1) & \cdots & 0 \\ \vdots & & 0 & \ddots & \vdots \\ 0 & \vdots & \vdots & \ddots & f(\zeta^{-\tilde{\gamma}^{p^{n-1}-2}} - 1) \\ f(\zeta^{-\tilde{\gamma}^{p^{n-1}-1}} - 1) & 0 & 0 & \cdots & 0 \end{pmatrix}$$

when we restrict it to $\mathrm{tw}_{\rho_n}(Y(E/F_\infty))_H$, since h acts on $Y(E/F_\infty)\otimes V_{\rho_n}$ (where V_{ρ_n} is the vector space of ρ_n) by multiplying the term in $Y(E/F_\infty)$ by $X+1$, and the term in V_{ρ_n} by the above matrix. So if we take the H-coinvariants then we get a vector space over $\mathbb{Q}_p(\zeta)$ of dimension p^{n-1} and $\tilde{\gamma}$ acts by the above matrix because $1\otimes b_j$ is equivalent to $(X+1)\otimes\zeta^{\tilde{\gamma}^{j-1}}b_j$ where b_j is the jth basis vector of V_{ρ_n}, therefore we need to substitute $\zeta^{-\tilde{\gamma}^{j-1}}-1$ into X in the jth component. The result follows by Lemma 2.5.3. □

Applying the Artin-formalism for Akashi series (Theorem A.44. in [17], see also [6]) and Proposition 2.5.1 we get the following corollary.

Corollary 2.5.5. *Under the Hypotheses 1 and 2 and the second case of Proposition 2.5.2, the characteristic element of the* $X(E/\mathbb{Q}(\mu_p, \sqrt[p^n]{m})^{cyc})$ *is*

$$T\prod_{j=0}^{n-1}\Big((T+1)^{p^j}-1\Big)^{p-1}p^{p^n\mu_{E/K}}.$$

In particular if $g_{E/F_n}=r_{E/F_n}$ *then* $g_{E/\mathbb{Q}(\mu_p,\sqrt[p^n]{m})}=r_{E/\mathbb{Q}(\mu_p,\sqrt[p^n]{m})}=(p-1)n+1$, *the order of vanishing of the above expression at* $T=0$.

We will need the following rather technical lemmata for the proof of Proposition 2.5.8.

Lemma 2.5.6. *The element* $\tilde{\gamma}_0$ *acts by conjugation trivially on a power series* $h(X)\in\mathbb{Z}_p[\![X]\!]$ *modulo the ideal* $((X+1)^{p^k}-1)$ *if and only if it is in the form*

$$h(X)\equiv\sum_{i=0}^{k}a_i\frac{(X+1)^{p^k}-1}{(X+1)^{p^i}-1}\mod((X+1)^{p^k}-1),$$

where a_i *is in* $\mathbb{Z}_p$ *for each* $0\le i\le k$.

Proof. Since $\mathbb{Z}_p[\![X]\!]/((X+1)^{p^k}-1)$ is isomorphic to the group ring $\mathbb{Z}_p[H/H_k]$ and the image of $\frac{(X+1)^{p^k}-1}{(X+1)^{p^i}-1}$ in $\mathbb{Z}_p[H/H_k]$ is the sum of elements of order at most p^{k-i}, it follows that $\tilde{\gamma}_0$ acts trivially on these elements. The other direction is also true because if $\tilde{\gamma}_0$ acts trivially on some element in $\mathbb{Z}_p[H/H_k]$ then the coefficient of elements of the same order must be the same, so it

can be written in the required form, since the sum of elements of exact order p^{k-i} is $\frac{(X+1)^{p^k}-1}{(X+1)^{p^i}-1} - \frac{(X+1)^{p^k}-1}{(X+1)^{p^{i-1}}-1}$. □

Lemma 2.5.7. *If x_{k+1} is an element in $\mathbb{Z}_p[\zeta_{p^{k+1}}]$ such that it is congruent to 1 modulo the maximal ideal $(\zeta_{p^{k+1}}-1)$ and $x_{k+1}^{1-\tilde{\gamma}_0} \equiv 1 \pmod{(\zeta_{p^{k+1}}-1)^{p^k}}$ then it is congruent modulo $(\zeta_{p^{k+1}}-1)^{p^k}$ to an element in the form*

$$1 + \sum_{i=0}^{k-1} a_i (\zeta_{p^{k+1}}-1)^{p^k - p^i}$$

with a_i in $\{0,1,2,\ldots,p-1\}$ for $0 \leq i \leq k-1$.

Proof. At first note that the ring $\mathbb{Z}_p[\zeta_{p^{k+1}}]/(\zeta_{p^{k+1}}-1)^{p^k}$ is isomorphic to the group algebra $\mathbb{F}_p[C_{p^k}]$ of the cyclic group C_{p^k} of p^k elements since p is divisible by $(\zeta_{p^{k+1}}-1)^{p^k}$. Moreover, the induced action of $\tilde{\gamma}_0$ is the generator of the automorphism group $\mathrm{Aut}(C_{p^k}) \cong C_{p^{k+1}-p^k}$ as acting on $\mathbb{F}_p[C_{p^k}]$. The fixed points of this action are those elements in the group algebra in which the elements of C_{p^k} having the same order also have the same coefficient. These correspond to the elements described in the statement via the isomorphism

$$\mathbb{Z}_p[\zeta_{p^{k+1}}]/(\zeta_{p^{k+1}}-1)^{p^k} \cong \mathbb{F}_p[C_{p^k}].$$

□

The following proposition is a generalization of Hilbert's 'Satz 90' and plays an important role in determining the structure of $Y(E/F_\infty)$ as a $\Lambda(G)$-module.

Proposition 2.5.8. *For a formal power series $f_0(X) \in \mathbb{Z}_p[[X]]$ the following are equivalent.*

(i) $N_{\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p}(f_0(\zeta_{p^n}-1)) = 1$ for all $n \geq 0$ and ζ_{p^n} a primitive p^n-th root of unity and we have

$$f_0(X) f_0(1/(X+1)-1) = \hat{g}(X)^{1-\tilde{\gamma}_0}$$

for some $\hat{g}(X)$ in $1 + X\mathbb{Z}_p[[X]]$.

(ii) $f_0(X)$ *is in the form* $g_\infty(X)^{1-\tilde{\gamma}_0}$ *for some* $g_\infty(X) \in 1 + X\mathbb{Z}_p[\![X]\!]$.

Proof. The direction (ii)⇒(i) is trivial, since the norms of $g(\zeta_{p^n} - 1)$ and $g(\zeta_{p^n} - 1)^{\tilde{\gamma}_0}$ are the same and if $f_0(X)$ is in this form then so is the power series $f_0(X)f_0(1/(X+1)-1)$. For the other direction we are going to prove that for all $k \geq 0$ there exists a $g_k(X) \in 1 + X\mathbb{Z}_p[\![X]\!]$ such that

$$f_0(X) \equiv g_k(X)^{1-\tilde{\gamma}_0} \mod ((X+1)^{p^k} - 1). \tag{2.26}$$

The statement will follow from this, since the set of such g_k's for a given k is compact and the projective limit of compact spaces is nonempty. So there exists a limit g_∞ of such g_k's which is also in $1 + X\mathbb{Z}_p[\![X]\!]$. Let us remark here that g_∞ is unique because if $g_\infty^{1-\tilde{\gamma}_0} = h_\infty^{1-\tilde{\gamma}_0}$ then g_∞/h_∞ is fixed under the conjugation by $\tilde{\gamma}_0$, so it is constant, and the constant term of both g_∞ and h_∞ are 1 which means they are equal.

Now we prove (2.26) by induction on k. For $k = 0$ it is easy to see that the condition (i) implies that $f_0(0) = 1$ (applying (i) with $n = 0$), so $g_0 \equiv 1$ is good. Let us assume now that we know the statement for some fixed $k \geq 0$. So we may assume without loss of generality that $f_0(X) \equiv 1$ mod $((X+1)^{p^k} - 1)$ because $f_0(X)$ satisfies condition (i) if and only if so does $f_0(X)/g_k^{1-\tilde{\gamma}_0}$ (applying (ii)⇒(i)). Now we apply (i) for $n = k+1$. From Hilbert's Theorem 90 we get that there is an element x_{k+1} in $\mathbb{Z}_p[\mu_{p^{k+1}}]$ such that $x_{k+1}^{1-\tilde{\gamma}_0} = f_0(\zeta_{p^{k+1}}-1)$ and p does not divide x_{k+1} (because we can multiply x_{k+1} by any integer power of p and $x_{k+1}^{1-\tilde{\gamma}_0}$ does not change). It is obvious that there exists some $h_{k+1} \in \mathbb{Z}_p[\![X]\!]$ such that $h_{k+1}(\zeta_{p^{k+1}} - 1) = x_{k+1}$. Furthermore, we have that this $h_{k+1}(X)$ can be chosen in $1 + X\mathbb{Z}_p[\![X]\!]$. Indeed, by the second assumption of (i) we have

$$h_{k+1}(\zeta_{p^{k+1}} - 1)h_{k+1}(\zeta_{p^{k+1}}^{-1} - 1) = k_0\hat{g}(\zeta_{p^{k+1}} - 1),$$

for some k_0 in $\mathbb{Z}_p$ since their quotient is fixed by $\tilde{\gamma}_0$. Now the v_{k+1}-valuation of $h_{k+1}(\zeta_{p^{k+1}} - 1)$ and $h_{k+1}(\zeta_{p^{k+1}}^{-1} - 1)$ are the same, so this valuation must be divisible by $(p^{k+1} - p^k)/2$ because $\hat{g}(\zeta_{p^{k+1}} - 1)$ is a unit. On the other hand this valuation must be divisible by $p-1$ because otherwise $h_{k+1}(\zeta_{p^{k+1}} -$

$1)^{1-\tilde{\gamma}_0}$ would not be 1 modulo the maximal ideal. Therefore it is divisible by $p^{k+1}-p^k$, and dividing $h_{k+1}(\zeta_{p^{k+1}}-1)$ by a number in $\mathbb{Z}_p$ we can normalize it such that $h_{k+1}(0)$ equals 1. Now it is well-known and also easy to see that the ideal generated by

$$(X+1)^{p^k}-1 \text{ and } \frac{(X+1)^{p^{k+1}}-1}{(X+1)^{p^k}-1}$$

(the latter is the minimum polynomial of $\zeta_{p^{k+1}}$) is equal to the ideal generated by p and X^{p^k} in the power series ring $\mathbb{Z}_p[\![X]\!]$. This means that if two power series q_1 and q_2 in $\mathbb{Z}_p[\![X]\!]$ are equal modulo the ideal generated by p and X^{p^k} then by the Chinese Remainder Theorem there exists another power series q in $\mathbb{Z}_p[\![X]\!]$ such that q is congruent to q_1 modulo the ideal $((X+1)^{p^k}-1)$ and to q_2 modulo $(\frac{(X+1)^{p^{k+1}}-1}{(X+1)^{p^k}-1})$. Now if we apply Lemma 2.5.7 and notice that

$$\frac{(X+1)^{p^k}-1}{(X+1)^{p^i}-1} \equiv X^{p^k-p^i} \pmod{p}$$

we get that $h_{k+1}(X)$ is congruent modulo the ideal generated by p and X^{p^k} to some element in the form

$$1+\sum_{i=0}^{k-1} a_i \frac{(X+1)^{p^k}-1}{(X+1)^{p^i}-1}.$$

This means that there is a formal power series $g_{k+1}(X)$ in $\mathbb{Z}_p[\![X]\!]$ such that it is congruent to $h_{k+1}(X)$ modulo $(\frac{(X+1)^{p^{k+1}}-1}{(X+1)^{p^k}-1})$ and to some element in the form

$$\sum_{i=0}^{k} a_i \frac{(X+1)^{p^k}-1}{(X+1)^{p^i}-1}$$

modulo $((X+1)^{p^k}-1)$ which element is in fact fixed under the conjugation by $\tilde{\gamma}_0$ (see Lemma 2.5.6). Moreover, $g_{k+1}(X)$ is invertible because so is $h_{k+1}(X)$. In other words, by the choice of $h_{k+1}(X)$, and since $f_0(X)$ is congruent to 1 modulo $((X+1)^{p^k}-1)$ by inductive assumption, we have that $f_0(X)$ is congruent to $g_{k+1}(X)^{1-\tilde{\gamma}_0}$ both modulo $(\frac{(X+1)^{p^{k+1}}-1}{(X+1)^{p^k}-1})$ and modulo $((X+1)^{p^k}-$

1), ie. modulo $((X+1)^{p^{k+1}}-1)$. Now since $g_{k+1}(X)$ is invertible in $\mathbb{Z}_p[\![X]\!]$, we can normalize it by its constant term to get a required element. $\square$

Note that G_0 also acts on $Y(E/F_\infty)$, so the action of $\tilde{\gamma}$ is the $p-1$-st power of the action of $\tilde{\gamma}_0$ (we choose the topological generator γ_0 of Γ_0 such that its $p-1$-st power is γ). This means that if $p^{-l}(\tilde{\gamma}_0 p^l) = f_0(X)$ then

$$f(X) = \prod_{i=0}^{p-2} \tilde{\gamma}_0^i f_0(X) \tilde{\gamma}_0^{-i}.$$

This motivates the following Corollary.

Corollary 2.5.9. *For a formal power series $f(X) \in p^{-l}\mathbb{Z}_p[\![X]\!]$ the following are equivalent.*

(*i*) *It satisfies the condition* (2.25) *and is in the form*

$$f(X) = \prod_{i=0}^{p-2} \tilde{\gamma}_0^i f_0(X) \tilde{\gamma}_0^{-i}$$

for some $f_0(X) \in p^{-l}\mathbb{Z}_p[\![X]\!]$ satisfying

$$f_0(X) f_0(1/(X+1)-1) = \hat{g}(X)^{1-\tilde{\gamma}_0}$$

with a $\hat{g}(X)$ in $1+X\mathbb{Z}_p[\![X]\!]$.

(*ii*) *It is in $\mathbb{Z}_p[\![X]\!]$ and can be written in the form $g(X)^{1-\tilde{\gamma}}$ where $g(X)$ is in $1+X\mathbb{Z}_p[\![X]\!]$.*

Proof. For the direction $(ii) \Rightarrow (i)$ it is easy to see that $f_0(X) = g(X)^{1-\tilde{\gamma}_0}$ is suitable and by the remark after Lemma 2.5.3 $g(X)^{1-\tilde{\gamma}}$ satisfies the condition (2.25).

The other direction follows from Proposition 2.5.8 once we note that the condition (2.25) implies that both $f(X)$ and $f_0(X)$ are integral since if we substitute any number in the form $(\zeta_{p^n}-1)$ into them we get numbers with norm 1 in some extension (by the remark after Lemma 2.5.3), so they are integral. Now if $f(X)$ (or similarly $f_0(X)$) was not integral then we take the

first index i such that the ith coefficient has the least (negative) p-valuation and get that $f(\zeta_{p^n}-1)$ would not be integral for n such that p^n-p^{n-1} (the valuation of p in $\mathbb{Z}_p[\zeta_{p^n}]$) is greater than i. □

Theorem 2.5.10. *Under the Hypotheses 1 and 2 and the second case of Proposition 2.5.2, $Y(E/F_\infty)$ is a finite index submodule of*

$$\Lambda(G)/\Lambda(G)(\tilde{\gamma}-1)$$

as a $\Lambda(G)$-module, which means that they represent the same element in the Grothendieck group $K_0(\mathfrak{M}_H(G))$. The characteristic elements of $Y(E/F_\infty)$ and $X(E/F_\infty)$ are $Y=\tilde{\gamma}-1$ and $Yp^{\mu_{E/K}}$, respectively, considered as elements of $K_1(\Lambda(G)_{S^*})$.

Proof. Since $f(X)$ is integral we can extend the action of G to the whole $\mathbb{Z}_p[\![X]\!]$ as $\tilde{\gamma}f_1(X) = (\tilde{\gamma}f_1(X)\tilde{\gamma}^{-1})f(X)$. We would like to use Corollary 2.5.9. The action of G extends to an action of G_0, and by the second remark after Theorem 2.2.2 we get a homomorphism from $X(E/F_\infty)$ to $a^1_{\Lambda(G_0)}(X(E/F_\infty)^\#)$ with finite kernel and cokernel. This means that there is a morphism

$$\Lambda(G_0)/\Lambda(G_0)(\tilde{\gamma}_0-f_0(X)) \to \Lambda(G_0)/\Lambda(G_0)(\tilde{\gamma}_0^{-1}-f_0(1/(X+1)-1)) \quad (2.27)$$

with finite kernel and cokernel. Therefore there is an element $\hat{g}_0(X)$ in

$$\Lambda(G_0)/\Lambda(G_0)(\tilde{\gamma}_0^{-1}-f_0(1/(X+1)-1))$$

such that $\tilde{\gamma}_0$ multiplies it to its $f_0(X)$-times. Indeed, $\hat{g}_0(X)$ is the image of 1 under the map (2.27). Moreover, since the cokernel of this morphism is finite, $\hat{g}_0(X)$ must be an invertible power series when identifying

$$\Lambda(G_0)/\Lambda(G_0)(\tilde{\gamma}_0^{-1}-f_0(1/(X+1)-1))$$

with $\mathbb{Z}_p[\![X]\!]$ as a $\Lambda(H)$-module (there are no finite index *principal* ideals in

$\mathbb{Z}_p[\![X]\!]$ other than $\mathbb{Z}_p[\![X]\!]$ itself). This means that

$$\begin{aligned} f_0(X)\hat{g}_0(X) &= (\tilde{\gamma}_0\hat{g}_0(X)\tilde{\gamma}_0^{-1})\cdot(\tilde{\gamma}_0 1), \text{ and} && (2.28)\\ \tilde{\gamma}_0^{-1}1 &= f(1/(X+1)-1). && (2.29)\end{aligned}$$

Applying $\tilde{\gamma}_0$ on (2.29) we get

$$\begin{aligned} 1 &= \tilde{\gamma}_0 f(1/(X+1)-1)\tilde{\gamma}_0^{-1}\cdot(\tilde{\gamma}_0 1)\\ \tilde{\gamma}_0 1 &= \tilde{\gamma}_0 f(1/(X+1)-1)^{-1}\tilde{\gamma}_0^{-1} && (2.30)\end{aligned}$$

and substituting (2.30) into (2.28) we have

$$\begin{aligned} \hat{g}(X)^{1-\tilde{\gamma}_0} &= f_0(X)f_0(1/(X+1)-1) \text{ with}\\ \hat{g}(X) &= \hat{g}_0(X)^{-1}f_0(1/(X+1)-1).\end{aligned}$$

Lemma 2.5.3 implies the equation for the formal power series $f(X)$, therefore the assumption (i) in Corollary 2.5.9 is satisfied, ie. so is (ii). Now if we apply the automorphism of the $\Lambda(H)$-module $\mathbb{Z}_p[\![X]\!]$ which sends 1 to $g(X)$ we get that $Y(E/F_\infty)$ is pseudo-isomorphic to the module $\mathbb{Z}_p[\![X]\!]$ on which $\tilde{\gamma}$ acts by conjugation. This module is clearly isomorphic to $\Lambda(G)/\Lambda(G)(\tilde{\gamma}-1)$. □

We can also determine the characteristic element of $Y(E/F_\infty)$ as a $\Lambda(G_0)$-module.

Corollary 2.5.11. *Under the Hypotheses 1 and 2 and the second case of Proposition 2.5.2, $Y(E/F_\infty)$ is a finite index submodule of*

$$\Lambda(G_0)/\Lambda(G_0)(\tilde{\gamma}_0-\alpha)$$

as a $\Lambda(G_0)$-module, where $\tilde{\gamma}_0$ is a lift of the topological generator γ_0 of Γ_0 to G_0 such that $\tilde{\gamma}=\tilde{\gamma}_0^{p-1}$ and α is -1 if the $\mathbb{Z}_p$-corank of the p^∞-Selmer group over $\mathbb{Q}$ is 0, and $+1$ if this rank is 1. So they represent the same element in the Grothendieck group $K_0(\mathfrak{M}_{H_0}(G_0))$. The characteristic element of $Y(E/F_\infty)$ is $\tilde{\gamma}_0-\alpha$ considered as an element of $K_1(\Lambda(G_0)_{S^*})$.

Proof. Note that the topological generator $\tilde{\gamma}_0$ of G_0 commute with $\tilde{\gamma}$, so this element can only act by multiplying by a constant on the power series identically 1 in $\mathbb{Z}_p[\![X]\!] = \Lambda(H)$ because the image is fixed by the action of $\tilde{\gamma}$ and this element fixes only the constant power series in this module. This constant α is forced to be of order dividing $p-1$, since $\tilde{\gamma}_0^{p-1}$ acts trivially. Moreover, the restriction map

$$H_0(\mathrm{Gal}(\mathbb{Q}(\mu_p, \sqrt[p^n]{m})^{cyc}/\mathbb{Q}(\sqrt[p^n]{m})^{cyc}), Y(E/\mathbb{Q}(\mu_p, \sqrt[p^n]{m}))) \to Y(E/\mathbb{Q}(\sqrt[p^n]{m}))$$

has finite kernel and cokernel [6, 25], so it can be easily seen that for any intermediate field $\mathbb{Q} \leq k \leq \mathbb{Q}(\mu_p)$ the characteristic power series is

$$T^{\varepsilon_k} \prod_{j=0}^{n-1} \left((T+1)^{p^j} - 1 \right)$$

for the module $Y(E/k(\sqrt[p^n]{m})^{cyc})$ where $\varepsilon_k = 1$ if the order of α divides the degree of k over $\mathbb{Q}$ and $\varepsilon_k = 0$ otherwise. On the other hand ε_k equals the rank of the p^∞-Selmer group over the field k. Since the parity conjecture is known in this case [28], $\varepsilon_k \equiv r_{E/k}$ modulo 2. Now the root number for any elliptic curve with good reduction at p is the same over $\mathbb{Q}(\mu_p)$ and over the unique quadratic field contained in it [16], so the p^∞-Selmer rank over this quadratic field must be 1, too, which means that α has order at most 2. □

Remark. It can be seen from the proof of the above corollary that in fact the $\Lambda(G)$-structure of a module M determines the $\Lambda(G_0)$ structure up to a constant in $\mathbb{Z}_p^\times$ of finite order whenever the module M is free of rank 1 over $\Lambda(H)$.

The functional equation. We obtain the following functional equation for the characteristic element of $X(E/F_\infty)$, as conjectured in [6], by applying the automorphism # (see section 1.2.2 for the definition) and noting that $\alpha = \pm 1$.

$$(p^{\mu_{E/K}}(\tilde{\gamma}_0 - \alpha))^\# = -\tilde{\gamma}_0^{-1} p^{\mu_{E/K}}(\tilde{\gamma}_0 - \alpha)\alpha^{-1}.$$

The sign of the functional equation is negative if and only if α is $+1$, or in other words the analytic rank of E over $\mathbb{Q}$ is odd. So the sign in this

functional equation is equal to the sign in the functional equation of the complex L-function of E over $\mathbb{Q}$, since the parity conjecture is known in this case [28].

Example. It is not easy to verify that $X(E/K^{cyc})$ is a free $\mathbb{Z}_p$-module of rank 1. However, C. Wuthrich has shown that the elliptic curve $79A1$ of Cremona's tables given by the equation

$$y^2 + xy + y = x^3 + x^2 - 2x$$

satisfies the conditions of the second case of Proposition 2.5.2 with $m = q = 79$ and $p = 3$. Moreover, in this case $P = (0,0) \in \mathbb{Q}^2$ is the generator of $E(K^{cyc})$, so $X(E/\mathbb{Q}^{cyc})$ is also a free $\mathbb{Z}_3$-module of rank 1. This means that in this case the characteristic element of the dual Selmer group $X(E/F_\infty)$ as a $\Lambda(G_0)$-module is $\tilde{\gamma}_0 - 1$ viewed as an element of $K_1(\Lambda(G_0)_{S^*})$.

2.5.2 The non-classical case

In this section we assume the first case of Proposition 2.5.2. Then we have $g_{E/F_n} \leq p^n - 1 \leq r_{E/F_n}$. Moreover, the characteristic power series for $Y(E/F_n^{cyc})$ is T^{p^n-1} for all $n \geq 1$ [6]. If, in addition, E has a prime conductor, Darmon and Tian [14] have some results in this direction, too. As in the previous section we can identify $Y(E/F_\infty)$ with a finite index submodule of $\Lambda(H) \cong \mathbb{Z}_p[\![X]\!]$ as a $\Lambda(H)$-module. So we can define $f(X)$ similarly, ie. $f(X) = p^{-l}\tilde{\gamma}p^l$ if $p^l \in Y(E/F_\infty) \leq \mathbb{Z}_p[\![X]\!]$.

Lemma 2.5.12. *Under the Hypotheses 1 and 2 and the first case of Proposition 2.5.2, the following functional equation holds:*

$$\prod_{j=0}^{p^{n-1}-1} f(\zeta_{p^n}^{1+jp} - 1) \;=\; 1, \tag{2.31}$$

where ζ_{p^n} is an arbitrary primitive p^nth root of unity ($n \geq 1$ integer). In particular $f(\zeta_p - 1) = 1$, but $f(0)$ is not necessarily 1, we only know that $f(0) \equiv 1 \pmod{p}$.

Proof. As in the previous section we know that

$$\prod_{j=0}^{p^{n-1}-1} f(\zeta_{p^n}^{1+jp}-1)$$

is an eigenvalue of $\tilde{\gamma}^{p^{n-1}}|_{Y(E/F_\infty)_{H_n}\otimes\mathbb{Q}_p}$ and that $\tilde{\gamma}^{p^{n-1}}$ has the unique eigenvalue 1 when acting on $Y(E/F_n^{cyc})\otimes\mathbb{Q}_p$, but the restriction homomorphism from $Y(E/F_\infty)_{H_n}$ to $Y(E/F_n^{cyc})$ does have a kernel of rank 1 over $\mathbb{Z}_p$. So the multiplicity of the eigenvalue 1 of $\tilde{\gamma}^{p^{n-1}}|_{Y(E/F_\infty)_{H_n}\otimes\mathbb{Q}_p}$ is at least p^n-1. On the other hand, the numbers

$$\prod_{j=0}^{p^{n-1}-1} f(\zeta^{1+jp}-1)$$

are eigenvalues of $\tilde{\gamma}^{p^{n-1}}|_{Y(E/F_\infty)_{H_n}\otimes\mathbb{Q}_p}$ for any ζ not necessarily primitive p^n-th root of unity as shown in the proof of Lemma 2.5.3. So at least all but one of these numbers are 1 and if this expression is 1 for some *primitive* p^kth root of unity then it is also 1 for all the other primitive p^k-th roots of unity ($1\leq k\leq n$). So the exception can only be the first root of unity 1 and the result follows. □

Proposition 2.5.13. *If $f(X)\in p^{-l}\mathbb{Z}_p[\![X]\!]$ is a formal power series in the form*

$$f(X)=\prod_{i=0}^{p-2}\tilde{\gamma}_0^i f_0(X)\tilde{\gamma}_0^{-i}$$

for some $f_0(X)\in p^{-l}\mathbb{Z}_p[\![X]\!]$ satisfying $f(0)=\chi(\tilde{\gamma})$ and

$$f_0(X)f_0(1/(X+1)-1)=\hat{g}(X)^{1-\tilde{\gamma}_0}\left(\frac{(X+1)^{\chi(\tilde{\gamma}_0)}-1}{X}\right)^2 \tag{2.32}$$

with a $\hat{g}(X)$ in $1+X\mathbb{Z}_p[\![X]\!]$ then the following are equivalent.

(*i*) *It satisfies the condition* (2.31).

(*ii*) *It is in* $\mathbb{Z}_p[\![X]\!]$ *and can be written in the form*

$$f(X) = g(X)^{1-\tilde{\gamma}} \frac{(1+X)^{\chi(\tilde{\gamma})} - 1}{X},$$

where $g(X) \in 1 + X\mathbb{Z}_p[\![X]\!]$.

Proof. It is easy to check that

$$N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_p)} \left(\frac{\zeta_{p^n}^{\chi(\tilde{\gamma})} - 1}{\zeta_{p^n} - 1} \right) = \frac{N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_p)} \left(\zeta_{p^n}^{\chi(\tilde{\gamma})} - 1 \right)}{N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_p)} \left(\zeta_{p^n} - 1 \right)} = 1,$$

hence a function in the form

$$g(X)^{1-\tilde{\gamma}} \frac{(1+X)^{\chi(\tilde{\gamma})} - 1}{X}$$

satisfies the condition (2.31). Moreover, $\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}|_{X=0} = \chi(\tilde{\gamma}) = f(0)$, so

$$f(X) \left(\frac{(1+X)^{\chi(\tilde{\gamma})} - 1}{X}|_{X=0} \right)^{-1}$$

satisfies the condition (i) in Corollary 2.5.9 because

$$\begin{aligned} \prod_{i=0}^{p-2} \tilde{\gamma}_0^i \frac{(X+1)^{\chi(\gamma_0)} - 1}{X} \tilde{\gamma}_0^{-i} &= \frac{(1+X)^{\chi(\tilde{\gamma})} - 1}{X}, \quad \text{and} \\ \frac{(1+X)^{\chi(\tilde{\gamma})} - 1}{X} \frac{1/(1+X)^{\chi(\tilde{\gamma})} - 1}{1/(X+1) - 1} &= \left(\frac{(X+1)^{\chi(\tilde{\gamma}_0)} - 1}{X} \right)^2 (X+1)^{1-\tilde{\gamma}_0}, \end{aligned}$$

hence it can be expressed in the form $g(X)^{1-\tilde{\gamma}}$. □

One gets the following Theorem the same way as Theorem 2.5.10.

Theorem 2.5.14. *Under the Hypotheses 1 and 2 and the first case of Proposition 2.5.2* $Y(E/F_\infty)$ *is a finite index submodule of*

$$\Lambda(G) \Big/ \Lambda(G) \left(\tilde{\gamma} - \frac{(1+X)^{\chi(\tilde{\gamma})} - 1}{X} \right)$$

as a $\Lambda(G)$-module, which means that they represent the same element in the Grothendieck group $K_0(\mathfrak{M}_H(G))$. The characteristic elements of $Y(E/F_\infty)$ and $X(E/F_\infty)$ are

$$\begin{aligned} Y+1-\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X} &= \tilde{\gamma}-\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X} \text{ and} \\ p^{\mu_{E/K}}\left(Y+1-\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}\right) &= p^{\mu_{E/K}}\left(\tilde{\gamma}-\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}\right), \end{aligned}$$

respectively, considered as elements of $K_1(\Lambda(G)_{S^*})$.

Proof. We would like to apply Proposition 2.5.13. The condition (2.32) follows from the existence of the map

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

with trivial kernel, and cokernel killed by X^2 (We use Theorem 2.2.2 and the fact there is only one prime in P_1 and P_2 is empty, and the local Tate module is killed by X^2 for this split multiplicative prime). So we only have to show that $f(0) = \chi(\tilde{\gamma})$ in this case. Since now we have a prime of split multiplicative reduction for E ramifying infinitely in this false Tate curve extension, it follows from the proof of Proposition 2.2.1 that the kernel of the corestriction homomorphism

$$Y(E/F_\infty)_H \to Y(E/K^{cyc})$$

is the Pontryagin dual of $\mathbb{Q}_p/\mathbb{Z}_p(-1)$ up to a finite module, so its characteristic element is $T+1-\chi(\gamma)$ where χ is the cyclotomic character. Furthermore, as we saw in the proof of Lemma 2.5.3, $f(0)$ is an eigenvalue of $\tilde{\gamma}|_{Y(E/F_\infty)_H}$, so $f(0) = \chi(\tilde{\gamma})$. □

Proposition 2.5.4 remains unchanged in this case. However, its corollary is a bit different from the one in Section 2.5.1 because in this case $X(E/K^{cyc})$ has rank zero. By applying the Artin-formalism for Akashi-series we get the following analogue of Corollary 2.5.5.

Corollary 2.5.15. *Under the Hypotheses 1 and 2 and the first case of Proposition 2.5.2, the characteristic element of the* Γ*-module* $X(E/\mathbb{Q}(\mu_p, \sqrt[p^n]{m})^{cyc})$ *is*

$$p^{p^n \mu_{E/K}} \prod_{j=0}^{n-1} \left((T+1)^{p^j} - 1\right)^{p-1}.$$

In particular if $g_{E/F_n} = r_{E/F_n}$ *then* $g_{E/\mathbb{Q}(\mu_p, \sqrt[p^n]{m})} = r_{E/\mathbb{Q}(\mu_p, \sqrt[p^n]{m})} = (p-1)n$*, the order of vanishing of the above formula at* $T = 0$*.*

Remark. A similar computation shows that assuming the standing hypotheses for this curve the characteristic element of $Y(E/\mathbb{Q}(\sqrt[p^n]{m})^{cyc})$ is

$$\prod_{j=0}^{n-1} \left((T+1)^{p^j} - 1\right).$$

As in the previous section if one looks at the possible actions of the elements of order $p-1$ of G_0 on $Y(E/F_\infty)$, one gets the following corollary.

Corollary 2.5.16. *Under the Hypotheses 1 and 2 and the first case of Proposition 2.5.2,* $Y(E/F_\infty)$ *is a finite index submodule of*

$$\Lambda(G_\mathbb{Q}) \Big/ \Lambda(G_\mathbb{Q}) \left(\tilde{\gamma}_0 - \frac{(X+1)^{\chi(\gamma_0)} - 1}{X}\right)$$

as a $\Lambda(G_\mathbb{Q})$*-module, where* $\tilde{\gamma}_0$ *is a lift of the topological generator* γ_0 *of* Γ_0 *to* $G_\mathbb{Q}$*, and* χ *is the cyclotomic character. So they represent the same element in the Grothendieck group* $K_0(\mathfrak{M}_{H_\mathbb{Q}}(G_\mathbb{Q}))$*. The characteristic element of* $Y(E/F_\infty)$ *is*

$$\tilde{\gamma}_0 - \frac{(X+1)^{\chi(\gamma_0)} - 1}{X}$$

considered as an element of $K_1(\Lambda(G_\mathbb{Q})_{S^*_\mathbb{Q}})$*.*

Proof. By comparing the action of $\tilde{\gamma}_0^{p-1}$ and $\tilde{\gamma}$ it is easy to see that the characteristic element is in the form

$$\tilde{\gamma}_0 - \alpha \frac{(X+1)^{\chi(\gamma_0)} - 1}{X},$$

where α is an element of finite order in $\mathbb{Z}_p^\times$. The constant α can also be determined in the following way. It is easy to see that if $\mathbb{Q} \leq k \leq \mathbb{Q}(\mu_p)$ is any intermediate field then the homology group

$$H_0(\mathrm{Gal}(F_\infty/k^{cyc}), X(E/F_\infty))$$

has rank 1 over $\mathbb{Z}_p$ if the order of $\alpha\chi(\gamma_0)$ modulo p divides the degree of k over $\mathbb{Q}$, and rank 0 otherwise. On the other hand, the short exact sequence

$$0 \to \mu_{p^\infty} \to E[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

and a little Kummer theory shows [6] that the restriction map from the above homology group to the cyclotomic Selmer group $X(E/k^{cyc})$ has infinite kernel if and only if the group μ_{p^∞} is contained in the multiplicative group of the localized field k_w^{cyc} at a prime w above q in k^{cyc}, where q is the unique prime dividing m in P_2. So $\alpha\chi(\gamma_0)$ and q have the same order modulo p, since $X(E/k^{cyc})$ has rank 0. Now q is a primitive root modulo p, since it is inert in $\mathbb{Q}(\mu_p)$. This means α can always be chosen 1. □

The functional equation. As in the previous section we can deduce some sort of functional equation for the characteristic element of the dual Selmer group $X(E/F_\infty)$. The only difference is that the characteristic element in this case is not fixed by the automorphism # modulo the image of $K_1(\Lambda(G))$ which means that the modules $X(E/F_\infty)$ and $\mathrm{Ext}^1_{\Lambda(G)}(X(E/F_\infty)^\#, \Lambda(G))$ do not represent the same element in the Grothendieck group $K_0(\mathfrak{M}_H(G))$. However, they are still pseudo-isomorphic and the characteristic elements are conjugates under the action of $(\Lambda(H)_R)^\times$. The functional equation is the following

$$p^{\mu_{E/K}} \left(\tilde{\gamma}_0 - \frac{(X+1)^{\chi(\gamma_0)} - 1}{X} \right)^\# = \tag{2.33}$$

$$= -\frac{X}{(X+1)^{\chi(\gamma_0)} - 1} \left(\frac{X+1}{X^2} p^{\mu_{E/K}} \left(\tilde{\gamma}_0 - \frac{(X+1)^{\chi(\gamma_0)} - 1}{X} \right) \frac{X^2}{X+1} \right) \tilde{\gamma}_0^{-1}$$

This means that the sign is negative as in the functional equation for the complex L-function of curve the curve twisted by the representations ρ_n, ie.

by all but finitely many self-dual irreducible Artin representations of the false Tate curve extension.

Proof of the equation (2.33). The right hand side of (2.33) equals

$$
\begin{aligned}
-p^{\mu_{E/K}}\left(\frac{X}{(X+1)^{\chi(\gamma_0)}-1}\frac{X+1}{X^2}\tilde{\gamma}_0\frac{X^2}{X+1}\tilde{\gamma}_0^{-1}-\tilde{\gamma}_0^{-1}\right)=\\
=p^{\mu_{E/K}}\left(\tilde{\gamma}_0^{-1}-\frac{X}{(X+1)^{\chi(\gamma_0)}-1}\frac{X+1}{X^2}\left(\tilde{\gamma}_0\frac{X^2}{X+1}\tilde{\gamma}_0^{-1}\right)\right)=\\
=p^{\mu_{E/K}}\left(\tilde{\gamma}_0^{-1}-\frac{X}{(X+1)^{\chi(\gamma_0)}-1}\frac{X+1}{X^2}\frac{\left((X+1)^{\chi(\gamma_0)}-1\right)^2}{(X+1)^{\chi(\gamma_0)}}\right)=\\
=p^{\mu_{E/K}}\left(\tilde{\gamma}_0^{-1}-\frac{(X+1)^{\chi(\gamma_0)}-1}{X}\frac{X+1}{(X+1)^{\chi(\gamma_0)}}\right)=\\
=p^{\mu_{E/K}}\left(\tilde{\gamma}_0^{-1}-\frac{\frac{1}{(X+1)^{\chi(\gamma_0)}}-1}{\frac{1}{X+1}-1}\right)=\\
=p^{\mu_{E/K}}\left(\tilde{\gamma}_0-\frac{(X+1)^{\chi(\gamma_0)}-1}{X}\right)^{\#}. \qquad (2.34)
\end{aligned}
$$

□

This above form of the functional equation of the characteristic element is what we get from section 2.1.3. However, we can formulate another form of the functional equation in terms of section 2.2 which is more useful for the analytic connections.

$$
\begin{aligned}
p^{\mu_{E/K}}\left(\tilde{\gamma}_0-\frac{(X+1)^{\chi(\gamma_0)}-1}{X}\right)^{\#}=\\
=p^{\mu_{E/K}}\left(\tilde{\gamma}_0-\frac{(X+1)^{\chi(\gamma_0)}-1}{X}\right)\frac{\mathrm{Frob}_q^{-1}-\frac{(X+1)^{-q}-1}{\frac{1}{X+1}-1}}{\mathrm{Frob}_q-\frac{(X+1)^q-1}{X}}.
\end{aligned}
$$

Indeed, we may choose $\tilde{\gamma}_0$ to be Frob_q because q is inert in the field K (hence so is in K^{cyc}), and ramifies totally in F_∞/K^{cyc}, so its decomposition subgroup is the whole Galois group $\mathrm{Gal}(F_\infty/\mathbb{Q})=G_0$. Moreover, $\chi(\mathrm{Frob}_q)=q$.

We end this section by giving a numerical example illustrating our results.

Example. Take the elliptic curve $E = 17A1$ given by the equation

$$y^2 + xy + y = x^3 - x^2 - x - 14.$$

This has good ordinary reduction at the prime $p = 7$ and the calculations in [17] show that it satisfies the conditions in the first case of Proposition 2.5.2 with $m = q = 17$. Since 17 is a primitive root modulo 7, in Corollary 2.5.16 α equals 1. This means that the characteristic element of the dual Selmer group $X(E/F_\infty)$ of this curve is

$$\tilde{\gamma}_0 - \frac{(X+1)^{\chi(\gamma_0)} - 1}{X}$$

as an element of $K_1(\Lambda(G_0)_{S^*})$, since the μ-invariant vanishes.

2.6 On Vogel's counterexample

Coates, Schneider and Sujatha proved [10] that for any finitely generated torsion $\Lambda(G)$-module M there exist reflexive left ideals of $\Lambda(G)$ and a $\Lambda(G)$-injection

$$\bigoplus_{i=1}^{r} \Lambda(G)/L_i \to M/M_0$$

with pseudo-null cokernel, where M_0 is the maximal pseudo-null submodule of M. They asked whether the reflexive left ideals can always be chosen principal. In the appendix of [39] there is an example of a nonprincipal reflexive left ideal of $\Lambda(G)$. That ideal was

$$L = \Lambda(G)\left(Q(G)\left(Y + 1 - \frac{(X+1)^{1+p} - 1 - p}{X - p}\right) \cap \Lambda(G)\right),$$

where $Q(G)$ denotes the formal skew power series ring (with the same ring-automorphism and derivation as in $\Lambda(G)$) over the field of fractions of $\Lambda(H)$. It is shown in the Appendix of [39] that L contains a (skew) polynomial of degree 2 in the variable Y. So $\Lambda(G)/L$ is generated by the elements $(1 + L)$

and $(Y+1+L)$ over $\Lambda(H)$. Moreover, the relation

$$(X-p)(Y+1+L) = \left((X+1)^{1+p}-1-p\right)(1+L)$$

is satisfied, therefore the map

$$\begin{aligned} \psi \,:\, \Lambda(G)/L &\to \mathbb{Z}_p[\![X]\!] \\ Y+1+L &\mapsto (X+1)^{1+p}-1-p \\ 1+L &\mapsto X-p \end{aligned}$$

is an injective $\Lambda(H)$-homomorphism with a cokernel of order p. It is easy to see that $(X-p)$ divides $((X+1)^{1+p}-(1+p)^{1+p})$ in $\mathbb{Z}_p[\![X]\!]$, so

$$\psi\left(\frac{(X+1)^{1+p}-(1+p)^{1+p}}{X-p}(1+L)-(Y+1+L)\right) = 1+p-(1+p)^{1+p}.$$

Further,

$$\begin{aligned} (Y+1)\left(\frac{(X+1)^{1+p}-(1+p)^{1+p}}{X-p}-Y-1\right)+ \\ +Y+1-\frac{(X+1)^{1+p}-(1+p)^{1+p}}{X-p} = \\ = -\left(Y+1-\frac{(X+1)^{1+p}-(1+p)^{1+p}}{(X+1)^{1+p}-1-p}\right)\times \\ \times\left(Y+1-\frac{(X+1)^{1+p}-1-p}{X-p}\right)\in L, \end{aligned}$$

which means that if we push out the action of $\Lambda(G)$ to $\mathbb{Z}_p[\![X]\!]$ via the map ψ then

$$(Y+1)(1+p-(1+p)^{1+p}) = 1+p-(1+p)^{1+p},$$

which means $\mathbb{Z}_p[\![X]\!]$ with this action is isomorphic to the module $\Lambda(G)/Y$. So there exists an injective $\Lambda(G)$-homomorphism with finite cokernel between $\Lambda(G)/L$ and $\Lambda(G)/Y$ and the characteristic element of $\Lambda(G)/L$ is Y viewed as an element of $K_1(\Lambda(G)_{S^*})$.

This means that there is still a hope that all $\Lambda(G)$-modules are pseudo-

isomorphic to the direct sum of quotients of $\Lambda(G)$ by principal ideals.

Chapter 3

The GL_2-extension

In this chapter we are going to deal with the GL_2-extension associated to elliptic curves.

Let E be an elliptic curve defined over $\mathbb{Q}$ and without complex multiplication, and $E[p^\infty]$ the group of all p-power division points on E. We define

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

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

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

By a classical result of Serre [34], G can be identified with an open subgroup of

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

as E does not admit complex multiplication.

3.1 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 3.1.1. *Let H be an open subgroup of the group*

$$\hat{H} = \{A \in \mathrm{GL}_2(\mathbb{Z}_p) \mid \det(A)^{p-1} = 1\}.$$

Then all finite $\Omega(H)$-modules represent the trivial element in the category $K_0(\Omega(H))$.

Proof. This follows from Theorem B in [2] as all the p-regular elements have centralizers of dimension at least 1 in H. □

Now we can state the main result of this section.

Proposition 3.1.2. *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-torsion part is finite and so represent the trivial element in $K_0(\mathfrak{M}_H(G))$. Moreover, we may also assume that M is isomorphic to $\mathbb{Z}_p$ with the trivial G-action on it, since we can take the tensor product of exact sequences with M over $\mathbb{Z}_p$ and it remains exact since M is a finitely generated free $\mathbb{Z}_p$-module. We can make the tensor products $\Lambda(G)$-modules by the diagonal action and we get that M is also trivial in $K_0(\mathfrak{M}_H(G))$.

Since G acts trivially on $\mathbb{Z}_p$, it suffices to prove that $\mathbb{Z}_p$ represents the trivial element in $K_0(\Lambda(\hat{H}))$ because if we take the projective resolution of $\mathbb{Z}_p$ as a $\Lambda(\hat{H})$-module, then we can extend the action of $\hat{H}$ to an action of $\mathrm{GL}_2(\mathbb{Z}_p)$ to the whole projective resolution of $\mathbb{Z}_p$ by taking the trivial action of $\hat{\Gamma} = \mathrm{GL}_2(\mathbb{Z}_p)/\hat{H}$. This works because we have

$$\mathrm{GL}_2(\mathbb{Z}_p) \cong \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p) \mid a \in 1 + p\mathbb{Z}_p \right\} \times \hat{H}.$$

Now the map from $K_0(\Lambda(\hat{H}))$ to $K_0(\Omega(\hat{H}))$ sending a projective $\Lambda(\hat{H})$-module P to the projective $\Omega(\hat{H})$-module P/pP is an isomorphism (since

the ideal generated by p is contained in the Jacobson radical of $\Lambda(\hat{H})$). $\mathbb{Z}_p$ is p-torsion free, therefore the class of $\mathbb{Z}_p$ maps to $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ under this map and we are done by lemma 3.1.1. □

3.2 Pairings

In this section we are going to construct a pairing map

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

The method used is similar to the one in section 2.2. For this we will need the following lemma which is a slight generalization of Proposition 1.3.1 of Perrin-Riou [29] to this non-commutative situation.

Lemma 3.2.1. *If the $\Lambda(G)$-module M lies in $\mathfrak{M}_H(G)$ then we have*

$$\mathrm{Ext}^1_{\Lambda(G)}(M, \Lambda(G)) \cong \varprojlim_L \mathrm{Ext}^1_{\Lambda(\Gamma_L)}(H_0(H_L, M), \Lambda(\Gamma_L))$$

where L runs through the finite Galois subextensions of F_∞, H_L is the Galois group $\mathrm{Gal}(F_\infty/L^{cyc})$*, and Γ_L equals* $\mathrm{Gal}(L^{cyc}/L)$.

Proof. It is a theorem of Jannsen [26] that since Γ_L is a finite index subgroup of $\Gamma_L^* := \mathrm{Gal}(L^{cyc}/\mathbb{Q})$ we have

$$\mathrm{Ext}^i_{\Lambda(\Gamma_L)}(M, \Lambda(\Gamma_L)) \cong \mathrm{Ext}^i_{\Lambda(\Gamma_L^*)}(M, \Lambda(\Gamma_L^*)).$$

Now since M is in $\mathfrak{M}_H(G)$ we have a long exact sequence

$$\begin{aligned} 0 \to \mathrm{Ext}^1_{\Lambda(G)}(M, I_L) \to \mathrm{Ext}^1_{\Lambda(G)}(M, \Lambda(G)) \to \\ \to \mathrm{Ext}^1_{\Lambda(G)}(M, \Lambda(\Gamma_L^*)) \to \mathrm{Ext}^2_{\Lambda(G)}(M, I_L) \to \cdots \end{aligned}$$

induced by the natural surjection

$$\Lambda(G) \to \Lambda(\Gamma_L^*)$$

with kernel $I_L \lhd \Lambda(G)$. Now the projective limit of $\mathrm{Ext}^i_{\Lambda(G)}(M, I_L)$ is trivial for $i = 1, 2$ since if l is any fixed element in I_L and $L \subset L'$ large enough then l is not in the image of the map

$$I_{L'} \hookrightarrow I_L.$$

So we obtain

$$\mathrm{Ext}^1_{\Lambda(G)}(M, \Lambda(G)) \cong \varprojlim_L \mathrm{Ext}^1_{\Lambda(G)}(M, \Lambda(\Gamma_L^*)). \tag{3.1}$$

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

$$0 \to M_1 \to P \to M \to 0, \text{ and}$$
$$0 \to M_2 \to H_0(H_L, P) \to H_0(H_L, M) \to 0.$$

Then by definition of M_2 we have a short exact sequence

$$0 \to H_1(H_L, M) \to H_0(H_L, M_1) \to M_2 \to 0.$$

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

$$\mathrm{Hom}_{\Lambda(G)}(N, \Lambda(\Gamma_L^*)) = \mathrm{Hom}_{\Lambda(\Gamma_L^*)}(H_0(H_L, N), \Lambda(\Gamma_L^*)).$$

So we have the following commutative diagram with exact rows and columns

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 & & a^0_{\Lambda(\Gamma_L^*)}(M_{H_L}) & = & \mathrm{Hom}_G(M, \Lambda(\Gamma_L^*)) & & \\
 & & \downarrow & & \downarrow & & \\
 & & a^0_{\Lambda(\Gamma_L^*)}(P_{H_L}) & = & \mathrm{Hom}_G(P, \Lambda(\Gamma_L^*)) & & \\
 & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & a^0_{\Lambda(\Gamma_L^*)}(M_2) & \longrightarrow & \mathrm{Hom}_G(M_1, \Lambda(\Gamma_L^*)) & \longrightarrow & a^0_{\Lambda(\Gamma_L^*)}(H_1(H_L, M)) \\
 & & \downarrow & & \downarrow & & \\
 & & a^1_{\Lambda(\Gamma_L^*)}(M_{H_L}) & \longrightarrow & \mathrm{Ext}^1_G(M, \Lambda(\Gamma_L^*)) & & \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array} \tag{3.2}$$

where for the sake of simplicity Hom_G, and Ext_G denotes $\mathrm{Hom}_{\Lambda(G)}$, and $\mathrm{Ext}_{\Lambda(G)}$, respectively. Now since M is in $\mathfrak{M}_H(G)$, $H_1(H_L, M)$ is a torsion $\Lambda(\Gamma_L)$-module and so its a^0 vanishes. This means that in (3.2) all the modules corresponding to each other in the two rows are isomorphic and so we have

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

The result follows from the isomorphism (3.1). □

Our main Theorem is the following.

Theorem 3.2.2. *Let E be an elliptic curve without complex multiplication and with good ordinary reduction at the prime $p \geq 5$. Then there is a map*

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

such that $\mathrm{Ker}(\varphi)$ *is finitely generated over $\mathbb{Z}_p$ (so it represents the trivial*

element in $\mathfrak{M}_H(G)$*) and* $\mathrm{Coker}(\varphi)$ *represents the same element in* $\mathfrak{M}_H(G)$ *as*

$$\bigoplus_{q|v_q(j_E)<0} \Lambda(G) \otimes_{\Lambda(G_q)} T_p(E)^{\mathrm{v}}.$$

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

$$X(E/L^{cyc}) \xrightarrow{\varphi_{2,L}} a^1_{\Lambda(\Gamma_L)}(X(E/L^{cyc})^{\#}) \xrightarrow{\varphi_{1,L}} a^1_{\Lambda(\Gamma_L)}(H_0(H_L, X(E/F_\infty)^{\#}))$$

(where φ_2 has been defined by Perrin-Riou [29]) with respect to finite Galois subextensions $L \subset F_\infty$ where $H_L := \mathrm{Gal}(F_\infty/L^{cyc})$ and $\Gamma_L := \mathrm{Gal}(L^{cyc}/L)$. Since by Lemma 3.2.1

$$\begin{aligned} \varprojlim_L X(E/L^{cyc}) &= X(E/F_\infty), \text{ and} \\ \varprojlim_L a^1_{\Lambda(\Gamma_L)}(H_0(H_L, X(E/F_\infty)^{\#})) &= a^1_{\Lambda(G)}(X(E/F_\infty)^{\#}), \end{aligned}$$

we certainly get a map

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

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

$$\begin{aligned} J_u(L^{cyc}) &:= \bigoplus_{u_L|u} H^1(L_{u_L}, E(\overline{L_{u_L}}))[p^\infty], \text{ and} \\ J_u(F_\infty) &:= \varprojlim_L J_u(L^{cyc}). \end{aligned}$$

We will use the following fundamental diagram

$$\begin{array}{ccccccc} 0 \to & \mathrm{Sel}(E/L^{cyc}) & \to H^1(F_R/L^{cyc}, E[p^\infty]) & \to \bigoplus_{u\in R^{cyc}} J_u(L^{cyc}) & \to 0 \\ & \downarrow r_L & \downarrow g_L & \downarrow \oplus h_{L,u} & \\ 0 \to & \mathrm{Sel}(E/F_\infty)^{H_L} & \to H^1(F_R/F_\infty, E[p^\infty])^{H_L} & \to \bigoplus_{u\in R^{cyc}} J_u(F_\infty)^{H_L} & \end{array} \tag{3.3}$$

to analyze the kernel and cokernel of the map

$$H_0(H_L, X(E/F_\infty)^\#) \to X(E/L^{cyc})^\#.$$

By (3.3) and the snake lemma we have an exact sequence

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

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

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

These cohomology groups are finite, and their number of generators is also bounded since the number of generators of H_L is bounded and $E[p^\infty]$ is cofinitely generated (by 2 elements). So the projective limit 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 3.1.2. Now we have a quasi-exact sequence (up to finite modules with bounded number of generators)

$$\begin{gathered} 0 \to \bigoplus_{u\in R} \mathrm{Hom}(\mathrm{Ker}(h_{L,u}), \mathbb{Q}_p/\mathbb{Z}_p)^\# \to \\ \to H_0(H_L, X(E/F_\infty)^\#) \to X(E/L^{cyc})^\# \to 0 \end{gathered}$$

and since $\mathrm{Ext}^2_{\Lambda(\Gamma)}(X(E/L^{cyc})^{\#})$ is trivial we get another quasi-exact sequence

$$0 \to a^1_{\Lambda(\Gamma)}(X(E/L^{cyc})^{\#}) \to a^1_{\Lambda(\Gamma)}(H_0(H_L, X(E/F_\infty)^{\#})) \to \\ \to \bigoplus_{u\in R} a^1_{\Lambda(\Gamma)}(\mathrm{Hom}(\mathrm{Ker}(h_{L,u}), \mathbb{Q}_p/\mathbb{Z}_p)^{\#}) \to 0. \tag{3.4}$$

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

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

and by a standard argument using Kummer theory [8, 25] we have that if w does not divide p then

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

Moreover, E has potential multiplicative reduction at the primes in $R\setminus\{p\}$, 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, so we have a short exact sequence

$$0 \to A \to E[p^\infty] \to B \to 0$$

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 structure of a $\mathrm{Gal}(F_\infty/\mathbb{Q})_u$-action which group is slightly bigger than $\mathrm{Gal}(F_\infty/L)_w$. By taking $H_{L,w}$-homology for L sufficiently large we get the exact sequence

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

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

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

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

have

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

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 [25, 8], so it is negligible. Therefore from (3.4) we obtain the quasi-exact sequence

$$0 \to a^1_{\Lambda(\Gamma)}(X(E/L^{cyc})^{\#}) \to a^1_{\Lambda(\Gamma)}(H_0(H_L, X(E/F_\infty)^{\#})) \to \\ \to \bigoplus_{u \in R\setminus\{p\}} \mathbb{Z}_p(-1) \to 0$$

as we have

$$a^1_{\Lambda(\Gamma)}(\mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p(-1), \mathbb{Q}_p/\mathbb{Z}_p)^{\#}) \cong \mathbb{Z}_p(-1).$$

Now we turn to the investigation of $\varphi_{L,2}$. The kernel of $\varphi_{L,2}$ is finite and bounded by $\mathrm{Hom}(H^1(L, E[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p)$, so its projective limit is finitely generated over $\mathbb{Z}_p$ and so trivial in $K_0(\mathfrak{M}_H(G))$. However, the cokernel of $\varphi_{L,2}$ is [23, 29]

$$\mathrm{Hom}\left(\varinjlim_{k\to\infty} \bigoplus_{u\in R\setminus\{p\}} \bigoplus_{u_L|u} H^1(\Gamma_k, E(L^{cyc}_{u_L})[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p\right) \tag{3.5}$$

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

$$0 \to \mu_{p^\infty} \to E(L^{cyc}_{u_L})[p^\infty] \to \mathbb{Z}/p^{r_L}\mathbb{Z} \to 0.$$

By the long exact sequence of Γ_k-cohomology we obtain $H^1(\Gamma_k, E(L^{cyc}_{u_L})) \cong \mathbb{Z}/p^{r_L}\mathbb{Z}$ independently of k where r_L tends to infinity as the field L grows since F_∞ contains the whole $E[p^\infty]$. So the projective limit of each local factor in (3.5) is $\mathbb{Z}_p$.

We saw that the cokernel of $\varprojlim_L \varphi_{L,1}$ is the direct sum of local terms which are isomorphic to $\mathbb{Z}_p(-1)$ and the cokernel of $\varprojlim_L \varphi_{L,2}$ is the sum of

local $\mathbb{Z}_p$'s up to modules finitely generated over $\mathbb{Z}_p$. The kernels of both are finitely generated over $\mathbb{Z}_p$. So the statement follows by the exact sequence

$$0 \to \mathbb{Z}_p \to T_p(E)^\vee \to \mathbb{Z}_p(-1) \to 0$$

as G permutes the primes above a prime q. □

3.3 Functional equations

In this section we are going to investigate the consequences of Theorem 3.2.2 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 need that the characteristic elements of $X(E/F_\infty)^\#$ and $a^1(X(E/F_\infty)^\#)$ are 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, however, in the GL_2-case one has to be a bit more careful.

3.3.1 The negligibility of higher extension groups

The following general proposition is the first step towards proving that the modules $X(E/F_\infty)^\#$ and $a^1(X(E/F_\infty)^\#)$ have the same characteristic element. It is a generalization of Proposition 2.1.10.

Proposition 3.3.1. *Let M be in the category $\mathfrak{M}_H(G)$. Then we have the following relation connecting the characteristic element ξ_M of M and the characteristic elements $\xi_{a^i(M)}$ of $a^i(M)$ for $1 \leq i \leq 5$.*

$$\xi_M = \prod_{i=1}^{5} \xi_{a^i(M)}^{(-1)^{i+1}}. \tag{3.6}$$

Proof. Because of the long exact sequence of $\mathrm{Ext}_{\Lambda(G)}(\cdot, \Lambda(G))$ it is enough to prove the statement separately for p-torsion modules and modules finitely generated over $\Lambda(H)$.

For p-torsion modules it suffices to show the statement for projective $\Omega(G)$-modules. For these modules we only have first extension groups. Furthermore, if M is a projective $\Omega(G)$-module then $a^1(M) \cong \mathrm{Hom}(M, \Omega(G))$ 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 its characteristic element is in the image of the map [7, 36]

$$\Lambda(G)_S^\times \to K_1(\Lambda(G)_{S^*}).$$

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

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

and their higher extension groups vanish as these modules have a projective resolution of length 1. So the equation (3.6) 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 (3.6) 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 $i \geq 2$ which is equivalent to that they represent the trivial element in $K_0(\mathfrak{M}_H(G))$. The key observation is that since we have a map

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

constructed in Theorem 3.2.2 we can relate the extension functors of the modules $X(E/F_\infty)^\#$ and $\mathrm{Ext}^1(X(E/F_\infty), \Lambda(G))$. This is why the following lemma is of interest to us.

Lemma 3.3.2. $\mathrm{Ext}^i(\mathrm{Ext}^1(X(E/F_\infty), \Lambda(G)), \Lambda(G))$ *is in the category* $\mathcal{C}^3$ *for* $i \geq 2$.

Proof. Let

$$0 \to P_5 \to \cdots \to P_0 \to X(E/F_\infty) \to 0$$

be the projective resolution of $X(E/F_\infty)$ 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 notations

$$\begin{aligned} a^i(N) &:= \mathrm{Ext}^i_{\Lambda(G)}(N, \Lambda(G)), \text{ and} \\ N^* &:= \mathrm{Hom}_{\Lambda(G)}(N, \Lambda(G)) \end{aligned}$$

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 $X(E/F_\infty)$ has trivial Ext^0 we have a short exact sequence

$$0 \to P_0^* \to M_0^* \to a^1(X(E/F_\infty)) \to 0.$$

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

$$0 \to M_1 \to P_1 \to M_0 \to 0$$

we get an exact sequence

$$0 \to M_0^* \to P_1^* \to M_1^* \to a^2(X(E/F_\infty)) \to 0 \tag{3.7}$$

that we can split up into two short exact sequences

$$\begin{aligned} 0 \to M_0^* \to P_1^* \to A \to 0, \text{ and} \\ 0 \to A \to M_1^* \to a^2(X(E/F_\infty)) \to 0 \end{aligned} \tag{3.8}$$

with some $\Lambda(G)$-module A. From the first exact sequence in (3.8) and because P_1^* is a projective module we get that

$$a^i(a^1(X(E/F_\infty))) \cong a^i(M_0^*) \cong a^{i+1}(A).$$

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

$$\cdots \to a^{i+1}(M_1^*) \to a^{i+1}(A) \to a^{i+2}(a^2(X(E/F_\infty))) \to \cdots \tag{3.9}$$

On the other hand, similarly to (3.7) and (3.8) we have two short exact sequences

$$\begin{aligned} 0 \to M_1^* \to P_2^* \to B \to 0, \text{ and} \\ 0 \to B \to M_2^* \to a^3(X(E/F_\infty)) \to 0 \end{aligned} \tag{3.10}$$

with some $\Lambda(G)$-module B. So by the same trick $a^{i+1}(M_1^*) \cong a^{i+2}(B)$ (with $i \geq 1$, although, we only need it for $i \geq 2$) and we have a long exact sequence

$$\cdots \to a^{i+2}(M_2^*) \to a^{i+2}(B) \to a^{i+3}(a^3(X(E/F_\infty))) \to \cdots \tag{3.11}$$

Now $a^{i+2}(M_2^*)$ vanishes for $i \geq 2$ because as explained above this extension group is isomorphic to $a^{i+3}(C)$ where C is defined by the short exact sequence

$$0 \to C \to M_3^* \to a^4(X(E/F_\infty)) \to 0,$$

and even $a^5(C)$ equals 0. Indeed, since C is torsion-free as a module over the Iwasawa algebra of a pro-p normal subgroup G' of G as so is M_3^*, its projective resolution as a $\Lambda(G')$-module has length at most 4 and so its 5th extension functor vanishes and we have [26]

$$\mathrm{Ext}^i_{\Lambda(G)}(C, \Lambda(G)) = \mathrm{Ext}^i_{\Lambda(G')}(C, \Lambda(G')).$$

By (3.11) this means that $a^{i+2}(B) \cong a^{i+3}(a^3(X(E/F_\infty)))$. So replacing isomorphic modules in (3.9) we get a long exact sequence

$$\to a^{i+3}(a^3(X(E/F_\infty))) \to a^i(a^1(X(E/F_\infty))) \to a^{i+2}(a^2(X(E/F_\infty))) \to \cdots$$

Now since $\Lambda(G)$ is Auslander regular [37, 38], we get that the first 3 extension groups of $a^{i+3}(a^3(X(E/F_\infty)))$ and $a^{i+2}(a^2(X(E/F_\infty)))$ vanish for $i \geq 2$ which means they are in the category $\mathcal{C}^3$ and then so is $a^i(a^1(X(E/F_\infty)))$. $\square$

The following is a slight generalization of Lemma 3.1.1. 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 3.3.3. *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 [1] 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) 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 is proven by Wadsley and Ardakov [2] 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.

So it remains to prove the statement for modules M without p-torsion. Now 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 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 $0 \leq i \leq 3$) and so finite because both conditions are equivalent to the Poincaré series of M being a polynomial [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 3.1.2. □

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 nontrivial 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 3.3.4. *Let E be an elliptic curve without complex multiplication and with good ordinary reduction at the prime $p \geq 5$. Then the characteristic element of $\mathrm{Ext}^1(X(E/F_\infty)^\#, \Lambda(G))$ is the same as the characteristic element of $X(E/F_\infty)^\#$.*

Proof. By Proposition 3.3.1 we only need to check that the extension groups $\mathrm{Ext}^i(X(E/F_\infty)^\#, \Lambda(G))$ have trivial characteristic element for any $i \geq 2$. By Theorem 3.2.2 (and taking inverted action) we have a map

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

such that its kernel has trivial characteristic element and its cokernel is equivalent to

$$\bigoplus_{q | v_q(j_E) < 0} \Lambda(G) \otimes_{\Lambda(G_q)} T_p(E)^{\mathrm{v}\#}.$$

in $K_0(\mathfrak{M}_H(G))$. Now $T_p(E)^{\mathrm{v}\#}$ is a free $\mathbb{Z}_p$-module of rank 2 and $\Lambda(G)$ is a flat $\Lambda(G_q)$-module, so

$$\Lambda(G) \otimes_{\Lambda(G_q)} T_p(E)^{\mathrm{v}\#}.$$

only has a nontrivial Ext^2 and its higher and lower Ext functors are trivial, since $T_p(E)^{\mathrm{v}\#}$ is pseudo-null $\Lambda(G_q)$-module of projective dimension 2. We are done by Lemmata 3.3.2, and 3.3.3, and the long exact sequence of the functor $\mathrm{Ext}(\cdot, \Lambda(G))$. □

3.3.2 Functional equation of the characteristic element

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

$$\Lambda(G) \otimes_{\Lambda(G_q)} T_p(E)^{\mathrm{v}} \tag{3.12}$$

for each prime q in $\mathbb{Q}$ with potentially multiplicative reduction for E. It can be easily seen that the characteristic element of (3.12) is the same as the

image of the characteristic element of $T_p(E)^\vee$ under the natural map

$$K_1(\Lambda(G_q)_{S_q}) \to K_1(\Lambda(G)_S)$$

where S_q is the canonical Ore-set in the Iwasawa algebra $\Lambda(G_q)$ (see section 1.2.2). So from now on we focus on determining the characteristic element of $T_p(E)^\vee$ 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_∞ [8], hence there exists an open subgroup $I_q^{(1)} \leq_o I_q$ of the inertia subgroup such that we have an exact sequence of $\Lambda(G_q)$-modules

$$0 \to A_q \to T_p(E)^\vee \to B_q \to 0, \tag{3.13}$$

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 $A_q := H^0(I_q^{(1)}, T_p(E)^\vee)$ is a $\Lambda(G_q)$-submodule of $T_p(E)^\vee$ 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

(*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 $T_p(E)^\vee$, we have the following isomorphisms of $\Lambda(G_q)$-modules.

$$\begin{aligned} A_q &\cong B_q(1), \\ B_q(2) &\cong \mathrm{Hom}(B_q, \mathbb{Z}_p), \text{ and} \\ A_q &\cong \mathrm{Hom}(A_q, \mathbb{Z}_p), \end{aligned}$$

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

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

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 $T_p(E)^{\mathrm{v}}$ since we have an exact sequence

$$0 \to A_q \to C_q \to B_q \to 0$$

similar to (3.13) as A_q and B_q by the above properties satisfy the exact sequences

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

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

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

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

$$\beta_q = \begin{cases} 1 + e_q \mathrm{Frob}_q & \textit{(non-split multiplicative reduction at } q\textit{)} \\ 1 - e_q \mathrm{Frob}_q & \textit{otherwise,} \end{cases}$$

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

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

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

Proof. Indeed, Frob_q acts on A_q trivially if the reduction is split multiplicative over the field where multiplicative reduction realizes, and by -1 if the

reduction is non-split multiplicative. So

$$A_q \otimes_{\mathbb{Z}_p} \Lambda(I_q^{(1)}) \cong P_q/P_q(1 \pm \mathrm{Frob}_q) \cong \Lambda(G_q)/\Lambda(G_q)(1 \pm e_q\mathrm{Frob}_q)$$

and the first statement of the result follows. For the second statement note that

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

so they have the same idempotent element. □

Remark. It can be easily seen that

$$\begin{aligned} \varepsilon_q &= 1 + e_q(\mathrm{Frob}_q^{-1} - 1) \qquad \text{if } \beta_q = 1 + e_q\mathrm{Frob}_q, \text{ and} \\ \varepsilon_q &= 1 - e_q(\mathrm{Frob}_q^{-1} + 1) \qquad \text{if } \beta_q = 1 - e_q\mathrm{Frob}_q. \end{aligned}$$

On the other hand the characteristic element of

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

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

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

is also a characteristic element for the module

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

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

$$\alpha_q := \frac{\left(X_q\beta_q X_q^{-1}\right)^{\#}}{X_q\beta_q X_q^{-1}} \tag{3.14}$$

and denoting its image under the map

$$K_1(\Lambda(G_q)_{S_q^*}) \to K_1(\Lambda(G)_{S^*})$$

by the same letter we have

$$\partial_G(\alpha_q) \cong \Lambda(G) \otimes_{\Lambda(G_q)} T_p(E)^{\mathrm{v}}. \tag{3.15}$$

So we obtain the following

Corollary 3.3.6. *Let E be an elliptic curve without complex multiplication and with good ordinary reduction at the prime $p \geq 5$ and assume that the dual Selmer $X(E/F_\infty)$ over the 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*

$$\xi^{\#}_{X(E/F_\infty)} = \xi_{X(E/F_\infty)} \varepsilon_0(X(E/F_\infty)) \prod_{q \in R \setminus \{p\}} \alpha_q \tag{3.16}$$

where the modifying factors α_q are defined in (3.14), $\varepsilon_0(X(E/F_\infty))$ is in $K_1(\Lambda(G))$ 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 3.2.2 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 $\Lambda(G) \otimes_{\Lambda(G_q)} T_p(E)^{\mathrm{v}}$ is α_q, and

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

□

3.4 Connections to the analytic side

In this section we investigate the compatibility of Corollary 3.3.6 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 will also investigate its consequences towards the parity conjecture.

3.4.1 Compatibility up to p-adic units

Let us recall at first the Main Conjecture over the GL_2-extension.

Let R_0 denote the set of rational primes at which E has potentially multiplicative reduction. Further, put $R := R_0 \cup \{p\}$. The conjecture concerning the existence of a p-adic L-function over the GL_2-extension is the following special case of Conjecture 1.3.2.

Conjecture 3.4.1 (Conjecture 5.7 in [7]). *Assume that $p \geq 5$ and that E has good ordinary reduction at p. Then there exists $\mathfrak{L}_E$ in $K_1(\Lambda(G_0)_{S^*_{\mathbb{Q}}})$ such that, for all Artin representations τ of G_0, we have $\mathfrak{L}_E(\tau) \neq \infty$, and*

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

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 (see also Conjecture 1.3.3).

Conjecture 3.4.2 (Conjecture 5.8 in [7]). *Assume that $p \geq 5$, E has good ordinary reduction at p, and $X(E/F_\infty)$ belongs to the category $\mathfrak{M}_{H_0}(G_0)$. Granted Conjecture* 3.4.1, *the p-adic L-function $\mathfrak{L}_E$ in $K_1(\Lambda(G_0)_{S^*_{\mathbb{Q}}})$ is a characteristic element of $X(E/F_\infty)$.*

The only evidence known so far supporting Conjecture 3.4.2 is that it is true whenever E admits complex multiplication and $X(E/F_\infty)$ is in the category $\mathfrak{M}_H(G)$ [7], [41], and [32].

In order to investigate the connections between Corollary 3.3.6 and Conjecture 3.4.2 we need the values of the local factors α_q at Artin representations.

Proposition 3.4.3. *Let τ be an Artin representation of the Galois group $G = \mathrm{Gal}(F_\infty/\mathbb{Q})$. Then we have*

$$\alpha_q(\tau) = \varepsilon_q\left(\tau^{(1)}_{G_q}\right) \frac{P_q(E,\tau,q^{-1})}{P_q(E,\tau^*,q^{-1})}, \tag{3.17}$$

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 (3.17) depend only on τ_{G_q} and are multiplicative with respect to 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

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

On the other hand, in this case $P_q(E,\tau,q^{-1}) = P_q(E,\tau^*,q^{-1}) = 1$ as $(T_p(E)^{\mathrm{v}}\otimes \tau)^{I_q}$ 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

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

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

$$\begin{aligned}
&\left(\frac{X_q+1}{X_q}\beta_q^{\#}\frac{X_q}{X_q+1}\right)(\tau_{G_q}) = \\
&= \left(\frac{X_q+1}{X_q}(1 \pm e_q\mathrm{Frob}_q^{-1})\frac{X_q}{X_q+1}\right)(\tau_{G_q}) = \\
&= \det(1 \pm \tau_{G_q}(X_q^{-1}e_qX_q)\tau_{G_q}(\frac{(X_q+1)^{1/q}-1}{X_q})\tau_{G_q}(\mathrm{Frob}_q^{-1}) \mid W_{\tau_{G_q}}) = \\
&= \det(1 \pm \tau_{G_q}(e_q)q^{-1}\tau_{G_q}(\mathrm{Frob}_q^{-1}) \mid W_{\tau_{G_q}})
\end{aligned}$$

as $X_q^{-1}e_qX_q = e_q$ since I_q is commutative. Moreover, e_q is the idempotent element in $\Lambda(I_q) \subset \Lambda(G_q)$ corresponding 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 1's 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 $T_p(E)^{\mathrm{v}I_q^{(1)}}$. Now by the self-duality of the Galois representation A_q this space is spanned by the vectors occuring in $(T_p(E)^{\mathrm{v}} \otimes W_{\tau_{G_q}})^{I_q}$. Hence we have

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

because we have the equality

$$(T_p(E)^{\mathrm{v}} \otimes W_{\tau_{G_q}})^{I_q} = (T_p(E)^{\mathrm{v}I_q^{(1)}} \otimes W_{\tau_{G_q}}^{I_q^{(1)}})^{I_q/I_q^{(1)}}$$

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

Remarks. 1. It is easy to see that the part of the statement of Proposition 2.4.3 dealing with the primes of split multiplicative reduction is a special case of this above Proposition. The (potentially) good primes, however, do not ramify infinitely in this GL_2-extension, that is why we do not deal with them in this chapter.

2. As in section 2.4.2 the above Proposition shows that the functional equation of the characteristic element of the dual Selmer is compatible with conjectural functional equation of the p-adic L-function up to p-adic units.

3.4.2 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 the following quantities.

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

(*ii*) $s_E(\tau) :=$ 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*) $\lambda_E(\tau) :=$ the $\mathcal{O}$-rank of the dual Selmer $X(\mathrm{tw}_\tau(E)/\mathbb{Q}^{cyc})$;

(*iv*) $w_E(\tau) :=$ 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

$$(-1)^{r_E(\tau)} = (-1)^{s_E(\tau)} = (-1)^{\lambda_E(\tau)} = w_E(\tau) \tag{3.18}$$

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 (3.16) 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

$$f(1/(T+1) - 1) = \varepsilon_f(T) f(T)$$

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 $T = 0$ 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 we call then the representation itself orthogonal or symplectic, respectively. The following theorem of Greenberg makes orthogonal representations easier to handle. We will use this later on.

Theorem 3.4.4 (Greenberg [21]). *Let τ be an orthogonal Artin representation of the group G. Then the order of vanishing of the characteristic power series of the module $X(\mathrm{tw}_\tau(E)/\mathbb{Q}^{cyc})$ 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 3.4.5. *Let τ be a self-dual Artin representation of the group G. Then we have*

$$\varepsilon_0(X(E/F_\infty))(\tau)\prod_{q\in R_0}\alpha_q(\tau)\equiv(-1)^{\mathrm{ord}_{T=0}\xi_{X(\mathrm{tw}_\tau(E)/\mathbb{Q}^{cyc})}}=(-1)^{\lambda_E(\tau)}\pmod{\mathcal{M}} \tag{3.19}$$

where $\xi_{X(\mathrm{tw}_\tau(E)/\mathbb{Q}^{cyc})}$ is the characteristic power series (in $\mathcal{O}[\![T]\!]$) of the Pontryagin dual of the Selmer group $\mathrm{Sel}(\mathrm{tw}_\tau(E)/\mathbb{Q}^{cyc})$. 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 sign in the functional equation of $\xi_{X(E/F_\infty)}(\tau)$ is by definition the reduction of the left hand side of equation (3.19) modulo the maximal ideal $\mathcal{M}$ of $\mathcal{O}$. So 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

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

whenever it is defined, and ∞ otherwise (see section 1.2.4). Moreover, by Lemma 3.7 in [7] $\Phi'_\tau(\xi_{X(E/F_\infty)})$ 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

Lemma 3.4 in [6]. As the higher homology groups $H_i(H, X(\mathrm{tw}_\tau(E)/F_\infty))$ for $i \geq 1$ are p-torsion by Lemmata 3.9 and 5.3 in [7] this Akashi series actually lies in $\mathcal{O}[\![T]\!][1/p]$. The sign in question is

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

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

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

with finite cokernel. The characteristic power series of the kernel of this homomorphism is $\Phi_\tau(X_q\beta_q X_q^{-1}\beta_q^{-1})$ and it does not vanish at $T = 0$. Indeed, otherwise $\tau(\mathrm{Frob}_q)$ would not have finite order (as it would have an eigenvalue equal to q^{-1}, the inverse of the eigenvalue of Frobenius acting on the kernel of the untwisted restriction homomorphism) which is impossible. The result follows. □

Now we turn to the description of $\varepsilon_0(X(E/F_\infty))$. Let $\{P_i \mid 1 \leq i \leq r\}$ be the 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 Theorem 6.7 in Volume I of [13] as $\Lambda(H)$ is complete with respect to its $\mathrm{Jac}(\Lambda(H))$-adic filtration—in other words it is a complete semi-local ring.

Proposition 3.4.6. *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*

$$\varepsilon_0(X(E/F_\infty))(\tau) \equiv \prod_{i=1}^{r}(1-2e_{P_i})(\tau)^{n_i} \prod_{q\in R_0} \varepsilon_q(\chi_{q,cyc}\tau) \pmod{\mathcal{M}}$$

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

Proof. By Corollary 3.3.6 we have

$$\begin{aligned} \xi^{\#}_{X(E/F_\infty)} &= \xi_{X(E/F_\infty)}\varepsilon_0(X(E/F_\infty))\prod_{q\in R}\alpha_q, \text{ so} \\ \left(\xi_{X(E/F_\infty)}\prod_{q\in R}(X_q\beta_q X_q^{-1})^{\#}\right)^{\#} &= \varepsilon_0(X(E/F_\infty))\xi_{X(E/F_\infty)}\prod_{q\in R}(X_q\beta_q X_q^{-1})^{\#}. \end{aligned}$$

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

$$\begin{aligned} \mathrm{sign}_\tau\colon K_0(\Lambda(H)) &\to \{\pm 1\} \\ [M] &\mapsto (-1)^{\sum_{i=0}^{\infty}(-1)^i \mathrm{rk}_{\mathcal{O}}(H_i(H,\mathrm{tw}_{\tau|H}(M)))}. \end{aligned} \tag{3.20}$$

Note that the summation is always finite in (3.20). 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

$$\varepsilon_M(\tau) \equiv \mathrm{sign}_\tau([M/M(p)]) \pmod{\mathcal{M}} \tag{3.21}$$

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 (3.21) on

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

On the other hand, we have

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

since e_{P_i} maps to an idempotent matrix of rank $m_i(\tau)$ via τ where $m_i(\tau)$ is the number of copies of τ in the representation space $(\mathcal{O}\otimes P_0)_{H_n}$ where H_n is contained in the kernel of τ. So it equals the $\mathbb{Z}_p$-rank of $(\mathrm{tw}_\tau(P_0))_H$ and

$$(1-2e_{P_i})(\tau)=\det(\tau(1-2e_{P_i}))=(-1)^{m_i(\tau)}=\mathrm{sign}_\tau(P_i). \tag{3.22}$$

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

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

For this let us notice that

$$\partial_G(X_q\beta_qX_q^{-1})\cong\Lambda(G)\otimes_{\Lambda(G_q)}\partial_{G_q}(X_q\beta_qX_q^{-1}) \tag{3.23}$$

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

$$\begin{aligned}\partial_{G_q}(X_q\beta_qX_q^{-1}) &\cong \chi_{q,cyc}\otimes\partial_{G_q}(\beta_q)\text{ and so}\\ \tau\otimes\partial_{G_q}(X_q\beta_qX_q^{-1}) &\cong (\chi_{q,cyc}\tau)\otimes\partial_{G_q}(\beta_q)\end{aligned}$$

because H_q acts on X_q+1 via $\chi_{q,cyc}$. Thus we have

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

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

For each prime q in R_0 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 nontrivial 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 3.4.3, 3.4.5, and 3.4.6 we get the following

Theorem 3.4.7. *If τ is any self-dual Artin representation of G then we have*

$$(-1)^{\lambda_E(\tau)} = \prod_{i=1}^{r}(1 - 2e_{P_i})(\tau)^{n_i} \prod_{q \in R_0} (-1)^{\langle \chi_q \chi_{q,cyc}^{-1}, \tau_{G_q} \rangle} \tag{3.24}$$

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

Proof. First of all note that both sides of (3.24) are a priori ± 1 by equation (3.22). Since τ is self-dual, by Proposition 3.4.3 we have

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

as the dimension of $\tau_{G_q}^{(1)}$ is even and so $\chi_{q,cyc}^{\dim \tau_{G_q}^{(1)}} = 1$. Hence we only need to verify that for any $q \neq p$ in R

$$(-1)^{\langle \chi_q \chi_{q,cyc}^{-1}, \tau_{G_q} \rangle} \equiv (X_q \varepsilon_q X_q^{-1})(\tau_{G_q}^{(2)}) = \varepsilon_q(\chi_{q,cyc} \tau_{G_q}^{(2)}) \pmod{\mathcal{M}} \tag{3.25}$$

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 (3.25) we apply our remark after Lemma 3.3.5,

$$\begin{aligned} \varepsilon_q &= 1 + e_q(\mathrm{Frob}_q^{-1} - 1) \text{ (non-split multiplicative reduction at } q) \\ \varepsilon_q &= 1 - e_q(\mathrm{Frob}_q^{-1} + 1) \text{ otherwise.} \end{aligned}$$

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 $I_q = I_q^{(1)}$, so $e_q = 1$, $\chi_q = 1$ and

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

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 $\chi_{q,cyc}^{-1}$.

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

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

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

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

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

where W is the subrepresentation of $\chi_{q,cyc}\tau_{G_q}$ on which I_q acts via the character χ_q because $\chi_{q,cyc}\tau_{G_q}^{(2)}(e_q)$ is the projection onto this space. Now this is (-1) to the dimension of the subspace of τ on which G_q acts via $\chi_q\chi_{q,cyc}^{-1}$ as this is exactly the tensor product of $\chi_{q,cyc}^{-1}$ 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. We call a subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ an *Iwahori subgroup* if it reduces modulo p to a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Recall that the Borel subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ are the conjugates of the subgroup containing upper triangular matrices in $\mathrm{GL}_2(\mathbb{F}_p)$.

Corollary 3.4.8. *Let τ be a self-dual representation of G which does not factor through the maximal pro-p normal subgroup G_0 of G. Then we have*

$$(-1)^{\lambda_E(\tau)} = \prod_{i=1}^{r}(1-2e_{P_i})(\tau)^{n_i} \prod_{q\in R_0}(-1)^{\langle \chi_q, \tau_{G_q}\rangle}.$$

Proof. This is a consequence of Lemma 6.18 in [6]. 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

$$\langle \chi_q, \tau_{G_q}\rangle = \langle \chi_q\chi_{q,cyc}^{-1}, \tau_{G_q}\rangle = (\langle \chi_q\chi_{q,cyc}^{-1}, \tau_{G_q}\rangle + \langle \chi_q\chi_{q,cyc}, \tau_{G_q}\rangle)/2. \qquad (3.26)$$

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 Lemma 6.18 in [6]. 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 (3.26). Moreover, if we have a self-dual irreducible 1-dimensional representation of an 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 (3.26) 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, so it has to be the whole τ as τ is irreducible. □

Now we can state our main result in this section.

Theorem 3.4.9. *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

$$(-1)^{\lambda_E(\tau)} = w_E(\tau) \tag{3.27}$$

holds for all self-dual representations τ of G/G_0 then it is also true for any self-dual representation τ of G.

Proof. Let τ be an Artin representation of G which does not factor through G/G_0. We would like to prove that both sides of (3.27) 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 [33], theorem 1 of part III) that we have a surjection

$$K_0(\mathrm{Rep}(G/G_0)) \to K_0(\mathrm{Rep}_{\mathrm{mod}-p}(G/G_0))$$

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 [21] (see also [30]) showed that the analytic root number only depends on the image of τ in $K_0(\mathrm{Rep}_{\mathrm{mod}-p}(G/G_0))$. So it remains to show the same for the parity of $\lambda_E(\tau)$. Since $\chi_q\chi_{q,cyc}^{-1}$ is a 1-dimensional representation which is trivial on the pro-p-Sylow subgroup of G_q it is clear that

$$\langle \chi_q\chi_{q,cyc}^{-1}, \tau_{G_q}\rangle$$

depends only on $\widetilde{\tau}^{ss}$. On the other hand by definition for each undecomposable projective module P_i of $\Lambda(H)$ we have

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

where $m_i(\tau)$ is the multiplicity of the irreducible modular H-representation corresponding to the projective module P_i in the modular representation $\widetilde{\tau}^{ss}$ and by nature depends only on $\widetilde{\tau}^{ss}$. The result follows. □

Remarks. 1. The Theorem above is closely related to Proposition 11.3 in [21]. 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 $\mathbb{Q}^{cyc}$. Moreover, we do not need the finiteness of the p-Selmer group over any finite extension of $\mathbb{Q}^{cyc}$. However, we do need the (weaker) assumption that $X(E/F_\infty)$ is in $\mathfrak{M}_H(G)$ and that E has good ordinary reduction at p.

2. The assumptions on the reduction type of E at 2 and 3 should be unnecessary, but the formulas of Rohrlich [30] for the local root numbers do not cover all the cases. For example, if G is contained in an Iwahori subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$—or equivalently if 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 an Iwahori subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$.

Proposition 3.4.10. *Let A be an open subgroup of the Iwahori subgroup*

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

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

$$\det\colon \tilde{A} \to \mathbb{F}_p^\times$$

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

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

$$\tau\colon A \to \mathrm{GL}_k(\overline{\mathbb{Q}})$$

is an irreducible symplectic Artin-representation. Now write $A_0 := A/\mathrm{Ker}(\tau)$. Since τ is Artin, 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 claim that A_0 is either abelian or can be written in the form

$$(P \rtimes S) \times C \tag{3.28}$$

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 of the claim. 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 $\mathrm{GL}_2(\mathbb{F}_p)$. So this complement is generated by 2 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 $n \geq 1$ be the smallest integer such that $\mathrm{Ker}(\tau)$ contains the intersection of A with the nth congruent subgroup

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

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 nontrivial normal p-subgroup in A_0 and so has a nontrivial 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 nontrivial subgroup of P_0 because otherwise that subgroup would be in the centre of A_0 which contradicts to the fact that it has odd order by our remark before the claim. 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 nontrivial element in P_0, namely the commutator of x and an arbitrary nontrivial element in P_0. Now $A/(A \cap I_0)$ is generated by 2 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 $\tilde{A}$, g_1 has to be the image of a diagonal matrix $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ such that one of α and β has to be a quadratic residue modulo p and the other one a quadratic nonresidue 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 claim follows by putting S and C to be the image of the group generated by g_1 and g_2, respectively. $\square$

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. So we may assume that A_0 is in the form (3.28). 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 claim S acts faithfully on P_0. Moreover, P_0 is an abelian group of exponent p so it can be viewed as a vectorspace over $\mathbb{F}_p$ and so we can pick up a nontrivial eigenvector $v \in P_0$ of the S-action (S is cyclic). This means that the subgroup generated by v is normal in $P \rtimes S$ 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 nontrivial invariant subspace of the underlying vectorspace 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 $\tau(v)$ are in pairs (ζ, ζ^{-1}) where ζ is a primitive pth root of unity 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

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

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

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

because if u is an eigenvector of v with eigenvalue ζ then if its inner product with w is nonzero 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 $X_i = -X_i^T$ for each $1 \leq i \leq l$ where $\cdot^T$ 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. □

Remarks. 1. The statement of Proposition 3.4.10 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 3.4.10.

2. 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

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

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 modulo 4. Now let σ the 2-dimensional representation of A which is trivial on the congruent subgroup,

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

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

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

Corollary 3.4.11. *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*

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

Proof. Since E has a p-isogeny over $\mathbb{Q}$, G is contained in an Iwahori subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$, so we can conjugate it into the particular Iwahori subgroup B in Poroposition 3.4.10. Moreover, by the Weil pairing the determinant map on the reduction of G to $\mathrm{GL}_2(\mathbb{F}_p)$ is surjective onto $\mathbb{F}_p^\times$ so by Proposition 3.4.10 we conclude that G does not have symplectic representations and so τ is orthogonal. For orthogonal representations the statement follows from Greenberg's Theorem (Theorem 3.4.4) and Theorem 3.4.9 (see also Theorem 6.2 in [6]) 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 proven [18]. Formally it 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 $\widetilde{\tau}^{ss}$ of the reduction of τ modulo the maximal ideal $\mathcal{M}$ in $\mathcal{O}$. By Proposition 3 in [31] it follows that if E has potentially multiplicative reduction at the prime q then the local root number at q is

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

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 $\dim \tau = \dim \widetilde{\tau}^{ss}$ and we are done. $\square$

3.5 Example

We end this chapter by giving an example of an elliptic curve illustrating our results. Let E be the elliptic curve 11A3 in Cremona's tables [12], of conductor 11. It has a minimal Weiestraß equation

$$E: \ y^2 + y = x^3 - x^2$$

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 we have that $E[5]$ fits into the exact sequence

$$0 \to \mathbb{Z}/5\mathbb{Z} \to E[5] \to \mu_5 \to 0.$$

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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $c \equiv 0 \mod 5^2$ and $a \equiv 1 \mod 5$. 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

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

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

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

has kernel of $\mathbb{Z}_p$-rank 4. Four elements of this kernel—which are independent over $\mathbb{Z}_p$—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

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

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, $\mathrm{Frob}_{11} = \begin{pmatrix} 11 & 0 \\ -50 & 1 \end{pmatrix}$ is a topological generator of the group G/H. Now we can apply Corollary 3.3.6. The functional equation of the characteristic element is in the form

$$\xi^\# = \xi\varepsilon_0 \frac{(X_{11}(1-\mathrm{Frob}_{11})X_{11}^{-1})^\#}{X_{11}(1-\mathrm{Frob}_{11})X_{11}^{-1}}, \tag{3.29}$$

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

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

the simplest example for ξ would be $\mathrm{Frob}_{11} - \frac{(X_{11}+1)^{11}-1}{X_{11}}$ because it certainly satisfies a functional equation in the form (3.29). 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 $X(E/L_1^{cyc})$ and $X(E/L_2^{cyc})$ 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's (see the end of [5] for details). Now let

$$\begin{aligned}
\gamma &:= \begin{pmatrix} \sqrt{11} & 0 \\ 0 & \sqrt{11} \end{pmatrix}, \\
\alpha &:= \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}, \\
\delta &:= \gamma \mathrm{Frob}_{11}^{-1} \left((1+X_{11})^3 + X_{11}^2(\alpha+1)X_{11} \right), \\
\xi_0 &:= \gamma^2 - \delta(\delta^{\#})^{-1}, \text{ and} \\
\xi_* &:= \gamma^2 - X_{11}\delta(\delta^{\#})^{-1}X_{11}^{-1}
\end{aligned}$$

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

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

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

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

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

$$\partial_G(\xi_0/\xi_*) = (\Lambda(G)/\Lambda(G)\xi_0) \,/\, (\Lambda(G)X_{11}/(\Lambda(G)\xi_0 \cap \Lambda(G)X_{11})) \text{ and}$$
$$\partial_G\left((\mathrm{Frob}_{11}-1)\left(\mathrm{Frob}_{11} - \frac{(X_{11}+1)^{11}-1}{X_{11}}\right)^{-1}\right) =$$
$$(\Lambda(G)/\Lambda(G)(\mathrm{Frob}_{11}-1)) \,/\, (\Lambda(G)X_{11}/(\Lambda(G)(\mathrm{Frob}_{11}-1) \cap \Lambda(G)X_{11}))$$

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 therefore so do ξ_* and $\mathrm{Frob}_{11} - \frac{(X_{11}+1)^{11}-1}{X_{11}}$. □

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

$$X(E/F_\infty)_{H_n} \to X(E/F_n^{cyc}).$$

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 $\mathbb{Q}$

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

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 3 generators, namely $a_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod{P^5}$, $a_2 = \begin{pmatrix} 6 & 0 \\ 0 & 1/6 \end{pmatrix} \pmod{P^5}$, and $a_3 = \begin{pmatrix} 1 & 0 \\ 25 & 1 \end{pmatrix} \pmod{P^5}$. 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 are 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 3.5.2. *Assume that $\partial_G(\xi_*) = X(E/F_\infty)$. Then the order of*

vanishing of the characteristic power series of $X(E/L_2^{cyc})$ *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

$$X(E/F_\infty)_{H_{L_2}} \to X(E/L_2^{cyc})$$

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

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

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 $\mathbb{Q}(E[5])^{cyc}$ and $\mathbb{Q}(E'[5])^{cyc}$ 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 3.5.3. *Assume that* $\partial_G(\xi_*) = X(E/F_\infty)$. *Then the characteristic power series of* $X(E/L_i^{cyc})$ $(i = 1, 3)$ *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

$$X(E/F_\infty)_{H_{L_i}} \to X(E/L_i^{cyc}) \qquad i = 1, 3$$

again. So it remains to prove that 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,

$$\begin{aligned} \rho(\xi_0) &= \det\left((T+1)\mathrm{id} - A(A^*)^{-1}\right) \qquad \text{where} \\ A &= \begin{pmatrix} f_1(\zeta_5) & g_1(\zeta_5) & 0 & 0 \\ 0 & f_1(\zeta_5^2) & g_1(\zeta_5^2) & 0 \\ 0 & 0 & f_1(\zeta_5^4) & g_1(\zeta_5^4) \\ g_1(\zeta_5^3) & 0 & 0 & f_1(\zeta_5^3) \end{pmatrix}, \end{aligned}$$

$f_1(x) = x^3 + (x-1)^3$, $g_1(x) = (x-1)^2(x^2-1)$, 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 $T = 0$. So 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 nonzero.

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 $X_{11} + 1$. So the matrix A has the form

$$A = \begin{pmatrix} f_2(\zeta_5) & g_2(\zeta_5) & 0 & 0 \\ 0 & f_2(\zeta_5^2) & g_2(\zeta_5^2) & 0 \\ 0 & 0 & f_2(\zeta_5^4) & g_2(\zeta_5^4) \\ g_2(\zeta_5^3) & 0 & 0 & f_2(\zeta_5^3) \end{pmatrix}$$

in this case where $f_2(x) = x + x^3(x-1)^3$ and $g_2(x) = x^3(x-1)^2(x^2-1)$. The result follows similarly as above. □

Remark. The characteristic element ξ_* described above is by far not the only one satisfying all the requirements. The proofs of the Propositions 3.5.1, 3.5.2, and 3.5.3 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 the rank of* $X_1(11)(F_\infty)$ *modulo torsion finite or infinite?*

Bibliography

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

[2] K. Ardakov, S. Wadsley, K_0 and the dimension filtration for p-torsion Iwasawa modules, preprint

[3] J.-E. Björk, Filtered Noetherian rings, in *Noetherian rings and their applications*, Mathematical Survey Monographs **24** (1987), 59–97.

[4] Th. Bouganis, V. Dokchitser, Algebraicity of L-values for elliptic curves in a false Tate curve tower, preprint

[5] J. Coates, Iwasawa algebras and arithmetic, Séminaire Bourbaki, Vol. 2001/2002, *Astérisque* **290** (2003), Exp. No. 896, vii, 37–52.

[6] J. Coates, T. Fukaya, K. Kato, R. Sujatha, Root numbers, Selmer groups, and non-commutative Iwasawa theory, paper in preparation

[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.* IHES **101** (2005), 163–208.

[8] J. Coates, S. Howson, Euler characteristics and elliptic curves II, *J. Math. Soc. Japan* **53**, no. 1 (2001), 175–235.

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

[10] J. Coates, P. Schneider, R. Sujatha, Modules over Iwasawa algebras, *Journal of the Inst. of Math. Jussieu* (2003) **2**(1), 73–108.

[11] J. Coates, R. Sujatha, Galois Cohomology of Elliptic Curves, in *Lecture Notes at the Tata Institute of Fundamental Research* **88**, Narosa (2000).

[12] J. Cremona, Elliptic curves data, `http://www.maths.nottingham.ac.uk/personal/jec/ftp/data`

[13] C.W. Curtis, I. Reiner, *Methods of Representation Theory*, J. Wiley (1981).

[14] H. Darmon and Y. Tian, Heegner points over false Tate curve extensions, *Talk in Montreal* (2005)

[15] P. Deligne, Valeur de fonctions L et périodes d'intégrales, *Proc. Symp. Pure Math.* **33** (1979), Part 2, 313–346.

[16] V. Dokchitser (with an appendix by T. Fisher), Root numbers of non-abelian twists of elliptic curves, *Proc. London Math. Soc.* (3) **91** (2005), 300–324.

[17] T. Dokchitser and V. Dokchitser (with an appendix by J. Coates and R. Sujatha), Computations in non-commutative Iwasawa theory, preprint

[18] T. Dokchitser, V. Dokchitser, Self-duality of Selmer groups, preprint.

[19] M. Flach, A generalisation of the Cassels-Tate pairing, *J. Reine Angew. Math.* **412** (1990), 113–127.

[20] T. Fukaya, K. Kato, A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory, preprint

[21] R. Greenberg, Iwasawa Theory, Projective Modules, and Modular Representations, preprint.

[22] R. Greenberg, Iwasawa theory for p-adic representations, in *Algebraic number theory*, Adv. Stud. Pure Math. **17** (1989), 97–137.

[23] R. Greenberg, Introduction to Iwasawa theory for elliptic curves, in *Arithmetic algebraic geometry* (Park City, UT, 1999), 407–464.

[24] Y. Hachimori and K. Matsuno, An analogue of Kida's formula for the Selmer groups of elliptic curves, *J. Algebraic Geom.* **8** (1999), 581–601.

[25] Y. Hachimori and O. Venjakob, Completely faithful Selmer groups over Kummer extensions, *Documenta Mathematica*, Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 443–478.

[26] U. Jannsen, Iwasawa modules up to isomorphism, in *Algebraic number theory*, Adv. Stud. Pure Math. **17** (1989), 171–207.

[27] K. Kato, K_1 of some non-commutative completed group rings. *K-Theory* **34** (2005), no. 2, 99–140.

[28] J. Nekovář, On the parity of ranks of Selmer groups. II, *C. R. Acad. Sci. Paris Sér. I Math.* **332** (2001), no. 2, 99–104.

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

[30] D. E. Rohrlich, Galois theory, elliptic curves, and root numbers, *Compositio Math.* **100** (1996), 311–349.

[31] D. E. Rohrlich, Scarcity and abundance of trivial zeros in division towers, *Journal of Algebraic Geometry*, to appear.

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

[33] J.-P. Serre, Linear representations of finite groups, *Graduate Texts in Math.*, Springer (1977).

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

[35] B. Stenström, *Rings of quotients* (Springer, 1975).

[36] L. N. Vaserstein, On the Whitehead determinant for semi-local rings, *J. Algebra* **283** (2005), no. 2, 690–699.

[37] O. Venjakob, Iwasawa theory of p-adic Lie extensions, PhD thesis, University of Heidelberg (2000)

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

[39] O. Venjakob (with an appendix by D. Vogel), A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory, *J. Reine Angew. Math.* **559** (2003), 153–191.

[40] D. Vogel, Nonprincipal reflexive left ideals in Iwasawa algebras II, `http://homepages.uni-regensburg.de/ vod05208/nonprincipal2.pdf`

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

[42] G. Zábrádi, Characteristic elements, pairings, and functional equations over the false Tate curve extension, to appear in *Math. Proc. Camb. Phil. Soc.*

[43] G. Zábrádi, Pairings and functional equations over the GL_2-extension, submitted to the *London Math. Soc.*