Math. Proc. Camb. Phil. Soc. (2008), **144**, 535 © 2008 *Cambridge Philosophical Society*
doi:10.1017/S0305004108001114 *Printed in the United Kingdom*
First published online 27 March 2008

Characteristic elements, pairings and functional equations over the false Tate curve extension

BY GERGELY ZÁBRÁDI

*Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge, CB*3 0*WB.*

(*Received* 10 *October* 2006; *revised* 29 *May* 2007)

Abstract

We construct a pairing on the dual Selmer group over false Tate curve extensions of an elliptic curve with good ordinary reduction at a prime $p \geqslant 5$. This gives a functional equation of the characteristic element which is compatible with the conjectural functional equation of the p-adic L-function. As an application we compute the characteristic elements of those modules – arising naturally in the Iwasawa-theory for elliptic curves over the false Tate curve extension – which have rank 1 over the subgroup of the Galois group fixing the cyclotomic extension of the ground field. We also show that the example of a non-principal reflexive left ideal of the Iwasawa algebra does not rule out the possibility that all torsion Iwasawa-modules are pseudo-isomorphic to the direct sum of quotients of the algebra by principal ideals.

1. *Introduction*

The main conjectures in Iwasawa theory usually state that there exists a p-adic L-function for the elliptic curve over a p-adic Lie extension of $\mathbb{Q}$ which interpolates the special values of the complex L-functions of the elliptic curve twisted by Artin representations of the Galois group, it is a characteristic element for the dual of the Selmer group, and it satisfies a functional equation in some sense. These are the only tools known at present for studying the rather mysterious relationship between the algebraic or arithmetic properties of elliptic curves and the special values of their complex L-functions, especially for attacking the conjecture of Birch and Swinnerton–Dyer. The p-adic L-function in the false Tate curve case (and also in the GL_2-case) lies in the algebraic K_1-group of $\Lambda(G)_{S^*}$, the Iwasawa algebra of the Galois group localized by a canonical Ore set defined in [**4**] (see also Section 3·2). In this paper we will investigate this conjecture mainly from its algebraic side, however, in Section 7 we will see the compatibility of the results with the analytic theory.

In Section 4 we investigate the integrality properties of characteristic elements. In Section 5 we construct a canonical characteristic element 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.

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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. The heuristics for the existence of this functional equation is the following. The p-adic L-function $\mathcal{L}_E$ conjecturally approximates a certain modification (see Conjecture 7·1 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 2·4 for precise statements). As $\mathcal{L}_E(\tau^*)$ and $\mathcal{L}_E(\tau)$ approximate the modification of $L(E, \tau, 1)$ and $L(E, \tau^*, 1)$, respectively, we can relate $\mathcal{L}_E(\tau^*)$ and $\mathcal{L}_E(\tau)$. Now if we define $\mathcal{L}_E^{\#}$ to be the element we get from $\mathcal{L}_E$ by replacing elements of G with their inverses then $\mathcal{L}_E(\tau) = \mathcal{L}_E^{\#}(\tau^*)$ is a tautology. 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 over the false Tate curve extension. 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 6 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 $p \geqslant 5$ and the dual Selmer $X(E/F_\infty)$ is in the category $\mathfrak{M}_H(G)$. This pairing is actually a map from $X(E/F_\infty)$ to the first extension group of $X(E/F_\infty)^{\#}$ with the Iwasawa algebra $\Lambda(G)$. The methods used are similar to Perrin–Riou's [**21**]. 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 7 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 remaining part of this paper we compute the characteristic elements of some modules in the category $\mathfrak{M}_H(G)$ (see definition in Section 3·2) arising naturally in Iwasawa theory for elliptic curves [**3**, **11**] when G is the semidirect product of two copies of $\mathbb{Z}_p$, or – in case the Galois group is down to $\mathbb{Q}$ – isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$. In Section 8 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 8·2 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 [**8**] have some results towards constructing Heegner points in this case, as well.

The assumption we made for the whole paper that the dual of the Selmer group $X(E/F_\infty)$ always lies in $\mathfrak{M}_H(G)$ is also conjectured [**4**] if the elliptic curve E has good ordinary reduction at the prime $p \geqslant 5$. In fact if the dual Selmer $X(E/K^{cyc})$ over the cyclotomic extension of the ground field K is finitely generated over $\mathbb{Z}_p$, which is equivalent to the assumption that its μ-invariant vanishes, we do know that $X(E/F_\infty)$ is in $\mathfrak{M}_H(G)$, moreover its p-torsion part is trivial [**17**].

As an application of the investigations of rank-1 Iwasawa-modules, in Section 9 we show that the example of a non-principal reflexive left ideal of the Iwasawa algebra does not rule

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

out the possibility that all torsion $\Lambda(G)$-modules are pseudo-isomorphic to the direct sum of quotients of $\Lambda(G)$ by principal ideals.

Throughout the paper all modules are assumed to be left modules, unless otherwise stated.

2. *Analytic preliminaries and notations*

2·1. *The false Tate curve extension*

Let $p \geqslant 5$ 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) $H_n = \mathrm{Gal}(F_\infty/F_n^{cyc})$.

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.

2·2. *Systems of l-adic representations*

If E/k is an elliptic curve defined over a number field k and $\tau\colon \mathrm{Gal}(\overline{\mathbb{Q}}/k) \to \mathrm{GL}_n(\overline{\mathbb{Q}})$ 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

$$M_l(E, \tau) := M_l(E) \otimes_{\overline{\mathbb{Q}_l}} M_l(\tau). \tag{2·1}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

2·3. *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

$$P_v(M, T) := \det\left(1 - \mathrm{Frob}_v^{-1} T \,\middle|\, M_l^{I_v}\right) \tag{2·2}$$

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

$$L_v(M, s) := P_v(M, N_{k/\mathbb{Q}}(v)^{-s})^{-1} \tag{2·3}$$

and the global L-function as an Euler-product

$$L(M, s) := \prod_v L_v(M, s). \tag{2·4}$$

We write

$$L(E/k, s) := L(M(E), k, s),\ \ L(\tau, s) := L(M(\tau), k, s),\ \ L(E, \tau, s) := L(M(E, \tau), k, s). \tag{2·5}$$

The L-series $L(\tau, s)$ converges to an analytic function on the half plane $\mathrm{R}s > 1$. The L-series $L(E/k, s)$ and $L(E, \tau, s)$ define analytic functions in the half plane $\mathrm{R}s > 3/2$. If $k = \mathbb{Q}$ and τ factors through a false Tate curve extension then $L(E, \tau, s)$ has an analytic continuation and satisfies a functional equation [**10**]. We define

$$g_{E/k} = \mathrm{rk}_{\mathbb{Z}}(E(k)), \qquad r_{E/k} = \mathrm{ord}_{s=1}(L(E/k, s)). \tag{2·6}$$

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

$$L(E, \tau_1 \oplus \tau_2) = L(E, \tau_1) L(E, \tau_2). \tag{2·7}$$

2·4. *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

$$\hat{L}(E, \tau, s) := \left(\frac{N(E, \tau)}{\pi^{2\dim \tau}}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{\dim \tau} \Gamma\left(\frac{s+1}{2}\right)^{\dim \tau} L(E, \tau, s), \tag{2·8}$$

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

$$\hat{L}(E, \tau, s) = w(E, \tau) \hat{L}(E, \tau^*, 2 - s), \tag{2·9}$$

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

3. *Algebraic preliminaries and notations*

3·1. *The dual Selmer and the Iwasawa algebra*

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

$$X(E/L) = \mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/L), \mathbb{Q}_p/\mathbb{Z}_p). \tag{3·1}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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

$$\Lambda(\mathcal{G}) = \varprojlim_{N \lhd_o \mathcal{G}} \mathbb{Z}_p[\mathcal{G}/N]. \tag{3·2}$$

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

$$\Omega(\mathcal{G}) = \varprojlim_{N \lhd_o \mathcal{G}} \mathbb{F}_p[\mathcal{G}/N]. \tag{3·3}$$

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 [**23**]

$$\Lambda(G) \cong \mathbb{Z}_p[[X]][[Y; \sigma, \delta]], \tag{3·4}$$

where σ is the ring automorphism induced by

$$X \longmapsto (X+1)^{\chi(\gamma)} - 1, \tag{3·5}$$

$\delta = \sigma - 1$ 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.

3·2. *K-theory and localization*

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

$$S^* = \bigcup_{n \geqslant 0} p^n S. \tag{3·6}$$

These are multiplicatively closed (left and right) Ore sets of $\Lambda(G)$ [**4**], 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 $\Lambda(H)$ [**4**]. 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 $K_1(\Lambda(G)_{S^*})$ [**4**]. It is a pre-image of the class of M under the connecting homomorphism

$$\partial_G \ : \ K_1(\Lambda(G)_{S^*}) \longrightarrow K_0(\mathfrak{M}_H(G)) \tag{3·7}$$

in the long exact sequence of localization in K-theory

$$\begin{aligned} \cdots \longrightarrow K_1(\Lambda(G)) \longrightarrow K_1(\Lambda(G)_{S^*}) \xrightarrow{\partial_G} K_0(\mathfrak{M}_H(G)) \longrightarrow K_0(\Lambda(G)) \\ \longrightarrow K_0(\Lambda(G)_{S^*}) \longrightarrow 0, \end{aligned} \tag{3·8}$$

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 [**4**]. 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

$$\begin{aligned} \cdots \longrightarrow K_1(\Lambda(G)) \longrightarrow K_1(\Lambda(G)_S) \xrightarrow{\partial_G} K_0(\mathfrak{N}_H(G)) \longrightarrow K_0(\Lambda(G)) \\ \longrightarrow K_0(\Lambda(G)_S) \longrightarrow 0. \end{aligned} \tag{3·9}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

As defined in [**3**] 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 #, ie. for an m element in M and g in G, $m^{\#}g = (g^{-1}m)^{\#}$.

Now if we restrict ourselves to modules in $\mathfrak{N}_H(G)$, then we can define another action on the characteristic elements in the following way. 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, i,e.

$$R = \{r(X) \in \mathbb{Z}_p[[X]] \mid r(X)^{1-\gamma} \in \mathbb{Z}_p[[X]]^{\times}\}. \tag{3·10}$$

LEMMA 3·1. *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. (We call a polynomial *distinguished* if its leading coefficient is a unit, and all the other coefficients are in the maximal ideal of the coefficient ring.) 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

$$r^{-1}Yr = r^{\gamma-1}Y + r^{\gamma-1} - 1. \tag{3·11}$$

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

$$(\Lambda(G)_S)^{\times} \hookrightarrow (\Lambda(G)_{S,R})^{\times} \text{ and} \tag{3·12}$$

$$(\Lambda(H)_R)^{\times} \hookrightarrow (\Lambda(G)_{S,R})^{\times}. \tag{3·13}$$

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 [**22**], 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 5 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 5·2 these commutators correspond to pseudo-null modules. Since [**19**]

$$K_0(\mathfrak{M}_H(G)) = K_0(\mathfrak{N}_H(G)) \oplus \mathbb{Z}, \tag{3·14}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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.

3·3. *Galois representations and twists*

As in [**4**], let O denote the ring of integers of some finite extension L of $\mathbb{Q}_p$, and let us assume that we are given a continuous homomorphism

$$\rho: G \longrightarrow \mathrm{GL}_n(O) \tag{3·15}$$

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

$$\mathrm{tw}_\rho(M) = M_O \otimes_O O^n. \tag{3·16}$$

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 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 [**4**] ρ induces a homomorphism

$$\Phi'_\rho: K_1(\Lambda(G)_{S^*}) \longrightarrow K_1(M_n(Q_O(\Gamma))) = Q_O(\Gamma)^\times, \tag{3·17}$$

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

$$\varphi: \Lambda_O(\Gamma)_\mathfrak{p} \longrightarrow L, \tag{3·18}$$

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

4. *Integrality properties of characteristic elements*

It follows from the results in Section 8 that the characteristic element of $X(E/F_\infty)$ is integral in the sense that it is in the image of the natural morphism

$$\Lambda(G) \cap (\Lambda(G)_{S^*})^\times \longrightarrow K_1(\Lambda(G)_{S^*}) \tag{4·1}$$

in those Heegner-like cases and in fact this is true for all $\Lambda(H)$-torsion free modules of rank 1 (compare to [**4**, conjecture 4·8]). Since the map

$$(\Lambda(G)_S)^\times/[(\Lambda(G)_S)^\times, (\Lambda(G)_S)^\times] \longrightarrow K_1(\Lambda(G)_S) \tag{4·2}$$

is an isomorphism [**22**], and the characteristic element can be induced from $K_1(\Lambda(G)_S)$ when the module has no p-torsion, one would expect that (4·1) 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 4·1. *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.*

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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 $1 \leqslant j \leqslant d$ there exist l_j's for which $p^{l_j}e_j$ is in $M \leqslant \Lambda(H)^d$. 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

$$p^{-l_j}\tilde{\gamma}(p^{l_j}e_j) = \sum_{i=1}^{d} a_{ij}e_i. \tag{4·3}$$

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

$$\begin{pmatrix} f_1(X) \\ f_2(X) \\ \vdots \\ f_d(X) \end{pmatrix} \in M \leqslant \mathbb{Z}_p[[X]]^d \text{ then} \tag{4·4}$$

$$\tilde{\gamma}\begin{pmatrix} f_1(X) \\ f_2(X) \\ \vdots \\ f_d(X) \end{pmatrix} = A\begin{pmatrix} \tilde{\gamma}f_1(X)\tilde{\gamma}^{-1} \\ \tilde{\gamma}f_2(X)\tilde{\gamma}^{-1} \\ \vdots \\ \tilde{\gamma}f_d(X)\tilde{\gamma}^{-1} \end{pmatrix}. \tag{4·5}$$

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 $1 \leqslant j \leqslant d$ 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 (4·5) and we are done.

Remarks.

(i) 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 $\Lambda(H)$.

(ii) 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 4·1 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

$$(Y+1)I - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } (Y+1)I - \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \tag{4·6}$$

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

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \tag{4·7}$$

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

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

PROPOSITION 4·2. *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 $\mathbb{Z}_p[[X]]^{d\times d}$ such that M is a finite index submodule of the $\Lambda(G)$-module*

$$\Lambda(G)^d/\Lambda(G)^d((Y+1)I-A), \tag{4·8}$$

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

$$\Lambda(G)^d((Y+1)I-A) := \{(x^t((Y+1)I-A)^t)^t \mid x \in \Lambda(G)^d \text{ a column vector}\}. \tag{4·9}$$

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

$$M_d(\Lambda(G)) \bigcap \mathrm{GL}_d(\Lambda(G)_{S^*}) \hookrightarrow \mathrm{GL}_d(\Lambda(G)_{S^*}) \longrightarrow K_1(\Lambda(G)_{S^*}). \tag{4·10}$$

Proof. From Lemma 4·1 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

$$\tilde{\gamma}\begin{pmatrix} f_1(X) \\ f_2(X) \\ \vdots \\ f_d(X) \end{pmatrix} = A \begin{pmatrix} \tilde{\gamma} f_1(X)\tilde{\gamma}^{-1} \\ \tilde{\gamma} f_2(X)\tilde{\gamma}^{-1} \\ \vdots \\ \tilde{\gamma} f_d(X)\tilde{\gamma}^{-1} \end{pmatrix}. \tag{4·11}$$

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 4·1.

LEMMA 4·3. *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

$$\varphi: \ \Lambda(H)^d \longrightarrow M \tag{4·12}$$

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 4·4. *If M is in the category $\mathfrak{M}_H(G)$ and has no p-torsion then the following are equivalent:*

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

(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 $H' \leqslant H$ open subgroups, and $i \geqslant 1$;*

Proof. The first three statements are certainly equivalent by applying Lemma 4·1 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 $H' \leqslant H$ open subgroups, and $i \geqslant 1$ 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 4·3. So it is in the form

$$0 \longrightarrow \Lambda(H)^d \xrightarrow{A} \Lambda(H)^d \longrightarrow M \longrightarrow 0, \tag{4·13}$$

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 $n \geqslant 0$ 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

$$z \hookrightarrow (z+1)^{\chi(\tilde{\gamma}^{-1})} - 1 \tag{4·14}$$

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

$$f\left(\left(\left((z+1)^{\chi(\tilde{\gamma}^{-1})} - 1\right) + 1\right)^{\chi(\tilde{\gamma})} - 1\right) = 0. \tag{4·15}$$

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 4·5. *Assume that a $\Lambda(G)$-module M is finitely generated over $\Lambda(H)$ and $H_i(H', M)$ vanishes for all $H' \leqslant H$ open subgroups, and $i \geqslant 1$. 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* (3·15)*, $\xi(\rho)$ is finite and in O, and $\Phi'_\rho(\xi)$ is in $\Lambda_O(\Gamma)$.*

5. *The sign in the functional equation*

In Section 6 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 $K_1(\Lambda(G)_{S^*})$.

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

LEMMA 5·1. *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 5·2. *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 5·1, $r_0(X)$ is in the form

$$r_0(X) = \prod_{i=0}^{n} \Phi_{p^i}(X)^{l_i} \tag{5·1}$$

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 $i \geqslant 0$. Now M is isomorphic to

$$\bigoplus_{j=1}^{n} (\mathbb{Z}_p[[X]]/\Phi_{p^i}(X))_j \tag{5·2}$$

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 4·3). This gives the required expression for the characteristic element 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 5·3. *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*

$$\deg(\xi_1) - \deg(\xi_2) = \operatorname{rank}_{\Lambda(H)}(M/M(p)) \tag{5·3}$$

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 5·2. So we may assume that M has trivial p-torsion and no nontrivial pseudo-null submodule. The statement follows from 4·2 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

$$a_R^i(M) := \operatorname{Ext}_R^i(M, R) \qquad (i \geqslant 0). \tag{5·4}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

PROPOSITION 5·4. *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 $1 \leqslant i \leqslant 3$.*

$$\xi_M = \prod_{i=1}^{3} \xi_{a^i_{\Lambda(G)}(M)}^{(-1)^{i+1}}. \tag{5·5}$$

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 $a^1_{\Lambda(G)}(M) \cong \mathrm{Hom}(M, \Omega(G))$ and so have the same characteristic element as M using the formula for the characteristic element of p-torsion modules [**1**] (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 4·3. The $\Lambda(G)$-modules which are projective as $\Lambda(H)$-modules are by Proposition 4·2 in the form

$$\Lambda(G)^d / \Lambda(G)^d((Y+1)I - A), \tag{5·6}$$

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,

$$a^1_{\Lambda(G)}\left(\Lambda(G)^d / \Lambda(G)^d((Y+1)I - A)\right) \cong \Lambda(G)^d / ((Y+1)I - A)\Lambda(G)^d \tag{5·7}$$

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

THEOREM 5·5. *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*

$$\xi_M^\# = \varepsilon(M)\xi_M \prod_{i=1}^{n} [f_i, r_i]^{k_i}, \tag{5·8}$$

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 5·4 we have

$$\xi_M^\# = \xi_{M^\#} = \prod_{i=1}^{3} \xi_{a^i_{\Lambda(G)}(M^\#)}^{(-1)^{i+1}}. \tag{5·9}$$

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 5·2.

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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 5·3. 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 (5·8) by the "denominators" of the commutators and get an equation of the form

$$\xi_M^{\#}\prod_{i=1}^{n_1}\left(r_{i,1}^{l_{i,1}}f_{i,1}^{k_{i,1}}r_{i,1}^{-l_{i,1}}\right)\prod_{j=1}^{n_2}f_{j,2}^{k_{j,2}} = \varepsilon(M)\xi_M\prod_{i=1}^{n_1}f_{i,1}^{k_{i,1}}\prod_{j=1}^{n_2}\left(r_{j,2}^{l_{j,2}}f_{j,2}^{k_{j,2}}r_{j,2}^{-l_{j,2}}\right), \tag{5·10}$$

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 $\Lambda(G)\bigcap\Lambda(G)_S^{\times}$ in $K_1(\Lambda(G)_S)$. Now we can reduce (5·10) 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

$$\left(r_{i,1}^{l_{i,1}}f_{i,1}^{k_{i,1}}r_{i,1}^{-l_{i,1}}\right) \equiv f_{i,1}^{k_{i,1}} \mod (X, p) \tag{5·11}$$

$$\left(r_{j,2}^{l_{j,2}}f_{j,2}^{k_{j,2}}r_{j,2}^{-l_{j,2}}\right) \equiv f_{j,2}^{k_{j,2}} \mod (X, p) \text{ and} \tag{5·12}$$

$$\xi_M \equiv Y^{\mathrm{rank}_{\Lambda(H)}(M)} \mod (X, p). \tag{5·13}$$

So the reduced functional equation is in the form

$$\left(\frac{1}{1+Y}-1\right)^{\mathrm{rank}_{\Lambda(H)}(M)} = \widetilde{\varepsilon(M)}Y^{\mathrm{rank}_{\Lambda(H)}(M)}. \tag{5·14}$$

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

6. *Pairings*

Following the ideas of Perrin–Riou [**21**] 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 $p \geqslant 5$. Moreover, let us assume that the dual of the Selmer group, $X(E/F_\infty)$ lies in the category $\mathfrak{M}_H(G)$. The strategy is that we take the projective limit of the homomorphisms

$$X\left(E/F_n^{cyc}\right) \longrightarrow a^1_{\Lambda(\Gamma)}\left(X\left(E/F_n^{cyc}\right)^{\#}\right) \tag{6·1}$$

constructed by Perrin–Riou [**21**] to get a map

$$X(E/F_\infty) \longrightarrow a^1_{\Lambda(G)}(X(E/F_\infty)^{\#}). \tag{6·2}$$

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 $X(E/F_\infty)$.

6·1. *Control theorems*

In this section we put together the already known [**17**, **21**] facts about the kernels and cokernels of the homomorphisms

$$H_0(X(E/F_\infty), H_n) \longrightarrow X\left(E/F_n^{cyc}\right) \qquad \text{and} \tag{6·3}$$

$$X\left(E/F_n^{cyc}\right) \longrightarrow a^1_{\Lambda(\Gamma)}\left(X\left(E/F_n^{cyc}\right)^{\#}\right). \tag{6·4}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

As in [**17**] 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,

$$P_1 := \{u \in P_0 \mid E/K^{cyc} \text{ has split multiplicative reduction at } u\} \tag{6·5}$$

$$P_2 := \{u \in P_0 \mid E \text{ has good reduction at } u \text{ and } E[p^\infty](K_u^{cyc}) \neq 0\}, \tag{6·6}$$

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 (6·3) and the kernel of (6·4) are bounded by $|E[p^\infty](F_\infty)|$, which is finite ([**17**, lemma 3·12]).

The kernel of (6·3) equals the Pontryagin dual of

$$\bigoplus_{u\in P_1\cup P_2,\ u|w} H^1(H_{n,w}, E[p^\infty](F_{\infty,w})) \tag{6·7}$$

modulo finite modules which are bounded by $|E[p^\infty](F_\infty)|$ [**17**]. Moreover, as $\mathrm{Gal}(F_n^{cyc}/K)_v$-modules

$$H^1(H_{n,w}, E[p^\infty](F_{\infty,w})) \cong \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p(-1) & \text{if } w \text{ corresponds to a prime } v \in P_1, \\ E[p^\infty](-1) & \text{if } w \text{ corresponds to a prime } v \in P_2, \end{cases} \tag{6·8}$$

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

$$0 \longrightarrow \mu_{p^\infty} \longrightarrow E[p^\infty] \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0 \tag{6·9}$$

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

$$0 \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1(H_{n,w}, \mu_{p^\infty}) \longrightarrow H^1(H_{n,w}, E[p^\infty]) \longrightarrow H^1(H_{n,w}, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow 0, \tag{6·10}$$

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

$$H^1(H_{n,w}, \mu_{p^\infty}) \cong \mathbb{Q}_p/\mathbb{Z}_p \qquad \text{and} \tag{6·11}$$

$$H^1(H_{n,w}, E[p^\infty]) \cong H^1(H_{n,w}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Q}_p/\mathbb{Z}_p(-1). \tag{6·12}$$

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 (6·4) equals the following modulo finite modules with order bounded by $|E[p^\infty](F_\infty)|$ [**15**, **21**]

$$\mathrm{Hom}\left(\varinjlim_{k\infty} \bigoplus_{u\in P_1^{(n)}} H^1\big(\Gamma_k, E[p^\infty]\big(F_{n,u}^{cyc}\big)\big), \mathbb{Q}_p/\mathbb{Z}_p\right). \tag{6·13}$$

Now since $E[p^\infty](F_{\infty,w}) = E[p^\infty]$ for any prime w above a prime in P_1 [**16**, **17**] (because F_∞ is the maximal tame p-extension), we have the exact sequence

$$0 \longrightarrow \mu_{p^\infty} \longrightarrow E[p^\infty]\big(F_{n,u}^{cyc}\big) \longrightarrow \mathbb{Z}/p^{r_n}\mathbb{Z} \longrightarrow 0 \tag{6·14}$$

with some $r_n \geqslant 0$ 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

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

PROPOSITION 6·1. *There exists a map*

$$X\big(E/F_n^{cyc}\big)\big(\longrightarrow a^1_{\Lambda(\Gamma)}\big(X\big(E/F_n^{cyc}\big)^{\#}\big)\big) \longrightarrow a^1_{\Lambda(\Gamma)}(H_0(H_n, X(E/F_\infty)^{\#})) \tag{6·15}$$

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

$$\bigoplus_{u\in P_2^{(n)}} T_p\big(E[p^\infty]\big(F_{n,u}^{cyc}\big)\big)^{\vee} \oplus \bigoplus_{u\in P_1^{(n)}} M_u^{(n)} \tag{6·16}$$

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

$$0 \longrightarrow \mathbb{Z}_p/p^{r_n}\mathbb{Z}_p \longrightarrow M_u^{(n)} \longrightarrow \mathbb{Z}_p(-1) \longrightarrow 0, \tag{6·17}$$

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

Proof. The quasi-exact sequence

$$0 \longrightarrow \bigoplus_{u\in P_1^{(n)}\cup P_2^{(n)},\, u|w} \mathrm{Hom}(H^1(H_{n,w}, E[p^\infty](F_{\infty,w})), \mathbb{Q}_p/\mathbb{Z}_p)^{\#} \tag{6·18}$$

$$\longrightarrow H_0(H_n, X(E/F_\infty)^{\#}) \longrightarrow X(E/F_n^{cyc})^{\#} \longrightarrow 0 \tag{6·19}$$

defines a quasi-exact sequence of extension functors

$$0 \longrightarrow a^1_{\Lambda(\Gamma)}\big(X\big(E/F_n^{cyc}\big)^{\#}\big) \longrightarrow a^1_{\Lambda(\Gamma)}(H_0(H_n, X(E/F_\infty)^{\#})) \tag{6·20}$$

$$\longrightarrow \bigoplus_{u\in P_1^{(n)}\cup P_2^{(n)},\, u|w} a^1_{\Lambda(\Gamma)}(\mathrm{Hom}(H^1(H_{n,w}, E[p^\infty](F_{\infty,w})), \mathbb{Q}_p/\mathbb{Z}_p)^{\#}) \longrightarrow 0, \tag{6·21}$$

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

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

$$H^1(H_{n,w}, E[p^\infty](F_{\infty,w})) = E[p^\infty](-1) \tag{6·22}$$

and therefore

$$a^1_{\Lambda(\Gamma)}(\mathrm{Hom}(H^1(H_{n,w}, E[p^\infty](F_{\infty,w})), \mathbb{Q}_p/\mathbb{Z}_p)^{\#}) \cong T_p(E[p^\infty])^{\vee}. \tag{6·23}$$

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

$$X\big(E/F_n^{cyc}\big) \longrightarrow a^1_{\Lambda(\Gamma)}\big(X\big(E/F_n^{cyc}\big)^{\#}\big). \tag{6·24}$$

On the other hand, if u is in P_1 then

$$H^1(H_{n,w}, E[p^\infty](F_{\infty,w})) = \mathbb{Q}_p/\mathbb{Z}_p(-1) \tag{6·25}$$

and therefore

$$a^1_{\Lambda(\Gamma)}(\mathrm{Hom}(H^1(H_{n,w}, E[p^\infty](F_{\infty,w})), \mathbb{Q}_p/\mathbb{Z}_p)^{\#}) \cong \mathbb{Z}_p(-1). \tag{6·26}$$

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

$$X\big(E/F_n^{cyc}\big) \longrightarrow a^1_{\Lambda(\Gamma)}\big(X\big(E/F_n^{cyc}\big)^{\#}\big). \tag{6·27}$$

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

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

6·2. *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 [**14**, **21**]. 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 [**3**, **4**, **13**].

THEOREM 6·2. *If E has good ordinary reduction at the prime $p \geqslant 5$ and $X(E/F_\infty)$ lies in the category $\mathfrak{M}_H(G)$ then there is an exact sequence*

$$0 \longrightarrow X(E/F_\infty) \xrightarrow{\varphi} a^1_{\Lambda(G)}(X(E/F_\infty)^\#) \longrightarrow \mathrm{Coker}(\varphi) \longrightarrow 0, \tag{6·28}$$

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

$$\bigoplus_{v \in P_1(K) \cup P_2(K)} \Lambda(G) \otimes_{\Lambda(G_v)} T_p(E[p^\infty](F_{\infty,w}))^\vee, \tag{6·29}$$

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

$$\Lambda(G) \otimes_{\Lambda(G_v)} T_p(E[p^\infty](F_{\infty,w}))^\vee \cong \bigoplus_{u \in P_1 \cup P_2,\ v|u|w} T_p(E[p^\infty](F_{\infty,w}))^\vee \tag{6·30}$$

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 (6·30).

We would like to take the projective limit of homomorphisms in Proposition 6·1

$$X\left(E/F_n^{cyc}\right) \longrightarrow a^1_{\Lambda(\Gamma)}(H_0(H_n, X(E/F_\infty)^\#)). \tag{6·31}$$

For this we first remark that there is a canonical identification

$$a^1_{\Lambda(\Gamma)}(H_0(H_n, X(E/F_\infty)^\#)) \cong a^1_{\Lambda(\mathrm{Gal}(F_n^{cyc}/K))}(H_0(H_n, X(E/F_\infty)^\#)) \tag{6·32}$$

as $\Lambda(\Gamma)$-modules [**18**]. Moreover the norm map from F_{n+1}^{cyc} to F_n^{cyc} induces a natural homomorphism

$$a^1_{\Lambda(\mathrm{Gal}(F_{n+1}^{cyc}/K))}(H_0(H_{n+1}, X(E/F_\infty)^\#)) \longrightarrow a^1_{\Lambda(\mathrm{Gal}(F_n^{cyc}/K))}(H_0(H_n, X(E/F_\infty)^\#)), \tag{6·33}$$

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

$$\bigoplus_{u \in P_2,\ u|w} T_p(E[p^\infty](F_{\infty,w}))^\vee \oplus \bigoplus_{u \in P_1} \varprojlim M_u^{(n)} \tag{6·34}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

up to finite modules. Because of (6·17) and the fact that $r_n \to \infty$ the projective limit of the modules $M_u^{(n)}$ fits into the exact sequence

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow \varprojlim M_u^{(n)} \longrightarrow \mathbb{Z}_p(-1) \longrightarrow 0. \tag{6·35}$$

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.

(i) For any w above a prime in P_1

$$T_p(E[p^\infty](F_{\infty,w}))^\vee \tag{6·36}$$

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

$$\mathbb{Z}_p \oplus \mathbb{Z}_p(-1) \tag{6·37}$$

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

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow T_p(E[p^\infty](F_{\infty,w}))^\vee \longrightarrow \mathbb{Z}_p(-1) \longrightarrow 0. \tag{6·38}$$

However, this exact sequence does not split.

(ii) 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

$$\bigoplus_{q \in P_1(\mathbb{Q}) \cup P_2(\mathbb{Q})} \Lambda(G_0) \otimes_{\Lambda(G_q)} T_p(E[p^\infty](F_{\infty,w}))^\vee, \tag{6·39}$$

where w is a prime in F_∞ above q.

6·3. *Functional equation of the characteristic element*

We are going to apply Theorems 6·2 and 5·5. Note that by Lemma 5·4 the characteristic element of

$$a^1_{\Lambda(G)}(X(E/F_\infty)^\#) \tag{6·40}$$

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 [**17**]. We get the following corollary on the characteristic element.

COROLLARY 6·3. *If E has good ordinary reduction at the prime $p \geqslant 5$ 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*

$$\xi^\#_{X(E/F_\infty)} = \xi_{X(E/F_\infty)} \varepsilon_0(X(E/F_\infty)) \prod_{v \in P_1(K) \cup P_2(K)} \alpha_v, \tag{6·41}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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

$$\alpha_v = \frac{\mathrm{Frob}_v^{-1} - \dfrac{(X+1)^{-N_{K/\mathbb{Q}}v} - 1}{\dfrac{1}{X+1} - 1}}{\mathrm{Frob}_v - \dfrac{(X+1)^{N_{K/\mathbb{Q}}v} - 1}{X}} \qquad \text{if } v \text{ is in } P_1(K) \text{ and} \tag{6·42}$$

$$\alpha_v = \frac{\left(\mathrm{Frob}_v^{-1} - \dfrac{(X+1)^{-b_v} - 1}{\dfrac{1}{X+1} - 1}\right)\left(\mathrm{Frob}_v^{-1} - \dfrac{(X+1)^{-N_{K/\mathbb{Q}}v} - 1}{\dfrac{1}{(X+1)^{b_v}} - 1}\right)}{\left(\mathrm{Frob}_v - \dfrac{(X+1)^{b_v} - 1}{X}\right)\left(\mathrm{Frob}_v - \dfrac{(X+1)^{N_{K/\mathbb{Q}}v} - 1}{(X+1)^{b_v} - 1}\right)} \text{ if } v \text{is in } P_2(K), \tag{6·43}$$

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

$$x^2 - (N_{K/\mathbb{Q}}v + 1 - \#\tilde{E}(\mathbb{F}_v))x + N_{K/\mathbb{Q}}v \tag{6·44}$$

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 $M \otimes_{\Lambda(G_v)} \Lambda(G)$ 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 6·2, we only have to verify the following statements. Firstly, there exists an element b_v in $\mathbb{Z}_p$ with

$$b_v^2 - (N_{K/\mathbb{Q}}v + 1 - \#\tilde{E}(\mathbb{F}_v))b_v + N_{K/\mathbb{Q}}v = 0 \tag{6·45}$$

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

$$\frac{\left(\mathrm{Frob}_v^{-1} - \dfrac{(X+1)^{-b_v} - 1}{\dfrac{1}{X+1} - 1}\right)\left(\mathrm{Frob}_v^{-1} - \dfrac{(X+1)^{-N_{K/\mathbb{Q}}v} - 1}{\dfrac{1}{(X+1)^{b_v}} - 1}\right)}{\left(\mathrm{Frob}_v - \dfrac{(X+1)^{b_v} - 1}{X}\right)\left(\mathrm{Frob}_v - \dfrac{(X+1)^{N_{K/\mathbb{Q}}v} - 1}{(X+1)^{b_v} - 1}\right)} \tag{6·46}$$

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

$$0 \longrightarrow X(T_p(E[p^\infty])^\vee \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[X]]) \longrightarrow T_p(E[p^\infty])^\vee \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[X]] \longrightarrow T_p(E[p^\infty]) \longrightarrow 0. \tag{6·47}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

Moreover, the numerator of (6·46) reduces to the characteristic polynomial of Frob_v^{-1} modulo X so it is a characteristic element to

$$T_p(E[p^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[X]]. \tag{6·48}$$

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

$$X(T_p(E[p^\infty])^\vee \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[X]]) \cong T_p(E[p^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[X]], \tag{6·49}$$

so the denominator

$$\begin{aligned}&\left(\mathrm{Frob}_v - \frac{(X+1)^{b_v}-1}{X}\right)\left(\mathrm{Frob}_v - \frac{(X+1)^{N_{K/\mathbb{Q}}v}-1}{(X+1)^{b_v}-1}\right)\\ &= \left(\left(\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-b_v}-1}{\frac{1}{X+1}-1}\right)\left(\mathrm{Frob}_v^{-1} - \frac{(X+1)^{-N_{K/\mathbb{Q}}v}-1}{\frac{1}{(X+1)^{b_v}}-1}\right)\right)^{\#}\end{aligned} \tag{6·50}$$

is a characteristic element to

$$X(T_p(E[p^\infty])^\vee \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[X]]). \tag{6·51}$$

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

$$\frac{\mathrm{Frob}_v^{-1} - \dfrac{(X+1)^{-N_{K/\mathbb{Q}}v}-1}{\dfrac{1}{X+1}-1}}{\mathrm{Frob}_v - \dfrac{(X+1)^{N_{K/\mathbb{Q}}v}-1}{X}} \tag{6·52}$$

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

$$\mathrm{Frob}_v(X+1)\mathrm{Frob}_v^{-1} = (X+1)^{N_{K/\mathbb{Q}}v} \tag{6·53}$$

it is easy to see that the following sequences are exact

$$0 \longrightarrow \Lambda(G_v)\Big/\left(\mathrm{Frob}_v - \frac{(X+1)^{N_{K/\mathbb{Q}}v}-1}{X}\right) \longrightarrow \Lambda(G)/(\mathrm{Frob}_v - 1) \longrightarrow \mathbb{Z}_p \longrightarrow 0, \tag{6·54}$$

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

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 5·5 and the formula [**17**]

$$\mathrm{rank}_{\Lambda(H)}(X(E/F_\infty)) = \mathrm{rank}_{\mathbb{Z}_p}(X(E/K^{cyc})) + |P_1(K)| + 2|P_2(K)|, \tag{6·55}$$

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. (i) 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

$$\xi_{\mathbb{Q},X(E/F_\infty)}^{\#} = \xi_{\mathbb{Q},X(E/F_\infty)}\varepsilon_0(\mathbb{Q}, X(E/F_\infty)) \prod_{q \in P_1(\mathbb{Q}) \cup P_2(\mathbb{Q})} \alpha_q. \tag{6·56}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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

$$\alpha_q = \frac{\mathrm{Frob}_q^{-1} - \dfrac{(X+1)^{-q}-1}{\dfrac{1}{X+1}-1}}{\mathrm{Frob}_q - \dfrac{(X+1)^q-1}{X}} \qquad \text{if } q \text{ is in } P_1(\mathbb{Q}) \text{ and} \tag{6·57}$$

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

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

$$x^2 - (q+1-\#\tilde{E}(\mathbb{F}_q))x + q \tag{6·58}$$

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

(ii) We chose a different normalization of the characteristic element of the cokernel in the above theorem from the one in Section 5 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 $\alpha_q\alpha_q^\# = 1$.

7. *Connections to the analytic side*

In this section we formulate the Main Conjecture for elliptic curves over the false Tate curve extension similarly to the GL_2 Main Conjecture introduced by Coates *et. al.* [**4**]. Then we compare the algebraic functional equation we got in the previous section for the characteristic element of the dual Selmer group and the conjectural functional equation of the p-adic L-function.

7·1. *The main conjecture*

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). It is Deligne's period conjecture [**9**] – which has already been proved [**2**] in the case when τ factors through the false Tate curve extension – that

$$\frac{L(E,\tau,1)}{\Omega_+(E)^{d^+(\tau)}\Omega_-(E)^{d^-(\tau)}} \in \overline{\mathbb{Q}}. \tag{7·1}$$

Let R denote the following set of rational primes

$$R := \{p\} \bigcup \{q \in \mathbb{Q} \text{ prime} : q \mid m \text{ and } E[p^\infty] \subseteq F_{\infty,w} \text{ for a } w \in F_\infty \text{ above } q\}. \tag{7·2}$$

We define the modified L-function

$$L_R(E,\tau,s) := \prod_{q \notin R} P_q(E,\tau,q^{-s})^{-1} \tag{7·3}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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

$$P_p(E,T) = 1 - a_pT + pT^2 = (1 - b_pT)(1 - c_pT), \qquad b_p \in \mathbb{Z}_p^\times, \tag{7·4}$$

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

CONJECTURE 7·1. *Assume that $p \geqslant 5$ and that E has good ordinary reduction at p. Then there exists $\mathfrak{L}_E$ in $K_1(\Lambda(G_0)_{S_\mathbb{Q}^*})$ such that, for all Artin representations τ of G_0, we have $\mathfrak{L}_E(\tau) \neq \infty$, and*

$$\mathfrak{L}_E(\tau^*) = \frac{L_R(E,\tau,1)}{\Omega_+(E)^{d^+(\tau)}\Omega_-(E)^{d^-(\tau)}} \cdot \varepsilon_p(\tau) \cdot \frac{P_p(\tau^*, b_p^{-1})}{P_p(\tau, c_p^{-1})} \cdot b_p^{-f_\tau}, \tag{7·5}$$

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 ([**4**, conjecture 5·7]), 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. The set defined in (7·2) is the right generalization to the false Tate curve case, since we only have to remove the Euler factors corresponding to those primes which both ramify infinitely in this extension, and satisfy the condition that if we complete F_∞ at a prime above them then the completion contains all the p-division points on the curve. This latter assumption is automatic for any prime in the GL_2-case.

Now we can state the main conjecture of Iwasawa theory for elliptic curves over the false Tate tower.

CONJECTURE 7·2 (The main conjecture). *Assume that $p \geqslant 5$, E has good ordinary reduction at p, and $X(E/F_\infty)$ belongs to the category $\mathfrak{M}_{H_0}(G_0)$. Granted Conjecture 7·1, the p-adic L-function $\mathfrak{L}_E$ in $K_1(\Lambda(G_0)_{S_\mathbb{Q}^*})$ is a characteristic element of $X(E/F_\infty)$.*

7·2. *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 7·3. *The values of α_q at irreducible Artin representations of G_0 are as follows*:

$$\alpha_q(\chi) = \frac{P_q(E,\chi,q^{-1})}{P_q(E,\overline{\chi},q^{-1})} \text{ and} \tag{7·6}$$

$$\alpha_q(\rho_n\chi) = \begin{cases} \left(\dfrac{q}{p}\right)\dfrac{P_q(E,\rho_n\chi,q^{-1})}{P_q(E,\rho_n\overline{\chi},q^{-1})}\chi(\mathrm{Frob}_q^{-1})^{p^{n-1}(p-1)}, & \text{if} \quad q \in P_1(\mathbb{Q}) \\ \dfrac{P_q(E,\rho_n\chi,q^{-1})}{P_q(E,\rho_n\overline{\chi},q^{-1})}, & \text{if} \quad q \in P_2(\mathbb{Q}), \end{cases} \tag{7·7}$$

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

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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 7·1 we have

$$\mathfrak{L}_E(\tau^*) = \frac{L_R(E,\tau,1)}{\Omega_+(E)^{d^+(\tau)}\Omega_-(E)^{d^-(\tau)}} \cdot \varepsilon_p(\tau) \cdot \frac{P_p\left(\tau^*, b_p^{-1}\right)}{P_p\left(\tau, c_p^{-1}\right)} \cdot b_p^{-f_\tau} \text{ and} \tag{7·8}$$

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

Moreover, the functional equation of the complex L is

$$\hat{L}(E,\tau,s) = w(E,\tau)\hat{L}(E,\tau^*,2-s), \tag{7·9}$$

where

$$\hat{L}(E,\tau,s) := \left(\frac{N(E,\tau)}{\pi^{2\dim\tau}}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{\dim\tau} \Gamma\left(\frac{s+1}{2}\right)^{\dim\tau} L(E,\tau,s). \tag{7·10}$$

From this we get that

$$L(E,\tau,1) = w(E,\tau)L(E,\tau^*,1) \tag{7·11}$$

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 (7·8) and (7·11) we get that

$$\frac{\mathcal{L}_E(\tau^*)}{\prod_{q\in R\setminus\{p\}} P_q(E,\tau,q^{-1})} \quad \text{and} \quad \frac{\mathcal{L}_E^{\#}(\tau^*)}{\prod_{q\in R\setminus\{p\}} P_q(E,\tau^*,q^{-1})} \tag{7·12}$$

are equal up to p-adic units. So Proposition 7·3 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 7·4. *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.*

$$w_{\mathrm{alg}}(E,\tau) = \begin{cases} (-1)^{t_{E/\mathbb{Q},p}} & \text{if } \tau \text{ is the trivial representation,} \\ (-1)^{t_{E/\mathbb{Q},p}+t_{E/K,p}} & \text{if } \tau \text{ is the real character of order 2,} \\ (-1)^{t_{E/K,p}} \prod_{q\in P_1(\mathbb{Q})} \left(\frac{q}{p}\right) & \text{if } \tau = \rho_n \text{ for some } n, \\ 1 & \text{if } \tau = \chi \oplus \overline{\chi} \text{ or } \rho_n \otimes (\chi \oplus \overline{\chi}) \text{ for some } n \text{ and} \\ & \qquad \chi \text{ character of } \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}), \end{cases} \tag{7·13}$$

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

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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 7·3. The statement regarding the sign in the analytic functional equation follows from the formulae for the root numbers [**10**], 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 [**20**]. For this let us reduce the equation

$$\xi^{\#}_{\mathbb{Q},X(E/F_\infty)} = \xi_{\mathbb{Q},X(E/F_\infty)}\varepsilon_0(\mathbb{Q}, X(E/F_\infty)) \prod_{q\in P_1(\mathbb{Q})\cup P_2(\mathbb{Q})} \alpha_q \tag{7·14}$$

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

$$\tilde{\xi}^{\#}_{\mathbb{Q},X(E/F_\infty)} \prod_{q\in P_1(\mathbb{Q})} (\mathrm{Frob}_q - q) \prod_{q\in P_2(\mathbb{Q})} (\mathrm{Frob}_q - b_q)(\mathrm{Frob}_q - q/b_q) \tag{7·15}$$

$$= \tilde{\xi}_{\mathbb{Q},X(E/F_\infty)}\tilde{\varepsilon}_0(\mathbb{Q}, X(E/F_\infty)) \prod_{q\in P_1(\mathbb{Q})} \left(\mathrm{Frob}_q^{-1} - q\right) \prod_{q\in P_2(\mathbb{Q})} \left(\mathrm{Frob}_q^{-1} - b_q\right)\left(\mathrm{Frob}_q^{-1} - q/b_q\right).$$

Now $\tilde{\xi}_{\mathbb{Q},X(E/F_\infty)}$ 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

$$(-1)^{t_{E/K,p}} = (-1)^{\mathrm{rank}_{\Lambda(H)}(X(E/F_\infty))} \prod_{q\in P_1(\mathbb{Q})} \left(\frac{q}{p}\right), \tag{7·16}$$

on the right-hand side of the equation (7·15) 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.

8. *Heegner-like cases*

Throughout this section we shall need the following hypotheses on p and the elliptic curve E imposed in [**3**].

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

$$\bigoplus_i \mathbb{Z}_p[[T]]/p^{\mu_i} \oplus \bigoplus_j \mathbb{Z}_p[[T]]/f_j^{m_j}, \tag{8·1}$$

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

$$f_M = \prod_i p^{\mu_i} \prod_j f_j^{m_j} \tag{8·2}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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 $\mu_{E/K} = 0$ [**17**].

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

$$p^{\mathrm{rank}_{\Omega(G)}\mathrm{gr}_p(M)} \tag{8·3}$$

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 8·1. *If E is an elliptic curve and $p \geqslant 5$ 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 $K \leqslant L \leqslant F_\infty$ 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 [**5**]. 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 $\Lambda(\mathrm{Gal}(F_\infty/L))$.

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:

$$P_1 = \{q \mid E \text{ has split multiplicative reduction at all primes } v \text{ of } K \text{ above } q\}, \tag{8·4}$$
$$P_2 = \{q \mid q \neq p, E \text{ has good reduction at } q, \tilde{E}_v(k_v)(p) \neq 0 \text{ for a } v \in K \text{ above } q\}:$$

The following proposition can be found in [**3**].

PROPOSITION 8·2. *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 subsections deal with these two cases.

8·1. *The classical case*

In this section let us assume the second case of Proposition 8·2. Therefore we have that $g_{E/F_n} \leqslant p^n \leqslant r_{E/F_n}$ for any positive integer n (see [**11**, appendix A]). 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 $n \geqslant 1$ [**3**]. Since there is an injective $\Lambda(H)$-homomorphism

$$Y(E/F_\infty) \hookrightarrow \Lambda(H) \tag{8·5}$$

with finite cokernel [**17**], 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

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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 8·3. *Under the Hypotheses* 1 *and* 2 *and the second case of Proposition* 8·2 *we have the following functional equation for the power series* $f(X)$:

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

$$f(0) = 1 \tag{8·6}$$

where ζ_{p^n} *is an arbitrary primitive* p^n*th root of unity* ($n \geqslant 1$ *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 $f_1(X) \in Y(E/F_\infty) \leqslant \mathbb{Z}_p[[X]]$ 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

$$Y(E/F_\infty)_{H_n} \longrightarrow Y\left(E/F_n^{cyc}\right) \tag{8·7}$$

are finite [**17**] and the characteristic element of $Y(E/F_n^{cyc})$ is T^{p^n}, the Akashi series (i.e. 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

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} (Y(E/F_\infty)/((X+1)^{p^n} - 1)Y(E/F_\infty)). \tag{8·8}$$

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

$$\tilde{\gamma}^{p^{n-1}} f_1(X) = \tilde{\gamma}^{p^{n-1}} f_1(X)\tilde{\gamma}^{-p^{n-1}} \prod_{j=0}^{p^{n-1}-1} \tilde{\gamma}^j f(X)\tilde{\gamma}^{-j}. \tag{8·9}$$

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

$$\prod_{j=0}^{p^{n-1}-1} f\left(\zeta_{p^n}^{\tilde{\gamma}^{-j}} - 1\right) = \prod_{j=0}^{p^{n-1}-1} f\left(\zeta_{p^n}^{1+jp} - 1\right) \tag{8·10}$$

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 $\mathrm{Gal}(F_n/K)$.

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

PROPOSITION 8·4. *Under the Hypotheses* 1 *and* 2 *and the second case of Proposition* 8·2*, 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

$$\rho_n(\tilde{\gamma})=\begin{pmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&&0&\ddots&\vdots\\0&\vdots&\vdots&\ddots&1\\1&0&0&\cdots&0\end{pmatrix},\qquad \rho_n(h)=\begin{pmatrix}\zeta&0&0&\cdots&0\\0&\zeta^{\tilde{\gamma}}&0&\cdots&0\\\vdots&0&\zeta^{\tilde{\gamma}^2}&\ddots&\vdots\\0&\vdots&\ddots&\ddots&0\\0&0&\cdots&0&\zeta^{\tilde{\gamma}^{p^{n-1}-1}}\end{pmatrix}, \quad (8\cdot11)$$

where ζ is a primitive p^nth root of unity, we have that the matrix of $\tilde{\gamma}|_{\mathrm{tw}_{\rho_n}(Y(E/F_\infty))_H}$ is

$$\begin{pmatrix}0&f(\zeta^{-1}-1)&0&\cdots&0\\0&0&f(\zeta^{-\tilde{\gamma}}-1)&\cdots&0\\\vdots&&0&\ddots&\vdots\\0&\vdots&\vdots&\ddots&f(\zeta^{-\tilde{\gamma}^{p^{n-1}-2}}-1)\\f(\zeta^{-\tilde{\gamma}^{p^{n-1}-1}}-1)&0&0&\cdots&0\end{pmatrix}, \quad (8\cdot12)$$

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 8·3.

Applying the Artin-formalism for Akashi series ([11, theorem A·44], see also [**3**]) and Proposition 8·1 we get the following corollary.

COROLLARY 8·5. *Under the Hypotheses* 1 *and* 2 *and the second case of Proposition* 8·2*, the characteristic element of the* Γ*-module* $X(E/\mathbb{Q}(\mu_p,\sqrt[p^n]{m})^{cyc})$ *is*

$$T\prod_{j=0}^{n-1}((T+1)^{p^j}-1)^{p-1}p^{p^n\mu_{E/K}}. \quad (8\cdot13)$$

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 8·8.

LEMMA 8·6. *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*

$$h(X)\equiv\sum_{i=0}^{k}a_i\frac{(X+1)^{p^k}-1}{(X+1)^{p^i}-1}\mod((X+1)^{p^k}-1), \quad (8\cdot14)$$

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

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 $((X+1)^{p^k}-1)/((X+1)^{p^i}-1)$ in $\mathbb{Z}_p[H/H_n]$ is the sum of elements of order at least p^i, it follows that $\tilde{\gamma}_0$ acts trivially on these elements. The other direction is

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

also true because if $\tilde{\gamma}_0$ acts trivially on some element in $\mathbb{Z}_p[H/H_n]$ 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^i is $((X+1)^{p^k}-1)/((X+1)^{p^i}-1) - ((X+1)^{p^k}-1)/((X+1)^{p^{i-1}}-1)$.

LEMMA 8·7. *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*

$$1 + \sum_{i=0}^{k-1} a_i (\zeta_{p^{k+1}}-1)^{p^k - p^i} \tag{8·15}$$

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

Proof. At first note that if the integer j is not divisible by $p-1$ then if we denote by v_{k+1} the $(\zeta_{p^{k+1}}-1)$-valuation on $\mathbb{Z}_p[\zeta_{p^{k+1}}]$, we have that

$$j = v_{k+1}((\zeta_{p^{k+1}}-1)^j) = v_{k+1}((1+(\zeta_{p^{k+1}}-1)^j s)^{1-\tilde{\gamma}_0} - 1) \tag{8·16}$$

for any s invertible element in $\mathbb{Z}_p[\zeta_{p^{k+1}}]$. This is true because

$$(\zeta_{p^{k+1}}-1)^{j\tilde{\gamma}_0} = \left(\zeta_{p^{k+1}}^{\chi(\tilde{\gamma}_0)}-1\right)^j \equiv \chi(\tilde{\gamma}_0)^j (\zeta_{p^{k+1}}-1)^j \pmod{(\zeta_{p^{k+1}}-1)^{j+1}}. \tag{8·17}$$

Let us assume now indirectly that x_{k+1} is not in the required form. Now equation (8·16) shows that $v_{k+1}(x_{k+1}-1)$ is divisible by $p-1$ because otherwise $x_{k+1}^{1-\tilde{\gamma}_0}$ could not be congruent to 1 modulo $(\zeta_{p^{k+1}}-1)^{p^k}$. Moreover, we claim that if j is not divisible by p then we have that

$$\begin{aligned} p^r(p-1)j + p^r &\leqslant v_{k+1}\left(\left(1+(\zeta_{p^{k+1}}-1)^{p^r(p-1)j}s\right)^{1-\tilde{\gamma}_0}-1\right) \\ &\leqslant p^r(p-1)j + p^{r+1} - 1 \end{aligned} \tag{8·18}$$

for any s invertible element in $\mathbb{Z}_p[\zeta_{p^{k+1}}]$ and provided that

$$p^r(p-1)j + p^{r+1} - 1 < p^{k+1} - p^k = v_{k+1}(p). \tag{8·19}$$

From this we get the statement because the v_{k+1}-valuation of $x_{k+1}-1$ can only be $p^k - p^i$ for some i in the set $\{0, 1, \ldots, k-1\}$ since this valuation is divisible by $p-1$ so is in the form $p^r(p-1)j$ for some positive integer j coprime to p and nonnegative integer r. Moreover, we are only interested in x_{k+1} modulo $(\zeta_{p^{k+1}}-1)^{p^k}$, so we may assume that $p^r(p-1)j < p^k$. Now by (8·18) the valuation of $x_{k+1}^{1-\tilde{\gamma}_0} - 1$ is at most $p^r(p-1)j + p^{r+1} - 1$. However, by assumption it is at least p^k. This means that

$$\begin{aligned} p^r(p-1)j + p^{r+1} - 1 &> p^k - 1 \\ v_{k+1}(x_{k+1}-1) = p^r(p-1)j &> p^k - p^{r+1}. \end{aligned} \tag{8·20}$$

The only number divisible by $p^r(p-1)$ which is greater than $p^k - p^{r+1}$ and less than p^k is $p^k - p^r$ so the v_{k+1}-valuation of $x_{k+1}-1$ is in this form. Moreover, by Lemma 8·6 we have that

$$\left(1 + a_i \frac{(X+1)^{p^k}-1}{(X+1)^{p^i}-1}\right)^{1-\tilde{\gamma}_0} \equiv 1 (\mathrm{mod}\,(X+1)^{p^k}-1 \tag{8·21}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

and if we substitute $\zeta_{p^{k+1}}-1$ into X and reduce the equation modulo p (p is divisible by $\zeta_{p^{k+1}}^{p^k}-1$ in $\mathbb{Z}_p[\zeta_{p^{k+1}}]$) we get that

$$(1+a_i(\zeta_{p^{k+1}}-1)^{p^k-p^i})^{1-\tilde{\gamma}_0}\equiv 1 \pmod{(\zeta_{p^{k+1}}-1)^{p^k}}, \tag{8·22}$$

so we can multiply x_{k+1} by $1+a_i(\zeta_{p^{k+1}}-1)^{p^k-p^i}$ to remove the coefficient of

$$(\zeta_{p^{k+1}}-1)^{p^k-p^i} \tag{8·23}$$

in x_{k+1} such that $x_{k+1}^{1-\tilde{\gamma}_0}$ does not change modulo $(\zeta_{p^{k+1}}-1)^{p^k}$. This can be done since

$$x_{k+1}(1+a_i(\zeta_{p^{k+1}}-1)^{p^k-p^i})\equiv x_{k+1}+a_i(\zeta_{p^{k+1}}-1)^{p^k-p^i} \pmod{(\zeta_{p^{k+1}}-1)^{p^k}}, \text{ and} \tag{8·24}$$

$$\begin{aligned}&(1+a_i(\zeta_{p^{k+1}}-1)^{p^k-p^i})(1+a_{i'}(\zeta_{p^{k+1}}-1)^{p^k-p^{i'}})\\ &\quad\equiv 1+a_i(\zeta_{p^{k+1}}-1)^{p^k-p^i}+a_{i'}(\zeta_{p^{k+1}}-1)^{p^k-p^{i'}} \pmod{(\zeta_{p^{k+1}}-1)^{p^k}}.\end{aligned} \tag{8·25}$$

Now we can remove the coefficients of $(\zeta_{p^{k+1}}-1)^{p^k-p^i}$ for all i, however, it followed from the indirect assumption that the valuation of $x_{k+1}-1$ was p^k-p^r for some r (see (8·20)). This is a contradiction and we are done. So it remains to prove the claim (8·18).

Proof of the claim. We can work modulo p because the v_{k+1}-valuation of p is $p^{k+1}-p^k > p^r(p-1)j+p^{r+1}-1$. At first we prove that

$$p^r(p-1)j+p^r \leqslant v_{k+1}\big(\big(1+(\zeta_{p^{k+1}}-1)^{p^r(p-1)j}s\big)^{1-\tilde{\gamma}_0}-1\big). \tag{8·26}$$

Indeed, we have

$$\begin{aligned}&\big(1+(\zeta_{p^{k+1}}-1)^{p^r(p-1)j}s\big)^{1-\tilde{\gamma}_0}-1\\ &\quad=s\frac{(\zeta_{p^{k+1}}-1)^{p^r(p-1)j}-(\zeta_{p^{k+1}}-1)^{p^r(p-1)j\tilde{\gamma}_0}}{\big(1+(\zeta_{p^{k+1}}-1)^{p^r(p-1)j}s\big)^{\tilde{\gamma}_0}}\end{aligned} \tag{8·27}$$

and after dividing by units and by $(\zeta_{p^{k+1}}-1)^{p^r(p-1)j}$ and reducing modulo p we only need to check that

$$(\zeta_{p^{k+1}}-1)^{p^r(p-1)j(\tilde{\gamma}_0-1)}\equiv 1 \pmod{(\zeta_{p^{k+1}}-1)^{p^r}}. \tag{8·28}$$

This follows from the fact that $(\zeta_{p^{k+1}}-1)^{(\tilde{\gamma}_0-1)}$ is a unit in $\mathbb{Z}_p[\zeta_{p^{k+1}}]$ and the $(p-1)$st power of any unit is congruent to 1 modulo the maximal ideal, and p^r is less than the valuation of p.

If we take the number

$$y_{k+1,r}=1+\left(\prod_{i=0}^{p^{r+1}-p^r-1}\big(\zeta_{p^{k+1}}^{\tilde{\gamma}_0^i}-1\big)\right)^j \tag{8·29}$$

then we have that $v_{k+1}(y_{k+1,r}-1)=p^r(p-1)j$ and

$$y_{k+1,r}^{1-\tilde{\gamma}_0}-1=\frac{\left(\prod_{i=0}^{p^{r+1}-p^r-1}\big(\zeta_{p^{k+1}}^{\tilde{\gamma}_0^i}-1\big)\right)^j}{1+\left(\prod_{i=0}^{p^{r+1}-p^r-1}\big(\zeta_{p^{k+1}}^{\tilde{\gamma}_0^i}-1\big)\right)^j}\left(1-\left(\frac{\zeta_{p^{k+1}}^{\tilde{\gamma}_0^{p^r(p-1)}}-1}{\zeta_{p^{k+1}}-1}\right)^j\right). \tag{8·30}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

Since p does not divide j it is easy to see that

$$v_{k+1}\left(1-\left(\frac{\zeta_{p^{k+1}}^{\tilde{\gamma}_0^{p^r(p-1)}}-1}{\zeta_{p^{k+1}}-1}\right)^j\right)=v_{k+1}\left(1-\left(\frac{\zeta_{p^{k+1}}^{1+p^{r+1}}-1}{\zeta_{p^{k+1}}-1}\right)^j\right)=p^{r+1}-1, \tag{8·31}$$

which means that $v_{k+1}(y_{k+1,r}^{1-\tilde{\gamma}_0}-1)=p^r(p-1)j+p^{r+1}-1$, i.e. maximal if the claim is true. Now we prove the second inequality by induction on r. Indirectly, let r be the smallest nonnegative integer for which the statement is not true. This means that there is an element $z_{k+1,r}$ in $\mathbb{Z}_p[\zeta_{p^{k+1}}]$ such that

$$\begin{aligned} v_{k+1}(z_{k+1,r}-1)&=v_{k+1}(y_{k+1,r}-1)<p^k\\ v_{k+1}\big(z_{k+1,r}^{1-\tilde{\gamma}_0}-1\big)&>v_{k+1}\big(y_{k+1,r}^{1-\tilde{\gamma}_0}-1\big), \text{ and so}\\ v_{k+1}((z_{k+1,r}/y_{k+1,r})^{1-\tilde{\gamma}_0}-1)&=v_{k+1}\big(y_{k+1,r}^{1-\tilde{\gamma}_0}-1\big). \end{aligned} \tag{8·32}$$

We may assume without loss of generality that $z_{k+1,r}$ is congruent to $y_{k+1,r}$ modulo $(\zeta_{p^{k+1}}-1)^{p^r(p-1)j+1}$ because we can replace $z_{k+1,r}$ with one of its prime to p powers. This means that $p^r(p-1)j<w:=v_{k+1}(z_{k+1,r}/y_{k+1,r}-1)<p^r(p-1)j+p^{r+1}-1$. Moreover, w must be divisible by $p-1$ because otherwise $v_{k+1}(z_{k+1,r}^{1-\tilde{\gamma}_0}-1)$ would also be w (see (8·16)) which contradicts to (8·33). On the other hand, since the only number divisible by $p^{r+1}-p^r$ in this region is $p^r(p-1)(j+1)=p^r(p-1)j+p^{r+1}-p^r$ and if w is equal to this number then by the other side of the inequality, which is already proven, we get that

$$v_{k+1}((z_{k+1,r}/y_{k+1,r})^{1-\tilde{\gamma}_0}-1)>(p^r(p-1)j+p^{r+1}-p^r)+p^r \tag{8·33}$$

which is a contradiction because $z_{k+1,r}^{1-\tilde{\gamma}_0}$ and $y_{k+1,r}^{1-\tilde{\gamma}_0}$ are not the same modulo

$$(\zeta_{p^{k+1}}-1)^{p^r(p-1)j+p^{r+1}}. \tag{8·34}$$

So $w=p^{r_0}(p-1)j_0$ for some $0\leqslant r_0<r$ and j_0 coprime to p. Now we are done since there is no number w with

$$p^r(p-1)j+p^{r+1}-p^{r_0+1}\leqslant w\leqslant p^r(p-1)j+p^{r+1}-p^{r_0}-1 \tag{8·35}$$

which is divisible by $p^{r_0}(p-1)$ and not divisible by $p^{r_0+1}(p-1)$ and these are the only possibilities for w by (8·33) and the inductional hypothesis.

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 8·8. *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 $n\geqslant 0$ and ζ_{p^n} a primitive p^nth root of unity and we have*

$$f_0(X)f_0(1/(X+1)-1)=\hat{g}(X)^{1-\tilde{\gamma}_0} \tag{8·36}$$

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 $f_0(X)f_0(1/(X+1)-1)$. For the other

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

direction we are going to prove that for all $k \geqslant 0$ there exists a $g_k(X) \in 1 + X\mathbb{Z}_p[[X]]$ such that

$$f_0(X) \equiv g_k(X)^{1-\tilde{\gamma}_0} \mod ((X+1)^{p^k} - 1). \tag{8·37}$$

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 (8·37) 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 $k \geqslant 0$. So we may assume without loss of generality that $f_0(X) \equiv 1 \bmod ((X+1)^{p^k} - 1)$ 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

$$h_{k+1}(\zeta_{p^{k+1}} - 1) h_{k+1}\left(\zeta_{p^{k+1}}^{-1} - 1\right) = k_0 \hat{g}(\zeta_{p^{k+1}} - 1), \tag{8·38}$$

for some k_0 in $\mathbb{Z}_p$ since there the 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

$$(X+1)^{p^k} - 1 \text{ and } \frac{(X+1)^{p^{k+1}} - 1}{(X+1)^{p^k} - 1} \tag{8·39}$$

(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 $\left(\dfrac{(X+1)^{p^{k+1}} - 1}{(X+1)^{p^k} - 1}\right)$. Now if we apply Lemma 8·7 and notice that

$$\frac{(X+1)^{p^k} - 1}{(X+1)^{p^i} - 1} \equiv X^{p^k - p^i} \pmod{p} \tag{8·40}$$

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

$$1 + \sum_{i=0}^{k-1} a_i \frac{(X+1)^{p^k} - 1}{(X+1)^{p^i} - 1}. \tag{8·41}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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 $\left(\frac{(X+1)^{p^{k+1}}-1}{(X+1)^{p^k}-1}\right)$ and to some element in the form

$$\sum_{i=0}^{k} a_i \frac{(X+1)^{p^k}-1}{(X+1)^{p^i}-1} \tag{8·42}$$

modulo $((X+1)^{p^k}-1)$ which element is in fact fixed under the conjugation by $\tilde{\gamma}_0$ (see Lemma 8·6). 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 $\left(\frac{(X+1)^{p^{k+1}}-1}{(X+1)^{p^k}-1}\right)$ 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.

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

$$f(X) = \prod_{i=0}^{p-2} \tilde{\gamma}_0^i f_0(X) \tilde{\gamma}_0^{-i}. \tag{8·43}$$

This motivates the following Corollary.

COROLLARY 8·9. *For a formal power series $f(X) \in p^{-l}\mathbb{Z}_p[[X]]$ the following are equivalent.*

(i) *It satisfies the condition* (8·6) *and is in the form*

$$f(X) = \prod_{i=0}^{p-2} \tilde{\gamma}_0^i f_0(X) \tilde{\gamma}_0^{-i} \tag{8·44}$$

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

$$f_0(X) f_0(1/(X+1)-1) = \hat{g}(X)^{1-\tilde{\gamma}_0} \tag{8·45}$$

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

Proof. For the direction (ii)⇒(i) it is easy to see that $f_0(X) = g(X)^{1-\tilde{\gamma}_0}$ is suitable and, by the remark after Lemma 8·3, $g(X)^{1-\tilde{\gamma}}$ satisfies the condition (8·6).

The other direction follows from Proposition 8·8 once we note that the condition (8·6) 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 8·3), 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 8·10. *Under the Hypotheses* 1 *and* 2 *and the second case of Proposition* 8·2, *$Y(E/F_\infty)$ is a finite index submodule of*

$$\Lambda(G)/\Lambda(G)(\tilde{\gamma}-1) \tag{8·46}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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 8·9. The action of G extends to an action of G_0, and by the second remark after Theorem 6·2 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

$$\Lambda(G_0)/\Lambda(G_0)(\tilde{\gamma}_0 - f_0(X)) \longrightarrow \Lambda(G_0)/\Lambda(G_0)\big(\tilde{\gamma}_0^{-1} - f_0(1/(X+1) - 1)\big) \tag{8·47}$$

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

$$\Lambda(G_0)/\Lambda(G_0)\big(\tilde{\gamma}_0^{-1} - f_0(1/(X+1) - 1)\big) \tag{8·48}$$

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 (8·47). Moreover, since the cokernel of this morphism is finite, $\hat{g}_0(X)$ must be an invertible power series when identifying

$$\Lambda(G_0)/\Lambda(G_0)\big(\tilde{\gamma}_0^{-1} - f_0(1/(X+1) - 1)\big) \tag{8·49}$$

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

$$f_0(X)\hat{g}_0(X) = \big(\tilde{\gamma}_0\hat{g}_0(X)\tilde{\gamma}_0^{-1}\big) \cdot (\tilde{\gamma}_0 1) \text{ and} \tag{8·50}$$

$$\tilde{\gamma}_0^{-1} 1 = f(1/(X+1) - 1). \tag{8·51}$$

Applying $\tilde{\gamma}_0$ on (8·51) we get

$$1 = \tilde{\gamma}_0 f(1/(X+1) - 1)\tilde{\gamma}_0^{-1} \cdot (\tilde{\gamma}_0 1) \tag{8·52}$$

$$\tilde{\gamma}_0 1 = \tilde{\gamma}_0 f(1/(X+1) - 1)^{-1}\tilde{\gamma}_0^{-1} \tag{8·53}$$

and substituting (8·53) into (8·50) we have

$$\hat{g}(X)^{1-\tilde{\gamma}_0} = f_0(X) f_0(1/(X+1) - 1) \text{ with} \tag{8·54}$$

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

Lemma 8·3 implies the equation for the formal power series $f(X)$, therefore the assumption (i) in Corollary 8·9 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 8·11. *Under the Hypotheses* 1 *and* 2 *and the second case of Proposition* 8·2, *$Y(E/F_\infty)$ is a finite index submodule of*

$$\Lambda(G_0)/\Lambda(G_0)(\tilde{\gamma}_0 - \alpha) \tag{8·55}$$

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 $K_1(\Lambda(G_0)_{S^*})$.*

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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

$$H_0(\mathrm{Gal}(\mathbb{Q}(\mu_p, \sqrt[p^n]{m})^{cyc}/\mathbb{Q}(\sqrt[p^n]{m})^{cyc}), Y(E/\mathbb{Q}(\mu_p, \sqrt[p^n]{m}))) \longrightarrow Y(E/\mathbb{Q}(\sqrt[p^n]{m})) \quad (8{\cdot}56)$$

has finite kernel and cokernel [**3**, **17**], so it can be easily seen that for any intermediate field $\mathbb{Q} \leqslant k \leqslant \mathbb{Q}(\mu_p)$ the characteristic power series for $Y(E/k(\sqrt[p^n]{m})^{cyc})$ is

$$T^{\varepsilon_k} \prod_{j=0}^{n-1} ((T+1)^{p^j} - 1), \quad (8{\cdot}57)$$

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 [**20**], $\varepsilon_k \equiv r_{E/k}$ 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 [**10**], so the p^∞-Selmer rank over this quadratic field must be 1, too, which means that α has order at most 2.

Remark 8·1. 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 [**3**], by applying the automorphism # (see Section 3·2 for the definition) and noting that $\alpha = \pm 1$.

$$(p^{\mu_{E/K}}(\tilde{\gamma}_0 - \alpha))^{\#} = -\tilde{\gamma}_0^{-1} p^{\mu_{E/K}}(\tilde{\gamma}_0 - \alpha)\alpha^{-1}. \quad (8{\cdot}58)$$

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 [**20**].

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

$$y^2 + xy + y = x^3 + x^2 - 2x \quad (8{\cdot}59)$$

satisfies the conditions of the second case of Proposition 8·2 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 $K_1(\Lambda(G_0)_{S^*})$.

8·2. *The non-classical case*

In this section we assume the first case of Proposition 8·2. Then we have that $g_{E/F_n} \leqslant p^n - 1 \leqslant r_{E/F_n}$. Moreover, the characteristic power series for $Y(E/F_n^{cyc})$ is T^{p^n-1} for all $n \geqslant 1$ [**3**]. If, in addition, E has a prime conductor, Darmon and Tian [**8**] have some results in this direction, too. As in the previous section we can identify $Y(E/F_\infty)$ with a finite index

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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 $p^l \in Y(E/F_\infty) \leqslant \mathbb{Z}_p[[X]]$.

LEMMA 8·12. *Under the Hypotheses* 1 *and* 2 *and the first case of Proposition* 8·2*, the following functional equation holds*:

$$\prod_{j=0}^{p^{n-1}-1} f\left(\zeta_{p^n}^{1+jp} - 1\right) = 1, \tag{8·60}$$

where ζ_{p^n} *is an arbitrary primitive* p^n*th root of unity* ($n \geqslant 1$ *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

$$\prod_{j=0}^{p^{n-1}-1} f\left(\zeta_{p^n}^{1+jp} - 1\right) \tag{8·61}$$

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

$$\prod_{j=0}^{p^{n-1}-1} f(\zeta^{1+jp} - 1) \tag{8·62}$$

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 8·3. 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^kth roots of unity ($1 \leqslant k \leqslant n$). So the exception can only be the first root of unity 1 and the result follows.

PROPOSITION 8·13. *If* $f(X) \in p^{-l}\mathbb{Z}_p[[X]]$ *is a formal power series in the form*

$$f(X) = \prod_{i=0}^{p-2} \tilde{\gamma}_0^i f_0(X) \tilde{\gamma}_0^{-i} \tag{8·63}$$

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

$$f_0(X) f_0(1/(X+1) - 1) = \hat{g}(X)^{1-\tilde{\gamma}_0} \left(\frac{(X+1)^{\chi(\tilde{\gamma}_0)} - 1}{X}\right)^2 \tag{8·64}$$

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

(i) *it satisfies the condition* (8·60);

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

$$f(X) = g(X)^{1-\tilde{\gamma}} \frac{(1+X)^{\chi(\tilde{\gamma})} - 1}{X}, \tag{8·65}$$

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

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

Proof. It is easy to check that

$$N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_p)}\left(\frac{\zeta_{p^n}^{\chi(\tilde{\gamma})}-1}{\zeta_{p^n}-1}\right)=\frac{N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_p)}\left(\zeta_{p^n}^{\chi(\tilde{\gamma})}-1\right)}{N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_p)}(\zeta_{p^n}-1)}=1, \tag{8·66}$$

hence a function in the form

$$g(X)^{1-\tilde{\gamma}}\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X} \tag{8·67}$$

satisfies the condition (8·60). Moreover, $\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}|_{X=0}=\chi(\tilde{\gamma})=f(0)$, so

$$f(X)\left(\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}\bigg|_{X=0}\right)^{-1} \tag{8·68}$$

satisfies the condition (i) in Corollary 8·9 because

$$\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}=\prod_{i=0}^{p-2}\tilde{\gamma}_0^i\frac{(X+1)^{\chi(\gamma_0)}-1}{X}\tilde{\gamma}_0^{-i} \text{ and} \tag{8·69}$$

$$\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}\frac{1/(1+X)^{\chi(\tilde{\gamma})}-1}{1/(X+1)-1}=\left(\frac{(X+1)^{\chi(\tilde{\gamma}_0)}-1}{X}\right)^2(X+1)^{1-\tilde{\gamma}_0},$$

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

One gets the following Theorem in the same way as Theorem 8·10.

THEOREM 8·14. *Under the Hypotheses* 1 *and* 2 *and the first case of Proposition* 8·2 $Y(E/F_\infty)$ *is a finite index submodule of*

$$\Lambda(G)/\Lambda(G)\left(\tilde{\gamma}-\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}\right) \tag{8·70}$$

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*

$$Y+1-\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}=\tilde{\gamma}-\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X} \text{ and} \tag{8·71}$$

$$p^{\mu_{E/K}}\left(Y+1-\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}\right)=p^{\mu_{E/K}}\left(\tilde{\gamma}-\frac{(1+X)^{\chi(\tilde{\gamma})}-1}{X}\right), \tag{8·72}$$

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

Proof. We would like to apply Proposition 8·13. Condition (8·64) follows from the existence of the map

$$X(E/F_\infty)\xrightarrow{\varphi}a^1_{\Lambda(G)}(X(E/F_\infty)^\#) \tag{8·73}$$

with trivial kernel, and cokernel killed by X^2 (we use Theorem 6·2 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 6·1 that the kernel of the corestriction homomorphism

$$Y(E/F_\infty)_H\longrightarrow Y(E/K^{cyc}) \tag{8·74}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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 8·3, $f(0)$ is an eigenvalue of $\tilde{\gamma}|_{Y(E/F_\infty)_H}$, so $f(0)=\chi(\tilde{\gamma})$.

Proposition 8·4 remains unchanged in this case. However, its corollary is a bit different from the one in Section 8·1 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 8·5.

COROLLARY 8·15. *Under the Hypotheses* 1 *and* 2 *and the first case of Proposition* 8·2, *the characteristic element of the* Γ*-module* $X(E/\mathbb{Q}(\mu_p, \sqrt[p^n]{m})^{cyc})$ *is*

$$p^{p^n\mu_{E/K}}\prod_{j=0}^{n-1}((T+1)^{p^j}-1)^{p-1}. \tag{8·75}$$

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

$$\prod_{j=0}^{n-1}((T+1)^{p^j}-1). \tag{8·76}$$

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 8·16. *Under the Hypotheses* 1 *and* 2 *and the first case of Proposition* 8·2, $Y(E/F_\infty)$ *is a finite index submodule of*

$$\Lambda(G_\mathbb{Q})\Big/\Lambda(G_\mathbb{Q})\left(\tilde{\gamma}_0-\frac{(X+1)^{\chi(\gamma_0)}-1}{X}\right) \tag{8·77}$$

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*

$$\tilde{\gamma}_0-\frac{(X+1)^{\chi(\gamma_0)}-1}{X} \tag{8·78}$$

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

$$\tilde{\gamma}_0-\alpha\frac{(X+1)^{\chi(\gamma_0)}-1}{X}, \tag{8·79}$$

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 $\mathbb{Q}\leqslant k\leqslant\mathbb{Q}(\mu_p)$ is any intermediate field then the homology group

$$H_0(\mathrm{Gal}(F_\infty/k^{cyc}), X(E/F_\infty)) \tag{8·80}$$

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

$$0\longrightarrow\mu_{p^\infty}\longrightarrow E[p^\infty]\longrightarrow\mathbb{Q}_p/\mathbb{Z}_p\longrightarrow 0 \tag{8·81}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

and a little Kummer theory shows [**3**] 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

$$p^{\mu_{E/K}}\left(\tilde{\gamma}_0 - \frac{(X+1)^{\chi(\gamma_0)}-1}{X}\right)^{\#} = -\frac{X}{(X+1)^{\chi(\gamma_0)}-1}\left(\frac{X+1}{X^2}p^{\mu_{E/K}}\left(\tilde{\gamma}_0 - \frac{(X+1)^{\chi(\gamma_0)}-1}{X}\right)\frac{X^2}{X+1}\right)\tilde{\gamma}_0^{-1}. \quad (8{\cdot}82)$$

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 Equation (8·82). The right-hand side of (8·82) equals

$$\begin{aligned}
&-p^{\mu_{E/K}}\left(\frac{X}{(X+1)^{\chi(\gamma_0)}-1}\frac{X+1}{X^2}\tilde{\gamma}_0\frac{X^2}{X+1}\tilde{\gamma}_0^{-1} - \tilde{\gamma}_0^{-1}\right)\\
&= p^{\mu_{E/K}}\left(\tilde{\gamma}_0^{-1} - \frac{X}{(X+1)^{\chi(\gamma_0)}-1}\frac{X+1}{X^2}\left(\tilde{\gamma}_0\frac{X^2}{X+1}\tilde{\gamma}_0^{-1}\right)\right)\\
&= p^{\mu_{E/K}}\left(\tilde{\gamma}_0^{-1} - \frac{X}{(X+1)^{\chi(\gamma_0)}-1}\frac{X+1}{X^2}\frac{\left((X+1)^{\chi(\gamma_0)}-1\right)^2}{(X+1)^{\chi(\gamma_0)}}\right)\\
&= p^{\mu_{E/K}}\left(\tilde{\gamma}_0^{-1} - \frac{(X+1)^{\chi(\gamma_0)}-1}{X}\frac{X+1}{(X+1)^{\chi(\gamma_0)}}\right)\\
&= p^{\mu_{E/K}}\left(\tilde{\gamma}_0^{-1} - \frac{\dfrac{1}{(X+1)^{\chi(\gamma_0)}}-1}{\dfrac{1}{X+1}-1}\right)\\
&= p^{\mu_{E/K}}\left(\tilde{\gamma}_0 - \frac{(X+1)^{\chi(\gamma_0)}-1}{X}\right)^{\#}. \qquad (8{\cdot}83)
\end{aligned}$$

This above form of the functional equation of the characteristic element is what we get from Section 5. However, we can formulate another form of the functional equation in terms

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

of Section 6 which is more useful for the analytic connections.

$$p^{\mu_{E/K}}\left(\tilde{\gamma}_0-\frac{(X+1)^{\chi(\gamma_0)}-1}{X}\right)^{\#}$$
$$p^{\mu_{E/K}}\left(\tilde{\gamma}_0-\frac{(X+1)^{\chi(\gamma_0)}-1}{X}\right)\frac{\mathrm{Frob}_q^{-1}-\dfrac{(X+1)^{-q}-1}{\frac{1}{X+1}-1}}{\mathrm{Frob}_q-\dfrac{(X+1)^q-1}{X}}. \tag{8·84}$$

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 some numerical examples illustrating our results.

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

$$y^2+xy+y=x^3-x^2-x-14. \tag{8·85}$$

This has good ordinary reduction at the prime $p=7$ and the calculations in [**11**] show that it satisfies the conditions in the first case of Proposition 8·2 with $m=q=17$. Since 17 is a primitive root modulo 7, in Corollary 8·16 α equals 1. This means that the characteristic element of the dual Selmer group $X(E/F_\infty)$ of this curve is

$$\tilde{\gamma}_0-\frac{(X+1)^{\chi(\gamma_0)}-1}{X} \tag{8·86}$$

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

9. *On Vogel's counterexample*

Coates, Schneider and Sujatha proved [**6**] that for any finitely generated torsion $\Lambda(G)$-module M there exist reflexive left ideals of $\Lambda(G)$ and a $\Lambda(G)$-injection

$$\bigoplus_{i=1}^{r}\Lambda(G)/L_i\longrightarrow M/M_0 \tag{9·1}$$

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 [**23**] there is an example of a nonprincipal reflexive left ideal of $\Lambda(G)$. That ideal was

$$L=\Lambda(G)\left(Q(G)\left(Y+1-\frac{(X+1)^{1+p}-1-p}{X-p}\right)\cap\Lambda(G)\right), \tag{9·2}$$

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 [**23**] 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

$$(X-p)(Y+1+L)=((X+1)^{1+p}-1-p)(1+L) \tag{9·3}$$

is satisfied, therefore the map

$$\begin{aligned}\psi:\Lambda(G)/L&\longrightarrow\mathbb{Z}_p[[X]]\\ Y+1+L&\longmapsto(X+1)^{1+p}-1-p\\ 1+L&\longmapsto X-p\end{aligned} \tag{9·4}$$

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

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

$$\psi\left(\frac{(X+1)^{1+p}-(1+p)^{1+p}}{X-p}(1+L)-(Y+1+L)\right)=1+p-(1+p)^{1+p}. \quad (9{\cdot}5)$$

Further,

$$(Y+1)\left(\frac{(X+1)^{1+p}-(1+p)^{1+p}}{X-p}-Y-1\right)+Y+1-\frac{(X+1)^{1+p}-(1+p)^{1+p}}{X-p}$$
$$=-\left(Y+1-\frac{(X+1)^{1+p}-(1+p)^{1+p}}{(X+1)^{1+p}-1-p}\right)\left(Y+1-\frac{(X+1)^{1+p}-1-p}{X-p}\right)\in L, \quad (9{\cdot}6)$$

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

$$(Y+1)(1+p-(1+p)^{1+p})=1+p-(1+p)^{1+p}, \quad (9{\cdot}7)$$

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.

Acknowledgements. I would like to thank my research supervisor, John Coates, for the problem and the encouragement. During this research I was holding an External Research Studentship of Trinity College, Cambridge.

REFERENCES

[**1**] K. Ardakov and S. Wadsley. Characteristic elements for p-torsion Iwasawa modules. *J. Algebraic Geom.* **15** (2006), 339–377.
[**2**] Th. Bouganis and V. Dokchitser. Algebraicity of L-values for elliptic curves in a false Tate curve tower, preprint.
[**3**] J. Coates, T. Fukaya, K. Kato and R. Sujatha. Root numbers, Selmer groups, and non-commutative Iwasawa theory, in preparation.
[**4**] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob. The GL_2 main conjecture for elliptic curves without complex multiplication. *Publ. Math. Inst. Hautes Études Sci.* **101** (2005), 163–208.
[**5**] J. Coates, P. Schneider and R. Sujatha. Links between cyclotomic and GL_2 Iwasawa theory, *Documenta Mathematica*. Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 187–215.
[**6**] J. Coates, P. Schneider and R. Sujatha. Modules over Iwasawa algebras. *J. Inst. Math. Jussieu* **2**(1) (2003), 73–108.
[**7**] J. Cremona. Elliptic curves data http://www.maths.nottingham.ac.uk/personal/jec/ftp/data.
[**8**] H. Darmon and Y. Tian. Heegner points over false Tate curve extensions. *Talk in Montreal* (2005).
[**9**] P. Deligne. Valeur de fonctions L et périodes d'intégrales. *Proc. Sympos. Pure Math.* **33** Part 2, (1979), 313–346.
[**10**] 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.
[**11**] T. Dokchitser and V. Dokchitser. (with an appendix by J. Coates and R. Sujatha). Computations in non-commutative Iwasawa theory, preprint.
[**12**] M. Flach. A generalisation of the Cassels–Tate pairing. *J. Reine Angew. Math.* **412** (1990), 113–127.
[**13**] T. Fukaya and K. Kato. A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory, preprint.
[**14**] R. Greenberg. Iwasawa theory for p-adic representations, in *Algebraic number theory*. *Adv. Stud. Pure Math.* **17** (1989), 97–137.
[**15**] R. Greenberg. Introduction to Iwasawa theory for elliptic curves, in *Arithmetic algebraic geometry* (Park City, UT, 1999), 407–464.

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press

[**16**] 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.
[**17**] Y. HACHIMORI AND O. VENJAKOB. Completely faithful Selmer groups over Kummer extensions, *Documenta Mathematica*. Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 443–478.
[**18**] U. JANNSEN. Iwasawa modules up to isomorphism, in *Algebraic number theory*. Adv. Stud. Pure Math. **17** (1989), 171–207.
[**19**] K. KATO. K_1 of some non-commutative completed group rings. *K-Theory* **34** (2005), no. 2, 99–140.
[**20**] J. NEKOVÁŘ. On the parity of ranks of Selmer groups. II, *C. R. Acad. Sci. Paris Sr. I Math.* **332** (2001), no. 2, 99–104.
[**21**] 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.
[**22**] L. N. VASERSTEIN. On the Whitehead determinant for semi-local rings. *J. Algebra* **283** (2005), no. 2, 690–699.
[**23**] 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.
[**24**] D. VOGEL. Nonprincipal reflexive left ideals in Iwasawa algebras II, preprint, http://homepages.uni-regensburg.de/ vod05208/nonprincipal2.pdf

https://doi.org/10.1017/S0305004108001114 Published online by Cambridge University Press