The GL_2 main conjecture for elliptic curves without complex multiplication

J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob

April 15, 2004

1 Introduction

The main conjectures of Iwasawa theory provide the only general method known at present for studying the mysterious relationship between purely arithmetic problems and the special values of complex L-functions, typified by the conjecture of Birch and Swinnerton-Dyer and its generalizations. Our goal in the present paper is to develop algebraic techniques which enable us to formulate a precise version of such a main conjecture for motives over a large class of p-adic Lie extensions of number fields. The methods which we develop in general were inspired by the Heidelberg Habilitation thesis of one of us (Venjakob [33]).

Let G be a compact p-adic Lie group with no element of order p and write $\Lambda(G)$ for the Iwasawa algebra of G (see §2). Let M be a finitely generated torsion $\Lambda(G)$-module and write $\chi(G, M)$ for its G-Euler characteristic (see §3, (34)). How can we define a characteristic element of M and in particular relate this to the Euler characteristic of M and its twists? Let us quickly recall how such characteristic elements are defined in classical commutative Iwasawa theory when $G = \mathbb{Z}_p^d$ for some integer $d \geq 1$. In this case, the structure theory for finitely generated torsion $\Lambda(G)$-modules [3] shows that there exist a finite number of non-zero elements $f_1, \cdots, f_r$ such that we have an exact sequence of $\Lambda(G)$-modules

$$0 \to \oplus_{i=1}^{r} \Lambda(G)/\Lambda(G) f_i \to M \to D \to 0,$$

where D is a pseudo-null $\Lambda(G)$-module. We then define a characteristic element of M to be

$$f_M := \prod_{i=1}^{r} f_i(T)$$

which is uniquely determined up to multiplication by a unit in $\Lambda(G)$. The classical theory (see [26, V16]) shows that if $H_0(G, M)$ is finite, then $\chi(G, M)$ and $\chi(G, D)$ are both finite, and we have

$$\chi(G, M) = \mid f_M(0) \mid_p^{-1}, \ \chi(G, D) = 1$$

where $f_M(0)$ denotes the image of f_M under the augmentation map from $\Lambda(G)$ to $\mathbb{Z}_p$.

In the non-commutative case, assuming G is p-valued, it is shown in [7] that there is an exact sequence

$$0 \to \oplus_{i=1}^{r} \Lambda(G)/L_i \to M/M_0 \to D \to 0,$$

where the L_i are non-zero reflexive left ideals of $\Lambda(G)$, M_0 is the maximal pseudo-null submodule of M, and D is some pseudo-null $\Lambda(G)$-module. The whole approach of the commutative case to define characteristic elements now seems to break down irretrievably. Firstly, it is no longer true (see [6]) that $\chi(G, D)$ is finite implies that $\chi(G, D) = 1$ for D pseudo-null. Secondly, it is also not true in general (see the appendix to [32]) that a reflexive left ideal in $\Lambda(G)$ is always principal.

The goal of this paper is to provide a way out of this dilemma via localisation techniques for an important class of G. Namely, we assume that G has a closed normal subgroup H such that $\Gamma = G/H \simeq \mathbb{Z}_p$. For example, this is automatically true when G is the Galois group of a p-adic Lie extension of a number field F, which contains the cyclotomic $\mathbb{Z}_p$-extension of F. We prove in §2 that the Iwasawa algebra $\Lambda(G)$ contains a canonical Ore set S^*, enabling us to define the localised algebra $\Lambda(G)_{S^*}$. Write $\mathfrak{M}_H(G)$ for the category consisting of all finitely generated $\Lambda(G)$-modules which are annihilated by S^*. We prove that a finitely generated module M belongs to $\mathfrak{M}_H(G)$ if and only if $M/M(p)$ is finitely generated over $\Lambda(H)$ where $M(p)$ denotes the p-primary submodule of M. We optimistically believe that $\mathfrak{M}_H(G)$ contains all the torsion $\Lambda(G)$-modules which are of interest in arithmetic applications (for a precise statement see Conjecture 5.1). We then exploit the well known localization sequence of K-theory for the Ore set S^* (see [28]) to define a characteristic element ξ_M in $K_1(\Lambda(G)_{S^*})$ for any module M in $\mathfrak{M}_H(G)$. We also show that one can relate ξ_M to the Euler charcateristics of twists of M by arbitrary continuous representations of G, with values in $GL_n(O)$, where O is the ring of integers of a finite extension of $\mathbb{Q}_p$. This uses the Akashi series of M which was introduced in [6].

The paper ends by formulating and briefly discussing the main conjecture for an elliptic curve E over $\mathbb{Q}$ over the field generated by the coordinates of its p-power division points, where p is a prime ≥ 5 of good ordinary reduction for E. We also give some numerical evidence in support of this main conjecture based on the remarkable calculations of [12]. We have striven to keep the technical discussions to a minimum in the present paper. A forthcoming paper (Fukaya and Kato, [14]) by two of us will consider quite generally the Iwasawa theory of motives over arbitrary p-adic Lie extensions of number fields and its connexion with the Tamagawa number conjecture. In particular, that work applies to any p-adic Lie extension with Galois group G, and does not need either of the two basic hypotheses made in the present paper (namely that G has no element of order p, and that G has a quotient isomorphic to $\mathbb{Z}_p$).

Acknowledgements: This work was greatly assisted by the generous hospitality provided by the Department of Mathematics of Kyoto University for JC, the Harishchandra Research Institute, Allahabad for JC and RS, and the Tata Institute of Fundamental Research, Mumbai for JC and OV. Finally, we would like to thank Peter Schneider for pointing out to us the alternative characterization of the Ore set S given at the end of §2.

2 The canonical Ore set.

Let G be a compact p-adic Lie group. We define

$$\Lambda(G) = \varprojlim_U \mathbb{Z}_p[G/U], \quad \Omega(G) = \varprojlim_U \mathbb{F}_p[G/U], \tag{1}$$

where U runs over all open normal subgroups of G. By a module over these algebras, we shall always mean, unless specified otherwise, a left module. It is well known that $\Lambda(G)$ and $\Omega(G)$ are left and right Noetherian. Moreover, if $\Lambda(G)$ has no zero divisors (e.g. if G is pro-p and has no element of order p), we shall always write $Q(G)$ for the skew field of fractions of $\Lambda(G)$.

We assume throughout this paper that G has a closed normal subgroup H such that

$$\Gamma = G/H \xrightarrow{\simeq} \mathbb{Z}_p. \tag{2}$$

Inspired by the results in Venjakob [33], our aim is to construct a certain canonical Ore set S in $\Lambda(G)$.

Definition. 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.

Let H' be any open subgroup of H. Then $\Lambda(H)$ is a free left or right module of rank $[H : H']$ over $\Lambda(H')$. Hence, if M is a $\Lambda(H)$-module, M will be finitely generated over $\Lambda(H)$ if and only if it is finitely generated over $\Lambda(H')$, and similarly if M is a right $\Lambda(H)$-module. To exploit this observation, we will choose $H' = J$, where J denotes any open normal subgroup of H which is pro-p. For such a pro-p J, $\Lambda(J)$ is a local ring, whose maximal ideal is the kernel of the augmentation map from $\Lambda(J)$ to $\mathbb{F}_p$, and we can then use Nakayama's lemma for $\Lambda(J)$-modules (see the proof of Lemma 2.1). Let

$$\varphi_J : \Lambda(G) \to \Lambda(G/J), \quad \psi_J : \Lambda(G) \to \Omega(G/J) \tag{3}$$

be the natural surjections. For J as above, let us note that we can always find an open subgroup J' of J which is normal in G because the set of G conjugates of such a J is finite.

Lemma 2.1. *Let J be any pro-p open subgroup of H, which is normal in G. Then* (i) *S is the set of all f in $\Lambda(G)$ such that $\Lambda(G/J)/\Lambda(G/J)\varphi_J(f)$ is a finitely generated $\mathbb{Z}_p$-module,* (ii) *S is the set of all f in $\Lambda(G)$ such that $\Omega(G/J)/\Omega(G/J)\psi_J(f)$ is finite, and* (iii) *S is the set of all f in $\Lambda(G)$ such that right multiplication by $\psi_J(f)$ on $\Omega(G/J)$ is injective.*

Proof. As remarked above, we can replace H by J in the definition of S. If f is any element of $\Lambda(G)$, and if we put $M = \Lambda(G)/\Lambda(G)f$, then we clearly have

$$(M)_J = \Lambda(G/J)/\Lambda(G/J)\varphi_J(f), \quad M/\mathfrak{m}_J M = \Omega(G/J)/\Omega(G/J)\psi_J(f), \tag{4}$$

where $\mathfrak{m}_J$ denotes the maximal ideal of $\Lambda(J)$. Thus assertions (i) and (ii) are immediate from Nakayama's lemma. To prove (iii), we use the important fact that we can always find a subgroup Π of G/J satisfying

$$\Pi \xrightarrow{\simeq} \mathbb{Z}_p, \quad \Pi \text{ is in the centre of } G/J. \tag{5}$$

To establish this, let us write Γ' for some lifting of Γ to G/J. Then we can write G/J as the semi-direct product of H/J and Γ', where Γ' acts on H/J via conjugation. But, as H/J is finite, an open subgroup of Γ' must clearly act trivially on H/J by conjugation,

and we take Π to be this open subgroup. Now $\Omega(\Pi)$ is isomorphic to the ring of formal power series $\mathbb{F}_p[[T]]$ in an indeterminate T with coefficients in $\mathbb{F}_p$. Thus the quotient field of $\Omega(\Pi)$, which we denote by $R(\Pi)$, is a commutative field. Consider

$$V(G/J) = R(\Pi) \otimes_{\Omega(\Pi)} \Omega(G/J) = \Omega(G/J) \otimes_{\Omega(\Pi)} R(\Pi). \tag{6}$$

It is a finite dimensional algebra over the commutative field $R(\Pi)$, which lies in its centre. If f is any element of $\Lambda(G)$, let us write $\alpha_J(f)$ for the element of $V(G/J)$ defined by $\psi_J(f)$. By linear algebra, right multiplication by $\alpha_J(f)$ is surjective if and only if it is injective. Note also that, as $\Omega(\Pi)$ is a discrete valuation ring with residue field $\mathbb{F}_p$, a finitely generated $\Omega(\Pi)$-module is $\Omega(\Pi)$-torsion if and only if it is finite. It follows easily that, for any f in $\Omega(G)$, $\Omega(G/J)/\Omega(G/J)\psi_J(f)$ is finite if and only if right multiplication by $\psi_J(f)$ on $\Omega(G/J)$ has finite kernel. But $\Omega(G/J)$ clearly has no finite $\Omega(G/J)$-submodule, and so the equivalence of (ii) and (iii) is now clear. □

Lemma 2.2. *Let J be any pro-p open subgroup of H, which is normal in G. Then* (i) *S is the set of all f in $\Lambda(G)$ such that $\Lambda(G)/f\Lambda(G)$ is a finitely generated right $\Lambda(H)$-module;* (ii) *S is the set of all f in $\Lambda(G)$ such that $\Lambda(G/J)/\varphi_J(f)\Lambda(G/J)$ is a finitely generated $\mathbb{Z}_p$-module,* (iii) *S is the set of all f in $\Lambda(G)$ such that $\Omega(G/J)/\psi_J(f)\Omega(G/J)$ is finite, and* (iv) *S is the set of all f in $\Lambda(G)$ such that the left multiplication by $\psi_J(f)$ on $\Omega(G/J)$ is injective.*

Proof. We first note that it suffices only to prove (iv). Indeed, once (iv) is established, we can simply reverse the arguments of the proof of Lemma 2.1, but carrying them out for right modules, to deduce (i), (ii), and (iii). To prove (iv), we simply note the following. It was shown at the end of the proof of Lemma 2.1 that S consists of all f in $\Lambda(G)$ such that there exists z in the algebra $V(G/J)$ with $z.\alpha_J(f) = 1$. But, as multiplication on the left or on the right in $V(G/J)$ is $R(\Pi)$-linear, and $V(G/J)$ is finite dimensional over $R(\Pi)$, it follows from linear algebra that $z.\alpha_J(f) = 1$ if and only if $\alpha_J(f).z = 1$. This completes the proof of lemma 2.2. □

Let M be a left or right $\Lambda(G)$-module. We say that M is S-torsion if, for each x in M, there exists s in S such that $s.x = 0$ or $x.s = 0$, according as the action is on the left or right.

Proposition 2.3. *Let M be a finitely generated left or right $\Lambda(G)$-module. Then M is finitely generated over $\Lambda(H)$ if and only if M is S-torsion.*

Proof. We give the argument for left $\Lambda(G)$-modules. Suppose first that M is S-torsion. Take a finite family $(x_i)_{1\le i\le r}$ of elements of M which generates M as a $\Lambda(G)$-module, and choose f_i in S such that $f_i.x_i = 0$ for each i. Thus we get a $\Lambda(G)$-surjection

$$\theta : \bigoplus_{i=1}^{r} \Lambda(G)/\Lambda(G)f_i \to M \tag{7}$$

by mapping 1 in the i-th direct summand to x_i. By the definition of S, each module occurring in the finite direct sum is finitely generated over $\Lambda(H)$, and hence M is also.

Conversely, assume that M is finitely generated over $\Lambda(H)$. We must show that every element x of M is annihilated by an element of S. As before, fix any pro-p open subgroup J of H, which is normal in G. Again, we choose a subgroup Π of G/J satisfying (5), and we identify $\Lambda(\Pi)$ with $\mathbb{Z}_p[[T]]$ by fixing a topological generator of Π. Now M is finitely generated over $\Lambda(J)$. Let τ denote any lifting of T to $\Lambda(G)$. For each integer $n \geq 1$, define the $\Lambda(J)$-submodule

$$U_n = \Lambda(J)x + \Lambda(J)\tau x + \cdots + \Lambda(J)\tau^n x. \tag{8}$$

Since $\Lambda(J)$ is Noetherian, it follows that there must exist an integer $n \geq 1$, and $a_0, \ldots, a_{n-1}$ in $\Lambda(J)$ such that

$$\tau^n x = (a_0 + a_1\tau + \cdots + a_{n-1}\tau^{n-1})x.$$

Hence, if we define

$$s_n = \tau^n - a_{n-1}\tau^{n-1} - \cdots - a_0,$$

we have $s_n.x = 0$. But clearly $\psi_J(s_n)$ is a non-zero element of $\Omega(\Pi)$, and hence, by (iii) of lemma 2.1, s_n belongs to S. This completes the proof of Proposition 2.3. □

Theorem 2.4. *The set S is multiplicatively closed, and is a left and right Ore set in $\Lambda(G)$. The elements of S are non-zero divisors in $\Lambda(G)$.*

Proof. Take s_1 and s_2 in S. Then we have the exact sequence of $\Lambda(G)$-modules

$$0 \to W \to \Lambda(G)/\Lambda(G)s_1s_2 \to \Lambda(G)/\Lambda(G)s_2 \to 0, \tag{9}$$

where $W = \Lambda(G)s_2/\Lambda(G)s_1s_2$. As W is a homomorphic image of $\Lambda(G)/\Lambda(G)s_1$, it follows that the $\Lambda(H)$-module in the middle of (9) is finitely generated over $\Lambda(H)$, and thus s_1s_2 belongs to S. Now take f to be any element of S, and x to be any element of $\Lambda(G)$. By Proposition 2.3, the left module $\Lambda(G)/\Lambda(G)f$ and the right module $\Lambda(G)/f\Lambda(G)$ are both S-torsion. Hence there exist s and s' in S such that $sx \in \Lambda(G)f$ and $xs' \in f\Lambda(G)$. This proves that S is a left and right Ore set in $\Lambda(G)$.

To prove the final assertion of the theorem, take f to be any element of S. Now

$$\Lambda(G) = \varprojlim_J \Lambda(G/J),$$

where the projective limit is taken over all pro-p open subgroups J of H, which are normal in G. Thus, fixing any such J, it suffices to show that $\varphi_J(f)$ is not a zero divisor in $\Lambda(G/J)$. As before, we choose a subgroup Π of G/J satisfying (5), and let $Q(\Pi)$ denote the quotient field of $\Lambda(\Pi)$. Consider the algebra

$$W(G/J) = Q(\Pi) \otimes_{\Lambda(\Pi)} \Lambda(G/J) = \Lambda(G/J) \otimes_{\Lambda(\Pi)} Q(\Pi), \tag{10}$$

which is finite dimensional over the commutative field $Q(\Pi)$, which lies in its centre. By virtue of (i) of Lemma 2.1 and (ii) of Lemma 2.2, we see that the image of $\varphi_J(f)$ in $W(G/J)$ has a right and left inverse. Hence $\varphi_J(f)$ cannot be a divisor of zero in $\Lambda(G/J)$, and the proof of Theorem 2.4 is complete. □

We are grateful to P. Schneider (Lemma 2.5 and Proposition 2.6 below are due to him) for kindly pointing out to us the following alternative characterisation of the set S.

Lemma 2.5. *For any two pro-p open subgroups $J \subseteq J'$ of H which are normal in G, the kernel of the natural map $\Omega(G/J) \to \Omega(G/J')$ is a nilpotent ideal.*

Proof. We recall that, quite generally, the prime radical $\mathcal{N}(A)$ in a Noetherian ring A is nilpotent and contains any other nilpotent ideal [19, 0.2.6, 2.3.7]. The assertion therefore is the claim that

$$\mathrm{Ker}\,(\Omega(G/J) \to \Omega(G/J') \subseteq \mathcal{N}(\Omega(G/J)).$$

The subgroup $\Delta := J'/J$ is a finite normal p-subgroup of G/J. The elements $\delta - 1$ for $\delta \in \Delta$ generate the above left hand side as a left ideal. Let $\Pi \subseteq G/J$ be a central subgroup as in the proof of Lemma 2.1; it maps isomorphically onto a central subgroup in G/J'. Hence we may view $\Omega(G/J) \to \Omega(G/J')$ as a map of $\Omega(\Pi)$-algebras. Since

$$\mathcal{N}(\Omega(G/J)) = \Omega(G/J) \cap \mathcal{N}(V(G/J))$$

it suffices to prove that

$$\mathrm{Ker}\,(V(G/J) \to V(G/J')) \subseteq \mathcal{N}(V(G/J)).$$

Again, the left hand side is generated, as a left ideal, by the elements $\delta - 1$ for $\delta \in \Delta$. The right hand side is the intersection of the annihilator (prime) ideals of all the simple modules over the finite dimensional $R(\Pi)$-algebra $V(G/J)$. Hence we have to show that Δ acts trivially on any simple $V(G/J)$-module E. Since Δ is a p-group and E is a vector space over a field of characteristic p, the fixed vectors E^Δ under Δ in E certainly are non-zero. Since Δ is normal in G/J, these fixed vectors E^Δ form a $V(G/J)$-submodule of E. Hence we must have $E^\Delta = E$. □

The lemma implies that the two sided ideal

$$\mathcal{N} := \text{preimage of } \mathcal{N}(\Omega(G/J)) \text{ in } \Lambda(G)$$

is independent of the choice of a pro-p open subgroup J in H which is normal in G.

Proposition 2.6. *The set S is equal to the set of all elements in $\Lambda(G)$ which are regular modulo $\mathcal{N}$.*

Proof. Choose a pro-p open subgroup $J \subseteq H$ which is normal in G. Since $\Lambda(G)/\mathcal{N} = \Omega(G/J)/\mathcal{N}(\Omega(G/J))$ an element $f \in \Lambda(G)$ is regular modulo $\mathcal{N}$ if and only if $\psi_J(f)$ is regular modulo $\mathcal{N}(\Omega(G/J))$, i.e. becomes a unit in the finite dimensional algebra $V(G/J)/\mathcal{N}(V(G/J))$. But units modulo nilpotent ideals are units. Hence f is regular modulo $\mathcal{N}$ if and only if $\Psi_J(f)$ is a non-zero divisor in $\Omega(G/J)$. By Lemma 2.1(iii) and 2.2(iii), the latter is equivalent to f belonging to S. □

3 Akashi series and Euler characteristics.

Most of the results in this section are already established in [33], but we reprove them here in a slightly different fashion. As always, G will denote a compact p-adic Lie group with a closed normal subgroup H such that $G/H = \Gamma$ is isomorphic to $\mathbb{Z}_p$. We fix from now on a topological generator of Γ, and identify $\Lambda(\Gamma)$ with the formal power series ring $\mathbb{Z}_p[[T]]$ by mapping this topological generator to $1+T$. We write $Q(\Gamma)$ for the fraction field of $\Lambda(\Gamma)$. Similarly, if O denotes the ring of integers of some finite extension of $\mathbb{Q}_p$, we write $\Lambda_O(\Gamma)$ (which we identify with $O[[T]]$) for the O-Iwasawa algebra of Γ, and $Q_O(\Gamma)$ for the quotient field of $\Lambda_O(\Gamma)$. Let S be the Ore set in $\Lambda(G)$ which is defined in §2. Since $p \notin S$, we shall also need to consider

Definition.

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

As p lies in the centre of $\Lambda(G)$, S^* is again a multiplicatively closed left and right Ore set in $\Lambda(G)$, all of whose elements are non-zero divisors. We write $\Lambda(G)_S$, $\Lambda(G)_{S^*}$ for the localizations of $\Lambda(G)$ at S and S^*, so that

$$\Lambda(G)_{S^*} = \Lambda(G)_S[\frac{1}{p}] \tag{11}$$

If M is a $\Lambda(G)$-module, we write $M(p)$ for the submodule of M consisting of all elements of finite order. It is clear from Proposition 2.3 that M will be S^*-torsion if and only if $M/M(p)$ is finitely generated over $\Lambda(H)$. We write $\mathfrak{M}_H(G)$ for the category of all finitely generated $\Lambda(G)$-modules, which are S^*-torsion. Note that in the special case in which $H = 1$ and $G = \Gamma$, $\mathfrak{M}_H(G)$ is the category of all finitely generated torsion $\Lambda(G)$-modules. Both for motivation, and because we shall need it later in this section, we prove the following lemma (see [6]).

Lemma 3.1. *For each M in $\mathfrak{M}_H(G)$, the homology groups $H_i(H, M)$ $(i \geq 0)$ are all finitely generated torsion $\Lambda(\Gamma)$-modules. If G has no element of order p, $H_i(H, M) = 0$ for $i \geq d$, where d is the dimension of G as a p-adic Lie group.*

Proof. We first observe that the $H_i(H, M)$ are finitely generated $\Lambda(\Gamma)$-modules, because

$$H_i(H, M) = \mathrm{Tor}_i^{\Lambda(G)}(\Lambda(G/H), M) \qquad (i \geq 0),$$

and the modules on the right are finitely generated over $\Lambda(\Gamma)$ since M is finitely generated over $\Lambda(G)$. Put $M_f = M/M(p)$. Now, for all $i \geq 0$, $H_i(H, M(p))$ is killed by p^t, where t is any integer ≥ 0 such that $p^t.M(p) = 0$. Also, $H_i(H, M_f)$ is a finitely generated $\mathbb{Z}_p$-module since M_f is finitely generated over $\Lambda(H)$. It now follows from the long exact sequence of H-homology that $H_i(H, M)$ is a torsion $\Lambda(\Gamma)$-module for all $i \geq 0$. The final assertion of the lemma is true because H has p-cohomological dimension $d-1$ when H has no elements of order p [24]. □

As above, 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

$$\rho : G \to GL_n(O), \tag{12}$$

where n is some integer ≥ 1. If M is a finitely generated $\Lambda(G)$-module, put $M_O = M \otimes_{\mathbb{Z}_p} O$, and define

$$\mathrm{tw}_\rho(M) = M_O \otimes_O O^n. \tag{13}$$

We endow $\mathrm{tw}_\rho(M)$ with the diagonal action of G i.e. if σ is in G, $\sigma(m \otimes z) = (\sigma m) \otimes (\sigma z)$, 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 $\Lambda(G)$.

Lemma 3.2. *If $M \in \mathfrak{M}_H(G)$, then, for all continuous representations ρ of the form* (12)*, $\mathrm{tw}_\rho(M) \in \mathfrak{M}_H(G)$.*

Proof. Assume that $M \in \mathfrak{M}_H(G)$. Since O is a free module of finite rank over $\mathbb{Z}_p$, it follows easily that $M_O \in \mathfrak{M}_H(G)$. Since $\mathrm{tw}_\rho(M_O(p))$ is killed by the same power of p which kills $M_O(p)$, it suffices to prove that $\mathrm{tw}_\rho(R)$ is finitely generated over $\Lambda(H)$, where $R = M_O/M_O(p)$. Now we have a surjection $\Lambda(H)^m \to R$, which plainly induces a surjection of $\Lambda(H)$-modules $\mathrm{tw}_{\rho_H}(\Lambda(H)^m) \to \mathrm{tw}_\rho(R)$, where ρ_H denotes the restriction of ρ to the subgroup H of G. But it is well known [33] that $\mathrm{tw}_{\rho_H}(\Lambda(H)^m)$ is again a free $\Lambda(H)$-module of finite rank. This completes the proof of Lemma 3.2. □

If R is a ring with unit element, we write $R^\times$ for the group of units of R, and $M_n(R)$ for the ring of $n \times n$-matrices with entries in R. By continuity, the group homomorphism ρ induces a ring homomorphism

$$\rho : \Lambda(G) \to M_n(O). \tag{14}$$

A second ring homomorphism

$$\Phi_\rho : \Lambda(G) \to M_n(\Lambda_O(\Gamma)), \tag{15}$$

which we now define, will play an important role in our work. If σ is in G, we write $\bar{\sigma}$ for its image in $\Gamma = G/H$. We define a continuous group homomorphism

$$G \to (M_n(O) \otimes_{\mathbb{Z}_p} \Lambda(\Gamma))^\times \tag{16}$$

by mapping σ to $\rho(\sigma) \otimes \bar{\sigma}$. Noting that

$$M_n(O) \otimes_{\mathbb{Z}_p} \Lambda(\Gamma) = M_n(\Lambda_O(\Gamma))$$

because O is a free $\mathbb{Z}_p$-module of finite rank, we obtain (15) by extending (16) to the whole of $\Lambda(G)$. Note that $\Phi_\rho(p) = pI_n$, where I_n is the unit matrix. Also it is easily seen that (14) is the composition of (15) with the map from $M_n(\Lambda_O(\Gamma))$ to $M_n(O)$ induced by the augmentation map from $\Lambda_O(\Gamma)$ to O.

Lemma 3.3. *The map* (15) *extends to a ring homomorphism, which we also denote by* Φ_ρ,

$$\Phi_\rho : \Lambda(G)_{S^*} \to M_n(Q_O(\Gamma)). \tag{17}$$

Proof. We must show that, for all s in S^*, $\Phi_\rho(s)$ is invertible in $M_n(Q_O(\Gamma))$, or equivalently that $\Phi_\rho(s)$ has non-zero determinant. Since this is clearly true for $s = p$, we can assume that s is in S. Let k denote the residue field of O, and let

$$\tilde{\Phi}_\rho : \Lambda(G) \to M_n(k[[T]])$$

denote the composition of Φ_ρ with the canonical map from $M_n(\Lambda_O(\Gamma))$ to $M_n(k[[T]])$. It suffices to show that $\tilde{\Phi}_\rho(s)$ has non-zero determinant. Note that $\tilde{\Phi}_\rho$ is induced by the map

$$G \to (M_n(k) \otimes_k k[[T]])^\times \tag{18}$$

given by $\sigma \mapsto \tilde{\rho}(\sigma) \otimes \bar{\sigma}$, where $\tilde{\rho}(\sigma)$ denotes the image of $\rho(\sigma)$ in $M_n(k)$. We now exploit the fact that $GL_n(k)$ is a finite group. Thus we can find a pro-p open subgroup J of H, which is normal in G, and which is contained in $\mathrm{Ker}\,(\tilde{\rho})$. Clearly $\tilde{\Phi}_\rho$ can be factored through a map

$$\delta : \Omega(G/J) \to M_n(k[[T]]). \tag{19}$$

Let ψ_J be given by (3). Then we must show that $\delta(\psi_J(s))$ has non-zero determinant. As in §2, we can find a central subgroup Π of G/J with $\Pi \xrightarrow{\simeq} \mathbb{Z}_p$. Replacing Π by an open subgroup if necessary, we may also assume that Π lies in the kernel of the homomorphism from G/J to $GL_n(k)$ induced by $\tilde{\rho}$. Hence it is clear from (18) that $\delta(\Omega(\Pi))$ must be contained in $k[[T]].I_n$. Let $R(\Pi)$ (resp. $Q(k[[T]])$) denote the quotient field of $\Omega(\Pi)$ (resp. $k[[T]]$). Since the natural map from Π to Γ is injective, $Q(k[[T]])$ can be viewed as a finite extension of $R(\Pi)$. Hence (19) induces a ring homomorphism

$$\alpha : R(\Pi) \otimes_{\Omega(\Pi)} \Omega(G/J) \to M_n(Q(k[[T]])). \tag{20}$$

But, as proven in §2, $\psi_J(s)$ is a unit in the algebra on the left in (20). Hence $\alpha(\psi_J(s))$ is invertible in $M_n(Q(k[[T]])$, and so has non-zero determinant. This completes the proof of Lemma 3.3. □

If R is a ring, we write $K_m R$ for the m-th K-group of R (we shall only need the cases $m = 0, 1$). Clearly (14) induces a homomorphism

$$K_1(\Lambda(G)) \to K_1(M_n(O)) = O^\times. \tag{21}$$

This can be extended to a map from $K_1(\Lambda(G)_{S^*})$ to $L \cup \{\infty\}$, where L is the fraction field of O, in the following manner. Firstly, (17) induces a homomorphism

$$\Phi'_\rho : K_1(\Lambda(G)_{S^*}) \to K_1(M_n(Q_O(\Gamma)))) = Q_O(\Gamma)^\times. \tag{22}$$

Let $\varphi : \Lambda_O(\Gamma) \to O$ be the augmentation map, and write $\mathfrak{p} = \mathrm{Ker}\,(\varphi)$. Of course, writing $\Lambda_O(\Gamma)_{\mathfrak{p}} \subset Q_O(\Gamma)$ for the localization of $\Lambda_O(\Gamma)$ at $\mathfrak{p}$, it is clear that φ extends naturally to a homomorphism

$$\varphi : \Lambda_O(\Gamma)_{\mathfrak{p}} \to L.$$

Let ξ be any element of $K_1(\Lambda(G)_{S^*})$. If $\Phi'_\rho(\xi)$ belongs to $\Lambda_O(\Gamma)_\mathfrak{p}$, we define $\xi(\rho)$ to be $\varphi(\Phi'_\rho(\xi))$. However, if $\Phi'_\rho(\xi)$ does not belong to $\Lambda_O(\Gamma)_\mathfrak{p}$, we define $\xi(\rho) = \infty$. This gives us the desired extension of (21).

We now use a well known localization theorem in K-theory to define the notion of a characteristic element for any module M in the category $\mathfrak{M}_H(G)$. To ensure that we can work with modules rather than complexes, we assume for the rest of this section the following

Hypothesis on G. G has no element of order p.

It is well known [4] that this implies that $\Lambda(G)$ has finite global dimension equal to $d+1$, where d is the dimension of G as a p-adic Lie group. Since $\mathfrak{M}_H(G)$ is the category of all finitely generated $\Lambda(G)$-modules which are S^*-torsion, there is a connecting homomorphism (see [28])

$$\partial_G : K_1(\Lambda(G)_{S^*}) \to K_0(\mathfrak{M}_H(G)), \tag{23}$$

where $K_0(\mathfrak{M}_H(G))$ denotes the Grothendieck group of the category $\mathfrak{M}_H(G)$, such that we have, as part of a larger exact sequence of localization, the exact sequence

$$\cdots \to K_1(\Lambda(G)) \to K_1(\Lambda(G)_{S^*}) \xrightarrow{\partial_G} K_0(\mathfrak{M}_H(G)) \to K_0(\Lambda(G)) \to K_0(\Lambda(G)_{S^*}) \to 0. \tag{24}$$

Proposition 3.4. *Assume that G has no element of order p. Then ∂_G is surjective.*

Before giving the proof of Proposition 3.4, we need the following preliminary lemma.

Lemma 3.5. *Let P be any pro-p open normal subgroup of G. Then the canonical map*

$$K_0(\Lambda(G)) \to K_0(\mathbb{Z}_p[G/P])$$

is injective.

Proof. Let $\Delta = G/P$, and let I denote the kernel of the natural map from $\Lambda(G)$ to $\mathbb{Z}_p[\Delta]$. Let M be any finitely generated projective $\Lambda(G)$-module such that the class of M/IM in $K_0(\mathbb{Z}_p[\Delta])$ is zero, i.e. we have a $\mathbb{Z}_p[\Delta]$-isomorphism

$$\alpha : M/IM \oplus \mathbb{Z}_p[\Delta]^r \xrightarrow{\simeq} \mathbb{Z}_p[\Delta]^r,$$

for some integer $r \geq 0$. Since M is a projective $\Lambda(G)$-module, we can find a $\Lambda(G)$-homomorphism

$$\beta : M \oplus \Lambda(G)^r \to \Lambda(G)^r \tag{25}$$

which lifts α. In particular, it is then clear that $(\mathrm{Coker}\,(\beta))_P = 0$, whence, as P is pro-p, it follows from Nakayama's lemma that $\mathrm{Coker}\,(\beta) = 0$. Taking P-homology of the exact sequence

$$0 \to \mathrm{Ker}\,(\beta) \to M \oplus \Lambda(G)^r \to \Lambda(G)^r \to 0,$$

and noting that $H_1(P, \Lambda(G)^r) = 0$ because $\Lambda(G)$ is a free $\Lambda(P)$-module of finite rank, we conclude that $(\mathrm{Ker}\,(\beta))_P = 0$, and so also $\mathrm{Ker}\,(\beta) = 0$. Thus β is an isomorphism, and the class of M in $K_0(\Lambda(G))$ is zero. This completes the proof of Lemma 3.5. □

We now prove Proposition 3.4. For the proof, we fix a pro-p open normal subgroup P of G, and put $\Delta = G/P$. We write $\mathcal{V} = \mathcal{V}(\Delta)$ for the set of irreducible representations of the finite group Δ over $\bar{\mathbb{Q}}_p$, and we take L to be some fixed finite extension of $\mathbb{Q}_p$ such that all representations in $\mathcal{V}$ can be realized over L. Thus we have an isomorphism of rings

$$\gamma : L[\Delta] \xrightarrow{\simeq} \prod_{\rho \in \mathcal{V}} M_{n_\rho}(L), \tag{26}$$

where n_ρ denotes the dimension of ρ. The proof proceeds by constructing a canonical homomorphism

$$\lambda : K_0(\Lambda(G)) \to \prod_{\rho \in \mathcal{V}} K_0(L), \tag{27}$$

which will be the composition $\lambda = \lambda_4 \circ \lambda_3 \circ \lambda_2 \circ \lambda_1$ of four natural maps λ_i $(i = 1, \ldots, 4)$, defined as follows. Firstly, λ_1 is the canonical map appearing in Lemma 3.5. Secondly, we take

$$\lambda_2 : K_0(\mathbb{Z}_p[\Delta]) \to K_0(\mathbb{Q}_p[\Delta])$$

and

$$\lambda_3 : K_0(\mathbb{Q}_p[\Delta]) \to K_0(L[\Delta])$$

to be the maps induced by the evident inclusions of rings. Finally, we take λ_4 to be the isomorphism

$$\lambda_4 : K_0(L[\Delta]) \xrightarrow{\simeq} \prod_{\rho \in \mathcal{V}} K_0(M_{n_\rho}(L)) \xrightarrow{\simeq} \prod_{\rho \in \mathcal{V}} K_0(L),$$

where the first map is induced by γ, and the second is given by Morita equivalence. Now λ_1 is injective by Lemma 3.5. Moreover, it is well known from the representation theory of finite groups that λ_2 is injective (see [27], Chap. 16, Theorem 34, Corollary 2) and that λ_3 is injective (see [27], Chap. 14, §14.6). Hence we conclude that the homomorphism λ is always injective.

To complete the proof of Proposition 3.4, we shall employ an alternative description of the map λ. Consider the map

$$\tau : K_0(\Lambda_O(G)) \to K_0(O) \tag{28}$$

induced by the augmentation map from $\Lambda_O(G)$ to O. Recall that, since G has no element of order p, $\Lambda_O(G)$ has finite global dimension, and we can identify $K_0(\Lambda_O(G))$ with the Grothendieck group of the category of all finitely generated $\Lambda_O(G)$-modules (see [19], §12.4.8). Let U (resp. A) be a finitely generated $\Lambda_O(G)$-module (resp. O-module), and write $[U]$ (resp. $[A]$) for the class of U (resp. A) in $K_0(\Lambda_O(G))$ (resp. $K_0(O)$). Then it is easily seen that τ is given explicitly by

$$\tau([U]) = \sum_{i \geq 0} (-1)^i [H_i(G, U)]. \tag{29}$$

Let us also note that τ clearly factors through the map

$$\varepsilon : K_0(\Lambda_O(G)) \to K_0(\Lambda_O(\Gamma)) \tag{30}$$

by the natural surjection from $\Lambda_O(G)$ to $\Lambda_O(\Gamma)$. Moreover, ε is given explicitly by

$$\varepsilon([U]) = \sum_{i\geq 0}(-1)^i[H_i(H,U)]. \tag{31}$$

Let $j : K_0(O) \to K_0(L)$ be the isomorphism induced by the inclusion of O in L. For each ρ in $\mathcal{V}$, let $\mathrm{tw}_\rho(M)$ be the $\Lambda_O(G)$-module defined by (13). For each finitely generated $\Lambda(G)$-module M, it can be readily verified that

$$\lambda([M]) = \prod_{\rho\in\mathcal{V}} j(\tau([\mathrm{tw}_\rho(M)])). \tag{32}$$

We can now finish the proof of Proposition 3.4. Suppose that M belongs to $\mathfrak{M}_H(G)$. By Lemmas 3.1 and 3.2, we conclude that $H_i(H, \mathrm{tw}_\rho(M))$ is $\Lambda_O(\Gamma)$-torsion for all $i \geq 0$, and thus their class in $K_0(\Lambda_O(\Gamma))$ vanishes since the latter is isomorphic to $\mathbb{Z}$, via the map which assigns to a finitely generated $\Lambda_O(\Gamma)$-module its rank. Hence it follows from (31) that $\varepsilon([\mathrm{tw}_\rho(M)]) = 0$, whence certainly $\tau([\mathrm{tw}_\rho(M)]) = 0$, for all ρ in $\mathcal{V}$. But then (32) implies that $\lambda([M]) = 0$, and so we must have $[M] = 0$, because λ is injective. It now follows from the exactness of (24) that ∂_G is surjective, and the proof of Proposition 3.4 is complete. □

In view of Proposition 3.4, we can now define the notion of a *characteristic element* for each M in $\mathfrak{M}_H(G)$.

Definition. For each M in $\mathfrak{M}_H(G)$, a characteristic element of M is any ξ_M in $K_1(\Lambda(G)_{S^*})$ such that

$$\partial_G(\xi_M) = [M]. \tag{33}$$

We recall that we say an $\Lambda(G)$-module M has finite G-Euler characteristic if $H_i(G, M)$ is finite for all $i \geq 0$. If M has finite G-Euler characteristic, we define

$$\chi(G, M) = \prod_{i\geq 0} \sharp(H_i(G, M))^{(-1)^i}, \tag{34}$$

the product on the right is finite beause of our hypothesis that G has no element of order p. The principal result of this section, which is directly inspired by a parallel result in [33], is the following relation between characteristic elements and G-Euler characteristics. We write $|\ |_p$ for the valuation of $\bar{\mathbb{Q}}_p$, normalized so that $|p|_p = 1/p$. For our continuous homomorphism

$$\rho : G \to GL_n(O),$$

we write $m_\rho = [L : \mathbb{Q}_p]$, where L is the quotient field of O. Let $\hat{\rho}$ denote the contragradient representation of G, i.e. $\hat{\rho}(g) = \rho(g^{-1})^t$ for g in G, where $'t'$ denotes the transpose matrix.

Theorem 3.6. *Assume that G has no element of order p. Take M in $\mathfrak{M}_H(G)$, and let ξ_M be a characteristic element of M. Then, for every continuous homomorphism $\rho : G \to GL_n(O)$ such that $\chi(G, \mathrm{tw}_{\hat{\rho}}(M))$ is finite, we have*

$$\xi_M(\rho) \neq 0,\ \infty, \tag{35}$$

and

$$\chi(G, \mathrm{tw}_{\hat{\rho}}(M)) = |\xi_M(\rho)|_p^{-m_\rho}, \tag{36}$$

where $m_\rho = [L : \mathbb{Q}_p]$*, and* L *is the quotient field of* O*.*

Before giving the proof of Theorem 3.6, we recall an important ingredient in it, which was first introduced in [6]. Assume M lies in $\mathfrak{M}_H(G)$. By Lemma 3.1, the $H_i(H, M)$ $(i \geq 0)$ are finitely generated torsion $\Lambda(\Gamma)$-modules, which are zero for $i \geq d$. Let $f_{i,M}$ denote a characterisitic power series for $H_i(H, M)$ as a $\Lambda(\Gamma)$-module. We then define the *Akashi series* $\mathrm{Ak}(M)$ by

$$\mathrm{Ak}(M) = \prod_{i \geq 0} f_{i,M}^{(-1)^i} \bmod \Lambda(\Gamma)^\times. \tag{37}$$

As is explained in [6], Ak induces in the evident fashion a homomorphism

$$\mathrm{Ak} : K_0(\mathfrak{M}_H(G)) \to Q(\Gamma)^\times / \Lambda(\Gamma)^\times. \tag{38}$$

Suppose now that M is also an O-module, so that we can regard the $H_i(H, M)$ as finitely generated torsion $\Lambda_O(\Gamma)$-modules. Let $g_{i,M}$ denote a characteristic power series of $H_i(H, M)$ as a $\Lambda_O(\Gamma)$-module. We then define

$$\mathrm{Ak}_O(M) = \prod_{i \geq 0} g_{i,M}^{(-1)^i} \bmod \Lambda_O(\Gamma)^\times. \tag{39}$$

Now $\Lambda_O(\Gamma)$ is a free $\Lambda(\Gamma)$-module of rank $m_\rho = [L : \mathbb{Q}_p]$, and we let N denote the norm map from $\Lambda_O(\Gamma)$ to $\Lambda(\Gamma)$. It follows from [3], Chap.VII, §4.8, Prop. 18 that $N(g_{i,M}) = f_{i,M} \bmod \Lambda(\Gamma)^\times$ for all $i \geq 0$, and so we conclude that

$$N(\mathrm{Ak}_O(M)) = \mathrm{Ak}(M). \tag{40}$$

We now begin the proof of Theorem 3.6. Since the map $M \mapsto \mathrm{tw}_{\hat{\rho}}(M)$ preserves exact sequences, we can define a map

$$\Delta_\rho : K_0(\mathfrak{M}_H(G)) \to Q_O(\Gamma)^\times / \Lambda_O(\Gamma)^\times \tag{41}$$

by

$$\Delta_\rho([M]) = \mathrm{Ak}_O(\mathrm{tw}_{\hat{\rho}}(M)). \tag{42}$$

Let

$$\partial_\Gamma : Q_O(\Gamma)^\times \to Q_O(\Gamma)^\times / \Lambda_O(\Gamma)^\times$$

be the natural surjection. Consider the diagram

$$\begin{array}{ccc} K_1(\Lambda(G)_{S^*}) & \xrightarrow{\partial_G} & K_0(\mathfrak{M}_H(G)) \\ {\scriptstyle \Phi'_\rho}\downarrow & & \downarrow{\scriptstyle \Delta_\rho} \\ Q_O(\Gamma)^\times & \xrightarrow{\partial_\Gamma} & Q_O(\Gamma)^\times / \Lambda_O(\Gamma)^\times. \end{array} \tag{43}$$

Lemma 3.7. *The diagram* (43) *is commutative.*

Let us now assume Lemma 3.7, and show that Theorem 3.6 follows. Let M and ξ_M be as in Theorem 3.6, and assume that $\chi(G, \mathrm{tw}_{\hat{\rho}}(M))$ is finite. As before, let $\varphi : \Lambda_O(\Gamma) \to O$ be the augmentation map, and $\mathfrak{p}$ its kernel. We again write

$$\varphi : \Lambda_O(\Gamma)_{\mathfrak{p}} \to L$$

for the homomorphism induced by φ. Since $\chi(G, \mathrm{tw}_{\hat{\rho}}(M))$ is finite, it is proven in [6] that $\varphi(f_{i,\mathrm{tw}_{\hat{\rho}}(M)}) \neq 0$ for all $i \geq 0$, that $\varphi(\mathrm{Ak}(\mathrm{tw}_{\hat{\rho}}(M))) \neq 0,\ \infty$, and that

$$\chi(G, \mathrm{tw}_{\hat{\rho}}(M)) = |\varphi(\mathrm{Ak}(\mathrm{tw}_{\hat{\rho}}(M)))|_p^{-1}. \tag{44}$$

Using (40) and the obvious fact that N commutes with the augumentation map, it follows that $\varphi(\mathrm{Ak}_O(\mathrm{tw}_{\hat{\rho}}(M))) \neq 0,\ \infty$, and that

$$\chi(G, \mathrm{tw}_{\hat{\rho}}(M)) = |\varphi(\mathrm{Ak}_O(\mathrm{tw}_{\hat{\rho}}(M)))|_p^{-m_\rho}. \tag{45}$$

But the commutativity of (43) shows that

$$\partial_\Gamma(\Phi'_\rho(\xi_M)) = \mathrm{Ak}_O(\mathrm{tw}_{\hat{\rho}}(M)). \tag{46}$$

Hence assertions (35) and (36) are clear from (45) and (46).

We now prove the commutativity of the diagram (43), which will complete the proof of Theorem 3.6. Let $K_0^{\mathrm{tor}}(M_n(\Lambda_O(\Gamma)))$ be the Grothendieck group of the category of all finitely generated torsion $M_n(\Lambda_O(\Gamma))$-modules. Now Morita equivalence and the functoriality of the localization sequence in K-theory shows that we have a commutative diagram

$$\begin{array}{ccc} K_1(\Lambda(G)_{S^*}) & \xrightarrow{\partial_G} & K_0(\mathfrak{M}_H(G)) \\ {\scriptstyle u_1}\downarrow & & \downarrow{\scriptstyle u_0} \\ K_1(M_n(Q_O(\Gamma))) & \xrightarrow{\partial_n} & K_0^{\mathrm{tor}}(M_n(\Lambda_O(\Gamma))) \\ {\scriptstyle v_1}\downarrow\cong & & \cong\downarrow{\scriptstyle v_0} \\ K_1(Q_O(\Gamma)) & \xrightarrow{\partial_1} & K_0^{\mathrm{tor}}(\Lambda_O(\Gamma)), \end{array} \tag{47}$$

where u_0 is induced by the ring homomorphism Φ_ρ given in (15), u_1 is induced by the extension (17) of Φ_ρ, ∂_n and ∂_1 are connecting homomorphisms of localization, and v_0 and v_1 are given by Morita equivalence. Granted the canonical identifications

$$K_1(Q_O(\Gamma)) = Q_O(\Gamma)^\times, \quad K_0^{\mathrm{tor}}(\Lambda_O(\Gamma)) = Q_O(\Gamma)^\times / \Lambda_O(\Gamma)^\times,$$

it therefore suffices to compute $v_0 \circ u_0$, and show that it is indeed $\Delta_{\hat{\rho}}$ given by $\hat{\rho}(g) = \rho(g^{-1})^t$. Take M in $\mathfrak{M}_H(G)$. We can find a finite resolution

$$0 \to P_r \to P_{r-1} \to \cdots \to P_0 \to M \to 0, \tag{48}$$

where each P_i is a finitely generated projective $\Lambda(G)$-module. Thus, viewing $M_n(\Lambda_O(\Gamma))$ as a right $\Lambda(G)$-module via the homomorphism Φ_ρ, we have, by definition,

$$u_0([M]) = \sum_{i \geq 0} (-1)^i [M_n(\Lambda_O(\Gamma)) \otimes_{\Lambda(G)} P_i]. \tag{49}$$

On the other hand, for an arbitrary ring R, the Morita equivalence between the category of $M_n(R)$-modules and the category of R-modules is given by $N \mapsto (R^n)^t \otimes_{M_n(R)} N$ where $(R^n)^t$ means the space of row vectors over R with n entries ($'t'$ denotes the transpose) on which $M_n(R)$ acts from the right in the evident way. Put $R = \Lambda_O(\Gamma)$. We endow $R \otimes_O (O^n)^t$ with the right G-action given by $(\tau \otimes x^t)g = \tau\bar{g} \otimes x^t\rho(g)^t$, where τ is in R, x is in O^n, g is in G, and $\bar{g}$ denotes the image of g in Γ. Recalling that the left G-action on $\mathrm{tw}_{\hat{\rho}}(P_i) = P_i \otimes_{\mathbb{Z}_p} O^n$ is given by $g(y \otimes x) = gy \otimes \hat{\rho}(g)x$ for y in P_i, we obtain an isomorphism of R-modules

$$(R \otimes_O (O^n)^t) \otimes_{\Lambda(G)} P_i \xrightarrow{\simeq} R \otimes_{\Lambda_O(G)} \mathrm{tw}_{\hat{\rho}}(P_i)$$

by mapping $\tau \otimes x^t \otimes y$ to $\tau \otimes y \otimes x$. Combining this isomorphism with the natural identification

$$((R^n)^t \otimes_{M_n(R)} M_n(R)) \otimes_{\Lambda(G)} P_i = (R \otimes_O (O^n)^t) \otimes_{\Lambda(G)} P_i,$$

we deduce finally that we have an isomorphism of R-modules

$$((R^n)^t \otimes_{M_n(R)} M_n(R)) \otimes_{\Lambda(G)} P_i \xrightarrow{\simeq} R \otimes_{\Lambda_O(G)} \mathrm{tw}_{\hat{\rho}}(P_i).$$

Hence

$$v_0([M_n(\Lambda_O(\Gamma)) \otimes_{\Lambda(G)} P_i]) = \Lambda_O(\Gamma) \otimes_{\Lambda_O(G)} \mathrm{tw}_{\hat{\rho}}(P_i). \tag{50}$$

But it has already been remarked that, if N is any free $\Lambda_O(G)$-module, then $\mathrm{tw}_{\hat{\rho}}(N)$ is again free. Hence it follows easily that $\mathrm{tw}_{\hat{\rho}}(P_i)$ is again a projective $\Lambda_O(G)$-module, and the exact sequence

$$0 \to \mathrm{tw}_{\hat{\rho}}(P_r) \to \mathrm{tw}_{\hat{\rho}}(P_{r-1}) \to \cdots \to \mathrm{tw}_{\hat{\rho}}(P_0) \to \mathrm{tw}_{\hat{\rho}}(M) \to 0$$

is a projective resolution of $\mathrm{tw}_{\hat{\rho}}(M)$. Tensoring this exact sequence with $\Lambda_O(\Gamma)$ over $\Lambda_O(G)$, we get a complex whose cohomology groups are the $H_i(H, \mathrm{tw}_{\hat{\rho}}(M))$ $(i \geq 0)$. Thus it follows that the image of $v_0 \circ u_0([M])$ under the canonical isomorphism from $K_0^{\mathrm{tor}}(\Lambda_O(\Gamma))$ to $Q_O(\Gamma)^\times/\Lambda_O(\Gamma)^\times$ is precisely $\mathrm{Ak}_O(\mathrm{tw}_{\hat{\rho}}(M))$. This completes the proof of Theorem 3.6. □

We say our continuous representation $\rho : G \to GL_n(O)$ is an *Artin representation* if $\mathrm{Ker}\,(\rho)$ is open in G, or equivalently if ρ factors through a finite quotient of G. The following stronger form of Theorem 3.6, but for a much more restricted class of modules, will be needed in the last section to study some of the consequences of the "main conjecture".

Theorem 3.8. *Assume that G has no element of order p. Let M be a module in $\mathfrak{M}_H(G)$, which, in addition, satisfies*

$$H_i(H', M) = 0 \quad \textit{for all } i \geq 1, \tag{51}$$

and for all open subgroups H' of H, which are normal in G. Let ξ_M denote a characteristic element of M. Then $\xi_M(\rho) \neq \infty$ for every Artin representation ρ of G. Moreover, for each Artin representation ρ of G, $\xi_M(\rho) \neq 0$ if and only if $\chi(G, \mathrm{tw}_{\hat{\rho}}(M))$ is finite.

The following lemma is the essential ingredient in the proof of Theorem 3.8.

Lemma 3.9. *Let M be a module in $\mathfrak{M}_H(G)$, satisfying* (51). *Then, if ρ is any Artin representation of G,*

$$\mathrm{Ak}_O(\mathrm{tw}_\rho(M)) \in \Lambda_O(\Gamma)[\frac{1}{p}] \text{ modulo } \Lambda_O(\Gamma)^\times. \tag{52}$$

Moreover, if $\varphi : \Lambda_O(\Gamma)_\mathfrak{p} \to L$ is the homomorphism induced by the augmentation map, then $\varphi(\mathrm{Ak}_O(\mathrm{tw}_\rho(M))) \neq 0$ if and only if $\chi(G, \mathrm{tw}_\rho(M))$ is finite.

Proof. Let ρ be any Artin representation of G, and put $W = \mathrm{tw}_\rho(M)$. Let $g_{i,W}$ denote the characteristic power series of $H_i(H, W)$ as a $\Lambda_O(\Gamma)$-module ($i \geq 0$). Let π denote a local parameter of O. We now prove that we can take

$$g_{i,W} = \pi^{\mu_i} \quad (i \geq 1) \tag{53}$$

for some integer $\mu_i \geq 0$. Take $H' = \mathrm{Ker}\,(\rho) \cap H$. Hence (51) holds for H', whence it follows easily that we have $H_i(H', M_O) = 0$ for all $i \geq 1$. But since $H' \subset \mathrm{Ker}\,(\rho)$, we have $W = M_O^n$ as H'-modules, and so we conclude that

$$H_i(H', W) = 0 \quad (i \geq 1). \tag{54}$$

Put $\Delta = H/H'$. It follows from (53) and the Hochschild-Serre spectral sequence that

$$H_i(H, W) = H_i(\Delta, W_{H'}) \quad (i \geq 1). \tag{55}$$

But the group on the right is clearly annihilated by the order of the finite group Δ, whence it is plain that the characteristic power series of the module on the left must be a power of π. This proves (53). Hence

$$\mathrm{Ak}_O(W) = g_{0,W} \prod_{i \geq 1} \pi^{(-1)^i \mu_i} \mod \Lambda_O(\Gamma)^\times, \tag{56}$$

and so assertion (52) is proven. It also follows from (56) that $\varphi(\mathrm{Ak}_O(W)) \neq 0$ if and only if $\varphi(g_{0,W}) \neq 0$. Now a standard argument with the Hochschild-Serre spectral sequence (see [6]) shows that $\chi(G, M)$ is finite if and only if $\varphi(g_{i,W}) \neq 0$ for all $i \geq 0$. But, in view of (53), it is clear that $\varphi(g_{i,W}) \neq 0$ for all $i \geq 0$ if and only if $\varphi(g_{0,W}) \neq 0$. This completes the proof of Lemma 3.9. □

Theorem 3.8 is an almost immediate consequence of Lemmas 3.7 and 3.9. By definition, for any Artin representation ρ of G, $\xi_M(\rho) \neq \infty$ means that $\Phi'_\rho(\xi_M)$ belongs to $\Lambda_O(\Gamma)_\mathfrak{p}$. But, by Lemma 3.7,

$$\partial_\Gamma(\Phi'_\rho(\xi_M)) = \mathrm{Ak}_O(\mathrm{tw}_{\hat{\rho}}(M)), \tag{57}$$

whence it is clear from (52) that $\Phi'_\rho(\xi_M)$ does belong to $\Lambda_O(\Gamma)_\mathfrak{p}$. The final assertion of Theorem 3.8 is also clear from (57) and the final assertion of Lemma 3.9. This completes the proof of Theorem 3.8. □

We next establish an analogue of the classical Artin formalism for G-Euler characteristics. The result is of interest in its own right, but we shall also use it to study the

numerical example at the end of this section. In fact, as we shall show, the Artin formalism holds for all compact p-adic Lie groups G with no element of order p, and we do not need for this result the existence of a closed normal subgroup H of G with $G/H \cong \mathbb{Z}_p$. We use similar notation to earlier. Let G' be an arbitrary open normal subgroup of G, and let $\Delta = G/G'$. Let $\mathcal{V} = \mathcal{V}(\Delta)$ denote the set of irreducible representations of Δ over $\bar{\mathbb{Q}}_p$. We take L to be any finite extension of $\mathbb{Q}_p$ such that all representations in $\mathcal{V}$ can be realized over L, and we write O for the ring of integers of L.

Theorem 3.10. *Let G be any compact p-adic Lie group with no element of order p, G' an open normal subgroup of G, and let $\Delta = G/G'$. Let M be a finitely generated $\Lambda(G)$-module. Then $\chi(G', M)$ is finite if and only if $\chi(G, \mathrm{tw}_\rho(M))$ is finite for all ρ in $\mathcal{V} = \mathcal{V}(\Delta)$. When $\chi(G', M)$ if finite, we have*

$$\chi(G', M)^{[L:\mathbb{Q}_p]} = \prod_{\rho \in \mathcal{V}} \chi(G, \mathrm{tw}_\rho(M))^{n_\rho}, \tag{58}$$

where n_ρ is the dimension of ρ.

We now prove Theorem 3.10. Put $R = O[\Delta]$. If ρ is in $\mathcal{V}$, we let L_ρ denote a free O-module of rank n_ρ, endowed with a left action of R which realizes ρ. We then have an exact sequence of left R-modules

$$0 \to R \to \bigoplus_{\rho \in \mathcal{V}} L_\rho^{n_\rho} \to W \to 0, \tag{59}$$

where W is finite. If U is any left R-module, we can view U as a right R-module by defining $u.\delta$ to be $\delta^{-1}.u$ for δ in Δ and u in U. In particular, we can view all the modules appearing in (59) to be right R-modules or $\Lambda_O(G)$-modules in this fashion. Now take M to be the module appearing in Theorem 3.10, and put $M_O = M \otimes_{\mathbb{Z}_p} O$. We take a resolution

$$0 \to P_n \to P_{n-1} \to \cdots \to P_0 \to M_O \to 0, \tag{60}$$

where P_i $(0 \leq i \leq n)$ is a finitely generated projective $\Lambda_O(G)$-module. Tensoring (59) on the right over $\Lambda_O(G)$ with P_i, we obtain an exact sequence

$$0 \to R \otimes_{\Lambda_O(G)} P_i \to \bigoplus_{\rho \in \mathcal{V}} (L_\rho \otimes_{\Lambda_O(G)} P_i)^{n_\rho} \to W \otimes_{\Lambda_O(G)} P_i \to 0, \tag{61}$$

the injectivity on the left is valid because P_i is projective. Hence we obtain an exact sequence of complexes

$$0 \to C \to \bigoplus_{\rho \in \mathcal{V}} D_\rho^{n_\rho} \to K \to 0, \tag{62}$$

where $C = (C_i)$, $D_\rho = (D_{\rho,i})$, $K = (K_i)$, with i running from 0 to n, are given by

$$C_i = R \otimes_{\Lambda_O(G)} P_i, \quad D_{\rho,i} = L_\rho \otimes_{\Lambda_O(G)} P_i, \quad K_i = W \otimes_{\Lambda_O(G)} P_i. \tag{63}$$

Now

$$R \otimes_{\Lambda_O(G)} M_O = (M_O)_{G'}, \quad L_\rho \otimes_{\Lambda_O(G)} M_O \xrightarrow{\simeq} (\mathrm{tw}_\rho(M)) \otimes_{\Lambda_O(G)} O = (\mathrm{tw}_\rho(M))_G. \tag{64}$$

Writing $H_i(C)$, $H_i(D_\rho)$, $H_i(K)$ for the i-th homology groups of the complexes C, D_ρ, K, we therefore have, for $0 \leq i \leq n$,

$$H_i(C) = H_i(G', M_O), \quad H_i(D_\rho) = H_i(G, \mathrm{tw}_\rho(M)). \tag{65}$$

Now, as O is flat over $\mathbb{Z}_p$,

$$H_i(G', M_O) = H_i(G', M) \otimes_{\mathbb{Z}_p} O. \tag{66}$$

The long exact sequence for the cohomology of the exact sequence of complexes (62) shows that the conclusions of Theorem 3.10 will all follow provided we can prove that

$$H_i(K) \text{ is finite for } 0 \leq i \leq n \text{ and } \prod_{i=0}^{n} \sharp(H_i(K))^{(-1)^i} = 1. \tag{67}$$

To establish (67), we note that each C_i is a projective finitely generated R-module, and hence C defines a class in $K_0(R)$, which we denote by $[C]$. In fact, we claim that $[C] = 0$. Indeed, the natural map from $K_0(R)$ to $K_0(L[\Delta])$ is injective (see [27], Chap. 16, Theorem 34, Corollary 2), and $[C]$ must be sent to zero under this map because of the fact that $H_i(C)$ is finite for $0 \leq i \leq n$. As $[C]$ maps to zero under an injective map, we must have $[C] = 0$. We now define a canonical homomorphism

$$\theta : K_0(R) \to \mathbb{Q}_p^\times. \tag{68}$$

Note that, if A is any finitely generated projective R-module, then $W \otimes_R A$ is clearly finite. Moreover, as A is projective, $\mathrm{Tor}_1^A(W, A) = 0$, and we therefore can define θ by sending $[A]$ to $\sharp(W \otimes_R A)$. In particular, as $[C] = 0$, we conclude that $\theta([C]) = 1$. But

$$K_i = W \otimes_R C_i \quad (i = 0, \cdots, n),$$

and so K_i is finite, and

$$\theta([C]) = \prod_{i=0}^{n} \sharp(K_i)^{(-1)^i} = \prod_{i=0}^{n} \sharp(H_i(K))^{(-1)^i}. \tag{69}$$

Since $\theta([C]) = 1$, (67) follows from (69). This completes the proof of Theorem 3.10. □

Example. We end this section by discussing a numerical example of our algebraic theory, arising from the arithmetic of elliptic curves. Let $E = X_1(11)$ be the elliptic curve over $\mathbb{Q}$ of conductor 11

$$y^2 + y = x^3 - x^2. \tag{70}$$

Take $p = 5$, and let E_{5^∞} denote the group of all 5-power division points on E. Define

$$F_\infty = \mathbb{Q}(E_{5^\infty}). \tag{71}$$

By the Weil pairing, F_∞ contains $\mathbb{Q}(\mu_{5^\infty})$, where μ_{5^∞} denotes the group of all 5-power roots of unity. In particular, F_∞ contains the cyclotomic $\mathbb{Z}_5$-extension of $\mathbb{Q}$, which we denote by $\mathbb{Q}^{\rm cyc}$. Define the Galois groups

$$G = G(F_\infty/\mathbb{Q}), \quad H = G(F_\infty/\mathbb{Q}^{\rm cyc}), \quad \Gamma = G(\mathbb{Q}^{\rm cyc}/\mathbb{Q}), \tag{72}$$

providing an example of compact 5-adic Lie groups to which our general theory applies. We remark in passing that not only is G open in $GL_2(\mathbb{Z}_5)$, but in fact it is well known ([13], Prop. 1.5) to be isomorphic to the subgroup of $GL_2(\mathbb{Z}_5)$ consisting of all elements $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix} \bmod 5.$$

We shall be interested in the following two irreducible Artin representations ρ_i $(i = 1, 2)$ of G. Let E_2 denote the unique elliptic curve over $\mathbb{Q}$ of conductor 11 with $E_2(\mathbb{Q}) = 0$ (thus E_2 is the curve A_2 of [13]). If we write E_5 and $E_{2,5}$ for the groups of 5-division points on E, E_2, respectively, and define

$$K_1 = \mathbb{Q}(E_5), \quad K_2 = \mathbb{Q}(E_{2,5}), \tag{73}$$

then K_1 and K_2 are both cyclic extensions of degree 5 of the field $\mathbb{Q}(\mu_5)$, and they are both contained in F_∞. Let χ_i $(i = 1, 2)$ denote any non-trivial character of the Galois group of K_i over $\mathbb{Q}(\mu_5)$. Then we define ρ_i to be the character of the Galois group of K_i over $\mathbb{Q}$ which is induced by χ_i, and we can then view ρ_i as an Artin representation of G. It is easily seen that ρ_i is irreducible of degree 4, and, in fact, ρ_i can be realized as a 4-dimensional representation even over $\mathbb{Q}$. Also $\hat{\rho}_i = \rho_i$ for $i = 1, 2$.

We write $X(E/F_\infty)$ for the compact Pontrjagin dual of the Selmer group of E over F_∞ (see §4 for a fuller discussion of Selmer groups). Then $X(E/F_\infty)$ is a finitely generated $\Lambda(G)$-module, and it is proven in [5] that $X(E/F_\infty)$ is finitely generated over $\Lambda(H)$. Hence $X(E/F_\infty)$ belongs to our category $\mathfrak{M}_H(G)$. We write $\xi_{E,5}$ for any choice of a characteristic element of $X(E/F_\infty)$.

Proposition 3.11. *Put $M = X(E/F_\infty)$. For $i = 1, 2$, $\chi(G, \mathrm{tw}_{\rho_i}(M))$ is finite, and, in fact,*

$$\chi(G, \mathrm{tw}_{\rho_1}(M)) = 5^3, \quad \chi(G, \mathrm{tw}_{\rho_2}(M)) = 5. \tag{74}$$

In view of Proposition 3.11, we deduce from Theorem 3.6 that $\xi_{E,5}(\rho_i) \neq 0, \infty$ $(i = 1, 2)$ and

$$|\xi_{E,5}(\rho_1)|_5^{-1} = 5^3, \quad |\xi_{E,5}(\rho_2)|_5^{-1} = 5. \tag{75}$$

We now prove Proposition 3.11, by combining Theorem 3.10 with the following explicit Euler characteristic formula for $X(E/F_\infty)$ (which is Theorem 1.1 of [5] applied to this example for the prime $p = 5$). Put $F = \mathbb{Q}(\mu_5)$, and let K be any finite extension of F, which is contained in F_∞. Write

$$G_K = G(F_\infty/K).$$

For each finite place v of K, we write d_v for the degree of K completed at v over the completion of $\mathbb{Q}$ at v, k_v for the residue field, and $\tilde{E}_v$ for the reduction of E modulo v. Let $Ш(E/K)$ be the Tate-Shafarevich group of E over K. Assume now that

$$E(K) \text{ and } Ш(E/K)(5) \text{ are both finite.} \tag{76}$$

Since $X(E/F_\infty)$ is finitely generated over $\Lambda(H)$, it follows that the hypotheses of Theorem 1.1 of [5] hold for E over K and the prime $p = 5$. Hence Theorem 1.1 of [5] shows that, putting $X = X(E/F_\infty)$, we have $\chi(G_K, X)$ is finite, and is given by the arithmetic formula

$$\chi(G_K, X) = \frac{\sharp(Ш(E/K)(5))}{\sharp(E(K)(5))^2} \times \prod_{v|11} (5|d_v|_5^{-1}) \times \prod_{v|5} \sharp(\tilde{E}_v(k_v)(5))^2 \ ; \tag{77}$$

here the first product on the right of (77) is taken over the primes v of K dividing 11, and the second over primes v of K dividing 5. When $K = F$, it is well known (see [9]) that

$$E(F)(5) = \mathbb{Z}/5\mathbb{Z}, \quad Ш(E/F)(5) = 0.$$

Since there are four primes of F above 11 with $d_v = 1$, and since there is a unique prime above 5 with residue field $\mathbb{F}_5$, we conclude from (77) that

$$\chi(G_F, X) = 5^4. \tag{78}$$

Taking next $K = K_1$, it is proven in [13] that

$$E(K_1) = (\mathbb{Z}/5\mathbb{Z})^2, \quad Ш(E/K_1)(5) = (\mathbb{Z}/5\mathbb{Z})^2,$$

and that there are four primes of K_1 above 11 with $d_v = 5$, and five primes of K_1 above 5 with residue field $\mathbb{F}_5$. Hence we conclude from (77) that

$$\chi(G_{K_1}, X) = 5^{16}. \tag{79}$$

Applying Theorem 3.10 to both of the open subgroups $G' = G_F$ and $G' = G_{K_1}$, we deduce that $\chi(G, \mathrm{tw}_{\rho_1}(X))$ is finite, and

$$\chi(G, \mathrm{tw}_{\rho_1}(X))^4 = 5^{12},$$

which proves the first assertion of Proposition 3.11. Now take $K = K_2$. It is proven in [13] that

$$E(K_2) = \mathbb{Z}/5\mathbb{Z}, \quad Ш(E/K_2)(5) = 0,$$

and that there are four primes of K_2 above 11 with $d_v = 5$, and one prime of K_2 above 5 with residue field $\mathbb{F}_5$. Hence we conclude from (77) that

$$\chi(G_{K_2}, X) = 5^8. \tag{80}$$

Applying Theorem 3.10 to both of the open subgroups $G' = G_F$ and $G' = G_{K_2}$, we deduce that $\chi(G, \mathrm{tw}_{\rho_2}(X))$ is finite, and

$$\chi(G, \mathrm{tw}_{\rho_2}(X))^4 = 5^4,$$

which proves the second assertion of Proposition 3.11. □

4 Additional properties of characteristic elements.

We now establish some additional properties of the characteristic elements of modules in the category $\mathfrak{M}_H(G)$, and of the group $K_1(\Lambda(G)_{S^*})$ in which they lie. We end this section with some conjectures about the integrality properties of characteristic elements.

We begin with some general remarks. Let R be a ring with unit element, which is left and right Noetherian. We recall that the Jacobson radical of R, which we denote by $\mathrm{Jac}(R)$, is the intersection of all maximal left ideals of R, or equivalently the intersection of all maximal right ideals of R. We say that R is *semi-local* if the ring $R/\mathrm{Jac}(R)$ is both left and right Artinian. The following lemma is well known (see [1], Chap.III, Prop. 2.12, and Chap.IX, Prop. 1.3).

Lemma 4.1. *Let I be a two sided ideal of a ring R, and assume that R is I-adically complete. If I is contained in $\mathrm{Jac}(R)$, then the natural map from $K_0(R)$ to $K_0(R/I)$ is an isomorphism.*

If G is an arbitrary compact p-adic Lie group, it is well known (see [20], Chap.V, Prop. 5.2.16) that $\Lambda(G)$ is a semi-local ring. We assume for the rest of this section that again G has a closed normal subgroup H such that G/H is isomorphic to $\mathbb{Z}_p$, and we let S be the Ore set in $\Lambda(G)$ defined in §2.

Proposition 4.2. *The ring $\Lambda(G)_S$ is semi-local.*

We first establish the following lemma.

Lemma 4.3. *Let J be any pro-p open subgroup of H which is normal in G, and let ψ_J be the homomorphism (3). Define $S_J = \psi_J(S)$. Then S_J is an Ore set of non-zero divisors in $\Omega(G/J)$, and the ring $\Omega(G/J)_{S_J}$ is Artinian.*

Proof. Lemmas 2.1 and 2.2 show that S_J consists of all non-zero divisors in $\Omega(G/J)$. Moreover, as S is an Ore set and ψ_J is surjective, it follows that S_J satisfies the Ore condition. Thus $\Omega(G/J)_{S_J}$ is the total ring of quotients of $\Omega(G/J)$. Now choose a subgroup Π of G/J satisfying (2), and let $\Omega(\Pi) = \mathbb{F}_p[[T]]$ and its quotient field $R(\Pi)$ be as in §2. Define Σ to be the set of non-zero elements of $\Omega(\Pi)$. If α is any element of Σ, it is clear that multiplication by α on the right or the left induces an automorphism of the $R(\Pi)$-vector space $V(G/J)$ defined by (6). Hence, by the proof of Lemmas 2.1 and 2.2, α belongs to S_J; in particular, α is not a divisor of zero in $\Omega(G/J)$. As $\Omega(\Pi)$ is in the centre of $\Omega(G/J)$, it follows that Σ is an Ore set in $\Omega(G/J)$. We claim that

$$\Omega(G/J)_{S_J} = \Omega(G/J)_{\Sigma}. \tag{81}$$

Note that (81) proves the assertion of Lemma 4.3, because the fact that $\Omega(G/J)$ is a finitely generated $\Omega(\Pi)$-module implies that $\Omega(G/J)_{\Sigma}$ is a finite dimensional vector space

over $R(\Pi)$, and so $\Omega(G/J)_\Sigma$ is Artinian. As $\Sigma \subset S_J$, to prove (81) we must show that every element of S_J is invertible in $\Omega(G/J)_\Sigma$. Take any s in S_J. As $\Omega(\Pi)$ lies in the centre of $\Omega(G/J)$, which is finitely generated over $\Omega(\Pi)$, s satisfies an equation (see [19], Lemma 5.3.2) of the form

$$s^n + a_1 s^{n-1} + \cdots + a_n = 0 \quad (a_i \in \Omega(\Pi)). \tag{82}$$

Moreover, since s is not a zero divisor in $\Omega(G/J)$, we can assume that $a_n \neq 0$. Now this equation can be rewritten as

$$(b_0 s^{n-1} + b_1 s^{n-1} + \cdots + b_{n-1})s = 1,$$

where $b_0 = -1/a_n$, and $b_i = -a_i/a_n$ $(i = 1, \cdots, n-1)$, proving that s has an inverse in $\Omega(G/J)_\Sigma$, as required. This completes the proof of Lemma 4.3. □

We now can prove Proposition 4.2. If M is any left $\Lambda(G)$-module, we define

$$M_S = \Lambda(G)_S \otimes_{\Lambda(G)} M.$$

Let J be any subgroup of G as in Lemma 4.3, and let I denote the kernel of ψ_J. Since $\Lambda(G)_S$ is flat over $\Lambda(G)$, we have the exact sequence

$$0 \to I_S \to \Lambda(G)_S \to \Omega(G/J)_S \to 0.$$

But

$$\Omega(G/J)_S = \Omega(G/J)_{S_J}.$$

Hence, by lemma 4.3, it suffices to show that I_S is contained in the Jacobson radical of $\Lambda(G)_S$. In view of [19], Theorem 0.3.8, we must prove that $1 - x$ is a unit in $\Lambda(G)_S$ for every x in I_S. Write $x = s^{-1}\theta$ with θ in I and s in S. Since θ is in I, $\psi_J(s - \theta) = \psi_J(s)$. Hence, by Lemma 2.1, $s - \theta$ belongs to S, But then

$$1 - x = s^{-1}(s - \theta)$$

is clearly a unit in $\Lambda(G)_S$, and the proof of Proposition 4.2 is complete. □

We remark that $\Lambda(G)_{S^*}$ is not, in general, a semi-local ring, as is shown by the following example. Take $G = H \times K$, where both H and K are isomorphic to $\mathbb{Z}_p$. Then we can identify $\Lambda(G)$ with $R = \mathbb{Z}_p[[U, V]]$ by mapping fixed topological generators of H and K to $U + 1$ and $V + 1$, respectively. Then the set S of §2 in this case is the complement of the prime ideal (p, U) in R. Thus R_S is a local ring of dimension 2, whose maximal ideal is generated by p and U. Hence $R_{S^*} = R_S[1/p]$ is a ring of dimension 1. But R_{S^*} has infinitely many prime ideals, and is certainly not semi-local. Indeed, if g is any irreducible distinguished polynomial in $\mathbb{Z}_p[U]$, then gR is a prime ideal whence gR_{S^*} is also prime because $S^* \cap gR$ is empty.

Theorem 4.4. *Assume that G has no element of order p. Then the natural maps $\Lambda(G)_S{}^\times \to K_1(\Lambda(G)_S)$ and $\Lambda(G)_{S^*}{}^\times \to K_1(\Lambda(G)_{S^*})$ are both surjective.*

If R is any semi-local ring, it is well known that the natural map $R^\times \to K_1 R$ is surjective (see [29], [30]). In view of Proposition 4.2, this establishes the first assertion of Theorem 4.4, and we now give the proof of the second assertion. We establish two preliminary lemmas. Note that, if P is a direct summand of $\Lambda(G)$ viewed as a left $\Lambda(G)$-module, then P is a finitely generated projective $\Lambda(G)$-module, and P/pP is a finitely generated projective $\Omega(G)$-module.

Lemma 4.5. *The group $K_0(\Omega(G))$ is generated by the classes $[P/pP]$, where P runs over all direct summands of $\Lambda(G)$ viewed as a left $\Lambda(G)$-module.*

Proof. Let $I = p\Lambda(G)$. Then I is contained in the Jacobson radical of $\Lambda(G)$ since, for each λ in I, $1-\lambda$ is invertible with inverse $\sum_{n=0}^{\infty} \lambda^n$. Moreover, $\Lambda(G)$ is I-adically complete, and so, by Lemma 4.1, the canonical map from $K_0(\Lambda(G))$ to $K_0(\Omega(G))$ is an isomorphism. In particular, $K_0(\Omega(G))$ is generated by the classes $[P/pP]$, where P ranges over all finitely generated projective $\Lambda(G)$-modules. To complete the proof of lemma, we must show that we still get a set of generators if we allow P to only run over the direct summands of $\Lambda(G)$. Pick a pro-p open normal subgroup U of G, and put $\Delta = G/U$. Let D denote the kernel of the natural map from $\Lambda(G)$ to $\mathbb{F}_p[\Delta]$, so that D is generated as a $\Lambda(G)$-module by the set W_U consisting of p and $1-u$, where u ranges over U. Now $\Lambda(U)$ is a local ring, whose maximal ideal $\mathrm{Jac}(\Lambda(U))$ is clearly generated by W_U. But $\Lambda(G)$ is finitely generated over $\Lambda(U)$, and so it is well known that ([19], Prop. 9.1.3)

$$\mathrm{Jac}(\Lambda(G)) \cap \Lambda(U) \subseteq \mathrm{Jac}(\Lambda(U)).$$

This proves that D is contained in $\mathrm{Jac}(\Lambda(G))$, and, as $\Lambda(G)$ is plainly D-adically complete, we conclude from Lemma 4.1 that the natural map from $K_0(\Lambda(G))$ to $K_0(\mathbb{F}_p[\Delta])$ is an isomorphism. Put

$$R = \mathbb{F}_p[\Delta]/\mathrm{Jac}(\mathbb{F}_p[\Delta]).$$

Since $\mathbb{F}_p[\Delta]$ is Artinian, $\mathrm{Jac}(\mathbb{F}_p[\Delta])$ is nilpotent, and so Lemma 4.1 proves that the canonical map from $K_0(\mathbb{F}_p[\Delta])$ to $K_0(R)$ is an isomorphism. However, R is a semisimple ring, and thus $K_0(R)$ is generated by the simple projective R-modules, and these are given precisely by the direct summands of R viewed as a left R-module. It is then well known (see [1], Chap.III, Prop. 2.12) that one can lift these generators of $K_0(R)$ successively back to $K_0(\mathbb{F}_p[\Delta])$ and to $K_0(\Lambda(G))$, so that they remain direct summands of $\mathbb{F}_p[\Delta]$ and $\Lambda(G)$, respectively. This completes the proof of Lemma 4.5. □

Lemma 4.6. *Put $R = \Lambda(G)[1/p]$, and assume that G has no element of order p. Then the natural map $R^\times \to K_1 R$ is surjective.*

Proof. Let $\mathcal{C}$ denote the category of all finitely generated $\Lambda(G)$-modules, which are annihilated by some power of p. Then, by dévissage, it is well known (see, for example, [19], Theorem 12.4.7) that we can naturally identify $K_0(\mathcal{C})$ with $K_0(\mathcal{D})$, where $\mathcal{D}$ is the category of all finitely generated $\Omega(G)$-modules. As G has no element of order p, $\Omega(G)$ has finite global dimension, an so we can identify $K_0(\mathcal{D})$ with $K_0(\Omega(G))$. Thus the localization sequence of K-theory for the multiplicative Ore set consisting of the powers of p lying in $\mathbb{Z}$ gives the commutative diagram

$$\begin{array}{ccccc} \Lambda(G)^\times & \xrightarrow{\ \hookrightarrow\ } & R^\times & \xrightarrow{\ g\ } & K_0(\Omega(G)) \\ \big\downarrow & & {\scriptstyle f}\big\downarrow & & \| \\ K_1(\Lambda(G)) & \longrightarrow & K_1(R) & \xrightarrow{\ \partial\ } & K_0(\Omega(G)) \end{array} \tag{83}$$

where $R = \Lambda(G)[1/p]$, f is the natural map, and the bottom row is exact. Also ∂ is the connecting homomorphism, and $g = \partial \circ f$. Since $\Lambda(G)$ is semi-local, the left vertical map is surjective (see [29], [30]). We conclude from (83) that f will be surjective provided we can prove g is surjective. We now proceed to show this.

By Lemma 4.5, $K_0(\Omega(G))$ is generated by the classes $[P/pP]$, where P runs over the direct summands of $\Lambda(G)$, viewed as a left $\Lambda(G)$-module. Hence it suffices to show that each such class belongs to the image of g. Take such a P, and let P' be the $\Lambda(G)$-module such that

$$P \oplus P' = \Lambda(G). \tag{84}$$

In terms of the decomposition (84), we can define endomorphisms of $\Lambda(G)$, viewed as a left $\Lambda(G)$-module, by

$$\alpha(x+y) = px + y, \quad \beta(x+y) = x + py \qquad (x \in P,\ y \in P').$$

Thus α and β are given, respectively, by multiplication on the right by $a = \alpha(1)$, $b = \beta(1)$. Since $ab = p$, it follows that a and b are both units in R. On the other hand, the explicit description of ∂ in the localization sequence (see [28]) shows that

$$\partial(f(a)) = [\operatorname{Coker}\alpha] = [P/pP].$$

This completes the proof of Lemma 4.6. □

We can now prove the second assertion of Theorem 4.4. As before, we let $R = \Lambda(G)[1/p]$, $\Omega(G) = \Lambda(G)/p\Lambda(G)$, and put

$$R' = \Lambda(G)_S[\frac{1}{p}] = \Lambda(G)_{S^*}, \quad \Omega'(G) = \Lambda(G)_S/p\Lambda(G)_S.$$

As in the proof of Lemma 4.6, we can identify the Grothendieck group of the category of all finitely generated $\Lambda(G)_S$-modules, which are annihilated by some power of p, with $K_0(\Omega'(G))$. Thus, parallel to (83), we have the exact sequence of localization

$$K_1(\Lambda(G)_S) \to K_1(R') \xrightarrow{\partial'} K_0(\Omega'(G)). \tag{85}$$

Let f' denote the natural map from $(R')^\times$ to $K_1(R')$, and put $g' = \partial' \circ f'$. As $\Lambda(G)_S$ is semi-local, the natural map from ${\Lambda(G)_S}^\times$ to $K_1(\Lambda(G)_S)$ is surjective. In view of this last remark, we conclude from the exact sequence (85) that f' is surjective provided g' is surjective. To establish the surjectivity of g', we note that we have a commutative diagram

$$\begin{array}{ccc} R^\times & \xrightarrow{g} & K_0(\Omega(G)) \\ \downarrow & & \downarrow h \\ (R')^\times & \xrightarrow{g'} & K_0(\Omega'(G)), \end{array}$$

where the vertical maps are the natural ones. We claim that both g and h are surjective, which will clearly imply that g' is surjective. But the surjectivity of g was proven in the course of the proof of Lemma 4.6. Let S' denote the image of S in $\Omega(G)$. By (iii) of Lemmas 2.1 and 2.2, S' consists of non-zero divisors in $\Omega(G)$, and it is plain that S' is an Ore set in $\Omega(G)$. As localization with respect to S is an exact functor, we see easily that

$$\Omega'(G) = \Omega(G)_{S'}.$$

But then it is well known ([19], Theorem 12.4.9) that the natural map h from $K_0(\Omega(G))$ to $K_0(\Omega(G)_{S'})$ is surjective. This completes the proof of Theorem 4.4. □

We next show that any module M in the category $\mathfrak{M}_H(G)$ has many twists ρ by continuous representations of G of the form (12) with finite G-Euler characteristics. Indeed, consider continuous representations

$$\eta : \Gamma \to O^\times. \tag{86}$$

Since $\Gamma = G/H$, we can always view such η as a continuous representation of G.

Lemma 4.7. *Assume that G has no element of order p, and let $M \in \mathfrak{M}_H(G)$. Then, for all but finitely many Artin characters η of Γ, $\chi(G, \mathrm{tw}_\eta(M))$ is finite. Moreover, if η is a fixed character of Γ of infinite order, $\chi(G, \mathrm{tw}_{\eta^n}(M))$ is finite for all but finitely many $n \in \mathbb{Z}$.*

Proof. We pick a topological generator γ_0 of Γ, and identify $\Lambda_O(\Gamma)$ with $O[[T]]$ by mapping γ_0 to $1+T$. As earlier, let $M_O = M \otimes_{\mathbb{Z}_p} O$. Since M belongs to $\mathfrak{M}_H(G)$, $H_i(H, M_O)$ is a torsion $\Lambda_O(\Gamma)$-module for all $i \geq 0$, and we write $f_{i,M}$ for a characteristic series of $H_i(H, M_O)$. Since $\eta(H) = 1$, we have

$$H_i(H, \mathrm{tw}_\eta(M)) = H_i(H, M_O) \otimes_O A_\eta,$$

where A_η denotes a free O -module of rank 1 on which Γ acts via η, i.e. $\gamma.a = \eta(\gamma)a$ for γ in Γ and a in A_η. It follows easily that

$$f_{i,\mathrm{tw}_\eta(M)}(T) = f_{i,M}(\eta(\gamma_0)^{-1}(1+T) - 1). \tag{87}$$

Now a standard argument with the Hochschild-Serre spectral sequence (see, for example, [6]) shows that $\chi(G, \mathrm{tw}_\eta(M))$ is finite provided $f_{i,\mathrm{tw}_\eta(M)}(0) \neq 0$, or equivalently

$$f_{i,M}(\eta(\gamma_0)^{-1} - 1) \neq 0 \qquad (0 \leq i \leq d-1)\ ; \tag{88}$$

here d denotes the dimension of G as a p-adic Lie group. Let $\mathfrak{Z}$ denote the set of all zeros of the $f_{i,M}(T)$ $0 \leq i \leq d-1$) lying in the maximal ideal of the ring of integers of

$\bar{\mathbb{Q}}_p$. By the Weierstrass Preparation Theorem, $\mathfrak{Z}$ is a finite set. Hence, as η runs over all the Artin characters of Γ, only finitely many of the $\eta(\gamma_0)^{-1} - 1$ can lie in $\mathfrak{Z}$, and the first assertion of the lemma is proven. Now suppose that η has infinite order, so that the characters η^n ($n \in \mathbb{Z}$) are all distinct. Thus, for fixed η of infinite order, only finitely many of the $\eta(\gamma_0)^{-n} - 1$, as n runs over $\mathbb{Z}$, can lie in $\mathfrak{Z}$, and the second assertion of Lemma 4.7 follows. □

The following two examples illustrate what differences occur between the commutative and the non-commutative theory, especially when one considers modules which lie outside the category $\mathfrak{M}_H(G)$ in the non-commutative case.

Example. Suppose now that G is commutative and has no element of order p, and let M be any finitely generated torsion $\Lambda(G)$-module. A slight generalization of a lemma of Greenberg [15] then shows that we can always find a closed subgroup H of G such that $\Gamma = G/H$ is isomorphic to $\mathbb{Z}_p$, and M belongs to the category $\mathfrak{M}_H(G)$. Thus, in this case, one can always find, by Lemma 4.7, continuous representations ρ of G such that $\chi(G, \mathrm{tw}_\rho(M))$ is finite. The following example shows that this last assertion is false, in general, when G is not commutative. Take $G = GL_3(\mathbb{Z}_p)$, and assume that $p \geq 5$ to ensure that G has no element of order p. Let

$$u = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad v = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad f = u - v.$$

Consider the module

$$M = \Lambda(G)/\Lambda(G)f.$$

We claim that, for every continuous representation ρ of G of the form (12), the Euler characteristic $\chi(G, \mathrm{tw}_\rho(M))$ is never finite. Indeed, a free resolution of $\mathrm{tw}_\rho(M)$ by $\Lambda_O(G)$-modules is given by

$$0 \to \mathrm{tw}_\rho(\Lambda(G)) \to \mathrm{tw}_\rho(\Lambda(G)) \to \mathrm{tw}_\rho(M) \to 0,$$

since, as was remarked earlier (see [33]), $\mathrm{tw}_\rho(\Lambda(G))$ is a free $\Lambda_O(G)$-module of rank n. Taking G-homology of this complex, it follows that $H_i(G, \mathrm{tw}_\rho(M)) = 0$ for $i \geq 2$, and that

$$H_1(G, \mathrm{tw}_\rho(M)) = \mathrm{Ker}\,(\rho(f)), \quad H_0(G, \mathrm{tw}_\rho(M)) = \mathrm{Coker}\,(\rho(f)).$$

But we now prove that 0 is an eigenvalue of $\rho(f)$ for every continuous ρ. We first note that for $a \in \mathbb{Z}_p$, we have a-th powers u^a and v^a defined as

$$u^a = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad v^a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}.$$

Taking a in $\mathbb{Z}_p^\times$, we define

$$\sigma_a = \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \tau_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and one verifies immediately that

$$\sigma_a u \sigma_a^{-1} = u^a, \quad \tau_a v \tau_a^{-1} = v^a.$$

Hence the eigenvalues of $\rho(u)$ and $\rho(v)$ in $\bar{\mathbb{Q}}_p$ must be stable under exponentiation by any a in $\mathbb{Z}_p^\times$. Since there are only finitely many of these eigenvalues, they must therefore all be p-power roots of unity. Moreover, $\rho(u)$ and $\rho(v)$ commute because $uv = vu$. Hence $\rho(u)$ and $\rho(v)$ must have a common eigenvector z, with respective eigenvalues α and β. Since α and β are both p-power roots of unity, we have either

$$\beta = \alpha^w \text{ or } \alpha = \beta^w \tag{89}$$

for some element w in $\mathbb{Z}$. Define

$$g = \begin{pmatrix} 1 & w-1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 & 0 \\ w-1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

One verifies that

$$g^{-1} u g = u, \quad g^{-1} v g = u^{1-w} v, \quad h^{-1} u h = u v^{1-w}, \quad h^{-1} v h = v. \tag{90}$$

If the first option of (89) holds, one uses the first two equations of (90) to verify that $\rho(g)z$ is an eigenvector of both $\rho(u)$ and $\rho(v)$ with the same eigenvalue α. Similarly, if the second option of (89) is true, one uses the second two equations of (90) to conclude that $\rho(h)z$ is an eigenvector for both $\rho(u)$ and $\rho(v)$ with the same eigenvalue. In either case, we see that 0 is an eigenvalue of $\rho(f)$, completing the proof that $\chi(G, \mathrm{tw}_\rho(M))$ is never finite.

Example. We give a second example to illustrate the differences between the commutative and non-commutative theory. Assume that G is p-valued in the sense of Lazard [17] (for example, provided $p > n+1$, every pro-p closed subgroup of $GL_n(\mathbb{Z}_p)$ is p-valued). Then it follows from [17] that both $\Lambda(G)$ and $\Omega(G) = \Lambda(G)/p\Lambda(G)$ have no zero divisors. We consider any $\Lambda(G)$-module of the form $M = \Lambda(G)/\Lambda(G)w$, where w is an element of $\Lambda(G)$, which is not a unit, and which does not belong to $p\Lambda(G)$. Since $\Omega(G)$ has no zero divisors, we see that M has no p-torsion. Moreover, it is easily seen that M is not pseudo-null as a $\Lambda(G)$-module in the sense of [33]. Further, in a similar manner to that of the previous example, we see that for every continuous representation ρ of G, we have $H_i(G, \mathrm{tw}_\rho(M)) = 0$ for $i \geq 2$, and

$$H_1(G, \mathrm{tw}_\rho(M)) = \mathrm{Ker}\,(\rho(w)), \quad H_0(G, \mathrm{tw}_\rho(M)) = \mathrm{Coker}\,(\rho(w)).$$

Suppose first that G is commutative. Thus G is isomorphic to $\mathbb{Z}_p^d$ for some integer $d \geq 1$, and $\Lambda(G)$ is isomorphic to the ring $\mathbb{Z}_p[[T_1, \cdots, T_d]]$ of formal power series in d variables

with coefficients in $\mathbb{Z}_p$. Identifying w with a formal power series $w(T_1, \cdots, T_d)$, and recalling that w is not a unit, and is not divisible by p, a well known argument with the Weierstrass preparation theorem shows that there always exist $\alpha_1, \cdots, \alpha_d$ in the maximal ideal of the ring of integers of $\bar{\mathbb{Q}}_p$ such that $w(\alpha_1, \cdots, \alpha_d) = 0$. Let O be the ring of integers of any finite extension of $\mathbb{Q}_p$ containing $\alpha_1, \cdots, \alpha_d$. We can define $\rho : G \to O^\times$ by specifying $\rho(\gamma_i) = \alpha_i + 1$ $(1 \leq i \leq d)$, where $\gamma_1, \cdots, \gamma_d$ denote the $\mathbb{Z}_p$-basis of G with $\gamma_i = T_i + 1$ $(1 \leq i \leq d)$. Clearly $\rho(w) = 0$, and thus $\mathrm{tw}_\rho(M)$ does not have finite G-Euler characteristic. On the other hand, take G to be kernel of the reduction map from $GL_3(\mathbb{Z}_p)$ to $\mathrm{GL}_3(\mathbb{F}_p)$, and assume that $p \geq 5$ to ensure that G is p-valued. Define

$$x = \begin{pmatrix} 1 & 0 & p \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad w = x - 1 - p.$$

An entirely analogous argument to that given for u and v in the previous example shows that, for every continuous representation ρ of G, the eigenvalues of $\rho(x)$ in $\bar{\mathbb{Q}}_p$ are all p-power roots of unity. Thus the eigenvalues of $\rho(w)$ in $\bar{\mathbb{Q}}_p$ are never zero, and so it follows that $\chi(G, \mathrm{tw}_\rho(M))$ is finite for every continuous representation ρ of G.

We end this section by making some conjectures about the integrality properties of characteristic elements of modules in the category $\mathfrak{M}_H(G)$. For brevity, let us write

$$R_1 = \Lambda(G), \quad R_2 = \Lambda(G)[\frac{1}{p}], \quad R_3 = \Lambda(G)_{S^*}. \tag{91}$$

Since S^* consists of non-zero divisors in $\Lambda(G)$, we have natural inclusions $R_1 \subset R_2 \subset R_3$. We also write

$$A_1 = \Lambda_O(\Gamma), \quad A_2 = \Lambda_O(\Gamma)[\frac{1}{p}]. \tag{92}$$

It is also convenient to give a name α to the canonical map

$$\alpha : R_3^\times \to K_1(R_3), \tag{93}$$

which we know is surjective by Theorem 4.4. Finally, we write $\mathfrak{R}(G)$ for the set of all continuous representations ρ of G of the form (11), where O is allowed to run over the rings of integers of all finite extensions of $\mathbb{Q}_p$, and $\mathfrak{A}(G)$ for the subset of $\mathfrak{R}(G)$ consisting of the Artin representations. In the next conjecture, the statements for all ρ in $\mathfrak{R}(G)$, and for all ρ in $\mathfrak{A}(G)$ will just be abbreviated to the respective assertions for all ρ, and for all Artin ρ.

Conjecture 4.8. *Assume that G has no element of order p. In each of the following four cases, the assertions* (a), (b), (c) *and* (d) *are equivalent for any element ξ of $K_1(R_3)$:-*

Case 1. (a) $\xi \in \alpha(R_2 \cap R_3^\times)$; (b) $\xi(\rho) \neq \infty$ *for all* ρ; (c) $\Phi'_\rho(\xi) \in A_2$ *for all* ρ; (d) $\Phi'_\rho(\xi) \in A_2$ *for all Artin* ρ.

Case 2. (a) $\xi \in \alpha(R_1 \cap R_3^\times)$; (b) $\xi(\rho)$ *is finite and in O for all* ρ; (c) $\Phi'_\rho(\xi) \in A_1$ *for all* ρ; (d) $\Phi'_\rho(\xi) \in A_1$ *for all Artin* ρ.

Case 3. (a) $\xi \in \alpha(R_2^\times)$; (b) $\xi(\rho) \neq 0, \infty$ *for all* ρ; (c) $\Phi'_\rho(\xi) \in A_2^\times$ *for all* ρ; (d) $\Phi'_\rho(\xi) \in A_2^\times$ *for all Artin* ρ.

Case 4. (a) $\xi \in \alpha(R_1^\times)$; (b) $\xi(\rho)$ *is finite and in* $O^\times$ *for all* ρ; (c) $\Phi'_\rho(\xi) \in A_1^\times$ *for all* ρ; (d) $\Phi'_\rho(\xi) \in A_1^\times$ *for all Artin* ρ.

We remark that Case 1 of Conjecture 4.8 has an interesting consequence for the modules M in $\mathfrak{M}_H(G)$ which, in addition, satisfy condition (51). Let M be any such module, and let ξ_M be a characteristic element of M. It follows from (52) and (57) that $\Phi'_\rho(\xi_M)$ belongs to A_2 for all ρ in $\mathfrak{A}(G)$. Hence, if Conjecture 4.8 is valid, the assertions (a), (b), and (c) of Case 1 would be true for ξ_M, and, in particular, we would have $\xi_M \in \alpha(R_2 \cap R_3^\times)$. But we have to confess that at present we are unable to prove (a), (b), and (c) of Case 1 for the characteristic elements of such modules M.

Lemma 4.9. *In each of the four cases of Conjecture* 4.8, (a) *implies* (b), (b) *and* (c) *are equivalent, and* (c) *implies* (d).

Proof. Plainly (c) implies (d), and it is also clear that (c) implies (b) since, by definition, $\xi(\rho)$ is the image of $\Phi'_\rho(\xi)$ under the augmentation map once $\Phi'_\rho(\xi)$ belongs to the localization of A_1 at the kernel of the augmentation map. The implication (a) implies (b) holds because if g is any element of $R_2^\times$ of the form $g = p^{-m}f$ with f in R_1 and m an integer ≥ 0, then, putting $\xi = \alpha(g)$, $\xi(\rho) = p^{-mn} \det \rho(f)$ for every ρ in $\mathfrak{R}(G)$. To prove that (b) implies (c), we make use of the following general remark. Recall that we have identified A_1 with $O[[T]]$ by mapping a fixed topological generator γ_0 of Γ to $1+T$. Let $\eta : \Gamma \to O^\times$ be any continuous homomorphism. Then we claim that, for all ξ in $K_1(R_3)$ and all ρ in $\mathfrak{R}(G)$, we have the identity

$$\Phi'_{\rho\eta}(\xi) = \Phi'_\rho(\xi)(\eta(\gamma)^{-1}(1+T) - 1), \tag{94}$$

where both sides of this equation are viewed as elements of the quotient field of $O[[T]]$. To establish (94), we note that $K_1(R_3)$ is generated as an abelian group by those ξ which are characteristic elements of modules M in $\mathfrak{M}_H(G)$, and, for such ξ, (94) follows from (87) and Lemma 3.7. We now use (94) to show that (b) implies (c) in Case 1. Suppose that, for some ρ in $\mathfrak{R}(G)$, we have $\Phi'_\rho(\xi) = f(T)/g(T)$, where $f(T)$ and $g(T)$ are relatively prime elements of $O[[T]]$, and $g(T)$ is not a power of the local parameter π of O. Thus $g(T)$ must have a zero $T = \alpha$ in the maximal ideal of the ring of integers of $\bar{\mathbb{Q}}_p$. Enlarging O if necessary, we can assume that α belongs to O, and define a continuous homomorphism $\eta : \Gamma \to O^\times$ by $\eta(\gamma_0) = (1+\alpha)^{-1}$. It is then clear from (94) that $\xi(\eta\rho) = \infty$, contradicting our assumption that (b) is valid. Similar arguments prove that (b) implies (c) in the remaining three cases of Conjecture 4.8, and the proof of Lemma 4.9 is complete. □

The strongest evidence we have for Conjecture 4.8 is that it is true when G is of the form $\mathbb{Z}_p^d \times \Delta$, where d is any integer ≥ 1 and Δ is a finite group of order prime to p. However, we omit the detailed proof in this case.

5 The main conjecture.

For brevity, we only discuss here the main conjecture for elliptic curves over $\mathbb{Q}$ over the field generated by the coordinates of all p-power division points on the curve, where p is a prime ≥ 5 of good ordinary reduction. However, it will be clear that a similar conjecture can be formulated in great generality for motives over p-adic Lie extensions of number fields which contain the cyclotomic $\mathbb{Z}_p$-extension of the base field.

If F is a finite extension of $\mathbb{Q}$, we write F^{cyc} for the cyclotomic $\mathbb{Z}_p$-extension of F, and put $\Gamma_F = G(F^{\mathrm{cyc}}/F)$. Let E be an elliptic curve defined over $\mathbb{Q}$, and E_{p^∞} the group of all p-power division points on E. We define

$$F_\infty = \mathbb{Q}(E_{p^\infty}). \tag{95}$$

By the Weil pairing, $F_\infty \supset \mathbb{Q}(\mu_{p^\infty})$, where μ_{p^∞} denotes the group of all p-power roots of unity. Hence F_∞ contains $\mathbb{Q}^{\mathrm{cyc}}$, and we define

$$G = G(F_\infty/\mathbb{Q}), \quad H = G(F_\infty/\mathbb{Q}^{\mathrm{cyc}}), \quad \Gamma = G(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}). \tag{96}$$

Thus G is a compact p-adic Lie group to which the abstract theory developed in the first four sections of this paper applies. In fact, the structure of G is well known. Indeed, G can be identified with a closed subgroup of $GL_2(\mathbb{Z}_p) = \mathrm{Aut}\,(E_{p^\infty})$. When E admits complex multiplication, G has dimension 2, and when E does not admit complex multiplication, G has dimension 4 [25].

If L is any algebraic extension of $\mathbb{Q}$, we recall that the classical Selmer group $\mathcal{S}(E/L)$ is defined by

$$\mathcal{S}(E/L) = \mathrm{Ker}\,(H^1(L, E_{p^\infty}) \to \prod_w (H^1(L_w, E(\bar{L}_w))),$$

where w runs over all non-archimedean places of L, and L_w denotes the union of the completions at w of all finite extensions of $\mathbb{Q}$ contained in L. We write

$$X(E/L) = \mathrm{Hom}\,(\mathcal{S}(E/L), \mathbb{Q}_p/\mathbb{Z}_p)$$

for the compact Pontrjagin dual of the discrete abelian group $\mathcal{S}(E/L)$. We shall mainly be interested in the case in which L is Galois over F, in which case both $\mathcal{S}(E/L)$ and $X(E/L)$ have a natural left action of $G(L/F)$, which extends to a left action of the whole Iwasawa algebra $\Lambda(G(L/F))$. It is easy to see that $X(E/L)$ is always a finitely generated $\Lambda(G(L/F))$-module.

We impose for the rest of the paper the following

Hypotheses on p. $p \geq 5$ and E has good ordinary reduction at p.

The condition $p \geq 5$ guarantees that G has no element of order p, since G is a closed subgroup of $GL_2(\mathbb{Z}_p)$. It is a basic question as to when, assuming our hypotheses on p, the dual Selmer group $X(E/F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$, or equivalently is S^*-torsion, where S^* is the Ore set defined in §3.

Conjecture 5.1. *Assuming our hypotheses on p, $X(E/F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$.*

We now briefly discuss what is known at present about Conjecture 5.1. Indeed, all we know is related to the following much older conjecture of Mazur [18].

Conjecture 5.2. *Assume E has good ordinary reduction at p. For each finite extension F of $\mathbb{Q}$, $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma_F)$-torsion.*

One might hope that Conjecture 5.1 is equivalent to knowing Conjecture 5.2 for all finite extensions F of $\mathbb{Q}$ contained in F_∞. At present, we can only prove some partial results in this direction, which we now describe. If F is a finite extension of $\mathbb{Q}$ contained in F_∞, we put

$$G_F = G(F_\infty/F), \quad H_F = G(F_\infty/F^{\mathrm{cyc}}). \tag{98}$$

Let X be a finitely generated $\Lambda(G)$-module. If L is a finite extension of $\mathbb{Q}$ in F_∞ such that G_L is pro-p, the μ-invariant of X viewed as a $\Lambda(G_L)$-module, is defined in [16] and [31]. Similarly, if Z is any finitely generated $\Lambda(\Gamma_F)$-module, we write $\mu_{\Gamma_F}(Z)$ for its classical μ-invariant. Also, for any field K in F_∞, we define

$$Y(E/K) = X(E/K)/X(E/K)(p). \tag{99}$$

Lemma 5.3. *Assume that $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$. Then, for each finite extension F of $\mathbb{Q}$ contained in F_∞, we have* (i) *$X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma_F)$-torsion*; (ii) *$H_i(H_F, X(E/F_\infty)) = 0$ for all $i \geq 1$*; (iii) *$H_i(H_F, Y(E/F_\infty))$ is finite for $i = 1, 2$, and zero for $i > 2$. Moreover, we have $\mu_{G_L}(X(E/F_\infty)) = \mu_\Gamma(X(E/L^{\mathrm{cyc}}))$ for each finite extension L of $\mathbb{Q}$ in F_∞ such that G_L is pro-p.*

Proof. We assume that $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$, so that $Y(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module. Take F to be any finite extension of $\mathbb{Q}$ contained in F_∞. Then $Y(E/F_\infty)_{H_F}$ is clearly a finitely generated $\mathbb{Z}_p$-module, because $Y(E/F_\infty)$ is then a finitely generated $\Lambda(H_F)$-module. Now we have the commutative diagram with exact rows

$$\begin{array}{ccccc} X(E/F_\infty)_{H_F} & \longrightarrow & Y(E/F_\infty)_{H_F} & \longrightarrow & 0 \\ \downarrow{\scriptstyle r_F} & & \downarrow{\scriptstyle s_F} & & \\ X(E/F^{\mathrm{cyc}}) & \longrightarrow & Y(E/F^{\mathrm{cyc}}) & \longrightarrow & 0, \end{array}$$

where r_F is the dual of the restriction map t_F from $\mathcal{S}(E/F^{\mathrm{cyc}})$ to $\mathcal{S}(E/F_\infty)^{H_F}$, and s_F is the corresponding induced map. We claim that the cokernel of r_F is finite. Indeed, the cokernel of r_F is dual to the kernel of the restriction map t_F, and $\mathrm{Ker}\,(t_F)$ is contained in $H^1(H_F, E_{p^\infty})$. But this latter group is proven to be finite in [8]. Since $\mathrm{Coker}\,(r_F)$ is finite, it follows that $\mathrm{Coker}\,(s_F)$ is also finite. As was remarked above, $Y(E/F_\infty)_{H_F}$ is a finitely generated $\mathbb{Z}_p$-module, and so we see that $Y(E/F^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module. Thus $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma_F)$-torsion, proving (i). To prove the remainder of Lemma 5.3, we invoke the arguments of [6], and do not repeat the detailed proofs of these here. Since $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma_F)$-torsion, Lemma 2.5 of [6] shows that $H_1(H_F, X(E/F_\infty)) = 0$. As we have shown $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma_F)$-torsion for all F, Lemma 2.1 and Remark 2.6 of [6] prove that $H_i(H_F, X(E/F_\infty)) = 0$ for all $i \geq 2$, establishing (ii). Turning to (iii), an entirely similar argument to that given in the proof of Proposition 2.13 of [6] gives that

$H_3(H_F, Y(E/F_\infty)) = 0$, and that $H_i(H_F, Y(E/F_\infty))$ $(i = 1, 2)$ are killed by a power of p. Hence, as the $H_i(H_F, Y(E/F_\infty))$ $(i \geq 0)$ are finitely generated $\mathbb{Z}_p$-modules, we conclude that $H_i(H_F, Y(E/F_\infty))$ must be finite for $i = 1, 2$. The final assertion of Lemma 5.3 now follows from formula (25) of Proposition 2.13 of [6], on noting that the μ-invariant of the $\Lambda(\Gamma_L)$-module $H_0(H_L, Y(E/F_\infty))$ is zero, because this module is finitely generated over $\mathbb{Z}_p$. This completes the proof of Lemma 5.3. □

Lemma 5.4. *Assume that $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma_F)$-torsion for all finite extensions F of $\mathbb{Q}$ in F_∞. Suppose, in addition, that there exists a finite extension L of $\mathbb{Q}$ contained in F_∞ satisfying: – (i) G_L is pro-p, (ii) $\mu_{G_L}(X(E/F_\infty)) = \mu_{\Gamma_L}(X(E/L^{\mathrm{cyc}}))$, and (iii) $H_1(H_L, Y(E/F_\infty))$ is finite. Then $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$.*

Proof. We first observe that $H_0(H_L, Y(E/F_\infty))$ is a finitely generated torsion $\Lambda(\Gamma_L)$-module, assuming the hypotheses of the lemma. Indeed, $H_0(H_L, Y(E/F_\infty))$ is a quotient of $H_0(H_L, X(E/F_\infty))$, and we claim that this latter module is a finitely generated torsion $\Lambda(\Gamma_L)$-module. This is because we are assuming that the finitely $\Lambda(\Gamma_L)$-module $X(E/L^{\mathrm{cyc}})$ is $\Lambda(\Gamma_L)$-torsion, and it is shown in [5] that the kernel of the natural map

$$r_L : X(E/F_\infty)_{H_L} \to X(E/L^{\mathrm{cyc}}),$$

which is the dual of the restriction map, is a finitely generated $\mathbb{Z}_p$-modules. Hence $\mathrm{Ker}\,(r_L)$ is a finitely generated torsion $\Lambda(\Gamma_L)$-module, and our claim follows. The delicate part of the proof is to now show that

$$\mu_{\Gamma_L}(H_0(H_L, Y(E/F_\infty))) = 0. \tag{100}$$

Indeed, (100) implies immediately that $Y(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module, completing the proof of the lemma. This is because (100) shows that $H_0(H_L, Y(E/F_\infty))$ is a finitely generated $\mathbb{Z}_p$-module, and hence, as H_L is pro-p, Nakayama's lemma gives that $Y(E/F_\infty)$ is finitely generated over $\Lambda(H_L)$. To prove (100), we invoke the full force of Proposition 2.13 of [6]. As remarked earlier, our assumption that $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma_F)$-torsion for all finite extensions F of $\mathbb{Q}$ in F_∞ implies that all the hypotheses of Proposition 2.13 of [6] are valid. Hence formula (25) of Proposition 2.13 of [6] holds. Inserting conditions (ii) and (iii) in formula (25) of [6], we conclude that the μ_{Γ_L}-invariants of $H_0(H_L, Y(E/F_\infty))$ and $H_2(H_L, Y(E/F_\infty))$ must add up to zero. Thus, as both are non-negative integers, both of these μ-invariants must be zero, proving (100) in particular. □

Corollary 5.5. *Assume that $p \geq 5$, E has good ordinary reduction at p, and E admits complex multiplication. Then $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$ if and only if there exists a finite extension L of $\mathbb{Q}$ in F_∞ such that G_L is pro-p and $\mu_{\Gamma_L}(X(E/L^{\mathrm{cyc}})) = 0$.*

Proof. It is a well known consequence of the proof of the two variable main conjecture for E over F_∞ (see [22]) that $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma_F)$-torsion for every finite extension F of $\mathbb{Q}$ in F_∞. Take L to be any finite extension of $\mathbb{Q}$ contained in F_∞ such that G_L is pro-p. Then it is well known that the thesis of Schneps [23] implies that $\mu_{G_L}(X(E/F_\infty)) = 0$. This in turn implies that $X(E/F_\infty)(p) = 0$ because $X(E/F_\infty)$ has no non-zero $\Lambda(G_L)$-pseudo-null submodule by [21]. We then have $H_i(H_L, Y(E/F_\infty)) = 0$ for all $i \geq 1$ because $Y(E/F_\infty) = X(E/F_\infty)$. The assertion of the corollary is now clear from Lemmas 5.3 and 5.4. □

The following is the one practical criterion we know at present for proving in some concrete examples that $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$.

Proposition 5.6. *Assume that there exists a finite extension L of $\mathbb{Q}$ contained in F_∞, and an elliptic curve E' defined over L, as follows*: – (i) *G_L is pro-p,* (ii) *E' is isogenous to E over L, and* (iii) *$X(E'/L^{\mathrm{cyc}})$ is finitely generated $\mathbb{Z}_p$-module. Then $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$.*

It is very probable that the hypotheses of Proposition 5.6 are valid for most elliptic curves E over $\mathbb{Q}$ and most primes p of good ordinary reduction. However, in our present state of knowledge, condition (iii) is difficult to verify in numerical examples. Here is an example of one isogeny class of curves to which it can be applied.

Example. Consider the three elliptic curves over $\mathbb{Q}$ of conductor 11, which we denote by E_i $(i = 0, 1, 2)$. Here E_1 is given by (70), and the other two are given by the equations

$$E_0 : y^2 + y = x^3 - x^2 - 10x - 20$$

$$E_2 : y^2 + y = x^3 - x^2 - 7820x - 263580$$

All three curves are isogenous over $\mathbb{Q}$, and so the field F_∞ is the same for the three curves and all primes p. Taking $p = 5$, and $L = \mathbb{Q}(\mu_5)$, it is well known [22] that G_L is pro-5 and $X(E_1/L^{\mathrm{cyc}}) = 0$. Hence Proposition 5.6 shows that $X(E_i/F_\infty)$ belongs to $\mathfrak{M}_H(G)$ for $p = 5$ and $i = 0, 1, 2$. At present, we do not know how to prove that $X(E_i/F_\infty)$ belongs to $\mathfrak{M}_H(G)$ for any good ordinary prime $p > 5$.

We now prove Proposition 5.6. Pick an isogeny $f : E' \to E$, which is defined over L. Note that $F_\infty = L(E'_{p^\infty})$. The natural homomorphism

$$r_L : X(E'/F_\infty)_{H_L} \to X(E'/L^{\mathrm{cyc}}),$$

which is the dual of the restriction map, has a kernel which is a finitely generated $\mathbb{Z}_p$-module (see [5]). Applying Nakayama's lemma, we deduce from (i) and (iii) that $X(E'/F_\infty)$ is finitely generated over $\Lambda(H_L)$. On the other hand, it is easily seen that our isogeny f induces a $\Lambda(G_L)$-homomorphism from $X(E/F_\infty)$ to $X(E'/F_\infty)$, whose kernel is killed by a power of p. Thus $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$, and the proof of Proposition 5.6 is complete. □

We end this paper by conjecturing the existence of a p-adic L-function attached to E over F_∞, and formulating a main conjecture which relates this p-adic L-function to $X(E/F_\infty)$. We refer the reader to [14] for motivation for the definition we have chosen for our p-adic L-function. If q is any prime number, we write Frob_q for the Frobenius automorphism of q in $\mathrm{Gal}(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)/I_q$, where, as usual, I_q denotes the inertia subgroup. To fix the definition of our local and global ε-factors, we follow the conventions and normalizations of [10]. In particular, we choose the sign of the local reciprocity map so that q is mapped to Frob_q^{-1}. We take the Haar measure on the adèle group of $\mathbb{Q}$ which is the usual Haar measure on $\mathbb{R}$, and, for each prime number q, gives $\mathbb{Z}_q$ volume 1. We

also fix the unique complex character of the adèle group of $\mathbb{Q}$ whose infinite component is $x \mapsto \exp(2\pi i x)$, and whose component at a finite prime q is $x \mapsto \exp(-2\pi i x)$. Now let ρ denote any Artin representation of G. In our earlier p-adic theory, we viewed ρ as being realized over the ring of integers of some finite extension of $\mathbb{Q}_p$. However, since ρ is an Artin representation of G, finite group theory tells us that there exists a finite extension of $\mathbb{Q}$, which we denote by K_ρ, such that ρ can be realized in a finite dimensional vector space V_ρ over K_ρ. We first recall the definition of the complex Artin L-function $L(\rho, s)$. It is given by the Euler product

$$L(\rho, s) = \prod_q P_q(\rho, q^{-s})^{-1},$$

where $P_q(\rho, T)$ is the polynomial

$$P_q(\rho, T) = \det(1 - \mathrm{Frob}_q^{-1}.T | V_\rho^{I_q}).$$

For each prime number q, we write $e_q(\rho)$ for the local ε-factor of ρ at q, normalized as in [10].

The complex L-function which is obtained by twisting E by the Artin representation ρ is defined as follows. For each prime number l, let

$$T_l(E) = \varprojlim E_{l^n}, \quad V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l, \quad H_l^1(E) = \mathrm{Hom}\,(V_l(E), \mathbb{Q}_l). \tag{101}$$

Moreover, we fix some prime λ of K_ρ above l, and put $V_{\rho,\lambda} = V_\rho \otimes_K K_{\rho,\lambda}$. Then

$$L(E, \rho, s) = \prod_q P_q(E, \rho, q^{-s})^{-1}, \tag{102}$$

where $P_q(E, \rho, T)$ is the polynomial

$$P_q(E, \rho, T) = \det(1 - \mathrm{Frob}_q^{-1}.T | (H_l^1(E) \otimes_{\mathbb{Q}_l} V_{\rho,\lambda})^{I_q});$$

here l is any prime number different from q. The Euler product $L(E, \rho, s)$ converges only for $\Re(s) > 3/2$, and the only thing known about its analytic continuation at present is that it has a meromorphic continuation when ρ factors through a soluble extension of $\mathbb{Q}$. We will assume the analytic continuation of $L(E, \rho, s)$ to $s = 1$ for all Artin characters ρ of G in what follows. The point $s = 1$ is critical for $L(E, \rho, s)$ for all Artin ρ, in the sense of [11] and the period conjecture of [11] asserts the following in this case. Fix a global minimal Weierstrass equation for E over $\mathbb{Z}$, and let ω denote the Néron differential of this equation. Let γ^+ (resp. γ^-) denote a generator for the subspace of $H_1(E(\mathbb{C}), \mathbb{Z})$ fixed by complex conjugation (resp. the subspace on which complex conjugation acts by -1). We define

$$\Omega_+(E) = \int_{\gamma^+} \omega, \quad \Omega_-(E) = \int_{\gamma^-} \omega.$$

Moreover, let $d^+(\rho)$ denote the dimension of the subspace of V_ρ on which complex conjugation acts by +1, and $d^-(\rho)$ the dimension of the subspace on which complex conjugation acts by -1. According to the period conjecture of [11], we have

$$\frac{L(E,\rho,1)}{\Omega_+(E)^{d^+(\rho)}\Omega_-(E)^{d^-(\rho)}} \in \bar{\mathbb{Q}} \tag{103}$$

for all Artin representation ρ of G. We shall assume (103) to define our conjectural p-adic L-function. We also tacitly suppose we have fixed embeddings of $\bar{\mathbb{Q}}$ into both $\mathbb{C}$ and $\bar{\mathbb{Q}}_p$.

Let j_E denote the j-invariant of E, and let R denote the set consisting of the prime p and all prime numbers q with $\mathrm{ord}_q(j_E) < 0$. We define

$$L_R(E,\rho,s) = \prod_{q \notin R} P_q(E,\rho,q^{-s})^{-1}. \tag{104}$$

Finally, we put

$$p^{f_\rho} = p\text{-part of the conductor of } \rho. \tag{105}$$

Also, since E is ordinary at p, we have

$$1 - a_p X + pX^2 = (1-uX)(1-wX), \quad u \in \mathbb{Z}_p^\times; \tag{106}$$

here, as usual, $p + 1 - a_p = \sharp(\tilde{E}_p(\mathbb{F}_p))$, where $\tilde{E}_p$ denotes the reduction of E modulo p. We recall that $\hat{\rho}$ denotes the contragredient representation of ρ.

Conjecture 5.7. *Assume that $p \geq 5$ and that E has good ordinary reduction at p. Then there exists $\mathcal{L}_E$ in $K_1(\Lambda(G)_{S^*})$ such that, for all Artin representations ρ of G, we have $\mathcal{L}_E(\rho) \neq \infty$, and*

$$\mathcal{L}_E(\rho) = \frac{L_R(E,\rho,1)}{\Omega_+(E)^{d^+(\rho)}\Omega_-(E)^{d^-(\rho)}} \cdot e_p(\rho) \cdot \frac{P_p(\hat{\rho},u^{-1})}{P_p(\rho,w^{-1})} \cdot u^{-f_\rho}; \tag{107}$$

here $e_p(\rho)$ denotes the local ε-factors at p attached to ρ.

We remark that, when E admits complex multiplication, Conjecture 5.7 is true, and can be deduced from the existence of the two variable p-adic L-function of Manin-Vishik, Katz, and Yager attached to E at the ordinary prime p. When E does not admit complex multiplication, the only evidence we have at present to support Conjecture 5.7 is some interesting but still fragmentary numerical data due to Balister [2] (unpublished) and T.Dokchitser-V.Dokchitser [12].

Conjecture 5.8 (The main conjecture). *Assume that $p \geq 5$, E has good ordinary reduction at p, and $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$. Granted Conjecture 5.7, the p-adic L-function $\mathcal{L}_E$ in $K_1(\Lambda(G)_{S^*})$ is a characteristic element of $X(E/F_\infty)$.*

It is plain that such a main conjecture will have many deep consequences for the arithmetic of E over F_∞ and its subfields. We do not enter into a discussion of these here, beyond mentioning the following almost immediate corollaries.

Corollary 5.9. *Assume Conjecture 5.8. Then, for each Artin representation ρ of G, $\chi(G, \mathrm{tw}_\rho(X(E/F_\infty)))$ is finite if and only if $L(E,\hat{\rho},1) \neq 0$.*

Corollary 5.10. *Assume Conjecture* 5.8. *Let ρ be an Artin representation of G such that $L(E,\hat{\rho},1)\neq 0$. As in Theorem* 3.6*, let m_ρ be the degree of the quotient field of O over $\mathbb{Q}_p$, where ρ is given by* (12)*. Then $\chi(G,\mathrm{tw}_{\hat{\rho}}(M))$ is equal to the m_ρ-th power of the inverse of the p-adic valuation of the right hand side of* (107)*.*

We make the following remark about the integrality properties of $\mathcal{L}_E$ and any characteristic element ξ_E of $X(E/F_\infty)$. On the one hand, the conjectured holomorphy of $L(E,\rho,s)$ at $s=1$ gives, via Conjecture 5.7, the assertion that $\mathcal{L}_E(\rho)\neq\infty$ for every Artin representation ρ of G. On the other hand, thanks to Lemma 5.3 and Theorem 3.8, the conjecture that $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$ implies that $\xi_E(\rho)\neq\infty$ for every Artin representation ρ of G. Note that Case 1 of Conjecture 4.8 would then imply that both $\mathcal{L}_E$ and ξ_E belong to the image of the natural map

$$\Lambda(G)[\frac{1}{p}]^\times\cap\Lambda(G)_{S^*}\hookrightarrow\Lambda(G)_{S^*}\to K_1(\Lambda(G)_{S^*}).$$

To prove Corollary 5.9, we observe that when $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$, Lemma 5.3 and Theorem 3.8 show that $\xi_E(\rho)\neq 0$ if and only if $\chi(G,\mathrm{tw}_{\hat{\rho}}(X(E/F_\infty)))$ is finite. If we assume Conjecture 5.8, we can take $\xi_E=\mathcal{L}_E$, and then it is clear from (107) that $\mathcal{L}_E(\rho)\neq 0$ if and only if $L(E,\rho,1)\neq 0$. Corollary 5.10 is then an immediate consequence of (107) and formula (36) of Theorem 3.6. □

Needless to say, the evidence in favour of Conjecture 5.8 is still very limited. When E admits complex multiplication, Conjecture 5.8 is true provided we assume that $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$ (see Corollary 5.5). Indeed it can be deduced from the proof by Yager [34] and Rubin [22] of what is usually called the two variable main conjecture (recall that in this case G is a p-adic Lie group of dimension 2). When E does not admit complex multiplication, the remarkable calculations of $L(E,\rho,1)$ made in [12] for certain Artin representations of small degree and small primes p provide some numerical evidence in favour of Conjecture 5.8. We end by giving their results for $E=X_1(11)$, $p=5$, and the two Artin representations ρ_1 and ρ_2 of degree 4 which are discussed at the end of §3.

Example. We use the same notation as at the end of §3. The following data is calculated in [12]. We have

$$d^+(\rho_i)=d^-(\rho_i)=2\quad(i=1,2)\tag{108}$$

$$f_{\rho_1}=3,\quad f_{\rho_2}=5\tag{109}$$

$$P_5(\rho_1,X)=1-X,\quad P_5(\rho_2,X)=1\tag{110}$$

$$P_5(E,\rho_1,X)=1-X+5X^2,\quad P_5(E,\rho_2,X)=1\tag{111}$$

$$P_{11}(E,\rho_1,X)=1,\quad P_{11}(E,\rho_2,X)=1\tag{112}$$

$$|e_5(\rho_1)|_5 = 5^{-3/2}, \quad |e_5(\rho_2)|_5 = 5^{-5/2} \tag{113}$$

Moreover, $\sharp(\tilde{E}(\mathbb{F}_5)) = 5$, and so

$$1 - a_5 X + 5X^2 = 1 - X + 5X^2 \tag{114}$$

Finally, even though $P_q(E, \rho_i, X)$ $(i = 1, 2)$ has degree 8 for all $q \neq 5, 11$, the remarkable calculations of [12] show that

$$\frac{L(E, \rho_1, 1)}{(\Omega_+(E)\Omega_-(E))^2} = \frac{-2^2}{11^2\sqrt{5}}, \quad \frac{L(E, \rho_2, 1)}{(\Omega_+(E)\Omega_-(E))^2} = \frac{-2^6}{11^2 5\sqrt{5}}. \tag{115}$$

Thus, since both of these L-values are non-zero, Proposition 3.11 shows that Corollary 5.9 holds for ρ_1 and ρ_2. Finally, one can use the above data to calculate the right hand side of (107), up to a 5-adic unit, for ρ_1 and ρ_2. Using (74) of Proposition 3.11, and recalling that ρ_1 and ρ_2 can both be realized over $\mathbb{Z}_5$, we deduce that Corollary 5.10 is also valid for ρ_1 and ρ_2.

References

[1] Bass, H., *Algebraic K-theory*, Benjamin, New York (1968).

[2] Balister, P., *Congruences between special values of L-functions* (unpublished).

[3] Bourbaki, N., *Commutative Algebra*, Hermann, Paris (1965).

[4] Brumer, A., *Pseudocompact algebras, profinite groups and class formations*, J. of Algebra **4** (1966) 442-470.

[5] Coates, J., and Howson, S., *Euler characteristics and elliptic curves* II, J. Math. Soc. Japan Proc. **53** (2001) 175–235.

[6] Coates, J., Schneider, P., and Sujatha, R., *Links between cyclotomic and GL_2 Iwasawa theory*, Doc. Math. Extra Volume : Kazuya Kato's 50th birthday (2003) 187–215.

[7] Coates, J., Schneider, P., and Sujatha, R., *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2** (2003) no. 1, 73–108.

[8] Coates, J., and Sujatha, R., *Euler-Poincaré characteristics of abelian varieties*, CRAS **329** Série I (1999) 309–313.

[9] Coates, J., and Sujatha, R., *Galois cohomology of elliptic curves*, TIFR Lecture notes series, Narosa Publishing House (2000).

[10] Deligne, P., *Les constantes des équations fonctionnelles des fonctions L*, Modular functions of one variable II LNM **349** Springer (1973) 501–597.

[11] Deligne, P., *Valeurs de fonctions L et périodes d'intégrales*, Proc. Sympos. Pure Math., XXXIII Automorphic forms, representations and L-functions, Part 2 Amer. Math. Soc. (1979) 313–346.

[12] Dokchitser, T., and Dokchitser V., Paper in preparation.

[13] Fisher, T., *Descent calculations for the elliptic curves of conductor* 11, Proc. London Math. Soc. **86** (2003) 583–606.

[14] Fukaya, T., and Kato, K., *A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory*, preprint (2003).

[15] Greenberg, R., *On the structure of certain Galois groups*, Invent. Math. **47** (1978) 85–99.

[16] Howson, S., *Euler characteristics as invariants of Iwasawa modules*, Proc. London Math. Soc. **85** (2002) 634–658.

[17] Lazard, M., *Groupes analytiques p-adiques*, Publ. Math. IHES **26** (1965) 389–603.

[18] Mazur, B., *Rational points of abelian varieties in towers of number fields*, Invent. Math. **18** (1972) 183–266.

[19] McConnell, J. C., and Robson, J. C., *Noncommutative Noetherian Rings*, Graduate Studies in Math. **30** AMS (1987).

[20] Neukirch, J., Schmidt, A., and Wingberg, K., *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften **323** Springer (2000).

[21] Perrin-Riou, B., *Groupes de Selmer d'une courbe elliptique à multiplication complexe*, Comp. Math. **43** (1981) 387–417.

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

[23] Schneps, L., *On the μ-invariant of p-adic L-functions*, J. Number Theory **25** (1987) 20-33.

[24] Serre, J.-P., *Sur la dimension cohomologique de groupes profinis*, Topology **3** (1965) 413–420, Oeuvres II 264-271.

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

[26] Serre, J.-P., *Algébre Locale, Multipicités*, 3rd ed. LNM **11** Springer (1975).

[27] Serre, J.-P., *Linear representations of finite groups*, Graduate Texts in Mathematics **42** Springer (1977).

[28] Swan, R., *Algebraic K-theory*, LNM **76** Springer (1968).

[29] Vaserstein, L. N., *On stabilization for general linear groups over a ring*, Math. USSR Sbornik **8** (1969) 383-400.

[30] Vaserstein, L. N., *On the Whitehead Determinant for Semi-local Rings*, Preprint (2004).

[31] Venjakob, O., *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. European Math. Soc. **4** (2002) 271–311.

[32] Venjakob, O. (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.

[33] Venjakob, O., *Characteristic elements in non-commutative Iwasawa theory*, Habilitationschschrift, Heidelberg University (2003).

[34] Yager, R.I., *On two variable p-adic L-functions*, Ann. of Math. **115** (1982) 411–449.

John Coates
DPMMS,
University of Cambridge,
Centre for Mathematical Sciences,
Wilberforce Road,
Cambridge CB3 0WB, England
J.H.Coates@dpmms.cam.ac.uk

Takako Fukaya
Faculty of Business and Commerce,
Keio University,
Hiyoshi, Kohoku-ku,
Yokohama, 223-8521, Japan
takakof@hc.cc.keio.ac.jp

Kazuya Kato
Department of Mathematics,
Kyoto University,
Kitashirakawa,
Kyoto 606-8502, Japan
kazuya@math.kyoto-u.ac.jp

Ramdorai Sujatha
School of Mathematics,
Tata Institute of Fundamental Research,
Homi Bhabha Road,
Mumbai 400 005, India
sujatha@math.tifr.res.in

Otmar Venjakob
Universität Heidelberg,
Mathematisches Institut,
Im Neuenheimer Feld 288,
D-69120 Heidelberg, Germany
otmar@mathi.uni-heidelberg.de