Congruences for critical values of higher derivatives of twisted Hasse-Weil L-functions

Werner Bley and Daniel Macias Castillo

June 11, 2013

Abstract

Let A be an abelian variety over a number field k and F a finite cyclic extension of k of p-power degree for an odd prime p. Under certain technical hypotheses, we obtain a reinterpretation of the equivariant Tamagawa number conjecture ('eTNC') for A, F/k and p in terms of explicit p-adic congruences involving values of derivatives of the Hasse-Weil L-functions of twists of A, normalised by completely explicit twisted regulators. This reinterpretation makes the eTNC amenable to numerical verification and furthermore leads to explicit predictions which refine well-known conjectures of Mazur and Tate.

1 Introduction

Let A be an abelian variety of dimension d defined over a number field k. We write A^t for the dual abelian variety. Let F/k be a finite Galois extension with group $G := \mathrm{Gal}(F/k)$. We let A_F denote the base change of A and consider the motive $M_F := h^1(A_F)(1)$ as a motive over k with a natural action of the semi-simple $\mathbb{Q}$-algebra $\mathbb{Q}[G]$.

We will study the equivariant Tamagawa number conjecture as formulated by Burns and Flach in [9] for the pair $(M_F, \mathbb{Z}[G])$. This conjecture asserts the validity of an equality in the relative algebraic K-group $K_0(\mathbb{Z}[G], \mathbb{R}[G])$. If p is a prime, we refer to the image of this equality in $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$ as the 'eTNC$_p$ for $(M_F, \mathbb{Z}[G])$'. If p does not divide the order of G the ring $\mathbb{Z}_p[G]$ is regular and one can use the techniques described in [8, §1.7] to give an explicit interpretation of this projection. In this manuscript, we will focus on primes p dividing the order of G where such an explicit interpretation is in general very difficult.

In [11], a close analysis of the finite support cohomology of Bloch and Kato for the base change of the p-adic Tate module of the dual abelian variety A^t is carried out under certain technical hypotheses on A and F. A consequence of this analysis is an explicit reinterpretation of the eTNC$_p$ in terms of a natural 'equivariant regulator' (see [11, Th. 4.1]). The main results of the present manuscript are based on the

explicit computation of this equivariant regulator in the special case where F/k is cyclic of degree p^n for an odd prime p. Under certain additional hypotheses on the structure of Tate-Shafarevich groups of A over the intermediate fields of F/k we obtain a completely explicit interpretation of the eTNC$_p$ (see Theorem 2.9). Whilst this is of independent theoretical interest, it also makes the eTNC$_p$ amenable to numerical verifications.

One of the main motivations behind our study of the equivariant Tamagawa number conjecture for the pair $(M_F, \mathbb{Z}[G])$ is the hope that it may provide a coherent overview of and a systematic approach to the study of explicit properties of leading terms and values at $s = 1$ of Hasse-Weil L-functions. In order to describe our current steps in this direction, we first recall the general philosophy of 'refined conjectures of the Birch and Swinnerton-Dyer type' that originates in the work of Mazur and Tate in [20]. These conjectures concern, for elliptic curves A defined over $\mathbb{Q}$ and certain abelian groups G, the properties of 'modular elements' $\theta_{A,G}$ belonging a priori to the rational group ring $\mathbb{Q}[G]$ and constructed from the modular symbols associated to A, therefore interpolating the values at $s = 1$ of the twisted Hasse-Weil L-functions associated to A and G. More precisely, the aim is to explicitly predict the precise power r (possibly infinite) of the augmentation ideal I of the integral group ring $\mathbb{Z}[G]$ with the property that $\theta_{A,G}$ belongs to I^r but not to I^{r+1}, and furthemore to explicitly describe the image of $\theta_{A,G}$ in the quotient I^r/I^{r+1} (whenever such an integer r exists). In the process of studying the modular element $\theta_{A,G}$, Mazur and Tate also predict that it should belong to the Fitting ideal over $\mathbb{Z}[G]$ of their 'integral Selmer group' $S(A/F)$ (and refer to such a statement as a 'weak main conjecture') and explicitly ask for a 'strong main conjecture' predicting an explicit generator of the Fitting ideal of an explicitly described natural modification of $S(A/F)$ (see [20, Remark after Conj. 3]).

However, it is well-known that in many cases of interest the modular element $\theta_{A,G}$ vanishes, thus rendering any such properties trivial, and it would therefore be desirable to carry out an analogous study for elements interpolating leading terms rather than values at $s = 1$ of the relevant Hasse-Weil L-functions, normalised by appropriate explicit regulators. Although the aim to study such elements already underlies the results of [11], one of the main advantages of confining ourselves to the special case in which the given extension of number fields F/k is cyclic of prime-power degree is that we are led to defining completely explicit 'twisted regulators' from our computation of the aforementioned equivariant regulator of [11]. Furthermore, we arrive at very explicit statements without having to restrict ourselves to situations in which the relevant Mordell-Weil groups are projective when considered as Galois modules. In particular, we derive predictions of the following nature for such an element $\mathcal{L}$ that interpolates leading terms at $s = 1$ of twisted Hasse-Weil L-functions normalised by our twisted regulators from the assumed validity of the eTNC$_p$ for $(M_F, \mathbb{Z}[G])$:

- a formula for the precise power $h \in \mathbb{Z}_{\geq 0}$ of the augmentation ideal $I_{G,p}$ of the integral group ring $\mathbb{Z}_p[G]$ with the property that $\mathcal{L}$ belongs to $I_{G,p}^h$ but not to

$I_{G,p}^{h+1}$ (expressed in terms of the ranks of the Mordell-Weil groups of A over the intermediate fields of F/k), and a formula for the image of $\mathcal{L}$ in the quotient $I_{G,p}^{h}/I_{G,p}^{h+1}$ (see Corollary 2.11);

- the statement that the element $\mathcal{L}$ of $\mathbb{Z}_p[G]$ (resp. a straightforward modification of $\mathcal{L}$) annihilates the p-primary Tate-Shafarevich group of A^t (resp. A) over F as a Galois module (see Theorem 2.12 and Corollary 2.14);

- and the explicit description of a natural quotient of (the Pontryagin dual of) the p-primary Selmer group of A over F whose Fitting ideal is generated by $\mathcal{L}$ (see Theorem 2.12).

The structure of the paper is as follows. In Section 2 we present our main results and in Section 4 we supply the proofs. In order to prepare for the proofs we recall in Section 3 the relevant material from [11]. In the final Section 5 we present some numerical computations.

We would like to thank David Burns and Christian Wuthrich for some helpful discussions concerning this project.

1.1 Notations and setting

We mostly adapt the notations from [11].

For a finite group Γ we write $\hat{\Gamma}$ for the set of irreducible E-valued characters of Γ, where E denotes either $\mathbb{C}$ or $\mathbb{C}_p$ (we will throughout our arguments have fixed an isomorphism of fields $j : \mathbb{C} \to \mathbb{C}_p$ and use it to implicitly identify both sets, with the intended meaning of $\hat{\Gamma}$ always clear from the context). We let $\mathbf{1}_\Gamma$ denote the trivial character of Γ and write $\check{\psi}$ for the contragrediant character of each $\psi \in \hat{\Gamma}$. We write

$$e_\psi = \frac{\psi(1)}{|\Gamma|} \sum_{\gamma \in \Gamma} \psi(\gamma)\gamma^{-1}$$

for the idempotent associated with $\psi \in \hat{\Gamma}$ and also set $\mathrm{Tr}_\Gamma := \sum_{\gamma\in\Gamma} \gamma$.

For any abelian group M we let M_{tor} denote its torsion subgroup and M_{tf} the torsion-free quotient M/M_{tor}. We also set $M_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} M$ and, if M is finitely generated, we set $\mathrm{rk}(M) := \dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} M)$.

For any $\mathbb{Z}_p[\Gamma]$-module M we write $M^\vee$ for the Pontryagin dual $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ and M^* for the linear dual $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$, each endowed with the natural contragredient action of Γ. Explicitly, for a homomorphism f and elements $m \in M$ and $\gamma \in \Gamma$, one has $(\gamma f)(m) = f(\gamma^{-1}m)$.

For any Galois extension of fields we abbreviate $\mathrm{Gal}(L/K)$ to $G_{L/K}$. We fix an algebraic closure K^c of K and abbreviate $G_{K^c/K}$ to G_K. For each non-archimedian place v of a number field we write κ_v for the residue field.

Throughout this paper, we will consider the following situation. We have fixed an odd prime p and a Galois extension F/k of number fields with group $G = G_{F/k}$.

Except in Section 3, the extension F/k will always be cyclic of degree p^n. We give ourselves an abelian variety A of dimension d defined over k. For each intermediate field L of F/k we write S_p^L, S_r^L and S_b^L for the set of non-archimedean places of L that are p-adic, which ramify in F/L and at which A/L has bad reduction respectively. Similarly, we write $S_\infty^L, S_\mathbb{R}^L$ and $S_\mathbb{C}^L$ for the sets of archimedean, real and complex places of L respectively. If $L = k$ we simply write $S_p, S_r, S_b, S_\infty, S_\mathbb{R}$ and $S_\mathbb{C}$.

Finally, we write $A(L)$ for the Mordell-Weil group and $Ш_p(A_L)$ for the p-primary Tate-Shafarevich group of A over L.

2 Statement of the main results

Recall that A is an abelian variety of dimension d defined over the number field k. Furthermore, F/k is cyclic of degree p^n where p is an odd prime.

We assume throughout this section that A/k and F/k are such that

(a) $p \nmid |A(k)_{tor}| \cdot |A^t(k)_{tor}|$,

(b) $p \nmid \prod_{v \in S_b} c_v(A,k)$, where $c_v(A,k)$ denotes the Tamagawa number of A at v,

(c) A has good reduction at all p-adic places,

(d) p is unramified in $F/\mathbb{Q}$,

(e) No place of bad reduction is ramified in F/k, i.e. $S_b \cap S_r = \emptyset$,

(f) $p \nmid \prod_{v \in S_r} |A(\kappa_v)|$,

(g) $Ш(A_F)$ is finite,

(h) $Ш_p(A_{F^H}) = 0$ for all non-trivial subgroups H of G.

Remarks 2.1. *a) Our assumptions (a) - (g) recover the hypotheses (a) - (i) of [11].*
b) We emphasize that in (h) we allow $Ш_p(A_F)$ to be non-trivial.

An understanding of the G-module structure of the relevant Mordell-Weil groups is key to our approach. We hence begin by applying a result of Yakovlev [22] in order to obtain such explicit descriptions. This approach is inspired by work of Burns, who obtained a similar result in [7, Prop. 7.2.6(i)]. For a non-negative integer m and a $\mathbb{Z}_p[G]$-module M we write $M^{<m>}$ for the direct sum of m copies of M. Furthermore, we set $[m] := \{1, \dots, m\}$.

Proposition 2.2. *There exist isomorphisms of $\mathbb{Z}_p[G]$-modules of the form*

$$A(F)_p \cong \bigoplus_{J \leq G} \mathbb{Z}_p[G/J]^{<m_J>} \cong A^t(F)_p,$$

for a set of non-negative integers $\{m_J : J \leq G\}$.

Proposition 2.2 has the following immediate consequence for the ranks of the relevant Mordell-Weil groups.

Corollary 2.3. *For any subgroup H of G we have*

$$\begin{aligned} &\mathrm{rk}(A(F^H)) = \mathrm{rk}(A^t(F^H)) = \\ = \ &\sum_{J>H} |G/J| m_J + |G/H| \sum_{J \leq H} m_J \leq |G/H| \mathrm{rk}(A(k)). \end{aligned}$$

Proposition 2.2 combines with Roiter's Lemma (see [12, (31.6)]) to imply the existence of points $P_{(J,j)} \in A(F)$ and $P^t_{(J,j)} \in A^t(F)$ for $J \leq G$ and $j \in [m_J]$ with the property that

$$\begin{array}{ll} A(F)_p = \bigoplus_{J \leq G} \bigoplus_{j \in [m_J]} \mathbb{Z}_p[G/J] P_{(J,j)}, & \mathbb{Z}_p[G/J] P_{(J,j)} \cong \mathbb{Z}_p[G/J], \\ A^t(F)_p = \bigoplus_{J \leq G} \bigoplus_{j \in [m_J]} \mathbb{Z}_p[G/J] P^t_{(J,j)}, & \mathbb{Z}_p[G/J] P^t_{(J,j)} \cong \mathbb{Z}_p[G/J]. \end{array} \tag{1}$$

Furthermore, our choice of points as in (1) guarantees that one also has

$$\begin{array}{ll} \mathbb{Q} \otimes_{\mathbb{Z}} A(F) = \bigoplus_{J \leq G} \bigoplus_{j \in [m_J]} \mathbb{Q}[G/J] P_{(J,j)}, & \mathbb{Q}[G/J] P_{(J,j)} \cong \mathbb{Q}[G/J], \\ \mathbb{Q} \otimes_{\mathbb{Z}} A^t(F) = \bigoplus_{J \leq G} \bigoplus_{j \in [m_J]} \mathbb{Q}[G/J] P^t_{(J,j)}, & \mathbb{Q}[G/J] P^t_{(J,j)} \cong \mathbb{Q}[G/J]. \end{array} \tag{2}$$

We now fix sets

$$\mathcal{P} = \{P_{(J,j)} \in A(F) : J \leq G, j \in [m_J]\}, \quad \mathcal{P}^t = \{P^t_{(J,j)} \in A^t(F) : J \leq G, j \in [m_J]\},$$

such that (2) holds. For $0 \leq t \leq n$ we write H_t for the (unique) subgroup of G of order p^{n-t} and set $P_{(t,j)} := P_{(H_t,j)}, P^t_{(t,j)} := P^t_{(H_t,j)}$. We also put $m_t := m_{H_t}$ and $e_{H_t} := \frac{1}{|H_t|}\mathrm{Tr}_{H_t} = \frac{1}{|H_t|}\sum_{g \in H_t} g$. We writte $\langle\ ,\ \rangle_F$ for the Néron-Tate height pairing $A(F) \times A^t(F) \to \mathbb{R}$ defined relative to the field F and define a matrix with entries in $\mathbb{C}[G]$ by setting

$$R(\mathcal{P}, \mathcal{P}^t) := \left(\frac{1}{|H_u|} \sum_{\tau \in G/H_u} \langle \tau \cdot P_{(u,k)}, P^t_{(t,j)} \rangle_F (\tau \cdot e_{H_u}) \right)_{(u,k),(t,j)},$$

where (u,k) is the row index with $0 \leq u \leq n$, $k \in [m_u]$, and (t,j) is the column index with $0 \leq t \leq n$, $j \in [m_t]$ (we always order sets of the form $\{(t,j) \colon 0 \leq t \leq n, j \in [m_t]\}$ lexicographically). We note that, since each point $P_{(u,k)}$ belongs to $A(F^{H_u})$, the action of G/H_u on $P_{(u,k)}$ is well-defined.

For any matrix $A = \left(a_{(u,k),(t,j)}\right)_{(u,k),(t,j)}$ indexed as above we define

$$A_{t_0} := \left(a_{(u,k),(t,j)}\right)_{(u,k),(t,j),u,t \geq t_0},$$

with the convention $A_{t_0} = 1$ whenever no entries $a_{(u,k),(t,j)}$ with $u, t \geq t_0$ exist. If A is a matrix with coefficients a_{ij} in $\mathbb{C}[G]$ or $\mathbb{C}_p[G]$, then for any $\psi \in \widehat{G}$ we write $\psi(A)$ for the matrix with coefficients $\psi(a_{ij})$. We also set $R_{t_0}(\mathcal{P}, \mathcal{P}^t) = R(\mathcal{P}, \mathcal{P}^t)_{t_0}$.

Definition 2.4. For each character $\psi \in \hat{G}$ we define $t_\psi \in \{0, \dots, n\}$ by the equality $\ker(\psi) = H_{t_\psi}$ and call

$$\lambda_\psi(\mathcal{P}, \mathcal{P}^t) := \det\left(\psi\left(R_{t_\psi}(\mathcal{P}, \mathcal{P}^t)\right)\right).$$

the 'lower ψ-minor' of $R(\mathcal{P}, \mathcal{P}^t)$.

Remark 2.5. *It is easy to see that the element $\sum_{\psi\in\widehat{G}} \lambda_\psi(\mathcal{P}, \mathcal{P}^t)e_\psi \in \mathbb{C}[G]$ depends upon the choice of points $\mathcal{P}$ and $\mathcal{P}^t$ satisfying (2) only modulo $\mathbb{Q}[G]^\times$. Similarly, for any given isomorphism of fieds $j : \mathbb{C} \to \mathbb{C}_p$, it is clear that the element $\sum_{\psi\in\widehat{G}} j(\lambda_\psi(\mathcal{P}, \mathcal{P}^t))e_\psi \in \mathbb{C}_p[G]$ depends upon the choice of points $\mathcal{P}$ and $\mathcal{P}^t$ satisfying (1) only modulo $\mathbb{Z}_p[G]^\times$.*

For any order Λ in $\mathbb{Q}[G]$ that contains $\mathbb{Z}[G]$ we let $\mathrm{C}(A, \Lambda)$ denote the integrality part of the equivariant Tamagawa number conjecture ('eTNC' for brevity) for the pair $(h^1(A_F)(1), \Lambda)$ as formulated by Burns and Flach in [9, Conj. 4(iv)]. Similarly, we let $\mathrm{C}(A, \mathbb{Q}[G])$ denote the rationality part as ormulated in [9, Conj. 4(iii) or Conj. 5]. We recall that, under the assumed validity of hypothesis (g), $\mathrm{C}(A, \Lambda)$ takes the form of an equality in the relative K-group $K_0(\Lambda, \mathbb{R}[G])$. For each embedding $j\colon \mathbb{R} \longrightarrow \mathbb{C}_p$ we denote by $\mathrm{C}_{p,j}(A, \Lambda)$ the image of this conjectural equality under the induced map $K_0(\Lambda, \mathbb{R}[G]) \longrightarrow K_0(\Lambda_p, \mathbb{C}_p[G])$. We then say that $\mathrm{C}_p(A, \Lambda)$ is valid if $\mathrm{C}_{p,j}(A, \Lambda)$ is valid for every isomorphism $j : \mathbb{C} \to \mathbb{C}_p$.

The eTNC is an equality between analytic and algebraic invariants associated with A/k and F/k. In the following we describe and define the analytic part. We first recall the definition of periods and Galois Gauss sums of [11, Sec. 3.3]. We fix Néron models $\mathcal{A}^t$ for A^t over $\mathcal{O}_k$ and $\mathcal{A}^t_v$ for $A^t_{k_v}$ over $\mathcal{O}_{k_v}$ for each v in S_p and then fix a k-basis $\{\omega_b\}_{b\in[d]}$ of the space of invariant differentials $H^0(A^t, \Omega^1_{A^t})$ which gives $\mathcal{O}_{k_v}$-bases of $H^0\big(\mathcal{A}^t_v, \Omega^1_{\mathcal{A}^t_v}\big)$ for each such v and is also such that each ω_b extends to an element of $H^0\big(\mathcal{A}^t, \Omega^1_{\mathcal{A}^t}\big)$.

For each v in $S_\mathbb{C}$ we fix a $\mathbb{Z}$-basis $\{\gamma_{v,a}\}_{a\in[2d]}$ of $H_1\big(\sigma_v(A^t)(\mathbb{C}), \mathbb{Z}\big)$. For each v in $S_\mathbb{R}$ we let c denote complex conjugation and fix a $\mathbb{Z}$-basis $\{\gamma^+_{v,a}\}_{a\in[d]}$ of $H_1\big(\sigma_v(A^t)(\mathbb{C}), \mathbb{Z}\big)^{c=1}$. For each v in $S_\mathbb{R}$, resp. $S_\mathbb{C}$, we then define periods by setting

$$\Omega_v(A/k) := \left|\det\left(\int_{\gamma^+_{v,a}} \omega_b\right)_{a,b}\right|, \text{ resp. } \Omega_v(A/k) := \left|\det\left(\int_{\gamma_{v,a}} \omega_b, c\Big(\int_{\gamma_{v,a}} \omega_b\Big)\right)_{a,b}\right|,$$

where in the first matrix (a, b) runs over $[d] \times [d]$ and in the second matrix (a, b) runs over $[2d] \times [d]$.

In our special case all characters are one-dimensional and, moreover, $|G|$ is odd. Therefore the definitions of [11] simplify and we set

$$\begin{aligned} \Omega(A/k) &:= \prod_{v\in S_\infty} \Omega_v(A/k), \\ w_\infty(k) &:= i^{|S_\mathbb{C}|}. \end{aligned}$$

For each place v in S_r we write $\bar{I}_v \subseteq G$ for the inertia group of v and Fr_v for the natural Frobenius in $G/\bar{I}_v$. We define the 'non-ramified characteristic' u_v by

$$u_v(\psi) := \begin{cases} -\psi(\mathrm{Fr}_v^{-1}), & \psi|_{\bar{I}_v} = 1, \\ 1, & \psi|_{\bar{I}_v} \neq 1. \end{cases}$$

and

$$u(\psi) := \prod_{v \in S_r} u_v(\psi).$$

For each character $\psi \in \widehat{G}$ we then define the modified Galois-Gauss sum by setting

$$\tau^*(\mathbb{Q}, \mathrm{ind}_k^{\mathbb{Q}}(\psi)) := u(\psi)\tau(\mathbb{Q}, \mathrm{ind}_k^{\mathbb{Q}}(\psi)) \in (\mathbb{Q}^c)^\times,$$

where each individual Galois-Gauss sum $\tau(\mathbb{Q}, \cdot)$ is as defined by Martinet in [19]. For each $\psi \in \widehat{G}$ we set

$$\mathcal{L}^*_\psi = \mathcal{L}^*_{A,F/k,\psi} := \frac{L^*_{S_r}(A, \check{\psi}, 1)\tau^*(\mathbb{Q}, \mathrm{ind}_k^{\mathbb{Q}}(\psi))^d}{\Omega(A/k)w_\infty(k)^d} \in \mathbb{C}^\times,$$

where here for each finite set Σ of places of k we write $L^*_\Sigma(A, \psi, 1)$ for the leading term in the Taylor expansion at $s = 1$ of the Σ-truncated ψ-twisted Hasse-Weil-L-function of A. Without any further mention we will always assume that the functions $L_\Sigma(A, \psi, s)$ have analytic continuation to $s = 1$ (as conjectured in [9, Conj. 4 (i)]) and recall that they are then expected to have a zero of order $r_\psi := \dim_{\mathbb{C}}(V_\psi \otimes_{\mathbb{Z}} A(F))^G$, where V_ψ denotes any $\mathbb{C}[G]$-module of character ψ (this is the rank conjecture [9, Conj. 4 (ii)]).

We finally define

$$\mathcal{L}^* = \mathcal{L}^*_{A,F/k} := \sum_{\psi \in \widehat{G}} \mathcal{L}^*_{A,F/k,\psi} e_\psi \in \mathbb{C}[G]^\times$$

and note that the element $\mathcal{L}^*$ defined in [11, Th. 4.1] specialises precisely to our definition.

Theorem 2.6. *$C(A, \mathbb{Q}[G])$ is valid if and only if*

$$\mathcal{L}^*_\psi \lambda_\psi(\mathcal{P}, \mathcal{P}^t)^{-1} \in \mathbb{Q}(\psi)$$

for all $\psi \in \widehat{G}$ and furthermore, for any $\gamma \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q})$,

$$\mathcal{L}^*_{\psi^\gamma} \lambda_{\psi^\gamma}(\mathcal{P}, \mathcal{P}^t)^{-1} = \gamma\left(\mathcal{L}^*_\psi \lambda_\psi(\mathcal{P}, \mathcal{P}^t)^{-1}\right),$$

for any, or equivalently every, choice of points $\mathcal{P}$ and $\mathcal{P}^t$ such that (2) holds.

Remarks 2.7. *(i) From the definitions of $u(\psi)$, $w_\infty(k)$ and the definition of local Euler factors it is immediately clear that in the statement of Theorem 2.6 we can replace $\mathcal{L}^*_\psi$ by*

$$\tilde{\mathcal{L}}^*_\psi := \frac{L^*(A, \check{\psi}, 1)\tau(\mathbb{Q}, \mathrm{ind}_k^{\mathbb{Q}}(\psi))^d}{\Omega(A/k)}.$$

(ii) The explicit conditions on elements of the form $\mathcal{L}^*_\psi \lambda_\psi(\mathcal{P}, \mathcal{P}^t)^{-1}$ given in Theorem 2.6 generalise and refine the predictions given by Fearnley and Kisilevsky in [15, 16]. For details see [2, Ex. 5.2]. In particular, we note that the numerical computations performed by Fearnley and Kisilevsky can be interpreted via Theorem 2.6 as supporting evidence for conjecture $C(A, \mathbb{Q}[G])$.

We fix a generator σ of G and define Σ to be the diagonal matrix indexed by pairs $(t, j), (s, i)$ with $\sigma^{p^t} - 1$ at the diagonal entry associated to (t, j) and zeros elsewhere. For any matrix $A = \left(a_{(u,k),(t,j)}\right)_{(u,k),(t,j)}$ indexed by tuples (u, k) and (t, j) as above we define

$$A^{t_0} := \left(a_{(u,k),(t,j)}\right)_{(u,k),(t,j),u,t \leq t_0},$$

once again with the convention $A^{t_0} = 1$ whenever no entries $a_{(u,k),(t,j)}$ with $u, t \leq t_0$ exist. We recall that for each character $\psi \in \widehat{G}$ we defined t_ψ such that $\ker(\psi) = H_{t_\psi}$. We define the the 'upper ψ-minor' of Σ by

$$\delta_\psi \;\; := \;\; \det\left(\psi\left(\Sigma^{t_\psi - 1}\right)\right).$$

It is easy to see that for another choice of generator of G, say τ, one has

$$\sum_{\psi \in \widehat{G}} \frac{\delta_\psi(\sigma)}{\delta_\psi(\tau)} e_\psi \in \mathbb{Z}_p[G]^\times.$$

Under our current hypotheses on the data $(A, F/k, p)$ and the additional hypothesis that $Ш_p(A_F) = 0$, and for any intermediate field L of F/k, we shall say that $\mathrm{BSD}_p(L)$ holds if, for any choice of $\mathbb{Z}$-bases $\{Q_i\}$ and $\{R_j\}$ of $A(L)$ and $A^t(L)$ respectively and of isomorphism $j : \mathbb{C} \to \mathbb{C}_p$, one has that

$$j\left(\frac{L^*(A/L, 1) \cdot (\sqrt{|d_L|})^d}{\det(\langle Q_i, R_j \rangle_L) \cdot \prod_{v \in S^L_\infty} \Omega_v(A/L)}\right) \in \mathbb{Z}_p^\times.$$

Here d_L denotes the discriminant of the field L and each period $\Omega_v(A/L)$ is as defined above but relative to the field L rather than k. It will become apparent in the proof of Theorem 2.8 below that the validity of $\mathrm{BSD}_p(L)$ is equivalent to the validity of the p-part of the eTNC for the pair $(h^1(A_L)(1), \mathbb{Z})$. We recall that hypotheses (a), (b) and (h) justify the fact that no orders of torsion subgroups of Mordell-Weil groups, Tamagawa numbers or orders of Tate-Shafarevich groups occur in this formulation, and furthermore note that, by explicitly computing integrals,

the periods $\Omega_v(A/L)$ can be related to those obtained by integrating measures as occurring in the classical formulation of the Birch and Swinnerton-Dyer conjecture – see, for example, Gross [18, p. 224].

For the remainder of this section, we assume that $C(A, \mathbb{Q}[G])$ is valid. It is then easy to see that, for any order Λ in $\mathbb{Q}[G]$ that contains $\mathbb{Z}[G]$, the validity of $\mathrm{C}_{p,j}(A, \Lambda)$ is independent of the choice of isomorphism $j : \mathbb{C} \to \mathbb{C}_p$, and so we fix such a j for the remainder of this section. In fact, all relevant elements of $\mathbb{C}[G]$ appearing in the statements of our results will actually belong to $\mathbb{Q}[G]$ (as a consequence of an easy application of Theorem 2.6) and so we will consider them simoultaneously as elements of $\mathbb{Q}_p[G] \subset \mathbb{C}_p[G]$ in the natural way without any explicit mention of j.

Let $\mathcal{M}$ denote the maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$. For any $\psi \in \widehat{G}$, let $\mathcal{O}_\psi$ be the valuation ring of $\mathbb{Q}_p(\psi)$. Let $\mathfrak{p}_\psi$ be the (unique) prime ideal of $\mathcal{O}_\psi$ above p. We write $v_{\mathfrak{p}_\psi}$ for the normalised valuation defined by $\mathfrak{p}_\psi$.

Theorem 2.8. *Let $\mathcal{P}$ and $\mathcal{P}^t$ be any choice of points such that (1) holds. We assume that $Ш_p(A_F) = 0$. Then the following are equivalent.*

(i) $C_p(A, \mathcal{M})$ is valid.

(ii) $BSD_p(L)$ is valid for all intermediate fields L of F/k.

(iii) For each $\psi \in \widehat{G}$ one has

$$v_{\mathfrak{p}_\psi}\left(\frac{\mathcal{L}_\psi^*}{\lambda_\psi(\mathcal{P}, \mathcal{P}^t)}\right) = b_\psi \text{ where } b_\psi := \sum_{s=0}^{t_\psi - 1} p^s m_s.$$

(iv)

$$\sum_{\psi \in \widehat{G}} \frac{\mathcal{L}_\psi^*}{\lambda_\psi(\mathcal{P}, \mathcal{P}^t)\delta_\psi} e_\psi \in \mathcal{M}_p^\times.$$

To describe the full range of implications of the validity of $C_p(A, \mathbb{Z}[G])$ requires yet more work and some further notations.

For each finite extension L/k and natural number n we write $\mathrm{Sel}^{(p^n)}(A_L)$ for the Selmer group associated to the isogeny $[p^n]$. We define the p-primary Selmer group by

$$\mathrm{Sel}_p(A_L) := \varinjlim \mathrm{Sel}^{(p^n)}(A_L).$$

We recall that one then obtains a canonical short exact sequence

$$0 \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}} A(F) \longrightarrow \mathrm{Sel}_p(A_F) \longrightarrow Ш_p(A_F) \longrightarrow 0$$

of $\mathbb{Z}_p[G]$-modules, from which upon taking Pontryagin duals one derives a canonical short exact sequence

$$0 \longrightarrow Ш_p(A_F)^\vee \longrightarrow \mathrm{Sel}_p(A_F)^\vee \longrightarrow A(F)_p^* \longrightarrow 0. \tag{3}$$

We will throughout use this canonical short exact sequence to fix identifications of $(\mathrm{Sel}_p(A_F)^\vee)_{\mathrm{tor}}$ with $Ш_p(A_F)^\vee$ and of $(\mathrm{Sel}_p(A_F)^\vee)_{\mathrm{tf}}$ with $A(F)_p^*$.

In [11] a suitable integral model $R\Gamma_f(k, T_{p,F}(A))$ of the finite support cohomology of Bloch and Kato for the base change through F/k of the p-adic Tate module of A^t is defined and then used in order to define an 'equivariant regulator' which is essential to the explicit reformulation of $\mathrm{C}_p(A, \mathbb{Z}[G])$ (see [11, Th. 4.1]). We will recall this reformulation and the relevant definitions in Section 3.

By [11, Lem. 3.1], $R\Gamma_f(k, T_{p,F}(A))$ is under our current hypotheses a perfect complex of $\mathbb{Z}_p[G]$-modules which is acyclic outside degrees 1 and 2 and whose cohomology groups in degrees 1 and 2 canonically identify with $A^t(F)_p$ and $\mathrm{Sel}_p(A_F)^\vee$ respectively. $R\Gamma_f(k, T_{p,F}(A))$ therefore uniquely determines a perfect element $\delta_{A,K,p}$ of $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(\mathrm{Sel}_p(A_F)^\vee, A^t(F)_p)$. We will use Proposition 2.2 to fix an explicit 2-syzygy of the form

$$0 \to M \xrightarrow{\iota} F^0 \to F^1 \to A(F)_p^* \to 0, \tag{4}$$

in which we set

$$M := \bigoplus_{(t,j)} \mathbb{Z}_p[G/H_t]$$

and both F^0 and F^1 are finitely generated free $\mathbb{Z}_p[G]$-modules and then use the exact sequence (4) to compute $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(A(F)_p^*, A^t(F)_p)$ via the explicit isomorphism

$$\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(A(F)_p^*, A^t(F)_p) \simeq \mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)/\iota_* \left(\mathrm{Hom}_{\mathbb{Z}_p[G]}(F^0, A^t(F)_p)\right).$$

If we now assume that $Ш_p(A_F)$ vanishes, we may identify $\mathrm{Sel}_p(A_F)^\vee$ and $A(F)_p^*$, so that $\delta_{A,F,p}$ uniquely determines an element of the above quotient. We will prove (see Lemmas 4.3 and 4.4 below) that we may choose a representative $\Phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)$ of $\delta_{A,F,p}$ with the following properties:

(P1) Φ is bijective,

(P2) Φ restricts to send an element $x_{(n,j)}$ of the (n,j)-th direct summand $\mathbb{Z}_p[G]$ to $x_{(n,j)}P^t_{(n,j)}$.

For a fixed choice of points $\mathcal{P}$ and $\mathcal{P}^t$ such that (1) holds and of $\Phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)$ as above, we fix a canonical $\mathbb{Z}_p[G/H_t]$-basis element $e_{(t,j)}$ of each direct summand $\mathbb{Z}_p[G/H_t]$ of M and fix any elements $\Phi_{(t,j),(s,i)}$ of $\mathbb{Z}_p[G]$ with the property that

$$\Phi(e_{(s,i)}) = \sum_{(t,j)} \Phi_{(t,j),(s,i)} P^t_{(t,j)}. \tag{5}$$

We thus obtain an invertible matrix $\left(\Phi_{(t,j),(s,i)}\right)_{(t,j),(s,i)}$ with entries in $\mathbb{Z}_p[G]$, which by abuse of notation we shall also denote by Φ. The matrix Φ is of the form

$$\left(\begin{array}{c|c} \left(\Phi_{(t,j),(s,i)}\right)_{t,s<n} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \hline \begin{matrix} 0 & \dots & 0 \end{matrix} & I_{m_n} \end{array}\right) \tag{6}$$

with I_{m_n} denoting the identity $m_n \times m_n$ matrix.

Recall the definition of t_ψ in Definition 2.4. We define the 'lower ψ-minor' of Φ by setting

$$\varepsilon_\psi(\Phi) := \det\left(\psi\left(\Phi_{t_\psi}\right)\right).$$

We note firstly that, since the chosen points $P^t_{(t,j)}$ satisfy (1), each element $\varepsilon_\psi(\Phi)$ (and, indeed, even the matrix $\psi\left(\Phi_{t_\psi}\right)$) is independent of our particular choice of elements $\Phi_{(t,j),(s,i)} \in \mathbb{Z}_p[G]$ with the property that (5) holds.

Theorem 2.9. *Let $\mathcal{P}$ and $\mathcal{P}^t$ be any choice of points such that (1) holds. Assume that $Ш_p(A_F) = 0$. Let $\Phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)$ be any representative of $\delta_{A,F,p}$ such that (P1) and (P2) hold. Then $C_p(A, \mathbb{Z}[G])$ is valid if and only if*

$$\sum_{\psi \in \widehat{G}} \frac{\mathcal{L}^*_\psi}{\lambda_\psi(\mathcal{P}, \mathcal{P}^t) \cdot \varepsilon_\psi(\Phi) \cdot \delta_\psi} e_\psi \in \mathbb{Z}_p[G]^\times. \tag{7}$$

Remark 2.10. *Theorem 2.9 can be reformulated in terms of explicit congruences.*

Via Theorem 2.9, we now obtain completely explicit predictions concerning congruences in the augmentation filtration of the integral group ring $\mathbb{Z}_p[G]$ for leading terms at $s = 1$ of the relevant Hasse-Weil-L-functions of A normalised by our explicit regulators. We recall that such predictions constitute a refinement and generalisation of the congruences for modular symbols that are conjectured by Mazur and Tate in [20].

In order to state such conjectural congruences, we require the following notation: if the inequality $\mathrm{rk}(A(F^J)) \leq |G/J|\mathrm{rk}(A(k))$ of Corollary 2.3 is strict for some subgroup J of G, we may and will denote by $H = H_{t_0}$ the smallest non-trivial subgroup of G with the property that $m_H \neq 0$. Hence t_0 is the maximal index with the properties $m_{t_0} \neq 0$ and $t_0 < n$. We then define

$$\mathcal{L} := \begin{cases} \sum_{\psi \in \widehat{G}} \frac{\mathcal{L}^*_\psi}{\det(\psi(R(\mathcal{P}, \mathcal{P}^t)))} e_\psi, & \text{if } \mathrm{rk}(A(F^J)) = |G/J|\mathrm{rk}(A(k)) \text{ for every } J, \\ \sum_{\psi|_H \neq 1} \frac{\mathcal{L}^*_\psi}{\lambda_\psi(\mathcal{P}, \mathcal{P}^t)} e_\psi, & \text{otherwise.} \end{cases}$$

We also let $I_{G,p}$ denote the kernel of the augmentaion map $\mathbb{Z}_p[G] \longrightarrow \mathbb{Z}_p$.

Corollary 2.11. *Let $\mathcal{P}$ and $\mathcal{P}^t$ be any choice of points such that (1) holds. Assume that $Ш_p(A_F) = 0$. Let $\Phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)$ be any representative of $\delta_{A,F,p}$ such that (P1) and (P2) hold. If $C_p(A, \mathbb{Z}[G])$ is valid, then*

(i) $\mathcal{L}$ *belongs to the ideal $I^h_{G,p}$ of $\mathbb{Z}_p[G]$, where $h := \sum_{t<n} m_t$.*

(ii) $\epsilon := \det\left(\mathbf{1}_G(\Phi)\right) \in \mathbb{Z}_p^\times$.

(iii) $v := (-1)^{d \cdot |S_r|} \frac{L^*_{S_r}(A/k,1) \cdot (\sqrt{|d_k|})^d}{\Omega(A) \cdot \det(\mathbf{1}_G(R(\mathcal{P}, \mathcal{P}^t)))} \in \mathbb{Z}_p^\times$.

(iv) $\mathcal{L} \equiv \frac{v}{\epsilon} \cdot \prod_{t<n} \left(\sigma^{p^t} - 1\right)^{m_t} \pmod{I_{G,p}^{h+1}}$.

The theory of organising matrices developed by Burns and the second named author in [10] allows one to derive the containment $\mathcal{L} \in I_{G,p}^h$ of Corollary 2.11(i) from the assumed validity of conjecture $C_p(A, \mathbb{Z}[G])$ in situations in which $Ш_p(A_F)$ is non-trivial. In this greater level of generality, it furthermore leads to explicit statements concerning annihilation of Tate-Shafarevich groups and (generalised) 'strong main conjectures' of the kind that Mazur and Tate explicitly ask for in [20, Remark after Conj. 3]. Namely, we obtain the following result:

Theorem 2.12. *Let $\mathcal{P}$ and $\mathcal{P}^t$ be any choice of points such that (1) holds. If $C_p(A, \mathbb{Z}[G])$ is valid, then*

(i) *$\mathcal{L}$ belongs to the ideal $I_{G,p}^h$ of $\mathbb{Z}_p[G]$, where $h := \sum_{t<n} m_t$.*

(ii) *$\mathcal{L}$ annihilates the $\mathbb{Z}_p[G]$-module $Ш_p(A_F^t)$.*

(iii) *There exists a (finitely generated) free $\mathbb{Z}_p[G]$-submodule Π of $\mathrm{Sel}_p(A_F)^\vee$ of (maximal) rank m_n with the property that $\mathcal{L}$ generates the Fitting ideal of the quotient $\mathrm{Sel}_p(A_F)^\vee/\Pi$.*

Remark 2.13. *It will become clear in the course of the proof that, provided that there exist sets of points $\mathcal{P}$ and $\mathcal{P}^t$ such that (1) holds from which one may construct the element $\mathcal{L}$, Theorem 2.12 remains valid even if hypothesis (h) fails to hold. This fact is relevant because, as we will see in Section 5, it allows us to obtain numerical supporting evidence for $C_p(A, \mathbb{Z}[G])$ (via verifying the explicit assertions of Theorem 2.12) in a wider range of situations.*

Let $\#\colon \mathbb{Z}_p[G] \longrightarrow \mathbb{Z}_p[G]$ denote the involution induced by $g \mapsto g^{-1}$. Recalling that the Cassels-Tate pairing induces a canonical isomorphism between $Ш_p(A_F)^\vee$ and $Ш_p(A_F^t)$, we immediately obtain the following corollary:

Corollary 2.14. *Under the assumptions of Theorem 2.12 one has that the element $\mathcal{L}^\#$ of $I_{G,p}^h$ annihilates the $\mathbb{Z}_p[G]$-module $Ш_p(A_F)$.*

3 An explicit reformulation of conjecture $\mathrm{C}_p(A, \mathbb{Z}[G])$

3.1 K-theory and refined Euler characteristics

Let R be either $\mathbb{Z}$ or $\mathbb{Z}_p$ and, for the moment, let G be any finite group. We write K for the quotient field of R end let $\mathbb{E}$ be a field extension of K. Let Λ be an R-order in $K[G]$. We recall that there is a canonical exact sequence of algebraic K-groups

$$K_1(\Lambda) \longrightarrow K_1(\mathbb{E}[G]) \xrightarrow{\partial^1_{\Lambda,\mathbb{E}}} K_0(\Lambda, \mathbb{E}[G]) \longrightarrow K_0(\Lambda) \longrightarrow K_0(\mathbb{E}[G]) \tag{8}$$

where $K_0(\Lambda, \mathbb{E}[G])$ is the relative algebraic K-group as defined by Swan in [21, p. 215].

For any ring Σ we write $\zeta(\Sigma)$ for its center. We let $\mathrm{nr}_{\mathbb{E}[G]}\colon K_1(\mathbb{E}[G]) \longrightarrow \zeta(\mathbb{E}[G])^\times$ denote the (injective) homomorphism induced by the reduced norm map. If Λ is a $\mathbb{Z}$-order in $\mathbb{Q}[G]$ we write

$$\begin{aligned} \delta_G &: \zeta(\mathbb{R}[G])^\times \longrightarrow K_0(\Lambda, \mathbb{R}[G]), \\ \delta_{G,p} &: \zeta(\mathbb{C}_p[G])^\times \longrightarrow K_0(\Lambda_p, \mathbb{C}_p[G]) \end{aligned}$$

for the extended boundary homomorphisms as defined in [9, Sec. 4.2]. Recall that

$$\delta_G \circ \mathrm{nr}_{\mathbb{R}[G]} = \partial^1_{\Lambda,\mathbb{R}}, \quad \delta_{G,p} \circ \mathrm{nr}_{\mathbb{C}_p[G]} = \partial^1_{\Lambda_p,\mathbb{C}_p}.$$

By the general construction described in [9, Prop. 2.5] (and [5, Lem. 5.1]) each pair $(C^\bullet, \lambda)$ consisting of a complex $C^\bullet \in D^p(\Lambda_p)$ and an isomorphism $\lambda\colon H^{ev}(C^\bullet) \longrightarrow H^{od}(C^\bullet)$ gives rise to a refined Euler characteristic $\chi_{G,p}(C^\bullet, \lambda) \in K_0(\Lambda_p, \mathbb{C}_p[G])$. For an explicit example of the computation of $\chi_{G,p}(C^\bullet, \lambda)$ in a special case, which is also relevant for the computations in this paper, we refer the reader to [3, Sec. 3].

It is well known that $\partial^1_{\Lambda_p,\mathbb{C}_p}$ is onto and that $\mathrm{nr}_{\mathbb{C}_p[G]}$ is an isomorphism. We therefore deduce from (8) that

$$K_0(\Lambda_p, \mathbb{C}_p[G]) \simeq \zeta(\mathbb{C}_p[G])^\times / \mathrm{nr}_{\mathbb{C}_p[G]}\left(K_1(\Lambda_p)\right). \tag{9}$$

Since Λ_p is semilocal, we can replace $K_1(\Lambda_p)$ by $\Lambda_p^\times$ in (9). Moreover, it follows from (9) that for an element $\xi \in \zeta(\mathbb{C}_p[G])^\times$ one has that $\delta_{G,p}(\xi) = 0$ if and only if $\xi \in \mathrm{nr}_{\mathbb{C}_p[G]}\left(\Lambda_p^\times\right)$. Finally, if G is abelian, we have that

$$K_0(\Lambda_p, \mathbb{C}_p[G]) \simeq \mathbb{C}_p[G]^\times / \Lambda_p^\times,$$

and hence $\delta_{G,p}(\xi) = 0$ if and only if $\xi \in \Lambda_p^\times$.

In this context we also recall [2, Lem. 2.5]. We naturally interpret $K_0(\Lambda, \mathbb{Q}[G])$ and $K_0(\Lambda_p, \mathbb{Q}_p[G])$ as subgroups of $K_0(\Lambda, \mathbb{R}[G])$ and $K_0(\Lambda_p, \mathbb{C}_p[G])$ respectively, and recall that if $\xi \in \zeta(\mathbb{R}[G])^\times$, then

$$\delta_G(\xi) \in K_0(\Lambda, \mathbb{Q}[G]) \iff \xi \in \zeta(\mathbb{Q}[G])^\times$$

while if $\xi \in \zeta(\mathbb{C}_p[G])^\times$, then

$$\delta_{G,p}(\xi) \in K_0(\Lambda_p, \mathbb{Q}_p[G]) \iff \xi \in \zeta(\mathbb{Q}_p[G])^\times.$$

We finally recall that, for any isomorphism $j : \mathbb{C} \cong \mathbb{C}_p$, there is an induced composite homomorphism of abelian groups

$$j_{G,*} : K_0\big(\Lambda, \mathbb{R}[G]\big) \to K_0\big(\Lambda, \mathbb{C}[G]\big) \cong K_0\big(\Lambda, \mathbb{C}_p[G]\big) \to K_0\big(\Lambda_p, \mathbb{C}_p[G]\big)$$

(where the first and third arrows are induced by the inclusions $\mathbb{R}[G] \subset \mathbb{C}[G]$ and $\Lambda \subset \Lambda_p$ respectively). We also write $j_* : \zeta(\mathbb{C}[G])^\times \to \zeta(\mathbb{C}_p[G])^\times$ for the obvious map induced by j, and note that it is straightforward to check that one has

$$j_{G,*} \circ \delta_G = \delta_{G,p} \circ j_*.$$

3.2 Relevant results from [11]

For a finite group Γ we write $D(\mathbb{Z}_p[\Gamma])$ for the derived category of complexes of left $\mathbb{Z}_p[\Gamma]$-modules. We also write $D^p(\mathbb{Z}_p[\Gamma])$ for the full triangulated subcategory of $D(\mathbb{Z}_p[\Gamma])$ comprising complexes that are perfect (that is, isomorphic in $D(\mathbb{Z}_p[\Gamma])$ to a bounded complex of finitely generated projective $\mathbb{Z}_p[\Gamma]$-modules).

We write $T_p(A)$ for the p-adic Tate module of the dual abelian variety A^t (sic!). With $\Sigma_k(F)$ denoting the set of k-embeddings $F \hookrightarrow k^c$ and $Y_{F/k,p} := \prod_{\Sigma_k(F)} \mathbb{Z}_p$ we set

$$T_{p,F}(A) := Y_{F/k,p} \otimes_{\mathbb{Z}_p} T_p(A),$$

where G acts on the first factor in the obvious way and G_k acts diagonally.

For a given isomorphism $j : \mathbb{C} \to \mathbb{C}_p$, conjecture $\mathrm{C}_{p,j}(A, \mathbb{Z}[G])$ is formulated in terms of an element $R\Omega_j\big(h^1(A_F)(1), \mathbb{Z}[G]\big)$ of $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$ that is constructed (unconditionally under the assumed validity of hypothesis (g)) via the formalism of virtual objects from the compactly supported étale cohomology complex $C^{c,\bullet}_{A,F} := R\Gamma_c\left(\mathcal{O}_{k,S}\left[\frac{1}{p}\right], T_{p,F}(A)\right)$ of $T_{p,F}(A)$ on $\mathrm{Spec}\left(\mathcal{O}_{k,S}\left[\frac{1}{p}\right]\right)$ (where we have set $S := S_r \cup S_b$) and the various canonical comparison morphisms between the relevant realisations and cohomology spaces associated to the motive $h^1(A_F)(1)$ (for more details see [9]).

Motivated by work of Bloch and Kato, and in order to isolate the main arithmetic difficulties involved in making $R\Omega_j\big(h^1(A_F)(1), \mathbb{Z}[G]\big)$ explicit, one defines (local and global) finite support cohomology complexes $R\Gamma_f(k_v, T_{p,F}(A))$ (for all $v \in S \cup S_p$) and $R\Gamma_f(k, T_{p,F}(A))$ (see [11, Sec. 3.2]) which fit in a canonical exact triangle in $D(\mathbb{Z}_p[G])$ (see [11, (13)]) of the form

$$C^{loc,\bullet}_{A,F}[-1] \longrightarrow C^{c,\bullet}_{A,F} \longrightarrow C^{f,\bullet}_{A,F} \longrightarrow C^{loc,\bullet}_{A,F}$$

with

$$C^{loc,\bullet}_{A,F} := \bigoplus_{v \in S_\infty} R\Gamma(k_v, T_{p,F}(A)) \oplus \bigoplus_{v \in S \cup S_p} R\Gamma_f(k_v, T_{p,F}(A))$$

and

$$C^{f,\bullet}_{A,F} := R\Gamma_f(k, T_{p,F}(A)).$$

However, if p divides $|G|$ it is not clear that it is always possible to define complexes $R\Gamma_f(k_v, T_{p,F}(A))$ so that $C^{f,\bullet}_{A,F}$ and $C^{loc,\bullet}_{A,F}$ are perfect. For that reason one has to introduce additional hypotheses (see e.g. [11, Lemma 3.1]) that do not occur in the formulation of conjecture $\mathrm{C}_{p,j}(A, \mathbb{Z}[G])$ using compactly supported cohomology.

On the other hand, under the assumptions of [11] the complex $R\Gamma_f(k, T_{p,F}(A))$ is perfect and acyclic outside degrees one and two. Moreover, there are canonical identifications of $H^1_f(k, T_{p,F}(A))$ and $H^2_f(k, T_{p,F}(A))$ with $A^t(F)_p$ and $\mathrm{Sel}_p(A_F)^\vee$ respectively (see [11, Lemma 3.1]). Hence the $\mathbb{C}$-linear extension of the Néron-Tate

height pairing of A defined relative to the field F induces a canonical trivialisation

$$\begin{aligned}\lambda_{A,F}^{\mathrm{NT},j}\colon \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^1\big(C_{A,F}^{f,\bullet}\big) &\cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} A^t(F)_p \\ &\cong \mathbb{C}_p \otimes_{\mathbb{C},j} (\mathbb{C} \otimes_{\mathbb{Z}} A^t(F)) \cong \mathbb{C}_p \otimes_{\mathbb{C},j} \mathrm{Hom}_{\mathbb{C}}\big(\mathbb{C} \otimes_{\mathbb{Z}} A(F), \mathbb{C}\big) \\ &\cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{\mathbb{Z}_p}\big(A(F)_p, \mathbb{Z}_p\big) \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^2\big(C_{A,F}^{f,\bullet}\big).\end{aligned}$$

To recall the statement of [11, Prop. 3.2] we let $\lambda_{A,F}^{\mathrm{exp},j}$ be the trivialisation of $C_{A,F}^{loc,\bullet}$ defined in loc.cit.. By unwinding the definition of $R\Omega_j\big(h^1(A_{/F})(1), \mathbb{Z}[G]\big)$ and relating the general formalism of virtual objects to the explicit refined Euler characteristics we work with, the equality

$$\begin{aligned}R\Omega_j\big(h^1(A_{/F})(1), \mathbb{Z}[G]\big) = \chi_{G,p}\left(C_{A,F}^{f,\bullet}, (\lambda_{A,F}^{\mathrm{NT},j})^{-1}\right) - \chi_{G,p}\left(C_{A,F}^{loc,\bullet}, \lambda_{A,F}^{\mathrm{exp},j}\right) \\ + \sum_{v \in S \cup S_p} \delta_{G,p}\big(L_v(A, F/k)\big)\end{aligned}$$

in $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$ is obtained, where the $L_v(A, F/k)$ are the 'local Euler factors' defined in the statement of [11, Prop. 3.2].

In [11, Th. 3.3], $\chi_{G,p}(C_{A,F}^{loc,\bullet}, \lambda_{A,F}^{\mathrm{exp},j})$ is subsequently explicitly computed (under their running hypothesis (a) - (i)). Consequently, it is finally proved in [11, Th. 4.1] that

$$j_{G,*}\big(T\Omega\big(h^1(A_{/F})(1), \mathbb{Z}[G]\big)\big) = \delta_{G,p}\left(j_*(\mathcal{L}_{A,F/k}^*)\right) + \chi_{G,p}\left(C_{A,F}^{f,\bullet}, (\lambda_{A,F}^{\mathrm{NT},j})^{-1}\right), \quad (10)$$

where $T\Omega\big(h^1(A_{/F})(1), \mathbb{Z}[G]\big)$ is the element defined in [9, Conj. 4], or equivalently that conjecture $\mathrm{C}_{p,j}(A, \mathbb{Z}[G])$ is valid if and only if

$$\delta_{G,p}\left(j_*(\mathcal{L}_{A,F/k}^*)\right) = -\chi_{G,p}\left(C_{A,F}^{f,\bullet}, (\lambda_{A,F}^{\mathrm{NT},j})^{-1}\right). \quad (11)$$

In order to prove our results stated in Section 2 we must therefore compute the refined Euler characteristic $\chi_{G,p}\left(C_{A,F}^{f,\bullet}, (\lambda_{A,F}^{\mathrm{NT},j})^{-1}\right)$ in terms of the heights of the chosen sets of points $\mathcal{P}$ and $\mathcal{P}^t$.

4 The proofs

4.1 The proof of Proposition 2.2

In this subsection we will prove Proposition 2.2. The existence of global points $P_{(t,j)}$ and $P_{(t,j)}^t$ such that (1) holds is then an immediate consequence of Roiter's lemma (see [12, (31.6)]). Our proof is modelled along the lines of proof of [11, Th. 2.6].

To ease notation we set $H^1 := H^1(C_{A,F}^{f,\bullet}) = A^t(F)_p$ and $H^2 := H^2(C_{A,F}^{f,\bullet}) = \mathrm{Sel}_p(A_F)^\vee$. We recall that, for any intermediate field L of F/k, we may and will use

the relevant canonical short exact sequence of the form (3) to identify $(\mathrm{Sel}_p(A_L)^\vee)_{\mathrm{tor}}$ with $Ш_p(A_L)^\vee$ and $(\mathrm{Sel}_p(A_L)^\vee)_{\mathrm{tf}}$ with $A(L)_p^*$.

By Lemma 4.1 below we know that $(H^2)_J$ is torsionfree for all $1 \neq J \leq G$. The second arrow in the natural exact sequence

$$\left(H^2_{\mathrm{tor}}\right)_J \longrightarrow \left(H^2\right)_J \longrightarrow \left(H^2_{\mathrm{tf}}\right)_J \longrightarrow 0$$

is therefore bijective and hence the modules $(H^2)_J \simeq (H^2_{\mathrm{tf}})_J$ are both torsion-free. By the definition of Tate cohomology, we have that the finite groups $\widehat{H}^{-1}(J, H^2)$ and $\widehat{H}^{-1}(J, H^2_{\mathrm{tf}})$ identify with (finite) submodules of $(H^2)_J \simeq (H^2_{\mathrm{tf}})_J$ and therefore both vanish.

Furthermore, since the complex $C^{f,\bullet}_{A,F}$ is perfect and acyclic outside degrees 1 and 2, for each subgroup J of G the group $\widehat{H}^1(J, H^1)$ is isomorphic to $\widehat{H}^{-1}(J, H^2)$ and hence also vanishes. In addition, since G is cyclic, the Tate cohomology of each J is periodic of order 2 and so $\widehat{H}^{-1}(J, H^1)$ also vanishes.

We next note that, since G is a p-group, hypothesis (a) implies that $A^t(F)_p = H^1$ is torsion-free.

We now apply the main result [22, Th. 2.4] of Yakovlev to see that both $A^t(F)_p = H^1$ and $A(F)_p^* = H^2_{\mathrm{tf}}$ are $\mathbb{Z}_p[G]$-permutation modules, that is, that there exist isomorphisms of the form

$$A^t(F)_p \simeq \bigoplus_{J \leq G} \mathbb{Z}_p[G/J]^{<r_J>}, \quad A(F)_p^* \simeq \bigoplus_{J \leq G} \mathbb{Z}_p[G/J]^{<s_J>}$$

for some sets of non-negative integers $\{r_J\}$ and $\{s_J\}$. But the Néron-Tate height pairing induces an isomorphism of $\mathbb{C}_p[G]$-modules between $\mathbb{C}_p \otimes_{\mathbb{Z}_p} A^t(F)_p$ and $\mathbb{C}_p \otimes_{\mathbb{Z}_p} A(F)_p^*$ and so by rank considerations we find that $r_J = s_J =: m_J$ for every J. Finally, it is easy to see that the $\mathbb{Z}_p$-linear dual of a permutation module is again a permutation module of the same shape. Therefore the canonical isomorphism $A(F)_p^{**} \simeq A(F)_p$ shows that one also has that

$$A(F)_p \simeq \bigoplus_{J \leq G} \mathbb{Z}_p[G/J]^{<m_J>}.$$

□

To complete the proof of Proposition 2.2 we finally require the following result:

Lemma 4.1. *For each $1 \neq J \leq G$ the module of J-coinvariants $(\mathrm{Sel}_p(A_F)^\vee)_J$ is $\mathbb{Z}_p$-torsionfree.*

Proof. Under the validity of our hypotheses, Greenberg proves in [17, Prop. 5.6] that the natural restriction homomorphism $\mathrm{res}_F^{F^J} : \mathrm{Sel}_p(A_{F^J}) \to \mathrm{Sel}_p(A_F)^J$ is bijective for every J. It follows that there is a canonical composite isomorphism of the form

$$(\mathrm{Sel}_p(A_F)^\vee))_J \cong \left(\mathrm{Sel}_p(A_F)^J)\right)^\vee \cong \mathrm{Sel}_p(A_{F^J})^\vee.$$

The result follows now from hypothesis (h) since we identify $(\mathrm{Sel}_p(A_{F^J})^\vee)_{\mathrm{tor}}$ with $Ш_p(A_{F^J})$. □

4.2 The proof of Theorem 2.9

Recall that in addition to our running hypothesis (a) - (h) we also assume that $Ш_p(A_F) = 0$. In particular, we identify $\mathrm{Sel}_p(A_F)^\vee$ with $A(F)_p^*$ via the canonical map in (3).

We fix an isomorphism of fields $j : \mathbb{C} \to \mathbb{C}_p$. From (11) and the discussion in §3.1 it is clear that it will be enough to show that

$$-\chi_{G,p}\left(C_{A,F}^{f,\bullet}, (\lambda_{A,F}^{\mathrm{NT},j})^{-1}\right) = \delta_{G,p}\left(\sum_{\psi\in\widehat{G}} j(\lambda_\psi(\mathcal{P},\mathcal{P}^t))\epsilon_\psi(\Phi)\delta_\psi e_\psi\right) \tag{12}$$

(we recall that, since we have assumed the validity of $\mathrm{C}(A,\mathbb{Q}[G])$, one actually has that the validity of $\mathrm{C}_{p,j}(A,\mathbb{Z}[G])$ is equivalent to the validity of $\mathrm{C}_p(A,\mathbb{Z}[G])$).

We begin by defining, for every pair (s,i), an element $P_{(s,i)}^* \in A(F)_p^*$ by setting, for every pair (t,j) and element τ of G,

$$P_{(s,i)}^*(\tau P_{(t,j)}) = \begin{cases} 1, & \text{if } s=t, i=j \text{ and } \tau \in H_s \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

Lemma 4.2. *$A(F)_p^* = \bigoplus_{(s,i)} \mathbb{Z}_p[G/H_s]P_{(s,i)}^*$ with each summand $\mathbb{Z}_p[G/H_s]P_{(s,i)}^*$ isomorphic to $\mathbb{Z}_p[G/H_s]$.*

Proof. If $\gamma \in G$, then

$$\begin{aligned} & \left(\gamma P_{(s,i)}^*\right)\left(\tau P_{(t,j)}\right) = P_{(s,i)}^*(\gamma^{-1}\tau P_{(t,j)}) = 1 \\ \iff \quad & s=t, i=j \text{ and } \gamma \equiv \tau (\mathrm{mod}\ H_s). \end{aligned} \tag{14}$$

Hence we have $\gamma P_{(s,i)}^* = P_{(s,i)}^*$ for $\gamma \in H_s$. Moreover, it easily follows that the maps $\gamma P_{(s,i)}^*$ with $\gamma \in G/H_s$ form a $\mathbb{Z}_p$-basis of $A(F)_p^*$ (actually the $\mathbb{Z}_p$-dual basis of $\tau P_{(t,j)}$ with $\tau \in G/H_t$). □

We now proceed to fix an explicit 2-syzygy of the form (4). For this purpose, we first recall that $H_t = \langle \sigma^{p^t} \rangle$. For each pair (t,j) corresponding to the subgroup H_t of G and $j \in [m_t]$ we hence have a 2-extension

$$0 \longrightarrow \mathbb{Z}_p[G/H_t] \xrightarrow{\iota_t} \mathbb{Z}_p[G] \xrightarrow{\sigma^{p^t}-1} \mathbb{Z}_p[G] \xrightarrow{\pi_{t,j}} \mathbb{Z}_p[G/H_t]P_{(t,j)}^* \longrightarrow 0.$$

In this sequence we let ι_t denote the (well-defined) map which sends the image of an element $x \in \mathbb{Z}_p[G]$ under the natural surjection $\mathbb{Z}_p[G] \to \mathbb{Z}_p[G/H_t]$ to the element $\mathrm{Tr}_{H_t}x$ of $\mathbb{Z}_p[G]$, while $\pi_{t,j}$ sends the element 1 of $\mathbb{Z}_p[G]$ to the element $P_{(t,j)}^* \in A(F)_p^*$ defined in (13). Lemma 4.2 then implies that, summing over all pairs (t,j) we obtain a 2-extension

$$0 \longrightarrow M \xrightarrow{\iota} F^0 \xrightarrow{\Theta} F^1 \xrightarrow{\pi} A(F)_p^* \longrightarrow 0.$$

with

$$\begin{aligned} F^0 = F^1 = X &:= \bigoplus_{(t,j)} \mathbb{Z}_p[G], \\ M &:= \bigoplus_{(t,j)} \mathbb{Z}_p[G/H_t]. \end{aligned}$$

We now recall that we have a canonical isomorphism

$$\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(A(F)^*_p, A^t(F)_p) \simeq \mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)/\iota_*(\mathrm{Hom}_{\mathbb{Z}_p[G]}(F^0, A^t(F)_p))$$

under which an element ϕ of $\mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)$ corresponds to the element $\epsilon(\phi)$ of $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(A(F)^*_p, A^t(F)_p)$ which has the bottom row of the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\iota} & X & \xrightarrow{\Theta} & X & \xrightarrow{\pi} & A(F)^*_p & \longrightarrow & 0 \\ & & {\scriptstyle\phi}\downarrow & & \downarrow & & \| & & \| & & \\ 0 & \longrightarrow & A^t(F)_p & \longrightarrow & X(\phi) & \longrightarrow & F^1 & \xrightarrow{\pi} & A(F)^*_p & \longrightarrow & 0, \end{array} \tag{15}$$

as a representative. In this diagram $X(\phi)$ is defined as the push-out of ι and ϕ. We now proceed to prove that, when considering perfect elements $\epsilon(\phi)$ of $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(A(F)^*_p, A^t(F)_p)$, one may without loss of generality restrict attention to a special class of elements ϕ of $\mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)$.

Lemma 4.3. *For all subgroups J of G one has*

(i) $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G], \mathbb{Z}_p[G/J]) = 0$,

(ii) $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G/J], \mathbb{Z}_p[G]) = 0$

Proof. Part (i) is clear. Concerning (ii), we first note that since $\mathbb{Z}_p[G/J]$ is $\mathbb{Z}_p$-torsion-free, there is an isomorphism of the form

$$\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G/J], \mathbb{Z}_p[G]) \cong H^2(G, \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[G/J], \mathbb{Z}_p[G])).$$

Since the Tate cohomology of G is periodic of order 2, the latter group is in turn isomorphic to $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[G/J], \mathbb{Z}_p[G]))$. An explicit computation now shows that the latter group vanishes, as required to complete the proof of the lemma. □

Lemma 4.3 now implies that we can without loss of generality restrict attention to those elements ϕ of $\mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)$ which satisfy (P2) and, in addition, by the argument of [3, Lemma 4.3], which are furthermore injective.

Lemma 4.4. *Suppose that $\phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)$ has all of the properties described in the previous paragraph. Then the element $\epsilon(\phi)$ of $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(A(F)^*_p, A^t(F)_p)$ is perfect if and only if ϕ is an isomorphism.*

Proof. The fact that ϕ restricts to send an element $x_{(n,j)}$ of the (n,j)-th direct summand $\mathbb{Z}_p[G]$ to $x_{(n,j)}P^t_{(n,j)}$ immediately implies that $\mathrm{cok}(\phi) = \mathrm{cok}(\phi')$ where

$$\phi' : \bigoplus_{(t,j),t<n} \mathbb{Z}_p[G/H_t] \to \bigoplus_{(t,j),t<n} \mathbb{Z}_p[G/H_t]P^t_{(t,j)}$$

is the map obtained by restriction of ϕ. Since ϕ is injective, the commutative diagram (15) implies that the 2-extension $\epsilon(\phi)$ is perfect if and only $\mathrm{cok}(\phi) = \mathrm{cok}(\phi')$ is cohomologically trivial. Note that H_{n-1} clearly acts trivially on $\mathrm{cok}(\phi')$. So, if $\mathrm{cok}(\phi')$ is cohomologically trivial, then

$$\mathrm{cok}(\phi')/p\,\mathrm{cok}(\phi') = \widehat{H}^0(H_{n-1}, \mathrm{cok}(\phi')) = 0.$$

It then follows that $\mathrm{cok}(\phi')$ must itself vanish, as required. □

We henceforth fix $\Phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(M, A^t(F)_p)$ representing the element $\delta_{A,F,p} \in \mathrm{Ext}^2_{\mathbb{Z}_p[G]}(\mathrm{Sel}_p(A_F)^\vee, A^t(F)_p)$ which is specified by $R\Gamma_f(k, T_{p,F}(A))$. Recall that by our current assumption $Ш_p(A_F) = 0$ we identify $\mathrm{Sel}_p(A_F)^\vee$ and $A(F)^*_p$. By Lemma 4.3 and 4.4 we may and will assume that Φ is an isomorphism and furthermore that the matrix defined in (5) is of the form (6).

Having justified our choice of homomorphism Φ, we now proceed to compute the term $-\chi_{G,p}\left(C^{f,\bullet}_{A,F}, (\lambda^{\mathrm{NT},j}_{A,F})^{-1}\right)$ that occurs in (12) via a generalisation of the computations done in [3, Sec. 4]. For brevity, given any $\mathbb{Z}_p[G]$-module N, resp. $\mathbb{Z}_p[G]$-homomorphism h, we set $N_{\mathbb{C}_p} := \mathbb{C}_p \otimes_{\mathbb{Z}_p} N$, resp. $h_{\mathbb{C}_p} := \mathbb{C}_p \otimes_{\mathbb{Z}_p} h$.

For any choice of respective splittings

$$s_1 : X_{\mathbb{C}_p} \to M_{\mathbb{C}_p} \oplus \mathrm{im}(\Theta)_{\mathbb{C}_p}$$

and

$$s_2 : X_{\mathbb{C}_p} \to \ker(\pi)_{\mathbb{C}_p} \oplus A(F)^*_{\mathbb{C}_p}$$

of the short exact sequences induced by scalar extension of

$$0 \to M \xrightarrow{\iota} X \xrightarrow{\Theta} \mathrm{im}(\Theta) \to 0$$

and

$$0 \to \ker(\pi) \to X \xrightarrow{\pi} A(F)^*_p \to 0$$

respectively, we write $\langle \lambda^{\mathrm{NT},j}_{A,F} \circ \Phi_{\mathbb{C}_p}, \Theta, s_1, s_2\rangle$ for the composite $\mathbb{C}_p[G]$-automorphism of $X_{\mathbb{C}_p}$ given by

$$\begin{aligned} X_{\mathbb{C}_p} &\xrightarrow{s_1} M_{\mathbb{C}_p} \oplus \mathrm{im}(\Theta)_{\mathbb{C}_p} \\ &\xrightarrow{(\Phi_{\mathbb{C}_p}, id)} A^t(F)_{\mathbb{C}_p} \oplus \mathrm{im}(\Theta)_{\mathbb{C}_p} \\ &\xrightarrow{(\lambda^{\mathrm{NT},j}_{A,F}, id)} A(F)^*_{\mathbb{C}_p} \oplus \mathrm{im}(\Theta)_{\mathbb{C}_p} \\ &= A(F)^*_{\mathbb{C}_p} \oplus \ker(\pi)_{\mathbb{C}_p} \\ &\xrightarrow{s_2^{-1}} X_{\mathbb{C}_p}. \end{aligned}$$

We also write $X^\bullet$ for the perfect complex of $\mathbb{Z}_p[G]$ modules $X \xrightarrow{\Theta} X$ with the first term placed in degree 1 and the modules $H^1(X^\bullet)$ and $H^2(X^\bullet)$ identified with M and $A(F)_p^*$ respectively via the top row of diagram (15). An explicit computation then shows that, independently of the choice of splittings s_1 and s_2, one has that

$$\begin{aligned}-\chi_{G,p}\left(C^{f,\bullet}_{A,F}, (\lambda^{\mathrm{NT},j}_{A,F})^{-1}\right) =& -\chi_{G,p}\left(X^\bullet, \Phi_{\mathbb{C}_p}^{-1}\circ(\lambda^{\mathrm{NT},j}_{A,F})^{-1}\right)\\ =&\delta_{G,p}\left(\det_{\mathbb{C}_p[G]}(\langle \lambda^{\mathrm{NT},j}_{A,F}\circ\Phi_{\mathbb{C}_p}, \Theta, s_1, s_2\rangle)\right).\end{aligned}$$

The proof of equality (12), and hence of Theorem 2.9, will thus be achieved by the following explicit computation.

Proposition 4.5. *There exist splittings s_1 and s_2 as above with the property that* $\det_{\mathbb{C}_p[G]}(\langle \lambda^{\mathrm{NT},j}_{A,F}\circ\Phi_{\mathbb{C}_p}, \Theta, s_1, s_2\rangle) = \sum_{\psi\in\widehat{G}} j(\lambda_\psi(\mathcal{P},\mathcal{P}^t))\epsilon_\psi(\Phi)\delta_\psi e_\psi$.

Proof. Let $\{w_{(s,i)} : s = 0,\dots,n, i\in[m_s]\}$ be the standard basis of X. For each pair (s,i) we write $W_s = W_{(s,i)}$ for the kernel of the canonical map

$$\mathbb{C}_p[G] \longrightarrow \mathbb{C}_p[G/H_s],$$

so that $W_s = (\sigma^{p^s}-1)\mathbb{C}_p[G] = (1-e_{H_s})\mathbb{C}_p[G]$. We then have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{C}_p[G/H_s] & \xrightarrow{\iota_s} & \mathbb{C}_p[G] & \xrightarrow{\sigma^{p^s}-1} & \mathbb{C}_p[G] & \xrightarrow{\pi_{s,i}} & \mathbb{C}_p[G/H_s]P^*_{(s,i)} \longrightarrow 0 \\ & & & & & \searrow \quad \nearrow & & & \\ & & & & & W_s & & & \end{array} \tag{16}$$

with furthermore $\bigoplus_{(s,i)} W_{(s,i)}$ equal to $\mathrm{im}(\Theta)_{\mathbb{C}_p} = \ker(\pi)_{\mathbb{C}_p}$. We now fix the required splittings s_1 and s_2 by summing over all pairs (s,i) the splittings of the short exact sequences in (16) given by

$$\mathbb{C}_p[G] \longrightarrow \mathbb{C}_p[G/H_s]\oplus W_s, \quad 1 \mapsto \left(\frac{1}{|H_s|}, \sigma^{p^s}-1\right) \tag{17}$$

and

$$\mathbb{C}_p[G] \longrightarrow \mathbb{C}_p[G/H_s]P^*_{(s,i)}\oplus W_s, \quad 1 \mapsto \left(P^*_{(s,i)}, 1-e_{H_s}\right) \tag{18}$$

respectively. Note that for the inverse map in (18) we have $(P^*_{(s,i)}, 0) \mapsto e_{H_s}$ and $(0, \sigma^{p^s}-1) \mapsto \sigma^{p^s}-1$.

After these preparations we proceed to compute the matrix $\Lambda^{\mathrm{NT}}(\Phi)$ which represents $\langle \lambda^{\mathrm{NT},j}_{A,F}\circ\Phi_{\mathbb{C}_p}, \Theta, s_1, s_2\rangle$ with respect to the fixed $\mathbb{C}_p[G]$-basis $\{w_{(s,i)}\}$ of $X_{\mathbb{C}_p}$. From (17) and (5) it follows easily that the composite of s_1 and $(\Phi_{\mathbb{C}_p}, id)$ maps $w_{(s,i)}$ to

$$\left(\frac{1}{|H_s|}\sum_{(t,j)}\Phi_{(t,j),(s,i)}P^t_{(t,j)}, \left(\dots, \sigma^{p^s}-1, \dots\right)\right)$$

in $A^t(F)_{\mathbb{C}_p} \oplus \mathrm{im}(\Theta)_{\mathbb{C}_p} = \left(\bigoplus_{(t,j)} \mathbb{C}_p[G/H_t]P^t_{(t,j)}\right) \oplus \left(\bigoplus_{(t,j)} W_t\right)$ with the only nonzero component in $\oplus_{(t,j)} W_t$ at the (s,i)-spot. By Lemma 4.6 below this is further mapped by $(\lambda^{\mathrm{NT},j}_{A,F}, id)$ to

$$\left(\frac{1}{|H_s|}\sum_{(t,j)} \Phi_{(t,j),(s,i)} \sum_{(u,k)} \left(\sum_{\tau \in G/H_u} j(\langle \tau P_{(u,k)}, P^t_{(t,j)}\rangle_F)\tau e_{H_u}\right) P^*_{(u,k)}, \left(\ldots, \sigma^{p^s}-1, \ldots\right)\right).$$

Rearranging the summation and applying the map s_2^{-1} as described in (18) we obtain

$$\sum_{(u,k)} \left(\frac{1}{|H_s|}\sum_{(t,j)} \Phi_{(t,j),(s,i)} \sum_{\tau \in G/H_u} j(\langle \tau P_{(u,k)}, P^t_{(t,j)}\rangle_F)\tau e_{H_u}\right) w_{(u,k)} + (\sigma^{p^s}-1)w_{(s,i)}.$$

We now fix a character $\psi \in \widehat{G}$. We have that

$$\begin{aligned} & \psi\left(\frac{1}{|H_s|}\sum_{(t,j)} \Phi_{(t,j),(s,i)} \sum_{\tau \in G/H_u} j(\langle \tau P_{(u,k)}, P^t_{(t,j)}\rangle_F)\tau e_{H_u}\right) \\ = & \begin{cases} \frac{1}{|H_s|}\sum_{(t,j)} \Phi_{(t,j),(s,i)} \sum_{\tau \in G/H_u} j(\langle \tau P_{(u,k)}, P^t_{(t,j)})\rangle_F \psi(\tau), & u \geq t_\psi, \\ 0, & u < t_\psi, \end{cases} \end{aligned}$$

while $\psi(\sigma^{p^s}-1)$ is equal to 0 if and only if $s \geq t_\psi$.

We immediately obtain that

$$\det\left(\psi\left(\Lambda^{\mathrm{NT}}(\Phi)\right)\right) = j(\lambda_\psi(\mathcal{P},\mathcal{P}^t)) \cdot \varepsilon_\psi(\Phi) \cdot \delta_\psi,$$

as required. □

We finally provide the relevant Lemma used in the course of the above proof.

Lemma 4.6.

$$\lambda^{\mathrm{NT},j}_{A,F}\left(P^t_{(t,j)}\right) = \sum_{(u,k)} \left(\sum_{\tau \in G/H_u} j(\langle \tau P_{(u,k)}, P^t_{(t,j)}\rangle_F)\tau e_{H_u}\right) P^*_{(u,k)}.$$

Proof. We recall that $\lambda^{\mathrm{NT},j}_{A,F}$ is induced by $\langle\ ,\ \rangle_F \colon A(F) \times A^t(F) \longrightarrow \mathbb{C}$. For $P^t \in A^t(F)$ we explicitly have $\lambda^{\mathrm{NT},j}_{A,F}(P^t) = j(\langle\ , P^t\rangle_F)$. Let $f \in A(F)^*_p$ denote the map defined by the right hand side of the equation in Lemma (4.6). From (14) we immdiately see that $e_{H_u}P^*_{(u,k)} = P^*_{(u,k)}$. For each pair (v,l) and $\gamma \in G/H_v$ we hence obtain

$$\begin{aligned} f(\gamma P_{(v,l)}) &= \sum_{(u,k)} \sum_{\tau \in G/H_u} j(\langle \tau P_{(u,k)}, P^t_{(t,j)}\rangle_F)\left(\tau P^*_{(u,k)}\right)\left(\gamma P_{(v,l)}\right) \\ &= j(\langle \gamma P_{(v,l)}, P^t_{(t,j)}\rangle_F) \\ &= \left(\lambda^{\mathrm{NT},j}_{A,F}(P^t_{(t,j)})\right)(\gamma P_{(v,l)}). \end{aligned}$$

□

4.3 The proof of Theorem 2.6

Since the validity of Theorem 2.6 does not rely in any crucial manner on the fact that the extension F/k is cyclic or even abelian, we elect to use notations throughout this proof that would be appropriate to studying conjecture $C(A, \mathbb{Q}[G])$ for any finite Galois extension F/k of group G.

We set $M = h^1(A_F)(1)$ and recall that $C(A, \mathbb{Q}[G])$ is formulated in [9, Conj. 5] as an equality of the form

$$[\Xi(M), \vartheta_\infty] + \delta(\mathrm{nr}^{-1}_{\mathbb{R}[G]}(\lambda L^*(M, 0))) = 0$$

in $\pi_0(V(\mathbb{Q}[G], \mathbb{R}[G]))$. For the readers convenience we briefly recall the notation used in [9]:

- For any unital associative ring we let $V(R)$ denote the (Picard) category of virtual objects over R. We also write $(X, Y) \mapsto X \cdot Y$ for the product and $\mathbf{1}_R$ for the unit object in $V(R)$. If $\mathcal{P}_0$ denotes the Picard category with unique object $\mathbf{1}_{\mathcal{P}_0}$ and $\mathrm{Aut}_{\mathcal{P}_0}(\mathbf{1}_{\mathcal{P}_0}) = 0$, then

  $$V(\mathbb{Q}[G], \mathbb{R}[G]) := V(\mathbb{Q}[G]) \times_{V(\mathbb{R}[G])} \mathcal{P}_0$$

  is the fibre product associated to the canonical functors $V(\mathbb{Q}[G]) \to V(\mathbb{R}[G])$ and $\mathcal{P}_0 \to V(\mathbb{R}[G])$.

- The leading term $L^*(M, 0)$ at $s = 0$ of the $\mathbb{Q}[G]$-equivariant motivic L-function of M is explicitly given by $\sum_{\chi \in \mathrm{Ir}(G)} e_\chi L^*(A, \check{\chi}, 1)$, and $\lambda \in \zeta(\mathbb{Q}[G])^\times$ is any element with the property that $\lambda L^*(M, 0)$ belongs to $\mathrm{im}(\mathrm{nr}_{\mathbb{R}[G]})$. The map

  $$\delta : K_1(\mathbb{R}[G]) \to \pi_0(V(\mathbb{Q}[G], \mathbb{R}[G]))$$

  is obtained by composing the map $\beta : \pi_1(V(\mathbb{R}[G])) \to \pi_0(V(\mathbb{Q}[G], \mathbb{R}[G]))$ arising from the Mayer-Vietoris exact sequence of the fibre product with the isomorphism $\iota_{\mathbb{R}} : K_1(\mathbb{R}[G]) \to \pi_1(V(\mathbb{R}[G]))$ which sends an element of $K_1(\mathbb{R}[G])$ represented by an automorphism ϕ of a finitely generated $\mathbb{R}[G]$-module P to $[\phi]_{\mathbb{R}[G]} \cdot \mathrm{id}([P]^{-1}_{\mathbb{R}[G]})$. Here $[-]_{\mathbb{R}[G]}$ denotes the universal determinant functor on the category of finitely generated $\mathbb{R}[G]$-modules and isomorphisms of such.There exists furthermore an analogous isomorphism $\iota_{\mathbb{Q}}$ for the category of finitely generated $\mathbb{Q}[G]$-modules.

- We set

  $$\Xi(M) := [\mathbb{Q} \otimes_{\mathbb{Z}} A^t(F)]^{-1}_{\mathbb{Q}[G]} \cdot [\mathbb{Q} \otimes_{\mathbb{Z}} A(F)^*]_{\mathbb{Q}[G]} \cdot \left(\prod_{v \in S^F_\infty} [H^0(F_v, H_v(M))]^{-1}_{\mathbb{Q}[G]} \right) \cdot [H_{\mathrm{dR}}(M)/F^0]_{\mathbb{Q}[G]}.$$

We refer the reader to [9, (29)] for a more detailed definition of $\Xi(M)$. In order to define ϑ_∞, we first let once again $\lambda^{NT}_{A,F} : \mathbb{R} \otimes_{\mathbb{Z}} A^t(F) \to \mathbb{R} \otimes_{\mathbb{Z}} A(F)^*$ denote the canonical isomorphism induced by the Néron-Tate height pairing and

$$\alpha_{A,F} : \mathbb{R} \otimes_{\mathbb{Q}} \bigoplus_{v \in S^F_\infty} H^0(F_v, H_v(M)) \to \mathbb{R} \otimes_{\mathbb{Q}} H_{\mathrm{dR}}(M)/F^0$$

denote the canonical period isomorphism described by Deligne in [13] (see also [9, (16)]). We finally define ϑ_∞ to be the canonical isomorphism in $V(\mathbb{R}[G])$ from $\mathbb{R}[G] \otimes_{\mathbb{Q}[G]} \Xi(A)$ to $\mathbf{1}_{\mathbb{R}[G]}$ that is induced by $[(\lambda^{NT}_{A,F})^{-1}]_{\mathbb{R}[G]}$ and $[\alpha^{-1}_{A,F}]_{\mathbb{R}[G]}$.

In order to state certain useful preliminary results, we now note that the $\mathbb{Q}[G]$-modules $X := \mathbb{Q} \otimes_{\mathbb{Z}} A^t(F)$ and $Y := \mathbb{Q} \otimes_{\mathbb{Z}} A(F)^*$, resp. $Z := \bigoplus_{v \in S^F_\infty} H^0(F_v, H_v(M))$ and $W := H_{\mathrm{dR}}(M)/F^0$, are isomorphic (as a consequence, for instance, of [1, p. 110]) and hence, since $\mathbb{Q}[G]$ is semisimple, there exist $\mathbb{Q}[G]$-modules M and N with the property that both $X \oplus M \cong Y \oplus M$ and $Z \oplus N \cong W \oplus N$ are free $\mathbb{Q}[G]$-modules. In the sequel we (choose bases and so) fix identifications of $X \oplus M$, $Y \oplus M$, $Z \oplus N$ and $W \oplus N$ with direct sums of copies of $\mathbb{Q}[G]$ and hence regard $\lambda^{NT}_{A,F} \oplus \mathrm{id}_{\mathbb{R} \otimes_{\mathbb{Q}} M}$ and $\alpha_{A,F} \oplus \mathrm{id}_{\mathbb{R} \otimes_{\mathbb{Q}} N}$ as elements of $K_1(\mathbb{R}[G])$. In order to prove Theorem 2.6 we require the following results, which are straightforward to deduce from the proof of Lemma 4.6 and the proof of [11, Lemma 3.5] respectively and are furthermore clearly independent of our choice of fixed identifications.

Lemma 4.7. $\mathrm{nr}_{\mathbb{R}[G]}(\lambda^{NT}_{A,F} \oplus \mathrm{id}_{\mathbb{R} \otimes_{\mathbb{Q}} M}) / \sum_{\chi \in \mathrm{Ir}(G)} e_\chi \lambda_\chi(\mathcal{P}, \mathcal{P}^t) \in \zeta(\mathbb{Q}[G])^\times$.

Lemma 4.8. $\mathrm{nr}_{\mathbb{R}[G]}(\alpha_{A,F} \oplus \mathrm{id}_{\mathbb{R} \otimes_{\mathbb{Q}} N}) / \sum_{\chi \in \mathrm{Ir}(G)} e_\chi \frac{w_\infty(k)^d \cdot \Omega(A/k)}{\tau^*(\mathbb{Q}, \mathrm{ind}^{\mathbb{Q}}_k(\chi))^d} \in \zeta(\mathbb{Q}[G])^\times$.

To proceed with the proof of Theorem 2.6, we first consider the following commutative diagram with exact rows:

$$\begin{array}{ccccc} K_1(\mathbb{Q}[G]) & \longrightarrow & K_1(\mathbb{R}[G]) & \xrightarrow{\partial^1} & K_0(\mathbb{Q}[G], \mathbb{R}[G]) \\ {\scriptstyle \iota_{\mathbb{Q}}}\downarrow & & {\scriptstyle \iota_{\mathbb{R}}}\downarrow & & {\scriptstyle c}\downarrow \\ \pi_1(V(\mathbb{Q}[G])) & \longrightarrow & \pi_1(V(\mathbb{R}[G])) & \xrightarrow{\beta} & \pi_0(V(\mathbb{Q}[G], \mathbb{R}[G])). \end{array} \tag{19}$$

Here c sends an element $[P, g, Q]$ to

$$[[P]_{\mathbb{Q}[G]} \cdot [Q]^{-1}_{\mathbb{Q}[G]}, [g]_{\mathbb{R}[G]} \cdot \mathrm{id}([\mathbb{R} \otimes_{\mathbb{Q}} Q]^{-1}_{\mathbb{R}[G]})].$$

The commutativity of this diagram is easy to check given the explicit nature of all maps involved, and it is also straightforward to prove that c is bijective (see for example the proof of [9, Prop. 2.5]). We hence have that $C(A, \mathbb{Q}[G])$ is valid if and only if in $K_0(\mathbb{Q}[G], \mathbb{R}[G])$ one has

$$\begin{aligned} 0 =& c^{-1}([\Xi(M), \vartheta_\infty] + \delta(\mathrm{nr}^{-1}_{\mathbb{R}[G]}(\lambda L^*(M, 0)))) \\ =& -[Z, \alpha_{A,F}, W] - [X, \lambda^{NT}_{A,F}, Y] + \partial^1(\mathrm{nr}^{-1}_{\mathbb{R}[G]}(\lambda L^*(M, 0))). \end{aligned}$$

It hence follows from the exactness of the top row of (19) that $C(A, \mathbb{Q}[G])$ is valid if and only if

$$-[\alpha_{A,F} \oplus \mathrm{id}_{\mathbb{R}\otimes_{\mathbb{Q}}N}] - [\lambda^{NT}_{A,F} \oplus \mathrm{id}_{\mathbb{R}\otimes_{\mathbb{Q}}M}] + \mathrm{nr}^{-1}_{\mathbb{R}[G]}(\lambda L^*(M,0)) \in \mathrm{im}(K_1(\mathbb{Q}[G])).$$

It is now straightforward to check that the latter condition is equivalent to the containment

$$L^*(M,0)/(\mathrm{nr}_{\mathbb{R}[G]}(\alpha_{A,F} \oplus \mathrm{id}_{\mathbb{R}\otimes_{\mathbb{Q}}N})\mathrm{nr}_{\mathbb{R}[G]}(\lambda^{NT}_{A,F} \oplus \mathrm{id}_{\mathbb{R}\otimes_{\mathbb{Q}}M})) \in \zeta(\mathbb{Q}[G])^\times.$$

By Lemmas 4.7 and 4.8, combined with the fact that the Euler factors involved in the truncation of each of the leading terms $L^*_{S_r}(A, \check{\psi}, 1)$ live by definition in $\zeta(\mathbb{Q}[G])^\times$, it is hence clear that the validity of $C(A, \mathbb{Q}[G])$ is equivalent to the containment

$$\sum_{\psi\in\widehat{G}} \frac{\mathcal{L}^*_\psi}{\lambda_\psi(\mathcal{P}, \mathcal{P}^t)} e_\psi \in \zeta(\mathbb{Q}[G])^\times.$$

By [2, Lem. 2.9] this containment is equivalent to the explicit condition described in Theorem 2.6.

4.4 The proof of Theorem 2.8

We assume now that $\mathrm{C}(A, \mathbb{Q}[G])$ is valid and proceed to prove the explicit interpretation of $C_p(A, \mathcal{M})$ claimed in Theorem 2.8 in any such situation. We begin by noting that, for any fixed isomorphism of fields $j : \mathbb{C} \to \mathbb{C}_p$, the respective maps $j_{G,*}$ restrict to give the vertical arrows in a natural commutative diagram with exact rows of the form

$$\begin{array}{ccccc} K_0(\mathbb{Z}[G], \mathbb{Q}[G])_{\mathrm{tor}} & \longrightarrow & K_0(\mathbb{Z}[G], \mathbb{Q}[G]) & \xrightarrow{\mu} & K_0(\mathcal{M}, \mathbb{Q}[G]) \\ {\scriptstyle j_{G,*}}\downarrow & & {\scriptstyle j_{G,*}}\downarrow & & {\scriptstyle j_{G,*}}\downarrow \\ K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G])_{\mathrm{tor}} & \longrightarrow & K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G]) & \xrightarrow{\mu_p} & K_0(\mathcal{M}_p, \mathbb{Q}_p[G]). \end{array} \tag{20}$$

We note that the exactness of the rows follows from [9, Lemma 11]. We now proceed to prove several useful results.

Lemma 4.9. *$C_p(A, \mathcal{M})$ holds if and only if $j_{G,*}\big(T\Omega\big(h^1(A_F)(1), \mathbb{Z}[G]\big)\big)$ belongs to $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G])_{\mathrm{tor}}$.*

Proof. The equality $T\Omega\big(h^1(A_F)(1), \mathcal{M}\big) = \mu\big(T\Omega\big(h^1(A_F)(1), \mathbb{Z}[G]\big)\big)$ proved in [9, Th. 4.1] combines with the commutativity of the right-hand square of diagram (20) to imply that

$$j_{G,*}\big(T\Omega\big(h^1(A_F)(1), \mathcal{M}\big)\big) = \mu_p\big(j_{G,*}\big(T\Omega\big(h^1(A_F)(1), \mathbb{Z}[G]\big)\big)\big).$$

The exactness of the bottom row of diagram (20) thus completes the proof. □

Lemma 4.10. *$C_p(A,\mathcal{M})$ holds if and only if $\sum_{\psi\in\widehat{G}} \frac{\mathcal{L}^*_\psi}{j(\lambda_\psi(\mathcal{P},\mathcal{P}^t))\epsilon_\psi(\Phi)\delta_\psi} e_\psi \in \mathcal{M}_p^\times$.*

Proof. Lemma 4.9 combines with equalities (10) and (12) to imply that $\mathrm{C}_p(A,\mathcal{M})$ holds if and only if

$$\mu_p\left(\delta_{G,p}\left(\sum_{\psi\in\widehat{G}} \frac{\mathcal{L}^*_\psi}{j(\lambda_\psi(\mathcal{P},\mathcal{P}^t))\epsilon_\psi(\Phi)\delta_\psi} e_\psi\right)\right) = 0.$$

We next note that the respective maps $\delta_{G,p}$ induce vertical (bijective) arrows in a commutative diagram of the form

$$\begin{array}{ccc} \mathbb{Q}_p[G]^\times/\mathbb{Z}_p[G]^\times & \longrightarrow & \mathbb{Q}_p[G]^\times/\mathcal{M}_p^\times \\ \downarrow & & \downarrow \\ K_0(\mathbb{Z}_p[G],\mathbb{Q}_p[G]) & \xrightarrow{\mu_p} & K_0(\mathcal{M}_p,\mathbb{Q}_p[G]) \end{array}$$

.

This completes the proof of the Lemma. □

Lemma 4.11. *$\varepsilon_\psi(\Phi) \in \mathbb{Z}_p[\psi]^\times$.*

Proof. The map $\Phi\otimes\mathcal{M}_p\colon M\otimes_{\mathbb{Z}_p[G]}\mathcal{M}_p \longrightarrow A^t(F)_p\otimes_{\mathbb{Z}_p[G]}\mathcal{M}_p$ is an isomorphism of $\mathcal{M}_p$-modules. Since $\mathcal{M}_p$ contains the $\mathbb{Q}_p[G]$-rational idempotents,

$$\Phi\otimes\mathbb{Z}_p[\psi]\colon M\otimes_{\mathbb{Z}_p[G]}\mathbb{Z}_p[\psi] \longrightarrow A^t(F)_p\otimes_{\mathbb{Z}_p[G]}\mathbb{Z}_p[\psi]$$

is an isomorphism of $\mathbb{Z}_p[\psi]$-modules. It is easy to see that $\Phi\otimes\mathbb{Z}_p[\psi]$ is represented by $\psi\left(\Phi_{t_\psi}\right)$. □

We now proceed to give the proof of Theorem 2.8.

The equivalence of (i) and (iv) follows directly upon combining Lemmas 4.10 and 4.11.

Furthermore it is straightforward to compute the valuation of each element δ_ψ. One has $v_{\mathfrak{p}_\psi}(\delta_\psi) = b_\psi$ with b_ψ defined as in Theorem 2.8, and hence (iii) and (iv) are clearly equivalent.

In order to prove the equivalence of (i) and (ii), we will use (a special case of) a general fact which we now describe. If H is any subgroup of G, we write $\rho^G_H\colon K_0(\mathbb{Z}_p[G],\mathbb{Q}_p[G]) \longrightarrow K_0(\mathbb{Z}_p[H],\mathbb{Q}_p[H])$ for the natural restriction map and $q^H_0\colon K_0(\mathbb{Z}_p[H],\mathbb{Q}_p[H]) \longrightarrow K_0(\mathbb{Z}_p,\mathbb{Q}_p)$ for the natural map induced by sending an element $[P,\phi,Q]$ of $K_0(\mathbb{Z}_p[H],\mathbb{Q}_p[H])$ to the element $[P^H,\phi^H,Q^H]$ of $K_0(\mathbb{Z}_p,\mathbb{Q}_p)$. By [6, Thm. 4.1] one then has that

$$K_0(\mathbb{Z}_p[G],\mathbb{Q}_p[G])_{\mathrm{tor}} = \bigcap_{H\leq G} \ker(q^H_0\circ\rho^G_H). \tag{21}$$

The functoriality properties of the element $T\Omega\big(h^1(A_F)(1),\mathbb{Z}[G]\big)$ with respect to the maps ρ_H^G and q_0^H proved in [9, Prop. 4.1] then imply that, for any subgroup H of G, one has that

$$(q_0^H \circ \rho_H^G)\big(j_{G,*}\big(T\Omega\big(h^1(A_F)(1),\mathbb{Z}[G]\big)\big)\big) = j_{0,*}\big(T\Omega\big(h^1(A_{F^H})(1),\mathbb{Z}\big)\big),$$

and so Lemma 4.9 combines with (21) to imply that $\mathrm{C}_p(A,\mathcal{M})$ holds if and only if, for every intermediate field L of F/k, the element $j_{G_{L/L},*}\big(T\Omega\big(h^1(A_L)(1),\mathbb{Z}\big)\big)$ vanishes, that is, if and only if the p-part of the eTNC holds for the pair $\big(h^1(A_L)(1),\mathbb{Z}\big)$. Noting that it is easy to check that the set of data $(A/L, L/L, p)$ satisfies all the hypotheses of Theorem 2.9 for any such field L (see for instance [11, Lem. 2.10] for a proof of a more general assertion), all that is left to do in order to prove the equivalence of (i) and (ii) is to apply Theorem 2.9. Indeed, any choice of $\mathbb{Z}$-bases $\{Q_i\}$ and $\{R_j\}$ of $A(L)$ and $A^t(L)$ respectively satisfy condition (1) for the set of data $(A/L, L/L, p)$, while an explicit computation proves that $\frac{\tau^*(\mathbb{Q},\mathrm{ind}_L^{\mathbb{Q}}(\mathbf{1}_{G_{L/L}}))}{w_\infty(L)} = \sqrt{|d_L|}$.

4.5 The proof of Corollary 2.11

For brevity we set

$$\lambda_\psi := \lambda_\psi(\mathcal{P},\mathcal{P}^t), \quad \epsilon_\psi := \epsilon_\psi(\Phi), \quad u := \sum_{\psi\in\widehat{G}} \frac{\mathcal{L}_\psi^*}{\lambda_\psi\epsilon_\psi\delta_\psi} e_\psi.$$

By Theorem 2.9 the validity of $C_p(A,\mathbb{Z}[G])$ is equivalent to the containment $u \in \mathbb{Z}_p[G]^\times$, which we assume holds throughout the proof. We also let $\varepsilon\colon \mathbb{Z}_p[G] \longrightarrow \mathbb{Z}_p$ denote the augmentation map.

We begin by noting that claim (ii) is just the $\psi = \mathbf{1}_G$ special case of Lemma 4.11, and proceed now to deduce claim (iii) from it. One clearly has that $\mathcal{L}_{\mathbf{1}_G}^*/(\lambda_{\mathbf{1}_G}\epsilon_{\mathbf{1}_G}\delta_{\mathbf{1}_G}) = \varepsilon(u) \in \mathbb{Z}_p^\times$ with $\delta_{\mathbf{1}_G}$ equal by definition to 1, while an explicit computation shows that $\frac{\tau^*(\mathbb{Q},\mathrm{ind}_k^{\mathbb{Q}}(\mathbf{1}_G))}{w_\infty(k)} = (-1)^{|S_r|}\sqrt{|d_k|}$. Claim (ii) therefore indeed implies that

$$v = \mathcal{L}_{\mathbf{1}_G}^*/\lambda_{\mathbf{1}_G} = \varepsilon(u)\cdot\epsilon_{\mathbf{1}_G} = \varepsilon(u)\cdot\epsilon \tag{22}$$

belongs to $\mathbb{Z}_p^\times$, as required.

In order to prove the remaining claims, we first note that, if $\mathrm{rk}(A(F^J)) = |G/J|\mathrm{rk}(A(k))$ for every subgroup J of G, then $h = 0$ by Proposition 2.2 while Φ can be chosen to be the identity matrix by property (P2) and each element δ_ψ is simply equal to 1 by convention. In any such case, claim (i) therefore reduces to the trivial statement $\mathcal{L} = u \in \mathbb{Z}_p[G]$ while claim (iv) simply reads $u \equiv v (\mathrm{mod}\ I_{G,p})$ and follows directly from (22). We therefore may and will henceforth assume that the inequality $\mathrm{rk}(A(F^J)) \leq |G/J|\mathrm{rk}(A(k))$ of Corollary 2.3 is strict for some subgroup J of G. We recall that $H = H_{t_0}$ denotes the smallest non-trivial subgroup of G with the property that $m_H \neq 0$.

In order to prove claim (i), we note first that for each $\psi \in \widehat{G}$ we have

$$\psi|_H \neq 1 \iff \ker(\psi) \subseteq H_{t_0} \text{ and } \ker(\psi) \neq H_{t_0} \iff t_\psi > t_0.$$

From the definitions of ϵ_ψ and δ_ψ one immediately deduces that for each $\psi \in \widehat{G}$ such that $\psi|_H \neq 1$ one has

$$\epsilon_\psi = 1, \quad \delta_\psi = \delta := \prod_{j=0}^{t_0} \left(\sigma^{p^j} - 1\right)^{m_j}.$$

Since $\delta e_\psi = 0$ for each ψ such that $\psi|_H = 1$ we deduce that $\mathcal{L} = \delta u \in \delta\mathbb{Z}_p[G] \subseteq I_{G,p}^h$, as required.

Finally, claim (iv) follows from (22) because u is clearly congruent to $\varepsilon(u) = v/\epsilon$ modulo $I_{G,p}$ and therefore $\mathcal{L} = \delta u$ is congruent to $\delta\frac{v}{\epsilon}$ modulo $I_{G,p}^{h+1}$, as required.

4.6 The proof of Theorem 2.12

We begin by defining a (free) $\mathbb{Z}_p[G]$-submodule

$$P := \bigoplus_{j \in [m_n]} \mathbb{Z}_p[G] P_{(n,j)}^*$$

of $A(F)_p^*$ and then fix, as we may, an injective lift $\kappa\colon P \longrightarrow \mathrm{Sel}_p(A_F)^\vee$ of the inclusion $P \subseteq A(F)_p^*$ through the canonical projection of (3). We also fix, as we may, a representative of the perfect complex $C_{A,F}^{f,\bullet}$ of the form $C^1 \to C^2$ in which both C^1 and C^2 are finitely generated, cohomologically-trivial $\mathbb{Z}_p[G]$-modules. We then obtain a commutative diagram with exact rows and columns of the form

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \bigoplus_j \mathbb{Z}_p[G]P_{(n,j)}^t & = & \bigoplus_j \mathbb{Z}_p[G]P_{(n,j)}^t & \xrightarrow{0} & \mathrm{im}(\kappa) & = & \mathrm{im}(\kappa) & \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\
0 & \to & A^t(F)_p & \to & C^1 & \to & C^2 & \to & \mathrm{Sel}_p(A_F)^\vee & \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\
0 & \to & N & \to & D^1 & \to & D^2 & \to & \mathrm{cok}(\kappa) & \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\
 & & 0 & & 0 & & 0 & & 0 &
\end{array} \tag{23}$$

in which we have set

$$N := \bigoplus_{t<n, j \in [m_t]} \mathbb{Z}_p[G/H_t].$$

The $\mathbb{Z}_p[G]$-modules D^1 and D^2 are finitely generated and cohomologically-trivial, and hence the central arrow of the bottom row of this diagram defines an object $D^\bullet$ of $D^p(\mathbb{Z}_p[G])$ which is acyclic outside of degrees 1 and 2 and has identifications of $H^1(D^\bullet)$ with N and of $H^2(D^\bullet)$ with $\mathrm{cok}(\kappa)$. We analogously define an object $B^\bullet$ of $D^p(\mathbb{Z}_p[G])$ represented by the perfect complex of $\mathbb{Z}_p[G]$-modules

$$\bigoplus_j \mathbb{Z}_p[G]P^t_{(n,j)} \xrightarrow{0} \mathrm{im}(\kappa).$$

Following [10, Sec. 2.1.4] we next define an idempotent $e_N := \sum_{\psi\in\Upsilon_N} e_\psi$ in $\mathbb{Q}_p[G]$ by letting Υ_N be the subset of $\widehat{G}$ comprising characters ψ with the property that $e_\psi(\mathbb{C}_p\otimes_{\mathbb{Z}_p} N) = 0$. For any object $C^\bullet$ of $D^p(\mathbb{Z}_p[G])$ we then obtain an object $e_NC^\bullet := e_N\mathbb{Z}_p[G]\otimes^{\mathbb{L}}_{\mathbb{Z}_p[G]} C^\bullet$ of $D^p(e_N\mathbb{Z}_p[G])$. In particular, the exact triangle represented by diagram (23) induces an exact triangle in $D^p(e_N\mathbb{Z}_p[G])$ of the form

$$e_NB^\bullet \longrightarrow e_NC^{f,\bullet}_{A,F} \longrightarrow e_ND^\bullet \longrightarrow e_NB^\bullet[1]. \tag{24}$$

But $e_ND^\bullet\otimes_{e_N\mathbb{Z}_p[G]} e_N\mathbb{C}_p[G]$ is acyclic and an immediate application of the additivity criterion of [5, Cor. 6.6] to triangle (24) implies that one has

$$\begin{aligned}-\chi_{e_N\mathbb{Z}_p[G],e_N\mathbb{C}_p[G]}(e_ND^\bullet,0) =& -\chi_{e_N\mathbb{Z}_p[G],e_N\mathbb{C}_p[G]}(e_NC^{f,\bullet}_{A,F}, e_N(\lambda^{\mathrm{NT},j}_{A,F})^{-1})\\ &+\chi_{e_N\mathbb{Z}_p[G],e_N\mathbb{C}_p[G]}(e_NB^\bullet,\lambda')\end{aligned} \tag{25}$$

where λ' denotes the canonical isomorphism

$$\begin{aligned}e_N(\mathbb{C}_p\otimes_{\mathbb{Z}_p}\mathrm{im}(\kappa)) =& e_N(\mathbb{C}_p\otimes_{\mathbb{Z}_p}\mathrm{Sel}_p(A_F)^\vee)\\ \xrightarrow{e_N(\lambda^{\mathrm{NT},j}_{A,F})^{-1}}& e_N(\mathbb{C}_p\otimes_{\mathbb{Z}_p}A^t(F)_p) = e_N(\mathbb{C}_p\otimes_{\mathbb{Z}_p}\bigoplus_j\mathbb{Z}_p[G]P^t_{(n,j)}).\end{aligned}$$

If we now write $\varphi : \bigoplus_j \mathbb{Z}_p[G]P^t_{(n,j)} \to \bigoplus_j \mathbb{Z}_p[G]P^*_{(n,j)}$ for the canonical isomorphism that maps an element $P^t_{(n,j)}$ to the element $P^*_{(n,j)}$, then one finds that

$$\begin{aligned}\chi_{e_N\mathbb{Z}_p[G],e_N\mathbb{C}_p[G]}(e_NB^\bullet,\lambda') =& \delta_{e_N\mathbb{Z}_p[G],e_N\mathbb{C}_p[G]}(\det_{e_N\mathbb{C}_p[G]}(\lambda'\circ e_N(\mathbb{C}_p\otimes_{\mathbb{Z}_p}(\kappa\circ\varphi))))\\ =& -\delta_{e_N\mathbb{Z}_p[G],e_N\mathbb{C}_p[G]}(\sum_{\psi\in\Upsilon_N} j(\lambda_\psi(\mathcal{P},\mathcal{P}^t))e_\psi),\end{aligned} \tag{26}$$

where the last equality follows from Lemma 4.6.

The assumed validity of $C_p(A,\mathbb{Z}[G])$ therefore combines via (11) with equalities (25) and (26) to imply that, in the terminology of [10, §2.3.2], the element

$$j_*(\sum_{\psi\in\Upsilon_N}\mathcal{L}^*_\psi\lambda_\psi(\mathcal{P},\mathcal{P}^t)^{-1}e_\psi) = j_*(\mathcal{L})$$

of $e_N\mathbb{C}_p[G]$ is a characteristic element for $e_ND^\bullet$. The result [10, Lem. 2.6] therefore implies that there exists a characteristic element $\mathcal{L}'$ for $D^\bullet$ in $\mathbb{C}_p[G]$ with the property

that $e_N\mathcal{L}' = j_*(\mathcal{L})$. Since $D^\bullet$ is clearly an admissible complex of $\mathbb{Z}_p[G]$-modules (in the terminology of [10, §2.1.1]), the results of [10, Cor. 3.3] therefore imply that the element $j_*(\mathcal{L})$ belongs to the ideal $I_{G,p}^{\tilde{h}}$ of $\mathbb{Z}_p[G]$, with $\tilde{h} := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{cok}(\kappa)_G)$, and furthermore generates $\mathrm{Fitt}_{\mathbb{Z}_p[G]}(\mathrm{cok}(\kappa))$. To proceed with the proof, we first note that it is straightforward to verify that $h = \tilde{h}$. We have hence proved that $j_*(\mathcal{L})$ belongs to $I_{G,p}^h$, as stated in claim (i) of Theorem 2.12. Furthermore, $\Pi := \mathrm{im}(\kappa)$ is clearly a finitely generated, free $\mathbb{Z}_p[G]$-submodule of $\mathrm{Sel}_p(A_F)^\vee$ of maximal rank m_n, and so the fact that the element $j_*(\mathcal{L})$ generates $\mathrm{Fitt}_{\mathbb{Z}_p[G]}(\mathrm{cok}(\kappa))$ proves claim (iii) of Theorem 2.12. To complete the proof, it is enough to note that, since $\mathrm{im}(\kappa)$ is torsion-free, the canonical composite homomorphism

$$Ш_p(A_F)^\vee \xrightarrow{\sim} (\mathrm{Sel}_p(A_F)^\vee)_{\mathrm{tor}} \subseteq \mathrm{Sel}_p(A_F)^\vee \to \mathrm{cok}(\kappa)$$

is injective and hence that one has that

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}(\mathrm{cok}(\kappa)) \subseteq \mathrm{Ann}_{\mathbb{Z}_p[G]}(Ш_p(A_F)^\vee).$$

Recalling finally that the Cassels-Tate pairing induces a canonical isomorphism between $Ш_p(A_F)^\vee$ and $Ш_p(A_F^t)$ completes the proof of claim (ii) and thus of Theorem 2.12.

5 Examples

In this section we gather some evidence, mostly numerical, in support of conjecture $\mathrm{C}_p(A, \mathbb{Z}[G])$. Our aim is to verify statements that would not follow in an straightforward manner from the validity of the Birch and Swinnerton-Dyer conjecture for all intermediate fields of F/k. Because of the equivalence of statements (i) and (ii) in Theorem 2.8 we therefore choose not to focus on presenting evidence for conjecture $\mathrm{C}_p(A, \mathcal{M})$ (although we also used our MAGMA programs to produce numerical evidence for $\mathrm{C}_p(A, \mathcal{M})$ by verifying statement (iii) of Theorem 2.8).

Throughout this section A will always denote an elliptic curve.

5.1 Verifications of conjecture $\mathrm{C}_p(A, \mathbb{Z}[G])$

For the verification of $\mathrm{C}_p(A, \mathbb{Z}[G])$ using Theorem 2.9 it is necessary to have explicit knowledge of a map Φ that represents the extension class $\delta_{A,F,p}$. Whenever $A(F)_p$ is not projective as a $\mathbb{Z}_p[G]$-module we are currently not able to numerically compute Φ, so we only deal with examples in which $A(F)_p$ is projective. To our best knowledge there are currently three instances of theoretical evidence (in situations in which our fixed cyclic extension F/k is not trivial):

- In [4], it is shown that for each elliptic curve $A/\mathbb{Q}$ with $L(A/\mathbb{Q}, 1) \neq 0$ there are infinitely many primes p and for each such prime p infinitely many (cyclic) p-extensions $F/\mathbb{Q}$ such that $\mathrm{C}_p(A, \mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})])$ holds. All of these examples satisfy our hypotheses and are such that $A(F)_p$ vanishes.

- In [11, Th. 5.1], $\mathrm{C}_p(A, \mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})])$ is proved for certain elliptic curves $A/\mathbb{Q}$, where F denotes the Hilbert p-classfield of an imaginary quadratic field k. This result combines with the functoriality properties of the eTNC to imply the validity of $\mathrm{C}_p(A, \mathbb{Z}[\mathrm{Gal}(F/k)])$. In these examples one has that $A(F)_p$ is a free $\mathbb{Z}_p[\mathrm{Gal}(F/k)]$-module of rank one.

- In [11, Cor. 5.5], certain S_3-extensions F/K are considered. Let k and L denote the quadratic and cubic subfield of F/K respectively. Under certain additional assumptions it is then shown that the validity of the Birch and Swinnerton-Dyer conjecture for A over the fields k, K and L implies the validity of $\mathrm{C}_p(A, \mathbb{Z}[\mathrm{Gal}(F/K)])$. Again by functoriality arguments, the validity of $\mathrm{C}_p(A, \mathbb{Z}[\mathrm{Gal}(F/k)])$ follows. We note that the assumptions are such that one again has that $A(F)_p$ is a free $\mathbb{Z}_p[\mathrm{Gal}(F/k)]$-module of rank one.

In the rest of this section we are concerned with numerical evidence. In [2, Sec. 6] there is a list of examples of elliptic curves $A/\mathbb{Q}$ and dihedral extensions $F/\mathbb{Q}$ of order $2p$ for which $\mathrm{C}_p(A, \mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$ is numerically verified. Here the quadratic subfield k is real and $A(F)_p$ vanishes. Again by functoriality arguments we obtain examples where $\mathrm{C}_p(A, \mathbb{Z}_p[\mathrm{Gal}(F/k)])$ is numerically verified. There are two further analogous numerical verifications in dihedral examples in [11, Sec. 5.3], one of degree 10 and one of degree 14, both of them with the property that $A(F)_p$ is a free $\mathbb{Z}_p[\mathrm{Gal}(F/k)]$-module of rank one.

In the following we fix an odd prime p and let q denote a prime such that $q \equiv 1 (\mathrm{mod}\ p)$. We let F denote the unique subfield of $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ of degree p and take k to be $\mathbb{Q}$. For $p \in \{3, 5, 7\}$ and $q < 50$ we went through the list of semistable elliptic curves of rank one and conductor $N < 200$ and checked numerically whether $L(A/\mathbb{Q}, \chi, 1) = 0$ and $L'(A/\mathbb{Q}, \chi, 1) \neq 0$ for a non-trivial character χ of G, and in addition, whether our hypotheses are satisfied. This resulted in a list of 50 examples (27 for $p = 3$, 20 for $p = 5$ and 3 for $p = 7$). In each of these examples we could find a point R such that $A(F)_p = \mathbb{Z}_p[G]R$ and numerically verify conjecture $C_p(A, \mathbb{Z}[G])$.

We now describe in detail an example with $[F : \mathbb{Q}] = 7$. Let A be the elliptic curve

$$E\colon y^2 + xy + y = x^3 + x^2 - 2x.$$

This is the curve 79a1 in Cremona's notation. It is known that $A(\mathbb{Q})$ is free of rank one generated by $P_1 = (0, 0)$ and that $Ш(A_{\mathbb{Q}}) = 0$. Moreover it satisfies the hypotheses used throughout the paper.

We take $p = 7$ and let F be the unique subfield of $\mathbb{Q}(\zeta_{29})$ of degree 7. Explicitly, F is the splitting field of

$$f(x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$$

and we let α denote a root of f. Using the MAGMA command *Points* it is easy to find a point R of infinite order in $A(F) \setminus A(\mathbb{Q})$,

$$R = \left(\frac{1}{17}(31\alpha^6 + 23\alpha^5 - 373\alpha^4 - 135\alpha^3 + 814\alpha^2 + 372\alpha - 86),\right.$$
$$\left.\frac{1}{17}(-35\alpha^6 - 83\alpha^5 + 380\alpha^4 + 771\alpha^3 - 811\alpha^2 - 1321\alpha + 232)\right).$$

By Proposition 2.2 we know that $A(F)_p$ is a permutation module, hence $A(F)_p \simeq \mathbb{Z}_p[G]$. Furthermore, [11, Cor. 2.5] now implies that $Ш_p(A_F) = 0$.

We set $Q_1 := \mathrm{Tr}_{F/\mathbb{Q}}(R) = (\frac{3}{4}, -\frac{3}{8})$ and easily verify that $Q_1 = -4P_1$. We checked numerically that $\mathbb{Z}_p[G]R = A(F)_p$.

Computing numerical approximations to the leading terms using Dokchitser's MAGMA implementation of [14] we obtain the following vector for $\left(\mathcal{L}^*_\chi/\lambda_\chi(\mathcal{P}, \mathcal{P}^t)\right)_{\chi\in\hat{G}}$

$$\begin{aligned}
&(-0.077586206896551724152,\\
&-0.49999999999999999992 + 2.1906431337674115362i,\\
&-0.49999999999999999996 + 0.62698016883135191886i,\\
&-0.49999999999999999998 - 0.24078730940376432202i,\\
&-0.49999999999999999992 - 2.1906431337674115362i,\\
&-0.49999999999999999996 - 0.62698016883135191886i,\\
&-0.49999999999999999998 + 0.24078730940376432202i)
\end{aligned}$$

This is very close to

$$\begin{aligned}
&(-9/116, \zeta_7^3 + \zeta_7^2 + \zeta_7, -\zeta_7^5 - \zeta_7^4 - \zeta_7 - 1, -\zeta_7^5 - \zeta_7^3 - \zeta_7 - 1,\\
&-\zeta_7^3 - \zeta_7^2 - \zeta_7 - 1, \zeta_7^5 + \zeta_7^4 + \zeta_7, \zeta_7^5 + \zeta_7^3 + \zeta_7)
\end{aligned}$$

It is now easy to verify the rationality conjecture $\mathrm{C}(A, \mathbb{Q}[G])$ by the criterion of Theorem 2.6. Moreover, the valuations of $-9/116$ and $\zeta_7^3 + \zeta_7^2 + \zeta_7$ at $\mathfrak{p}_\chi$ are 0, so that by Theorem 2.8 we deduce the validity of $\mathrm{C}_p(A, \mathcal{M})$. Finally, one easily checks that $-9/116 \equiv \zeta_7^3 + \zeta_7^2 + \zeta_7 (\mathrm{mod}\ (1 - \zeta_7))$, so that the element in (7) is actually a unit in $\mathbb{Z}_p[G]$, thus (numerically) proving $\mathrm{C}_p(A, \mathbb{Z}[G])$.

5.2 Evidence in support of conjecture $\mathrm{C}_p(A, \mathbb{Z}[G])$

In this subsection we collect evidence for statements that we have shown to follow from the validity of $\mathrm{C}_p(A, \mathbb{Z}[G])$ and focus on situations in which $A(F)_p$ is not $\mathbb{Z}_p[G]$-projective. In particular, we aim to verify claim (i) of Theorem 2.12. Since we can neither compute the module $Ш_p(A_F)$ nor a map Φ as required, we are not able to verify any other claim of either Corollary 2.11 or Theorem 2.12.

Again we want to focus on evidence which goes beyond implications of the Birch and Swinnerton-Dyer conjecture for A over all intermediate fields of F/k. We assume

the notation of Theorem 2.12, so in particular set $h = \sum_{t<n} m_t$. If $k = \mathbb{Q}$ and $m_n = 0$, then the element $\mathcal{L}$ is essentially the Mazur-Tate modular element (see [20]) and the validity of the Birch and Swinnerton-Dyer conjecture would imply that it belongs to $I_{G,p}$ in the type of situations under consideration. Hence, if $m_n = 0$, we only searched for examples where $h > 1$.

If F/k is cyclic of order p, then $I_{G,p}^h = (\sigma - 1)^h \mathcal{M}_p$ for all $h \geq 1$. Letting u and δ denote the elements defined in the proof of Corollary 2.11 we hence note that, if $\mathrm{C}_p(A, \mathcal{M})$ is valid, then $u \in \mathcal{M}^\times$ and the proof of Corollary 2.11 clearly shows that $\mathcal{L} = \delta u$ is contained in $\delta \mathcal{M}_p = I_{G,p}$. We therefore further restricted our search for interesting examples to cases where $[F : k] = p^n$ with $n \geq 2$.

Restricted by the complexity of the computations and the above considerations we are therefore lead to consider the following types of examples:

(i) $A(F)_p \simeq \mathbb{Z}_p^{m_0} \oplus \mathbb{Z}_p[G/H_1]^{m_1} \oplus \mathbb{Z}_p[G]^{m_2}, \quad [F : \mathbb{Q}] = 3^2,$
$(m_0, m_1, m_2) = (1, 1, 0),$

(ii) $A(F)_p \simeq \mathbb{Z}_p^{m_0} \oplus \mathbb{Z}_p[G/H_1]^{m_1} \oplus \mathbb{Z}_p[G]^{m_2}, \quad [F : \mathbb{Q}] = 3^2,$
$(m_0, m_1, m_2) = (m_0, 0, 0), \quad m_0 \geq 2.$

We note that, whenever $Ш_p(A_F)$ is trivial, the validity of $\mathrm{C}_p(A, \mathbb{Z}[G])$ implies by Corollary 2.11 that h is the exact order of vanishing, i.e., that $\mathcal{L} \in I_{G,p}^h \setminus I_{G,p}^{h+1}$. However, this need not be true if $Ш_p(A_F)$ is non-trivial. In such cases, by Theorem 2.12 (iii), $C_p(A, \mathbb{Z}[G])$ does predict that $\mathcal{L}$ generates the Fitting ideal of $\mathrm{Sel}_p(A_F)^\vee$ since $m_n = 0$ immediately implies $\Pi = 0$.

Let q denote a prime such that $q \equiv 1 (\mathrm{mod}\ 3^2)$. We let F denote the unique subfield of $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ of degree 9 and take k to be $\mathbb{Q}$.

We checked two examples of type (i), namely those given by the pairs $(E, q) \in \{(681c1, 19), (1070a1, 19)\}$. In both cases we were able to find a points P_0 and P_1 such that $A(F)_p = \mathbb{Z}_p P_0 \oplus \mathbb{Z}_p[G/H] P_1$, where H denotes the subgroup of order 3. Each time we numerically found that $Ш_p(A_F) = 0$ (predicted by the Birch and Swinnerton-Dyer conjecture for A over F) and verified that h is the precise order of vanishing, as predicted by Corollary 2.11.

Concerning examples of type (ii) went through the list of semistable elliptic curves of rank 2 and conductor $N < 750$ and produced by numerically checking L-values and derivatives a list of 12 examples satisfying the necessary hypotheses. In each of these examples we had $h = m_0 = 2$ and could numerically verify the containment $\mathcal{L} \in I_{G,p}^2$. Whenever $Ш_p(A_F)$ was trivial we also checked that $\mathcal{L} \notin I_{G,p}^3$.

We finally present one example in detail. Let A be the elliptic curve

$$E\colon y^2 + y = x^3 + x^2 - 2x.$$

This is the curve 389a1 in Cremona's notation. It is known that $A(\mathbb{Q})$ is free of rank two generated by $P_1 = (0, 0)$ and $P_2 = (-1, 1)$ and that $Ш(A_\mathbb{Q}) = 0$. Moreover it satisfies the hypotheses required to apply Theorem 2.12 (see Remark 2.13).

Computing numerical approximations to the leading terms we find that the order of vanishing at each non-trivial character is 0. The rank part of the Birch and Swinnerton-Dyer conjecture therefore predicts that $\mathrm{rk}(A(F)) = 2$. We checked that $\langle P_1, P_2\rangle_{\mathbb{Z}}$ is 3-saturated in $A(F)$ and therefore (conjecturally) conclude that $A(F)_p = \langle P_1, P_2\rangle_{\mathbb{Z}_p} \simeq \mathbb{Z}_p^2$.

The Birch and Swinnerton-Dyer conjecture predicts that $|Ш_p(A_F)| = 81$. We therefore cannot test for the precise order of vanishing.

Computing leading terms, periods and regulators we find the following numerical approximations to $\left(\mathcal{L}_\chi^*/\lambda_\chi(\mathcal{P},\mathcal{P}^t)\right)_{\chi\in\hat{G}}$

$$\begin{aligned}&(-1.243243, 1.500000 + 2.598076i, 1.500000 - 2.598076i,\\ &0.358440 + 2.032818i, 0.286988 - 0.104455i, -3.645429 + 3.058878i,\\ &0.358440 - 2.032818i, 0.286988 + 0.104455i, -3.645429 - 3.058878i).\end{aligned}$$

The actual computation was done with a precision of 30 decimal digits.

This is very close to

$$\begin{aligned}&(-46/37, \quad 3\zeta_3 + 3, \quad -3\zeta_3,\\ &2\zeta_9^3 - \zeta_9^2 + 2\zeta_9, \quad -\zeta_9^4 - 2\zeta_9^3 + 2\zeta_9^2 - 2, \quad \zeta_9^5 + 2\zeta_9^4 + 2\zeta_9^3 + \zeta_9^2,\\ &-2\zeta_9^5 + \zeta_9^4 - 2\zeta_9^3 - 2\zeta_9^2 + \zeta_9 - 2, \quad -\zeta_9^5 - 2\zeta_9^4 + 2\zeta_9^3 - 2\zeta_9, \quad 2\zeta_9^5 - 2\zeta_9^3 - \zeta_9 - 2).\end{aligned}$$

It is now easy to verify the rationality conjecture $\mathrm{C}(A, \mathbb{Q}[G])$ by the criterion of Theorem 2.6. We finally find that

$$\mathcal{L} = -\sigma + 2\sigma 2 - \sigma^3 + 2\sigma^5 - 2\sigma^6 - 2\sigma^7 + 2\sigma^8$$

and easily check that $\mathcal{L} \in I_{G,p}^2$.

References

[1] M. F. Atiyah, C. T. C. Wall, Cohomology of Groups, In: 'Algebraic Number Theory', J. W. S. Cassels, A. Fröhlich (eds.), 94-115 Academic Press, London, 1967.

[2] W. Bley, Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture, Exp. Math. **20** (2011), 426-456.

[3] W. Bley, Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture (part II), Math. Comp. **81** (2012), 1681-1705.

[4] W. Bley, ETNC and modular symbols, Math. Ann. **356** (2013), 179-190.

[5] M. Breuning, D. Burns, Additivity of Euler characteristics in relative algebraic K-groups, Homotopy and Applications **7** (2005), 11-36.

[6] D. Burns, Equivariant Whitehead torsion and refined Euler characteristics, CRM Proceedings and Lecture Notes **36** (2004) 35-59.

[7] D. Burns, Leading terms and values of equivariant motivic L-functions, Pure App. Math. Q. **6** (2010) 83-172 (John Tate Special Issue, Part II).

[8] D. Burns, M. Flach, Motivic L-functions and Galois module structures, Math. Ann. **305** (1996) 65-102.

[9] D. Burns, M. Flach, Tamagawa numbers for motives with (non-commutative) coefficients, Documenta Math. **6** (2001) 501-570.

[10] D. Burns, D. Macias Castillo, Organising matrices for arithmetic complexes, to appear in Int. Math. Res. Notices.

[11] D. Burns, D. Macias Castillo, C. Wuthrich, On Mordell-Weil groups and congruences between derivatives of Hasse-Weil L-functions, submitted for publication.

[12] C. W. Curtis, I. Reiner, Methods of Representation Theory, Vol. I and II, John Wiley and Sons, New York, 1987.

[13] P. Deligne, Valeurs de fonctions L et périodes d'intégrales, Proc. Sym. Pure Math. **33**(2) (1979) 313-346.

[14] T. Dokchitser, Computing special values of motivic L-functions, Experiment. Math. **13**(2) (2004) 137-149.

[15] J. Fearnley, H. Kisilevsky, Critical values of derivatives of twisted elliptic L-functions, Exp. Math. **19** (2010) 149-160.

[16] J. Fearnley, H. Kisilevsky, Critical values of higher derivatives of twisted elliptic L-functions, Exp. Math. **21** (2012) 213-222.

[17] R. Greenberg, Galois Theory for the Selmer Group of an Abelian Variety, Compos. Math. **136** (2003) 255-297.

[18] B. H. Gross, On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication, in: Number theory related to Fermat's last theorem (Cambridge, Mass., 1981), Prog. Math. **26**, Birkhauser Boston, Mass., 1982, pp. 219-236.

[19] J. Martinet, Character theory and Artin L-functions, in: Algebraic number fields (ed. A. Fröhlich), pp. 1-87, Academic Press, London, 1977.

[20] B. Mazur, J. Tate, Refined Conjectures of the Birch and Swinnerton-Dyer type, Duke Math. J. **54** (1987) 711-750.

[21] R. G. Swan, Algebraic K-Theory, Springer, New York (1978).

[22] A. V. Yakovlev, Homological definability of p-adic representations of a ring with power basis, Izvestia A N SSSR, ser. Math. **34** (1970), 321-342. (Russian)

Werner Bley, Mathematisches Institut der Universität München, Theresienstr. 39, 80333 München, Germany, E-mail: bley@math.lmu.de

Daniel Macias Castillo, Instituto de Ciencias Matemáticas (ICMAT), Madrid 28049, Spain, E-mail: daniel.macias@icmat.es