NUMERICAL EVIDENCE FOR THE EQUIVARIANT BIRCH AND SWINNERTON-DYER CONJECTURE

WERNER BLEY

Abstract. Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a finite Galois extension with group G. We write E_K for the base change of E and consider the equivariant Tamagawa number conjecture for the pair $(h^1(E_K)(1), \mathbb{Z}[G])$. This conjecture is an equivariant refinement of the Birch and Swinnerton-Dyer conjecture for E/K. For almost all primes l we derive an explicit formulation of the conjecture which makes it amenable to numerical verifications. We use this to provide convincing numerical evidence in favour of the conjecture.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve and let $K/\mathbb{Q}$ be a finite Galois extension with group $G = \mathrm{Gal}(K/\mathbb{Q})$. We write E_K for the base change of E. We consider the motive $M = h^1(E)(1)$ and regard $M_K := h^0(\mathrm{Spec}(K)) \otimes_{h^0(\mathrm{Spec}(\mathbb{Q}))} M = h^1(E_K)(1)$ as a motive over $\mathbb{Q}$ with a natural left action of the rational group ring $\mathbb{Q}[G]$ via the first factor. We write $\zeta(\mathbb{C}[G])$ for the center of the complex group ring $\mathbb{C}[G]$ and $L(M_K, s)$ for the $\zeta(\mathbb{C}[G])$-valued L-function of M_K which is defined and analytic in $\mathrm{Re}(s) > 1/2$. It is conjectured that $L(M_K, s)$ has meromorphic continuation to all of $\mathbb{C}$. Assuming this conjecture we write $L^*(M_K)$ for the leading term in its Taylor expansion at $s = 0$. To be more explicit, we let $\mathrm{Irr}(G)$ be the set of absolutely irreducible characters of G. For any character χ we write $L(E/\mathbb{Q}, \chi, s)$ for the twisted Hasse-Weil-L-function and $L^*(E/\mathbb{Q}, \chi, 1)$ for the leading term in the Taylor expansion at $s = 1$. The center $\zeta(\mathbb{C}[G])$ is canonically isomorphic to $\prod_{\chi \in \mathrm{Irr}(G)} \mathbb{C}$ and via this identification $L^*(M_K)$ equals $(L^*(E/\mathbb{Q}, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}(G)}$. It is easily shown that $L^*(M_K) \in \zeta(\mathbb{R}[G])^\times$ (see Remark 3.2).

The 'Equivariant Tamagawa Number Conjecture' (for short ETNC) formulated by Burns and Flach in [12] for the pair $(M_K, \mathbb{Z}[G])$ is equivalent to an equality of the form

$$\delta(L^*(M_K)) = \chi(M_K) \tag{1}$$

where δ is a canonical homomorphism from the unit group $\zeta(\mathbb{R}[G])^\times$ to the relative algebraic K-group $K_0(\mathbb{Z}[G], \mathbb{R})$ and $\chi(M_K)$ is a certain Euler characteristic in this relative group constructed from the various motivic cohomology groups, realizations, comparison isomorphisms and regulators associated to M_K and its Kummer dual. We note in passing that the ETNC is formulated in much more generality and that the general formulation is comparatively abstract. Indeed, in our elliptic curve case with $K = \mathbb{Q}$ the ETNC is equivalent to the Birch and Swinnerton-Dyer conjecture (for short BSD). But even this basic fact is not evident and we refer the reader to [24] or [36] for a detailed proof. For the base change of an elliptic curve

Date: November 5, 2010.

the ETNC is an 'equivariant BSD conjecture'. Our main result Proposition 4.4 makes this apparent for arbitrary elliptic curves $E/\mathbb{Q}$ and Galois extensions $K/\mathbb{Q}$.

The aim of this article is to describe an approach for converting the rather involved and abstract conjectural equality (1) into a form which is amenable to numerical computations. In this way we systematically improve upon work of Navilarekallu [30] which originally was the motivation for this manuscript.

As in the classical case of the BSD conjecture the ETNC splits into three parts: an 'equivariant rank conjecture', an 'equivariant rationality conjecture' and an 'equivariant integrality conjecture'.

We will use work of T. Dokchitser [17] to compute numerical approximations to the leading terms of the twisted Hasse-Weil-L-functions and for our general approach we will then usually assume the validity of the rank conjecture. However, in our concrete examples in Section 6 we are often able to deduce the rank conjecture from theoretical results or from an explicit computation of Selmer groups.

We then show how to compute numerical approximations to equivariant periods and to equivariant regulators (provided that we are able to compute the Mordell-Weil group $E(K)$). Combining these computations we are able to numerically verify the rationality conjecture up to the precision of our computations.

From now on we assume the validity of the equivariant rationality conjecture. We note in passing that there are important results in the literature (without being exhaustive we only mention [22, 25, 26, 27, 37] and recent results of Bertolini and Darmon) from which one can possibly deduce the equivariant rationality conjecture provided that the analytic (equivariant) rank is at most 1. This will be part of a further research project. In our numerical examples we mostly consider elliptic curves E defined over $\mathbb{Q}$ and dihedral extensions $K/\mathbb{Q}$ of order $2l$ for an odd prime l such that the Mordell-Weil group $E(K)$ is finite. In this case, where all absolutely irreducible characters are of degree 1 or 2, there is important work of Shimura [33, 34] which probably allows to deduce the equivariant rationality conjecture. In a slightly different situation, namely for subextensions of the false Tate curve tower, Bouganis and V. Dokchitser in [7] successfully apply Shimura's work to deduce algebraicity and Galois equivariance of twisted BSD quotients. Similar arguments will hopefully work in our context.

Furthermore we throughout assume that the Tate-Shafarevic group $Ш(E/K)$ is finite. Again it is possible to deduce finiteness of $Ш(E/K)$ in many examples provided that the analytic rank is at most 1 from the above mentioned work, however, since the aim of this paper is to work out the additional difficulties of the equivariant conjecture, we prefer to make the general assumption that $Ш(E/K)$ is finite.

A further main result of this paper (Corollary 4.7) shows that we can use the computational results from the verification of the rationality conjecture to prove the l-part of the ETNC for all primes l outside a finite set of difficult primes. This finite set contains in most cases the prime divisors of $\#G$ and the prime divisors of $\#Ш(E/K)$. There are two different reasons why we get into difficulties with these primes. Our approach is restricted to the case that certain cohomology groups are perfect $\mathbb{Z}_l[G]$-modules. If $l \nmid \#G$ the ring $\mathbb{Z}_l[G]$ is regular so that this assumption is satisfied for every finitely generated $\mathbb{Z}_l[G]$-module. On the other hand, even if $l \mid \#G$ there are some rare cases where the modules under consideration are perfect, so that we can also produce numerical evidence for these interesting primes (see the examples in Section 6). Primes dividing $\#Ш(E/K)$ are difficult just because we are not able to compute $Ш(E/K)$ as a Galois module (which would be necessary in order to compute Euler characteristics). The situation is even worse because we do not dispose of an algorithm to compute $\#Ш(E/K)$. In order to compute a conjectural candidate for the set of difficult primes we will assume the validity of the classical BSD conjecture for E/K and use it to compute a conjectural value for $\#Ш(E/K)$.

We point out that the equivariant BSD conjecture has far reaching explicit consequences (see [14]) which could not be derived from non-equivariant versions. This may indicate that any theoretical or numerical verification of the equivariant version requires a lot of additional effort. A lot of the additional algorithmic problems are hidden in the algorithms described in [5]. In particular, it can be shown that the ETNC is true if and only if the twisted BSD quotients satisfy certain congruences. For cyclic groups Z_p, dihedral groups D_{2p}, p an odd prime, and the alternating group A_4 we explicitly determine these congruences.

We will illustrate our results in Section 6 with some explicit examples. More examples can be computed using the MAGMA implementations available from

`http://www.mathematik.uni-kassel.de/~bley/pub.html`.

The structure of the paper is as follows.

In the first part of Section 2 we review algebraic preliminaries like determinant functors, categories of virtual objects and the construction of Euler characteristics in these categories. These very abstract concepts are used to formulate the ETNC in [12]. Following an approach of Burns [13] we then make the construction of Euler characteristics more explicit in terms of relative algebraic K-groups and in this way amenable to numerical computations. In particular, in the second part of Section 2 we recall the algorithmic methods of [5] which allow the computation of the relevant relative algebraic K-groups and provide methods to compute in them. For certain small groups we explicity determine the above mentioned congruences.

In Section 3 we describe the ETNC for the base change of an elliptic curve and in Section 4 we then derive our main theoretical results (Proposition 4.4 and Corollary 4.7) which are the basis for our numerical computations. In Section 5 we comment upon the algorithmic aspects of our work and in the final Section 6 we describe several interesting examples in detail. In particular, we have chosen the examples such that we can apply our methods for a prime divisor l of $\#G$ and such that the explicit congruences can be seen.

In future work [1] we will study the l-part of ETNC for elliptic curves E/K and cyclic extensions $K/\mathbb{Q}$ of prime power order l^n, l odd.

Acknowledgements: I am very grateful to David Burns and Tom Fisher for their interest and helpful discussions. I also would like to thank the referee for his careful reading of the manuscript and many valuable comments.

2. Algebraic preliminaries

2.1. **Determinant functors and virtual objects.** Let R by any associative unital ring. Let $\mathrm{PMod}(R)$ denote the category of finitely generated projective R-modules and write $\mathrm{PMod}(R)^\bullet$ for the category of bounded complexes of such modules. We also write $D(R)$ for the derived category of complexes of R-modules and

$D^{perf}(R)$ for the full triangulated subcategory of $D(R)$ consisting of those complexes which are isomorphic in $D(R)$ to an object in $\mathrm{PMod}(R)^\bullet$. These complexes are called perfect. Recall that $C^\bullet$ is perfect if and only if there exists a complex $P^\bullet \in \mathrm{PMod}(R)^\bullet$ and a quasi-isomorphism $P^\bullet \longrightarrow C^\bullet$. We say that an R-module N is perfect if the complex $N[0]$ belongs to $D^{perf}(R)$.

Our main reference for determinant functors, Picard categories and virtual objects is [12]. Let $V(R)$ denote the Picard category of virtual objects associated to $\mathrm{PMod}(R)$ and write $[\cdot]_R$ for the universal determinant functor

$$[\cdot]_R \colon (\mathrm{PMod}(R), is) \longrightarrow V(R),$$

where $(\mathrm{PMod}(R), is)$ denotes the subcategory of all isomorphisms in $\mathrm{PMod}(R)$. By [12, Prop. 2.1] this functor extends to a functor

$$[\cdot]_R \colon \big(D^{perf}(R), is\big) \longrightarrow V(R).$$

We recall that $V(R)$ is equipped with a canonical bifunctor $(L, M) \mapsto LM$. We fix a unit object $\mathbf{1}_R$ and for each object L an inverse L^{-1} with an isomorphism $LL^{-1} \simeq \mathbf{1}_R$. Each element of $V(R)$ is of the form $[P]_R[Q]_R^{-1}$ for modules $P, Q \in \mathrm{PMod}(R)$. Furthermore, $[P]_R$ and $[Q]_R$ are isomorphic in $V(R)$ if and only if their classes in $K_0(R)$ coincide.

For any Picard category $\mathcal{P}$ we define $\pi_0(\mathcal{P})$ to be the group of isomorphism classes of objects of $\mathcal{P}$ and set $\pi_1(\mathcal{P}) := \mathrm{Aut}_{\mathcal{P}}(\mathbf{1}_{\mathcal{P}})$. The groups $\pi_0(V(R))$ and $\pi_1(V(R))$ are naturally isomorphic to $K_0(R)$ and $K_1(R)$, respectively.

Let A be a finite dimensional semisimple $\mathbb{Q}$-algebra. For any extension field F of $\mathbb{Q}$ we put $A_F := A \otimes_{\mathbb{Q}} F$ and abbreviate $A_p := A \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Let $\mathcal{A} \subseteq A$ be a $\mathbb{Z}$-order and set

$$\mathcal{A}_p := \mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \quad \hat{\mathcal{A}} := \mathcal{A} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}} \simeq \prod_p \mathcal{A}_p, \quad \hat{A} := A \otimes_{\mathbb{Z}} \hat{\mathbb{Z}} \simeq \prod_p A_p.$$

For $L \in \mathrm{PMod}(\mathcal{A})$ we set

$$L_p := L \otimes_{\mathbb{Z}} \mathbb{Z}_p, \quad L_{\mathbb{Q}} := L \otimes_{\mathbb{Z}} \mathbb{Q}, \quad L_F := L \otimes_{\mathbb{Z}} F.$$

We set $\mathbb{V}(\mathcal{A}) := V(\hat{\mathcal{A}}) \times_{V(\hat{A})} V(A)$ and recall that elements in $\mathbb{V}(\mathcal{A})$ are of the form $(\hat{X}, Y, \hat{\theta})$ with $\hat{X} \in V(\hat{\mathcal{A}}), Y \in V(A)$ and $\hat{\theta} : \hat{X} \otimes_{\hat{\mathcal{A}}} \hat{A} \xrightarrow{\simeq} Y \otimes_A \hat{A}$ an isomorphism in $V(\hat{A})$. Note that the tensor in this context is the functor between categories of virtual objects induced by the tensor functor on the level of modules by the universal property [12, (2.3),f]. Note also that we can identify $\hat{X}$ with $\prod_p X_p \in \prod_p V(\mathcal{A}_p)$ where $X_p := \hat{X} \otimes_{\hat{\mathcal{A}}} \mathcal{A}_p \in V(\mathcal{A}_p)$.

There is a natural monoidal functor $V(\mathcal{A}) \longrightarrow \mathbb{V}(\mathcal{A})$ induced by

$$[L]_{\mathcal{A}} \mapsto \left(\prod_p [L_p]_{\mathcal{A}_p}, [L_{\mathbb{Q}}]_A, \prod_p [\theta_p] \right),$$

where $\theta_p \colon L_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = L \otimes_{\mathbb{Z}} \mathbb{Q}_p \xrightarrow{id} L \otimes_{\mathbb{Z}} \mathbb{Q}_p = L_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is the natural map.

Let $\mathcal{P}_0$ be the Picard category with unique object $\mathbf{1}_{\mathcal{P}_0}$ and $\mathrm{Aut}_{\mathcal{P}_0}(\mathbf{1}_{\mathcal{P}_0}) = 0$. Following [12] we define $\mathbb{V}(\mathcal{A}, F)$ to be the fibre product category $\mathbb{V}(\mathcal{A}) \times_{V(A_F)} \mathcal{P}_0$. Explicitly, elements in $\mathbb{V}(\mathcal{A}, F)$ are given by triples

$$\left(\left(\hat{X}, Y, \hat{\theta} \right), \mathbf{1}_{\mathcal{P}_0}, \theta_\infty \right),$$

where

$$
\begin{aligned}
&\hat{X} \in V(\hat{A}),\\
&Y \in V(A),\\
&\hat{\theta} : \hat{X} \otimes_{\hat{A}} \hat{A} \xrightarrow{\simeq} Y \otimes_A \hat{A},\\
&\theta_\infty : Y \otimes_A A_F \xrightarrow{\simeq} \mathbf{1}_{A_F}.
\end{aligned} \tag{2}
$$

We usually omit $\mathbf{1}_{\mathcal{P}_0}$ in the notation.

By [12, Prop. 2.5] one has a canonical isomorphism

$$\iota_{\mathcal{A},F} \colon \pi_0\mathbb{V}(\mathcal{A},F) \simeq K_0(\mathcal{A},F),$$

where $K_0(\mathcal{A},F)$ is the relative algebraic K-group as defined in [35, page 215]. Following the proof of [12, Prop. 2.5] we explicitly describe the inverse of $\iota_{\mathcal{A},F}$. Let $[P,\varphi,Q]$ be an element in $K_0(\mathcal{A},F)$ with $P,Q \in \mathrm{PMod}(\mathcal{A})$ and an isomorphism $\varphi : P \otimes_{\mathcal{A}} A_F \longrightarrow Q \otimes_{\mathcal{A}} A_F$ of A_F-modules. Then

$$\iota^{-1}_{\mathcal{A},F}\left([P,\varphi,Q]\right) = \left(\left(\prod_p [P_p]_{\mathcal{A}_p}[Q_p]^{-1}_{\mathcal{A}_p}, [P \otimes_{\mathcal{A}} A]_A [Q \otimes_{\mathcal{A}} A]^{-1}_A, \prod_p \theta_p\right), \varphi_{triv}\right)$$

where each θ_p is the canonical map and φ_{triv} is the composite

$$[P \otimes_{\mathcal{A}} A_F]_{A_F}[Q \otimes_{\mathcal{A}} A_F]^{-1}_{A_F} \longrightarrow [Q \otimes_{\mathcal{A}} A_F]_{A_F}[Q \otimes_{\mathcal{A}} A_F]^{-1}_{A_F} \longrightarrow \mathbf{1}_{A_F}.$$

Here the first isomorphism is induced by φ.

If we set $V(\mathcal{A},F) := V(\mathcal{A}) \times_{V(A_F)} \mathcal{P}_0$, then the functor $V(\mathcal{A}) \longrightarrow \mathbb{V}(\mathcal{A})$ induces a canonical functor $V(\mathcal{A},F) \longrightarrow \mathbb{V}(\mathcal{A},F)$ and a homomorphism

$$\pi_0 V(\mathcal{A},F) \longrightarrow \pi_0\mathbb{V}(\mathcal{A},F),$$

and hence a homomorphism $\pi_0 V(\mathcal{A},F) \longrightarrow K_0(\mathcal{A},F)$ which we also denote by $\iota_{\mathcal{A},F}$. In the same way we obtain isomorphisms (see again [12, Prop. 2.5])

$$\iota_{\mathcal{A}_p,\mathbb{Q}_p} \colon \pi_0 V(\mathcal{A}_p,\mathbb{Q}_p) \simeq K_0(\mathcal{A}_p,\mathbb{Q}_p),$$

Given data as in (2) we therefore obtain an element

$$\iota_{\mathcal{A},F}\left(\left(\left(\hat{X},Y,\hat{\theta}\right),\theta_\infty\right)\right) \in K_0(\mathcal{A},F).$$

In the context of the ETNC we are, in addition, given an element $\mathcal{L}^* \in \zeta(A_F)^\times$. There is a canonical commutative diagram of the form

$$
\begin{tikzcd}
K_1(\mathcal{A}) \arrow[r] & K_1(A_F) \arrow[r, "\partial^1_{\mathcal{A},F}"] & K_0(\mathcal{A},F) \arrow[r, "\partial^0_{\mathcal{A},F}"] & K_0(\mathcal{A}) \arrow[r] & K_0(A_F) \\
K_1(\mathcal{A}) \arrow[r] \arrow[u, equal] & K_1(A) \arrow[r, "\partial^1_{\mathcal{A},\mathbb{Q}}"] \arrow[u, hook] & K_0(\mathcal{A},\mathbb{Q}) \arrow[r, "\partial^0_{\mathcal{A},\mathbb{Q}}"] \arrow[u, hook] & K_0(\mathcal{A}) \arrow[r] \arrow[u, equal] & K_0(A) \arrow[u]
\end{tikzcd} \tag{3}
$$

If R is a finite dimensional semisimple algebra over either a global field or a local field, then we have an injective reduced norm map

$$\mathrm{Nrd}_R : K_1(R) \longrightarrow \zeta(R)^\times.$$

If G is a finite group, then $\mathrm{Nrd}_{\mathbb{R}[G]}$ is in general not surjective. However, by [12, Sec. 4.2] there always exists a canonical 'extended boundary homomorphism'

$$\delta \colon \zeta(\mathbb{R}[G])^\times \longrightarrow K_0(\mathbb{Z}[G],\mathbb{R})$$

such that $\delta \circ \mathrm{Nrd}_{\mathbb{R}[G]} = \partial^1_{\mathbb{Z}[G],\mathbb{R}}$. See [10, Sec. 2.1.2] for a conceptual description of δ.

The conjectures we wish to consider in this paper are essentially of the form

$$T\Omega := \iota_{\mathbb{Z}[G],\mathbb{R}}\left(\left(\left(\hat{X}, Y, \hat{\theta}\right), \theta_\infty\right)\right) - \delta(\mathcal{L}^*) = 0$$

in $K_0(\mathbb{Z}[G], \mathbb{R})$. In the sequel we set $\mathcal{A} = \mathbb{Z}[G]$, $A = \mathbb{Q}[G]$ and $F = \mathbb{R}$.

For our computational purposes, in particular to be able to apply the results and algorithms of [5], we need to reinterprete this construction in terms of explicit elements of $K_0(\mathcal{A}, F)$. Here we essentially follow the approach of Burns in [13]. For any bounded complex $P^\bullet$ we define objects P^{all}, P^{ev} and P^{od} by

$$P^{all} = \bigoplus_{i\in\mathbb{Z}} P^i, \quad P^{ev} = \bigoplus_{i \text{ even}} P^i, \quad P^{od} = \bigoplus_{i \text{ odd}} P^i.$$

We write $Z^\bullet(P^\bullet), B^\bullet(P^\bullet)$ and $H^\bullet(P^\bullet)$ for the complexes of cycles, boundaries and cohomology of $P^\bullet$, each with zero differentials.

In arithmetical applications we often have the following data

$$\begin{array}{lll} & (a) & Y^{ev}, Y^{od} \in \mathrm{PMod}(A) \text{ together with an } A_F-\text{isomorphism} \\ & & Y^{ev} \otimes_{\mathbb{Q}} F \xrightarrow{\theta_F} Y^{od} \otimes_{\mathbb{Q}} F. \\ & (b) & X_p^\bullet \in \mathrm{PMod}(\mathcal{A}_p)^\bullet \text{ together with isomorphisms} \\ (4) & & H^{ev}(X_p^\bullet) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\theta_p^{ev}} Y^{ev} \otimes_{\mathbb{Q}} \mathbb{Q}_p, \\ & & H^{od}(X_p^\bullet) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\theta_p^{od}} Y^{od} \otimes_{\mathbb{Q}} \mathbb{Q}_p. \\ & (c) & \mathcal{L}^* \in \zeta(A_F)^\times. \end{array}$$

This data is related to the data given in (2) in the following way

$$\begin{array}{rcl} \hat{X} & = & \prod_p [X_p^\bullet]_{\mathcal{A}_p}, \\ Y & = & [Y^{ev}]_A [Y^{od}]_A^{-1}, \\ \theta_\infty : Y \otimes_A A_F & = & [Y^{ev} \otimes_A A_F]_{A_F} [Y^{od} \otimes_A A_F]_{A_F}^{-1} \\ & \simeq & [Y^{od} \otimes_A A_F]_{A_F} [Y^{od} \otimes_A A_F]_{A_F}^{-1} \\ & \simeq & \mathbf{1}_{A_F}, \text{ with the first isomorphism induced by } \theta_F \\ \theta_p : X_p & = & \left[X_p^\bullet \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\right]_{A_p} \\ & \stackrel{\alpha_1}{\simeq} & [H^{ev}(X_p^\bullet \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)]_{A_p} [H^{od}(X_p^\bullet \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)]_{A_p}^{-1} \\ & \stackrel{\alpha_2}{\simeq} & [Y^{ev} \otimes_{\mathbb{Q}} \mathbb{Q}_p)]_{A_p} [Y^{od} \otimes_{\mathbb{Q}} \mathbb{Q}_p)]_{A_p}^{-1} \\ & = & [Y \otimes_{\mathbb{Q}} \mathbb{Q}_p]_{A_p}. \end{array}$$

Here α_1 is the canonical isomorphism of [12, Prop. 2.1e] and α_2 is induced by θ_p^{ev} and θ_p^{od}.

Let $\mathbb{C}_p$ denote the completion of a fixed algebraic closure of $\mathbb{Q}_p$. For every prime p and every homomorphism $j : \mathbb{R} \to \mathbb{C}_p$ we obtain induced maps $j_* : K_0(\mathbb{Z}[G], \mathbb{R}) \to K_0(\mathbb{Z}_p[G], \mathbb{C}_p)$ and $j_* : \zeta(\mathbb{R}[G])^\times \longrightarrow \zeta(\mathbb{C}_p[G])^\times$. We fix p and j and consider the map $\theta_p' : X_p^{ev} \otimes_{\mathbb{Z}_p} \mathbb{C}_p \longrightarrow X_p^{od} \otimes_{\mathbb{Z}_p} \mathbb{C}_p$ defined by

$$\begin{aligned}
X_p^{ev} \otimes_{\mathbb{Z}_p} \mathbb{C}_p &\overset{\beta_1}{\simeq} \big(H^{ev}(X_p^\bullet) \otimes_{\mathbb{Z}_p} \mathbb{C}_p\big) \oplus \big(B^{all}(X_p^\bullet) \otimes_{\mathbb{Z}_p} \mathbb{C}_p\big) \\
&\overset{\beta_2}{\simeq} \big(Y^{ev} \otimes_{\mathbb{Z}_p} \mathbb{C}_p\big) \oplus \big(B^{all}(X_p^\bullet) \otimes_{\mathbb{Z}_p} \mathbb{C}_p\big) \\
&\overset{\beta_3}{\simeq} \big(Y^{od} \otimes_{\mathbb{Z}_p} \mathbb{C}_p\big) \oplus \big(B^{all}(X_p^\bullet) \otimes_{\mathbb{Z}_p} \mathbb{C}_p\big) \\
&\overset{\beta_4}{\simeq} \big(H^{od}(X_p^\bullet) \otimes_{\mathbb{Z}_p} \mathbb{C}_p\big) \oplus \big(B^{all}(X_p^\bullet) \otimes_{\mathbb{Z}_p} \mathbb{C}_p\big) \\
&\overset{\beta_5}{\simeq} X_p^{od} \otimes_{\mathbb{Z}_p} \mathbb{C}_p.
\end{aligned}$$

The isomorphisms β_1 and β_5 are induced by choosing splittings of the tautological exact sequences

$$\begin{gathered}
0 \longrightarrow Z^i(X_p^\bullet \otimes_{\mathbb{Q}_p} \mathbb{C}_p) \longrightarrow X_p^i \otimes_{\mathbb{Q}_p} \mathbb{C}_p \longrightarrow B^{i+1}(X_p^\bullet \otimes_{\mathbb{Q}_p} \mathbb{C}_p) \longrightarrow 0 \\
0 \longrightarrow B^i(X_p^\bullet \otimes_{\mathbb{Q}_p} \mathbb{C}_p) \longrightarrow Z^i(X_p^\bullet \otimes_{\mathbb{Q}_p} \mathbb{C}_p) \longrightarrow H^i(X_p^\bullet \otimes_{\mathbb{Q}_p} \mathbb{C}_p) \longrightarrow 0,
\end{gathered}$$

β_2 and β_4 are induced by θ_p^{ev} and θ_p^{od}, respectively, and β_3 by θ_F. It can be shown that the refined Euler characteristic $[X_p^{ev}, \theta_p', X_p^{od}] \in K_0(\mathbb{Z}_p[G], \mathbb{C}_p)$ does not depend on any of the above choices. See [9, Section 6] or [13] for more information on this construction of refined Euler characteristics and its relation to the Euler characteristic used in [12].

Lemma 2.1. *Assume that $X_p^\bullet \otimes_{\mathbb{Z}_p} \mathbb{C}_p$ is acyclic outside degrees 1 and 2. Then*

$$j_*\left(\iota_{\mathbb{Z}[G],\mathbb{R}}\left(\left(\hat{X}, Y, \prod_p \theta_p\right), \theta_\infty\right)\right) = [X_p^{ev}, \theta_p', X_p^{od}].$$

Proof. We consider the diagram

$$\begin{array}{ccc}
\pi_0\mathbb{V}(\mathbb{Z}[G], \mathbb{R}) & \xrightarrow{pr_j} & \pi_0 V(\mathbb{Z}_p[G], \mathbb{C}_p) \\
\big\downarrow{\scriptstyle \iota_{\mathbb{Z}[G],\mathbb{R}}} & & \big\downarrow{\scriptstyle \iota_{\mathbb{Z}_p[G],\mathbb{C}_p}} \\
K_0(\mathbb{Z}[G], \mathbb{R}) & \xrightarrow{j_*} & K_0(\mathbb{Z}_p[G], \mathbb{C}_p)
\end{array}$$

It follows from the explicit descriptions of $\iota_{\mathbb{Z}[G],\mathbb{R}}^{-1}$ and $\iota_{\mathbb{Z}_p[G],\mathbb{C}_p}^{-1}$ that the diagram is commutative. From [9, Th. 6.2 and Cor. 6.3] we deduce that

$$\iota_{\mathbb{Z}_p[G],\mathbb{C}_p}\left(pr_j\left(\left(\hat{X}, Y, \prod_p \theta_p\right), \theta_\infty\right)\right) = [X_p^{ev}, \theta_p', X_p^{od}].$$

Hence the result follows. □

Remark 2.2. Although [9, Th. 6.2] is more general we chose to formulate Lemma 2.1 with the acyclicity condition. This simplification suffices for our applications and, moreover, we can use the additivity result [9, Th. 5.7] without introducing any correction terms.

Let C denote a finite perfect $\mathbb{Z}_p[G]$-module. Recall that a finite $\mathbb{Z}_p[G]$-module C is perfect if and only if there exists a projective resolution

$$0 \longrightarrow P^{-1} \xrightarrow{\alpha} P^0 \longrightarrow C \longrightarrow 0$$

of length 2. Then the element

$$\chi_{\mathbb{Z}_p[G],\mathbb{Q}_p}(C) := [P^{-1}, \alpha \otimes \mathbb{Q}_p, P^0] \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$$

does not depend on the choice of the above resolution.

For any $\mathbb{Z}_p[G]$-module P we write P_{tors} for the submodule of $\mathbb{Z}_p$-torsion elements and set $P_{tf} := P/P_{tors}$.

Lemma 2.3. *Assume that we have data given as in (4). Let p be a fixed prime and $j : \mathbb{R} \longrightarrow \mathbb{C}_p$ an embedding.*

(a) If all cohomology modules $H^i(X_p^\bullet), i \in \mathbb{Z}$, are $\mathbb{Z}_p[G]$-perfect, then

$$j_*\left(\iota_{\mathbb{Z}[G],\mathbb{R}}\left(\left(\hat{X}, Y, \prod_p \theta_p\right), \theta_\infty\right)\right) = [H^{ev}(X_p^\bullet), \theta_p^{''}, H^{od}(X_p^\bullet)]$$

with $\theta_p^{''} = (\theta_p^{od} \otimes \mathbb{C}_p)^{-1} \circ (\theta_F \otimes \mathbb{C}_p) \circ (\theta_p^{ev} \otimes \mathbb{C}_p)$.

(b) If, in addition, $H^i(X_p^\bullet)_{tors}$ is $\mathbb{Z}_p[G]$-perfect for all $i \in \mathbb{Z}$, then

$$\begin{aligned} & j_*\left(\iota_{\mathbb{Z}[G],\mathbb{R}}\left(\left(\hat{X}, Y, \prod_p \theta_p\right), \theta_\infty\right)\right) \\ = \ & [H^{ev}(X_p^\bullet)_{tf}, \theta_p^{''}, H^{od}(X_p^\bullet)_{tf}] - \chi_{\mathbb{Z}_p[G],\mathbb{Q}_p}(H^{ev}(X_p^\bullet)_{tors}) + \chi_{\mathbb{Z}_p[G],\mathbb{Q}_p}(H^{od}(X_p^\bullet)_{tors}). \end{aligned}$$

Proof. Part (a) follows from the definition of θ_p' and [12, Prop. 2.1e]. If the modules $H^{ev}(X_p^\bullet)_{tors}$ and $H^{od}(X_p^\bullet)_{tors}$ are also $\mathbb{Z}_p[G]$-perfect, then

$$\begin{aligned} & j_*\left(\iota_{\mathbb{Z}[G],\mathbb{R}}\left(\left(\hat{X}, Y, \prod_p \theta_p\right), \theta_\infty\right)\right) \\ = \ & [H^{ev}(X_p^\bullet)_{tf}, \theta_p^{''}, H^{od}(X_p^\bullet)_{tf}] + [H^{ev}(X_p^\bullet)_{tors}, 0, H^{od}(X_p^\bullet)_{tors}]. \end{aligned}$$

Part (b) follows now from the very definition of the second summand by devissage. □

For later reference we record the following lemma. We write $\delta_p \colon \zeta(\mathbb{C}_p[G])^\times \longrightarrow K_0(\mathbb{Z}_p[G], \mathbb{C}_p)$ for the extended boundary homomorphism. Note that

$$\delta_p = \partial^1_{\mathbb{Z}_p[G],\mathbb{C}_p} \circ \mathrm{Nrd}^{-1}_{\mathbb{C}_p[G]} \quad \text{and} \quad \delta_p \circ j_* = j_* \circ \delta.$$

Lemma 2.4. *a) Let $\xi \in \zeta(\mathbb{R}[G])^\times$. Then*

$$\delta(\xi) \in K_0(\mathbb{Z}[G], \mathbb{Q}) \iff \xi \in \zeta(\mathbb{Q}[G])^\times.$$

b) Let $\xi \in \zeta(\mathbb{C}_p[G])^\times$. Then

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

Proof. We recall the definition of δ. By the Weak Approximation Theorem we may choose $\lambda \in \zeta(\mathbb{Q}[G])^\times$ such that $\lambda\xi$ is in the image of the reduced norm map $\mathrm{Nrd}_{\mathbb{R}[G]}$. We shorten $\partial^1_{\mathbb{Z}[G],\mathbb{R}}$ to ∂^1. Then

$$\delta(\xi) = \partial^1\left(\mathrm{Nrd}^{-1}_{\mathbb{R}[G]}(\lambda\xi)\right) - \sum_p \delta_p(\lambda)$$

and therefore

$$\delta(\xi) \in K_0(\mathbb{Z}[G], \mathbb{Q}) \iff \partial^1(\mathrm{Nrd}^{-1}_{\mathbb{R}[G]}(\lambda\xi)) \in K_0(\mathbb{Z}[G], \mathbb{Q}).$$

An easy diagram chase using diagram (3) implies that $\partial^1(\mathrm{Nrd}_{\mathbb{R}[G]}^{-1}(\lambda\xi)) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ if and only if there exists $\eta \in K_1(\mathbb{Q}[G])$ such that

$$\mathrm{Nrd}_{\mathbb{R}[G]}^{-1}(\lambda\xi)/\eta \in \mathrm{im}(K_1(\mathbb{Z}[G]) \longrightarrow K_1(\mathbb{Q}[G])).$$

It follows that $\xi \in \zeta(\mathbb{Q}[G])$.

Let $\delta_{\mathbb{Q}} \colon \zeta(\mathbb{Q}[G])^\times \longrightarrow K_0(\mathbb{Z}[G], \mathbb{Q})$. The reverse implication is immediate from the commutative diagram

$$\begin{tikzcd} \zeta(\mathbb{Q}[G])^\times \arrow[r, "\subseteq"] \arrow[d, "\delta_{\mathbb{Q}}"] & \zeta(\mathbb{R}[G])^\times \arrow[d, "\delta"] \\ K_0(\mathbb{Z}[G], \mathbb{Q}) \arrow[r, "\subseteq"] & K_0(\mathbb{Z}[G], \mathbb{R}) \end{tikzcd}$$

The proof of b) is similar, but easier, because in the local case the reduced norm map is an isomorphism. $\square$

Proposition 2.5. *Assume the situation of (4). Let p be a prime and $j : \mathbb{R} \longrightarrow \mathbb{C}_p$ an embedding. Assume that X_p^{ev} and X_p^{od} are free $\mathbb{Z}_p[G]$-modules. Let $(v_1, \dots, v_d)$ and $(w_1, \dots, w_d)$ denote $\mathbb{Q}_p[G]$-basis of $X_p^{ev} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $X_p^{od} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, respectively. Let $B \in \mathrm{Gl}_d(\mathbb{C}_p[G])$ represent θ_p' with respect to the chosen basis. Set*

$$\Omega_p := [X_p^{ev}, \theta_p', X_p^{od}] - j_*(\delta(\mathcal{L}^*)).$$

Then

$$\Omega_p \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p) \iff \mathrm{Nrd}_{\mathbb{C}_p[G]}(B)/j_*(\mathcal{L}^*) \in \zeta(\mathbb{Q}_p[G])^\times.$$

Proof. Let $F^0 := \mathbb{Z}_p[G]v_1 \oplus \ldots \oplus \mathbb{Z}_p[G]v_d$ and $F^1 := \mathbb{Z}_p[G]w_1 \oplus \ldots \oplus \mathbb{Z}_p[G]w_d$. Then

$$[F^0, B, F^1] - [X_p^{ev}, \theta_p', X_p^{od}] \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p).$$

Writing $\partial_p^1 = \partial^1_{\mathbb{Z}_p[G], \mathbb{C}_p}$ one therefore has

$$\begin{aligned} \Omega_p \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p) &\iff [F^0, B, F^1] - j_*(\delta(\mathcal{L}^*)) \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p) \\ &\iff \partial_p^1([\mathbb{C}_p[G]^r, B]) - \delta_p(j_*(\mathcal{L}^*)) \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p) \\ &\iff \delta_p\left(\mathrm{Nrd}_{\mathbb{C}_p[G]}(B)/j_*(\mathcal{L}^*)\right) \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p) \\ &\iff \mathrm{Nrd}_{\mathbb{C}_p[G]}(B)/j_*(\mathcal{L}^*) \in \zeta(\mathbb{Q}_p[G])^\times, \end{aligned}$$

where the last equivalence follows from Lemma (2.4). $\square$

In the next section we will recall from [5] how the relative algebraic K-group $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ can be explicitly computed as an abstract abelian group and how the element Ω_p can be realized as an element of this abstract group.

Remark 2.6. a) The assumption in Proposition 2.5 is no restriction because we can always find a projective $\mathbb{Z}_p[G]$-module Z such that both $X_p^{ev} \oplus Z$ and $X_p^{od} \oplus Z$ are $\mathbb{Z}_p[G]$-free. Indeed, the canonical map $K_0(\mathbb{Z}_p[G]) \longrightarrow K_0(\mathbb{C}_p[G])$ is injective by [15, (32.1)], so that the existence of the isomorphism θ_p' implies that $[X_p^{ev}] = [X_p^{od}]$ in $K_0(\mathbb{Z}_p[G])$. By [15, II, page 79] we further conclude that $X_p^{ev} \simeq X_p^{od}$ as $\mathbb{Z}_p[G]$-modules.

b) The definition of θ_p' shows that for rationality questions it is enough to consider the map $Y^{ev} \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow Y^{od} \otimes_{\mathbb{Z}} \mathbb{R}$ induced by $\theta_{\mathbb{R}}$. More explicitly, let $\mathbb{Q}[G] = A_1 \oplus \ldots \oplus A_r$ be the Wedderburn decomposition of $\mathbb{Q}[G]$ with corresponding idempotents $e_1, \dots, e_r$. We set $Y_i^{ev} := e_i Y^{ev}$ and $Y_i^{od} := e_i Y^{od}$. Then each A_i is a central simple algebra and we denote by S_i the unique simple A_i-module. Then $Y_i^{ev} \simeq S_i^{d_i}$ and $Y_i^{od} \simeq S_i^{d_i}$. By abuse of language, we refer to the explicit choice of such isomorphisms as 'a choice of $\mathbb{Q}[G]$-basis' for Y^{ev} and Y^{od}.

These isomorphisms combine with $\theta_{\mathbb{R}}$ to define an isomorphism

$$\tau : \bigoplus_{i=1}^{r} \left(S_i^{d_i} \otimes_{\mathbb{Q}} \mathbb{R} \right) \simeq Y^{ev} \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\theta_{\mathbb{R}}} Y^{od} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \bigoplus_{i=1}^{r} \left(S_i^{d_i} \otimes_{\mathbb{Q}} \mathbb{R} \right).$$

Then one has:

$$\Omega \in K_0(\mathbb{Z}[G], \mathbb{Q}) \iff \mathrm{Nrd}_{\mathbb{R}[G]}(\tau)/\mathcal{L}^* \in \zeta(\mathbb{Q}[G])^\times.$$

2.2. **Relative algebraic K-groups.** In this section we recall results from [5] which will be used to perform explicit computations in the relative algebraic K-groups $K_0(\mathbb{Z}[G], \mathbb{Q})$ and $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$. For the definitions of these groups we refer the reader to [35, page 215] or [5, Sec. 2.1].

We set $\mathcal{A} := \mathbb{Z}[G]$, $A := \mathbb{Q}[G]$ and choose a maximal order $\mathcal{M}$ in A containing $\mathcal{A}$. We take $C := \zeta(A)$ to be the centre of A and write $\mathcal{O}_C$ for the maximal order in C.

We let $DT(\mathcal{A}_p)$ denote the torsion subgroup of the finitely generated abelian group $K_0(\mathcal{A}_p, \mathbb{Q}_p)$. It is well-known that the map on relative groups induced by the functor $\mathcal{M}_p \otimes_{\mathcal{A}_p} \_$ gives the top exact sequence of the following commutative diagram. The vertical maps are induced by the reduced norm map (see [5, Th. 2.2 and 2.4] for more details).

$$\begin{tikzcd}
0 \arrow[r] & DT(\mathcal{A}_p) \arrow[r] & K_0(\mathcal{A}_p, \mathbb{Q}_p) \arrow[r] & K_0(\mathcal{M}_p, \mathbb{Q}_p) \arrow[r] & 0 \\
0 \arrow[r] & \mathcal{O}_{C_p}^\times/\mathrm{Nrd}_{A_p}(\mathcal{A}_p^\times) \arrow[r] \arrow[u, "\simeq"] & C_p^\times/\mathrm{Nrd}_{A_p}(\mathcal{A}_p^\times) \arrow[r] \arrow[u, "\simeq"', "\delta_p"] & C_p^\times/\mathcal{O}_{C_p}^\times \arrow[r] \arrow[u, "\simeq"] & 0
\end{tikzcd} \tag{5}$$

For $\xi \in K_0(\mathcal{A}_p, \mathbb{Q}_p)$ we will often write $\tilde{\xi}$ for any lift of ξ via the middle vertical isomorphism, i.e., $\delta_p(\tilde{\xi}) = \xi$.

Next we briefly recall from [5, Sec. 2.2] how the diagram (5) can be used to perform explicit computations in $K_0(\mathcal{A}_p, \mathbb{Q}_p)$.

The primitive idempotents of C will be denoted by $e_1, \ldots, e_r$. For $i = 1, \ldots, r$ we set $A_i := Ae_i$. Then

$$A = A_1 \oplus \ldots \oplus A_r \tag{6}$$

is a decomposition into indecomposable ideals A_i of A. Each A_i is a $\mathbb{Q}$-algebra with identity element e_i. The centers $K_i := \zeta(A_i)$ are finite field extensions of $\mathbb{Q}$ via $\mathbb{Q} \to K_i, \alpha \mapsto \alpha e_i$, and we have $\mathbb{Q}$-algebra isomorphisms $A_i \simeq \mathrm{Mat}_{n_i}(D_i)$ for each $i = 1, \ldots, r$, where D_i is a skew field with $\zeta(D_i) \simeq K_i$. The Wedderburn decomposition induces decompositions

$$\begin{aligned} C &= K_1 \oplus \ldots \oplus K_r, \\ \mathcal{O}_C &= \mathcal{O}_{K_1} \oplus \ldots \oplus \mathcal{O}_{K_r}. \end{aligned}$$

Let $\mathfrak{f}$ be a full, two-sided ideal of $\mathcal{M}$ contained in $\mathcal{A}$ and put $\mathfrak{g} := \mathcal{O}_C \cap \mathfrak{f}$. Since $\mathcal{M}$ contains the idempotents e_i the ideal $\mathfrak{f}$ of $\mathcal{M}$ decomposes into $\mathfrak{f} = \mathfrak{f}_1 \oplus \ldots \oplus \mathfrak{f}_r$

and similarly $\mathfrak{g} = \mathfrak{g}_1 \oplus \ldots \oplus \mathfrak{g}_r$. By [5, Th. 2.6] the reduced norm Nrd_A on A induces a homomorphism

$$\mu\colon K_1(\mathcal{A}/\mathfrak{f}) \longrightarrow (\mathcal{O}_C/\mathfrak{g})^\times$$

and a canonical isomorphism $DT(\mathcal{A}) \simeq \mathrm{cok}(\mu)$, where $DT(\mathcal{A})$ denotes the torsion subgroup of $K_0(\mathcal{A}, \mathbb{Q})$. This isomorphism encodes certain congruences implied by the triviality of an element in $DT(\mathcal{A})$.

For a rational prime p one has canonical isomorphisms

$$A_p \simeq \bigoplus A_{i,\mathfrak{P}},$$

where for given $i \in \{1, \ldots, r\}$, $\mathfrak{P}$ runs through all maximal ideals of $\mathcal{O}_{K_i}$ dividing p and $A_{i,\mathfrak{P}}$ is defined as $A_i \otimes_{K_i} K_{i,\mathfrak{P}}$, where $K_{i,\mathfrak{P}}$ denotes completion of K_i with respect to $\mathfrak{P}$. Similarly we have a canonical isomorphism

$$C_p \simeq \bigoplus K_{i,\mathfrak{P}}. \tag{7}$$

We write $I_p(C)$ for the group of fractional ideals of C with support above p. Then (5) together with (7) induces a canonical identification of $K_0(\mathcal{M}_p, \mathbb{Q}_p)$ with $I_p(C)$.

We put $\mathfrak{a}_p$ for the p-primary part of a fractional ideal $\mathfrak{a}$. Then one has a hommorphism

$$\mu_p\colon K_1(\mathcal{A}_p/\mathfrak{f}_p) \longrightarrow \left(\mathcal{O}_{C_p}/\mathfrak{g}_p\right)^\times \simeq \bigoplus_{i=1}^{r} (\mathcal{O}_{K_i}/\mathfrak{g}_{i,p})^\times$$

and a canonical isomorphism

$$DT(\mathcal{A}_p) \simeq \mathrm{cok}(\mu_p). \tag{8}$$

Combined with the isomorphism δ_p from (5) this is the origin of explicit congruences. See the next section for even more explicit versions of these congruences in the case of cyclic groups Z_p, dihedral groups D_{2p} and the alternating group A_4.

We obtain the following canonical short exact sequence

$$0 \longrightarrow \mathrm{cok}(\mu_p) \longrightarrow K_0(\mathcal{A}_p, \mathbb{Q}_p) \longrightarrow I_p(C) \longrightarrow 0.$$

After choosing an explicit splitting we have by [5, Prop. 2.7] a non-canonical isomorphism

$$K_0(\mathcal{A}_p, \mathbb{Q}_p) \simeq \mathrm{cok}(\mu_p) \oplus I_p(C).$$

In [5, Sec. 3 and 4] it is shown how the right hand side can be computed explicitly and how to solve the logarithm problem. We briefly recall the logarithm algorithm, for the details we refer the reader to [5, Sec. 4.1].

Let $\eta = [P, \varphi, Q] \in K_0(\mathcal{A}_p, \mathbb{Q}_p)$. By Remark 2.6 a) we may without loss of generality assume that P and Q are $\mathcal{A}_p$-free. Then one computes $\mathcal{A}_p$-basis $\nu_1, \ldots, \nu_d$ and $\omega_1, \ldots, \omega_d$ of P and Q and a matrix $S \in \mathrm{Gl}_d(A_p)$ such that $(\varphi(\nu_1), \ldots, \varphi(\nu_d)) = (\omega_1, \ldots, \omega_d)S$. In all of our applications we will be able to choose $S \in \mathrm{Gl}_d(A)$. If $\tilde{\eta} := \mathrm{Nrd}_A(S)$, then $\tilde{\eta}$ represents η via the middle vertical isomorphism in (5) and we will use [5, Prop. 2.7] to read $\tilde{\eta}$ in $\mathrm{cok}(\mu_p) \oplus I_p(C)$. In particular, we have a test whether $[P, \varphi, Q] = 0$ in $K_0(\mathcal{A}_p, \mathbb{Q}_p)$. If $\tilde{\eta} = (\eta_1, \ldots, \eta_r)$ with $\eta_i \in K_i$, then

$$[P, \varphi, Q] = 0 \iff \begin{cases} v_{\mathfrak{P}}(\eta_i) = 0, & \forall i \in \{1, \ldots, r\} \text{ and } \mathfrak{P} \mid p \\ \text{and} & \\ (\bar{\eta}_1, \ldots \bar{\eta}_r) \in \mathrm{im}(\mu_p), & \end{cases}$$

where $\bar{\eta}_i$ is the image of η_i under the projection $\mathcal{O}_{K_i,p}^\times \longrightarrow (\mathcal{O}_{K_i}/\mathfrak{g}_{i,p})^\times$.

Example 2.7. Let p be a prime and let T be a finite perfect $\mathbb{Z}_p[G]$-module. Then T is also perfect as a $\mathbb{Z}[G]$-module and we may choose a $\mathbb{Z}[G]$-projective resolution of the form

$$0 \longrightarrow Q \xrightarrow{\alpha} P \longrightarrow T \longrightarrow 0$$

By a fundametal result of Swan (see [15, Th. (32.11)]) the projectives P and Q are locally free and we can therefore apply the algorithm of [5, Sec. 4.2] to compute $\mathbb{Z}_p[G]$-basis $\nu_1, \ldots, \nu_d$ of $Q \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and $\omega_1, \ldots, \omega_d$ of $P \otimes_{\mathbb{Z}} \mathbb{Z}_p$. The algorithm of loc.cit. actually produces elements $\nu_i \in Q$ and $\omega_j \in P$. Hence we obtain a matrix $S \in \mathrm{Gl}_d(A)$ which represents α. Then $\tilde{\eta} := \mathrm{Nrd}_A(S) \in C^\times \subseteq C_p^\times$ represents $\chi_{\mathbb{Z}_p[G],\mathbb{Q}_p}(T) \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$.

Note that in the case $\#G = 1$ this just generalizes the notion of the order of the p-primary part of T.

We conclude this section by explicitly describing the element

$$\Omega_p = [X_p^{ev}, \theta_p', X_p^{od}] - \delta_p(j_*(\mathcal{L}*))$$

from Proposition 2.5. We assume that $v_1, \ldots, v_d$, respectively $w_1, \ldots, w_d$, constitute a $\mathbb{Z}_p[G]$-basis of X_p^{ev}, respectively X_p^{od}. Then Ω_p is represented by

$$\mathrm{Nrd}_{\mathbb{C}_p[G]}(B)/j_*(\mathcal{L}^*).$$

By Lemma 2.4 the element Ω_p is rational if and only if

$$\mathrm{Nrd}_{\mathbb{C}_p[G]}(B)/j_*(\mathcal{L}^*) \in \zeta(\mathbb{Q}_p[G])^\times.$$

If this is the case, we can interprete $\mathrm{Nrd}_{\mathbb{C}_p[G]}(B)/j_*(\mathcal{L}^*) = (\eta_1, \ldots, \eta_r)$ in $\mathrm{cok}(\mu_p) \oplus I_p(C)$ and thus determine the image of Ω_p in $\mathrm{cok}(\mu_p) \oplus I_p(C)$.

In our applications the modules $X_p^{ev} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $X_p^{od} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ are usually of the form $X^{ev} \otimes_{\mathbb{Z}} \mathbb{Q}_p$ and $X^{od} \otimes_{\mathbb{Z}} \mathbb{Q}_p$ with finitely generated $\mathbb{Z}[G]$-modules X^{ev} and X^{od}. In this case the rationality question can be treated by studying the quotient $\mathrm{Nrd}_{\mathbb{R}[G]}(B)/\mathcal{L}^*$, where B is a matrix computed with respect to any choice of $\mathbb{Q}[G]$-basis.

It remains to explain how we actually perform the test $\mathrm{Nrd}_{\mathbb{R}[G]}(B)/\mathcal{L}^* \in \zeta(\mathbb{Q}[G])^\times$. Let $\mathrm{Irr}(G)$ denote the set of absolutely irreducible characters. By Wedderburn's theorem $\mathbb{C}[G] \simeq \prod_{\chi \in \mathrm{Irr}(G)} M_{n_\chi}(\mathbb{C})$, which induces a canonical isomorphism $\zeta(\mathbb{C}[G]) \simeq \prod_{\chi \in \mathrm{Irr}(G)} \mathbb{C}$. Explicitly,

$$\prod_{\chi \in \mathrm{Irr}(G)} \mathbb{C} \longrightarrow \zeta(\mathbb{C}[G]), \quad (\alpha_\chi)_{\chi \in \mathrm{Irr}(G)} \mapsto \sum_{\chi \in \mathrm{Irr}(G)} \alpha_\chi e_\chi$$

with the central primitive idempotents $e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g) g^{-1}$.

Lemma 2.8. *Let $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ and let $\alpha = (\alpha_\chi)_{\chi \in \mathrm{Irr}(G)} \in \prod_{\chi \in \mathrm{Irr}(G)} \mathbb{C} \simeq \zeta(\mathbb{C}[G])$. Then one has*

$$\alpha \in \zeta(F[G]) \iff \alpha_{\sigma \circ \chi} = \sigma(\alpha_\chi)$$

for all $\chi \in \mathrm{Irr}(G)$ and all $\sigma \in \mathrm{Aut}(\mathbb{C}/F)$.

Proof. We have to show that $\sum_{\chi \in \mathrm{Irr}(G)} \alpha_\chi e_\chi \in F[G]$ if and only if $\alpha_{\sigma \circ \chi} = \sigma(\alpha_\chi)$ for all $\chi \in \mathrm{Irr}(G)$ and all $\sigma \in \mathrm{Aut}(\mathbb{C}/F)$. This amounts to show that

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1) \alpha_\chi \chi(g) \in F, \forall g \iff \alpha_{\sigma \circ \chi} = \sigma(\alpha_\chi), \forall \chi, \sigma.$$

If $\sum_\chi \chi(1)\alpha_\chi \chi(g) \in F, \forall g \in G$, then we easily show that

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)(\alpha_{\sigma\circ\chi} - \sigma(\alpha_\chi))(\sigma \circ \chi)(g) = 0$$

for all $g \in G$. The assertion now follows from the linear independence of absolutely irreducible characters.

Conversely, we deduce that

$$\sigma\left(\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\alpha_\chi \chi(g)\right) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\alpha_\chi \chi(g)$$

for all $\sigma \in \mathrm{Aut}(\mathbb{C}/F)$. Since for any $\beta \in \mathbb{C}$ one has

$$\beta \in F \iff \sigma(\beta) = \beta, \quad \forall \sigma \in \mathrm{Aut}(\mathbb{C}/F),$$

the result follows. $\square$

For $\chi \in \mathrm{Irr}(G)$ we write $\mathbb{Q}(\chi)$ for the extension generated over $\mathbb{Q}$ by the values of χ. We recall that $\mathbb{Q}(\chi)/\mathbb{Q}$ is an abelian extension. By Lemma 2.8 one has

$$\alpha \in \zeta(\mathbb{Q}[G]) \iff \alpha_\chi \in \mathbb{Q}(\chi) \text{ and } \alpha_{\sigma\circ\chi} = \sigma(\alpha_\chi)$$

for all $\chi \in \mathrm{Irr}(G)$ and all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$. This can be efficiently checked if we dispose of good approximations of the complex numbers α_χ and bounds for the denominators.

We fix a set $\mathrm{Irr}_\mathbb{Q}(G) \subseteq \mathrm{Irr}(G)$ of representatives of $\mathrm{Irr}(G)$ modulo the action of $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. Thus we identify C with $\prod_{\chi\in\mathrm{Irr}_\mathbb{Q}(G)} \mathbb{Q}(\chi)$. Once we know or trust in the validity of the rationality conjecture, we will work in $\prod_{\chi\in\mathrm{Irr}_\mathbb{Q}(G)} \mathbb{Q}(\chi)$. Note that the fields K_i, $i = 1, \ldots, r$, can be identified with the character fields $\mathbb{Q}(\chi)$, $\chi \in \mathrm{Irr}_\mathbb{Q}(G)$.

2.3. **Explicit congruences.** Assume that $\alpha = (\alpha_\chi)_\chi \in \prod_{\chi\in\mathrm{Irr}_\mathbb{Q}(G)} \mathbb{Q}(\chi) \simeq C^\times$. We let p denote an odd prime. In this section we will consider the cyclic groups Z_p, the dihedral groups D_{2p} and the alternating group A_4 and exemplary rephrase the condition $\delta_p(\alpha) = 0$ in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ in terms of explicit congruences. On the one hand this serves as an explicit illustration of the methods introduced in [5], on the other hand it leads to very remarkable congruences which are conjecturally satisfied by the twisted BSD quotients (see Remark 4.5).

Let p be a rational prime and G an arbitrary finite group. We adopt the notation from the previous subsection. Let $\mathfrak{f} := \{\lambda \in \mathbb{Q}[G] \mid \lambda\mathcal{M} \subseteq \mathbb{Z}[G]\}$ be the conductor of $\mathbb{Z}[G]$ in $\mathcal{M}$. Let $\mathfrak{g} := \mathfrak{f} \cap \mathcal{O}_C$ be the central conductor. Note that we dispose of an explicit formula for $\mathfrak{g}$ by [15, Th. (27.13)].

We recall that

$$\delta_p(\alpha) \in DT(\mathbb{Z}_p[G]) \iff \alpha_\chi \in \mathcal{O}^\times_{\mathbb{Q}(\chi),p} \text{ for all } \chi \in \mathrm{Irr}_\mathbb{Q}(G).$$

The explicit congruences are encoded in the canonical isomorphism (8). We will exemplary make this explicit for the groups Z_p, D_{2p} and A_4.

Let $G = \langle g_0 \rangle$ be cyclic of order p. Let ζ_p be a fixed primitive p-th root of unity and define irreducible characters χ_0 and χ_1 by $\chi_0(g_0) = 1$ and $\chi_1(g_0) = \zeta_p$. Then

$$\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta_p), \quad \lambda \mapsto (\chi_0(\lambda), \chi_1(\lambda)).$$

Let $\alpha = (\alpha_0, \alpha_1) \in \mathbb{Q}^\times \oplus \mathbb{Q}(\zeta_p)^\times$ be a p-adic unit (i.e. $\alpha \in \mathcal{O}_{C_p}^\times$). Then

$$\delta_p((\alpha_0, \alpha_1)) = 0 \text{ in } DT(\mathbb{Z}_p[Z_p]) \iff \alpha_0 \equiv \alpha_1 (\mathrm{mod}\ (1-\zeta_p)). \tag{9}$$

For a proof and the generalization for cyclic groups of prime power order we refer the reader to [1, Section 5].

Let now $G = \langle \sigma, \tau \mid \sigma^p = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle$ be the dihedral group D_{2p} for an odd prime p. Then $\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}(\zeta_p)^+)$ and we fix such an isomorphism by

$$\sigma \mapsto \left(1, 1, \begin{pmatrix} 0 & -1 \\ 1 & \zeta_p + \zeta_p^{-1} \end{pmatrix}\right), \quad \tau \mapsto \left(1, -1, \begin{pmatrix} 1 & \zeta_p + \zeta_p^{-1} \\ 0 & -1 \end{pmatrix}\right).$$

From [5, Th. 1.1] we know that $DT(\mathbb{Z}_p[G]) \simeq Z_{p-1}$ (where for $n \in \mathbb{N}$ we write Z_n for the cyclic group of order n). Let $H = \langle \sigma \rangle$. By [8, Prop. 3.2] we know that the restriction map

$$\mathrm{res}\colon DT(\mathbb{Z}_p[G]) \longrightarrow DT(\mathbb{Z}_p[H])$$

is injective. Let $\alpha = (\alpha_0, \alpha_1, \alpha_2) \in \mathbb{Q}^\times \oplus \mathbb{Q}^\times \oplus \mathbb{Q}(\zeta_p)^{+\times}$ be a p-adic unit. By [8, Lemma 3.9] or [2, page 575] one has $res(\alpha) = (\alpha_0\alpha_1, \alpha_2)$, so that we conclude from the result for cyclic groups Z_p that

$$\delta_p((\alpha_0, \alpha_1, \alpha_2)) = 0 \text{ in } DT(\mathbb{Z}_p[D_{2p}]) \iff \alpha_0\alpha_1 \equiv \alpha_2 (\mathrm{mod}\ \mathfrak{p}) \tag{10}$$

where $\mathfrak{p}$ denotes the unique prime ideal of $\mathbb{Q}(\zeta_p)^+$ over the rational prime p. It is also well known (see e.g. [8, Prop. 3.2]) that $DT(\mathbb{Z}_2[D_{2p}])$ is trivial.

Let now G be the alternating group A_4. If $\sigma = (1,2)(3,4)$ and $\nu = (1,2,3)$, then $G = \langle \sigma, \nu \rangle$. We have $\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta_3) \oplus M_3(\mathbb{Q})$ and we fix such an isomorphism by

$$\sigma \mapsto \left(1, 1, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}\right), \quad \nu \mapsto \left(1, \zeta_3, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\right).$$

From [5, Th. 1.2] we know that $DT(\mathbb{Z}_2[G]) \simeq Z_2$ and $DT(\mathbb{Z}_3[G]) \simeq Z_2$. We have $\mathcal{O}_C = (\mathbb{Z}, \mathbb{Z}[\zeta_3], \mathbb{Z})$ and $\mathfrak{g} = (12\mathbb{Z}, 4(1-\zeta_3), 4\mathbb{Z})$. We first consider $p = 3$. Clearly $(\mathcal{O}_C/\mathfrak{g}_3)^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \oplus (\mathbb{Z}[\zeta_3]/(1-\zeta_3))^\times \simeq Z_2 \times Z_2$. Since $\mathrm{Nrd}_{\mathbb{Q}[G]}(1+\nu) = (2, 1+\zeta_3, 2) \equiv (-1,-1) (\mathrm{mod}\ \mathfrak{g}_3)$ it follows that $\mathrm{im}(\mu_3) = \{(1,1), (-1,-1)\}$ and we obtain

$$\delta_3((\alpha_0, \alpha_1, \alpha_2)) = 0 \text{ in } DT(\mathbb{Z}_3[A_4]) \iff \alpha_1 \equiv \alpha_0 (\mathrm{mod}\ (1-\zeta_3)). \tag{11}$$

For $p = 2$ one has $(\mathcal{O}_C/\mathfrak{g}_2)^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \oplus (\mathbb{Z}[\zeta_3]/(4))^\times \oplus (\mathbb{Z}/4\mathbb{Z})^\times \simeq Z_2 \times (Z_2 \times Z_6) \times Z_2$. By explicit computation we show that

$$\begin{aligned} \mathrm{Nrd}_{\mathbb{Q}[G]}(2+\nu) &\equiv (-1, 2+\zeta_3, 1) (\mathrm{mod}\ \mathfrak{g}_2), \\ \mathrm{Nrd}_{\mathbb{Q}[G]}(-1+2\nu) &\equiv (1, -1+2\zeta_3, -1) (\mathrm{mod}\ \mathfrak{g}_2), \\ \mathrm{Nrd}_{\mathbb{Q}[G]}(-\sigma) &\equiv (-1,-1,-1) (\mathrm{mod}\ \mathfrak{g}_2). \end{aligned}$$

Again by explicit computation one verifies that the classes of $\mathrm{Nrd}_{\mathbb{Q}[G]}(2+\nu)$, $\mathrm{Nrd}_{\mathbb{Q}[G]}(-1+2\nu)$ and $\mathrm{Nrd}_{\mathbb{Q}[G]}(-\sigma)$ generate the kernel of the surjective homomorphism

$$(\mathcal{O}_C/\mathfrak{g}_2)^\times \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times, \quad (\alpha_0, \alpha_1, \alpha_2) \mapsto \alpha_0 N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\alpha_1)\alpha_2.$$

Together with $DT(\mathbb{Z}_2[G]) \simeq Z_2$ it follows that $\mathrm{im}(\mu_2)$ equals this kernel, so that

$$\delta_2((\alpha_0, \alpha_1, \alpha_2)) = 0 \text{ in } DT(\mathbb{Z}_2[A_4]) \iff \alpha_0 N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\alpha_1) \equiv \alpha_2 (\mathrm{mod}\ 4). \tag{12}$$

3. The ETNC for the base change of an elliptic curve

Let $K/\mathbb{Q}$ be a finite Galois extension with group G. Let E be an elliptic curve defined over $\mathbb{Q}$. We denote the base change $\mathrm{Spec}(K)\times_{\mathrm{Spec}(\mathbb{Q})} E$ by E_K and consider $M_K = h^1(E_K)(1)$ as a motive over $\mathbb{Q}$. The Galois group G naturally acts on M_K via the first factor and thus we have a natural action of $A = \mathbb{Q}[G]$ on the realizations and motivic cohomology groups attached to M_K. For an explicit description of the realizations we refer the reader to [14, Sec. 4.1].

The purpose of this section is to provide an explicit description of the ETNC for the pair $(M_K, \mathbb{Z}[G])$. Our main reference is [12], from where we adopt most of our notation. Further references are the survey articles of Flach [18], [19] and Venjakob [36].

We first note that by Poincaré duality the dual motive $M_K^*(1)$ identifies with M_K. The motivic cohomology spaces $H_f^0(M_K)$ and $H_f^1(M_K)$ are given by

$$H_f^0(M_K) = 0, \quad H_f^1(M_K) = E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$$

where, as usual, $E(K)$ denotes the Mordell-Weil group of E/K.

For a number field F we write G_F for the absolute Galois group. Let v be a place of K. We write K_v for the completion of K at v, and fix an algebraic closure $\bar{K}_v$ of K_v and an embedding $\bar{K}$ into $\bar{K}_v$. We denote by $G_v \subseteq G_K$ the corresponding decomposition group and, if v is non-archimedean, by $I_v \subseteq G_v$ the inertia group. We write $Fr_v \in G_v/I_v$ for the Frobenius substitution.

For any number field F we let $\Sigma(F)$ denote the set of embeddings of F into $\mathbb{C}$. We define $H_K := \bigoplus_{\Sigma(K)} \mathbb{Q}$. The groups G and $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ act on $\Sigma(K)$ and endow H_K with the structure of a $(\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \times G)$-module. Let $\{w_j : j \in \Sigma(K)\}$ denote the canonical $\mathbb{Q}$-basis of H_K. We write $c \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ for complex conjugation. Then $cw_j = w_{c\circ j}$ and $\sigma w_j = w_{j\circ\sigma^{-1}}$ for $\sigma \in G$.

For any commutative ring R and any $R[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]$-module X we write X^+ and X^- for the submodules on which complex conjugation acts by $+1$ and -1, respectively.

We write $\rho_K : \mathbb{C} \otimes_{\mathbb{Q}} K \longrightarrow \mathbb{C} \otimes_{\mathbb{Q}} H_K$ for the canonical $\mathbb{C}[\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \times G]$-equivariant isomorphism which is induced by $z \otimes \alpha \mapsto (zj(\alpha))_{j\in\Sigma(K)}$. Let $\tilde{\rho}_K : \mathbb{R} \otimes_{\mathbb{Q}} K \longrightarrow \mathbb{R} \otimes_{\mathbb{Q}} H_K$ be the $\mathbb{R}[G]$-equivariant isomorphism defined in [2, page 554] where it is denoted by π_K.

We write ∞ for the archimedean place of $\mathbb{Q}$ and let $S_\infty(K)$ denote the set of archimedean places of K. For each $v \in S_\infty(K)$ we choose $\sigma_v \in \Sigma(K)$ corresponding to v. Since E is defined over $\mathbb{Q}$ one has $\sigma E_K = E_K$ for all $\sigma \in \Sigma(K)$. As usual, we write M_B for the Betti realization, that is

$$M_B = \bigoplus_{\sigma\in\Sigma(K)} H^1(\sigma E_K(\mathbb{C}), 2\pi i\mathbb{Q}) = H_K \otimes_{\mathbb{Q}} H^1(E(\mathbb{C}), 2\pi i\mathbb{Q}).$$

By identifying $H^1(E(\mathbb{C}), 2\pi i\mathbb{Q})$ with the dual homology $\mathcal{H} := \mathrm{Hom}_{\mathbb{Q}}(H_1(E(\mathbb{C}), \mathbb{Q}), 2\pi i\mathbb{Q})$ we obtain

$$M_B^+ \simeq \bigoplus_{v\in S_\infty(K)} H^1(\sigma_v E_K(\mathbb{C}), 2\pi i\mathbb{Q})^{G_v} \simeq [H_K \otimes_{\mathbb{Q}} \mathcal{H}]^+ .$$

We write M_{dR} for the deRham realization,

$$M_{dR} = H^1_{dR}(E/K)$$

with the natural decreasing filtration $\{F^iH^1_{dR}(E/K)\}_{i\in\mathbb{Z}}$ shifted by 1. Thus

$$M_{dR}/M^0_{dR} = H^1_{dR}(E/K)/F^1H^1_{dR}(E/K) \simeq H^1(E_K, \mathcal{O}_{E_K}).$$

The G-module $H^1(E_K, \mathcal{O}_{E_K})$ is isomorphic to $K \otimes_{\mathbb{Q}} H^1(E, \mathcal{O}_E)$. Now $H^1(E, \mathcal{O}_E)$ is canonically isomorphic to $\Omega^1_E(E)^* := \mathrm{Hom}(\Omega^1_E(E), \mathbb{Q})$, so that we finally identify

$$M_{dR}/M^0_{dR} \simeq K \otimes_{\mathbb{Q}} \Omega^1_E(E)^*.$$

We let ω_0 denote a Néron differential and let γ_+ and γ_- be $\mathbb{Z}$-generators of $H_1(E(\mathbb{C}), \mathbb{Z})^+$ and $H_1(E(\mathbb{C}), \mathbb{Z})^-$, respectively. We define

$$\Omega_+ := \int_{\gamma_+} \omega_0, \quad \Omega_- := \int_{\gamma_-} \omega_0.$$

We write $\omega_0^* \in \Omega^1_E(E)^*$ for the map which sends ω_0 to 1. Similarly we define $\mathbb{Q}$-linear maps $\gamma_+^*, \gamma_-^* \in \mathcal{H}$ by

$$\gamma_+^*(\gamma_+) = 2\pi i, \quad \gamma_+^*(\gamma_-) = 0, \quad \gamma_-^*(\gamma_+) = 0, \quad \gamma_-^*(\gamma_-) = 2\pi i.$$

For $\gamma = a\gamma_+ + b\gamma_- \in H_1(E(\mathbb{C}), \mathbb{Q})$, $a, b \in \mathbb{Q}$, we set $\gamma^* := a\gamma_+^* + b\gamma_-^*$. Finally we define

$$\begin{aligned} \pi \quad : \quad & \mathbb{C} \otimes_{\mathbb{Q}} \mathcal{H} \longrightarrow \mathbb{C} \otimes_{\mathbb{Q}} \Omega^1_E(E)^* \\ & z \otimes \gamma^* \mapsto \left(\omega \mapsto z \int_\gamma \omega \right). \end{aligned}$$

We write $\pi_K : \mathbb{R} \otimes_{\mathbb{Q}} M_B^+ \longrightarrow \mathbb{R} \otimes_{\mathbb{Q}} M_{dR}/M^0_{dR}$ for the period isomorphism. Then π_K is explicitly given by the following composite of $\mathbb{R}[G]$-equivariant maps

$$\begin{array}{cl} & \mathbb{R} \otimes_{\mathbb{Q}} [H_K \otimes_{\mathbb{Q}} \mathcal{H}]^+ \\ = & \mathbb{R} \otimes_{\mathbb{Q}} H_K^+ \otimes_{\mathbb{Q}} \mathcal{H}^+ \oplus \mathbb{R} \otimes_{\mathbb{Q}} H_K^- \otimes_{\mathbb{Q}} \mathcal{H}^- \\ = & \left(\mathbb{R} \otimes_{\mathbb{Q}} H_K^+\right) \otimes_{\mathbb{R}} \left(\mathbb{R} \otimes_{\mathbb{Q}} \mathcal{H}^+\right) \oplus \left(\mathbb{R} \otimes_{\mathbb{Q}} H_K^-\right) \otimes_{\mathbb{R}} \left(\mathbb{R} \otimes_{\mathbb{Q}} \mathcal{H}^-\right) \\ \xrightarrow{(id\otimes\pi, id\otimes\pi)} & \left(\mathbb{R} \otimes_{\mathbb{Q}} H_K^+\right) \otimes_{\mathbb{R}} \left(\mathbb{R} \otimes_{\mathbb{Q}} \Omega^1_E(E)^*\right) \oplus \left(\mathbb{R} \otimes_{\mathbb{Q}} H_K^-\right) \otimes_{\mathbb{R}} \left(i\mathbb{R} \otimes_{\mathbb{Q}} \Omega^1_E(E)^*\right) \\ \xrightarrow{(id,-i)} & \left(\mathbb{R} \otimes_{\mathbb{Q}} H_K^+\right) \otimes_{\mathbb{R}} \left(\mathbb{R} \otimes_{\mathbb{Q}} \Omega^1_E(E)^*\right) \oplus \left(\mathbb{R} \otimes_{\mathbb{Q}} H_K^-\right) \otimes_{\mathbb{R}} \left(\mathbb{R} \otimes_{\mathbb{Q}} \Omega^1_E(E)^*\right) \\ = & \left(\mathbb{R} \otimes_{\mathbb{Q}} H_K\right) \otimes_{\mathbb{R}} \left(\mathbb{R} \otimes_{\mathbb{Q}} \Omega^1_E(E)^*\right) \\ \xrightarrow{\tilde{\rho}_K^{-1}\otimes id} & \left(\mathbb{R} \otimes_{\mathbb{Q}} K\right) \otimes_{\mathbb{R}} \left(\mathbb{R} \otimes_{\mathbb{Q}} \Omega^1_E(E)^*\right) \\ = & \mathbb{R} \otimes_{\mathbb{Q}} K \otimes_{\mathbb{Q}} \Omega^1_E(E)^*. \end{array}$$

Proposition 3.1. *Fix $\iota \in \Sigma(K)$ and define $\tau \in G$ by $c \circ \iota = \iota \circ \tau$. Let $\alpha_0 \in K$ be a normal basis element.*

a) The elements $\frac{1+c}{2} w_\iota \otimes \gamma_+^* + \frac{1-c}{2} w_\iota \otimes \gamma_-^*$ and $\alpha_0 \otimes \omega_0^*$ are $\mathbb{Q}[G]$-basis of $[H_K \otimes_{\mathbb{Q}} \mathcal{H}]^+$ and $K \otimes_{\mathbb{Q}} \Omega^1_E(E)^*$, respectively.

b) With respect to these basis the period isomorphism π_K is represented by

$$\lambda_{\alpha_0} := \left(\Omega_+ \frac{1+\tau}{2} + \Omega_- \frac{1-\tau}{2} \right) \left(\sum_{\sigma \in G} (\iota \circ \sigma)(\alpha_0) \sigma^{-1} \right)^{-1}$$

Proof. a) is obvious. For the proof of b) we write $\pi_K = \left(\tilde{\rho}_K^{-1} \otimes id\right) \circ f$ and first compute the matrix for

$$f \colon \mathbb{R} \otimes_{\mathbb{Q}} [H_K \otimes_{\mathbb{Q}} \mathcal{H}]^+ \longrightarrow \left(\mathbb{R} \otimes_{\mathbb{Q}} H_K\right) \otimes_{\mathbb{R}} \left(\mathbb{R} \otimes_{\mathbb{Q}} \Omega^1_E(E)^*\right)$$

with respect to the basis $W := 1\otimes\frac{1+c}{2}w_\iota\otimes\gamma_+^* + 1\otimes\frac{1-c}{2}w_\iota\otimes\gamma_-^*$ and $(1\otimes w_\iota)\otimes(1\otimes\omega_0^*)$.

The basis element W is mapped to

$$\left(\Omega_+\otimes\frac{1+c}{2}w_\iota - i\Omega_-\otimes\frac{1-c}{2}w_\iota\right)\otimes(1\otimes\omega_0^*).$$

By the definition of τ one has

$$\left(\Omega_+\frac{1+\tau}{2} - i\Omega_-\frac{1-\tau}{2}\right)(1\otimes w_\iota) = \left(\Omega_+\otimes\frac{1+c}{2}w_\iota - i\Omega_-\otimes\frac{1-c}{2}w_\iota\right).$$

Next we compute the matrix of the map $\tilde\rho_K : (\mathbb{R}\otimes_\mathbb{Q} K) \longrightarrow \mathbb{R}\otimes_\mathbb{Q} H_K$ with respect to the basis $1\otimes\alpha_0$ and $1\otimes w_\iota$. One has

$$\tilde\rho_K(1\otimes\alpha_0) = (\mathrm{Re}(\iota(\sigma(\alpha_0)) + \mathrm{Im}(\iota(\sigma(\alpha_0)))_{\sigma\in G}.$$

On the other hand one computes

$$\begin{aligned}&\left(\sum_{\sigma\in G}\iota(\sigma(\alpha_0))\sigma^{-1}\right)\left(\frac{1+\tau}{2} - i\frac{1-\tau}{2}\right)(1\otimes w_\iota)\\ =\ & (\mathrm{Re}(\iota(\sigma(\alpha_0))) + \mathrm{Im}(\iota(\sigma(\alpha_0))))_{\sigma\in G}.\end{aligned}$$

Summarizing we obtain

$$\begin{aligned}&\pi_K(W) = \left(\left(\tilde\rho_K^{-1}\otimes id\right)\circ f\right)(W)\\
=\ & \left(\Omega_+\frac{1+\tau}{2} - i\Omega_-\frac{1-\tau}{2}\right)\left(\tilde\rho_K^{-1}\otimes id\right)((1\otimes w_\iota)\otimes(1\otimes\omega_0^*))\\
=\ & \left(\Omega_+\frac{1+\tau}{2} - i\Omega_-\frac{1-\tau}{2}\right)\left(\frac{1+\tau}{2} - i\frac{1-\tau}{2}\right)^{-1}\left(\sum_{\sigma\in G}(\iota\circ\sigma)(\alpha_0)\sigma^{-1}\right)^{-1}(1\otimes\alpha_0\otimes\omega_0^*)\\
=\ & \left(\Omega_+\frac{1+\tau}{2} - i\Omega_-\frac{1-\tau}{2}\right)\left(\frac{1+\tau}{2} + i\frac{1-\tau}{2}\right)\left(\sum_{\sigma\in G}(\iota\circ\sigma)(\alpha_0)\sigma^{-1}\right)^{-1}(1\otimes\alpha_0\otimes\omega_0^*)\\
=\ & \left(\Omega_+\frac{1+\tau}{2} + \Omega_-\frac{1-\tau}{2}\right)\left(\sum_{\sigma\in G}(\iota\circ\sigma)(\alpha_0)\sigma^{-1}\right)^{-1}(1\otimes\alpha_0\otimes\omega_0^*)\end{aligned}$$

□

For a ring R and a R-module W we set $W^* := \mathrm{Hom}_R(W,R)$ whenever there is no danger of confusion. Following [12, (29)] we define

$$\begin{aligned}\Xi = \Xi(M_K) &:= [H^1_f(M_K)]^{-1}_{\mathbb{Q}[G]}[H^1_f(K, M_K^*(1))^*]_{\mathbb{Q}[G]}[M_B^+]^{-1}_{\mathbb{Q}[G]}[M_{dR}/M^0_{dR}]_{\mathbb{Q}[G]}\\ &= [E(K)\otimes_\mathbb{Z}\mathbb{Q}]^{-1}_{\mathbb{Q}[G]}[(E(K)\otimes_\mathbb{Z}\mathbb{Q})^*]_{\mathbb{Q}[G]}[M_B^+]^{-1}_{\mathbb{Q}[G]}[M_{dR}/M^0_{dR}]_{\mathbb{Q}[G]}\end{aligned}$$

The height pairing induces an $\mathbb{R}[G]$-equivariant isomorphism

$$\delta\colon E(K)\otimes_\mathbb{Z}\mathbb{R} \longrightarrow (E(K)\otimes_\mathbb{Z}\mathbb{R})^*.$$

Together with the period isomorphism π_K we obtain an isomorphism in $V(A_\mathbb{R}) = V(\mathbb{R}[G])$

$$\theta_\infty : \Xi\otimes_{\mathbb{Q}[G]}\mathbb{R}[G] \longrightarrow \mathbf{1}_{\mathbb{R}[G]}.$$

Let $S_{ram}(K/\mathbb{Q})$ be the set of rational primes which ramify in $K/\mathbb{Q}$ and $S_{bad}(E)$ the set of rational primes where E has bad reduction. We put $S := S_{ram}(K/\mathbb{Q})\cup S_{bad}(E)$ and for a fixed prime l we set $S_l := S\cup\{l\}$. We let $T_l(E) := \varprojlim E[l^n]$ denote the l-adic Tate module of E and set $T_l := \mathbb{Z}_l[G]\otimes_{\mathbb{Z}_l}T_l(E)$ which we regard as a (left) module over $G_{\mathbb{Q}} \times G$. Explicitly, $G_{\mathbb{Q}}$ acts diagonally and $g(\lambda \otimes t) = \lambda g^{-1} \otimes t$ for $g \in G, \lambda \in \mathbb{Z}_l[G]$ and $t \in T_l(E)$. We further define

$$V_l(E) := T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l, \quad V_l := T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

Although not visible in the notation, the modules T_l and V_l depend both on E and K.

We let $R\Gamma_c(\mathbb{Z}_{S_l}, T_l)$ denote the complex defined in [12, Sec. 3.2 - 3.3] and let

$$\theta_l \colon \Xi \otimes_A A_l \longrightarrow [R\Gamma_c(\mathbb{Z}_{S_l}, T_l)] \otimes_A A_l.$$

be the isomorphism defined in [12, Sec. 3.4]. Given this data we obtain an element

$$R\Omega := \iota_{\mathbb{Z}[G],\mathbb{R}} \left(\left(\left(\prod_l [R\Gamma_c(\mathbb{Z}_{S_l}, T_l)], \Xi, \prod_l \theta_l^{-1} \right), \theta_\infty \right) \right)$$

in $K_0(\mathbb{Z}[G], \mathbb{R})$.

Next we will formulate the conjecture for which we wish to provide numerical evidence. For each character $\psi \in \mathrm{Irr}(G)$ we write $L(E/\mathbb{Q}, \psi, s)$ for the twisted Hasse-Weil- L-function. We assume that $L(E/\mathbb{Q}, \psi, s)$ has analytic continuation to all of $\mathbb{C}$ and write $L^*(E/\mathbb{Q}, \psi, 1)$ for the leading term in its Taylor expansion at $s = 1$.

In order to compare the vector of twisted Hasse-Weil-L-functions to the motivic L-function it is necessary to recall the precise definition of the twisted Hasse-Weil-L-functions. The l-adic representation attached to E is

$$H_l(E) := \mathrm{Hom}(V_l(E), \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} \bar{\mathbb{Q}}_l.$$

For $\chi \in \mathrm{Irr}(G)$ we write V_χ for a representation space for χ and without loss of generality we may regard V_χ as a $\bar{\mathbb{Q}}_l$-vector space. For primes $p \neq l$ we define local polynomials by

$$P_p(E, \chi, T) := \det\left(1 - Fr_p^{-1} T \mid \left(H_l(E) \otimes_{\bar{\mathbb{Q}}_l} V_\chi\right)^{I_p}\right).$$

As usual we put $L_p(E, \chi, s) := P_p(E, \chi, p^{-s})$ and $L(E/\mathbb{Q}, \chi, s) := \prod_p L_p(E, \chi, s)^{-1}$. The l-adic realization of M_K is given by

$$H_l(M_K) := \mathrm{Hom}(V_l(E), \mathbb{Q}_l)(1) \otimes_{\mathbb{Q}_l} H_{K,l}.$$

where we have put $H_{K,l} := H_K \otimes_{\mathbb{Z}} \mathbb{Z}_l$. If we fix an embedding $\iota : K \hookrightarrow \bar{\mathbb{Q}}$ then $H_l(M_K)$ gets identified with $\mathrm{Hom}(V_l(E), \mathbb{Q}_l)(1) \otimes_{\mathbb{Q}_l} \mathbb{Q}_l[G]^*$ where $\mathbb{Q}_l[G]^* := \mathrm{Hom}(\mathbb{Q}_l[G], \mathbb{Q}_l)$ denotes the contragredient representation. By [12, Rem. 7], the motivic L-function associated to M_K is defined by the Euler factors

$$\mathrm{Nrd}_{\mathbb{C}[G]}\left(1 - Fr_p^{-1} T \mid H_l(M_K)^{I_p}\right) = \left(\det\left(1 - \frac{1}{p} Fr_p^{-1} T \mid (H_l(E) \otimes_{\bar{\mathbb{Q}}_l} V_{\bar{\chi}})^{I_p}\right)\right)_{\chi \in \mathrm{Irr}(G)}.$$

It easily follows that $L(M_K, s) = (L(E/\mathbb{Q}, \bar{\chi}, s+1))_{\chi \in \mathrm{Irr}(G)}$.

Remark 3.2. Since $L(E/\mathbb{Q}, \bar{\chi}, s+1)$ is the complex conjugate of $L(E/\mathbb{Q}, \chi, s+1)$ for each real value s, it follows from Proposition 2.8 that $L^*(M_K) = (L(E/\mathbb{Q}, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}(G)}$ belongs to $\zeta(\mathbb{R}[G])^\times$.

Remark 3.3. For later reference we compute the refined Euler characteristic of the complex

$$T_l^{I_p} \xrightarrow{1 - Fr_p^{-1}} T_l^{I_p}$$

where the non-trivial modules are placed in degrees 0 and 1 under the assumption that $T_l^{I_p}$ is $\mathbb{Z}_l[G]$-perfect. In this case the refined Euler characteristic associated with the above complex is represented by $(L_p(E,\bar{\chi},1))_{\chi\in\mathrm{Irr}(G)}$ via the middle vertical isomorphism of diagram (5). Indeed, the Weil pairing induces a $G_{\mathbb{Q}}$-equivariant isomorphism $T_l(E)\simeq \mathrm{Hom}(T_l(E),\mathbb{Z}_l)(1)$. Moreover, $T_l=\mathbb{Z}_l[G]\otimes_{\mathbb{Z}_l} T_l(E)$ as (left) G-module, so that the assertion easily follows. For the same reason we always have

$$\det\left(1-Fr_p^{-1}\mid V_l^{I_p}\right)=(L_p(E,\bar{\chi},1))_{\chi\in\mathrm{Irr}(G)}. \tag{13}$$

We now set

$$\mathcal{L}^*:=\left(L^*(E/\mathbb{Q},\bar{\psi},1)\right)_{\psi\in\mathrm{Irr}(G)}\in\zeta(\mathbb{R}[G])^\times,$$

so that $L^*(M_K)=\mathcal{L}^*$. If we define

$$T\Omega:=R\Omega+\delta(\mathcal{L}^*),$$

then the ETNC (see [12, Conj. 4 (iv)]) for the pair $(M_K,\mathbb{Z}[G])$ can be stated in the form

Conjecture 3.4.

$$T\Omega=0 \text{ in } K_0(\mathbb{Z}[G],\mathbb{R}).$$

For a set of places P of $\mathbb{Q}$ we write $P(K)$ for the set of places of K lying above places in P. In the next section we will (assuming the rationality conjecture [12, Conj. 4 (iii)] and certain further hypothesis on K, E and l) describe the l-part $T\Omega_l\in K_0(\mathbb{Z}_l[G],\mathbb{Q}_l)$ of $T\Omega$ in terms of refined Euler characteristics. To that end we will define a $\mathbb{Z}_l[G]$-perfect complex $R\Gamma_f(\mathbb{Q},T_l)$ and for each $v\in S_\infty(K)\cup S_l(K)$ a $\mathbb{Z}_l[G]$-perfect complex $R\Gamma_f(K_v,T_l(E))$ such that there is an exact triangle

$$\bigoplus_{v\in S_\infty(K)\cup S_l(K)} R\Gamma_f(K_v,T_l(E))[-1]\longrightarrow R\Gamma_c(\mathbb{Z}_{S_l},T_l)\longrightarrow R\Gamma_f(K,T_l(E)).$$

This may be considered as an explicit integral version of the middle column of diagram (26) in [12].

We will now use the additivity of refined Euler characteristics (see [9, Th. 5.7] and our Remark 2.2) and the explicit nature of the complexes $R\Gamma_f(K,T_l(E))$ and $R\Gamma_f(K_v,T_l(E))$ to describe $R\Omega$. We write $\chi_{\mathbb{Z}_l[G],\mathbb{C}_l}$ for the refined Euler characteristic introduced in [13]. In this way we obtain

$$\begin{aligned} R\Omega_l &= \chi_{\mathbb{Z}_l[G],\mathbb{C}_l}\left(\bigoplus_{v\in S_\infty(K)\cup S_l(K)} R\Gamma_f(K_v,T_l(E))[-1],\pi_K^{-1}\right)\\ &+ \chi_{\mathbb{Z}_l[G],\mathbb{C}_l}\left(R\Gamma_f(K,T_l(E)),\delta^{-1}\right). \end{aligned} \tag{14}$$

To conclude this section we aim to formulate an explicit rationality conjecture. As we will see one has

$$H_f^i(K,V_l(E))=H_f^i(K,T_l(E))\otimes_{\mathbb{Z}_l}\mathbb{Q}_l=\begin{cases}0, & i\neq 1,2,\\ E(K)\otimes_{\mathbb{Z}}\mathbb{Q}_l, & i=1,\\ (E(K)\otimes_{\mathbb{Z}}\mathbb{Q}_l)^*, & i=2.\end{cases} \tag{15}$$

Moreover, by [12, (28)] there is an isomorphism in $D^{perf}(\mathbb{Q}_l[G])$

$$\bigoplus_{v\in S_\infty(K)} R\Gamma_f(K_v,V_l(E))\simeq\left(M_B^+\otimes_{\mathbb{Q}}\mathbb{Q}_l\right)[0],$$

and by [12, (22)] an exact triangle

$$\left(\left(M_{dR}/M_{dR}^0\right)\otimes_{\mathbb{Q}}\mathbb{Q}_p\right)[-1]\longrightarrow\bigoplus_{v|l}R\Gamma_f(K_v,V_l(E))\longrightarrow\bigoplus_{v|l}\left(V_{l,v}\xrightarrow{\phi_v}V_{l,v}\right).$$

Just for the moment, we content ourselves with observing that the terms resulting from $\left(V_{l,v}\xrightarrow{\phi_v}V_{l,v}\right)$ for $v\in S_l(K)$ are rational and, in fact, will give certain Euler factors. In order to state the rationality conjecture we can therefore neglect these terms. To tie up with the situation described in (4) we set

$$\begin{aligned}
Y^{ev}&:=(E(K)\otimes_{\mathbb{Z}}\mathbb{Q})^*\oplus\left(M_{dR}/M_{dR}^0\right),\\
Y^{od}&:=(E(K)\otimes_{\mathbb{Z}}\mathbb{Q})\oplus M_B^+,\\
\theta_{\mathbb{R}}&:=\delta^{-1}\oplus\pi_K^{-1},\\
X_l^\bullet&:=R\Gamma_f(K,T_l(E))\oplus\bigoplus_{v|l\infty}R\Gamma_f(K_v,T_l(E))[-1].
\end{aligned}$$

Recall that for the rationality conjecture we do not have to consider the maps θ_l^{ev} and θ_l^{od} (see Remark 2.6). Note also that it is usually more convenient to separate the height and period isomorphism and thus to consider

$$\begin{aligned}
&Y_1^{ev}:=(E(K)\otimes_{\mathbb{Z}}\mathbb{Q})^*,\quad Y_1^{od}:=E(K)\otimes_{\mathbb{Z}}\mathbb{Q},\quad \theta_{1,\mathbb{R}}:=\delta^{-1},\\
&X_{1,l}^\bullet:=R\Gamma_f(K,T_l(E))
\end{aligned}$$

and

$$\begin{aligned}
&Y_2^{ev}:=\left(M_{dR}/M_{dR}^0\right),\quad Y_2^{od}:=M_B^+,\quad \theta_{2,\mathbb{R}}:=\pi_K^{-1},\\
&X_{2,l}^\bullet:=\bigoplus_{v|l\infty}R\Gamma_f(K_v,T_l(E))[-1].
\end{aligned}$$

Let τ_1 be defined as in Remark 2.6 (b) with respect to Y_1^{ev} and Y_1^{od}. Let α_0 be a normal basis element for $K/\mathbb{Q}$. For each $\chi\in\mathrm{Irr}(G)$ we choose a $\mathbb{C}$-space V_χ which realizes χ. Let $T_\chi:G\longrightarrow\mathrm{Gl}(V_\chi)$ denote the corresponding representation and define $d_+(\chi):=\dim_{\mathbb{C}}\left(V_\chi^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}\right)$ and $d_-(\chi):=\mathrm{codim}_{\mathbb{C}}\left(V_\chi^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}\right)$.

We set

$$\begin{aligned}
\mathrm{Reg}&=\left(\mathrm{Reg}_\chi\right)_{\chi\in\mathrm{Irr}(G)}:=\mathrm{Nrd}_{\mathbb{R}[G]}(\tau_1),\\
R=R(\alpha_0)=\left(R_\chi\right)_{\chi\in\mathrm{Irr}(G)}&:=\left(\det\left(\sum_{\sigma\in G}\iota(\sigma(\alpha_0))T_\chi(\sigma^{-1})\right)\right)_{\chi\in\mathrm{Irr}(G)},\\
\Omega=\left(\Omega_\chi\right)_{\chi\in\mathrm{Irr}(G)}&:=\left(\Omega_+^{d_+(\chi)}\Omega_-^{d_-(\chi)}\right)_{\chi\in\mathrm{Irr}(G)},
\end{aligned}$$

and note that $\mathrm{Nrd}_{\mathbb{R}[G]}(\lambda_{\alpha_0})=\Omega/R(\alpha_0)$, where λ_{α_0} is defined in Proposition 3.1. From Remark 2.6 (b) we deduce that the rationality part of [12, Conjecture 4] is equivalent to

Conjecture 3.5.

$$u\in\zeta(\mathbb{Q}[G])^\times,\ \text{where } u:=\frac{\mathcal{L}^*R}{\Omega\mathrm{Reg}}\ \text{and } \mathcal{L}^*:=\left(L^*(E/\mathbb{Q},\bar\psi,1)\right)_{\psi\in\mathrm{Irr}(G)}.$$

Remark 3.6. Conjecture 3.5 does not depend on the choice of α_0. Indeed, if β_0 is another normal basis element, then $\beta_0=\lambda\alpha_0$ with $\lambda\in\mathbb{Q}[G]^\times$. It is then easy to see that $R(\beta_0)=\mathrm{Nrd}_{\mathbb{Q}[G]}(\lambda)R(\alpha_0)$.

We will compute complex approximations to

$$u = (u_\chi)_{\chi \in \mathrm{Irr}(G)} \in \prod_\chi \mathbb{C}^\times \simeq \zeta(\mathbb{C}[G])^\times$$

and then use Lemma 2.8 to numerically verify the rationality conjecture.

4. Explicit version of the ETNC

In this section we will define the complexes $R\Gamma_f(\mathbb{Q}, T_l)$ and $R\Gamma_f(\mathbb{Q}_p, T_l)$ and explicitly describe their cohomology. We will closely follow [11] and [14, Sec. 12].

Under certain hypothesis on E, K and l (see below), we will derive an explicit version of ETNC in terms of refined Euler characteristics of classical objects of the theory of elliptic curves, such as the Mordell-Weil group and the Tate-Shafarevic group.

We fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ and an embedding $\iota\colon \bar{\mathbb{Q}} \longrightarrow \mathbb{C}$. Recall that we have defined $\tau \in G$ by $c \circ \iota = \iota \circ \tau$ with $c \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ denoting complex conjugation. We set $G_\infty = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and identify G_∞ via ι with a subgroup of $G_\mathbb{Q}$. For each rational prime p we fix an embedding $j_p\colon \bar{\mathbb{Q}} \longrightarrow \bar{\mathbb{Q}}_p$. With respect to j_p we let $G_p \subseteq G_\mathbb{Q}$ denote the decomposition group and $I_p \subseteq G_p$ the ramification subgroup. Finally we let $\bar{I}_p \subseteq \bar{G}_p \subseteq G$ denote the ramification and decomposition group of p in $K/\mathbb{Q}$.

For a profinite group Π and a continuous Π-module N we denote by $C^\bullet(\Pi, N)$ the standard complex of continuous cochains. We write $\mathbb{Z}_{S_l}$ for the ring of S_l integers and G_{S_l} for the Galois group of the maximal subextension of $\bar{\mathbb{Q}}$ which is unramified outside S_l. Following [12, Sec. 3.2-3.4] we set

$$\begin{aligned} R\Gamma(\mathbb{Z}_{S_l}, T_l) &:= C^\bullet(G_{S_l}, T_l), \\ R\Gamma_c(\mathbb{Z}_{S_l}, T_l) &:= \mathrm{Cone}\left(R\Gamma(\mathbb{Z}_{S_l}, T_l) \longrightarrow \bigoplus_{p \in S_l} C^\bullet(G_p, T_l) \right)[-1], \end{aligned}$$

where the morphism here is induced by the natural maps $G_p \subseteq G_\mathbb{Q} \longrightarrow G_{S_l}$.

We now proceed to define the remaining complexes in the true triangle

$$R\Gamma_c(\mathbb{Z}_{S_l}, T_l) \longrightarrow R\Gamma_f(\mathbb{Q}, T_l) \longrightarrow \bigoplus_{p \in S_l \cup \{\infty\}} R\Gamma_f(\mathbb{Q}_p, T_l)$$

Our aim is to define these complexes such that they are $\mathbb{Z}_l[G]$-perfect. We point out that for $l \nmid \#G$ the algebra $\mathbb{Z}_l[G]$ is regular, so that every complex of $\mathbb{Z}_l[G]$-modules with only finitely many non-trivial cohomology groups all of which are finitely generated is automatically perfect.

For a finite place v of K we write $\mathcal{O}_{K_v}$ for the valuation ring in the completion K_v and $\mathfrak{m}_v$ for the maximal ideal. Let $k_v := \mathcal{O}_{K_v}/\mathfrak{m}_v$ denote the residue class field. We write $E_0(K_v)$ for the points of $E(K_v)$ which reduce to a non-singular point on the reduced curve $\bar{E}(k_v)$. Let $\bar{E}_{ns}(k_v)$ denote the group of non-singular points of $\bar{E}(k_v)$.

We will need the following

Hypothesis:

(H0) $Ш(E/K)$ is finite.

(H1) l is at most tamely ramified in $K/\mathbb{Q}$.

(H2) (a) If $l \in S$ or $l = 2$, then $l \nmid \#G$.

(b) If $l \notin S$ and $l \neq 2$, then $l \nmid \bar{I}_p$ for all $p \in S$.

(H3) $S_{bad}(E) \cap S_{ram}(K/\mathbb{Q}) = \emptyset$.
(H4) If $l \mid \#G$, then
 (a) $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$, $(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*$ are $\mathbb{Z}_l[G]$-perfect and $l \nmid \#E(K)_{tors}$.
 (b) $l \nmid \#\text{Ш}(E/K)$.
(H5) If $l \notin S$ and $l \neq 2$, then $l \nmid \#(E(K_v)/E_0(K_v))$ for all $v \in S(K)$.

(H2) and (H3) are needed to show that the above complexes are perfect. (H1), (H4) and (H5) will be needed to be able to compute the refined Euler characteristics of these complexes. Note that (H2) possibly excludes certain prime divisors l of $\#G$ from our considerations. However, in certain circumstances all of the hypothesis (H1) - (H5) are conjecturally satisfied for some divisors l of $\#G$. Explicit examples are given in Section 6. We remark also that with some additional effort it would be possible to relax (H5) by stipulating it only for $l \mid \#G$, but for a related, more complicated module. However, in this case the computation of the relevant Euler characteristics becomes more complicated and less suitable for numerical computations (see Remark 4.3).

If $p = \infty$ we define $R\Gamma_f(\mathbb{Q}_p, T_l)$ to be the complex $H^0(\mathbb{Q}_\infty, T_l)[0] = T_l^{G_\infty}[0]$. Then $R\Gamma_f(\mathbb{Q}_\infty, T_l)$ is indeed a perfect complex. This is clear for $l \nmid \#G$ by the preceeding remark. In general, we may identify $E(\mathbb{C})$ with the complex torus $\mathbb{C}/(\mathbb{Z}\Omega_+ \oplus \mathbb{Z}\Omega_-)$. In this way we obtain an isomorphism of G_∞-modules $T_l(E) \simeq \mathbb{Z}_l\Omega_+ \oplus \mathbb{Z}_l\Omega_-$. Using this identification it is clear that

$$T_l(E)^{G_v} \simeq \begin{cases} \mathbb{Z}_l\Omega_+, & \text{if } v \text{ is real}, \\ \mathbb{Z}_l\Omega_+ \oplus \mathbb{Z}_l\Omega_-, & \text{if } v \text{ is complex}, \end{cases}$$

for each $v \mid \infty$. Hence $R\Gamma_f(\mathbb{Q}_\infty, T_l)$ is free of rank 1 as a $\mathbb{Z}_l[G]$-module generated by Ω_+ if K is totally real, and by $\frac{1+\tau}{2} \otimes \Omega_+ + \frac{1-\tau}{2} \otimes \Omega_-$ if K is complex (note that $l \neq 2$ by (H2a) if K is complex). For later reference we record

$$T_l^{G_\infty} \simeq \mathbb{Z}_l[G]\left(\frac{1+\tau}{2} \otimes \Omega_+ + \frac{1-\tau}{2} \otimes \Omega_-\right). \tag{16}$$

For a $\mathbb{Z}$-module A we write $A^{\wedge l}$ for the l-completion $\varprojlim A/l^n A$. For each pair of primes p and l we write $H^1_f(\mathbb{Q}_p, T_l)_{BK}$ for the finite support cohomology group defined by Bloch and Kato in [6, Sec. 3]. We will explicitly describe this group. From Kummer theory we obtain a natural monomorphism $E(K_v)^{\wedge l} \longrightarrow H^1(K_v, T_l(E))$ for each place $v \mid p$. By [6, after (3.2)] the group $H^1_f(K_v, T_l(E))_{BK}$ is equal to the image of $E(K_v)$ in $H^1(K_v, T_l(E))$ under the composite map $E(K_v) \longrightarrow E(K_v)^{\wedge l} \longrightarrow H^1(K_v, T_l(E))$. Using (23) one can show that $E(K_v) \longrightarrow E(K_v)^{\wedge l}$ is onto, so that

$$H^1_f(\mathbb{Q}_p, T_l)_{BK} \simeq \bigoplus_{v \mid p} E(K_v)^{\wedge l}.$$

The next definition is motivated by [14, Sec. 12.2 and Rem. 12.4.2]. We need the following notations. If $p \notin S$ and $p \neq 2$, then we define a finitely generated $\mathbb{Z}_p[G]$-module by setting $\mathcal{D}_p := D_{cr,p}(T_p) \simeq \mathcal{O}_{K,p} \otimes_{\mathbb{Z}_p} D_{cr,p}(T_p(E))$ where $\mathcal{O}_{K,p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K$ and $D_{cr,p}$ is the quasi-inverse to the functor of Fontaine and Lafaille that is used by Niziol in [31]. For each such p we also write ϕ_p for the natural $\mathbb{Z}_p[G]$-equivariant Frobenius on $\mathcal{D}_p$.

We define

$$R\Gamma_f(\mathbb{Q}_p, T_l) = \begin{cases} T_l^{I_p} \overset{1-Fr_p^{-1}}{\longrightarrow} T_l^{I_p}, & \text{if } l \notin S, l \neq 2, l \neq p, \\ F^0\mathcal{D}_p \overset{1-\phi_p^0}{\longrightarrow} \mathcal{D}_p, & \text{if } l \notin S, l \neq 2, l = p, \\ H^1_f(\mathbb{Q}_p, T_l)_{BK}, & \text{if } l \in S \text{ or } l = 2, \end{cases}$$

where Fr_p is the natural Frobenius in $\mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$, ϕ_p^0 is the restriction of ϕ_p to $F^0\mathcal{D}_p \subseteq \mathcal{D}_p$. In the first two cases the modules are placed in degrees 0 and 1, in the third case the module is placed in degree 1.

The following lemma and its proof are analogous to [14, Lem. 12.2.1].

Lemma 4.1. *Assume (H2) and (H3). Then $R\Gamma_f(\mathbb{Q}_p, T_l)$ is a perfect complex of $\mathbb{Z}_l[G]$-modules.*

Proof. If $l \in S$ or $l = 2$ the result is clear because in this case $\mathbb{Z}_l[G]$ is regular. If $l \notin S, l \neq 2$ and $l = p$ we note that p is unramified in $K/\mathbb{Q}$ by definition of S, and hence $\mathcal{O}_{K,p}$ is a free $\mathbb{Z}_p[G]$-module.Thus $F^0\mathcal{D}_p \simeq \mathcal{O}_{K,p} \otimes_{\mathbb{Z}_p} F^0 D_{cr,p}(T_p(E))$ and $\mathcal{D}_p \simeq \mathcal{O}_{K,p} \otimes_{\mathbb{Z}_p} D_{cr,p}(T_p(E))$ are finitely generated $\mathbb{Z}_p[G]$-modules of finite projective dimension.

Finally, if $l \notin S, l \neq 2$ and $l \neq p$, we first note that

$$T_l^{I_p} = (\mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l} T_l(E))^{I_p} = \mathbb{Z}_l[G]^{I_p} \otimes_{\mathbb{Z}_l} T_l(E)^{I_p}$$

because of (H3). If $p \in S_{ram}(K/\mathbb{Q})$, then $T_l^{I_p} = \mathbb{Z}_l[G]^{\bar{I}_p} \otimes_{\mathbb{Z}_l} T_l(E)$. We write $e_{\bar{I}_p}$ for the idempotent associated with $\bar{I}_p$. By (H2b) we have $\mathbb{Z}_l[G] = \mathbb{Z}_l[G]e_{\bar{I}_p} \oplus \mathbb{Z}_l[G](1 - e_{\bar{I}_p}) = \mathbb{Z}_l[G]^{\bar{I}_p} \oplus \mathbb{Z}_l[G](1 - e_{\bar{I}_p})$. Therefore $T_l^{I_p}$ is a direct summand of $\mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l} T_l(E) \simeq \mathbb{Z}_l[G]^2$ and thus projective.

If $p \in S_{bad}(E)$, then $T_l^{I_p} = \mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l} T_l(E)^{I_p}$ is clearly $\mathbb{Z}_l[G]$-free. $\square$

We define the complex $R\Gamma(\mathbb{Q}, T_l)$ as in [11, (1.33)] and proceed to recall the computation of its cohomology (for more details see [11, Sec. 1.5.1]). For an arbitrary $\mathbb{Z}_l$-module W we write W^* for the linear dual $\mathrm{Hom}_{\mathbb{Z}_l}(W, \mathbb{Z}_l)$ and $W^\vee$ for the Pontriyagin dual $\mathrm{Hom}_{cont}(W, \mathbb{Q}_l/\mathbb{Z}_l)$.

We note that the Weil pairing induces an isomorphism between T_l and $T_l^*(1)$. Furthermore, we recall that

$$H^i(\mathbb{Z}_{S_l}, T_l) \simeq \begin{cases} 0, & \text{if } i = 0, \\ E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l, & \text{if } i = 1. \end{cases}$$

4.1. **The case $l \notin S$ and $l \neq 2$.** For a finite $\mathbb{Z}$-module C we write C_{l^∞} for the l-Sylow subgroup of C.

From [11, (1.35)-(1.37)] we derive

$$\begin{aligned} &H^0_f(\mathbb{Q}, T_l) = H^0(\mathbb{Z}_{S_l}, T_l) = 0, \\ &H^3_f(\mathbb{Q}, T_l) = \left(H^1(\mathbb{Z}_{S_l}, T_l^*(1))_{tors}\right)^\vee \simeq \left((E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)_{tors}\right)^\vee, \\ &H^i_f(\mathbb{Q}, T_l) = 0 \text{ for } i \geq 4. \end{aligned}$$

Defining $Ш(T_l^*(1))$ as in [11] we have the short exact sequence (see [11, (1.36)])

$$0 \longrightarrow Ш(T_l^*(1))^\vee \longrightarrow H^2_f(\mathbb{Q}, T_l) \longrightarrow H^1_f(\mathbb{Q}, T_l^*(1))^* \longrightarrow 0. \tag{17}$$

By this sequence we identify $H^2_f(\mathbb{Q}, T_l)_{tors}$ with $Ш(T_l^*(1))^\vee$ and $H^2_f(\mathbb{Q}, T_l)_{tf}$ with $H^1_f(\mathbb{Q}, T_l^*(1))^*$.

We let

$$C(\mathbb{Q}_p, T_l) \simeq H^0(\mathbb{Q}_p, H^1(I_p, T_l)_{tors})$$

be the module introduced in [11, (1.38)], so that we have exact sequences (by [11, 1.38)] and the displayed exact sequence succeeding it)

$$0 \longrightarrow H^1_f(\mathbb{Q}_p, T_l) \longrightarrow H^1_f(\mathbb{Q}_p, T_l)_{BK} \longrightarrow C(\mathbb{Q}_p, T_l) \longrightarrow 0 \tag{18}$$

and

(19)

$$0 \longrightarrow H^1_f(\mathbb{Q}, T_l) \longrightarrow H^1_f(\mathbb{Q}, T_l)_{BK} \longrightarrow \mathcal{C} \longrightarrow Ш(T_l^*(1))^\vee \longrightarrow Ш(T_l^*(1))^\vee_{BK} \longrightarrow 0.$$

with

$$\mathcal{C} := \bigoplus_{p \in S_l} C(\mathbb{Q}_p, T_l).$$

We claim that under our assumptions the module $\mathcal{C}$ is trivial. If $p = l$, then $H^1(I_l, T_l) = \mathrm{Hom}_{\mathrm{cont}}(I_l, T_l)$ because I_l acts trivial on T_l (recall that $l \notin S$). Therefore $H^1(I_l, T_l)$ is torsion free and $C(\mathbb{Q}_l, T_l)$ is trivial. Assume now that $p \neq l$. We fix a place v of K above p and set $L := K_v\mathbb{Q}_p^{ur}$ where $\mathbb{Q}_p^{ur}$ denotes the maximal unramified extension of $\mathbb{Q}_p$. Furthermore we put $U := \mathrm{Gal}(\bar{\mathbb{Q}}_p/L)$. From the inflation-restriction sequence we derive

$$0 \longrightarrow H^1(\bar{I}_p, T_l^U) \longrightarrow H^1(I_p, T_l) \longrightarrow H^1(U, T_l)^{\bar{I}_p} \longrightarrow H^2(\bar{I}_p, T_l^U).$$

If $p \in S_{ram}(K/\mathbb{Q})$, then $p \notin S_{bad}(E)$ because of (H3) and we obtain $T_l^U = \mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l} T_l(E)$ which is a cohomologically trivial $\bar{I}_p$-module. Hence $H^1(I_p, T_l) \simeq H^1(U, T_l)^{\bar{I}_p} \simeq \mathrm{Hom}_{cont}(U, T_l)^{\bar{I}_p}$, where the second isomorphism holds because U acts trivially on T_l. It follows that $H^1(I_p, T_l)$ is torsion free which, in turn, proves the claim for primes $p \in S_{ram}(K/\mathbb{Q})$.

For $p \notin S_{ram}(K/\mathbb{Q})$ we have $\bar{I}_p = 1$, so that we get $H^1(I_p, T_l) \simeq H^1(U, T_l)$. Now $U = I_p$ acts trivially on $\mathbb{Z}_l[G]$ and we obtain $H^1(I_p, T_l) \simeq \mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l} H^1(U, T_l(E))$. It follows that

$$\begin{aligned} & H^1(I_p, T_l)_{tors}^{G_p} \\ \simeq\ & \left(\mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l} H^1(I_p, T_l(E))_{tors}\right)^{G_p} \\ \simeq\ & \mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l[\bar{G}_p]} H^1(I_p, T_l(E))_{tors}^{\mathrm{Gal}(\bar{\mathbb{Q}}_p/K_v)}. \end{aligned}$$

By [23, Exp. IX, (11.3.8)] the group $H^1(I_p, T_l(E))_{tors}^{\mathrm{Gal}(\bar{\mathbb{Q}}_p/K_v)}$ can be identified with the l-primary part of $E(K_v)/E_0(K_v)$ and the claim follows now from (H5).

From (18) and (19) we now deduce

$$H^1_f(\mathbb{Q}_p, T_l) \simeq H^1_f(\mathbb{Q}_p, T_l)_{BK}, H^1_f(\mathbb{Q}, T_l) \simeq H^1_f(\mathbb{Q}, T_l)_{BK}, Ш(T_l^*(1)) \simeq Ш(T_l^*(1))_{BK}.$$

By [11, (1.39)] we may identify $Ш(T_l^*(1))^\vee_{BK}$ with $Ш(T_l)_{BK}$, which in turn identifies with $Ш(E/K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$.

We recall from [6, Prop. 5.4] that $H^1_f(\mathbb{Q}, T_l)_{BK} \simeq E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$, so that

$$H^1_f(\mathbb{Q}, T_l) \simeq E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l, \quad H^2_f(\mathbb{Q}, T_l)_{tf} \simeq \left(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l\right)^*.$$

Our next aim is to compute the refined Euler characteristic $\chi_{\mathbb{Z}_l[G], \mathbb{C}_l}(R\Gamma_f(\mathbb{Q}, T_l), \delta^{-1})$ introduced in (14) in terms of classical modules of the theory of elliptic curves. In full generality this is a very difficult task because it seems to be very hard to compute the complex $R\Gamma_f(\mathbb{Q}, T_l)$. Our hypothesis allow us to use [12, Prop. 2.1 (4)], so that we can work entirely with the cohomology modules.

Lemma 4.2. *Assume (H0) - (H5) and write* $\chi = \chi_{\mathbb{Z}_l[G],\mathbb{C}_l}$. *Then*

$$\begin{aligned}\chi(R\Gamma_f(\mathbb{Q},T_l),\delta^{-1}) &= [(E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l)^*, \delta^{-1}, E(K)_{tf}\otimes_{\mathbb{Z}}\mathbb{Z}_l] \\ &- \chi(\text{Ш}(E/K)_{l^\infty},0) \\ &+ \chi(E(K)_{l^\infty},0)+\chi(E(K)^\vee_{l^\infty},0)\end{aligned}$$

Proof. The proof follows from the preceeding computation of cohomology and Lemma 2.3. □

Remark 4.3. If we relax (H5) the module $\mathcal{C}$ is possibly non-trivial. Combining the exact sequences (17) and (19) we derive

$$0 \longrightarrow H^1_f(\mathbb{Q},T_l) \longrightarrow H^1_f(\mathbb{Q},T_l)_{BK} \longrightarrow \mathcal{C} \longrightarrow H^2_f(\mathbb{Q},T_l) \longrightarrow \mathcal{S} \longrightarrow 0 \tag{20}$$

with a module $\mathcal{S}$ which sits is a short exact sequence of the form

$$0 \longrightarrow \text{Ш}(E/K)\otimes_{\mathbb{Z}}\mathbb{Z}_l \longrightarrow \mathcal{S} \longrightarrow H^1_f(\mathbb{Q},T_l)^* \longrightarrow 0. \tag{21}$$

The module $\mathcal{S}$ is related to the integral Selmer group defined by Mazur and Tate in [29] (see [14, Lem. 12.2.2] and its proof). It is certainly possible to compute $\chi(R\Gamma_f(\mathbb{Q},T_l),\delta^{-1})$ in this more general setting for $l\nmid \#G$, however, any description of $\chi(R\Gamma_f(\mathbb{Q},T_l),\delta^{-1})$ would then involve the modules $\mathcal{S}$, $\mathcal{C}$ and $\text{Ш}(T_l^*(1))$. For computational purposes this seems to be less useful.

We now compute $\chi(R\Gamma_f(\mathbb{Q}_p,T_l),0)$ for $p\neq l,\infty$. Recall that we are still in the case $l\notin S, l\neq 2$. From the definition of $R\Gamma_f(\mathbb{Q}_p,T_l)$ we immediately obtain

$$\chi(R\Gamma_f(\mathbb{Q}_p,T_l),0) = [T_l^{I_p}, 1-Fr_p^{-1}, T_l^{I_p}].$$

By Remark 3.3 this Euler characteristic is represented by $(L(E/\mathbb{Q},\bar\chi,1))_{\chi\in\mathrm{Irr}(G)}$.

We let $\mathcal{E}$ be a Néron model for E over $\mathbb{Z}$. Because of hypothesis (H3) we may regard $\mathrm{Spec}(\mathcal{O}_K)\times_{\mathrm{Spec}(\mathbb{Z})}\mathcal{E}$ as a Néron model $\mathcal{E}_K$ of E over K. Recall that we identified $t_{dR}(M_K) := M_{dR}/M^0_{dR} \simeq H^1(E_K,\mathcal{O}_{E_K}) \simeq K\otimes_{\mathbb{Q}}\Omega^1_E(E)^*$. In this way the integral lattice $H^1(\mathcal{E}_K,\mathcal{O}_{\mathcal{E}_K})$ is identified with $\mathcal{O}_K\otimes_{\mathbb{Z}}\Omega^1_{\mathcal{E}}(\mathcal{E})^*$. Recall that $\Omega^1_{\mathcal{E}}(\mathcal{E})^* = \mathbb{Z}\omega_0^*$. We define $H_{K,\mathbb{Z}} := \bigoplus_{\sigma\in\Sigma(K)}\mathbb{Z}\subseteq H_K$ and $\mathcal{H}_{\mathbb{Z}} := \mathrm{Hom}_{\mathbb{Z}}(H^1(E(\mathbb{C}),\mathbb{Z}),2\pi i\mathbb{Z})\subseteq\mathcal{H}$. Finally we define $H_{K,\mathbb{Z}_l} := \mathbb{Z}_l\otimes_{\mathbb{Z}} H_{K,\mathbb{Z}}$ and $\mathcal{H}_{\mathbb{Z}_l} := \mathbb{Z}_l\otimes_{\mathbb{Z}}\mathcal{H}_{\mathbb{Z}}$.

We will compare the refined Euler characteristic of

$$R\Gamma_f(\mathbb{Q}_\infty,T_l)\oplus R\Gamma_f(\mathbb{Q}_l,T_l).$$

with the l-part of

$$\Big[(H_{K,\mathbb{Z}}\otimes_{\mathbb{Z}}\mathcal{H}_{\mathbb{Z}})^+, \pi_K, H^1(\mathcal{E}_K,\mathcal{O}_{\mathcal{E}_K})\Big] = \Big[(H_{K,\mathbb{Z}}\otimes_{\mathbb{Z}}\mathcal{H}_{\mathbb{Z}})^+, \pi_K, \mathcal{O}_K\otimes_{\mathbb{Z}}\Omega^1_{\mathcal{E}}(\mathcal{E})^*\Big]$$

in $K_0(\mathbb{Z}_l[G],\mathbb{C}_l)$.

Using the fixed embedding $\iota\colon K\longrightarrow\mathbb{C}$ we identify $H_{K,\mathbb{Z}}\simeq\mathbb{Z}[G]$. It is easily shown that

$$(H_{K,\mathbb{Z}_l}\otimes_{\mathbb{Z}_l}\mathcal{H}_{\mathbb{Z}_l})^+ = \mathbb{Z}_l[G]\left(\frac{1+\tau}{2}\otimes\gamma_+^* + \frac{1-\tau}{2}\otimes\gamma_-^*\right).$$

By (16) we may therefore identify $R\Gamma_f(\mathbb{Q}_\infty,T_l) = T_l^{G_\infty}[0]$ and $(H_{K,\mathbb{Z}_l}\otimes_{\mathbb{Z}_l}\mathcal{H}_{\mathbb{Z}_l})^+$.

For each prime p we write $t_p(V_p)$ for the tangent space $D_{dR}(V_p)/F^0D_{dR}(V_p)$ of V_p (see [12, page 521] for the precise definition) and

$$\kappa_p\colon \mathbb{Q}_p \otimes_{\mathbb{Q}} t_{dR}(M_K) \longrightarrow t_p(V_p)$$

for the canonical comparison isomorphism of [12, (23)]. For any embedding $j\colon \mathbb{R} \longrightarrow \mathbb{C}_l$ we write $\pi_{K,j}$ for the composite map

$$\mathbb{C}_l \otimes_{\mathbb{R},j} \mathbb{R} \otimes_{\mathbb{Q}} (H_K \otimes_{\mathbb{Q}} \mathcal{H})^+] \stackrel{(\mathbb{C}_l\otimes\pi_K)}{\longrightarrow} \mathbb{C}_l \otimes_{\mathbb{R},j} \mathbb{R} \otimes_{\mathbb{Q}} K \otimes_{\mathbb{Q}} \Omega^1_E(E)^* \stackrel{(\mathbb{C}_l\otimes\kappa_l)}{\longrightarrow} \mathbb{C}_l \otimes_{\mathbb{Q}_l} t_l(V_l).$$

Since $l \notin S$ and $l \ne 2$ the theory of Fontaine and Messing implies that

$$\kappa_l\left(\mathbb{Z}_l \otimes_{\mathbb{Z}} H^1(\mathcal{E}_K, \mathcal{O}_{\mathcal{E}_K})\right) = \mathcal{D}_l/F^0\mathcal{D}_l$$

(see the proof of [14, Lem. 12.4.1]). In particular, $\mathcal{D}_l/F^0\mathcal{D}_l$ is $\mathbb{Z}_l[G]$-projective since $\mathbb{Z}_l \otimes_{\mathbb{Z}} H^1(\mathcal{E}_K, \mathcal{O}_{\mathcal{E}_K}) \simeq \mathbb{Z}_l \otimes_{\mathbb{Z}} \mathcal{O}_K \otimes_{\mathbb{Z}} \Omega^1_{\mathcal{E}}(\mathcal{E})^*$ is $\mathbb{Z}_l[G]$-free as $l \notin S$ is unramified in $K/\mathbb{Q}$.

Since $\mathcal{D}_l \stackrel{1-\phi_l}{\longrightarrow} \mathcal{D}_l$ is injective, the short exact sequence of complexes (with vertical differentials)

$$\begin{tikzcd}
0 \arrow[r] & F^0\mathcal{D}_l \arrow[r, "\subseteq"] \arrow[d, "1-\phi_l^0"] & \mathcal{D}_l \arrow[r] \arrow[d, "1-\phi_l"] & \mathcal{D}_l/F^0\mathcal{D}_l \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{D}_l \arrow[r, "="] & \mathcal{D}_l \arrow[r] & 0 &
\end{tikzcd}$$

implies that $0 \longrightarrow \mathcal{D}_l/F^0\mathcal{D}_l \longrightarrow H^1_f(\mathbb{Q}_l, T_l) \longrightarrow \mathcal{D}_l/(1-\phi_l)\mathcal{D}_l \longrightarrow 0$ is exact. It follows that $H^1_f(\mathbb{Q}_l, T_l)$ is $\mathbb{Z}_l[G]$-perfect and

$$\begin{aligned}
& j_*\left(\left[(H_{K,\mathbb{Z}} \otimes_{\mathbb{Z}} \mathcal{H}_{\mathbb{Z}})^+, \pi_K, \mathcal{O}_K \otimes_{\mathbb{Z}} \Omega^1_{\mathcal{E}}(\mathcal{E})^*\right]\right) \\
= & \left[T_l^{G_\infty}, \pi_{K,j}, \kappa_l\left(\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathcal{O}_K \otimes_{\mathbb{Z}} H^1(\mathcal{E}_K, \mathcal{O}_{\mathcal{E}_K})\right)\right] \\
= & \left[T_l^{G_\infty}, \pi_{K,j}, \mathcal{D}_l/F^0\mathcal{D}_l\right] \\
= & \left[T_l^{G_\infty}, \pi_{K,j}, H^1_f(\mathbb{Q}_l, T_l)\right] - [\mathcal{D}_l, 1-\phi_l, \mathcal{D}_l] \\
= & \chi_{\mathbb{Z}_l[G],\mathbb{C}_l}\left(R\Gamma_f(\mathbb{Q}_\infty, T_l) \oplus R\Gamma_f(\mathbb{Q}_l, T_l), \pi_K\right) - [\mathcal{D}_l, 1-\phi_l, \mathcal{D}_l],
\end{aligned}$$

where the last equality follows from Lemma 2.3.

In summary, we obtain for $l \notin S$, $l \ne 2$

$$\begin{aligned}
& R\Omega_l = \\
& [(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*, \delta^{-1}, E(K)_{tf} \otimes_{\mathbb{Z}} \mathbb{Z}_l] + \chi(E(K)_{l^\infty}, 0) + \chi(E(K)^\vee_{l^\infty}, 0) \\
& -\chi(Ш(E/K)_{l^\infty}, 0) - \sum_{p\in S}\left[T_l^{I_p}, 1-Fr_p^{-1}, T_l^{I_p}\right] \\
& -j_*\left(\left[(H_{K,\mathbb{Z}} \otimes_{\mathbb{Z}} \mathcal{H}_{\mathbb{Z}})^+, \pi_K, \mathcal{O}_K \otimes_{\mathbb{Z}} \Omega^1_{\mathcal{E}}(\mathcal{E})^*\right]\right) - [\mathcal{D}_l, 1-\phi_l, \mathcal{D}_l].
\end{aligned} \tag{22}$$

4.2. **The case $l \in S$ or $l = 2$.** By our assumptions $l \nmid \#G$. We recall from [11, end of Sec. 1.5] that

$$\begin{aligned}
H^i_f(\mathbb{Q}, T_l)_{BK} &= 0 \text{ for } i \ne 1,2,3, \\
H^1_f(\mathbb{Q}, T_l)_{BK} &= E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l, \\
H^3_f(\mathbb{Q}, T_l)_{BK} &= E(K)^\vee_{l^\infty}
\end{aligned}$$

and

$$0 \longrightarrow Ш(E/K) \otimes_{\mathbb{Z}} \mathbb{Z}_l \longrightarrow H^2_f(\mathbb{Q}, T_l)_{BK} \longrightarrow (E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^* \longrightarrow 0.$$

As before we write $\chi = \chi_{\mathbb{Z}_l[G],\mathbb{C}_l}$ for the refined Euler characteristic. If v is a finite place of K we also put $\chi_v = \chi_{\mathbb{Z}_l[G_v],\mathbb{C}_l}$ for the refined Euler characteristic in $K_0(\mathbb{Z}_l[G_v], \mathbb{C}_l)$. If we write $\mathrm{ind}_{G_v}^G : K_0(\mathbb{Z}_l[G_v], \mathbb{C}_l) \longrightarrow K_0(\mathbb{Z}_l[G], \mathbb{C}_l)$ for the natural induction map, then $\chi = \mathrm{ind}_{G_v}^G \circ \chi_v$.

Applying Lemma 2.3 we obtain

$$\begin{aligned} \chi(R\Gamma_f(\mathbb{Q}, T_l), \delta^{-1}) &= [(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*, \delta^{-1}, E(K)_{tf} \otimes_{\mathbb{Z}} \mathbb{Z}_l] \\ &+ \chi(E(K)_{l^\infty}, 0) + \chi(E(K)^\vee_{l^\infty}, 0) - \chi(Ш(E/K)_{l^\infty}, 0). \end{aligned}$$

We write $\hat{E}$ for the formal group associated with E. Then we have the basic short exact sequence

$$0 \longrightarrow \hat{E}(\mathfrak{m}_v) \longrightarrow E_0(K_v) \longrightarrow \bar{E}_{ns}(k_v) \longrightarrow 0. \tag{23}$$

We recall that $H^1_f(\mathbb{Q}_p, T_l) \simeq \bigoplus_{v|p} E(K_v)^{\wedge l}$. For $p \neq l$ and $v \mid p$ we first note that $\hat{E}(\mathfrak{m}_v)^{\wedge l} = 0$. From (23) we derive the short exact sequence

$$0 \longrightarrow \bar{E}_{ns}(k_v)_{l^\infty} \longrightarrow E(K_v)^{\wedge l} \longrightarrow (E(K_v)/E_0(K_v))_{l^\infty} \longrightarrow 0,$$

so that $H^1_f(\mathbb{Q}_p, T_l)_{BK}$ is finite and, by Lemma 2.3,

$$\chi(R\Gamma_f(\mathbb{Q}_p, T_l), 0) = \mathrm{ind}_{G_v}^G \chi_v \left(\bar{E}_{ns}(k_v)_{l^\infty}, 0\right) + \mathrm{ind}_{G_v}^G \chi_v \left((E(K_v)/E_0(K_v))_{l^\infty}, 0\right).$$

As in the previous case we must now relate the Euler characteristic of $R\Gamma_f(\mathbb{Q}_\infty, T_l) \oplus R\Gamma_f(\mathbb{Q}_l, T_l)$ and the element $\left[(H_{K,\mathbb{Z}} \otimes_{\mathbb{Z}} \mathcal{H}_{\mathbb{Z}})^+, \pi_K, \mathcal{O}_K \otimes_{\mathbb{Z}} \Omega^1_{\mathcal{E}}(\mathcal{E})^*\right]_l$.

We write

$$\exp_p^{BK} : t_p(V_p) \longrightarrow H^1_f(\mathbb{Q}_p, V_p)$$

for the isomorphism given by the Bloch-Kato exponential map and recall that the logarithm attached to the formal group $\hat{E}$ induces an isomorphism

$$\log_v : E(K_v)^{\wedge l} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \simeq K_v.$$

We use the commutative diagram

$$\begin{tikzcd} \mathbb{Q}_l \otimes_{\mathbb{Q}} K \otimes_{\mathbb{Q}} \Omega^1_E(E)^* \arrow[rr, "\kappa_l"] \arrow[d, "="] & & t_l(V_l) \arrow[d, "\exp_l^{BK}"] \\ \bigoplus_{v|l} K_v \otimes \omega_0^* \arrow[d, "\simeq"] & & \mathbb{Q}_l \otimes_{\mathbb{Z}_l} H^1_f(\mathbb{Q}_l, T_l)_{BK} \arrow[d, "\simeq"] \\ \bigoplus_{v|l} K_v & & \bigoplus_{v|l} E(K_v)^{\wedge l} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \arrow[ll, "\oplus \log_v"'] \end{tikzcd}$$

For each place $v \mid l$ we choose a positive integer n_v such that $\log_v$ induces an isomorphism between $\hat{E}(\mathfrak{m}_v^{n_v})$ and $\mathfrak{m}_v^{n_v}$. For every prime p we fix a place v_p above

p. We obtain

$$
\begin{aligned}
& j_*\left(\left[(H_{K,\mathbb{Z}}\otimes_{\mathbb{Z}}\mathcal{H}_{\mathbb{Z}})^+, \pi_K, \mathcal{O}_K\otimes_{\mathbb{Z}}\Omega^1_{\mathcal{E}}(\mathcal{E})^*\right]\right)\\
= & \left[T_l^{G_\infty}, \pi_{K,j}, \kappa_l(\mathbb{Z}_l\otimes_{\mathbb{Z}}\mathcal{O}_K\otimes_{\mathbb{Z}}\Omega^1_{\mathcal{E}}(\mathcal{E})^*)\right]\\
= & \left[T_l^{G_\infty}, \pi_{K,j}, \kappa_l(\oplus_{v|l}\mathcal{O}_{K_v}\otimes\omega_0^*)\right]\\
= & \left[T_l^{G_\infty}, \exp_l^{BK}\circ\pi_{K,j}, (\exp_l^{BK}\circ\kappa_l)(\oplus_{v|l}\mathcal{O}_{K_v}\otimes\omega_0^*)\right]\\
= & \left[T_l^{G_\infty}, \exp_l^{BK}\circ\pi_{K,j}, (\exp_l^{BK}\circ\kappa_l)(\oplus_{v|l}\mathfrak{m}_v^{n_v}\otimes\omega_0^*)\right] + \left[\oplus_{v|l}\mathfrak{m}^{n_v}, id, \oplus_{v|l}\mathcal{O}_{K_v}\right]\\
\overset{(i)}{=} & \left[T_l^{G_\infty}, \exp_l^{BK}\circ\pi_{K,j}, \oplus_{v|l}\hat{E}(\mathfrak{m}_v^{n_v})\right] + \left[\oplus_{v|l}\mathfrak{m}^{n_v}, id, \oplus_{v|l}\mathcal{O}_{K_v}\right]\\
= & \left[T_l^{G_\infty}, \exp_l^{BK}\circ\pi_{K,j}, \oplus_{v|l}\hat{E}(\mathfrak{m}_v)\right] - \left[\oplus_{v|l}\hat{E}(\mathfrak{m}^{n_v}), id, \oplus_{v|l}\hat{E}(\mathfrak{m})\right] + \left[\oplus_{v|l}\mathfrak{m}^{n_v}, id, \oplus_{v|l}\mathcal{O}_{K_v}\right]\\
\overset{(ii)}{=} & \left[T_l^{G_\infty}, \exp_l^{BK}\circ\pi_{K,j}, \oplus_{v|l}E_0(K_v)^{\wedge l}\right] - \chi(\oplus_{v|l}\bar{E}_{ns}(k_v)_{l^\infty}, 0) + \left[\oplus_{v|l}\mathfrak{m}, id, \oplus_{v|l}\mathcal{O}_{K_v}\right]\\
= & \left[T_l^{G_\infty}, \exp_l^{BK}\circ\pi_{K,j}, H^1_f(\mathbb{Q}_l, T_l)_{BK}\right]\\
& -\chi(\oplus_{v|l}\left(E(K_v)/E_0(K_v)\right)_{l^\infty}, 0) - \chi(\oplus_{v|l}\bar{E}_{ns}(k_v)_{l^\infty}, 0) + \left[\oplus_{v|l}\mathfrak{m}, id, \oplus_{v|l}\mathcal{O}_{K_v}\right]\\
= & \left[T_l^{G_\infty}, \exp_l^{BK}\circ\pi_{K,j}, H^1_f(\mathbb{Q}_l, T_l)_{BK}\right]\\
& -\mathrm{ind}_{G_{v_l}}^G\left(\chi_{v_l}((E(K_{v_l})/E_0(K_{v_l}))_{l^\infty}, 0)\right) - \mathrm{ind}_{G_{v_l}}^G\left(\chi_{v_l}(\bar{E}_{ns}(k_{v_l})_{l^\infty}, 0)\right) + \mathrm{ind}_{G_{v_l}}^G\left(\chi_{v_l}(k_{v_l}, 0)\right)\\
\overset{(iii)}{=} & \chi\left(R\Gamma_f(\mathbb{Q}_\infty, T_l)\oplus R\Gamma_f(\mathbb{Q}_l, T_l), \pi_K\right)\\
& -\mathrm{ind}_{G_{v_l}}^G\left(\chi_{v_l}((E(K_{v_l})/E_0(K_{v_l}))_{l^\infty}, 0)\right) - \mathrm{ind}_{G_{v_l}}^G\left(\chi_{v_l}(\bar{E}_{ns}(k_{v_l})_{l^\infty}, 0)\right) + \mathrm{ind}_{G_{v_l}}^G\left(\chi_{v_l}(k_{v_l}, 0)\right)
\end{aligned}
$$

Here (i) is induced by the diagram and our choice of integers n_v, (ii) comes from (23) and (iii) follows from Lemma 2.3.

In summary, we obtain for $l \in S$ or $l = 2$ (always assuming $l \nmid \#G$)

$$
\begin{aligned}
R\Omega_l \;=\; & [(E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l)^*, \delta^{-1}, E(K)_{tf}\otimes_{\mathbb{Z}}\mathbb{Z}_l]\\
& -j_*\left(\left[(H_{K,\mathbb{Z}}\otimes_{\mathbb{Z}}\mathcal{H}_{\mathbb{Z}})^+, \pi_K, \mathcal{O}_K\otimes_{\mathbb{Z}}\Omega^1_{\mathcal{E}}(\mathcal{E})^*\right]\right)\\
& +\chi(E(K)_{l^\infty}, 0) + \chi(E(K)^\vee_{l^\infty}, 0) - \chi(\text{Ш}(E/K)_{l^\infty}, 0)\\
& -\sum_{p\in S_l}\mathrm{ind}_{G_{v_p}}^G\left(\chi_{v_p}(\bar{E}_{ns}(k_{v_p})_{l^\infty}, 0)\right)\\
& -\sum_{p\in S_l}\mathrm{ind}_{G_{v_p}}^G\left(\chi_{v_p}(\left(E(K_{v_p})/E_0(K_{v_p})\right)_{l^\infty}, 0)\right)\\
& +\mathrm{ind}_{G_{v_l}}^G\left(\chi_{v_l}(k_{v_l}, 0)\right)
\end{aligned}
\tag{24}
$$

If $E(K)_{tf}\otimes_{\mathbb{Z}}\mathbb{Z}_l$ and $(E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l)^*$ are $\mathbb{Z}_l[G]$-projective, then by the arguments of Remark 2.6(a) we can find a $\mathbb{Z}_l[G]$-module Z such that both $(E(K)_{tf}\otimes_{\mathbb{Z}}\mathbb{Z}_l)\oplus Z$ and $(E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l)^*\oplus Z$ are $\mathbb{Z}_l[G]$-free. Then one has

$$[(E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l)^*, \delta^{-1}, E(K)_{tf}\otimes_{\mathbb{Z}}\mathbb{Z}_l] = [(E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l)^*\oplus Z, \delta^{-1}\oplus id, (E(K)_{tf}\otimes_{\mathbb{Z}}\mathbb{Z}_l)\oplus Z]$$

so that without loss of generality we may assume that we can work with $\mathbb{Z}_l[G]$-basis.

If T is a finite perfect $\mathbb{Z}_l[G]$-module, then we write $\tilde{\chi}_{\mathbb{Z}_l[G],\mathbb{C}_l}(T,0)$ for any lift of $\chi_{\mathbb{Z}_l[G],\mathbb{C}_l}(T,0)$ via the middle vertical map of (5). Analogously we use the notation $\tilde{\chi}$ and $\tilde{\chi}_v$.

Recall the definition of $u = \frac{\mathcal{L}^* R}{\Omega \mathrm{Reg}}$ in Conjecture 3.5.

Proposition 4.4. *Assume hypothesis (H0) - (H5) and let α_0 be a normal basis element such that $\mathcal{O}_{K,l} = \mathbb{Z}_l[G]\alpha_0$. Assume that $u = u_l$ is computed with respect to α_0 and a $\mathbb{Z}_l[G]$-basis of $E(K)_{tf} \otimes_{\mathbb{Z}} \mathbb{Z}_l$ and $(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*$. Assume also that the rationality conjecture holds.*
If $l \notin S$ and $l \neq 2$ we set

$$\xi_l \quad := \quad \tilde{\chi}(E(K)_{l^\infty}, 0)^{-1} \cdot \tilde{\chi}(E(K)^\vee_{l^\infty}, 0)^{-1} \cdot \tilde{\chi}(\text{Ш}(E/K)_{l^\infty}, 0).$$

If $l \in S$ or $l = 2$ we set

$$\begin{aligned} \xi_l \quad := \quad & \tilde{\chi}(E(K)_{l^\infty}, 0)^{-1} \cdot \tilde{\chi}(E(K)^\vee_{l^\infty}, 0)^{-1} \cdot \tilde{\chi}(\text{Ш}(E/K)_{l^\infty}, 0) \\ & \prod_{p \in S_l} \mathrm{ind}^G_{G_{v_p}} \tilde{\chi}_{v_p}\left(\bar{E}_{ns}(k_{v_p})_{l^\infty}, 0\right) \cdot \prod_{p \in S_l} \mathrm{ind}^G_{G_{v_p}} \tilde{\chi}_{v_p}\left(\left(E(K_{v_p})/E_0(K_{v_p})\right)_{l^\infty}, 0\right) \\ & \mathrm{ind}^G_{G_{v_l}} \tilde{\chi}_{v_l}(k_{v_l}, 0)^{-1} \prod_{p \in S_l} \left(L_p(E, \bar{\chi}, 1)\right)^{-1}_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)} \end{aligned}$$

Then

$$T\Omega_l = 0 \iff u_l = \xi_l \text{ in } \mathrm{cok}(\mu_l) \oplus I_l(C). \tag{25}$$

Proof. The Euler factor terms $[T_l^{I_p}, 1 - Fr_p^{-1}, T_l^{I_p}]$ and $[\mathcal{D}_l, 1 - \phi_l, \mathcal{D}_l]$ in (22) cancel because of the identification made in [12, (24)] applied to (19) and (22) of loc.cit. See Remark 3.3.

For the same reason we obtain the local Euler factors $(L_p(E, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)}$ in (24). Indeed, by (13) the local factors $(L_p(E, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)}$ represent the refined Euler characteristics of the complexes $(V_p \xrightarrow{\phi_p} V_p)$ which occur in (19) and (22) of loc.cit. □

Remark 4.5. The local Euler factors in the above formulae can be computed using their explicit definition. For the computation of the refined Euler characteristics of finite modules we use the method explained in Example 2.7. Hence we obtain ξ_l as an element in $C^\times$.

If $u_l \xi_l^{-1} = (\eta_1, \dots, \eta_r)$ with $\eta_i \in K_i$, then $T\Omega_l = 0$ if and only if

$$\begin{aligned} & v_{\mathfrak{P}}(\eta_i) = 0, \quad \forall i \in \{1, \dots, r\} \text{ and } \mathfrak{P} \mid l \text{ in } K_i/\mathbb{Q}, \text{ and} \\ & (\bar{\eta}_1, \dots, \bar{\eta}_r) \in \mathrm{im}(\mu_l), \end{aligned}$$

where $\bar{\eta}_i$ denotes the image of η_i under the projection $\mathcal{O}^\times_{K_i,l} \longrightarrow (\mathcal{O}_{K_i}/\mathfrak{g}_{i,l})^\times$ and μ_l is the isomorphism from (8). Recall that this means that the η_i have to satisfy certain complicated congruences. In Section 2.3 we made these congruences explicit for cyclic groups Z_l, dihedral groups D_{2l} and the alternating group A_4. For explicit examples see Sections 6.1, 6.2 and 6.3 where we consider dihedral extensions $K/\mathbb{Q}$ of degree $2l$ for an odd prime l. In each of these examples the prime l is of particular interest because we have to check that the BSD quotients satisfy the congruence (10).

Remark 4.6. The element u_l in (25) depends on the choice of α_0, however, the validity of the statement $u_l = \xi_l$ in $\mathrm{cok}(\mu_l) \oplus I_l(C)$ is independent of this choice. If

β_0 is another $\mathbb{Z}_l[G]$-generator of $\mathcal{O}_{K,l}$, then $\beta_0 = \lambda\alpha_0$ with a unit $\lambda \in \mathbb{Z}_l[G]^\times$. As in (3.6) we see that $u_l(\beta_0) = \mathrm{Nrd}_{\mathbb{Q}_l[G]}(\lambda)u_l(\alpha_0)$. Hence the independence follows from the fact that $\mathrm{Nrd}_{\mathbb{Q}_l[G]}(\lambda)$ is a unit in $\mathcal{O}_{C,l}$ which is contained in the image of μ_l.

We fix a normal basis element α_0 and $\mathbb{Q}[G]$-basis of $E(K)\otimes_{\mathbb{Z}}\mathbb{Q}$ and $(E(K)\otimes_{\mathbb{Z}}\mathbb{Q})^*$ in the sense of Remark 2.6 b) and compute u with respect to these basis. Note that for almost all primes l the element α_0 constitutes a $\mathbb{Z}_l[G]$-basis of $\mathcal{O}_{K,l}$ and the chosen $\mathbb{Q}[G]$-basis of $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$, respectively $(E(K) \otimes_{\mathbb{Z}} \mathbb{Q})^*$, is a $\mathbb{Z}_l[G]$-basis of $E(K)_{tf} \otimes_{\mathbb{Z}} \mathbb{Z}_l$, respectively $(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*$. For all these primes l we can use this fixed u as u_l in Proposition 4.4.

We define two finite sets of rational primes

$$\begin{aligned} HP_1 &= S \cup \{2\} \cup \{l : l \mid \#G\} \cup \{l : l \mid \#E(K_v)/E_0(K_v) \text{ for a } v \in S_l(K)\} \cup \\ &\quad \{l : l \mid \#E(K)_{tors}\} \cup \{l : l \mid \#\text{Ш}(E/K)\}, \\ HP_2 &= \{l : u_l \neq u\}. \end{aligned}$$

So for all $l \notin HP_2$ we can use the fixed u as u_l in Proposition 4.4. Note that HP_2 depends on the choice of α_0 and the $\mathbb{Q}[G]$-basis of $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $(E(K) \otimes_{\mathbb{Z}} \mathbb{Q})^*$. Finally we set

$$HP := HP_1 \cup HP_2.$$

We say that an element $w = (w_1, \ldots, w_r) \in \zeta(\mathbb{Q}[G])^\times$ has support in HP, if $(w_i, p) = 1$ for $i = 1, \ldots, r$ and all primes $p \notin HP$.

Corollary 4.7. *Assume (H0) and (H3) and the rationality conjecture. Let $l \notin HP$ be a rational prime. Then l satisfies the hypothesis (H1),(H2), (H4) and (H5) and*

$$T\Omega_l = 0 \iff u \text{ has support in } HP.$$

Proof. There first assertion is clear from the definition of HP. If $l \notin HP$, then we are in the case $l \notin S$ and $l \neq 2$. By definition of HP_1 the element ξ_l is trivial. By definition of HP_2 we have $u = u_l$. Since $l \nmid \#G$, we have $\mathrm{cok}(\mu_l) = 0$, so that $T\Omega_l = 0$ if and only if u is prime to l in the sense of Remark 4.5. ☐

By the corollary we can, in principle, numerically verify ETNC for almost all primes l as soon as we have computed a good approximation of $u \in \prod_{\chi\in\mathrm{Irr}(G)} \mathbb{C}^\times$. If the computed u makes us believe that the rationality conjecture holds, and if we are able to round u to an element of $u' \in \prod_{\chi\in\mathrm{Irr}_{\mathbb{Q}}(G)} \mathbb{Q}(\chi)^\times$, we only have to check if u' has support in HP.

Of course, the main restriction to our approach is our incapability of computing the Mordell-Weil group and the Tate-Shafarevic group. In order to obtain at least some numerical evidence we will usually trust in the equivariant rank conjecture and thus assume that the analytic rank equals the geometric rank r and compute r by computing approximations to the L-values. Even here our approach is rather vague since we do not dispose of a criterion which would allow to decide whether an L-value is actually 0 from the knowledge of numerical approximations.

However, numerical computations can prove that the analytic rank is 0 and in this case (assuming that K is totally real) we can use results proved independently by Longo and Tian-Zhang (see [16, Th. 3.7]) to deduce that the algebraic rank is also 0.

If $r = 0$ or in the rare case that $r > 0$ and we know generators for $E(K)$ we use the usual Birch and Swinnerton-Dyer conjecture to compute a conjectural value for $\#Ш(E/K)$. In a sense our results can be characterized as 'deducing numerical evidence for ETNC from the classical BSD-conjecture for E/K'.

5. Computational remarks

In this section we describe how we perform our computations.

5.1. **Computation of L-values.** For the computation of the leading coefficients $L^*(E/\mathbb{Q},\chi,1)$, $\chi \in \mathrm{Irr}(G)$, we use the algorithm of Dokchitser decribed in [17]. Actually we apply the MAGMA [28] implementation of this algorithm.

We use the algorithm to compute complex approximations to the derivatives $L^{(k)}(E/\mathbb{Q},\chi,1)$ of the twisted Hasse-Weil-L-functions at $s=1$. We also use these values to guess the order of vanishing of $L(E/\mathbb{Q},\chi,s)$ at $s=1$ in a very naive way. Explicitly we set

$$\tilde{r}(\chi) := \min\{k \geq 0 \mid |L^{(k)}(E/\mathbb{Q},\chi,1)| > \varepsilon\}$$

where $\varepsilon > 0$ is a chosen lower bound which seems to be reasonable in an unspecific way. At least one can hope that $\tilde{r}(\chi)$ is equal to the order of $L(E/\mathbb{Q},\chi,s)$ at $s=1$.

5.2. **Computation of periods.** For the computation of periods associated to $h^1(E_K)(1)$ considered as a motive over $\mathbb{Q}$ with coefficients in $\mathbb{Q}[G]$ we apply Proposition 3.1. The computation of Ω_+ and Ω_- is standard and we just use the implementation provided by MAGMA. It is usually very efficient to compute a normal basis element α_0 just by trial and error. Without loss of generality we assume that $\alpha_0 \in \mathcal{O}_K$. Then the exceptional set HP_2 contains

$$HP_2' = \{l \mid l \text{ divides } [\mathcal{O}_K : \mathbb{Z}[G]\alpha_0]\}$$

which can be computed easily.

If we want to check the conjecture for primes $l \in HP$ we must assume hypothesis (H), in particular, that l is at most tamely ramified in $K/\mathbb{Q}$. In this case we can use algorithm [5, Alg. 4.2] to compute $\alpha_0 \in \mathcal{O}_K$ such that $\mathcal{O}_{K,l} = \mathbb{Z}_l[G]\alpha_0$.

However, it is reasonable to compute u such that the exceptional set HP is as small as possible. Under certain assumptions on the group G (which are, e.g., satisfied for all groups with $\#G < 32$) we can often use the methods of [3, 4] to compute $\alpha_0 \in \mathcal{O}_K$ such that $HP_2' \subseteq HP_1$. This is possible because for small groups G the ring of integers $\mathcal{O}_K$ is often free over the associated order $\mathcal{A} = \mathcal{A}(\mathbb{Q}[G];\mathcal{O}_K) := \{\lambda \in \mathbb{Q}[G] \mid \lambda(\mathcal{O}_K) \subseteq \mathcal{O}_K\}$ and in this case the algorithm of loc.cit. computes a free generator α_0 such that $\mathcal{O}_K = \mathcal{A}\alpha_0$. Basic properties of associated orders then imply that $\mathcal{O}_{K,l} = \mathbb{Z}_l[G]\alpha_0$ for all $l \nmid \#G$.

5.3. **Computation of equivariant regulators.** Our possibilities to compute regulators are very limited because in most cases we are not able to compute the Mordell-Weil group $E(K)$ when $K \neq \mathbb{Q}$ (or a subgroup of finite index in $E(K)$). Henceforth we assume $r > 0$ and that

$$E(K) = E(K)_{tors} \oplus \mathbb{Z}P_1 \oplus \ldots x \oplus \mathbb{Z}P_r$$

is explicitly known. Note, however, that for the rationality conjecture it would be enough to know a subgroup of finite index.

We consider $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ and remind the reader of Remark 2.6 b) where the general recipe for the computation of regulators is described. However, for our actual computations described in the next section it will be enough to consider irreducible rational characters $\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)$ which factor through the commutator subgroup G'. For all other characters we assume that $e_\chi(E(K)\otimes_{\mathbb{Z}}\mathbb{Q})$ is trivial. Under these circumstances it is rather straightforward to compute a $\mathbb{Q}[G]$-basis in the sense of Remark 2.6 b). We describe the computation of the equivariant regulator in this case.

Let $\psi \in \mathrm{Irr}(G)$ denote an absolutely irreducible abelian character and set $F := K^{\ker(\psi)}$. Let $\chi = \sum_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q})}\psi^\sigma$ be the associated rational character. Then $e_\chi\mathbb{Q}[G]\simeq\mathbb{Q}(\psi)$ is a field and $e_\chi(E(K)\otimes_{\mathbb{Z}}\mathbb{Q}) = e_\chi(E(F)\otimes_{\mathbb{Z}}\mathbb{Q})$ is a finite dimensional $e_\chi\mathbb{Q}[G]$-vector space. Let $Q_1,\dots,Q_d$ be a $e_\chi\mathbb{Q}[G]$-basis.

For an abelian character φ we write $\varphi\mid\chi$ if φ is a constituent of χ. If $a = (a_\varphi)_{\varphi\in\mathrm{Irr}(G)}\in\prod_{\varphi\in\mathrm{Irr}(G)}\simeq\zeta(\mathbb{C}[G])$, then we write a_χ for the χ-part $(a_\varphi)_{\varphi\mid\chi}\in\prod_{\varphi\mid\chi}\simeq\zeta(e_\chi\mathbb{C}[G])$

Proposition 5.1. *Assume the above notation. With respect to the $e_\chi\mathbb{Q}[G]$-basis $Q_1,\dots,Q_d$ and $Q_1^*,\dots,Q_d^*$ with Q_i^* defined below in (26) the χ-part of the regulator is given by*

$$\mathrm{Reg}_\chi := \Big(\det\left(\langle Q_i, e_{\bar\psi^\sigma}Q_j\rangle\right)_{1\le i,j\le d}\Big)_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q})}.$$

Proof. The set $\{e_\varphi Q_i \mid i=1,\dots,d,\varphi\mid\chi\}$ is a $\mathbb{C}$-basis of $e_\chi(E(K)\otimes_{\mathbb{Z}}\mathbb{C})$. We define the dual basis by

$$(e_\varphi Q_i)^*(e_\lambda Q_j) = \begin{cases}1, & \text{if } \varphi=\lambda \text{ and } i=j,\\ 0, & \text{otherwise.}\end{cases}$$

Then one easily verifies that

$$e_\lambda(e_\varphi Q_i)^* = \begin{cases}(e_\varphi Q_i)^*, & \text{if } \varphi=\bar\lambda,\\ 0, & \text{otherwise.}\end{cases}$$

The elements

$$Q_i^* := \sum_{\varphi\mid\chi}(e_{\bar\varphi}Q_i)^*,\quad i=1,\dots,d, \tag{26}$$

form a $e_\chi\mathbb{Q}[G]$-basis of $(e_\chi(E(K)\otimes_{\mathbb{Z}}\mathbb{Q}))^*$. Then

$$\begin{aligned}\langle e_\varphi Q_i, \_\rangle &= \sum_{j,\lambda}\langle e_\varphi Q_i, e_\lambda Q_j\rangle(e_\lambda Q_j)^*\\ &= \sum_{j,\lambda}\langle Q_i, e_{\bar\varphi}e_\lambda Q_j\rangle(e_\lambda Q_j)^*\\ &= \sum_j\langle Q_i, e_{\bar\varphi}Q_j\rangle(e_{\bar\varphi}Q_j)^*\end{aligned}$$

Hence

$$\begin{aligned}\langle e_\chi Q_i, \_\rangle &= \sum_{\varphi\mid\chi}\sum_j\langle Q_i, e_{\bar\varphi}Q_j\rangle(e_{\bar\varphi}Q_j)^*\\ &= \sum_j\left(\sum_{\varphi\mid\chi}\langle Q_i, e_{\bar\varphi}Q_j\rangle e_\varphi\right)\left(\sum_{\varphi\mid\chi}(e_{\bar\varphi}Q_j)^*\right)\\ &= \sum_j\left(\sum_{\varphi\mid\chi}\langle Q_i, e_{\bar\varphi}Q_j\rangle e_\varphi\right)Q_j^*.\end{aligned}$$

Therefore with respect to the basis $Q_1, \ldots, Q_d$ and $Q_1^*, \ldots, Q_d^*$ the regulator map is represented by the matrix $\left(\sum_{\varphi|\chi} \langle Q_i, e_{\bar{\varphi}} Q_j \rangle e_\varphi\right)_{1 \le i,j \le d}$ and the result follows upon computing the reduced norm.

□

For integrality considerations we restrict ourselves to the case where $l \neq 2$ and $l \nmid \#G$. Then $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is $\mathbb{Z}_l[G]$-perfect and we wish to compute a $e_\chi \mathbb{Z}_l[G]$-basis $Q_1, \ldots, Q_d$ of $e_\chi(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)$. Since $e_\chi \mathbb{Z}_l[G]$ naturally identifies with $\prod_{\mathfrak{P}|l} \mathbb{Z}_l[\psi]$ which is a product of discrete valuation rings such a basis always exists. From

$$Q_i^*(Q_j) = \begin{cases} \chi(1), & \text{if } i = j, \\ 0, & \text{if } i \neq j \end{cases}$$

we see that $\frac{1}{\chi(1)} Q_1^*, \ldots, \frac{1}{\chi(1)} Q_d^*$ is a $e_\chi \mathbb{Z}_l[G]$-basis of $e_\chi(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*$.

Working with localisations rather than completions we can also consider $e_\chi(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_{(l)})$ as a module over $e_\chi \mathbb{Z}_{(l)}[G] \simeq \mathbb{Z}_{(l)}[\psi] \subseteq \mathbb{Q}(\psi)$ which is principal ideal ring (because it is Dedekind with only finitely many maximal ideals). It is then quite standard to compute a basis from the knowledge of $P_1, \ldots, P_r$.

Example 5.2. In [21] Fearnley and Kisilevsky consider the situation when $K/\mathbb{Q}$ is a cyclic extension of odd prime degree l and examine the case that $L(E/\mathbb{Q}, \psi, s)$ have simple zeroes for all non-trivial characters $\psi \in \mathrm{Irr}(G)$. We write $\hat{G}$ for the group of linear characters of G and fix a generator ψ_0 of $\hat{G}$. Let $\chi := \sum_{\gamma \in \mathrm{Gal}(\mathbb{Q}(\psi_0)/\mathbb{Q})} \psi_0^\gamma$ denote the associated irreducible rational character. The computations described in loc.cit. suggest that for non-trivial ψ and a point $P \in E(K)$ of infinite order with trace 0 (i.e., $P \in e_\chi(E(K) \otimes_{\mathbb{Z}} \mathbb{Q})$ is a $e_\chi \mathbb{Q}[G]$-basis) one has

$$L'(E/\mathbb{Q}, \psi, 1) = \frac{\tau(\psi)}{\mathfrak{f}_\psi} \Omega_+ \lambda_\psi(P) \alpha_\psi(P)$$

with a Gauss sum $\tau(\psi)$, the conductor $\mathfrak{f}_\psi$ of ψ, $\lambda_\psi(P) := \sum_{\sigma \in G} \psi(\sigma^{-1}) \langle P, P^\sigma \rangle$ and an algebraic number $\alpha_\psi(P) \in \mathbb{Q}(\psi)$ which satisfies $\alpha_{\psi^\gamma}(P) = \alpha_\psi(P)^\gamma$ for all $\gamma \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q})$. In other words this means that $(\alpha_\psi(P))_{\psi|\chi} \in \zeta(e_\chi \mathbb{Q}[G])^\times$.

The results and computations of loc.cit. are completely consistent with the rationality conjecture 3.5 and provide numerical evidence for it. Indeed, one easily shows that $\lambda_\psi(P) = \langle P, e_{\bar{\psi}} P \rangle$, so that we deduce from Proposition 5.1

$$\mathrm{Reg}_\chi \equiv \left(\lambda_{\psi_0^\gamma}(P)\right)_{\gamma \in \mathrm{Gal}(\mathbb{Q}(\psi_0)/\mathbb{Q})}$$

where $\equiv$ means up to a multiplicative factor in $e_\chi \mathbb{Q}[G]^\times \subseteq \prod_{\psi \neq 1} \mathbb{C}^\times$. Furthermore, by [20, §9(i), (ii)] one has

$$(\tau(\psi_0^\gamma))_{\gamma \in \mathrm{Gal}(\mathbb{Q}(\psi_0)/\mathbb{Q})} \equiv \left(\sum_{\sigma \in G} \psi_0^\gamma(\sigma) \sigma(\alpha_0) \right)_{\gamma \in \mathrm{Gal}(\mathbb{Q}(\psi_0)/\mathbb{Q})}.$$

Recall that the right hand side is exactly the χ-part of the resolvent R from Conjecture 3.5.

5.4. **Computation of refined Euler characteristics of finite perfect modules.** Let T be a finite perfect $\mathbb{Z}_l[G]$-module. The recipe for the computation of $\chi_{\mathbb{Z}_l[G],\mathbb{Q}_l}(T)$ is already given in Example 2.7. We give two applications.

Proposition 5.3. *Let $F/\mathbb{Q}_p$ denote a finite Galois extension with group D. Let v denote the normalized discrete valuation of F. Let $E/\mathbb{Q}_p$ be an elliptic curve so that E/F has split multiplicative reduction. Then*

(a) $\#E(F)/E_0(F) = c$ with $c := -v(j(E))$.

(b) Let l be a prime. Then $E(F)/E_0(F) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is $\mathbb{Z}_l[D]$-perfect if and only if $l \nmid c$ or $l \nmid \#D$.

(c) Set $c_l := \#\left(E(F)/E_0(F) \otimes_{\mathbb{Z}} \mathbb{Z}_l\right)$. If $l \nmid c$ or $l \nmid \#D$, then $\chi_{\mathbb{Z}_l[D],\mathbb{Q}_l}(E(F)/E_0(F)\otimes_{\mathbb{Z}} \mathbb{Z}_l)$ is represented by $(c_l, 1, \ldots, 1) \in \zeta(\mathbb{Q}[D])^\times$.

Proof. We apply [32, Th. 14.1]. E is isomorphic over F to the Tate curve E_q with $v(q) = c$. The isomorphism $E_q(F) \simeq F^\times/q^{\mathbb{Z}}$ induces a D-equivariant isomorphism $E(F)/E_0(F) \simeq F^\times/(q^{\mathbb{Z}} \times \mathcal{O}_F^\times)$. Note that D acts trivially on the right hand side so that $F^\times/(q^{\mathbb{Z}} \times \mathcal{O}_F^\times) \simeq \mathbb{Z}/c\mathbb{Z}$ as Galois modules. a) and b) are now immediate. To prove c) we may assume $l \nmid \#D$. Then we have a projective resolution of $\mathbb{Z}_{(l)}[D]$-modules

$$0 \longrightarrow \mathbb{Z}_{(l)}[D] \stackrel{c_l e_D + (1-e_D)}{\longrightarrow} \mathbb{Z}_{(l)}[D] \longrightarrow \mathbb{Z}/c_l\mathbb{Z} \longrightarrow 0.$$

The result follows. $\square$

Proposition 5.4. *Let $F/\mathbb{Q}_l$ denote a finite Galois extension with group D and ramification subgroup I. Let v denote the normalized discrete valuation of F. Let k_v denote the residue class field. Then k_v is $\mathbb{Z}_l[D]$-perfect if and only if $l \nmid \#I$. In this case $\chi_{\mathbb{Z}_l[D],\mathbb{Q}_l}(k_v)$ is represented by $(a_\psi)_\psi \in \zeta(\mathbb{Q}[D])^\times \simeq \prod_{\psi \in \mathrm{Irr}_{\mathbb{Q}}(D)} \mathbb{Q}(\psi)$ with*

$$a_\psi = \begin{cases} l, & \text{if } I \subseteq \ker(\psi), \\ 1, & \text{otherwise.} \end{cases}$$

Proof. By the normal basis theorem on has $k_v \simeq \mathbb{F}_l[D/I]$. One easily shows that $\hat{H}^0(D, \mathbb{F}_l[D/I]) \simeq \mathbb{F}_l/|I|\mathbb{F}_l$. It follows that if k_v is perfect, then $l \nmid \#I$. Conversely, if $l \nmid \#I$, then we have the projective resolution

$$0 \longrightarrow \mathbb{Z}_l[D] \stackrel{le_I + (1-e_I)}{\longrightarrow} \mathbb{Z}_l[D] \longrightarrow k_v \longrightarrow 0$$

and the result follows. $\square$

In general we assume that the finite perfect $\mathbb{Z}_l[G]$-module T is given by a $\mathbb{Z}[G]$-generating set $t_1, \ldots, t_d$ with explicitly known G-action, i.e.

$$gt_i = \sum_{j=1}^{d} a_{g,j} t_j, \quad a_{g,j} \in \mathbb{Z}[G], g \in G.$$

It is then easy to compute a $\mathbb{Z}[G]$-resolution of the form

$$0 \longrightarrow Q \longrightarrow P \stackrel{\pi}{\longrightarrow} T \longrightarrow 0$$

with $P := \mathbb{Z}[G]^d$, $\pi(e_i) := t_i$ where e_i denotes the canonical basis and $Q := \ker(\pi)$. We then proceed as described in Example 2.7.

In this way it is, in principle, possible to compute the refined Euler characteristics of $E(K)_{l^\infty}, E(K)^\vee_{l^\infty}$ and $\bar{E}_{ns}(k_{v_p})_{l^\infty}$, at least in small examples where we are able to provide an explicit generating set with explicitly known G-action. If v is a place of bad reduction we can use Tate's algorithm to determine the reduction type and then use [32, Ex. III, 3.5] in order to compute $\bar{E}_{ns}(k_v)_{l^\infty}$.

5.5. **Computation of $E(K)$ and $Ш(E/K)$.** The computation of $E(K)$ is very difficult even if $K = \mathbb{Q}$ and does usually not work if $K \neq \mathbb{Q}$. In our examples we mostly consider pairs (E, K) such that the analytic rank of E/K is 0 and K is totally real. In this case we use [16, Th. 3.7] to deduce that the algebraic rank is also equal to 0. In small examples (see e.g. Section 6.1) it is sometimes possible to prove that the algebraic rank is trivial by a Selmer group computation.

If $r > 0$ we generally assume the validity of the equivariant rank conjecture and only consider examples where the equivariant rank conjecture implies that $E(K)$ is built from subgroups $E(F)$ where F ranges over the subfields of $K/\mathbb{Q}$ with $[F : \mathbb{Q}] \leq 2$. For $F = \mathbb{Q}$ we use the MAGMA routine to compute $E(\mathbb{Q})$ and if F is a quadratic extension we look at the associated quadratic twist E_d of E and compute $E_d(\mathbb{Q})$. Computing the isomorphism $E \simeq E_d$ (defined over F) we then obtain $E(F)$.

Our ability to compute $Ш(E/K)$ is even more limited. We remind the reader that throughout the manuscript we assume finiteness of $Ш(E/K)$. In order to compute $\#Ш(E/K)$ we use the classical BSD conjecture for E/K. In this way we obtain a conjectural value for $\#Ш(E/K)$ which we wish to use to compute the associated refined Euler characteristic. Since we only dispose of the (conjectural) order of $Ш(E/K)$ we are usually restricted to deal with primes l which do not divide this order. However, in some rare cases (see e.g. Section 6.2) it suffices to know this order to compute the refined Euler characteristic of $Ш(E/K)$. Moreover, in some examples (see Section 6.1 and 6.3) the computations lead to a conjectural description of the structure of $Ш(E/K)$ as a Galois module.

5.6. **Computation of induction.** If H is a subgroup of G then there is a canonical induction map $\mathrm{ind}_H^G : K_0(\mathbb{Z}_l[H], \mathbb{Q}_l) \longrightarrow K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)$. We refer the reader to [5, Sec. 6] where we provide an algorithmic description of this map.

6. Examples

In this section we illustrate our results with some explicit examples. The computational results of this section can be reproduced using the MAGMA implementations available from

`http://www.mathematik.uni-kassel.de/~bley/pub.html`.

6.1. **Navilarekallu's example.** In this subsection we redo the example from [30]. Let

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

and K be the splitting field of $f(x) = x^3 - 4x + 1$. Then $K/\mathbb{Q}$ is an S_3-extension. The elliptic curve E is denoted $11A1$ in Cremona's database. Its conductor is $N_E = 11$ and the discriminant of K is given by $d_{K/\mathbb{Q}} = 229^3$. The field K is totally real and contains the quadratic subfield $F := \mathbb{Q}(\sqrt{229})$. Actually, K is the Hilbert class field of F.

We have $S = \{11, 229\}$. For a rational prime q we fix a place v_q of K above q. One easily computes

$$\begin{aligned}
&\#\bar{I}_{229} = 2,\\
&\#\bar{E}_{ns}(k_{v_2}) = 5, \#\bar{E}_{ns}(k_{v_3}) = 20, \#\bar{E}_{ns}(k_{v_5}) = 140,\\
&\#\bar{E}_{ns}(k_{v_{11}}) = 1330, \#\bar{E}_{ns}(k_{v_{229}}) = 215\\
&E(K)_{tors} = E(\mathbb{Q})_{tors} \text{ is cyclic of order } 5,\\
&E \text{ has split multiplcative reduction at } v_{11} \text{ with } c_{v_{11}} = 5,\\
&(L_{11}(E/Q, \bar{\chi}, 1)) = (10/11, 10/11, 133/121),\\
&(L_{229}(E/Q, \bar{\chi}, 1)) = (215/229, 1, 215/229)\\
&\mathrm{ind}_{G_{v_{11}}}^{G} \chi_{G_{v_{11}}}(k_{v_{11}}) = (11, 11, 121),\\
&\mathrm{ind}_{G_{v_{229}}}^{G} \chi_{G_{v_{11}}}(k_{v_{229}}) = (229, 1, 229).
\end{aligned}$$

The L-values can easily be computed with a precision of 20 or more decimal digits. We give here only the first 6 decimal digits: $(L(E/\mathbb{Q}, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)} = (0.253842, 0.419359, 2.66127)$. Therefore the analytic rank for each of the L-functions is trivial. By [16, Th. 3.7] (which has been proved independently by Longo and Tian-Zhang) we have $E(K) = E(K)_{tors} = E(\mathbb{Q})_{tors}$.

In this small case this can also be proved by algorithmic methods. Let K_1 be the number field defined by $f(x) = x^3 - 4x + 1$. Then the computation of Selmer groups using the MAGMA routine TwoSelmerGroup shows that $\mathrm{Sel}^{(2)}(E/K_1)$ and $\mathrm{Sel}^{(2)}(E/F)$ are trivial. It follows quite easily that $E(K)$ must be torsion.

We obtain

$$u = (0.200000, -5.00000, -25.0000),$$

which numerically confirms the rationality conjecture. We point out that the resolvents and therefore also the value for u depend on the choice of the integral normal basis element α_0. The algorithm of [3] does not always produce the same generator, so that one may obtain different results when running the algorithm. Note, however, that the validity of the ETNC does not depend on this choice (see Remark 4.6).

From the BSD-conjecture we conclude the conjectural order $\#Ш(E/K) = 625$, so that $HP = \{2, 3, 5, 11, 229\}$. By Corollary 4.7 we immediately obtain a numerical confirmation for all primes $l \notin HP$.

For $l = 2$ hypothesis (H2a) is not satisfied and for $l = 5$ we do not have (H5). For $l = 3$ we have $\xi_l = (1, 1, 1)$. So $u = u\xi_l^{-1}$ is a torsion element in $K_0(\mathbb{Z}_3[G], \mathbb{Q}_3)$. Here $K_0(\mathbb{Z}_3[G], \mathbb{Q}_3)_{tors}$ is cyclic of order 2 and by the methods of [5] we can check that u is indeed trivial in this group. We can also directly check the explicit congruence (10) which becomes $-1 \equiv -25 (\mathrm{mod}\ 3)$ in this example.

For $l \in \{11, 229\}$ the group $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ is trivial and from the above data one easily deduces the validity of the l-part of ETNC.

Although we do not have (H5) for $l = 5$ one can try to proceed as in Remark 4.3. By Proposition 5.3 we can compute the refined Euler characteristic of $\mathcal{C}$ (see Remark 4.3 for the notation). Since we do not know how to rigorously compute the Euler characteristics of $\mathcal{S}$ and $H_f^1(\mathbb{Q}, T_l)^*$ we only get a very vague idea about the Galois structure of $Ш(E/K)$. However, by the conjectural validity of ETNC at $l = 5$ one is tempted to guess that $\tilde{\chi}(Ш(E/K)_{5^\infty}) = (1, 1, \frac{1}{25})$. One may therefore guess that $Ш(E/K)_{5^\infty}$ lives in the 2-dimensional component of $\mathbb{Q}_5[G]$ and has the resolution

$$0 \longrightarrow M_2(\mathbb{Z}_5) \overset{\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}}{\longrightarrow} M_2(\mathbb{Z}_5) \longrightarrow Ш(E/K)_{5^\infty} \longrightarrow 0.$$

This was verified by T.Fisher in private communication.

6.2. **A D_5-Example.** In this example we let E be the curve $73A1$ in Cremona's notation. We let K be the number field defined by the irreducible polynomial

$$f(x) = x^{10} - 2x^9 - 20x^8 + 2x^7 + 69x^6 - x^5 - 69x^4 + 2x^3 + 20x^2 - 2x - 1.$$

Then $K/\mathbb{Q}$ is a Galois extension with dihedral group D_5. We have $N_E = 73$ and $d_{K/\mathbb{Q}} = 401^5$. The field K is totally real and contains the quadratic subfield $F := \mathbb{Q}(\sqrt{401})$. Hence $S = \{73, 401\}$. Actually, K is the Hilbert class field of F.

We have four characters

	id	τ	σ	σ^2
χ_1	1	1	1	1
χ_2	1	-1	1	1
χ_3	2	0	$\zeta_5 + \zeta_5^{-1}$	$\zeta_5^2 + \zeta_5^{-2}$
χ_4	2	0	$\zeta_5^2 + \zeta_5^{-2}$	$\zeta_5 + \zeta_5^{-1}$

Hence $\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(K_3)$ with $K_3 = \mathbb{Q}(\beta)$ where $\beta := \zeta_5 + \zeta_5^{-1}$. Elements in the center of $\mathbb{C}[G]$ will be denoted by 4-tuples $z = (z_1, \dots, z_4), z_i \in \mathbb{C}$. Recall that $z \in \zeta(\mathbb{Q}[G])$ if and only if $z_1, z_2 \in \mathbb{Q}$, $z_3, z_4 \in K_3$ and $\varphi(z_3) = z_4$, where $\langle \varphi \rangle = \mathrm{Gal}(K_3/\mathbb{Q})$. Elements in $z \in \zeta(\mathbb{Q}[G])$ will be represented by tuples $z = (z_{\chi_1}, z_{\chi_2}, z_{\chi_3})$.

The L-values were computed with a precision of 20 decimal digits and are given by

$$\begin{aligned} & (L(E/\mathbb{Q}, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)} \\ = \; & (1.1826604672413298661, 2.1261328339601570537, \\ & 0.16304872052191552777, 7.6598191709443800630). \end{aligned}$$

The analytic rank of each of the twisted L-functions is therefore 0 and as in the first example the theorem of Longo and Tian-Zhang (see [16, Th. 3.7]) allows us to conclude that $E(K)$ is finite.

The numerical computation of L-values, resolvents and periods leads to

$$\begin{aligned} u \; = \; & (0.49999999999999999999, 18.000000000000000008, \\ & 0.58359213500126187216, 27.416407864998738187). \end{aligned}$$

Numerically this confirms the rationality conjecture because u is close to

$$(1/2, 18, -12\beta + 8, 12\beta + 20)$$

and $\varphi(-12\beta + 8) = 12\beta + 20$. The minimal polynomial of $-12\beta + 8$ is given by $x^2 - 28x + 16$. Again we point out that the resolvents and therefore also the value for u depend on the choice of the integral normal basis element α_0.

We further see that

$$\begin{aligned}
&\#\bar{I}_{401} = 2,\\
&\#\bar{E}_{ns}(k_{v_2}) = 22, \#\bar{E}_{ns}(k_{v_3}) = 16, \#\bar{E}_{ns}(k_{v_5}) = 3044,\\
&\#\bar{E}_{ns}(k_{v_{73}}) = 2073071592, \#\bar{E}_{ns}(k_{v_{401}}) = 388,\\
&E(K)_{tors} = E(\mathbb{Q})_{tors} \text{ is cyclic of order } 2,\\
&E \text{ has split multiplcative reduction at } v_{73} \text{ with } c_{v_{73}} = 2,\\
&(L_{73}(E/Q, \bar{\chi}, 1)) = (72/73, 72/73, \frac{1}{5329}(73\beta + 5403), \frac{1}{5329}(-73\beta + 5330),\\
&(L_{401}(E/Q, \bar{\chi}, 1)) = (388/401, 1, 388/401, 388/401),\\
&\mathrm{ind}_{G_{v_{73}}}^{G} \chi_{G_{v_{11}}}(k_{v_{11}}) = (73, 73, 5329),\\
&\mathrm{ind}_{G_{v_{401}}}^{G} \chi_{G_{v_{401}}}(k_{v_{401}}) = (401, 1, 401).
\end{aligned}$$

Recall that any element $z \in \zeta(\mathbb{Q}[G])$ is represented by a tuple $z = (z_{\chi_1}, z_{\chi_2}, z_{\chi_3})$. This explains why some of the above tuples have only 3 components.

From the BSD conjecture we derive the conjectural order $\#\text{Ш}(E/K) = 2304 = 2^8 3^2$. Thus we have $HP = \{2, 3, 5, 73, 401\}$ and by Corollary 4.7 the ETNC is numerically confirmed outside HP.

For $l = 2$ we cannot perform our computations because 2 divides $\#G$.

For $l = 3$ our MAGMA implementation terminates without verifying the 3-part of ETNC because 3 divides the order of $\text{Ш}(E/K)$. In general we are not able to compute the refined Euler characteristic of $\text{Ш}(E/K)$ if l divides $\#\text{Ш}(E/K)$ because we have no information about its Galois structure. However, in some special cases like this one, it is possible to pin down the exact Euler characteristic by purely representation theoretic considerations. Here $\text{Ш}(E/K)[3]$ is conjecturally bicyclic of order 9 and we may consider it as a representation over $\mathbb{F}_3$. There are three irreducible representations over $\mathbb{F}_3$, namely the trivial character, the sign character and a 2-dimensional representation (defined over $\mathbb{F}_9$). A BSD-computation for $E/\mathbb{Q}$ and E/F shows that $\#\text{Ш}(E/\mathbb{Q})[3] = 1$ and $\#\text{Ш}(E/F) = 9$ so that we obtain $\tilde{\chi}(\text{Ш}(E/K)) = (1, 9, 1)$. Using this we can also confirm the validity of ETNC at $l = 3$.

For $l \in \{73, 401\}$ the $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ is trivial and from the above data one easily deduces the validity of the l-part of the ETNC.

Most interesting is the case $l = 5$ because in this case we have non-trivial torsion subgroup $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ so that we must verify the explicit congruence (10). We have $\xi_5 = (1, 1, 1)$, so that $\eta := u\xi_5^{-1} = (1/2, 18, -12\beta + 8)$. Let $\mathfrak{p}$ denote the unique prime lying over 5 in K_3. Then one easily checks that the valuation at $\mathfrak{p}$ of $\frac{1}{2} \cdot 18 - (-12\beta + 8)$ equals 1, as predicted by the ETNC.

6.3. **A D_7-Example.** In this example we let E be the curve $11A1$ in Cremona's notation. We let K be the number field defined by the irreducible polynomial

$$\begin{aligned}
f(x) \quad = \quad & x^{14} - 2x^{13} - 25x^{12} + 69x^{11} + 161x^{10} -\\
& 632x^9 - 147x^8 + 2146x^7 - 1171x^6 - 2669x^5 + 2682x^4 +\\
& 667x^3 - 1466x^2 + 336x + 49.
\end{aligned}$$

Then $K/\mathbb{Q}$ is a Galois extension with dihedral group D_7. We have $N_E = 11$ and $d_{K/\mathbb{Q}} = 577^7$. The field K is totally real and contains the quadratic subfield $F := \mathbb{Q}(\sqrt{577})$. Hence $S = \{11, 577\}$. Actually, K is the Hilbert class field of F.

We have five characters

	id	τ	σ	σ^2	σ^3
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	1
χ_3	2	0	$\zeta_7+\zeta_7^{-1}$	$\zeta_7^2+\zeta_7^{-2}$	$\zeta_7^3+\zeta_7^{-3}$
χ_4	2	0	$\zeta_7^2+\zeta_7^{-2}$	$\zeta_7^4+\zeta_7^{-4}$	$\zeta_7^6+\zeta_7^{-6}$
χ_5	2	0	$\zeta_7^3+\zeta_7^{-3}$	$\zeta_7^6+\zeta_7^{-6}$	$\zeta_7^2+\zeta_7^{-2}$

Hence $\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(K_3)$ with $K_3 = \mathbb{Q}(\beta)$ where $\beta := \zeta_7 + \zeta_7^{-1}$. Elements in the center of $\mathbb{C}[G]$ will be denoted by 5-tuples $z = (z_1, \dots, z_5), z_i \in \mathbb{C}$. Recall that $z \in \zeta(\mathbb{Q}[G])$ if and only if $z_1, z_2 \in \mathbb{Q}$, $z_3, z_4, z_5 \in K_3$ are Galois conjugates. Elements in $z \in \zeta(\mathbb{Q}[G])$ will be represented by tuples $z = (z_{\chi_1}, z_{\chi_2}, z_{\chi_3})$.

The L-values were computed with a precision of 30 decimal digits and are given by

$$\begin{aligned}
&(L(E/\mathbb{Q}, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)} \\
= \;&(0.253841860855910684337758923351, 0.264189373454632540506329085616, \\
&8.46480303158617169018788040257, 1.07820141250454111015938289065, \\
&0.516343882321445768698269093336).
\end{aligned}$$

The analytic rank of each of the twisted L-functions is therefore 0 and as before the theorem of Longo and Tian-Zhang (see [16, Th. 3.7]) allows us to conclude that $E(K)$ is finite.

The numerical computation of L-values, resolvents and periods leads to

$$\begin{aligned}
u \;=\; &(-0.199999999999999999999999958641, -5.00000000000000000000000004909, \\
&126.222933488057632838305516431, 16.0776033026947639028170113251, \\
&7.69946320924760325930251071912).
\end{aligned}$$

Numerically this confirms the rationality conjecture because u is close to

$$(-1/5, -5, 25\beta^2 + 50\beta + 25, -50\beta^2 - 25\beta + 125, 25\beta^2 - 25\beta)$$

and the last three components are Galois conjugates. The minimal polynomial of $25\beta^2 + 50\beta + 25$ is given by $x^3 - 150x^2 + 3125x - 15625$. Once again we point out that the resolvents and therefore also the value for u depend on the choice of the integral normal basis element α_0.

We further see that

$$\begin{aligned}
&\#\bar{I}_{577} = 2, \\
&\#\bar{E}_{ns}(k_{v_2}) = 145, \#\bar{E}_{ns}(k_{v_5}) = 35, \#\bar{E}_{ns}(k_{v_7}) = 60, \\
&\#\bar{E}_{ns}(k_{v_{11}}) = 19487170, \#\bar{E}_{ns}(k_{v_{577}}) = 545, \\
&E(K)_{tors} = E(\mathbb{Q})_{tors} \text{ is cyclic of order } 5, \\
&E \text{ has split multiplcative reduction at } v_{73} \text{ with } c_{v_{73}} = 5, \\
&(L_{11}(E/Q, \bar{\chi}, 1)) = (10/11, 10/11, \frac{1}{121}(-11\beta^2 + 144))), \\
&(L_{577}(E/Q, \bar{\chi}, 1)) = (545/577, 1, 545/577), \\
&\mathrm{ind}_{G_{v_{11}}}^{G} \chi_{G_{v_{11}}}(k_{v_{11}}) = (11, 11, 121), \\
&\mathrm{ind}_{G_{v_{577}}}^{G} \chi_{G_{v_{577}}}(k_{v_{577}}) = (577, 1, 577).
\end{aligned}$$

Recall that any element $z \in \zeta(\mathbb{Q}[G])$ is represented by a tuple $z = (z_{\chi_1}, z_{\chi_2}, z_{\chi_3})$. This explains why the above tuples have only 3 components.

From the BSD conjecture we derive the conjectural order $\#\text{Ш}(E/K) = 5^{12}$. Thus we have $HP = \{2, 5, 7, 11, 577\}$ and by Corollary 4.7 the ETNC is numerically confirmed outside HP.

For $l = 2$ we cannot perform our computations because 2 divides $\#G$.

For $l = 5$ we cannot perform the computations because 5 divides the order of $\text{Ш}(E/K)$ and the Tamagawa numbers. As in Example 6.1 we try to proceed as in Remark 4.3. By the conjectural validity of ETNC at $l = 5$ one may guess that $\tilde{\chi}(\text{Ш}(E/K)_{5^\infty}) = (1, 1, \frac{1}{25})$. One may therefore guess that $\text{Ш}(E/K)_{5^\infty}$ lives in the 2-dimensional component of $\mathbb{Q}_5[G]$ and has the resolution

$$0 \longrightarrow M_2(\mathbb{Z}_5[\zeta_7]^+) \xrightarrow{\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}} M_2(\mathbb{Z}_5[\zeta_7]^+) \longrightarrow \text{Ш}(E/K)_{5^\infty} \longrightarrow 0.$$

Note that $\mathbb{Z}_5[\zeta_7]^+/5\mathbb{Z}_5[\zeta_7]^+ = \mathbb{F}_{5^3}$ so that this matches with the conjectural order of $\text{Ш}(E/K)$.

For $l \in \{11, 577\}$ the $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ is trivial and from the above data one easily deduces the validity of the l-part of the ETNC.

The most interesting prime is $l = 7$ because in this case we have non-trivial torison subgroup $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ so that we must verify the explicit congruence (10). We have $\xi_7 = (1, 1, 1)$, so that $\eta := u\xi_7^{-1} = (-1/5, -5, 25\beta^2 + 50\beta + 25)$. Let $\mathfrak{p}$ denote the unique prime lying over 7 in K_3. Then one easily checks that the valuation at $\mathfrak{p}$ of $\frac{-1}{5} \cdot (-5) - (25\beta^2 + 50\beta + 25)$ equals 1, as predicted by the ETNC.

6.4. **More dihedral examples.** We have numerically checked a few more D_l-examples which are completely analogous to the previous examples. We searched for cases where we could apply our methods for the prime l. In particular we needed the Mordell-Weil group $E(K)$ to be finite. In all our examples K is a totally real number field, so that we can apply [16, Th. 3.7]. In all the examples our computations numerically confirm the l-part of ETNC.

In the following we list our examples. In each of our examples K is the Hilbert class field of the real quadratic field $\mathbb{Q}(\sqrt{d})$. The elliptic curve is referenced as in

Cremona's tables.

	d	E
D_3	229	$11a1$
	229	$17a1$
	257	$11a1$
	257	$17a1$
	733	$17a1$
	761	$17a1$
D_5	$19 \cdot 43$	$17a1$
	$19 \cdot 43$	$37b1$
	$7 \cdot 199$	$17a1$
	$7 \cdot 199$	$19a1$
	1429	$17a1$
	1429	$19a1$
D_7	577	$11a1$
	577	$17b1$
	577	$19a1$
	1009	$37b1$

With more effort it is certainly possible to compute more examples. We refer the interested reader to the batch files in

`http://www.mathematik.uni-kassel.de/~bley/pub.html` .

6.5. **Another D_5-Example (incomplete).** In this example we let again E be the curve $11A1$ in Cremona's notation. We take the same number field K as in the first D_5 example, namely the Hilbert class field of $F := \mathbb{Q}(\sqrt{401})$. We have $N_E = 11$ and $d_{K/\mathbb{Q}} = 401^4$. Hence $S = \{11, 401\}$.

Recall that$\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(K_3)$ with $K_3 = \mathbb{Q}(\beta)$ where $\beta := \zeta_5 + \zeta_5^{-1}$.

The computation of L-values showed that conjecturally

$$\begin{aligned} &\mathrm{ord}_{s=1}(L(E/\mathbb{Q}, \chi_i, s)) = 0 \text{ for } i = 1, 3, 4, \\ &\mathrm{ord}_{s=1}(L(E/\mathbb{Q}, \chi_2, s)) = 2. \end{aligned}$$

The leading terms in the Taylor expansion of the twisted L-series were computed with a precision of 20 decimal digits and are given by

$$\begin{aligned} & (L^*(E/\mathbb{Q}, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)} \\ = \; & (0.25384186085591068434, 11.064607087619745148, \\ & 5.2651360430010329737, 0.76817299610176707595). \end{aligned}$$

The validity of the rank conjecture would imply that the χ_2-eigenspace of $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ is 2-dimensional. Since $K^{\ker(\chi_2)} = \mathbb{Q}(\sqrt{401}) =: F$ this implies that conjecturally $\mathrm{rk}(E(F)) = 2$. By considering the quadratic twist of $E/\mathbb{Q}$

$$E_{401} : y^2 = x^3 - 2153446992x - 69667552958832$$

we compute

$$E(F)/E(F)_{tors} = \langle P_1, P_2 \rangle$$

with

$$P_1 = \left(\frac{74}{9}, \frac{53}{54}\sqrt{401} - \frac{1}{2} \right), \quad P_2 = \left(6, \frac{1}{2}\sqrt{401} - \frac{1}{2} \right).$$

One checks that the conjugate of P_i is $-P_i$ for $i = 1, 2$ so that by Proposition 5.1 we obtain for the χ_2-part of the equivariant regulator

$$\det\left((\langle P_i, P_j\rangle)_{i,j\in\{1,2\}}\right) = 34.914427985010413291.$$

Possibly $\langle P_1, P_2\rangle$ is not the full Mordell-Weil group $E(K)$. However, if we content ourselves with checking the rationality conjecture, then this information is enough.

Together with the computations of L-values, resolvents and periods we obtain

$$\begin{aligned} u &= (0.20000000000000000000, -5.0000000000000000017, \\ &\quad -65.450849718747376977, -9.5491502812526296414). \end{aligned}$$

Numerically this confirms the rationality conjecture because u is close to

$$(1/5, -5, -25\beta - 50, 25\beta - 25)$$

and $\varphi(-25\beta - 5) = 25\beta - 25$. The minimal polynomial of $-25\beta - 5$ is given by $x^2 + 75x + 625$. Again we note that u also depends on the choice of α_0.

We further see that

$$\begin{aligned} &\#\bar{I}_{401} = 2, \\ &\#\bar{E}_{ns}(k_{v_2}) = 25, \#\bar{E}_{ns}(k_{v_5}) = 3025, \#\bar{E}_{ns}(k_{v_{11}}) = 161050, \#\bar{E}_{ns}(k_{v_{401}}) = 400 \\ &E(K)_{tors} = E(\mathbb{Q})_{tors} \text{ is cyclic of order } 5, \\ &E \text{ has split multiplcative reduction at } v_{11} \text{ with } c_{v_{11}} = 5, \\ &(L_{11}(E/Q, \bar{\chi}, 1)) = (10/11, 10/11, \frac{1}{121}(-11\beta + 122)), \\ &(L_{401}(E/Q, \bar{\chi}, 1)) = (400/401, 1, 400/401), \\ &\mathrm{ind}_{G_{v_{11}}}^{G} \chi_{G_{v_{11}}}(k_{v_{11}}) = (11, 11, 121), \\ &\mathrm{ind}_{G_{v_{401}}}^{G} \chi_{G_{v_{401}}}(k_{v_{401}}) = (401, 1, 401). \end{aligned}$$

Recall that any element $z \in \zeta(\mathbb{Q}[G])$ is represented by a tuple $z = (z_{\chi_1}, z_{\chi_2}, z_{\chi_3})$.

Although we cannot be sure that we have computed the full Mordell-Weil group $E(K)$ it seems to be most likely that we have found a subgroup of finite index and that the only primes that possibly divide this index are 2 and 5. Therefore, as long as we exclude these primes from our considerations, we still obtain some evidence for the integrality conjecture.

Assuming $E(K) = \langle P_1, P_2\rangle$ we derive from the BSD conjecture the conjectural order $\#\text{Ш}(E/K) = 5^8$. Thus we have $HP = \{2, 5, 11, 401\}$ and by Corollary 4.7 the ETNC is numerically confirmed outside HP.

As already mentioned we cannot expect any integrality statements for $l = 2, 5$, which would also not be possible for other reasons because for $l = 2$ we cannot perform our computations because 2 divides $\#G$, and $l = 5$ divides $\#G$ and we have non-trivial cohomology modules such as $\text{Ш}(E/K)$ and $E(K)$ which may not be $\mathbb{Z}_l[G]$-perfect. Also, (H5) is not satisfied.

For $l \in \{11, 401\}$ the $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ is trivial and from the above data one easily deduces the validity of the l-part of the ETNC.

References

[1] W. Bley, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture (part II)*, preprint 2010.

[2] W. Bley, D. Burns, *Equivariant epsilon constants, discriminants and étale cohomology*, Proc. London Math. Soc. **87** (2003), 545–590.
[3] W. Bley, H. Johnston, *Computing generators of free modules over orders in group algebras*, J.Algebra (Computational Section), **320** (2008), 836–852.
[4] W. Bley, H. Johnston, *Computing generators of free modules over orders in group algebras II*, to appear in Math.Comp..
[5] W. Bley, S.M.J. Wilson, *Computations in relative algebraic K-groups*, LMS JCM **12** (2009), 166–194.
[6] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, In: 'The Grothendieck-festschrift' vol. 1, Progress in Math. **86** Birkhäuser, Boston, (1990), 333 - 400.
[7] T. Bouganis, V. Dokchitser, *Algebraicity of L-values for elliptic curves in a false Tate curve tower*, Math. Proc. Cambridge Philos. Soc. **142** (2007), 193–204.
[8] M. Breuning, *On equivariant global epsilon constants for certain dihedral extensions*, Math. Comp. **73** (2004), 881–898.
[9] M. Breuning, D. Burns, *Additivity of Euler characteristics in relative algebraic K-groups*, Homology, Homotopy and Applications **7** (2005), 11-36.
[10] M. Breuning, D. Burns, *Leading terms of Artin L-functions at $s = 0$ and $s = 1$*, Compositio Math. **143** (2007), 1427-1464.
[11] D. Burns, M. Flach, *Motivic L-functions and Galois module structures*, Math. Ann. **305** (1996) 65-102.
[12] D. Burns, M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients*, Documenta Math. **6** (2001) 501-570.
[13] D. Burns, *Equivariant Whitehead torsion and refined Euler characteristics*, CRM Proceedings and Lecture Notes, Vol. 36 (American Mathematical Society, Providence, RI, 2004), 35-59.
[14] D. Burns, *Leading terms and values of equivariant motivic L-functions*, Pure App. Math. Q. **6** (2010), (John Tate Special Issue, Part II), 83–172.
[15] C. Curtis, I. Reiner, Methods of representation theory, volume I and II. Wiley, 1981 and 1987.
[16] H. Darmon, *Heegner points, Stark-Heegner points and values of L-series*, International Congress of Mathematicians. Vol.II, 313–345, Eur. Math. Soc., Zürich, 2006.
[17] T. Dokchitser, *Computing Special Values of Motivic L-Functions*, Experiment. Math. **13** (2004), 137–149.
[18] M. Flach, *The equivariant Tamagawa number conjecture - A survey*, in: 'Stark's Conjecture: recent progress and new directions' (eds. D.Burns, C.Popescu, J.Sands and D.Solomon), Contemp. Math. **358** Amer. Math. Soc.,(2004) 79-126.
[19] M. Flach, *Iwasawa theory and motivic L-functions*, Pure and Applied Mathematics Quaterly **5**, Number 1, (2009) 255-294.
[20] A. Fröhlich, *L-values at zero and multiplicative Galois module structure (also Galois-Gauss sums and additive Galois module structure*, J.Reine Angew. Math **397**, (1989) 42-99.
[21] J. Fearnley, H. Kisilevsky, *Critical values of derivatives of twisted elliptic L-functions*, Experiment. Math. **19** (2010), 149–160.
[22] B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L-series*, Inventiones Mathematicae **84 (2)**, (1986) 225-320.
[23] A. Grothendieck, *Groupes de Monodromie en Géométrie Algébrique (SGA 7 I)*, Lecture Notes in Math. **288**, Springer Verlag, 1972.
[24] G. Kings, *An introduction to the equivariant Tamagawa number conjecture: the relation to the Birch-Swinnerton-Dyer conjecture*, Preprint Nr. 26/2009, Universität Regensburg.
[25] V.A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, *Progr. in Math.* **87**, Boston, Boston, MA (1990).
[26] V.A. Kolyvagin, D.Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Leningrad Math.J. **1**, (1990) 1229-1253.
[27] V.A. Kolyvagin, D.Y. Logachev, *Finiteness of* Ш *over totally real fields*, USSR Izvestiya **39**, (1992) 829-853.
[28] MAGMA, Version V2.15-9, Sydney 2010.
[29] B. Mazur, J. Tate, *Refined conjectures of the Birch and Swinnerton-Dyer type*, Duke Math. J. **54** (1987), 711–750.
[30] T. Navilarekallu, *Equivariant Birch-Swinnerton-Dyer conjecture for the base change of elliptic curves: an example*, International Mathematics Research Notices, Vol. 2008, 33 pages.
[31] W. Niziol, *Cohomology of crystalline representations*, Duke Math. J. **71** (1993), 747–791.

[32] J.H. Silverman, *The arithmetic of elliptic curves*, Springer Verlag (1986).
[33] G. Shimura, *On the periods of modular forms*, Math.Ann. **229** (1977), 211–221.
[34] G. Shimura, *The special values of the zeta functions associated to Hilbert modular forms*, Duke Math. J. **45** (1978).
[35] R. G. Swan, *Algebraic K-theory*, Lecture Notes in Mathematics **76**, Springer Verlag (1968).
[36] O. Venjakob, *From the Birch and Swinnerton-Dyer Conjecture over the Equivariant Tamagawa Number Conjecture to non-commutative Iwasawa theory*, in 'L-functions and Galois representations', London Math. Soc. Lecture Note Ser., vol. 320, Cambridge University Press, Cambridge, 2007, 333–380.
[37] S. Zhang, *Heights of Heegner points on Shimura curves*, Annals of Math. **153**, (2001) 27-147.

Fachbereich für Mathematik und Naturwissenschaften der Universität Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, Germany
E-mail address: bley@mathematik.uni-kassel.de