

ON EQUIVARIANT GLOBAL EPSILON CONSTANTS FOR CERTAIN DIHEDRAL EXTENSIONS

MANUEL BREUNING

ABSTRACT. We consider a conjecture of Bley and Burns which relates the epsilon constant of the equivariant Artin L -function of a Galois extension of number fields to certain natural algebraic invariants. For an odd prime number p , we describe an algorithm which either proves the conjecture for all degree $2p$ dihedral extensions of the rational numbers or finds a counterexample. We apply this to show the conjecture for all degree 6 dihedral extensions of \mathbb{Q} . The correctness of the algorithm follows from a finiteness property of the conjecture which we prove in full generality.

1. INTRODUCTION

Let L/K be a Galois extension of number fields with Galois group G . In [5], Bley and Burns conjectured an equality in the relative algebraic K -group $K_0(\mathbb{Z}[G], \mathbb{R})$ involving the epsilon constant of the equivariant Artin L -function of the extension, an equivariant discriminant and certain local terms coming from étale cohomology. This conjecture fits into the general framework of the equivariant Tamagawa number conjectures of Burns and Flach [7]: it can be shown to express the compatibility of the equivariant Tamagawa number conjectures for $(h^0(\text{Spec}(L)), \mathbb{Z}[G])$ and $(h^0(\text{Spec}(L))(1), \mathbb{Z}[G])$ with the functional equation of the equivariant Artin L -function of L/K . It is also known to be a strong refinement of the second Chinburg conjecture.

The conjecture is known in some cases. In [5] it is shown to be valid for extensions that are at most tamely ramified and for abelian extensions of \mathbb{Q} with odd conductor. However, for non-abelian wildly ramified extensions very little is known. Bley and Burns considered certain dihedral extensions of \mathbb{Q} where the conjecture follows easily from the cases mentioned above, and Snaith showed it in [16] for some degree 8 quaternion extensions of \mathbb{Q} . In [3], Bley developed an algorithm that can demonstrate the validity of the conjecture for certain abelian extensions L/K , but hitherto the implementation of this algorithm only gave numerical evidence rather than a complete proof.

This paper now establishes the conjecture for a natural class of non-abelian, possibly wildly ramified extensions.

Received by the editor November 25, 2002.

2000 *Mathematics Subject Classification*. Primary 11R33; Secondary 11R42, 11Y40.

Key words and phrases. Equivariant Tamagawa number conjecture, equivariant epsilon constants, dihedral extensions.

The author was supported by the DAAD and the EPSRC.

Theorem 1.1. *The conjecture is true for all Galois extensions L/\mathbb{Q} with $\text{Gal}(L/\mathbb{Q})$ the dihedral group of order 6.*

We remark that several of the steps leading to this result are true in much greater generality and might therefore themselves be of some independent interest. In section 2 we recall the conjecture of Bley and Burns and show how it can be expressed in local terms. From this we deduce the following finiteness result.

Theorem 1.2. *Let K be a number field and G a finite group. There exists a finite set of Galois extensions L/K with $\text{Gal}(L/K) \cong G$ such that the validity of the conjecture for these finitely many extensions implies the validity of the conjecture for all extensions L/K with $\text{Gal}(L/K) \cong G$.*

In section 3 we prove a result about the relative algebraic K_0 -group of the integral group ring of dihedral groups, which in conjunction with functorial properties of the conjecture gives an important reduction step. Finally, in the last section, we apply these results to develop an algorithm that, for an odd prime p , either proves the conjecture for all degree $2p$ dihedral extensions of the rational numbers or finds a counterexample. Our algorithm relies on Bley's algorithm applied to certain cyclic extensions. Using a modification of the existing implementation of Bley's algorithm in PARI/GP, we prove Theorem 1.1.

Acknowledgement. I am very grateful to Werner Bley and David Burns for numerous helpful discussions and to Dimitrij Kusnezow and Werner Bley for giving permission to use and modify their implementation of Bley's algorithm.

2. THE CONJECTURE

In this section we recall the conjecture of [5] and prove that all ingredients of the conjecture are local. We then apply this to show Theorem 1.2.

Notation. We first recall some notation from [5, sections 2 and 3]. For a finite group G , we need the relative K_0 -group $K_0(\mathbb{Z}[G], \mathbb{Q})$ and the K_1 -groups $K_1(\mathbb{Z}[G])$, $K_1(\mathbb{Q}[G])$. The reduced norm induces an injective map $K_1(\mathbb{Q}[G]) \rightarrow \zeta(\mathbb{Q}[G])^\times$ where $\zeta(\mathbb{Q}[G])$ is the centre of the group algebra, and the image is denoted by $\zeta(\mathbb{Q}[G])^{\times+}$. The map $\hat{\partial}_{\mathbb{Z}[G], \mathbb{Q}}^1 : \zeta(\mathbb{Q}[G])^{\times+} \rightarrow K_0(\mathbb{Z}[G], \mathbb{Q})$ is the composite of the inverse of the reduced norm map and the natural map $K_1(\mathbb{Q}[G]) \rightarrow K_0(\mathbb{Z}[G], \mathbb{Q})$ coming from the exact localization sequence in K -theory. For a subgroup H of G , we write i_H^G for the induction map on any of these K -groups (including $i_H^G : \zeta(\mathbb{Q}[H])^{\times+} \rightarrow \zeta(\mathbb{Q}[G])^{\times+}$ via the isomorphism given by the reduced norm). We also need these groups with \mathbb{Q} replaced by \mathbb{Q}^c (an algebraic closure of \mathbb{Q}) or \mathbb{Q}_l or \mathbb{R} , \mathbb{Z} replaced by \mathbb{Z}_l , etc.

If K is a number field, we write $S_f(K)$ for the set of finite places of K . The completion of K at $v \in S_f(K)$ is denoted by K_v and the residue characteristic of v by $l(v)$. Also $S_l(K)$ is the set of places above the rational prime l , and more generally if L/K is an extension of number fields and $v \in S_f(K)$, then $S_v(L)$ is the set of places of L above v .

The conjecture. Now let L/K be a Galois extension of number fields with group G . For each $v \in S_f(K)$ we fix a place $w \in S_v(L)$ with corresponding embedding $i_w : L \rightarrow L_w$. The decomposition group of w is denoted by G_w and identified with $\text{Gal}(L_w/K_v)$. Let S be a finite subset of $S_f(K)$, containing the places which ramify

in L/K . For each $v \in S$, we choose a full projective $\mathbb{Z}_{l(v)}[G_w]$ -sublattice \mathcal{L}_w of \mathcal{O}_{L_w} which is contained in a sufficiently high power of the maximal ideal, such that $\exp(\mathcal{L}_w)$ is defined. Let \mathcal{L} denote the full projective $\mathbb{Z}[G]$ -sublattice of L which, at each prime l , has l -adic completion

$$(1) \quad \mathcal{L}_l = \left(\prod_{v \in S_l(K) \setminus S} \mathcal{O}_{L,v} \right) \times \left(\prod_{v \in S_l(K) \cap S} \mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l[G_w]} \mathcal{L}_w \right).$$

To state the conjecture, we need the following invariants: $\mathcal{E}_{L/K} \in K_0(\mathbb{Z}[G], \mathbb{R})$ the equivariant global epsilon constant [5, section 3.1], $\delta_{L/K}(\mathcal{L}) \in K_0(\mathbb{Z}[G], \mathbb{R})$ the equivariant discriminant [5, section 3.2], and cohomological elements $I(v, \mathcal{L}) = I(v, \exp(\mathcal{L}_w)) \in K_0(\mathbb{Z}[G_w], \mathbb{Q})$ for each $v \in S$ [5, sections 3.3 and 4.1]. We will write $I(L_w/K_v, \mathcal{L}_w)$ for $I(v, \mathcal{L})$ to make clear that its definition depends only on the local extension and on \mathcal{L}_w . One knows that $\mathcal{E}_{L/K} - \delta_{L/K}(\mathcal{L}) \in K_0(\mathbb{Z}[G], \mathbb{Q})$. With these definitions, [5, Conjecture 4.1] is

Conjecture 2.1. *For any set S and lattice \mathcal{L} as above, one has*

$$\mathcal{E}_{L/K} - \delta_{L/K}(\mathcal{L}) = \sum_{v \in S} i_{G_w}^G(I(L_w/K_v, \mathcal{L}_w)) \in K_0(\mathbb{Z}[G], \mathbb{Q}).$$

This conjecture is independent of the choices of S and \mathcal{L} [5, Remark 4.2 (iii)] and will be denoted by $C(L/K)$. We also consider its l -components under the decomposition $K_0(\mathbb{Z}[G], \mathbb{Q}) \cong \bigoplus_l K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)$ and refer to the l -part of the conjecture as $C_l(L/K)$.

The conjecture expressed in local terms. Note that the left-hand side of Conjecture 2.1 contains essentially global objects. We now want to show that $C_l(L/K)$ has an equivalent version which only involves terms coming from the completions at primes above l . To do this we must introduce some notation related to local extensions. Let E/F be a Galois extension of l -adic fields with Galois group Γ . We denote by $\Sigma(E)$ the set of all embeddings $E \rightarrow \mathbb{Q}_l^c$, and we define a $\mathbb{Z}_l[\Gamma]$ -module $H_E := \bigoplus_{\sigma \in \Sigma(E)} \mathbb{Z}_l$ and a $\mathbb{Q}_l^c[\Gamma]$ -isomorphism $\rho_E : E \otimes_{\mathbb{Q}_l} \mathbb{Q}_l^c \rightarrow H_E \otimes_{\mathbb{Z}_l} \mathbb{Q}_l^c$, $e \otimes z \mapsto (\sigma(e)z)_{\sigma \in \Sigma(E)}$.

We write $\tau(\mathbb{Q}_l, \psi)$ for the local Galois Gauss sum of a character ψ of $\text{Gal}(\mathbb{Q}_l^c/\mathbb{Q}_l)$ (for the definition and basic properties of local Galois Gauss sums see [11, II. §4]). For a finite extension F of \mathbb{Q}_l the induction map from characters of $\text{Gal}(\mathbb{Q}_l^c/F)$ to characters of $\text{Gal}(\mathbb{Q}_l^c/\mathbb{Q}_l)$ is written as $i_F^{\mathbb{Q}_l}$. Finally, $\text{Irr}(\Gamma)$ denotes the set of irreducible characters of the finite group Γ . We define the equivariant local Galois Gauss sum of E/F by

$$\tau_{E/F} := (\tau(\mathbb{Q}_l, i_F^{\mathbb{Q}_l} \chi))_{\chi \in \text{Irr}(\Gamma)} \in \prod_{\chi \in \text{Irr}(\Gamma)} (\mathbb{Q}^c)^\times = \zeta(\mathbb{Q}^c[\Gamma])^\times.$$

From now on we fix an embedding $k : \mathbb{Q}^c \rightarrow \mathbb{Q}_l^c$. We also denote the induced map $\zeta(\mathbb{Q}^c[\Gamma])^\times \rightarrow \zeta(\mathbb{Q}_l^c[\Gamma])^\times$ by k . Using the formula for Galois action on Galois Gauss sums [11, II. Theorem 5.1], it is easy to see that $\hat{\delta}_{\mathbb{Z}_l[\Gamma], \mathbb{Q}_l^c}^1(k(\tau_{E/F}))$ is independent of the choice of k .

If \mathcal{L} is a full projective $\mathbb{Z}_l[\Gamma]$ -sublattice of \mathcal{O}_E which is contained in a sufficiently high power of the maximal ideal, we define

$$J(E/F) := -\hat{\delta}_{\mathbb{Z}_l[\Gamma], \mathbb{Q}_l^c}^1(k(\tau_{E/F})) + [\mathcal{L}, \rho_E, H_E] + I(E/F, \mathcal{L})_l \in K_0(\mathbb{Z}_l[\Gamma], \mathbb{Q}_l^c),$$

where $I(E/F, \mathcal{L})_l$ is the image of $I(E/F, \mathcal{L})$ under the map

$$K_0(\mathbb{Z}[\Gamma], \mathbb{Q}) \rightarrow K_0(\mathbb{Z}_l[\Gamma], \mathbb{Q}_l) \subseteq K_0(\mathbb{Z}_l[\Gamma], \mathbb{Q}_l^c).$$

The definition of $J(E/F)$ is independent of the choice of \mathcal{L} . This can be shown in the same way as the independence of \mathcal{L} for Conjecture 2.1.

Now consider again a global extension L/K and $G = \text{Gal}(L/K)$. We write \mathcal{O}_l^t for the valuation ring of the maximal tamely ramified extension of \mathbb{Q}_l in \mathbb{Q}_l^c and $\iota : K_0(\mathbb{Z}_l[G], \mathbb{Q}_l^c) \rightarrow K_0(\mathcal{O}_l^t[G], \mathbb{Q}_l^c)$ for the natural scalar extension map.

Theorem 2.2. $C_l(L/K)$ is valid if and only if one has

$$\sum_{v \in S_l(K)} \iota(i_{G_w}^G(J(L_w/K_v))) = 0$$

in $K_0(\mathcal{O}_l^t[G], \mathbb{Q}_l^c)$.

Proof. We use the notation and results of [5, section 7]. Write $\lambda_k : K_0(\mathbb{Z}[G], \mathbb{Q}^c) \rightarrow K_0(\mathbb{Z}_l[G], \mathbb{Q}_l^c)$ for the map induced by $\mathbb{Z}_l \otimes_{\mathbb{Z}} -$ and k . Note that $\lambda_k \circ \hat{\partial}_{\mathbb{Z}[G], \mathbb{Q}^c}^1 = \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1 \circ k$. In the proof of [5, Theorem 7.5] it is shown that $C_l(L/K)$ is equivalent to the equality

$$(2) \quad \iota \circ \lambda_k(\mathcal{E}_{L/K} - \delta_{L/K}(\mathcal{L})) = \sum_{v \in S} \iota \circ \lambda_k(i_{G_w}^G(I(L_w/K_v, \mathcal{L}_w)))$$

in $K_0(\mathcal{O}_l^t[G], \mathbb{Q}_l^c)$. Without loss of generality we can assume that $S_l(K) \subseteq S$.

By [5, equation (35)],

$$(3) \quad \lambda_k(\mathcal{E}_{L/K} - \delta_{L/K}(\mathcal{L})) = \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1(k(\tau_{L/K})) - \lambda_k([\mathcal{L}, \rho_L, H_L]).$$

Here $\tau_{L/K}$ is the equivariant global Galois Gauss sum defined in [5, equation (12)]. The definitions of H_L and ρ_L will be recalled below. Next we observe that for $\chi \in \text{Irr}(G)$, $\tau(\mathbb{Q}, i_K^{\mathbb{Q}}(\chi)) = \prod_p \prod_{v \in S_p(K)} \tau(\mathbb{Q}_p, i_{K_v}^{\mathbb{Q}_p}(\chi|_{G_w}))$, and thus the induction formula before [5, Proposition 7.3] implies that

$$(4) \quad \tau_{L/K} = \prod_{v \in S_f(K)} i_{G_w}^G(\tau_{L_w/K_v}).$$

Lemma 2.3. If $v \notin S_l(K)$, then one has

$$\iota \circ \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1 \circ k(i_{G_w}^G(\tau_{L_w/K_v})) = \iota \circ \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1(i_{G_w}^G(*(-f_w)))$$

in $K_0(\mathcal{O}_l^t[G], \mathbb{Q}_l^c)$ with $*(-f_w) \in \zeta(\mathbb{Q}_l^c[G_w])^\times$ as in [5, section 7].

Proof. Let p be the residue characteristic of v . We can factorize $i_{G_w}^G(\tau_{L_w/K_v})$ as

$$i_{G_w}^G(\tau_{L_w/K_v}) = \tau_{L/K, v} \cdot i_{\{e\}}^G(\tau_{K_v})$$

with $\tau_{L/K, v}$ as in [5, section 7], $\tau_{K_v} = \tau(\mathbb{Q}_p, i_{K_v}^{\mathbb{Q}_p}(1_{\Omega_{K_v}})) \in (\mathbb{Q}^c)^\times$ and $\{e\}$ denoting the trivial subgroup of G . By [5, Proposition 7.3] we need only show that

$$\iota \circ \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1 \circ k(i_{\{e\}}^G(\tau_{K_v})) = 0$$

in $K_0(\mathcal{O}_l^t[G], \mathbb{Q}_l^c)$. From the definition of the maps it follows directly that $\iota \circ \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1 \circ k \circ i_{\{e\}}^G = i_{\{e\}}^G \circ \hat{\partial}_{\mathcal{O}_l^t[\{e\}], \mathbb{Q}_l^c}^1 \circ k$; therefore it suffices to show $k(\tau_{K_v}) \in (\mathcal{O}_l^t)^\times$. The formula for the Galois action on local Galois Gauss sums (cf. [11, II. Theorem 5.1]) shows that $\tau_{K_v} \in \mathbb{Q}(\zeta_{p^\infty})$. Also, τ_{K_v} is only divisible by primes above p (this follows for example from [11, II. Proposition 4.1]) and thus $k(\tau_{K_v}) \in (\mathcal{O}_l^t)^\times$. \square

We continue with the proof of Theorem 2.2. By (3), (4) and Lemma 2.3 the left-hand side of (2) is equal to

$$(5) \quad \sum_{v \in S_l(K)} \iota \circ \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1 \circ k \circ i_{G_w}^G(\tau_{L_w/K_v}) + \sum_{v \notin S_l(K)} \iota \circ \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1 \circ i_{G_w}^G(*(-f_w)) - \iota \circ \lambda_k([\mathcal{L}, \rho_L, H_L]).$$

For $v \in S \setminus S_l(K)$, [5, Proposition 7.1] shows that

$$\lambda_k(i_{G_w}^G(I(L_w/K_v, \mathcal{L}_w))) = \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1 \circ i_{G_w}^G(*(-f_w)).$$

Combining this equality with [5, Lemma 4.5], we see that the right-hand side of (2) is equal to

$$(6) \quad \sum_{v \in S_l(K)} \iota \circ \lambda_k(i_{G_w}^G(I(L_w/K_v, \mathcal{L}_w))) + \sum_{v \notin S_l(K)} \iota \circ \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1 \circ i_{G_w}^G(*(-f_w)).$$

For $v \in S_l(K)$ there are identities $i_{G_w}^G \circ \hat{\partial}_{\mathbb{Z}_l[G_w], \mathbb{Q}_l^c}^1 \circ k = \hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1 \circ k \circ i_{G_w}^G$ and $i_{G_w}^G(I(L_w/K_v, \mathcal{L}_w)) = \lambda_k(i_{G_w}^G(I(L_w/K_v, \mathcal{L}_w)))$ which imply that

$$i_{G_w}^G(J(L_w/K_v)) = -\hat{\partial}_{\mathbb{Z}_l[G], \mathbb{Q}_l^c}^1 \circ k \circ i_{G_w}^G(\tau_{L_w/K_v}) + i_{G_w}^G([\mathcal{L}_w, \rho_{L_w}, H_{L_w}]) + \lambda_k(i_{G_w}^G(I(L_w/K_v, \mathcal{L}_w))).$$

We now use the following Lemma 2.4 to rewrite $\lambda_k([\mathcal{L}, \rho_L, H_L])$ in (5). It then immediately follows that the expressions (5) and (6) are equal if and only if one has

$$\sum_{v \in S_l(K)} \iota(i_{G_w}^G(J(L_w/K_v))) = 0.$$

This concludes the proof of the theorem. □

Lemma 2.4. *With the notation as above, one has an equality*

$$\lambda_k([\mathcal{L}, \rho_L, H_L]) = \sum_{v \in S_l(K)} i_{G_w}^G([\mathcal{L}_w, \rho_{L_w}, H_{L_w}])$$

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

Proof. We recall that $H_L = \bigoplus_{\Sigma(L)} \mathbb{Z}$ with $\Sigma(L)$ the set of all embeddings $L \rightarrow \mathbb{Q}^c$, and $\rho_L : L \otimes_{\mathbb{Q}} \mathbb{Q}^c \rightarrow H_L \otimes_{\mathbb{Z}} \mathbb{Q}^c$ is defined by $e \otimes z \mapsto (\sigma(e)z)_{\sigma \in \Sigma(L)}$.

There exists a commutative diagram of $\mathbb{Q}_l^c[G]$ -equivariant isomorphisms

$$\begin{array}{ccc} \bigoplus_{v \in S_l(K)} \mathbb{Q}_l^c[G] \otimes_{\mathbb{Q}_l^c[G_w]} (L_w \otimes_{\mathbb{Q}_l} \mathbb{Q}_l^c) & \xrightarrow{\cong} & \bigoplus_{v \in S_l(K)} \mathbb{Q}_l^c[G] \otimes_{\mathbb{Q}_l^c[G_w]} (H_{L_w} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l^c) \\ \downarrow \cong & & \downarrow \cong \\ (L \otimes_{\mathbb{Q}} \mathbb{Q}^c) \otimes_{\mathbb{Q}^c} \mathbb{Q}_l^c & \xrightarrow{\cong} & (H_L \otimes_{\mathbb{Z}} \mathbb{Q}^c) \otimes_{\mathbb{Q}^c} \mathbb{Q}_l^c. \end{array}$$

Here the upper horizontal map is $\bigoplus_{v \in S_l(K)} \mathbb{Q}_l^c[G] \otimes_{\mathbb{Q}_l^c[G_w]} \rho_{L_w}$ and the lower one is $\rho_L \otimes_{\mathbb{Q}^c} \mathbb{Q}_l^c$ via $k : \mathbb{Q}^c \rightarrow \mathbb{Q}_l^c$. The vertical maps are defined as follows. The left one

is the canonical isomorphism

$$\begin{aligned} \bigoplus_{v \in S_l(K)} \mathbb{Q}_l^c[G] \otimes_{\mathbb{Q}_l^c[G_w]} (L_w \otimes_{\mathbb{Q}_l} \mathbb{Q}_l^c) &\cong \bigoplus_{v \in S_l(K)} (\mathbb{Q}_l[G] \otimes_{\mathbb{Q}_l[G_w]} L_w) \otimes_{\mathbb{Q}_l} \mathbb{Q}_l^c \\ &\cong (L \otimes_{\mathbb{Q}} \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} \mathbb{Q}_l^c \\ &\cong (L \otimes_{\mathbb{Q}} \mathbb{Q}^c) \otimes_{\mathbb{Q}^c} \mathbb{Q}_l^c. \end{aligned}$$

To define the right vertical map, we first note that there is an isomorphism of $\mathbb{Z}_l[G]$ -lattices $\bigoplus_{v \in S_l(K)} (\mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l[G_w]} H_{L_w}) \cong H_L \otimes_{\mathbb{Z}} \mathbb{Z}_l$ which depends on the choice of k and is induced by the map $\Sigma(L_w) \rightarrow \Sigma(L)$ sending $\sigma : L_w \rightarrow \mathbb{Q}_l^c$ to $k^{-1} \circ \sigma \circ i_w : L \rightarrow \mathbb{Q}^c$ where $i_w : L \rightarrow L_w$ is the embedding corresponding to the place w . Using this isomorphism, the map on the right-hand side is

$$\begin{aligned} \bigoplus_{v \in S_l(K)} \mathbb{Q}_l^c[G] \otimes_{\mathbb{Q}_l^c[G_w]} (H_{L_w} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l^c) &\cong \bigoplus_{v \in S_l(K)} (\mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l[G_w]} H_{L_w}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l^c \\ &\cong (H_L \otimes_{\mathbb{Z}} \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l^c \\ &\cong (H_L \otimes_{\mathbb{Z}} \mathbb{Q}^c) \otimes_{\mathbb{Q}^c} \mathbb{Q}_l^c. \end{aligned}$$

By explicitly comparing definitions, one verifies that the diagram is commutative. Recall that by (1) we have an isomorphism of $\mathbb{Z}_l[G]$ -lattices $\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong \bigoplus_{v \in S_l(K)} (\mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l[G_w]} \mathcal{L}_w)$. Therefore

$$\begin{aligned} \lambda_k([\mathcal{L}, \rho_L, H_L]) &= [\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{Z}_l, \rho_L \otimes_{\mathbb{Q}_l^c} \mathbb{Q}_l^c, H_L \otimes_{\mathbb{Z}} \mathbb{Z}_l] \\ &= \sum_{v \in S_l(K)} [\mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l[G_w]} \mathcal{L}_w, \mathbb{Q}_l^c[G] \otimes_{\rho_{L_w}} \mathbb{Z}_l[G] \otimes_{\mathbb{Z}_l[G_w]} H_{L_w}] \\ &= \sum_{v \in S_l(K)} i_{G_w}^G([\mathcal{L}_w, \rho_{L_w}, H_{L_w}]). \quad \square \end{aligned}$$

A finiteness property of the conjecture. From Theorem 2.2 and a well-known finiteness property of p -adic fields we can now easily deduce the finiteness result Theorem 1.2.

Proof of Theorem 1.2. Fix a prime l . For each $v \in S_l(K)$ we let R_v be a set of representatives of isomorphism classes of Galois extensions E/K_v for which $\text{Gal}(E/K_v)$ is isomorphic to a subgroup of G . It is well known that R_v is finite (see e.g. [10, II. Proposition 14]).

Let L/K be a Galois extension with $\text{Gal}(L/K) \cong G$. If $v \in S_l(K)$ and $w \in S_v(L)$, then L_w is K_v -isomorphic to some $E_{L,v} \in R_v$. Fixing an isomorphism $\varphi : \text{Gal}(L/K) \rightarrow G$ and isomorphisms $L_w \cong E_{L,v}$ which induce $\varphi_w : \text{Gal}(L_w/K_v) \rightarrow \text{Gal}(E_{L,v}/K_v)$, we see that

$$(7) \quad \sum_{v \in S_l(K)} \iota(i_{\text{Gal}(L_w/K_v)}^{\text{Gal}(L/K)}(J(L_w/K_v))) = 0 \in K_0(\mathcal{O}_l^t[\text{Gal}(L/K)], \mathbb{Q}_l^c)$$

if and only if

$$(8) \quad \sum_{v \in S_l(K)} \iota(i_{\text{Gal}(E_{L,v}/K_v)}^G(J(E_{L,v}/K_v))) = 0 \in K_0(\mathcal{O}_l^t[G], \mathbb{Q}_l^c)$$

where the embedding $\text{Gal}(E_{L,v}/K_v) \rightarrow G$ is induced by φ , φ_w and the inclusion $\text{Gal}(L_w/K_v) \rightarrow \text{Gal}(L/K)$. Note that equality (7) is equivalent to the validity of $C_l(L/K)$ by Theorem 2.2.

Since there are only finitely many different extensions $E_{L,v} \in R_v$ and for each of these extensions only finitely many possible embeddings $\text{Gal}(E_{L,v}/K_v) \rightarrow G$, there are only finitely many different sums of the form (8). This shows that if $C_l(L/K)$ is true for a set of extensions L/K with $\text{Gal}(L/K) \cong G$ that contains enough extensions to obtain all sums in (8) that come from global extensions, then $C_l(L/K)$ is true for all extensions L/K with $\text{Gal}(L/K) \cong G$.

Hence there exist finitely many extensions L/K with $\text{Gal}(L/K) \cong G$ such that $C(L/K)$ for these extensions implies $C_l(L/K)$ for all extensions L/K with Galois group G and all $l \mid |G|$. This suffices, because for $l \nmid |G|$, $C_l(L/K)$ holds by [5, Corollary 7.6]. \square

3. RELATIVE K -GROUPS OF DIHEDRAL GROUP RINGS

For any finite group G we write $K_0(\mathbb{Z}[G], \mathbb{Q})_{\text{tors}}$ for the torsion subgroup of $K_0(\mathbb{Z}[G], \mathbb{Q})$. In this section we study this torsion subgroup in the case $G = D_n$, the dihedral group of order $2n$, with n odd. D_n has a unique cyclic subgroup of order n , which we denote by C_n . The main result of this section is

Theorem 3.1. *Let n be an odd integer. Then the restriction map on the torsion part of the relative K_0 -group*

$$\text{res} : K_0(\mathbb{Z}[D_n], \mathbb{Q})_{\text{tors}} \rightarrow K_0(\mathbb{Z}[C_n], \mathbb{Q})_{\text{tors}}$$

is injective.

Number theoretic applications. Theorem 3.1 can be applied to Conjecture 2.1 as follows. In [5, Corollary 6.3] it is shown that Conjecture 2.1 is true modulo the torsion subgroup of $K_0(\mathbb{Z}[G], \mathbb{Q})$. Combining the functorial properties of Conjecture 2.1 (cf. [5, Theorem 6.1]) with Theorem 3.1 therefore shows that if L/K is any extension with $\text{Gal}(L/K) \cong D_n$ and n odd, then $C(L/K)$ is equivalent to $C(L/L^{C_n})$, i.e. we have reduced the conjecture to a cyclic extension.

A second application is to Burns' $T\Omega(L/K, 0)$ -conjecture [6]. One can show that $T\Omega(L/K, 0) \in K_0(\mathbb{Z}[G], \mathbb{Q})_{\text{tors}}$ if and only if the strong Stark conjecture holds for the extension L/K [6, Theorem 2.2.4], and for dihedral extensions where this is known to be true, Theorem 3.1 again gives a reduction step to cyclic extensions. This also shows that Bley's algorithm in [2] can be used to obtain evidence for the $T\Omega(L/K, 0)$ -conjecture for certain dihedral extensions. This is particularly interesting since, at the moment, very little evidence exists for this conjecture in non-abelian extensions.

Outline of the proof. For any group G we have the natural isomorphism

$$K_0(\mathbb{Z}[G], \mathbb{Q}) \cong \bigoplus_p K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$$

and the restriction map respects this decomposition. Theorem 3.1 therefore follows from the next proposition.

Proposition 3.2. (1) *Let n be an odd integer. Then $K_0(\mathbb{Z}_2[D_n], \mathbb{Q}_2)_{\text{tors}} = 0$.*

(2) *Let n be an odd integer and p an odd prime number. Then*

$$\text{res} : K_0(\mathbb{Z}_p[D_n], \mathbb{Q}_p)_{\text{tors}} \rightarrow K_0(\mathbb{Z}_p[C_n], \mathbb{Q}_p)_{\text{tors}}$$

is injective.

The first part of this proposition is known (cf. [5, Lemma 8.2]), but for completeness we will include a proof. For any prime number p and any finite group G recall the following part of the exact localization sequence of K -theory

$$K_1(\mathbb{Z}_p[G]) \longrightarrow K_1(\mathbb{Q}_p[G]) \longrightarrow K_0(\mathbb{Z}_p[G], \mathbb{Q}_p) \longrightarrow 0.$$

The torsion part $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)_{\text{tors}}$ is the image of $K_1(\mathcal{M}_p)$ in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$, where \mathcal{M}_p is any maximal \mathbb{Z}_p -order in $\mathbb{Q}_p[G]$, i.e. we have an isomorphism

$$(9) \quad K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)_{\text{tors}} \cong \frac{\text{im}(K_1(\mathcal{M}_p) \rightarrow K_1(\mathbb{Q}_p[G]))}{\text{im}(K_1(\mathbb{Z}_p[G]) \rightarrow K_1(\mathbb{Q}_p[G]))}.$$

To compute these groups, we need an explicit description of the Wedderburn decomposition of $\mathbb{Q}_p[G]$. We then use the isomorphism $K_1(\mathbb{Q}_p[G]) \cong \zeta(\mathbb{Q}_p[G])^\times$ induced by the reduced norm and compute the image of $K_1(\mathcal{M}_p)$ in $\zeta(\mathbb{Q}_p[G])^\times$. The image of $K_1(\mathbb{Z}_p[G])$ is in general difficult to describe, but for the cyclic group C_n it can be done using congruences, and for the dihedral group we can give a characterization of $\mathbb{Z}_p[D_n]^\times$ inside $\mathbb{Q}_p[D_n]^\times$ which suffices for our purposes. We then compute the restriction map $\text{res} : K_1(\mathbb{Q}_p[D_n]) \rightarrow K_1(\mathbb{Q}_p[C_n])$ which induces the map $\text{res} : K_0(\mathbb{Z}_p[D_n], \mathbb{Q}_p)_{\text{tors}} \rightarrow K_0(\mathbb{Z}_p[C_n], \mathbb{Q}_p)_{\text{tors}}$ by (9).

Preliminaries. We introduce the following notation. For each positive integer n , we fix a primitive n -th root of unity ζ_n and set $\omega_n := \zeta_n + \zeta_n^{-1}$. Then $\mathbb{Q}(\zeta_n)$ has ring of integers $\mathbb{Z}[\zeta_n]$, and $\mathbb{Q}(\omega_n)$ is the maximal real subfield of $\mathbb{Q}(\zeta_n)$ and has ring of integers $\mathbb{Z}[\omega_n]$. For $n > 2$, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\omega_n)] = 2$ and $\{1, \zeta_n\}$ is a $\mathbb{Q}(\omega_n)$ -basis of $\mathbb{Q}(\zeta_n)$. We write $\mathbb{Q}_{p,n}$ for the \mathbb{Q}_p -algebra $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_n)$.

Lemma 3.3. *For every $i \in \mathbb{Z}$ there exist (uniquely determined) polynomials $f_i(x), g_i(x) \in \mathbb{Z}[x]$ such that*

$$\zeta_n^i = f_i(\omega_n) + g_i(\omega_n)\zeta_n \quad \text{for all } n \geq 1.$$

In fact, $f_0(x) = 1, g_0(x) = 0$ and $f_i(x) = -g_{i-1}(x), g_i(x) = f_{i-1}(x) + g_{i-1}(x)x$ for all $i \in \mathbb{Z}$.

Proof. This follows easily by induction on i , using $\zeta_n^2 - \omega_n\zeta_n + 1 = 0$. □

Recall the following part of representation theory (cf. [15, section 12.2]). Let G be a finite group and let V_i be the distinct irreducible representations of G over \mathbb{Q} . Hence $S_i := \text{End}_G(V_i)$ is a skew-field. Let $n_i := [V_i : S_i]$ and fix an S_i -basis of V_i . Then $\text{End}_{S_i}(V_i) \cong M_{n_i}(S_i^\circ)$, the ring of $n_i \times n_i$ -matrices with entries in the opposite ring of S_i . The maps $\rho_i : \mathbb{Q}[G] \rightarrow \text{End}_{S_i}(V_i) \cong M_{n_i}(S_i^\circ)$ induce an isomorphism $\mathbb{Q}[G] \cong \prod_i M_{n_i}(S_i^\circ)$. For $A_i \in M_{n_i}(S_i^\circ)$ we denote its trace as a \mathbb{Q} -endomorphism of V_i by $\chi_i(A_i)$. The inverse of the isomorphism $\mathbb{Q}[G] \rightarrow \prod_i M_{n_i}(S_i^\circ)$ is the map $(A_i)_i \mapsto \sum_{g \in G} b_g g$ with $b_g = \frac{1}{|G|} \sum_i n_i \chi_i(\rho_i(g^{-1})A_i)$. If S_i is commutative, then $S_i^\circ = S_i$ and for $A_i \in M_{n_i}(S_i)$, $\chi_i(A_i) = \text{Tr}_{S_i/\mathbb{Q}}(\text{Tr}(A_i))$ where $\text{Tr}_{S_i/\mathbb{Q}}$ is the trace of the field extension S_i/\mathbb{Q} and Tr is the trace of the matrix A_i .

Rational representations of cyclic groups. We first consider the cyclic group $C_n = \langle r : r^n = 1 \rangle$, where r is a fixed generator. For each divisor d of n , C_n acts \mathbb{Q} -linearly on $\mathbb{Q}(\zeta_d)$, r acting as multiplication by ζ_d . This representation is irreducible over \mathbb{Q} and $\text{End}_{C_n}(\mathbb{Q}(\zeta_d)) = \mathbb{Q}(\zeta_d)$. The corresponding map $\mathbb{Q}[C_n] \rightarrow \mathbb{Q}(\zeta_d)$ is the linear extension of $r^i \mapsto \zeta_d^i$. We obtain the following well-known result.

Lemma 3.4. *The map $r^i \mapsto (\zeta_d^i)_{d|n}$ extends to an isomorphism of \mathbb{Q} -algebras $\mathbb{Q}[C_n] \cong \prod_{d|n} \mathbb{Q}(\zeta_d)$. The inverse of this map is $(a_d)_{d|n} \mapsto \sum_{g \in C_n} b_g g$ with*

$$b_{r^i} = \frac{1}{n} \sum_{d|n} \text{Tr}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\zeta_d^{-i} a_d).$$

We will always use this isomorphism as an identification. The commutative \mathbb{Q} -algebra $\prod_{d|n} \mathbb{Q}(\zeta_d)$ contains $\mathcal{N} := \prod_{d|n} \mathbb{Z}[\zeta_d]$ as unique maximal \mathbb{Z} -order. To obtain a decomposition of $\mathbb{Q}_p[C_n]$, we simply apply $\mathbb{Q}_p \otimes_{\mathbb{Q}}$ to the isomorphism in Lemma 3.4; thus $\mathbb{Q}_p[C_n] \cong \prod_{d|n} \mathbb{Q}_{p,d}$. This is in general not the Wedderburn decomposition of $\mathbb{Q}_p[C_n]$ but it suffices for our purposes. Note that after tensoring with \mathbb{Q}_p the map $\text{Tr}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}} : \mathbb{Q}(\zeta_d) \rightarrow \mathbb{Q}$ becomes $\text{Tr}_{\mathbb{Q}_{p,d}/\mathbb{Q}_p} : \mathbb{Q}_{p,d} \rightarrow \mathbb{Q}_p$. The maximal \mathbb{Z}_p -order in $\mathbb{Q}_p[C_n]$ is $\mathcal{N}_p = \mathbb{Z}_p \otimes \mathcal{N}$. The next lemma is an immediate consequence of Lemma 3.4.

Lemma 3.5. *An element $(a_d)_{d|n} \in \prod_{d|n} \mathbb{Z}_p \otimes \mathbb{Z}[\zeta_d] = \mathcal{N}_p$ lies in $\mathbb{Z}_p[C_n]$ if and only if the congruences*

$$\sum_{d|n} \text{Tr}_{\mathbb{Q}_{p,d}/\mathbb{Q}_p}(\zeta_d^i a_d) \equiv 0 \pmod{n} \quad \text{for all } i \in \mathbb{Z}$$

hold in \mathbb{Z}_p .

Considering $1 \in \mathbb{Z}_p[C_n]$, we see that the relations of Lemma 3.5 hold with all $a_d = 1$. If $g(x) \in \mathbb{Z}[x]$ is any polynomial, then $g(\omega_d) = \tilde{g}(\zeta_d)$ with $\tilde{g}(x) = g(x + x^{-1}) \in \mathbb{Z}[x, x^{-1}]$. Thus

Corollary 3.6. *For every polynomial $g(x) \in \mathbb{Z}[x]$ the relation*

$$\sum_{d|n} \text{Tr}_{\mathbb{Q}_{p,d}/\mathbb{Q}_p}(g(\omega_d)) \equiv 0 \pmod{n}$$

holds in \mathbb{Z}_p .

From the above decomposition of $\mathbb{Q}_p[C_n]$ we derive the following description of the relevant K_1 -groups:

$$\begin{aligned} K_1(\mathbb{Q}_p[C_n]) &\cong \mathbb{Q}_p[C_n]^\times = \prod_{d|n} \mathbb{Q}_{p,d}^\times, \\ \text{im}(K_1(\mathcal{N}_p) \rightarrow K_1(\mathbb{Q}_p[C_n])) &\cong \mathcal{N}_p^\times = \prod_{d|n} (\mathbb{Z}_p \otimes \mathbb{Z}[\zeta_d])^\times, \\ \text{im}(K_1(\mathbb{Z}_p[C_n]) \rightarrow K_1(\mathbb{Q}_p[C_n])) &\cong \mathbb{Z}_p[C_n]^\times = \mathbb{Z}_p[C_n] \cap \mathcal{N}_p^\times. \end{aligned}$$

Rational representations of dihedral groups. Now we consider $D_n = \langle r, s : r^n = 1, s^2 = 1, srs = r^{-1} \rangle$, the dihedral group of order $2n$. Here it is important to assume that n is odd. More details on the rational representations of dihedral groups can be found in [8, (7.39)].

D_n has two 1-dimensional representations over \mathbb{Q} , $\sigma : \mathbb{Q}[D_n] \rightarrow \mathbb{Q}$ with $\sigma(r) = \sigma(s) = 1$ and $\tilde{\sigma} : \mathbb{Q}[D_n] \rightarrow \mathbb{Q}$ with $\tilde{\sigma}(r) = 1, \tilde{\sigma}(s) = -1$. The other irreducible representations over \mathbb{Q} are obtained as follows. Let $d > 2$ be a divisor of n . Then D_n acts on $\mathbb{Q}(\zeta_d)$, r acting as multiplication by ζ_d and s acting by complex conjugation. This representation is irreducible over \mathbb{Q} , $\text{End}_{D_n}(\mathbb{Q}(\zeta_d)) = \mathbb{Q}(\omega_d)$ and with respect

to the $\mathbb{Q}(\omega_d)$ -basis $\{1, \zeta_d\}$ we obtain the homomorphism $\rho_d : \mathbb{Q}[D_n] \rightarrow M_2(\mathbb{Q}(\omega_d))$ with

$$(10) \quad r^i \mapsto \begin{pmatrix} f_i(\omega_d) & f_{i+1}(\omega_d) \\ g_i(\omega_d) & g_{i+1}(\omega_d) \end{pmatrix}, \quad r^i s \mapsto \begin{pmatrix} f_i(\omega_d) & f_{i-1}(\omega_d) \\ g_i(\omega_d) & g_{i-1}(\omega_d) \end{pmatrix}, \quad \text{for all } i \in \mathbb{Z}.$$

Note that $2\text{Tr}_{\mathbb{Q}(\omega_d)/\mathbb{Q}}(x) = \text{Tr}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(x)$ for $d > 2$ and $x \in \mathbb{Q}(\omega_d)$. We obtain the following decomposition of $\mathbb{Q}[D_n]$.

Lemma 3.7. *Let n be an odd integer. Then the map $b \mapsto (\sigma(b), \tilde{\sigma}(b), (\rho_d(b))_{d|n, d>2})$ is an isomorphism of \mathbb{Q} -algebras $\mathbb{Q}[D_n] \cong \mathbb{Q} \times \mathbb{Q} \times \prod_{d|n, d>2} M_2(\mathbb{Q}(\omega_d))$. The inverse of this map is $(\alpha, \tilde{\alpha}, (A_d)_{d|n, d>2}) \mapsto \sum_{g \in D_n} b_g g$ with*

$$(11) \quad b_g = \frac{1}{2n} \left(\alpha + \tilde{\sigma}(g^{-1})\tilde{\alpha} + \sum_{d|n, d>2} \text{Tr}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\text{Tr}(\rho_d(g^{-1})A_d)) \right).$$

Again, we will always use this isomorphism as an identification. Define a map $\rho_1 : D_n \rightarrow M_2(\mathbb{Q}(\omega_1))$ by (10) with $d = 1$ and where in addition we restrict i to the range $0 \leq i \leq n - 1$. We remark that this map is not a homomorphism. If we set $A_1 = \begin{pmatrix} \alpha & \alpha - \tilde{\alpha} \\ 0 & \tilde{\alpha} \end{pmatrix}$, then one immediately verifies that $\alpha + \tilde{\sigma}(g^{-1})\tilde{\alpha} = \text{Tr}_{\mathbb{Q}(\zeta_1)/\mathbb{Q}}(\text{Tr}(\rho_1(g^{-1})A_1))$ for all $g \in D_n$; thus all summands in (11) can be written in a unified form. The \mathbb{Q} -algebra $\mathbb{Q} \times \mathbb{Q} \times \prod_{d|n, d>2} M_2(\mathbb{Q}(\omega_d))$ contains $\mathcal{M} := \mathbb{Z} \times \mathbb{Z} \times \prod_{d|n, d>2} M_2(\mathbb{Z}[\omega_d])$ as a maximal \mathbb{Z} -order and it is clear that $\mathbb{Z}[D_n]$ lies in this order. Applying $\mathbb{Q}_p \otimes_{\mathbb{Q}}$ to the isomorphism in Lemma 3.7 gives a decomposition of $\mathbb{Q}_p[D_n]$, and $\mathcal{M}_p = \mathbb{Z}_p \otimes \mathcal{M}$ is a maximal \mathbb{Z}_p -order in $\mathbb{Q}_p[D_n]$. The next lemma is an easy consequence of Lemma 3.7.

Lemma 3.8. *Let n be an odd integer. For $A = (\alpha, \tilde{\alpha}, (A_d)_{d|n, d>2}) \in \mathbb{Z}_p \times \mathbb{Z}_p \times \prod_{d|n, d>2} M_2(\mathbb{Z}_p \otimes \mathbb{Z}[\omega_d]) = \mathcal{M}_p$ write $A_1 = \begin{pmatrix} \alpha & \alpha - \tilde{\alpha} \\ 0 & \tilde{\alpha} \end{pmatrix}$. Then A belongs to $\mathbb{Z}_p[D_n]$ if and only if the congruences*

$$\sum_{d|n} \text{Tr}_{\mathbb{Q}_p, d/\mathbb{Q}_p}(\text{Tr}(\rho_d(g)A_d)) \equiv 0 \pmod{2n} \quad \text{for all } g \in D_n$$

hold in \mathbb{Z}_p .

From the above decomposition of $\mathbb{Q}_p[D_n]$ we derive the following description of the relevant K_1 -groups:

$$K_1(\mathbb{Q}_p[D_n]) \cong \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \times \prod_{d|n, d>2} (\mathbb{Q}_p \otimes \mathbb{Q}(\omega_d))^\times,$$

$$\text{im}(K_1(\mathcal{M}_p) \rightarrow K_1(\mathbb{Q}_p[D_n])) \cong \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times \times \prod_{d|n, d>2} (\mathbb{Z}_p \otimes \mathbb{Z}[\omega_d])^\times.$$

The restriction map for the K_1 -group. We now consider C_n as a subgroup of $D_n = \langle r, s : r^n = 1, s^2 = 1, srs = r^{-1} \rangle$ and take r to be the fixed generator of C_n .

Lemma 3.9. *Let n be an odd integer and p any prime number. Then the restriction map*

$$\begin{aligned} K_1(\mathbb{Q}_p[D_n]) &\cong \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \times \prod_{d|n, d>2} (\mathbb{Q}_p \otimes \mathbb{Q}(\omega_d))^\times \\ &\rightarrow K_1(\mathbb{Q}_p[C_n]) \cong \mathbb{Q}_p^\times \times \prod_{d|n, d>2} (\mathbb{Q}_p \otimes \mathbb{Q}(\zeta_d))^\times \end{aligned}$$

is given by $(\alpha, \tilde{\alpha}, (a_d)_{d|n, d>2}) \mapsto (\alpha \tilde{\alpha}, (a_d)_{d|n, d>2})$.

Proof. A preimage of $(\alpha, \tilde{\alpha}, (a_d)_{d|n, d>2})$ under the reduced norm is given by

$$\left(\alpha, \tilde{\alpha}, \left(\begin{matrix} a_d & 0 \\ 0 & 1 \end{matrix} \right)_{d|n, d>2} \right) \in \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \times \prod_{d|n, d>2} GL_2(\mathbb{Q}_p \otimes \mathbb{Q}(\omega_d)) = \mathbb{Q}_p[D_n]^\times.$$

Under the decomposition $\mathbb{Q}_p[C_n] \cong \mathbb{Q}_p \times \prod_{d|n, d>2} \mathbb{Q}_{p,d}$ and $\mathbb{Q}_p[D_n] \cong \mathbb{Q}_p \times \mathbb{Q}_p \times \prod_{d|n, d>2} M_2(\mathbb{Q}_p \otimes \mathbb{Q}(\omega_d))$ the embedding $\mathbb{Q}_p[C_n] \rightarrow \mathbb{Q}_p[D_n]$ is given by

$$\begin{aligned} (1, 0, \dots, 0) &\mapsto \left(1, 1, \left(\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \right)_{d|n, d>2} \right), \\ (0, \dots, 0, \zeta_d^i, 0, \dots, 0) &\mapsto \left(0, 0, \dots, \left(\begin{matrix} f_i(\omega_d) & f_{i+1}(\omega_d) \\ g_i(\omega_d) & g_{i+1}(\omega_d) \end{matrix} \right), \dots \right). \end{aligned}$$

We can therefore treat each component separately. With respect to the \mathbb{Q}_p -basis $(1, 0), (0, 1)$ of $\mathbb{Q}_p \times \mathbb{Q}_p$, $(\alpha, \tilde{\alpha})$ is mapped to the matrix $\begin{pmatrix} \alpha & 0 \\ 0 & \tilde{\alpha} \end{pmatrix} \in GL_2(\mathbb{Q}_p)$ which has reduced norm $\alpha \tilde{\alpha} \in \mathbb{Q}_p^\times$. With respect to the $\mathbb{Q}_p \otimes \mathbb{Q}(\zeta_d)$ -basis $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ of $M_2(\mathbb{Q}_p \otimes \mathbb{Q}(\omega_d))$, $\begin{pmatrix} a_d & 0 \\ 0 & 1 \end{pmatrix}$ is mapped to the same matrix considered as a matrix in $M_2(\mathbb{Q}_p \otimes \mathbb{Q}(\zeta_d))$ which has reduced norm $a_d \in (\mathbb{Q}_p \otimes \mathbb{Q}(\zeta_d))^\times$. \square

The restriction map for the relative K_0 -group. We now apply the preparations to obtain some results about the injectivity and surjectivity of the map $\text{res} : K_0(\mathbb{Z}_p[D_n], \mathbb{Q}_p)_{\text{tors}} \rightarrow K_0(\mathbb{Z}_p[C_n], \mathbb{Q}_p)_{\text{tors}}$.

Remark 3.10. Note that the map $\text{res} : K_0(\mathbb{Z}_p[D_n], \mathbb{Q}_p) \rightarrow K_0(\mathbb{Z}_p[C_n], \mathbb{Q}_p)$ is never injective. For odd n this follows easily from Lemma 3.9 and for even n it can be shown in a similar manner. Thus in Proposition 3.2 it is essential to restrict to the torsion subgroup.

Proof of Proposition 3.2. Part 1. Let $a \in \text{im}(K_1(\mathcal{M}_2) \rightarrow K_1(\mathbb{Q}_2[D_n]))$. We must show that $a \in \text{im}(K_1(\mathbb{Z}_2[D_n]) \rightarrow K_1(\mathbb{Q}_2[D_n]))$. Write $a = (\alpha, \tilde{\alpha}, (a_d)_{d|n, d>2}) \in \mathbb{Z}_2^\times \times \mathbb{Z}_2^\times \times \prod_{d|n, d>2} (\mathbb{Z}_2 \otimes \mathbb{Z}(\omega_d))^\times$ and let $A = (\alpha, \tilde{\alpha}, (A_d)_{d|n, d>2}) \in \mathbb{Z}_2^\times \times \mathbb{Z}_2^\times \times \prod_{d|n, d>2} GL_2(\mathbb{Z}_2 \otimes \mathbb{Z}(\omega_d)) = \mathcal{M}_2^\times$ be an element mapping to a under the reduced norm. Since $\alpha \equiv \tilde{\alpha} \equiv 1 \pmod{2}$, $\text{Tr}_{\mathbb{Q}_2, 1/\mathbb{Q}_2}(\text{Tr}(\rho_1(g)A_1)) = \alpha + \tilde{\sigma}(g)\tilde{\alpha} \equiv 0 \pmod{2}$, and for $d > 2$, $\text{Tr}_{\mathbb{Q}_2, d/\mathbb{Q}_2}(\text{Tr}(\rho_d(g)A_d)) = 2\text{Tr}_{\mathbb{Q}_2 \otimes \mathbb{Q}(\omega_d)/\mathbb{Q}_2}(\text{Tr}(\rho_d(g)A_d)) \equiv 0 \pmod{2}$. As n is invertible in \mathbb{Z}_2 , Lemma 3.8 shows $A \in \mathbb{Z}_2[D_n] \cap \mathcal{M}_2^\times = \mathbb{Z}_2[D_n]^\times$; hence a is in the image of $K_1(\mathbb{Z}_2[D_n])$.

Part 2. Let $a \in \text{im}(K_1(\mathcal{M}_p) \rightarrow K_1(\mathbb{Q}_p[D_n]))$ with $\text{res}(a) \in \text{im}(K_1(\mathbb{Z}_p[C_n]) \rightarrow K_1(\mathbb{Q}_p[C_n]))$. We must show that $a \in \text{im}(K_1(\mathbb{Z}_p[D_n]) \rightarrow K_1(\mathbb{Q}_p[D_n]))$. Write

$a = (\alpha, \tilde{\alpha}, (a_d)_{d|n, d>2}) \in \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times \times \prod_{d|n, d>2} (\mathbb{Z}_p \otimes \mathbb{Z}[\omega_d])^\times$. By Lemma 3.9, $\text{res}(a) = (a_1, (a_d)_{d|n, d>2})$ with $a_1 = \alpha\tilde{\alpha}$; thus by Lemma 3.5

$$(12) \quad \sum_{d|n} \text{Tr}_{\mathbb{Q}_p, d/\mathbb{Q}_p}(\zeta_d^i a_d) \equiv 0 \pmod n \quad \text{for all } i \in \mathbb{Z}.$$

Consider $A = (\alpha, \tilde{\alpha}, (A_d)_{d|n, d>2}) \in \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times \times \prod_{d|n, d>2} GL_2(\mathbb{Z}_p \otimes \mathbb{Z}[\omega_d]) = \mathcal{M}_p^\times$ with $A_d = \begin{pmatrix} a_d \tilde{\alpha}^{-1} & \alpha - \tilde{\alpha} \\ 0 & \tilde{\alpha} \end{pmatrix}$ for $d | n$. For $d = 1$ this agrees with the previous definition of A_1 . Clearly A maps to a under the reduced norm. It suffices to show that $A \in \mathbb{Z}_p[D_n]$. Thus we must check the relations of Lemma 3.8.

$$\begin{aligned} & \sum_{d|n} \text{Tr}_{\mathbb{Q}_p, d/\mathbb{Q}_p}(\text{Tr}(\rho_d(g)A_d)) \\ &= \sum_{d|n} \text{Tr}_{\mathbb{Q}_p, d/\mathbb{Q}_p} \left(\text{Tr} \left(\begin{pmatrix} f_i(\omega_d) & f_{i\pm 1}(\omega_d) \\ g_i(\omega_d) & g_{i\pm 1}(\omega_d) \end{pmatrix} \begin{pmatrix} a_d \tilde{\alpha}^{-1} & \alpha - \tilde{\alpha} \\ 0 & \tilde{\alpha} \end{pmatrix} \right) \right) \\ &= \tilde{\alpha}^{-1} \left(\sum_{d|n} \text{Tr}_{\mathbb{Q}_p, d/\mathbb{Q}_p}(f_i(\omega_d)a_d) \right) + \sum_{d|n} \text{Tr}_{\mathbb{Q}_p, d/\mathbb{Q}_p}(g_i(\omega_d)(\alpha - \tilde{\alpha}) + g_{i\pm 1}(\omega_d)\tilde{\alpha}) \\ &\equiv 0 \pmod n \end{aligned}$$

where for the last congruence we used (12) and Corollary 3.6. Since 2 is invertible in \mathbb{Z}_p , this proves the proposition. \square

Corollary 3.11. *For an odd prime p , $\text{res} : K_0(\mathbb{Z}[D_p], \mathbb{Q})_{\text{tors}} \rightarrow K_0(\mathbb{Z}[C_p], \mathbb{Q})_{\text{tors}}$ is an isomorphism, and $K_0(\mathbb{Z}[C_p], \mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/p\mathbb{Z})^\times$. In particular, $K_0(\mathbb{Z}[D_p], \mathbb{Q})_{\text{tors}}$ is non-trivial.*

Proof. The injectivity of the restriction map is Theorem 3.1. The surjectivity can be seen as follows. For $l \neq p$, $K_0(\mathbb{Z}_l[C_p], \mathbb{Q}_l)_{\text{tors}} = 0$; thus we must only prove the surjectivity of $\text{res} : K_0(\mathbb{Z}_p[D_p], \mathbb{Q}_p)_{\text{tors}} \rightarrow K_0(\mathbb{Z}_p[C_p], \mathbb{Q}_p)_{\text{tors}}$. By (9) and Lemma 3.9, this is equivalent to the equality

$$\mathbb{Z}_p^\times \times \mathbb{Z}_p[\zeta_p]^\times = (\mathbb{Z}_p^\times \times \mathbb{Z}_p[\omega_p]^\times)(\mathbb{Z}_p[C_p]^\times).$$

Suppose $(a_1, a_p) \in \mathbb{Z}_p^\times \times \mathbb{Z}_p[\zeta_p]^\times$. Then we can find $b_1 \in \mathbb{Z}_p^\times$ such that $b_1 \equiv a_p \pmod{(1 - \zeta_p)}$. Then $(a_1 b_1^{-1}, 1) \in \mathbb{Z}_p^\times \times \mathbb{Z}_p[\omega_p]^\times$ and the congruences $b_1 + \text{Tr}_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(\zeta_p^i a_p) \equiv b_1 + (p - 1)a_p \equiv 0 \pmod{(1 - \zeta_p)}$ for all $i \in \mathbb{Z}$ show that $(b_1, a_p) \in \mathbb{Z}_p[C_p]^\times$ by Lemma 3.5.

The isomorphism $K_0(\mathbb{Z}[C_p], \mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is well known. In our notation, it is given by $K_0(\mathbb{Z}_p[C_p], \mathbb{Q}_p)_{\text{tors}} \cong (\mathbb{Z}_p^\times \times \mathbb{Z}_p[\zeta_p]^\times)/\mathbb{Z}_p[C_p]^\times \rightarrow (\mathbb{Z}_p[\zeta_p]/(1 - \zeta_p))^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times$, $(a_1, a_p) \mapsto a_1 a_p^{-1} \pmod{(1 - \zeta_p)}$. \square

Remark 3.12. (1) In [9], Kim proved that $K_0(\mathbb{Z}[D_3], \mathbb{Q})_{\text{tors}}$ has order two. However, he did not compute the restriction map $\text{res} : K_0(\mathbb{Z}[D_3], \mathbb{Q})_{\text{tors}} \rightarrow K_0(\mathbb{Z}[C_3], \mathbb{Q})_{\text{tors}}$.

(2) If p is an odd prime, then $\text{res} : K_0(\mathbb{Z}_p[D_n], \mathbb{Q}_p)_{\text{tors}} \rightarrow K_0(\mathbb{Z}_p[C_n], \mathbb{Q}_p)_{\text{tors}}$ is injective for all n , not only for odd n . For even n this can be seen by essentially the same method, but when writing down matrices A_d as in the proof of Proposition 3.2, part 2, it is necessary to distinguish the cases $d | q$, $2 | d | 2q$ and $d \nmid 2q$, where q is the largest power of p dividing

- n . Note, however, that for even n the map $\text{res} : K_0(\mathbb{Z}_2[D_n], \mathbb{Q}_2)_{\text{tors}} \rightarrow K_0(\mathbb{Z}_2[C_n], \mathbb{Q}_2)_{\text{tors}}$ is in general not injective.
- (3) For any prime p and positive integer n , it can be shown that the restriction map $\text{res} : K_0(\mathbb{Z}_p[D_n], \mathbb{Q}_p)_{\text{tors}} \rightarrow K_0(\mathbb{Z}_p[C_n], \mathbb{Q}_p)_{\text{tors}}$ is surjective if and only if either $p \nmid n$, $n = p$ or $n = 2p$.

4. AN ALGORITHM FOR CERTAIN DIHEDRAL EXTENSIONS

Let p be an odd prime number and let D_p be the dihedral group of order $2p$. In this section we describe an algorithm which either proves Conjecture 2.1 for all D_p -extensions of \mathbb{Q} or finds a counterexample. We then discuss our implementation of this algorithm and apply it to prove Theorem 1.1.

Algorithm 4.1. *Given an odd prime number p , this algorithm either proves Conjecture 2.1 for all D_p -extensions of \mathbb{Q} or finds an extension L/K of number fields (not a dihedral extension) for which $C(L/K)$ is invalid.*

1. Classify the D_p -extensions of \mathbb{Q}_p . For each such extension E/\mathbb{Q}_p perform steps 2 and 3.
2. Let F be the quadratic subfield of E . Compute a quadratic number field K and a cyclic extension L/K of degree p (L need not be Galois over \mathbb{Q}) such that L and K have unique primes above p and the completion of L/K at these primes is E/F .
3. For the extension L/K computed in step 2 prove or disprove $C(L/K)$. If $C(L/K)$ is invalid, output L/K as a counterexample and terminate the algorithm.
4. (Here we have performed steps 2 and 3 for all extensions found in step 1 and in each case verified $C(L/K)$.) Output the message that $C(L/\mathbb{Q})$ is valid for all D_p -extensions L/\mathbb{Q} .

Theorem 4.2. *Algorithm 4.1 is correct, i.e. it either proves Conjecture 2.1 for all D_p -extensions of \mathbb{Q} or finds a counterexample.*

Proof. Assume that the algorithm did not find a counterexample L/K . We must show that Conjecture 2.1 holds for all D_p -extensions of \mathbb{Q} . Let L'/\mathbb{Q} be any D_p -extension. If the decomposition group of p has odd order (i.e. is either trivial or equal to C_p), then $C(L'/\mathbb{Q})$ holds by [5, Theorem 8.1 (ii)]. If the decomposition group of p has order two, then $C(L'/\mathbb{Q})$ is true by [5, Theorem 8.1 (i)]. Hence we can assume that L' has a unique prime above p and that the completion of L' at this prime is therefore itself a D_p -extension of \mathbb{Q}_p . Let K' be the quadratic subfield of L' . As explained at the beginning of section 3, Theorem 3.1 implies that $C(L'/\mathbb{Q})$ is equivalent to $C(L'/K')$. Furthermore, $C(L'/K')$ is equivalent to $C_p(L'/K')$ because for $l \neq p$, $K_0(\mathbb{Z}_l[\text{Gal}(L'/K')], \mathbb{Q}_l)_{\text{tors}} = 0$. The completion of L'/K' at the unique primes above p is one of the local extensions E/F found in step 1, and Theorem 2.2 shows that $C_p(L'/K')$ is equivalent to $\iota(J(E/F)) = 0$. Again by Theorem 2.2, $\iota(J(E/F)) = 0$ is equivalent to $C_p(L/K)$ where L/K is the extension constructed in step 2 and $C_p(L/K)$ was shown to be valid in step 3. \square

We now describe each step of the algorithm in more detail.

Step 1. The first step is the classification of all D_p -extensions of \mathbb{Q}_p . By a result of Fröhlich (cf. [11, Exercise 7]) this can be done as follows.

If F/\mathbb{Q}_p is a quadratic extension and E/F a cyclic extension of degree p with $N_{E/F}(E^\times)$ invariant under $\text{Gal}(F/\mathbb{Q}_p)$ and $\mathbb{Q}_p^\times \subseteq N_{E/F}(E^\times)$, then E/\mathbb{Q}_p is Galois with $\text{Gal}(E/\mathbb{Q}_p) \cong D_p$. Conversely every D_p -extension of \mathbb{Q}_p arises in this way.

For any local field F we write \mathfrak{p}_F for the maximal ideal and $U_F^{(i)} = 1 + \mathfrak{p}_F^i$ for the i -th principal units ($i > 0$). Let μ_i denote the group of i -th roots of unity. As $\mathbb{Q}_p^\times = p^\mathbb{Z} \times \mu_{p-1} \times U_{\mathbb{Q}_p}^{(1)}$ and $U_{\mathbb{Q}_p}^{(1)} \cong \mathbb{Z}_p$, \mathbb{Q}_p^\times has three subgroups of index 2. The three corresponding quadratic extensions are the unramified quadratic extension, the quadratic extension contained in $\mathbb{Q}_p(\zeta_p)$ and a ramified quadratic extension not contained in $\mathbb{Q}_p(\zeta_p)$.

Proposition 4.3. *Let p be an odd prime. The number of D_p -extensions of \mathbb{Q}_p containing the quadratic field F is as follows.*

- (1) *If F is the unramified quadratic extension, then there is a unique D_p -extension (of conductor \mathfrak{p}_F^2 over F).*
- (2) *If F is the quadratic extension contained in $\mathbb{Q}_p(\zeta_p)$, then for $p = 3$ there are four non-isomorphic D_p -extensions (one of conductor \mathfrak{p}_F^2 over F and three of conductor \mathfrak{p}_F^4), and for $p \geq 5$ there is a unique D_p -extension (of conductor \mathfrak{p}_F^2 over F).*
- (3) *If F is the ramified quadratic extension not contained in $\mathbb{Q}_p(\zeta_p)$, then there is a unique D_p -extension (of conductor \mathfrak{p}_F^2 over F).*

Proof. We must find all subgroups $M \subseteq F^\times$ of index p that contain \mathbb{Q}_p^\times and that are invariant under $\text{Gal}(F/\mathbb{Q}_p)$. In particular, $(F^\times)^p \mathbb{Q}_p^\times \subseteq M$.

Case 1: Here $F^\times = p^\mathbb{Z} \times \mu_{p^2-1} \times U_F^{(1)}$ and $\mathbb{Q}_p^\times = p^\mathbb{Z} \times \mu_{p-1} \times U_{\mathbb{Q}_p}^{(1)}$ under this decomposition. We have $(U_F^{(1)})^p = U_F^{(2)}$; thus $(F^\times)^p = p^{p\mathbb{Z}} \times \mu_{p^2-1} \times U_F^{(2)}$ and therefore $F^\times / ((F^\times)^p \mathbb{Q}_p^\times) \cong U_F^{(1)} / (U_F^{(2)} U_{\mathbb{Q}_p}^{(1)})$. One easily sees that this quotient has order p ; hence $M = (F^\times)^p \mathbb{Q}_p^\times$ is the unique subgroup of the type we want.

Case 2: Here $F = \mathbb{Q}_p(\pi)$ with $\pi = \sqrt{-p}$ and π is a prime of F . For $p = 3$, $F^\times = \pi^\mathbb{Z} \times \mu_2 \times \mu_3 \times U_F^{(2)}$ and $\mathbb{Q}_p^\times = \pi^{2\mathbb{Z}} \times \mu_2 \times \{1\} \times U_{\mathbb{Q}_p}^{(1)}$ under this decomposition. We have $(U_F^{(2)})^3 = U_F^{(4)}$; thus $(F^\times)^3 = \pi^{3\mathbb{Z}} \times \mu_2 \times \{1\} \times U_F^{(4)}$. Therefore $F^\times / ((F^\times)^3 \mathbb{Q}_3^\times) \cong \mu_3 \times U_F^{(2)} / (U_F^{(4)} U_{\mathbb{Q}_3}^{(1)})$ which is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Hence there are four subgroups of the type we want (invariance under $\text{Gal}(F/\mathbb{Q}_p)$ is easily checked). For $p \geq 5$, $F^\times = \pi^\mathbb{Z} \times \mu_{p-1} \times U_F^{(1)}$ and $\mathbb{Q}_p^\times = \pi^{2\mathbb{Z}} \times \mu_{p-1} \times U_{\mathbb{Q}_p}^{(1)}$ under this decomposition. We have $(U_F^{(1)})^p = U_F^{(3)}$; thus $(F^\times)^p = \pi^{p\mathbb{Z}} \times \mu_{p-1} \times U_F^{(3)}$. As $U_F^{(3)} U_{\mathbb{Q}_p}^{(1)} = U_F^{(2)}$, $F^\times / ((F^\times)^p \mathbb{Q}_p^\times) \cong U_F^{(1)} / U_F^{(2)}$ which has order p . Hence there exists a unique subgroup M of the type we want.

Case 3: Here $F = \mathbb{Q}_p(\pi)$ with $\pi = \sqrt{-p\zeta_{p-1}}$ and π is a prime of F . Also $F^\times = \pi^\mathbb{Z} \times \mu_{p-1} \times U_F^{(1)}$ and we have $(U_F^{(1)})^p = U_F^{(3)}$. We can now proceed as in the $p \geq 5$ part of case 2. \square

We will see that Proposition 4.3 contains all necessary information about D_p -extensions of \mathbb{Q}_p . Therefore step 1 does not require any further computations.

Step 2. Let E/\mathbb{Q}_p be a D_p -extension and let F be the quadratic subfield. We consider the question of how to find a quadratic number field K and a cyclic extension L/K of degree p with completion E/F . Let K be any quadratic number field with a unique prime \mathfrak{p} above p and for which $K_{\mathfrak{p}} = F$ (it is easy to see that such a field

K can be found algorithmically). The Grunwald-Wang theorem (cf. [1, Theorem 5, p. 103]) guarantees the existence of an extension L/K with the properties we want. Let \mathfrak{m} be the conductor of such an extension. The \mathfrak{p} -part of \mathfrak{m} is determined by the local extension E/F and is therefore known by Proposition 4.3. Any other prime appears in \mathfrak{m} with exponent at most one. Thus by enumerating all cyclic extensions of degree p of K which satisfy this restriction on the conductor, we will come across an extension of the form we want and we need a method to recognize it. To test whether a cyclic extension L/K given by a subgroup H of the ray class group $Cl_{\mathfrak{m}}$ has the correct completion at \mathfrak{p} , we use the well-known commutative diagram from class-field theory [12, VI. Satz (5.6)]:

$$\begin{array}{ccc} K_{\mathfrak{p}}^{\times} & \xrightarrow{\varphi} & \text{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}}) \\ \downarrow & & \downarrow \cong \\ Cl_{\mathfrak{m}} & \longrightarrow & \text{Gal}(L/K) . \end{array}$$

Here the upper map φ is the local Artin map and the lower map is the global Artin map with kernel H . The left-hand map is given by the inclusion of $K_{\mathfrak{p}}^{\times}$ into the idele class group, followed by the map from the idele class group to the ray class group [12, VI. Theorem (7.1)]. The right-hand map is an isomorphism because \mathfrak{p} is totally ramified. $L_{\mathfrak{p}}/\mathbb{Q}_p$ is dihedral if and only if $\mathbb{Q}_p^{\times} \subseteq \ker(\varphi)$, because the proof of Proposition 4.3 shows that $\ker(\varphi)$ is then automatically invariant under $\text{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$. Also \mathbb{Q}_p^{\times} is topologically generated by p , ζ_{p-1} and $1+p$ and ζ_{p-1} is obviously in the kernel of φ . Thus we must only check that p and $1+p$ are in the kernel of φ ; i.e. their image in $Cl_{\mathfrak{m}}$ lies in the subgroup H . This can easily be done on a computer. In the case $p=3$ and $F=\mathbb{Q}_3(\zeta_3)$ we must also check which of the four possible dihedral extensions we get. This can be done by testing an additional element which generates the corresponding norm group; for further details on this case see the proof of Theorem 1.1 below.

Step 3. The third step in Algorithm 4.1 is the proof of $C(L/K)$ for the cyclic extension constructed above. For this one can use the algorithm developed by Bley in [3]. This algorithm, which is based on the abelian version of Conjecture 2.1 described in [4], can be applied to certain abelian extensions L/K , including cyclic extensions. For such an extension it then proves or disproves the conjecture.

Implementation. We have not implemented step 2 of the algorithm which finds the global cyclic extensions L/K , because for $p=3$ one easily finds suitable extensions without using the enumeration of all cyclic extensions described above (see the proof of Theorem 1.1 below). A limited version of Bley's algorithm was implemented by Kusnezow in PARI/GP: It only works for cyclic extensions of odd prime degree of real quadratic fields with class number one, and it only gives numerical evidence and not a proof for the conjecture. We will see that the restrictions on the extension are not a problem for $p=3$ (for $p \geq 5$ compare Remark 4.5), but of course numerical evidence is not sufficient. Bley remarked in his paper [3] that, in principle, the conjecture can be proved on a computer, because the computation of Galois Gauss sums and norm resolvents (which a priori are complex numbers) can be done in a large enough number field. However, this turns out to be extremely slow so that in general the computations cannot be done in reasonable time. But if we start with a cyclic extension L/K of odd prime degree such that L/\mathbb{Q} is dihedral,

then the situation is much simpler. To show this, we must first recall the following notation of Bley’s paper. Suppose L/K is an abelian extension with Galois group G . Let \hat{G} be the group of linear characters of G , $e_\chi \in \mathbb{Q}^c[G]$ the idempotent corresponding to $\chi \in \hat{G}$ and $\mathcal{N}_{K/\mathbb{Q}}(\theta) := \prod_{\tau \in \Sigma(K)} \sum_{g \in G} \hat{\tau}g(\theta)g^{-1} \in \mathbb{Q}^c[G]$ the norm resolvent with $\hat{\tau}$ an extension of τ to L and θ a normal basis generator of L/K . We write $Nf(\chi)$ for the norm of the conductor of $\chi \in \hat{G}$.

Lemma 4.4. *Let L/\mathbb{Q} be a D_n -extension with n odd, K the quadratic subfield and $G = \text{Gal}(L/K)$. Then*

- (1) $\sum_{\chi \in \hat{G}} \tau(K, \chi)e_\chi \in \mathbb{Q}[G]^\times$ and $\mathcal{N}_{K/\mathbb{Q}}(\theta) \in \mathbb{Q}[G]^\times$.
- (2) For every $\chi \in \hat{G}$, $\tau(K, \chi) = \sqrt{Nf(\chi)}$ and this number is a rational integer.

Proof. Our assumption L/\mathbb{Q} dihedral implies that the transfer map $\text{Gal}(L/\mathbb{Q})^{\text{ab}} \rightarrow \text{Gal}(L/K)$ is trivial. Therefore the Galois action formula [11, II. Theorem 7.2] shows that

$$(13) \quad \sigma(\tau(K, \chi)) = \tau(K, \sigma \circ \chi)$$

for all $\sigma \in \Omega_{\mathbb{Q}}$ and $\chi \in \hat{G}$.

- (1) By the definition of e_χ ,

$$\sum_{\chi \in \hat{G}} \tau(K, \chi)e_\chi = \frac{1}{|G|} \sum_{g \in G} \left(\sum_{\chi \in \hat{G}} \chi(g)\tau(K, \chi) \right) g^{-1}.$$

Equation (13) immediately implies that $\sum_{\chi \in \hat{G}} \chi(g)\tau(K, \chi) \in \mathbb{Q}$ for every $g \in G$; therefore $\sum_{\chi \in \hat{G}} \tau(K, \chi)e_\chi \in \mathbb{Q}[G]$. The same argument applied to $\tau(K, \chi)^{-1}$ instead of $\tau(K, \chi)$ shows that $\sum_{\chi \in \hat{G}} \tau(K, \chi)e_\chi$ is invertible in $\mathbb{Q}[G]$. By [3, section 3.7], $\left(\sum_{\chi \in \hat{G}} \tau(K, \chi)e_\chi\right)^{-1} \mathcal{N}_{K/\mathbb{Q}}(\theta) \in \mathbb{Q}[G]^\times$; therefore $\mathcal{N}_{K/\mathbb{Q}}(\theta) \in \mathbb{Q}[G]^\times$.

(2) By [11, II. Definition 7.2], $\tau(K, \chi) = \sqrt{Nf(\chi)}W(\bar{\chi})W_\infty(\chi)^{-1}$. One easily sees that $W_\infty(\chi)$, the infinite part of the root number, is equal to 1 in this case. The Artin root number is inductive; thus $W(\bar{\chi}) = W(i_K^{\mathbb{Q}}(\bar{\chi}))$. Now, $i_K^{\mathbb{Q}}(\bar{\chi})$ is an orthogonal character and therefore its root number is 1 [17, Corollary 1, p. 124]. To see that $\tau(K, \chi) = \sqrt{Nf(\chi)}$ is rational, we again apply equation (13) and observe that $f(\sigma \circ \chi) = f(\chi)$ for all $\sigma \in \Omega_{\mathbb{Q}}$ and $\chi \in \hat{G}$. □

In the situation of Lemma 4.4 it is therefore not necessary to generate a number field which contains both Galois Gauss sums and the norm resolvent. This observation simplifies the implementation of the algorithm and makes the computations significantly faster. We applied this result in our modification of the existing implementation of Bley’s algorithm (written in PARI/GP). Thus our modified implementation works only for a very restricted class of extensions L/K , namely L/K cyclic of odd prime degree, K real quadratic of class number one, L/\mathbb{Q} dihedral, but for such an extension it really either proves or disproves the conjecture. The implementation and a computer readable form of the field extensions used in the following proof are available at <http://www.mth.kcl.ac.uk/~breuning/>.

Computations. We now show that our restricted implementation of Algorithm 4.1 suffices to prove Theorem 1.1. Afterwards we discuss the difficulties which appear for prime numbers greater than 3.

Proof of Theorem 1.1. By Proposition 4.3 there are six D_3 -extensions of \mathbb{Q}_3 and we must first find global realizations of these extensions. All the computations were done with PARI/GP, Version 2.1.4 (cf. [13]).

Let $K = \mathbb{Q}(\sqrt{2})$. Then the completion of K at the unique prime \mathfrak{p} above 3 is the unramified quadratic extension of \mathbb{Q}_3 . Let $\mathfrak{m} = \mathfrak{p}^2(5) = (45)$. Then $Cl_{\mathfrak{m}} \cong \mathbb{Z}/12 \times \mathbb{Z}/3$ with generators $g_1 = (7\sqrt{2}-24)$ and $g_2 = (14)$ for the cyclic components. The extension corresponding to the subgroup $H = \langle g_1^3, g_2 \rangle$ has the properties we want.

Let $K = \mathbb{Q}(\sqrt{6})$. Then the completion of K at the unique prime \mathfrak{p} above 3 is the field $\mathbb{Q}_3(\zeta_3)$. The proof of Proposition 4.3 shows that the four non-isomorphic cyclic extensions E of $K_{\mathfrak{p}}$ of degree 3 which are dihedral over \mathbb{Q}_3 can be distinguished by checking which subgroup of $U_{K_{\mathfrak{p}}}^{(1)}/(U_{K_{\mathfrak{p}}}^{(4)}U_{\mathbb{Q}_3}^{(1)})$ lies in the kernel of the local Artin map ($U_{K_{\mathfrak{p}}}^{(4)}U_{\mathbb{Q}_3}^{(1)}$ is automatically contained in the kernel for these extensions). One easily checks that the four subgroups of order 3 are generated by $1 + \sqrt{6}$, $1 + 2\sqrt{6}$, $1 + 3\sqrt{6}$ and $1 + 4\sqrt{6}$.

If $\mathfrak{m} = \mathfrak{p}^2(11) = (33)$, then $Cl_{\mathfrak{m}}$ has a unique subgroup H of index 3 with conductor \mathfrak{m} , and the corresponding extension is the dihedral extension with $1 + 3\sqrt{6}$ in the local norm group.

If $\mathfrak{m} = \mathfrak{p}^4 = (9)$, then $Cl_{\mathfrak{m}} \cong \mathbb{Z}/3 \times \mathbb{Z}/3$ with generators $g_1 = (3\sqrt{6} + 1)$ and $g_2 = (2)$. The subgroup $H = \langle g_1^3, g_2 \rangle$ corresponds to the dihedral extension with $1 + 4\sqrt{6}$ in the local norm group.

If $\mathfrak{m} = \mathfrak{p}^4(11) = (99)$, then $Cl_{\mathfrak{m}} \cong \mathbb{Z}/60 \times \mathbb{Z}/3 \times \mathbb{Z}/3$ with generators $g_1 = (45\sqrt{6} + 1)$, $g_2 = (-33\sqrt{6} + 1)$ and $g_3 = (43)$. For the subgroup $H = \langle g_1^3, g_1^2g_2, g_3 \rangle$ we obtain the extension corresponding to $1 + \sqrt{6}$, and for $H = \langle g_1^3, g_1g_2, g_3 \rangle$ we obtain the extension corresponding to $1 + 2\sqrt{6}$.

Let $K = \mathbb{Q}(\sqrt{3})$. Then the completion of K at the unique prime \mathfrak{p} above 3 is the ramified quadratic extension of \mathbb{Q}_3 not contained in $\mathbb{Q}_3(\zeta_3)$. If $\mathfrak{m} = \mathfrak{p}^2(5) = (15)$, then $Cl_{\mathfrak{m}}$ has a unique subgroup H of index 3 with conductor \mathfrak{m} which gives the field we want.

In all 6 cases, the global extension L/\mathbb{Q} is dihedral; therefore it was possible to apply our implementation of the algorithm, and in all 6 cases the conjecture was validated. This concludes the proof of Theorem 1.1. \square

Remark 4.5. We conclude this paper with some remarks on the case $p \geq 5$. In theory, Algorithm 4.1 can prove Conjecture 2.1 for all D_p -extensions of \mathbb{Q} . However, at the moment two problems arise when one tries to use the existing implementation of step 3 of the algorithm for primes greater than 3.

First, in our implementation the restrictions on the extension are too strict. For example, there is no real quadratic field K of class number one with a unique prime above 5 such that its completion is the ramified quadratic extension not contained in $\mathbb{Q}_5(\zeta_5)$ (i.e. case 3 in Proposition 4.3). In fact, by using results from the theory of genera and its refinements (cf. [14, (2.1) and (2.29)]), one easily shows that $\mathbb{Q}(\sqrt{5})$ is the only real quadratic field in which 5 ramifies and the class number is odd.

The second problem is that even in those cases where one can find a global extension which satisfies all conditions necessary for the existing implementation, the computations are often extremely slow. The most time-consuming steps are the computational class field theory which is used to find a defining polynomial for the ray class field and the computation of the Fitting ideal in Bley's algorithm.

REFERENCES

- [1] E. Artin, J. Tate, *Class field theory*, W.A. Benjamin, Inc., New York-Amsterdam, 1968. MR **36**:6383
- [2] W. Bley, *Computation of Stark-Tamagawa units*, Math. Comp. **72** (2003), 1963–1974.
- [3] W. Bley, *Numerical evidence for a conjectural generalization of Hilbert’s Theorem 132*, LMS J. Comput. Math. **6** (2003), 68–88 (electronic).
- [4] W. Bley, D. Burns, *Étale cohomology and a generalisation of Hilbert’s Theorem 132*, Math. Z. **239** (2002), no. 1, 1–25. MR **2002j**:11135
- [5] W. Bley, D. Burns, *Equivariant epsilon constants, discriminants and étale cohomology*, preprint 2001, to appear in Proc. London Math. Soc.
- [6] D. Burns, *Equivariant Tamagawa numbers and Galois module theory I*, Compositio Math. **129** (2001), no. 2, 203–237. MR **2002g**:11152
- [7] D. Burns, M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients*, Doc. Math. **6** (2001), 501–570. MR **2002m**:11055
- [8] C. W. Curtis, I. Reiner, *Methods of representation theory. Vol. I*, John Wiley & Sons, Inc, New York, 1981. MR **82i**:20001
- [9] S. Y. Kim, *On the Equivariant Tamagawa Number Conjecture for Quaternion fields*, thesis, King’s College London (2002).
- [10] S. Lang, *Algebraic number theory*, Second Edition, Graduate Texts in Mathematics 110, Springer-Verlag, New York, 1994. MR **95f**:11085
- [11] J. Martinet, *Character theory and Artin L-functions*, in: *Algebraic number fields* (ed. A. Fröhlich), pp. 1–87, Academic Press, London, 1977. MR **56**:5502
- [12] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 1992.
- [13] The Pari Group, PARI/GP, Version 2.1.4, 2000 Bordeaux, available from <http://www.parigp-home.de/>.
- [14] D. Pumplün, *Über die Klassenzahl und die Grundeinheit des reellquadratischen Zahlkörpers*, J. Reine Angew. Math. **230** (1968), 167–210. MR **37**:189
- [15] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics 42, Springer-Verlag, New York-Heidelberg, 1977. MR **56**:8675
- [16] V. Snaith, *Burns’ equivariant Tamagawa invariant $T\Omega^{loc}(N/\mathbb{Q}, 1)$ for some quaternion fields*, to appear in J. London Math. Soc.
- [17] J. T. Tate, *Local constants*, in: *Algebraic number fields* (ed. A. Fröhlich), pp. 89–131, Academic Press, London, 1977. MR **56**:15613

DEPARTMENT OF MATHEMATICS, KING’S COLLEGE LONDON, STRAND, LONDON WC2R 2LS,
UNITED KINGDOM

E-mail address: breuning@mth.kcl.ac.uk