ALGORITHMIC PROOF OF THE EPSILON CONSTANT CONJECTURE

WERNER BLEY AND RUBEN DEBEERST

ABSTRACT. In this paper we will algorithmically prove the global epsilon constant conjecture for all Galois extensions $L/\mathbb{Q}$ of degree at most 15. In fact, we will obtain a slightly more general result whose proof is based on an algorithmic proof of the local epsilon constant conjecture for Galois extensions $E/\mathbb{Q}_p$ of small degree. To this end we will present an efficient algorithm for the computation of local fundamental classes and address several other problems arising in the algorithmic proof of the local conjecture.

1. INTRODUCTION

For a tamely ramified Galois extension L/K of number fields with Galois group G, the ring of integers $\mathcal{O}_L$ has been studied as a projective $\mathbb{Z}[G]$-module. Cassou-Noguès and Fröhlich defined a root number class $W_{L/K}$ associated to the epsilon constants occuring in the functional equation of Artin L-functions, and it was conjectured by Fröhlich and proved by Taylor in 1981 that this class is equal to the class of $\mathcal{O}_L$ in the reduced projective class group $\mathrm{Cl}(\mathbb{Z}[G])$, see [19, 35].

In 1985 Chinburg defined an element $\Omega(L/K, 2)$ in $\mathrm{Cl}(\mathbb{Z}[G])$ for arbitrary Galois extensions L/K with $\mathrm{Gal}(L/K) = G$ using cohomological methods and proved that it matches the class of $\mathcal{O}_L$ for tamely ramified extensions. His $\Omega(2)$-conjecture, stating the equality of $\Omega(L/K, 2)$ and $W_{L/K}$ in $\mathrm{Cl}(\mathbb{Z}[G])$, therefore generalizes Fröhlich's conjecture to wildly ramified extensions, cf. [15].

Later, Burns and the first named author formulated in [4] a conjectural description of epsilon constants in the relative algebraic K-group $K_0(\mathbb{Z}[G], \mathbb{R})$, which implies Chinburg's $\Omega(2)$-conjecture via the canonical surjection $K_0(\mathbb{Z}[G], \mathbb{R}) \twoheadrightarrow \mathrm{Cl}(\mathbb{Z}[G])$. More precisely, they define an equivariant epsilon constant $\mathscr{E}_{L/K}$ in $K_0(\mathbb{Z}[G], \mathbb{R})$ and an element involving algebraic invariants, which project to the root number class and to $\Omega(L/K, 2)$, respectively. If we denote the difference of $\mathscr{E}_{L/K}$ and the algebraic invariant by $T\Omega^{\mathrm{loc}}(L/K, 1)$, then the global epsilon constant conjecture predicts the vanishing of $T\Omega^{\mathrm{loc}}(L/K, 1)$ in $K_0(\mathbb{Z}[G], \mathbb{R})$. Burns and the first named author proved their conjecture for tamely ramified extensions and for abelian extensions of $\mathbb{Q}$ with odd conductor. They also proved that $T\Omega^{\mathrm{loc}}(L/K, 1)$ is an element of the torsion subgroup $K_0(\mathbb{Z}[G], \mathbb{Q})_{\mathrm{tor}}$ of $K_0(\mathbb{Z}[G], \mathbb{R})$, see [4, Cor. 6.3]. The results of Breuning and Burns in [11] imply that the conjecture is true for all abelian extensions of $\mathbb{Q}$.

The global epsilon constant conjecture fits into the more general framework of the equivariant Tamagawa number conjecture (ETNC) formulated by Burns and Flach in [13]. ETNC conjecturally describes the leading term of an equivariant motivic L-function at integer arguments by cohomological invariants. In the number field case, the global epsilon constant conjecture of [4] is in fact motivated by the conjectured compatibility of the ETNC for the leading terms of Artin L-functions at $s = 0$ and $s = 1$ with the functional equation. In [10] Burns and Breuning study explicit variants of these two conjectures and the relation to the global epsilon constant conjecture. More recently, they proved in [11] assuming Leopoldt's conjecture that their explicit conjecture at $s = 1$ is equivalent to the relevant case of the ETNC.

The decomposition $K_0(\mathbb{Z}[G], \mathbb{Q}) = \bigoplus_p K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ splits $T\Omega^{\mathrm{loc}}(L/K, 1)$ into p-parts. This has been further refined by Breuning in [8] stating an independent conjecture for Galois extensions E/F of local number fields in the group $K_0(\mathbb{Z}_p[D], \mathbb{Q}_p)$ where $D = \mathrm{Gal}(E/F)$. He defined an element $R_{E/F} \in K_0(\mathbb{Z}_p[D], \mathbb{Q}_p)$ incorporating local epsilon constants and algebraic invariants associated to the local number field extension E/F and conjectured the vanishing of $R_{E/F}$. Breuning proved his local epsilon constant conjecture in [8] for tamely ramified extensions, for abelian extensions of $\mathbb{Q}_p$ with $p \neq 2$, for all S_3-extensions, and for certain infinite families of dihedral and quaternion extensions.

Moreover, this local conjecture is related to the global conjecture by the equation $T\Omega^{\mathrm{loc}}(L/K, 1)_p = \sum_v \mathrm{i}_{G_w}^G(R_{L_w/K_v})$ where v runs through all places of K above p, w is a fixed place of L above v, G_w denotes the decomposition group and $\mathrm{i}_{G_w}^G$ is the induction map on the relative K-group, cf. [8, Thm. 4.1].

We fix a base field K and a finite group G. Using the result for tame extensions, one concludes that the validity of the global conjecture for all Galois extensions L/K with $\mathrm{Gal}(L/K)$ isomorphic to G depends upon the validity of the local conjecture for only finitely many local extensions.

Subsequently, Breuning and the first named author presented an algorithm in [3] which proves the local epsilon constant conjecture for a given local number field extension. To establish a practical algorithm, there were, however, still some tasks which needed a more efficient solution. In this paper we will address these problems, give solutions, and present computational results.

These computations together with known theoretical results will prove:

Theorem 1. *a) If p is odd, then the local epsilon constant conjecture is valid for all Galois extensions E of $\mathbb{Q}_p$ with $[E : \mathbb{Q}_p] \leq 15$.*

b) If $p = 2$, then the local epsilon constant conjecture is valid for all non-abelian Galois extensions E of $\mathbb{Q}_2$ with $[E : \mathbb{Q}_2] \leq 15$. In addition, it is valid for all abelian extensions E of $\mathbb{Q}_2$ with $[E : \mathbb{Q}_p] \leq 7$.

Remark 2. In the statement of Theorem 1 we only considered extensions $E/\mathbb{Q}_p$ of degree ≤ 15 because only in these cases our computations led to new results. As already mentioned, the local epsilon constant conjecture is proven by Breuning for all tamely ramified extensions (p arbitrary) and all abelian extensions $E/\mathbb{Q}_p$ with $p \neq 2$.

We point out that we could not prove the local conjecture for wildly ramified abelian extensions $E/\mathbb{Q}_2$ of degree $8 \leq [E : \mathbb{Q}_2] \leq 15$. The main reason for this is that the unramified extension of degree 8 over $\mathbb{Q}_2$ cannot be represented as the

completion of a Galois extension $L/\mathbb{Q}$ of degree 8.[1] Instead, we have to use an extension L/K of degree 8, with $[L : \mathbb{Q}] = 16$ and $[K : \mathbb{Q}] = 2$, and this increases the complexity of the computations a lot.

The above relation between $T\Omega^{\mathrm{loc}}(L/K, 1)_p$ and R_{L_w/K_v} will imply results for global Galois extensions $L/\mathbb{Q}$ which satisfy the following property.

Property $(*)$ We say that the Galois extension L/K of number fields satisfies Property $(*)$ if for every wildly ramified place v of K with $w|v|p$ one of the following cases is satisfied

$a)$ $K_v = \mathbb{Q}_p, p > 2$ and G_w is abelian,

$b)$ $K_v = \mathbb{Q}_p, p = 2, G_w$ is abelian and $|G_w| \leq 7$

$c)$ $K_v = \mathbb{Q}_p, p \geq 2, G_w$ is non-abelian and $|G_w| \leq 15$.

Corollary 3. *The global epsilon constant conjecture is valid for all Galois extensions L/K which satisfy Property $(*)$.*

The projection onto the class group also proves Chinburg's conjecture:

Corollary 4. *Chinburg's $\Omega(2)$-conjecture is valid for all Galois extensions L/K which satisfy Property $(*)$.*

Moreover, the functorial properties of [8, Prop. 3.3] imply the following result:

Corollary 5. *The global epsilon constant conjecture and Chinburg's $\Omega(2)$-conjecture are valid for global Galois extensions E/F for which $K \subseteq F \subseteq E \subseteq L$ with a Galois extension L/K that satisfies Property $(*)$.*

Remark 6. If $L/\mathbb{Q}$ is a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \simeq A_5$, the alternating group of order 60, then $L/\mathbb{Q}$ satisfies Property $(*)$. More generally, if K is a number field where $2, 3$ and 5 are completely split, then each A_5-extension L/K satisfies Property $(*)$.

Corollary 7. *The global epsilon constant conjecture and Chinburg's $\Omega(2)$-conjecture are valid for all global Galois extensions E/F for which $\mathbb{Q} \subseteq F \subseteq E \subseteq L$ with a Galois extension $L/\mathbb{Q}$ of degree $[L : \mathbb{Q}] \leq 15$.*

The main contents of this article are as follows. After introducing some notation we will present an efficient algorithm for the computation of local fundamental classes in §2. In §3 we will recall the formulation of the epsilon constant conjectures and related known results. To apply an algorithm of Breuning and the first named author for the proof of this conjecture (see [3]) we will present heuristics to represent local extensions using global number fields in §4. Thereafter, §5 gives an overview of the algorithm and addresses details and problems which either needed more efficient solutions or which occurred during the implementation of the algorithm. In §6 we finally summarize all theoretical results that restrict the problem to the verification of the local epsilon constant conjecture for finitely many local extensions of $\mathbb{Q}_p$. These problems have then been solved by a computer and we give some details on the computations and their results. Altogether, this will complete the proof of Theorem 1 and its corollaries.

---

[1]This is Wang's counterexample to Grunwald's original statement of his theorem.

Notation: For a (local or global) number field L we write $\mathcal{O}_L$ for its ring of integers. If L is a local number field with prime ideal $\mathfrak{P}$, we write U_L for the units $(\mathcal{O}_L)^\times$ and $U_L^{(n)}$ for the n-units $1 + \mathfrak{P}^n$.

For a group G and a G-module A we write $H^n(G, A)$ for the cohomology group in degree n as defined in [29, I§2] and we will use the inhomogeneous description using n-cochains $C^n(G, A) := \mathrm{Map}(G^n, A)$ and $C^0(G, A) := A$. As usual, we write $\hat{H}^n(G, A)$ for the Tate cohomology groups.

Let L/K denote a local Galois extension with Galois group G. We will also use the notation of class formations of [33, XI§2] and let $u_{L/K}$ denote the local fundamental class of L/K as defined in [33, XIII§3f.], i.e. the element which is mapped to $\frac{1}{[L:K]} + \mathbb{Z}$ by the local invariant isomorphism $\mathrm{inv}_{L/K} : \hat{H}^2(G, L^\times) \xrightarrow{\simeq} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.[2]

Acknowledgement: It is a pleasure for us to thank the referees for their very careful reading of the manuscript and many valuable comments. In particular, the formulation of our corollaries is motivated by a suggestion of one of the referees.

2. An efficient algorithm to compute the local fundamental class

Throughout this section L/K will denote a Galois extension of $\mathbb{Q}_p$ with Galois group $G = \mathrm{Gal}(L/K)$. Our goal is to find the local fundamental class represented as a cocycle in $\hat{H}^2(G, L^\times)$.

A direct method to compute the image of the local fundamental class under $\hat{H}^2(G, L^\times) \to \hat{H}^2(G, L^\times/U_L^{(k)})$ for any $k \geq 0$ has been described in [3, §2.4]. Let N be an unramified extension of K with cyclic Galois group C and of degree $[N : K] = [L : K]$ and let Γ denote the Galois group of LN/K. Then there is a commutative diagram

$$
\begin{array}{ccc}
 & & \hat{H}^2(C, N^\times) \\
 & & \downarrow{\scriptstyle\mathrm{inf}} \\
\hat{H}^2(G, L^\times) & \xhookrightarrow{\ \mathrm{inf}\ } & \hat{H}^2(\Gamma, (LN)^\times) \\
\downarrow & & \downarrow \\
\hat{H}^2(G, L^\times/U_L^{(k)}) & \xhookrightarrow{\ \mathrm{inf}\ } & \hat{H}^2(\Gamma, (LN)^\times/U_{LN}^{(k)})
\end{array}
$$

in which all inflation maps are injective, either by [3, Lem. 2.5] or [33, VII, §6, Prop. 5] combined with Hilbert's Theorem 90. Based on this diagram, the authors describe an algorithm which consists of the following steps:

(1) Find the fundamental class in $\hat{H}^2(C, N^\times)$.
(2) Compute the image under the composition

$$\hat{H}^2(C, N^\times) \xrightarrow{\mathrm{inf}} \hat{H}^2(\Gamma, (LN)^\times) \to \hat{H}^2(\Gamma, (LN)^\times/U_{LN}^{(k)}).$$

(3) Find the preimage under the map

$$\hat{H}^2(G, L^\times/U_L^{(k)}) \xrightarrow{\mathrm{inf}} \hat{H}^2(\Gamma, (LN)^\times/U_{LN}^{(k)}).$$

---

[2]Similar definitions can be found in [29, (3.1.3), (7.1.4)].

If φ denotes the Frobenius automorphism in $C = \langle \varphi \rangle$ and $\pi \in K$ is a uniformizing element, the fundamental class in $\hat{H}^2(C, N^\times)$ is given by (see [26, §30, Sec. 4 and §31, Sec. 4])

$$\gamma(\varphi^i, \varphi^j) = \begin{cases} 1 & \text{if } i + j < [N : K], \\ \pi & \text{if } i + j \geq [N : K] \end{cases}$$

Since the groups $(LN)^\times / U_{LN}^{(k)}$ and $L^\times / U_L^{(k)}$ are finitely generated, one can compute their cohomology groups using linear algebra [22]. However, this method turns out to be ineffective even for local fields of small degree.

The basis of a new algorithm to compute the local fundamental class is the theory of Serre [33] and especially exercise 2 of chapter XIII, §5. We recall the results of this exercise and show how to turn it into an efficient algorithm.

Let E be the maximal unramified subextension of L/K and $d := [E : K]$. Denote the maximal unramified extension of K by $\widetilde{K}$ and the Frobenius automorphism of $\widetilde{K}/K$ by φ. Then $\text{Gal}(\widetilde{K}/K) = \overline{\langle \varphi \rangle}$ and $\text{Gal}(\widetilde{K}/E) = \overline{\langle \varphi^d \rangle}$. We set $\widetilde{L} := \widetilde{K}L$ and note that $\widetilde{L}$ is the maximal unramified extension of L. We always identify $\text{Gal}(\widetilde{L}/L)$ with $\text{Gal}(\widetilde{K}/E)$ by restriction.

The Galois group of $\widetilde{L}/K$ is given by

$$\text{Gal}(\widetilde{L}/K) = \{(\tau, \sigma) \in \text{Gal}(\widetilde{K}/K) \times G \,|\, \sigma|_E = \tau|_E\}.$$

We consider $L_{nr} := \widetilde{K} \otimes_K L$, for which we have the following representation:

Lemma 8. *(i) The map $L_{nr} = \widetilde{K} \otimes_K L \to \prod_{i=0}^{d-1} \widetilde{L}$ defined by sending elements $a \otimes b$ to $\big(ab, \varphi(a)b, \ldots, \varphi^{d-1}(a)b\big)$ is an isomorphism.*

(ii) The Galois action of $\langle \varphi \rangle \times G$ on elements $y = (y_0, y_1, \ldots, y_{d-1}) \in \prod_{i=0}^{d-1} \widetilde{L}$ induced by this isomorphism is uniquely described by

$$(\varphi, 1)(y) = (y_1, y_2, \ldots, \varphi^d(y_0)),$$
$$(\varphi^j, \sigma)(y) = (\hat{\sigma}(y_0), \hat{\sigma}(y_1), \ldots, \hat{\sigma}(y_{d-1})), \text{if } \sigma|_E = \varphi^j|_E.$$

Here $\hat{\sigma} \in \text{Gal}(\widetilde{L}/K)$ is the unique element such that $\hat{\sigma}|_{\widetilde{K}} = \varphi^j$ and $\hat{\sigma}|_L = \sigma$.

Proof. Direct computation, cf. [33, XIII §5, Ex. 2]. $\qquad\qquad\square$

Remark 9. For arbitrary $(\varphi^s, \sigma) \in \langle \varphi \rangle \times G$ one chooses $j \in \mathbb{Z}$ such that $\sigma|_E = \varphi^j|_E$. Then $(\varphi^s, \sigma) = (\varphi^{s-j}, 1)(\varphi^j, \sigma)$ and and the action of each of the factors is given by the lemma. Explicitly, there is a unique $\hat{\sigma} \in \text{Gal}(\widetilde{L}/K)$ such that $\hat{\sigma}|_L = \sigma$, $\hat{\sigma}|_{\widetilde{K}} = \varphi^j$ and (φ^s, σ) acts as $(\varphi^{s-j}, 1)\hat{\sigma}$ (with $\hat{\sigma}$ acting diagonally).

Let $\widehat{L}$ be the completion of the maximal unramified extension $\widetilde{L}$ of L.

Lemma 10. *For every $c \in U_{\widehat{L}}$ there exists $x \in U_{\widehat{L}}$ such that $x^{\varphi^d - 1} = c$.*

Proof. This is [28, V, Lem. 2.1] or [33, XIII, Prop. 15] applied to the totally ramified extension L/E with φ^d generating $\text{Gal}(\widetilde{K}/E)$. Since this will be an essential part of the algorithm, we sketch the constructive proof of [28].

Denote the residue class field of $\widehat{L}$ by κ, the cardinality of the residue class field of E by q and let $\phi = \varphi^d$. Let π be a uniformizing element of L.

Since κ is algebraically closed, one finds a solution to $x^\phi = x^q = xc$ in κ and one can write $c = x_1^{\phi-1} a_1$ with $x_1 \in U_{\widehat{L}}$ and $a_1 \in U_{\widehat{L}}^{(1)}$. Similarly, one finds $x_2 \in U_{\widehat{L}}^{(1)}$

and $a_2 \in U_{\widehat{L}}^{(2)}$ such that $a_1 = x_2^{\phi-1} a_2$. Indeed, if we set $a_1 := 1 + b_1\pi$, $x_2 := 1 + y_2\pi$, then we need to solve

$$a_1 x_2^{1-\phi} \equiv 1 - (y_2^\phi - y_2 - b_1)\pi \equiv 1 \pmod{\pi^2},$$

i.e., we must solve the equation $y_2^q - y_2 - b_1 = 0$ in κ.

Proceeding this way one has

$$c = (x_1 x_2 \cdots x_n)^{\phi-1} a_n, \quad x_1 \in U_{\widehat{L}}, \ x_i \in U_{\widehat{L}}^{(i-1)}, \ a_n \in U_{\widehat{L}}^{(n)}$$

and passing to the limit solves the equation in $U_{\widehat{L}}$. $\qquad\square$

This fact can be generalized to our case. Let $\widehat{L}_{nr}$ be the completion of L_{nr}, so $\widehat{L}_{nr} \simeq \prod_{i=0}^{d-1} \widehat{L}$, and $w : \widehat{L}_{nr} \to \mathbb{Z}$ the sum of the valuations.

Lemma 11. *For every $c \in \widehat{L}_{nr}^\times$ with $w(c) = 0$ there exists $x \in \widehat{L}_{nr}^\times$ such that $x^{\varphi-1} = c$.*

Proof. If $c = (c_0, \ldots c_{d-1}) \in \prod_{i=0}^{d-1} \widehat{L}^\times$ and $w(c) = 0$, then $\prod_{i=0}^{d-1} c_i \in \widehat{L}^\times$ has valuation 0 and there exists $y \in \widehat{L}^\times$ for which $y^{\varphi^d-1} = \prod c_i$ by Lemma 10. Then the element $x = (y, yc_0, yc_0c_1, \ldots, yc_0 \cdots c_{d-2})$ satisfies

$$x^{\varphi-1} = \frac{(yc_0, yc_0c_1, \ldots, yc_0 \cdots c_{d-2}, \varphi^d(y))}{(y, yc_0, yc_0c_1, \ldots, yc_0 \cdots c_{d-2})} = (c_0, c_1, \ldots, c_{d-1}) = c$$

since $\varphi^d(y) = y \prod_{i=0}^{d-1} c_i$. $\qquad\square$

We prepare our main result by the following lemma.

Lemma 12.   (i) $\ker(w) = \{y^{\varphi-1} \mid y \in \widehat{L}_{nr}^\times\}$,

(ii) $\ker(\varphi - 1) = L^\times$, $L^\times$ being diagonally embedded in $\widehat{L}_{nr}^\times$, and

(iii) $\widehat{L}_{nr}^\times$ is a cohomologically trivial G-module.

Proof. This is [33, XIII §5, Ex. 2(a)]. For a detailed proof see [17, Lemma 2.13]. $\square$

We denote $V := \ker(w)$ and from Lemma 12 we get the exact sequences

$$(1) \qquad\qquad 0 \longrightarrow V \longrightarrow \widehat{L}_{nr}^\times \xrightarrow{w} \mathbb{Z} \longrightarrow 0$$

$$(2) \qquad \text{and} \quad 0 \longrightarrow L^\times \longrightarrow \widehat{L}_{nr}^\times \xrightarrow{\varphi-1} V \longrightarrow 0.$$

Since $\widehat{L}_{nr}^\times$ is cohomologically trivial, the connecting homomorphisms of their long exact cohomology sequences provide isomorphisms $\delta_1 : \hat{H}^0(G, \mathbb{Z}) \to \hat{H}^1(G, V)$, $\delta_2 : \hat{H}^1(G, V) \to \hat{H}^2(G, L^\times)$ and we consider the composition

$$(3) \qquad\qquad \Phi_{L/K} : \hat{H}^0(G, \mathbb{Z}) \xrightarrow{\;\simeq\;} \hat{H}^2(G, L^\times).$$

Its inverse $\Phi_{L/K}^{-1}$ induces an isomorphism

$$\overline{\text{inv}}_{L/K} : \hat{H}^2(G, L^\times) \simeq \hat{H}^0(G, \mathbb{Z}) \xrightarrow{\cdot \frac{1}{[L:K]}} \tfrac{1}{[L:K]} \mathbb{Z}/\mathbb{Z}.$$

Proposition 13.   (i) *The map $\overline{\text{inv}}$ is an invariant map in the sense of [33, XI, §2]. Therefore the elements $\overline{u}_{L/K} := \Phi_{L/K}(1 + [L : K]\mathbb{Z})$ are fundamental classes with respect to the class formation associated to $\overline{\text{inv}}$.*

(ii) *The element $\overline{u}_{L/K}$ is the inverse of the local fundamental class $u_{L/K}$.*

Proof. This is [33, XIII §5, Ex. 2(c) and (d)]. For a detailed proof we refer the reader to [17, Prop. 2.14]. Since parts of the proof will be turned into an algorithm (see Remark 14) we recall some of the details.

Part (i) can be proved by verifying the axioms of a class formation.

In order to prove (ii) it suffices to show $\overline{u}_{N/K} = u_{N/K}^{-1}$ where N/K denotes the unramified extension of K of degree $[L : K]$. Indeed, by the axioms of a class formation we have

$$\mathrm{inv}_{L/K} = \mathrm{inv}_{LN/K} \circ \mathrm{inf}_{L/K}^{LN/K}, \quad \mathrm{inv}_{N/K} = \mathrm{inv}_{LN/K} \circ \mathrm{inf}_{N/K}^{LN/K},$$

and the same identities with inv replaced by $\overline{\mathrm{inv}}$. It follows that $\mathrm{inf}_{L/K}^{LN/K}(u_{L/K}) = \mathrm{inf}_{N/K}^{LN/K}(u_{N/K})$ and $\mathrm{inf}_{L/K}^{LN/K}(\overline{u}_{L/K}) = \mathrm{inf}_{N/K}^{LN/K}(\overline{u}_{N/K})$. Since $\mathrm{inf}_{L/K}^{LN/K}$ is injective we deduce from $\overline{u}_{N/K} = u_{N/K}^{-1}$ the desired equality $\overline{u}_{L/K} = u_{L/K}^{-1}$.

For the unramified case one can make a direct computation of $\Phi_{L/K}(1+[L : K]\mathbb{Z})$ by applying the connecting homomorphisms δ_1 and δ_2 as follows. For δ_1 we consider the commutative diagram

(4)
$$
\begin{array}{ccccccccc}
 & & & & \widehat{L}_{nr}^{\times} & & \mathbb{Z} & & \\
 & & & & \| & & \| & & \\
0 & \longrightarrow & C^0(G,V) & \longrightarrow & C^0(G,\widehat{L}_{nr}^{\times}) & \overset{w}{\longrightarrow} & C^0(G,\mathbb{Z}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \partial_1} & & \downarrow & & \\
0 & \longrightarrow & C^1(G,V) & \longrightarrow & C^1(G,\widehat{L}_{nr}^{\times}) & \overset{w^*}{\longrightarrow} & C^1(G,\mathbb{Z}) & \longrightarrow & 0
\end{array}
$$

which is induced by the exact sequence (1), and where w^* is the map on the group of cochains induced by w. If π is any uniformizing element of $\widehat{L}^{\times}$, the element $a = (1,\ldots,1,\pi) \in \widehat{L}_{nr}^{\times} = C^0(G,\widehat{L}_{nr}^{\times})$ is a preimage of 1 via w. Applying ∂_1 yields $\alpha \in C^1(G,\widehat{L}_{nr}^{\times})$, which is defined by

$$\alpha(\sigma) := \frac{\sigma(a)}{a} = \begin{cases} \left(1,\ldots,1,\frac{\hat{\sigma}(\pi)}{\pi}\right), & \text{if } \hat{\sigma}|_E = 1 \\ \left(1,\ldots,1,\hat{\sigma}(\pi), \underbrace{1,\ldots,1,\frac{1}{\pi}}_{j \text{ components}}\right), & \text{if } \hat{\sigma}|_E = \varphi^{-j}, 1 \leq j \leq d-1 \end{cases}$$

The commutativity of the diagram then implies $\alpha \in C^1(G,V)$.

For the connecting homomorphism δ_2 we consider the commutative diagram

(5)
$$
\begin{array}{ccccccccc}
0 & \longrightarrow & C^1(G,L^{\times}) & \longrightarrow & C^1(G,\widehat{L}_{nr}^{\times}) & \overset{\varphi-1}{\longrightarrow} & C^1(G,V) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \partial_2} & & \downarrow & & \\
0 & \longrightarrow & C^2(G,L^{\times}) & \longrightarrow & C^2(G,\widehat{L}_{nr}^{\times}) & \longrightarrow & C^2(G,V) & \longrightarrow & 0
\end{array}
$$

which arises from the exact sequence (2). To find a preimage of α via $\varphi - 1$, we need elements in $\widehat{L}_{nr}^{\times}$ which are mapped to $\frac{\sigma(a)}{a}$ by $\varphi - 1$. By Lemma 11 these preimages are given by

$$(6) \quad \beta(\sigma) := \begin{cases} (u_\sigma,\ldots,u_\sigma) & \text{if } \hat{\sigma}|_E = 1 \\ (u_\sigma,\ldots,u_\sigma, \underbrace{u_\sigma\hat{\sigma}(\pi),\ldots,u_\sigma\hat{\sigma}(\pi)}_{j \text{ components}}) & \text{if } \hat{\sigma}|_E = \varphi^{-j}, 1 \leq j \leq d-1 \end{cases}$$

where u_σ solves $u_\sigma^{\varphi^d-1} = \frac{\hat\sigma(\pi)}{\pi}$. The commutativity of the diagram again implies that the cocycle

(7) $$\gamma(\sigma,\tau) := (\partial_2\beta)(\sigma,\tau) = \frac{\sigma(\beta(\tau))\beta(\sigma)}{\beta(\sigma\tau)}$$

has values in $L^\times$ and we obtain $\bar u_{L/K} = \Phi_{L/K}(1 + [L:K]\mathbb{Z}) = \gamma \in \hat H^2(G, L^\times)$.

If L/K is unramified, one can choose π to be a uniformizing element of K and set $\sigma = \varphi^i$, $\tau = \varphi^j$. Then $\frac{\hat\sigma(\pi)}{\pi} = 1$ for all $\hat\sigma \in \mathrm{Gal}(\widetilde L/K)$ and every $u_\sigma \in L^\times$ solves $u_\sigma^{\varphi^n-1} = \frac{\hat\sigma(\pi)}{\pi}$. If one chooses $u_\sigma = \frac{1}{\pi}$ for $\sigma \neq id$ and $u_{id} = 1$, one can easily check that $\bar u_{L/K}(\sigma,\tau) = 1$, if $i + j < d$ and $\bar u_{L/K}(\sigma,\tau) = \pi^{-1}$ otherwise. Hence, $\bar u_{L/K}$ is the inverse of the local fundamental class, cf. [3, §2.4]. A detailed proof can be found in the second author's dissertation [17]. □

Remark 14. From the construction above one directly obtains an algorithm. The uniformizing element π of $\widehat L^\times$ in the proof above can be chosen to be a uniformizing element of L. Then approximations to the elements u_σ can be computed by successively applying the constructive steps of the proof of Lemma 10. This involves solving equations in the algebraically closed residue class field of $\widehat L^\times$. However, we cannot do computations in $\widehat L^\times$ directly, but rather work in an appropriate subfield, starting with L. Whenever we cannot solve one of these equations in the residue class field of L, we generate an appropriate algebraic extension and work there from then on. In worst case, this means that we have to generate an algebraic extension in every step. And, hence, the extensions involved in the computations often get very large.

To avoid this problem we proceed as follows. Let π_K and π_L be uniformizing elements of K and L, e the ramification degree and d the inertia degree of L/K. Let N be the unramified extension of K of degree $[L:K]$. Then $F := LN$ is the unramified extension of L of degree e. We set $L_{nr} := \prod_d F$ and let E be the maximal unramified extension of K in L with Frobenius automorphism φ. In the algorithm below, we construct a special uniformizing element π in F such that $N_{F/L}(\frac{\hat\sigma(\pi)}{\pi}) = 1$. One can then prove that the elements u_σ can be constructed in F.

Algorithm 15 (Local fundamental class).

Input: An extension L/K over $\mathbb{Q}_p$ with Galois group G and a precision $k \in \mathbb{N}$.

Output: The local fundamental class $u_{L/K} \in C^2(G, L^\times)$ up to the finite precision k, i.e. its image in $\hat H^2(G, L^\times/U_L^{(k)})$.

1 Solve the norm equation $N_{F/L}(v) \equiv u \bmod U_L^{(k+2)}$ with $u = \pi_K\pi_L^{-e} \in U_L$ and $v \in U_F/U_F^{(k+2)}$. Define $\pi = v\pi_L$.

2 For each $\sigma \in G$, let $\hat\sigma \in \mathrm{Gal}(F/K)$ be the automorphism which is uniquely determined by $\hat\sigma|_L = \sigma$ and $(\hat\sigma|_N)^{-1} = \varphi^j$ with $0 \le j \le d-1$. Then compute $u_\sigma \in U_F$ such that $u_\sigma^{\varphi^d-1} = \frac{\hat\sigma(\pi)}{\pi} \bmod U_F^{(k+2)}$.

3 Define $\beta \in C^1(G, L_{nr}^\times)$ and $\gamma \in C^2(G, L^\times)$ by (6) and (7).

Return: γ^{-1}.

Note that the choice of j in this algorithm corresponds to the choice of j in the proof of Proposition 13, see in particular equation (6).

Proof of correctness. Step 1: Since u has valuation 0 and F/L is unramified, there exists an element $v \in U_F$ such that its norm is equal to u. Then π is a uniformizing element of F and has norm $N_{F/L}(\pi) = u\pi_L^e = \pi_K$.

Step 2: The elements $\frac{\hat{\sigma}(\pi)}{\pi}$ have norm

$$N_{F/L}\left(\frac{\hat{\sigma}(\pi)}{\pi}\right) = \frac{1}{\pi_K}\prod_{i=1}^{e}\varphi^{di}\left(\hat{\sigma}(\pi)\right) = \frac{1}{\pi_K}\,\hat{\sigma}\left(\prod_{i=1}^{e}\varphi^{di}(\pi)\right) = 1.$$

Let $H = \mathrm{Gal}(F/L)$. Since $\hat{H}^{-1}(H, U_F) = {}_{N_H}U_F/I_H U_F = 1$ for the unramified extension F/L, there exists $x \in U_F$ with $x^{\varphi - 1} = \frac{\hat{\sigma}(\pi)}{\pi}$. By successively applying the steps in the constructive proof of [28, V, Lem. 2.1] (see Lemma 10) one can construct an element $x \in U_F$ with $x^{\varphi - 1} \equiv \frac{\hat{\sigma}(\pi)}{\pi} \mod U_F^{(k+2)}$.

Step 3: The computation in the proof of Proposition 13 shows that the cocycle γ from (7) represents the inverse of the local fundamental class.

If we compute the elements u_σ modulo $U_F^{(k+2)}$, we also know the images of β to the same precision. To compute γ^{-1} we divide by $\sigma(\beta(\tau))$ and $\beta(\sigma)$ and each of these operations can reduce the precision at most by one because all elements in (6) have at most valuation 1. The other operations involved in ∂_2 (addition, multiplication and application of σ) do not reduce the precision. Hence, we know the images of γ modulo $U_L^{(k)}$. $\qquad\square$

This algorithm has been implemented in MAGMA [6] and its source code is bundled with the second author's dissertation [17]. For a small example where the Galois group is $G = S_3$, this algorithm computes the local fundamental class within a few seconds whereas the direct linear algebra method took more than an hour.

The implementation of this more efficient algorithm made several interesting applications possible. In the second author's dissertation [17], Algorithm 15 is used in algorithms for computations in Brauer groups of (global) number field extensions and for the computation of global fundamental classes. In addition, the algorithm was also applied in a completely different context: based on the Shafarevic-Weil theorem, Greve used the algorithm in his dissertation [20] to compute Galois groups of local extensions.

3. EPSILON CONSTANT CONJECTURES

We recall the statements of the global and local epsilon constant conjectures of [4] and [8] and some important related results. These conjectures are formulated as equations in relative K-groups for group rings.

Let R be an integral domain, E an extension of $\mathrm{Quot}(R)$ and G a finite group. For a ring A we write $K_0(A)$ for the Grothendieck group of finitely generated projective A-modules and $K_1(A)$ for the abelianization of the infinite general linear group $\mathrm{Gl}(A)$. Then there is an exact sequence

$$(8) \qquad K_1(R[G]) \to K_1(E[G]) \xrightarrow{\partial^1_{R[G],E}} K_0(R[G], E) \to K_0(R[G]) \to K_0(E[G])$$

with the relative algebraic K-group $K_0(R[G], E)$ defined in terms of generators and relations as in [34, p. 215]. An overview of the relevant results concerning these K-groups is given in [7]. We write $\mathrm{Z}(E[G])$ for the center of $E[G]$ and we will use the reduced norm map $\mathrm{nr} : K_1(E[G]) \to \mathrm{Z}(E[G])^\times$, which is injective in our cases, and the map $\widehat{\partial}^1_{R[G],E} := \partial^1_{R[G],E} \circ \mathrm{nr}^{-1}$ from $\mathrm{im}(\mathrm{nr})$ to $K_0(R[G], E)$.

The two cases we are interested in are the following. For $R = \mathbb{Z}_p$ and E an extension of $\mathbb{Q}_p$ the reduced norm is an isomorphism (e.g. see [7, Prop. 2.2]) and we obtain a map $\widehat{\partial}^1_{G,E} := \widehat{\partial}^1_{\mathbb{Z}_p[G],E} = \partial^1_{\mathbb{Z}_p[G],E} \circ \mathrm{nr}^{-1}$ from $\mathrm{Z}(E[G])^\times$ to $K_0(\mathbb{Z}_p[G], E)$.

For $R = \mathbb{Z}, E = \mathbb{R}$ the reduced norm map is not surjective but the decomposition

(9) $$K_0(\mathbb{Z}[G], \mathbb{Q}) \simeq \coprod_p K_0(\mathbb{Z}_p[G], \mathbb{Q}_p),$$

and the Weak Approximation Theorem still allow us to define a canonical map $\widehat{\partial}^1_{G,\mathbb{R}}$ from $\mathrm{Z}(\mathbb{R}[G])^\times$ to $K_0(\mathbb{Z}[G], \mathbb{R})$, such that $\widehat{\partial}^1_{G,\mathbb{R}} \circ \mathrm{nr} = \partial^1_{G,\mathbb{R}}$, cf. [4, §3.1] or [10, Lem. 2.2].

3.1. **The global epsilon constant conjecture.** The global epsilon constant conjecture is formulated in the relative K-group $K_0(\mathbb{Z}[G], \mathbb{R})$. For a Galois extension L/K of number fields it describes a relation between the epsilon factors arising in the functional equation of Artin L-functions and algebraic invariants related to L/K. We briefly sketch its formulation which is due to Burns and the first named author and refer to [4] for more details.

The completed Artin L-function $\Lambda(L/K, \chi, s)$ satisfies the functional equation

(10) $$\Lambda(L/K, \chi, s) = \varepsilon(L/K, \chi, s)\, \Lambda(L/K, \bar{\chi}, 1 - s)$$

with an epsilon factor $\varepsilon(L/K, \chi, s) := W(\chi)A(\chi)^{\frac{1}{2}-s}$ and $W(\chi), A(\chi)$ as defined in [19, Chp. I, (5.22)]. The equivariant epsilon function is defined by $\varepsilon(L/K, s) := (\varepsilon(L/K, \chi, s))_{\chi \in \mathrm{Irr}(G)}$ and its value $\epsilon_{L/K} := \varepsilon(L/K, 0) \in \mathrm{Z}(\mathbb{R}[G])^\times$ is called the equivariant global epsilon constant. We define a corresponding element in the relative K-group $K_0(\mathbb{Z}[G], \mathbb{R})$ by $\mathscr{E}_{L/K} := \widehat{\partial}^1_{G,\mathbb{R}}(\epsilon_{L/K})$ and also refer to it as the equivariant global epsilon constant.

Let S be a finite set of non-archimedean places of K, including all non-archimedean places which ramify in L. For each $v \in S$ with $v|p$ we fix a place w of L above v and choose a full projective $\mathbb{Z}_p[G_w]$-sublattice $\mathscr{L}_w$ of $\mathcal{O}_{L_w}$ upon which the v-adic exponential map is well-defined (and hence injective). For each place w which does not lie above some $v \in S$ we set $\mathscr{L}_w = \mathcal{O}_{L_w}$ and we define $\mathscr{L} \subseteq \mathcal{O}_L$ by its p-adic completions

$$\mathscr{L}_p = \prod_{v|p} \mathscr{L}_w \otimes_{\mathbb{Z}_p[G_w]} \mathbb{Z}_p[G] \subseteq L_p := L \otimes_{\mathbb{Q}} \mathbb{Q}_p.$$

For each finite place w of L we also write $w : L^\times \longrightarrow \mathbb{Z}$ for the standard valuation of L normalized such that $w(L^\times) = \mathbb{Z}$. We let $\Sigma(L)$ denote the set of all embeddings of L into $\mathbb{C}$ and set $H_L := \prod_{\sigma \in \Sigma(L)} \mathbb{Z}$. We define the G-equivariant discriminant by $\delta_{L/K}(\mathscr{L}) := [\mathscr{L}, \pi_L, H_L] \in K_0(\mathbb{Z}[G], \mathbb{R})$ where π_L is induced by $\rho_L : L \otimes_{\mathbb{Q}} \mathbb{C} \to H_L \otimes_{\mathbb{Z}} \mathbb{C}$, $l \otimes z \mapsto (\sigma(l)z)_{\sigma \in \Sigma(L)}$ as in [4, §3.2].

Let $X \subseteq \mathcal{O}_{L_w}^\times$ be any cohomologically trivial $\mathbb{Z}[G_w]$-submodule of finite index, e.g. $X = \exp_v(\mathscr{L}_w)$. Then $\hat{H}^2(G_w, L_w^\times) \simeq \hat{H}^2(G_w, L_w^\times/X)$ and by [29, Th. 2.2.10] there is an isomorphism $\hat{H}^2(G_w, L_w^\times/X) \simeq \mathrm{Ext}^2_{G_w}(\mathbb{Z}, L_w^\times/X)$. For a cocycle $\gamma \in \hat{H}^2(G_w, L_w^\times/X)$ one can apply the construction of [29, p. 115] to obtain a 2-extension

$$0 \to L_w^\times/X \to C(\gamma) \to \mathbb{Z}[G_w] \to \mathbb{Z} \to 0$$

representing γ in $\mathrm{Ext}^2_{G_w}(\mathbb{Z}, L_w^\times/X)$.

If γ represents the local fundamental class then the complex

$$K_w^\bullet(X) := \left[C(\gamma) \to \mathbb{Z}[G_w] \right]$$

is perfect. Here the modules are placed in degrees 0 and 1. We write $E_w(X)$ for its refined Euler characteristic in $K_0(\mathbb{Z}[G_w], \mathbb{Q})$ where the trivialization

$$H^0(K_w^\bullet(X)) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq L_w^\times / X \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} \mathbb{Q} \simeq H^1(K_w^\bullet(X)) \otimes_{\mathbb{Z}} \mathbb{Q}$$

is induced by the valuation map $w : L_w^\times \to \mathbb{Z}$. For the general construction of refined Euler characteristics we refer the reader to [12, §2]. For the construction in our special case see [4, §3.3], in particular, a triple representing $E_w(X)$ in $K_0(\mathbb{Z}[G_w], \mathbb{Q})$ is given in [4, Lem. 3.7].

Furthermore, let $m_w \in \mathrm{Z}(\mathbb{Q}[G_w])^\times$ be the element defined in [4, §4.1] which we also call the *correction term*. It is defined as follows. For a subgroup $H \subseteq G$ and $x \in \mathrm{Z}(\mathbb{Q}[H])$ we let $^*x \in \mathrm{Z}(\mathbb{Q}[H])^\times$ denote the invertible element which on the *Wedderburn decomposition* $\mathrm{Z}(\mathbb{Q}[H]) = \prod_{i=1}^r F_i$ with suitable extensions $F_i/\mathbb{Q}$ is given by $^*x = (^*x_i)_{i=1\ldots r}$ with $^*x_i = 1$ if $x_i = 0$ and $^*x_i = x_i$ otherwise. If φ_w denotes a lift of the Frobenius automorphism in G_w/I_w, then the correction term is defined by

$$(11) \qquad m_w = \frac{^*(|G_w/I_w|e_{G_w}) \cdot {}^*((1 - \varphi_w \mathrm{N} v^{-1}) e_{I_w})}{^*((1 - \varphi_w^{-1}) e_{I_w})} \in \mathrm{Z}(\mathbb{Q}[G_w])^\times.$$

Finally, we define elements

$$I_G(v, \mathscr{L}) := \mathrm{i}_{G_w}^G \big(\widehat{\partial}_{G_w, \mathbb{R}}^1 (m_w) - E_w(\exp_v(\mathscr{L}_w)) \big)$$

$$\text{and} \quad T\Omega^{\mathrm{loc}}(L/K, 1) := \mathscr{E}_{L/K} - \delta_{L/K}(\mathscr{L}) - \sum_{v \in S} I_G(v, \mathscr{L})$$

in $K_0(\mathbb{Z}[G], \mathbb{R})$. One can show that $T\Omega^{\mathrm{loc}}(L/K, 1)$ is independent of the choices of S and $\mathscr{L}$ (cf. [4, Rem. 4.2]). By [4, Prop. 3.4]) we have $T\Omega^{\mathrm{loc}}(L/K, 1) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ and we can state the conjecture as follows.

Conjecture 16 (Global epsilon constant conjecture). *For every finite Galois extension L/K of number fields the element $T\Omega^{\mathrm{loc}}(L/K, 1)$ is zero in $K_0(\mathbb{Z}[G], \mathbb{Q})$. We denote this conjecture by* $\mathrm{EPS}(L/K)$.

This conjecture has been proved for tamely ramified extensions ([4, Cor. 7.7]), for abelian extensions $L/\mathbb{Q}$ (see the proof of our Corollary 3), for all S_3-extensions $L/\mathbb{Q}$ ([9]), and finally, for certain infinite families of dihedral and quaternion extensions ([8]). Moreover, the global conjecture $\mathrm{EPS}(L/K)$ is known to be valid modulo the subgroup $K_0(\mathbb{Z}[G], \mathbb{Q})_{\mathrm{tor}}$, i.e., $T\Omega^{\mathrm{loc}}(L/K, 1) \in K_0(\mathbb{Z}[G], \mathbb{Q})_{\mathrm{tor}}$ (see [4, Cor. 6.3]).

We write $\mathrm{EPS}_p(L/K)$ for the projection of the conjecture onto $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ via the decomposition (9). We immediately obtain

Corollary 17. *The global conjecture $\mathrm{EPS}(L/K)$ is valid if and only if its p-part $\mathrm{EPS}_p(L/K)$ is valid for all primes p.*

3.2. **The local epsilon constant conjecture.** We will now describe a related conjecture for local Galois extensions L_w/K_v over $\mathbb{Q}_p$, which was formulated by Breuning in [8], and we will see how it refines the global conjectures $\mathrm{EPS}(L/K)$ and $\mathrm{EPS}_p(L/K)$. The equivariant global epsilon function of L/K can be written as a product of equivariant local epsilon functions related to its completions L_w/K_v. Their value at zero is called the equivariant local epsilon constant and the local conjecture describes it in terms of algebraic elements of the extension L_w/K_v. Here we refer to [8] for details.

Let $\mathbb{C}_p$ denote the completion of an algebraic closure $\mathbb{Q}_p^c$ of $\mathbb{Q}_p$. Every character χ of $G_w = \mathrm{Gal}(L_w/K_v)$ can be viewed as a character of $\mathrm{Gal}(\mathbb{Q}_p^c/K_v)$. The local

Galois Gauss sum from [27, Chp. II, § 4] associated with the induced character $\mathrm{i}_{K_v}^{\mathbb{Q}_p}\chi$ of $\mathrm{Gal}(\mathbb{Q}_p^c/\mathbb{Q}_p)$ will be denoted by $\tau_{L_w/K_v}(\chi) \in \mathbb{C}$ and we set

$$\tau_{L_w/K_v} := \left(\tau_{L_w/K_v}(\chi)\right)_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G_w)} \in \mathrm{Z}(\mathbb{C}[G_w])^{\times}.$$

The choice of an embedding $\iota \colon \mathbb{C} \to \mathbb{C}_p$ induces a map $\mathrm{Z}(\mathbb{C}[G_w])^{\times} \to \mathrm{Z}(\mathbb{C}_p[G_w])^{\times}$ and we obtain the *equivariant local epsilon constant*

$$T_{L_w/K_v} := \widehat{\partial}_{G_w,\mathbb{C}_p}^1(\iota(\tau_{L_w/K_v})) \in K_0(\mathbb{Z}_p[G_w],\mathbb{C}_p).$$

As in the global case one chooses a full projective $\mathbb{Z}_p[G_w]$-sublattice $\mathscr{L}_w$ of $\mathcal{O}_{L_w}$ upon which the exponential function is well-defined. Similarly one defines the *equivariant local discriminant* in $K_0(\mathbb{Z}_p[G_w],\mathbb{C}_p)$ by $\delta_{L_w/K_v}(\mathscr{L}_w) = [\mathscr{L}_w, \rho_{L_w}, H_{L_w}]$, where $H_{L_w} = \bigoplus_{\sigma \in \Sigma(L_w)} \mathbb{Z}_p$ and ρ_{L_w} is the isomorphism $\mathscr{L}_w \otimes_{\mathbb{Z}_p} \mathbb{C}_p \to H_{L_w} \otimes_{\mathbb{Z}_p} \mathbb{C}_p$, $l \otimes z \mapsto (\sigma(l)z)_{\sigma \in \Sigma(L_w)}$. Here $\Sigma(L_w)$ denotes the set of embeddings $L_w \hookrightarrow \mathbb{C}_p$. There is an explicit description of $\delta_{L_w/K_v}(\mathscr{L}_w)$ in [3, § 4.2.5] which we will recall in §5.3.

We write $E_w(\exp_v(\mathscr{L}_w))_p$ for the projection of the Euler characteristic $E_w(\exp_v(\mathscr{L}_w))$ onto $K_0(\mathbb{Z}_p[G_w],\mathbb{Q}_p)$ by (9). The difference $C_{L_w/K_v} := E_w(\exp_v(\mathscr{L}_w))_p - \delta_{L_w/K_v}(\mathscr{L}_w)$ is independent of $\mathscr{L}_w$ by [8, Prop. 2.6] and is called the *cohomological term* of L_w/K_v.

To state the local conjecture we also need the *unramified term* U_{L_w/K_v}. It is the unique element in $K_0(\mathbb{Z}_p[G_w],\mathbb{C}_p)$ which satisfies the Galois invariance property [8, Prop. 2.12 b)] and is mapped to zero by the scalar extension map $K_0(\mathbb{Z}_p[G_w],\mathbb{Q}_p) \to K_0(\mathcal{O}_p^t[G_w],\mathbb{C}_p)$ where $\mathcal{O}_p^t$ is the ring of integers of the maximal tamely ramified extension of $\mathbb{Q}_p$ in $\mathbb{C}_p$. The proof of its existence in [8, Prop. 2.12] includes an explicit description of U_{L_w/K_v}, which we will also recall in §5.3.

Conjecture 18 (Local epsilon constant conjecture). *For every Galois extension L_w/K_v of local fields over $\mathbb{Q}_p$ the element*

$$R_{L_w/K_v} := T_{L_w/K_v} + C_{L_w/K_v} + U_{L_w/K_v} - \widehat{\partial}_{G_w,\mathbb{C}_p}^1(m_w)$$

is zero in $K_0(\mathbb{Z}_p[G_w],\mathbb{C}_p)$. We denote this conjecture by $\mathrm{EPS}^{\mathrm{loc}}(L_w/K_v)$.

This conjecture has been proved in [8] for tamely ramified extensions, for abelian extensions $M/\mathbb{Q}_p$ with $p \neq 2$, for all S_3-extensions of $\mathbb{Q}_p$ (p arbitrary), and for certain other special cases. Actually some of the results on the global conjecture were obtained by the local conjecture which can be regarded as a refinement of the p-part of the global conjecture.

Theorem 19 (Local-global principle). *One has the equality*

$$T\Omega^{\mathrm{loc}}(L/K,1)_p = \sum_{v|p} \mathrm{i}_{G_w}^G(R_{L_w/K_v})$$

in $K_0(\mathbb{Z}_p[G],\mathbb{Q}_p)$ and one can deduce:

(i) $\mathrm{EPS}^{\mathrm{loc}}(E/F)$ for all $E/F/\mathbb{Q}_p \Rightarrow \mathrm{EPS}_p(L/K)$ for all $L/K/\mathbb{Q}$,

(ii) if $p \neq 2$: $\mathrm{EPS}_p(L/K)$ for all $L/K/\mathbb{Q} \Rightarrow \mathrm{EPS}^{\mathrm{loc}}(E/F)$ for all $E/F/\mathbb{Q}_p$, and

(iii) for fixed $L/K/\mathbb{Q}$ and p: $\mathrm{EPS}^{\mathrm{loc}}(L_w/K_v)$ for all $w|v|p \Rightarrow \mathrm{EPS}_p(L/K)$.

Proof. [8, Thm. 4.1, Cor. 4.2 and Thm. 4.3].   □

As a consequence, for $p \neq 2$, parts (i) and (ii) imply the equivalence of the local conjecture for extensions of $\mathbb{Q}_p$ and the p-part of the global conjecture.

3.3. **An algorithm.** We recall the functorial properties of the global and local epsilon constant conjectures.

Proposition 20 (Functorial property)**.** *For a Galois extension L/K of number fields with intermediate field F/K and a local Galois extension M/N over $\mathbb{Q}_p$ with intermediate field E/N one has:*

(i) $\mathrm{EPS}(L/K) \Rightarrow \mathrm{EPS}(L/F)$ *and* $\mathrm{EPS}(L/K) \Rightarrow \mathrm{EPS}(F/K)$ *if F/K is Galois.*
(ii) $\mathrm{EPS}^{\mathrm{loc}}(M/N) \Rightarrow \mathrm{EPS}^{\mathrm{loc}}(M/E)$ *and* $\mathrm{EPS}^{\mathrm{loc}}(M/N) \Rightarrow \mathrm{EPS}^{\mathrm{loc}}(E/N)$ *if E/N is Galois.*

Proof. [4, Thm. 6.1] and [8, Prop. 3.3]. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

The functorial properties together with the known results mentioned so far imply the following corollary.

Corollary 21. *Let $n \in \mathbb{N}$ be a fixed integer. Then the local epsilon constant conjecture $\mathrm{EPS}^{\mathrm{loc}}(M/\mathbb{Q}_p)$ for all extensions $M/\mathbb{Q}_p$ of degree $[M : \mathbb{Q}_p] \leq n$ with $p \leq n$ implies the global epsilon constant conjecture $\mathrm{EPS}(F/K)$ for all Galois extensions F/K where F can be embeded into a Galois extension $L/\mathbb{Q}$ of degree $[L : \mathbb{Q}] \leq n$.*

Proof. All extensions below are assumed to be Galois. We conclude

$$
\begin{aligned}
& \mathrm{EPS}^{\mathrm{loc}}(M/\mathbb{Q}_p) && \forall [M : \mathbb{Q}_p] \leq n, p \leq n && \\
\Rightarrow\ & \mathrm{EPS}^{\mathrm{loc}}(M/\mathbb{Q}_p) && \forall [M : \mathbb{Q}_p] \leq n, \forall p && (\text{since } \mathrm{EPS}^{\mathrm{loc}}(M/\mathbb{Q}_p) \text{ is} \\
& && && \text{valid for tame extensions}) \\
\Rightarrow\ & \mathrm{EPS}_p(L/\mathbb{Q}) && \forall [L : \mathbb{Q}] \leq n, \forall p && (\text{by Theorem 19 (iii)}) \\
\Rightarrow\ & \mathrm{EPS}(L/\mathbb{Q}) && \forall [L : \mathbb{Q}] \leq n && (\text{by decomposition (9)}) \\
\Rightarrow\ & \mathrm{EPS}(F/K) && \forall F \subseteq L, [L : \mathbb{Q}] \leq n && (\text{by Proposition 20})
\end{aligned}
$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

It is well-known that for fixed p and n there are only finitely many Galois extensions $M/\mathbb{Q}_p$ with degree $[M : \mathbb{Q}_p] = n$. So the local conjecture for finitely many extensions implies the global conjecture for an infinite number of extensions. And these finitely many local extensions can be handled algorithmically:

(1) For a fixed positive integer n, compute for all $p \leq n$ all local Galois extensions of $\mathbb{Q}_p$ of degree $\leq n$. This can be done using an algorithm due to Pauli and Roblot [30] which performs well enough up to degree 15. However, we were not able to compute all local extensions of degree 16 of $\mathbb{Q}_2$.
(2) For every local extension $M/\mathbb{Q}_p$, find a global Galois extension L/K of number fields with places $w|v$, such that $L_w = M$, $K_v = \mathbb{Q}_p$ and $[L : K] = [M : \mathbb{Q}_p]$. Such an extensions L/K is called a *global representation* for $M/\mathbb{Q}_p$ and is needed to do exact computations in step (3).
(3) Apply the algorithm of Breuning and the first named author [3] to prove or disprove the local epsilon constant conjecture for these extensions.

In the next section we will discuss how step (2) can be handled. Afterwards, we recall the algorithm of [3], and finally, we present our algorithmic results and their consequences.

4. Global representations of local Galois extensions

To do exact computations for a fixed Galois extension $M/\mathbb{Q}_p$ in the algorithm of Breuning and the first named author, we will need a global Galois extension L/K of number fields with corresponding primes $\mathfrak{P}|\mathfrak{p}$ for which $K_{\mathfrak{p}} = \mathbb{Q}_p$ and $L_{\mathfrak{P}} = M$. Such an extension L/K will be called global representation for $M/\mathbb{Q}_p$ and is denoted by $(L, \mathfrak{P})/(K, \mathfrak{p})$.

The proof of the existence of such a global representation involves the Galois closure of a number field [3, Lem. 2.1 and 2.2], but for computational reasons we need a representation which has small degree over $\mathbb{Q}$, or even better, with $K = \mathbb{Q}$.

Henniart shows in [21] that a global representation L/K for the local extension $M/\mathbb{Q}_p$ exists with $K = \mathbb{Q}$ if $p \neq 2$. And if $p = 2$, there exists a global representation with K quadratic over $\mathbb{Q}$. Unfortunately, it is not clear how to find these small representations algorithmically. We therefore present some heuristics.

4.1. **Search database of Klüners and Malle.** The database of Klüners and Malle [25] contains polynomials generating Galois extensions of $\mathbb{Q}$ for all subgroups G of permutation groups S_n up to degree $n = 15$. In particular, the database contains polynomials for all Galois groups of order $n \leq 15$. Among those one will often find a polynomial generating a global representation for $M/\mathbb{Q}_p$, if $[M : \mathbb{Q}_p] \leq 15$.

4.2. **Parametric polynomials.** Here we consider polynomials $f \in K(t_1, \ldots, t_n)[x]$ with indeterminates t_i over a field K. Such a polynomial f is said to be *parametric* for a given group G, if the splitting field L of f is a Galois extension of $K(t_1, \ldots, t_n)$ with group isomorphic to G and, moreover, if for every Galois extension N/K with $\mathrm{Gal}(N/K) \simeq G$ there exist parameters $\alpha_1, \ldots, \alpha_n \in K$ such that the splitting field of $f(\alpha_1, \ldots, \alpha_n)[x] \in K[x]$ is isomorphic to N. Since K is countable, one can systematically enumerate those polynomials f and one will eventually find a polynomial whose splitting field is a global representation for M (provided it exists). In our applications, we could find such a polynomial f by randomly testing different values for the indeterminates t_i.

The book [23] by Jensen et. al. contains parametric polynomials (or methods to construct them) for a lot of groups. In particular, it contains polynomials for all non-abelian groups of order ≤ 15, except for the generalized quaternion group Q_{12} of order 12. However, there do not exist parametric polynomials for all groups. The smallest group for which the non-existence is proved is the cyclic group of order 8 [23, § 2.6].

4.3. **Class field theory.** As a last heuristic, we will use class field theory to construct abelian extensions with prescribed ramification.[3] A discussion of class field theoretic algorithms implemented in Magma is given by Fieker in [18]. For the general theory we refer the reader to [28, Ch. VI].

If L/K denotes an abelian extension of number fields with conductor $\mathfrak{f}$, then $\mathfrak{p}|\mathfrak{f}$ if and only if $\mathfrak{p}$ is ramified in L/K and, moreover, $\mathfrak{p}^2|\mathfrak{f}$ if and only if $\mathfrak{p}$ is wildly ramified in L/K, cf. [18, § 2.4, p. 44].

One can therefore possibly find abelian extensions of K with prescribed ramification at certain places by choosing an appropriate modulus $\mathfrak{f}$, constructing the

---

[3]Thanks to Jürgen Klüners for suggesting the application of this method.

corresponding ray class field, and computing suitable subfields of the requested degree.

4.4. **Global representations for extensions up to degree 15.** Let $M/\mathbb{Q}_p$ be a Galois extension of local fields with group G. For the computation of the unramified characteristic (see (14)) we will also have to consider the unramified extension N_f of $\mathbb{Q}_p$ of degree $f = \exp(G^{\mathrm{ab}})$, where f denotes the exponent of the abelianization G^{ab} of G. Note that for Algorithm 15 we do not need global representations of the fields used in the algorithm.

Since the local conjecture is known to be valid for tamely ramified extensions and abelian extensions of $\mathbb{Q}_p$, $p \neq 2$, it suffices to discuss the performance of the heuristic methods in the following cases:

(a) wildly ramified extensions M of $\mathbb{Q}_p$ with non-abelian Galois group G for all primes p,
(b) wildly ramified extensions M of $\mathbb{Q}_2$, with abelian Galois group G, and
(c) unramified extensions of $\mathbb{Q}_p$ of degree $f = \exp(G^{\mathrm{ab}})$ for all primes p.

In all of these cases we restrict to extensions of degree ≤ 15 since for degree 16 we cannot compute all extensions of $\mathbb{Q}_2$. The hypothesis of wild ramification implies that we only have to consider primes $p = 2, 3, 5$ and 7. The primes 11 and 13 are not considered because they can only occur (up to degree ≤ 15) in abelian extensions of degree 11 and 13, for which both the local and global epsilon conjecture is known to be true.

4.4.1. *Case (a).* First consider extensions with *non-abelian* Galois group. For most of the non-abelian wildly-ramified local extensions we found polynomials of the appropriate degree in the database [25] generating a global representation. In fact, there were just three D_4–extensions of $\mathbb{Q}_2$ and three D_7–extensions of $\mathbb{Q}_7$ not being represented by any polynomial (of degree 8 or 14 respectively) in this database.

By [23, Cor. 2.2.8] every D_4–extension of $\mathbb{Q}$ is the splitting field of a polynomial $f(x) = x^4 - 2stx^2 + s^2t(t-1) \in \mathbb{Q}[x]$ with suitable $s, t \in \mathbb{Q}$. Experimenting with small integers s and t and computing the splitting field of f quickly provides global representations for all D_4–extensions of $\mathbb{Q}_2$.

Finally, we used class field theory to construct global Galois representations for the three non-isomorphic D_7–extensions of $\mathbb{Q}_7$: by taking quadratic extensions K of $\mathbb{Q}$ which are non-split at $p = 7$ and computing all C_7–extensions of K which are subfields of the ray class field $K^{\mathfrak{m}}$, $\mathfrak{m} = 49\mathcal{O}_K$, one finds D_7–extensions where $p = 7$ is ramified with ramification index 7 or 14 and where p does not split. Experimenting with different fields K as above one finds global Galois representations for all three D_7–extensions of $\mathbb{Q}_7$.

This completes the construction of global representations for all non-abelian wildly ramified local extensions of $\mathbb{Q}_p$, $p = 2, 3, 5, 7$, up to degree 15.

4.4.2. *Case (b).* Using the database [25] we can again find polynomials for all abelian extensions over $\mathbb{Q}_2$ of degree ≤ 7. For extensions of higher degree, the heuristics were not as successful. But to obtain a *global* result up to degree 15, it is sufficient to consider abelian extension of $\mathbb{Q}_2$ of degree ≤ 7 (see the proof of Corollary 3).

4.4.3. *Case (c)*. For each of the pairs $(L/\mathbb{Q}, p)$ with Galois group G constructed in cases (a) and (b), Algorithm 22 also needs a extension N of $\mathbb{Q}$ which is unramified and non-split at p and is of degree $f = \exp(G^{\mathrm{ab}})$.

For non-abelian extensions of degree ≤ 15 the maximum degree of N can easily be determined to be $f = 4$. And in the abelian case, we need unramified extensions of degree ≤ 7.

Most of these unramified extensions can be constructed as a subfield of a cyclotomic field $\mathbb{Q}(\zeta_n)$ generated by an n-th root of unity ζ_n. In the other cases one finds global representations using the database [25].

A complete list of polynomials which were found using these heuristics is contained in the second named author's dissertation [17].

5. Algorithmic proof of the local epsilon constant conjecture

We briefly recall the algorithm described by Breuning and the first named author in [3, §4.2]. There the authors explain in detail how each of the terms in the local conjecture can be computed and how this results in an algorithmic proof of the local conjecture for a given local Galois extension L_w/K_v. Since by the functorial properties of the local conjecture one has $\mathrm{EPS}^{\mathrm{loc}}(L_w/\mathbb{Q}_p) \Rightarrow \mathrm{EPS}^{\mathrm{loc}}(L_w/K_v)$, we will only consider extensions $L_w/\mathbb{Q}_p$.

For the rest of this section, fix the Galois extensions L/K and N/K and a prime $\mathfrak{p}$ of K as the input of the algorithm. We assume that L/K (resp. N/K) is a global representation of $L_w/\mathbb{Q}_p$ (resp. the unramified extension of $\mathbb{Q}_p$ of degree $f := \exp(G^{\mathrm{ab}})$). For simplicity, the unique prime ideal above $\mathfrak{p}$ in the fields L, N, or any subextension of L/K will also be denoted by $\mathfrak{p}$. If it is necessary to avoid confusion, we will write $\mathfrak{p}_K$, $\mathfrak{p}_L$ and $\mathfrak{p}_N$. Furthermore, we will identify the ideals $\mathfrak{p}_L | \mathfrak{p}_K$ with places $w|v$ of L and K, respectively, such that $L_w = L_{\mathfrak{p}}$ and $K_v = K_{\mathfrak{p}}$. We write $e_{w|v} = e(L_w/\mathbb{Q}_p)$ for the ramification index. Recall that for a finite place w of L we write $w : L^\times \longrightarrow \mathbb{Z}$ for the normalized valuation associated with w (or $\mathfrak{p}_L$).

We will first recall the complete algorithm of [3] and then explain each step. In step 2 we will construct a big number field E which, among other things, is a splitting field for G. Hence the Wedderburn decomposition of $E[G]$ induces a canonical isomorphism $Z(E[G])^\times \simeq \prod_{\chi \in \mathrm{Irr}(G)} E^\times$.

Algorithm 22 (Proof of the local epsilon constant conjecture)**.**

Input: An extension $(L, \mathfrak{P})/(K, \mathfrak{p})$ with $K_{\mathfrak{p}} = \mathbb{Q}_p$ in which L/K is Galois with group G and a Galois extension N/K of degree $\exp(G^{\mathrm{ab}})$ in which $\mathfrak{p}$ is non-split and unramified.

Output: True if $\mathrm{EPS}^{\mathrm{loc}}(L_{\mathfrak{P}}/\mathbb{Q}_p)$ was successfully checked.

(Construction of the coefficient field)

1 Compute all characters χ of G and use Brauer induction to find an integer t such that the Galois Gauss sums can be computed in $\mathbb{Q}(\zeta_m, \zeta_{p^t})$, $m = \exp(G)$ (cf. [3, Rem. 2.7]).

2 Construct the composite field E of L, N and $\mathbb{Q}(\zeta_m, \zeta_{p^t})$ and fix a complex embedding $\iota : E \hookrightarrow \mathbb{C}$ and a prime ideal $\mathfrak{Q}$ of E above p.

(Computation of cohomological term)

3 Let $\theta \in L$ be a generator of a normal basis of L/K with $w(\theta) > \frac{e(L_w/\mathbb{Q}_p)}{p-1}$, define $\mathscr{L} = \mathbb{Z}_p[G]\theta \in \mathcal{O}_{L_w}$ and compute k such that $(\mathfrak{P}\mathcal{O}_{L_w})^k \subseteq \mathscr{L}$ (cf. [3, Sec. 4.2.3]).

4 Compute a cocycle representing the local fundamental class up to precision k in $\hat{H}^2(G, L_w^\times/U_{L_w}^{(k)})$ and its projection onto $\hat{H}^2(G, L_w^\times/\exp_v(\mathscr{L}_w))$ (cf. Algorithm 15).

5 Construct a complex representing this cocycle by [29, p. 115] and compute the Euler characteristic $E_w(\exp_v(\mathscr{L}_w)) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ as in [3, §4.2.4].

(Computation of the terms in $\prod_\chi E^\times$)

6 Compute the correction term $m_{L_\mathfrak{P}/\mathbb{Q}_p} = m_w \in \mathrm{Z}(\mathbb{Q}[G])^\times \subseteq \mathrm{Z}(E[G])^\times \simeq \prod_\chi E^\times$ defined in (11).

7 Compute the element $d_{L_\mathfrak{P}/\mathbb{Q}_p} \in L[G]^\times \subseteq E[G]^\times$ of (13) below, such that $\mathrm{nr}(d_{L_\mathfrak{P}/\mathbb{Q}_p})$ represents the equivariant discriminant $\delta_{L_\mathfrak{P}/\mathbb{Q}_p}(\mathscr{L})$.

8 Compute the element $u_{L_\mathfrak{P}/\mathbb{Q}_p} \in N[G]^\times \subseteq E[G]^\times$ using (14) below, such that $\mathrm{nr}(u_{L_\mathfrak{P}/\mathbb{Q}_p})$ represents the unramified term $U_{L_\mathfrak{P}/\mathbb{Q}_p}$.

9 Use the canonical homomorphism $E[G]^\times \to K_1(E[G])$, the reduced norm map $\mathrm{nr}: K_1(E[G]) \to \mathrm{Z}(E[G])$ and Wedderburn decomposition of $\mathrm{Z}(E[G])$ to represent these two terms in $\prod_\chi E^\times$.

10 Compute the equivariant epsilon constant $\tau_{L_\mathfrak{P}/\mathbb{Q}_p} \in \prod_\chi \mathbb{Q}(\zeta_{p^t}, \zeta_m)^\times \subseteq \prod_\chi E^\times$ via Galois Gauss sums.

(Computations in relative K-groups)

11 Read $E_w(\exp_v(\mathscr{L}_w))$ and the tuples from above as elements in $K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$.

12 Compute the sum $R_{L_\mathfrak{P}/\mathbb{Q}_p} \in K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$ of the resulting elements.

Return: True if $R_{L_\mathfrak{P}/\mathbb{Q}_p}$ is zero, and false otherwise.

Proof. [3, §4.2]. $\square$

All steps were explained in detail in [3]. However, there were some problems that needed further improvements to give a practical algorithm. Firstly, the existence of global representations is due to a theoretical argument by Henniart in [21] which we still cannot make explicit. For the construction of these representations we gave some heuristics in the previous section which we successfully applied to extensions of small degree. Secondly, the computation of local fundamental classes as presented in [3, §2.4] is not very efficient and is significantly improved by Algorithm 15. And thirdly, Wilson and the first named author [5] developed new algorithms for computations in the relative algebraic K-groups $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$.

Below we will discuss each part of the algorithm separately.

5.1. Constructing the coefficient field.

As explained in [3, §4.2.2] we need to construct a global field E, in which all the computations take place.

For the computation of the unramified term, we will need a cyclic extension N/K which is unramified and non-split at $\mathfrak{p}$.

Another extension involved is $\mathbb{Q}(\zeta_m, \zeta_{p^t})$, where m is the exponent of G and t is computed as described below. By Brauer's theorem [32, Sec. 12.3, Theorem 24] the field $\mathbb{Q}(\zeta_m)$ is a splitting field for all irreducible characters of G and therefore

contains all character values. The root of unity ζ_{p^t} is used to represent Galois Gauss sums and the integer t is determined as follows.

For each character χ of G one computes subgroups H, linear characters ϕ of H, and coefficients $c_{(H,\phi)} \in \mathbb{Z}$ such that $\chi - \chi(1)1_G = \sum_{(H,\phi)} c_{(H,\phi)} \mathrm{ind}_H^G(\phi - 1_H)$. Such a relation exists by Brauer's induction theorem, cf. [3, § 2.5]. If $\mathfrak{f}(\phi)$ denotes the *Artin conductor* of ϕ and e the ramification index of $(L^H)_{\mathfrak{p}}/\mathbb{Q}_p$, then t must satisfy $t \geq v_{\mathfrak{p}}(\mathfrak{f}(\phi))/e$ for all pairs (H,ϕ) and all χ. This choice of t will allow to compute the epsilon constants as elements of $\mathbb{Q}(\zeta_m, \zeta_{p^t})$, see also [3, Rem. 2.7].

The composite field of the three fields L, N and $\mathbb{Q}(\zeta_m, \zeta_{p^t})$ is denoted by E, giving the following situation:

$$(12) \qquad \begin{array}{ccc} & E & \\ & \diagup \mid \diagdown & \\ \mathbb{Q}(\zeta_m, \zeta_{p^t}) & L & N \\ & \diagdown \mid \diagup & \\ & \mathbb{Q} & \end{array}$$

We then fix a complex embedding $\iota : E \hookrightarrow \mathbb{C}$. The embedding ι is essential because some of the terms in the conjecture depend on the particular choice of the embedding: for example, the definition of the standard additive character below, see also [3, § 2.5]. So once we compute an algebraic element representing this value, we have to maintain its embedding into $\mathbb{C}$. Since we still try to avoid computations in such a big field E, this implies the following: whenever we do calculations in a subfield $F \subseteq E$, we have to choose embeddings $\iota_1 : F \hookrightarrow \mathbb{C}$ and $\iota_2 : F \hookrightarrow E$ such that the diagram

$$\begin{array}{ccc} E & \overset{\iota}{\hookrightarrow} & \mathbb{C} \\ \iota_2 \uparrow & \nearrow \iota_1 & \\ F & & \end{array}$$

is commutative, i.e. $\iota_1 = \iota \circ \iota_2$.

We also fix a prime ideal $\mathfrak{Q}$ of E above p and an embedding $E \hookrightarrow E_{\mathfrak{Q}}$ such that $E \hookrightarrow E_{\mathfrak{Q}} \hookrightarrow \mathbb{C}_p$ and $E \overset{\iota}{\hookrightarrow} \mathbb{C} \hookrightarrow \mathbb{C}_p$ coincide. Then all the invariants appearing in the conjecture lie in the subgroup $K_0(\mathbb{Z}_p[G], E_{\mathfrak{Q}})$ of $K_0(\mathbb{Z}_p[G], \mathbb{C}_p)$ and they can therefore be represented by tuples in $Z(E_{\mathfrak{Q}}[G]) \simeq \prod_{\chi \in \mathrm{Irr}(G)} E_{\mathfrak{Q}}^{\times}$. In fact, we will see that all these elements are already represented by elements in $\prod_{\chi \in \mathrm{Irr}(G)} E^{\times}$ and can therefore be computed globally.

5.2. Computation of the cohomological term.
The lattice $\mathscr{L} = \mathbb{Z}[G]\theta \subseteq \mathcal{O}_L$ is computed using a normal basis element θ for L/K and the integer k for which $\mathfrak{p}^k \subseteq \mathscr{L}$ can then be found experimentally. The details are explained in [3, § 4.2.3]).

We compute a cocycle $\gamma \in Z^2(G, L_w^{\times}/U_{L_w}^{(k)})$ representing the local fundamental class up to precision k using Algorithm 15 and then the projection of γ onto $Z^2(G, L_w^{\times}/\exp_v(\mathscr{L}_w))$. Note that the quotient $L_w^f := L_w^{\times}/\exp_v(\mathscr{L}_w)$ can be computed globally, cf. [2, Rem. 3.6]. We can then construct the corresponding complex $P_w = [L_w^f(\gamma) \to \mathbb{Z}[G]]$ using the splitting module $L_w^f(\gamma)$ of [29, Chp. III, § 1, p. 115] and the Euler characteristic $E_w(\exp_v(\mathscr{L}_w)) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ using the explicit construction of [3, § 4.2.4].

5.3. Computation of the terms in $\prod_\chi E^\times$.

The correction term m_w is explicitly defined as a tuple in $\prod_\chi E^\times$ by (11). For the equivariant discriminant and the unramified term we recall the following formulas from [3, §§ 4.2.5 and 4.2.7]:

$$(13) \qquad d_{L_w/\mathbb{Q}_p} = \sum_{\tau \in G} \tau(\theta)\tau^{-1} \in L[G]^\times \subseteq E[G]^\times,$$

$$(14) \qquad u_{L_w/\mathbb{Q}_p} = \sum_{i=0}^{s-1} \varphi_{\mathfrak{p}}^i(\xi)\sigma^{-i} \in N[G]^\times \subseteq E[G]^\times.$$

We explain the notation in the latter equation. The element $\sigma \in G$ is a lift of the local norm residue symbol $(p, F_{\mathfrak{p}}/K_{\mathfrak{p}}) \in \mathrm{Gal}(F_{\mathfrak{p}}/K_{\mathfrak{p}}) \simeq \mathrm{Gal}(F/K)$ with F being the maximal abelian subextension in L/K. An algorithm to compute local norm residue symbols is described in [1, Alg. 3.1]. If s denotes the order of σ and $N_1 \subseteq N$ is the subextension of N/K of degree $[N_1 : K] = s$, then we denote the Frobenius automorphism of N_1/K with respect to $\mathfrak{p}$ by $\varphi_{\mathfrak{p}} \in \mathrm{Gal}(N_1/K)$, and finally, $\xi \in \mathcal{O}_{N_1}$ is an integral normal basis element for the extension $(N_1)_{\mathfrak{p}}/K_{\mathfrak{p}}$.

By [3, Sec. 4.2.5 and 4.2.7] the equivariant discriminant and the unramified term are represented by $\mathrm{nr}(d_{L_w/\mathbb{Q}_p})$ and $\mathrm{nr}(u_{L_w/\mathbb{Q}_p})$ as elements in $\mathrm{Z}(E[G])^\times \simeq \prod_{\chi \in \mathrm{Irr}(G)} E^\times$. Recall that reduced norms can be computed by one of the algorithms described in [3, Sec. 3.2] or [5, Sec. 3.3].

The equivariant epsilon constant $\tau_{L_{\mathfrak{p}}/\mathbb{Q}_p}$ is computed in $\prod_\chi E^\times$ by *local Galois Gauss sums* as follows.

For each χ, we have already computed subgroups H of G, linear characters ϕ of H, and coefficients $c_{(H,\phi)} \in \mathbb{Z}$ such that $\chi - \chi(1)1_G = \sum_{(H,\phi)} c_{(H,\phi)} \mathrm{ind}_H^G(\phi - 1_H)$. Since Galois Gauss sums are additive, inductive in degree 0, and equal to 1 for the trivial character, we obtain

$$\tau(L_{\mathfrak{p}}/\mathbb{Q}_p, \chi) = \prod_{(H,\phi)} \tau\big((L^{\mathrm{ker}(\phi)})_{\mathfrak{p}}/(L^H)_{\mathfrak{p}}, \phi\big)^{c_{(H,\phi)}} \in \mathbb{Q}(\zeta_m, \zeta_{p^t}) \subseteq E^\times.$$

For the completions at $\mathfrak{p}$ of the abelian extension $M = L^{\mathrm{ker}(\phi)}$ over $N = L^H$, Galois Gauss sums are given by the formula

$$\tau(M_{\mathfrak{p}}/N_{\mathfrak{p}}, \phi) = \sum_x \phi\Big(\Big(\frac{x}{c}, M_{\mathfrak{p}}/N_{\mathfrak{p}}\Big)\Big) \psi_{N_{\mathfrak{p}}}\Big(\frac{x}{c}\Big) \in \mathbb{Q}(\zeta_m, \zeta_{p^t}) \subseteq E^\times$$

where x runs through a system of representatives of $\mathcal{O}_{N_{\mathfrak{p}}}^\times/U_{N_{\mathfrak{p}}}^{(s)} \simeq (\mathcal{O}_N/\mathfrak{p}^s)^\times$, s is the valuation $v_{\mathfrak{p}}(\mathfrak{f}(\phi))$ of the *Artin conductor* $\mathfrak{f}(\phi)$ of ϕ, $c \in N$ generates the ideal $\mathfrak{f}(\phi)\mathcal{D}_{N_{\mathfrak{p}}}$, where $\mathcal{D}_{N_{\mathfrak{p}}}$ denotes the *different* of the extension $N_{\mathfrak{p}}/\mathbb{Q}_p$, and $\psi_{N_{\mathfrak{p}}}$ is the *standard additive character* of $N_{\mathfrak{p}}$.

The above formulas allow the construction of the equivariant epsilon constant as a tuple $\tau_{L_{\mathfrak{p}}/\mathbb{Q}_p} = \big(\tau(L_{\mathfrak{p}}/\mathbb{Q}_p, \chi)\big)_\chi \in \prod_\chi E^\times$. For details see [3, § 2.5].

5.3.1. *Computations in relative K-groups.* In the following we have to combine the computations of the previous steps to find $R_{L_{\mathfrak{p}}/\mathbb{Q}_p}$ and show that its sum represents zero in $K_0(\mathbb{Z}_p[G], E_{\mathfrak{Q}})$. In [5] Wilson and the first named author describe the relative K-group as an abstract group. Using their methods it will be clear how to read elements of the form $\widehat{\partial}_{G_w, \mathbb{Q}_p}^1(x)$ for $x \in \prod_\chi E^\times$ and triples $[A, \theta, B]$ in the group $K_0(\mathbb{Z}_p[G], E_{\mathfrak{Q}})$.

We will recall the algorithms of [5] and — since they are not yet implemented in full generality — we will discuss a simple modification for special extensions F of $\mathbb{Q}$ which are totally split at the fixed prime p.

First we introduce some more notation: Let K be a number field and G a finite group. Let $\mathrm{Irr}_K(G) = \{\chi_1, \ldots, \chi_r\}$ denote a set of orbit representatives of $\mathrm{Irr}(G)$ modulo the action of $\mathrm{Gal}(K^c/K)$. Then the *Wedderburn decomposition* of $K[G]$ induces a decomposition of its center $C := \mathrm{Z}(K[G])$ into character fields $K_i := K(\chi_i), i = 1, \ldots, r$, so that we have $C = \bigoplus_{i=1}^r K_i$.

Choose a maximal $\mathcal{O}_K$-order $\mathcal{M}$ of $K[G]$ containing $\mathcal{O}_K[G]$ and a two-sided ideal $\mathfrak{f}$ of $\mathcal{M}$ which is contained in $\mathcal{O}_K[G]$ (e.g. $\mathfrak{f} = |G|\,\mathcal{M}$) and define $\mathfrak{g} := \mathcal{O}_C \cap \mathfrak{f}$. Then the decomposition of C similarly splits $\mathcal{M}$ into $\bigoplus_{i=1}^r \mathcal{M}_i$ and the ideals $\mathfrak{f}$ and $\mathfrak{g}$ into ideals $\mathfrak{f}_i$ of $\mathcal{M}_i$ and $\mathfrak{g}_i$ of $\mathcal{O}_{K_i}$. For a prime $\mathfrak{p}$ in $\mathcal{O}_K$, we further write $C_\mathfrak{p}$ for the localization $C_\mathfrak{p} = K_\mathfrak{p} \otimes_\mathbb{Q} C = \bigoplus_{i=1}^r K_\mathfrak{p} \otimes_\mathbb{Q} K_i = \bigoplus_{i=1}^r \bigoplus_{\mathfrak{P}|\mathfrak{p}} (K_i)_\mathfrak{P}$, and $\mathfrak{a}_{i,\mathfrak{p}}$ for the part of an ideal $\mathfrak{a}_i$ of $\mathcal{O}_{K_i}$ above $\mathfrak{p}$.

The reduced norm map induces a homomorphism $\mu_\mathfrak{p} : K_1(\mathcal{O}_{K_\mathfrak{p}}[G]/\mathfrak{f}_\mathfrak{p}) \to \bigoplus_{i=1}^r (\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^\times$ whose cokernel is used in the description of the relative K-group $K_0(\mathcal{O}_{K_\mathfrak{p}}[G], K_\mathfrak{p})$. Then the main algorithmic result of Wilson and the first named author is the following.

Proposition 23. *There are isomorphisms*

$$K_0(\mathcal{O}_{K_\mathfrak{p}}[G], K_\mathfrak{p}) \xrightarrow{\bar{n}} C_\mathfrak{p}^\times / \mathrm{nr}(\mathcal{O}_{K_\mathfrak{p}}[G]^\times) \xrightarrow{\bar{\varphi}} I(C_\mathfrak{p}) \times \mathrm{coker}(\mu_\mathfrak{p}),$$

$\bar{n}$ being the natural isomorphism of [5, Th. 2.2(ii)] and $\bar{\varphi}$ being induced by

$$(15) \qquad
\begin{aligned}
\varphi : \quad C_\mathfrak{p}^\times = \bigoplus_{i=1}^r (K_i)_\mathfrak{p} &\longrightarrow & I(C_\mathfrak{p}) \times \bigoplus_{i=1}^r (\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^\times \\
(\nu_1, \ldots, \nu_r) &\longmapsto & \left(\left(\textstyle\prod_\mathfrak{P} \mathfrak{P}^{v_\mathfrak{P}(\nu_i)} \right)_i, (\bar{\mu}_1, \ldots, \bar{\mu}_r) \right),
\end{aligned}$$

where $\mu_i := \nu_i \prod_\mathfrak{P} \pi_{i,\mathfrak{P}}^{-v_\mathfrak{P}(\nu_i)}$ and $\pi_{i,\mathfrak{P}} \in \mathcal{O}_{K_i}$ are uniformizing elements having valuation 1 at $\mathfrak{P}$ and which are congruent to 1 modulo $\mathfrak{g}_{\mathfrak{P}'}$ for all other primes $\mathfrak{P}'$ above $\mathfrak{p}$ in K_i/K.

Proof. [5, Prop. 2.7]. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Wilson and the first named author describe an algorithm to compute the group $I(C_\mathfrak{p}) \times \mathrm{coker}(\mu_\mathfrak{p})$. From the definition of φ, it is clear how a tuple $\nu = (\nu_i)_i$ of elements with values $\nu_i \in K_i$ represents an element in this group. Furthermore, for every triple $[A, \theta, B] \in K_0(\mathcal{O}_K[G], K)$ with projective $\mathcal{O}_K[G]$-modules A and B and $\theta : A_K \xrightarrow{\cong} B_K$, the algorithm of [5, Sec. 4.1] produces a representative of $[A, \theta, B]$ in $\mathrm{Z}(K[G])^\times$. In this way, we can compute a representative of $E_w(\exp_v(\mathcal{L}_w))$ in $\mathrm{Z}(\mathbb{Q}[G])^\times \subseteq \mathrm{Z}(E[G])^\times \simeq \prod_\chi E^\times$.

In theory, this solves the remaining problems for Algorithm 22. Indeed, since we have representatives of each of the individual terms in $\prod_\chi E^\times$, we can represent $R_{L_w/\mathbb{Q}_p}$ by an element $(a_\chi)_\chi \in \prod_\chi E^\times \subseteq \prod_\chi E_\mathfrak{Q}^\times$. If $F \subseteq E$ denotes the decomposition field of $\mathfrak{Q}$ and $\mathfrak{q} := \mathfrak{Q} \cap F$, then $K_0(\mathcal{O}_{F_\mathfrak{q}}[G], F_\mathfrak{q}) = K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ and $K_0(\mathcal{O}_{F_\mathfrak{q}}[G], E_\mathfrak{Q}) = K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$. Since $R_{L_w/\mathbb{Q}_p} \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p) \subseteq K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$ it follows that $\omega(a_\chi) = a_{\omega \circ \chi}$ for all $\chi \in \mathrm{Irr}(G)$ and all $\omega \in \mathrm{Gal}(E/F)$ (see [3, bottom of page 788]). In other words, $a_\chi \in F(\chi)$ for each $\chi \in \mathrm{Irr}(G)$ and $\sigma(a_\chi) = a_{\sigma \circ \chi}$ for all $\sigma \in \mathrm{Gal}(F(\chi)/F)$. So the natural approach using the work of [5] would be

to work with the $\mathfrak{q}$-part of $K_0(\mathcal{O}_F[G], F)$. But in practice, unfortunately, this has only been implemented in MAGMA for $K = \mathbb{Q}$ and $\mathfrak{p} = p\mathbb{Z}$.

The field F is an extension of $\mathbb{Q}$ which is totally split at p. We obviously have $F_{\mathfrak{q}} = \mathbb{Q}_p$ and $K_0(\mathbb{Z}_p[G], F_{\mathfrak{q}}) \simeq K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$. If F satisfies certain conditions, this isomorphism of relative K-groups is *canonically* given by isomorphisms on the ideal part $I(C_{\mathfrak{p}})$ and the cokernel part $\mathrm{coker}(\mu_{\mathfrak{p}})$.

Proposition 24. *Let $K = \mathbb{Q}$ and $\mathfrak{p} = p\mathbb{Z}$. Let $F/\mathbb{Q}$ be a Galois extension which is totally split at p and for which $F \cap K_i = \mathbb{Q}$ for all $i = 1, \ldots, r$. Let $\mathfrak{q}$ be a fixed prime ideal of F above p. Then the following holds:*

(i) The center $C' = \mathrm{Z}(F[G])$ splits into character fields $F_i = FK_i$.

(ii) For every ideal $\mathfrak{P}$ of K_i there is exactly one prime ideal $\mathfrak{Q}$ in F_i lying above $\mathfrak{P}$ and $\mathfrak{q}$.

(iii) There are canonical isomorphisms

$$I(C_{\mathfrak{p}}) \simeq I(C'_{\mathfrak{q}}) \quad and \quad \bigoplus_{i=1}^{r}(\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^{\times} \simeq \bigoplus_{i=1}^{r}(\mathcal{O}_{F_i}/\mathfrak{g}'_{i,\mathfrak{q}})^{\times}$$

where $\mathfrak{g}' := \mathfrak{g}\mathcal{O}_{C'}$.

(iv) One can use $\mathcal{M}' := \mathcal{O}_F \otimes_{\mathbb{Z}} \mathcal{M}$ and $\mathfrak{f}' := \mathcal{O}_F \otimes_{\mathbb{Z}} \mathfrak{f}$ in order to compute $K_0(\mathcal{O}_{F_{\mathfrak{q}}}[G], F_{\mathfrak{q}})$ as in Proposition 23. Denote the corresponding homomorphisms in (15) by φ' and $\mu'_{\mathfrak{q}}$. If we use the same uniformizing elements for φ and φ', then

$$
\begin{array}{ccc}
C_{\mathfrak{p}}^{\times}/\mathrm{nr}(\mathbb{Z}_p[G]^{\times}) & \xrightarrow{\bar{\varphi}} & I(C_{\mathfrak{p}}) \times \mathrm{coker}(\mu_{\mathfrak{p}}) \\
\downarrow{\simeq} & & \downarrow{\simeq} \\
(C'_{\mathfrak{q}})^{\times}/\mathrm{nr}(\mathcal{O}_{F_{\mathfrak{q}}}[G]^{\times}) & \xrightarrow{\bar{\varphi}'} & I(C'_{\mathfrak{q}}) \times \mathrm{coker}(\mu'_{\mathfrak{q}})
\end{array}
$$

commutes. Here the right hand vertical isomorphism is induced by (iii).

Proof. (i) Since F and K_i are disjoint over $\mathbb{Q}$, one has $\mathrm{Irr}_{\mathbb{Q}}(G) = \mathrm{Irr}_F(G)$ and $F(\chi_i) = FK(\chi_i)$.

(ii) If $\mathfrak{Q}'$ is any prime ideal in F_i above $\mathfrak{p}$ and $\mathfrak{P}' = \mathfrak{Q}' \cap K_i$, $\mathfrak{q}' = \mathfrak{Q}' \cap F$, then the automorphisms τ and σ for which $\tau(\mathfrak{P}') = \mathfrak{P}$ and $\sigma(\mathfrak{q}') = \mathfrak{q}$ define an element $\rho = \sigma \times \tau$ in the Galois group of $F_i/\mathbb{Q}$ and $\mathfrak{Q} = \rho(\mathfrak{Q}')$ is a prime ideal which lies above both $\mathfrak{P}$ and $\mathfrak{q}$. Since $F \cap K_i = \mathbb{Q}$ and $F/\mathbb{Q}$ is totally split at $\mathfrak{p}$, the extension F_i/K_i is also totally split at every prime ideal $\mathfrak{P}'$ above $\mathfrak{p}$. The uniqueness of $\mathfrak{Q}$ therefore follows from degree arguments.

(iii) Let $\mathfrak{P}$ be a prime ideal of K_i and $\mathfrak{Q}$ the prime ideal of F_i which lies above $\mathfrak{q}$ and $\mathfrak{P}$. Then the valuation $v_{\mathfrak{Q}}$ of F_i extends the valuation $v_{\mathfrak{P}}$ of K_i and if we identify each pair $\mathfrak{P}$ and $\mathfrak{Q}$, we get an isomorphism

$$I(C_{\mathfrak{p}}) = \prod_{i=1}^{r}\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{\mathbb{Z}} \simeq \prod_{i=1}^{r}\prod_{\mathfrak{Q}|\mathfrak{q}} \mathfrak{Q}^{\mathbb{Z}} = I(C'_{\mathfrak{q}}).$$

Since $\mathfrak{P} \subset K_i$ is totally split in F_i we have isomorphisms $\mathcal{O}_{K_i}/\mathfrak{P} \simeq \mathcal{O}_{F_i}/\mathfrak{Q}$. The inclusions $\mathcal{O}_{K_i} \subseteq \mathcal{O}_{F_i}$ therefore induce isomorphisms $(\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^{\times} \simeq (\mathcal{O}_{F_i}/\mathfrak{g}'_{i,\mathfrak{q}})^{\times}$.

(iv) Since $\mathfrak{q}|\mathfrak{p}$ is unramified the order $\mathcal{M}'$ is maximal at $\mathfrak{q}$. This implies the first part of (iv). The commutativity follows from straightforward verification. $\square$

5.4. **Further remarks.** 1. As mentioned before, the algorithms of [5] to compute $K_0(\mathbb{Z}_p[G], F_{\mathfrak{q}})$ are just implemented for $F = \mathbb{Q}$. The extension to $F/\mathbb{Q}$ described above will work if F is totally split at p, $F/\mathbb{Q}$ is Galois, and $F \cap \mathbb{Q}(\chi) = \mathbb{Q}$ for all characters χ. The first condition is always true since we want to work with the decomposition field $F \subseteq E$ of $\mathfrak{Q}$, and the latter conditions are valid in all cases we consider in the computational results below.

2. The computation of the prime ideal $\mathfrak{Q}$ in E is a very hard problem when the degree of E gets large. In the last part of Algorithm 22 we will therefore try to replace E by a much smaller field E'. Let $\mathcal{I} := \tau_{L_w/\mathbb{Q}_p} u_{L_w/\mathbb{Q}_p}/(m_w d_{L_w/\mathbb{Q}_p}) \in \prod_\chi E^\times$ be the element combining all the invariants except the cohomological term. So $R_{L_w/K_v} = \widehat{\partial}^1_{G,E_{\mathfrak{Q}}}(\mathcal{I}) + E_w(\exp_v(\mathscr{L}_w))_p$ and since R_{L_w/K_v} and $E_w(\exp_v(\mathscr{L}_w))_p$ are both elements of $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$, the element $\widehat{\partial}^1_{G,E_{\mathfrak{Q}}}(\mathcal{I})$ is also in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$. As in [3, bottom of page 788] we deduce that $\mathcal{I}_\chi \in F(\zeta_m)$ where $m = \exp(G)$ and $F = E^{G_{\mathfrak{Q}}}$ denotes the decomposition field of $\mathfrak{Q}$.

To compute a small field E' without computing the ideal $\mathfrak{Q}$ and its decomposition group itself we proceed as follows: for every χ we compute the minimal polynomial m_χ of $\mathcal{I}_\chi$. Then we compute the composite field E' of the splitting fields of the polynomials m_χ and $\mathbb{Q}(\zeta_m)$. We note that the splitting fields will always be subfields of E. The computation of these fields is also a difficult task, but where this approach could take hours, the computation of $\mathfrak{Q}$ did not succeed in several days.

In the end, E' is a subfield of E such that $\mathcal{I}_\chi, \zeta_m \in E'$. Compute an ideal $\mathfrak{q}'$ of E' above p, denote the decomposition field of $\mathfrak{q}'$ by F, and compute $\mathfrak{q} = \mathcal{O}_F \cap \mathfrak{q}'$. Then it follows from above that $\mathcal{I}_\chi \in F(\zeta_m)$ and $\mathcal{I} = \tau_{L_w/\mathbb{Q}_p} u_{L_w/\mathbb{Q}_p}/(m_w d_{L_w/\mathbb{Q}_p}) \in \prod_\chi F(\zeta_m)^\times$. In our computations, these fields F were at most of degree 4 over $\mathbb{Q}$ and they were always Galois so that we could apply Proposition 24 for the remaining computations in $K_0(\mathbb{Z}_p[G], F_{\mathfrak{q}}) = K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$.

Note that all computations were independent of the choice of the prime ideal $\mathfrak{Q}$ above p because all invariants were actually computed globally. The proof of the conjecture will therefore also be independent of the choice of $\mathfrak{q}'$.

6. Computational results

Algorithm 22 has been implemented in Magma [6] and is bundled with the second author's dissertation [17].It has been tested for various extensions up to degree 20 and the computation time turns out to depend essentially on the degree of the composite field E.

The most complicated extension for which we proved the local epsilon constant conjecture was an extension of degree 10 of $\mathbb{Q}_5$ with Galois group D_5. The composite field E then had degree 200 over $\mathbb{Q}$. The computation of the epsilon constants, which needs an embedding $E \hookrightarrow \mathbb{C}$, already took about 7 hours, but the most time-consuming part (about 6.5 days) of Algorithm 22 was the computation of minimal polynomials and their splitting fields mentioned in the remarks above. The field E' then just had degree 4 over $\mathbb{Q}$ making the remaining computations very fast. The total time needed to prove the local conjecture in this case was about 7 days.[4]

Using the representations obtained in §4 we can prove Theorem 1 algorithmically.

---

[4]All computations were performed with Magma version 2.15-9 on a dual core AMD Opteron machine with 1.8 GHz and 16 GB memory.

Proof of Theorem 1. Since the local conjecture is valid for abelian extensions of $\mathbb{Q}_p$, $p \neq 2$, the only primes to consider are $p = 2, 3, 5, 7$. All local extensions for these primes of degree ≤ 15 that are either non-abelian, or abelian with $p = 2$ and of degree ≤ 6 have been considered in §4.4 and global representations have been found using the heuristics described in §4. Also global representations for the corresponding unramified extensions — which are of degree at most 6 — could be found using the database [25].

For each of those extensions we then continued with Algorithm 22 to prove the local epsilon constant conjecture. Details of the computations can be found in the author's dissertation [17]. This completes the proof of Theorem 1. □

Using some already known results we can also prove:

Corollary 25. *The local epsilon constant conjecture is valid for Galois extensions*
(a) $M/\mathbb{Q}_p$, $p \neq 2$, of degree $[M : \mathbb{Q}_p] \leq 15$,
(b) $M/\mathbb{Q}_2$ non-abelian and of degree $[M : \mathbb{Q}_2] \leq 15$,
(c) $M/\mathbb{Q}_2$ of degree $[M : \mathbb{Q}_2] \leq 7$.

Proof. The cases not considered in the theorem above are extensions of $\mathbb{Q}_p$, $p \neq 2$, which are either tamely ramified or have abelian Galois group, and extensions of $\mathbb{Q}_2$ which are tamely ramified. These cases have already been proved in [8]. Note that for degree 7 there is just one extension of $\mathbb{Q}_2$ which is also tamely ramified. □

We finally provide the proofs of Corollary 3 and Corollary 7.

Proof of Corollary 3. We recall that $\mathrm{EPS}^{\mathrm{loc}}(E/F)$ is true for all tamely ramified Galois extensions and for all abelian extensions $E/\mathbb{Q}_p$, $p \neq 2$. Combining these results with Corollary 25 we deduce Corollary 3 from Theorem 19 (iii). □

Proof of Corollary 7. If $L/\mathbb{Q}$ is abelian, the global conjecture is already known to be valid by combining [11, Cor. 1.3] with [10, Thm. 5.2]. Note that the compatibility conjecture of Breuning and Burns stated in [10, Conj. 5.3] is equivalent to Conjecture 16 (which is the conjecture Bley and Burns stated in [4]) by [10, Rem. 5.4].

If $L/\mathbb{Q}$ is Galois with $[L : \mathbb{Q}] \leq 15$ then $L/\mathbb{Q}$ does not satisfy Property $(*)$ if and only if 2 is wildly ramified with abelian decomposition group G_w such that $8 \leq |G_w| \leq 15$. But in these cases $\mathrm{Gal}(L/\mathbb{Q}) = G_w$ is abelian and we can use the above mentioned result for the global absolutely abelian case. □

Corollaries 4 and 5 finally follow from Corollary 3.

REFERENCES

1. V. Acciaro and J. Klüners. *Computing local Artin maps, and solvability of norm equations.* J. Symbolic Comput. **30** (2000), no. 3, 239–252.
2. W. Bley. *Numerical evidence for a conjectural generalization of Hilbert's theorem 132.* LMS J. Comput. Math. **6** (2003), 66–88.
3. W. Bley and M. Breuning. *Exact algorithms for p-adic fields and epsilon constant conjectures.* Illinois J. Math. **52** (2008), 773–797.
4. W. Bley and D. Burns. *Equivariant epsilon constants, discriminants and étale cohomology.* Proc. London Math. Soc. (3) **87** (2003), 545–590.
5. W. Bley and S. M. J. Wilson. *Computations in relative algebraic K-groups.* LMS J. Comput. Math. **12** (2009), 166–194.
6. W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system I: The user language.* J. Symb. Comp. **24** (1997), 235–265.

7. M. Breuning. *Equivariant epsilon constants for Galois extensions of number fields and p-adic fields*. Ph.D. thesis, King's College, London, May 2004.

8. M. Breuning. *Equivariant local epsilon constants and étale cohomology*. J. London Math. Soc. (2) **70** (2004), 289–306.

9. M. Breuning. *On equivariant global epsilon constants for certain dihedral extensions*. Math. Comp. **73** (2004), 881–898.

10. M. Breuning and D. Burns. *Leading terms of Artin L-functions at $s = 0$ and $s = 1$*. Compos. Math. **143** (2007), 1427–1464.

11. M. Breuning and D. Burns. *On equivariant dedekind zeta-functions at $s = 1$*, Doc. Math., Extra volume: Andrei A. Suslin sixtieth birthday (2010), 289–306.

12. D. Burns. *Equivariant Whitehead torsion and refined Euler characteristics*. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 35–59. Amer. Math. Soc., Providence, RI, 2004.

13. D. Burns and M. Flach. *Tamagawa numbers for motives with (non-commutative) coefficients*. Doc. Math. **6** (2001), 501–570 (electronic).

14. D. Burns and M. Flach. *On the equivariant Tamagawa number conjecture for Tate motives. II*. Doc. Math. (2006), Extra Vol., 133–163 (electronic).

15. T. Chinburg. *Exact sequences and galois module structure*. Annals of Mathematics **121** (1985), 351–376.

16. Henri Cohen. *Advanced topics in computational number theory*, vol. 193 of *Graduate Texts in Mathematics*. Springer, New York, 2000.

17. R. Debeerst. *Algorithms for Tamagawa Number Conjectures*. Ph.D. thesis, University of Kassel, 2011. URL `http://kobra.bibliothek.uni-kassel.de/handle/urn:nbn:de:hebis:34-2011060937825`.

18. C. Fieker. *Applications of the class field theory of global fields*. In *Discovering mathematics with Magma*, pages 31–62. Springer, Berlin, 2006.

19. A. Fröhlich. *Galois module structure of algebraic integers*. Springer, Berlin, 1983.

20. Christian Greve. *Galoisgruppen von Eisensteinpolynomen über p-adischen Körpern*. Ph.D. thesis, Universität Paderborn, Oct. 2010.

21. G. Henniart. *Relèvement global d'extensions locales: quelques problèmes de plongement*. Math. Ann. **319** (2001), 75–87.

22. D. F. Holt. *Cohomology and group extensions in Magma*. In *Discovering mathematics with Magma*, pages 221–241. Springer, Berlin, 2006.

23. C. U. Jensen, A. Ledet, and N. Yui. *Generic Polynomials*. Cambridge University Press, 2002.

24. J. W. Jones and D. P. Roberts. *Database of local fields*. URL `http://math.la.asu.edu/~jj/localfields/`.

25. J. Klüners and G. Malle. *A database for field extensions of the rationals*. LMS J. Comput. Math. **4** (2001), 182–196. URL `http://www.math.uni-duesseldorf.de/~klueners/minimum/`.

26. F. Lorenz. *Einführung in die Algebra II*. Spektrum Akademischer Verlag, Heidelberg, 1997.

27. J. Martinet. *Character theory and Artin L-functions*. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 1–87. Academic Press, London, 1977.

28. J. Neukirch. *Algebraic number theory*. Springer, 1999.

29. J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*. Springer, Berlin, 2000.

30. S. Pauli and X.-F. Roblot. *On the computation of all extensions of a p-adic field of a given degree*. Math. Comp. **70** (2001), 1641–1659.

31. I. Reiner. *Maximal orders*, vol. 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, Oxford, 2003.

32. J.-P. Serre. *Linear representations of finite groups*. Springer, 1977.

33. J.-P. Serre. *Local fields*. Springer, New York, 1979.

34. R. G. Swan. *Algebraic K-theory*. Lecture Notes in Mathematics (76). Springer, Berlin, 1968.

35. M. J. Taylor. *On Fröhlich's conjecture for rings of integers of tame extensions*. Invent. Math. **63** (1981), 41–79.

WERNER BLEY, UNIVERSITÄT MÜNCHEN, THERESIENSTR. 39, 80333 MÜNCHEN, GERMANY
E-mail address: `bley@math.lmu.de`

RUBEN DEBEERST, UNIVERSITÄT KASSEL, HEINRICH-PLETT-STR. 40, 34132 KASSEL, GERMANY
E-mail address: `debeerst@math.uni-kassel.de`