ALGORITHMIC PROOF OF THE EPSILON CONSTANT CONJECTURE

WERNER BLEY AND RUBEN DEBEERST

Abstract. In this paper we will algorithmically prove the local and global epsilon constant conjectures for all fields of absolute degree lower or equal to 15. 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.

1. Introduction

For a tamely ramified Galois extensions $L|K$ 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 epsilon constants of symplectic characters of G, 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 [16, 29].

In 1985 Chinburg defined an element $\Omega(L|K,2)$ in $\mathrm{Cl}(\mathbb{Z}[G])$ for arbitrary $L|K$ 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. [12].

Later, Burns and the first author formulated 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 element $\mathscr{E}_{L|K}$ associated to epsilon constants of all characters of G and an element involving algebraic invariants, which project to the root number class and to $\Omega(L|K,2)$, respectively. The global epsilon constant conjecture then predicates the vanishing of their difference, which is also denoted by $T\Omega^{\mathrm{loc}}(L|K,1)$. Burns and the first 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 subgroup $K_0(\mathbb{Z}[G],\mathbb{Q})_{\mathrm{tor}}$ of $K_0(\mathbb{Z}[G],\mathbb{R})$, see [3, Cor. 6.3].

This conjecture fits into the more general framework of the equivariant Tamagawa number conjecture (ETNC) formulated by Burns and Flach in [11]. ETNC conjecturally describes the leading term of an motivic equivariant L-function with cohomological invariants. Concerning number fields, Burns and the first author subsequently formulated a compatibility of the conjectures for the leading terms at

Date: Version of 7th July 2011.
2000 *Mathematics Subject Classification.* Primary 11Y40. Secondary 11R33, 11S25.
Key words and phrases. epsilon constant conjecture, local fundamental classes.
The second author was supported by DFG grant BL 395/3-1.

$s = 0$ and $s = 1$ in [3]. An overview of the two conjectures and their compatibility conjecture is given by Breuning and Burns in [8] and in [9] they recently proved the equivalence to the more general conjectures from [11] for the conjecture at $s = 1$ assuming Leopold's conjecture.

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 [7] stating an independent conjecture for local number fields in the group $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$. He defined an element $R_{L_w|K_v} \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ incorporating local epsilon constants and algebraic invariants associated to a local number field extension $L_w|K_v$ and conjectured the vanishing of $R_{L_w|K_v}$. Breuning proved his local epsilon constant conjecture for tamely ramified extensions, for abelian extensions of $\mathbb{Q}_p$ with $p \neq 2$, for all S_3-extensions, and for some 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 and $\mathrm{i}_{G_w}^G$ denotes the induction map on the relative K-group, cf. [7, Thm. 4.1]. Using the result for tame extensions, one concludes that the validity of the global conjecture for fixed G and K depends upon the validity of the local conjecture for only finitely many local extensions.

Subsequently, Breuning and the first author presented an algorithm in [2] 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 will prove:

Theorem 1. *The local epsilon constant conjecture is valid for all wildly ramified, non-abelian Galois extensions L of $\mathbb{Q}_p$ with degree $[L : \mathbb{Q}_p] \leq 15$. It is also valid for abelian extensions L of $\mathbb{Q}_2$ with $[L : \mathbb{Q}_p] \leq 6$.*

The above relation between $T\Omega^{\mathrm{loc}}(L|K, 1)_p$ and $R_{L_w|K_v}$ and the known results for tame extensions and abelian extensions then imply the following result for global fields.

Corollary 2. *The global epsilon constant conjecture is valid for all Galois extensions L of $\mathbb{Q}$ with degree $[L : \mathbb{Q}] \leq 15$.*

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

Corollary 3. *Chinburg's $\Omega(2)$-conjecture is valid for all Galois extensions L of $\mathbb{Q}$ with degree $[L : \mathbb{Q}] \leq 15$.*

Moreover, the functorial properties from [7, Prop. 3.3], which states that for number field extensions $L|F|K$ in which $L|K$ is Galois the local conjecture for $L|K$ implies the local conjecture for $L|F$, imply the following result:

Corollary 4. *The global epsilon constant conjecture and Chinburg's $\Omega(2)$-conjecture are valid for global Galois extensions $E|F$ for which E is contained in a Galois extension $L|\mathbb{Q}$ with $[L : \mathbb{Q}] \leq 15$.*

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 definition of the epsilon constant conjectures and their most important relations and results. To apply an algorithm of Breuning and the first author for the proof of this conjecture (see [2]) we will present heuristics to represent local extensions using global number fields in §4. Thereafter, §5 gives an overview of that 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 thus also for the above corollaries.

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 $H^i(G,A)$ for the n-dimensional cohomology group as in [24, I§2] and we will use the inhomogeneous description using n-cochains $C^n(G,A) := \mathrm{Hom}_G(G^n, A)$ and $C^0(G,A) := A$.

Let $L|K$ denote a local Galois extension with Galois group G. We will also use the notation of class formations from [27, XI§2] and let $u_{L|K}$ denote the local fundamental class of $L|K$ as defined in [27, XIII§3f.], i.e. the element which is mapped to $\frac{1}{[L:K]}+\mathbb{Z}$ by the canonical isomorphism $\mathrm{inv}_{L|K} : H^2(G, L^\times) \xrightarrow{\simeq} \frac{1}{[L:K]}\mathbb{Z}+\mathbb{Z}$, which is called the local invariant map.[1]

2. An efficient algorithm to compute the local fundamental class

Throughout this section $L|K$ will denote a local 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 $H^2(G, L^\times)$.

A direct method to compute the image of the local fundamental class under $H^2(G,L^\times) \to H^2(G, L^\times/U_L^{(k)})$ for any $k \geq 0$ has been described in [2, §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

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

in which the bottom map is injective by [2, Lem. 2.5]. The authors then deduce an algorithm following the following steps:

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

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

[1]Similar definitions can be found in [24, (3.1.3), (7.1.4)].

(3) Find the preimage under the map

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

If φ denotes the Frobenius automorphism in $C = \langle\varphi\rangle$ and $\pi \in K$ is a uniformizing element, the fundamental class in $H^2(C, N^\times)$ is given by (see [26, Chp. 7, (30.1)])

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

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 [18]. However, this method turns out to be ineffective even for number fields of small degree.

The basis of a new algorithm to compute the local fundamental class is the theory from Serre [27] and especially exercise 2 from chapter XIII, §5. We recall the results from 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, such that its Galois group is $\mathrm{Gal}(\widetilde{K}|K) = \overline{\langle\varphi\rangle}$ and $\mathrm{Gal}(\widetilde{K}|E) = \overline{\langle\varphi^d\rangle}$.

The maximal unramified extension of L is $\widetilde{L} = L\widetilde{K}$ and the Galois group of $\widetilde{L}|K$ is given by $\mathrm{Gal}(\widetilde{L}|K) = \{(\sigma, \tau) \in G \times \mathrm{Gal}(\widetilde{K}|K) \,\big|\, \sigma|_E = \tau|_E\}$. We consider $L_{nr} := \widetilde{K} \otimes_K L$, for which we have the following representation:

Lemma 5. *(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 given by*

$$\begin{aligned} (\varphi \times 1)(y) &= (y_1, y_2, \ldots, \varphi^d(y_0)) \\ (\varphi^j \times \sigma)(y) &= (\hat\sigma(y_0), \hat\sigma(y_1), \ldots, \hat\sigma(y_{d-1})) \\ \text{and} \qquad (1 \times \sigma)(y) &= (\varphi^{-j} \times 1)(\hat\sigma(y_0), \hat\sigma(y_1), \ldots, \hat\sigma(y_{d-1})) \end{aligned}$$

for $\sigma \in G$ *and where* $\hat\sigma$ *is any element of* $G_{\widetilde{L}|K}$ *satisfying* $\hat\sigma|_L = \sigma$ *and* $\hat\sigma|_{\widetilde{K}} = \varphi^j$.

Proof. Direct computation, cf. [27, XIII §5, Ex. 2]. □

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

Lemma 6. *For every* $c \in U_{\widehat{L}}$ *there exists* $x \in \widehat{L}^\times$ *such that* $x^{\varphi^d - 1} = c$.

Proof. This is [23, V, Lem. 2.1] or [27, XIII, Prop. 15] applied to the totally ramified extension $L|E$ with φ^d generating $\mathrm{Gal}(\widetilde{K}|E)$. Since this will be an essential part of the algorithm, we sketch the constructive proof of [23].

Denote the residue class field of $\widehat{L}$ by κ, the cardinality of the residue class field of E by q and let $\phi = \varphi^d$. 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 $a_1 = x_2^{\phi-1} a_2$. 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 $\widehat{L}^\times$. $\square$

This fact can be generalized to our case. Let $\widehat{L}_{nr}$ be the completion of L_{nr} and $w : \widehat{L}_{nr} \to \mathbb{Z}$ the sum of the valuations.

Lemma 7. *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 $c = (c_0, \dots c_{d-1}) \in \prod_{i=0}^{d-1} \widehat{L}^\times$ 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 6. Then the element $x = (y, yc_0, yc_0c_1, \dots, yc_0 \cdots c_{d-2})$ satisfies

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

since $\varphi^d(y) = y \prod_{i=0}^{d-1} c_i$. Hence, x solves the equation $x^{\varphi-1} = c$. $\square$

We prepare or main result by the following lemma.

Lemma 8. *(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 $L_{nr}^\times$, and*
(iii) $\widehat{L}_{nr}^\times$ is a cohomologically trivial G-module.

Proof. [27, XIII §5, Ex. 2(a)]. $\square$

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

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

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

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

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

Its inverse $\Phi_{L|K}^{-1}$ directly defines an isomorphism

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

which satisfies the properties of an invariant map.

Proposition 9. *(i) The elements $\overline{u}_{L|K} := \Phi_{L|K}(1 + [L : K]\mathbb{Z})$ are fundamental classes for the class formation with respect to the isomorphism $\overline{\mathrm{inv}}$, i.e. $\overline{\mathrm{inv}}_{L|K}(\overline{u}_{L|K}) = \frac{1}{[L:K]} + \mathbb{Z}$.*
(ii) The element $\overline{u}_{L|K}$ is the inverse of the local fundamental class $u_{L|K}$.

Proof. This is [27, XIII §5, Ex. 2(c) and (d)].

Part (i) can be proved by verifying the axioms of a class formation. Then two elements $\overline{u}_{L|K}$ and $\overline{u}_{L'|K}$ with $[L' : K] = [L : K]$ have the same invariant $\overline{\mathrm{inv}}_{L|K}(v_{L|K}) = \overline{\mathrm{inv}}_{L'|K}(v_{L'|K})$ and it is sufficient to prove (ii) for unramified extensions.

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

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

from the long exact cohomology sequence of (1), 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 $a = (1,\dots,1,\pi) \in \widehat{L}_{nr}^{\times} = C^0(G,\widehat{L}_{nr}^{\times})$ is a preimage of 1 via w. Applying ∂_1 yields $\alpha \in C^1(G,\widehat{L}_{nr}^{\times})$, which is defined by

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

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

For the connecting homomorphism δ_2 we consider the commutative diagram

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

which arises from the cohomology sequence of (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 7 these preimages are given by

$$\beta(\sigma) := \begin{cases} (u_\sigma,\dots,u_\sigma) & \text{if } \hat{\sigma}|_{\widetilde{K}} = 1 \\ (u_\sigma,\dots,u_\sigma,\underbrace{u_\sigma\hat{\sigma}(\pi),\dots,u_\sigma\hat{\sigma}(\pi)}_{j \text{ components}}) & \text{if } \hat{\sigma}|_{\widetilde{K}} = \varphi^{-j}, 1 \le j \le d-1 \end{cases} \tag{6}$$

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

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

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 an 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 $\sigma \ne 1$ and $u_\sigma = 1$, one can easily check that $\overline{u}_{L|K}(\sigma,\tau) = \pi$, if $i + j < d$ and $\overline{u}_{L|K}(\sigma,\tau) = 1$ otherwise. Hence, $\overline{u}_{L|K}$ is the inverse of the local fundamental class, cf. [2, §2.4]. A detailed proof can be found in the second author's dissertation [14]. □

Remark 10. 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 an uniformizing element of L. Then the elements u_σ can be computed by successively applying the constructive steps of the proof of Lemma 6. 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 get very large.

To avoid this problem in the algorithm below, we construct a special uniformizing element π in an unramified extension F of L 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 without any other algebraic extension.

Algorithm 11 (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 $H^2(G, L^\times/U_L^{(k)})$.

1 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 F be the unramified extension of L of degree e, $L_{nr} = \prod_d F$ and let E be the maximal unramified extension of K in L with Frobenius automorphism φ.

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

3 For each $\sigma \in G$, let $\hat\sigma \in \mathrm{Gal}(F|K)$ be defined by $\hat\sigma|_L = \sigma$ and $\hat\sigma|_E = \varphi^j, 0 \le j \le d-1$. Then compute $u_\sigma \in F$ such that $u_\sigma^{\varphi^d - 1} = \frac{\hat\sigma(\pi)}{\pi} \mod U_F^{(k+2)}$.

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

Return: γ^{-1}.

Proof of correctness. Step 2: Since u has valuation 0 and $F|L$ is unramified, there exists an element $v \in F$ 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 3: The elements $\frac{\hat\sigma(\pi)}{\pi}$ have norm

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

Let $H = \mathrm{Gal}(L|F)$. Since $H^{-1}(H, U_F) = {}_{N_H}U_F/I_H U_F = 1$ for the unramified extension $F|L$, there exists $x \in F$ with $x^{\varphi-1} = \frac{\sigma(\pi)}{\pi}$. By successively applying the steps in the constructive proof of [23, V, Lem. 2.1] (see Lemma 6) one can construct an element $x \in U_F$ with $x^{\varphi-1} \equiv \frac{\sigma(\pi)}{\pi} \mod U_F^{(k+2)}$.

Step 4: The direct computation in the proof of Proposition 9 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 by one. 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 $U_F^{(k)}$. □

This algorithm has been implemented in Magma [5] and its source code is bundled with the second author's dissertation [14]. For a small example were the Galois group is $G = S_3$, this algorithm computes the local fundamental class within a few seconds where the direct linear algebra method took more than an hour.

3. Epsilon constant conjectures

We recall the statements of the global and local epsilon constant conjectures from [3] and [7] and some important related results. These conjectures are formulated as equations in relative K-groups for group rings.

Let R be a ring, E an extension of $\mathrm{Quot}(R)$ and G a 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

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

with the relative algebraic K-group $K_0(R[G],E)$ defined in terms of generators and relations as in [28, p. 215]. An overview of these K-groups is given in [6]. We write $Z(E[G])$ for the center of $E[G]$ and we will use the reduced norm map $\mathrm{nr} : K_1(E[G]) \to Z(E[G])^\times$, 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 norm map is an isomorphism (e.g. see [6, 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 $Z(E[G])^\times$ to $K_0(\mathbb{Z}_p[G],E)$.

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

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

and the Weak Approximation Theorem still allow us to define a map $\widehat{\partial}^1_{G,\mathbb{R}}$ from $Z(\mathbb{R}[G])^\times$ to $K_0(\mathbb{Z}[G],\mathbb{R})$ by $\widehat{\partial}^1_{G,\mathbb{R}}(x) := \widehat{\partial}^1_{\mathbb{Z}[G],\mathbb{R}}(\lambda x) - \sum_p \widehat{\partial}^1_{\mathbb{Z}_p[G],\mathbb{Q}_p}(\lambda)$ where the summation ranges over all primes and $\lambda \in Z(\mathbb{Q}[G])^\times \subseteq Z(\mathbb{Q}_p[G])^\times$ must be chosen such that $\lambda x \in \mathrm{im}(\mathrm{nr})$. One can show that this definition does not depend on the choice of λ and provides a well-defined unique map from $Z(\mathbb{R}[G])$ to $K_0(\mathbb{Z}[G],\mathbb{R})$, cf. [3, §3.1] or [8, Lem. 2.2].

Altogether, we have maps $\partial^1_{G,E} : Z(E[G])^\times \to K_0(\mathbb{Z}_p[G],E)$ for $E|\mathbb{Q}_p$, $\widehat{\partial}^1_{G,\mathbb{Q}} : Z(\mathbb{Q}[G])^\times \to K_0(\mathbb{Z}[G],\mathbb{Q})$ and $\widehat{\partial}^1_{G,\mathbb{R}} : Z(\mathbb{R}[G])^\times \to K_0(\mathbb{Z}[G],\mathbb{R})$.

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 number field extension $L|K$ it describes a relation between epsilon factors from the functional equation of the Artin $\mathcal{L}$-function and algebraic invariants related to $L|K$. We roughly recall its formulation of Burns and the first author and refer to [3] for more details.

The completion $\Lambda(L|K,\chi,s)$ of the Artin $\mathcal{L}$-function satisfies the functional equation

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

with epsilon factors $\varepsilon(L|K,\chi,s) := W(\chi)A(\chi)^{\frac{1}{2}-s}$ and $W(\chi), A(\chi)$ as defined in [16, 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 $\epsilon_{L|K} := \varepsilon(L|K,0) \in Z(\mathbb{R}[G])^\times$ is called the equivariant global epsilon constant. We can 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 places of K, including all infinite places and all 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 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

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

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 $H_L = \prod_{\sigma\in\Sigma(L)}\mathbb{Z}$ and 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 [3, §3.2]. Hereby, $\Sigma(L)$ denotes all embeddings of L into $\mathbb{C}$.

Let $X\subseteq\mathcal{O}_{L_w}$ be a cohomologically trivial submodule, e.g. $X = \exp_w(\mathscr{L}_w)$. Then $H^2(G_w, L_w^\times)\simeq H^2(G_w, L_w^\times/X)$ and by [24, Th. 2.2.10].there is an isomorphism $H^2(G_w, L_w^\times/X)\simeq \mathrm{Ext}^2_{G_w}(\mathbb{Z}, L_w^\times/X)$. For a cocycle $\gamma\in H^2(G_w,L_w^\times/X)$ one can apply the construction from [24, p. 115] to obtain a 2-extension $0\to L_w^\times/X\to C(\gamma)\to\mathbb{Z}[G]\to\mathbb{Z}\to 0$ representing γ in $\mathrm{Ext}^2_{G_w}(\mathbb{Z},L_w^\times/X)$. Then the perfect complex $\left[C(\gamma)\to\mathbb{Z}[G]\right]$ also represents γ and has cohomology $L_w^\times/X$ in degree 0 and $\mathbb{Z}$ in degree 1. We write $E_w(X)$ for the refined Euler characteristic in $K_0(\mathbb{Z}[G],\mathbb{Q})$ of this complex and the trivialization induced by the valuation $w : L_w^\times/X\otimes\mathbb{Q}\simeq\mathbb{Q}$, as it was defined by Burns in [10, §2]. A triple representing $E_w(X)$ in $K_0(\mathbb{Z}[G],\mathbb{Q})$ is given in [3, Lem. 3.7], for a construction in our situation see also [3, §3.3].

Furthermore, let $m_w\in \mathrm{Z}(\mathbb{Q}[G_w])^\times$ be the element defined in [3, § 4.1] which is also called 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* $\mathrm{Z}(\mathbb{Q}[H]) = \prod_{i=1}^r F_i$ for suitable extensions $F_i|\mathbb{Q}$ is given by $x = (x_i)_{i=1\dots r}\mapsto({}^*x_i)$ with ${}^*x_i = 1$ if $x_i = 0$ and ${}^*x_i = x_i$ otherwise. Let φ_w denote a lift of the Frobenius automorphism in G_w/I_w, then the correction term is defined by

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

Finally, we define elements

$$\begin{aligned} I_G(v,\mathscr{L}) &:= \mathrm{i}^G_{G_w}\left(\widehat{\partial}^1_{G_w,\mathbb{Q}_p}(m_w) - E_w(\exp_v(\mathscr{L}_w))\right)\\ \text{and}\quad T\Omega^{\mathrm{loc}}(L|K,1) &:= \mathscr{E}_{L|K} - \delta_{L|K}(\mathscr{L}) - \textstyle\sum_{v\in S} I_G(v,\mathscr{L})\end{aligned}$$

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 or $\mathscr{L}$ (cf. [3, Rem. 4.2]) and we state the conjecture as follows.

Conjecture 12 (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 $K_0(\mathbb{Z}[G],\mathbb{R})$. We denote this conjecture by* $\mathrm{EPS}(L|K)$.

This conjecture has been proved for tamely ramified extensions, for abelian extensions $L|\mathbb{Q}$, for S_3-extensions, and for some dihedral and quaternion extensions, cf. [3, 7, 11]. 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 [3, Cor. 6.3]). We can therefore 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) of $K_0(\mathbb{Z}[G],\mathbb{Q})$. For this p-part of the global conjecture we get the following relation:

Lemma 13. *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.*

Proof. [3, Thm. 4.6]. □

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 [7], 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 [7] for details.

Let $\mathbb{C}_p$ denote the completion of an algebraic closure of $\mathbb{Q}_p$. For every character χ of $G_w=\mathrm{Gal}(L_w|K_v)$ one has an induced character $\mathrm{i}_{K_v}^{\mathbb{Q}_p}\chi$ of $\mathrm{Aut}(\mathbb{C}_p|\mathbb{Q}_p)$. The local Galois Gauss sum from [22, Chp. II, § 4] of this induced character 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*

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

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 $\mathscr{L}_w\otimes_{\mathbb{Z}_p}\mathbb{C}_p\to H_{L_w}\otimes_{\mathbb{Z}_p}\mathbb{C}_p$, $l\otimes z\mapsto(\sigma(l)z)_{\sigma\in\Sigma(L_w)}$. Hereby $\Sigma(L_w)$ denotes the set of embeddings $L_w\hookrightarrow\mathbb{C}_p$. By the surjectivity of the homomorphism $\partial^1: K_1(\mathbb{C}_p[G_w])\to K_0(\mathbb{Z}_p[G_w],\mathbb{C}_p)$ the equivariant local discriminant is represented by an element $d_{L_w|K_v}\in\mathbb{C}_p[G_w]^\times\subseteq K_1(\mathbb{C}_p[G_w])$. This element will be used later and we recall its explicit formula from [2, § 4.2.5] in (13).

We write $E_w(\mathscr{L}_w)_p$ for the projection of the Euler characteristic $E_w(\mathscr{L}_w)$ onto $K_0(\mathbb{Z}_p[G_w],\mathbb{Q}_p)$ by (9). The difference $E_w(\mathscr{L}_w)_p-\delta_{L_w|K_v}(\mathscr{L}_w)$, which is denoted by $C_{L_w|K_v}$ in [7], is independent of $\mathscr{L}_w$ by [7, 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 a unique element in $K_0(\mathbb{Z}_p[G_w],\mathbb{C}_p)$ which 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 the existence in [7, Prop. 2.12] includes an explicit formula for a representative $u_{L_w|K_v} \in \mathbb{C}_p[G_w]^\times \subseteq K_1(\mathbb{C}_p[G_w])$ with $\partial^1(u_{L_w|K_v}) = U_{L_w|K_v}$, which we will recall in (14).

Conjecture 14 (Local epsilon constant conjecture)**.** *For every Galois extension $L_w|K_v$ of local fields over $\mathbb{Q}_p$ the element*

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

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 for tamely ramified extensions, for abelian extensions $M|\mathbb{Q}_p$ with $p \neq 2$, for S_3-extensions of $\mathbb{Q}_3$, and for some other special cases [7]. 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 15 (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. [7, Thm. 4.1 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.** An important result for local and global extensions is the functorial property.

Proposition 16 (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 $E|K$ 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* $\mathrm{EPS}^{\mathrm{loc}}(M|N) \Rightarrow \mathrm{EPS}^{\mathrm{loc}}(E|K)$ *if $E|K$ is Galois.*

Proof. [3, Thm. 6.1] and [7, Prop. 4.25]. □

Together with known results one obtains the following:

Corollary 17. *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. This can be proved as follows (all extensions below are assumed to be Galois):

$$\begin{array}{llll} & \mathrm{EPS}^{\mathrm{loc}}(M|\mathbb{Q}_p) & \forall [M:\mathbb{Q}_p]\leq n, p\leq n & \\ \Rightarrow & \mathrm{EPS}^{\mathrm{loc}}(M|\mathbb{Q}_p) & \forall [M:\mathbb{Q}_p]\leq n, \forall p & \text{(result (D) for tame extensions)} \\ \Rightarrow & \mathrm{EPS}_p(L|\mathbb{Q}) & \forall [L:\mathbb{Q}]\leq n, \forall p & \text{(by Theorem 15)} \\ \Rightarrow & \mathrm{EPS}(L|\mathbb{Q}) & \forall [L:\mathbb{Q}]\leq n & \text{(by decomposition (9))} \\ \Rightarrow & \mathrm{EPS}(F|K) & \forall F\subseteq L, [L:\mathbb{Q}]\leq n & \text{(by Proposition 16)} \end{array}$$

□

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

(1) For a finite integer n, compute all local Galois extensions of $\mathbb{Q}_p$ up to degree n, with $p\leq n$. This can be done using an algorithm by Pauli and Roblot [25] 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 *global representation* for $M|\mathbb{Q}_p$ and is needed to do exact computations in step (3).
(3) Apply the algorithm by Breuning and the first author [2] to prove the local epsilon constant conjecture of these extensions.

In the next section we will discuss how step 2 can be handled. Afterwards we recall the algorithm from [2] and present 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 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 [2, 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 [17] 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 [21] 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, if $[M:\mathbb{Q}_p]\leq 15$.

4.2. **Generic polynomials.** Here we consider polynomials $f \in K(t_1, \dots, t_n)[x]$ with arbitrary indeterminates t_i over a field K. It is said to be *generic* for a group G, if the splitting field L of f is a Galois extension of $K(t_1, \dots, t_n)$ with group G and, moreover, all extensions of $K(t_1, \dots, t_n)$ with group G are given by a polynomial f of this form. For specializations of values $t_1, \dots t_n \in \mathbb{Q}$ (possibly with certain restrictions) and $K = \mathbb{Q}$ one will get a Galois extension of $\mathbb{Q}$ with this group G and randomly testing different values will also return a global representation for M.

The book [19] by Jensen et. al. contains generic 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 generic polynomials for all groups. The smallest group for which the non-existence is proved is the cyclic group of order eight [19, § 2.6].

4.3. **Class field theory.** As a last heuristic, we will use class field theory to construct abelian extensions with prescribed ramification.[2] For a field extensions K of $\mathbb{Q}$, there is a one-to-one correspondence between abelian extensions $L|K$ and subgroups of the idèle class group C_K and each of those extensions $L|K$ has Galois group $\mathrm{Gal}(L|K) \simeq C_K / \mathrm{N}_{L|K} C_L$, cf. [23, Chp. VI, § 6].

For a *modulus* $\mathfrak{m} = \prod \mathfrak{p}^{n_\mathfrak{p}}$ — where $\mathfrak{p}$ runs through all (finite and infinite) places and $n_\mathfrak{p} \in \mathbb{N} \cup \{0\}$ and $n_\mathfrak{p} \in \{0, 1\}$ for $\mathfrak{p}|\infty$ — one studies in particular the ray class field $K^\mathfrak{m}|K$. It is the extension corresponding to the subgroup $\left(\prod_\mathfrak{p} U_\mathfrak{p}^{(n_\mathfrak{p})}\right)K^\times/K^\times \subseteq C_K$ where $U_\mathfrak{p}^{(0)} = \mathcal{O}_{K_\mathfrak{p}}^\times$ and $U_\mathfrak{p}^{(n_\mathfrak{p})} = 1 + \mathfrak{p}^n$ for finite $\mathfrak{p}$, $U_\mathfrak{p}^{(0)} = \mathbb{R}^\times$ and $U_\mathfrak{p}^{(1)} = \mathbb{R}_{>0}$ for real $\mathfrak{p}$, and $U_\mathfrak{p}^{(n_\mathfrak{p})} = \mathbb{C}^\times$ for complex $\mathfrak{p}$. This abelian extension of K can be constructed using algorithms described by Cohen in [13, Chp. 4]. A discussion of algorithms implemented in Magma is given by Fieker in [15].

Given an extension $L|K$ one defines the *conductor* $\mathfrak{f}$ to be the greatest common divisor of all moduli $\mathfrak{m}$ for which $L \subseteq K^\mathfrak{m}$. For this conductor one can prove that $\mathfrak{p}|\mathfrak{f}$ 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. [15, § 2.4, p. 44].

One can therefore possibly find abelian extensions of K with prescribed ramification at certain places by choosing an appropriate modulus, constructing the 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. In the algorithm of Breuning the first author we will also have to consider 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. Since the local conjecture is known to be valid for tamely ramified extensions and abelian extensions of $\mathbb{Q}_p$, $p \neq 2$, we will 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,
(b) wildly ramified extensions M of $\mathbb{Q}_2$, with abelian Galois group G, and
(c) unramified extensions of $\mathbb{Q}_p$ of degree $f = \exp(G^{\mathrm{ab}})$ in each of the two situations above.

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

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, which are not considered in the cases above.

4.4.1. *Case (a).* First consider extensions with *non-abelian* Galois group. For almost all those non-abelian wildly-ramified local extensions we found polynomials of the appropriate degree in the database [21] 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 [19, 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 undecomposed at $p = 7$ and computing all C_7–extensions of K which are subfields of $K^{\mathfrak{m}}$, $\mathfrak{m} = 49\mathcal{O}_K$, one finds D_7–extensions where $p = 7$ is ramified with ramification index 7 or 14 and where p does not decompose. 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 [21] 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 2).

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 18 also needs a extension N of $\mathbb{Q}$ which is unramified and undecomposed 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 [21].

A complete list of polynomials which were found using these heuristics can be found in the second author's dissertation [14].

5. Algorithmic proof of the local epsilon constant conjecture

We briefly recall the algorithm described by Breuning and the first author in [2, §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 $L_w|\mathbb{Q}_p$ below.

For the rest of this section, fix the Galois extensions $L|K$ and $N|K$ and a prime $\mathfrak{p}$ of K as in the input of the algorithm. 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 $K_v = K_\mathfrak{p}$.

Algorithm 18 (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 undecomposed 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 $\mathbb{Q}(\zeta_m, \zeta_{p^t})$, $m = \exp(G^{\mathrm{ab}})$.

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 $(\mathfrak{P}\mathcal{O}_{L_w})^k \subseteq \mathscr{L}$.

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

5 Construct a complex representing this cocycle by [24, p. 115] and compute the Euler characteristic $E_w(\exp_v(\mathscr{L}_w)) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ as in [2, §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 $d_{L_\mathfrak{P}|\mathbb{Q}_p} \in L[G]^\times \subseteq E[G]^\times$ from (13), which represents the equivariant discriminant $\delta_{L_\mathfrak{P}|\mathbb{Q}_p}(\mathscr{L}) \in K_0(\mathbb{Z}[G], E_\mathfrak{Q})$.

8 Compute the element $u_{L_\mathfrak{P}|\mathbb{Q}_p} \in N[G]^\times \subseteq E[G]^\times$ using (14), which represents the unramified term $U_{L_\mathfrak{P}|\mathbb{Q}_p} \in K_0(\mathbb{Z}[G], E_\mathfrak{Q})$.

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 three 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 $E_w(\mathscr{L})$ 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. [2, §4.2]. □

All steps were explained in detail in [2]. However, there were some problems that needed further improvements to give a practical algorithm. First, the existence of global representations is due to a theoretical argument by Henniart in [17] 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. Second, the computation of local fundamental classes as presented in [2, § 2.4] is not very efficient and is significantly improved by Algorithm 11. And, finally, their has been made considerable progress on the computation of the relative K-group $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ in [4].

Below we will discuss each part for the algorithm separately.

5.1. **Constructing the coefficient field.** As explained in [2, § 4.2.2] we need to construct a global field E, in which all the computations take place.

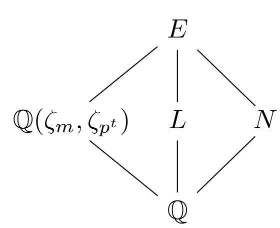
For the computation of the unramified term, we will need a cyclic extensions $N|K$ which is unramified and undecomposed at $\mathfrak{p}$.

Another extension involved is $\mathbb{Q}(\zeta_m, \zeta_{p^t})$, where m is the exponent of G^{ab} and t is computed as in [2, Rem. 2.7]: By representation theory the field $\mathbb{Q}(\zeta_m)$ contains the values of all characters of G. 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. [2, § 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. Below, this choice of t allows us to compute the epsilon constants as elements of $\mathbb{Q}(\zeta_m, \zeta_{p^t})$, see also [2, Rem. 2.7].

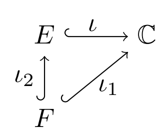
The composite field of the three fields L, N and $\mathbb{Q}(\zeta_m, \zeta_{p^t})$ is denoted by E, giving the following situation:

(12)



We then fix a complex embedding $\iota : E \hookrightarrow \mathbb{C}$. Since E contains the roots of unity ζ_m, the center $\mathrm{Z}(E[G])$ decomposes into $\mathrm{Z}(E[G]) = \prod_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} E$.

The fixed embedding ι is essential because some of the elements in the conjecture depend on the particular choice of the embedding: for example, the definition of the standard additive character below, see also [2, § 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



is commutative, i.e. $\iota_1 = \iota|_F$.

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 $E \overset{\iota}{\hookrightarrow} \mathbb{C} \hookrightarrow \mathbb{C}_p$ commute. 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 $\mathrm{Z}(E_{\mathfrak{Q}}[G]) \simeq \prod_{\chi \in \mathrm{Irr}(G)} E_{\mathfrak{Q}}^\times$. In fact, we will see that all these elements are also represented by elements in $\prod_{\chi \in \mathrm{Irr}(G)} E^\times$ and can be computed globally.

5.2. **Computation of cohomological term.** The lattice $\mathscr{L} = \mathbb{Z}[G]\theta \subseteq \mathcal{O}_L$ is computed using a normal basis element θ (see also [2, § 4.2.3]). The integer k for which $\mathfrak{p}^k \subseteq \mathscr{L}$ can then be found experimentally by global computations.

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 11 and its projection in $Z^2(G, L_w^\times / \exp(\mathscr{L}))$. We can then construct the corresponding complex $P_w = \left[L_w^f(\gamma) \to \mathbb{Z}[G]\right]$ using the splitting module $L_w^f(\gamma)$ from [24, Chp. III, § 1, p. 115] and the Euler characteristic $E_w(\mathscr{L}_w) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ can be computed using the explicit construction from [2, § 4.2.4].

5.3. **Computation of the terms in $\prod_\chi E^\times$.** The correction term m_w is directly defined as tuple in $\prod_\chi E^\times$ by (11). For the equivariant discriminant and the unramified term we have the following formulas from [2, §§ 4.2.5 and 4.2.7]:

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

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

Hereby, $\varphi_{\mathfrak{p}}$ denotes the Frobenius automorphism of $N|K$ with respect to $\mathfrak{p}$, $\xi \in \mathcal{O}_N$ is an integral normal basis element for $N_{\mathfrak{p}}|K_{\mathfrak{p}}$, and σ is a lift of the local norm residue symbol $(p, F_{\mathfrak{p}}|K_{\mathfrak{p}}) \in \mathrm{Gal}(F_{\mathfrak{p}}|K_{\mathfrak{p}}) \simeq \mathrm{Gal}(F|K)$ where F is the maximal abelian subextension in $L|K$. An algorithm to compute local norm residue symbols is described in [1, Alg. 3.1].

These group ring elements provide elements in $K_1(\mathbb{C}_p[G])$ through the homomorphism $E[G]^\times \to K_1(\mathbb{C}_p[G])$ by $E[G] \subseteq E_{\mathfrak{Q}}[G] \subseteq \mathbb{C}_p[G]$. The element $u_{L_w|\mathbb{Q}_p} \in N[G]$ represents the unramified term by definition ([7, Prop. 2.12]) and $d_{L_w|\mathbb{Q}_p} \in L[G]$ represents the equivariant discriminant through the surjective homomorphism $\partial^1 : K_1(\mathbb{C}_p[G]) \to K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$ by [2, § 4.2.5].

Using the reduced norm map $\mathrm{nr} : K_1(E[G]) \hookrightarrow \mathrm{Z}(E[G])^\times$ one obtains elements in $\mathrm{Z}(E[G])^\times$ and by the *Wedderburn decomposition* $\mathrm{Z}(E[G])^\times \simeq \prod_\chi E^\times$ the equivariant discriminant and the unramified term are finally represented by tuples in $\prod_{\chi \in \mathrm{Irr}(G)} E^\times \subset \prod_{\chi \in \mathrm{Irr}(G)} E_{\mathfrak{Q}}^\times$.

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, cf. [2, § 2.5].

For each χ, we already computed subgroups H of G, linear characters ϕ of H, and coefficients $c_{(H,\phi)} \in \mathbb{Z}$ such that $\chi - \chi(1)1_G = \sum_{(H,\phi)} c_{(H,\phi)} \mathrm{ind}_H^G(\phi - 1_H)$ by Brauer induction. Then the Galois Gauss sum of χ can be computed by Galois

Gauss sums of abelian extensions $L^{\ker(\phi)}|L^H$:

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

For localizations of the abelian extension $M = L^{\ker(\phi)}$ 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 $\mathfrak{f}(\phi)\mathcal{D}_{N_{\mathfrak{p}}}$, $\mathcal{D}_{N_{\mathfrak{p}}}$ 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 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 [2, § 2.5].

5.3.1. *Computations in relative K-groups.* In the following we have to combine the computations from 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 [4] Wilson and the first author describe the relative K-group as an abstract group. Using their methods it will be clear how to read elements of the form $\widehat{\partial}^1_{G_w,\mathbb{Q}_p}(x)$ 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 recall the description from [4] for group rings and — since their algorithms are not yet implemented in full generality — we will discuss a simple modification for extensions F of $\mathbb{Q}$ which are totally split at a given prime p.

First we introduce some more notation: Let K be a number field and G a finite group. The *Wedderburn decomposition* of $K[G]$ gives a decomposition of its center $C := \mathrm{Z}(K[G])$ into character fields K_i such that $C = \bigoplus_{i=1}^r K_i$. Each character field K_i corresponds to an irreducible character $\chi_i \in \mathrm{Irr}_K(G)$ and K_i is the field $K(\chi_i)$ which is obtained from K by adjoining the values of χ_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 included 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 result of Wilson and the first author is the following.

Proposition 19. *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 a natural isomorphism and $\bar{\varphi}$ being induced by

$$\begin{array}{rrcl} \varphi: & C_{\mathfrak{p}}^\times = \bigoplus_{i=1}^r (K_i)_{\mathfrak{p}} & \longrightarrow & I(C_{\mathfrak{p}}) \times \bigoplus_{i=1}^r (\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^\times \\ & (\nu_1,\dots,\nu_r) & \longmapsto & \Big(\big(\prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(\nu_i)}\big)_i, (\bar{\mu}_1,\dots,\bar{\mu}_r)\Big), \end{array} \tag{15}$$

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. [4, Prop. 2.7]. □

Wilson and the first author describe an algorithm to compute the group $I(C_{\mathfrak{p}}) \times \operatorname{coker}(\mu_{\mathfrak{p}})$ 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 $\theta : A_K \xrightarrow{\simeq} B_K$, one can compute a representative of $[A_{\mathfrak{p}}, \theta_{\mathfrak{p}}, B_{\mathfrak{p}}]$ in this group as follows. Every element $[A_{\mathfrak{p}}, \theta_{\mathfrak{p}}, B_{\mathfrak{p}}]$ is represented by an element in $K_1(K_{\mathfrak{p}}[G])$ by choosing $\mathcal{O}_{K_{\mathfrak{p}}}[G]$-bases of $A_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$ and computing a matrix in $\mathrm{Gl}_n(K_{\mathfrak{p}}[G])$ which represents the isomorphism $\theta_{\mathfrak{p}}$ with respect to this basis. From the reduced norm map $\mathrm{nr} : K_1(K_{\mathfrak{p}}[G]) \xrightarrow{\simeq} \mathrm{Z}(K_{\mathfrak{p}}[G])$ one then obtains a representative in $C_{\mathfrak{p}}^{\times}$ and applying $\bar{\varphi}$ finally provides the element in $I(C_{\mathfrak{p}}) \times \operatorname{coker}(\mu_{\mathfrak{p}})$ which corresponds to $[A_{\mathfrak{p}}, \theta_{\mathfrak{p}}, B_{\mathfrak{p}}]$. For details we refer to [4, § 4].

In theory, this solves the remaining problems for Algorithm 18. But in practice, this has only been implemented in Magma for $K = \mathbb{Q}$ and $\mathfrak{p} = p\mathbb{Z}$. In our case, however, we have to work with the decomposition field $F \subseteq E$ of $\mathfrak{Q}$. This field F is a Galois extension of $\mathbb{Q}$ which is totally split at p. Then for any prime $\mathfrak{q}|p$ 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 $\operatorname{coker}(\mu_{\mathfrak{p}})$.

Proposition 20. *Let* $F|\mathbb{Q}$ *be a number field which is totally split at* p *and for which* $F \cap K_i = K = \mathbb{Q}$ *for all* i*. 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

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

where $\mathfrak{h} := \mathcal{O}_{C'} \cap \mathfrak{f}$*.*

Proof. (i) The character fields K_i arise from $K = \mathbb{Q}$ by adjoining the values of a specific character in $\mathrm{Irr}_{\mathbb{Q}}(G)$. Since F and K_i are disjoint over $\mathbb{Q}$, one has the same irreducible characters over F: $\mathrm{Irr}_{\mathbb{Q}}(G) = \mathrm{Irr}_F(G)$. The character fields F_i then arise by adjoining the same character values and $F_i = FK_i$.

(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 $\mathfrak{q}$. The uniqueness of $\mathfrak{Q}$ 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 $(\mathfrak{P}, \mathfrak{Q})$, 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 $\mathcal{O}_{K_i}/\mathfrak{P} \simeq \mathcal{O}_{F_i}/\mathfrak{Q}$. Moreover, the $\mathfrak{q}$-part of $\mathfrak{h}$ is given by the part of $\mathfrak{g}\mathcal{O}_{C'}$ lying above $\mathfrak{q}$. The inclusions $\mathcal{O}_{K_i} \subseteq \mathcal{O}_{F_i}$ therefore induce isomorphisms $(\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^{\times} \simeq (\mathcal{O}_{F_i}/\mathfrak{h}_{i,\mathfrak{q}})^{\times}$. □

5.4. **Further remarks.** 1. As mentioned before, the algorithms from [4] 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 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 condition is valid in all cases we consider in the computational results below.

2. The computation of the prime ideal $\mathfrak{Q}$ in E is a though job when the degree of E gets large. In the last part of Algorithm 18 we will therefore proceed as follows. 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 $R_{L_w|K_v} = \widehat{\partial}^1_{G_w,E_{\mathfrak{Q}}}(\mathcal{I}) + E_w(\mathscr{L}_w)_p$ and since $R_{L_w|K_v}$ and $E_w(\mathscr{L}_w)_p$ are both elements of $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$, the element $\widehat{\partial}^1_{G_w,E_{\mathfrak{Q}}}(\mathcal{I})$ is also in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$. Hence, $\mathcal{I} \in \mathrm{Z}(\mathbb{Q}_p[G])^{\times}$ and each component $\mathcal{I}_\chi \in \mathbb{Q}_p(\zeta_m)$, $m = \exp(G)$. Since each component $\mathcal{I}_\chi$ is determined by a global element in E, we have $\mathcal{I}_\chi \in F' := \mathbb{Q}_p(\zeta_m) \cap E$. Here, the intersection is taken in the fixed completion of the algebraic closure $\mathbb{C}_p$ of $E_{\mathfrak{Q}}$. We therefore obtain $\mathcal{I} \in \mathrm{Z}(F'[G])^{\times} \simeq \prod_{\chi} (F')^{\times}$ and if $F = E^{G_{\mathfrak{Q}}}$ denotes the decomposition field of $\mathfrak{Q}$, then $F' = F(\zeta_m)$.

As mentioned above, we want to omit the computation of $\mathfrak{Q}$. So instead of working with E, we would like to work with a small subfield of E. The field $F' = F(\zeta_m)$ would be a good choice but this still involves the computation of the decomposition field of $\mathfrak{Q}$ and hence also the computation of $\mathfrak{Q}$ itself.

Instead we continue as follows: for every χ we compute the minimal polynomial m_χ of $\mathcal{I}_\chi$. Then we compute the composite field F' of the splitting fields of the polynomials m_χ with $\mathbb{Q}(\zeta_m)$. Although the computation of the splitting fields is also a difficult task, we note that these fields will always be subfields of E and where this approach could take hours, the computation of $\mathfrak{Q}$ did not succeed in several days.

In the end, F' is the composite field such that $\mathcal{I}_\chi, \zeta_m \in F'$. Compute the ideal $\mathfrak{q}'$ of F' 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 $\mathcal{I} = \tau_{L_w|\mathbb{Q}_p} u_{L_w|\mathbb{Q}_p}/(m_w d_{L_w|\mathbb{Q}_p}) \in \prod_{\chi} F(\zeta_m)^{\times}$.

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 18 has been implemented in Magma [5] and is bundled with the second author's dissertation [14].[3] It has been tested for various extensions up to

[3] http://kobra.bibliothek.uni-kassel.de/handle/urn:nbn:de:hebis:34-2011060937825

degree 20 and the computation time turns out to depend especially 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 embeddings $E \hookrightarrow \mathbb{C}$, already took about 7 hours, but the most time-consuming part (about 6.5 days) of Algorithm 18 was the computation of minimal polynomials and their splitting field mentioned in the remarks above. The field F' 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.

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

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 $p = 2$ have been considered in §4.4 and global representations have been found by 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 [21].

For each of those extensions we then continued with Algorithm 18 to prove the local epsilon constant conjecture. Details of the computations can be found in the author's dissertation [14]. This completes the proof of Theorem 1. □

Using some already known result we can also prove:

Corollary 21. *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* $[M : \mathbb{Q}_p] \leq 15$,
(c) $M|\mathbb{Q}_2$ *of degree* $[M : \mathbb{Q}_p] \leq 7$.

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 before [7]. Note that for degree 7 there is just one extension of $\mathbb{Q}_2$ which is also tamely ramified. □

We can then prove Corollary 2.

Proof of Corollary 2. If $L|\mathbb{Q}$ is abelian, the global conjecture is already known to be valid. For the non-abelian case, we recall that by Theorem 15 conjecture $\mathrm{EPS}(L|\mathbb{Q})$ is valid if $\mathrm{EPS}^{\mathrm{loc}}(L_w|\mathbb{Q}_p)$ is valid for all primes p and places $w|p$. If $L|\mathbb{Q}$ is non-abelian of degree ≤ 15, the local extension $L_w|\mathbb{Q}_p$ is either non-abelian of degree at most 15 or abelian of degree at most 7. Therefore the result follows from the above corollary. □

Corollaries 3 and 4 finally follow from Corollary 2.

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 and M. Breuning. *Exact algorithms for p-adic fields and epsilon constant conjectures.* Illinois J. Math. **52** (2008), 773–797.

3. W. Bley and D. Burns. *Equivariant epsilon constants, discriminants and étale cohomology.* Proc. London Math. Soc. (3) **87** (2003), 545–590.
4. W. Bley and S. M. J. Wilson. *Computations in relative algebraic K-groups.* LMS J. Comput. Math. **12** (2009), 166–194.
5. W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system I: The user language.* J. Symb. Comp. **24** (1997), 235–265.
6. M. Breuning. *Equivariant epsilon constants for Galois extensions of number fields and p-adic fields.* Ph.D. thesis, King's College, London, May 2004.
7. M. Breuning. *Equivariant local epsilon constants and étale cohomology.* J. London Math. Soc. (2) **70** (2004), 289–306.
8. M. Breuning and D. Burns. *Leading terms of Artin L-functions at $s = 0$ and $s = 1$.* Compos. Math. **143** (2007), 1427–1464.
9. M. Breuning and D. Burns. *On equivariant dedekind zeta-functions at $s = 1$*, November 2009. Preprint.
10. 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.
11. D. Burns and M. Flach. *Tamagawa numbers for motives with (non-commutative) coefficients.* Doc. Math. **6** (2001), 501–570 (electronic).
12. T. Chinburg. *Exact sequences and galois module structure.* Annals of Mathematics **121** (1985), 351–376.
13. Henri Cohen. *Advanced topics in computational number theory*, vol. 193 of *Graduate Texts in Mathematics*. Springer, New York, 2000.
14. 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.
15. C. Fieker. *Applications of the class field theory of global fields.* In *Discovering mathematics with Magma*, pages 31–62. Springer, Berlin, 2006.
16. A. Fröhlich. *Galois module structure of algebraic integers.* Springer, Berlin, 1983.
17. G. Henniart. *Relèvement global d'extensions locales: quelques problèmes de plongement.* Math. Ann. **319** (2001), 75–87.
18. D. F. Holt. *Cohomology and group extensions in Magma.* In *Discovering mathematics with Magma*, pages 221–241. Springer, Berlin, 2006.
19. C. U. Jensen, A. Ledet, and N. Yui. *Generic Polynomials.* Cambridge University Press, 2002.
20. J. W. Jones and D. P. Roberts. *Database of local fields.* URL http://math.la.asu.edu/~jj/localfields/.
21. 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/.
22. 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.
23. J. Neukirch. *Algebraische Zahlentheorie.* Springer, 1992.
24. J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields.* Springer, Berlin, 2000.
25. 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.
26. I. Reiner. *Maximal orders*, vol. 28 of *London Mathematical Society Monographs. New Series.* The Clarendon Press Oxford University Press, Oxford, 2003.
27. J.-P. Serre. *Local fields.* Springer, New York, 1979.
28. R. G. Swan. *Algebraic K-theory.* Lecture Notes in Mathematics (76). Springer, Berlin, 1968.
29. 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