EXACT ALGORITHMS FOR p-ADIC FIELDS AND EPSILON CONSTANT CONJECTURES

WERNER BLEY AND MANUEL BREUNING

Abstract. We develop several algorithms for computations in Galois extensions of p-adic fields. Our algorithms are based on existing algorithms for number fields and are exact in the sense that we do not need to consider approximations to p-adic numbers. As an application we describe an algorithmic approach to prove or disprove various conjectures for local and global epsilon constants.

1. Introduction

For computations in algebraic number fields numerous algorithms have been developed. These include not only algorithms for classical problems like the computation of the ring of integers and its unit group and ideal class group, but also algorithmic approaches to more complex topics in algebraic number theory, for example class field theory. For a discussion of many of these computational questions we refer to the books [8] and [9]. Most of these algorithms have been implemented and applied to numerically verify (and in some cases prove) conjectures for number fields.

In contrast to the case of number fields, much less algorithmic work has been done for p-adic fields. Before one can perform any p-adic computations one has, of course, to deal with the important question how to represent p-adic objects in such a way that errors of approximation are minimized or completely avoided. In our opinion already this question is not sufficiently addressed in most of the existing literature.

In this paper we describe algorithms for some computational problems in Galois extensions of p-adic fields. Our strategy is to represent a local Galois extension as the completion of a global Galois extension. This has two advantages: firstly, we can use many of the existing algorithms for number fields to perform computations in p-adic fields, and secondly, taking global objects as representatives of local quantities allows us to do exact computations in p-adic fields without the need to consider approximations.

In §2 we explain in detail how representing local Galois extensions as completions of global Galois extensions works. We then develop algorithms for some problems related to Galois extensions of p-adic fields, in particular for the computation of local norm residue symbols, local fundamental classes and local epsilon constants. In the algorithm for local epsilon constants we must apply a version of Brauer's induction theorem. This is treated algorithmically in §3, where we also describe other representation theoretic algorithms. The main objective in this section is to

Date: September 19, 2006.

The second author was supported by EPSRC grant GR/S91772/01.

discuss computational questions in certain relative algebraic K-groups with coefficients in a p-adic field. This is done in §3.3 where we combine ideas from §2 with the representation theoretic algorithms.

We apply most of the results of §2 and §3 in §4 where we develop an algorithmic approach to several conjectures for local and global epsilon constants. Our main algorithm is for the local epsilon constant conjecture of Breuning [6].

Theorem 1.1. *There exists an algorithm which for a given prime number p and positive integer n proves or disproves the local epsilon constant conjecture of* [6] *for every Galois extension $L/\mathbb{Q}_p$ of degree n.*

From this local result we then deduce that one can computationally prove two well-known conjectures for global epsilon constants (Chinburg's $\Omega(2)$-conjecture [7] and the global epsilon constant conjecture of Bley and Burns [3]) for infinite families of Galois extensions of number fields.

Corollary 1.2. *There exists an algorithm which for a given positive integer n either proves the global epsilon constant conjecture of* [3] *for every Galois extension $L/\mathbb{Q}$ of degree n or finds a counterexample to the local epsilon constant conjecture.*

Corollary 1.3. *There exists an algorithm which for a given positive integer n either proves Chinburg's $\Omega(2)$-conjecture of* [7] *for every Galois extension $L/\mathbb{Q}$ of degree n or finds a counterexample to the local epsilon constant conjecture.*

In general, our approach cannot be used to computationally disprove these global conjectures. See Remark 4.1 for further details.

Remark 1.4. Let E/F be a Galois extension of p-adic fields. If the local epsilon constant conjecture is valid for any Galois extension $L/\mathbb{Q}_p$ which contains E/F as a subextension, then functorial properties imply that it is also valid for E/F. Hence it is no loss of generality if we restrict ourselves to consider only Galois extensions $L/\mathbb{Q}_p$. A similar remark applies to the global epsilon constant conjecture and to Chinburg's $\Omega(2)$-conjecture.

We remark that the existence of these algorithms for epsilon constant conjectures is currently only of theoretical interest because a useful implementation seems to be unlikely in the near future (compare the discussion in §4.3).

Notations: We write $\mathrm{Gal}(L/K)$ for the Galois group of a Galois extension of fields L/K. For a number field K we let $\mathcal{O}_K$ denote its ring of algebraic integers. If $\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal, then we write $K_\mathfrak{p}$ for the completion of K with respect to $\mathfrak{p}$, and $\mathcal{O}_{K_\mathfrak{p}}$ for the ring of integers of $K_\mathfrak{p}$. We write $H^i(G, M)$, $i \in \mathbb{Z}$, for the Tate cohomology groups of a finite group G and G-module M. For any ring R we let $R^\times$ denote its unit group and $\zeta(R)$ its centre.

2. Exact computations in local Galois extensions

In this section we describe various ideas and algorithms which allow us to perform exact computations in Galois extensions of p-adic fields using well-known algorithms for number fields.

2.1. **Global representation of local Galois extensions.** Let M be a p-adic field, i.e. a finite extension of the p-adic numbers $\mathbb{Q}_p$. To perform exact computations in M it is convenient to represent the field M as the completion of a number field. A pair $(K, \mathfrak{p})$ where K is a number field and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ will be called a global representation of M if there exists a continuous isomorphism from M to the completion $K_\mathfrak{p}$. Every p-adic field M has a global representation $(K, \mathfrak{p})$. Note however, that $(K, \mathfrak{p})$ and the isomorphism $M \cong K_\mathfrak{p}$ are not uniquely determined by M.

To be able to work in an extension N/M of p-adic fields we need compatible global representations of M and N. We call $(L, \mathfrak{P})$ an extension of $(K, \mathfrak{p})$, in symbols $(L, \mathfrak{P})/(K, \mathfrak{p})$, if L/K is an extension of number fields, $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_L$ which lies over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, and $[L : K] = [L_\mathfrak{P} : K_\mathfrak{p}]$. Clearly, in this case $\mathfrak{P}$ is the unique prime of L lying over $\mathfrak{p}$. We say that an extension $(L, \mathfrak{P})/(K, \mathfrak{p})$ is a global representation of the extension N/M, if the extension $L_\mathfrak{P}/K_\mathfrak{p}$ is isomorphic to N/M, i.e. if there exists a continuous isomorphism $N \cong L_\mathfrak{P}$ which restricts to an isomorphism $M \cong K_\mathfrak{p}$.

Lemma 2.1. *Every extension N/M of p-adic fields has a global representation $(L, \mathfrak{P})/(K, \mathfrak{p})$.*

Proof. Let $(K, \mathfrak{p})$ be a global representation of M. It follows from Krasner's lemma that there exists a polynomial $f(x) \in K[x]$ such that $f(x)$ is irreducible over $K_\mathfrak{p} \cong M$ and $N = M(\alpha)$ for some root α of $f(x)$ in N (compare [13, Ch. III, §4, Exercise 4]). The field $L = K[x]/(f(x))$ has the required properties. □

If $(L, \mathfrak{P})/(K, \mathfrak{p})$ is a global representation of a p-adic Galois extension N/M, then the extension L/K is not necessarily Galois. The computation of the action of $\mathrm{Gal}(N/M)$ on N/M is considerably easier if L/K is itself Galois. The following lemma shows that it is always possible to find a global representation with this additional property.

Lemma 2.2. *Let $(L, \mathfrak{P})/(K, \mathfrak{p})$ be an extension such that $L_\mathfrak{P}/K_\mathfrak{p}$ is Galois. Then one can compute a global representation $(L', \mathfrak{P}')/(K', \mathfrak{p}')$ of $L_\mathfrak{P}/K_\mathfrak{p}$ such that L'/K' is Galois.*

Proof. Let L' be a Galois closure of L over K. Using the assumption that $L_\mathfrak{P}/K_\mathfrak{p}$ is Galois, it is not difficult to show (for example by choosing the Galois closure of L/K inside the completion $L_\mathfrak{P}$) that $\mathfrak{P}$ is completely split in the extension L'/L. Hence if we fix a prime $\mathfrak{P}'$ of L' above $\mathfrak{P}$ then $L'_{\mathfrak{P}'} = L_\mathfrak{P}$. Let K' be the decomposition field of $\mathfrak{P}'$ in the extension L'/K and $\mathfrak{p}'$ the prime of K' below $\mathfrak{P}'$. Then the extension $(L', \mathfrak{P}')/(K', \mathfrak{p}')$ has the required properties. □

We call an extension $(L, \mathfrak{P})/(K, \mathfrak{p})$ Galois (resp. abelian) if L/K is Galois (resp. abelian). Note that if $(L, \mathfrak{P})/(K, \mathfrak{p})$ is Galois, then $L_\mathfrak{P}/K_\mathfrak{p}$ is also Galois and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$.

Remark 2.3. The proof of Lemma 2.2 involves various operations for Galois extensions of number fields. It is well known that all these operations can be done algorithmically, however, for completeness we sketch the main ideas. To compute the Galois closure of the extension L/K we choose a primitive element α of L over K and let $f(x) \in K[x]$ be its minimal polynomial. We then factorize $f(x)$ in $L[x]$ by [8, Alg. 3.6.4]. If all factors of $f(x)$ are linear, then L/K is Galois, otherwise

we adjoin a root β of a non-linear factor to L, and repeat the process with the extension $L(\beta)/K$. To find a primitive element for $L(\beta)/K$ one can for example use [9, Alg. 2.1.11].

The Galois group of the extension L'/K can be computed as a permutation group on the roots of the minimal polynomial of a primitive element. Indeed, if $L' = K(\eta)$, then we only have to factorize the minimal polynomial of η in $L'[x]$ using [8, Alg. 3.6.4].

The decomposition group G of $\mathfrak{P}'$ in the extension L'/K can be computed as $G = \{\sigma \in \mathrm{Gal}(L'/K) : \sigma(a_i) \in \mathfrak{P}' \text{ for all } i = 1, \dots, n\}$, where $a_1, \dots, a_n$ are generators of the $\mathcal{O}_K$-module $\mathfrak{P}'$. The decomposition field K' is the subfield of L' fixed by G. If $L' = K(\eta)$, then K' is generated by the elementary symmetric functions in $\{\eta^\sigma : \sigma \in G\}$ and is therefore computable.

Remark 2.4. We have shown that given a p-adic Galois extension N/M there always exists a Galois extension $(L, \mathfrak{P})/(K, \mathfrak{p})$ such that $L_\mathfrak{P}/K_\mathfrak{p} \cong N/M$. For computational purposes it would be desirable, if the field K (and therefore also L) had small degree over $\mathbb{Q}$. If p is odd, then the results of Henniart [12] imply that there exists a Galois extension $(L, \mathfrak{P})/(K, \mathfrak{p})$ such that $L_\mathfrak{P}/K_\mathfrak{p} \cong N/M$ and $[K : \mathbb{Q}] = [M : \mathbb{Q}_p]$. However, it is not clear to us how to make Henniart's arguments computationally explicit.

2.2. **Ramification groups and Frobenius automorphism.** Let $(L, \mathfrak{P})$ be a global representation of a p-adic field and $v_{L_\mathfrak{P}} : L_\mathfrak{P}^\times \to \mathbb{Z}$ the normalized valuation of the field $L_\mathfrak{P}$. If $x \in L^\times \subset L_\mathfrak{P}^\times$ then $v_{L_\mathfrak{P}}(x)$ is the exponent of $\mathfrak{P}$ in the prime ideal factorization of the principal ideal (x) of L and can therefore be computed by [8, Alg. 4.8.17]. An element $\pi \in L^\times$ is a prime element in $L_\mathfrak{P}$ if and only if $v_{L_\mathfrak{P}}(\pi) = 1$, so in particular any $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$ is a prime in $L_\mathfrak{P}$.

Now let $(L, \mathfrak{P})/(K, \mathfrak{p})$ be a Galois extension and $G = \mathrm{Gal}(L/K) \cong \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$ its Galois group. Recall that for a real number $s \geq -1$ one defines the ramification group G_s of the extension $L_\mathfrak{P}/K_\mathfrak{p}$ to be

$$G_s = \{\sigma \in G : v_{L_\mathfrak{P}}(\sigma a - a) \geq s + 1 \text{ for all } a \in \mathcal{O}_{L_\mathfrak{P}}\}.$$

In particular, $G_{-1} = G$. To compute the groups G_s we first compute $\mathcal{O}_K$-generators $a_1, \dots, a_n$ of $\mathcal{O}_L$. Then $a_1, \dots, a_n$ also generate $\mathcal{O}_{L_\mathfrak{P}}$ as $\mathcal{O}_{K_\mathfrak{p}}$-module and hence

$$G_s = \{\sigma \in G : v_{L_\mathfrak{P}}(\sigma a_i - a_i) \geq s + 1 \text{ for all } i = 1, \dots, n\}.$$

Note that for an integer $s \geq -1$ the condition $v_{L_\mathfrak{P}}(\sigma a_i - a_i) \geq s + 1$ is equivalent to $\sigma a_i - a_i \in \mathfrak{P}^{s+1}$, and is therefore easy to verify computationally.

The group G_0 is the inertia group of the extension $L_\mathfrak{P}/K_\mathfrak{p}$. An element $\sigma \in G$ maps to the Frobenius automorphism in G/G_0 if and only if $\sigma a_i - a_i^{|\mathcal{O}_K/\mathfrak{p}|} \in \mathfrak{P}$ for all $i = 1, \dots, n$ (where $a_1, \dots, a_n$ are $\mathcal{O}_K$-generators of $\mathcal{O}_L$ as above). Clearly such a σ can be found computationally. If $M = L^{G_0}$ and $\mathfrak{p}_M$ is the unique prime of M above $\mathfrak{p}$, then $(M, \mathfrak{p}_M)/(K, \mathfrak{p})$ is a Galois extension which represents the maximal unramified subextension of $L_\mathfrak{P}/K_\mathfrak{p}$.

2.3. **Local class field theory computed globally.** Suppose that $(L, \mathfrak{P})/(K, \mathfrak{p})$ is an abelian Galois extension and let $G = \mathrm{Gal}(L/K) \cong \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. We want to perform class field theoretic computations for the local extension $L_\mathfrak{P}/K_\mathfrak{p}$ by using methods from computational global class field theory for the extension L/K.

The conductor of the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is the $\mathfrak{p}$-part of the conductor of L/K. It can therefore be computed using [9, Alg. 4.4.4]. Similarly, if χ is an abelian character of G, then the conductor of χ considered as a character of $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is the $\mathfrak{p}$-part of the conductor of χ considered as a character of $\mathrm{Gal}(L/K)$. The conductor of χ can therefore be computed as the $\mathfrak{p}$-part of the conductor of $L^{\ker(\chi)}/K$.

Let $\alpha \in K^\times \subset K_{\mathfrak{p}}^\times$. We want to compute the local norm residue symbol $(\alpha, L_{\mathfrak{P}}/K_{\mathfrak{p}}) \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \cong G$ as a global Artin symbol $(\mathfrak{a}, L/K) \in \mathrm{Gal}(L/K) = G$ for a suitable ideal $\mathfrak{a}$ of K. In the following we describe how we can compute such an ideal $\mathfrak{a}$. We refer the reader to [16, Ch. VI] for the necessary facts from global class field theory. We would like to emphasize that we define the conductor of L/K as in [16], i.e. for us the conductor is always an ideal of K and not a modulus consisting of an ideal and an infinite part.

Let $\mathfrak{f}$ be the conductor of L/K. We set $\mathfrak{p}_0 = \mathfrak{p}$ and let $\mathfrak{f} = \prod_{k=0}^{r} \mathfrak{p}_k^{s_k}$ be the prime ideal decomposition of $\mathfrak{f}$, where $s_1, \ldots, s_r > 0$ and $s_0 \geq 0$. We write $J(K)$, resp. $J(L)$, for the idèle group of K, resp. L. For a finite place $\mathfrak{q}$ of K and integer $s \geq 0$ we let $U_{K_{\mathfrak{q}}}^{(s)}$ denote the group of n-units in $K_{\mathfrak{q}}$ (with $U_{K_{\mathfrak{q}}}^{(0)} = \mathcal{O}_{K_{\mathfrak{q}}}^\times$). We let $J_{\mathfrak{f}}(K)$ be the subgroup of idèles $(\gamma_{\mathfrak{q}}) \in J(K)$ such that $\gamma_{\mathfrak{p}_k} \in U_{K_{\mathfrak{p}_k}}^{(s_k)}$ for $k = 0, \ldots, r$ and $\gamma_{\mathfrak{q}} > 0$ for every real place $\mathfrak{q}$. Let $I_{\mathfrak{f}}(K)$, resp. $I_{\mathfrak{f}}(L)$, denote the group of fractional ideals of K, resp. L, which are coprime to $\mathfrak{f}$, and $P_{\mathfrak{f}}(K)$ the subgroup of $I_{\mathfrak{f}}(K)$ which consists of the principal ideals with a generator c such that $c \equiv 1 (\mathrm{mod}^\times\ \mathfrak{f})$ and c is totally positive. Then the relation between local and global class field theory is summarized in the diagram

$$\begin{array}{ccccccc}
\frac{K_{\mathfrak{p}}^\times}{N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}}^\times)} & \longrightarrow & \frac{J(K)}{K^\times N_{L/K}(J(L))} & \xleftarrow{\simeq} & \frac{J_{\mathfrak{f}}(K)}{K^\times N_{L/K}(J(L)) \cap J_{\mathfrak{f}}(K)} & \xrightarrow{\mathrm{cont}} & \frac{I_{\mathfrak{f}}(K)}{P_{\mathfrak{f}}(K) N_{L/K}(I_{\mathfrak{f}}(L))} \\
\downarrow{\scriptstyle (\ ,L_{\mathfrak{P}}/K_{\mathfrak{p}})} & & & & & & \downarrow{\scriptstyle (\ ,L/K)} \\
\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) & & & & & & \mathrm{Gal}(L/K).
\end{array}$$

Here all unnamed maps are the natural ones and cont is induced by taking the content of an idèle. We set $e = v_{\mathfrak{p}}(\alpha)$, and choose an element $\pi \in \mathcal{O}_K$ such that

$$v_{\mathfrak{p}_k}(\pi) = \begin{cases} 0, & \text{if } k = 1, \ldots, r, \\ 1, & \text{if } k = 0. \end{cases}$$

We let $\xi \in \mathcal{O}_K$ denote a solution of the simultaneous congruences

$$\begin{aligned} \xi &\equiv \pi^e (\mathrm{mod}\ \mathfrak{p}_k^{s_k}), \quad k = 1, \ldots, r, \\ \xi &\equiv \frac{\pi^e}{\alpha} (\mathrm{mod}\ \mathfrak{p}_0^{\max(1,s_0)}), \end{aligned}$$

with the additional requirement that $\sigma(\xi/\pi^e) > 0$ for all real embeddings $\sigma : K \hookrightarrow \mathbb{R}$ (such a ξ can be found by a combination of the Chinese remainder theorem and [9, Alg. 4.2.20]). From the above diagram we derive that $(\alpha, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = (\mathfrak{a}, L/K)$ for

$$\mathfrak{a} = \xi \prod_{\mathfrak{q} \mid \pi, \mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{-e v_{\mathfrak{q}}(\pi)}.$$

It remains to compute $(\mathfrak{a}, L/K) \in G$. If

$$\mathfrak{a} = \prod_{j=1}^{l} \mathfrak{q}_j^{e_j}$$

is the prime ideal decomposition of $\mathfrak{a}$, then $(\mathfrak{a}, L/K) = \prod_{j=1}^{l} (\mathfrak{q}_j, L/K)^{e_j}$. For every $\mathfrak{q}_j$ the Artin symbol $(\mathfrak{q}_j, L/K) \in G$ is given by the Frobenius automorphism of $\mathfrak{q}_j$ in L/K. Therefore we can easily determine $(\mathfrak{q}_j, L/K)$ as the unique element g_j in the decomposition group $G_{\mathfrak{q}_j}$ of $\mathfrak{q}_j$ such that

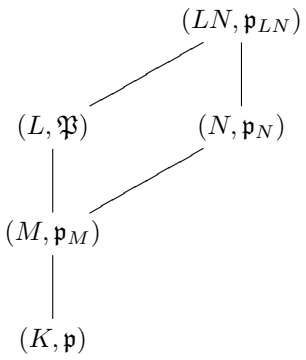
$$g_j(a_i) \equiv {a_i}^{|\mathcal{O}_K/\mathfrak{q}_j|} (\mathrm{mod}\ \mathfrak{Q}_j)$$

for $i = 1, \dots, n$, where $\mathfrak{Q}_j$ is any prime of L above $\mathfrak{q}_j$ and $a_1, \dots, a_n$ are $\mathcal{O}_K$-generators of $\mathcal{O}_L$.

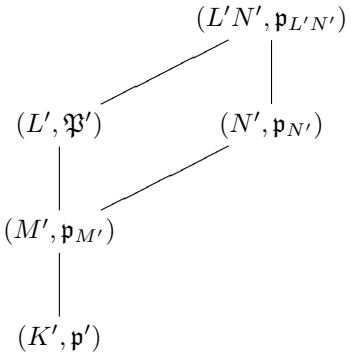
2.4. **Computing the local fundamental class.** Let $(L, \mathfrak{P})/(K, \mathfrak{p})$ be a Galois extension with Galois group $G = \mathrm{Gal}(L/K) \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ (not necessarily abelian). Recall that the local invariant map is a canonical isomorphism $H^2(G, L_{\mathfrak{P}}^{\times}) \cong \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$ and that the preimage of $\frac{1}{|G|} + \mathbb{Z}$ in $H^2(G, L_{\mathfrak{P}}^{\times})$ is called the fundamental class of the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. As in §2.3 we let $U_{L_{\mathfrak{P}}}^{(n)}$ denote the group of n-units in $L_{\mathfrak{P}}$ (with $U_{L_{\mathfrak{P}}}^{(0)} = \mathcal{O}_{L_{\mathfrak{P}}}^{\times}$). In this subsection we describe an algorithm that for any given $n \geq 0$ computes a 2-cocycle $G \times G \to L_{\mathfrak{P}}^{\times}/U_{L_{\mathfrak{P}}}^{(n)}$ which represents the image of the fundamental class under $H^2(G, L_{\mathfrak{P}}^{\times}) \to H^2(G, L_{\mathfrak{P}}^{\times}/U_{L_{\mathfrak{P}}}^{(n)})$. Note that the finitely generated G-module $L_{\mathfrak{P}}^{\times}/U_{L_{\mathfrak{P}}}^{(n)}$ can be computed globally. Indeed, if $\pi \in L$ is a prime element in $L_{\mathfrak{P}}$, then it is not difficult to explicitly describe the action of G on $\pi^{\mathbb{Z}} \times (\mathcal{O}_L/\mathfrak{P}^n)^{\times}$ for which the isomorphism of abelian groups $L_{\mathfrak{P}}^{\times}/U_{L_{\mathfrak{P}}}^{(n)} \cong \pi^{\mathbb{Z}} \times (\mathcal{O}_{L_{\mathfrak{P}}}^{\times}/U_{L_{\mathfrak{P}}}^{(n)}) \cong \pi^{\mathbb{Z}} \times (\mathcal{O}_L/\mathfrak{P}^n)^{\times}$ becomes G-equivariant.

Locally we would like to take the compositum of the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ and the unramified extension of $K_{\mathfrak{p}}$ of degree $|G|$. To obtain a global representation of this situation we proceed as follows. Let $M = L^{G_0}$ be the maximal extension of K in L that is unramified at $\mathfrak{p}$, and write $\mathfrak{p}_M$ for the unique prime of M above $\mathfrak{p}$. Let $(N, \mathfrak{p}_N)/(M, \mathfrak{p}_M)$ be an extension (not necessarily Galois) such that $N_{\mathfrak{p}_N}/M_{\mathfrak{p}_M}$ is the unramified extension of degree $|G|/[M : K]$. Then the compositum LN has a unique prime $\mathfrak{p}_{LN}$ lying over $\mathfrak{p}$ and $(LN)_{\mathfrak{p}_{LN}}$ is the required compositum of $L_{\mathfrak{P}}$ and the unramified extension of $K_{\mathfrak{p}}$ of degree $|G|$. Thus we have constructed the following diagram of extensions.

(1)



Now we apply the method of the proof of Lemma 2.2 to the extension $(LN, \mathfrak{p}_{LN})/(K, \mathfrak{p})$ and obtain a Galois extension $((LN)', \mathfrak{p}_{(LN)'})/(K', \mathfrak{p}')$ such that $K \subseteq K'$, $LN \subseteq (LN)'$, and $(LN)_{\mathfrak{p}_{LN}}/K_{\mathfrak{p}} = (LN)'_{\mathfrak{p}_{(LN)'}}/K'_{\mathfrak{p}'}$. A simple ramification argument shows that LN and K' are linearly disjoint over K. If we form the composita $L' = LK'$, $N' = NK'$ and $M' = MK'$ in $(LN)'$, then $(LN)' = L'N'$ and diagram (1) lifts to the diagram



in which all extensions are Galois. The inclusion of the Galois extension L/K into the Galois extension L'/K' induces an isomorphism of Galois groups $G \cong \mathrm{Gal}(L'/K')$ and an isomorphism of G-modules $L_{\mathfrak{P}}^{\times}/U_{L_{\mathfrak{P}}}^{(n)} \cong L'^{\times}_{\mathfrak{P}'}/U_{L'_{\mathfrak{P}'}}^{(n)}$, and therefore also an isomorphism of cohomology groups

$$H^2\Big(G, L_{\mathfrak{P}}^{\times}/U_{L_{\mathfrak{P}}}^{(n)}\Big) \cong H^2\Big(\mathrm{Gal}(L'/K'), L'^{\times}_{\mathfrak{P}'}/U_{L'_{\mathfrak{P}'}}^{(n)}\Big).$$

Hence if we can compute the required 2-cocycle for the extension $(L', \mathfrak{P}')/(K', \mathfrak{p}')$, then we can also compute such a 2-cocycle for $(L, \mathfrak{P})/(K, \mathfrak{p})$. So it suffices to consider the situation where all extensions in diagram (1) are Galois. We will assume this from now on. To simplify the notation we will simply write $\mathfrak{p}$ for all the prime ideals appearing in (1); it will always be clear from the context which of the prime ideals is meant. Let $\Gamma = \mathrm{Gal}(LN/K)$, $H = \mathrm{Gal}(LN/L)$ and $C = \mathrm{Gal}(N/K)$. Note that the extension $N_{\mathfrak{p}}/K_{\mathfrak{p}}$ is unramified and that therefore C is a cyclic group which is generated by the Frobenius automorphism.

Lemma 2.5. *The inclusion $L_{\mathfrak{p}}^{\times} \subseteq (LN)_{\mathfrak{p}}^{\times}$ induces an isomorphism of G-modules $L_{\mathfrak{p}}^{\times}/U_{L_{\mathfrak{p}}}^{(n)} \cong \big((LN)_{\mathfrak{p}}^{\times}/U_{(LN)_{\mathfrak{p}}}^{(n)}\big)^H$. The inflation map* $\mathrm{inf} : H^2\big(G, L_{\mathfrak{p}}^{\times}/U_{L_{\mathfrak{p}}}^{(n)}\big) \to H^2\big(\Gamma, (LN)_{\mathfrak{p}}^{\times}/U_{(LN)_{\mathfrak{p}}}^{(n)}\big)$ *is injective.*

Proof. We first note that the extension $(LN)_{\mathfrak{p}}/L_{\mathfrak{p}}$ is unramified and that therefore

$$H^i\big(H, U_{(LN)_{\mathfrak{p}}}^{(n)}\big) = 0 \qquad \text{for all} \qquad i \in \mathbb{Z} \tag{2}$$

by [16, V.1.2] and [17, I.1.7.5]. In addition, $U_{L_{\mathfrak{p}}}^{(n)} = \big(U_{(LN)_{\mathfrak{p}}}^{(n)}\big)^H$. Now consider the short exact sequence of Γ-modules

$$0 \to U_{(LN)_{\mathfrak{p}}}^{(n)} \to (LN)_{\mathfrak{p}}^{\times} \to (LN)_{\mathfrak{p}}^{\times}/U_{(LN)_{\mathfrak{p}}}^{(n)} \to 0.$$

Taking H-invariants we obtain the long exact cohomology sequence

$$\begin{aligned}0 &\to U_{L_\mathfrak{p}}^{(n)} \to L_\mathfrak{p}^\times \to \big((LN)_\mathfrak{p}^\times/U_{(LN)_\mathfrak{p}}^{(n)}\big)^H\\ &\to H^1\big(H, U_{(LN)_\mathfrak{p}}^{(n)}\big) \to H^1(H,(LN)_\mathfrak{p}^\times) \to H^1\big(H,(LN)_\mathfrak{p}^\times/U_{(LN)_\mathfrak{p}}^{(n)}\big)\\ &\to H^2\big(H, U_{(LN)_\mathfrak{p}}^{(n)}\big) \to \dots.\end{aligned}$$

Hence equation (2) for $i=1$ implies that we can identify the G-modules $L_\mathfrak{p}^\times/U_{L_\mathfrak{p}}^{(n)}$ and $\big((LN)_\mathfrak{p}^\times/U_{(LN)_\mathfrak{p}}^{(n)}\big)^H$, and Hilbert's Theorem 90 and equation (2) for $i=2$ imply that $H^1\big(H,(LN)_\mathfrak{p}^\times/U_{(LN)_\mathfrak{p}}^{(n)}\big)=0$. Now we deduce the second statement of the lemma from [20, VII, §6, Prop. 5]. □

We now consider the following commutative diagram.

$$\begin{array}{ccc} & & H^2(C,N_\mathfrak{p}^\times)\\ & & \big\downarrow{\scriptstyle \inf}\\ H^2(G,L_\mathfrak{p}^\times) & \xrightarrow{\quad\inf\quad} & H^2(\Gamma,(LN)_\mathfrak{p}^\times)\\ \big\downarrow & & \big\downarrow\\ H^2(G,L_\mathfrak{p}^\times/U_{L_\mathfrak{p}}^{(n)}) & \xrightarrow{\quad\inf\quad} & H^2(\Gamma,(LN)_\mathfrak{p}^\times/U_{(LN)_\mathfrak{p}}^{(n)})\end{array}$$

In the group $H^2(\Gamma,(LN)_\mathfrak{p}^\times)$ the image of the fundamental class of $L_\mathfrak{p}/K_\mathfrak{p}$ under $\inf: H^2(G,L_\mathfrak{p}^\times)\to H^2(\Gamma,(LN)_\mathfrak{p}^\times)$ and the image of the fundamental class of $N_\mathfrak{p}/K_\mathfrak{p}$ under $\inf: H^2(C,N_\mathfrak{p}^\times)\to H^2(\Gamma,(LN)_\mathfrak{p}^\times)$ coincide because $[LN:L]=[LN:N]$, cf. [20, XI, §3 and XIII, §4]. Since by Lemma 2.5 the bottom horizontal map is injective, we can compute the image of the fundamental class of $L_\mathfrak{p}/K_\mathfrak{p}$ under $H^2(G,L_\mathfrak{p}^\times)\to H^2(G,L_\mathfrak{p}^\times/U_{L_\mathfrak{p}}^{(n)})$ in the following three steps:

1. Find the fundamental class of $N_\mathfrak{p}/K_\mathfrak{p}$ in $H^2(C,N_\mathfrak{p}^\times)$.
2. Compute its image under the composite homomorphism
$$H^2(C,N_\mathfrak{p}^\times)\xrightarrow{\inf} H^2(\Gamma,(LN)_\mathfrak{p}^\times)\to H^2(\Gamma,(LN)_\mathfrak{p}^\times/U_{(LN)_\mathfrak{p}}^{(n)}).$$
3. Find the preimage under $H^2(G,L_\mathfrak{p}^\times/U_{L_\mathfrak{p}}^{(n)})\xrightarrow{\inf} H^2(\Gamma,(LN)_\mathfrak{p}^\times/U_{(LN)_\mathfrak{p}}^{(n)})$.

We now explain how these steps can be accomplished computationally. For that purpose we will represent all cohomology classes by inhomogeneous cochains.

Step 1. Let $\pi\in K$ be a prime in $K_\mathfrak{p}$ and $\varphi\in C$ the Frobenius automorphism. For $0\le i,j<[N:K]$ define a map $\gamma: C\times C\to N^\times\subset N_\mathfrak{p}^\times$ by

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

Then a direct computation shows that γ is a 2-cocycle, and using the definition of the local invariant map (see e.g. [17, Ch. VII, §1]) it is not difficult to verify that it represents the fundamental class in $H^2(C,N_\mathfrak{p}^\times)$ (alternatively see [14, §30, Sec. 4 and §31, Sec. 4]).

Step 2. The image of the cohomology class of γ under

$$H^2(C,N_\mathfrak{p}^\times)\xrightarrow{\inf} H^2(\Gamma,(LN)_\mathfrak{p}^\times)\to H^2(\Gamma,(LN)_\mathfrak{p}^\times/U_{(LN)_\mathfrak{p}}^{(n)})$$

is represented by the 2-cocycle γ' which is the composite

$$\Gamma \times \Gamma \to C \times C \xrightarrow{\gamma} N_{\mathfrak{p}}^{\times} \to (LN)_{\mathfrak{p}}^{\times} \to (LN)_{\mathfrak{p}}^{\times}/U_{(LN)_{\mathfrak{p}}}^{(n)}.$$

Since the values of γ lie in $N^{\times}$, we can compute γ' using the global representations of the p-adic fields.

Step 3. We now must find a cocycle $\gamma'' : G \times G \to L_{\mathfrak{p}}^{\times}/U_{L_{\mathfrak{p}}}^{(n)}$ whose cohomology class is mapped to the cohomology class of γ' under the inflation map $H^2(G, L_{\mathfrak{p}}^{\times}/U_{L_{\mathfrak{p}}}^{(n)}) \to H^2(\Gamma, (LN)_{\mathfrak{p}}^{\times}/U_{(LN)_{\mathfrak{p}}}^{(n)})$. This can be achieved by explicitly computing the (inhomogeneous) standard resolution of the G-module $L_{\mathfrak{p}}^{\times}/U_{L_{\mathfrak{p}}}^{(n)}$ and of the Γ-module $(LN)_{\mathfrak{p}}^{\times}/U_{(LN)_{\mathfrak{p}}}^{(n)}$, and by describing the inflation map in terms of these resolutions. All abelian groups in the standard resolution and all homomorphisms (i.e. the boundary homomorphisms and the inflation map on cochains) can be computed effectively, therefore we can apply the algorithms for finitely generated abelian groups in [9, §4.1] to compute the required cocycle γ''.

2.5. **Computation of local epsilon constants and Galois Gauss sums.** Our standard reference for this subsection is [15, Ch. II].

Let $(L, \mathfrak{P})/(K, \mathfrak{p})$ be a Galois extension and $G = \mathrm{Gal}(L/K) \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. The local Galois Gauss sum of a complex valued character χ of G will be denoted by $\tau(\chi) = \tau(L_{\mathfrak{P}}/K_{\mathfrak{p}}, \chi) \in \mathbb{C}^{\times}$ and the Artin conductor by $\mathfrak{f}(\chi)$ (this is an ideal of $K_{\mathfrak{p}}$ which we can identify with a power of the ideal $\mathfrak{p}$ in K). From $\tau(\chi)$ and $\mathfrak{f}(\chi)$ we can obtain the local root number $W(\chi) = W(L_{\mathfrak{P}}/K_{\mathfrak{p}}, \chi)$ by the equation

$$\tau(\chi) = W(\bar{\chi})\sqrt{\mathrm{N}(\mathfrak{f}(\chi))},$$

cf. [15, Ch. II, §4]. In fact, from $\tau(\chi)$ and $\mathfrak{f}(\chi)$ one can also compute the epsilon constants $\varepsilon(\chi, \psi, dx)$ defined in [10] for any non-trivial additive character ψ and Haar measure dx on $K_{\mathfrak{p}}$. Indeed, the formulas [10, (5.3), (5.4)] allow us to reduce to the case where ψ is the standard additive character and dx is the Haar measure which is self-dual with respect to ψ, and in this case the local epsilon constants $\varepsilon(\chi, \psi, dx)$ can be expressed in terms of $W(\chi)$ and $\mathfrak{f}(\chi)$ (using [10, (5.5)] and $W(\chi) = \varepsilon(\chi\omega_{1/2}, \psi, dx)$). In order to compute local epsilon constants it is therefore enough to compute Artin conductors and local Galois Gauss sums.

By definition, $\mathfrak{f}(\chi) = \mathfrak{p}^{n(\chi)}$ where $n(\chi) = \sum_{i=0}^{\infty} \frac{|G_i|}{|G_0|}\mathrm{codim}(V_{\chi}^{G_i})$. Here V_{χ} is a $\mathbb{C}[G]$-module affording the character χ. Since $\dim(V_{\chi}^{G_i}) = \langle 1_{G_i}, \chi|_{G_i}\rangle_{G_i}$, where $\langle , \rangle_{G_i}$ denotes the usual scalar product on characters, we can easily compute $\mathfrak{f}(\chi)$ by applying the results of §2.2. Often the values of the character χ will not be given as complex numbers but as elements of a sufficiently large number field E which is not canonically embedded into $\mathbb{C}$. We remark that the definition of $\mathfrak{f}(\chi)$ makes also sense for these E-valued characters.

In the remainder of this subsection we explain the computation of local Galois Gauss sums. We first observe that the values of all characters χ and the local Galois Gauss sums $\tau(L_{\mathfrak{P}}/K_{\mathfrak{p}}, \chi)$ are complex numbers which are algebraic over $\mathbb{Q}$. This allows us to replace $\mathbb{C}$ by a sufficiently large number field E. More precisely, let E be a number field which satisfies

(a) E is a splitting field for all subgroups of G (so in particular we can apply the results from §3.1),

(b) E contains a fixed primitive p^t-th root of unity ζ_{p^t}, where t is sufficiently large (see Remark 2.6 for a precise statement).

For an E-valued character χ of G we define the E-valued local Galois Gauss sum to be $\iota^{-1}\big(\tau(L_{\mathfrak{P}}/K_{\mathfrak{p}}, \iota\circ\chi)\big)$, where $\iota : E \hookrightarrow \mathbb{C}$ is any embedding which sends ζ_{p^t} to $\exp(2\pi i/p^t)$ (here $i = \sqrt{-1} \in \mathbb{C}$ is fixed once and for all). It follows from [15, Ch. II, Theorem 5.1] that this definition depends only on the fixed p^t-th root of unity $\zeta_{p^t} \in E$. In the following all characters and local Galois Gauss sums are E-valued, and to simplify the notation we will always write $\tau(L_{\mathfrak{P}}/K_{\mathfrak{p}}, \chi)$ instead of $\iota^{-1}(\tau(L_{\mathfrak{P}}/K_{\mathfrak{p}}, \iota\circ\chi))$.

Next we explain how we can compute the standard additive character of a p-adic field which is given by a global representation $(M, \mathfrak{p})$. Recall that the complex valued standard additive character $M_{\mathfrak{p}} \to \mathbb{C}^\times$ is the composite of the following maps

$$M_{\mathfrak{p}} \xrightarrow{(1)} \mathbb{Q}_p \xrightarrow{(2)} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{(3)} \mathbb{Q}/\mathbb{Z} \xrightarrow{(4)} \mathbb{C}^\times$$

where (1) is the trace $\mathrm{Tr}_{M_{\mathfrak{p}}/\mathbb{Q}_p}$, (2) and (3) are canonical and (4) is the complex exponential map $x+\mathbb{Z} \mapsto \exp(2\pi i x)$. Let $\mathcal{D}_{M_{\mathfrak{p}}}$ denote the different of the extension $M_{\mathfrak{p}}/\mathbb{Q}_p$. We define the E-valued standard additive character $\psi_{M_{\mathfrak{p}}} : p^{-t}\mathcal{D}_{M_{\mathfrak{p}}}^{-1} \to E^\times$ to be the composite of the inclusion $p^{-t}\mathcal{D}_{M_{\mathfrak{p}}}^{-1} \hookrightarrow M_{\mathfrak{p}}$, the complex valued standard additive character $M_{\mathfrak{p}} \to \mathbb{C}^\times$ and ι^{-1}, where again $\iota : E \hookrightarrow \mathbb{C}$ is any embedding which sends ζ_{p^t} to $\exp(2\pi i/p^t)$; note that we can use ι^{-1} because $\mathrm{Tr}_{M_{\mathfrak{p}}/\mathbb{Q}_p}(p^{-t}\mathcal{D}_{M_{\mathfrak{p}}}^{-1}) \subseteq p^{-t}\mathbb{Z}_p$.

For $z \in M \cap p^{-t}\mathcal{D}_{M_{\mathfrak{p}}}^{-1}$ we can compute $\psi_{M_{\mathfrak{p}}}(z)$ as follows. Let F be any Galois extension of $\mathbb{Q}$ which contains M, and fix a prime $\mathfrak{q}$ of F lying above the prime $\mathfrak{p}$ of M. Let $\mathcal{G} = \mathrm{Gal}(F/\mathbb{Q})$, $\mathcal{H} = \mathrm{Gal}(F/M)$, and write $\mathcal{G}_{\mathfrak{q}}$ and $\mathcal{H}_{\mathfrak{q}}$ for the decomposition subgroups. Then any set $\{\sigma_1, \dots, \sigma_l\}$ of representatives of $\mathcal{G}_{\mathfrak{q}}/\mathcal{H}_{\mathfrak{q}}$ is a full set of embeddings $\{\sigma : M_{\mathfrak{p}} \hookrightarrow F_{\mathfrak{q}}\}$. Hence $\mathrm{Tr}_{M_{\mathfrak{p}}/\mathbb{Q}_p}(z) = \sum_{i=1}^{l} \sigma_i(z) \in F \cap \mathbb{Q}_p = F^{\mathcal{G}_{\mathfrak{q}}}$ can be computed globally. Next we have to find $r \in \mathbb{Z}[p^{-1}]$ such that

$$\mathrm{Tr}_{M_{\mathfrak{p}}/\mathbb{Q}_p}(z) - r \in \mathbb{Z}_p \cap F = \{x \in F^{\mathcal{G}_{\mathfrak{q}}} : v_{\mathfrak{q}}(x) \geq 0\}.$$

This can be achieved by a finite search because there exists such r with $r \in \{\frac{a}{p^t} : a = 0, \dots, p^t - 1\}$. In this way, if $r = \frac{a}{p^t}$, we obtain

$$\psi_{M_{\mathfrak{p}}}(z) = \iota^{-1}(\exp(2\pi i r)) = \zeta_{p^t}^a.$$

We now describe the computation of the local Galois Gauss sum $\tau(L_{\mathfrak{P}}/K_{\mathfrak{p}}, \chi) \in E$, where χ is an E-valued character of G. To simplify the notation we write $M_{\mathfrak{p}}$ in place of $M_{\mathfrak{P}\cap M}$ for any intermediate field M of L/K. Using the algorithm in §3.1 we can write

$$\chi - \chi(1)1_G = \sum_{(H,\varphi)} c_{(H,\varphi)} \mathrm{ind}_H^G(\varphi - 1_H) \tag{3}$$

where 1_H denotes the trivial character of a subgroup H of G. Since the local Galois Gauss sums are additive, inductive in degree 0, and equal to 1 for the trivial

character, we have

$$\begin{aligned}\tau(L_\mathfrak{p}/K_\mathfrak{p},\chi) &= \tau(L_\mathfrak{p}/K_\mathfrak{p},\chi-\chi(1)1_G)\\ &= \prod_{(H,\varphi)} \tau\big(L_\mathfrak{p}/K_\mathfrak{p},\mathrm{ind}_H^G(\varphi-1_H)\big)^{c_{(H,\varphi)}}\\ &= \prod_{(H,\varphi)} \tau\big(L_\mathfrak{p}/(L^H)_\mathfrak{p},\varphi\big)^{c_{(H,\varphi)}}.\end{aligned}$$

It therefore suffices to compute $\tau(L_\mathfrak{p}/M_\mathfrak{p},\varphi)$ where M is an intermediate field of L/K and φ is a character of $\mathrm{Gal}(L/M)$ of degree one. If $N=L^{\ker(\varphi)}$, then $\tau(L_\mathfrak{p}/M_\mathfrak{p},\varphi)=\tau(N_\mathfrak{p}/M_\mathfrak{p},\varphi)$. Thus we are reduced to the abelian case.

Suppose now that $(N,\mathfrak{p})/(M,\mathfrak{p})$ is abelian and φ is a character of $\mathrm{Gal}(N/M)$ of degree one. We set $s=v_\mathfrak{p}(\mathfrak{f}(\varphi))$, and compute an element $c\in M$ which generates the ideal $\mathfrak{f}(\varphi)\mathcal{D}_{M_\mathfrak{p}}$ of $\mathcal{O}_{M_\mathfrak{p}}$. Note that s and c can be computed globally. The local Galois Gauss sum $\tau(N_\mathfrak{p}/M_\mathfrak{p},\varphi)$ is given by the explicit formula

$$\tau(N_\mathfrak{p}/M_\mathfrak{p},\varphi)=\sum_x \varphi\left(\left(\frac{x}{c},N_\mathfrak{p}/M_\mathfrak{p}\right)\right)\psi_{M_\mathfrak{p}}\left(\frac{x}{c}\right), \tag{4}$$

where x runs through a set of representatives of $\mathcal{O}_{M_\mathfrak{p}}^\times$ modulo $U_{M_\mathfrak{p}}^{(s)}$. These representatives can be computed globally because $\mathcal{O}_{M_\mathfrak{p}}^\times/U_{M_\mathfrak{p}}^{(s)}\cong(\mathcal{O}_M/\mathfrak{p}^s)^\times$. The local norm residue symbols $(y,N_\mathfrak{p}/M_\mathfrak{p})$ for $y\in M^\times\subseteq M_\mathfrak{p}^\times$ can be computed as explained in §2.3, and the values of $\psi_{M_\mathfrak{p}}$ can be computed as explained above.

Remark 2.6. The integer t must be sufficiently large to ensure that $\psi_{M_\mathfrak{p}}\left(\frac{x}{c}\right)$ in (4) is defined, i.e. we must have $x/c\in p^{-t}\mathcal{D}_{M_\mathfrak{p}}^{-1}$. An easy calculation shows that this is satisfied if $t\geq\frac{s}{e(M_\mathfrak{p}/\mathbb{Q}_p)}$ where $e(M_\mathfrak{p}/\mathbb{Q}_p)$ is the ramification index of the extension $M_\mathfrak{p}/\mathbb{Q}_p$. Hence t must be an integer which satisfies $t\geq\frac{v_\mathfrak{p}(\mathfrak{f}(\varphi))}{e((L^H)_\mathfrak{p}/\mathbb{Q}_p)}$ for all pairs (H,φ) with $c_{(H,\varphi)}\neq 0$. In particular, we can determine a suitable t as soon as (3) is computed.

2.6. **Computation of (integral) normal bases.** Let $(L,\mathfrak{P})/(K,\mathfrak{p})$ be a Galois extension and $G=\mathrm{Gal}(L/K)\cong\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. Our intention is to compute an element $a\in L$ that generates a normal basis of the extension $L_\mathfrak{P}/K_\mathfrak{p}$, i.e. such that $\{\sigma(a):\sigma\in G\}$ is a basis of $L_\mathfrak{P}$ as $K_\mathfrak{p}$-vector space. Applying an algorithm of Girstmair [11] we compute a normal basis element $a\in L$ for the global extension L/K. Since $L_\mathfrak{P}=L\otimes_K K_\mathfrak{p}=LK_\mathfrak{p}$ the element a also generates a normal basis for $L_\mathfrak{P}/K_\mathfrak{p}$.

Now assume that $L_\mathfrak{P}/K_\mathfrak{p}$ is at most tamely ramified. Then by a theorem of Noether the ring of integers $\mathcal{O}_{L_\mathfrak{P}}$ is a free $\mathcal{O}_{K_\mathfrak{p}}[G]$-module of rank 1. In this situation we want to compute an integral normal basis, i.e. an element $a\in\mathcal{O}_{L_\mathfrak{P}}$ such that $\{\sigma(a):\sigma\in G\}$ is a $\mathcal{O}_{K_\mathfrak{p}}$-basis of $\mathcal{O}_{L_\mathfrak{P}}$. Since $\mathcal{O}_{L_\mathfrak{P}}$ is a free $\mathcal{O}_{K_\mathfrak{p}}[G]$-module it follows that $\mathcal{O}_{L_\mathfrak{P}}/\mathfrak{p}\mathcal{O}_{L_\mathfrak{P}}\cong\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a free $(\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})[G]\cong(\mathcal{O}_K/\mathfrak{p})[G]$-module. If $a\in\mathcal{O}_L$ is any element with the property that the image of a in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a basis of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ as $(\mathcal{O}_K/\mathfrak{p})[G]$-module, then a generates an integral normal basis of $\mathcal{O}_{L_\mathfrak{P}}$ by Nakayama's lemma. Since $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is finite, such an element $a\in\mathcal{O}_L$ can be found computationally.

3. Algorithms for representation theory

In this section we develop algorithms which are representation theoretic in nature. One of these algorithms was already used in §2.5, and the other algorithms are needed for §4.

3.1. **Computational Brauer induction.** Let G be a finite group and E a finite extension of $\mathbb{Q}$ which is a splitting field of every subgroup of G. A sufficient condition for this to be satisfied is that E contains the m-th roots of unity where m is the exponent of G, cf. [19, §12.3, Theorem 24] or [14, §33, Satz 15]. In the following, all the (virtual) characters we consider have values in the field E. We write $R(G)$ for the group of all virtual characters of G, and $\mathrm{Irr}(G)$ for the set of irreducible characters.

By Brauer's induction theorem every virtual character $\chi \in R(G)$ can be written (in general non-uniquely) as

$$\chi = \sum_{(H,\varphi)} c_{(H,\varphi)} \mathrm{ind}_H^G(\varphi), \tag{5}$$

where (H, φ) runs through all pairs consisting of a subgroup H of G and a one-dimensional character φ of H, $\mathrm{ind}_H^G(\varphi)$ is the induction of the character φ, and the coefficients $c_{(H,\varphi)}$ are rational integers. For a given $\chi \in R(G)$ we want to compute such coefficients $c_{(H,\varphi)}$.

First note that for any subgroup H of G we can represent a virtual character $\varphi \in R(H)$ as a function from the conjugacy classes of H to E. This representation also allows us to compute the induced character $\mathrm{ind}_H^G(\varphi)$. The set $\mathrm{Irr}(G)$ of irreducible characters of G can be computed, for example using the Dixon-Schneider algorithm. It is well-known that $\mathrm{Irr}(G)$ is a $\mathbb{Z}$-basis of $R(G)$, and that for any $\chi \in R(G)$ we can easily compute the coefficients with respect to this basis using the scalar product of characters.

Now given $\chi \in R(G)$ we can compute coefficients $c_{(H,\varphi)} \in \mathbb{Z}$ as in (5) as follows. We let $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_r\}$ and compute coefficients $b_i \in \mathbb{Z}$ such that $\chi = \sum_{i=1}^r b_i \chi_i$. For each pair (H, φ) we compute coefficients $a_{(H,\varphi),i} \in \mathbb{Z}$ such that $\mathrm{ind}_H^G(\varphi) = \sum_{i=1}^r a_{(H,\varphi),i} \chi_i$. Then we obtain coefficients $c_{(H,\varphi)}$ as an integer solution of the system of linear equations

$$\sum_{(H,\varphi)} a_{(H,\varphi),i} c_{(H,\varphi)} = b_i, \quad i = 1, \ldots, r.$$

To find such an integer solution we apply the Hermite normal form techniques of [8, §2.4].

Remark 3.1. Alternatively, one can compute canonical coefficients $c_{(H,\varphi)}$ by using Boltje's Brauer induction formula, cf. [4].

In §2.5 we applied the following variant of Brauer's induction theorem. Let $\chi \in R(G)$ be of degree 0. We denote the trivial character of a subgroup H of G by 1_H. There exist rational integers $c'_{(H,\varphi)}$ such that

$$\chi = \sum_{(H,\varphi)} c'_{(H,\varphi)} \mathrm{ind}_H^G(\varphi - 1_H)$$

where again (H,φ) runs through all pairs as above (cf. [19, Exercise 10.6]). Obviously, with a slight variation of the argument above, it is possible to compute coefficients $c'_{(H,\varphi)}$ in this situation.

3.2. **Computing reduced norms.** As in §3.1 we consider a finite group G and a finite extension E of $\mathbb{Q}$ which is a splitting field of every subgroup of G. For $a \in E[G]^\times$ we want to compute the reduced norm $\mathrm{nr}(a) \in \prod_{\chi\in\mathrm{Irr}(G)} E^\times$ which is defined as follows. Let $E[G] = \prod_{\chi\in\mathrm{Irr}(G)} A_\chi$ be the Wedderburn decomposition of $E[G]$ and $a = (a_\chi)_{\chi\in\mathrm{Irr}(G)}$ under this decomposition. Then $\mathrm{nr}(a) = (\mathrm{nr}_{A_\chi/E}(a_\chi))_{\chi\in\mathrm{Irr}(G)}$, where $\mathrm{nr}_{A_\chi/E}(a_\chi) \in E^\times$ is the reduced norm of the element a_χ in the central simple E-algebra A_χ.

For every character χ of G we define $\mathrm{Det}_\chi(a) \in E^\times$ by $\mathrm{Det}_\chi(a) = \det(T_\chi(a))$ where $T_\chi : G \to \mathrm{GL}_{\chi(1)}(E)$ is a representation with character χ (extended linearly to $T_\chi : E[G] \to \mathrm{Mat}_{\chi(1)}(E)$). Since $\mathrm{Det}_{\chi_1+\chi_2}(a) = \mathrm{Det}_{\chi_1}(a)\cdot\mathrm{Det}_{\chi_2}(a)$ we can define $\mathrm{Det}_\chi(a)$ for a virtual character χ. Now if $a = (a_\chi)_{\chi\in\mathrm{Irr}(G)}$ is as above, then for $\chi \in \mathrm{Irr}(G)$ we have $\mathrm{nr}_{A_\chi/E}(a_\chi) = \mathrm{Det}_\chi(a)$. However, for given $\chi \in \mathrm{Irr}(G)$ it is in general a very difficult problem to compute an explicit matrix representation $T_\chi : G \to \mathrm{GL}_{\chi(1)}(E)$ with character χ. We use Brauer induction to reduce the computation of $\mathrm{Det}_\chi(a)$ to the computation of $\mathrm{Det}_\psi(a)$ for characters ψ for which we can easily compute corresponding matrix representations.

More precisely, let $\chi \in \mathrm{Irr}(G)$ and use the algorithm from §3.1 to compute integers $c_{(H,\varphi)}$ such that $\chi = \sum_{(H,\varphi)} c_{(H,\varphi)}\mathrm{ind}_H^G(\varphi)$, where (H,φ) runs through pairs of subgroups H of G and one-dimensional characters φ of H. Then

$$\mathrm{nr}_{A_\chi/E}(a_\chi) = \mathrm{Det}_\chi(a) = \prod_{(H,\varphi)} \mathrm{Det}_{\mathrm{ind}_H^G(\varphi)}(a)^{c_{(H,\varphi)}}.$$

It is not difficult to compute $\mathrm{Det}_{\mathrm{ind}_H^G(\varphi)}(a)$ because φ is one-dimensional and we can therefore easily construct an explicit matrix representation with character $\mathrm{ind}_H^G(\varphi)$ (for example by using [19, Exercise 3.5]).

We will also need the reduced norm map

$$K_1(E[G]) \xrightarrow{\mathrm{nr}} \prod_{\chi\in\mathrm{Irr}(G)} E^\times.$$

Explicitly, if $A = (a_{ij}) \in \mathrm{GL}_n(E[G])$ represents an element $a \in K_1(E[G])$, then we set $\mathrm{Det}_\chi(a) = \det(T_\chi(A))$ for each character χ of G, where $T_\chi(A) = (T_\chi(a_{ij})) \in \mathrm{GL}_{n\chi(1)}(E)$. Then one has

$$\mathrm{nr}(a) = (\mathrm{Det}_\chi(a))_{\chi\in\mathrm{Irr}(G)}.$$

Since again $\mathrm{Det}_{\chi_1+\chi_2}(a) = \mathrm{Det}_{\chi_1}(a)\cdot\mathrm{Det}_{\chi_2}(a)$, we can proceed as above and use Brauer induction to compute $\mathrm{Det}_\chi(a)$ for $\chi \in \mathrm{Irr}(G)$.

3.3. **Computations in relative algebraic K-groups.** Let G be a finite group and E a finite Galois extension of $\mathbb{Q}$ which is a splitting field of every subgroup of G. Let p be a prime number and fix a prime ideal $\mathfrak{Q}$ of E over p. In this subsection we discuss computational questions in the relative algebraic K-group $K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$. We refer the reader to [21, p. 215] for the definition of this group in terms of generators and relations, and to [3, §2] or [6, §2.2] for a summary of some of its properties.

First we recall that there exists the following commutative diagram with exact rows.

$$\begin{array}{ccccccc} K_1(\mathbb{Z}_p[G]) & \longrightarrow & K_1(\mathbb{Q}_p[G]) & \longrightarrow & K_0(\mathbb{Z}_p[G],\mathbb{Q}_p) & \longrightarrow & 0 \\ \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle \subseteq} & & \downarrow{\scriptstyle \subseteq} & & \\ K_1(\mathbb{Z}_p[G]) & \longrightarrow & K_1(E_{\mathfrak{Q}}[G]) & \longrightarrow & K_0(\mathbb{Z}_p[G],E_{\mathfrak{Q}}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{nr}}\ {\scriptstyle \simeq} & & & & \\ & & \prod_{\mathrm{Irr}(G)} E_{\mathfrak{Q}}^{\times} & & & & \end{array} \tag{6}$$

We also recall that for a semilocal ring R the canonical map $R^{\times} \longrightarrow K_1(R)$ is surjective. In particular we have epimorphisms

$$\mathbb{Z}_p[G]^{\times} \longrightarrow K_1(\mathbb{Z}_p[G]), \quad \mathbb{Q}_p[G]^{\times} \longrightarrow K_1(\mathbb{Q}_p[G]). \tag{7}$$

From diagram (6) it is clear that tuples $(a_\chi)_{\chi\in\mathrm{Irr}(G)} \in \prod_{\mathrm{Irr}(G)} E^{\times} \subset \prod_{\mathrm{Irr}(G)} E_{\mathfrak{Q}}^{\times}$ represent elements in $K_0(\mathbb{Z}_p[G],E_{\mathfrak{Q}})$. Note that in general not every element in $K_0(\mathbb{Z}_p[G],E_{\mathfrak{Q}})$ is represented by a tuple $(a_\chi)_{\chi\in\mathrm{Irr}(G)}$ with all $a_\chi \in E^{\times}$, but we shall see that all the elements we are interested in have this property.

If P and Q are finitely generated projective $\mathbb{Z}[G]$-modules and $\varphi : P\otimes E \to Q\otimes E$ is an isomorphism of $E[G]$-modules, then we obtain an element $[P\otimes_{\mathbb{Z}}\mathbb{Z}_p, \varphi\otimes_E E_{\mathfrak{Q}}, Q\otimes_{\mathbb{Z}}\mathbb{Z}_p]$ in $K_0(\mathbb{Z}_p[G],E_{\mathfrak{Q}})$. This element has a representative in $\prod_{\mathrm{Irr}(G)} E^{\times}$ which can be computed as follows. Since P is projective over $\mathbb{Z}[G]$ we know that $P\otimes\mathbb{Z}_p$ is free over $\mathbb{Z}_p[G]$ and we can therefore compute elements $e_1,\dots,e_n \in P$ such that $e_1\otimes 1,\dots,e_n\otimes 1 \in P\otimes\mathbb{Z}_p$ is a $\mathbb{Z}_p[G]$-basis (this is a finite problem because by Nakayama's lemma any lift of a $(\mathbb{Z}/p\mathbb{Z})[G]$-basis of P/pP works). Similarly we can compute $f_1,\dots,f_n \in Q$ such that $f_1\otimes 1,\dots,f_n\otimes 1 \in Q\otimes\mathbb{Z}_p$ is a $\mathbb{Z}_p[G]$-basis of $Q\otimes\mathbb{Z}_p$. With respect to these bases we then express the isomorphism φ as a matrix A in $\mathrm{GL}_n(E[G])$. The triple $[P\otimes\mathbb{Z}_p, \varphi\otimes E_{\mathfrak{Q}}, Q\otimes\mathbb{Z}_p]$ is represented by $\mathrm{nr}(A) \in \prod_{\mathrm{Irr}(G)} E^{\times}$, which can be computed as described at the end of §3.2.

From (6) and (7) we derive that the element represented by a tuple $(a_\chi) \in \prod_{\mathrm{Irr}(G)} E^{\times} \subset \prod_{\mathrm{Irr}(G)} E_{\mathfrak{Q}}^{\times}$ lies in the subgroup $K_0(\mathbb{Z}_p[G],\mathbb{Q}_p)$ of $K_0(\mathbb{Z}_p[G],E_{\mathfrak{Q}})$ if and only if (a_χ) lies in the subgroup $\mathrm{nr}(\mathbb{Q}_p[G]^{\times})$ of $\prod_{\mathrm{Irr}(G)} E_{\mathfrak{Q}}^{\times}$. This is equivalent to $\omega(a_\chi) = a_{\omega\circ\chi}$ for all $\chi \in \mathrm{Irr}(G)$ and all $\omega \in \mathrm{Gal}(E_{\mathfrak{Q}}/\mathbb{Q}_p)$. It can be tested computationally because since $a_\chi \in E$ it is equivalent to $\omega(a_\chi) = a_{\omega\circ\chi}$ for all $\chi \in \mathrm{Irr}(G)$ and all $\omega \in \mathrm{Gal}(E/\mathbb{Q})_{\mathfrak{Q}}$ (the decomposition group of $\mathfrak{Q}$).

Finally we want an algorithm to decide whether a tuple $(a_\chi) \in \prod_{\mathrm{Irr}(G)} E^{\times} \subset \prod_{\mathrm{Irr}(G)} E_{\mathfrak{Q}}^{\times}$ represents the zero element in $K_0(\mathbb{Z}_p[G],E_{\mathfrak{Q}})$. It follows from (6) and (7) that (a_χ) represents 0 in $K_0(\mathbb{Z}_p[G],E_{\mathfrak{Q}})$ if and only $(a_\chi) \in \mathrm{nr}(\mathbb{Z}_p[G]^{\times})$. Let $\mathcal{M}$ denote a maximal order in $\mathbb{Q}_p[G]$ containing $\mathbb{Z}_p[G]$. Let m be a positive integer such that $p^m\mathcal{M}$ is contained in the Jacobson radical $\mathrm{rad}(\mathbb{Z}_p[G])$ of $\mathbb{Z}_p[G]$ (for example we can take $m = v_p(|G|)+1$). Note that the maximal order $\mathcal{M}$ is only needed to justify the correctness of the following algorithm; in the algorithm itself we need only m and it is not necessary to compute $\mathcal{M}$. Choose a set of representatives $r_1,\dots,r_l \in \mathbb{Z}[G]$ for the finite group $(\mathbb{Z}[G]/p^m\mathbb{Z}[G])^{\times}$. The isomorphisms

$$(\mathbb{Z}[G]/p^m\mathbb{Z}[G])^{\times} \cong (\mathbb{Z}_p[G]/p^m\mathbb{Z}_p[G])^{\times} \cong \mathbb{Z}_p[G]^{\times}/(1+p^m\mathbb{Z}_p[G])$$

(where the second isomorphism follows from [2, Lemma 3.6]) imply that $r_1, \dots, r_l$ is also a set of representatives of $\mathbb{Z}_p[G]^\times/(1+p^m\mathbb{Z}_p[G])$. From the inclusions

$$\mathrm{nr}(1+p^m\mathbb{Z}_p[G]) \subseteq \mathrm{nr}(1+p^m\mathcal{M}) \subseteq \mathrm{nr}(\mathbb{Z}_p[G]^\times)$$

it therefore follows that $(a_\chi) \in \mathrm{nr}(\mathbb{Z}_p[G]^\times)$ if and only if $\mathrm{nr}(r_i)\cdot(a_\chi) \in \mathrm{nr}(1+p^m\mathcal{M})$ for (at least) one of the r_i. To test if a tuple lies in $\mathrm{nr}(1+p^m\mathcal{M})$ we use the criterion stated in the following lemma.

Lemma 3.2. *A tuple $(b_\chi) \in \prod_{\mathrm{Irr}(G)} E_\mathfrak{Q}^\times$ lies in $\mathrm{nr}(1+p^m\mathcal{M})$ if and only if the following two conditions are satisfied:*

(1) $(b_\chi) \in \mathrm{nr}(\mathbb{Q}_p[G]^\times)$.
(2) $b_\chi \in 1+p^m\mathcal{O}_{E_\mathfrak{Q}}$ *for all* $\chi \in \mathrm{Irr}(G)$.

Proof. Let $\mathbb{Q}_p[G] \cong \prod_i \mathrm{Mat}_{m_i}(D_i)$ be the Wedderburn decomposition of $\mathbb{Q}_p[G]$. We denote the center of the skew field D_i by K_i. The maximal order $\mathcal{M} \subset \mathbb{Q}_p[G]$ decomposes as $\mathcal{M} \cong \prod_i \mathcal{M}_i$, where each $\mathcal{M}_i$ is a maximal order in $\mathrm{Mat}_{m_i}(D_i)$. From [2, Corollary 2.3] we deduce that $\mathrm{nr}_{\mathrm{Mat}_{m_i}(D_i)/K_i}(1+p^m\mathcal{M}_i) = 1+p^m\mathcal{O}_{K_i} \subset K_i^\times$. The inclusion $\prod_i K_i^\times \cong \mathrm{nr}(\mathbb{Q}_p[G]^\times) \subseteq \prod_{\mathrm{Irr}(G)} E_\mathfrak{Q}^\times$ identifies $\prod_i K_i^\times$ with

$$\left\{(b_\chi) \in \prod_{\chi\in\mathrm{Irr}(G)} E_\mathfrak{Q}^\times : \omega(b_\chi) = b_{\omega\circ\chi} \text{ for all } \chi \text{ and all } \omega \in \mathrm{Gal}(E_\mathfrak{Q}/\mathbb{Q}_p)\right\}.$$

Under this identification $\prod_i(1+p^m\mathcal{O}_{K_i})$ corresponds to

$$\left\{(b_\chi) \in \prod_{\chi\in\mathrm{Irr}(G)} E_\mathfrak{Q}^\times : \omega(b_\chi) = b_{\omega\circ\chi} \text{ for all } \chi \text{ and all } \omega \in \mathrm{Gal}(E_\mathfrak{Q}/\mathbb{Q}_p), \text{ and } b_\chi \in 1+p^m\mathcal{O}_{E_\mathfrak{Q}} \text{ for all } \chi\right\}.$$

From this the result follows. □

Hence a tuple $(a_\chi) \in \prod_{\mathrm{Irr}(G)} E^\times$ represents 0 in $K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$ if and only if $(a_\chi) \in \mathrm{nr}(\mathbb{Q}_p[G]^\times)$ and for (at least) one of the representatives r_i the tuple $(b_\chi) = \mathrm{nr}(r_i)\cdot(a_\chi)$ has the property that $v_\mathfrak{Q}((b_\chi-1)/p^m) \geq 0$ for all $\chi \in \mathrm{Irr}(G)$.

4. Algorithms to prove epsilon constant conjectures

In this section we describe our algorithmic approach to various epsilon constant conjectures. In §4.1 we quickly recall the relevant facts about these conjectures and show that from an algorithm for the local conjecture one can easily deduce algorithms for the global conjectures; this will prove Corollaries 1.2 and 1.3. In §4.2 we then develop our main algorithm for the local epsilon constant conjecture, which demonstrates Theorem 1.1. We conclude with some computational remarks in §4.3.

4.1. **The epsilon constant conjectures.** Let L/K be a Galois extension of p-adic fields and $G = \mathrm{Gal}(L/K)$. The local epsilon constant conjecture of [6] is a conjecture relating the equivariant local Galois Gauss sum of L/K to a natural cohomological invariant of this extension. More precisely the equality

$$T_{L/K} + E_{L/K}(\exp(\mathcal{L}))_p - [\mathcal{L}, \rho_L, H_L] + U_{L/K} - M_{L/K} = 0 \tag{8}$$

is conjectured to hold in the relative algebraic K-group $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p^c)$, where $\mathbb{Q}_p^c$ is an algebraic closure of $\mathbb{Q}_p$. We only sketch the ideas behind the invariants appearing in (8); for the precise definitions and a detailed discussion see [6, §2]. The invariant $T_{L/K}$ comes from the local Galois Gauss sums of all irreducible characters of L/K, and $U_{L/K}$ is an unramified counterpart of $T_{L/K}$. The term $M_{L/K}$ is an explicit correction term (it is essentially a quotient of leading terms of local L-factors). Next, $\mathcal{L}$ is any full projective $\mathbb{Z}_p[G]$-lattice contained in a sufficiently large power of the maximal ideal of $\mathcal{O}_L$ (the validity of the conjecture is independent of the choice of $\mathcal{L}$), and $E_{L/K}(\exp(\mathcal{L}))_p$ is an Euler characteristic of a cochain complex constructed from the local fundamental class in $H^2(G, L^\times)$. Finally, $[\mathcal{L}, \rho_L, H_L]$ is given explicitly in terms of all embeddings $L \hookrightarrow \mathbb{Q}_p^c$.

Now we consider a Galois extension L/K of number fields with Galois group $G = \mathrm{Gal}(L/K)$. The global epsilon constant conjecture of [3] is a conjectural equality in the relative algebraic K-group $K_0(\mathbb{Z}[G], \mathbb{R})$, which relates the equivariant global epsilon constant of L/K to natural semi-local cohomological invariants. It can be shown that this conjecture splits into p-parts for all rational prime numbers p, and that the validity of the p-part of the global conjecture for L/K is closely related to the validity of the local conjectures for all completions of L/K at primes above p. This is discussed in detail in [6, §4]. Finally we recall that the $\Omega(2)$-conjecture for the global extension L/K (as formulated in [7]) is the conjectural equality of the Cassou-Noguès–Fröhlich root number class of L/K and of Chinburg's invariant $\Omega(L/K, 2)$ in the projective class group $\mathrm{Cl}(\mathbb{Z}[G])$. It is shown in [3, Remark 4.2(iv)] that the $\Omega(2)$-conjecture for L/K is the image of the global epsilon constant conjecture under the canonical projection $K_0(\mathbb{Z}[G], \mathbb{R}) \to \mathrm{Cl}(\mathbb{Z}[G])$.

In §4.2 we will prove Theorem 1.1, i.e. we will describe an algorithm to prove or disprove the local epsilon constant conjecture for all Galois extensions $L/\mathbb{Q}_p$ of degree n. Assuming this result for the moment we now deduce Corollaries 1.2 and 1.3.

Proof of Corollary 1.2. For every prime number p dividing n use the algorithm in Theorem 1.1 to prove the local epsilon constant conjecture for all extensions $M/\mathbb{Q}_p$ of degree dividing n (or to find a counterexample to the local conjecture). The validity of all these local conjectures implies the validity of the global conjecture for all Galois extensions $L/\mathbb{Q}$ of degree n. Indeed, if $p \mid n$, then the validity of the p-part of the global conjecture follows from the local conjectures by [6, Cor. 4.2]. If $p \nmid n$, then $K_0(\mathbb{Z}_p[\mathrm{Gal}(L/\mathbb{Q})], \mathbb{Q}_p)$ is torsion free. Hence the p-part of the global conjecture follows from [3, Cor. 6.3(i)]. □

Proof of Corollary 1.3. By [3, Remark 4.2(iv)], the global epsilon constant conjecture for $L/\mathbb{Q}$ implies Chinburg's $\Omega(2)$-conjecture for $L/\mathbb{Q}$. Hence Corollary 1.3 follows from Corollary 1.2. □

Remark 4.1. Suppose that the algorithm of Corollary 1.2 finds a counterexample to the local epsilon constant conjecture. If p is an odd prime number, then by a result of Henniart [12] and the discussion in [6, §4.1] we know that there exists a Galois extension of number fields for which the global conjecture fails, though not necessarily an extension $L/\mathbb{Q}$ of degree n. However, if the counterexample to the local conjecture is a Galois extension of p-adic fields with $p = 2$, then we cannot conclude that this disproves the global epsilon constant conjecture.

4.2. **The algorithm for the local epsilon constant conjecture.** In this subsection we describe the algorithm whose existence was stated in Theorem 1.1. We first roughly explain the complete algorithm and then give further details for the individual steps.

In the initial step we compute a list of Galois extensions $(L,\mathfrak{P})/(K,\mathfrak{p})$ with $K_\mathfrak{p}=\mathbb{Q}_p$ such that the extensions $L_\mathfrak{P}/K_\mathfrak{p}$ form a complete list of all Galois extensions of $\mathbb{Q}_p$ of degree n. Then for each Galois extension $(L,\mathfrak{P})/(K,\mathfrak{p})$ in this list we verify the local epsilon constant conjecture for $L_\mathfrak{P}/K_\mathfrak{p}$. Let $(L,\mathfrak{P})/(K,\mathfrak{p})$ be one of these extensions and $G=\mathrm{Gal}(L/K)\cong\mathrm{Gal}(L_\mathfrak{P}/\mathbb{Q}_p)$. We construct a number field E and a prime $\mathfrak{Q}$ of E above p such that all invariants appearing in (8) lie in the subgroup $K_0(\mathbb{Z}_p[G],E_\mathfrak{Q})$ of $K_0(\mathbb{Z}_p[G],\mathbb{Q}_p^c)$. Thus these invariants can be represented by tuples in $\prod_{\mathrm{Irr}(G)}E_\mathfrak{Q}^\times$, and in fact, as we shall see, by tuples in $\prod_{\mathrm{Irr}(G)}E^\times$. We will compute a representing tuple for each invariant, and finally verify that the product of these tuples represents 0 in $K_0(\mathbb{Z}_p[G],E_\mathfrak{Q})$. In §4.2.1 we describe the construction of the list of extensions $(L,\mathfrak{P})/(K,\mathfrak{p})$, and in §4.2.2 – §4.2.9 we then explain how for any extension in this list we can verify the corresponding local epsilon constant conjecture.

4.2.1. *Constructing the Galois extensions.* Using the algorithm of Pauli and Roblot [18] we can compute all extensions of $\mathbb{Q}_p$ of degree n. In fact, we can compute these extensions as global representations $(L,\mathfrak{P})/(\mathbb{Q},p)$. We are only interested in extensions $(L,\mathfrak{P})/(\mathbb{Q},p)$ for which $L_\mathfrak{P}/\mathbb{Q}_p$ is Galois. To check for which extensions this is the case we can use Panayi's root finding algorithm (which is explained in [18, §8]) to test whether the minimal polynomial of a primitive element of $L_\mathfrak{P}/\mathbb{Q}_p$ splits into linear factors over $L_\mathfrak{P}$. Alternatively we could test whether $\mathfrak{P}$ is completely split in the Galois closure of L over $\mathbb{Q}$ (this is equivalent to $L_\mathfrak{P}/\mathbb{Q}_p$ being Galois).

For every extension $(L,\mathfrak{P})/(\mathbb{Q},p)$ for which $L_\mathfrak{P}/\mathbb{Q}_p$ is Galois we then use Lemma 2.2 to compute a Galois extension $(L',\mathfrak{P}')/(K',\mathfrak{p}')$ which represents $L_\mathfrak{P}/\mathbb{Q}_p$.

Thus we have constructed a finite list of Galois extensions $(L,\mathfrak{P})/(K,\mathfrak{p})$ representing all Galois extensions of $\mathbb{Q}_p$ of degree n. For each of these extensions we now perform the steps in §4.2.2 – §4.2.9. Let G denote the Galois group $\mathrm{Gal}(L/K)\cong\mathrm{Gal}(L_\mathfrak{P}/\mathbb{Q}_p)$.

4.2.2. *Constructing the coefficient field.* As in §2.4 we may and will assume that we have a diagram of fields as in (1), where all field extensions are Galois. Recall that $N_{\mathfrak{P}_N}/K_\mathfrak{p}$ is the unramified extension of degree n. We let m denote a multiple of the exponent of G (e.g. $m=n$) and choose $t\in\mathbb{N}$ large enough so that the local Galois Gauss sums $\tau(L_\mathfrak{P}/K_\mathfrak{p},\chi)$ for all $\chi\in\mathrm{Irr}(G)$ can be computed in $\mathbb{Q}(\zeta_m,\zeta_{p^t})$ (see Remark 2.6). Finally we let E be the Galois closure of $LN\mathbb{Q}(\zeta_m,\zeta_{p^t})$ over $\mathbb{Q}$ and fix a prime $\mathfrak{Q}$ of E over $\mathfrak{p}$. The field $E_\mathfrak{Q}$ takes the place of $\mathbb{Q}_p^c$ in our computations.

4.2.3. *Computing the lattice $\mathcal{L}$.* Our procedure to compute $\mathcal{L}$ is motivated by [1, §3.1]. Let $\theta\in L$ be a generator of a normal basis of the extension L/K and therefore also of the extension $L_\mathfrak{P}/K_\mathfrak{p}$ (compare §2.6). We can assume that $\theta\in\mathcal{O}_L$ and that $v_\mathfrak{P}(\theta)>\frac{e(L_\mathfrak{P}/\mathbb{Q}_p)}{p-1}$, where $e(L_\mathfrak{P}/\mathbb{Q}_p)$ denotes the ramification index of the extension $L_\mathfrak{P}/\mathbb{Q}_p$. This condition ensures that the p-adic exponential function is defined for θ. We define $\mathcal{L}=\mathcal{O}_{K_\mathfrak{p}}[G]\cdot\theta\subseteq\mathcal{O}_{L_\mathfrak{P}}$, so that $\mathcal{L}$ is a free $\mathbb{Z}_p[G]=\mathcal{O}_{K_\mathfrak{p}}[G]$-submodule of $\mathcal{O}_{L_\mathfrak{P}}$.

In order to be able to perform all our computations globally we will also need a positive integer $m > \frac{e(L_\mathfrak{P}/\mathbb{Q}_p)}{p-1}$ such that $(\mathfrak{P}\mathcal{O}_{L_\mathfrak{P}})^m \subseteq \mathcal{L}$, cf. [1, Lemma 3.5]. The integer m can be computed globally by first finding an ideal $\mathfrak{a}$ of $\mathcal{O}_L$ such that $\mathfrak{a} \subseteq \mathcal{O}_K[G]\cdot\theta \subseteq \mathcal{O}_L$ and then considering the $\mathfrak{P}$-part of $\mathfrak{a}$. If $k \in \mathbb{N}$ denotes the index of $\mathcal{O}_K[G]\cdot\theta$ in $\mathcal{O}_L$, then $\mathfrak{a} = k\mathcal{O}_L$ is a possible choice. Since $m > \frac{e(L_\mathfrak{P}/\mathbb{Q}_p)}{p-1}$, the p-adic exponential function gives a bijection $(\mathfrak{P}\mathcal{O}_{L_\mathfrak{P}})^m \cong U_{L_\mathfrak{P}}^{(m)}$.

The quotient $L_\mathfrak{P}^\times/\exp(\mathcal{L})$ is a finitely generated G-module which can be computed globally. Indeed, $L_\mathfrak{P}^\times/U_{L_\mathfrak{P}}^{(m)}$ can be computed globally (cf. §2.4), so the isomorphism $L_\mathfrak{P}^\times/\exp(\mathcal{L}) \cong \big(L_\mathfrak{P}^\times/U_{L_\mathfrak{P}}^{(m)}\big)/\big(\exp(\mathcal{L})/U_{L_\mathfrak{P}}^{(m)}\big)$ shows that it suffices to compute the image of $\exp(\mathcal{L})$ in $L_\mathfrak{P}^\times/U_{L_\mathfrak{P}}^{(m)}$. Since this image is generated by $\exp(\theta)\cdot U_{L_\mathfrak{P}}^{(m)}$ as a $\mathbb{Z}[G]$-module, it suffices to compute $\exp(\theta)$ with a certain precision, cf. [1, Remark 3.6].

4.2.4. *Computing* $E_{L_\mathfrak{P}/K_\mathfrak{p}}(\exp(\mathcal{L}))_p$. To compute $E_{L_\mathfrak{P}/K_\mathfrak{p}}(\exp(\mathcal{L}))_p$ we use [3, Lemma 3.7] (with $D = G$ and $X = \exp(\mathcal{L})$).

Using the algorithm from §2.4 we can compute a 2-cocycle which represents the image of the fundamental class in $H^2\big(G, L_\mathfrak{P}^\times/U_{L_\mathfrak{P}}^{(m)}\big)$. Applying the map $L_\mathfrak{P}^\times/U_{L_\mathfrak{P}}^{(m)} \to L_\mathfrak{P}^\times/\exp(\mathcal{L})$ gives a cocycle with values in $L_\mathfrak{P}^\times/\exp(\mathcal{L})$. Then we apply the construction in [17, p. 115] to this cocycle and obtain an explicit 2-extension of $\mathbb{Z}[G]$-modules

$$0 \to L_\mathfrak{P}^\times/\exp(\mathcal{L}) \to C(\gamma) \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

which represents the image of the fundamental class under

$$H^2(G, L_\mathfrak{P}^\times) \to H^2(G, L_\mathfrak{P}^\times/\exp(\mathcal{L})) = \mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, L_\mathfrak{P}^\times/\exp(\mathcal{L})).$$

Since $\exp(\mathcal{L})$ is cohomologically trivial, it follows from a well-known property of the local fundamental class that $C(\gamma)$ is also cohomologically trivial. Next we find a projective resolution

$$0 \to \mathcal{K} \to F \to C(\gamma) \to 0$$

with F a free $\mathbb{Z}[G]$-module. We remark that we may assume that each of the modules here is given by a $\mathbb{Z}$-basis, so that the computation of free resolutions and kernels can be achieved using linear algebra over $\mathbb{Z}$.

By [3, Lemma 3.7] we know that

$$E_{L_\mathfrak{P}/K_\mathfrak{p}}(\exp(\mathcal{L})) = [\mathcal{K} \oplus \mathbb{Z}[G], \tilde{\theta}, F] \in K_0(\mathbb{Z}[G], \mathbb{Q}),$$

where $\tilde{\theta} : (\mathcal{K} \oplus \mathbb{Z}[G]) \otimes \mathbb{Q} \to F \otimes \mathbb{Q}$ is a certain isomorphism of $\mathbb{Q}[G]$-modules. From the explicit description of $\tilde{\theta}$ in [3] it is clear how to find this map algorithmically, provided that we know how to compute sections of surjective maps of $\mathbb{Q}[G]$-modules. If $\varphi : A \to B$ is a surjection of finitely generated $\mathbb{Q}[G]$-modules, then we can find a $\mathbb{Q}[G]$-linear section $s : B \to A$ by first choosing any $\mathbb{Q}$-linear section $t : B \to A$ and then defining $s = \frac{1}{|G|}\sum_{\sigma\in G} t^\sigma$ where $t^\sigma(b) = \sigma(t(\sigma^{-1}(b)))$ for $b \in B$, cf. the standard proof of Maschke's Theorem.

The invariant $E_{L_\mathfrak{P}/K_\mathfrak{p}}(\exp(\mathcal{L}))_p$ is the image of $E_{L_\mathfrak{P}/K_\mathfrak{p}}(\exp(\mathcal{L}))$ under the composite homomorphism $K_0(\mathbb{Z}[G], \mathbb{Q}) \to K_0(\mathbb{Z}_p[G], \mathbb{Q}_p) \hookrightarrow K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$. A tuple in $\prod_{\mathrm{Irr}(G)} E^\times$ representing $E_{L_\mathfrak{P}/K_\mathfrak{p}}(\exp(\mathcal{L}))_p$ can therefore be computed as explained in §3.3.

4.2.5. *Computing* $[\mathcal{L}, \rho_{L_\mathfrak{P}}, H_{L_\mathfrak{P}}]$. Let $\Sigma(L_\mathfrak{P})$ denote the set of continuous embeddings $L_\mathfrak{P} \hookrightarrow E_\mathfrak{Omega}$ and put $H_{L_\mathfrak{P}} = \bigoplus_{\sigma\in\Sigma(L_\mathfrak{P})} \mathbb{Z}_p$. By construction L is a subfield of E and we may identify $G = \mathrm{Gal}(L/K)$ and $\Sigma(L_\mathfrak{P})$. If $\sigma_0 \in G$ denotes the identity element, then the element $b = (b_\sigma)_{\sigma\in\Sigma(L_\mathfrak{P})} \in H_{L_\mathfrak{P}}$ with $b_{\sigma_0} = 1$ and $b_\sigma = 0$ for $\sigma \neq \sigma_0$ is a $\mathbb{Z}_p[G]$-basis of $H_{L_\mathfrak{P}}$. Thus $H_{L_\mathfrak{P}}$ is a free $\mathbb{Z}_p[G]$-module of rank 1. Recall also that $\mathcal{L}$ is a free $\mathbb{Z}_p[G]$-module of rank 1 generated by θ.

The map

$$\rho_{L_\mathfrak{P}} : \mathcal{L} \otimes_{\mathbb{Z}_p} E_\mathfrak{Omega} \to H_{L_\mathfrak{P}} \otimes_{\mathbb{Z}_p} E_\mathfrak{Omega}, \quad \rho_{L_\mathfrak{P}}(l \otimes z) = (\sigma(l)z)_{\sigma\in\Sigma(L_\mathfrak{P})}$$

is an isomorphism of $E_\mathfrak{Omega}[G]$-modules. The matrix of this isomorphism with respect to the basis θ of $\mathcal{L}$ and the basis b of $H_{L_\mathfrak{P}}$ is the 1×1-matrix $A = \sum_{\sigma\in G} \sigma(\theta)\cdot\sigma^{-1} \in E[G]^\times \subset E_\mathfrak{Omega}[G]^\times$. Therefore a tuple in $\prod_{\mathrm{Irr}(G)} E^\times \subset \prod_{\mathrm{Irr}(G)} E_\mathfrak{Omega}^\times$ which represents $[\mathcal{L}, \rho_{L_\mathfrak{P}}, H_{L_\mathfrak{P}}]$ is given by $\mathrm{nr}(A)$. Clearly we can compute A and hence using the algorithm of §3.2 also $\mathrm{nr}(A)$.

4.2.6. *Computing* $T_{L_\mathfrak{P}/K_\mathfrak{p}}$. By the definition of $T_{L_\mathfrak{P}/K_\mathfrak{p}}$ in [6, §2.3], this invariant is represented by the tuple $(\tau(L_\mathfrak{P}/K_\mathfrak{p}, \chi))_{\chi\in\mathrm{Irr}(G)} \in \prod_{\mathrm{Irr}(G)} E^\times \subset \prod_{\mathrm{Irr}(G)} E_\mathfrak{Omega}^\times$. The computation of local Galois Gauss sums was explained in §2.5.

4.2.7. *Computing* $U_{L_\mathfrak{P}/K_\mathfrak{p}}$. The invariant $U_{L_\mathfrak{P}/K_\mathfrak{p}}$ is discussed in [6, §2.5]. The proof of [6, Prop. 2.12] shows that $U_{L_\mathfrak{P}/K_\mathfrak{p}}$ is represented by the tuple $\mathrm{nr}(u) \in \prod_{\mathrm{Irr}(G)} E^\times$ where $u \in E[G]^\times$ is given by an explicit formula. More precisely, to find u we must compute the maximal abelian subextension $(F, \mathfrak{p}_F)$ of $(L, \mathfrak{P})/(K, \mathfrak{p})$, and then the local norm residue symbol $(p, F_{\mathfrak{p}_F}/K_\mathfrak{p}) \in \mathrm{Gal}(F_{\mathfrak{p}_F}/K_\mathfrak{p}) \cong \mathrm{Gal}(F/K)$. Let $\varphi \in G$ be an element such that $\varphi|_F = (p, F_{\mathfrak{p}_F}/K_\mathfrak{p})$ and write s for the order of φ. Let $N_1 \subseteq N$ be the subextension of N/K with $[N_1 : K] = s$. Then $(N_1)_{\mathfrak{p}_{N_1}}/K_\mathfrak{p}$ is the unramified extension of degree s. Let $f \in \mathrm{Gal}(N_1/K)$ denote the Frobenius automorphism with respect to $\mathfrak{p}$ and compute an integral normal basis element $\xi \in \mathcal{O}_{N_1}$ for the extension $(N_1)_{\mathfrak{p}_{N_1}}/K_\mathfrak{p}$. Then

$$u = \sum_{i=0}^{s-1} f^i(\xi)\varphi^{-i} \in N_1[G] \subseteq E[G].$$

Thus we can compute u and then $\mathrm{nr}(u)$.

4.2.8. *Computing* $M_{L_\mathfrak{P}/K_\mathfrak{p}}$. We denote the centre of a ring R by $\zeta(R)$ and its multiplicative group by $\zeta(R)^\times$. In [6, §2.6] an explicit invariant $m_{L_\mathfrak{P}/K_\mathfrak{p}}$ in $\zeta(\mathbb{Q}[G])^\times$ is defined. In order to compute $m_{L_\mathfrak{P}/K_\mathfrak{p}}$ one has to compute the inertia group and Frobenius automorphism, which can be done as explained in §2.2. Under the natural inclusion $\zeta(\mathbb{Q}[G])^\times \subset \zeta(E[G])^\times \cong \prod_{\mathrm{Irr}(G)} E^\times$ the invariant $M_{L_\mathfrak{P}/K_\mathfrak{p}}$ is represented by $m_{L_\mathfrak{P}/K_\mathfrak{p}}$. Thus we can compute a tuple representing $M_{L_\mathfrak{P}/K_\mathfrak{p}}$.

4.2.9. *Check if zero in* $K_0(\mathbb{Z}_p[G], E_\mathfrak{Omega})$. We have computed tuples in $\prod_{\mathrm{Irr}(G)} E^\times$ representing each of the invariants in (8). Using the algorithm from §3.3 we can verify whether the product of these tuples represents 0 in $K_0(\mathbb{Z}_p[G], E_\mathfrak{Omega})$ and thus whether the local epsilon constant conjecture for the extension $L_\mathfrak{P}/K_\mathfrak{p}$ is true or not.

4.3. **Computational remarks.** We would like to conclude with some remarks about possible implementations of this algorithm. Because of the length of this algorithm any implementation in full generality would be a major project. However, at the moment it seems unlikely that such an implementation would prove any interesting new cases of the conjectures: several steps in the algorithm (for example the computation of the fundamental class) require the generation of very large number fields, and current algorithms are too slow to perform the necessary computations in these fields. Furthermore certain steps work by enumerating finite sets (e.g. the step to test whether an element in $K_0(\mathbb{Z}_p[G], E_{\mathfrak{Q}})$ is equal to 0) which again can be a very time consuming task. We therefore feel that the expected results would not justify the effort required for a full implementation of this algorithm.

A more useful approach is to restrict implementations to special classes of Galois extensions. This has the advantage that the implementation can be simplified, for example by restricting to Galois groups of a special structure, and that theoretical results for special types of extensions can reduce the amount of necessary computations. This approach was taken in [1] and [5], where algorithms for certain cyclic, respectively dihedral, extensions were developed and implemented (for the global epsilon constant conjecture of [3], but they could easily be modified to deal with the local conjecture instead).

References

[1] W. Bley, *Numerical evidence for a conjectural generalization of Hilbert's Theorem 132*, LMS J. Comput. Math. **6** (2003), 68–88 (electronic).

[2] W. Bley, R. Boltje, *Computation of locally free class groups*, in: F. Hess, S. Pauli, M. Pohst (Eds.), Algorithmic Number Theory, Lecture Notes in Computer Science **4076**, Springer (2006), 72–86.

[3] W. Bley, D. Burns, *Equivariant epsilon constants, discriminants and étale cohomology*, Proc. London Math. Soc. **87** (2003), 545–590.

[4] R. Boltje, *A canonical Brauer induction formula*, Astérisque **181-182** (1990), 31–59.

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

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

[7] T. Chinburg, *Exact sequences and Galois module structure*, Ann. of Math. **121** (1985), 351–376.

[8] H. Cohen, *A course in computational algebraic number theory*, Springer Verlag (1993).

[9] H. Cohen, *Advanced topics in computational number theory*, Springer Verlag (2000).

[10] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, in: *Modular functions of one variable, II*, Springer (1973), 501–597.

[11] K. Girstmair, *An algorithm for the construction of a normal basis*, J. Number Theory **78** (1999), 36–45.

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

[13] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd edition, Springer Verlag (1984).

[14] F. Lorenz, *Einführung in die Algebra II*, Spektrum Akademischer Verlag (1997).

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

[16] J. Neukirch, *Algebraische Zahlentheorie*, Springer Verlag (1992).

[17] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Springer Verlag (2000).

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

[19] J.-P. Serre, *Linear representations of finite groups*, Springer Verlag (1977).

[20] J.-P. Serre, *Local fields*, Springer Verlag (1979).

[21] R. G. Swan, *Algebraic K-theory*, Lecture Notes in Mathematics **76**, Springer Verlag (1968).

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

Department of Mathematics, King's College London, Strand, London WC2R 2LS, United Kingdom
E-mail address: manuel.breuning@kcl.ac.uk