Equivariant epsilon constant conjectures for weakly ramified extensions

Werner Bley and Alessandro Cobbe

Abstract

We study the local epsilon constant conjecture as formulated by Breuning in [3]. This conjecture fits into the general framework of the equivariant Tamagawa number conjecture (ETNC) and should be interpreted as a consequence of the expected compatibility of the ETNC with the functional equation of Artin-L-functions.

Let $K/\mathbb{Q}_p$ be unramified. Under some mild technical assumption we prove Breuning's conjecture for weakly ramified abelian extensions N/K with cyclic ramification group. As a consequence of Breuning's local-global principle we obtain the validity of the global epsilon constant conjecture as formulated in [1] and of Chinburg's $\Omega(2)$-conjecture as stated in [9] for certain infinite families F/E of weakly and wildly ramified extensions of number fields.

1 Introduction

We fix a Galois extension F/E of number fields and set $\Gamma := \mathrm{Gal}(F/E)$. Let S be a sufficiently large finite set of places of E which, in particular, includes all archimedean places and all places which ramify in F/E. Let $\zeta_{F/E,S}(s)$ denote the S-truncated equivariant zeta-function of F/E as defined in [5, Sec. 2.3] which takes values in the centre $Z(\mathbb{C}[\Gamma])$ of the complex group ring $\mathbb{C}[\Gamma]$. We recall that $\zeta_{F/E,S}(s)$ can be considered as the vector consisting of S-truncated Artin L-functions for all irreducible characters of Γ. For each rational integer m we write $\zeta^*_{F/E,S}(m)$ for the leading non-zero coefficient in the Taylor expansion of $\zeta_{F/E,S}(s)$ at $s = m$. It follows easily that $\zeta^*_{F/E,S}(m)$ is contained in the unit group of $Z(\mathbb{R}[\Gamma])$ (cf. [5, Lemma 2.7]).

Continuing work of Burns in [7], Breuning and Burns formulate in [5] explicit conjectures for the image of $\zeta^*_{F/E,S}(0)$, resp. $\zeta^*_{F/E,S}(1)$, under the canonical homomorphism $\hat{\partial}$ from $Z(\mathbb{R}[\Gamma])$ to the relative algebraic K-group $K_0(\mathbb{Z}[\Gamma], \mathbb{R})$. We recall that the conjectural formula for $\zeta^*_{F/E,S}(0)$ is equivalent to the *lifted root number conjecture* of Gruenberg, Ritter and Weiss (cf. [11]), and moreover, is expected to be equivalent to the equivariant Tamagawa number conjecture for the pair $(h^0(\mathrm{Spec}(F)), \mathbb{Z}[\Gamma])$ (cf. [5, Prop. 4.4 and Rem. 4.5]). Under some technical hypothesis the conjectural formula for $\zeta^*_{F/E,S}(1)$ is shown in [6, Th. 1.1 and Cor. 1.2] to be equivalent to the equivariant Tamagawa number conjecture as applied to the pair $(h^0(\mathrm{Spec}(F))(1), \mathbb{Z}[\Gamma])$.

In this paper we provide new evidence for the functional equation compatibility of these conjectures. To be more specific, we recall that Breuning and Burns define elements $T\Omega(F/E, m)$ in $K_0(\mathbb{Z}[\Gamma], \mathbb{R})$ for $m = 0, 1$ and state their conjectures in the form $T\Omega(F/E, m) = 0$ (cf. [5, Conj. 3.3 and 4.1]). Motivated by the work in [1] they define a further element $T\Omega^{\mathrm{loc}}(F/E, 1)$ in $K_0(\mathbb{Z}[\Gamma], \mathbb{R})$ and show in [5, Th. 5.2] that

$$\psi_\Gamma^* \left(T\Omega(F/E, 0)\right) - T\Omega(F/E, 1) = T\Omega^{\mathrm{loc}}(F/E, 1).$$

Here ψ_Γ^* denotes a natural involution on the algebraic K-group $K_0(\mathbb{Z}[\Gamma], \mathbb{R})$.

The leading term conjectures for $\zeta_{F/E,S}^*(0)$ and $\zeta_{F/E,S}^*(1)$ force the following conjecture which we want to study in this paper.

Conjecture 1. (cf. [5, Conj. 5.3]) One has the equality

$$T\Omega^{\mathrm{loc}}(F/E, 1) = 0$$

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

By [1, Rem. 5.4] Conjecture 1 is equivalent to Conjecture 4.1 of [1]. We recall that for every Galois extension F/E the invariant $T\Omega^{\mathrm{loc}}(F/E, 1)$ lies in the finite group $K_0(\mathbb{Z}[\Gamma], \mathbb{Q})_{\mathrm{tors}}$, the torsion subgroup of $K_0(\mathbb{Z}[\Gamma], \mathbb{Q}) \subseteq K_0(\mathbb{Z}[\Gamma], \mathbb{R})$ ([1, Cor. 6.3 (i)]). Moreover, Conjecture 1 is known if F/E is at most tamely ramified ([1, Cor. 7.7]), if F is an abelian extension of $\mathbb{Q}$ with odd conductor ([1, Cor. 5.4 (ii)]) or if F is an extension of $\mathbb{Q}$ of degree ≤ 15 ([2, Cor. 7]). We also recall that by [1, Rem. 4.2 (iv)] Conjecture 1 implies Chinburg's $\Omega(2)$-conjecture as stated in [9].

Conjecture 1 is essentially of local nature. In fact, it is a local approach which lies behind the proofs of the known cases mentioned above. Based on this observation, Breuning stated in [3] an independent conjecture for Galois extensions N/K of local number fields. We write G for the Galois group of N/K. Breuning defined an element $R_{N/K}$ in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ incorporating local epsilon constants and algebraic invariants associated to N/K. We will briefly recall the definition of $R_{N/K}$ in Section 2. Breuning stated the following conjecture.

Conjecture 2. (cf. [3, Conj. 3.2]) One has the equality

$$R_{N/K} = 0$$

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

Since $T\Omega^{\mathrm{loc}}(F/E, 1)$ is contained in the subgroup $K_0(\mathbb{Z}[\Gamma], \mathbb{Q})$ it can be studied prime by prime. We let $T\Omega^{\mathrm{loc}}(F/E, 1)_p \in K_0(\mathbb{Z}_p[\Gamma], \mathbb{Q}_p)$ denote its p-primary part. Then the local conjecture is related to the global conjecture by the equation

$$T\Omega^{\mathrm{loc}}(F/E, 1)_p = \sum_v i_{\Gamma_w}^{\Gamma} \left(R_{F_w/E_v}\right),$$

where v runs through all places of E above p, w is a fixed place of F lying over v, Γ_w denotes the decomposition group and $i_{\Gamma_w}^{\Gamma}$ is the induction map on the relative algebraic K-group, cf. [3, Th. 4.1].

In [3, 4] Breuning proved Conjecture 2 for tamely ramified extensions, for abelian extensions of $\mathbb{Q}_p$ with $p \neq 2$, for all S_3-extensions of $\mathbb{Q}_p$, and for certain families of dihedral and quaternion extensions. If p is odd, an algorithmic proof for Conjecture 2 is given in [2] for all Galois extensions of degree ≤ 15. If $p = 2$, the conjecture is also proved in loc.cit. for all non-abelian Galois extensions of $\mathbb{Q}_2$ with $[N : \mathbb{Q}_2] \leq 15$ and, in addition, for all abelian extensions $N/\mathbb{Q}_2$ with $[N : \mathbb{Q}_2] \leq 7$.

In this manuscript we will focus on weakly and wildly ramified extensions N/K of an unramified extension $K/\mathbb{Q}_p$. We recall that N/K is weakly ramified, if the second ramification group in lower numbering is trivial.

We state the main result of our work.

Theorem 1. *Let p be an odd prime and let $K/\mathbb{Q}_p$ be a finite unramified extension. Let m denote the degree of $K/\mathbb{Q}_p$. Let N/K be a weakly and wildly ramified finite abelian extension with cyclic ramification group. Let d denote the inertia degree of N/K and assume that m and d are relatively prime. Then Conjecture 2 is true for N/K.*

Remark 1. The assumptions of the theorem imply that the ramification group is cyclic of order p (cf. [15, Cor. 3.4]). More precisely, $|G| = pd, |G_0| = |G_1| = p$ and $|G_i| = 1$ for $i \geq 2$. Here G_i for $i \geq 0$ denotes the higher ramification subgroup.

The invariant $R_{N/K}$ incorporates amongst other terms the equivariant local epsilon constant and a certain equivariant discriminant attached to N/K. Whereas the main ingredient in the definition of the equivariant epsilon constant is a local Gauß sum, equivariant discriminants are closely related to norm-resolvents. The relation between norm-resolvents and Galois Gauß sums in the context of Theorem 1 is analyzed by Pickett and Vinatier in [15]. Indeed, Theorem 2 of loc.cit. was one of the main motivations and a starting point for our project. In addition, the strategy for the proof of Theorem 1 was inspired by the reductions made in Section 3.3 of loc.cit.

The above relation between $T\Omega^{\mathrm{loc}}(F/E, 1)_p$ and R_{F_w/E_v} implies results for global Galois extensions F/E which satisfy the following property.

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

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

b) $E_v = \mathbb{Q}_p$, $p = 2$, Γ_w is abelian and $|\Gamma_w| \leq 7$,

c) $E_v = \mathbb{Q}_p$, $p \geq 2$, Γ_w is non-abelian and $|\Gamma_w| \leq 15$,

d) $E_v/\mathbb{Q}_p$ is unramified, $p > 2$, F_w/E_v is abelian and weakly ramified with cyclic ramification group and $[E_v : \mathbb{Q}_p]$ is coprime with the inertia degree of F_w/E_v.

Every tamely ramified extension F/E obviously satisfies Property $(*)$. It is easy to construct infinite families of weakly and wildly ramified extensions of number fields which satisfy condition d) using class field theory. In particular, if p is an odd prime, $E/\mathbb{Q}$ an extension of number fields in which p is unramified and F/E a cyclic extension of degree p which is at most weakly ramified, then F/E satisfies Property $(*)$.

Corollary 1. *Conjecture 1 is valid for all Galois extensions F/E which satisfy Property* $(*)$*.*

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

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

Moreover, the functorial properties of [3, Prop. 3.3] imply the following result:

Corollary 3. *Conjecture 1 and Chinburg's $\Omega(2)$-conjecture are valid for global Galois extensions F/E for which $E' \subseteq E \subseteq F \subseteq F'$ with a Galois extension F'/E' that satisfies Property* $(*)$*.*

In Section 2 we will first recall Breuning's conjecture and then give a short description of the organization of the manuscript.

Notations Given a field extension F/E, we will denote the norm and the trace by $\mathcal{N}_{F/E}$ and $\mathcal{T}_{F/E}$ respectively. If K is a local field, then v_K will always denote its normalized valuation. We will write $\mathcal{O}_K$ and $\mathfrak{p}_K$ for the valuation ring and the maximal ideal respectively. Furthermore, U_K will denote the units of $\mathcal{O}_K$ and $U_K^{(n)} := \{u \in U_K : u \equiv 1 \pmod{\mathfrak{p}_K^n}\}$ the higher principal units.

If K is a field we write K^c for an algebraic closure. For a finite group G we write $\mathrm{Irr}_{\mathbb{Q}^c}(G)$ for the set of absolutely irreducible characters of G. We often implicitly fix an embedding $\mathbb{Q}^c \hookrightarrow \mathbb{Q}_p^c$ and view $\mathbb{Q}^c$-valued characters as valued in $\mathbb{Q}_p^c$.

If $H \leq G$ is a subgroup, then $e_H = \frac{1}{|H|}\sum_{\sigma\in H}\sigma$ denotes the usual subgroup idempotent. We also set $T_H := |H|e_H$. For $a \in G$ we abbreviate $e_a = e_{\langle a\rangle}$ and $T_a = T_{\langle a\rangle}$.

For a $\mathbb{Z}$-module M and a prime p we often write M_p for $M \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

2 The local epsilon constant conjecture

In this section we briefly recall the formulation of Breuning's local epsilon constant conjecture. For further details we refer the reader to [3, Sec. 2].

2.1 The shape of the conjecture

The element $R_{N/K}$ is of the form

$$R_{N/K} = T_{N/K} + C_{N/K} + U_{N/K} - M_{N/K}$$

where each of the terms is an element in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p^c)$. This algebraic K-group lies in an exact localization sequence of the form

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

If G is abelian, the determinant induces an isomorphism $K_1(\mathbb{Q}_p^c[G]) \simeq \mathbb{Q}_p^c[G]^\times$. Since $\mathbb{Z}_p[G]$ is semilocal the natural map $\mathbb{Z}_p[G]^\times \longrightarrow K_1(\mathbb{Z}_p[G])$ is onto, so that in the abelian case we can and will identify $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p^c)$ with $\mathbb{Q}_p^c[G]^\times/\mathbb{Z}_p[G]^\times$. Furthermore, we identify $\mathbb{Q}_p^c[G]^\times$ with $\prod_\chi \left(\mathbb{Q}_p^c\right)^\times$ where χ runs through the set $\mathrm{Irr}_{\mathbb{Q}^c}(G)$.

The term $T_{N/K}$ is called the *equivariant local epsilon constant.* If K is a finite extension of $\mathbb{Q}_p$ and χ a character of $\mathrm{Gal}(K^c/K)$ with values in $\mathbb{Q}^c$ we write $\tau_K(\chi) \in \mathbb{Q}^c$ for the local Galois Gauß sum as defined in [13, II, Sec. 4]. Let N/K be an abelian extension of p-adic fields and put $G := \mathrm{Gal}(N/K)$. We set

$$\tau_{N/K} := \left(\tau_{\mathbb{Q}_p}\left(i_K^{\mathbb{Q}_p}\chi\right)\right)_{\chi\in\mathrm{Irr}_{\mathbb{Q}^c}(G)} \in \prod_\chi (\mathbb{Q}^c)^\times = \mathbb{Q}^c[G]^\times.$$

Let $k\colon \mathbb{Q}^c \longrightarrow \mathbb{Q}_p^c$ be any embedding and also write $k\colon \mathbb{Q}^c[G] \longrightarrow \mathbb{Q}_p^c[G]$ for the induced map. Then $T_{N/K} \in \mathbb{Q}_p^c[G]^\times/\mathbb{Z}_p[G]^\times$ is defined to be the class represented by $k(\tau_{N/K})$. By [3, Lemma 2.2] the definition $T_{N/K}$ does not depend on the choice of the embedding k.

We call $C_{N/K}$ the *cohomological term.* Let $\mathcal{L}$ be a full projective $\mathbb{Z}_p[G]$-sublattice of $\mathcal{O}_N$ which is contained in a sufficiently high power of the maximal ideal such that the exponential map of N is defined on $\mathcal{L}$. We recall that in [1, Sec. 3.3] a cohomological term $E(X) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ is defined for every cohomologically trivial $\mathbb{Z}[G]$-submodule X of finite index in U_N. We write $E(X)_p \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ for its p-part. Then, by [3, Prop. 2.6],

$$C_{N/K} = E(\exp(\mathcal{L}))_p - [\mathcal{L}, \rho_N, H_N]$$

in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p^c)$. The computation of $E(\exp(\mathcal{L}))_p$ in our special situation is the technical heart of this paper. We therefore postpone its definition to Section 2.2. For the definition of $[\mathcal{L}, \rho_N, H_N]$ we just recall that for a normal basis element $\theta \in \mathcal{O}_N$ and $\mathcal{L} := \mathcal{O}_K[G]\theta$ the element $[\mathcal{L}, \rho_N, H_N]$ is represented by $\left(\delta_K \mathcal{N}_{K/\mathbb{Q}_p}(\theta \mid \chi)\right)_{\chi \in \mathrm{Irr}_{\mathbb{Q}^c}(G)} \in \prod_\chi (\mathbb{Q}^c)^\times$ where $\mathcal{N}_{K/\mathbb{Q}_p}(\theta \mid \chi)$ denotes the norm resolvent and δ_K is a root of the discriminant of K (cf. [3, Lemma 2.7]).

We continue to describe the *correction term* $M_{N/K}$. To simplify the notation we assume that G is abelian. For $x \in \mathbb{Q}_p[G]$ we define an invertible element ${}^*x \in \mathbb{Q}_p[G]^\times$ as follows. If $\mathbb{Q}_p[G] = \prod F_i$ is the Wedderburn decomposition of $\mathbb{Q}_p[G]$ and $x = (x_i)$ under this decomposition, then ${}^*x = (({}^*x)_i)$ with $({}^*x)_i = x_i$ if $x_i \neq 0$ and $({}^*x)_i = 1$ if $x_i = 0$. Let I be the ramification group of G and let $\sigma \in G$ be a lift of the Frobenius automorphism in G/I. Put $q := |\mathcal{O}_K/\mathfrak{p}_K|$. Then $M_{N/K} \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ is represented by

$$m_{N/K} := \frac{{}^*(|G/I|e_G){}^*((1-\sigma q^{-1})e_I)}{{}^*((1-\sigma^{-1})e_I)}.$$

Finally we discuss the *unramified term* $U_{N/K}$. We write $\mathcal{O}_p^t$ for the ring of integers in the maximal tamely ramified extension of $\mathbb{Q}_p$ in $\mathbb{Q}_p^c$. Let $\iota\colon K_0(\mathbb{Z}_p[G], \mathbb{Q}_p^c) \longrightarrow K_0(\mathcal{O}_p^t[G], \mathbb{Q}_p^c)$ be the natural scalar extension map. We recall that by Taylor's fixed point theorem the restriction of ι to the subgroup $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ is injective. If G is abelian, this injectivity is equivalent to

$$\mathbb{Q}_p[G]^\times / \mathbb{Z}_p[G]^\times \hookrightarrow \mathbb{Q}_p^c[G]^\times / \mathcal{O}_p^t[G]^\times.$$

By [3, Prop. 2.12] we have $\iota(U_{N/K}) = 0$. The properties of $U_{N/K}$ with respect to the action of $\mathrm{Gal}(\mathbb{Q}_p^c/\mathbb{Q}_p)$ ensure that $R_{N/K} \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$. By Taylor's fixed point theorem it therefore suffices to show that $\iota(R_{N/K}) = 0$ (cf. [3, Cor. 3.5]). In the abelian case it therefore suffices to prove that a representative of $T_{N/K} + C_{N/K} - M_{N/K}$ actually lies in $\mathcal{O}_p^t[G]^\times$.

2.2 Definition of $E(X)$

Let N/K be a finite Galois extension of p-adic fields with group G. Let $X \subseteq U_N$ be any cohomologically trivial $\mathbb{Z}[G]$-submodule of finite index. The element $E(X) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ is defined in [1, (19)]. We recall here the approach summarized in [1, Lemma 3.7] which allows an explicit description of $E(X)_p$. This approach is based on the observation of Burns and Flach made in [8, Prop. 3.5 (a)] that relates certain complexes arising from the cohomology of the sheaf $\mathbb{G}_m$ to 2-extensions representing the fundamental class of local class field theory.

We fix a $\mathbb{Z}[G]$-equivariant resolution of $\mathbb{Z}$ of the form

$$0 \longrightarrow \Sigma \xrightarrow{\subset} \mathbb{Z}[G]^r \xrightarrow{d_2} \mathbb{Z}[G] \xrightarrow{d_1} \mathbb{Z} \longrightarrow 0$$

where $\Sigma := \ker(d_2)$ and compute groups of the form $\mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ with respect to this resolution. We then choose a morphism $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(\Sigma, N^\times/X)$ which represents the image of the local fundamental class under the canonical isomorphism $\mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, N^\times) \longrightarrow \mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, N^\times/X)$. Without loss of generality we may assume that φ is surjective. We then set $B := \ker(d_1)$ and $\mathcal{K} := \ker(\varphi)$ and we write i_1, i_2 and i_3 for the inclusion morphisms $\mathcal{K}_\mathbb{Q} \xrightarrow{\subset} \Sigma_\mathbb{Q}$, $\Sigma_\mathbb{Q} \xrightarrow{\subset} \mathbb{Q}[G]^r$ and $B_\mathbb{Q} \xrightarrow{\subset} \mathbb{Q}[G]$ respectively. We also choose $\mathbb{Q}[G]$-equivariant sections ρ, σ and τ to the morphisms $\varphi_\mathbb{Q}, d_{2,\mathbb{Q}} : \mathbb{Q}[G]^r \longrightarrow B_\mathbb{Q}$ and $d_{1,\mathbb{Q}}$ respectively. We then write $\tilde{\theta}$ for the composite isomorphism

$$\begin{array}{rcl} (\mathcal{K} \oplus \mathbb{Z}[G])_\mathbb{Q} & \xrightarrow{(\mathrm{id},(\tau,i_3)^{-1})} & \mathcal{K}_\mathbb{Q} \oplus (\mathbb{Q} \oplus B_\mathbb{Q}) \\ & \xrightarrow{(\mathrm{id},\nu_N^{-1},\mathrm{id})} & \mathcal{K}_\mathbb{Q} \oplus \left(N^\times/X\right)_\mathbb{Q} \oplus B_\mathbb{Q} \\ & \xrightarrow{(i_1,\rho,\mathrm{id})} & \Sigma_\mathbb{Q} \oplus B_\mathbb{Q} \\ & \xrightarrow{(i_2,\sigma)} & \mathbb{Q}[G]^r. \end{array} \qquad (1)$$

By [1, Lemma 3.7] the module $\mathcal{K}$ is finitely generated and $\mathbb{Z}[G]$-projective and, moreover,

$$E(X) = [\mathcal{K} \oplus \mathbb{Z}[G], \tilde{\theta}, \mathbb{Z}[G]^r]$$

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

Suppose now that G is abelian. In order to compute a representative of $E(X)_p$ in $\mathbb{Q}_p[G]^\times/\mathbb{Z}_p[G]^\times \simeq K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ we first note that $\mathcal{K}_p \oplus \mathbb{Z}_p[G]$ is $\mathbb{Z}_p[G]$-free. We choose $\mathbb{Z}_p[G]$-bases of $\mathcal{K}_p \oplus \mathbb{Z}_p[G]$ and $\mathbb{Z}_p[G]^r$, respectively, and let $A_{\tilde{\theta}} \in \mathrm{Gl}_r(\mathbb{Q}_p[G])$ denote the matrix which represents $\tilde{\theta}$ with respect to this choice of bases. Then $E(X)_p$ is represented by $\det(A_{\tilde{\theta}})$.

2.3 Plan of the manuscript

In Section 4 we will compute the term $E(\exp(\mathcal{L}))_p$ for extensions N/K as in Theorem 1 and a special choice of lattice $\mathcal{L}$. The term $[\mathcal{L}, \rho_N, H_N] - T_{N/K}$ is represented by the quotient of a norm resolvent by Galois Gauß sums. In Section 5 we will use the main result of [15] to quickly compute this term. Finally in Section 6 we calculate $M_{N/K}$ and complete the proof of Theorem 1 by showing that a representative of $T_{N/K} + C_{N/K} - M_{N/K}$ lies in $\mathcal{O}_p^t[G]^\times$.

3 The setting

3.1 Definitions and notation

In this section we fix the setting in which we will work. We will consider local field extensions as follows.

$$\begin{tikzcd}
 & & N_0 \arrow[dl, dash] \arrow[dr, dash] & \\
 & N \arrow[dl, dash] \arrow[dr, dash] & & K_{\mathrm{nr}} \arrow[dl, dash] \\
M \arrow[dr, dash] & & K' \arrow[dl, dash] \arrow[dr, dash] & \\
 & K \arrow[dr, dash] & & \tilde{K}' \arrow[dl, dash] \\
 & & \mathbb{Q}_p. &
\end{tikzcd}$$

Here $K/\mathbb{Q}_p$ is the unramified extension of degree m and K'/K is the unramified extension of degree d. We assume throughout that $(m,d)=1$. Furthermore, M/K is a weakly and wildly ramified cyclic extension of degree p. Since $(m,d)=1$, there exists $\tilde{K}'/\mathbb{Q}_p$ of degree d such that $K' = K\tilde{K}'$. Further we set $N = MK'$, K_{nr} the maximal unramified extension of K and $N_0 = K_{\mathrm{nr}}N$. We will prove Conjecture 2 for the extension N/K.

Let $F \in \mathrm{Gal}(N_0/M) \cong \mathrm{Gal}(K_{\mathrm{nr}}/K)$ be the Frobenius automorphism, let $F_0 = F^d \in \mathrm{Gal}(N_0/N) \cong \mathrm{Gal}(K_{\mathrm{nr}}/K')$ and put $q = p^m$. We consider elements $a, b \in \mathrm{Gal}(N_0/K)$ such that $\mathrm{Gal}(M/K) = \langle a|_M \rangle$, $a|_{K_{\mathrm{nr}}} = 1$, $b|_M = 1$ and $b|_{K_{\mathrm{nr}}} = F^{-1}$. Since there will be no ambiguity, we will denote by the same letters a, b their restrictions to N. Then $\mathrm{Gal}(N/K) = \langle a, b \rangle$ and $\mathrm{ord}(a) = p, \mathrm{ord}(b) = d$.

Lemma 3.1.1. *Let L/k be a finite tamely ramified Galois extension of p-adic fields. Then there exists a normal integral basis generator of trace one.*

Proof. Put $\Delta := \mathrm{Gal}(L/k)$. By Noether's Theorem there exists an element $\theta \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_k[\Delta]\theta$. Let $t := \mathcal{T}_{L/k}(\theta)$. Then $t \in \mathcal{O}_k^\times$ and $\frac{\theta}{t}$ is an integral normal basis generator of trace one. $\square$

Let us call A such an element for the extension $K/\mathbb{Q}_p$ and let θ_2 be such an element for the extension $\tilde{K}'/\mathbb{Q}_p$.

Lemma 3.1.2. *There exists an element $\theta_1 \in \mathfrak{p}_M$ such that $\mathcal{O}_K[\mathrm{Gal}(M/K)]\theta_1 = \mathfrak{p}_M$ and we can assume that $\mathcal{T}_{M/K}\theta_1 = p$.*

Proof. By [12, Th. 1.1 and Lemma 1.4 (b)] there exists an element $\tilde{\theta}_1 \in \mathfrak{p}_M$ such that $\mathcal{O}_K[\mathrm{Gal}(M/K)]\tilde{\theta}_1 = \mathfrak{p}_M$ and $\mathcal{T}_{M/K}(\tilde{\theta}_1) = up$ with a unit $u \in \mathcal{O}_K^\times$. We set $\theta_1 := \frac{1}{u}\tilde{\theta}_1$. $\square$

For the rest of the paper we fix an element $\theta_1 \in \mathfrak{p}_M$ as in Lemma 3.1.2. Since $a \in G_1 \setminus G_2$, where G_i is the i-th ramification group of $G = \mathrm{Gal}(N/K)$, we know by [16, Sec. IV.2, Prop. 5] that $\theta_1^{a-1} \equiv 1 - \alpha_1\theta_1 \pmod{\mathfrak{p}_M^2}$ for some unit $\alpha_1 \in \mathcal{O}_M^\times$. Since

α_1 can be replaced by any element in the same residue class in $\mathcal{O}_M/\mathfrak{p}_M = \mathcal{O}_K/\mathfrak{p}_K$, we can assume that $\alpha_1 \in \mathcal{O}_K^\times$.

By our choice of A, we know that $A, A^f, \dots A^{f^{m-1}}$ is a basis of $\mathcal{O}_K$ over $\mathbb{Z}_p$, where f denotes the Frobenius automorphism of $K_{\mathrm{nr}}/\mathbb{Q}_p$. Since $1 = \mathcal{T}_{K/\mathbb{Q}_p} A = \sum_{i=0}^{m-1} A^{f^i}$ and $\alpha_1 \in \mathcal{O}_K^\times$ it easily follows that also

$$\alpha_1, \alpha_2 = \alpha_1 A, \alpha_3 = \alpha_1 A^f, \dots, \alpha_m = \alpha_1 A^{f^{m-2}} \tag{2}$$

constitute a basis of $\mathcal{O}_K$ over $\mathbb{Z}_p$. In particular, we have the equality $A = \frac{\alpha_2}{\alpha_1}$.

Lemma 3.1.3. *With the above notation, $X^p - X + A\theta_2$ divides $X^{q^d} - X + 1$ in $\mathcal{O}_{K'}/\mathfrak{p}_{K'}[X]$.*

Proof. We have

$$X^{q^d} - X + 1 = X^{p^{md}} - X + \mathcal{T}_{K'/\mathbb{Q}_p}(A\theta_2) \equiv \sum_{i=0}^{md-1} (X^p - X + A\theta_2)^{p^i} \pmod{\mathfrak{p}_{K'}}$$

and the right hand side is clearly a multiple of $X^p - X + A\theta_2$. □

Now we choose an element $x_2 \in \mathcal{O}_{K_{\mathrm{nr}}}$ so that the class of $\frac{x_2}{\alpha_1}$ modulo $\mathfrak{p}_{K_{\mathrm{nr}}}$ is a root of the polynomial $X^p - X + A\theta_2$. Let $\zeta_{q^d-1} \in \mathcal{O}_{K'}^\times$ be a primitive (q^d-1)-th root of unity.

Lemma 3.1.4. *We have*

$$(\zeta_{q^d-1}(1 + x_2\theta_1))^{F_0 - 1} \equiv \theta_1^{a-1} \equiv 1 - \alpha_1\theta_1 \pmod{\mathfrak{p}_{N_0}^2}.$$

Proof. By the choice of x_2 and Lemma 3.1.3 we obtain

$$\left(\frac{x_2}{\alpha_1}\right)^{q^d} - \frac{x_2}{\alpha_1} \equiv -1 \pmod{\mathfrak{p}_{K_{\mathrm{nr}}}}.$$

Multiplying by $\alpha_1^{q^d}$ and observing $\alpha_1^{q^d-1} \equiv 1 \pmod{\mathfrak{p}_{K_{\mathrm{nr}}}}$ we obtain

$$x_2^{q^d} - x_2 \equiv -\alpha_1 \pmod{\mathfrak{p}_{N_0}}. \tag{3}$$

Now we conclude

$$\begin{aligned}
\big(\zeta_{q^d-1}(1 + x_2\theta_1)\big)^{F_0 - 1} &= (1 + x_2\theta_1)^{b^{-d}} (1 + x_2\theta_1)^{-1} \\
&\equiv (1 + x_2^{b^{-d}}\theta_1)(1 - x_2\theta_1) \pmod{\mathfrak{p}_{N_0}^2} \\
&\equiv 1 + x_2^{b^{-d}}\theta_1 - x_2\theta_1 \equiv 1 - \alpha_1\theta_1 \pmod{\mathfrak{p}_{N_0}^2},
\end{aligned}$$

where the last congruence follows from (3). □

Let $\hat{N}_0$ denote the completion of N_0.

Lemma 3.1.5. *For all $u \in U_{\hat{N}_0}$ there exists $z \in U_{\hat{N}_0}$ such that $z^{F_0 - 1} = u$. In particular, there exists $\gamma \in U_{N_0}$ such that $\gamma^{F_0-1} \equiv \theta_1^{a-1} \pmod{\mathfrak{p}_{N_0}^{p+1}}$ and the element γ can be chosen so that $\gamma \equiv \zeta_{q^d-1}(1 + x_2\theta_1) \pmod{\mathfrak{p}_{N_0}^2}$.*

Proof. The first part of the lemma is contained in [14, Sec. V, Lemma 2.1]. The second part follows from the constructions made in the proof of loc.cit. combined with Lemma 3.1.4. For the reader's convenience we carry out the details.

Since the residue field of N_0 is algebraically closed, there exists a solution $z_1 \in U_{N_0}$ of $z^{F_0} \equiv z^{q^d} \equiv zu \pmod{\mathfrak{p}_{N_0}}$.

Now let us assume that $i \geq 2$ and that we have an element $z_{i-1} \in U_{N_0}$ such that $z_{i-1}^{F_0-1} \equiv u \pmod{\mathfrak{p}_{N_0}^{i-1}}$. By assumption, $uz_{i-1}^{1-F_0} - 1$ is a multiple of θ_1^{i-1}. So we can find a solution $y_i \in \mathcal{O}_{N_0}$ of

$$X^{F_0} - X - \frac{uz_{i-1}^{1-F_0} - 1}{\theta_1^{i-1}} \equiv 0 \pmod{\mathfrak{p}_{N_0}}.$$

Multiplying by θ_1^{i-1}, we get

$$y_i^{F_0}\theta_1^{i-1} \equiv y_i\theta_1^{i-1} + uz_{i-1}^{1-F_0} - 1 \pmod{\mathfrak{p}_{N_0}^i}.$$

Now we set $z_i := z_{i-1}(1 + y_i\theta_1^{i-1})$ and easily verify that $z_i^{F_0-1} \equiv u \pmod{\mathfrak{p}_{N_0}^i}$. The z_i form a Cauchy sequence which converges to an element $z \in U_{\hat{N}_0}$ with the requested properties.

If $u = \theta_1^{a-1}$, then by Lemma 3.1.4 we can start the construction of the sequence of the z_i from the element $z_2 = \zeta_{q^d-1}(1 + x_2\theta_1)$ and take $\gamma = z_{p+1}$. □

For the rest of the paper we fix an elemment $\gamma \in U_{N_0}$ as in Lemma 3.1.5.

3.2 Some preliminary results

In this subsection we collect some preliminary results which will be needed in Section 4. We assume all the notations introduced in Subsection 3.1.

Lemma 3.2.1. *We have*

$$\mathcal{N}_{M/K}(1 - \alpha_1\theta_1) \equiv 1 \pmod{\mathfrak{p}_M^{p+1}}.$$

Proof. Recalling that by [16, Sec. V.6, Prop. 8] $\mathcal{N}_{M/K}U_M^{(2)} \subseteq U_K^{(2)} \subseteq U_M^{(p+1)}$, we obtain

$$\mathcal{N}_{M/K}(1 - \alpha_1\theta_1) \equiv \mathcal{N}_{M/K}(\theta_1^{a-1}) = 1 \pmod{\mathfrak{p}_M^{p+1}}.$$

□

Lemma 3.2.2. *We have*

$$\mathcal{N}_{M/K}(\theta_1) \equiv -\alpha_1^{1-p}p \pmod{\mathfrak{p}_M^{p+1}}.$$

Proof. By [16, Sec. V.3, Lemma 4] we have $\mathcal{T}_{M/K}(\mathfrak{p}_M^2) = \mathfrak{p}_K^2$. In addition, by [16, Sec. V.3, Lemma 5] and Lemma 3.2.1 we obtain

$$1 \equiv \mathcal{N}_{M/K}(1 - \alpha_1\theta_1) \equiv 1 + \mathcal{N}_{M/K}(-\alpha_1\theta_1) + \mathcal{T}_{M/K}(-\alpha_1\theta_1) \pmod{\mathfrak{p}_M^{p+1}}.$$

Since $\alpha_1 \in \mathcal{O}_K^\times$ and $\mathcal{T}_{M/K}(\theta_1) = p$ the result easily follows. □

Lemma 3.2.3. *We have*

$$p - T_a = (a-1)^{p-1}u,$$

for some unit u of $\mathbb{Z}_p[a]$ such that the augmentation $\varepsilon(u) = (p-1)!$.

Proof. One can take, for example, $u = \prod_{i=1}^{p-1} \frac{a^i-1}{a-1}$. $\square$

Lemma 3.2.4. *The element $(a-1)^{p-1} - T_a$ is a multiple of p in $\mathbb{Z}_p[a]$. In particular,*

$$(a-1)^{p-1}\theta_1 \equiv T_a\theta_1 = p \pmod{\mathfrak{p}_N^{p+1}}.$$

Proof. Easy exerciese. $\square$

Lemma 3.2.5. *Let $x \in N^\times$ such that $v_N(x) \in \{1, 2, \dots, p-1\}$. Then $v_N((a-1)x) = v_N(x) + 1$.*

Proof. We have to show that $v_N(x^{a-1}-1) = 1$ which is equivalent to $x^{a-1} \in U_N^{(1)} \setminus U_N^{(2)}$. By our assumptions we have $a \in G_1 \setminus G_2$. If $v_N(x) = 1$, then $\mathcal{O}_N = \mathcal{O}_{K'}[x]$ by [16, Sec. I.6, Prop. 18] and, furthermore, [16, Sec. IV.1, Lemma 1] implies $x^{a-1} \in U_N^{(1)} \setminus U_N^{(2)}$. If $v_N(x) \in \{2, \dots, p-1\}$, then we choose $s, t \in \mathbb{Z}$ such that $sv_N(x) + tp = 1$. Then $v_N(x^s p^t) = 1$, so that $(x^{a-1})^s = (x^s p^t)^{a-1} \in U_N^{(1)} \setminus U_N^{(2)}$. Hence $x^{a-1} \notin U_N^{(2)}$, while clearly $x^{a-1} \in U_N^{(1)}$. $\square$

In the following we write $(T_a, (a-1)^j) \subseteq \mathcal{O}_K[G]$ for the $\mathcal{O}_K[G]$-submodule generated by T_a and $(a-1)^j$ where j is a non-negative integer.

Lemma 3.2.6. *a) Put $\theta := \theta_1\theta_2$. Then $\mathfrak{p}_N = \mathcal{O}_K[G]\theta$.*
b) For $j = 0, \dots, p-1$ we have $\mathfrak{p}_N^{j+1} = (p, (a-1)^j)\theta = (T_a, (a-1)^j)\theta$.

Proof. Part (a) is immediate from $\mathcal{O}_N = \mathcal{O}_M\mathcal{O}_{K'}$ and the definition of θ_1 and θ_2.

By Lemma 3.2.3 we have $(T_a, (a-1)^j) = (p, (a-1)^j)$ which shows the second equality in (b). Lemma 3.2.5 implies the chain of inclusions $I\theta \subseteq \mathfrak{p}_N^{j+1} \subseteq \mathfrak{p}_N = \mathcal{O}_K[G]\theta$, where we have set $I = I_j := (T_a, (a-1)^j)$. Since θ is a normal basis element we derive $[\mathcal{O}_K[G] : I] = [\mathcal{O}_K[G]\theta : I\theta]$. So it is enough to show the inequality $[\mathcal{O}_K[G] : I] \le [\mathfrak{p}_N : \mathfrak{p}_N^{j+1}]$. We observe that

$$\mathcal{O}_K[G] = \bigoplus_{i=0}^{p-1} \mathcal{O}_K[b](a-1)^i.$$

Finally, in order to complete the proof, we recall that $[\mathfrak{p}_N : \mathfrak{p}_N^{j+1}] = q^{dj}$ and note that the q^{dj} elements in $\bigoplus_{i=0}^{j-1} (\mathcal{O}_K/\mathfrak{p}_K)[b](a-1)^i$ cover the quotient $\mathcal{O}_K[G]/I$. $\square$

4 The computation of $E(\exp(\mathcal{L}))_p$

We assume the notations introduced in the previous section. We put $\mathcal{L} := p\mathfrak{p}_N = \mathfrak{p}_N^{p+1}$. By Lemma 3.1.2 $\mathcal{L}$ is a free $\mathbb{Z}_p[G]$-submodule of $\mathcal{O}_N$. Moreover, the exponential function of N is defined on $\mathcal{L}$ and by [14, II, Satz (5.5)] we have $\exp(\mathcal{L}) = U_N^{(p+1)}$. In this section we will compute a representative in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p) \simeq \mathbb{Q}_p[G]^\times/\mathbb{Z}_p[G]^\times$ for $E(\exp(\mathcal{L}))_p = E(U_N^{(p+1)})_p$ as described at the end of Section 2.2.

4.1 The local fundamental class

We will need the algebra $N_{\mathrm{nr}} = K_{\mathrm{nr}} \otimes_K N$, on which the group $\mathrm{Gal}(K_{\mathrm{nr}}/K) \times G$ acts canonically. We obtain an isomorphism $N_{\mathrm{nr}} \to N_0^d$ by sending $x \otimes y$ to $(F^{d-1}(x)y, F^{d-2}(x)y, \dots, F(x)y, xy)$. Then the action of $\mathrm{Gal}(K_{\mathrm{nr}}/K) \times G$ on N_{nr} induces an action on N_0^d. For later reference we explicitly describe the action for some particular elements (see [9, Sec. VI]):

$$\begin{aligned}
&(F^{-1} \times b)(x_1, x_2, \dots, x_d) = (x_1^b, x_2^b, \dots, x_d^b),\\
&(1 \times a)(x_1, x_2, \dots, x_d) = (x_1^a, x_2^a, \dots, x_d^a),\\
&(F \times 1)(x_1, x_2, \dots, x_d) = (x_d^{F_0}, x_1, x_2, \dots, x_{d-1}).
\end{aligned} \tag{4}$$

In particular, we deduce from (4)

$$\begin{aligned}
&(1 \times b)(x_1, x_2, \dots, x_d)\\
= \ &(F \times 1)(F^{-1} \times b)(x_1, x_2, \dots, x_d) = ((x_d^b)^{F_0}, x_1^b, x_2^b, \dots, x_{d-1}^b).
\end{aligned} \tag{5}$$

If L is a field extension of $\mathbb{Q}_p$ we put $L(s) := L^\times / U_L^{(s)}$ for each non-negative integer s. Let $\omega : N_{\mathrm{nr}}^\times \to \mathbb{Z}$ be the sum of the discrete valuations of the different components of $N_{\mathrm{nr}}^\times \simeq (N_0^\times)^d$. By the same arguments as in the proof of [9, Prop. 6.1] we obtain the following proposition.

Lemma 4.1.1. *We have the following exact sequence*

$$0 \to N(p+1) \to N_{\mathrm{nr}}(p+1) \xrightarrow{(F-1)\times 1} N_{\mathrm{nr}}(p+1) \xrightarrow{\omega} \mathbb{Z} \to 0 \tag{6}$$

of $\mathbb{Z}[G]$-modules. The extension class of this sequence is induced by the negative of the local fundamental class in $\mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, N^\times)$.

Proof. Analogous to the proof of [9, Prop. 6.1]. □

Let

$$\mathcal{F}' = \mathbb{Z}[G]z_1 \oplus \mathbb{Z}[G]z_2,$$

$$\mathcal{F}_{\geq n} = \bigoplus_{j=n}^{p-1} \bigoplus_{k=1}^{m} \mathbb{Z}[G]v_{k,j}$$

and let

$$\mathcal{F} = \mathcal{F}_{\geq 0}.$$

Note that the assignment $v_{k,j} \mapsto \alpha_k w_j$ induces an isomorphism

$$\mathcal{F}_p := \mathcal{F} \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{\simeq} \bigoplus_{j=0}^{p-1} \bigoplus_{k=1}^{m} \mathbb{Z}_p[G]\alpha_k w_j = \bigoplus_{j=0}^{p-1} \mathcal{O}_K[G]w_j \tag{7}$$

of free $\mathbb{Z}_p[G]$-modules.

In the following we let $[x_1, \dots, x_d]$ denote the class in $N_{\mathrm{nr}}(p+1)$ represented by $(x_1, \dots, x_d)$. If $x = x_1 = \dots = x_d$ we will often write $[x]$ instead of $[x, \dots, x]$.

Lemma 4.1.2. *There is a commuting diagram*

$$\begin{tikzcd}
0 \arrow[r] & X(2) \oplus \mathcal{F} \arrow[r] \arrow[d, "f_4"] & \mathcal{F}' \oplus \mathcal{F} \arrow[r, "\delta_2"] \arrow[d, "f_3"] & \mathbb{Z}[G]z_0 \arrow[r] \arrow[d, "f_2"] & \mathbb{Z} \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & N(p+1) \arrow[r] & N_{\mathrm{nr}}(p+1) \arrow[r, "(F-1)\times 1"] & N_{\mathrm{nr}}(p+1) \arrow[r] & \mathbb{Z} \arrow[r] & 0.
\end{tikzcd}$$

of $\mathbb{Z}[G]$*-modules with*

$$\begin{aligned}
&\delta_2(z_1) = (b-1)z_0, \\
&\delta_2(z_2) = (a-1)z_0, \\
&\delta_2(v_{k,j}) = 0 \textit{ for all } k \textit{ and } j, \\
&f_2(z_0) = f_3(z_1) = [\theta_1, 1, 1, \dots, 1], \\
&f_3(z_1) = [\theta_1, 1, \dots, 1], \\
&f_3(z_2) = [\gamma, \gamma, \dots, \gamma], \\
&f_3(v_{k,j}) = 1 + \alpha_k (a-1)^j \theta \textit{ for all } k \textit{ and } j.
\end{aligned}$$

Further, $X(2) := \ker(\delta_2 \mid_{\mathcal{F}'})$ *and* f_4 *is the restriction of* f_3 *to* $X(2) \oplus \mathcal{F}$*.*

Proof. Straightforward verification. □

The diagram in Lemma 4.1.2 will be fundamental for our proof of Theorem 1. We will use the top exact sequence to compute groups of the form $\mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, \_)$. By Proposition 4.1.4 below we can then apply the recipe described in Section 2.2 with $\Sigma = X(2) \oplus \mathcal{F}$ and $\varphi = -f_4$ to compute $E(U_N^{(p+1)})_p$.

In the remainder of this subsection we will provide the proof of the following lemma.

Lemma 4.1.3. *The homomorphism* f_4 *is surjective.*

As a consequence we obtain

Proposition 4.1.4. *The map* $-f_4$ *represents the local fundamental class.*

Proof. This can be proved by mimicking the proof of [9, Lemma 6.3]. □

Lemma 4.1.5. *We have*

$$X(2) = \langle (a-1)z_1 - (b-1)z_2, T_b z_1, T_a z_2 \rangle_{\mathbb{Z}[G]}.$$

Proof. The inclusion "$\supseteq$" is immediate from the definition of δ_2. Let us consider the reverse inclusion. Let

$$x = \sum_{i=0}^{p-1} \sum_{j=0}^{d-1} \alpha_{i,j} a^i b^j z_1 + \sum_{i=0}^{p-1} \sum_{j=0}^{d-1} \beta_{i,j} a^i b^j z_2 \in X(2)$$

with $\alpha_{i,j}, \beta_{i,j} \in \mathbb{Z}$. From $\delta_2(x) = 0$ we derive

$$\alpha_{i,j-1} - \alpha_{i,j} + \beta_{i-1,j} - \beta_{i,j} = 0 \qquad (8)$$

for all $0 \le i < p$ and $0 \le j < d$. Here and in the following we regard all indices as integers modulo p and d respectively.

From (8) we deduce that $\alpha := \sum_{i=0}^{p-1} \alpha_{i,j}$ does not depend on the choice of j. Now we are looking for integers $\gamma_{i,j}, \mu_i, \nu_j$, for $0 \le i < p$ and $0 \le j < d$, such that

$$\begin{aligned} x &= \sum_{i=0}^{p-1} \sum_{j=0}^{d-1} \gamma_{i,j} a^i b^j ((a-1)z_1 - (b-1)z_2) + \sum_{i=0}^{p-1} \mu_i a^i T_b z_1 + \sum_{j=0}^{d-1} \nu_j b^j T_a z_2 \\ &= \sum_{i=0}^{p-1} \sum_{j=0}^{d-1} (\gamma_{i-1,j} - \gamma_{i,j} + \mu_i) a^i b^j z_1 + \sum_{i=0}^{p-1} \sum_{j=0}^{d-1} (-\gamma_{i,j-1} + \gamma_{i,j} + \nu_j) a^i b^j z_2. \end{aligned}$$

So, in other words, the lemma is proved if we find integers $\gamma_{i,j}, \mu_i, \nu_j$ such that

$$\alpha_{i,j} = \gamma_{i-1,j} - \gamma_{i,j} + \mu_i \tag{9}$$

and

$$\beta_{i,j} = -\gamma_{i,j-1} + \gamma_{i,j} + \nu_j. \tag{10}$$

With $\nu_j := \beta_{0,j}$, $\mu_0 := \alpha$, $\mu_i = 0$ for $i > 0$ and $\gamma_{i,j} = -\sum_{1 \le \ell \le i} \alpha_{\ell,j}$ it is straightforward to verify (9). Equality (10) is proved by an easy induction on i using (8). □

We evaluate f_4 at the three special elements of $X(2)$ given by the last lemma.

Lemma 4.1.6. *We have*

$$f_4((a-1)z_1 - (b-1)z_2) = [\gamma]^{1-b}, \tag{11}$$

$$f_4(T_b z_1) = [\theta_1] \tag{12}$$

and

$$f_4(T_a z_2) = [\gamma]^{T_a}. \tag{13}$$

Proof. Straightforward computation using (4), (5), $\theta_1^b = \theta_1$ and $[\theta_1, 1, \dots, 1]^{a-1} = [\theta_1^b, 1, \dots, 1]^{a-1} = [\gamma^{b(F_0-1)}, 1, \dots, 1]$. □

We write $\hat{f}_4 \colon X(2)_p \oplus \mathcal{F}_p \longrightarrow N(p+1)_p$ for the p-completion of f_4. For an element $\beta \in \mathcal{O}_K[G]$ we write $\beta = \sum_{k=1}^m \lambda_k \alpha_k$ with uniquely determined $\lambda_k \in \mathbb{Z}_p[G]$ and according to (7) we set $\hat{f}_4(\beta w_j) := \prod_{k=1}^m f_4(v_{k,j})^{\lambda_k}$.

Lemma 4.1.7. *Let $\beta \in \mathcal{O}_K[G]$. Then we have for $j = 0, \dots, p-1$*

$$\hat{f}_4(\beta w_j) \equiv 1 + (a-1)^j \beta\theta \pmod{U_N^{(j+2)}}.$$

Proof. As above we write $\beta = \sum_{k=1}^m \lambda_k \alpha_k$. We note that that for $n \ge 1$ the map $x \mapsto 1 + x$ induces an isomorphism $\mathfrak{p}_N^n / \mathfrak{p}_N^{n+1} \simeq U_N^{(n)} / U_N^{(n+1)}$ of $\mathbb{Z}_p[G]$-modules. By Lemma 3.2.5 we have $v_N((a-1)^j\theta) = j + 1$. Therefore,

$$\begin{aligned} \hat{f}_4(\beta w_j) &= \prod_{k=1}^m (1 + \alpha_k (a-1)^j \theta)^{\lambda_k} \\ &\equiv 1 + \sum_{k=1}^m \lambda_k \alpha_k (a-1)^j \theta \pmod{U_N^{(j+2)}} \\ &\equiv 1 + \beta (a-1)^j \theta \pmod{U_N^{(j+2)}}. \end{aligned}$$

□

Lemma 4.1.8. *For $j = 0, \ldots, p$, any element of $U_N^{(j+1)}/U_N^{(p+1)}$ is the image under $\hat{f}_4$ of an element in $(\mathcal{F}_{\geq j})_p$.*

Proof. For $j = p$, $\mathcal{F}_{\geq p} = \{0\}$ and $U_N^{(p+1)}/U_N^{(p+1)} = \{0\}$, so the result is trivial.

We assume the result for $j + 1$ and proceed by descending induction. If $x \in U_N^{(j+1)}/U_N^{(p+1)}$, then $x = 1 + \mu p\theta + \nu(a-1)^j\theta$ for some $\mu, \nu \in \mathcal{O}_K[G]$ by Lemma 3.2.6. Since $\mu p\theta \in \mathfrak{p}_N^{p+1}$, Lemma 4.1.7 implies

$$x \equiv 1 + \nu(a-1)^j\theta \equiv \hat{f}_4(\nu w_j) \pmod{U_N^{j+2}}.$$

This means that x is the product of an element in the image of $(\mathcal{F}_{\geq j})_p$ and an element in $U_N^{(j+2)}/U_N^{(p+1)}$, which is by assumption in the image of $(\mathcal{F}_{\geq j+1})_p \subseteq (\mathcal{F}_{\geq j})_p$. □

After these preparations we are ready to provide the proof of Lemma 4.1.3.

Proof of Lemma 4.1.3. We recall the properties of γ described in Lemma 3.1.5. Since a is in the inertia group, by (13) we obtain $f_4(T_a z_2) = [\gamma]^{T_a} \equiv [\gamma]^p \pmod{\mathfrak{p}_N}$. Since $\gamma \equiv \zeta_{q^d-1} \pmod{\mathfrak{p}_{N_0}}$, its class is a generator of $U_N/U_N^{(1)}$. Since p is co-prime to the order $q^d - 1$ of $U_N/U_N^{(1)}$, we conclude that the projection of $f_4(X(2))$ onto $N(1)$ contains the torsion subgroup $U_N/U_N^{(1)}$ of $N(1)$.

By (12) we obtain $f_4(T_b z_1) = [\theta_1]$ and recall that θ_1 is a prime element in N. We conclude that any element of $N(p+1)$ is the product of an element in the image of f_4 and an element in $U_N^{(1)}/U_N^{(p+1)}$. It therefore remains to prove that $U_N^{(1)}/U_N^{(p+1)}$ is also in the image of f_4. Since $U_N^{(1)}/U_N^{(p+1)}$ is a finite p-group this follows immediately from Lemma 4.1.8. □

4.2 The kernel of $\hat{f}_4$

In order to compute a representative of $E(\exp(\mathcal{L}))_p$ we have to compute a $\mathbb{Z}_p[G]$-basis of $\ker(f_4)_p = \ker(\hat{f}_4)$. As a first step in this direction we construct certain explicit elements in $\ker(\hat{f}_4)$ and show that they form a complete set of generators. We then manipulate this set of generators in order to obtain a basis. The main result is summarized in Proposition 4.2.10.

Lemma 4.2.1. *Let $\tilde{m}$ be an integer such that $m\tilde{m} \equiv 1 \pmod d$. Set*

$$\tilde{t}_1 \;:=\; (a-1)z_1 - (b-1)z_2 + \left(\sum_{i=2}^{m} \alpha_i b^{1-(i-2)\tilde{m}} + \left(\alpha_1 - \sum_{i=2}^{m} \alpha_i\right) b^{\tilde{m}}\right) w_0.$$

Then there exists $y_1 \in (\mathcal{F}_{\geq 1})_p$, such that $t_1 := \tilde{t}_1 + y_1 \in \ker(\hat{f}_4)$.

Proof. We calculate $\hat{f}_4(\tilde{t}_1)$ modulo $\mathfrak{p}_N^2$. First we recall that $\gamma \equiv \zeta_{q^d-1}(1 + x_2\theta_1) \pmod{\mathfrak{p}_{N_0}^2}$ by Lemma 3.1.5. Note also that for any integer $s \geq 2$ one has $\zeta_{q^d-1} = 1$ in the p-completion $N(s)_p$ of $N(s)$. By the definition of $\hat{f}_4$, Lemma 4.1.6 and Lemma 4.1.7,

$$\begin{aligned}\hat{f}_4(\tilde{t}_1) &\equiv \gamma^{1-b}(1 + \alpha_1 b^{\tilde{m}}\theta) \prod_{i=2}^{m} \left((1 + \alpha_i b^{1-(i-2)\tilde{m}}\theta)(1 + \alpha_i b^{\tilde{m}}\theta)^{-1}\right) \pmod{\mathfrak{p}_{N_0}^2} \\ &\equiv (1 + x_2\theta)^{1-b} \left(1 + \alpha_1 \theta^{b^{\tilde{m}}} + \sum_{i=0}^{m-2} \alpha_{i+2}\theta^{b^{1-i\tilde{m}}} - \sum_{i=0}^{m-2} \alpha_{i+2}\theta^{b^{\tilde{m}}}\right) \pmod{\mathfrak{p}_{N_0}^2}.\end{aligned}$$

Now we see that

$$\begin{aligned}(1+x_2\theta_1)^{1-b} &\equiv (1+x_2\theta_1)(1+x_2\theta_1)^{-b} \equiv (1+x_2\theta_1)(1-x_2^b\theta_1) \pmod{\mathfrak{p}_{N_0}^2}\\ &\equiv 1+x_2\theta_1 - x_2^b\theta_1 \equiv 1+\left(\left(\frac{x_2}{\alpha_1}\right)^F - \frac{x_2}{\alpha_1}\right)^b \alpha_1\theta_1 \pmod{\mathfrak{p}_{N_0}^2}\\ &\equiv 1+\left(\left(\frac{x_2}{\alpha_1}\right)^q - \frac{x_2}{\alpha_1}\right)^b \alpha_1\theta_1 \pmod{\mathfrak{p}_{N_0}^2}.\end{aligned} \tag{14}$$

By the choice of the basis $\alpha_1,\dots,\alpha_m$ in (2) we have $A^{f^i} = \frac{\alpha_{i+2}}{\alpha_1}$ for $i=0,\dots,m-2$ and $A^{f^{m-1}} = 1-\sum_{i=0}^{m-2} A^{f^i} = 1-\sum_{i=0}^{m-2}\frac{\alpha_{i+2}}{\alpha_1}$. So we get

$$\begin{aligned}\left(\frac{x_2}{\alpha_1}\right)^q - \frac{x_2}{\alpha_1} &\equiv \sum_{i=0}^{m-1}\left(\left(\frac{x_2}{\alpha_1}\right)^{p^{i+1}} - \left(\frac{x_2}{\alpha_1}\right)^{p^i}\right) \pmod{\mathfrak{p}_{N_0}}\\ &\equiv \sum_{i=0}^{m-1}\left(\left(\frac{x_2}{\alpha_1}\right)^p - \left(\frac{x_2}{\alpha_1}\right)\right)^{p^i} \pmod{\mathfrak{p}_{N_0}}\\ &\overset{(i)}{\equiv} -\sum_{i=0}^{m-1}(A\theta_2)^{p^i} \pmod{\mathfrak{p}_{N_0}}\\ &\overset{(ii)}{\equiv} -\sum_{i=0}^{m-2} A^{p^i}\theta_2^{p^{im\tilde{m}}} - A^{p^{m-1}}\theta_2^{p^{(m-1)m\tilde{m}}} \pmod{\mathfrak{p}_{N_0}}\\ &\equiv -\sum_{i=0}^{m-2}\frac{\alpha_{i+2}}{\alpha_1}\theta_2^{q^{i\tilde{m}}} - \left(1-\sum_{i=0}^{m-2}\frac{\alpha_{i+2}}{\alpha_1}\right)\theta_2^{q^{1-\tilde{m}}} \pmod{\mathfrak{p}_{N_0}}.\end{aligned}$$

The congruence (i) follows from our choice of x_2 and (ii) is immediate from $\theta_2 \in \tilde{K}'$.

Combining the last congruence with the computation in (14) and recalling that $\theta_1^b = \theta_1$ we obtain

$$\begin{aligned}(1+x_2\theta_1)^{1-b} &\equiv 1-\left(\sum_{i=0}^{m-2}\frac{\alpha_{i+2}}{\alpha_1}\theta_2^{q^{i\tilde{m}}} + \left(1-\sum_{i=0}^{m-2}\frac{\alpha_{i+2}}{\alpha_1}\right)\theta_2^{q^{1-\tilde{m}}}\right)^b \alpha_1\theta_1 \pmod{\mathfrak{p}_{N_0}^2}\\ &\equiv 1-\sum_{i=0}^{m-2}\alpha_{i+2}\theta^{b^{1-i\tilde{m}}} - \alpha_1\theta^{b^{\tilde{m}}} + \sum_{i=0}^{m-2}\alpha_{i+2}\theta^{b^{\tilde{m}}} \pmod{\mathfrak{p}_{N_0}^2}.\end{aligned}$$

So we conclude that

$$\hat{f}_4(\tilde{t}_1) \equiv 1-\left(\alpha_1\theta^{b^{\tilde{m}}} + \sum_{i=0}^{m-2}\alpha_{i+2}\theta^{b^{1-i\tilde{m}}} - \sum_{i=0}^{m-2}\alpha_{i+2}\theta^{b^{\tilde{m}}}\right)^2 \equiv 1 \pmod{\mathfrak{p}_{N_0}^2}.$$

Therefore $\hat{f}_4(\tilde{t}_1)^{-1} \in U_N^{(2)}/U_N^{(p+1)}$ and by Lemma 4.1.8 there exists $y_1 \in (\mathcal{F}_{\geq 1})_p$ such that $\hat{f}_4(y_1) \equiv \hat{f}_4(\tilde{t}_1)^{-1} \pmod{\mathfrak{p}_N^{p+1}}$, i.e. $\tilde{t}_1 + y_1 \in \ker(\hat{f}_4)$. □

Lemma 4.2.2. *The element*

$$t_2 := T_a z_2 - \beta w_{p-1} \text{ with } \beta = \begin{cases}\alpha_1, & \text{if } m=1,\\ \alpha_2, & \text{if } m>1,\end{cases}$$

is in the kernel of $\hat{f}_4$.

Proof. Since $\zeta_{q^d-1} = 1$ in $N(p+1)_p$ and $\gamma \equiv \zeta_{q^d-1}(1+x_2\theta_1) \pmod{\mathfrak{p}_{N_0}^2}$ the formulae in Lemma 4.1.6 and Lemma 4.1.7 imply

$$\begin{aligned}\hat{f}_4(t_2) &\equiv \gamma^{T_a}(1-\beta(a-1)^{p-1}\theta) \pmod{\mathfrak{p}_{N_0}^{p+1}}\\ &\equiv \mathcal{N}_{N_0/K_{\mathrm{nr}}}(1+x_2\theta_1)(1-\beta(a-1)^{p-1}\theta) \pmod{\mathfrak{p}_{N_0}^{p+1}}.\end{aligned}$$

Note that by [16, Sec. V.6, Prop. 8] we know that $\mathcal{N}_{N_0/K_{\mathrm{nr}}}U_{N_0}^{(2)} \subseteq U_{K_{\mathrm{nr}}}^{(2)} \subseteq U_{N_0}^{(2p)} \subseteq U_{N_0}^{(p+1)}$ so that it suffices to work with γ modulo $\mathfrak{p}_{N_0}^2$. Using Lemma 3.2.4, [16, Sec. V.3, Lemma 5], the fact that $x_2 \in \mathcal{O}_{K_{\mathrm{nr}}}$ and Lemma 3.2.2, we get

$$\begin{aligned}\hat{f}_4(t_2) &\equiv \mathcal{N}_{N_0/K_{\mathrm{nr}}}(1+x_2\theta_1)(1-\beta\theta_2 p) \pmod{\mathfrak{p}_{N_0}^{p+1}}\\ &\equiv (1+\mathcal{T}_{N_0/K_{\mathrm{nr}}}(x_2\theta_1)+\mathcal{N}_{N_0/K_{\mathrm{nr}}}(x_2\theta_1))(1-\beta\theta_2 p) \pmod{\mathfrak{p}_{N_0}^{p+1}}\\ &\equiv (1+x_2p - x_2^p\alpha_1^{1-p}p)(1-\beta\theta_2 p) \pmod{\mathfrak{p}_{N_0}^{p+1}}\\ &\equiv 1+(x_2 - x_2^p\alpha_1^{1-p} - \beta\theta_2)p \pmod{\mathfrak{p}_{N_0}^{p+1}}.\end{aligned}$$

By the choice of x_2 made after Lemma 3.1.3 we have

$$x_2^p\alpha_1^{1-p} = \alpha_1\left(\frac{x_2}{\alpha_1}\right)^p \equiv \alpha_1\cdot\left(\frac{x_2}{\alpha_1} - A\theta_2\right) \equiv x_2 - A\alpha_1\theta_2 \equiv x_2 - \beta\theta_2 \pmod{\mathfrak{p}_{K_{\mathrm{nr}}}},$$

so that $\hat{f}_4(t_2) \equiv 1 \pmod{\mathfrak{p}_{N_0}^{p+1}}$. □

Lemma 4.2.3. *The elements t_1 and t_2 generate $\left(\ker\hat{f}_4 + \mathcal{F}_p\right)/\mathcal{F}_p$ as a $\mathbb{Z}_p[G]$-module.*

Proof. We write $W \subseteq X(2)_p \oplus \mathcal{F}_p$ for the $\mathbb{Z}_p[G]$-submodule which is generated by $\mathcal{F}_p$, t_1 and t_2. For each $x \in \ker\hat{f}_4$ we have to show that $x \in W$. In the following all congruences are modulo W. By Lemma 4.1.5 there exist $x_1, x_2, x_3 \in \mathbb{Z}_p[G]$ such that

$$x \equiv x_1((a-1)z_1 - (b-1)z_2) + x_2T_bz_1 + x_3T_az_2.$$

From the definitions of t_1 and t_2 we immediately obtain

$$T_az_2 \in W \text{ and } (a-1)z_1 - (b-1)z_2 \in W.$$

Hence $x \equiv x_2T_bz_1$. Without loss of generality we may assume $x_2 \in \mathbb{Z}_p[a]$. By considering $\hat{f}_4(x)$ modulo $U_N^{(1)}$ and using Lemma 4.1.6, we see that, to kill the $[\theta_1]$, x_2 must be in the augmentation ideal. Therefore there exists $x_4 \in \mathbb{Z}_p[a]$ such that $x_2 = x_4(a-1)$. Then $x \equiv x_4(a-1)T_bz_1 = x_4T_b((a-1)z_1 - (b-1)z_2) \equiv 0$. □

Lemma 4.2.4. *Let $0 \le j \le p-1$, $1 \le k \le m$. Then there exists $\mu_{j,k} \in (\mathcal{F}_{\ge j+2})_p$ such that the element*

$$s_{j,k} = \alpha_k(a-1)w_j - \alpha_kw_{j+1} + \mu_{j,k}$$

is in the kernel of $\hat{f}_4$. Here w_p should be interpreted as 0.

Proof. For $l \geq 1$ we put $\eta_l := \alpha_k(a-1)^{l-1}\theta$. Note that $v_N(\eta_l) = l$ for $1 \leq l \leq p$. In the following all congruences are modulo $U_N^{(j+3)}$. Then we compute

$$\begin{aligned}
&\hat{f}_4((a-1)\alpha_k w_j - \alpha_k w_{j+1}) \\
&\quad = (1+\eta_{j+1})^{a-1}(1+\eta_{j+2})^{-1} \\
&\quad \equiv (1+a\eta_{j+1})(1-\eta_{j+1}+\eta_{j+1}^2)(1-\eta_{j+2}) \\
&\quad \equiv (1-\eta_{j+1}+\eta_{j+1}^2+a\eta_{j+1}-(a\eta_{j+1})\eta_{j+1})(1-\eta_{j+2}) \\
&\quad \equiv (1+\eta_{j+2}-\eta_{j+1}\eta_{j+2})(1-\eta_{j+2}) \\
&\quad \equiv (1+\eta_{j+2})(1-\eta_{j+2}) \equiv 1.
\end{aligned}$$

Now we conclude using Lemma 4.1.8 as in the proof of Lemma 4.2.1. □

By construction, any element of $\mathcal{F}_p' \oplus \mathcal{F}_p$ can be written as a linear combination of z_1, z_2 and $\alpha_i w_j$, for $i = 1, \ldots, m$ and $j = 0, \ldots, p-1$ with coefficients in $\mathbb{Z}_p[G]$. In this context we will speak of z_1-, z_2- and $\alpha_i w_j$-components of elements of $\ker \hat{f}_4$.

We recall that $\tilde{m}$ is an integer such that $m\tilde{m} \equiv 1 \pmod{d}$.

Lemma 4.2.5. *The element*

$$r_1 = T_a t_1 + (b-1)t_2$$

belongs to $\ker \hat{f}_4 \cap \mathcal{F}_p$ *and its* $\alpha_1 w_0$*-component is* $m^{\tilde{m}} T_a$*.*

Proof. By the definition of t_1 and t_2 in Lemmata 4.2.1 and 4.2.2 the element r_1 belongs to $\ker(\hat{f}_4)$. Hence it suffices to prove that the z_1- and z_2-components of r_1 are zero and the $\alpha_1 w_0$-component is T_a. This follows by a straightforward computation. □

Lemma 4.2.6. *The elements*

$$r_k = \alpha_k T_a w_0 + (b^{-\tilde{m}}\alpha_{k+1} - \alpha_k) w_{p-1},$$

for $1 < k < m$*, and*

$$r_m = \alpha_m T_a w_0 + \left(b^{-\tilde{m}}\alpha_1 - b^{-\tilde{m}} \sum_{i=2}^{m} \alpha_i - \alpha_m \right) w_{p-1}$$

are in the kernel of $\hat{f}_4$*.*

Proof. For $1 < k \leq m$, using [16, Sec. V.3, Lemma 4 and Lemma 5], Lemma 3.1.2 and Lemma 3.2.2,

$$\begin{aligned}
\hat{f}_4(\alpha_k T_a w_0) &\equiv \mathcal{N}_{N/K'}(1+\alpha_k\theta) \pmod{\mathfrak{p}_N^{p+1}} \\
&\equiv 1 + \mathcal{N}_{N/K'}(\alpha_k\theta) + \mathcal{T}_{N/K'}(\alpha_k\theta) \pmod{\mathfrak{p}_N^{p+1}} \\
&\equiv 1 + (\theta_2\alpha_k)^p \mathcal{N}_{N/K'}(\theta_1) + \theta_2\alpha_k \mathcal{T}_{N/K'}(\theta_1) \pmod{\mathfrak{p}_N^{p+1}} \\
&\equiv 1 - (\theta_2\alpha_k)^p \alpha_1^{1-p} p + \theta_2\alpha_k p \pmod{\mathfrak{p}_N^{p+1}} \\
&\equiv 1 + \left(\frac{\theta_2\alpha_k}{\alpha_1} - \left(\frac{\theta_2\alpha_k}{\alpha_1}\right)^p \right) \alpha_1 p \pmod{\mathfrak{p}_N^{p+1}}.
\end{aligned}$$

Now we note that $\theta_2^p \equiv \theta_2^{p^{m\tilde{m}}} \equiv \theta_2^{q^{\tilde{m}}} \equiv \theta_2^{b^{-\tilde{m}}} \pmod{\mathfrak{p}_{\tilde{K}'}}$ and by (2) we have for $1 < k < m$,

$$\left(\frac{\alpha_k}{\alpha_1}\right)^p = \left(A^{f^{k-2}}\right)^p \equiv A^{p^{k-1}} \equiv \frac{\alpha_{k+1}}{\alpha_1} \pmod{\mathfrak{p}_K}$$

and

$$\left(\frac{\alpha_m}{\alpha_1}\right)^p = \left(A^{f^{m-2}}\right)^p \equiv A^{f^{m-1}} = 1 - \sum_{i=0}^{m-2} A^{f^i} = 1 - \sum_{i=0}^{m-2} \frac{\alpha_{i+2}}{\alpha_1} \pmod{\mathfrak{p}_K}.$$

Therefore, for $1 < k < m$,

$$\begin{aligned}\hat{f}_4(\alpha_k T_a w_0) &\equiv 1 + \left(\frac{\theta_2 \alpha_k}{\alpha_1} - \frac{\theta_2^{b^{-\tilde{m}}} \alpha_{k+1}}{\alpha_1}\right) \alpha_1 p \pmod{\mathfrak{p}_N^{p+1}} \\ &\equiv 1 + \left(\alpha_k \theta_2 - \alpha_{k+1} \theta_2^{b^{-\tilde{m}}}\right) p \pmod{\mathfrak{p}_N^{p+1}}\end{aligned}$$

and

$$\begin{aligned}\hat{f}_4(\alpha_m T_a w_0) &\equiv 1 + \left(\frac{\theta_2 \alpha_m}{\alpha_1} - \theta_2^{b^{-\tilde{m}}} \left(1 - \sum_{i=0}^{m-2} \frac{\alpha_{i+2}}{\alpha_1}\right)\right) \alpha_1 p \pmod{\mathfrak{p}_N^{p+1}} \\ &\equiv 1 + \left(\alpha_m \theta_2 - \alpha_1 \theta_2^{b^{-\tilde{m}}} + \sum_{i=2}^{m} \alpha_i \theta_2^{b^{-\tilde{m}}}\right) p \pmod{\mathfrak{p}_N^{p+1}}.\end{aligned}$$

Recalling Lemma 3.2.4, for $1 < k < m$ we obtain

$$\begin{aligned}\hat{f}_4((b^{-\tilde{m}}\alpha_{k+1} - \alpha_k) w_{p-1}) &\equiv (1 + \alpha_{k+1} p \theta_2)^{b^{-\tilde{m}}} (1 + \alpha_k p \theta_2)^{-1} \pmod{\mathfrak{p}_N^{p+1}} \\ &\equiv 1 - \left(\alpha_k \theta_2 - \alpha_{k+1} \theta_2^{b^{-\tilde{m}}}\right) p \pmod{\mathfrak{p}_N^{p+1}}\end{aligned}$$

and

$$\begin{aligned}&\hat{f}_4\left(\left(b^{-\tilde{m}}\alpha_1 - b^{-\tilde{m}} \sum_{i=2}^{m} \alpha_i - \alpha_m\right) w_{p-1}\right) \\ &\equiv (1 + \alpha_1 p \theta_2)^{b^{-\tilde{m}}} \prod_{i=2}^{m} (1 + \alpha_i p \theta_2)^{-b^{-\tilde{m}}} (1 + \alpha_m p \theta_2)^{-1} \pmod{\mathfrak{p}_N^{p+1}} \\ &\equiv 1 - \left(\alpha_m \theta_2 - \alpha_1 \theta_2^{b^{-\tilde{m}}} + \sum_{i=2}^{m} \alpha_i \theta_2^{b^{-\tilde{m}}}\right) p \pmod{\mathfrak{p}_N^{p+1}}\end{aligned}$$

Therefore we conclude that in all cases $r_k \in \ker \hat{f}_4$. □

Lemma 4.2.7. *The $pm + m$ elements $r_k, s_{j,k}$ for $0 \leq j \leq p-1$, $1 \leq k \leq m$ generate $\ker \hat{f}_4 \cap \mathcal{F}_p$ as a $\mathbb{Z}_p[G]$-module.*

Proof. We define elements $r_{j,k}$, for $0 \leq j \leq p-1$, $1 \leq k \leq m$, as follows: $r_{0,k} = r_k$ and $r_{j,k} = T_a s_{j-1,k}$, for $j > 0$. It will suffice to show that the $2pm$ elements $r_{j,k}, s_{j,k}$ for $0 \leq j \leq p-1$, $1 \leq k \leq m$ are generators of $\ker \hat{f}_4 \cap \mathcal{F}_p$.

It is obvious that they generate $\ker \hat{f}_4 \cap (\mathcal{F}_{\geq p})_p = \{0\}$. Let us assume they generate $\ker \hat{f}_4 \cap (\mathcal{F}_{\geq j+1})_p$, for some $j < p$, and let us prove that they generate $\ker \hat{f}_4 \cap (\mathcal{F}_{\geq j})_p$.

Let $x \in \ker \hat{f}_4 \cap (\mathcal{F}_{\geq j})_p$. We can write $x = \lambda_1 w_j + \lambda_2$, for some $\lambda_1 \in \mathcal{O}_K[G]$ and $\lambda_2 \in (\mathcal{F}_{\geq j+1})_p$. Then by Lemma 4.1.7 we have $\hat{f}_4(x) \equiv 1 + (a-1)^j \lambda_1 \theta \pmod{U_N^{(j+2)}}$, which must be congruent to 1 by the assumption that $x \in \ker \hat{f}_4$. Hence

$$(a-1)^j \lambda_1 \theta \in \mathfrak{p}_N^{j+2}. \tag{15}$$

By Lemma 3.2.5, if $v_N(\lambda_1\theta) = 1$, then $v_N((a-1)^j\lambda_1\theta) = j+1$ (recall that $j < p$), and this contradicts (15). Hence $v_N(\lambda_1\theta) > 1$, so that Lemma 3.2.6 implies $\lambda_1\theta \in \mathfrak{p}_N^2 = (T_a, a-1)\theta$. It follows that $\lambda_1 \in (T_a, a-1)$. So in particular $\lambda_1 w_j$ is a sum of a linear combination of the elements $r_{j,k}$ and $s_{j,k}$, for $k = 1, \ldots, m$, and an element in $(\mathcal{F}_{\geq j+1})_p$. Hence also x is a combination of the elements $r_{j,k}$ and $s_{j,k}$ and an element in $(\mathcal{F}_{\geq j+1})_p$, which must also be in $\ker \hat{f}_4$. To conclude we only need to recall the inductive hypothesis. □

Now we consider the $\alpha_i w_{p-1}$-components, $i = 1, \ldots, m$, of t_2 and r_k for $k = 2, \ldots, m$. We write these components as the columns of an $m \times m$ matrix $\mathcal{M}$. We have to distinguish two cases. If $m > 1$,

$$\mathcal{M} = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & 0 & b^{-\tilde{m}} \\ -1 & -1 & 0 & \ldots & 0 & 0 & 0 & -b^{-\tilde{m}} \\ 0 & b^{-\tilde{m}} & -1 & \ldots & 0 & 0 & 0 & -b^{-\tilde{m}} \\ 0 & 0 & b^{-\tilde{m}} & \ldots & 0 & 0 & 0 & -b^{-\tilde{m}} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & \ldots & b^{-\tilde{m}} & -1 & 0 & -b^{-\tilde{m}} \\ 0 & 0 & 0 & \ldots & 0 & b^{-\tilde{m}} & -1 & -b^{-\tilde{m}} \\ 0 & 0 & 0 & \ldots & 0 & 0 & b^{-\tilde{m}} & -1-b^{-\tilde{m}} \end{pmatrix}.$$

If $m = 1$, then the matrix is determined only by t_2 and, recalling its definition from Lemma 4.2.2, we get $\mathcal{M} = (-1)$.

Lemma 4.2.8. *The determinant of $\mathcal{M}$ is $(-1)^m b^{-\tilde{m}(m-1)} = (-1)^m b^{\tilde{m}-1}$.*

Proof. This is an easy calculation. □

Lemma 4.2.9. *For $k = 1, \ldots, m$ we have $s_{p-1,k} \in \langle t_2, r_2, \ldots, r_m \rangle_{\mathbb{Z}_p[G]}$.*

Proof. We fix k such that $1 \leq k \leq m$. Recall that $s_{p-1,k} = \alpha_k(a-1)w_{p-1}$. By Lemma 4.2.8 there is a $\mathbb{Z}_p[G]$-linear combination x of t_2 and the elements r_i, $i = 2, \ldots, m$, such that the $\alpha_k w_{p-1}$-component of x is 1 and the $\alpha_j w_{p-1}$-components for $j \neq k$ are zero. The components of x outside of $\alpha_i w_{p-1}$ are (by the definition of t_2 and r_i) always multiples of T_a. Therefore we can conclude that $(a-1)x = s_{p-1,k}$. □

We are now ready to state and prove the main result of this subsection.

Proposition 4.2.10. *The $pm+1$ elements t_1, t_2, r_k, for $k = 2, \ldots, m$, $s_{j,k}$ for $0 \leq j \leq p-2$, $1 \leq k \leq m$ constitute a $\mathbb{Z}_p[G]$-basis of* $\ker \hat{f}_4$.

Proof. By Lemma 4.2.9 and the definition of r_1, it is enough to show that the $pm + m + 2$ elements t_1, t_2 and $r_k, s_{j,k}$ for $0 \leq j \leq p-1$, $1 \leq k \leq m$ are generators. This has been shown in Lemma 4.2.3 and Lemma 4.2.7. □

Writing the z_1-, z_2- and $\alpha_i w_j$-components of the above generators as the columns of a matrix $\mathfrak{M}$ we obtain

$$\mathfrak{M} = \begin{pmatrix} a-1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1-b & T_a & 0 & 0 & 0 & \cdots & 0 & 0 \\ v & 0 & T_a\tilde{I} & (a-1)I & 0 & \cdots & 0 & 0 \\ * & 0 & 0 & -I & (a-1)I & \cdots & 0 & 0 \\ * & 0 & 0 & * & -I & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ * & 0 & 0 & * & * & \cdots & -I & (a-1)I \\ * & -e_2 & \tilde{\mathcal{M}} & * & * & \cdots & * & -I \end{pmatrix},$$

where I is the $m \times m$-identity matrix and $\tilde{\mathcal{M}}$ and $\tilde{I}$ denote the matrices obtained by removing the first column of $\mathcal{M}$ and I respectively. If $m > 1$ the vector e_2 is the second vector in the canonical basis of $\mathbb{Z}_p[G]^m$, and if $m = 1$ we set $e_2 = (1)$. Finally, $v \in \mathbb{Z}_p[G]^m$ is a vector with first component $b^{\tilde{m}}$.

4.3 Computation of the representative of $E(\exp(\mathcal{L}))_p$

We recall that $G = \mathrm{Gal}(N/K) = \langle a \rangle \times \langle b \rangle$. Any irreducible character ψ of G decomposes as $\psi = \chi\phi$, where χ is an irreducible character of $\langle a \rangle$ and ϕ an irreducible character of $\langle b \rangle$.

We also recall that we always identify $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ with $\mathbb{Q}_p[G]^\times / \mathbb{Z}_p[G]^\times$. The following proposition describes a representative of $E(\exp(\mathcal{L}))_p$ in $\mathbb{Q}_p[G]^\times$, which we regard as a subset of $\mathbb{Q}_p^c[G]^\times \simeq \bigoplus_{\chi,\phi} \mathbb{Q}_p^{c,\times}$.

Proposition 4.3.1. *We assume the setting introduced in Section 3. For $\mathcal{L} = \mathfrak{p}_N^{p+1}$ the element $E(\exp(\mathcal{L}))_p$ is represented by $\varepsilon \in \mathbb{Q}_p[G]^\times$ where*

$$\varepsilon_{\chi\phi} = \begin{cases} dp^m & \text{if } \chi = \chi_0 \text{ and } \phi = \phi_0, \\ \frac{\phi(b)^{\tilde{m}}}{1-\phi(b)} p^m & \text{if } \chi = \chi_0 \text{ and } \phi \neq \phi_0, \\ (-1)^{m+1}\phi(b)^{\tilde{m}-1}(\chi(a)-1)^{m(p-1)} & \text{if } \chi \neq \chi_0. \end{cases}$$

Proof. By Proposition 4.1.4 the map $-f_4$ represents the local fundamental class. Following the recipe described in Section 2.2 we therefore consider the following diagram.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[dr] & & 0 & & \\
 & \ker f_4 \arrow[d, "i_1"] & & \ker \delta_1 \arrow[ur] \arrow[dr, "i_3"] \arrow[dl, dotted, "\sigma"'] & & & \\
0 \arrow[r] & X(2) \oplus \mathcal{F} \arrow[r, "i_2"] \arrow[d, bend right, "-f_4"'] & \mathcal{F}' \oplus \mathcal{F} \arrow[ur, bend left, "\delta_2"] \arrow[rr, "\delta_2"] & & \mathbb{Z}[G]z_0 \arrow[r, bend right, "\delta_1"'] & \mathbb{Z} \arrow[r] \arrow[l, dotted, bend right, "\mathcal{I}"'] & 0 \\
 & N(p+1) \arrow[u, dotted, "\rho"'] \arrow[d] & & & & & \\
 & 0 & & & & &
\end{tikzcd}$$

Here the dotted maps τ, σ, ρ denote G-equivariant splitting morphisms. They only exist after tensoring with $\mathbb{Q}$. Since we are only interested in the p-part of $E(\exp(\mathcal{L}))$ we tensor right away with $\mathbb{Q}_p$. In the following, if Y is a $\mathbb{Z}$-module, we set $Y_{\mathbb{Q}_p} := \mathbb{Q}_p \otimes_{\mathbb{Z}} Y$.

Explicitly, we define $\tau : \mathbb{Q}_p \to \mathbb{Q}_p[G]z_0$ by setting $\tau(1) = e_G z_0$. For the definition of σ we first note that $(\ker \delta_1)_{\mathbb{Q}_p}$ is generated by $(1 - e_G)z_0$ as a $\mathbb{Q}_p[G]$-module. It is easy to see that $\sigma((1 - e_G)z_0) := \frac{1-e_b}{b-1} e_a z_1 + \frac{1-e_a}{a-1} z_2$ determines a well defined splitting $\sigma : (\ker \delta_1)_{\mathbb{Q}_p} \to (\mathcal{F}' \oplus \mathcal{F})_{\mathbb{Q}_p}$. Here $\frac{1-e_b}{b-1}$ denotes the inverse of $b - 1$ on the $(1 - e_b)$-component of $\mathbb{Q}_p[b]$. Analogously we define $\frac{1-e_a}{a-1}$.

Finally, we also need to define $\rho : N(p + 1)_{\mathbb{Q}_p} \to (X(2) \oplus \mathcal{F})_{\mathbb{Q}_p}$. We have $N(p + 1)_{\mathbb{Q}_p} = \langle \theta_1 \rangle_{\mathbb{Q}_p} \simeq \mathbb{Q}_p$ because $U_N/U_N^{(p+1)}$ is torsion. We define $\rho(\theta_1) := -e_a T_b z_1$ and easily see that it defines a G-equivariant splitting of $-f_4$.

In the following all maps are morphisms of $\mathbb{Q}_p[G]$-modules. To simplify our notation this will not be apparent in the notation. The isomorphism $\tilde{\theta}$ of Section 2.2 specialized to our situation is now explicitly given by

$$\begin{aligned} \tilde{\theta} : (\ker f_4)_{\mathbb{Q}_p} \oplus \mathbb{Q}_p[G] &\xrightarrow{(\mathrm{id},(\tau,i_3)^{-1})} (\ker f_4)_{\mathbb{Q}_p} \oplus (\mathbb{Q}_p \oplus (\ker d_1)_{\mathbb{Q}_p}) \\ &\xrightarrow{(\mathrm{id},\nu_N^{-1},\mathrm{id})} (\ker f_4)_{\mathbb{Q}_p} \oplus N(p+1)_{\mathbb{Q}_p} \oplus (\ker d_1)_{\mathbb{Q}_p} \\ &\xrightarrow{(i_1,\rho,\mathrm{id})} (X(2) \oplus \mathcal{F})_{\mathbb{Q}_p} \oplus (\ker d_1)_{\mathbb{Q}_p} \\ &\xrightarrow{(i_2,\sigma)} \mathcal{F}'_{\mathbb{Q}_p} \oplus \mathcal{F}_{\mathbb{Q}_p}. \end{aligned}$$

We fix $\mathbb{Z}_p[G]$-basis of $\ker \hat{f}_4 \oplus \mathbb{Z}_p[G]$ and $\mathcal{F}'_p \oplus \mathcal{F}_p$, respectively. For $\ker \hat{f}_4 \oplus \mathbb{Z}_p[G]$ we take $(0, 1), (v_l, 0)$, $1 \le l \le pm + 1$, where v_l runs through the elements specified in Proposition 4.2.10. For $\mathcal{F}'_p \oplus \mathcal{F}_p$ we simply use the basis $z_1, z_2, \alpha_k w_j$, $1 \le k \le m, 0 \le j \le p - 1$. We now compute the matrix $A_{\tilde{\theta}}$ with respect to these bases. Following the definition of $\tilde{\theta}$ we get

$$\begin{aligned} \tilde{\theta} : (0,1) &\mapsto (0, 1, 1 - e_G) \\ &\mapsto (0, \theta_1, 1 - e_G) \\ &\mapsto (-e_a T_b z_1, 1 - e_G) \\ &\mapsto -e_a T_b z_1 + \frac{1 - e_b}{b - 1} e_a z_1 + \frac{1 - e_a}{a - 1} z_2. \end{aligned}$$

Writing the z_1-, z_2- and $\alpha_i w_j$-components of $\tilde{\theta}((0, 1))$ as a column vector we obtain

$$w = \begin{pmatrix} e_a \left(\frac{1-e_b}{b-1} - T_b\right) \\ \frac{1-e_a}{a-1} \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since $\tilde{\theta}|_{\ker \hat{f}_4} = i_2 \circ i_1$ is the inclusion, we obtain $A_{\tilde{\theta}} = (w, \mathfrak{M})$ which is the matrix whose columns are w and the columns of the matrix $\mathfrak{M}$ defined at the end of Section 4.2.

Case 1: $\chi = 1$ and $\phi = 1$.
Here $(\chi\phi)(A_{\tilde{\theta}})$ is of the form

$$\begin{pmatrix} -d & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & p & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \chi\phi(v) & 0 & p\tilde{I} & 0 & 0 & \cdots & 0 & 0 \\ 0 & * & 0 & 0 & -I & 0 & \cdots & 0 & 0 \\ 0 & * & 0 & 0 & * & -I & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & * & 0 & 0 & * & * & \cdots & -I & 0 \\ 0 & * & -e_2 & \chi\phi(\tilde{\mathcal{M}}) & * & * & \cdots & * & -I \end{pmatrix},$$

where we recall that the first component of the vector v is $b^{\tilde{m}}$. The determinant is $(-1)^{(p-1)m} dp^m = dp^m$.

Case 2: $\chi = 1$ and $\phi \neq 1$.
In this case $(\chi\phi)(A_{\tilde{\theta}})$ is of the form

$$\begin{pmatrix} \frac{1}{\phi(b)-1} & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1-\phi(b) & p & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \chi\phi(v) & 0 & p\tilde{I} & 0 & 0 & \cdots & 0 & 0 \\ 0 & * & 0 & 0 & -I & 0 & \cdots & 0 & 0 \\ 0 & * & 0 & 0 & * & -I & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & * & 0 & 0 & * & * & \cdots & -I & 0 \\ 0 & * & -e_2 & \chi\phi(\tilde{\mathcal{M}}) & * & * & \cdots & * & -I \end{pmatrix}.$$

The determinant is

$$-(-1)^{(p-1)m} \frac{\phi(b)^{\tilde{m}}}{\phi(b)-1} p^m = \frac{\phi(b)^{\tilde{m}}}{1-\phi(b)} p^m.$$

Case 3: $\chi \neq 1$ and any ϕ.
The matrix $(\chi\phi)(A_{\tilde{\theta}})$ is here given by

$$\begin{pmatrix} 0 & \chi(a)-1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ \frac{1}{\chi(a)-1} & 1-\phi(b) & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \chi\phi(v) & 0 & (\chi(a)-1)I & 0 & \cdots & 0 & 0 \\ 0 & * & 0 & -I & (\chi(a)-1)I & \cdots & 0 & 0 \\ 0 & * & 0 & * & -I & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & * & 0 & * & * & \cdots & -I & (\chi(a)-1)I \\ 0 & * & \chi\phi(\mathcal{M}) & * & * & \cdots & * & -I \end{pmatrix}.$$

Using Lemma 4.2.8 we compute for the determinant

$$-(-1)^{(p-1)m^2} \det(\chi\phi(\mathcal{M}))(\chi(a)-1)^{m(p-1)} = (-1)^{m+1}\phi(b)^{\tilde{m}-1}(\chi(a)-1)^{m(p-1)}.$$

This concludes the proof of Proposition 4.3.1. $\square$

5 The computation of $T_{N/K} - [\mathcal{L}, \rho_N, H_N]$

In this section we will compute a representative of $T_{N/K} - [\mathcal{L}, \rho_N, H_N]$ in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p^c) \simeq \mathbb{Q}_p^c[G]^\times / \mathbb{Z}_p[G]^\times$. The individual terms are described in Section 2.1.

5.1 Norm resolvents and Gauß sums

If L/K is a finite abelian extension of p-adic fields with Galois group H and $\beta \in L$ a normal basis element for L/K, i.e $L = K[H]\beta$, then we define the resolvent of β for every irreducible character χ of H by

$$(\beta \mid \chi) := \sum_{g \in H} g(\beta)\chi(g^{-1}).$$

The norm resolvent $\mathcal{N}_{K/\mathbb{Q}_p}(\beta \mid \chi)$ is defined by

$$\mathcal{N}_{K/\mathbb{Q}_p}(\beta \mid \chi) := \prod_{\omega} (\beta \mid \chi^{\omega^{-1}})^{\omega},$$

where ω runs through a (right) transversal of $\mathrm{Gal}(\mathbb{Q}_p^c/\mathbb{Q}_p)$ modulo $\mathrm{Gal}(\mathbb{Q}_p^c/K)$.

For later reference we state the following lemma which is well known and easy to prove.

Lemma 5.1.1. *a) Let $L_2 \supseteq L_1 \supseteq K$ be a tower of extensions of finite abelian p-adic fields. Let $\beta \in L_2$ be a normal basis element for L_2/K and let χ be an irreducible character of $\mathrm{Gal}(L_1/K)$. We write $\psi = \mathrm{inf}_{\mathrm{Gal}(L_1/K)}^{\mathrm{Gal}(L_2/K)}(\chi)$ for the inflation of χ. Then*

$$(\beta \mid \psi) = (\mathcal{T}_{L_2/L_1}(\beta) \mid \chi).$$

b) Let L_1/K and L_2/K be finite abelian extensions of p-adic fields such that $L_1 \cap L_2 = K$. Let β_1 and β_2 be normal basis elements for L_1 and L_2, respectively. We write each irreducible character χ of $\mathrm{Gal}(L_1L_2/K)$ in the form $\chi = \chi_1\chi_2$ with irreducible characters of $\mathrm{Gal}(L_1/K)$ and $\mathrm{Gal}(L_2/K)$. Then $\beta := \beta_1\beta_2$ is a normal basis element for L_1L_2/K and

$$(\beta \mid \chi) = (\beta_1 \mid \chi_1)(\beta_2 \mid \chi_2).$$

Proof. Easy verification. □

Given an extension L/K of local fields and an irreducible character ψ of $\mathrm{Gal}(L/K)$ we will use the short notation $\psi(\alpha)$ to denote $\psi((\alpha, L/K))$ where $(\alpha, L/K)$ is the Artin symbol for $\alpha \in K^\times$.

Lemma 5.1.2. *Let L/K be a finite abelian wildly and weakly ramified extension with group H. Suppose that $K/\mathbb{Q}_p$ is unramified. Let χ, ϕ denote irreducible characters of H and suppose that ϕ is unramified. Then*

$$\tau_K(\phi) = 1 \qquad \textit{and} \qquad \tau_K(\phi\chi) = \phi(p^{-2})\tau_K(\chi).$$

Proof. This is a simple reformulation of [15, Prop. 3.8]. If $K/\mathbb{Q}_p$ is an arbitrary finite extension, then we let $D_K = \pi_K^s \mathcal{O}_K$ denote the absolute different of $K/\mathbb{Q}_p$. Then $\tau_K(\phi) = \phi(\pi_K^{-s})$ by the definition of s and local Galois Gauß sums. If $K/\mathbb{Q}_p$ is unramified, then $s = 0$ and we obtain the first equality. The second equality is the last displayed equality in the proof of [15, Prop. 3.8] with $s = 0$ and $\pi_K = p$. □

Following the arguments of [15, bottom of page 1188] we apply Corollary 3.4 of loc.cit. with $\pi = p$. So there exist extensions $\tilde{M}$ and $\tilde{K}'$ such that $\tilde{M}/K$ is a weakly and wildly ramified extension of degree p, the extension $\tilde{K}'/K$ is unramified and such that we have a diagram of the form

$$\begin{tikzcd}
 & \tilde{N} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\tilde{M} \arrow[dr, dash] & N \arrow[d, dash] & \tilde{K}' \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Moreover we may assume that $\tilde{N}/N$ is unramified. By [14, V, Cor. (5.6)] p belongs to the norm group $\mathcal{N}_{\tilde{M}/K}(\tilde{M}^\times)$, so that we can apply [15, Th. 2].

Lemma 5.1.3. *There exist a normal basis generator $\alpha_{\tilde{M}}$ of the square root of the inverse different of $\tilde{M}/K$ and choices in the definitions of the norm resolvents such that for all irreducible characters $\tilde{\chi}$ of* $\mathrm{Gal}(\tilde{M}/K)$ *we have*

$$\frac{\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{\tilde{M}} \mid \tilde{\chi})}{\tau_K(\tilde{\chi})} = \begin{cases} 1, & \tilde{\chi} = \tilde{\chi}_0, \\ p^{-m}\tilde{\chi}(4), & \tilde{\chi} \neq \tilde{\chi}_0. \end{cases}$$

Proof. By [15, Th. 2] and using the notation of loc. cit. we may assume that

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{\tilde{M}}|\tilde{\chi})\tau_K^\star(\tilde{\chi} - \tilde{\chi}^2) = 1. \tag{16}$$

The proof of Lemma 5.1.3 now follows immediately from the definition of $\tau_K^\star$. In a little more detail, if $\tilde{\chi} = \tilde{\chi}_0$ is the trivial character, then $\tau_K^\star(\chi - \chi^2) = 1$ and also $\tau_K(\tilde{\chi}_0) = 1$. For $\tilde{\chi} \neq \tilde{\chi}_0$ we have

$$\tau_K^\star(\tilde{\chi} - \tilde{\chi}^2) = \tilde{\chi}\left(\frac{c_{\tilde{\chi}}}{4c_{K,2}}\right)\psi_K(c_{\tilde{\chi}}^{-1})^{-1},$$

by [15, Prop. 3.9]. Furthermore, $\tau_K(\tilde{\chi}) = p^m\tilde{\chi}(c_{\tilde{\chi}}^{-1})\psi_K(c_{\tilde{\chi}}^{-1})$, by the last displayed formula in the proof of [15, Prop. 3.9]. In our case we can choose $c_{K,2} = p^2$ and since p is in the norm group of $\tilde{M}/K$ we have $\tilde{\chi}(c_{K,2}) = 1$. Hence we obtain $\tau_K^\star(\tilde{\chi} - \tilde{\chi}^2) = p^m\tau_K(\tilde{\chi})^{-1}\tilde{\chi}(4)^{-1}$. The result now follows from (16). $\square$

We now fix $\alpha_{\tilde{M}}$ as in Lemma 5.1.3. Choose an integral normal basis element $\tilde{\theta}_2$ of $\tilde{K}'/K$ such that $\mathcal{T}_{\tilde{K}'/K}(\tilde{\theta}_2) = 1$ and set

$$\alpha_M := \mathcal{T}_{\tilde{N}/M}(\alpha_{\tilde{M}}\tilde{\theta}_2).$$

It is easy to verify that α_M is a $\mathcal{O}_K[G]$-generator of the square root of the inverse different of M/K.

Lemma 5.1.4. *Let χ be an irreducible character of* $\mathrm{Gal}(M/K)$. *Then*

$$\frac{\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M|\chi)}{\tau_K(\chi)} = \begin{cases} 1 & \text{if } \chi = \chi_0 \\ p^{-m}\chi(4) & \text{if } \chi \neq \chi_0. \end{cases}$$

Proof. We write inf for $\inf_{\mathrm{Gal}(M/K)}^{\mathrm{Gal}(\tilde{N}/K)}$. Since $\tilde{N}/M$ is unramified we see that for each irreducible character χ of $\mathrm{Gal}(M/K)$ we obtain $\inf(\chi) = \tilde{\chi}\tilde{\phi}_0$, where $\tilde{\phi}_0$ is the trivial character of $\mathrm{Gal}(\tilde{K}'/K)$ and $\tilde{\chi}$ is a uniquely determined irreducible character of $\mathrm{Gal}(\tilde{M}/K)$. Moreover, $\chi = \chi_0$ if and only if $\tilde{\chi} = \tilde{\chi}_0$.

By Lemma 5.1.1 we have

$$(\alpha_M \mid \chi) = (\alpha_{\tilde{M}}\tilde{\theta}_2 \mid \inf(\chi)) = (\alpha_{\tilde{M}} \mid \tilde{\chi})(\tilde{\theta}_2 \mid \tilde{\phi}_0) = (\alpha_{\tilde{M}} \mid \tilde{\chi})$$

because $(\tilde{\theta}_2 \mid \tilde{\phi}_0) = \mathcal{T}_{\tilde{K}'/K}\tilde{\theta}_2 = 1$. Recall that local Galois Gauß sums are invariant under inflation of characters (see e.g. [15, (5)] and [13, pp. 18 and 22]). We therefore get from $\inf(\chi) = \inf_{\mathrm{Gal}(\tilde{M}/K)}^{\mathrm{Gal}(\tilde{N}/K)}(\tilde{\chi})$

$$\frac{\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M|\chi)}{\tau_K(\chi)} = \frac{\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{\tilde{M}}\theta_2|\mathrm{inf}\chi)}{\tau_K(\mathrm{inf}\chi)} = \frac{\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{\tilde{M}}|\tilde{\chi})}{\tau_K(\tilde{\chi})}.$$

To conclude by Lemma 5.1.3 we notice that

$$\tilde{\chi}(4) = \inf_{\mathrm{Gal}(\tilde{M}/K)}^{\mathrm{Gal}(\tilde{N}/K)}(\tilde{\chi})((4|\tilde{N}/K)) = \inf_{\mathrm{Gal}(M/K)}^{\mathrm{Gal}(\tilde{N}/K)}(\chi)((4|\tilde{N}/K)) = \chi(4).$$

□

Proposition 5.1.5. *We assume the setting introduced in Section 2.1. Let $\psi = \chi\phi$ be a character of G. Then*

$$\frac{\mathcal{N}_{K/\mathbb{Q}_p}(p^2\alpha_M\theta_2|\chi\phi)}{\tau_K(\phi\chi)} = \begin{cases} p^{2m}\mathcal{N}_{K/\mathbb{Q}_p}(\theta_2|\phi) & \text{if } \chi = \chi_0 \\ p^m\chi(4)\mathcal{N}_{K/\mathbb{Q}_p}(\theta_2|\phi)\phi(p^2) & \text{if } \chi \neq \chi_0, \end{cases}$$

Proof. The result follows from Lemma 5.1.1, Lemma 5.1.2 and Lemma 5.1.4. □

5.2 A representative for $T_{N/K} - [\mathcal{L}, \rho_n, H_N]$

In the following proposition we describe a representative in $\mathbb{Q}_p^c[G]^\times$ for the element $T_{N/K} - [\mathcal{L}, \rho_n, H_N]$.

Proposition 5.2.1. *We assume the setting introduced in Section 2.1. For $\mathcal{L} = \mathfrak{p}_N^{p+1}$ the element $T_{N/K} - [\mathcal{L}, \rho_n, H_N]$ is represented by $\eta \in \mathbb{Q}_p^c[G]^\times$ where*

$$(\eta)_{\chi\phi} = \begin{cases} p^{-2m}\mathcal{N}_{K/\mathbb{Q}_p}(\theta_2|\phi)^{-1}\delta_K^{-1} & \text{if } \chi = \chi_0 \\ p^{-m}\chi(4)^{-1}\mathcal{N}_{K/\mathbb{Q}_p}(\theta_2|\phi)^{-1}\phi(b)^2\delta_K^{-1} & \text{if } \chi \neq \chi_0, \end{cases}$$

where δ_K is a square root of the discriminant of K.

Proof. Recall that $\mathcal{L} = \mathcal{O}_K[G](p^2\alpha_M\theta_2)$. As already explained in Section 2.1 the element $[\mathcal{L}, \rho_n, H_N]$ is then represented by $\left((\delta_K\mathcal{N}_{K/\mathbb{Q}_p}(p^2\alpha_M\theta_2 \mid \chi\phi)\right)_{\chi,\phi}$.

By definition the term $T_{N/K}$ is represented by $\left(\tau_{\mathbb{Q}_p}(i_K^{\mathbb{Q}_p}(\chi\phi)\right)_{\chi,\phi}$. Since Gauß sums are inductive in degree zero and $\tau_K(\phi) = 1$ for unramified characters by Lemma 5.1.2 we have

$$\tau_{\mathbb{Q}_p}(i_K^{\mathbb{Q}_p}\chi\phi) = \tau_{\mathbb{Q}_p}(i_K^{\mathbb{Q}_p}(\chi\phi - \chi_0\phi_0))\tau_{\mathbb{Q}_p}(i_K^{\mathbb{Q}_p}(\chi_0\phi_0) = \tau_K(\chi\phi)\tau_{\mathbb{Q}_p}(i_K^{\mathbb{Q}_p}\chi_0\phi_0).$$

Since $K/\mathbb{Q}_p$ is unramified, $i_K^{\mathbb{Q}_p}(\chi_0\phi_0)$ is a sum of unramified characters so that $\tau_{\mathbb{Q}_p}(i_K^{\mathbb{Q}_p}\chi_0\phi_0) = 1$ and we obtain $\tau_{\mathbb{Q}_p}(i_K^{\mathbb{Q}_p}\chi\phi) = \tau_K(\chi\phi)$. Furthermore, $\phi(p^2) = \phi((p^2, K'/K)) = \phi(F^2) = \phi(b)^{-2}$ by [16, XIII, §4, Prop. 13] and the definition of b. Combining these observations with Proposition 5.1.5 concludes the proof of the proposition. □

6 Proof of Theorem 1

In our setting the correction term $M_{N/K}$ is explicitly given by

$$M_{N/K} = \frac{{}^*(de_G)\,{}^*((1-b^{-1}q^{-1})e_I)}{{}^*((1-b)e_I)}.$$

It is represented by $m = m_{N/K}$ where

$$m_{\chi\phi} = \begin{cases} d(1-q^{-1}) & \text{if } \chi = \chi_0 \text{ and } \phi = \phi_0 \\ \frac{1-\phi(b)^{-1}q^{-1}}{1-\phi(b)} & \text{if } \chi = \chi_0 \text{ and } \phi \neq \phi_0 \\ 1 & \text{if } \chi \neq \chi_0. \end{cases}$$

As explained in Section 2.3 we must show that a representative of $T_{N/K} + C_{N/K} - M_{N/K}$ lies in $\mathcal{O}_p^t[G]^\times$.

Combining the results of the previous sections we see that $T_{N/K} + C_{N/K} - M_{N/K}$ is represented by an element $\omega \in \mathbb{Q}_p^c[G]^\times$ where $\omega = \varepsilon\eta/m$. Let $W_{\theta_2} \in \mathcal{O}_p^t[G]$ be such that $\chi\phi(W_{\theta_2}) = \mathcal{N}_{K/\mathbb{Q}_p}(\theta_2|\phi)\delta_K$. Then

$$\begin{aligned}
\omega_{\chi\phi} &= \begin{cases} \frac{dp^m}{p^{2m}d(1-q^{-1})} \cdot \frac{1}{\chi\phi(W_{\theta_2})} & \text{if } \chi = \chi_0 \text{ and } \phi = \phi_0 \\ \frac{\phi(b)^{\tilde{m}}p^m(1-\phi(b))}{(1-\phi(b))p^{2m}(1-\phi(b)^{-1}q^{-1})} \cdot \frac{1}{\chi\phi(W_{\theta_2})} & \text{if } \chi = \chi_0 \text{ and } \phi \neq \phi_0 \\ \frac{(-1)^{m+1}\phi(b)^{\tilde{m}-1}(\chi(a)-1)^{m(p-1)}}{p^m\chi(4)\phi(b)^{-2}} \cdot \frac{1}{\chi\phi(W_{\theta_2})} & \text{if } \chi \neq \chi_0 \end{cases} \\
&= \begin{cases} \frac{1}{p^m-1} \cdot \frac{1}{\chi\phi(W_{\theta_2})} & \text{if } \chi = \chi_0 \text{ and } \phi = \phi_0 \\ \frac{\phi(b)^{\tilde{m}+1}}{\phi(b)p^m-1} \cdot \frac{1}{\chi\phi(W_{\theta_2})} & \text{if } \chi = \chi_0 \text{ and } \phi \neq \phi_0 \\ (-1)^{m+1}\frac{\phi(b)^{\tilde{m}+1}}{\chi(4)} \cdot \left(\frac{(\chi(a)-1)^{p-1}}{p}\right)^m \cdot \frac{1}{\chi\phi(W_{\theta_2})} & \text{if } \chi \neq \chi_0 \end{cases} \\
&= \begin{cases} \frac{\phi(b)^{\tilde{m}+1}}{\phi(b)p^m-1} \cdot \frac{1}{\chi\phi(W_{\theta_2})} & \text{if } \chi = \chi_0 \\ (-1)^{m+1}\frac{\phi(b)^{\tilde{m}+1}}{\chi(4)} \cdot \left(\frac{(\chi(a)-1)^{p-1}}{p}\right)^m \cdot \frac{1}{\chi\phi(W_{\theta_2})} & \text{if } \chi \neq \chi_0. \end{cases}
\end{aligned}$$

We can easily write ω as an element of $\mathbb{Q}_p^c[G]^\times$,

$$\omega = \frac{1}{W_{\theta_2}}\left(\frac{b^{\tilde{m}+1}}{bq-1}e_a + (-1)^{m+1}b^{\tilde{m}+1}\sigma_4^{-1}\left(\frac{(a-1)^{p-1}}{p}\right)^m(1-e_a)\right),$$

where $\sigma_4 = (4, M/K) \in \mathrm{Gal}(M/K) = \langle a\rangle \subseteq G$. We have to prove that $\omega \in \mathcal{O}_p^t[G]^\times$.

Since $K/\mathbb{Q}_p$ is unramified, we know that δ_K is a unit in $\mathcal{O}_p^t[G]^\times$. Then by [10, Sec. I, Prop. 4.3] the same is true for W_{θ_2}. Since also $bq-1$ is clearly a unit, we can study $\tilde{\omega} = W_{\theta_2}(bq-1)\omega$ instead of ω. We have

$$\tilde{\omega} = b^{\tilde{m}+1}e_a - b^{\tilde{m}+1}\sigma_4^{-1}\left(-\frac{(a-1)^{p-1}}{p}\right)^m(bq-1)(1-e_a).$$

We first show that $\tilde{\omega}$ is contained in $\mathcal{O}_p^t[G]$. To that end it is enough to show that the coefficient of b^j for all j is contained in $\mathcal{O}_p^t[a]$. The only non-zero coefficients are those of $b^{\tilde{m}+1}$ and $b^{\tilde{m}+2}$ which are, respectively,

$$e_a + \sigma_4^{-1}\left(-\frac{(a-1)^{p-1}}{p}\right)^m(1-e_a).$$

and

$$-\sigma_4^{-1}\left(-\frac{(a-1)^{p-1}}{p}\right)^m q(1-e_a).$$

The second one has clearly coefficients in $\mathbb{Z}_p$. As for the first one, its integrality is equivalent to

$$1 \equiv \chi(\sigma_4)^{-1}\left(-\frac{(\chi(a)-1)^{p-1}}{p}\right)^m \pmod{1-\zeta_p},$$

for any non-trivial character χ, which follows from $\frac{(\chi(a)-1)^{p-1}}{p} \equiv -1 \pmod{1-\zeta_p}$.

We have now shown that $\omega \in \mathcal{O}_p^t[G]$. By [3, Cor. 3.8] ω is actually a unit in $\mathcal{M}^t$ where $\mathcal{M}^t$ denotes the maximal order in $\mathbb{Q}_p^t[G]$. Here $\mathbb{Q}_p^t = \mathrm{Quot}(\mathcal{O}_p^t)$ denotes the maximal tamely ramified extension of $\mathbb{Q}_p$. It follows that $\omega \in (\mathcal{M}^t)^\times \cap \mathcal{O}_p^t[G] = \mathcal{O}_p^t[G]^\times$.

References

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

[2] W. Bley and R. Debeerst. Algorithmic proof of the epsilon constant conjecture. *Math. Comp.*, 82(284):2363–2387, 2013.

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

[4] M. Breuning. On equivariant global epsilon constants for certain dihedral extensions. *Math. Comp.*, 73(246):881–898 (electronic), 2004.

[5] M. Breuning and D. Burns. Leading terms of Artin L-functions at $s = 0$ and $s = 1$. *Compos. Math.*, 143(6):1427–1464, 2007.

[6] M. Breuning and D. Burns. On equivariant Dedekind zeta-functions at $s = 1$. *Doc. Math.*, (Extra volume: Andrei A. Suslin sixtieth birthday):119–146, 2010.

[7] D. Burns. Equivariant Tamagawa numbers and Galois module theory. I. *Compositio Math.*, 129(2):203–237, 2001.

[8] D. Burns and M. Flach. On Galois structure invariants associated to Tate motives. *Amer. J. Math.*, 120(6):1343–1397, 1998.

[9] T. Chinburg. Exact sequences and Galois module structure. *Ann. of Math. (2)*, 121(2):351–376, 1985.

[10] A. Fröhlich. *Galois module structure of algebraic integers*, volume 1 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1983.

[11] K. W. Gruenberg, J. Ritter, and A. Weiss. A local approach to Chinburg's root number conjecture. *Proc. London Math. Soc. (3)*, 79(1):47–80, 1999.

[12] B. Köck. Galois structure of Zariski cohomology for weakly ramified covers of curves. *Amer. J. Math.*, 126(5):1085–1107, 2004.

[13] 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.

[14] J. Neukirch. *Algebraic number theory. (Algebraische Zahlentheorie.)*. Berlin etc.: Springer-Verlag, 1992.

[15] E. J. Pickett and S. Vinatier. Self-dual integral normal bases and Galois module structure. *Compos. Math.*, 149(7):1175–1202, 2013.

[16] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.