COMPOSITIO MATHEMATICA

Self-dual integral normal bases and Galois module structure

Erik Jarl Pickett and Stéphane Vinatier

Compositio Math. **149** (2013), 1175–1202.

doi:10.1112/S0010437X12000851

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY

Compositio Math. 149 (2013) 1175–1202
doi:10.1112/S0010437X12000851

Self-dual integral normal bases and Galois module structure

Erik Jarl Pickett and Stéphane Vinatier

Abstract

Let N/F be an odd-degree Galois extension of number fields with Galois group G and rings of integers $\mathfrak{O}_N$ and $\mathfrak{O}_F = \mathfrak{O}$. Let $\mathcal{A}$ be the unique fractional $\mathfrak{O}_N$-ideal with square equal to the inverse different of N/F. B. Erez showed that $\mathcal{A}$ is a locally free $\mathfrak{O}[G]$-module if and only if N/F is a so-called weakly ramified extension. Although a number of results have been proved regarding the freeness of $\mathcal{A}$ as a $\mathbb{Z}[G]$-module, the question remains open. In this paper we prove that $\mathcal{A}$ is free as a $\mathbb{Z}[G]$-module provided that N/F is weakly ramified and under the hypothesis that for every prime $\wp$ of $\mathfrak{O}$ which ramifies wildly in N/F, the decomposition group is abelian, the ramification group is cyclic and $\wp$ is unramified in $F/\mathbb{Q}$. We make crucial use of a construction due to the first author which uses Dwork's exponential power series to describe self-dual integral normal bases in Lubin–Tate extensions of local fields. This yields a new and striking relationship between the local norm-resolvent and the Galois Gauss sum involved. Our results generalise work of the second author concerning the case of base field $\mathbb{Q}$.

1. Introduction

Let N/F denote an odd-degree Galois extension of number fields. By Hilbert's formula for the valuation of the different $\mathfrak{D}$ of N/F, there exists a fractional ideal $\mathcal{A}$ $(= \mathcal{A}_{N/F})$ of the ring of integers $\mathfrak{O}$ $(= \mathfrak{O}_F)$ of F such that

$$\mathcal{A}^2 = \mathfrak{D}^{-1}.$$

This ideal is known as the *square root of the inverse different*. It is an ambiguous ideal, in the sense that it is stable under the action of the Galois group G of N/F and is hence an $\mathfrak{O}[G]$-module. B. Erez has shown $\mathcal{A}$ to be locally free if and only if N/F is weakly ramified, i.e. if the second ramification group of any prime ideal $\mathfrak{p}$ of $\mathfrak{O}_N$ is trivial. The study of $\mathcal{A}$ as an $\mathfrak{O}[G]$-module has too many obstructions to be dealt with (in particular, $\mathfrak{O}$ may not be principal); so following the work of Fröhlich, Taylor and others (for the Galois module structure of the ring of integers in a tame extension), we consider the structure of $\mathcal{A}$ as a $\mathbb{Z}[G]$-module.

In [Ere91] it was proved that if N/F is tamely ramified, then $\mathcal{A}$ is always free over $\mathbb{Z}[G]$. The question of whether $\mathcal{A}$ is free as a $\mathbb{Z}[G]$-module when N/F is wildly but weakly ramified is still open. In this paper we prove the following global result.

Theorem 1. *Let N/F denote an odd-degree weakly ramified Galois extension of number fields, and suppose that for any wildly ramified prime $\mathfrak{p}$ of $\mathfrak{O}_N$, the decomposition group is abelian, the*

Received 1 June 2010, accepted in final form 7 November 2012, published online 10 May 2013.
2010 Mathematics Subject Classification 11R04, 11R33, 11S31 (primary), 11R20, 11R29, 11R32, 11S15, 11S20, 11S80 (secondary).
Keywords: Galois module, square root of the inverse different, weakly ramified extensions, Dwork's power series, self-dual integral normal basis, Galois Gauss sum.

ramification group is cyclic and the localised extension $F_\wp/\mathbb{Q}_p$ is unramified, where $\wp = \mathfrak{p} \cap F$ and $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. Then $\mathcal{A}$ is a free $\mathbb{Z}[G]$-module.

This result generalises [Vin01, théorème 1.2], which is the natural analogue in the absolute case where $F = \mathbb{Q}$. In that case, ramification groups at wildly ramified places are always cyclic of prime order. In the relative case, we will see that the abelian decomposition group assumption yields that the ramification group is p-elementary abelian at a wildly ramified place above a rational prime p. Therefore, our hypothesis about ramification groups at wildly ramified places in fact mimics the situation in the absolute case.

As in Taylor's celebrated theorem for rings of integers in tame extensions of number fields [Tay81, Theorem 1], our result reveals a deep connection between two kinds of invariants of the extension N/F: the Galois Gauss sum, of analytic nature, that emerges in the constant of the functional equation of the Artin L-function of F, and the norm-resolvents attached to semi-local normal basis generators of $\mathcal{A}$, which are entirely of algebraic nature *a priori*.

Generalisation of the link between these objects to the relative situation has been made possible by the exhibition in [Pic09] of explicit normal basis generators for cyclic weakly ramified extensions of an unramified extension of $\mathbb{Q}_p$. These generators are constructed using values of Dwork's p-adic exponential power series at certain units and have very nice properties; in particular, they are self-dual with respect to the trace form. Of course, the norm-resolvents we attach to them can no longer be thought of as completely algebraic in nature.

Dwork originally introduced his power series in the context of p-adic differential operators, when considering the zeta function of a hypersurface [Dwo64]. In this paper, we demonstrate that Dwork's power series is extremely useful when considering Galois module structure in extensions of both local and number fields. We hope that this work will lead to further investigation of the connections between these two subject areas.

The core of this paper is § 4, where we use the rich properties of Pickett's basis generators to compute the product of a norm-resolvent and a modified twisted Galois Gauss sum in local cyclic wildly and weakly ramified extensions. We obtain the following local result (the objects will be defined below).

Theorem 2. *Let $p \neq 2$ be a rational prime, K an unramified finite extension of $\mathbb{Q}_p$, and M a cyclic wildly and weakly ramified extension of K such that p belongs to the norm group of M/K. There exist a normal basis generator α_M of the square root of the inverse different of M/K and choices in the definitions of the norm-resolvent $\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid .\,)$ and of the modified Galois Gauss sum $\tau_K^\star$ such that, for any character χ of $\mathrm{Gal}(M/K)$,*

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi)\tau_K^\star(\chi - \psi_2(\chi)) = 1,$$

where ψ_2 is the second Adams operator.

Before proving this result in § 4, we introduce the technical tools for our study in § 2. Then, in § 3, we give some preliminary results and explain how to reduce the proof of Theorem 1 to that of Theorem 2.

We hope to deal with the general relative abelian case in a future publication, but we have no explicit description of a normal basis generator which lends itself so well to calculations of the type used in this paper; see [Pic09, Remark 13(2)] and [Pic10, Introduction]. We are therefore not able to generalise the explicit computations of § 4 at this stage.

Throughout this paper, N/F is an odd-degree weakly ramified extension of number fields with Galois group G.

2. Strategy

In this section, we first explain briefly how Fröhlich's Hom-description translates the problem of showing that $\mathcal{A}$ is a free $\mathbb{Z}[G]$-module into the study of an equivariant morphism on the group of virtual characters of G, with idelic values. For each rational prime p, the local components above p of this morphism decompose as a product of factors indexed by the prime ideals of $\mathfrak{O}$. We recall from the literature the properties of these factors that we need, except for those of the $\wp$-factors of the p-component when $\wp \mid p$ is wildly ramified in N/F, which will be dealt with in §§ 3 and 4.

First, we fix some notation for the paper.

Notation 2.1. Let $\mathbb{Q}^c$ denote the algebraic closure in the field of complex numbers of the field $\mathbb{Q}$ of rational numbers; for any rational prime p, we fix an algebraic closure $\mathbb{Q}_p^c$ of the field of p-adic numbers $\mathbb{Q}_p$. Any number field (respectively, finite extension of $\mathbb{Q}_p$) L that we consider is assumed to be contained in $\mathbb{Q}^c$ (respectively, $\mathbb{Q}_p^c$), and we set $\Omega_L = \mathrm{Gal}(\mathbb{Q}^c/L)$ (respectively, $\Omega_L = \mathrm{Gal}(\mathbb{Q}_p^c/L)$). We let L^{ab} be the maximal abelian extension of L in $\mathbb{Q}^c$ (respectively, $\mathbb{Q}_p^c$) and write $\mathrm{Gal}(L^{\mathrm{ab}}/L)$ as Ω_L^{ab}.

When L is a number field, we denote by $\mathfrak{O}_L$ its ring of integers; if $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_L$, we denote by $L_{\mathfrak{p}}$ the completion (also called the 'localisation') of L at $\mathfrak{p}$. When L is a finite extension of $\mathbb{Q}_p$, we denote by $\mathfrak{O}_L$ the valuation ring of L and by θ_L the Artin reciprocity map $L^\times \to \Omega_L^{\mathrm{ab}}$.

2.1 The class group

To prove Theorem 1 we use the classic strategy developed by Fröhlich. We associate to the $\mathbb{Z}[G]$-module $\mathcal{A}$ its class $(\mathcal{A})$ in the class group of locally free $\mathbb{Z}[G]$-modules $\mathrm{Cl}(\mathbb{Z}[G])$. Since the order of G is odd, triviality of the class $(\mathcal{A})$ is equivalent to $\mathcal{A}$ being free as a $\mathbb{Z}[G]$-module, which is our goal. Fröhlich's Hom-description of $\mathrm{Cl}(\mathbb{Z}[G])$ reads as follows:

$$\mathrm{Cl}(\mathbb{Z}[G]) \cong \frac{\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J(E))}{\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, E^\times)\,\mathrm{Det}(\mathcal{U}(\mathbb{Z}[G]))}.$$

Here R_G is the additive group of virtual characters of G with values in $\mathbb{Q}^c$, E is a 'big enough' number field (in particular, E is Galois over $\mathbb{Q}$ and contains N and the values of the elements of R_G) and $J(E)$ is its idèle group. The homomorphisms in $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J(E))$ are those which commute with the natural actions of $\Omega_{\mathbb{Q}}$ on R_G and $J(E)$. The group $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, E^\times)$ embeds in the former one through the diagonal embedding of $E^\times$ in $J(E)$, and $\mathcal{U}(\mathbb{Z}[G]) = \mathbb{R}[G]^\times \times \prod_l \mathbb{Z}_l[G]^\times$ with l running over all rational primes. We now briefly define the Det morphism, as well as local and semi-local resolvents and norm-resolvents. For a more complete account of Fröhlich's Hom-description, see [Frö83].

2.2 Determinants and resolvents

Let B/A be a finite Galois extension of number fields, let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_B$, and set $\wp = \mathfrak{p} \cap A$. In the following, the symbols K, L, H, $\mathbb{Q}_*$ and R may have two different meanings corresponding, respectively, to the semi-local and local situations:

K	L	H	$\mathbb{Q}_*$	R
A	$B \otimes_A A_\wp$	$\mathrm{Gal}(B/A)$	$\mathbb{Q}$	R_H
$A_\wp$	$B_{\mathfrak{p}}$	$\mathrm{Gal}(B_{\mathfrak{p}}/A_\wp)$	$\mathbb{Q}_p$	$R_{H,p}$

In the table, we have denoted by $R_{H,p}$ the group of virtual characters of H with values in $\mathbb{Q}_p^c$. Let χ be the character of an irreducible matrix representation Θ of H, and let $x = \sum_{h\in H} x_h h \in L[H]$; then

$$\mathrm{Det}_\chi(x) = \det\Big(\sum_{h\in H} x_h \Theta(h)\Big),$$

where det stands for the matrix determinant. Extending this formula by linearity to any $\chi \in R$ yields the morphism

$$\mathrm{Det} : L[H]^\times \longrightarrow \mathrm{Hom}(R, (\mathbb{Q}_*^c)^\times).$$

The restriction of Det_χ to H yields an abelian character of H which we denote by $\det_\chi$. It can be extended to Ω_K by letting $\det_\chi(\omega) = \det_\chi(\omega\,|_L)$ for any $\omega \in \Omega_K$.

In order to find a representative character function of the image of $(\mathcal{A})$ under the Hom-description of $\mathrm{Cl}(\mathbb{Z}[G])$, one needs to consider resolvents and norm-resolvents.

Definition 2.2. Let $\alpha \in L$ and $\chi \in R$. The resolvent and norm-resolvent of α at χ with respect to L/K are defined, respectively, as

$$(\alpha \mid \chi) = (\alpha \mid \chi)_H = \mathrm{Det}_\chi\Big(\sum_{h\in H} \alpha^h h^{-1}\Big), \quad \mathcal{N}_{K/\mathbb{Q}_*}(\alpha \mid \chi) = \prod_{\omega\in\Omega} (\alpha \mid \chi^{\omega^{-1}})^\omega,$$

where the product is over a (right) transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_*}$.

Notice that the norm-resolvent depends on the choice of the right transversal Ω. In view of [Frö83, Proposition I.4.4(ii)], changing Ω multiplies the norm-resolvent by $\det_\chi(h)$ for some $h \in H$, i.e. by an element in the denominator of the Hom-description. It follows that when using norm-resolvents to describe a representative function for $(\mathcal{A})$, we may choose Ω freely. When $K/\mathbb{Q}_p$ is Galois (in the local context), restriction of $\mathbb{Q}_p$-automorphisms to K maps any such Ω onto $\mathrm{Gal}(K/\mathbb{Q}_p)$. When H is abelian, the formulas simplify to

$$(\alpha \mid \chi) = \sum_{h\in H} \alpha^h \chi(h^{-1}), \quad \mathcal{N}_{K/\mathbb{Q}_*}(\alpha \mid \chi) = \prod_{\omega\in\Omega}\Big(\sum_{h\in H} \alpha^{h\omega}\chi(h^{-1})\Big).$$

2.3 A representative for $(\mathcal{A})$

We now describe a representative f of $(\mathcal{A})$ in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$. Such a representative is not unique, since it can be modified by multiplication by any element in the denominator of the Hom-description. Indeed, we construct f by slightly modifying Erez's representative $v_{N/F}$ (see [Ere91, Theorem 3.6]) to enable more precise computations at wildly ramified places, the goal being to show that f itself lies in the denominator of the Hom-description.

We define the representative morphism f of $(\mathcal{A})$ by giving for each rational prime p its semi-local component f_p taking values in $J_p(E) = \prod_{\mathcal{P}|p} E_\mathcal{P}^\times$, where the product is over the prime ideals of $\mathfrak{O}_E$ above p. This group embeds in $J(E)$ as the subgroup consisting of the idèles $(y_\mathcal{P})_\mathcal{P} \in J(E)$ such that $y_\mathcal{P} = 1$ if $\mathcal{P}$ is a prime ideal of $\mathfrak{O}_E$ that does not divide p. It decomposes into the cartesian product $J_p(E) = \prod_{\wp|p} J_\wp(E)$, where the product is over the prime ideals $\wp$ of $\mathfrak{O}$ above p and $J_\wp(E) = \prod_{\mathcal{P}|\wp} E_\mathcal{P}^\times$. Note that, with similar definitions at a lower level, $J_\wp(F) = F_\wp^\times$ diagonally embeds into $J_\wp(E)$ and $J_\wp(N)$ embeds into $J_\wp(E)$ via the map $(x_\mathfrak{p})_{\mathfrak{p}|\wp} \mapsto (y_\mathcal{P})_{\mathcal{P}|\wp}$, such that $y_\mathcal{P} = x_\mathfrak{p}$ if $\mathcal{P}|\mathfrak{p}$.

Furthermore, $J_\wp(E)$ is isomorphic to $(E \otimes_F F_\wp)^\times$ via the isomorphism

$$\mathcal{I}_\wp = \prod_\iota (\iota \otimes 1) : (E \otimes_F F_\wp)^\times \xrightarrow{\sim} J_\wp(E)$$

built on the various embeddings ι of E in $\mathbb{Q}_p^c$ that fix $\wp$. These embeddings are in one-to-one correspondence with the prime ideals of $\mathfrak{O}_E$ above $\wp$. In the following we may not always distinguish between $J_\wp(E)$ and $(E \otimes_F F_\wp)^\times$.

First, consider the case where p is a rational prime that does not divide the order of G. Under this assumption, $\mathbb{Z}_p[G]$ is a maximal order in $\mathbb{Q}_p[G]$, which, by [Frö83, Proposition I.2.2], implies that

$$\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, \mathcal{U}_p(E)) = \mathrm{Det}(\mathbb{Z}_p[G]^\times)$$

where $\mathcal{U}_p(E) = \prod_{\mathcal{P}|p} \mathfrak{O}_{E_\mathcal{P}}^\times$. On the other hand, Erez has shown that his representative $v_{N/F}$ takes values in $\mathcal{U}(E) = \prod_\mathcal{P} \mathfrak{O}_{E_\mathcal{P}}^\times$ (see [Ere91, Theorem 2′]). It follows that $(v_{N/F})_p$ belongs to the p-component of the denominator of the Hom-description, and hence we may set $f_p = 1$. Similar arguments show that we may also set $f_\infty = 1$, where ∞ stands for the Archimedean place of $\mathbb{Q}$.

From now on, we suppose that p is a rational prime dividing the order of G. The p-component f_p of our representative f is essentially made up of two ingredients: the global Galois Gauss sum of F and norm-resolvents associated to semi-local generators of $\mathcal{A}$.

2.3.1 *Norm-resolvents.* We begin with the latter ingredient. Since N/F is weakly ramified, we know by Erez's criterion [Ere91, Theorem 1] that the square root of the inverse different $\mathcal{A}$ is locally free. Specifically, for each prime ideal $\wp$ of $\mathfrak{O}$ above p, there exists $\beta_\wp \in N \otimes_F F_\wp$ such that $\mathcal{A} \otimes_\mathfrak{O} \mathfrak{O}_{F_\wp} = \mathfrak{O}_{F_\wp}[G]\beta_\wp$. The semi-local resolvent $(\beta_\wp \mid \chi)$, for $\chi \in R_G$, takes values in $(E \otimes_F F_\wp)^\times$, identified with $J_\wp(E)$ through the isomorphism $\mathcal{I}_\wp$, and then embedded in $J(E)$. The norm-resolvent is then obtained as

$$\mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \mid \chi) = \prod_{\omega \in \Omega} (\beta_\wp \mid \chi^{\omega^{-1}})^\omega,$$

where the product is over a (right) transversal Ω of Ω_F in $\Omega_\mathbb{Q}$. The action of Ω on $J(E)$ permutes the semi-local subgroups $J_\wp(E)$ corresponding to prime ideals $\wp$ of $\mathfrak{O}$ above p; hence the norm-resolvent $\mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \mid \chi)$ takes values in $J_p(E)$. If $\mathcal{Q}$ is any prime ideal of $\mathfrak{O}_E$ above p, we denote by $\mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \mid \chi)_\mathcal{Q}$ its component in $E_\mathcal{Q}^\times$. Accordingly, we denote by β_p the idèle in $J_p(N)$ whose components in the subgroups $J_\wp(N)$, where $\wp$ is above p, are the $\beta_\wp$ introduced above. The norm-resolvent $\mathcal{N}_{F/\mathbb{Q}}(\beta_p \mid \chi)$ belongs to $J_p(E) = \prod_{\mathcal{Q}|p} E_\mathcal{Q}^\times$, with $\mathcal{Q}$-component

$$\mathcal{N}_{F/\mathbb{Q}}(\beta_p \mid \chi)_\mathcal{Q} = \prod_{\wp|p} \mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \mid \chi)_\mathcal{Q}.$$

2.3.2 *Galois Gauss sums.* We now turn to the global Galois Gauss sum, which is a product of local ones. For each prime ideal ℓ of $\mathfrak{O}$, we fix a prime ideal $\mathcal{L}$ of E above ℓ and set $\mathfrak{l} = \mathcal{L} \cap N$ and $l\mathbb{Z} = \mathcal{L} \cap \mathbb{Q}$. Recall the one-to-one correspondence between prime ideals of $\mathfrak{O}_E$ above ℓ and embeddings of E into $\mathbb{Q}_l^c$ that fix ℓ, and let $\iota_{\mathcal{L}/\ell}$ denote the embedding associated to $\mathcal{L}$. It induces an isomorphism between the Galois group of the local extension $N_\mathfrak{l}/F_\ell$ and the decomposition group $G(\ell)$ of $\mathcal{L}/\ell$, sending $\gamma \in \mathrm{Gal}(N_\mathfrak{l}/F_\ell)$ to $\iota_{\mathcal{L}/\ell}\gamma\iota_{\mathcal{L}/\ell}^{-1} \in \mathrm{Gal}(N/F)$ (the action on elements is written exponentially and thus to the right; see [Frö83, III, (2.7)]). We may thus identify $G(\ell)$ and $\mathrm{Gal}(N_\mathfrak{l}/F_\ell)$ in the following.

In § 3.2 we define the local Galois Gauss sum $\tau_{F_\ell}(\chi)$ when $\chi \in R_{G(\ell)}$ is abelian and at most weakly ramified; for a general definition of the Galois Gauss sum see, for instance, [Frö83, I.5]. We also recall how this Galois Gauss sum is modified at (at most) tamely ramified places, and

present an analogous modification at wildly and weakly ramified places. In both cases we denote[1] the resulting character function by $\tau^\star_{F_\ell}$. Following Erez [Ere91, § 3], we finally twist our modified Galois Gauss sum using the action of the second Adams operator ψ_2, and get

$$T^\star_\ell(\chi) = \tau^\star_{F_\ell}(\chi - \psi_2(\chi)).$$

Set $\widetilde{T}^\star_\ell = \mathrm{Ind}^G_{G(\ell)} T^\star_\ell$; that is, by the definition of induction on character functions,

$$\widetilde{T}^\star_\ell(\chi) = T^\star_\ell(\chi_\ell) = \tau^\star_{F_\ell}(\chi_\ell - \psi_2(\chi_\ell)),$$

where for $\chi \in R_G$ we denote by χ_ℓ the restriction of χ to $G(\ell)$.

We now have for each prime ideal ℓ of $\mathfrak{O}$ a function $\widetilde{T}^\star_\ell$ on virtual characters of G; we shall see in § 3.2.3 that it is in fact almost always trivial: (7) shows that $\widetilde{T}^\star_\ell = 1$ whenever ℓ is unramified in N/F. Let S_T and S_W be the sets of prime ideals of $\mathfrak{O}$ that are, respectively, tamely and wildly ramified in N/F; their union S contains all the prime ideals ℓ of $\mathfrak{O}$ such that $\widetilde{T}^\star_\ell$ is non-trivial, and we define the global twisted modified Galois Gauss sum associated to F as

$$T^\star = \prod_{\ell \in S} \widetilde{T}^\star_\ell \in \mathrm{Hom}(R_G, E^\times).$$

It takes values in $E^\times$, which diagonally embeds into $J(E)$ and hence into each $J_p(E)$.

2.3.3 *All together.* We will prove the following result in § 3.2.3.

Proposition 2.3. *For any rational prime p and $\chi \in R_G$, set*

$$f_p(\chi) = T^\star(\chi)\mathcal{N}_{F/\mathbb{Q}}(\beta_p \mid \chi) = T^\star(\chi) \prod_{\wp \mid p} \mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \mid \chi)$$

if p divides the order of G, and $f_p(\chi) = 1$ otherwise; furthermore, set $f_\infty = 1$. Then $f = (f_p)_p$ is a representative of $(\mathcal{A})$ in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$.

2.4 Localising and cutting into pieces

We fix a rational prime p dividing the order of G. The $\Omega_\mathbb{Q}$-equivariant component f_p of our representative takes semi-local values. We first transform it into a character function with local values, and then split it into factors that will be dealt with separately.

We use the localisation procedure described in [Frö83, II.2 and III.2]. Let $\mathcal{Q}$ be a prime ideal of $\mathfrak{O}_E$ above p. The associated embedding $\iota = \iota_{\mathcal{Q}/p}$ embeds E into $E_\mathcal{Q} \subset \mathbb{Q}_p^c$. It gives rise to a homomorphism $E \otimes_\mathbb{Q} \mathbb{Q}_p \to E_\mathcal{Q}$, again denoted by ι, and an isomorphism $\chi \mapsto \chi^\iota$ of R_G onto $R_{G,p}$, the ring of virtual characters of G with values in $\mathbb{Q}_p^c$. We know by [Frö83, Lemma II.2.1] that it yields an isomorphism

$$\iota^* : \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J_p(E)) \xrightarrow{\sim} \mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G,p}, E_\mathcal{Q}^\times) \tag{1}$$

defined by $\iota^*(v)(\theta) = v(\theta^{\iota^{-1}})^\iota$, such that

$$\iota^*(\mathrm{Det}(\mathbb{Z}_p[G]^\times)) = \mathrm{Det}(\mathbb{Z}_p[G]^\times). \tag{2}$$

Here the left-hand side Det group takes semi-local values (on characters with values in $\mathbb{Q}^c$), whereas the right-hand side takes local values (on characters with values in $\mathbb{Q}_p^c$). However, the ambiguity in the notation should not present a problem thanks to this isomorphism.

[1] When dealing with a tamely ramified place, we also use the standard notation $\tau^*_{F_\ell}$ (with an asterisk instead of a star in the exponent).

We now compute $\iota^*(f_p)$. Let $\theta \in R_{G,p}$ and set $\chi = \theta^{\iota^{-1}}$; then

$$\iota^*(f_p)(\theta) = \prod_{\ell \in S} T_\ell^\star(\chi_\ell)^\iota \prod_{\wp \mid p} \mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \mid \chi)^\iota.$$

For each $\ell \in S$ we let $\mathcal{T}_\ell^\star \in \mathrm{Hom}(R_{G(\ell),p}, E_{\mathcal{Q}}^\times)$ be such that for $\phi \in R_{G(\ell),p}$,

$$\mathcal{T}_\ell^\star(\phi) = T_\ell^\star(\phi^{\iota^{-1}})^\iota.$$

Then $T_\ell^\star(\chi_\ell)^\iota = \mathcal{T}_\ell^\star(\theta_\ell)$, since $\iota : R_G \hookrightarrow R_{G,p}$ commutes with restriction of characters to $G(\ell)$.

Recall from § 2.3.2 that we have fixed a prime ideal $\mathcal{P}$ of $\mathfrak{O}_E$ above each prime ideal $\wp$ of $\mathfrak{O}$, and set $\mathfrak{p} = \mathcal{P} \cap N$. We have not specified the semi-local generator $\beta_\wp$ yet, but in view of [Ere91, Theorem 1] and [Frö83, Proposition III.2.1], which has already been checked by Erez to apply to our situation, we may choose a local generator $\alpha_\wp \in N_\mathfrak{p}^\times$ such that $\mathcal{A}_{N_\mathfrak{p}/F_\wp} = \mathfrak{O}_{F_\wp}[G(\wp)]\alpha_\wp$ and set

$$(\beta_\wp)_\mathfrak{p} = \alpha_\wp, \quad (\beta_\wp)_{\mathfrak{p}'} = 0$$

for any prime ideal $\mathfrak{p}'$ of $\mathfrak{O}_N$ above $\wp$ and distinct from $\mathfrak{p}$. It then follows from [Frö83, Theorem 19] (see also [Ere91, Proposition 5.1]) that, for $\chi \in R_G$,

$$\mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \mid \chi)_\mathcal{Q} = \mathcal{N}_{F_\wp/\mathbb{Q}_p}(\alpha_\wp \mid \chi_\wp^\iota) \det_{\chi^\iota}(\gamma_\mathcal{Q})$$

for some $\gamma_\mathcal{Q} \in G$ independent of χ. Note that the $\mathcal{Q}$-component $B_\mathcal{Q}$ of our semi-local norm-resolvent $B = \mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \mid \chi)$ equals B^ι (strictly speaking, we should write $B^{\mathcal{I}_\wp \iota}$, but we have identified $J_\wp(E)$ with $E \otimes_F F_\wp$ and hence omitted $\mathcal{I}_\wp$). Define $\mathcal{R}_\wp \in \mathrm{Hom}(R_{G(\wp),p}, E_\mathcal{Q}^\times)$ by

$$\mathcal{R}_\wp(\phi) = \mathcal{N}_{F_\wp/\mathbb{Q}_p}(\alpha_\wp \mid \phi)$$

for $\phi \in R_{G(\wp),p}$. Upon reordering the factors in $\iota^*(f_p)$, we get

$$\iota^*(f_p)(\theta) = \prod_{\wp' \nmid p} \mathrm{Ind}_{G(\wp')}^G(\mathcal{T}_{\wp'}^\star)(\theta) \prod_{\wp \mid p} (\mathrm{Ind}_{G(\wp)}^G(\mathcal{R}_\wp \mathcal{T}_\wp^\star)(\theta) \det_\theta(\gamma_\mathcal{Q})).$$

Most of the factors of $\iota^*(f_p)$ can be dealt with using previous results, which have already been gathered in [Vin01, § 4.2] in the absolute case.

LEMMA 2.4. *Let $E_\mathcal{Q}^0$ and $E_\mathcal{Q}^1$ denote the maximal subextensions of $E_\mathcal{Q}$ over $\mathbb{Q}_p$ which are unramified and tamely ramified, respectively.*

(i) *Suppose $\wp' \nmid p$; then $\mathcal{T}_{\wp'}^\star \in \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^0}[G(\wp')]^\times)$.*

(ii) *Suppose $\wp \mid p$ and $\wp \notin S_W$; then $\mathcal{R}_\wp \mathcal{T}_\wp^\star \in \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^1}[G(\wp)]^\times)$.*

Proof. Note first that since $\widetilde{T}_{\wp'}^\star = 1$ when $\wp' \notin S$, the same holds for $\mathcal{T}_{\wp'}^\star$. If $\wp' \nmid p$ and $\wp' \in S_T$, our modified Galois Gauss sum $\tau_{F_{\wp'}}^\star$ coincides with $\tau_{F_{\wp'}}^*$, the usual modified Galois Gauss sum (recall the footnote in § 2.3.2); so we may use [Tay81, Theorem 3] together with [CT85, (2-7)] (for the twist of the Galois Gauss sum by the Adams operator). Suppose now that $\wp' \in S_W$. We shall prove in Lemma 3.7 below (see also § 3.2.3) that $T_{\wp'}^\star$ can then be replaced by its non-modified analogue $T_{\wp'} : \chi \in R_{G(\wp')} \mapsto \tau_{F_{\wp'}}(\chi - \psi_2(\chi))$, whose behaviour is controlled by the immediate extension of the result in [Vin01, Lemme 4.7] to the relative case (noticing that the only part of Lemme 2.1 which is required in its proof, '$G_0 = G_1$', remains true; see Remark 3.5 below). This proves assertion (i).

If $\wp \mid p$ and $\wp \notin S_W$, once again our modified Galois Gauss sum is the usual one, $\tau_{F_\wp}^*$; so assertion (ii) follows from [Vin01, Lemme 4.3], whose proof is readily checked to apply to the current relative situation. □

In § 3 we will show, assuming Theorem 2, that assertion (ii) of the preceding lemma also holds when $\wp \in S_W$. We now explain how to deduce Theorem 1 from this result. Using the functorial properties of the group determinant regarding induction on character functions [Frö83, Theorem 12], it yields

$$\iota^*(f_p) \in \mathrm{Det}(\mathfrak{O}_{E^1_{\mathfrak{Q}}}[G]^\times).$$

In view of (1), we know that $\iota^*(f_p)$ is $\Omega_{\mathbb{Q}_p}$-equivariant. Therefore

$$\iota^*(f_p) \in \mathrm{Det}(\mathfrak{O}_{E^1_{\mathfrak{Q}}}[G]^\times)^{\Omega_{\mathbb{Q}_p}} = \mathrm{Det}(\mathfrak{O}_{E^1_{\mathfrak{Q}}}[G]^\times)^{\mathrm{Gal}(E^1_{\mathfrak{Q}}/\mathbb{Q}_p)} = \mathrm{Det}(\mathbb{Z}_p[G]^\times),$$

using Taylor's fixed point theorem for group determinants [Tay81, Theorem 6]. It follows from (2) that $f_p \in \mathrm{Det}(\mathbb{Z}_p[G]^\times)$ for every rational prime p dividing the order of G, and this proves Theorem 1.

3. Preliminary results

The core of this paper is the study of the remaining factor $\mathcal{R}_\wp \mathcal{T}^\star_\wp$ when $\wp$ is a prime ideal of $\mathfrak{O}$ which is wildly ramified in N/F (so that the rational prime p below $\wp$ divides the order of G). In this case, because of the assumption in Theorem 1, the local extension is abelian and weakly ramified. In order to prepare for extensive study of this factor in the next section, we devote § 3.1 to the description of these extensions, using results from Lubin–Tate theory; in § 3.2 we define the Galois Gauss sum of characters of Galois groups of such extensions, explain how we modify it and state some of its properties; finally, in § 3.3, we show how to deduce from Theorem 2 that $\mathcal{R}_\wp \mathcal{T}^\star_\wp \in \mathrm{Det}(\mathfrak{O}_{E^1_{\mathfrak{Q}}}[G(\wp)]^\times)$ when $\wp \in S_W$.

3.1 Local abelian weakly ramified extensions

Let K denote a finite extension of $\mathbb{Q}_p$ for some rational prime p, let d denote the residual degree of $K/\mathbb{Q}_p$, and set $q = p^d$. We intend to make use of Lubin–Tate theory to describe the wildly and weakly ramified abelian extensions of K, so we begin by fixing some (standard) notation. We refer to [Ser67, § 3] or [Iwa86] for, respectively, a brief or more detailed exposition of the theory.

If π is a uniformising parameter of K and n a non-negative integer, we denote by $K_{\pi,n}$ the nth division field associated to π over K. This is the same notation as in [Ser67], but note that the numbering is different in [Iwa86]. We set $K_\pi = \bigcup_{n\geqslant 1} K_{\pi,n}$. For a positive integer s, we denote by K^s_{un} the unramified extension of K of degree s contained in $\mathbb{Q}_p^{\mathrm{c}}$; we let $K_{\mathrm{un}} = \bigcup_{s\geqslant 1} K^s_{\mathrm{un}}$ be the maximal unramified extension of K in $\mathbb{Q}_p^{\mathrm{c}}$. Recall that K^{ab} stands for the maximal abelian extension of K in $\mathbb{Q}_p^{\mathrm{c}}$, with $\mathrm{Gal}(K^{\mathrm{ab}}/K) = \Omega_K^{\mathrm{ab}}$. Lubin–Tate theory states that any abelian extension of K is contained in the compositum of K_π and K_{un}:

$$K^{\mathrm{ab}} = K_\pi K_{\mathrm{un}}.$$

We remark that the fields $K_{\pi,n}$ and K_π depend on the uniformising parameter π; yet we have the following result.

Lemma 3.1. *Given uniformising parameters π and π' of K, for all $n \in \mathbb{N}$ there exists an $s \in \mathbb{N}$ such that $K_{\pi,n}K^s_{\mathrm{un}} = K_{\pi',n}K^s_{\mathrm{un}}$.*

Proof. In [Ser67, § 3.7], Serre proved the result $K^{\mathrm{ab}} = K_\pi K_{\mathrm{un}}$ by first showing that $K_\pi K_{\mathrm{un}} = K_{\pi'} K_{\mathrm{un}}$ for all uniformising parameters π and π'. Following his proof, we can actually replace K_π (respectively, $K_{\pi'}$) with $K_{\pi,n}$ (respectively, $K_{\pi',n}$) at every step to get

$$K_{\pi,n}K_{\mathrm{un}} = K_{\pi',n}K_{\mathrm{un}}.$$

This means that the compositum $K_{\pi,n}K_{\pi',n}$ must be contained in $K_{\pi,n}K_{\mathrm{un}}$, and therefore the extension $K_{\pi,n}K_{\pi',n}/K_{\pi,n}$ is unramified. We know that $[K_{\pi,n}K_{\pi',n} : K_{\pi,n}]$ is finite, and therefore $K_{\pi,n}K_{\pi',n} = K_{\pi,n}K_{\mathrm{un}}^s$ for some s. The result now follows by symmetry. □

PROPOSITION 3.2. *Let π be a given uniformising parameter of K and let L/K be a weakly ramified abelian extension. Then there exist fields L^{tot} and L^{un} such that $L \subseteq L^{\mathrm{tot}}L^{\mathrm{un}}$, $L^{\mathrm{tot}} \subseteq K_{\pi,2}$, and $L^{\mathrm{tot}}L^{\mathrm{un}}/L$ and L^{un}/K are unramified.*

Note that K_π/K is totally ramified, so $L^{\mathrm{tot}} \subseteq K_{\pi,2}$ implies that L^{tot}/K is totally ramified.

Proof. From [Pic10, Theorem 4.1] and its proof, we know that there exist fields $\tilde{L}^{\mathrm{tot}}$ and $\tilde{L}^{\mathrm{un}}$ such that $L \subseteq \tilde{L}^{\mathrm{tot}}\tilde{L}^{\mathrm{un}}$, $\tilde{L}^{\mathrm{tot}}/K$ is totally ramified, and $\tilde{L}^{\mathrm{tot}}\tilde{L}^{\mathrm{un}}/L$ and $\tilde{L}^{\mathrm{un}}/K$ are unramified; we also know that $\tilde{L}^{\mathrm{tot}}/K$ is abelian totally and weakly ramified, so there exists a uniformising parameter π' of K such that $\tilde{L}^{\mathrm{tot}} \subset K_{\pi'}$. Further, let H denote the Galois group of $\tilde{L}^{\mathrm{tot}}/K$ and c the valuation of its conductor: set $U_K^0 = \mathfrak{O}_K^\times$ and $U_K^n = 1 + \pi^n\mathfrak{O}_K$ for any positive integer n; then c is the minimal integer $n \geqslant 0$ such that U_K^n is contained in the norm group $N_{\tilde{L}^{\mathrm{tot}}/K}((\tilde{L}^{\mathrm{tot}})^\times)$. We know that $c = (|H_0| + |H_1|)/|H_0|$ by [Iwa86, Corollary to Lemma 7.14]; hence $c \leqslant 2$. Combining [Iwa86, Proposition 7.2(ii) and Lemma 7.4] (remembering that the numbering of division fields there is different from ours), we get

$$\tilde{L}^{\mathrm{tot}} \subset K_{\pi',2}.$$

From Lemma 3.1 we then have an integer s such that $K_{\mathrm{un}}^s K_{\pi',2} = K_{\mathrm{un}}^s K_{\pi,2}$. Our result then follows by taking $L^{\mathrm{un}} = \tilde{L}^{\mathrm{un}}K_{\mathrm{un}}^s$ and $L^{\mathrm{tot}} = \tilde{L}^{\mathrm{tot}}K_{\mathrm{un}}^s \cap K_{\pi,2}$. □

Let $\Gamma^{(n)} = \mathrm{Gal}(K_{\pi,n}/K)$; then the Artin map $\theta_K : K^\times \to \Omega_K^{\mathrm{ab}}$ yields an isomorphism $(\mathfrak{O}_K/\pi^n\mathfrak{O}_K)^\times \cong \Gamma^{(n)}$ so that

$$\Gamma^{(2)} \cong \Gamma^{(1)} \times \Gamma,$$

where $\Gamma^{(1)}$ is cyclic of order $q-1$ and $\Gamma = \{\theta_K(1+\pi u), u \in \mathfrak{O}_K/\pi\mathfrak{O}_K\}$; hence $\Gamma \cong \mathfrak{O}_K/\pi\mathfrak{O}_K$ is p-elementary abelian of order q. We state the following fact for future reference.

PROPOSITION 3.3. *The subextension $M_{\pi,2}$ of $K_{\pi,2}/K$ fixed by $\Gamma^{(1)}$ has*

$$r = \frac{p^d - 1}{p-1} = 1 + p + \cdots + p^{d-1}$$

subextensions M_i, $1 \leqslant i \leqslant r$, of degree p over K, each of which is the fixed subextension of $M_{\pi,2}/K$ by the kernel of an irreducible character χ_i of $\mathrm{Gal}(M_{\pi,2}/K) \cong \Gamma$.

Proof. See, for instance, [Vin05, § 2.2]. □

Notice further that $K_{\pi,2} = K_{\pi,1}M_{\pi,2}$ and that $M_{\pi,2}$ is the maximal p-extension of K contained in $K_{\pi,2}$.

COROLLARY 3.4. *In the notation of Proposition 3.2, suppose further that L/K is wildly ramified; then the conclusion of Proposition 3.2 holds with $L^{\mathrm{tot}} \subseteq M_{\pi,2}$. If, moreover, the ramification group of L/K is cyclic, then $L^{\mathrm{tot}} = M_i$ for an integer $i \in \{1, \ldots, r\}$.*

Proof. Let $H = \mathrm{Gal}(L/K)$ and, for $i \geqslant -1$, let H_i denote the ith ramification subgroup (in lower notation). One has $H_1 \neq H_2 = 1$ since L/K is wildly and weakly ramified, so $H_0/H_1 = 1$ by [Ser68, IV.2, Corollary 2 to Proposition 9]; in particular, H_0 is a p-group.

Let L^{tot} and L^{un} be as given by Proposition 3.2. They are linearly disjoint over K, so $\mathrm{Gal}(L^{\mathrm{tot}}L^{\mathrm{un}}/K)$ equals the direct product $\mathrm{Gal}(L^{\mathrm{tot}}/K) \times \mathrm{Gal}(L^{\mathrm{un}}/K)$ and the ramification

group of $L^{\mathrm{tot}}L^{\mathrm{un}}/K$ equals that of L^{tot}/K. Since L^{tot}/K is totally ramified and $L^{\mathrm{tot}}L^{\mathrm{un}}/L$ is unramified, this yields (e.g. using Herbrand's theorem)

$$\mathrm{Gal}(L^{\mathrm{tot}}/K) = \mathrm{Gal}(L^{\mathrm{tot}}/K)_0 = H_0.$$

Since H_0 is a p-group, we get that $L^{\mathrm{tot}} \subseteq {K_{\pi,2}}^{\Gamma^{(1)}} = M_{\pi,2}$. Further, $\mathrm{Gal}(L^{\mathrm{tot}}/K)$ is a quotient of the p-elementary abelian group Γ and so has to be of order p if cyclic. □

3.2 Local weakly ramified Galois Gauss sums

Here, again, p is a fixed rational prime and K is a finite extension of $\mathbb{Q}_p$. Recall from Notation 2.1 that $\mathbb{Q}^{\mathrm{c}}$ denotes the algebraic closure of $\mathbb{Q}$ in the field of complex numbers. For any non-negative integer n, let ξ_n be the p^nth primitive root of unity in $\mathbb{Q}^{\mathrm{c}}$ given by $\xi_n = \exp(2i\pi/p^n)$, with the standard complex number notation; in particular, $\xi_0 = 1$. In the following, we shall use the notation

$$\zeta = \xi_1, \quad \xi = \xi_2, \tag{3}$$

since we will mainly be concerned with these two p^nth roots of unity. From now on we shall use the letter π to denote a uniformising parameter of K.

3.2.1 *Abelian Galois Gauss sum.* Let L be a finite abelian extension of K with Galois group H. We denote by $\widehat{H}$ the group of irreducible characters of H with values in $\mathbb{Q}^{\mathrm{c}}$. Any $\chi \in \widehat{H}$ can be seen as a character of $K^\times$ using the composition of the Artin map θ_K of K with the restriction of automorphisms to L,

$$\theta_{L/K} : K^\times \to \Omega_K^{\mathrm{ab}} \twoheadrightarrow \mathrm{Gal}(L/K) = H.$$

We shall also denote by χ the character of $K^\times$ obtained in this way. Set $U_K^0 = \mathfrak{O}_K^\times$ and let $U_K^m = 1 + \pi^m\mathfrak{O}_K$ for any positive integer m. The conductor $\mathfrak{f}(\chi)$ of the character χ is $\pi^m\mathfrak{O}_K$, where m is the smallest integer such that $\chi(U_K^m) = 1$.

Let $\mathfrak{D}_K = \pi^s\mathfrak{O}_K$ denote the absolute different of $K/\mathbb{Q}_p$, and let ψ_K denote the standard additive character of K, which is defined by composing the trace $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}_p}$ with the additive homomorphism $\psi_p : \mathbb{Q}_p \to (\mathbb{Q}^{\mathrm{c}})^\times$ such that $\psi_p(\mathbb{Z}_p) = 1$ and, for any natural integer n, $\psi_p(1/p^n) = \xi_n$, the p^nth root of unity defined above. The (local) Galois Gauss sum τ_K is then defined by

$$\tau_K(\chi) = \sum_x \chi\left(\frac{x}{\pi^{s+m}}\right)\psi_K\left(\frac{x}{\pi^{s+m}}\right)$$

(see [Mar77, II.2, p. 29]), where m is such that $\mathfrak{f}(\chi) = \pi^m\mathfrak{O}_K$ and x runs through a set of representatives of U_K^0/U_K^m. In particular, $\tau_K(\chi) = \chi(\pi^{-s})$ if χ is unramified, i.e. if $\mathfrak{f}(\chi) = \mathfrak{O}_K$.

The Galois Gauss sum is now defined on $\widehat{H}$. Since $\widehat{H}$ is a basis of the free group of virtual characters R_H, we extend τ_K to a function on R_H by linearity: $\tau_K(\chi + \chi') = \tau_K(\chi)\tau_K(\chi')$. Inductivity in degree 0 then enables one to extend τ_K to virtual characters of non-abelian extensions of K; see [Frö83, Theorem 18]. Note that the conductor function $\mathfrak{f}$ extends to R_H in the same way.

Before modifying the abelian Galois Gauss sum, we define the non-ramified part n_χ of $\chi \in \widehat{H}$ by $n_\chi = \chi$ if χ is unramified, and $n_\chi = 0$ otherwise. The map $\chi \mapsto n_\chi$ then extends to an endomorphism of the additive group R_H by linearity ($n_{\chi+\chi'} = n_\chi + n_{\chi'}$). One easily checks that if $\chi \in R_H$ is such that $\chi = n_\chi$, then

$$\tau_K(\chi) = \det_\chi(\pi^{-s}) = \det_\chi(\mathfrak{D}_K^{-1}). \tag{4}$$

3.2.2 *Modification in the tame and weak cases.* In this paper, we only have to consider the case where L/K is tamely or weakly ramified, i.e. where H_1 or H_2 is trivial. Since $\theta_{L/K}$ sends U_K^m to the mth ramification group in the upper numbering, H^m (see [Ser67, 4.1, Theorem 1]), and since $H^1 = H_1$ and $H_2 = 1$ implies $H^2 = 1$, we see that for $\chi \in \widehat{H}$ we will always have $\pi^2\mathfrak{O}_K \subseteq \mathfrak{f}(\chi)$. We shall say that $\chi \in \widehat{H}$ is unramified if $\mathfrak{f}(\chi) = \mathfrak{O}_K$, tamely ramified if $\mathfrak{f}(\chi) = \pi\mathfrak{O}_K$ and weakly ramified if $\mathfrak{f}(\chi) = \pi^2\mathfrak{O}_K$. We shall also say that $\chi \in R_H$ is unramified if $\mathfrak{f}(\chi) = \mathfrak{O}_K$.

Remark 3.5. If L/K is wildly and weakly ramified and abelian, then $H_0 = H_1$ (see the proof of Corollary 3.4); thus any $\chi \in \widehat{H}$ is either unramified or weakly ramified. Indeed, in the abelian case, the tame and 'wild and weak' situations do not occur simultaneously.

We recall how the Galois Gauss sum is modified in the tame abelian situation. Fix an element $c_{K,1} \in K$ such that $c_{K,1}\mathfrak{O}_K = \pi\mathfrak{D}_K$. Suppose that L/K is (at most) tamely ramified and χ is a virtual character of H. Recall from above the definition of the non-ramified part n_χ of χ. The (tame) non-ramified characteristic of χ is $y_{K,1}(\chi) = (-1)^{\deg(n_\chi)} \det_{n_\chi}(\pi)$, and its modified Galois Gauss sum is

$$\tau_K^\star(\chi) = \tau_K(\chi) y_{K,1}(\chi)^{-1} \det_\chi(c_{K,1}).$$

This function is usually denoted by τ_K^* (see [Frö83, IV.1]); we changed the asterisk in the exponent into a star to stress the fact that the Galois Gauss sum will be modified in a different (yet similar) way in the wild and weak case. Indeed, the above remark enables us to treat these two cases separately.

Fix an element $c_{K,2} \in K$ such that $c_{K,2}\mathfrak{O}_K = \pi^2\mathfrak{D}_K$. Note that if K' is a finite Galois extension of K with uniformising parameter π' and Galois group H', with $H'_0 = H'_1$ and $H'_2 = 1$ (a property referred to as 'purely weakly ramified'), then $c_{K,2}\mathfrak{O}_{K'} = \pi'^2\mathfrak{D}_{K'}$.

Suppose that L/K is wildly and weakly ramified and abelian.

Definition 3.6. The (weak) non-ramified characteristic of $\chi \in R_H$ is

$$y_{K,2}(\chi) = (-1)^{\deg(n_\chi)} \det_{n_\chi}(\pi^2);$$

its modified Galois Gauss sum is

$$\tau_K^\star(\chi) = \tau_K(\chi) y_{K,2}(\chi)^{-1} \det_\chi(c_{K,2}).$$

Note that since n_χ is an unramified character, $y_{K,2}(\chi)$ does not depend on the choice of the uniformising parameter π. In contrast, $\tau_K^\star$ depends on the choice of the element $c_{K,2}$, unless χ is unramified; changing $c_{K,2}$ multiplies $\tau_K^\star$ by an element of $\mathrm{Det}(H_0)$.

For the purposes of this paper we will only need the abelian modified Galois Gauss sum. Nevertheless, this notion extends to non-abelian characters as in the tame situation. First, one shows using the results in § 3.1 that there exists a maximal 'purely weakly ramified' (see above) extension K^{pw} of K; let $R_{(K)}^{\mathrm{pw}}$ denote the free group generated by the characters of the irreducible representations of $\mathrm{Gal}(K^{\mathrm{pw}}/K)$ over $\mathbb{Q}^{\mathrm{c}}$ with open kernel. One then easily checks that the proof of [Frö83, Theorem 29(ii)] shows, *mutatis mutandis*, that $y_{K,2}$ is fully inductive; that is, for $K \subseteq K' \subset K^{\mathrm{pw}}$ and $\chi \in R_{(K')}^{\mathrm{pw}}$,

$$y_{K',2}(\chi) = y_{K,2}(\mathrm{ind}\,\chi),$$

where ind χ is the induced character of χ in $R_{(K)}^{\mathrm{pw}}$. Since τ_K is inductive in degree 0 in the purely weakly ramified context as well as in the tame one (see, for instance, [Mar77, II.4, p. 39]), and since the same holds for $\det(c_{K,2})$ (see the proof of [Frö83, Proposition IV.1.1(iv)]), the above

definition yields modified Galois Gauss sums $\tau^\star_{K'}$ on $R^{\mathrm{pw}}_{(K')}$ for any K'/K contained in K^{pw}, which are inductive in degree 0.

We now check that our modification only involves factors in the denominator of the Hom-description; see [Frö83, Theorem 29(i)] for the tame case.

Lemma 3.7. *Suppose that L/K is abelian, of Galois group H, and either tamely or wildly and weakly ramified. The map $\tau^\star_K/\tau_K$ belongs to* $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_H, (\mathbb{Q}^{\mathrm{c}})^\times)\,\mathrm{Det}(H)$.

Proof. Let $i = 1$ or 2, depending on whether L/K is tamely or weakly ramified, and let $\chi \in R_H$. Clearly, $y_{K,i}$ is $\Omega_{\mathbb{Q}}$-equivariant and takes roots-of-unity values, since $\det_{n_\chi}$ is an abelian character. Set $h_{K,i} = \theta_{L/K}(c_{K,i}) \in H$; then $\det_\chi(c_{K,i}) = \det_\chi(h_{K,i})$. Therefore $\chi \mapsto \det_\chi(c_{K,i}) \in \mathrm{Det}(H)$. □

Note that when $\chi \in \widehat{H}$ is weakly ramified, we get $\tau^\star_K(\chi) = \tau_K(\chi)\chi(c_{K,2})$. Further, recall from [Tat77, § 1] that in this case the Galois Gauss sum is linked to the local root number $W(\chi)$ by

$$\tau_K(\chi) = p^d W(\chi^{-1}), \tag{5}$$

where d is the residual degree of $K/\mathbb{Q}_p$. We now show the following very useful property; see [Frö83, Proposition IV.1.1(vi)] for the analogous statement in the tame situation.

Proposition 3.8. *Suppose that L/K is wildly and weakly ramified with abelian Galois group H and that $\chi, \phi \in \widehat{H}$ with ϕ unramified. Then*

$$\tau^\star_K(\phi) = -1, \quad \tau^\star_K(\phi\chi) = \tau^\star_K(\chi).$$

Proof. One has $\tau_K(\phi) = \phi(\pi^{-s})$, $y_{K,2}(\phi) = -\phi(\pi^2)$ and $\phi(c_{K,2}) = \phi(\pi^{2+s})$, hence the result for $\tau^\star_K(\phi)$. The result for $\tau^\star_K(\phi\chi)$ follows when χ is unramified. Suppose that χ is ramified; thus $\mathfrak{f}(\chi) = \mathfrak{f}(\phi\chi) = \pi^2\mathfrak{O}_K$ and we get, using (5) above together with [Tat77, § 1 Corollary 2], that

$$\tau_K(\phi\chi) = p^d W(\phi^{-1}\chi^{-1}) = p^d\phi^{-1}(\pi^{2+s})W(\chi^{-1}) = \phi(\pi^{-2-s})\tau_K(\chi).$$

Further, $y_{K,2}(\chi\phi) = 1 = y_{K,2}(\chi)$ and $\chi\phi(c_{K,2}) = \phi(\pi^{2+s})\chi(c_{K,2})$, hence the result for $\tau^\star_K(\phi\chi)$. □

More generally, when L/K is abelian and either tamely or wildly and weakly ramified, and $\phi \in R_H$ is unramified, one can check from Definition 3.6, using (4), that $\tau^\star_K(\phi) = (-1)^{\deg(\phi)}$.

3.2.3 *Twisting.* The last step in building the morphism f defined in § 2.3 is to twist the modified Galois Gauss sum by ψ_2, the second Adams operation, which is the endomorphism of R_G defined by $\psi_2(\chi)(g) = \chi(g^2)$ for $\chi \in R_G$ and $g \in G$. The properties of ψ_2, together with Lemma 3.7 above, enable us to show that f is, as claimed, a representative of $(\mathcal{A})$.

Proof of Proposition 2.3. One only has to check that the quotient of f by Erez's representative $v_{N/F}$ (see [Ere91, Theorem 3.6]) lies in the denominator of the Hom-description. Choosing the same semi-local normal basis generators $\beta_\wp$ to define f and $v_{N/F}$ (the change of semi-local generator lies in the denominator of the Hom-description; see [Frö83, Corollary to Proposition I.4.2]), this quotient is the global valued morphism on R_G given by

$$\frac{f}{v_{N/F}} = \prod_{\ell \in S} \mathrm{Ind}^G_{G(\ell)}\left(\frac{\tau^\star_{F_\ell}/\tau_{F_\ell}}{\Psi_2(\tau^\star_{F_\ell}/\tau_{F_\ell})}\right),$$

where Ψ_2 is the second Adams operator, defined by $\Psi_2(v)(\chi) = v(\psi_2(\chi))$ if v is a character function. Fix an $\ell \in S$. We know by Lemma 3.7 that $\tau^\star_{F_\ell}/\tau_{F_\ell} \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{G(\ell)}, E^\times)\,\mathrm{Det}(G(\ell))$.

By [CT85, (2-7)], Ψ_2 preserves $\mathrm{Det}(\mathbb{Z}_l[G(\ell)]^\times)$ for every rational prime l, and hence $\Psi_2(\mathrm{Det}(G(\ell))) \subset \mathrm{Det}(\mathbb{Z}[G(\ell)]^\times)$. Further, ψ_2 commutes with the action of $\Omega_\mathbb{Q}$ on $R_{G(\ell)}$ (see [Ere91, Proposition-Definition 3.5]), and hence Ψ_2 preserves $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_{G(\ell)}, E^\times)$. Applying [Frö83, Theorem 12], we see that $f/v_{N/F}$ belongs to $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^\times)\,\mathrm{Det}(\mathcal{U}(\mathbb{Z}[G]))$ as required. □

3.2.4 *Alternative expressions of the twisted modified Galois Gauss sum.* We return to the previous setting, so that L/K is an abelian weakly ramified extension of p-adic fields, with Galois group H. The abelian hypothesis yields that if $\chi \in \widehat{H}$, then $\psi_2(\chi) = \chi^2$ and hence $\tau_K^\star(\chi - \psi_2(\chi)) = \tau_K^\star(\chi)/\tau_K^\star(\chi^2)$. If, moreover, χ is weakly ramified, then

$$\tau_K^\star(\chi - \psi_2(\chi)) = \chi(c_{K,2})^{-1}\tau_K(\chi - \chi^2). \tag{6}$$

Note also that for any $\chi \in R_H$, $\psi_2(\chi)$ has the same degree as χ. If χ is unramified, it follows that

$$\tau_K^\star(\chi - \psi_2(\chi)) = 1. \tag{7}$$

Recall that ψ_K is the standard additive character of K defined in § 3.2.1 (and be aware that ψ_2 and ψ_K are very different functions).

Proposition 3.9. *Suppose that $\chi \in \widehat{H}$ is weakly ramified; then there exists $c_\chi \in K$ such that*

$$c_\chi \mathfrak{O}_K = \mathfrak{f}(\chi)\mathfrak{D}_K \quad \text{and} \quad \chi(1+y)^{-1} = \psi_K(c_\chi^{-1}y) \ \text{ for all } y \in \pi\mathfrak{O}_K. \tag{8}$$

Furthermore, for any such c_χ,

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

Proof. This result is a direct consequence of [Tat77, § 1]. Using (5) and applying [Tat77, § 1, Proposition 1] to $\alpha = \chi^{-1}$ and $\mathfrak{a} = \pi\mathfrak{O}_K$, we get the existence of c_χ in K satisfying conditions (8) above; we also get that, for any such c_χ,

$$\tau_K(\chi) = p^d\chi(c_\chi^{-1})\psi_K(c_\chi^{-1}).$$

It only remains to notice that c_χ satisfies conditions (8) for χ if and only if $c_\chi/2$ satisfies the same for χ^2, to obtain the result through (6). □

We deduce a result which will be required later.

Corollary 3.10. *Suppose $K/\mathbb{Q}_p$ is unramified and set $v_{K,2} = p^2/c_{K,2} \in \mathfrak{O}_K^\times$. Suppose that $\chi \in \widehat{H}$ is weakly ramified; then there exists $v_\chi \in \mathfrak{O}_K^\times$ such that for all $u \in \mathfrak{O}_K$, $\chi(1+up)^{-1} = \zeta^{\mathrm{Tr}(uv_\chi)}$. Under this condition, one has*

$$\tau_K^\star(\chi - \chi^2) = \chi\left(\frac{v_{K,2}}{4v_\chi}\right)\xi^{-\mathrm{Tr}(v_\chi)}.$$

Furthermore:

(i) *v_χ is uniquely defined modulo p, but $v_\chi + ap$ also satisfies the above condition for any $a \in \mathfrak{O}_K$;*

(ii) *if $j \in \{1, \dots, p-1\}$, v_{χ^j} can be chosen equal to jv_χ.*

Proof. Since $K/\mathbb{Q}_p$ is unramified, p is a uniformising parameter of K and $\mathfrak{f}(\chi)\mathfrak{D}_K = \mathfrak{f}(\chi) = p^2\mathbb{Z}_p$. Take $c_\chi \in K$ satisfying conditions (8) for χ, and set $v_\chi = p^2/c_\chi$; then $v_\chi \in \mathfrak{O}_K^\times$, and for all $u \in \mathfrak{O}_K$ one has $\chi(1+up)^{-1} = \psi_K(uv_\chi/p) = \zeta^{\mathrm{Tr}(uv_\chi)}$. Conversely, if v_χ satisfies these conditions,

then $c_\chi = p^2/v_\chi$ satisfies conditions (8) and the formula given in Proposition 3.9 yields the formula for the Galois Gauss sum.

Let k denote the residue field of K. The trace form $T(x,y) = \mathrm{Tr}_{k/(\mathbb{Z}_p/p\mathbb{Z}_p)}(xy)$ is a non-degenerate symmetric bilinear form from $k \times k$ to $\mathbb{Z}_p/p\mathbb{Z}_p$ and hence induces an isomorphism $y \mapsto T(\,.\,,y)$ between k and its dual. If $v_\chi \in \mathfrak{O}_K^\times$ satisfies the condition of the corollary, then $T(\,.\,, v_\chi \bmod p)$ is given by this condition, and hence $v_\chi \bmod p$ is unique. The two last assertions are readily checked. □

Remark 3.11. Under the hypothesis of Corollary 3.10, we get

$$\tau_K^\star(\chi - \chi^2)^p = \zeta^{-\mathrm{Tr}(v_\chi)} = \chi(1+p);$$

so the modified twisted Galois Gauss sum is a pth root of unity if and only if $\chi(1+p)$ is trivial, namely when $\theta_{L/K}(1+p)$ belongs to $\ker(\chi)$. If $K/\mathbb{Q}_p$ is ramified, we get by Proposition 3.9 that $\chi(1+p)^{-1} = \psi_K(c_\chi^{-1}p) = \psi_K(c_\chi^{-1})^p$; therefore we have

$$\tau_K^\star(\chi - \chi^2)^p = \chi(1+p) = 1$$

since $p \in \pi^2\mathfrak{O}_K$. The modified abelian weakly ramified twisted Galois Gauss sum is thus always a pth root of unity in the ramified base field case.

3.3 Reduction of the problem

Recall that p is a rational prime dividing the order of G (in particular, $p \neq 2$ since $[N:F]$ is odd), $\mathcal{Q}$ is a prime ideal of $\mathfrak{O}_E$ above p, and $\wp$ is a prime ideal of $\mathfrak{O}$ above p which is wildly ramified in N/F. In § 2.3.2 we fixed a prime ideal $\mathcal{P}$ of E above $\wp$ and denoted by $\iota_{\mathcal{P}/\wp}$ the corresponding embedding of E into $\mathbb{Q}_p^c$ fixing $\wp$; recall that we also used $G(\wp)$ to denote the image in G of $\mathrm{Gal}(N_\mathfrak{p}/F_\wp)$, where $\mathfrak{p} = \mathcal{P} \cap N$, under the homomorphism induced by $\iota_{\mathcal{P}/\wp}$. We introduce the following useful notation.

Notation 3.12. If K is a finite extension of $\mathbb{Q}_p$ and L/K is weakly ramified with Galois group H, let α_L denote a normal basis generator of the square root of the inverse different $\mathcal{A}_{L/K}$ of L/K and $\mathcal{RT}_K^\star(L)$ the morphism from $R_{H,p}$ to $E_\mathcal{Q}^\times$ given by

$$\mathcal{RT}_K^\star(L)(\chi) = \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_L \mid \chi)\mathcal{T}_K^\star(\chi).$$

We will sometimes write $\tau_K^\star(\chi - \chi^2)$ instead of $\mathcal{T}_K^\star(\chi)$, when the context makes it clear what we mean.

We are thus interested in computing $\mathcal{RT}_{F_\wp}^\star(N_\mathfrak{p}) = \mathcal{R}_\wp\mathcal{T}_\wp^\star$.

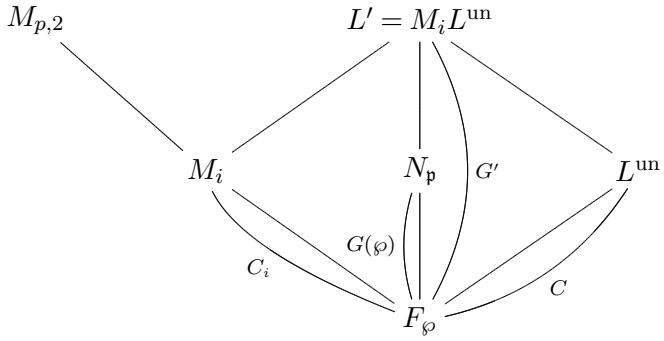
By the hypothesis in Theorem 1, $F_\wp$ is unramified over $\mathbb{Q}_p$ and $N_\mathfrak{p}/F_\wp$ is abelian, is wildly and weakly ramified, and has cyclic ramification group. We are therefore in a position to apply Corollary 3.4 with $K = F_\wp$, uniformising parameter $\pi = p$, and $L = N_\mathfrak{p}$. Recall that $M_{p,2}$ has $r = (p^d-1)/(p-1)$ subextensions M_i, $1 \leqslant i \leqslant r$, of degree p over $F_\wp$. We know that there exist an unramified extension $L^{\mathrm{un}}/F_\wp$ and an integer $1 \leqslant i \leqslant r$ such that

$$N_\mathfrak{p} \subseteq M_iL^{\mathrm{un}} \quad \text{and} \quad M_iL^{\mathrm{un}}/N_\mathfrak{p} \text{ is unramified.}$$

Proposition 3.13. *Let $C_i = \mathrm{Gal}(M_i/F_\wp)$; then*

$$\mathcal{RT}_{F_\wp}^\star(M_i) \in \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^1}[C_i]^\times) \implies \mathcal{RT}_{F_\wp}^\star(N_\mathfrak{p}) \in \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^1}[G(\wp)]^\times).$$

Before giving the proof, we describe these extensions in a diagram where we introduce some notation for the Galois groups involved.



Proof. There will be two steps in the reduction process: from M_i to $L' = M_i L^{\mathrm{un}}$ and from L' to $N_{\mathfrak{p}}$. For the first step, we shall take advantage of the fact that $L'/F_\wp$ is the compositum of the totally ramified extension $M_i/F_\wp$ and the unramified extension $L^{\mathrm{un}}/F_\wp$.

LEMMA 3.14. *Let K be a finite Galois extension of $\mathbb{Q}_p$ and K^t its maximal tame extension in $\mathbb{Q}_p^{\mathrm{c}}$. Let L_u be an unramified extension of K such that $L_u/\mathbb{Q}_p$ is Galois, let L_1/K be an abelian totally wildly and weakly ramified extension, and set $L_2 = L_1 L_u$, $G_1 = \mathrm{Gal}(L_1/K)$ and $G_2 = \mathrm{Gal}(L_2/K)$. Then*

$$\mathcal{RT}_K^\star(L_1) \in \mathrm{Det}(\mathfrak{O}_{K^t}[G_1]^\times) \implies \mathcal{RT}_K^\star(L_2) \in \mathrm{Det}(\mathfrak{O}_{K^t}[G_2]^\times).$$

Notice that the existence of a normal basis generator α_{L_2} for $\mathcal{A}_{L_2/K}$ is ensured by [Ere91, § 2, Theorem 1] and [Vin01, Proposition 2.2(ii)].

Proof. Since L_u/K is unramified, let us denote by C its cyclic Galois group. Then $G_2 = G_1 \times C$, and any irreducible character χ_2 of G_2 decomposes as a product $\chi_2 = \chi_1\chi_C$ where χ_1 (respectively, χ_C) is an irreducible character of G_1 (respectively, C). Let β denote a normal basis generator for $\mathfrak{O}_{L_u} = \mathcal{A}_{L_u/K}$ over $\mathfrak{O}_K$. Since L_1/K and L_u/K are linearly disjoint, one has $\mathcal{A}_{L_2/K} = \mathcal{A}_{L_1/K} \otimes_{\mathfrak{O}_K} \mathfrak{O}_{L_u}$. This implies that $\alpha_{L_1} \otimes \beta$ is a normal basis generator for $\mathcal{A}_{L_2/K}$ over $\mathfrak{O}_K$, so there exists $u \in \mathfrak{O}_K[G_2]^\times$ such that $\alpha_{L_2} = (\alpha_{L_1} \otimes \beta)u$. By [Frö83, § I, Corollary to Proposition 4.2], this yields

$$\begin{aligned}(\alpha_{L_2} \mid \chi_2) &= (\alpha_{L_1} \otimes \beta \mid \chi_2)\,\mathrm{Det}_{\chi_2}(u)\\ &= (\alpha_{L_1} \mid \chi_1)(\beta \mid \chi_C)\,\mathrm{Det}_{\chi_2}(u)\\ &= (\alpha_{L_1} \mid \chi_1)\,\mathrm{Det}_{\chi_C}(B)\,\mathrm{Det}_{\chi_2}(u), \qquad (9)\end{aligned}$$

where $B = \sum_{c\in C} c(\beta)c^{-1} \in \mathfrak{O}_{L_u}[C]^\times$ by [Frö83, Proposition I.4.3]. Note that χ_C is the restriction to C of χ_2 and that $[\chi_C \mapsto \mathrm{Det}_{\chi_C}(B)] \in \mathrm{Det}(\mathfrak{O}_{L_u}[C]^\times)$; so $[\chi_2 \mapsto \mathrm{Det}_{\chi_C}(B)] \in \mathrm{Det}(\mathfrak{O}_{L_u}[G_2]^\times)$ by the functorial properties of Det. Consequently, let $v \in \mathfrak{O}_{L_u}[G_2]^\times$ be such that $(\alpha_{L_2} \mid \chi_2) = (\alpha_{L_1} \mid \chi_1)\,\mathrm{Det}_{\chi_2}(v)$. To compute the norm-resolvent $\mathcal{N}_{K/\mathbb{Q}_p}$, we need to choose a transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$. Since $\Omega_{\mathbb{Q}_p}/\Omega_K = \mathrm{Gal}(L_u/\mathbb{Q}_p)/\mathrm{Gal}(L_u/K)$, we can choose Ω so that $\Omega|_{L_u} \subset \mathrm{Gal}(L_u/\mathbb{Q}_p)$. With this choice, $v' = \prod_\Omega v^\omega \in \mathfrak{O}_{L_u}[G_2]^\times$ is such that

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_2} \mid \chi_2) = \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_1} \mid \chi_1)\,\mathrm{Det}_{\chi_2}(v').$$

We now consider the twisted modified Galois Gauss sum. Since χ_C is an unramified character, we know from Proposition 3.8 that $\tau_K^\star(\chi_2 - \chi_2^2) = \tau_K^\star(\chi_1 - \chi_1^2)$. This yields

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_2} \mid \chi_2)\tau_K^\star(\chi_2 - \chi_2^2) = \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_1} \mid \chi_1)\tau_K^\star(\chi_1 - \chi_1^2)\,\mathrm{Det}_{\chi_2}(v').$$

Suppose $\mathcal{RT}^\star_K(L_1) \in \mathrm{Det}(\mathfrak{O}_{K^t}[G_1]^\times)$; then by induction of character functions, the map $\chi_2 \mapsto \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_1} \mid \chi_1)\tau_K(\chi_1 - \chi_1^2)$ belongs to $\mathrm{Det}(\mathfrak{O}_{K^t}[G_2]^\times)$, and the same holds for $\chi_2 \mapsto \mathrm{Det}_{\chi_2}(v')$ and thus for $\mathcal{RT}^\star_K(L_2)$. □

Suppose $\mathcal{RT}^\star_{F_\wp}(M_i) \in \mathrm{Det}(\mathfrak{O}_{E^1_\mathcal{Q}}[C_i]^\times)$. We know that $L' = M_i L^{\mathrm{un}}$ is unramified over $N_\mathfrak{p}$ and that $N_\mathfrak{p}/F_\wp$ is weakly ramified; therefore $L'/F_\wp$ is weakly ramified. We then apply Lemma 3.14 to $K = F_\wp$, $L_1 = M_i$ and $L_u = L^{\mathrm{un}}$, and get that $\mathcal{RT}^\star_{F_\wp}(L') \in \mathrm{Det}(\mathfrak{O}_{E^1_\mathcal{Q}}[G']^\times)$.

We consider the restriction of $F_\wp$-automorphisms of L' to $N_\mathfrak{p}$: $G' \twoheadrightarrow G(\wp)$. This induces an inflation map on characters, $\mathrm{inf} : R_{G(\wp),p} \to R_{G',p}$, which in turn induces a co-inflation map on character functions,

$$\mathrm{coinf} = \mathrm{coinf}^{G'}_{G(\wp)} : \mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G',p}, E^\times_\mathcal{Q}) \to \mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G(\wp),p}, E^\times_\mathcal{Q});$$

we know by [Frö83, Theorem 12(ii)] that

$$\mathrm{coinf}\, \mathcal{RT}^\star_{F_\wp}(L') \in \mathrm{Det}(\mathfrak{O}_{E^1_\mathcal{Q}}[G(\wp)]^\times). \tag{10}$$

We now show the following result.

Lemma 3.15. *Let K be a finite Galois extension of $\mathbb{Q}_p$, and let $L_2/L_1/K$ be a tower of abelian extensions such that L_2/K is weakly ramified. Set $G_1 = \mathrm{Gal}(L_1/K)$ and $G_2 = \mathrm{Gal}(L_2/K)$. Then there exists $v \in \mathfrak{O}_K[G_1]^\times$ such that*

$$\mathrm{coinf}\, \mathcal{RT}^\star_K(L_2) = \mathcal{RT}^\star_K(L_1)\, \mathrm{Det}(v).$$

Proof. For $\chi \in R_{G_1,p}$, one has

$$\begin{aligned}\mathrm{coinf}\, \mathcal{RT}^\star_K(L_2)(\chi) &= \mathcal{RT}^\star_K(L_2)(\mathrm{inf}\, \chi)\\ &= \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_2} \mid \mathrm{inf}\, \chi)\tau^\star_K(\mathrm{inf}\, \chi - (\mathrm{inf}\, \chi)^2).\end{aligned}$$

We know that the Galois Gauss sum is inflation invariant (use (5) and see [Mar77, pp. 18 and 22]), that is, $\tau_K(\mathrm{inf}\, \chi) = \tau_K(\chi)$. The same clearly holds for the twisted Galois Gauss sum as well as for its modified version, thanks to (6) and the fact that

$$(\mathrm{inf}\, \chi)(c_{K,2}) = \chi(\theta_{L_2/K}(c_{K,2})|_{L_1}) = \chi(\theta_{L_1/K}(c_{K,2})) = \chi(c_{K,2}).$$

For the resolvent, we know by [Frö83, III, Lemma 1.5] (which is readily checked to apply to non-tame extensions) that

$$(\alpha_{L_2} \mid \mathrm{inf}\, \chi)_{G_2} = (\mathrm{Tr}_{L_2/L_1}(\alpha_{L_2}) \mid \chi)_{G_1},$$

where the subscripts stress the fact that the sums defining the two resolvents are not indexed by the same group. Further, since $\mathcal{A}_{L_1/K} = \mathrm{Tr}_{L_2/L_1}(\mathcal{A}_{L_2/K})$ (see [Ere91, § 5]), $\mathrm{Tr}_{L_2/L_1}(\alpha_{L_2})$ is a normal basis generator for $\mathcal{A}_{L_1/K}$, so there exists some $u \in \mathfrak{O}_K[G_1]^\times$ such that $\mathrm{Tr}_{L_2/L_1}(\alpha_{L_2}) = u\alpha_{L_1}$. As in formula (9), this yields

$$(\mathrm{Tr}_{L_2/L_1}(\alpha_{L_2}) \mid \chi) = (\alpha_{L_1} \mid \chi)\, \mathrm{Det}_\chi(u),$$

and so, for any transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$, we get

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_2} \mid \mathrm{inf}\, \chi) = \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_1} \mid \chi)\, \mathrm{Det}_\chi(v),$$

where $v = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)} u^\sigma \in \mathfrak{O}_K[G_1]^\times$. □

Proposition 3.13 now follows from Lemma 3.15 and (10). □

Since we have applied Corollary 3.4 to $F_\wp$ with uniformising parameter p, we know that $M_i \subseteq (F_\wp)_{p,2}$, and thus p belongs to the norm group $N_{M_i/K}(M_i^\times)$ of M_i/K by [Iwa86, Lemma 7.4].

Assuming Theorem 2, we get that $\mathcal{RT}^\star_{F_\wp}(M_i)=1$ for appropriate choices of α_{M_i}, of the transversal Ω of $\Omega_{F_\wp}$ in $\Omega_{\mathbb{Q}_p}$ that defines the norm-resolvent, and of the element $c_{F_\wp,2}$ of $\mathfrak{O}_{F_\wp}$ that defines the modified twisted Galois Gauss sum. Therefore, it follows from Proposition 3.13 that for $\wp\in S_W$,

$$\mathcal{RT}^\star_{F_\wp}(N_\mathfrak{P})\in \mathrm{Det}(\mathfrak{O}_{E^1_\mathfrak{Q}}[G(\wp)]^\times),$$

as asserted. We are left with proving Theorem 2, which is the goal of the next section.

4. The local computation

We fix a rational prime p and an unramified finite extension K of $\mathbb{Q}_p$; we denote by k its residue field and set $d=[K:\mathbb{Q}_p]=[k:\mathbb{Z}_p/p\mathbb{Z}_p]$. Let M be a cyclic wildly and weakly ramified extension of K, with Galois group H, such that p belongs to the norm group $N_{M/K}(M^\times)$ of M/K, i.e. $M\subset K_p$; thus M is one of the degree-p subextensions M_i of $K_{p,2}/K$ in Proposition 3.3 applied to $\pi=p$. It follows that M is the fixed subfield of $M_{p,2}/K$ by the kernel of an irreducible character χ of $\mathrm{Gal}(M_{p,2}/K)$, and the irreducible characters of H are the χ^j, for $0\leqslant j\leqslant p-1$ (χ^0 is the trivial character χ_0).

Let $0\leqslant j\leqslant p-1$; then $\mathcal{RT}^\star_K(M)(\chi^j)=\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M\mid\chi^j)\tau^\star_K(\chi^j-\chi^{2j})$. We first use the explicit construction from [Pic09] of a self-dual normal basis generator α_M for $\mathcal{A}_{M/K}$ over $\mathfrak{O}_K$ to calculate the norm-resolvent $\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M\mid\chi^j)$. We then calculate the modified twisted Galois Gauss sum $\tau^\star_K(\chi^j-\chi^{2j})$, and show that $\mathcal{RT}^\star_K(M)=1$ for appropriate choices of the transversal Ω defining the norm-resolvent and the element $c_{K,2}$ of K defining the modified Galois Gauss sum.

4.1 Dwork's exponential power series

Let $\gamma\in\mathbb{Q}_p^c$ be a root of the polynomial $X^{p-1}+p$ and note that, as this is an Eisenstein polynomial, γ will be a uniformising parameter of $K(\gamma)$.

DEFINITION 4.1. We define Dwork's exponential power series as

$$E_\gamma(X)=\exp(\gamma X-\gamma X^p),$$

where the right-hand side is to be thought of as the power series expansion of the exponential function.

Here we recall some important properties of Dwork's power series. Let $\mathbb{C}_p$ denote the completion of $\mathbb{Q}_p^c$ and $|\cdot|_p:\mathbb{C}_p\to\mathbb{R}$ its absolute value, such that $|p|_p=p^{-1}$. For instance,

$$|\gamma|_p=|N_{K(\gamma)/\mathbb{Q}_p}(\gamma)|_p^{1/[K(\gamma):\mathbb{Q}_p]}=|p|_p^{1/[K(\gamma):K]}=p^{-1/(p-1)},$$

where $N_{K(\gamma)/\mathbb{Q}_p}$ stands for the norm from $K(\gamma)$ to $\mathbb{Q}_p$. We denote by ord_p the associated valuation: for $a\in\mathbb{C}_p$, $|a|_p=p^{-\mathrm{ord}_p(a)}$. For $r\in\mathbb{R}$, let $D(r^-)=\{a\in\mathbb{C}_p:|a|_p<r\}$ (respectively, $D(r^+)=\{a\in\mathbb{C}_p:|a|_p\leqslant r\}$) denote the so-called open (respectively, closed) disc of radius r about 0.

The radius of convergence of a series $\sum_n a_nX^n$ with coefficients in $\mathbb{C}_p$ is $(\limsup|a_n|_p^{1/n})^{-1}$; it equals the largest real number r such that the series converges in $D(r^-)$ (see [Kob77, IV1]). From standard theory, we know that the radius of convergence of exp is $p^{-1/(p-1)}$. If we write $E_\gamma(X)=\sum_{n\geqslant0}e_nX^n$, then $|e_n|_p^{1/n}\leqslant p^{(1-p)/p^2}$ for all positive n by [Lan80, 14, Lemma 2.2(i)], and therefore the radius of convergence of E_γ is at least $p^{(p-1)/p^2}$. In particular, E_γ converges on $D(1^+)$ and hence on $\mathfrak{O}_K$. Note that one has $E_\gamma(a)=\exp(\gamma a-\gamma a^p)$ for $a\in D(1^-)$, because then $|\gamma a-\gamma a^p|_p=|\gamma a|_p<p^{-1/(p-1)}$, but this expression cannot be used when $|a|_p=1$: the image of

the unit circle of $\mathbb{C}_p$ under $\gamma X - \gamma X^p$ is not contained in the disc of convergence of exp. For such an a, only the series in the coefficients e_n is available.

Nevertheless, if $a \in D(1^+)$, then $|p\gamma a|_p \leqslant |p\gamma|_p < p^{-1/(p-1)}$, and the same holds for $|p\gamma a^p|_p$. Using the homomorphic property of the exponential power series, we deduce that

$$E_\gamma(a)^p = \exp(p\gamma a)\exp(-p\gamma a^p).$$

In particular, $E_\gamma(1)$ is a pth root of unity. By [Lan80, 14, Lemma 2.2(ii)] and the power series expansion of exp, we obtain

$$E_\gamma(X) \equiv 1 + \gamma X \bmod \gamma^2 \mathfrak{O}_{\mathbb{Q}_p(\gamma)}[[X]]. \tag{11}$$

This shows that $E_\gamma(1)$ is in fact a primitive pth root of unity. Further, the different choices of γ correspond to different choices of this root of unity; therefore we may choose γ so that $E_\gamma(1) = \zeta$, where ζ was defined in § 3.2. We remark that $[K(\zeta) : K] = [K(\gamma) : K]$ and $\zeta \in K(\gamma)$, and therefore $K(\gamma) = K(\zeta)$; we shall now denote this field by K'.

Formula (11) also shows that if we let $u \in \mathfrak{O}_K$ be a unit, then $E_\gamma(u) - 1$ is a uniformising parameter in K'.

Let $\mu \in \mathbb{Z}_p$ and set $B_\mu(X) = \sum_{n\geqslant 0}(\mu(\mu-1)\cdots(\mu-n+1)/n!)X^n$. This series belongs to $\mathbb{Z}_p[[X]]$ and converges on $D(1^-)$; see [Kob77, p. 81]. For any sequence of rational integers $(\mu_i)_i$ converging towards μ, one has $B_\mu(X) = \lim_i B_{\mu_i}(X)$ (coefficient-wise). Further, the μ_i can be taken to be positive, in which case $B_{\mu_i}(X) = (1+X)^{\mu_i}$, so that we may abbreviate the notation and write $B_\mu(X) = (1+X)^\mu$. Using the fact that $\exp(X)^{\mu_i} = \exp(\mu_i X)$ for every i, and taking the limit of the coefficients as i goes to infinity, one deduces that

$$\exp(\mu X) = \exp(X)^\mu.$$

We consider the power series $E_\gamma(X)^\mu = B_\mu(E_\gamma(X) - 1)$ and, using (11), see that it converges on $D(1^+)$. Substituting μX for X in E_γ yields a power series $E_\gamma(\mu X)$ that also converges on $D(1^+)$. Further, let μ_{p-1} denote the subgroup of $\mathbb{Z}_p^\times$ of $(p-1)$th roots of unity. Then we get the following result.

Lemma 4.2. *Let $\mu \in \mu_{p-1}$; then $E_\gamma(\mu X) = E_\gamma(X)^\mu$.*

Proof. The result is straightforward, since

$$\exp(\gamma\mu X - \gamma(\mu X)^p) = \exp(\mu(\gamma X - \gamma X^p)) = \exp(\gamma X - \gamma X^p)^\mu. \qquad \square$$

4.2 The Kummer extensions in $K_{p,2}$

In this section we will sometimes identify the multiplicative groups of the residue fields k and $\mathbb{Z}_p/p\mathbb{Z}_p$ with their Teichmüller lifts; that is, letting μ_{q-1} and μ_{p-1} denote the groups of roots of unity of order prime to p in K and $\mathbb{Q}_p$, respectively, we have $k^\times \cong \mu_{q-1}$ and $(\mathbb{Z}_p/p\mathbb{Z}_p)^\times \cong \mu_{p-1}$. Specifically,

$$\mathfrak{O}_K^\times = \mu_{q-1} \times (1 + p\mathfrak{O}_K) \quad \text{and} \quad \mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p).$$

Since $K/\mathbb{Q}_p$ is unramified, we shall also identify its Galois group and that of the residue extension, and set $\Sigma = \mathrm{Gal}(k/(\mathbb{Z}_p/p\mathbb{Z}_p)) = \mathrm{Gal}(K/\mathbb{Q}_p)$.

We now let η be a normal basis generator for k over $\mathbb{Z}_p/p\mathbb{Z}_p$ and, as described, we will often think of η as actually lying in $\mathfrak{O}_K^\times$. The conjugates of η under Σ are the η^{p^j}, $0 \leqslant j \leqslant d-1$, so each $u \in k$ has a unique decomposition

$$u = \sum_{j=0}^{d-1} u_j \eta^{p^j}$$

with coefficients $u_j \in \mathbb{Z}_p/p\mathbb{Z}_p$. For ease of notation we identify $0 \in \mathbb{Z}_p/p\mathbb{Z}_p$ and $0 \in \mathfrak{O}_K$, so that each $u_j \in \mathbb{Z}_p/p\mathbb{Z}_p$ can be seen as an element $u_j \in \{0\} \cup \mu_{p-1} \subset \mathbb{Z}_p$. To $u \in k$ as above we associate

$$x_u = \prod_{j=0}^{d-1} E_\gamma(\eta^{p^j})^{u_j} = \prod_{j=0}^{d-1} E_\gamma(u_j \eta^{p^j}) \in K' \tag{12}$$

(recall that K' contains γ and is a complete field). The second equality comes from Lemma 4.2; note that x_u does not equal $E_\gamma(u)$ since E_γ is not a group homomorphism on the additive group $D(1)^+$. Further, $x_0 = 1$, and when $u \in k^\times$ it follows from (11) that $x_u \equiv 1 + \gamma u \bmod \gamma^2 \mathfrak{O}_{K'}$, so that $x_u - 1$ is a uniformising parameter in K'.

Proposition 4.3. *There are exactly $r = (p^d - 1)/(p-1)$ degree-p extensions of K' contained in $K_{p,2}$, given by $L_i = K'M_i$, $1 \leqslant i \leqslant r$. Further, $k^\times/(\mathbb{Z}_p/p\mathbb{Z}_p)^\times$ is in one-to-one correspondence with the set $\{L_i : 1 \leqslant i \leqslant r\}$ via the map $\bar{u} \mapsto K'(x_u^{1/p})$.*

Proof. From [Pic09, Theorem 5], we know that every degree-p extension of K' contained in $K_{p,2}$ is generated by the pth root of an element $\prod_{j=0}^{d-1} E_\gamma(\eta^{p^j})^{n_j}$, with exponents $n_j \in \{0, 1, \ldots, p-1\}$ which are not all zero. (In fact, the statement in [Pic09] requires one element in the basis of k over $\mathbb{Z}_p/p\mathbb{Z}_p$ to equal 1, but this is never used in the proof, so we can use a normal basis here instead.) To such an element corresponds a unique $u = \sum_j u_j \eta^{p^j} \in k^\times$, where u_j is the coset of n_j modulo $p\mathbb{Z}_p$. Let us lift each u_j in $\{0\} \cup \mu_{p-1} \subset \mathbb{Z}_p$ and write $u_j = n_j + pm_j$ with $m_j \in \mathbb{Z}_p$; then

$$x_u = \prod_{j=0}^{d-1} E_\gamma(\eta^{p^j})^{n_j} \cdot \left(\prod_{j=0}^{d-1} E_\gamma(\eta^{p^j})^{m_j} \right)^p.$$

We conclude that the degree-p extensions of K' contained in $K_{p,2}$ are the $L_{(u)} = K'(x_u^{1/p})$ for $u \in k^\times$.

Multiplying u by an element μ in $(\mathbb{Z}_p/p\mathbb{Z}_p)^\times$ changes x_u to $x_{\mu u} = {x_u}^\mu$. If we let $\mu = n + p\mu'$ with $n \in \{1, \ldots, p-1\}$ and $\mu' \in \mathbb{Z}_p$, we find that $x_{\mu u}$ equals a prime-to-p power of x_u multiplied by the pth power of an element of K', so its pth root generates the same extension of K' as that of x_u. Therefore the map given in the statement is well defined and surjective. For any integer $1 \leqslant i \leqslant r$, the compositum $M_iK' = L_i$ is a degree-p extension of K' contained in $K_{p,2}$, so we get that the map is a one-to-one correspondence. □

Remark 4.4. Keeping the notation used in the proof, it would be nice to show that $L_{(u)}$ is also generated by the pth root of $E_\gamma(u)$. We would then get a generating set (for the degree-p extensions of K' contained in $K_{p,2}$) that would not depend on the choice of a basis of k over $\mathbb{Z}_p/p\mathbb{Z}_p$. However, the fact that E_γ is not homomorphic on the additive group $D(1)^+$ does not make this goal easy to achieve.

4.3 Lifting Galois automorphisms

We now set $L = K'M$; thus, by the former result, $L = K'(x_\varepsilon^{1/p})$ for an element ε of $k^\times$ which is uniquely determined modulo $(\mathbb{Z}_p/p\mathbb{Z}_p)^\times$ by M. We fix ε for the rest of the paper and set $x = x_\varepsilon$ for brevity. We describe our field extensions in Figure 1, where we let $H = \mathrm{Gal}(M/K)$ and $\Delta = \mathrm{Gal}(L/M)$.

We need to study how the elements of $\mathrm{Gal}(K'/K)$ and $\Sigma' = \mathrm{Gal}(K'/\mathbb{Q}_p(\zeta))$ can be lifted, respectively, to automorphisms of L (recall that $L \subset K^{\mathrm{ab}}$) and of the Galois closure $\widetilde{L}$ of $L/\mathbb{Q}_p(\zeta)$.

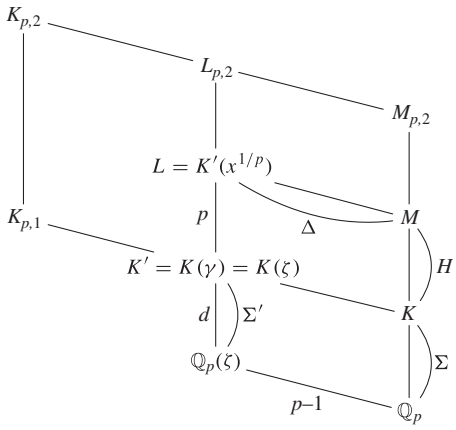


FIGURE 1. Extensions diagram.

We have the following group isomorphisms:

$$\begin{array}{ccccc} \mu_{p-1} & \cong & (\mathbb{Z}_p/p\mathbb{Z}_p)^\times & \cong & \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) \cong \mathrm{Gal}(K'/K) \\ \mu & \longmapsto & \mu \bmod p & \longmapsto & (s_\mu : \zeta \mapsto \zeta^\mu). \end{array}$$

As a consequence of (11) in § 4.1, we know that $x-1$ is a uniformising parameter of K. As noted in [Pic09] before Lemma 9, this implies that $x^{1/p}-1$ is a uniformising parameter of L. It follows that both $x-1$ and $x^{1/p}-1$ belong to $D(1^-)$, so we may consider raising x and $x^{1/p}$ to the μth power for any $\mu \in \mathbb{Z}_p$. [Pic09, Lemma 10] applied to x (with appropriate choices of the exponents n_i) yields that, for any $\mu \in \mu_{p-1}$,

$$s_\mu(x) = x^\mu.$$

Since $[L : K'] = p$, each automorphism $s_\mu \in \mathrm{Gal}(K'/K)$ has p distinct liftings in $\mathrm{Gal}(L/K)$, which are determined by their value at $x^{1/p}$. More precisely, let us fix a pth root of $s_\mu(x)$ in L, by setting

$$s_\mu(x)^{1/p} = (x^{1/p})^\mu = x^{\mu/p}$$

where $x^{1/p}$ is our previous (implicit) choice of a pth root of x. Any lifting $\widetilde{s}$ of s_μ satisfies $\widetilde{s}(x^{1/p})^p = s_\mu(x)$, so there exists an integer $n \in \{0, \dots, p-1\}$ such that $\widetilde{s}(x^{1/p}) = \zeta^n s_\mu(x)^{1/p}$, and n determines $\widetilde{s}$. One easily checks that, for any integer k,

$$\widetilde{s}^k(x^{1/p}) = \zeta^{nk\mu^{k-1}} x^{\mu^k/p},$$

so $\widetilde{s}^{p-1} = 1$ if and only if $n = 0$. Further, in this case, one obtains that $\widetilde{s}$ has the same order in $\mathrm{Gal}(L/K)$ as μ does in μ_{p-1}. We have thus proved the following result.

PROPOSITION 4.5. *Let μ denote a primitive $(p-1)$th root of unity. Then $\mathrm{Gal}(L/K)$ contains exactly one element $\widetilde{s}_\mu$ that maps ζ to ζ^μ, is of order $p-1$, and hence generates Δ and fixes M. Further, $\widetilde{s}_\mu(x^{1/p}) = x^{\mu/p}$.*

We now consider extending automorphisms in $\Sigma' = \mathrm{Gal}(K'/\mathbb{Q}_p(\zeta))$. Since γ is fixed by Σ', one checks that $\sigma(x) = x_{\sigma(\varepsilon)}$ for any $\sigma \in \Sigma'$. Therefore, by Kummer theory, $L/\mathbb{Q}_p(\zeta)$ is Galois if and only if every $x_{\sigma(\varepsilon)}$ can be written as $x^m y^p$ for some integer m prime to p and some $y \in K'$. Using the fact that the elements of Σ' act on η by raising it to its p^nth power for $n \in \{0, 1, \dots, d-1\}$, one then checks that this only happens when $\varepsilon = t \sum_{n=0}^{d-1} s^{d-n-1} \eta^{p^n}$ for some $s, t \in (\mathbb{Z}_p/p\mathbb{Z}_p)^\times$

with s of order dividing d. In particular, $s=1$ yields $L=K(\xi)=K\cdot\mathbb{Q}_p(\xi)$, which is always Galois over $\mathbb{Q}_p(\zeta)$; recall that ξ and ζ were defined in (3).

Since $L/\mathbb{Q}_p(\zeta)$ is not Galois in the general case, we consider the Galois closure $\widetilde{L}$ of $L/\mathbb{Q}_p(\zeta)$, given by $\widetilde{L}=K'(\{\sigma(x)^{1/p}:\sigma\in\Sigma'\})$. The extension $\widetilde{L}/K'$ is Kummer and its Galois group is p-elementary abelian, of order p^m for some integer m (equal to 1 if and only if $L/\mathbb{Q}_p(\zeta)$ is Galois). Let $\sigma_1=1$ and $\sigma_2,\dots,\sigma_m\in\Sigma'$ be such that $\widetilde{L}$ is the compositum of the m degree-p extensions $K'(\sigma_n(x)^{1/p})$, $1\leqslant n\leqslant m$, of K'. Any $\sigma\in\Sigma'$ extends to $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}_p(\zeta))$ in $p^m=[\widetilde{L}:K']$ different ways, determined by the values at the $\sigma_n(x)^{1/p}$, $1\leqslant n\leqslant m$. More precisely, let us fix a pth root of $\sigma\sigma_n(x)$ for each $n\in\{1,\dots,m\}$; then a lifting $\widetilde{\sigma}$ of σ is determined by the integers $k(n)\in\{0,1,\dots,p-1\}$ such that, for any n, $\widetilde{\sigma}(\sigma_n(x)^{1/p})=\zeta^{k(n)}(\sigma\sigma_n(x))^{1/p}$. The choices of the $k(n)$ for all the n yield the p^m possible liftings of σ; hence each of these choices is realised. In particular, taking $k(1)=0$, we see that there exists a lifting $\widetilde{\sigma}$ of σ to $\widetilde{L}$ such that

$$\widetilde{\sigma}(x^{1/p})=\sigma(x)^{1/p} \tag{13}$$

for any prior choice of a pth root of $\sigma(x)$. We deduce the following result, where $N_{K'/\mathbb{Q}_p(\zeta)}(x)$ denotes the norm of x from K' to $\mathbb{Q}_p(\zeta)$.

Proposition 4.6. *For any choice of a pth root of $N_{K'/\mathbb{Q}_p(\zeta)}(x)$, there exists a transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$ such that each $\omega\in\Omega$ fixes ζ and*

$$\prod_{\omega\in\Omega}(x^{1/p})^{\omega}=N_{K'/\mathbb{Q}_p(\zeta)}(x)^{1/p}.$$

Proof. Since $K/\mathbb{Q}_p$ is Galois, choosing a transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$ is the same as choosing a way to extend the elements of $\Sigma=\mathrm{Gal}(K/\mathbb{Q}_p)$ to act on $\mathbb{Q}_p^{\mathrm{c}}$. By Galois theory, we know that there is only one way to extend these to Σ'. Let $\sigma\in\Sigma'$; then for any choice of a pth root of $\sigma(x)$, there exists $\omega_\sigma\in\Omega_{\mathbb{Q}_p}$ that extends the lifting $\widetilde{\sigma}$ of σ defined in (13), namely

$$(x^{1/p})^{\omega_\sigma}=\widetilde{\sigma}(x^{1/p})=\sigma(x)^{1/p}.$$

The set $\Omega=\{\omega_\sigma:\sigma\in\Sigma'\}$ defined this way is a transversal of Ω_K in $\Omega_{\mathbb{Q}_p}$, and

$$\prod_{\omega\in\Omega}(x^{1/p})^{\omega}=\prod_{\sigma\in\Sigma'}\sigma(x)^{1/p},$$

which can be made to equal any pth root of $N_{K'/\mathbb{Q}_p(\zeta)}(x)$ for a suitable choice of the pth roots of the $\sigma(x)$, $\sigma\in\Sigma'$. By construction, the restriction of each $\omega\in\Omega$ to K' belongs to Σ' and hence fixes ζ. □

4.4 The norm-resolvent

We begin by exhibiting a (self-dual) normal basis generator for the square root of the inverse different $\mathcal{A}_{M/K}$, which we then use to compute the norm-resolvent involved in $\mathcal{RT}^{\star}_K(M)$. Recall that x was defined at the beginning of § 4.3.

Lemma 4.7. *Let*

$$\alpha_M=\frac{1+\mathrm{Tr}_\Delta(x^{1/p})}{p}.$$

Then α_M is a self-dual normal basis generator for $\mathcal{A}_{M/K}$.

Proof. This lemma is a consequence of [Pic09, Theorem 12]. □

The extension L/K' is Kummer with generator $x^{1/p}$, so its Galois group is generated by the automorphism defined by $x^{1/p} \mapsto \zeta x^{1/p}$. Further, by Galois theory, the restriction of this automorphism to M generates $H = \mathrm{Gal}(M/K)$. This enables us to fix a generator h of H and the irreducible character χ of $\mathrm{Gal}(M/K)$ such that M is the fixed subfield of $M_{p,2}$ by $\ker(\chi)$ (this condition only determines χ up to a prime-to-p power).

Notation 4.8. Let $\widetilde{h} \in \mathrm{Gal}(L/K')$ be such that $\widetilde{h}(x^{1/p}) = \zeta x^{1/p}$ and set $h = \widetilde{h}|_M$. Let χ be the irreducible character of $\mathrm{Gal}(M_{p,2}/K)$ such that $\ker(\chi) = \mathrm{Gal}(M_{p,2}/M)$ and $\chi(h) = \zeta$.

We can now state the theorem that we will prove in this subsection. Recall the notation from (3) and the fact that $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}_p}$.

Theorem 4.9. *There exists a choice of the transversal Ω defining the norm-resolvent such that $\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi_0) = 1$ and, for any $j \in \{1, \dots, p-1\}$,*

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi^j) = \xi^{j(2-j^{1-p})\mathrm{Tr}(\varepsilon)},$$

where j^{1-p} is the inverse of j^{p-1} in $\mathbb{Z}_p$.

Before we can prove this theorem, we must derive the properties of certain elements. We begin with the calculation of the norm $N_{K'/\mathbb{Q}_p(\zeta)}(x)$, which establishes a new link between x and ε.

Lemma 4.10. *The norm of x from K' to $\mathbb{Q}_p(\zeta)$ can be expressed as $N_{K'/\mathbb{Q}_p(\zeta)}(x) = \zeta^{\mathrm{Tr}(\varepsilon)}$.*

Proof. Recall that $\Sigma' = \mathrm{Gal}(K'/\mathbb{Q}_p(\zeta))$ fixes $\gamma \in \mathbb{Q}_p(\zeta)$; so, if $\sigma \in \Sigma'$ and $u \in \mathfrak{O}_K$, $\sigma(E_\gamma(u)) = E_\gamma(\sigma(u))$. Further, σ acts on η by raising it to the power p^n for some $0 \leqslant n \leqslant d-1$, and it fixes μ_{p-1}. Therefore, writing $\varepsilon = \sum_j e_j \eta^{p^j}$ with coefficients $e_j \in \mathbb{Z}_p/p\mathbb{Z}_p$, we have

$$N_{K'/\mathbb{Q}_p(\zeta)}(x) = \prod_{n=0}^{d-1} \prod_{j=0}^{d-1} E_\gamma(\eta^{p^{n+j}})^{e_j}.$$

For each $0 \leqslant j, n \leqslant d-1$, consider the power series $E_\gamma(\eta^{p^{n+j}} X)$ obtained by substituting $\eta^{p^{n+j}} X$ for X in E_γ; it converges on $D(1^+)$, and

$$\begin{aligned}\prod_{n=0}^{d-1} E_\gamma(\eta^{p^{n+j}} X) &= \exp\left(\sum_{n=0}^{d-1} (\gamma \eta^{p^{n+j}} X - \gamma \eta^{p^{n+j+1}} X^p) \right) \\ &= \exp(\mathrm{Tr}(\eta)(\gamma X - \gamma X^p)) \\ &= E_\gamma(X)^{\mathrm{Tr}(\eta)},\end{aligned}$$

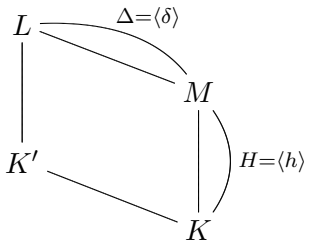
which also converges on $D(1^+)$. Evaluating at $X = 1$ and using the above formula for the norm yields the result, since $\mathrm{Tr}(\varepsilon) = \mathrm{Tr}(\eta) \sum_j e_j$. □

In view of Proposition 4.6, we now fix our transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$ so that each $\omega \in \Omega$ fixes ζ and the product of the Ω-conjugates of $x^{1/p}$ equals $\xi^{\mathrm{Tr}(\varepsilon)}$, which is a pth root of $N_{K'/\mathbb{Q}_p(\zeta)}(x)$ by the preceding lemma. We then get the following result.

Lemma 4.11. *We have $\prod_{\omega \in \Omega} (x^{1/p})^\omega = \xi^{\mathrm{Tr}(\varepsilon)}$.*

Recall that $\mathrm{Gal}(M/K) = H = \langle h \rangle$, where h is as in Notation 4.8. Let $\mathrm{Gal}(L/M) = \Delta = \langle \delta \rangle$; then, by Proposition 4.5, $\delta = \widetilde{s}_\mu$ for some primitive $(p-1)$th root of unity μ, and also $\delta(\zeta) = \zeta^\mu$

and $\delta(x^{1/p}) = x^{\mu/p}$. We have the following diagram.



We now compute the resolvent for the normal basis generator α_M that was defined in Lemma 4.7.

PROPOSITION 4.12. *One has* $(\alpha_M \mid \chi_0) = 1$ *and, for* $j \in \{1, \dots, p-1\}$,

$$(\alpha_M \mid \chi^j) = (x^{1/p})^{\mu^s},$$

where $0 \leqslant s \leqslant p-2$ *is such that* $\mu^s \equiv j \bmod p$.

Proof. The definitions of the resolvent and α_M yield

$$(\alpha_M \mid \chi^j) = \sum_{t=0}^{p-1} \frac{1 + h^t(\mathrm{Tr}_\Delta(x^{1/p}))}{p} \chi^j(h^{-t}).$$

Let $t \in \{0, 1, \dots, p-1\}$; then

$$h^t(\mathrm{Tr}_\Delta(x^{1/p})) = \sum_{s=0}^{p-2} \widetilde{h}^t((x^{1/p})^{\mu^s}) = \sum_{s=0}^{p-2} \zeta^{t\mu^s} (x^{1/p})^{\mu^s}.$$

If $j = 0$, then χ^j is the trivial character χ_0, so that

$$(\alpha_M \mid \chi_0) = 1 + \frac{1}{p} \sum_{t=0}^{p-1} \sum_{s=0}^{p-2} \zeta^{t\mu^s} (x^{1/p})^{\mu^s} = 1 + \frac{1}{p} \sum_{s=0}^{p-2} \left(\sum_{t=0}^{p-1} \zeta^{t\mu^s} \right) (x^{1/p})^{\mu^s}$$

and $\sum_{t=0}^{p-1} \zeta^{t\mu^s} = 0$; hence $(\alpha_M \mid \chi_0) = 1$.

We now assume $j \neq 0$. Since $\chi^j(h) = \zeta^j$, and hence $\sum_{t=0}^{p-1} \chi^j(h^{-t}) = 0$, we get

$$(\alpha_M \mid \chi^j) = \frac{1}{p} \sum_{s=0}^{p-2} \left(\sum_{t=0}^{p-1} \zeta^{t(\mu^s - j)} \right) (x^{1/p})^{\mu^s}.$$

We observe that

$$\sum_{t=0}^{p-1} \zeta^{t(\mu^s - j)} = \begin{cases} p & \text{if } \mu^s \equiv j \bmod p, \\ 0 & \text{otherwise,} \end{cases}$$

and the result follows. □

We are now in a position to prove Theorem 4.9.

Proof of Theorem 4.9. When $j = 0$, the result is clear. We now assume that $j \neq 0$. Recall the choice we made before Lemma 4.11 for our transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$. Since χ^j takes values in $\mathbb{Q}_p(\zeta)$, which is fixed by Ω, Definition 2.2 of the norm-resolvent yields

$$\begin{aligned} \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi^j) &= \prod_\Omega (\alpha_M \mid \chi^j)^\omega = \prod_\Omega ((x^{1/p})^{\mu^s})^\omega \\ &= \left(\prod_\Omega (x^{1/p})^\omega \right)^{\mu^s} = \xi^{\mu^s \mathrm{Tr}(\varepsilon)}, \end{aligned}$$

using Lemma 4.11. Writing $\mu^s \equiv j + ap \bmod p^2$ for some $a \in \{0, 1, \dots, p-1\}$ and raising to the $(p-1)$th power gives $1 \equiv j^{p-1} - apj^{p-2} \bmod p^2$; thus

$$ap \equiv (j^{p-1} - 1)j^{2-p} \equiv j - j^{2-p} \bmod p^2.$$

It follows that $\mu^s \equiv j(2 - j^{1-p}) \bmod p^2$, which ends the proof of Theorem 4.9. □

4.5 The modified twisted Galois Gauss Sum

Recall from Notation 4.8 that χ is the character of $\mathrm{Gal}(M_{p,2}/K)$ such that M is the fixed field of $\ker(\chi)$ and $\chi(h) = \zeta$ for our choice of generator h of $H = \mathrm{Gal}(M/K)$. Our character χ is weakly ramified, so we know from Corollary 3.10 that there exists $v \in \mathfrak{O}_K^\times$ such that

$$\chi(1 + up)^{-1} = \zeta^{\mathrm{Tr}(uv)} \quad \text{for all } u \in \mathfrak{O}_K. \tag{14}$$

We are going to show that v can be chosen so that its trace from K to $\mathbb{Q}_p$ equals that of ε. In order to do that, we need some properties of the pth Hilbert symbol (see [FV02, ch. IV]). We have $\mathrm{char}(K') = 0$ and $\zeta \in K'$. Let $\mu_p = \langle \zeta \rangle$ denote the group of pth roots of unity in $\mathbb{Q}_p^c$. The pth Hilbert symbol of K' is defined as

$$\begin{array}{rccc} (\ ,\ )_{p,K'}: & K'^\times \times K'^\times & \longrightarrow & \mu_p \\ & (a, b) & \longmapsto & \dfrac{\theta_{K'}(a)(b^{1/p})}{b^{1/p}}. \end{array}$$

Proposition 4.13. *For all $u \in \mathfrak{O}_K$, we have*

$$(1 + up, x)_{p,K'} = \chi(1 + up)^{-1}.$$

Proof. The proof proceeds in several steps. Let $L_{p,2}$ be the compositum of the fields L_i for $i \in \{1, \dots, r\}$. Recall that we identify the residue field $k = \{0\} \cup k^\times$ with $\{0\} \cup \mu_{q-1} \subset \mathfrak{O}_K$ through Teichmüller's lifting. We first show the following equalities.

Lemma 4.14. *We have* $\mathrm{Gal}(L_{p,2}/K') = \theta_{L_{p,2}/K'}(U_K^1/U_K^2) = \{\theta_{L_{p,2}/K'}(1 + up) : u \in k\}$.

Proof. First, note that $L_{p,2} \subset K_{p,2}$; so $\theta_{L_{p,2}/K}$ is trivial on U_K^2 and the same holds for $\theta_{L_{p,2}/K'}$ (for instance by using [Iwa86, Theorem 6.16]). Hence we may consider $\theta_{L_{p,2}/K'}(U_K^1/U_K^2)$, which, as a set, clearly equals $\{\theta_{L_{p,2}/K'}(1 + up) : u \in k\}$.

By local class field theory, $\mathrm{Gal}(M_{p,2}/K) = \theta_{M_{p,2}/K}(U_K^1)$ and the intersection of the kernel of $\theta_{M_{p,2}/K}$ with U_K^1 is U_K^2 (since $M_{p,2} \subset K_{p,2}$ and $[M : K] = q$). It follows that $\mathrm{Gal}(M_{p,2}/K) = \theta_{M_{p,2}/K}(U_K^1/U_K^2)$.

Since $L_{p,2} = M_{p,2}K'$ with K'/K and $M_{p,2}/K$ linearly disjoint, the functorial properties of the Artin reciprocity map yield

$$\theta_{L_{p,2}/K'}|_{M_{p,2}} = \theta_{M_{p,2}/K} \circ N_{K'/K} \tag{15}$$

(see [Iwa86, Theorem 6.9]), where $N_{K'/K}$ stands for the norm from K' to K. For $u \in k$ we have $1 + up \in \mathfrak{O}_K$, so $N_{K'/K}(1 + up) = (1 + up)^{p-1} \equiv 1 - up \bmod p^2\mathfrak{O}_K$. We get that $N_{K'/K}$ is an isomorphism from U_K^1/U_K^2 into itself, and therefore

$$\theta_{L_{p,2}/K'}(U_K^1/U_K^2)\big|_{M_{p,2}} = \mathrm{Gal}(M_{p,2}/K).$$

This yields the result using Galois theory, since the restriction map $g \mapsto g|_{M_{p,2}}$ is an isomorphism from $\mathrm{Gal}(L_{p,2}/K')$ to $\mathrm{Gal}(M_{p,2}/K)$. □

Lemma 4.15. *There exists $t \in \{1, \dots, p-1\}$ such that, for all $u \in k$,*

$$(1 + up, x)_{p,K'}^t = \chi(1 + up)^{-1}.$$

Proof. By definition, $\chi(1-up)=1$ if and only if $\theta_{M_{p,2}/K}(1-up)$ fixes M. This, in turn, is equivalent to $\theta_{L_{p,2}/K'}(1+up)$ fixing L, since $L=MK'$ and we know by (15) that $\theta_{L_{p,2}/K'}(1+up)$ is the only lifting of $\theta_{M_{p,2}/K}(1-up)$ to $L_{p,2}/K'$. Using $L=K'(x^{1/p})$ and the definition of the Hilbert symbol, we get

$$\chi(1-up)=1 \iff (1+up,x)_{p,K'}=1.$$

The properties of the Hilbert symbol and the fact that $\theta_{L_{p,2}/K'}$ is trivial on U_K^2 give us

$$\begin{aligned}(1+up,x)_{p,K'}(1+u'p,x)_{p,K'} &= (1+up+u'p+uu'p^2,x)_{p,K'}\\ &= (1+(u+u')p,x)_{p,K'}\end{aligned}$$

for $u,u'\in k$, which means that $u\mapsto(1+up,x)_{p,K'}$ is a character of the additive group of k. We also know that $u\mapsto\chi(1-up)$ is a character of the additive group of k (since $u\mapsto\theta_{M_{p,2}/K}(1-up)$ is). Therefore $u\mapsto(1+up,x)_{p,K'}$ and $u\mapsto\chi(1-up)$ are characters of the same p-elementary abelian group which have the same kernel of index p. It follows that $(1+up,x)_{p,K'}^t=\chi(1-up)=\chi(1+up)^{-1}$ for some t. □

To finish the proof of Proposition 4.13, note that the arguments in the proof of Lemma 4.14 can be adjusted to show that $\mathrm{Gal}(L/K')=\langle\theta_{L/K'}(1+ap)\rangle$ for an appropriate element $a\in\mathfrak{O}_K$. Hence there exists an integer $n\in\{1,\dots,p-1\}$ such that

$$\widetilde{h}=\theta_{L/K'}(1+ap)^n=\theta_{L/K'}((1+ap)^n)=\theta_{L/K'}(1+wp+p^2b)$$

for some $b\in\mathfrak{O}_K$, where we let $w\in\mu_{q-1}$ be such that $w\equiv na \bmod p\mathbb{Z}_p$. Since $\theta_{L/K'}(1+wp+p^2b)|_M=\theta_{M/K}(1-wp)=\theta_{L/K'}(1+wp)|_M$, we get that

$$\widetilde{h}=\theta_{L/K'}(1+wp)\quad\text{and}\quad h=\widetilde{h}|_M=\theta_{M/K}(1-wp);$$

hence

$$\chi(1+wp)^{-1}=\chi(1-wp)=\chi(h)=\zeta=\frac{\widetilde{h}(x^{1/p})}{x^{1/p}}=(1+wp,x)_{p,K'},$$

which implies $t=1$ in the preceding lemma. □

We can now show the announced result, recalling that $\mathrm{Tr}=\mathrm{Tr}_{K/\mathbb{Q}_p}$.

COROLLARY 4.16. *There exists $v_\chi\in\mathfrak{O}_K^\times$ such that v_χ satisfies condition (14) from Corollary 3.10 for χ and $\mathrm{Tr}(v_\chi)=\mathrm{Tr}(\varepsilon)$.*

Proof. Throughout this proof we fix $u\in\mathbb{Z}_p/p\mathbb{Z}_p$. We let $\mathrm{ver}:\Omega^{\mathrm{ab}}_{\mathbb{Q}_p}\to\Omega^{\mathrm{ab}}_{\mathbb{Q}_p(\zeta)}$ be the transfer map from $\mathbb{Q}_p$ to $\mathbb{Q}_p(\zeta)$. From [Iwa86, Theorem 6.16 and (3), p. 93], where ver is written as $t_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}$, we know that

$$\theta_{\mathbb{Q}_p(\zeta)}(1+up)=\mathrm{ver}(\theta_{\mathbb{Q}_p}(1+up))=\prod_{\tau\in\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)}\tau\theta_{\mathbb{Q}_p}(1+up)\tau^{-1}.$$

As $\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ and $\Omega^{\mathrm{ab}}_{\mathbb{Q}_p}$ commute, we get $\theta_{\mathbb{Q}_p(\zeta)}(1+up)=\theta_{\mathbb{Q}_p}(1+up)^{p-1}$. By [Ser67, § 3.1, Remark after Theorem 2], we know that $\theta_{\mathbb{Q}_p}(1+up)(\xi)=\xi^{1-up}$, so that

$$\theta_{\mathbb{Q}_p(\zeta)}(1+up)(\xi)=\xi^{1+up}. \tag{16}$$

Using the properties of the Hilbert symbol, we make the following derivation:

$$\begin{aligned}(1+up,x)_{p,K'} &= (1+up, N_{K'/\mathbb{Q}_p(\zeta)}(x))_{p,\mathbb{Q}_p(\zeta)} && \text{(from [FV02, IV, § 5])}\\ &= (1+up,\zeta^{\mathrm{Tr}(\varepsilon)})_{p,\mathbb{Q}_p(\zeta)} && \text{(from Lemma 4.10)}\\ &= (1+up,\zeta)_{p,\mathbb{Q}_p(\zeta)}^{\mathrm{Tr}(\varepsilon)} = \left(\frac{\theta_{\mathbb{Q}_p(\zeta)}(1+up)(\xi)}{\xi}\right)^{\mathrm{Tr}(\varepsilon)}\\ &= \left(\frac{\xi^{1+up}}{\xi}\right)^{\mathrm{Tr}(\varepsilon)} && \text{(from equation (16))}\\ &= (\xi^{up})^{\mathrm{Tr}(\varepsilon)} = \zeta^{u\mathrm{Tr}(\varepsilon)}.\end{aligned}$$

On the other hand, take $v\in\mathfrak{O}_K^\times$ satisfying condition (14). Then, from Proposition 4.13, we know that $(1+up,x)_{p,K'}=\chi(1+up)^{-1}=\zeta^{\mathrm{Tr}(uv)}$, and so we have

$$(1+up,x)_{p,K'}=\zeta^{u\mathrm{Tr}(v)}.$$

Comparing this with the former equality yields $\mathrm{Tr}(\varepsilon)\equiv\mathrm{Tr}(v)\bmod p\mathbb{Z}_p$, so let $a\in\mathbb{Z}_p$ be such that $\mathrm{Tr}(\varepsilon)=\mathrm{Tr}(v)+pa$. Since $K/\mathbb{Q}_p$ is unramified, there exists $b\in\mathfrak{O}_K$ such that $\mathrm{Tr}(b)=a$, so $\mathrm{Tr}(\varepsilon)=\mathrm{Tr}(v+pb)=\mathrm{Tr}(v_\chi)$ if we let $v_\chi=v+pb$, which proves the result using property (i) of Corollary 3.10. □

We deduce the following expression for the modified twisted Galois Gauss sum, using the statement and property (ii) of Corollary 3.10. Note that since $p\neq 2$, $(p^2/4v_\chi)\mathfrak{O}_K=\pi^2\mathfrak{D}_K$, so we may set $c_{K,2}=p^2/4v_\chi$.

Theorem 4.17. *Let v_χ be as in Corollary 4.16 and set $c_{K,2}=p^2/4v_\chi$. Then $\tau_K^\star(\chi_0-\chi_0^2)=1$ and, for any $j\in\{1,\dots,p-1\}$,*

$$\tau_K^\star(\chi^j-\chi^{2j})=\chi^j(j^{-1})\xi^{-j\mathrm{Tr}(\varepsilon)}.$$

The dependency relationships between our constants might look complicated, so let us try to sum up how we fixed them. Our primitive pth root of unity ζ came first; the extension M/K under study determined a unit ε up to $(\mathbb{Z}_p/p\mathbb{Z}_p)^\times$; we defined a Kummer generator x, then a generator h of $H=\mathrm{Gal}(M/K)$, and then a generator χ of $\widehat{H}$; with χ came the unit v_χ, but only modulo $p\mathfrak{O}_K$; the knowledge of ε enabled us to fix v_χ in Corollary 4.16 and, finally, $c_{K,2}$ in Theorem 4.17.

Apart from the dependency upon the choice of ζ, which is shared by the usual Galois Gauss sum, our modified Galois Gauss sum thus also depends on M. This does not prevent the deduction of Theorem 1 from Theorem 2, since only one extension $M_i/F_\wp$ has to be considered at each wildly and weakly ramified prime ideal $\wp$ of $\mathfrak{O}$.

4.6 The product

We can now end the proof of Theorem 2. By Theorems 4.9 and 4.17, the product of our norm-resolvent and modified twisted Galois Gauss sum is 1 when evaluated at the trivial character, and we have, for $j\in\{1,\dots,p-1\}$,

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M\mid\chi^j)\tau_K^\star(\chi^j-\chi^{2j})=(\chi(j^{-1})\zeta^{\mathrm{Tr}(\varepsilon)(1-j^{1-p})/p})^j.$$

Note that $1-j^{1-p}\in p\mathbb{Z}_p$. We now wish to show that the above expression equals 1. We are thus left with showing that $\chi(j)=\zeta^{\mathrm{Tr}(\varepsilon)(1-j^{1-p})/p}$, which is equivalent to $\theta_{M/K}(j)=h^{\mathrm{Tr}(\varepsilon)(1-j^{1-p})/p}$, since $h\in H$ is such that $\chi(h)=\zeta$. It is also equivalent to showing that

$$\theta_{M/K}(j)^{p-1}=h^{\mathrm{Tr}(\varepsilon)(j^{1-p}-1)/p}.$$

In order to shift this relation to $\mathrm{Gal}(L/K')$, we notice that $\theta_{M/K}(j)^{p-1} = \theta_{M/K}(N_{K'/K}(j)) = \theta_{L/K'}(j)|_M$ and recall that $\widetilde{h}|_M = h$. Thus the relation holds if and only if

$$\theta_{L/K'}(j) = \widetilde{h}^{\mathrm{Tr}(\varepsilon)(j^{1-p}-1)/p}.$$

We can now evaluate these automorphisms at $x^{1/p}$, recalling that $\widetilde{h}(x^{1/p}) = \zeta x^{1/p}$ and $(j,x)_{p,K'} = \theta_{L/K'}(j)(x^{1/p})/x^{1/p}$; so we are left with proving that

$$(j,x)_{p,K'} = \zeta^{\mathrm{Tr}(\varepsilon)(j^{1-p}-1)/p}.$$

Using Lemma 4.10 and the properties of the Hilbert symbol, we get

$$(j,x)_{p,K'} = (j, N_{K'/\mathbb{Q}_p(\zeta)}(x))_{p,\mathbb{Q}_p(\zeta)} = (j,\zeta)_{p,\mathbb{Q}_p(\zeta)}^{\mathrm{Tr}(\varepsilon)} = \left(\frac{\theta_{\mathbb{Q}_p(\zeta)}(j)(\xi)}{\xi}\right)^{\mathrm{Tr}(\varepsilon)}.$$

From [Ser67, § 3.1, Remark after Theorem 2] we know that $\theta_{\mathbb{Q}_p}(j)(\xi) = \xi^{-j}$. Therefore, reasoning as in the proof of Corollary 4.16, we get

$$\theta_{\mathbb{Q}_p(\zeta)}(j)(\xi) = (\mathrm{ver}\,\theta_{\mathbb{Q}_p}(j))(\xi) = \theta_{\mathbb{Q}_p}(j)^{p-1}(\xi) = \xi^{j^{-(p-1)}} = \xi^{j^{1-p}}$$

and hence

$$(j,x)_{p,K'} = (\xi^{j^{1-p}-1})^{\mathrm{Tr}(\varepsilon)} = (\zeta^{(j^{1-p}-1)/p})^{\mathrm{Tr}(\varepsilon)},$$

as desired.

This ends the proof of Theorem 2 and hence also that of Theorem 1.

Acknowledgements

The authors would like to express their deep gratitude to Philippe Cassou-Noguès and Martin J. Taylor for many useful comments and suggestions; specifically, Philippe Cassou-Noguès pointed out an embarrassing misuse of Fröhlich's Hom-description in the first version of this paper, and helped to solve the problem. The authors also thank Régis Blache for an enlightening discussion about p-adic analysis, as well as the anonymous referee for their very careful reading of the manuscript.

References

CT85 P. Cassou-Noguès and M. J. Taylor, *Opérations d'Adams et groupe des classes d'algèbre de groupe*, J. Algebra **95** (1985), 125–152.

Dwo64 B. Dwork, *On the zeta functions of a hypersurface. II*, Ann. of Math. (2) **80** (1964), 227–299.

Ere91 B. Erez, *The Galois structure of the square root of the inverse different*, Math. Z. **208** (1991), 239–255.

FV02 I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions*, second edition (American Mathematical Society, Providence, RI, 2002).

Frö83 A. Fröhlich, *Galois module structure of algebraic integers* (Springer, Berlin, 1983).

Iwa86 K. Iwasawa, *Local class field theory* (Oxford University Press, Oxford, 1986).

Kob77 N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Graduate Texts in Mathematics, vol. 58 (Springer, New York, 1977).

Lan80 S. Lang, *Cyclotomic fields II* (Springer, New York, 1980).

Mar77 J. Martinet, *Character theory and Artin L-functions*, in *Algebraic number fields: L-functions and Galois properties*, Proceedings of a Symposium at the University of Durham, 1975 (Academic Press, London, 1977), 1–87.

Pic09 E. J. Pickett, *Explicit construction of self-dual integral normal bases for the square-root of the inverse different*, J. Number Theory **129** (2009), 1773–1785.

Pic10 E. J. Pickett, *Construction of self-dual integral normal bases in abelian extensions of finite and local fields*, Int. J. Number Theory **6** (2010), 1565–1588.

Ser67 J. P. Serre, *Local class field theory*, in *Algebraic number theory*, eds J. W. S. Cassels and A. Fröhlich (Academic Press, London, 1967).

Ser68 J. P. Serre, *Corps locaux* (Hermann, Paris, 1968).

Tat77 J. T. Tate, *Local constants*, in *Algebraic number fields: L-functions and Galois properties*, Proceedings of a Symposium at the University of Durham, 1975 (Academic Press, London, 1977), 89–131, Prepared in collaboration with C. J. Bushnell and M. J. Taylor.

Tay81 M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), 41–79.

Vin01 S. Vinatier, *Structure galoisienne dans les extensions faiblement ramifiées de* $\mathbb{Q}$, J. Number Theory **91** (2001), 126–152.

Vin05 S. Vinatier, *Galois module structure in weakly ramified 3-extensions*, Acta Arith. **119** (2005), 171–186.

Erik Jarl Pickett erik_pickett@hotmail.com
53 Parkfield Crescent, Kimpton, Herts, SG4 8EQ, UK

Stéphane Vinatier stephane.vinatier@unilim.fr
XLIM-DMI, 123 avenue Albert Thomas, 87060 Limoges, France