ON THE SQUARE ROOT OF THE INVERSE DIFFERENT

A. AGBOOLA, D. BURNS, L. CAPUTO AND Y. KUANG

Abstract. Let F_π be a finite, Galois-algebra extension of a number field F, with group G. Suppose that F_π/F is weakly ramified, and that the square root A_π of the inverse different $\mathfrak{D}_\pi^{-1}$ is defined. (This latter condition holds if, for example, $|G|$ is odd.) B. Erez has conjectured that the class (A_π) of A_π in the locally free class group $\mathrm{Cl}(\mathbf{Z}G)$ of $\mathbf{Z}G$ is equal to the Cassou-Noguès-Fröhlich root number class $W(F_\pi/F)$ associated to F_π/F. This conjecture has been verified in many cases. We establish a precise formula for (A_π) in terms of $W(F_\pi/F)$ in all cases that A_π is defined and F_π/F is tame, and are thereby able to deduce that, in general, (A_π) is not equal to $W(F_\pi/F)$.

Contents

1. Introduction

Let G be a finite group, and suppose that F_π/F is a G-Galois algebra extension of number fields. Write $\mathfrak{D}_\pi$ for the different of F_π/F and O_π for the ring of integers of F_π. If $\mathfrak{P}$ is any

Date: Version of October 4, 2022.

prime of O_π, the power $v_{\mathfrak{P}}(\mathfrak{D}_\pi)$ of $\mathfrak{P}$ occurring in $\mathfrak{D}_\pi$ is given by

$$v_{\mathfrak{P}}(\mathfrak{D}_\pi) = \sum_{i=0}^{\infty} \left(|G_{\mathfrak{P}}^{(i)}| - 1 \right),$$

where $G_{\mathfrak{P}}^{(i)}$ denotes the i-th ramification group at $\mathfrak{P}$ (see [23, Chapter IV, Proposition 4]). This implies that if, for example, $|G|$ is odd, then the inverse different $\mathfrak{D}_\pi^{-1}$ has a square root, i.e. there exists a unique fractional ideal A_π of O_π such that

$$A_\pi^2 = \mathfrak{D}_\pi^{-1}.$$

(Let us remark at once that if $|G|$ is even, then $\mathfrak{D}_\pi^{-1}$ may well—but of course need not—also have a square root.)

Recall that F_π/F is said to be *weakly ramified* if $G_{\mathfrak{P}}^{(2)} = 0$ for all prime ideals $\mathfrak{P}$ of O_π. B. Erez has shown that F_π/F is weakly ramified if and only if A_π is a locally free $O_F G$-module (see [10, Theorem 1]). Hence, if F_π/F is weakly ramified, it follows that A_π is a locally free $\mathbf{Z}G$-module, and so defines an element (A_π) in the locally free class group $\mathrm{Cl}(\mathbf{Z}G)$ of $\mathbf{Z}G$. The following result is due to Erez (see [10, Theorem 3]).

Theorem 1.1. *Suppose that F_π/F is tamely ramified, and that $|G|$ is odd. Then A_π is a free $\mathbf{Z}G$-module.* □

Based on this and other results, S. Vinatier has made the following conjecture (cf. [30, Conjecture] and [4, Section 1.2]):

Conjecture 1.2. *Suppose that F_π/F is weakly ramified, and that $|G|$ is odd. Then A_π is a free $\mathbf{Z}G$-module.* □

The first detailed study of the Galois structure of A_π when $|G|$ is even is due to the third-named author and Vinatier [4]. By studying the Galois structure of certain torsion modules first considered by S. Chase [6], they proved the following result, and thereby were able to exhibit the first examples for which $(A_\pi) \neq 0$ in $\mathrm{Cl}(\mathbf{Z}G)$ (see [4, Theorem 2]).

Theorem 1.3. *Suppose that F_π/F is tame and locally abelian (i.e. the decomposition group at every ramified prime of F_π/F is abelian). Assume also that A_π exists. Then $(A_\pi) = (O_\pi)$ in $\mathrm{Cl}(\mathbf{Z}G)$.* □

A well-known theorem of M. Taylor asserts that, if F_π/F is tame, then

$$(O_\pi) = W(F_\pi/F), \tag{1.1}$$

where $W(F_\pi/F)$ denotes the Cassou-Noguès-Fröhlich root number class, which is defined in terms of Artin root numbers attached to non-trivial irreducible symplectic characters of G.

(In particular, if $|G|$ is odd, and so has no non-trivial irreducible symplectic characters, then $W(F_\pi/F) = 0$.)

We therefore see that Theorem 1.3 may be viewed as saying that if F_π/F is tame and locally abelian, and if A_π exists, then we have

$$(A_\pi) = (O_\pi) = W(F_\pi/F).$$

In light of the results described above, Erez has made the following (unpublished) conjecture:

Conjecture 1.4. *Suppose that F_π/F is weakly ramified, and that A_π exists. Then*

$$(A_\pi) = W(F_\pi/F).$$

$\square$

Conjecture 1.4 includes Vinatier's Conjecture 1.2 as a special case, and was the motivation for the work described in [4]. It also explains almost all previously obtained results on the $\mathbf{Z}G$-structure of A_π. In a different direction, the conjecture is related to recent work of Bley, Hahn and the second author [3] concerning metric structures arising from A_π (for more details of which see the PhD thesis [17] of the fourth author).

In this paper we show that, in general, Conjecture 1.4 fails for tame extensions. For each tame extension F_π/F we use the signs at infinity of certain symplectic Galois-Jacobi sums to define an element $\mathcal{J}^*_\infty(F_\pi/F) \in \mathrm{Cl}(\mathbf{Z}G)$. The class $\mathcal{J}^*_\infty(F_\pi/F)$ is of order at most 2, and is often, but not always, equal to zero. We prove the following result.

Theorem 1.5. *Suppose that F_π/F is tame, and that A_π exists. Then*

$$(A_\pi) - (O_\pi) = \mathcal{J}^*_\infty(F_\pi/F)$$

i.e. (see (1.1)*)*

$$(A_\pi) = W(F_\pi/F) + \mathcal{J}^*_\infty(F_\pi/F). \tag{1.2}$$

$\square$

Our proof of Theorem 1.5 combines methods from [1] and [2] involving relative algebraic K-theory with the use of non-abelian Galois-Jacobi sums, the explicit computation by Fröhlich and Queyrut of the local root numbers of dihedral representations and a detailed representation-theoretic analysis of the failure (in the relevant cases) of induction functors to commute with Adams operators. In particular, it is interesting to compare our use of Galois-Jacobi sums with the methods of [4], where abelian Jacobi sums play a critical role.

Remark 1.6. It remains an open question as to whether (1.2) continues to hold if the tameness hypothesis is relaxed. □

For any integer $m \geq 1$, we write H_{4m} for the generalised quaternion group of order $4m$. The following result, which is obtained by combining Theorem 1.5 with work of Fröhlich on root numbers (see [11]), gives infinitely many counterexamples to Conjecture 1.4.

Theorem 1.7. *Let F be an imaginary quadratic field such that $\mathrm{Cl}(O_F)$ contains an element of order 4. Then for any sufficiently large prime ℓ with $\ell \equiv 3 \pmod 4$, there are infinitely many tame, $H_{4\ell}$-extensions F_π/F such that A_π exists and $(A_\pi) \neq (O_\pi)$ in $\mathrm{Cl}(\mathbf{Z}H_{4\ell})$.*

An outline of the contents of this paper is as follows. In Section 2 we recall certain basic facts about relative algebraic K-theory from [1] and [2]. In Section 3, we discuss how ideals in Galois algebras give rise to elements in certain relative K-groups. Section 4 contains a description of the Stickelberger factorisation of certain tame resolvends (see [2, Section 7]) in the case of both rings of integers and square roots of inverse differents, while Section 5 develops properties of Stickelberger pairings, and explains how these may be used to give explicit descriptions of the tame resolvends considered in the previous section. In Section 6 we recall a number of facts concerning Galois-Gauss sums. We define Galois-Jacobi sums, and we establish some of their basic properties. In Section 7 we compute the signs of local Galois-Jacobi sums at symplectic characters by combining an analysis of the behaviour of Adams operators with respect to induction functors together with the theorem of Fröhlich and Queyrut. In Section 9, we prove Theorem 1.5. Finally, in Section 10, we prove Theorem 1.7.

Acknowledgements: The first-named author learned of the work of [4] and of the conjecture of Erez from conversations with Philippe Cassou-Noguès and Boas Erez. He is is extremely grateful to them, as well as to Werner Bley and Cindy Tsang for their subsequent interest in this project. We are also very grateful to Dominik Bullach for additional insight into the manner in which counterexamples to Conjecture 1.4 can be derived from Theorem 1.5 (see Remark 10.9).

Notation and conventions.

For any field L, we write L^c for an algebraic closure of L, and we set $\Omega_L := \mathrm{Gal}(L^c/L)$. If L is a number field or a non-archimedean local field (by which we shall always mean a finite extension of $\mathbf{Q}_p$ for some prime p), then O_L denotes the ring of integers of L. If L is an archimedean local field, then we adopt the usual convention of setting $O_L = L$.

Throughout this paper, F will denote a number field. For each place v of F, we fix an embedding $F^c \to F_v^c$, and we view Ω_{F_v} as being a subgroup of Ω_F via this choice of embedding. We write I_v for the inertia subgroup of Ω_{F_v} when v is finite.

The symbol G will always denote a finite group upon which Ω_F acts trivially. If H is any finite group, we write $\mathrm{Irr}(H)$ for the set of irreducible F^c-valued characters of H and R_H for the corresponding ring of virtual characters. We write $\mathbf{1}_H$ (or simply $\mathbf{1}$ if there is no danger of confusion) for the trivial character in R_H.

If L is a number field or a local field, and Γ is any group upon which Ω_L acts continuously, we identify Γ-torsors over L (as well as their associated algebras, which are Hopf-Galois extensions associated to $A_\Gamma := (L^c\Gamma)^{\Omega_L}$) with elements of the set $Z^1(\Omega_L, \Gamma)$ of Γ-valued continuous 1-cocycles of Ω_L (see [24, I.5.2]). If $\pi \in Z^1(\Omega_L, \Gamma)$, then we write L_π/L for the corresponding Hopf-Galois extension of L, and O_π for the integral closure of O_L in L_π. (Thus $O_\pi = L_\pi$ if L is an archimedean local field.) Each such L_π is a principal homogeneous space (p.h.s.) of the Hopf algebra $\mathrm{Map}_{\Omega_L}(\Gamma, L^c)$ of Ω_L-equivariant maps from Γ to L^c. It may be shown that if $\pi_1, \pi_2 \in Z^1(\Omega_L, \Gamma)$, then $L_{\pi_1} \simeq L_{\pi_2}$ if and only if π_1 and π_2 differ by a coboundary. The set of isomorphism classes of Γ-torsors over L may be identified with the pointed cohomology set $H^1(L, \Gamma) := H^1(\Omega_L, \Gamma)$. We write $[\pi] \in H^1(L, \Gamma)$ for the class of L_π in $H^1(L, \Gamma)$. If L is a number field or a non-archimedean local field we write $H^1_t(L, \Gamma)$ for the subset of $H^1(L, \Gamma)$ consisting of those $[\pi] \in H^1(L, \Gamma)$ for which L_π/L is at most tamely ramified. If L is an archimedean local field, we set $H^1_t(L, \Gamma) = H^1(L, \Gamma)$. We denote the subset of $H^1_t(L, \Gamma)$ consisting of those $[\pi] \in H^1_t(L, \Gamma)$ for which L_π/L is unramified at all (including infinite) places of L by $H^1_{nr}(L, \Gamma)$. (So, with this convention, if L is an archimedean local field, we have $H^1_{nr}(L, \Gamma) = 0$.)

If A is any algebra, we write $Z(A)$ for the centre of A. If A is an R-algebra for some ring R, and $R \to R_1$ is an extension of R, we write $A_{R_1} := A \otimes_R R_1$ to denote extension of scalars from R to R_1.

2. Relative algebraic K-theory

The purpose of this section is briefly to recall a number of basic facts concerning relative algebraic K-theory that we shall need. For a more extensive discussion of these topics, the reader is strongly encouraged to consult [2, Section 5] as well as [1, Sections 2 and 3] and [25, Chapter 15].

Let R be a Dedekind domain with field of fractions L of characteristic zero, and suppose that G is a finite group upon which Ω_L acts trivially. Let $\mathfrak{A}$ be any finitely-generated R-algebra satisfying $\mathfrak{A} \otimes_R L \simeq LG$.

For any extension Λ of R, we write $K_0(\mathfrak{A},\Lambda)$ for the relative algebraic K-group that arises via the extension of scalars afforded by the map $R \to \Lambda$. Each element of $K_0(\mathfrak{A},\Lambda)$ is represented by a triple $[M,N;\xi]$, where M and N are finitely generated, projective $\mathfrak{A}$-modules, and $\xi : M \otimes_R \Lambda \xrightarrow{\sim} N \otimes_R \Lambda$ is an isomorphism of $\mathfrak{A} \otimes_R \Lambda$-modules.

Recall that there is a long exact sequence of relative algebraic K-theory (see [25, Theorem 15.5])

$$K_1(\mathfrak{A}) \xrightarrow{\iota} K_1(\mathfrak{A} \otimes_R \Lambda) \xrightarrow{\partial^1_{\mathfrak{A},\Lambda}} K_0(\mathfrak{A},\Lambda) \xrightarrow{\partial^0_{\mathfrak{A},\Lambda}} K_0(\mathfrak{A}) \to K_0(\mathfrak{A} \otimes_R \Lambda). \tag{2.1}$$

The first and last arrows in this sequence are induced by the extension of scalars map $R \to \Lambda$, while the map $\partial^0_{\mathfrak{A},\Lambda}$ sends the triple $[M,N;\xi]$ to the element $[M]-[N] \in K_0(\mathfrak{A})$.

The map $\partial^1_{\mathfrak{A},\Lambda}$ is defined as follows. The group $K_1(\mathfrak{A} \otimes_R \Lambda)$ is generated by elements of the form (V,ϕ), where V is a finitely generated, free $\mathfrak{A} \otimes_R \Lambda$-module, and $\phi : V \xrightarrow{\sim} V$ is an $\mathfrak{A} \otimes_R \Lambda$-isomorphism. To define $\partial^1_{\mathfrak{A},\Lambda}((V,\phi))$, we choose any projective $\mathfrak{A}$-submodule T of V such that $T \otimes_{\mathfrak{A}} \Lambda = V$, and we set

$$\partial^1_{\mathfrak{A},\Lambda}((V,\phi)) := [T,T;\phi].$$

It may be shown that this definition is independent of the choice of T.

Let $\mathrm{Cl}(\mathfrak{A})$ denote the locally free class group of $\mathfrak{A}$. If Λ is a field (as will in fact always be the case in this paper), then (2.1) yields an exact sequence

$$K_1(\mathfrak{A}) \xrightarrow{\iota} K_1(\mathfrak{A} \otimes_R \Lambda) \xrightarrow{\partial^1_{\mathfrak{A},\Lambda}} K_0(\mathfrak{A},\Lambda) \xrightarrow{\partial^0_{\mathfrak{A},\Lambda}} \mathrm{Cl}(\mathfrak{A}) \to 0, \tag{2.2}$$

and this is the form of the long exact sequence of relative algebraic K-theory that we shall use in this paper.

We shall make heavy use of the fact that computations in relative K-groups and in locally free class groups may be carried out using functions on the characters of G. Suppose that L is either a number field or a local field, and write R_G for the ring of virtual characters of G. The group Ω_L acts on R_G via the rule given by

$$\chi^{\omega}(g) = \omega(\chi(g)),$$

where $\omega \in \Omega_L$, $\chi \in \mathrm{Irr}(G)$, and $g \in G$. For each element $a \in (L^cG)^\times$, we define $\mathrm{Det}(a) \in \mathrm{Hom}(R_G,(L^c)^\times)$ as follows. If T is any representation of G with character ϕ, then we set $\mathrm{Det}(a)(\phi) := \det(T(a))$. It may be shown that this definition is independent of the choice of representation T, and so depends only upon the character ϕ.

The map Det is essentially the same as the reduced norm map

$$\mathrm{nrd} : (L^cG)^\times \to Z(L^cG)^\times \tag{2.3}$$

(see [2, Remark 4.2]): (2.3) induces an isomorphism

$$\mathrm{nrd} : K_1(L^cG) \xrightarrow{\sim} Z(L^cG)^\times \simeq \mathrm{Hom}(R_G, (L^c)^\times), \tag{2.4}$$

and we have $\mathrm{Det}(a)(\phi) = \mathrm{nrd}(a)(\phi)$.

Suppose now that we are working over a number field F (i.e. $L = F$ above). We define the group of finite ideles $J_f(K_1(FG))$ to be the restricted direct product over all finite places v of F of the groups $\mathrm{Det}(F_vG)^\times \simeq K_1(F_vG)$ with respect to the subgroups $\mathrm{Det}(O_{F_v}G)^\times$. (We shall require no use of the infinite places of F in the idelic descriptions given below. See e.g. [9, pages 226–228] for details concerning this point.)

For each finite place v of F, we write

$$\mathrm{loc}_v : \mathrm{Det}(FG)^\times \to \mathrm{Det}(F_vG)^\times \subseteq \mathrm{Hom}_{\Omega_{F_v}}(R_G, (F_v^c)^\times)$$

for the obvious localisation map.

Let E be any extension of F. Then the homomorphism

$$\mathrm{Det}(FG)^\times \to J_f(K_1(FG)) \times \mathrm{Det}(EG)^\times; \quad x \mapsto ((\mathrm{loc}_v(x))_v, x^{-1})$$

induces a homomorphism

$$\Delta_{\mathfrak{A},E} : \mathrm{Det}(FG)^\times \to \frac{J_f(K_1(FG))}{\prod_{v\nmid\infty} \mathrm{Det}(\mathfrak{A}_v)^\times} \times \mathrm{Det}(EG)^\times.$$

Theorem 2.1. *(a) There is a natural isomorphism*

$$\mathrm{Cl}(\mathfrak{A}) \xrightarrow{\sim} \frac{J_f(K_1(FG))}{\mathrm{Det}(FG)^\times \prod_{v\nmid\infty} \mathrm{Det}(\mathfrak{A}_v)^\times}.$$

(b) There is a natural isomorphism

$$h_{\mathfrak{A},E} : K_0(\mathfrak{A}, E) \xrightarrow{\sim} \mathrm{Coker}(\Delta_{\mathfrak{A},E}).$$

(c) Let v be a finite place of F, and suppose that L_v is any extension of F_v. Then there are isomorphisms

$$K_0(\mathfrak{A}_v, L_v) \simeq K_1(L_vG)/\iota(K_1(\mathfrak{A}_v)) \simeq \mathrm{Det}(L_vG)^\times / \mathrm{Det}(\mathfrak{A}_v)^\times.$$

Proof. Part (a) is due to A. Fröhlich (see e.g [15, Chapter I]). Part (b) is proved in [1, Theorem 3.5], and a proof of part (c) is given in [2, Lemma 5.7]. □

Remark 2.2. Suppose that $x \in K_0(\mathfrak{A}, E)$ is represented by the idele $[(x_v)_v, x_\infty] \in J_f(K_1(FG))\times \mathrm{Det}(EG)^\times$. Then $\partial^0(x) \in \mathrm{Cl}(\mathfrak{A})$ is represented by the idele $(x_v)_v \in J_f(K_1(FG))$. □

Remark 2.3. Suppose that $[M,N;\xi] \in K_0(O_FG,E)$, and that M and N are locally free $\mathfrak{A}$-modules of rank one. An explicit representative in $J_f(K_1(FG)) \times \mathrm{Det}(EG)^\times$ of $h_{\mathfrak{A},E}([M,N;\xi])$ may be constructed as follows.

For each finite place v of F, fix $\mathfrak{A}_v$-bases m_v of M_v and n_v of N_v. Fix also an FG-basis n_∞ of N_F, and choose an isomorphism $\theta : M_F \xrightarrow{\sim} N_F$ of FG-modules.

The element $\theta^{-1}(n_\infty)$ is an FG-basis of M_F. Hence, for each place v, we may write

$$m_v = \mu_v \cdot \theta^{-1}(n_\infty),$$
$$n_v = \nu_v \cdot n_\infty,$$

where $\mu_v, \nu_v \in (F_vG)^\times$.

If we write $\theta_E : M_E \xrightarrow{\sim} N_E$ for the isomorphism afforded by θ via extension of scalars, then we see that the isomorphism $\xi \circ \theta_E^{-1} : N_E \xrightarrow{\sim} N_E$ is given by $n_\infty \mapsto \nu_\infty \cdot n_\infty$ for some $\nu_\infty \in (EG)^\times$.

A representative of $h_{\mathfrak{A},E}([M,N;\xi])$ is given by the image of $[(\mu_v \cdot \nu_v^{-1})_v, \nu_\infty]$ in $J_f(K_1(FG)) \times \mathrm{Det}(EG)^\times$. □

Remark 2.4. We see from Theorem 2.1(b) and (c) that there are isomorphisms

$$K_0(\mathfrak{A},F) \simeq \frac{J_f(K_1(FG))}{\prod_{v\nmid\infty} \mathrm{Det}(\mathfrak{A}_v)^\times} \simeq \frac{\mathrm{Hom}_{\Omega_F}(R_G, J_f(F^c))}{\prod_{v\nmid\infty} \mathrm{Det}(\mathfrak{A}_v)^\times} \simeq \oplus_{v\nmid\infty} K_0(\mathfrak{A}_v, F_v).$$

There is a natural injection

$$K_0(\mathfrak{A},F) \to K_0(\mathfrak{A},F^c)$$
$$[M,N;\xi] \to [M,N;\xi_{F^c}],$$

where $\xi_{F^c} : M_{F^c} \xrightarrow{\sim} N_{F^c}$ is the isomorphism obtained from $\xi : M_F \xrightarrow{\sim} N_F$ via extension of scalars from F to F^c. It is not hard to check that this map is induced by the inclusion map

$$J_f(K_1(FG)) \to J_f(K_1(FG)) \times \mathrm{Det}(F^cG)^\times$$
$$(x_v)_v \to [(x_v)_v, 1].$$

□

We now recall the description of the restriction of scalars map on relative K-groups and locally free class groups in terms of the isomorphism given by Theorem 2.1(b).

Suppose that $\mathcal{F}/F$ is a finite extension, and that E is an extension of $\mathcal{F}$. Then restriction of scalars from $O_{\mathcal{F}}$ to O_F yields homomorphisms

$$K_0(\mathfrak{A}_{O_{\mathcal{F}}}, E) \to K_0(\mathfrak{A}, E)$$

and

$$\mathrm{Cl}(\mathfrak{A}_{O_{\mathcal{F}}}) \to \mathrm{Cl}(\mathfrak{A})$$

which may be described as follows (see e.g. [15, Chapter IV] or [27, Chapter 1]).

Let $\{\omega\}$ be any transversal of $\Omega_{\mathcal{F}}\backslash\Omega_F$. Then the map

$$J_f(K_1(\mathcal{F}G)) \times \mathrm{Det}(EG)^\times \to J_f(K_1(FG)) \times \mathrm{Det}(EG)^\times$$
$$[(y_v)_v, y_\infty] \mapsto \prod_\omega [(y_v)_v, y_\infty]^\omega$$

induces homomorphisms

$$\mathcal{N}_{\mathcal{F}/F} : K_0(\mathfrak{A}_{O_{\mathcal{F}}}, E) \to K_0(\mathfrak{A}, E) \tag{2.5}$$

and

$$\mathcal{N}_{\mathcal{F}/F} : \mathrm{Cl}(\mathfrak{A}_{O_{\mathcal{F}}}) \to \mathrm{Cl}(\mathfrak{A}). \tag{2.6}$$

These homomorphisms are independent of the choice of $\{\omega\}$ and are equal to the natural maps on relative K-groups (resp. locally free class groups) afforded by restriction of scalars from $O_{\mathcal{F}}$ to O_F.

We conclude this section by recalling the definitions of certain induction maps on relative algebraic K-groups and on locally free class groups of group rings (see e.g. [15, Chapter II] or [27, Chapter I]).

Suppose that G is a finite group, and that H is a subgroup of G. Let E be an algebraic extension of F. Then extension of scalars from O_FH to O_FG yields natural homomorphisms

$$\mathrm{Ind}_H^G : K_0(O_FH, E) \to K_0(O_FG, E) \tag{2.7}$$

and

$$\mathrm{Ind}_H^G : \mathrm{Cl}(O_FH) \to \mathrm{Cl}(O_FG). \tag{2.8}$$

It may be shown that these homomorphisms are induced (via the isomorphisms described in Theorem 2.1) by the maps

$$\mathrm{Ind}_H^G : \mathrm{Hom}(R_H, J(F^c)) \to \mathrm{Hom}(R_G, J(F^c));$$
$$\mathrm{Ind}_H^G : \mathrm{Hom}(R_H, (F^c)^\times) \to \mathrm{Hom}(R_G, (F^c)^\times)$$

given by

$$(\mathrm{Ind}_H^G f)(\chi) = f(\chi\mid_H), \quad \chi \in R_G. \tag{2.9}$$

It is not hard to check from the definitions that the following diagram commutes:

$$\begin{array}{ccc} K_0(O_F H, E) & \xrightarrow{\mathrm{Ind}_H^G} & K_0(O_F G, E) \\ {\scriptstyle \partial^0}\Big\downarrow & & {\scriptstyle \partial^0}\Big\downarrow \\ \mathrm{Cl}(O_F H) & \xrightarrow{\mathrm{Ind}_H^G} & \mathrm{Cl}(O_F G). \end{array} \tag{2.10}$$

3. Galois algebras and ideals

Let L be either a number field or a local field, and suppose that $\pi \in Z^1(\Omega_L, G)$ is a continuous G-valued Ω_L 1-cocycle. We may define an associated G-Galois L-algebra L_π by

$$L_\pi := \mathrm{Map}_{\Omega_L}({}^\pi G, L^c),$$

where ${}^\pi G$ denotes the set G endowed with an action of Ω_L via the cocycle π (i.e. $g^\omega = \pi(\omega)\cdot g$ for $g \in {}^\pi G$ and $\omega \in \Omega_L$), and L_π is the algebra of L^c-valued functions on ${}^\pi G$ that are fixed under the action of Ω_L. The group G acts on L_π via the rule

$$a^g(h) = a(h \cdot g)$$

for all $g \in G$ and $h \in {}^\pi G$.

The Wedderburn decomposition of the algebra L_π may be described as follows. Set

$$L^\pi := (L^c)^{\mathrm{Ker}(\pi)},$$

so $\mathrm{Gal}(L^\pi/L) \simeq \pi(\Omega_L)$. Then

$$L_\pi \simeq \prod_{\pi(\Omega_L)\backslash G} L^\pi, \tag{3.1}$$

and this isomorphism depends only upon the choice of a transversal of $\pi(\Omega_L)$ in G. It may be shown that every G-Galois L-algebra is of the form L_π for some π, and that L_π is determined up to isomorphism by the class $[\pi]$ of π in the pointed cohomology set $H^1(L, G)$. In particular, every Galois algebra may be viewed as being a sub-algebra of the L^c-algebra $\mathrm{Map}(G, L^c)$.

Definition 3.1. The *resolvend* map $\mathbf{r}_G$ on $\mathrm{Map}(G, L^c)$ is defined by

$$\begin{aligned} \mathbf{r}_G : \mathrm{Map}(G, L^c) &\to L^c G \\ a &\mapsto \sum_{g \in G} a(g) \cdot g^{-1}. \end{aligned}$$

(This is an isomorphism of L^cG-modules, but it is not an isomorphism of L^c-algebras because it does not preserve multiplication.) □

Suppose now that L_π/L is a G-extension, and that $\mathcal{L} \subseteq L_\pi$ is a non-zero projective $O_L G$-module. Then there are isomorphisms

$$\mathrm{Map}(G, L^c) \simeq \mathcal{L} \otimes_{O_L} L^c, \quad L^c G \simeq O_L G \otimes_{O_L} L^c,$$

and so the triple $[\mathcal{L}, O_L G; \mathbf{r}_G]$ yields an element of $K_0(O_L G, L^c)$.

Proposition 3.2. *Let F_π/F be a G-extension of a number field F, and suppose that $\mathcal{L}_i \subseteq F_\pi$ $(i = 1, 2)$ are non-zero projective $O_F G$-modules. For each place v of F, choose a basis $l_{i,v}$ of $\mathcal{L}_{i,v}$ over $O_{F_v} G$, as well as a basis l_∞ of F_π over FG.*

(a) *The element $[\mathcal{L}_i, O_F G; \mathbf{r}_G] \in K_0(O_F G, F^c)$ is represented by the image of the idele $[(\mathbf{r}_G(l_{i,v}) \cdot \mathbf{r}_G(l_\infty)^{-1})_v, \mathbf{r}_G(l_\infty)^{-1}] \in J_f(K_1(FG)) \times \mathrm{Det}(F^c G)^\times$.*

(b) *The element*

$$[\mathcal{L}_1, O_F G; \mathbf{r}_G] - [\mathcal{L}_2, O_F G; \mathbf{r}_G] \in K_0(O_F G, F^c)$$

is represented by the image of the idele

$$[(\mathbf{r}_G(l_{1,v}) \cdot \mathbf{r}_G(l_{2,v}^{-1}))_v, 1] \in J_f(K_1(FG)) \times \mathrm{Det}(F^c G)^\times.$$

(c) *We have that*

$$[\mathcal{L}_1, O_F G; \mathbf{r}_G] - [\mathcal{L}_2, O_F G; \mathbf{r}_G] \in K_0(O_F G, F) \subseteq K_0(O_F G, F^c).$$

Proof. For each finite place v of F, write

$$l_{i,v} = x_{i,v} \cdot l_\infty,$$

with $x_{i,v} \in (F_v G)^\times$. Then it follows from Remark 2.3 that $[\mathcal{L}_i, O_F G; \mathbf{r}_G] \in K_0(O_F G, F^c)$ is represented by the image of the idele $[(x_{i,v})_v, \mathbf{r}_G(l_\infty)^{-1}] \in J_f(K_1(FG)) \times \mathrm{Det}(F^c G)^\times$. However

$$x_{i,v} = \mathbf{r}_G(l_{i,v}) \cdot \mathbf{r}_G(l_\infty)^{-1}$$

(because the resolvend map is an isomorphism of $F^c G$ and $F_v^c G$-modules), and this implies (a). Part (b) now follows directly from (a).

To show part (c), we first recall that

$$K_0(O_F G, F) \simeq \oplus_{v \nmid \infty} K_0(O_{F_v} G, F_v) \simeq \oplus_{v \nmid \infty} \mathrm{Det}(F_v G)^\times / \mathrm{Det}(O_{F_v} G)^\times,$$

and that an element $c \in K_0(O_F G, F^c)$ lies in $K_0(O_F G, F)$ if it has an idelic representative lying in $J_f(K_1(FG)) \times \mathrm{Det}(FG)^\times \subseteq J_f(K_1(FG)) \times \mathrm{Det}(F^c G)^\times$ (see Remark 2.4).

Now a standard property of resolvends implies that

$$\mathbf{r}_G(l_{i,v})^\omega = \mathbf{r}_G(l_{i,v}) \cdot \pi(\omega)$$

for every $\omega \in \Omega_{F_v}$ (see e.g. [2, 2.2]), and so we see that $(\mathbf{r}_G(l_{1,v}) \cdot \mathbf{r}_G(l_{2,v}^{-1}))_v \in (F_vG)^\times$ for each v. (In fact, as we may take $l_{1,v} = l_{2,v}$ for almost all v, we may suppose that $(\mathbf{r}_G(l_{1,v}) \cdot \mathbf{r}_G(l_{2,v}^{-1}))_v = 1$ for almost all v.) Hence it now follows from (b) that $[\mathcal{L}_1, O_FG; F^c] - [\mathcal{L}_2, O_FG; F^c] \in K_0(O_FG, F)$, as claimed. □

It is a classical result, due to E. Noether, that a G-extension F_π/F is tamely ramified if and only if O_π is a locally free (and therefore projective) O_FG-module. S. Ullom has shown that if F_π/F is tame, then in fact all G-stable ideals in O_π are locally free. He also showed that if any G-stable ideal B, say, in a G-extension F_π/F is locally free, then all second ramification groups at primes dividing B are equal to zero (see [29]). If F_π/F is any G-extension for which $|G|$ is odd (and so the square root A_π of the inverse different automatically exists), then Erez has shown that A_π is a locally free O_FG-module if and only if all second ramification groups associated to F_π/F vanish, i.e. if and only if F_π/F is weakly ramified. In fact, as pointed out by the third-named author and Vinatier, [4, pp. 109, footnote 1] the proof of [10, Theorem 1] shows that if F_π/F is any weakly ramified extension such that A_π exists, then A_π is locally free.

Definition 3.3. Suppose that $[\pi] \in H^1_t(F, G)$, and that A_π exists. We define

$$\mathfrak{c} = \mathfrak{c}(\pi) := [A_\pi, O_FG; \mathbf{r}_G] - [O_\pi, O_FG; \mathbf{r}_G] \in K_0(O_FG, F) \subseteq K_0(O_FG, F^c).$$

□

4. Local decomposition of tame resolvends

Our goal in this section is to recall certain facts from [2, Section 7] concerning Stickelberger factorisations of resolvends of normal integral basis generators of tame local extensions, and to describe similar results concerning resolvends of basis generators of the square root of the inverse different (when this exists).

Let L be a local field, and fix a uniformiser $\varpi = \varpi_L$ of L. Set $q := |O_L/\varpi_L O_L|$.

Fix also a compatible set of roots of unity $\{\zeta_m\}$, and a compatible set $\{\varpi^{1/m}\}$ of roots of ϖ. (Hence if m and n are any two positive integers, then we have $(\zeta_{mn})^m = \zeta_n$, and $(\varpi^{1/mn})^m = \varpi^{1/n}$.)

Let L^{nr} (respectively L^t) denote the maximal unramified (respectively tamely ramified) extension of L. Then

$$L^{nr} = \bigcup_{\substack{m \geq 1 \\ (m,q)=1}} L(\zeta_m), \quad L^t = \bigcup_{\substack{m \geq 1 \\ (m,q)=1}} L(\zeta_m, \varpi^{1/m}).$$

The group $\Omega^{nr} := \mathrm{Gal}(L^{nr}/L)$ is topologically generated by a Frobenius element ϕ which may be chosen to satisfy

$$\phi(\zeta_m) = \zeta_m^q, \qquad \phi(\varpi^{1/m}) = \varpi^{1/m}$$

for each integer m coprime to q. Our choice of compatible roots of unity also uniquely specifies a topological generator σ of $\Omega^r := \mathrm{Gal}(L^t/L^{nr})$ by the conditions

$$\sigma(\varpi^{1/m}) = \zeta_m \cdot \varpi^{1/m}, \qquad \sigma(\zeta_m) = \zeta_m$$

for all integers m coprime to q. The group $\Omega^t := \mathrm{Gal}(L^t/L)$ is topologically generated by ϕ and σ, subject to the relation

$$\phi \cdot \sigma \cdot \phi^{-1} = \sigma^q. \tag{4.1}$$

The reader may find it helpful to keep in mind the following explicit example, due to C. Tsang (cf. [28, Proposition 4.2.2]), while reading the next two sections.

Example 4.1. (C. Tsang) Suppose that L contains the e-th roots of unity with $(e, q) = 1$, and set $M := L(\varpi_L^{1/e})$. Write $\varpi_M := \varpi_L^{1/e}$; then ϖ_M is a uniformiser of M. Set $H := \mathrm{Gal}(M/L) = \langle s \rangle$, say.

Let n be an integer with $0 \leq |n| \leq e - 1$, and let us consider the ideal

$$\varpi_M^n O_M = \varpi_L^{n/e} O_M$$

as an $O_L H$-module. Set

$$\alpha = \frac{1}{e} \sum_{i=0}^{e-1} \varpi_M^{n+i} = \frac{1}{e} \sum_{i=0}^{e-1} \varpi_L^{(n+i)/e}.$$

We wish to explain why

$$O_L H \cdot \alpha = \varpi_M^n \cdot O_M,$$

and to give some motivation for the definition of the Stickelberger pairings in Definition 5.1 below.

Suppose that $s(\varpi_M) = \zeta \cdot \varpi_M$, where ζ is a primitive e-th root of unity. Then for each $0 \leq j \leq e - 1$, we have

$$s^j(\alpha) = \frac{1}{e} \sum_{i=0}^{e-1} \zeta^{(i+n)j} \varpi_M^{i+n}.$$

Multiplying both sides of this last equality by $\zeta^{-(l+n)j}$, where $0 \leq l \leq e - 1$ gives

$$s^j(\alpha)\zeta^{-(l+n)j} = \frac{1}{e} \sum_{i=0}^{e-1} \zeta^{(i-l)j} \varpi_M^{i+n}.$$

Now sum over j to obtain

$$\sum_{j=0}^{e-1} s^j(\alpha)\zeta^{-(l+n)j} = \frac{1}{e}\sum_{i=0}^{n}\varpi_M^{i+n}\sum_{j=0}^{e-1}\zeta^{(i-l)j} = \varpi_M^{l+n}.$$

So, if for any $\chi \in \mathrm{Irr}(H)$, we choose the unique integer $(\chi, s)_{H,n}$ in the set

$$\{l+n \mid 0 \le l \le e-1\}$$

such that $\chi(s) = \zeta^{(\chi,s)_{H,n}}$, then we see that

$$\mathrm{Det}(\mathbf{r}_H(\alpha))(\chi) = \sum_{j=0}^{e-1} s^j(\alpha)\zeta^{-(l+n)j} = \varpi_M^{(\chi,s)_{H,n}}. \tag{4.2}$$

The cases $n = 0$ and $n = (1-e)/2$ (for e odd) correspond to the ring of integers and the square root of the inverse different respectively, and we see the appearance of the relevant Stickelberger pairing (see Definition 5.1 below) in each case.

It follows from (4.2) that

$$B_n := \{\varpi_M^{l+n} : 0 \le l \le e-1\} \subseteq O_L H \cdot \alpha.$$

As B_n is an O_L-basis of the ideal $\varpi_M^n \cdot O_M$, and as $\zeta_e \in O_L$, we see that

$$O_L H \cdot \alpha = \varpi_M^n \cdot O_M,$$

i.e. α is a free generator of $\varpi_M^n \cdot O_M$ as an $O_L H$-module. $\square$

Definition 4.2. If $g \in G$, we set

$$\beta_g := \frac{1}{|g|}\sum_{i=0}^{|g|-1}\varpi^{i/|g|};$$

note that β_g depends only upon $|g|$, and so in particular we have

$$\beta_g = \beta_{\gamma^{-1}g\gamma}$$

for every $\gamma \in G$. We define $\varphi_g \in \mathrm{Map}(G, L^c)$ by setting

$$\varphi_g(\gamma) = \begin{cases} \sigma^i(\beta_g) & \text{if } \gamma = g^i; \\ 0 & \text{if } \gamma \notin \langle g \rangle. \end{cases}$$

Then

$$\mathbf{r}_G(\varphi_g) = \sum_{i=0}^{|g|-1}\varphi_g(g^i)g^{-i} = \sum_{i=0}^{|g|-1}\sigma^i(\beta_g)g^{-i}. \tag{4.3}$$

$\square$

Suppose now that $\pi \in Z^1(\Omega_L, G)$, with $[\pi] \in H^1_t(L, G)$. Write $s := \pi(\sigma)$ and $t := \pi(\phi)$. We define, $\pi_r, \pi_{nr} \in \mathrm{Map}(\Omega^t, G)$ by setting

$$\pi_r(\sigma^m \phi^n) = \pi(\sigma^m) = s^m, \tag{4.4}$$

$$\pi_{nr}(\sigma^m \phi^n) = \pi(\phi^n) = t^n, \tag{4.5}$$

so that

$$\pi = \pi_r \cdot \pi_{nr}.$$

It may be shown that in fact $\pi_{nr} \in \mathrm{Hom}(\Omega^{nr}, G)$, and so corresponds to a unramified G-extension $L_{\pi_{nr}}$ of L. It may also be shown that $\pi_r \in \mathrm{Hom}(\Omega^r, G)$, corresponding to a totally (tamely) ramified extension $L^{nr}_{\pi_r}/L^{nr}$. If we write $[\widetilde{\pi}]$ for the image of $[\pi]$ under the natural restriction map $H^1(L, G) \to H^1(L^{nr}, G)$, then $[\widetilde{\pi}] = [\pi_r]$. The element φ_s is a normal integral basis generator of the extension $L^{nr}_{\pi_r}/L^{nr}$. (See [2, Section 7] for proofs of these assertions.) If in addition $|s|$ is odd, then the inverse different of L_π/L has a square root A_π, and

$$A_\pi = \varpi^{(1-|s|)/2|s|} \cdot O_\pi.$$

We can now state the Stickelberger factorisation theorem for resolvends of normal integral bases.

Theorem 4.3. *If $a_{nr} \in L_{\pi_{nr}}$ is any normal integral basis generator of $L_{\pi_{nr}}/L$, then the element $a \in L_\pi$ defined by*

$$\mathbf{r}_G(a_{nr}) \cdot \mathbf{r}_G(\varphi_s) = \mathbf{r}_G(a) \tag{4.6}$$

is a normal integral basis generator of L_π/L.

Proof. See [2, Theorem 7.9]. □

We shall now describe a similar result (due to C. Tsang when G is abelian) concerning $O_L G$-generators of the square root of the inverse different of a tame extension of L.

Definition 4.4. Suppose that $g \in G$ and that $|g|$ is odd. Set

$$\beta^*_g = \frac{1}{|g|} \sum_{i=0}^{|g|-1} \varpi^{\frac{1}{|g|}(i + \frac{1-|g|}{2})}.$$

Define $\varphi^*_g \in \mathrm{Map}(G, L^c)$ by

$$\varphi^*_g(\gamma) = \begin{cases} \sigma^i(\beta^*_g) & \text{if } \gamma = g^i; \\ 0 & \text{if } \gamma \notin \langle g \rangle. \end{cases}$$

Then

$$\mathbf{r}_G(\varphi^*_g) = \sum_{i=0}^{|g|-1} \varphi_g(g^i) g^{-i} = \sum_{i=0}^{|g|-1} \sigma^i(\beta^*_g) g^{-i}. \tag{4.7}$$

Theorem 4.5. *(cf. [2, Theorem 7.9]) If a_{nr} is any choice of n.i.b. generator of $L_{\pi_{nr}}/L$, then the element b of L_π defined by*

$$\mathbf{r}_G(b) = \mathbf{r}_G(a_{nr}) \cdot \mathbf{r}_G(\varphi_s^*) \tag{4.8}$$

satisfies $A_\pi = O_L G \cdot b$.

Proof. To ease notation, set $N := L^{nr}$ and $H := \langle s \rangle$.

Write $[\widetilde{\pi}] \in H^1(N, G)$ for the image of $[\pi] \in H^1(L, G)$ under the restriction map $H^1(L, G) \to H^1(N, G)$. Then $A_{\widetilde{\pi}} = O_N \cdot A_\pi$, because N/L is unramified. Hence, to establish the desired result, it suffices to show that

$$A_{\widetilde{\pi}} = O_N G \cdot b. \tag{4.9}$$

As $\mathbf{r}_G(a_{nr}) \in (O_N G)^\times$, (4.9) is equivalent to the equality

$$A_{\widetilde{\pi}} = O_N G \cdot \varphi_s^*. \tag{4.10}$$

Now

$$N_{\widetilde{\pi}} \simeq \prod_{H \backslash G} N^{\widetilde{\pi}}, \tag{4.11}$$

where $N^{\widetilde{\pi}} = N(\varpi^{1/|s|})$ (cf. (3.1)), and this isomorphism induces a decomposition

$$A_{\widetilde{\pi}} = \prod_{H \backslash G} A^{\widetilde{\pi}}, \tag{4.12}$$

where

$$A^{\widetilde{\pi}} = A(N^{\widetilde{\pi}}) = \varpi^{(1-|s|)/2|s|} \cdot O_N$$

is the square root of the inverse different of the extension $N^{\widetilde{\pi}}/N$.

It therefore follows from the definition of φ_s^* that (4.10) holds if and only if

$$A^{\widetilde{\pi}} = O_N H \cdot \beta_s^*. \tag{4.13}$$

This last equality follows exactly as in [28, Proposition 4.2.2], and a proof is given by taking $n = (1-e)/2$ (for e odd) in Example 4.1 above. □

Proposition 4.6. *Suppose that $[\pi] \in H^1_t(L, G)$ and that $s := \pi(\sigma)$ is of odd order. Then the class*

$$\mathfrak{c}(\pi) := [A_\pi, O_L G; \mathbf{r}_G] - [O_\pi, O_L G; \mathbf{r}_G] \in K_0(O_L G, L) \simeq \mathrm{Det}(LG)^\times / \mathrm{Det}(O_L G)^\times$$

is represented by $\mathrm{Det}(\mathbf{r}_G(\varphi_s^*)) \cdot \mathrm{Det}(\mathbf{r}_G(\varphi_s))^{-1} \in \mathrm{Det}(LG)^\times$.

Proof. This is a direct consequence of Theorems 4.3 and 4.5, together with the proof of Proposition 3.2(c). □

5. Stickelberger pairings and resolvends

Our goal in this section is to describe explicitly the elements $\mathrm{Det}(\mathbf{r}_G(\varphi_s))$ and $\mathrm{Det}(\mathbf{r}_G(\varphi_s^*))$ constructed in the previous section. We begin by recalling the definition of two Stickelberger pairings. The first of these is due to L. McCulloh, while the second is due to C. Tsang in the case of abelian G. See [2, Definition 9.1] and [28, Definition 2.5.1].

Definition 5.1. Let $\zeta = \zeta_{|G|}$ be a fixed, primitive, $|G|$-th root of unity. Suppose first that G is cyclic. For $g \in G$ and $\chi \in \mathrm{Irr}(G)$, write $\chi(g) = \zeta^r$ for some integer r.

(1) We define

$$\langle \chi, g \rangle_G = \{r/|G|\},$$

where $0 \leq \{r/|G|\} < 1$ denotes the fractional part of $r/|G|$.

Alternatively (cf. Example 4.1), if we choose r to be the unique integer in the set $\{l : 0 \leq l \leq |G| - 1\}$ such that $\chi(g) = \zeta^r$, then

$$\langle \chi, g \rangle_G = r/|G|.$$

(2) Suppose that $|G|$ is odd, and choose $r \in [(1 - |G|)/2, (|G| - 1)/2]$ to be the unique integer such that $\chi(g) = \zeta^r$. Define

$$\langle \chi, g \rangle_G^* = r/|G|.$$

We extend each of these to pairings

$$\mathbf{Q}R_G \times \mathbf{Q}G \to \mathbf{Q}$$

via linearity. Finally, we extend the definitions to arbitrary finite groups G by setting

$$\langle \chi, s \rangle_G := \langle \chi \mid_{\langle s \rangle}, s \rangle_{\langle s \rangle}$$

and

$$\langle \chi, s \rangle_G^* := \langle \chi \mid_{\langle s \rangle}, s \rangle_{\langle s \rangle}^*,$$

where the second definition of course only makes sense when the order $|s|$ of s is odd. $\square$

We shall make use of the following alternative descriptions of the above Stickelberger pairing using the standard inner product on R_G (see [2, Proposition 9.2]). For each element $s \in G$, write $\zeta_{|s|} = \zeta_{|G|}^{|G|/|s|}$, and define a character ξ_s of $\langle s \rangle$ by $\xi_s(s^i) = \zeta_{|s|}^i$. Set

$$\Xi_s := \frac{1}{|s|} \sum_{j=1}^{|s|-1} j \xi_s^j.$$

For $|s|$ odd, we also define

$$\Xi_s^* := \frac{1}{|s|}\sum_{j=1}^{(|s|-1)/2} j(\xi_s^j - \xi_s^{-j}).$$

Let $(-,-)_G$ denote the standard inner product on R_G.

Proposition 5.2.

(a) *If $s \in G$ and $\chi \in R_G$, we have*

$$\langle \chi, s\rangle_G = (\mathrm{Ind}_{\langle s\rangle}^G(\Xi_s), \chi)_G.$$

(b) *If furthermore $|s|$ is odd, then we have*

$$\langle \chi, s\rangle_G^* = (\mathrm{Ind}_{\langle s\rangle}^G(\Xi_s^*), \chi)_G.$$

(c) *If $|s|$ is odd, then*

$$\Xi_s^* - \Xi_s = -\sum_{j=1}^{(|s|-1)/2} \xi_s^{-j}.$$

(d) *For s odd, write*

$$d(s) := -\sum_{j=1}^{(|s|-1)/2} \xi_s^{-j}.$$

Then, for each $\chi \in R_G$, we have

$$\langle \chi, s\rangle_G^* - \langle \chi, s\rangle_G = (\mathrm{Ind}_{\langle s\rangle}^G(d(s)), \chi)_G.$$

Proof. Part (a) is proved in [2, Proposition 9.2]. The proof of (b) is the same *mutatis mutandis*. Part (c) follows directly from the definitions of Ξ_s and Ξ_s^*, and then (d) follows from (a) and (b). □

We may use Proposition 5.2 to describe the relationship between the two Stickelberger pairings in Definition 5.1 when $|s|$ is odd.

In the sequel, for any finite group Γ (which will be clear from context), and any natural number k, we write ψ_k for the k-th Adams operator on R_Γ. Thus, if $\chi \in R_\Gamma$ and $\gamma \in \Gamma$, then one has $\psi_k(\chi)(\gamma) = \chi(\gamma^k)$. In particular, we recall that, for all k, ψ_k commutes with the restriction and inflation functors, as well as with the action of $\Omega_{\mathbf{Q}}$ on R_Γ (see [10, Proposition-Definition 3.5]). If L is a number field or a local field, we also write ψ_k for the homomorphism

$$\mathrm{Hom}(R_\Gamma, (L^c)^\times) \to \mathrm{Hom}(R_\Gamma, (L^c)^\times)$$

defined by setting

$$\psi_k(f)(\chi) = f(\psi_k(\chi))$$

for $f \in \mathrm{Hom}(R_\Gamma, (L^c)^\times)$ and $\chi \in R_\Gamma$.

Proposition 5.3. *Suppose that $s \in G$ is of odd order, and set $H := \langle s \rangle$.*

(a) *If $1 \leq j \leq |s| - 1$, then*

$$\begin{aligned}(\Xi_s^*, \xi^j)_H &= (\Xi_s, \xi^{2j} - \xi^j)_H \\ &= (\Xi_s, \psi_2(\xi^j) - \xi^j)_H.\end{aligned}$$

(b) *(C. Tsang) For each $\chi \in R_G$, we have*

$$\langle \chi, s \rangle_G^* = \langle \psi_2(\chi) - \chi, s \rangle_G.$$

Proof. (a) If $1 \leq j \leq |s|/2$, then we have

$$(\Xi_s, \xi_s^{2j} - \xi_s^j)_H = \frac{2j - j}{|s|} = \frac{j}{|s|},$$

while if $|s|/2 \leq j \leq s - 1$, then

$$(\Xi_s, \xi_s^{2j} - \xi_s^j)_H = \frac{(2j - |s|) - j}{|s|} = \frac{j - |s|}{|s|}.$$

Thus in each case we have

$$(\Xi_s^*, \xi_s^j)_H = (\Xi_s, \xi_s^{2j} - \xi_s^j)_H,$$

and this establishes the claim.

(b) Proposition 5.2(b), together with Frobenius reciprocity, gives

$$\begin{aligned}\langle \chi, s \rangle_G^* &= (\mathrm{Ind}_{\langle s \rangle}^G(\Xi_s^*), \chi)_G \\ &= (\Xi_s^*, \chi \mid_H)_H.\end{aligned}$$

The desired result now follows from part (a), together with the fact that, for any $\chi \in R_G$, we have the equality

$$\psi_2(\chi) \mid_H = \psi_2(\chi \mid_H).$$

□

The following result describes the elements $\mathrm{Det}(\mathbf{r}_G(\varphi_s))$ and $\mathrm{Det}(\mathbf{r}_G(\varphi_s^*))$ in terms of Stickelberger pairings. In what follows, we retain the notation and conventions of Section 4.

Proposition 5.4. *Suppose that $\chi \in R_G$ and $s \in G$.*

(a) *We have*

$$\mathrm{Det}(\mathbf{r}_G(\varphi_s))(\chi) = \varpi^{\langle \chi, s \rangle_G}.$$

(b) *If $|s|$ is odd, then we have*

$$\mathrm{Det}(\mathbf{r}_G(\varphi_s^*))(\chi) = \varpi^{\langle \chi, s \rangle_G^*}.$$

(c) *For $|s|$ odd, we have*

$$
\begin{aligned}
[\mathrm{Det}(\mathbf{r}_G(\varphi_s^*)) \cdot \mathrm{Det}(\mathbf{r}_G(\varphi_s))^{-1}](\chi) &= \varpi^{\langle \chi, s\rangle_G^* - \langle \chi, s\rangle_G} \\
&= \varpi^{\langle \psi_2(\chi) - 2\chi, s\rangle_G} \\
&= \frac{\mathrm{Det}(\mathbf{r}_G(\varphi_s))(\psi_2(\chi))}{\mathrm{Det}(\mathbf{r}_G(\varphi_s))(2\chi)}.
\end{aligned}
$$

That is to say,

$$\mathrm{Det}(\mathbf{r}_G(\varphi_s^*)) \cdot \mathrm{Det}(\mathbf{r}_G(\varphi_s))^{-1} = \psi_2(\mathrm{Det}(\mathbf{r}_G(\varphi_s))) \cdot \mathrm{Det}(\mathbf{r}_G(\varphi_s))^{-2}.$$

Proof. Part (a) is proved in [2, Proposition 10.5(a)]. The proof of (b) is very similar, using [28, Proposition 4.2.2], which in fact shows the result for G abelian. Part (c) follows from parts (a) and (b), and Proposition 5.3. □

Corollary 5.5. *Suppose that $[\pi] \in H^1_t(L, G)$, and that $s := \pi(\sigma)$ is of odd order. Then a representing homomorphism for the class*

$$\mathfrak{c}(\pi) = [A_\pi, O_L G; \mathbf{r}_G] - [O_\pi, O_L G; \mathbf{r}_G]$$

in

$$K_0(O_L G, L) \simeq \frac{\mathrm{Det}(LG)^\times}{\mathrm{Det}(O_L G)^\times} \simeq \frac{\mathrm{Hom}_{\Omega_L}(R_G, (L^c)^\times)}{\mathrm{Det}(O_L G)^\times}$$

is the map $f_\pi \in \mathrm{Hom}_{\Omega_L}(R_G, (L^c)^\times)$ given by

$$f_\pi(\chi) = \varpi^{\langle \psi_2(\chi) - 2\chi, s\rangle_G}.$$

Proof. This follows from Propositions 4.6 and 5.4(c). □

6. Galois-Gauss and Galois-Jacobi sums

Let L be a local field of residual characteristic p. Suppose that $[\pi] \in H^1_t(L, G)$, and recall that we have (see (3.1))

$$L_\pi \simeq \prod_{\pi(\Omega_L)\backslash G} L^\pi.$$

Set $H := \pi(\Omega_L) = \mathrm{Gal}(L^\pi/L)$, and write $\tau^*(L^\pi/L, -) \in \mathrm{Hom}(R_H, (\mathbf{Q}^c)^\times)$ for the adjusted Galois-Gauss sum homomorphism associated to L^π/L (see [14, Chapter IV, (1.7)]). We define $\tau^*(L_\pi/L, -) \in \mathrm{Hom}(R_G, (\mathbf{Q}^c)^\times)$ by composing $\tau^*(L^\pi/L, -)$ with the natural map $R_G \to R_H$.

For a finite group Γ, we write $\mathrm{Irr}_p(\Gamma)$ for the set of $\mathbf{Q}_p^c$-valued irreducible characters of Γ and $R_{\Gamma,p}$ for the free abelian group on $\mathrm{Irr}_p(\Gamma)$. We fix a local embedding $\mathrm{Loc}_p : \mathbf{Q}^c \to \mathbf{Q}_p^c$, and we shall identify $\mathrm{Irr}(\Gamma)$ with $\mathrm{Irr}_p(\Gamma)$ via this choice of embedding.

For each rational prime $l \neq p$, we fix a semi-local embedding $\mathrm{Loc}_l : \mathbf{Q}^c \to (\mathbf{Q}^c)_l := \mathbf{Q}^c \otimes_{\mathbf{Q}} \mathbf{Q}_l$. (Caveat: note that this is not the same thing as a local embedding $\mathbf{Q}^c \to \mathbf{Q}_l^c$!) For each rational prime l, write $\mathbf{Q}_l^t$ for the maximal, tamely ramified extension of $\mathbf{Q}_l$.

We shall require the following results.

Proposition 6.1. *Fix a rational prime l.*

(a) *Let K be an unramified extension of $\mathbf{Q}_l$. Then, for any integer k, we have that*

$$\psi_k(\mathrm{Det}(O_K G)^\times) \subseteq \mathrm{Det}(O_K G)^\times.$$

(b) *Let Γ be a finite group with abelian p-Sylow subgroups. Then, for any integer k,*

$$\psi_k(\mathrm{Det}(O_{\mathbf{Q}_p^t}\Gamma)^\times) \subseteq \mathrm{Det}(O_{\mathbf{Q}_p^t}\Gamma)^\times.$$

(c) *Suppose that $l \neq p$. Then*

$$\mathrm{Loc}_l(\tau^*(L_\pi/L, -)) \in \mathrm{Det}(O_{\mathbf{Q}(\mu_p),l}G)^\times.$$

Proof. Parts (a) and (b) are results of Cassou-Noguès and Taylor. For part (a) see, e.g. [27, Chapter 9, Theorem 1.2], and note that for this particular result we do not need to assume that $(k, |G|) = 1$. For part (b) see [5, pp. 83, Remark].

Part (c) follows from [14, Chapter IV, Theorems 30], where analogous results are proved for $\tau^*(L^\pi/L, -)$; the corresponding results for $\tau^*(L_\pi/L, -)$ are then a direct consequence of the definition of $\tau^*(L_\pi/L, -)$. $\square$

The following result is entirely analogous to [14, Chapter IV, Lemma 2.1]. Recall that if $f \in \mathrm{Hom}(R_\Gamma, (\mathbf{Q}_p^c)^\times)$, then $\omega \in \Omega_{\mathbf{Q}_p}$ acts on f by the rule

$$f^\omega(\chi) = f(\chi^{\omega^{-1}})^\omega.$$

Lemma 6.2. *Let $L/\mathbf{Q}_p$ be a finite extension, and let $\{\nu\}$ be any right transversal of Ω_L in $\Omega_{\mathbf{Q}_p}$. Suppose that $f \in \mathrm{Hom}_{\Omega_{L^{\mathrm{nr}}}}(R_\Gamma, (\mathbf{Q}_p^c)^\times)$. Then (cf.* (2.5) *and* (2.6)*):*

$$\mathcal{N}_{L/\mathbf{Q}_p} f := \prod_\nu f^\nu \in \mathrm{Hom}_{\Omega_{\mathbf{Q}_p^{\mathrm{nr}}}}(R_\Gamma, (\mathbf{Q}_p^c)^\times).$$

Proof. It suffices to show that this result holds with respect to a particular choice of transversal of Ω_L in $\Omega_{\mathbf{Q}_p}$.

We first observe that, as $\Omega_{\mathbf{Q}_p^{\mathrm{nr}}}$ is normal in $\Omega_{\mathbf{Q}_p}$, $\Omega_L \cdot \Omega_{\mathbf{Q}_p^{\mathrm{nr}}}$ is a subgroup of $\Omega_{\mathbf{Q}_p}$. We choose a right transversal $\{\omega\}$ of $\Omega_L \cdot \Omega_{\mathbf{Q}_p^{\mathrm{nr}}}$ in $\Omega_{\mathbf{Q}_p}$.

Next, we choose a right transversal $\{\sigma\}$ of $\Omega_L \cap \Omega_{\mathbf{Q}_p^{\mathrm{nr}}}$ in $\Omega_{\mathbf{Q}_p^{\mathrm{nr}}}$. It follows that $\{\sigma\}$ is also a right transversal of Ω_L in $\Omega_L \cdot \Omega_{\mathbf{Q}_p^{\mathrm{nr}}}$. We now deduce that $\{\sigma\omega\}$ is a right transversal of Ω_L in $\Omega_{\mathbf{Q}_p}$. We also note that

$$\Omega_L \cap \Omega_{\mathbf{Q}_p^{\mathrm{nr}}} = \Omega_{L^{\mathrm{nr}}} \cap \Omega_{\mathbf{Q}_p^{\mathrm{nr}}},$$

and that (since $\Omega_{\mathbf{Q}_p^{\mathrm{nr}}}$ is normal in $\Omega_{\mathbf{Q}_p}$),

$$\omega_i^{-1}(\Omega_{L^{\mathrm{nr}}} \cap \Omega_{\mathbf{Q}_p^{\mathrm{nr}}})\omega_i = \omega_i^{-1}\Omega_{L^{\mathrm{nr}}}\omega_i \cap \Omega_{\mathbf{Q}_p^{\mathrm{nr}}}$$

for any $\omega_i \in \{\omega\}$.

Now suppose that $f \in \mathrm{Hom}_{\Omega_{L^{\mathrm{nr}}}}(R_\Gamma, (\mathbf{Q}_p^c)^\times)$ and that $\omega_i \in \{\omega\}$. Then

$$f^{\omega_i} \in \mathrm{Hom}_{\omega_i^{-1}\Omega_{L^{\mathrm{nr}}}\omega_i}(R_\Gamma, (\mathbf{Q}_p^c)^\times),$$

and so

$$f^{\omega_i} \in \mathrm{Hom}_{(\omega_i^{-1}\Omega_{L^{\mathrm{nr}}}\omega_i)\cap\Omega_{\mathbf{Q}_p^{nr}}}(R_\Gamma, (\mathbf{Q}_p^c)^\times).$$

Now observe that, for fixed $\omega_i \in \{\omega\}$, $\{\omega_i^{-1}\sigma\omega_i\}_\sigma$ is a right transversal of $\omega_i^{-1}\Omega_{L^{\mathrm{nr}}}\omega_i \cap \Omega_{\mathbf{Q}_p^{nr}}$ in $\Omega_{\mathbf{Q}_p^{\mathrm{nr}}}$, and so

$$\prod_\sigma (f^{\omega_i})^{\omega_i^{-1}\sigma\omega_i} \in \mathrm{Hom}_{\Omega_{\mathbf{Q}_p^{\mathrm{nr}}}}(R_\Gamma, (\mathbf{Q}_p^c)^\times).$$

Hence finally we obtain

$$\prod_{\omega,\sigma} (f^{\omega})^{\omega^{-1}\sigma\omega} = \prod_{\omega,\sigma} f^{\sigma\omega} \in \mathrm{Hom}_{\Omega_{\mathbf{Q}_p^{\mathrm{nr}}}}(R_\Gamma, (\mathbf{Q}_p^c)^\times),$$

as required. □

Proposition 6.3. *Let a_π be any n.i.b. generator of L_π/L. Suppose also that the square root A_π of the inverse different of L_π/L exists (i.e. that $s := \pi(\sigma)$ is of odd order), and that $A_\pi = O_L G \cdot b_\pi$. Then:*

(a) $\mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(b_\pi))^{-1} \cdot \psi_2(\mathrm{Det}(\mathbf{r}_G(a_\pi))) \cdot \mathrm{Det}(\mathbf{r}_G(a_\pi))^{-1}] \in \mathrm{Det}(O_{\mathbf{Q}_p^t}G)^\times$.

(b) (i) $\mathrm{Loc}_p[(\tau^*(L_\pi/L, -))]^{-1} \cdot \mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(a_\pi))] \in \mathrm{Det}(O_{\mathbf{Q}_p^t}G)^\times$.

(ii) $\mathrm{Loc}_p[\psi_2(\tau^*(L_\pi/L, -))]^{-1} \cdot \mathcal{N}_{L/\mathbf{Q}_p}[\psi_2(\mathrm{Det}(\mathbf{r}_G(a_\pi)))] \in \mathrm{Det}(O_{\mathbf{Q}_p^t}G)^\times$.

(c) $\mathrm{Loc}_p[\psi_2(\tau^*(L_\pi/L, -)) \cdot (\tau^*(L_\pi/L, -))^{-1}]^{-1} \cdot \mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(b_\pi))] \in \mathrm{Det}(O_{\mathbf{Q}_p^t}G)^\times$.

(d) $\mathrm{Loc}_p[\psi_2(\tau^*(L_\pi/L, -)) \cdot (\tau^*(L_\pi/L, -))^{-2}]^{-1} \cdot \mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(b_\pi)) \cdot \mathrm{Det}(\mathbf{r}_G(a_\pi))^{-1}]$ *belongs to* $\mathrm{Det}(O_{\mathbf{Q}_p^t}G)^\times$.

(e) *With the notation of Proposition 4.6, the element*

$$\mathrm{Loc}_p[\psi_2(\tau^*(L_\pi/L, -)) \cdot (\tau^*(L_\pi/L, -))^{-2}]^{-1} \cdot \mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(\varphi_s^*)) \cdot \mathrm{Det}(\mathbf{r}_G(\varphi_s))^{-1}]$$

belongs to $\mathrm{Det}(O_{\mathbf{Q}_p^t}G)^\times$.

Proof. (a) Recall from [2, Definition 7.12] that, for any n.i.b. generator a_π of L_π/L, one has

$$\mathbf{r}_G(a_\pi) = u \cdot \mathbf{r}_G(a_{nr}) \cdot \mathbf{r}_G(\varphi_s),$$

where $u \in (O_L G)^\times$ and $\mathbf{r}_G(a_{nr}) \in (O_{L^{nr}}G)^\times$. Furthermore, $u \cdot a_{nr}$ is also a n.i.b generator of $L_{\pi_{nr}}/L$.

Hence

$$\mathrm{Det}(\mathbf{r}_G(a_\pi)\cdot \mathbf{r}_G(\varphi_s)^{-1}) = \mathrm{Det}(u\cdot a_{\mathrm{nr}}) \in \mathrm{Det}(O_{L^{\mathrm{nr}}}G)^\times,$$

and Lemma 6.2 implies that also

$$\mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(a_\pi)\cdot \mathbf{r}_G(\varphi_s)^{-1})] \in \mathrm{Det}(O_{\mathbf{Q}_p^{nr}}G)^\times,$$

It now follows from Proposition 6.1 that the product

$$\mathcal{N}_{L/\mathbf{Q}_p}[(\mathrm{Det}(\mathbf{r}_G(a_\pi))\cdot \mathrm{Det}(\mathbf{r}_G(\varphi_s))^{-1})^{-1}\cdot \psi_2\big(\mathrm{Det}(\mathbf{r}_G(a_\pi))\cdot \mathrm{Det}(\mathbf{r}_G(\varphi_s))^{-1}\big)] \tag{6.1}$$

belongs to $\mathrm{Det}(O_{\mathbf{Q}_p^{nr}}G)^\times$.

Part (a) now follows from (6.1), together with Proposition 5.4(c) and the Stickelberger factorisation of $\mathbf{r}_G(b_\pi)$ (see Theorem 4.5).

(b) Let O^π denote the integral closure of O_L in L^π and fix an element $\alpha \in L^\pi$ such that $O^\pi = O_L H\cdot\alpha$. It follows from [14, Chapter IV, Theorem 31] that there exists an element $w\in (O_{\mathbf{Q}_p^t}H)^\times$ such that

$$\mathrm{Loc}_p(\tau^*(L^\pi/L,-))^{-1}\cdot \mathcal{N}_{L/\mathbf{Q}_p}\mathrm{Det}(\mathbf{r}_H(\alpha)) = \mathrm{Det}(w) \tag{6.2}$$

Under our hypotheses, the inertia subgroup of H is cyclic of order $|s|$ coprime to p. Hence Proposition 6.1(b) implies that

$$\mathrm{Loc}_p[\psi_2(\tau^*(L^\pi/L,\,-))]^{-1}\cdot \mathcal{N}_{L/\mathbf{Q}_p}[\psi_2(\mathrm{Det}(\mathbf{r}_H(\alpha)))] \tag{6.3}$$

belongs to $\psi_2(\mathrm{Det}(O_{\mathbf{Q}_p^t}H)^\times) \subseteq \mathrm{Det}(O_{\mathbf{Q}_p^t}H)^\times \subseteq \mathrm{Det}(O_{\mathbf{Q}_p^t}G)^\times$.

Next, we construct a map $a_\pi\in \mathrm{Map}(G,L^c)$ associated to α by setting

$$a_\pi(\gamma) := \begin{cases} \tilde\gamma(\alpha), & \text{if} \quad \gamma=\pi(\tilde\gamma) \text{ for } \tilde\gamma\in\Omega_L;\\ 0, & \text{otherwise.}\end{cases}$$

It is easy to see from (3.1) that $a_\pi\in L_\pi$ and satisfies that $O_\pi = O_L G\cdot a$. In particular, for each $\chi\in R_G$, we have

$$\mathrm{Det}_\chi(\mathbf{r}_G(a_\pi)) = \mathrm{Det}_\chi\big(\sum_{\gamma\in G} a_\pi(\gamma)\gamma^{-1}\big) = \mathrm{Det}_\chi\big(\sum_{\gamma\in H}\tilde\gamma(\alpha)\gamma^{-1}\big) = \mathrm{Det}_{\mathrm{res}\chi}(\mathbf{r}_H(\alpha)),$$

with $\mathrm{res} := \mathrm{res}^G_H : R_+G \to R_H$. This implies that

$$\begin{aligned} \mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(a_\pi))] = &\quad \mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_H(\alpha))],\\ \mathcal{N}_{L/\mathbf{Q}_p}[\psi_2(\mathrm{Det}(\mathbf{r}_G(a_\pi)))] = &\quad \mathcal{N}_{L/\mathbf{Q}_p}[\psi_2(\mathrm{Det}(\mathbf{r}_H(\alpha)))].\end{aligned} \tag{6.4}$$

We now see from the definition of $\tau^*(L_\pi/L,-)$ that (i) follows from (6.2), (6.4), while part (ii) is a consequence of (6.3) and (6.4).

(c) Follows from (a) and (b) above.

(d) Follows from (b)(i) together with (c).

(e) Follows from (d) above.

□

Proposition 6.3(d) and (e) motivate the following definition.

Definition 6.4. We retain the notation established above. Define the *adjusted Galois-Jacobi sum homomorphism associated to* L_π/L, $J^*(L_\pi/L,-) \in \mathrm{Hom}(R_G, (\mathbf{Q}^c)^\times)$, by

$$J^*(L_\pi/L,-) := \psi_2(\tau^*(L_\pi/L,-)) \cdot (\tau^*(L_\pi/L,-))^{-2}.$$

It follows from the Galois action formulae for Galois-Gauss sums (see [14, pp. 119 and 152]) that in fact $J^*(L_\pi/L,-) \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, (\mathbf{Q}^c)^\times)$. □

Remark 6.5. Let $\tau(L^\pi/L,-) \in \mathrm{Hom}(R_H, (\mathbf{Q}^c)^\times)$ denote the (unadjusted) Galois-Gauss sum associated to L^π/L, and write $\tau(L_\pi/L,-) \in \mathrm{Hom}(R_G, (\mathbf{Q}^c)^\times)$ for the composition of $\tau(L^\pi/L,-)$ with the natural map $R_G \to R_H$. We remark that the Galois-Jacobi sum $J(L_\pi/L,-) \in \mathrm{Hom}(R_G, (\mathbf{Q}^c)^\times)$ defined by

$$J(L_\pi/L,-) := \psi_2(\tau(L_\pi/L,-)) \cdot (\tau(L_\pi/L,-))^{-2}$$

is a special case of the non-abelian Jacobi sums first introduced by A. Fröhlich (see [13]). □

Proposition 6.6.

(a) *Suppose that* $l \neq p$. *Then*

$$\mathrm{Loc}_l(J^*(L_\pi/L,-)) \in \mathrm{Det}(\mathbf{Z}_l G^\times).$$

(b) *Using the notation of Proposition 6.3, we have*

$$\mathrm{Loc}_p(J^*(L_\pi/L,-))^{-1} \cdot \mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(b_\pi)) \cdot \mathrm{Det}(\mathbf{r}_G(a_\pi))^{-1}] \in \mathrm{Det}(\mathbf{Z}_p G^\times).$$

Hence

$$\mathrm{Loc}_p(J^*(L_\pi/L,-))^{-1} \cdot \mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(\varphi_s^*)) \cdot \mathrm{Det}(\mathbf{r}_G(\varphi_s))^{-1}] \in \mathrm{Det}(\mathbf{Z}_p G^\times).$$

Proof. (a) Recall that $J^*(L_\pi/L,-) \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_G, (\mathbf{Q}^c)^\times)$, and that $\mathbf{Q}(\mu_p)/\mathbf{Q}$ is unramified at l. It therefore follows from Proposition 6.1 (a) and (c), together with Taylor's fixed point theorem for determinants (see [27, Chapter 8, Theorem 1.2]), that

$$\mathrm{Loc}_l(J^*(L_\pi/L,-)) \in [\mathrm{Det}(O_{\mathbf{Q}_l(\mu_p)} G^\times)]^{\Omega_{\mathbf{Q}_l}} = \mathrm{Det}(\mathbf{Z}_l G^\times),$$

as claimed.

(b) As both of the functions $\mathrm{Loc}_p(J^*(L_\pi/L,\,-))$ and $\mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(b_\pi))\cdot\mathrm{Det}(\mathbf{r}_G(a_\pi))^{-1}]$ lie in $\mathrm{Hom}_{\Omega_{\mathbf{Q}_p}}(R_G,(\mathbf{Q}_p^c)^\times)$, we see from Proposition 6.3(d) that

$$\mathrm{Loc}_p(J^*(L_\pi/L,\,-))^{-1}\cdot\mathcal{N}_{L/\mathbf{Q}_p}[\mathrm{Det}(\mathbf{r}_G(b_\pi))\cdot\mathrm{Det}(\mathbf{r}_G(a_\pi))^{-1}]\in[\mathrm{Det}(O_{\mathbf{Q}_p^t}G^\times)]^{\Omega_{\mathbf{Q}_p}}=\mathrm{Det}(\mathbf{Z}_pG^\times).$$

The final assertion now follows at once from the Stickelberger factorisations of $\mathbf{r}_G(a_\pi)$ and $\mathbf{r}_G(b_\pi)$ (see Theorems 4.3 and 4.5). □

7. Symplectic Galois-Jacobi sums I

In this section we fix data L, G and π as in Section 6. We write $\mathrm{Symp}(G)$ for the set of irreducible symplectic characters of G. For each $\chi\in\mathrm{Irr}(G)$, we write $\tau(L_\pi/L,\chi)$ for the associated (unadjusted) Galois-Gauss sum, and

$$J(L_\pi/L,\,-):=\psi_2(\tau(L_\pi/L,\,-))\cdot(\tau(L_\pi/L,\,-))^{-2}$$

for the (unadjusted) Galois-Jacobi sum (see Remark 6.5).

We shall prove the following result concerning symplectic Galois-Jacobi sums.

Theorem 7.1. *Suppose that $\chi\in\mathrm{Symp}(G)$. Then $J(L_\pi/L,\chi)$ is a strictly positive real number.*

We see from the decomposition (3.1) that it is enough to prove this result after replacing the Galois algebra L_π by the field L^π and the group G by the Galois group $\pi(\Omega_L)=\mathrm{Gal}(L^\pi/L)$. In the sequel, we shall therefore restrict to the case that L_π/L is a finite Galois extension of p-adic fields and G is its Galois group.

To prove Theorem 7.1, it is therefore enough to show that for each χ in $\mathrm{Symp}(G)$ the quotient $\tau(L,\psi_2(\chi))/\tau(L,2\chi)$ is a strictly positive real number.

To verify this, we recall that, since each such χ is real-valued, the definition of the local root number $W(L,\chi)$ implies that

$$\tau(L,\chi)=W(L,\chi)\cdot\mathbf{N}_L\mathfrak{f}(L_\pi/L,\chi)^{1/2}.$$

(cf. [18, Chapter II, Section 4, Definition]). Hence, since $\mathbf{N}_L\mathfrak{f}(L_\pi/L,\chi)^{1/2}>0$, it is enough to prove the following result.

Theorem 7.2. *Let E/F be a tamely ramified Galois extension of non-archimedean local fields that has odd ramification degree and set $G:=\mathrm{Gal}(E/F)$. Then for each χ in $\mathrm{Symp}(G)$ one has $W(F,\psi_2(\chi))=W(F,2\chi)=1$.*

This sort of result is, in principle, hard to prove both because root numbers of symplectic characters are difficult to compute and because Adams operators do not in general commute with induction functors. We therefore prove two preliminary results that help address these problems.

The first of these results is entirely representation-theoretic in nature.

In the sequel, for any finite group Γ and character ϕ in R_Γ, we write $\mathrm{Tr}(\phi)$ for the real-valued character $\phi + \overline{\phi}$.

Lemma 7.3. *Let Δ be a subgroup of a finite group Γ, fix a character ϕ of Δ and consider the virtual character*

$$\mathrm{I}^2_\Gamma(\phi) := \psi_2(\mathrm{Ind}^\Gamma_\Delta(\phi)) - \mathrm{Ind}^\Gamma_\Delta(\psi_2(\phi)).$$

For elements γ and δ of Γ, we set $\gamma^\delta := \delta\gamma\delta^{-1}$.

(a) *Let $\mathcal{T}$ be a set of coset representatives of Δ in Γ. Then for every $\gamma \in \Gamma$, one has*

$$(\mathrm{I}^2_\Gamma(\phi))(\gamma) = \sum_\tau \phi((\gamma^\tau)^2),$$

where the sum runs over all $\tau \in \mathcal{T}$ for which $(\gamma^\tau)^2 \in \Delta$ and $\gamma^\tau \notin \Delta$.

(b) *If Δ is a subnormal subgroup of Γ of odd index, then $\mathrm{I}^2_\Gamma(\phi) = 0$.*

(c) *Assume Γ is a semi-direct product of a supersolvable group by an abelian normal subgroup Υ.*

(i) *Then for every irreducible character μ of Γ, there exists a subgroup Υ' of Γ that contains Υ and a linear character λ of Υ' such that $\mu = \mathrm{Ind}^\Gamma_{\Upsilon'}(\lambda)$.*

In addition, if $\Upsilon \subseteq \Delta$, the index of Δ in Γ is a power of 2 and Γ has cyclic Sylow 2-subgroups, then the following claims are also valid.

(ii) *If ϕ is real-valued, then $\mathrm{I}^2_\Gamma(\phi)$ is an integral linear combination of characters of the form $\mathrm{Ind}^\Gamma_{\Delta'}\lambda$ and $\mathrm{Tr}(\phi')$, where Δ' runs over subgroups of Γ that contain Δ, λ over homomorphisms $\Delta' \to \{\pm 1\}$ and ϕ' over elements of R_Γ.*

(iii) *If ϕ is induced from a proper normal subgroup of Δ of 2-power index that contains Υ, then $\mathrm{I}^2_\Gamma(\phi) = 0$.*

(d) *Assume Γ is generalized quaternion, Δ is the cyclic subgroup of Γ of index 2 and ϕ is irreducible (and hence linear). Then ϕ^2 is trivial on the centre Z of Γ and*

$$\psi_2\big(\mathrm{Ind}^\Gamma_\Delta\phi\big) = \mathrm{Inf}^\Gamma_{\Gamma/Z}\big(\mathrm{Ind}^{\Gamma/Z}_{\Delta/Z}(\phi^2)\big) + \mathrm{Inf}^\Gamma_{\Gamma/\Delta}(\chi_{\Gamma/\Delta}) - \mathbf{1}_\Gamma,$$

where we regard ϕ^2 as a character of Δ/Z and write $\chi_{\Gamma/\Delta}$ for the unique non-trivial homomorphism $\Gamma/\Delta \to (\mathbf{Q}^c)^\times$.

Proof. Part (a) follows directly from the explicit formula for induced characters and the fact that for each $\gamma \in \Gamma$, and $\tau \in \mathcal{T}$ one has $(\gamma^\tau)^2 \in \Delta$ whenever $\gamma^\tau \in \Delta$.

To prove part (b), we fix a chain of subgroups

$$\Delta = \Gamma(1) \subset ... \subset \Gamma(t-1) \subset \Gamma(t) = \Gamma \tag{7.1}$$

such that each $\Gamma(i)$ is normal in $\Gamma(i+1)$. Then the equality

$$\mathrm{I}^2_\Gamma(\phi) = \sum_{i=1}^{i=t-1} \mathrm{Ind}^\Gamma_{\Gamma(i+1)}\big(\mathrm{I}^2_{\Gamma(i+1),\Gamma(i)}(\mathrm{Ind}^{\Gamma(i)}_\Delta \phi)\big), \tag{7.2}$$

where

$$\mathrm{I}^2_{\Gamma(i+1),\Gamma(i)}(\chi) = \psi_2(\mathrm{Ind}^{\Gamma(i+1)}_{\Gamma(i)}\chi) - \mathrm{Ind}^{\Gamma(i+1)}_{\Gamma(i)}(\psi_2(\chi)),$$

reduces us to the case Δ is normal in Γ. In this case, the claim follows immediately from the formula in part (a) and the fact that, under the stated conditions, for every $\gamma \in \Gamma$ and $\tau \in \mathcal{T}$ one has $(\gamma^\tau)^2 \in \Delta \iff \gamma^\tau \in \Delta$.

Turning to part (c), we note first that, under the stated hypothesis on Γ, claim (c)(i) follows from [22, Section 8.5, Exercise 8.10] and the argument of [22, Section 8.2, Proposition 25].

To verify (c)(ii) and (c)(iii) we assume the additional hypotheses on Γ and note, in particular, that since Γ has cyclic Sylow 2-subgroups, Cayley's normal 2-complement theorem implies that Γ, and therefore also its quotient Γ/Υ, has a normal 2-complement. Writing Υ_1/Υ for the normal 2-complement of Γ/Υ, the given assumptions imply $\Upsilon_1 \subseteq \Delta$ and so, since Γ/Υ_1 is cyclic of 2-power order, there exists a chain of subgroups (7.1) in which $\Gamma(i)$ has index 2 in $\Gamma(i+1)$ for each i. The corresponding equality (7.2) then reduces claims (c)(ii) and (c)(iii) to the case that Δ has index two in Γ. In this case $|\mathcal{T}| = 2$ and, for every $\gamma \in \Gamma$ and $\tau \in \mathcal{T}$, one has $(\gamma^\tau)^2 \in \Delta$ and, in addition, $\gamma^\tau \notin \Delta \iff \gamma \notin \Delta$ and so the formula in part (a) implies

$$(I^2_\Gamma(\phi))(\gamma) = \begin{cases} 0, & \text{if } \gamma \in \Delta, \\ \sum_{\tau\in\mathcal{T}} \phi((\gamma^\tau)^2), & \text{if } \gamma \notin \Delta. \end{cases} \tag{7.3}$$

Now, by (c)(i), every irreducible character of Γ has the form $\mu = \mathrm{Ind}^\Gamma_{\Upsilon'}(\lambda)$, where Υ' is a suitable subgroup of Γ that contains Υ and λ a linear character of Υ'. Further, if $\Upsilon' \not\subset \Delta$, then the index of Υ' in Γ is odd so μ has odd degree and so, by [20, Theorem A], is real-valued if and only if it is a homomorphism of the form $\Upsilon' \to \{\pm 1\}$. Claim (c)(ii) follows directly from this fact and the observation that $I^2_\Gamma(\phi)$ is real-valued if ϕ is real-valued.

To prove claim (c)(iii), we assume $\phi = \mathrm{Ind}^\Delta_{\Delta'}\phi'$, where Δ' is a normal subgroup of Δ that contains Υ and is of 2-power index. In this case, the formula (7.3) implies that if $I^2_\Gamma(\phi)$ is non-zero, then there exists an element of $\Gamma \setminus \Delta$ whose square belongs to Δ'. However, since $\Upsilon_1 \subseteq \Delta'$, the image in the (cyclic) group Γ/Δ' of any element in $\Gamma \setminus \Delta$ has order divisible by 4 and so its square cannot belong to Δ'. This proves (c)(iii).

Next, under the hypotheses of (d), for every $\gamma \in \Gamma$ one has $\gamma^2 \in \Delta$ and hence

$$\big(\psi_2(\mathrm{Ind}_\Delta^\Gamma \phi)\big)(\gamma) = (\mathrm{Ind}_\Delta^\Gamma \phi)(\gamma^2) = \phi^2(\gamma) + \phi^2(\gamma^{-1}).$$

In particular, since $\phi^2(z) = 1$ for every $z \in Z$, this formula implies $\psi_2(\mathrm{Ind}_\Delta^\Gamma \phi)$ is the inflation of a character function on the dihedral group Γ/Z, and then the displayed formula in part (d) is verified by an easy explicit computation. □

In the sequel, for each finite Galois extension E/F of p-adic fields, and each complex character χ of $\mathrm{Gal}(E/F)$ we abbreviate the root number $W(F, \chi)$ to $W(\chi)$.

Part (c) of the following result relies on the central result of Fröhlich and Queyrut in [16].

Proposition 7.4. *Let E/F be a finite Galois extension of p-adic fields. Set $G := \mathrm{Gal}(E/F)$ and assume that the inertia subgroup of G has odd order.*

(a) *For all ϕ in R_G one has $W(\mathrm{Tr}(\phi)) = 1$.*

(b) *If H is a normal subgroup of G and G/H is cyclic, then for each ϕ in R_H one has*

$$W(\mathrm{Ind}_H^G \phi) = \begin{cases} W(\phi), & \text{if } G/H \text{ has odd order,} \\ W(\phi)W(\chi_{G/H})^{\phi(1)}, & \text{if } G/H \text{ has even order,} \end{cases}$$

where, in the second case, $\chi_{E'/F}$ is the non-trivial character of $\mathrm{Gal}(E'/F)$, with E' the quadratic extension of F in E.

(c) *Assume G is dihedral of order congruent to 2 modulo 4, write L for the unique quadratic extension of F in E and set $H := \mathrm{Gal}(E/L)$. Then for each homomorphism $\phi : H \to (\mathbf{Q}^c)^\times$, one has $W(\mathrm{Ind}_H^G \phi) = W(\chi_{G/H})$, where $\chi_{G/H}$ is the non-trivial character of G/H.*

Proof. It is enough to prove claim (a) in the case that ϕ is a character of G, represented by a homomorphism $T_\phi : G \to \mathrm{GL}_d(\mathbf{Q}^c)$. In this case, the general result of [18, Chapter II, Section 4, Corollary] implies that

$$W(\mathrm{Tr}(\phi)) = W(\phi)W(\bar{\phi}) = \det_\phi(\rho_F(-1)),$$

where $\det_\phi$ is the homomorphism $G^{\mathrm{ab}} \to (\mathbf{Q}^c)^\times$ induced by sending each g in G to $\det(T_\phi(g))$ and ρ_F is the reciprocity map $F^\times \to G^{\mathrm{ab}}$. In addition, -1 belongs to $O_F^\times$ and so is sent by ρ_F to an element of the inertia subgroup of G^{ab} of order dividing two. In particular, since this inertia group has odd order, one has $\rho_F(-1) = 1$ and so $\det_\phi(\rho_F(-1)) = 1$. This proves claim (a).

To prove part (b), we use the inductivity of local root numbers in degree zero to compute

$$\begin{aligned}W(\mathrm{Ind}_H^G\phi) &= W(\mathrm{Ind}_H^G(\phi - \phi(1)\mathbf{1}_H))W(\mathrm{Ind}_H^G 1_H)^{\phi(1)}\\ &= W(\phi - \mathbf{1}_H)W(\mathrm{Ind}_H^G\mathbf{1}_H)^{\phi(1)}\\ &= W(\phi)W(\mathbf{1}_H)^{-1}\prod_{\theta\in(G/H)^*} W(\theta)^{\phi(1)},\end{aligned}$$

where $(G/H)^*$ denotes the group of homomorphisms $G/H \to (\mathbf{Q}^c)^\times$, and the last equality is true because $\mathrm{Ind}_H^G\mathbf{1}_H$ is equal to the sum of θ over $(G/H)^*$. Now, if G/H is odd, respectively even, then the only real-valued functions in $(G/H)^*$ are $\mathbf{1}_G$, respectively $\mathbf{1}_G$ and $\chi_{G/H}$, and all other homomorphisms occur in complex conjugate pairs. The result of part (b) therefore follows from the above displayed formula after isolating the conjugate pairs in the product that occurs in the final term, applying the result of part (a) to each of these pairs, and noting that $W(\mathbf{1}_H) = W(\mathbf{1}_G) = 1$.

To prove part (c) we recall that, by a result of Fröhlich and Queyrut [16, Section 4, Theorem 3], one has $W(\phi) = \phi(\rho_L(x))$, where ρ_L is the reciprocity map $L^\times \to H$ and x is any element of $L \setminus F$ with $x^2 \in F^\times$. In addition, since ϕ is of dihedral-type, it is trivial on restriction to $F^\times$ (cf. [16, Section 3, Lemma 1]) and so $\phi(\rho_L(x))^2 = \phi(\rho_L(x^2)) = \phi(1) = 1$. On the other hand, the order of ϕ is odd (since it divides $|H| = |G|/2$ which, under the given hypothesis on $|G|$, is odd) and so $\phi(\rho_L(x))^2 = 1$ implies $\phi(\rho_L(x)) = 1$ and hence also $W(\phi) = 1$.

This last equality then combines with a straightforward application of the general result of part (b) to prove the formula in part (c). □

We are now ready to prove Theorem 7.2. At the outset we note that G is the semi-direct product of its inertia subgroup I by the cyclic quotient group G/I. We further note that, by assumption, the group I is cyclic of odd order, and hence, in particular, that G is supersolvable.

Fix χ in $\mathrm{Symp}(G)$. Then, since χ is tamely ramified, one has $W(\chi) \in \{\pm 1\}$ (cf. [14, Chapter III, Theorem 21(iii)]) and so $W(2\chi) = W(\chi)^2 = 1$. It is therefore enough for us to prove that $W(\psi_2(\chi)) = 1$.

Next we note that, by Lemma 7.3(c)(i), there exists a subgroup J of G that contains I and a linear character ϕ of J such that one has $\chi = \mathrm{Ind}_J^G\phi$. In particular, since J contains I and G/I is cyclic, there exists a normal subgroup H of G with $J \trianglelefteq H \trianglelefteq G$ and such that H/J is cyclic of 2-power order and G/H is cyclic of odd order.

Then one has $\chi = \mathrm{Ind}_H^G\chi'$ with $\chi' := \mathrm{Ind}_J^H\phi$ and we claim that χ' belongs to $\mathrm{Symp}(H)$. To see this we note χ' is an irreducible character of H (since χ is irreducible) and so, by the

Frobenius-Schur Theorem (cf. [9, Theorem (73.13)]), the sum $c_H(\chi') := |H|^{-1}\sum_{h\in H}\chi(h^2)$ belongs to $\{-1,0,1\}$ and is equal to -1 if and only if χ' is symplectic. In addition, since H is normal in G and of odd index one has $g^2\in H \iff g\in H$ for each $g\in G$ and so

$$\begin{aligned}
c_G(\chi) = c_G(\mathrm{Ind}_H^G\chi') &= |G|^{-1}\sum_{g\in G}(\mathrm{Ind}_H^G\chi')(g^2)\\
&= |G|^{-1}\sum_{\tau\in\mathcal{T}}\sum_{h\in H}(\chi')^\tau(h^2)\\
&= |\mathcal{T}|^{-1}\sum_{\tau\in\mathcal{T}}c_H((\chi')^\tau)
\end{aligned}$$

where $\mathcal{T}$ is a set of coset representatives of H in G and $(\chi')^\tau$ is the irreducible character of H that sends each element h to $\chi'(h^\tau)$. In particular, since both $c_G(\chi)=-1$ (as $\chi\in\mathrm{Symp}(G)$) and each $c_H((\chi')^\tau)$ belongs to $\{-1,0,1\}$, the displayed equality implies that $c_H((\chi')^\tau)=-1$ for all τ. Thus one has $c_H(\chi')=-1$ and so $\chi'\in\mathrm{Symp}(H)$, as claimed.

Now, since G/H is cyclic of odd order, one has $W(\psi_2(\chi)) = W(\mathrm{Ind}_H^G(\psi_2(\chi')) = W(\psi_2(\chi'))$, where the first equality follows from Lemma 7.3(b) and the second from Proposition 7.4(b). Thus, if necessary after replacing G by H (and χ by χ'), we can assume in the sequel that χ has 2-power degree.

Next we note that, since G is supersolvable, an induction theorem of Martinet (cf. [18, Chapter III, Theorem 5.2]) implies that either $\chi = \mathrm{Tr}(\mathrm{Ind}_{H'}^G\phi')$, where ϕ' is a linear character of some subgroup H' of G, or that χ is the induction to G of a quaternion character of a subgroup. In view of Proposition 7.4(a), we can therefore also assume in the sequel that there exists a subgroup J_1 of G that has 2-power index, and hence contains I, and a quaternion character ϕ_1 of J_1 such that $\chi = \mathrm{Ind}_{J_1}^G\phi_1$.

This implies J_1 has a quotient Q isomorphic to a generalized quaternion group and that

$$\phi_1 = \mathrm{Inf}_Q^{J_1}(\mathrm{Ind}_P^Q\theta), \tag{7.4}$$

where P is the cyclic subgroup of Q of index 2 and θ a homomorphism $P\to(\mathbf{Q}^c)^\times$. Let J_1' denote the inverse image of P under the quotient map $J_1\to Q$, and set $\phi_1' := \mathrm{Inf}_P^{J_1'}\theta$ (so ϕ_1' is a linear character of J_1'). Then the subgroup J_1' is of index 2 in J_1, and (7.4) implies

$$\phi_1 = \mathrm{Ind}_{J_1'}^{J_1}\phi_1'. \tag{7.5}$$

Now, as J_1' has 2-power index in G, it contains I. Thus, since G/I is cyclic, one has $J_1'\trianglelefteq G$ and G/J_1' is cyclic of 2-power order. In particular, since the degree $(\psi_2(\phi_1))(1)=\phi_1(1)$ is even, one therefore has

$$W(\psi_2(\chi)) = W(\psi_2(\mathrm{Ind}_{J_1}^G\phi_1)) = W(\mathrm{Ind}_{J_1}^G(\psi_2(\phi_1))) = W(\psi_2(\phi_1)),$$

where the second equality follows from Lemma 7.3(c)(iii) (after taking account of (7.5)) and the third from Proposition 7.4(b).

In addition, since Q is the Galois group of a tamely ramified extension of p-adic fields that has odd ramification degree, it is the semi-direct product of a cyclic (inertia) subgroup of odd order by a cyclic group. In particular, since such a group can have no quotient isomorphic to H_8, the group Q must be isomorphic to H_{4m}, with m odd. In view of (7.4), we can therefore apply Lemma 7.3(d) (with Γ, Δ and ϕ taken to be Q, P and θ) to deduce that

$$W(\psi_2(\phi_1)) = W(\psi_2(\mathrm{Ind}_P^Q\theta)) = W(\mathrm{Ind}_{P/N}^{Q/N}(\lambda))W(\chi_{Q/P}),$$

where N denotes the centre of Q (so N is the unique subgroup of P of order two) and λ denotes θ^2, regarded as a homomorphism $P/N \to (\mathbf{Q}^c)^\times$.

Finally, since the group Q/N is generalized dihedral with $|Q/N| = 2m \equiv 2$ modulo 4, and the inertia subgroup of Q/N has odd order, the theorem of Fröhlich and Queyrut implies (via Proposition 7.4(c)) that $W(\mathrm{Ind}_{P/N}^{Q/N}(\lambda)) = W(\chi_{Q/P})$. Upon subsituting this fact into the last two displayed formulas, we deduce that $W(\psi_2(\chi)) = W(\chi_{Q/P})^2 = 1$.

This completes the proof of Theorem 7.1.

8. Symplectic Galois-Jacobi Sums II

We retain the notation of the previous two sections. For any real number x, we write $\mathrm{sgn}(x) \in \{\pm 1\}$ for the sign of x. In this section we shall examine $\mathrm{sgn}(J^*(L_\pi/L, \chi))$ for $\chi \in \mathrm{Symp}(G)$. This will in turn lead to the definition of $\mathcal{J}^*_\infty(F_\pi/F) \in \mathrm{Cl}(\mathbf{Z}G)$ for F a number field and $[\pi] \in H^1_t(F, G)$.

Recall that for each $\chi \in R_G$, the adjusted Galois-Gauss sum is defined (in [14, Chapter IV, Section 1]) by setting

$$\tau^*(L, \chi) := \tau(L, \chi)y(L, \chi)^{-1}z(L, \chi),$$

for suitable roots of unity $y(L, \chi)$ and $z(L, \chi)$ in $\mathbf{Q}^c$. [14, Chapter IV, Theorem 29(i)] implies that $y(K, \chi) = 1$ for all χ in $\mathrm{Symp}(G)$. One can also check (directly from the definitions) that $z(L, \psi_2(\chi)) = z(L, \chi)^2$ and hence that $z(L, \chi) = z(L, \psi_2(\chi)) = 1$ for each χ in $\mathrm{Symp}(G)$.

Recall that Theorem 7.1 asserts that $J(L_\pi/L, \chi) > 0$ whenever $\chi \in \mathrm{Symp}(G)$. The following result is now a direct consequence of the definition of the adjusted Galois-Jacobi sum $J^*(L_\pi/L, \chi)$.

Theorem 8.1. *Suppose that $\chi \in \mathrm{Symp}(G)$. Then*

$$\mathrm{sgn}(J^*(L_\pi/L, \chi) = \mathrm{sgn}(y(L_\pi/L, \psi_2(\chi))).$$

□

The following Propostion shows that $\mathrm{sgn}(y(L_\pi/L,\psi_2(\chi))) = -1$ is possible.

Proposition 8.2. *Let M/L be a tamely ramified Galois extension with $\Gamma := \mathrm{Gal}(M/L) \simeq H_{4m}$, with m odd. Suppose that the inertia subgroup Γ_0 of Γ is odd. Then for each $\chi \in \mathrm{Symp}(G)$, we have $y(M/L,\psi_2(\chi)) = -1$.*

Proof. For ease of notation, we write e.g. $y(\chi)$ rather than $y(M/L,\chi)$.

To prove the desired result, we shall use Lemma 7.3. Let Δ be the cyclic subgroup of Γ of index 2. Then all irreducible symplectic characters of Γ can be written in the form $\chi = \mathrm{Ind}_\Delta^\Gamma \phi$, where ϕ is a linear character of Δ. It is easy to see that the order of ϕ does not divide 2 (for otherwise $\mathrm{Ind}_\Delta^\Gamma\phi$ would be an orthogonal character of Γ; see [18, Chapter III, Theorem 3.1]), and that ϕ (and hence also ϕ^2) is non-trivial on Γ_0 (since Γ_0 has odd order).

Let Z denote the centre of Γ and let $\chi_{\Gamma/\Delta}$ denote the unique non-trivial homomorphism $\Gamma/\Delta \to (\mathbf{Q}^c)^\times$. Using the formula in Lemma 7.3(d), one can compute that

$$\begin{aligned} y(\psi_2(\chi)) &= y(\psi_2(\mathrm{Ind}_\Delta^\Gamma\phi)) \\ &= y(\mathrm{Inf}_{\Gamma/Z}^\Gamma(\mathrm{Ind}_{\Delta/Z}^{\Gamma/Z}(\phi^2)))\cdot y(\mathrm{Inf}_{\Gamma/\Delta}^\Gamma(\chi_{\Gamma/\Delta}))\cdot y(\mathbf{1}_\Gamma)^{-1} \\ &= (-1)^{\deg(n_0)}\mathrm{det}_{n_0}(\sigma)\cdot(-1)\chi_{\Gamma/\Delta}(\sigma)\cdot(-1)\mathbf{1}_\Gamma(\sigma)^{-1} \\ &= 1\cdot 1\cdot(-1) = -1, \end{aligned}$$

where ϕ^2 is regarded as a character of Γ/Z, σ is the Frobenius element in Γ/Γ_0 lifted to Γ, and $n_0 := n(\mathrm{Inf}_{\Gamma/Z}^\Gamma(\mathrm{Ind}_{\Delta/Z}^{\Gamma/Z}(\phi^2)))$ denotes the unramified part (cf. [14, Chapter I, (5.6)]) of $\mathrm{Inf}_{\Gamma/Z}^\Gamma(\mathrm{Ind}_{\Delta/Z}^{\Gamma/Z}(\phi^2))$. The third equality above holds since clearly $\mathrm{Inf}_{\Gamma/\Delta}^\Gamma(\chi_{\Gamma/\Delta})$ and $\mathbf{1}_\Gamma$ are both linear and unramified. The fourth equality follows from the fact that $n_0 = 0$ (since ϕ^2 is irreducible and ramified, by [14, Chapter III, Proposition 1.3(ii)] the unramified part $n(\mathrm{Ind}_{\Delta/Z}^{\Gamma/Z}(\phi^2)) = 0$ and therefore $n_0 = 0$). □

The above discussion motivates the following definition.

Definition 8.3. We define $J_\infty^*(L_\pi/L,-) \in \mathrm{Hom}_{\Omega_\mathbf{Q}}(R_G, J(\mathbf{Q}^c))$ by its values on $\chi \in \mathrm{Irr}(G)$ as follows:

$$J_\infty^*(L_\pi/L,\chi)_v = \begin{cases} \mathrm{sgn}(J^*(L_\pi/L,\chi)) & \text{if } \chi \in \mathrm{Symp}(G) \text{ and } v|\infty; \\ 1 & \text{otherwise.} \end{cases}$$

We write $J_\infty^*(L_\pi/L)$ for the element of $K_0(\mathbf{Z}G,\mathbf{Q})$ represented by the homomorphism $J_\infty^*(L_\pi/L,-)$. Similarly, we also write $J^*(L_\pi/L)$ for the element of $K_0(\mathbf{Z}G,\mathbf{Q})$ represented by $J^*(L_\pi/L,-)$. □

Theorem 8.4. *We have*

$$J^*(L_\pi/L,-)\cdot J^*_\infty(L_\pi/L,-)^{-1}\in \mathrm{Det}(\mathbf{Q}^cG),$$

and so

$$\partial^0(J^*(L_\pi/L))=\partial^0(J^*_\infty(L_\pi/L)).$$

Proof. To ease notation, set $f=J^*(L_\pi/L,-)\cdot J^*_\infty(L_\pi/L,-)^{-1}$.

Then, since $f\in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_G,(\mathbf{Q}^c)^\times)$ the Hasse-Schilling-Maass Norm Theorem (cf. [8, Theorem (7.48)]) implies that the first equality is equivalent to asserting that $f(\chi)$ is a strictly positive real number for every χ in $\mathrm{Symp}(G)$. This in turn follows at once from the definition of $J^*_\infty(L_\pi/L,-)$.

The second equality is now an immediate consequence of the fact that $\partial^0(\mathrm{Det}(\mathbf{Q}^cG))=0$. □

Suppose now that F is a number field, and that $[\pi]\in H^1_t(F,G)$. We also recall that $F_{\pi,v}:=F_\pi\otimes_F F_v\simeq F_{v,\pi_v}$ (see e.g. [19, (2.4)]).

Definition 8.5. We set

$$J^*(F_\pi/F):=\sum_{v\nmid\infty}J^*(F_{v,\pi_v}/F_v)\in K_0(\mathbf{Z}G,\mathbf{Q}),$$

and

$$J^*_\infty(F_\pi/F):=\sum_{v\nmid\infty}J^*_\infty(F_{v,\pi_v}/F_v)\in K_0(\mathbf{Z}G,\mathbf{Q}).$$

(Note that the infinite sums make sense as $J^*_\infty(F_{v,\pi_v}/F_v)=J^*(F_{v,\pi_v}/F_v)=0$ for all places v that are unramified in F_π/F.)

We define $\mathcal{J}^*(F_\pi/F)\in \mathrm{Cl}(\mathbf{Z}G)$ by

$$\mathcal{J}^*(F_\pi/F):=\partial^0(J^*(F_\pi/F)),\quad \mathcal{J}^*_\infty(F_\pi/F):=\partial^0(J^*_\infty(F_\pi/F))$$

(see 2.2). □

Proposition 8.6. *Suppose that F is a number field, and $[\pi]\in H^1_t(F,G)$. Then*

$$\mathcal{J}^*(F_\pi/F)=\mathcal{J}^*_\infty(F_\pi/F).$$

Proof. This is a direct consequence of Theorem 8.4 and Definition 8.5. □

9. Proof of Theorem 1.5

Let $[\pi] \in H^1_t(F,G)$, and write

$$\mathfrak{c}(\pi) = [A_\pi, O_F G; \mathbf{r}_G] - [O_\pi, O_F G; \mathbf{r}_G] \in K_0(O_F G, F) \subseteq K_0(O_F G, F^c).$$

For each finite place v of F, we write $[\pi_v]$ for the image of $[\pi]$ in $H^1_t(F_v, G)$.

Recall that

$$K_0(O_F G, F) \simeq \frac{\mathrm{Hom}_{\Omega_F}(R_G, J_f(F^c))}{\prod_{v\nmid\infty} \mathrm{Det}(O_{F_v} G)^\times}.$$

A representing homomorphism in $\mathrm{Hom}_{\Omega_F}(R_G, J_f(F^c))$ of $\mathfrak{c}(\pi)$ is $f = (f_v)_v$ defined by

$$f_v(\chi) = \varpi_v^{\langle \psi_2(\chi) - 2\chi, s_v\rangle_G},$$

using the notation of Corollary 5.5. Let $\mathrm{Ram}(\pi)$ denote the set of finite places of F at which F_π/F is ramified. If $v \notin \mathrm{Ram}(\pi)$, then $s_v = 1$ and so $f_v = 1$.

Definition 9.1. Suppose that $v \in \mathrm{Ram}(\pi)$. Then we define $\mathfrak{c}(\pi; v) \in K_0(O_F G, F)$ to be the element represented by $f^{(v)} = (f^{(v)}_w)_w \in \mathrm{Hom}_{\Omega_F}(R_G, J_f(F^c))$ given by

$$f^{(v)}_w(\chi) = \begin{cases} f_v(\chi) = \varpi_v^{\langle \psi_2(\chi) - 2\chi, s_v\rangle_G} & \text{if } w = v; \\ 1 & \text{otherwise.} \end{cases}$$

Lemma 9.2. *We have*

$$\mathfrak{c}(\pi) = \sum_{v \in \mathrm{Ram}(\pi)} \mathfrak{c}(\pi; v). \tag{9.1}$$

Proof. It follows from the definitions that

$$f = \prod_{v \in \mathrm{Ram}(\pi)} f^{(v)},$$

and this implies the result. □

We can now prove Theorem 1.5.

Theorem 9.3. *Suppose that $[\pi] \in H^1_t(F,G)$ and that A_π is defined. Then*

$$\partial^0(\mathcal{N}_{F/\mathbf{Q}}(\mathfrak{c}(\pi)) \cdot \mathcal{J}^*_\infty(F_\pi/F)^{-1} = 0,$$

and so there is an equality

$$(A_\pi) - (O_\pi) = \mathcal{J}^*_\infty(F_\pi/F),$$

i.e. (see (1.1)*)*

$$(A_\pi) - W(F_\pi/F) = \mathcal{J}^*_\infty(F_\pi/F),$$

in $\mathrm{Cl}(\mathbf{Z}G)$*.*

Proof. Lemma 9.2 implies that in order to show that

$$\partial^0(\mathcal{N}_{F/\mathbf{Q}}(\mathfrak{c}(\pi)) \cdot \mathcal{J}^*_\infty(F_\pi/F)^{-1} = 0,$$

it suffices to show that

$$\partial^0(\mathcal{N}_{F/\mathbf{Q}}(\mathfrak{c}(\pi; v)) \cdot \mathcal{J}^*_\infty(F_{v,\pi_v}/F_v)^{-1} = 0$$

for each $v \in \mathrm{Ram}(\pi)$. Theorem 8.4 implies that this is equivalent to showing that

$$\partial^0(\mathcal{N}_{F/\mathbf{Q}}(\mathfrak{c}(\pi; v)) \cdot \mathcal{J}^*(F_{v,\pi_v}/F_v)^{-1} = 0$$

for each $v \in \mathrm{Ram}(\pi)$.

We see from the description of $\mathrm{Cl}(\mathbf{Z}G)$ given in Theorem 2.1(a) that this last equality will in turn follow if, for each $v \in \mathrm{Ram}(\pi)$, we show that

$$J^*(F_{v,\pi_v}/F_v, -)^{-1} \cdot (\mathcal{N}_{F/\mathbf{Q}}(f^{(v)})) \in \prod_l \mathrm{Det}(\mathbf{Z}_l G)^\times.$$

To show this last inclusion, we first observe that Proposition 6.6(a) implies that the inclusion holds at all rational primes l not lying below v.

For each rational prime l that lies below v, we fix an embedding $\mathrm{Loc}_l : \mathbf{Q}^c \to \mathbf{Q}_l^c$ and use it to identify $\mathrm{Irr}(\Gamma)$ with $\mathrm{Irr}_l(\Gamma)$. We recall in particular that such an isomorphism $R_G \to R_{G,l}$ in turn induces an isomorphism $\mathrm{Hom}_{\Omega_F}(R_G, (\mathbf{Q}^c)_l^\times) \to \mathrm{Hom}_{\Omega_{F_v}}(R_{G,l}, (\mathbf{Q}_l^c)^\times)$ (cf. [14, Chapter II, Lemma 2.1]). Then, reasoning analogously to the proof of [14, Theorem 19, pp. 114–116], one can deduce from Proposition 6.6(b) that

$$\mathcal{N}_{F_v/\mathbf{Q}_l}(f_v) \cdot \mathrm{Loc}_l\big(\mathcal{N}_{F/\mathbf{Q}}(f^{(v)})\big)^{-1} \in \mathrm{Det}(\mathbf{Z}_l G).$$

This establishes the desired inclusion at rational primes lying below v and completes the proof of the desired result. □

Remark 9.4. Let us make some remarks concerning Theorem 9.3 when F_π/F is locally abelian.

Suppose that $v \in \mathrm{Ram}(\pi)$. Set $s_v := \pi(\sigma_v)$, and write $H_v := \langle s_v \rangle$. Proposition 5.2(d) with $G = H_v$ and Proposition 5.3(b) imply that for each $\chi \in R_{H_v}$, we have

$$\begin{aligned}\langle \chi, s_v \rangle^*_{H_v} - \langle \chi, s_v \rangle_{H_v} &= (d(s_v), \chi)_{H_v} \\ &= \langle \psi_2(\chi) - \chi, s_v \rangle_{H_v}.\end{aligned}$$

Now suppose also that F_v contains a primitive $|s_v|$-th root of unity. This implies in particular that the extension $F_v^{\pi_v}/F_v$ is abelian. Let $\mathfrak{b}(\pi; v) \in K_0(FH_v, F)$ be the element represented by $\rho^{(v)} = (\rho_w^{(v)})_w \in \mathrm{Hom}_{\Omega_F}(R_{H_v}, J_f(F^c))$ defined by

$$\rho_w^{(v)}(\chi) = \begin{cases} \varpi_v^{(d(s_v),\chi)_{H_v}} = \varpi_v^{\langle \psi_2(\chi)-\chi, s_v\rangle_{H_v}} & \text{if } w = v; \\ 1 & \text{otherwise} \end{cases}$$

Observe that without the hypothesis concerning the number of roots of unity in F_v, we would only have that $\rho^{(v)} \in \mathrm{Hom}(R_{H_v}, J_f(F^c))$ rather than $\rho^{(v)} \in \mathrm{Hom}_{\Omega_F}(R_{H_v}, J_f(F^c))$. We also see from the definitions of $\mathfrak{c}(\pi; v)$ and $\mathfrak{b}(\pi; v)$ (see also (2.7) and (2.9)) that $\mathfrak{c}(\pi; v) = \mathrm{Ind}_{H_v}^G \mathfrak{b}(\pi; v)$.

Hence if for every $v \in \mathrm{Ram}(\pi)$, F_v contains a primitive $|s_v|$-th root of unity–which is precisely what happens if F_π/F is locally abelian–then we have

$$\mathfrak{c}(\pi) = \sum_{v \in \mathrm{Ram}(\pi)} \mathrm{Ind}_{H_v}^G \mathfrak{b}(\pi; v), \tag{9.2}$$

and so (using (2.10))

$$\begin{aligned} \partial^0(\mathfrak{c}(\pi)) &= \sum_{v \in \mathrm{Ram}(\pi)} \partial^0(\mathrm{Ind}_{H_v}^G \mathfrak{b}(\pi; v)) \\ &= \sum_{v \in \mathrm{Ram}(\pi)} \mathrm{Ind}_{H_v}^G \partial^0(\mathfrak{b}(\pi; v)) \\ &= 0. \end{aligned}$$

We now deduce from Theorem 9.3 that $\mathcal{J}_\infty^*(F_\pi/F) = 0$.

A comparison of (9.2) and (9.1) highlights the crucial difference between the locally abelian case and the general case. In both cases, the class $\mathfrak{c}(\pi)$ may be decomposed into a sum over the places $v \in \mathrm{Ram}(\pi)$ of classes $\mathfrak{c}(\pi; v) \in K_0(O_F G, F^c)$. However, in the locally abelian case, these classes $\mathfrak{c}(\pi; v)$ are induced from cyclic subgroups of G, while in the general case they are not. This is why Theorem 9.3 may be proved in the locally abelian case using abelian Jacobi sums thereby showing that in this situation $\mathcal{J}_\infty^*(F_\pi/F) = 0)$, which is what is done in [4]. □

10. Proof of Theorem 1.7

Let F be any imaginary quadratic field such that $\mathrm{Cl}(O_F)$ contains an element of order 4. In this section we shall construct infinitely many counterexamples to Conjecture 1.4 by showing that if ℓ is any sufficiently large prime with $\ell \equiv 3 \pmod 4$ and G is the generalised quaternion group $H_{4\ell}$, then there are infinitely many tame G-extensions F_π/F of fields such that A_π exists and $\mathcal{J}_\infty^*(F_\pi/F) \neq 0$. Hence, for these extensions, $(O_\pi) \neq (A_\pi)$ in $\mathrm{Cl}(\mathbf{Z}G)$. This will prove Theorem 1.7.

In what follows we fix an imaginary quadratic field F such that $\mathrm{Cl}(O_F)$ contains an element of order 4. To prove Theorem 1.7, it will suffice to prove the following result, which we shall derive as a consequence of works of Fröhlich (see [11]).

Lemma 10.1. *Suppose that ℓ is a sufficiently large prime and that $G \simeq H_{4\ell}$. Then, there exists a G-extension F_π/F of fields such that:*

(a) *F_π/F is ramified at only a single prime $\mathfrak{p}$ of F with $\mathfrak{p} \nmid \ell$;*
(b) *The prime $\mathfrak{p}$ does not split in F_π/F;*
(c) *The ramification index of $\mathfrak{p}$ is equal to ℓ;*

Before we prove this result, we shall first show that Lemma 10.1 implies Theorem 1.7.

Proof of Theorem 1.7. First we note that the decomposition subgroup of G at $\mathfrak{p}$ is equal to $H_{4\ell}$. We also recall that, for an odd prime ℓ, the generalised quaternion group $H_{4\ell}$ has a single, irreducible, non-trivial symplectic character χ, say.

If $\mathfrak{q}$ is unramified in F_π/F, then one has $\mathrm{sgn}(y(F_{\pi,\mathfrak{q}}/F_\mathfrak{q}, \psi_2(\chi))) = 1$. On the other hand, Theorem 8.1 and Proposition 8.2 imply that

$$\mathrm{sgn}(J^*(F_{\pi,\mathfrak{p}}/F_\mathfrak{p}, \chi)) = \mathrm{sgn}(y(F_{\pi,\mathfrak{p}}/F_\mathfrak{p}, \psi_2(\chi))) = -1.$$

In particular, if we now assume in addition that $\ell \equiv 3 \pmod 4$, then it follows from [14, Chapter II, Proposition 4.4] that the element $\mathcal{J}^*_\infty(F_\pi/F) \in \mathrm{Cl}(\mathbf{Z}G)$ (see Definition 8.3 and 8.5, and Proposition 8.6) is non-trivial. (We remark in passing that if instead $\ell \equiv 1 \pmod 4$, then the same argument shows that $\mathcal{J}^*_\infty(F_\pi/F) = 0$.) □

The remainder of this section will be devoted to the construction of the extensions described in Lemma 10.1.

Let L be an unramified, cyclic extension of F of degree 4. We write E/F for the quadratic subextension of L/F and write $\varphi_{E/F}$ for the quadratic character of E/F on ideals of F. We also view this as an idele class character of F. If ω denotes the idele class character of E that cuts out the extension L/E, then ω is of quaternion type (i.e. the restriction of ω to $J(F)$ is equal to $\varphi_{E/F}$—see [11, p. 405].)

For each prime ℓ, the symbol η_ℓ will denote a primitive ℓ-th root of unity. Then, following [11, Theorem 4], we consider the following conditions on primes.

Property 10.2. Let ℓ be an odd prime such that:

(a) $[F(\eta_\ell) : F]$ is even;
(b) $E \not\subseteq F(\eta_\ell + \eta_\ell^{-1})$;
(c) the class number of E is not divisible by ℓ.

We remark that these properties are satisfied for all sufficiently large ℓ. (We observe, in particular, that in our case 10.2(b) is automatically satisfied for sufficiently large ℓ since E/F is unramified.)

Henceforth we therefore fix a prime ℓ satisfying 10.2 and abbreviate η_ℓ to η. We then write Σ_- for the set of primes $\mathfrak{p}$ of F satisfying the following properties (see [11, (8.5)]).

Property 10.3. Let $\mathfrak{p}$ be a finite prime of F such that:

(a) The prime $\mathfrak{p}$ is inert in E/F (ie. $\varphi_{E/F}(\mathfrak{p}) = -1$);
(b) $N_{F/\mathbf{Q}} \equiv -1 \pmod{\ell}$.

In what follows, if $\mathfrak{p} \in \Sigma_-$, we write $\mathfrak{p}_E$ for the unique prime of E lying above $\mathfrak{p}$.

Our argument relies on the following result of Fröhlich (see [11, pp. 432–434]). We state the result, and then describe an outline of the proof. We refer the reader to [11] for complete details.

Theorem 10.4. *There are infinitely many primes in Σ_- (in fact a subset of positive Chebotarev density) for which the following statement is true: there exists a non-trivial idele class character θ of E of order ℓ, and of dihedral type (i.e. the restriction of θ to $J(F)$ is trivial) which is ramified at $\mathfrak{p}_E$ and which is unramified at all other finite places of E.*

Proof. We remark that necessary conditions for such a θ to exist are given in [11, Section 8, Lemma 5]. The existence of θ is demonstrated on pp. 433–434 of loc.cit. via the following argument.

Recall that η is a primitive ℓ-th root of unity, and set

$$M := E(\eta).$$

(Note that this field is denoted by L in [11, p. 433, l. 9], which is an unfortunate clash of notation with the field L defined earlier in loc. cit. (see [11, p. 407]).

Write $\widetilde{M}$ for the extension of M obtained by adjoining the elements

$$\{y^{1/\ell} \mid y \in O_E^\times\}.$$

It is shown in loc. cit. that, for each prime $\mathfrak{p}$ of F satisfying the following Frobenius conditons, there exists an idele class character θ of E satisfying the properties we seek:

Property 10.5. For every prime $\mathfrak{P}$ of $\widetilde{M}$ lying above $\mathfrak{p}$, the Frobenius element $\delta = (\mathfrak{P}, \widetilde{M}/F)$ satisfies:

(F1) $\delta^2 = 1$;
(F2) $\delta|_E$ is non-trivial (so $\mathfrak{p}$ does not split in E/F);
(F3) $\delta\,|_{F(\eta)}$ is non-trivial (so $\mathfrak{p}$ satisfies Property 10.3(b) above).

The set of primes $\mathfrak{p}$ of F satisfying Property 10.5 has positive Chebotarev density, and all such primes lie in Σ_-. $\square$

Let θ be an idele class character of E as constructed in Theorem 10.4, and let N/E denote the extension cut out by θ. Then N/E is cyclic of order ℓ, ramified (necessarily totally) at $\mathfrak{p}_E$, and at no other primes of E. As θ is of dihedral type, the extension N/F is dihedral of order 2ℓ.

Set $\psi := \omega\theta$. Then ψ is an idele class character of E of quaternion type, and we deduce that $F_{\pi(\psi)} := NL$ is an $H_{4\ell}$ extension of F. (Note that the field that we call $F_{\pi(\psi)}$ is denoted by the symbol F_ψ in [11].) The extension $F_{\pi(\psi)}/F$ is ramified only at $\mathfrak{p}$, with ramification index ℓ. We have the following diagram of fields and corresponding idele class characters (where we write φ for $\varphi_{E/F}$):

$$\begin{tikzcd}
& F_{\pi(\psi)} = NL \arrow[dl, dash] \arrow[dr, dash] & & \\
N \arrow[dr, dash, "\theta"] \arrow[ddr, dash] & & L \arrow[dl, dash, "\omega"'] & \widetilde{M} \arrow[dl, dash] \arrow[dll, dash] \\
& E \arrow[r, dash] \arrow[d, dash, "\varphi"] & M = E(\eta) \arrow[dl, dash] & \\
& F & &
\end{tikzcd}$$

To complete the proof of Lemma 10.1, it suffices to show that, in Theorem 10.4, there are infinitely many choices of $\mathfrak{p}$ (and so of θ) such that the decomposition group of $\mathfrak{p}$ in $F_{\pi(\psi)}/F$ is not abelian. This is equivalent to imposing an additional Frobenius condition on $\mathfrak{p}$. In order to do this, we require the following lemma.

Lemma 10.6. *The extension $\widetilde{M}/E$ and L/E are linearly disjoint. Hence $[\widetilde{M}L : \widetilde{M}] = 2$.*

Proof. The extension $\widetilde{M}/E$ has a unique quadratic sub-extension, viz. the unique quadratic sub-extension of M/E (recall that $M = E(\eta)$). This extension is ramified at places above $\mathfrak{p}$, and so cannot be equal to the unramified quadratic extension L/E. $\square$

We now fix an element $\delta_1 \in \mathrm{Gal}(\widetilde{M}L/F)$ which maps under the obvious quotient map onto the element $\delta \in \mathrm{Gal}(\widetilde{M}/F)$ constructed in the proof of Theorem 10.4 (see (10.5)), and we consider the set of primes $\mathfrak{p}$ of F satisfying the following Frobenius condition:

Property 10.7. For every prime $\mathfrak{Q}$ of $\widetilde{M}L$ lying above $\mathfrak{p}$,

(F4) the Frobenius element $(\mathfrak{Q}, \widetilde{M}L/F)$ lies in the conjugacy class of δ_1.

The set of primes $\mathfrak{p}$ satisfying (10.7) has positive Chebotarev density, and plainly if $\mathfrak{p}$ satisfies (10.7), then it also satisfies (10.5).

Suppose that $\mathfrak{p}$ satisfies (10.7). Then the corresponding extension $F_{\pi(\psi)}/F$ constructed above is an $H_{4\ell}$-extension unramified outside $\mathfrak{p}$, in which $\mathfrak{p}$ is non-split and ramified, with ramification index ℓ. Hence $F_{\pi(\psi)}/F$ an extension satistisfying the conditions of Lemma 10.1.

This completes the proof of Lemma 10.1.

Remark 10.8. It is shown in [11, Theorem 4] that for the extensions $F_{\pi(\psi)}/F$ constructed above satisfying the conditions of Lemma 10.1, we have

$$W(F_{\pi(\psi)}/F) = \varphi_{E/F}(\mathfrak{p}) = -1.$$

This implies that $(O_{\pi(\psi)}) \neq 0$ (see (1.1)), and so, since $\mathcal{J}^*_\infty(F_{\pi(\psi)}/F) \neq 0$, it follows from Theorem 1.5 that $(A_{\pi(\psi)}) = 0$. $\square$

Remark 10.9. Dominik Bullach has explained to us how explicit counterexamples to Conjecture 1.4 can also be derived from Theorem 1.5 by using general results of Neukirch on the embedding problem (see [21]) rather than the explicit computations of Fröhlich in [11]. $\square$

References

[1] A. Agboola, D. Burns, *Twisted forms and relative algebraic K-theory*, Proc. London Math. Soc. **92** (2006), 1–28.

[2] A. Agboola, L. R. McCulloh, *On the relative Galois module structure of rings of integers in tame extensions*, Algebra & Number Theory **12** (2018), 1823–1886.

[3] W. Bley, D. Burns, C. Hahn, *On refined metric and Hermitian structures in arithmetic I: Galois–Gauss sums and weak ramification*, Ann. K-Theory **5** (2020), 79-140.

[4] L. Caputo, S. Vinatier, *Galois module structure of the square root of the inverse different in even degree tame extensions of number fields*, J. Algebra **468** (2016), 103–154.

[5] Ph. Cassou-Nogues, M. J. Taylor, 'Galois module structure for wild extensions', in: Algebraic Number Theory and Diophantine Analysis: Proceedings of the International Conference held in Graz, Austria, August 30 to September 5, 1998, (ed. F. Halter-Koch, Robert F. Tichy, Berlin, New York: De Gruyter, 2011), 69-92.

[6] S. U. Chase, *Ramification invariants and torsion Galois module structure in number fields*, J. Algebra **91** (1984), 207–257.

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

[8] C. W. Curtis, I. Reiner, *Methods of Representation Theory, Volume I*, Wiley, 1987.

[9] C. W. Curtis, I. Reiner, *Methods of Representation Theory, Volume II*, Wiley, 1987.

[10] B. Erez, *The Galois structure of the square root of the inverse different*, Math. Zeit. **208** (1991), 239–255.

[11] A. Fröhlich, *Artin root numbers, conductors, and representations for generalized quaternion groups*, Proc. London Math. Soc. **28** (1974), no. 3, 402–428.

[12] A. Fröhlich, *Arithmetic and Galois module structure for tame extensions*, Crelle **286/287** (1976), 380–440.

[13] A. Fröhlich, *Non-abelian Jacobi sums*, In: Number Theory and Algebra, Academic Press (1977), 71–75.

[14] A. Fröhlich, *Galois module structure of rings of integers*, Springer, (1983).

[15] A. Fröhlich, *Classgroups and Hermitian modules*, Birkhäuser, (1984).

[16] A. Fröhlich, J. Queyrut, *On the functional equation of the Artin L-function for characters of real representations*, Invent. Math. **20** (1973) 125-138.

[17] Y. Kuang, *On the Galois-Gauss sums of weakly ramified characters*, PhD thesis, King's College London, 2022.

[18] J. Martinet, *Character theory and Artin L-functions*, Algebraic Number Fields (A. Fröhlich, ed.), 1-87, Academic Press, London 1977.

[19] L. R. McCulloh, *Galois module structure of abelian extensions*, J. Reine Angew. Math. **375/376** (1987) 259-306.

[20] G. Navarro, L. Sanus, P. H. Tiep, *Real characters and degrees*, Israel J. Math. **171** (2009) 157-173.

[21] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math., **21** (1973) 59-116.

[22] J.P. Serre, *Linear Representations of Finite Groups*, Springer GTM **42** (1977).

[23] J.-P. Serre, *Local Fields*, Springer GTM **67** (1979).

[24] J.-P. Serre, *Galois cohomology*, Springer (1987).

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

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

[27] M. J. Taylor, *Classgroups of group rings*, CUP (1984).

[28] C. Tsang, *On the Galois module structure of the square root of the inverse different in abelian extensions*, PhD thesis, 2016.

[29] S. V. Ullom, *Normal bases in Galois extensions of number fields,* Nagoya Math. J. **34** (1969), 153–167.

[30] S. Vinatier, *Sur la racine carrée de la codifférente*, J. Théorie Nombres Bordeaux 15 (2003), 393-410.

A. A.: Department of Mathematics, University of California, Santa Barbara, CA 93106.
Email address: agboola@math.ucsb.edu

D. B.: King's College London, Department of Mathematics, London WC2R 2LS.
Email address: david.burns@kcl.ac.uk

L. C.: Madrid, Spain.
Email address: luca.caputo@gmx.com

Y. K.: Zhuhai, China
Email address: yu.kuang.3@gmail.com