ON THE RELATIVE GALOIS MODULE STRUCTURE OF RINGS OF INTEGERS IN TAME EXTENSIONS

A. AGBOOLA AND L. R. MCCULLOH

ABSTRACT. Let F be a number field with ring of integers O_F and let G be a finite group. We describe an approach to the study of the set of realisable classes in the locally free class group $\mathrm{Cl}(O_F G)$ of $O_F G$ that involves applying the work of the second-named author in the context of relative algebraic K theory. For a large class of soluble groups G, including all groups of odd order, we show (subject to certain mild conditions) that the set of realisable classes is a subgroup of $\mathrm{Cl}(O_F G)$. This may be viewed as being a partial analogue in the setting of Galois module theory of a classical theorem of Shafarevich on the inverse Galois problem for soluble groups.

CONTENTS

Date: July10, 2018. Final version. To appear in Algebra and Number Theory.

1. Introduction

Suppose that F is a number field with ring of integers O_F, and let G be a finite group. If F_π/F is any tame Galois G-algebra extension of F, then a classical theorem of E. Noether implies that the ring of integers O_π of F_π is a locally free O_FG-module, and so determines a class (O_π) in the locally free class group $\mathrm{Cl}(O_FG)$ of O_FG. Hence, if we write $H^1_t(F,G)$ for the pointed set of isomorphism classes of tame G-extensions of F, then we obtain a map of pointed sets

$$\psi : H^1_t(F,G) \to \mathrm{Cl}(O_FG); \quad [\pi] \mapsto (O_\pi).$$

Even when G is abelian, so that $H^1_t(F,G)$ is actually a group, this map is almost never a group homomorphism. We say that an element $c \in \mathrm{Cl}(O_FG)$ is *realisable* if $c = (O_\pi)$ for some tame Galois G-algebra extension F_π/F, and we write $\mathcal{R}(O_FG)$ for the collection of realisable classes in $\mathrm{Cl}(O_FG)$. These classes are natural objects of study, and they have arisen in a number of different contexts in Galois module theory. The problem of describing $\mathcal{R}(O_FG)$ for a given G may be viewed as being a loose analogue of the inverse Galois problem in the setting of arithmetic Galois module theory.

When G is abelian, the second-named author has given a complete description of $\mathcal{R}(O_FG)$ by showing that it is equal to the kernel of a certain Stickelberger homomorphism on $\mathrm{Cl}(O_FG)$ (see [21]). In particular, he has shown that $\mathcal{R}(O_FG)$ is in fact a group. In subsequent unpublished work ([23], [22]) he showed that, for arbitrary G, the set $\mathcal{R}(O_FG)$ is always contained in the kernel of this Stickelberger homomorphism, and he raised the question of whether or not $\mathcal{R}(O_FG)$ is in fact always equal to this kernel. This question has inspired research by a number of different authors, and we refer the reader to e.g. [8], [9], [13], and to the bibliographies of these papers, for further information concerning previous work on this problem.

In this paper we shall describe a new approach to studying this topic that involves combining the methods introduced by the second-named author in [21] and [23] with techniques

involving relative algebraic K-theory and categorical twisted forms introduced by D. Burns and the first-named author in [3]. This enables us to both clarify certain aspects of the theory of realisable classes and to establish new results. Although our perspective is somewhat different, it should be stressed that many of the main ideas that we use are in fact already present in some form in [21] and [23].

Let us now describe the contents of this paper in more detail. In Section 2 we recall some basic facts concerning principal homogeneous spaces, Galois algebras and resolvends; these play a key role in everything that follows. Next, we assemble a number of technical results explaining how resolvends may be used to compute discriminants of rings of integers in Galois G-extensions. We also discuss how certain Galois cohomology groups may be expressed in terms of resolvends in a manner that is very useful for calculations in class groups and K-groups. In Section 4 we explain how determinants of resolvends may be represented in terms of certain character maps, and we recall an approximation theorem of A. Siviero (which is in turn a variant of [21, Theorem 2.14]).

We begin Section 5 by outlining the results we need about twisted forms and relative algebraic K-groups from [3]. Each tame G-extension F_π/F of F has an associated resolvend isomorphism

$$\mathbf{r}_G : F_\pi \otimes_F F^c \simeq F^c G$$

of F^cG-modules, and this may be used to construct a categorical twisted form which is represented by an element $[O_\pi, O_F G; \mathbf{r}_G]$ in a certain relative algebraic K-group $K_0(O_F G, F^c)$. The group $K_0(O_F G, F^c)$ admits a natural surjection onto the locally free class group $\mathrm{Cl}(O_F G)$, sending $[O_\pi, O_F G; \mathbf{r}_G]$ to (O_π), and so there is a map of pointed sets

$$\Psi : H^1_t(F, G) \to K_0(O_F G, F^c); \quad [\pi] \mapsto [O_\pi, O_F G; \mathbf{r}_G]$$

which is a refinement (more precisely, a lifting) of the map ψ above.

Crucial to our approach is the fact that each of the constructions that we have just described admits a local variant. Let v be any place of F, and write $H^1_t(F_v, G)$ for the pointed set of isomorphism classes of tame G-extensions of F_v. Then there is a localisation homomorphism

$$\lambda_v : K_0(O_F G, F^c) \to K_0(O_{F_v} G, F_v^c)$$

as well as a map of pointed sets

$$\Psi_v : H^1_t(F_v, G) \to K_0(O_{F_v} G, F_v^c); \quad [\pi_v] \mapsto [O_{\pi_v}, O_{F_v} G; \mathbf{r}_G].$$

The following result reflects the fact that $[O_\pi, O_F G; \mathbf{r}_G]$ is a much finer structure invariant than (O_π) (see Proposition 13.1 below):

Proposition A. *The kernel of* Ψ *is finite.*

Let G' denote the derived subgroup of G. We may identify $H^1(F, G')$ with a subset of $H^1(F, G)$ via the exact sequence $0 \to G' \to G \to G^{ab} \to 0$. Proposition A is proved by showing that $\mathrm{Ker}(\Psi)$ is a subset of the pointed set $H^1_{fnr}(F, G')$ of isomorphism classes of G'-Galois F-algebras that are unramified at all finite places of F; this last set is finite because there are only finitely many unramified extensions of F of bounded degree. If G is abelian, the map Ψ is injective (see Proposition 14.3). In many cases one can show that $\mathrm{Ker}(\Psi) = H^1_{fnr}(F, G')$, but we do not know whether this equality always holds.

Write $K\mathcal{R}(O_F G)$ for the image of Ψ, i.e. for the collection of realisable classes of $K_0(O_F G, F^c)$. The central conjecture of this paper gives a precise description of $K\mathcal{R}(O_F G)$ in terms of a local-global principle for the relative algebraic K-group $K_0(O_F G, F^c)$. This may be described as follows.

For each place v of F, let $H^1_{nr}(F_v, G)$ denote the subset $H^1_t(F_v, G)$ consisting of isomorphism classes of unramified G-extensions of F_v. We define a pointed set of ideles $J(H^1_t(F, G))$ of $H^1_t(F, G)$ to be the restricted direct product over all places v of the sets $H^1_t(F_v, G)$ with respect to the subsets $H^1_{nr}(F_v, G)$ (see Definition 6.2). The natural maps $H^1_t(F, G) \to H^1_t(F_v, G)$ for each v induce a map $H^1_t(F, G) \to J(H^1_t(F, G))$. We also define a group of ideles $J(K_0(O_F G, F^c))$ of $K_0(O_F G, F^c)$ to be the restricted direct product over all places of F of the groups $K_0(O_{F_v} G, F_v^c)$ with respect to the subgroups $K_0(O_{F_v} G, O_{F_v^c})$ (see Definition 5.8). We show that the maps λ_v above induce an injective localisation map

$$\lambda : K_0(O_F G, F^c) \to J(K_0(O_F G, F^c))$$

(see Proposition 5.9), and that the maps Ψ_v induce an idelic version

$$\Psi^{id} : J(H^1_t(F, G)) \to J(K_0(O_F G, F^c))$$

of the map Ψ (see Definition 6.2). We conjecture that $K\mathcal{R}(O_F G)$ has the following description (see Conjecture 6.5 below):

Conjecture B. $K\mathcal{R}(O_F G) = \lambda^{-1}(\mathrm{Im}(\Psi^{id}))$.

In other words, our conjecture predicts that an element x lies in the image of Ψ if and only if $\lambda_v(x)$ lies in the image of Ψ_v for every place v of F. We remark that it follows directly from the definitions that

$$K\mathcal{R}(O_F G) \subseteq \lambda^{-1}(\mathrm{Im}(\Psi^{id})).$$

We point out that, in contrast to $\mathcal{R}(O_F G)$, it is not difficult to show that if G is non-trivial, then $K\mathcal{R}(O_F G)$ is never a subgroup of $K_0(O_F G, F^c)$ (cf. [3, Remarks 6.13(i)], [2,

Remark 2.10(iii)]). Nevertheless, by applying the methods of [21] and [23] in the present context, we show that Conjecture B implies both an affirmative answer to the second-named author's question concerning $\mathcal{R}(O_FG)$ as well as a positive solution to the inverse Galois problem for G over F (see Theorems 6.6, 6.7 and 13.6 below):

Theorem C. *If Conjecture B holds, then $\mathcal{R}(O_FG)$ is a subgroup of $\mathrm{Cl}(O_FG)$. Furthermore, if $c \in \mathcal{R}(O_FG)$, then there exist infinitely many $[\pi] \in H^1_t(F,G)$ such that F_π is a field and $(O_\pi) = c$. The extensions F_π/F may be chosen to have ramification disjoint from any finite set S of places of F. In particular, the inverse Galois problem for G admits a positive solution over F.*

In order to orient the reader, we shall now briefly indicate the main ideas involved in the proof of Theorem C.

We begin by observing that the long exact sequence of relative algebraic K-theory yields a sequence

$$K_1(F^cG) \xrightarrow{\partial^1} K_0(O_FG, F^c) \xrightarrow{\partial^0} \mathrm{Cl}(O_FG) \to 0.$$

Hence, in order to show that $\mathcal{R}(O_FG) = \mathrm{Im}(\psi)$ is a subgroup of $\mathrm{Cl}(O_FG)$, it suffices to show that $\partial^1(K_1(F^cG)) \cdot \mathrm{Im}(\Psi)$ is a subgroup of $K_0(O_FG, F^c)$.

To do this, we first show that it suffices to prove that

$$\lambda(\partial^1(K_1(F^cG))) \cdot \mathrm{Im}(\Psi^{id})$$

is a subgroup of $J(K_0(O_FG, F^c))$. Once this is done, it is not hard to show that $\partial^1(K_1(F^cG)) \cdot \mathrm{Im}(\Psi)$ is equal to the kernel of the homomorphism

$$K_0(O_FG, F^c) \xrightarrow{\lambda} J(K_0(O_FG, F^c)) \to \frac{J(K_0(O_FG, F^c))}{\lambda[\partial^1(K_1(F^cG))] \cdot \mathrm{Im}(\Psi^{id})},$$

and so is indeed a subgroup of $K_0(O_FG, F^c)$ (see Theorem 6.7 below). The crux of the proof of the first part of Theorem C therefore consists of showing that $\lambda(\partial^1(K_1(F^cG))) \cdot \mathrm{Im}(\Psi^{id})$ is a subgroup of $K_0(O_FG, F^c)$.

This is accomplished as follows. Write $G(-1)$ for the group G (viewed as a set) endowed with an action of Ω_F via the inverse cyclotomic character. Although in general this is only an action on G as a set (rather than via automorphisms of G), the induced action on conjugacy classes of G does induce an action on the centre $Z(F^c[G])$ of the group ring F^cG. We write $Z(F^c[G(-1)])$ to denote $Z(F^c[G])$ endowed with this action. We set

$$\Lambda(FG) := Z(F^c[G(-1)])^{\Omega_F},$$

and we write $\Lambda(O_FG)$ for the (unique) O_F-maximal order in $\Lambda(FG)$. For each place v of F, we define $\Lambda(F_vG)$ and $\Lambda(O_{F_v}G)$ in an analogous manner. We write $J(\Lambda(FG))$ for the

restricted direct product over all places of F of the groups $\Lambda(F_vG)^\times$ with respect to the subgroups $\Lambda(O_{F_v}G)^\times$.

Let $\mathrm{Irr}(G)$ denote the set of irreducible characters of G. Motivated by an analysis of normal integral basis generators of tame local extensions, we define a Stickelberger pairing

$$\langle -, - \rangle_G : \mathrm{Irr}(G) \times G \to \mathbf{Q}.$$

(Loosely speaking, this may be viewed as being a monodromy-type pairing that encodes ramification data associated to tame extensions of local fields in a uniform manner (cf. Definition 10.6 below).) We then use this pairing to construct a K-theoretic transpose Stickelberger homomorphism

$$K\Theta^t : J(\Lambda(FG)) \to J(K_0(O_FG, F^c)).$$

The homomorphism $K\Theta^t$ is closely related to the map Ψ^{id} in the following way. We show that even though the map Ψ_v is just a map of pointed sets, the image $\Psi_v(H^1_{nr}(F_v, G))$ of the restriction of Ψ_v to $H^1_{nr}(F_v, G)$ is in fact a subgroup of $K_0(O_{F_v}G, F_v^c)$ for each v. Using an approximation theorem for $J(\Lambda(FG))$, we show further that, for a suitable choice of auxiliary ideal $\mathfrak{a}$ of O_F, the homomorphism $K\Theta^t$ may be used to construct a homomorphism

$$\Theta^t_{\mathfrak{a}} : \mathrm{Cl}'^{+}_{\mathfrak{a}}(\Lambda(O_FG)) \to \frac{J(K_0(O_FG, F^c))}{\lambda[\partial^1(K_1(F^cG))] \cdot \prod_v \Psi_v(H^1_{nr}(F_v, G))},$$

where $\mathrm{Cl}'^{+}_{\mathfrak{a}}(\Lambda(O_FG))$ is a certain finite quotient of $J(\Lambda(FG))$. We prove that

$$\mathrm{Im}(\Theta^t_{\mathfrak{a}}) = \mathrm{Im}(\overline{\Psi^{id}}),$$

where $\overline{\Psi^{id}}$ denotes the composition of Ψ^{id} with the obvious quotient map

$$J(K_0(O_FG, F^c)) \to \frac{J(K_0(O_FG, F^c))}{\lambda[\partial^1(K_1(F^cG))] \cdot \prod_v \Psi_v(H^1_{nr}(F_v, G))}.$$

We then show that this in turn implies that

$$\lambda(\partial^1(K_1(F^cG))) \cdot \mathrm{Im}(K\Theta^t) = \lambda(\partial^1(K_1(F^cG))) \cdot \mathrm{Im}(\Psi^{id}). \tag{1.1}$$

In particular, this proves that the right-hand side of (1.1) is a subgroup of $J(K_0(O_FG, F^c))$, as claimed. This completes our outline of the proof of the first part of Theorem C.

The strategy of the proof of the second part of Theorem C may be very roughly described as follows. Suppose that $x \in \lambda^{-1}(\mathrm{Im}(\Psi^{id}))$. By using the map $K\Theta^t$ together with a suitable approximation theorem on $J(K_0(O_FG, F^c))$, we show that there are infinitely many $y \in \lambda^{-1}(\mathrm{Im}(\Psi^{id}))$ such that (i) $\partial^0(y) = \partial^0(x)$, and (ii) each y corresponds via Conjecture B to an element $[\pi_y] \in H^1_t(F, G)$ which is ramified (away from S) in such a way that $\pi_y \in \mathrm{Hom}(\Omega_F, G)$ is forced to be surjective. This in turn implies that F_{π_y} is a field (rather than

just a Galois algebra), and so the inverse Galois problem for G admits a positive solution over F.

Let us now turn to our results concerning the validity of Conjecture B.

When G is abelian, we obtain the following refinement of [21, Theorem 6.7] (see Theorem 14.2 below):

Theorem D. *Conjecture B is true if G is abelian.*

By combining our methods with work of Neukirch, we are able to establish a variant of Conjecture B for a large class of soluble groups, including all groups of odd order (see Theorems 16.4 and 16.5 below). We thereby obtain the following result, which may be viewed as being a partial analogue of a classical theorem of Shafarevich (see [29]) on the inverse Galois problem for soluble groups in the context of arithmetic Galois module theory. (See Theorem 16.7 of the main text.)

Theorem E. *Suppose that G is of odd order and that $(|G|, h_F) = 1$, where h_F denotes the class number of F. Suppose also that F contains no non-trivial $|G|$-th roots of unity. Then $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$. If $c \in \mathcal{R}(O_F G)$, then there exist infinitely many $[\pi] \in H^1_t(F, G)$ such that F_π is a field and $(O_\pi) = c$. The extensions F_π/F may be chosen to have ramification disjoint from any finite set S of places of F.*

While it is perhaps conceivable that it might be possible to remove the hypothesis $(|G|, h_F) = 1$ of Theorem E using methods similar to those of the present paper (although we do not as yet know how to do this), the same probably cannot be said of the condition concerning the number of roots of unity in F. This latter hypothesis is forced upon us because our proof makes crucial use of a lifting theorem of Neukirch (see Section 15) where such hypotheses are unavoidable (cf. the last paragraph of the Introduction of [24]). It would be interesting to determine whether or not the methods of [29] can be used to prove a result similar to Theorem E for all soluble groups.

The results and techniques introduced in this paper suggest a number of different avenues of further investigation. For example, our methods may also be applied in the context of the relative Galois module structure of the square root of the inverse different as studied by C. Tsang (see [35], [36]), and it seems reasonable to expect that an analogue of Theorem E holds in this setting. Applying the methods of [1] to the study of counting and equidistribution problems involving cohomological classes in relative algebraic K-groups should lead to new results concerning similar problems for number fields, generalising certain aspects of e.g. [37] and [19]. Our techniques may also be applied in the setting of global function fields (see

[3] and [4]), and it would be of interest to further investigate the connection between the approach adopted here and that taken in e.g. [10] (cf. for example, [3, Section 4]).

Here is an outline of the rest of this paper. In Section 7, we explain a hitherto unpublished result of the second-named author that describes how resolvends of normal integral bases of tamely ramified extensions of non-archimedean local fields admit certain *Stickelberger factorisations* (see Definition 7.12); this is a non-abelian analogue of a version of Stickelberger's factorisation of abelian Gauss sums. A somewhat analogous (but much simpler) framework over $\mathbf{R}$ is described in Section 8.

In Section 9, we recall the definition and properties of the Stickelberger pairing. We also give a new character-theoretic description of this pairing (see Proposition 9.2) as well as an application of this description (see Corollary 9.4).

We construct a K-theoretic version of the transpose Stickelberger homomorphism in Section 10, and we also briefly describe an alternative approach to defining the Stickelberger pairing and establishing its basic properties. In Section 11 we construct transpose Stickelberger homomorphisms $\Theta^t_{\mathfrak{a}}$ on modified narrow ray class groups $\mathrm{Cl}'_{\mathfrak{a}}{}^{+}(\Lambda(O_F G))$. These are used in Section 12 to prove Theorem 6.6, thereby completing the proof of the first part of Theorem C.

In Section 13 we prove Proposition A, and we explain how a weaker form of Conjecture B implies that every realisable class in $\mathrm{Cl}(O_F G)$ may be realised (in infinitely many ways) by rings of integers of tame field (and not merely Galois algebra) G-extensions of F. This proves the second part of Theorem C.

We give a proof of Theorem D in Section 14. In Section 15, we describe work of Neukirch on the solution to an embedding problem that is required for the proof of Theorem E. This proof is completed in Section 16 via showing that a suitable variant of Conjecture B holds for a large class of soluble groups (see Definition 16.1 and Theorems 16.3 and 16.4).

We are very grateful indeed to Andrea Siviero for his extremely detailed comments on an earlier draft of this paper, and to Ruth Sergel for her most perceptive remarks at a critical stage of this project. We heartily thank Nigel Byott and Cindy Tsang for the many very helpful comments, questions and corrections that we received from them, and Bob Guralnick for a very helpful remark concerning the proof of Corollary 9.4 below. We are also extremely grateful to the anonymous referees whose very careful reading of the manuscript led us to correct and considerably strengthen our original results, and to significantly improve our exposition.

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 $h \in H$, then we write $c(h)$ for the conjugacy class of h in H and $\mathcal{C}(H)$ for the set of conjugacy classes of H. We denote the derived subgroup of H by 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 [27, I.5.2] and Section 2 below). 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 $H^1_t(L, G) = H^1(L, G)$. 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 L is a number field, we write $H^1_{fnr}(F, \Gamma)$ for the subset of $H^1_t(F, \Gamma)$ consisting of those $[\pi] \in H^1_t(F, \Gamma)$ for which L_π/L is unramified at all finite places of L.

If A is any algebra, we write $Z(A)$ for the centre of A. If A is semisimple, we write

$$\mathrm{nrd} : A^\times \to Z(A)^\times, \quad \mathrm{nrd} : K_1(A) \to Z(A)^\times$$

for the reduced norm maps on $A^\times$ and $K_1(A)$ respectively (cf. [16, Chapter II, §1]). 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.

If S_1 and S_2 are sets, we sometimes use the notation $S_1 \xrightarrow{\text{epi}} S_2$ to denote a surjective map from S_1 to S_2.

2. Principal homogeneous spaces and resolvends

In this section we shall describe some basic facts concerning principal homogeneous spaces and resolvends.

Throughout this section, the symbol L denotes either a number field or a local field.

2.1. **Principal homogeneous spaces.** [21, Section 1], [7, Section 1]. Let Γ be any finite group upon which Ω_L acts continuously on the left, and write $Z^1(\Omega_L, \Gamma)$ for the set of Γ-valued continuous Ω_L 1-cocycles. If $\pi \in Z^1(\Omega_L, \Gamma)$, then we write ${}^\pi\Gamma$ for the set Γ endowed with the following modified action of Ω_L: if

$$\Gamma \to {}^\pi\Gamma; \quad \gamma \mapsto \overline{\gamma}$$

is the identity map on the underlying sets, then

$$\overline{\gamma}^\omega = \overline{\pi(\omega) \cdot \gamma^\omega}$$

for each $\gamma \in \Gamma$ and $\omega \in \Omega_L$. The group Γ acts on ${}^\pi\Gamma$ via right multiplication.

We define an associated L-algebra L_π by

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

this is the algebra of L^c-valued functions on ${}^\pi\Gamma$ that are fixed under the action of Ω_L. The Hopf algebra

$$A = A_L := (L^c\Gamma)^{\Omega_L}$$

acts on L_π via the rule

$$(\alpha \cdot a)(\gamma) = \sum_{g \in \Gamma} \alpha_g \cdot a(\gamma \cdot g)$$

for all $\gamma \in \Gamma$ and $\alpha = \sum_{g \in \Gamma} \alpha_g \cdot g \in A$. The algebra L_π is a principal homogeneous space (p.h.s. for short) of the Hopf algebra

$$B := \mathrm{Map}_{\Omega_L}(\Gamma, L^c). \tag{2.1}$$

It may be shown that every p.h.s. of B is isomorphic to an algebra of the form L_π for some π, and so every such p.h.s. may be viewed as being a subset of the L^c-algebra $\mathrm{Map}(\Gamma, L^c)$. It is easy to check that

$$L_\pi \otimes_L L^c = L^c\Gamma \cdot \ell_\Gamma,$$

where $\ell_\Gamma \in \mathrm{Map}(\Gamma, L^c)$ is defined by

$$\ell_\Gamma(\gamma) = \begin{cases} 1 & \text{if } \gamma = 1; \\ 0 & \text{otherwise.} \end{cases}$$

This implies that L_π is a free, rank one A-module.

The Wedderburn decomposition of L_π may be described as follows. For any $\overline{\gamma} \in {}^\pi\Gamma$, write $\mathrm{Stab}(\overline{\gamma})$ for the stabiliser of $\overline{\gamma}$ in Ω_L, and set

$$L(\overline{\gamma}) := (L^c)^{\mathrm{Stab}(\overline{\gamma})}.$$

Then

$$L_\pi \simeq \prod_{\Omega_L \backslash {}^\pi\Gamma} L(\overline{\gamma}),$$

where $\Omega_L\backslash{}^\pi\Gamma$ denotes the set of Ω_L-orbits of ${}^\pi\Gamma$, and the product is taken over a set of orbit representatives. In general, the field $L(\overline{\gamma})$ is not normal over L. However, if Ω_L acts trivially on Γ, then $Z^1(\Omega_L, \Gamma) = \mathrm{Hom}(\Omega_L, \Gamma)$, and for each $\overline{\gamma} \in^\pi \Gamma$, we have

$$L(\overline{\gamma}) = (L^c)^{\mathrm{Ker}(\pi)} =: L^\pi, \tag{2.2}$$

with $\mathrm{Gal}(L^\pi/L) \simeq \pi(\Omega_L)$. In this case, we have that

$$L_\pi \simeq \prod_{\Gamma/\pi(\Omega_L)} L^\pi, \tag{2.3}$$

and this isomorphism depends only upon the choice of a transversal of $\pi(\Omega_L)$ in Γ.

Remark 2.1. For most of this paper we shall only need to consider the case in which Ω_L acts trivially on Γ; in this situation $A = L\Gamma$, and L_π is a Γ-Galois L-algebra. A notable exception to this will occur in Section 7, when we take L to be a non-archimedean local field, and we construct a canonical subextension of a tame extension L_π/L (see Definitions 7.4 and 7.6). This canonical sub-extension is complementary to the maximal unramified sub-extension of L_π/L, and is not usually a Galois algebra extension of L. It is however, a p.h.s. of a Hopf algebra of the form (2.1) associated to a certain group Γ equipped (as a set) with a non-trivial Ω_L-action. □

2.2. **Resolvends.** [21, Section 1], [7, Section 2].

Since every p.h.s. of B may be viewed as being a subset of $\mathrm{Map}(\Gamma, L^c)$, it is natural to consider the Fourier transforms of elements of $\mathrm{Map}(\Gamma, L^c)$. These arise via the *resolvend map*

$$\mathbf{r}_\Gamma : \mathrm{Map}(\Gamma, L^c) \to L^c\Gamma; \qquad a \mapsto \sum_{s\in\Gamma} a(s)s^{-1}.$$

The map $\mathbf{r}_\Gamma$ is an isomorphism of left $L^c\Gamma$-modules, but not of algebras, because it does not preserve multiplication. It is easy to show that for any $a \in \mathrm{Map}(\Gamma, L^c)$, we have that $a \in L_\pi$ if and only if $\mathbf{r}_\Gamma(a)^\omega = \mathbf{r}_\Gamma(a) \cdot \pi(\omega)$ for all $\omega \in \Omega_L$. It may also be shown that an element $a \in L_\pi$ generates L_π as an A-module if and only if $\mathbf{r}_\Gamma(a) \in (L^c\Gamma)^\times$. Two elements $a_1, a_2 \in \mathrm{Map}(\Gamma, L^c)$ with $\mathbf{r}_\Gamma(a_1), \mathbf{r}_\Gamma(a_2) \in (L^c\Gamma)^\times$ generate the same p.h.s. as an A-module if and only if $\mathbf{r}_\Gamma(a_1) = b \cdot \mathbf{r}_\Gamma(a_2)$ for some $b \in A^\times$. If a is any generator of L_π as an A-module, then a Γ-valued Ω_L 1-cocycle that represents the class $[\pi]$ of π in the pointed cohomology set $H^1(L, \Gamma)$ is given by

$$\omega \mapsto \mathbf{r}_\Gamma(a)^{-1} \cdot \mathbf{r}_\Gamma(a)^\omega.$$

We define pointed sets (where in each case the distinguished element is afforded by $1 \in A_{L^c}^\times = (L^c\Gamma)^\times$):

$$H(A) := \left\{\alpha \in A_{L^c}^\times : \alpha^{-1} \cdot \alpha^\omega \in \Gamma \quad \forall \omega \in \Omega_L\right\};$$
$$\mathcal{H}(A) := H(A)/\Gamma = \{\alpha \cdot \Gamma : \alpha \in H(A)\},$$

and we write $r_\Gamma(a) \in \mathcal{H}(A)$ for the image in $\mathcal{H}(A)$ of $\mathbf{r}_\Gamma(a) \in H(A)$. The element $r_\Gamma(a)$ is referred to as the *reduced resolvend* of a. If $\mathfrak{A}$ is any O_L-order in A, then we define $H(\mathfrak{A})$ and $\mathcal{H}(\mathfrak{A})$ in a similar manner. Hence we have

$$H(\mathfrak{A}) = \mathfrak{A}_{O_{L^c}} \cap H(A), \quad \mathcal{H}(\mathfrak{A}) = H(\mathfrak{A})/\Gamma.$$

Write L^t for the maximal, tamely ramified extension of L. We set

$$H_t(A) := \{\alpha \in H(A) : \alpha^\omega = \alpha \quad \forall \omega \in \Omega_{L^t}\};$$
$$\mathcal{H}_t(A) := H_t(A)/\Gamma = \{\alpha \cdot \Gamma : \alpha \in H_t(A)\},$$

and we define $H_t(\mathfrak{A})$ and $\mathcal{H}_t(\mathfrak{A})$ analogously for any O_L-order $\mathfrak{A}$ in A.

We shall now give a characterisation of the set $H(A)$ that avoids any explicit mention of Galois action. This is a non-abelian version of a description of $H(A)$ in terms of primitive elements of quotients of groups of units in Hopf algebras in the abelian case (see [3, Theorem 6.4]).

In order to do this, we first note that there are Ω_L-equivariant homomorphisms of algebras

$$\Delta, i_1, i_2 : A_{L^c} \to A_{L^c} \otimes_{L^c} A_{L^c}$$

induced by the maps

$$\Delta(\gamma) = \gamma \otimes \gamma, \quad i_1(\gamma) = \gamma \otimes 1, \quad i_2(\gamma) = 1 \otimes \gamma$$

for $\gamma \in \Gamma$.

We define a map of pointed sets

$$\mathcal{P} : A_{L^c}^{\times} \to (A_{L^c} \otimes_{L^c} A_{L^c})^{\times}; \quad x \mapsto \Delta(x) \cdot [i_1(x) \cdot i_2(x)]^{-1}.$$

It is easy to verify that

$$\mathcal{P}(x_1 \cdot x_2) = \Delta(x_1) \cdot \mathcal{P}(x_2) \cdot [i_1(x_1) \cdot i_2(x_1)]^{-1}.$$

As $\mathcal{P}(\gamma) = 1$ for each $\gamma \in \Gamma$, it follows that $\mathcal{P}$ induces a map of pointed sets (which we denote by the same symbol):

$$\mathcal{P} : A_{L^c}^{\times}/\Gamma \to (A_{L^c} \otimes_{L^c} A_{L^c})^{\times}.$$

Theorem 2.2. *Let $x \in A_{L^c}^{\times}$. Then $x \in H(A)$ if and only if $\mathcal{P}(x) \in (A \otimes_L A)^{\times}$.*

Proof. Suppose that $x \in H(A)$. Then if $\omega \in \Omega_L$, we have

$$x^{\omega} = x \cdot \gamma_{\omega}$$

for some $\gamma_{\omega} \in \Gamma$. Hence

$$\begin{aligned}
[\Delta(x)(i_1(x)i_2(x))^{-1}]^{\omega} &= \Delta(x)(\gamma_{\omega} \otimes \gamma_{\omega})[i_1(x)(\gamma_{\omega} \otimes 1)i_2(x)(1 \otimes \gamma_{\omega})]^{-1} \\
&= \Delta(x)(\gamma_{\omega} \otimes \gamma_{\omega})(1 \otimes \gamma_{\omega})^{-1} i_2(x)^{-1} (\gamma_{\omega} \otimes 1)^{-1} i_1(x)^{-1} \\
&= \Delta(x)(\gamma_{\omega} \otimes \gamma_{\omega})(1 \otimes \gamma_{\omega})^{-1} (\gamma_{\omega} \otimes 1)^{-1} i_2(x)^{-1} i_1(x)^{-1} \\
&= \Delta(x)[i_1(x)i_2(x)]^{-1}.
\end{aligned}$$

This shows that

$$\mathcal{P}(x) \in [(A_{L^c} \otimes_{L^c} A_{L^c})^{\times}]^{\Omega_L} = (A \otimes_L A)^{\times}.$$

Suppose conversely that $\mathcal{P}(x) \in (A \otimes_L A)^{\times}$, and that $x^{\omega} = x \cdot u_{\omega}$ for each $\omega \in \Omega_L$. We wish to show that $u_{\omega} \in \Gamma$. As the maps Δ, i_1, and i_2 are Ω_L-equivariant, we have that

$$\Delta(x)^{\omega} = \Delta(x) \cdot \Delta(u_{\omega}), \quad i_1(x)^{\omega} = i_1(x) \cdot i_1(u_{\omega}), \quad i_2(x)^{\omega} = i_2(x) \cdot i_2(u_{\omega}),$$

and a straightforward computation shows that

$$\mathcal{P}(x)^{\omega} = \Delta(x) \cdot \mathcal{P}(u_{\omega}) \cdot [i_1(x) \cdot i_2(x)]^{-1}.$$

As $\mathcal{P}(x) = \mathcal{P}(x)^\omega$, this implies that $\mathcal{P}(u_\omega) = 1$, i.e. that

$$\Delta(u_\omega) = i_1(u_\omega) \cdot i_2(u_\omega).$$

It now follows that $u_\omega \in \Gamma$ via an argument identical to that given in [3, Theorem 6.4]. □

Let F be a number field. Our next result shows that the pointed set $H(A_F)$ of resolvends satisfies a Hasse principle.

Proposition 2.3. *Let F be a number field, and suppose that $x \in (F^c\Gamma)^\times$. Then $x \in H(A_F)$ if and only if $\mathrm{loc}_v(x) \in H(A_{F_v})$ for every finite place v of F.*

Proof. We first observe that the map $\mathcal{P}$ commutes with localisation, i.e. for each finite place v of F, we have

$$\mathrm{loc}_v(\mathcal{P}(x)) = \mathcal{P}(\mathrm{loc}_v(x)) \tag{2.4}$$

for all $x \in (F^c\Gamma)^\times$. Hence we have

$$\begin{aligned} x \in H(A_F) &\iff \mathcal{P}(x) \in (A_F \otimes_F A_F)^\times \quad \text{(from Theorem 2.2);} \\ &\iff \mathrm{loc}_v(\mathcal{P}(x)) \in (A_{F_v} \otimes_{F_v} A_{F_v})^\times \quad \text{for each finite } v; \\ &\iff \mathcal{P}(\mathrm{loc}_v(x)) \in (A_{F_v} \otimes_{F_v} A_{F_v})^\times \quad \text{for each finite } v \text{ (from (2.4));} \\ &\iff \mathrm{loc}_v(x) \in H(A_{F_v}) \quad \text{for each finite } v \text{ (from Theorem 2.2).} \end{aligned}$$

□

Remark 2.4. It is also possible to give a proof of Proposition 2.3 directly from the definition of $H(A_F)$. The standard such proof that was known to the authors is valid only for abelian groups Γ; we are grateful to an anonymous referee for explaining how this proof may be modified so as to hold for arbitrary finite groups.

Suppose that $x \in A_{F^c}^\times$ is such that, for each finite place v of F, we have $\mathrm{loc}_v(x) \in H(A_{F_v})$. We wish to show that $x \in H(A_F)$.

Let E/F be any finite Galois extension such that Ω_E fixes x. Then the action of Ω_F on x factors through the action of the finite group $D := \mathrm{Gal}(E/F)$. Hence, to prove the desired result, it suffices to show that for any $\delta \in D$, we have $x^\delta = x \cdot \gamma_\delta$, with $\gamma_\delta \in \Gamma$.

Let $\mathcal{G}_F$ denote the subgroup of Ω_F generated by the subgroups Ω_{F_v} as v runs over the finite places of F. As each element of Ω_F is conjugate to an element of Ω_{F_v} for some v, it follows via the Chebotarev density theorem that the image $\overline{\mathcal{G}}_F$ of $\mathcal{G}_F$ in D has non-trivial intersection with every conjugacy class of D. A lemma of Jordan now implies that $\overline{\mathcal{G}}_F$ must be equal to the whole of D (see [28, p. 435, Theorem 4']). The result we seek now follows at once. □

3. Resolvends and cohomology

Recall that F is a number field and G is a finite group upon which Ω_F acts trivially. In this section, we explain, following [21, §2], how resolvends may be used to compute discriminants of rings of integers of G-Galois extensions of F, and to describe certain Galois cohomology groups.

For each $[\pi] \in H^1(F, G)$, the standard trace map

$$\mathrm{Tr} : \mathrm{Map}(G, F^c) \to F^c$$

induces a trace map

$$\mathrm{Tr} : F_\pi \to F$$

via restriction. This in turn yields an associated, non-degenerate bilinear form $(a, b) \mapsto \mathrm{Tr}(ab)$ on F_π. If M is any full O_F-lattice in F_π, then we set

$$M^* := \{b \in F_\pi | \, \mathrm{Tr}(b \cdot M) \subseteq O_F\}$$

and

$$\mathrm{disc}(O_\pi/O_F) := [O_\pi^* : O_\pi]_{O_F},$$

where the symbol $[- : -]_{O_F}$ denotes the O_F-module index. We see from the isomorphism (2.3) that we have

$$\mathrm{disc}(O_\pi/O_F) = \mathrm{disc}(O_{F^\pi}/O_F)^{[G:\pi(\Omega_F)]},$$

where $\mathrm{disc}(O_{F^\pi}/O_F)$ denotes the usual discriminant of the number field F^π over F, and so it follows that

$$\mathrm{disc}(O_\pi/O_F) = O_F$$

if and only if F_π/F is unramified at all finite places of F.

Definition 3.1. We write $[-1]$ for the maps induced on $\mathrm{Map}(G, F^c)$ and F^cG by the map $g \mapsto g^{-1}$ on G. □

Lemma 3.2. *Suppose that $a, b \in F_\pi$ for some $[\pi] \in H^1(F, G)$. Then*

$$\mathbf{r}_G(a) \cdot \mathbf{r}_G(b)^{[-1]} = \sum_{s \in G} \mathrm{Tr}(a^s b) \cdot s^{-1} \in FG.$$

Proof. This may be verified via a straightforward calculation (see e.g. [20, (1.6)], and note that the calculation given there is valid for an arbitrary finite group G). □

Corollary 3.3. *Suppose that $F_\pi = FG \cdot a$. Then we have:*
(i) $\mathbf{r}_G(a)^{-1} = \mathbf{r}_G(b)^{[-1]}$*, where* $b \in F_\pi$ *satisfies* $\mathrm{Tr}(a^s b^t) = \delta_{s,t}$.
(ii) $(O_F G \cdot a)^* = O_F G \cdot b$.
(iii) $[(O_F G \cdot a)^* : O_F G \cdot a]_{O_F} = [O_F G : O_F G \cdot \mathbf{r}_G(a) \cdot \mathbf{r}_G(a)^{[-1]}]_{O_F}$.
(iv) $\mathbf{r}_G(a) \in (O_{F^c} G)^\times$ *if and only if* $O_\pi = O_F G \cdot a$ *and* $\mathrm{disc}(O_\pi / O_F) = O_F$.
Analogous results hold if F is replaced by F_v for any finite place v of F.

Proof. Exactly as in [21, 2.10 and 2.11]. □

Lemma 3.4. *Suppose that L is either a number field or a local field. Then*
(i) $H^1(L, (L^c G)^\times) = 1$;
(ii) $H^1(L, Z(L^c G)^\times) = 1$.

Proof. For each $\chi \in \mathrm{Irr}(G)$, write $d(\chi)$ for the degree of χ, and $M_{d(\chi)}(L^c)$ for the algebra of $d(\chi) \times d(\chi)$-matrices over L^c. Then the Wedderburn isomorphism of algebras

$$L^c G \simeq \bigoplus_{\chi \in \mathrm{Irr}(G)} M_{d(\chi)}(L^c)$$

yields isomorphisms of groups

$$(L^c G)^\times \simeq \bigoplus_{\chi \in \mathrm{Irr}(G)} \mathrm{GL}_{d(\chi)}(L^c), \quad Z(L^c G)^\times \simeq \bigoplus_{\chi \in \mathrm{Irr}(G)} (L^c)^\times.$$

Let $\chi_1, \ldots, \chi_m \in \mathrm{Irr}(G)$ be a set of representatives of $\Omega_L \backslash \mathrm{Irr}(G)$. Write $\mathrm{Stab}(\chi_i)$ for the stabiliser of χ_i in Ω_L, and set $L[\chi_i] := (L^c)^{\mathrm{Stab}(\chi_i)}$. There are isomorphisms of Ω_L-modules

$$(L^c G)^\times \simeq \bigoplus_{i=1}^m \mathrm{Ind}_{\Omega_{L[\chi_i]}}^{\Omega_L}(\mathrm{GL}_{d(\chi_i)}(L^c)), \quad Z(L^c G)^\times \simeq \bigoplus_{i=1}^m \mathrm{Ind}_{\Omega_{L[\chi_i]}}^{\Omega_L}(L^c)^\times.$$

We have

$$\begin{aligned} H^1(L, (L^c G)^\times) &\simeq H^1(L, \bigoplus_{i=1}^m \mathrm{Ind}_{\Omega_{L[\chi_i]}}^{\Omega_L} \mathrm{GL}_{d(\chi_i)}(L^c)) \\ &\simeq \bigoplus_{i=1}^m H^1(L[\chi_i], \mathrm{GL}_{d(\chi_i)}(L^c)) \\ &= 1, \end{aligned}$$

where the second isomorphism follows via Shapiro's Lemma and the third is standard consequence of Hilbert's Theorem 90. This proves (i). The proof of (ii) is very similar. □

Recall that two pointed sets S_1 and S_2 are said to be *isomorphic* if there is a bijection of sets

$$f : S_1 \to S_2$$

with $f(x_1) = f(x_2)$, where x_i is the distinguished element of S_i, $(i = 1, 2)$.

A sequence

$$\cdots \to S_{i-1} \xrightarrow{f_i} S_i \xrightarrow{f_{i+1}} S_{i+1} \to \cdots$$

of pointed sets is said to be *exact* if there is an equality of sets

$$\mathrm{Im}(f_i) = f_{i+1}^{-1}(x_{i+1}),$$

where x_{i+1} is the distinguished element of S_{i+1}.

Theorem 3.5. *(a) There is an exact sequence of pointed sets*

$$1 \to G \to (FG)^\times \to \mathcal{H}(FG) \to H^1(F, G) \to 1. \tag{3.1}$$

(b) For each finite place v of F, recall that $H^1_{nr}(F_v, G)$ denotes the subset of $H^1(F_v, G)$ consisting of those $[\pi_v] \in H^1(F_v, G)$ for which the associated G-Galois extension F_{π_v}/F_v is unramified. Then there is an exact sequence of pointed sets

$$1 \to G \to (O_{F_v}G)^\times \to \mathcal{H}(O_{F_v}G) \to H^1_{nr}(F_v, G) \to 1. \tag{3.2}$$

(c) There are exact sequences of pointed sets

$$1 \to G \to (FG)^\times \to \mathcal{H}_t(FG) \to H^1_t(F, G) \to 1, \tag{3.3}$$

and

$$1 \to G \to (F_vG)^\times \to \mathcal{H}_t(F_vG) \to H^1_t(F_v, G) \to 1 \tag{3.4}$$

for each place v of F.

Proof. When G is abelian, parts (a) and (b) are proved in [21, pages 268 and 273] by considering the Ω_F and Ω_{F_v}-cohomology of the exact sequences of abelian groups

$$1 \to G \to (F^cG)^\times \to (F^cG)^\times/G \to 1 \tag{3.5}$$

and

$$1 \to G \to (O_{F_v^c}G)^\times \to (O_{F_v^c}G)^\times/G \to 1$$

respectively. If G is non-abelian, and these exact sequences are viewed as exact sequences of pointed sets instead, then a similar proof of part (a) also holds, as is pointed out in [21, page 268]: taking Ω_F-cohomology of the exact sequence (3.5) of pointed sets yields an exact sequence

$$1 \to G \to (FG)^\times \to \mathcal{H}(FG) \to H^1(F, G) \to H^1(F, (F^cG)^\times), \tag{3.6}$$

and since $H^1(F, (F^cG)^\times) = 1$ (see Lemma 3.4(i)), (3.1) immediately follows.

Alternatively, we could also argue directly (as is done in [21]) that the map $\mathcal{H}(FG) \to H^1(F, G)$ in (3.6) is surjective. Let us briefly describe the argument given in [21]. Suppose that $[\pi] \in H^1(F, G)$, and let $a \in F_\pi$ be a normal basis generator of F_π/F. Set $\alpha = \mathbf{r}_G(a)$; then the coset $\alpha \cdot G \in \mathcal{H}(FG)$ lies in the pre-image of $[\pi]$, and so it follows that (3.6) is indeed surjective on the right, as claimed.

Part (b) follows from Corollary 3.3(iv) (cf. the proof of (2.12) on [21, page 273]).

The proof of (c) is very similar to that of (a). Let F^t and F_v^t denote the maximal tamely ramified extensions of F and F_v respectively, and set $\Omega_F^t := \mathrm{Gal}(F^t/F)$, $\Omega_{F_v}^t := \mathrm{Gal}(F_v^t/F_v)$. Then (c) follows via considering the Ω_F^t and $\Omega_{F_v}^t$-cohomology of the exact sequences of pointed sets

$$1 \to G \to (F^tG)^\times \to (F^tG)^\times/G \to 1$$

and

$$1 \to G \to (F_v^tG)^\times \to (F_v^tG)^\times/G \to 1$$

respectively, using the direct argument given in [21, page 268] that we have described above. □

Suppose that L is a number field or a local field. Recall that $Z(LG)$ denotes the centre of LG. Before stating our next result, we note that the reduced norm map

$$\mathrm{nrd} : (LG)^\times \to Z(LG)^\times$$

induces an injection $G^{ab} \to Z(LG)^\times$. (More explicitly, if we identify $Z(L^cG)^\times$ with $\prod_{\chi \in \mathrm{Irr}(G)} (L^c)^\times$ via the Wedderburn decomposition of L^cG (cf. the proof of Lemma 3.4), then the injection $G^{ab} \to Z(L^G)^\times$ is induced by the map $G \to Z(L^cG)^\times$ given by $g \mapsto [(\det(\chi))(g)]_\chi$, where $\det(\chi)$ is the abelian character of G defined below in Definition 4.3. See also (4.5).) In what follows, we shall identify G^{ab} with its image in $Z(LG)^\times$ under this map. We set

$$H(Z(LG)) := \left\{\alpha \in Z(L^cG)^\times : \alpha^{-1} \cdot \alpha^\omega \in G^{ab} \quad \forall \omega \in \Omega_L\right\};$$
$$\mathcal{H}(Z(LG)) := H(Z(LG))/G^{ab} = \{\alpha \cdot G^{ab} : \alpha \in H(Z(LG))\}.$$

We define $H(Z(\mathfrak{A}))$ and $\mathcal{H}(Z(\mathfrak{A}))$ analogously for any O_L-order $\mathfrak{A}$ in LG.

Proposition 3.6. *Let L be a number field or a local field. Then there is an exact sequence of abelian groups:*

$$1 \to G^{ab} \to Z(LG)^\times \to \mathcal{H}(Z(LG)) \to H^1(L, G^{ab}) \to 1. \tag{3.7}$$

Proof. This follows at once from taking Ω_L cohomology of the exact sequence of abelian groups

$$1 \to G^{ab} \to Z(L^cG)^\times \to Z(L^cG)^\times/G^{ab} \to 1,$$

arising from the injection $G^{ab} \to Z(L^cG)^\times$ induced by the reduced norm map $\mathrm{nrd} : (LG)^\times \to Z(LG)^\times$ as described above, and noting that $H^1(\Omega_L, Z(L^cG)^\times) = 1$, via Lemma 3.4(ii). □

It is easy to see that the group $(LG)^\times$ acts on the pointed set $\mathcal{H}(LG)$ by left multiplication. Write $(LG)^\times\backslash\mathcal{H}(LG)$ for the quotient set afforded by this action. It follows from Theorem 3.5 and Proposition 3.6 that there are isomorphisms

$$H^1(L,G) \xrightarrow{\sim} (LG)^\times\backslash\mathcal{H}(LG)$$

and

$$H^1(L,G^{ab}) \xrightarrow{\sim} Z(LG)^\times\backslash\mathcal{H}(Z(LG))$$

of pointed sets and abelian groups respectively, and that the following diagram commutes:

$$\begin{array}{ccc} H^1(L,G) & \xrightarrow{\sim} & (LG)^\times\backslash\mathcal{H}(LG) \\ \downarrow & & \downarrow \mathrm{nrd} \\ H^1(L,G^{ab}) & \xrightarrow{\sim} & Z(LG)^\times\backslash\mathcal{H}(Z(LG)). \end{array} \tag{3.8}$$

(Here the left-hand vertical arrow is induced by the quotient map $G \to G^{ab}$, while the right-hand vertical arrow is induced by the reduced norm map $\mathrm{nrd} : (L^cG)^\times \to Z(L^cG)^\times$.)

We shall need the following result in Section 6.

Proposition 3.7. *Let F be a number field. For each finite place v of F, the image of the map*

$$\mathrm{nrd} : (O_{F_v}G)^\times\backslash\mathcal{H}(O_{F_v}G) \to Z(O_{F_v}G)^\times\backslash\mathcal{H}(Z(O_{F_v}G))$$

of pointed sets is in fact a group.

Proof. Just as in the case of (3.8), we see from the exact sequences (3.2) and (3.7) that there is a commutative diagram

$$\begin{array}{ccc} H^1_{nr}(F_v,G) & \xrightarrow{\sim} & (O_{F_v}G)^\times\backslash\mathcal{H}(O_{F_v}G) \\ \downarrow & & \downarrow \mathrm{nrd} \\ H^1_{nr}(F_v,G^{ab}) & \longrightarrow & Z(O_{F_v}G)^\times\backslash\mathcal{H}(Z(O_{F_v}G)) \\ \downarrow \cap & & \downarrow \cap \\ H^1(F_v,G^{ab}) & \xrightarrow{\sim} & Z(F_vG)^\times\backslash\mathcal{H}(Z(F_vG)). \end{array} \tag{3.9}$$

The middle horizontal arrow of (3.9) is therefore injective, and its image is a subgroup of $Z(O_{F_v}G)^\times\backslash\mathcal{H}(Z(O_{F_v}G))$. Hence, to prove the desired result, it suffices to show that the map $H^1_{nr}(F_v, G) \to H^1_{nr}(F_v, G^{ab})$ is surjective. This is in turn an immediate consequence of the fact that the Galois group $\mathrm{Gal}(F_v^{nr}/F_v)$ is profinite free on a single generator. □

4. Determinants and character maps

In this section we shall describe how determinants of resolvends may be represented in terms of certain character maps.

Let L be a number field or a local field.

Suppose that Γ is any finite group upon which the absolute Galois group Ω_L of L acts (possibly trivially). Then Ω_L also acts on the ring R_Γ of virtual characters of Γ according to the following rule: if $\chi \in \mathrm{Irr}(\Gamma)$ and $\omega \in \Omega_L$, then, for each $\gamma \in \Gamma$, we have $\chi^\omega(\gamma) = \omega(\chi(\omega^{-1}(\gamma)))$.

We begin by recalling some well-known facts and definitions concerning determinant maps (see e.g. [16, Chapter II] or [17, Chapter I]).

Definition 4.1. For each element a of $\mathrm{GL}_n(L^cG)$, we define an element

$$\mathrm{Det}(a) \in \mathrm{Hom}(R_G, (L^c)^\times) \simeq Z(L^cG)^\times \tag{4.1}$$

in the following way: if T is any representation of G over L^c with character ϕ, then we set

$$\mathrm{Det}(a)(\phi) := \det(T(a)).$$

It may be shown that this definition depends only upon the character ϕ, and not upon the choice of representation T. The map

$$\mathrm{Det} : \mathrm{GL}_n(L^cG) \to \mathrm{Hom}(R_G, (L^c)^\times)$$

is Ω_L-equivariant, and so induces a map

$$\mathrm{Det} : \mathrm{GL}_n(LG) \to \mathrm{Hom}_{\Omega_L}(R_G, (L^c)^\times).$$

□

Remark 4.2. The map Det in (4.1) above is essentially the same as the reduced norm map. Let

$$\mathrm{nrd} : (L^cG)^\times \to Z(L^cG)^\times \tag{4.2}$$

denote the reduced norm. Then (4.2) induces an isomorphism

$$\mathrm{nrd} : K_1(L^cG) \xrightarrow{\sim} Z(L^cG)^\times \simeq \mathrm{Hom}(R_G, (L^c)^\times) \tag{4.3}$$

(see e.g. [12, Theorem 45.3]). Suppose now that ϕ is any L^c-valued character of G, and let $a \in (L^cG)^\times$. Then we have that

$$\mathrm{Det}(a)(\phi) = \mathrm{nrd}(a)(\phi)$$

(see [17, Chapter I, Proposition 2.7]). □

Definition 4.3. Suppose that $\chi \in \mathrm{Irr}(G)$. We define an abelian character $\det(\chi)$ of G as follows. Let T be any representation of G over L^c affording χ. For each element $g \in G$, we set

$$(\det(\chi))(g) = \mathrm{Det}(T(g)).$$

Then $\det(\chi)$ is independent of the choice of T, and may be viewed as being a character of G^{ab}. We extend det to a homomorphism $R_G \to (G^{ab})^\wedge$, where $(G^{ab})^\wedge$ denotes the group of characters of G^{ab}, by defining

$$\det\left(\sum_{\chi\in\mathrm{Irr}(G)} a_\chi \chi\right) = \prod_{\chi\in\mathrm{Irr}(G)} (\det(\chi))^{a_\chi},$$

and we set

$$A_G := \mathrm{Ker}(\det).$$

Hence we have an exact sequence of groups

$$0 \to A_G \to R_G \xrightarrow{\det} (G^{ab})^\wedge \to 0. \tag{4.4}$$

□

Applying the functor $\mathrm{Hom}(-, (L^c)^\times)$ to (4.4), we obtain an exact sequence

$$0 \to G^{ab} \to \mathrm{Hom}(R_G, (L^c)^\times) \xrightarrow{\mathrm{rag}} \mathrm{Hom}(A_G, (L^c)^\times) \to 0, \tag{4.5}$$

which is surjective on the right because $(L^c)^\times$ is divisible. It follows that there are Ω_L-equivariant isomorphisms

$$\mathrm{Hom}(A_G, (L^c)^\times) \simeq \mathrm{Hom}(R_G, (L^c)^\times)/G^{ab} \simeq Z(L^cG)^\times/G^{ab}. \tag{4.6}$$

In what follows, we shall sometimes identify $\mathrm{Hom}(A_G, (L^c)^\times)$ with $Z(L^cG)^\times/G^{ab}$ via (4.6) without explicit mention.

Taking Ω_L-cohomology of (4.5) yields an exact sequence

$$0 \to G^{ab} \to \mathrm{Hom}_{\Omega_L}(R_G, (L^c)^\times) \xrightarrow{\mathrm{rag}} \mathrm{Hom}_{\Omega_L}(A_G, (L^c)^\times) \to H^1(L, G^{ab}) \to 1, \tag{4.7}$$

which is surjective on the right via Lemma 3.4(ii).

Definition 4.4. Let R_G^s denote the (additive) subgroup of R_G generated by the symplectic characters of G. Thus, R_G^s is generated by the irreducible symplectic characters of G, together with elements of the form $\chi + \overline{\chi}$, where $\chi \in R_G$ and $\overline{\chi}$ denotes the complex conjugate of χ. All virtual characters lying in R_G^s are real-valued.

If F is a number field, and v is a real place of F, we write $\mathrm{Hom}^+_{\Omega_{F_v}}(R_G, (F_v^c)^\times)$ for those elements $f \in \mathrm{Hom}_{\Omega_{F_v}}(R_G, (F_v^c)^\times)$ for which $f(\eta) > 0$ for all $\eta \in R_G^s$. Note that if $f \in \mathrm{Hom}_{\Omega_{F_v}}(R_G, (F_v^c)^\times)$ and $\chi \in R_G$, then we automatically have

$$f(\chi + \overline{\chi}) = f(\chi) \cdot \overline{f(\chi)} > 0.$$

Hence in fact $f \in \mathrm{Hom}^+_{\Omega_{F_v}}(R_G, (F_v^c)^\times)$ if and only if f is positive on all irreducible, symplectic characters of G. In particular, if G has no non-trivial irreducible symplectic characters (e.g. if $|G|$ is odd), then we have

$$\mathrm{Hom}^+_{\Omega_{F_v}}(R_G, (F_v^c)^\times) = \mathrm{Hom}_{\Omega_{F_v}}(R_G, (F_v^c)^\times).$$

We write $Z(F_vG)^\times_+$ for the image of $\mathrm{Hom}^+_{\Omega_{F_v}}(R_G, (F_v^c)^\times)$ in $Z(F_vG)^\times$ under the isomorphism

$$\mathrm{Hom}_{\Omega_{F_v}}(R_G, (F_v^c)^\times) \xrightarrow{\sim} Z(F_vG)^\times.$$

□

Proposition 4.5. *Let F be a number field. For each place v of F, we write*

$$\mathrm{Det} : (F_v^cG)^\times \to \mathrm{Hom}(R_G, (F_v^c)^\times) \simeq Z(F_v^cG)^\times \tag{4.8}$$

for the determinant homomorphism afforded by Definition 4.1.

(i) If v is real, then (4.8) *induces an isomorphism*

$$\mathrm{Det}((F_vG)^\times) \simeq \mathrm{Hom}^+_{\Omega_{F_v}}(R_G, (F_v^c)^\times) \simeq Z(F_vG)^\times_+. \tag{4.9}$$

(ii) If v is finite or complex, then the map (4.8) *induces isomorphisms*

$$\mathrm{Det}((F_vG)^\times) \simeq \mathrm{Hom}_{\Omega_{F_v}}(R_G, (F_v^c)^\times) \simeq Z(F_vG)^\times, \tag{4.10}$$

$$\mathrm{Det}(\mathcal{H}(F_vG)) \simeq \mathrm{Hom}_{\Omega_{F_v}}(A_G, (F_v^c)^\times). \tag{4.11}$$

(iii) If v is finite of residue characteristic coprime to $|G|$, so $O_{F_v}G$ is an O_{F_v}-maximal order in F_vG, then (4.8) *induces isomorphisms*

$$\mathrm{Det}((O_{F_v}G)^\times) \simeq \mathrm{Hom}_{\Omega_{F_v}}(R_G, (O_{F_v^c})^\times) \simeq Z(O_{F_v}G)^\times, \tag{4.12}$$

$$\mathrm{Det}(\mathcal{H}(O_{F_v}G)) \simeq \mathrm{Hom}_{\Omega_{F_v}}(A_G, (O_{F_v^c})^\times). \tag{4.13}$$

Proof. The isomorphisms (4.9), (4.10) and (4.12) are standard and are explained in e.g. [16, Chapter II, §1].

Suppose that v is either finite or complex. Theorem 3.5(a) and (4.10) yield the following commutative diagram:

$$\begin{array}{ccccccc}
G & \xrightarrow{\subseteq} & (F_vG)^\times & \longrightarrow & \mathcal{H}(F_vG) & \xrightarrow{\text{epi}} & H^1(F_v,G) \\
\downarrow & & \downarrow{\scriptstyle \text{Det}} & & \downarrow{\scriptstyle \text{Det}} & & \downarrow{\scriptstyle \text{epi}} \\
G^{ab} & \xrightarrow{\subseteq} & \text{Det}((F_vG)^\times) & \longrightarrow & \text{Det}(\mathcal{H}(F_vG)) & \xrightarrow{\text{epi}} & H^1(F_v,G^{ab}) \\
\| & & \downarrow{\scriptstyle \sim} & & \downarrow & & \| \\
G^{ab} & \xrightarrow{\subseteq} & \text{Hom}_{\Omega_{F_v}}(R_G,(F_v^c)^\times) & \longrightarrow & \text{Hom}_{\Omega_{F_v}}(A_G,(F_v^c)^\times) & \xrightarrow{\text{epi}} & H^1(F_v,G^{ab}),
\end{array} \tag{4.14}$$

and this implies that the map

$$\text{Det}(\mathcal{H}(F_vG)) \to \text{Hom}_{\Omega_{F_v}}(A_G,(F_v^c)^\times)$$

is an isomorphism, which proves (4.11).

Suppose now that v is finite of residue characteristic coprime to $|G|$. In order to establish (4.13), we first observe that applying the functor $\text{Hom}(-,(O_{F_v^c})^\times)$ to the exact sequence (4.4) yields a sequence

$$0 \to G^{ab} \to \text{Hom}(R_G,(O_{F_v^c})^\times) \to \text{Hom}(A_G,(O_{F_v^c})^\times) \to 1 \tag{4.15}$$

which is surjective on the right because $(O_{F_v^c})^\times$ is divisible. Taking Ω_{F_v}-cohomology of (4.15) yields

$$\begin{aligned} 0 \to G^{ab} &\to \text{Hom}_{\Omega_{F_v}}(R_G,(O_{F_v^c})^\times) \to \text{Hom}_{\Omega_{F_v}}(A_G,(O_{F_v^c})^\times) \to \\ &\to H^1(F_v,G^{ab}) \xrightarrow{f} H^1(F_v,\text{Hom}(R_G,(O_{F_v^c})^\times)). \end{aligned} \tag{4.16}$$

Now since $v \nmid |G|$, $Z(O_{F_v}G)$ is an O_{F_v}-maximal order in (the split algebra) $Z(F_vG)$, and $Z(O_{F_v^c}G)^\times \simeq \text{Hom}(R_G,(O_{F_v^c})^\times)$ (cf. (4.12)). Suppose that $\pi \in \text{Ker}(f)$. Then there exists $u \in Z(O_{F_v^c}G)^\times$ such that $u^\omega \cdot u^{-1} = \pi(\omega)$ for all $\omega \in \Omega_{F_v}$. This implies that $u^{|G^{ab}|} \in Z(O_{F_v}G)^\times$. As $v \nmid |G^{ab}|$ and $Z(O_{F_v}G)$ is a maximal order, it follows that $u \in Z(O_{F_v^{nr}}G)^\times$, and so $\pi \in H^1_{nr}(F_v,G^{ab})$. Hence there is an exact sequence

$$0 \to G^{ab} \to \text{Hom}_{\Omega_{F_v}}(R_G,(O_{F_v^c})^\times) \to \text{Hom}_{\Omega_{F_v}}(A_G,(O_{F_v^c})^\times) \to H^1_{nr}(F_v,G^{ab}). \tag{4.17}$$

We recall also (see the proof of Proposition 3.7) that the natural map $H^1_{nr}(F_v,G) \to H^1_{nr}(F_v,G^{ab})$ is surjective because the group $\text{Gal}(F_v^{nr}/F_v)$ is profinite free on a single generator. Theorem 3.5(b) together with (4.12) and (4.17) now yield the following commutative

diagram:

$$\begin{array}{ccccccc}
G & \xrightarrow{\subseteq} & (O_{F_v}G)^\times & \longrightarrow & \mathcal{H}(O_{F_v}G) & \xrightarrow{\text{epi}} & H^1_{nr}(F_v, G) \\
\downarrow & & \downarrow \text{Det} & & \downarrow \text{Det} & & \downarrow \text{epi} \\
G^{ab} & \xrightarrow{\subseteq} & \text{Det}((O_{F_v}G)^\times) & \longrightarrow & \text{Det}(\mathcal{H}(O_{F_v}G)) & \xrightarrow{\text{epi}} & H^1_{nr}(F_v, G^{ab}) \\
\| & & \downarrow \sim & & \downarrow & & \| \\
G^{ab} & \xrightarrow{\subseteq} & \text{Hom}_{\Omega_{F_v}}(R_G, (O_{F_v^c})^\times) & \longrightarrow & \text{Hom}_{\Omega_{F_v}}(A_G, (O_{F_v^c})^\times) & \longrightarrow & H^1_{nr}(F_v, G^{ab}).
\end{array} \tag{4.18}$$

It follows from (4.18) that the third row of this diagram is surjective on the right. Since $\text{Det}(\mathcal{H}(O_{F_v}G))$ is a subgroup of $\text{Hom}_{\Omega_{F_v}}(A_G, (O_{F_v^c})^\times)$, we see that the map

$$\text{Det}(\mathcal{H}(O_{F_v}G)) \to \text{Hom}_{\Omega_{F_v}}(A_G, (O_{F_v^c})^\times)$$

is an isomorphism. This establishes (4.13). □

If on the other hand v is finite and $v \mid |G|$, so $O_{F_v}G$ is not an O_{F_v}-maximal order in F_vG, then we have

$$\text{Det}(\mathcal{H}(O_{F_v}G)) \subseteq \text{Hom}_{\Omega_{F_v}}(A_G, (O^c_{F_v})^\times),$$

but this inclusion is not in general an equality. If $\mathfrak{a}$ is any integral ideal of O_F, set

$$U_{\mathfrak{a}}(O_{F_v^c}) := (1 + \mathfrak{a}O_{F_v^c}) \cap (O_{F_v^c})^\times,$$

and write $U_\alpha(O_{F_v^c})$ instead of $U_{\mathfrak{a}}(O_{F_v^c})$ when $\mathfrak{a} = \alpha O_F$. We shall need the following result of A. Siviero (which is a variant of [21, Theorem 2.14]) in Section 11.

Proposition 4.6. *(A. Siviero) Let v be a finite place of F. Then if $N \in \mathbf{Z}_{>0}$ is divisible by a sufficiently large power of $|G|$, we have*

$$\text{Hom}_{\Omega_{F_v}}(A_G, U_N(O_{F_v^c})) \subseteq \text{Det}(\mathcal{H}(O_{F_v}G)) \subseteq \text{Hom}_{\Omega_{F_v}}(A_G, (O_{F_v^c})^\times).$$

Proof. This is shown in [30, Theorem 5.1.10] when G is abelian, and the proof for arbitrary finite G is quite similar. As [30] is not widely accessible, we describe the argument.

If $v \nmid |G|$, then Proposition 4.5(iii) implies that we have

$$\text{Hom}_{\Omega_{F_v}}(A_G, O^\times_{F_v^c}) = \text{Det}(\mathcal{H}(O_{F_v}G)) = \text{Hom}_{\Omega_{F_v}}(A_G, (O_{F_v^c})^\times),$$

and so it follows that the desired result holds in this case. We may therefore suppose that $v \mid |G|$.

We first observe that the group

$$\frac{\mathrm{Hom}_{\Omega_{F_v}}(A_G, (O_{F_v^c})^\times)}{\mathrm{Det}((O_{F_v}G)^\times/G)}$$

is annihilated by $|G^{ab}|[\mathrm{Det}(\mathcal{M}_v^\times) : \mathrm{Det}(O_{F_v}G)^\times]$, where $\mathcal{M}_v$ denotes any O_{F_v}-maximal order in F_vG containing $O_{F_v}G$. Since A_G is finitely generated, it follows that $\mathrm{Det}((O_{F_v}G)^\times/G)$ is of finite index in $\mathrm{Hom}_{\Omega_{F_v}}(A_G, (O_{F_v^c})^\times)$, and so is an open subgroup of $\mathrm{Hom}_{\Omega_{F_v}}(A_G, (O_{F_v^c})^\times)$. The result now follows from the fact that, because $v \mid |G|$, the collection of groups

$$\left\{\mathrm{Hom}_{\Omega_{F_v}}(A_G, U_{|G|^n}(O_{F_v^c})) \mid n \geq 0\right\}$$

is a fundamental system of neighbourhoods of the identity of $\mathrm{Hom}_{\Omega_{F_v}}(A_G, (O_{F_v^c})^\times)$. □

Remark 4.7. When G is abelian, it follows from [21, Theorem 2.14] that we may take $N = |G|^2$ in Proposition 4.6. □

We shall also require the following related result in Section 15.

Proposition 4.8. *Let Γ be a finite group with an action of Ω_F. Suppose that $v \mid |\Gamma|$ is a finite place of F, and write $\mathfrak{p}_v$ for the maximal ideal of O_{F_v}. Then for all sufficiently large n, we have*

$$\mathrm{Hom}_{\Omega_{F_v}}(A_\Gamma, U_{\mathfrak{p}_v^n}(O_{F_v^c})) \subseteq \mathrm{rag}[\mathrm{Hom}_{\Omega_{F_v^c}}(R_\Gamma, (O_{F_v^c})^\times)].$$

Proof. The proof of this is very similar to that of Proposition 4.6. We observe that

$$|\Gamma^{ab}| \cdot \mathrm{Hom}_{\Omega_{F_v^c}}(A_\Gamma, (O_{F_v^c})^\times) \subseteq \mathrm{rag}[\mathrm{Hom}_{\Omega_{F_v^c}}(R_\Gamma, (O_{F_v^c})^\times)],$$

which implies that $\mathrm{rag}[\mathrm{Hom}_{\Omega_{F_v^c}}(R_\Gamma, (O_{F_v^c})^\times)]$ is an open subgroup of $\mathrm{Hom}_{\Omega_{F_v^c}}(A_\Gamma, (O_{F_v^c})^\times)$ because A_Γ is finitely generated. The desired result now follows from the fact that the collection of groups $\{\mathrm{Hom}_{\Omega_{F_v}}(A_\Gamma, U_{\mathfrak{p}_v^n}(O_{F_v^c})) \mid n \geq 0\}$ is a fundamental system of neighbourhoods of the identity of $\mathrm{Hom}_{\Omega_{F_v^c}}(A_\Gamma, (O_{F_v^c})^\times)$. □

5. Twisted forms and relative K-groups

Recall that G is a finite group upon which Ω_F acts trivially. In this section, we shall recall some basic facts concerning categorical twisted forms and relative algebraic K-groups. The reader may consult [3] and [32, Chapter 15] for some of the details that we omit.

5.1. **Twisted forms.** Suppose that R is a Dedekind domain with field of fractions L of characteristic zero. (For notational convenience, we shall sometimes also allow ourselves to take $R = L$.) Let $\mathfrak{A}$ be any R-algebra which is finitely generated as an R-module and which satisfies $\mathfrak{A} \otimes_R L \simeq LG$.

Definition 5.1. Let Λ be any extension of R, and write $\mathcal{P}(\mathfrak{A})$ and $\mathcal{P}(\mathfrak{A} \otimes_R \Lambda)$ for the categories of finitely generated, projective $\mathfrak{A}$ and $\mathfrak{A} \otimes_R \Lambda$-modules respectively. A *categorical* Λ*-twisted* $\mathfrak{A}$*-form* (or *twisted form* for short) is an element of the fibre product category $\mathcal{P}(\mathfrak{A}) \times_{\mathcal{P}(\mathfrak{A} \otimes_R \Lambda)} \mathcal{P}(\mathfrak{A})$, where the fibre product is taken with respect to the functor $\mathcal{P}(\mathfrak{A}) \to \mathcal{P}(\mathfrak{A} \otimes_R \Lambda)$ afforded by extension of scalars. In concrete terms therefore, a twisted form consists of 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. □

Example 5.2. If F_π/F is any G-extension, and $\mathcal{L}_\pi \subseteq F_\pi$ is any non-zero projective $O_F G$-module, then $(\mathcal{L}_\pi, O_F G; \mathbf{r}_G)$ is a categorical F^c-twisted $O_F G$-form. In particular, if F_π/F is a tame G-extension, then $(O_\pi, O_F G; \mathbf{r}_G)$ is a categorical F^c-twisted $O_F G$-form. Similarly, if v is any place of F, then (still assuming F_π/F to be tame) $(O_{\pi,v}, O_{F_v} G; \mathbf{r}_G)$ is a categorical F_v^c-twisted $O_{F_v} G$-form. We shall mainly be concerned with twisted forms of these types in this paper. □

We write $K_0(\mathfrak{A}, \Lambda)$ for the Grothendieck group associated to the fibre product category $\mathcal{P}(\mathfrak{A}) \times_{\mathcal{P}(\mathfrak{A} \otimes_R \Lambda)} \mathcal{P}(\mathfrak{A})$, and we write $[M, N; \xi]$ for the isomorphism class of the twisted form $(M, N; \xi)$ in $K_0(\mathfrak{A}, \Lambda)$. The group $K_0(\mathfrak{A}, \Lambda)$ is often called *the relative* K*-group with respect to the homomorphism* $\mathfrak{A} \to \Lambda$. Recall (see [32, Theorem 15.5]) that there is a long exact sequence of relative algebraic K-theory:

$$K_1(\mathfrak{A}) \to K_1(\mathfrak{A} \otimes_R \Lambda) \xrightarrow{\partial^1_{\mathfrak{A},\Lambda}} K_0(\mathfrak{A}, \Lambda) \xrightarrow{\partial^0_{\mathfrak{A},\Lambda}} K_0(\mathfrak{A}) \to K_0(\mathfrak{A} \otimes_R \Lambda). \tag{5.1}$$

The first and last arrows in this sequence are afforded by extension of scalars from R to Λ. The map $\partial^0_{\mathfrak{A},\Lambda}$ is defined by

$$\partial^0_{\mathfrak{A},\Lambda}([M, N; \lambda]) = [M] - [N].$$

The map $\partial^1_{\mathfrak{A},\Lambda}$ is defined by first recalling that the group $K_1(\mathfrak{A} \otimes_R \Lambda)$ is generated by pairs 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. If T is any projective $\mathfrak{A}$-submodule of V satisfying $T \otimes_{\mathfrak{A}} \Lambda \simeq V$, then 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.

We shall often ease notation and write e.g. ∂^0 rather than $\partial^0_{\mathfrak{A},\Lambda}$ when no confusion is likely to result.

5.2. **Idelic description and localisation.** [16, Chapter II, §1]. Let us retain the notation established above, and suppose in addition that we now work over a number field F. The reduced norm map

$$\mathrm{nrd} : (FG)^\times \to Z(FG)^\times$$

induces isomorphisms

$$K_1(FG) \simeq \mathrm{nrd}(K_1(FG)) \simeq \mathrm{nrd}((FG)^\times) \simeq \mathrm{Det}((FG)^\times) \subseteq Z(FG)^\times \tag{5.2}$$

and

$$K_1(F_vG) \simeq \mathrm{nrd}(K_1(F_vG)) \simeq \mathrm{nrd}((F_vG)^\times) \simeq \mathrm{Det}((F_vG)^\times) \subseteq Z(F_vG)^\times \tag{5.3}$$

for each place v of F. In general the natural map $K_1(\mathfrak{A}_v) \to K_1(F_vG)$ is not injective, and so the reduced norm map

$$\mathrm{nrd} : K_1(\mathfrak{A}_v) \to Z(\mathfrak{A}_v)^\times$$

is not an isomorphism (although it is surjective if $\mathfrak{A}_v$ is an O_{F_v}-maximal order in F_vG). If we write $K_1(\mathfrak{A}_v)'$ for the image of $K_1(\mathfrak{A}_v)$ in $K_1(F_vG)$, then (5.3) induces isomorphisms

$$K_1(\mathfrak{A}_v)' \simeq \mathrm{nrd}(K_1(\mathfrak{A}_v)') \simeq \mathrm{nrd}((\mathfrak{A}_v)^\times) \simeq \mathrm{Det}(\mathfrak{A}_v^\times). \tag{5.4}$$

We shall make frequent use of the identifications (5.2), (5.3) and (5.4) (as well as those afforded by Proposition 4.5) in what follows, sometimes without explicit mention.

For each place v of F, we write

$$\mathrm{loc}_v : K_1(FG) \to K_1(F_vG)$$

for the obvious localisation map.

Definition 5.3. We define the group of ideles $J(K_1(FG))$ of $K_1(FG)$ to be the restricted direct product over all 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 define the group of finite ideles $J_f(K_1(FG))$ in a similar manner but with the restricted direct product taken over all finite places v of F. □

If E is any extension of F, then the homomorphism

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

induces a homomorphism

$$\Delta_{\mathfrak{A},E} : \mathrm{Det}(FG)^\times \to \frac{J(K_1(FG))}{\prod_v \mathrm{Det}(\mathfrak{A}_v)^\times} \times \mathrm{Det}(EG)^\times.$$

Theorem 5.4. *(a) There is a natural isomorphism*

$$\mathrm{Cl}(\mathfrak{A}) \xrightarrow{\sim} \frac{J(K_1(FG))}{\mathrm{Det}(FG)^\times \prod_v \mathrm{Det}(\mathfrak{A}_v)^\times}.$$

(b) There is a natural isomorphism

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

□

Proof. Part (a) is a well-known result of A. Fröhlich (see e.g [17, Chapter I]. Part (b) is proved in [3, Theorem 3.5]. □

Remark 5.5. If $[M, N; \xi] \in K_0(\mathfrak{A}, E)$ and M, N are locally free $\mathfrak{A}$-modules of rank one (which is the only case that we shall need in this paper), then $h_{\mathfrak{A},E}([M, N; \xi])$ may be described explicitly as follows.

For each place v of F, we choose $\mathfrak{A}_v$-bases m_v of M_v and n_v of N_v. We also choose an FG basis n_∞ of N_F, as well as an FG-module isomorphism $\theta : M_F \xrightarrow{\sim} N_F$. Then, for each v, we may write $n_v = \nu_v \cdot n_\infty$, with $\nu_v \in (F_vG)^\times$. As $\theta^{-1}(n_\infty)$ is an FG-basis of M_F, we may write $m_v = \mu_v \cdot \theta^{-1}(n_\infty)$, with $\mu_v \in (F_vG)^\times$. Finally, writing θ_E for the map $M_E \to N_E$ afforded by θ via extension of scalars from F to E, we have that $(\xi \circ \theta_E^{-1})(n_\infty) = \nu_\infty \cdot n_\infty$ for some $\nu_\infty \in (EG)^\times$. Then 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 $J(K_1(FG)) \times K_1(EG)$, and a representative of $\partial^0(h_{\mathfrak{A},E}([M, N; \xi])) \in \mathrm{Cl}(\mathfrak{A})$ is given by the image of $(\mu_v \cdot \nu_v^{-1})_v \in J(K_1(FG))$. □

Remark 5.6. As $\mathfrak{A}_v = F_vG$ when v is infinite (by convention), we see that

$$\frac{J(K_1(FG))}{\prod_v \mathrm{Det}(\mathfrak{A}_v)^\times} \simeq \frac{J_f(K_1(FG))}{\prod_{v \nmid \infty} \mathrm{Det}(\mathfrak{A}_v)^\times}.$$

Hence the infinite places of F in fact play no explicit role on the right-hand sides of the isomorphisms given by Theorem 5.4, and so these isomorphisms may be formulated using the finite idele group $J_f(K_1(FG))$ of $K_1(FG)$ instead of the full idele group $J(K_1(FG))$. □

Lemma 5.7. *Suppose that v is a place of F and that E_v is any extension of F_v. Then there is an isomorphism*

$$K_0(\mathfrak{A}_v, E_v) \simeq \mathrm{Det}(E_vG)^\times / \mathrm{Det}(\mathfrak{A}_v)^\times.$$

Proof. This follows directly from the long exact sequence of relative K-theory (5.1) applied to $K_0(\mathfrak{A}_v, E_v)$, together with (5.3) and (5.4). □

For each place v of F, there is a localisation map on relative K-groups:

$$\lambda_v : K_0(\mathfrak{A}, E) \to K_0(\mathfrak{A}_v, E_v); \quad [M, N; \xi] \mapsto [M_v, N_v; \xi_v],$$

where ξ_v denotes the map obtained from ξ via extension of scalars from E to E_v. It is not hard to check that, in terms of the descriptions of $K_0(\mathfrak{A}, E)$ and $K_0(\mathfrak{A}_v, E_v)$ afforded by Theorem 5.4 and Lemma 5.7, the map λ_v is that induced by the homomorphism (which we denote by the same symbol λ_v)

$$\lambda_v : J(K_1(FG)) \times \mathrm{Det}(EG)^\times \to \mathrm{Det}(E_vG)^\times; \quad [(x_v)_v, x_\infty] \mapsto [x_v \cdot \mathrm{loc}_v(x_\infty)].$$

Definition 5.8. We define the idele group $J(K_0(\mathfrak{A}, E))$ of $K_0(\mathfrak{A}, E)$ to be the restricted direct product over all places v of F of the groups $K_0(\mathfrak{A}_v, E_v)$ with respect to the subgroups $K_0(\mathfrak{A}_v, O_{E_v})$.

We define the group of finite ideles $J_f(K_0(\mathfrak{A}, F^c))$ in a similar manner, but with the restricted direct product taken over all finite places of F. □

Proposition 5.9. *(a) The homomorphism*

$$\lambda := \prod_v \lambda_v : K_0(\mathfrak{A}, E) \to \prod_v K_0(\mathfrak{A}_v, E_v)$$

is injective.

(b) If F has no real places or if G admits no irreducible symplectic characters, then the homomorphism

$$\lambda_f := \prod_{v \nmid \infty} \lambda_v : K_0(\mathfrak{A}, E) \to \prod_{v \nmid \infty} K_0(\mathfrak{A}_v, E_v)$$

is injective.

(c) The image of λ lies in the idele group $J(K_0(\mathfrak{A}, E))$.

Proof. (a) Suppose that $\alpha \in K_0(\mathfrak{A}, E)$ lies in the kernel of λ, and let

$$[(x_v)_v, x_\infty] \in J(K_1(FG)) \times \mathrm{Det}(EG)^\times$$

be a representative of α. Then for each v, we have

$$x_v \cdot \mathrm{loc}_v(x_\infty) \in \mathrm{Det}(\mathfrak{A}_v)^\times \subseteq \mathrm{Det}(F_vG)^\times. \tag{5.5}$$

Since $x_v \in \mathrm{Det}(F_vG)^\times \subseteq Z(F_vG)^\times$, we see that $\mathrm{loc}_v(x_\infty) \in Z(F_vG)^\times$ for each v. Hence $x_\infty \in Z(FG)^\times$, and so via the Hasse–Schilling norm theorem (see [33, Theorem 7.6] or [11, Theorem 7.8]) we deduce that $x_\infty \in \mathrm{Det}(FG)^\times$. Hence α is also represented by the idele

$$[(\mathrm{loc}_v(x_\infty))_v, x_\infty^{-1}] \cdot [(x_v)_v, x_\infty] = [(x_v \cdot \mathrm{loc}_v(x_\infty))_v, 1],$$

and now (5.5) and Theorem 5.4(b) imply that $\alpha = 0$ in $K_0(\mathfrak{A}, E)$. Therefore λ is injective, as claimed.

(b) The proof of this assertion is virtually identical to that of part (a). Using the same notation as in the proof of part (a), we see that $\mathrm{loc}_v(x_\infty) \in \mathrm{Det}(F_vG)^\times \simeq Z(F_vG)^\times$ for each finite place v of F. This implies that $x_\infty \in Z(FG)^\times$. Under our hypotheses, we have that $\mathrm{Det}(FG)^\times \simeq Z(FG)^\times$, and so $x_\infty \in \mathrm{Det}(FG)^\times$. The remainder of the argument proceeds exactly as in the proof of part (a).

(c) If $\beta = [M, N; \xi] \in K_0(\mathfrak{A}, E)$, then for all but finitely many places v, the isomorphism $\xi_v : M \otimes_{O_F} E_v \xrightarrow{\sim} N \otimes_{O_F} E_v$ obtained from ξ via extension of scalars from E to E_v restricts to an isomorphism $M \otimes_{O_F} O_{E_v} \xrightarrow{\sim} N \otimes_{O_F} O_{E_v}$. Hence, for all but finitely many v, we have that $\lambda_v(\beta) \in K_0(\mathfrak{A}_v, O_{E_v})$, and so $\lambda(\beta) \in J(K_0(\mathfrak{A}, E))$, as asserted. □

6. Cohomological classes in relative K-groups

Recall that F is a number field and that G is a finite group upon which Ω_F acts trivially. In this section we shall explain how the set of realisable classes $\mathcal{R}(O_FG) \subseteq \mathrm{Cl}(O_FG)$ may be studied via imposing local cohomological conditions on elements of the relative K-group $K_0(O_FG, F^c)$.

Definition 6.1. We define maps Ψ and Ψ_v (for each place v of F) by

$$\Psi = \Psi_G : H^1_t(F, G) \to K_0(O_FG, F^c); \quad [\pi] \mapsto [O_\pi, O_FG; \mathbf{r}_G]$$

and

$$\Psi_v = \Psi_{G,v} : H^1_t(F_v, G) \to K_0(O_{F_v}G, F_v^c); \quad [\pi_v] \mapsto [O_{\pi_v}, O_{F_v}G; \mathbf{r}_G].$$

We set

$$K\mathcal{R}(O_FG) := \mathrm{Im}(\Psi).$$

□

Definition 6.2. We define the pointed set of ideles $J(H^1_t(F, G))$ of $H^1_t(F, G)$ to be the restricted direct product over all places v of F of the pointed sets $H^1_t(F_v, G)$ with respect to the pointed subsets $H^1_{nr}(F_v, G)$, and we write

$$\Psi^{id} : J(H^1_t(F, G)) \to J(K_0(O_FG, F^c))$$

for the map afforded by the maps $\Psi_v : H^1_t(F_v, G) \to K_0(O_{F_v}G, F_v^c)$. □

In general, $K\mathcal{R}(O_FG)$ is not a subgroup of $K_0(O_FG, F^c)$. However, although $H^1_{nr}(F_v, G)$ is in general merely a pointed set and not a group, the following result holds.

Proposition 6.3. *Let v be any place of F, and write Ψ_v^{nr} for the restriction of Ψ_v to $H^1_{nr}(F_v, G)$. Then $\mathrm{Im}(\Psi_v^{nr})$ is a subgroup of $K_0(O_{F_v}G, F_v^c)$.*

Proof. If v is infinite, then $H^1_{nr}(F_v, G) = 0$, and so $\mathrm{Im}(\Psi_v^{nr}) = 0$. For finite v, the result follows from Proposition 3.7 and Lemma 5.7. □

Definition 6.4. We say that an element $x \in K_0(O_FG, F^c)$ is *cohomological* (respectively *cohomological at v*) if $x \in \mathrm{Im}(\Psi)$ (respectively $\lambda_v(x) \in \mathrm{Im}(\Psi_v)$). We say that x is *locally cohomological* if x is cohomological at v for all places v of F. We write

$$\mathrm{LC}(O_FG) := \lambda^{-1}(\mathrm{Im}(\Psi^{id}))$$

for the subset of $K_0(O_FG, F^c)$ consisting of locally cohomological elements. □

The long exact sequence of relative K-theory (5.1) applied to $K_0(O_FG, F^c)$ yields a long exact sequence

$$K_1(O_FG) \to K_1(F^cG) \xrightarrow{\partial^1} K_0(O_FG, F^c) \xrightarrow{\partial^0} \mathrm{Cl}(O_FG) \to 0, \tag{6.1}$$

where $\mathrm{Cl}(O_FG)$ denotes the locally free class group of O_FG. We set

$$\psi := \partial^0 \circ \Psi,$$

and we write

$$\mathcal{R}(O_FG) := \mathrm{Im}(\psi).$$

The second-named author has conjectured that that $\mathcal{R}(O_FG)$ is always a subgroup of $\mathrm{Cl}(O_FG)$, and he has proved that this is true whenever G is abelian (see [21, Corollary 6.20]). The following conjecture gives a precise characterisation of the image $K\mathcal{R}(O_FG)$ of Ψ.

Conjecture 6.5. An element of $K_0(O_FG, F^c)$ is cohomological if and only if it is locally cohomological. In other words, we have that

$$K\mathcal{R}(O_FG) = \mathrm{LC}(O_FG).$$

□

Let us now explain why Conjecture 6.5 implies that $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$. In order to do this, we shall require the following result which is equivalent to a theorem of the second-named author when G is abelian, and whose proof relies on results contained in [21] and [23]. Before stating the result, we remind the reader that $\prod_v \mathrm{Im}(\Psi_v^{nr})$ is not merely a pointed set, but is in fact a subgroup of $J(K_0(O_F G, F^c))$ (see Proposition 6.3).

Theorem 6.6. *Let*

$$\overline{\Psi^{id}} : J(H_t^1(F, G)) \to \frac{J(K_0(O_F G, F^c))}{\lambda[\partial^1(K_1(F^c G))] \cdot \prod_v \mathrm{Im}(\Psi_v^{nr})}$$

denote the map of pointed sets given by the composition of the map Ψ^{id} with the quotient homomorphism

$$J(K_0(O_F G, F^c)) \to \frac{J(K_0(O_F G, F^c))}{\lambda[\partial^1(K_1(F^c G))] \cdot \prod_v \mathrm{Im}(\Psi_v^{nr})}.$$

Then the image of $\overline{\Psi^{id}}$ is in fact a group. Hence it follows that

$$\lambda[\partial^1(K_1(F^c G))] \cdot \mathrm{Im}(\Psi^{id})$$

is a subgroup of $J(K_0(O_F G, F^c))$.

This theorem will be proved in Section 12. It implies the following result.

Theorem 6.7. *If Conjecture 6.5 holds, then $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$.*

Proof. It follows from the exact sequence (6.1) that $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$ if and only if $\partial^1(K_1(F^c G)) \cdot K\mathcal{R}(O_F G)$ is a subgroup of $K_0(O_F G, F^c)$. However, if Conjecture 6.5 is true, then Theorem 6.6 implies that

$$\partial^1(K_1(F^c G)) \cdot K\mathcal{R}(O_F G) = \partial^1(K_1(F^c G)) \cdot \mathrm{LC}(O_F G) \tag{6.2}$$

is the kernel of the homomorphism

$$K_0(O_F G, F^c) \xrightarrow{\lambda} J(K_0(O_F G, F^c)) \to \frac{J(K_0(O_F G, F^c))}{\lambda[\partial^1(K_1(F^c G))] \cdot \mathrm{Im}(\Psi^{id})},$$

where the last arrow denotes the obvious quotient homomorphism. This implies the desired result. □

We conclude this section with the following result on unramified locally cohomological classes in $K_0(O_F G, F^c)$. This will be used in the proofs of Theorem 16.4 and Theorem E of the Introduction (see Section 16 below).

Proposition 6.8. *(a) Let L be the maximal, abelian, everywhere unramified (including at all infinite places) extension of F of exponent $|G^{ab}|$, and suppose that $y \in K_0(O_FG, F^c)$ lies in the kernel of the map*

$$\beta : K_0(O_FG, F^c) \xrightarrow{\lambda_F} J(K_0(O_FG, F^c)) \to \frac{J(K_0(O_FG, F^c))}{\prod_v \mathrm{Im}(\Psi_v^{nr})}.$$

Then y lies in the kernel of the extension of scalars map

$$e_L : K_0(O_FG, F^c) \to K_0(O_LG, F^c).$$

Hence, if $(h_F^+, |G^{ab}|) = 1$ (where h_F^+ denotes the narrow class number of F), then $L = F$, and so β is injective.

(b) Suppose that G admits no non-trivial irreducible symplectic characters, or that F has no real places, and that $y \in K_0(O_FG, F^c)$ lies in the kernel of the map

$$\beta_f : K_0(O_FG, F^c) \xrightarrow{\lambda_{f,F}} J_f(K_0(O_FG, F^c)) \to \frac{J_f(K_0(O_FG, F^c))}{\prod_{v\nmid\infty} \mathrm{Im}(\Psi_v^{nr})}.$$

Then y lies in the kernel of the extension of scalars map

$$e_M : K_0(O_FG, F^c) \to K_0(O_MG, F^c),$$

where M is the maximal, abelian, unramified (at all finite places) extension of F of exponent $|G^{ab}|$.

Hence if $(h_F, |G^{ab}|) = 1$ then $L = F$, and so β_f is injective.

Proof. (a) Suppose that $y = [(y_v), y_\infty]$ lies in the kernel of β, and let E/F be the smallest Galois extension such that Ω_E fixes y_∞. For each place v of F, let $w(v)$ be the place of E afforded by our fixed choice of embedding $F^c \to F_v^c$.

As y lies in the kernel of β, we have that $y_v \cdot \mathrm{loc}_v(y_\infty) \in \mathrm{Im}(\Psi_v^{nr})$ for each place v. Hence, for each v, $\mathrm{loc}_v(y_\infty) \in H(Z(F_vG))$ is an unramified G^{ab}-resolvend over F_v (cf. Proposition 3.6). It follows that, for each v, the extension $E_{w(v)}/F_v$ is unramified and that $[E_{w(v)} : F_v]$ divides $|G^{ab}|$. This implies that E/F is unramified at all places v, and is of exponent dividing $|G^{ab}|$. Hence $E \subseteq L$, and so $y_\infty \in \mathrm{Det}(LG)^\times$.

Now since $y_v \cdot \mathrm{loc}_v(y_\infty) \in \mathrm{Im}(\Psi_v^{nr})$ for each place v, we see that in fact $y_v \cdot \mathrm{loc}_v(y_\infty) \in \mathrm{Det}(O_{L_v}G)^\times$. Hence $e_L(y)$ is in the kernel of the localisation map

$$\lambda_L : K_0(O_LG, F^c) \to J(K_0(O_LG, F^c)),$$

and since λ_L is injective (see Proposition 5.9(a)) it follows that $e_L(y) = 0$.

The final assertion now follows immediately.

(b) Virtually identical to the proof of (a), except that here, because either G admits no irreducible symplectic characters or F has no real places, we may appeal to the injectivity of the localisation map $\lambda_{f,M}$ (see Proposition 5.9(b)) rather than that of λ_M. □

7. Local extensions I

The goal of this section is to describe how resolvends of normal integral bases of tamely ramified, non-archimedean local extensions admit *Stickelberger factorisations* (see Definition 7.12). This reflects the fact that every tamely ramified G-extension of F_v is a compositum of an unramified extension of F_v and a twist of a totally ramified extension of F_v. All of the results in this section are based on unpublished notes of the second-named author.

For each finite place v of F, we fix a uniformiser ϖ_v of F_v, and we write q_v for the order of the residue field of F_v. We fix a compatible set of roots of unity $\{\zeta_m\}$, and a compatible set $\{\varpi_v^{1/m}\}$ of roots of ϖ_v. So, if m and n are any two positive integers, then we have $(\zeta_{mn})^m = \zeta_n$, and $(\varpi_v^{1/mn})^m = \varpi_v^{1/n}$.

Recall that F_v^{nr} (respectively F_v^t) denotes the maximal unramified (respectively tamely ramified) extension of F_v. Then

$$F_v^{nr} = \bigcup_{\substack{m\geq 1\\(m,q_v)=1}} F_v(\zeta_m), \quad F_v^t = \bigcup_{\substack{m\geq 1\\(m,q_v)=1}} F_v(\zeta_m, \varpi_v^{1/m}).$$

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

$$\phi_v(\zeta_m) = \zeta_m^{q_v}, \qquad \phi_v(\varpi_v^{1/m}) = \varpi_v^{1/m}$$

for each integer m coprime to q_v. Our choice of compatible roots of unity also uniquely specifies a topological generator σ_v of $\mathrm{Gal}(F_v^t/F_v^{nr})$ by the conditions

$$\sigma_v(\varpi_v^{1/m}) = \zeta_m \cdot \varpi_v^{1/m}, \qquad \sigma_v(\zeta_m) = \zeta_m$$

for all integers m coprime to q_v. The group $\Omega_v^t := \mathrm{Gal}(F_v^t/F_v)$ is topologically generated by ϕ_v and σ_v, subject to the relation

$$\phi_v \cdot \sigma_v \cdot \phi_v^{-1} = \sigma_v^{q_v}. \tag{7.1}$$

While reading the remainder of this section (especially Proposition 7.7 below), it may be helpful for the reader to keep in mind the statement and proof of the following well-known result which provides some motivation for a number of subsequent constructions.

Proposition 7.1. *Set $L := F_v$. Let n be a positive integer with $(n, q_v) = 1$, and suppose that $\mu_n \subseteq L$. Set $E = L(\varpi_v^{1/n})$, $\Gamma = \mathrm{Gal}(E/L) = \mathbf{Z}/n\mathbf{Z}$, and $\beta = \sum_{i=0}^{n-1} \varpi_v^{i/n}$. Then $O_E = O_L\Gamma \cdot \beta$.*

Proof. We first observe that plainly $O_L\Gamma \cdot \beta \subseteq O_E$, as $\beta \in O_E$.

Let χ denote the Kummer character of Γ, defined by

$$\chi(\gamma) = \frac{\gamma(\varpi_v^{1/n})}{\varpi_v^{1/n}} \in \mu_n$$

for each $\gamma \in \Gamma$. Then $\widehat{\Gamma} = \langle \chi \rangle$, and for each $0 \leq j \leq n-1$, we have

$$\begin{aligned}\left(\sum_{\gamma} \chi^j(\gamma)\gamma^{-1}\right) \cdot \beta &= \left(\sum_{\gamma} \chi^j(\gamma)\gamma^{-1}\right) \cdot \left(\sum_{i=0}^{n-1} \varpi_v^{i/n}\right) \\ &= \sum_{i=0}^{n-1} \left(\sum_{\gamma} \chi^j(\gamma) \cdot \chi^{-i}(\gamma) \cdot \varpi_v^{i/n}\right) \\ &= n \cdot \varpi_v^{j/n}.\end{aligned}$$

As $n \in O_L^{\times}$, we therefore see that $\{\varpi_v^{j/n}\}_{j=0}^{n-1} \subseteq O_L\Gamma \cdot \beta$, which implies that $O_E \subseteq O_L\Gamma \cdot \beta$. This implies the desired result. □

Definition 7.2. For each finite place v of F, we define

$$\Sigma_v(G) := \{s \in G \mid s^{q_v} \in c(s)\}$$

(recall that $c(s)$ denotes the conjugacy class of s in G). Plainly if $s \in \Sigma_v(G)$, then both $c(s)$ and $\langle s \rangle$ are subsets of $\Sigma_v(G)$. Let us also remark that if $s \in \Sigma_v(G)$, then the order $|s|$ of s is coprime to q_v. □

Definition 7.3. If $s \in G$, we set

$$\beta_s := \frac{1}{|s|} \sum_{i=0}^{|s|-1} \varpi_v^{i/|s|};$$

note that β_s depends only upon $|s|$, and so in particular we have

$$\beta_s = \beta_{g^{-1}sg}$$

for every $g \in G$. We define $\varphi_{v,s} \in \mathrm{Map}(G, O_{F_v^c})$ by setting

$$\varphi_{v,s}(g) = \begin{cases} \sigma_v^i(\beta_s) & \text{if } g = s^i; \\ 0 & \text{if } g \notin \langle s \rangle. \end{cases}$$

Then

$$\mathbf{r}_G(\varphi_{v,s}) = \sum_{i=0}^{|s|-1} \varphi_{v,s}(s^i)s^{-i} = \sum_{i=0}^{|s|-1} \sigma_v^i(\beta_s)s^{-i}. \tag{7.2}$$

We note that for each $g \in G$, we have

$$\mathbf{r}_G(\varphi_{v,g^{-1}sg}) = g^{-1} \cdot \mathbf{r}_G(\varphi_{v,s}) \cdot g, \tag{7.3}$$

and so

$$\mathrm{Det}(\mathbf{r}_G(\varphi_{v,g^{-1}sg})) = \mathrm{Det}(\mathbf{r}_G(\varphi_{v,s})), \tag{7.4}$$

i.e. the element $\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s}))$ depends only upon the conjugacy class $c(s)$ of s in G. We remark that it will be shown later as a consequence of properties of the Stickelberger pairing that $\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s}))$ in fact determines the subgroup $\langle s \rangle$ of G up to conjugation (see Remark 4.2 and Proposition 10.5(b)).

We shall see that generators of inertia subgroups of tame Galois G-extensions of F_v lie in $\Sigma_v(G)$, and that the elements $\varphi_{v,s}$ for $s \in G$ with $(|s|, q_v) = 1$ may be used to construct normal integral basis generators of tame (and of course totally ramified) Galois G-extensions of F_v^{nr}. □

In order to ease notation, we shall now set $L := F_v$ and $O := O_L$, and we shall drop the subscript v from our notation for the rest of this section.

Suppose now that L_π/L is a tamely ramified Galois G-extension of L, corresponding to $\pi \in \mathrm{Hom}(\Omega^t, G)$. We are going to describe the second-named author's decomposition of resolvends of normal integral basis generators of L_π/L (see [23] and also [7, Section 6]). When G is abelian, this decomposition is an analogue of a version of Stickelberger's factorisation of Gauss sums.

Write $s := \pi(\sigma)$, $t := \pi(\phi)$; then $t \cdot s \cdot t^{-1} = s^q$, and so $s \in \Sigma(G)$. We define $\pi_r, \pi_{nr} \in \mathrm{Map}(\Omega^t, G)$ by setting

$$\pi_r(\sigma^m\phi^n) = \pi(\sigma^m) = s^m, \tag{7.5}$$

$$\pi_{nr}(\sigma^m\phi^n) = \pi(\phi^n) = t^n. \tag{7.6}$$

If $\omega_i \in \Omega^t$ $(i = 1, 2)$ with $\omega_i = \sigma^{m_i} \cdot \phi^{n_i}$, then a straightforward calculation using (7.1) shows that

$$\omega_1 \cdot \omega_2 = \sigma^{m_1 + m_2 q^{n_1}} \cdot \phi^{n_1+n_2}.$$

This implies that $\pi_{nr} \in \mathrm{Hom}(\Omega^{nr}, G)$. Plainly we have

$$\pi(\omega) = \pi_r(\omega) \cdot \pi_{nr}(\omega) \tag{7.7}$$

for every $\omega = \sigma^m \cdot \phi^n \in \Omega^t$. The map $\pi_{nr} \in \mathrm{Hom}(\Omega^{nr}, G)$ corresponds to an unramified Galois G-extension $L_{\pi_{nr}}$ of L (see Remark 7.10 below for a more detailed discussion of this point). Since $L_{\pi_{nr}}/L$ is unramified, $O_{\pi_{nr}}$ is a free $O_L G$-module. Let a_{nr} be any normal integral basis generator of this extension. Note that $\mathbf{r}_G(a_{nr}) \in H(OG)$, because $L_{\pi_{nr}}/L$ is unramified (see Corollary 3.3(iv)).

Definition 7.4. Let $G(\pi_{nr})$ denote the group G with Ω^t-action given by

$$\omega(g) = \pi_{nr}(\omega) \cdot g \cdot \pi_{nr}(\omega)^{-1}$$

for $\omega \in \Omega^t$ and $g \in G$. □

Lemma 7.5. *The map π_r is a $G(\pi_{nr})$-valued 1-cocycle of Ω^t.*

Proof. Suppose that $\omega_1, \omega_2 \in \Omega^t$. Then since $\pi_{nr} \in \mathrm{Hom}(\Omega^{nr}, G)$ and $\pi = \pi_r \cdot \pi_{nr}$, a straightforward calculation shows that

$$\pi_r(\omega_1\omega_2) = \pi_r(\omega_1) \cdot \pi_{nr}(\omega_1) \cdot \pi_r(\omega_2) \cdot \pi_{nr}(\omega_1)^{-1},$$

and this establishes the desired result. □

Definition 7.6. We write ${}^{\pi_r}G(\pi_{nr})$ for the set G endowed with the following action of Ω^t: for every $g \in G$ and $\omega \in \Omega^t$ we have

$$g^{\omega} = \pi_r(\omega) \cdot \pi_{nr}(\omega) \cdot g \cdot \pi_{nr}(\omega)^{-1}.$$

Lemma 7.5 implies that if $\omega_1, \omega_2 \in \Omega^t$, then

$$g^{(\omega_1\omega_2)} = (g^{\omega_2})^{\omega_1}.$$

We set

$$L_{\pi_r}(\pi_{nr}) := \mathrm{Map}_{\Omega^t}({}^{\pi_r}G(\pi_{nr}), L^t).$$

The algebra $(L^t G(\pi_{nr}))^{\Omega^t}$ acts on $L_{\pi_r}(\pi_{nr})$ via the rule

$$(\alpha \cdot a)(h) = \sum_{g \in G} \alpha_g \cdot a(h \cdot g)$$

for all $h \in G$ and $\alpha = \sum_{g \in G} \alpha_g \cdot g \in (L^t G(\pi_{nr}))^{\Omega^t}$. □

Proposition 7.7. *(a) Recall that $s \in \Sigma(G)$. We have that $\varphi_s \in L_{\pi_r}(\pi_{nr})$.*
(b) Set

$$\mathfrak{A}(\pi_{nr}) = (O_{L^c} G(\pi_{nr}))^{\Omega^t},$$

and let $O_{\pi_r}(\pi_{nr})$ be the integral closure of O_L in $L_{\pi_r}(\pi_{nr})$. Then

$$\mathfrak{A}(\pi_{nr}) \cdot \varphi_s = O_{\pi_r}(\pi_{nr}).$$

(c) For any $\alpha_r \in L_{\pi_r}(\pi_{nr})$ and $\omega \in \Omega^t$, we have

$$\mathbf{r}_G(\alpha_r)^\omega = \pi_{nr}(\omega)^{-1} \cdot \mathbf{r}_G(\alpha_r) \cdot \pi(\omega).$$

Proof. (a) Suppose that $\omega = \sigma^m \cdot \phi^n \in \Omega^t$. If $g \in G$ and $g \notin \langle s \rangle$, then we have that

$$\varphi_s(g^\omega) = 0 = \varphi_s(g)^\omega.$$

On the other hand, we also have

$$\begin{aligned}
\varphi_s((s^i)^\omega) &= \varphi_s((s^i)^{\sigma^m\phi^n}) \\
&= \varphi_s(s^m \cdot t^n \cdot s^i \cdot t^{-n}) \\
&= \varphi_s(s^{m+iq^n}) \\
&= \sigma^{m+iq^n}(\beta_s) \\
&= (\sigma^m \cdot \phi^n) \cdot \sigma^i(\beta_s) \\
&= \varphi_s(s^i)^\omega.
\end{aligned}$$

Hence $\varphi_s \in L_{\pi_r}(\pi_{nr})$, as claimed.

(b) The proof of this assertion is very similar to that of [7, Lemma 6.6], which is in turn an analogue of [21, 5.4].

Set $H = \langle s \rangle$. Then Ω^t acts transitively on ${}^{\pi_r}H(\pi_{nr}) \subseteq^{\pi_r} G(\pi_{nr})$, and so the algebra

$$L_{\pi_r}(\pi_{nr})^H := \mathrm{Map}_{\Omega^t}({}^{\pi_r}H(\pi_{nr}), L^t)$$

may be identified with a subfield of L^t via identifying $b \in L_{\pi_r}(\pi_{nr})^H$ with $x_b = b(\mathbf{1}) \in L^t$. We have that

$$x_b^{\sigma^m} = b(s^m), \quad x_b^\phi = x_b,$$

and so it follows that $L_{\pi_r}(\pi_{nr})^H$ is the subfield of L^t consisting of those elements of L^t that are fixed by both ϕ and $\sigma^{|s|}$. This implies that $L_{\pi_r}(\pi_{nr})^H = L[\varpi^{1/|s|}]$ (which in general will not be normal over L), and that the integral closure of O_L in $L_{\pi_r}(\pi_{nr})^H$ is equal to $O_L[\varpi^{1/|s|}]$. Plainly $\beta_s \in O_L[\varpi^{1/|s|}]$ (as $|s|$ is invertible in O_L), and the element β_s corresponds to the element $\varphi_s|_H \in L_{\pi_r}(\pi_{nr})^H$.

If we set $\mathfrak{A}(\pi_{nr})_H := (O_{L^t}H(\pi_{nr}))^{\Omega^t}$, then for each integer k with $0 \leq k \leq |s|-1$, it is not hard to check that

$$\left(\sum_{i=0}^{|s|-1} \zeta_{|s|}^{-ki} s^i\right)^\phi = \sum_{i=0}^{|s|-1} \zeta_{|s|}^{-ki} s^i,$$

and so we see that

$$\sum_{i=0}^{|s|-1} \zeta_{|s|}^{-ki} s^i \in \mathfrak{A}(\pi_{nr})_H.$$

A straightforward computation (cf. [21, 5.4]) also shows that

$$\left(\sum_{i=0}^{|s|-1} \zeta_{|s|}^{-ki} s^i \right) \cdot \beta_s = \varpi^{k/|s|}.$$

It therefore follows that $\mathfrak{A}(\pi_{nr})_H \cdot \beta_s = O_L[\varpi^{1/|s|}]$, and this in turn implies that

$$\mathfrak{A}(\pi_{nr}) \cdot \varphi_s = O_{\pi_r}(\pi_{nr}),$$

as asserted.

(c) We have

$$\begin{aligned}
\mathbf{r}_G(\alpha_r)^\omega &= \sum_{g \in G} \alpha_r(g)^\omega \cdot g^{-1} \\
&= \sum_{g \in G} \alpha_r(g^\omega) \cdot g^{-1} \\
&= \sum_{g \in G} \alpha_r(\pi_r(\omega) \cdot \pi_{nr}(\omega) \cdot g \cdot \pi_{nr}^{-1}(\omega)) \cdot g^{-1} \\
&= \sum_{g \in G} \alpha_r(g) \cdot \pi_{nr}(\omega)^{-1} \cdot g^{-1} \cdot \pi_r(\omega) \cdot \pi_{nr}(\omega) \\
&= \pi_{nr}(\omega)^{-1} \cdot \mathbf{r}_G(\alpha_r) \cdot \pi(\omega),
\end{aligned}$$

as claimed. □

Corollary 7.8. *For any $\alpha_r \in L_{\pi_r}(\pi_{nr})$ and $\alpha_{nr} \in L_{\pi_{nr}}$, there is a unique $\alpha \in L_\pi$ such that*

$$\mathbf{r}_G(\alpha_{nr}) \cdot \mathbf{r}_G(\alpha_r) = \mathbf{r}_G(\alpha).$$

Proof. Proposition 7.7(c) implies that, for any $\omega \in \Omega^t$, we have

$$[\mathbf{r}_G(\alpha_{nr}) \cdot \mathbf{r}_G(\alpha_r)]^\omega = \mathbf{r}_G(\alpha_{nr}) \cdot \mathbf{r}_G(\alpha_r) \cdot \pi(\omega),$$

and so $\mathbf{r}_G(\alpha_{nr}) \cdot \mathbf{r}_G(\alpha_r) \in H(LG)$. As the map $\mathbf{r}_G$ is bijective, it follows that there is a unique $\alpha \in \mathrm{Map}(G, L^c)$ such that

$$\mathbf{r}_G(\alpha_{nr}) \cdot \mathbf{r}_G(\alpha_r) = \mathbf{r}_G(\alpha),$$

and that $\alpha \in L_\pi$. □

Theorem 7.9. *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*

$$\mathbf{r}_G(a_{nr}) \cdot \mathbf{r}_G(\varphi_s) = \mathbf{r}_G(a) \tag{7.8}$$

is a normal integral basis generator of L_π/L.

Proof. The proof of this assertion is very similar to that of the analogous result in the abelian case described in [21, (5.7), page 283]. We first observe that plainly $O_L G \cdot a \subseteq O_\pi$ because $a_{nr} \in O_{\pi_{nr}}$ and $\varphi_s \in O_{\pi_r}(\pi_{nr})$. Hence, to prove the desired result, it suffices to show that

$$\mathrm{disc}(O_L G \cdot a/O_L) = \mathrm{disc}(O_\pi/O_L).$$

This will in turn follow if we show that

$$\mathrm{disc}(O_{L^{nr}} G \cdot a/O_{L^{nr}}) = \mathrm{disc}(O_\pi/O_L) \cdot O_{L^{nr}}.$$

Recall (see (2.3)) that we may write $L_\pi \simeq \bigoplus_{G/\pi(\Omega^t)} L^\pi$, where L^π is a field with $\mathrm{Gal}(L^\pi/L) \simeq \pi(\Omega^t)$. Under this last isomorphism, the inertia subgroup of $\mathrm{Gal}(L^\pi/L)$ is isomorphic to $\langle s \rangle$. The standard formula for tame field discriminants therefore yields

$$\mathrm{disc}(O^\pi/O_L) = \varpi^{(|s|-1)|\pi(\Omega^t)|/|s|} \cdot O_L$$

and so we have

$$\mathrm{disc}(O_\pi/O) = \varpi^{(|s|-1)|G|/|s|} \cdot O_L. \tag{7.9}$$

Now $\mathbf{r}_G(a_{nr}) \in (O_{L^{nr}} G)^\times$, and we see from the proof of Proposition 7.7(b) that

$$\begin{aligned} O_{L^{nr}} G \cdot a &= O_{L^{nr}} G \cdot \varphi_s \\ &= O_{\pi_r}(\pi_{nr}) \otimes_{O_L} O_{L^{nr}} \\ &\simeq \bigoplus_{G/\langle s \rangle} O_{L^{nr}}[\varpi^{1/|s|}]. \end{aligned}$$

Since

$$\mathrm{disc}(O_{L^{nr}}[\varpi^{1/|s|}]/O_{L^{nr}}) = \varpi^{|s|-1} \cdot O_{L^{nr}},$$

it follows that

$$\begin{aligned} \mathrm{disc}(O_{L^{nr}} G \cdot a/O_{L^{nr}}) &= \varpi^{(|s|-1)|G|/|s|} \cdot O_{L^{nr}} \\ &= \mathrm{disc}(O_\pi/O) \cdot O_{L^{nr}}, \end{aligned}$$

and this establishes the desired result. □

Remark 7.10. We caution the reader that $L_{\pi_{nr}}$ is *not* in general equal to the maximal unramified subextension of L_π/L, even when L_π is a field. Suppose, for example, that L_π is a field, and write L_0 for the maximal unramified subextension of L_π/L. Set $f = [L_0 : L]$. Then it is not hard to check that

$$L_{\pi_{nr}} \simeq \prod_{i=1}^{|G|/f} L_0, \tag{7.10}$$

and so $L_{\pi_{nr}}$ is a Galois algebra with 'core field' L_0. If $\alpha \in O_{L_0}$ is such that $O_{L_0} = O_L[\mathrm{Gal}(L_0/L)] \cdot \alpha$, then we may take $a_{nr} = (\alpha, 0, \ldots, 0)$ under the identification given by (7.10).

Suppose further that L contains the $|s|$-th roots of unity, and that $L_\pi = L_0 \cdot L(\varpi^{1/|s|})$. To ease notation, write $M := L(\varpi^{1/|s|})$, and set $H = \langle s \rangle$. Then a calculation similar to (but simpler than) that given in the proof of Proposition 7.7(b) (see also Proposition 7.1) shows that $O_M = O_L[H] \cdot \beta_s$, and it may be shown by computing the coefficient of $\mathbf{1}_G$ on the left-hand side of (7.8) that $a = \alpha \cdot \beta_s$, as is of course well-known. □

Remark 7.11. Suppose that $s \in G$ with $(|s|, q) = 1$. A straightforward computation (cf. the proofs of Propositions 7.1 and 7.7(b)) shows that for every $\omega \in \Omega_{L^{nr}}$, we may write

$$\mathbf{r}_G(\varphi_s)^\omega = \mathbf{r}_G(\varphi_s) \cdot \tilde{\varphi}_s(\omega)$$

where $[\tilde{\varphi}_s] \in H^1_t(L^{nr}, G)$, and that φ_s is a normal integral basis generator of $L^{nr}_{\tilde{\varphi}_s}/L^{nr}$. We have that $[\tilde{\varphi}_{s_1}] = [\tilde{\varphi}_{s_2}]$ in $H^1_t(L^{nr}, G)$ if and only if $c(s_1) = c(s_2)$. It is easy to show that every element of $H^1_t(L^{nr}, G)$ is of the form $[\tilde{\varphi}_s]$ for some $s \in G$ with $(|s|, q) = 1$ (cf. the proof of Proposition 7.1 again). □

Definition 7.12. Let a be any normal integral basis generator of L_π/L. Theorem 7.9 implies that we may write

$$\mathbf{r}_G(a) = u \cdot \mathbf{r}_G(a_{nr}) \cdot \mathbf{r}_G(\varphi_s), \tag{7.11}$$

where $u \in (OG)^\times$ and a_{nr} is any normal integral basis generator of $L_{\pi_{nr}}/L$. This may be viewed as being a non-abelian analogue of a version of Stickelberger's factorisation of abelian Gauss sums (see [18, pages XXXV–XXXVI, and Theorems 135 and 136] and [21, Introduction]), and so we call (7.11) a *Stickelberger factorisation* of $\mathbf{r}_G(a)$. □

8. Local extensions II

Our goal in this section is to state certain results analogous to, (but very much simpler than), those in Section 7, for extensions of F_v where v is an infinite place of F. This section may therefore be viewed as being a 'supplement at infinity' to Section 7 (cf. [17, Chapter

I, §3]). We remind the reader that, if v is infinite, by convention, we set $O_{F_v}G = F_vG$ and $H^1_t(F_v, G) = H^1(F_v, G)$.

Suppose first that v is a complex place of F. Then

$$K_0(O_{F_v}G, F_v^c) = 0, \quad H^1(F_v, G) = 0,$$

and we set $\Sigma_v(G) = \{1\}$. As this case is totally degenerate, we therefore suppose henceforth in this section that v is real. We set $L = F_v \simeq \mathbf{R}$, and for the remainder of this section, we drop any further reference to v from our notation.

Set $\mathrm{Gal}(L^c/L) = \langle\sigma\rangle$, and fix a primitive fourth root of unity $\zeta_4 \in L^c$ (cf. the choice of compatible roots of unity made at the beginning of Section 7), so $L^c = L(\zeta_4)$.

Write

$$\Sigma(G) := \{s \in G \mid s^2 = e\}. \tag{8.1}$$

(Note that this set is in fact independent of v.) For each $s \in \Sigma(G)$, we set

$$\beta_s = \frac{1}{2}(1 + \zeta_4).$$

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

$$\varphi_s(g) = \begin{cases} \sigma^i(\beta_s) & \text{if } g = s^i; \\ 0 & \text{if } g \notin \langle s\rangle. \end{cases}$$

Then it is easy to check that

$$\mathbf{r}_G(\varphi_s) = \beta_s \cdot e + \sigma(\beta_s) \cdot s = \frac{1}{2}[(1 + \zeta_4) \cdot e + (1 - \zeta_4) \cdot s].$$

Proposition 8.1. *Suppose that $\pi \in \mathrm{Hom}(\Omega_L, G)$ with $\pi(\sigma) = s$. Then $\varphi_s \in L_\pi$, and*

$$L_\pi = LG \cdot \varphi_s.$$

Proof. The first assertion follows directly from the definition of φ_s. The second is an immediate consequence of the fact that $\mathbf{r}_G(\varphi_s) \in (L^cG)^\times$, because

$$\frac{1}{2}\left((1 + \zeta_4) \cdot e + (1 - \zeta_4) \cdot s\right) \cdot \frac{1}{2}\left((1 - \zeta_4) \cdot e + (1 + \zeta_4) \cdot s\right) = 1.$$

□

Proposition 8.2. *Suppose that $\chi \in R_G$, and write*

$$\chi\,|_{\langle s\rangle} = a \cdot \mathbf{1} + b \cdot \varepsilon,$$

where ε denotes the unique non-trivial irreducible character of $\langle s\rangle$. Then

$$[\mathrm{Det}(\mathbf{r}_G(\varphi_s))](\chi) = (-1)^{b/2}.$$

Proof. This follows via a straightforward computation:

$$\begin{aligned}[\mathrm{Det}(\mathbf{r}_G(\varphi_s))](\chi) &= \mathbf{1}(\mathbf{r}_G(\varphi_s))^a \cdot \varepsilon(\mathbf{r}_G(\varphi_s))^b \\ &= (\beta_s + \sigma(\beta_s))^a \cdot (\beta_s - \sigma(\beta_s))^b \\ &= 1^a \cdot \zeta_4^b \\ &= (-1)^{b/2}.\end{aligned}$$

□

Remark 8.3. In terms of the Stickelberger pairing $\langle -, - \rangle_G$ which will be introduced in the next section, Proposition 8.2 asserts that

$$[\mathrm{Det}(\mathbf{r}_G(\varphi_s))](\chi) = (-1)^{\langle \chi, s \rangle_G}.$$

□

9. The Stickelberger pairing

Definition 9.1. The *Stickelberger pairing* is a $\mathbf{Q}$-bilinear pairing

$$\langle -, - \rangle_G : \mathbf{Q}R_G \times \mathbf{Q}G \to \mathbf{Q} \tag{9.1}$$

that is defined as follows.

Let $\zeta_{|G|}$ be a fixed, primitive $|G|$-th root of unity (cf. the conventions established at the beginning of Section 7), and suppose first that G is abelian. Then if $\chi \in \mathrm{Irr}(G)$ and $g \in G$, we may write $\chi(g) = \zeta_{|G|}^r$ for some integer r. We define

$$\langle \chi, g \rangle_G = \left\{ \frac{r}{|G|} \right\},$$

where $\{x\}$ denotes the fractional part of $x \in \mathbf{Q}$, and we extend this to a pairing on $\mathbf{Q}R_G \times \mathbf{Q}G$ via linearity. For arbitrary finite G, the Stickelberger pairing is defined via reduction to the abelian case by setting

$$\langle \chi, g \rangle_G = \langle \chi \mid_{\langle g \rangle}, g \rangle_{\langle g \rangle}.$$

It is easy to check that both definitions agree when G is abelian. □

We shall now explain a different way of expressing the Stickelberger pairing using the standard inner product on R_G. In order to do this, we must introduce some further notation.

For each $s \in G$, we set $m_s := |G|/|s|$. We define a character ξ_s of $\langle s \rangle$ by $\xi_s(s^i) = \zeta_{|G|}^{im_s}$; so ξ_s is a generator of the group of irreducible characters of $\langle s \rangle$. Then it follows from Definition

9.1 that

$$\langle \xi_s^\alpha, s^\beta \rangle_{\langle s \rangle} = \left\{ \frac{\alpha\beta}{|s|} \right\}.$$

Define

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

Proposition 9.2. *Let $(-,-)_G$ denote the standard inner product on R_G, and suppose that $\chi \in R_G$, $s \in G$. Then we have*

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

Proof. Suppose that

$$\chi \mid_{\langle s \rangle} = \sum_{j=0}^{|s|-1} a_j \xi_s^j,$$

where $a_j \in \mathbf{Z}$ for each j. Then we have

$$\begin{aligned} \langle \chi, s \rangle_G &= \sum_{j=0}^{|s|-1} a_j \langle \xi_s^j, s \rangle_{\langle s \rangle} \\ &= \sum_{j=0}^{|s|-1} a_j \left\{ \frac{j}{|s|} \right\} \\ &= \frac{1}{|s|} \sum_{j=0}^{|s|-1} a_j j. \end{aligned}$$

On the other hand, via Frobenius reciprocity, we have

$$\begin{aligned} (\chi, \mathrm{Ind}_{\langle s \rangle}^G(\Xi_s))_G &= (\chi \mid_{\langle s \rangle}, \Xi(s))_{\langle s \rangle} \\ &= \left(\sum_{j=0}^{|s|-1} a_j \xi_s^j, \frac{1}{|s|} \sum_{j=0}^{|s|-1} j\xi_s^j \right)_{\langle s \rangle} \\ &= \frac{1}{|s|} \sum_{j=0}^{|s|-1} a_j j \\ &= \langle \chi, s \rangle_G, \end{aligned}$$

and this establishes the desired result. □

In order to apply Poposition 9.2, we shall require the following result concerning traces of sums of roots of unity.

Lemma 9.3. *Let $n > 1$ be an integer, and suppose that ζ is any primitive n-th root of unity. Write*

$$y := \sum_{i=1}^{n-1} i \cdot \zeta^i.$$

Then

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(y) = -\frac{1}{2} n\phi(n),$$

where ϕ is the Euler ϕ-function. In particular, $\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(y) \neq 0$.

Proof. Each ζ^i is a primitive d-th root of unity for some divisor d of n, and so it follows that

$$y = \sum_{d|n} \sum_{\substack{1 \leq r \leq d-1 \\ (r,d)=1}} \frac{nr}{d} \zeta^{nr/d}.$$

If $d|n$, then applying Möbius inversion to the identity $x^d - 1 = \prod_{m|d} \Phi_m(x)$ (where $\Phi_m(x)$ denotes the m-th cyclotomic polynomial) yields $\Phi_m(x) = \prod_{m|d} (x^{m.} - 1)^{\mu(d/m)}$, whence it is not hard to show that $\mathrm{Tr}_{\mathbf{Q}(\varepsilon)/\mathbf{Q}}(\varepsilon) = \mu(d)$ for any primitive d-th root ε of unity. Hence $\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\varepsilon) = \phi(n)\mu(d)/\phi(d)$, and so we have

$$\begin{aligned} \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(y) &= \sum_{d|n} \sum_{\substack{1 \leq r \leq d-1 \\ (r,d)=1}} \frac{nr}{d} \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^{nr/d}) \\ &= n \sum_{d|n} \frac{\mu(d)}{d} \frac{\phi(n)}{\phi(d)} s(d), \end{aligned}$$

where

$$s(d) = \begin{cases} 1 & \text{if } d = 1; \\ \sum_{\substack{1 \leq i \leq d-1 \\ (i,d)=1}} i & \text{if } d > 1. \end{cases}$$

It is well known that

$$s(d) = \frac{1}{2} d\phi(d)$$

for any integer $d > 1$ (see e.g. [6, Theorem 7.7]). It therefore follows that

$$\begin{aligned} \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(y) &= \frac{1}{2} n\phi(n) \sum_{\substack{d|n \\ d>1}} \mu(d) \\ &= -\frac{1}{2} n\phi(n), \end{aligned}$$

as claimed. □

We can now state the following corollary to Proposition 9.2.

Corollary 9.4. *Suppose that s_1 and s_2 are elements of G.*

(i) If $c(s_1) = c(s_2)$, then $\langle \chi, s_1\rangle_G = \langle \chi, s_2\rangle_G$ for all $\chi \in \mathbf{Q}R_G$.

(ii) If $\langle \chi, s_1\rangle_G = \langle \chi, s_2\rangle_G$ for all $\chi \in \mathbf{Q}R_G$, then $\langle s_1\rangle$ is conjugate to $\langle s_2\rangle$ in G.

(iii) We have that $\langle \chi, s_1\rangle_G = 0$ for all $\chi \in \mathbf{Q}R_G$ if and only if $s_1 = e$.

Proof. (i) Let $\chi \in R_G$ and $s \in G$. It follows from the definition of the Stickelberger pairing that for fixed χ, the value of $\langle \chi, s\rangle_G$ depends only upon the conjugacy class $c(s)$ of s in G. Hence, if $c(s_1) = c(s_2)$, then $\langle \chi, s_1\rangle_G = \langle \chi, s_2\rangle_G$ for all $\chi \in \mathbf{Q}R_G$.

(ii) To show this we use Proposition 9.2. We first note that a straightforward computation shows that the degree of the virtual character $\mathrm{Ind}_{\langle s\rangle}^G(\Xi_s)$ is equal to $|G|(|s|-1)/2|s|$, and so we see that $\mathrm{Ind}_{\langle s\rangle}^G(\Xi_s)$ determines $|s|$. Next, we remark that If $\{t_i\}$ is a set of representatives of $G/\langle s\rangle$, then for each $g \in G$, we have

$$[\mathrm{Ind}_{\langle s\rangle}^G(\Xi_s)](g) = \sum_{t_i^{-1}gt_i \in \langle s\rangle} \xi_s(t_i^{-1}gt_i), \tag{9.2}$$

and so the character $\mathrm{Ind}_{\langle s\rangle}^G(\Xi_s)$ vanishes on all elements of G that are not conjugate to an element of $\langle s\rangle$.

Proposition 9.2 implies that under our hypotheses, $\mathrm{Ind}_{\langle s_1\rangle}^G(\Xi_{s_1}) = \mathrm{Ind}_{\langle s_2\rangle}^G(\Xi_{s_2})$. Hence, to prove the desired result, it suffices to show that $[\mathrm{Ind}_{\langle s_1\rangle}^G(\Xi_{s_1})](s_1) \neq 0$, because then

$$[\mathrm{Ind}_{\langle s_2\rangle}^G(\Xi_{s_1})](s_1) = [\mathrm{Ind}_{\langle s_1\rangle}^G(\Xi_{s_1})](s_1) \neq 0,$$

which implies (since $|s_1| = |s_2|$) that s_1 is conjugate to a generator of $\langle s_2\rangle$.

Now if s_1^a is any generator of $\langle s_1\rangle$, then $\xi_{s_1}(s_1^a)$ is a primitive $|s_1|$-th root of unity, and we have

$$\xi_{s_1}(s_1^a) = \sum_{i=1}^{|s_1|-1} i\xi_{s_1}(s_1^a)^i.$$

Hence if ζ denotes any primitive $|s_1|$-th root of unity, Lemma 9.3 implies that

$$\mathrm{Tr}_{\mathbf{Q}(\zeta)\mathbf{Q}}(\xi_{s_1}(s_1^a)) = -\frac{1}{2}|s_1|\phi(|s_1|).$$

It follows from (9.2) that $\mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}[\mathrm{Ind}_{s_1}^G(\Xi_{s_1})](s_1)$ is equal to a non-zero multiple of $-|s_1|\phi(|s_1|)/2$, and so is non-zero. This in turn implies that $[\mathrm{Ind}_{s_1}^G(\Xi_{s_1})](s_1)$ is also non-zero, thereby establishing the desired result.

(iii) Proposition 9.2 implies that $\langle \chi, s_1\rangle_G = 0$ for all $\chi \in \mathbf{Q}R_G$ if and only if $(\mathrm{Ind}_{\langle s_1\rangle}^G(\Xi_{s_1}), \chi)_G = 0$ for all $\chi \in \mathbf{Q}R_G$. The latter condition holds if and only if $\mathrm{Ind}_{\langle s_1\rangle}^G(\Xi_{s_1}) = 0$ and this happens if and only if $s_1 = e$. □

Remark 9.5. (a) The converse to Corollary 9.4(i) does not hold in general, e.g. it fails for the dihedral group D_{2p} of order $2p$, where $p > 3$ is a prime. (See [30, Chapter 3] or [31] for an explicit description of the Stickelberger pairing in this case.)

(b) Let $\chi_1, \ldots, \chi_d$ (respectively $c_1, \ldots, c_d$) be the set of irreducible characters (respectively conjugacy classes) of G. We refer the reader to [5] for computations and conjectures concerning the rank of the $d \times d$-matrix $[\langle \chi_i, c_j \rangle_G]$ associated to the Stickelberger pairing $\langle -, - \rangle_G$ when G is cyclic. □

10. The Stickelberger map and transpose homomorphisms

10.1. **The Stickelberger map.**

Definition 10.1. The *Stickelberger map*

$$\Theta = \Theta_G : \mathbf{Q}R_G \to \mathbf{Q}G \tag{10.1}$$

is defined by

$$\Theta(\chi) = \sum_{g \in G} \langle \chi, g \rangle_G \cdot g.$$

□

We write $G(-1)$ for the set G endowed with an action of Ω_F via the inverse cyclotomic character. Note that in general, for non-abelian G, this Ω_F-action is not an action on G via group automorphisms; it is only an action on the set G. However, it does induce an action on the additive group $\mathbf{Q}G(-1)$, which is all that we shall require.

The following proposition summarises some basic properties of the Stickelberger map.

Proposition 10.2. *(a) We have that $\Theta(\chi) \in Z(\mathbf{Q}G)$ for all $\chi \in R_G$, i.e. in fact*

$$\Theta : \mathbf{Q}R_G \to Z(\mathbf{Q}G).$$

(b) Suppose that $\chi \in R_G$. Then $\Theta(\chi) \in \mathbf{Z}G$ if and only if $\chi \in A_G$. Hence Θ induces a homomorphism $A_G \to \mathbf{Z}G$.

(c) The map

$$\Theta : \mathbf{Q}R_G \to \mathbf{Q}G(-1)$$

is Ω_F-equivariant.

Proof. The proofs of these assertions for arbitrary G are essentially the same as those in the case of abelian G. See [21, Propositions 4.3 and 4.5].

(a) It follows from the definition of the Stickelberger pairing that if $\chi \in R_G$ and $g \in G$, then $\langle \chi, g \rangle_G$ is determined by the conjugacy class $c(g)$ of g in G. This implies that $\Theta(R_G) \subseteq Z(\mathbf{Q}G)$, as claimed.

(b) Suppose that $\chi \in R_G$ and $g \in G$. Write

$$\chi \mid_{\langle g \rangle} = \sum_{\eta} a_\eta \eta,$$

where the sum is over irreducible characters of $\langle g \rangle$, and set $\zeta_{|g|} := \zeta_{|G|}^{|G|/|g|}$. Then

$$\begin{aligned}(\det(\chi))(g) &= \det(\chi \mid_{\langle g \rangle})(g) \\ &= \prod_{\eta} \eta(g)^{a_\eta} \\ &= \prod_{\eta} \zeta_{|g|}^{|g| \langle a_\eta \eta, g \rangle_{\langle g \rangle}} \\ &= \zeta_{|g|}^{|g| \sum_\eta \langle a_\eta \eta, g \rangle_{\langle g \rangle}} \\ &= \zeta_{|g|}^{|g| \langle \chi, g \rangle_G}.\end{aligned}$$

It now follows that $\langle \chi, g \rangle_G \in \mathbf{Z}$ for all $g \in G$ if and only if $\chi \in \mathrm{Ker}(\det) = A_G$, as required.

(c) Let κ denote the cyclotomic character of Ω_F, and suppose that $\chi \in R_G$ is of degree one. Then, for each $g \in G$ and $\omega \in \Omega_F$, we have

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

and so

$$\langle \chi^\omega, g \rangle_G = \langle \chi, g^{\kappa(\omega)} \rangle_G. \tag{10.2}$$

It follows via bilinearity that (10.2) holds for all $\chi \in R_G$ and all $g \in G$. Hence, if we view $\Theta(\chi)$ as being an element of $\mathbf{Q}G(-1)$, then

$$\begin{aligned}\Theta(\chi^\omega) &= \sum_{g \in G} \langle \chi^\omega, g \rangle_G \cdot g \\ &= \sum_{g \in G} \langle \chi, g^{\kappa(\omega)} \rangle_G \cdot g \\ &= \sum_{g \in G} \langle \chi, g \rangle_G \cdot g^{\kappa^{-1}(\omega)} \\ &= \Theta(\chi)^\omega.\end{aligned}$$

□

10.2. **Transpose Stickelberger homomorphisms.** We see from Proposition 10.2 that dualising the homomorphism

$$\Theta : A_G \to Z(\mathbf{Z}G)$$

and twisting by the inverse cyclotomic character yields an Ω_F-equivariant *transpose Stickelberger homomorphism*

$$\Theta^t : \mathrm{Hom}(Z(\mathbf{Z}G(-1)), (F^c)^\times) \to \mathrm{Hom}(A_G, (F^c)^\times). \tag{10.3}$$

Composing (10.3) with the sequence of homomorphisms

$$\mathrm{Hom}(A_G, (F^c)^\times) \xrightarrow{\sim} Z(F^cG)^\times/G^{ab} \to \frac{\mathrm{Det}(F^cG)^\times}{\mathrm{Det}(O_FG)^\times} \to K_0(O_FG, F^c), \tag{10.4}$$

(where the first arrow is given by (4.6), the second via (the inverse of) (4.3), and the third is via the homomorphism ∂^1 of (6.1)) yields a homomorphism

$$K\Theta^t : \mathrm{Hom}(Z(\mathbf{Z}G(-1)), (F^c)^\times) \to K_0(O_FG, F^c). \tag{10.5}$$

Hence, if we write $\mathcal{C}(G(-1))$ for the set of conjugacy classes of G endowed with Ω_F-action via the inverse cyclotomic character, and set

$$\begin{aligned}\Lambda(O_FG) := \mathrm{Hom}_{\Omega_F}(Z(\mathbf{Z}G(-1)), O_{F^c}) &= \mathrm{Map}_{\Omega_F}(\mathcal{C}(G(-1)), O_{F^c}) \\ &= Z(O_{F^c}[G(-1)])^{\Omega_F}; \\ \Lambda(FG) := \mathrm{Hom}_{\Omega_F}(Z(\mathbf{Z}G(-1)), F^c) &= \mathrm{Map}_{\Omega_F}(\mathcal{C}(G(-1)), F^c) \\ &= Z(F^c[G(-1)])^{\Omega_F},\end{aligned}$$

then $K\Theta^t$ induces a homomorphism (which we denote by the same symbol):

$$K\Theta^t : \Lambda(FG)^\times \to K_0(O_FG, F^c).$$

For each place v of F, we may apply the discussion above with F replaced by F_v to obtain local versions

$$\Theta_v^t : \mathrm{Hom}(Z(\mathbf{Z}G(-1)), (F_v^c)^\times) \to \mathrm{Hom}(A_G, (F_v^c)^\times) \tag{10.6}$$

and

$$K\Theta_v^t : \Lambda(F_vG)^\times \to K_0(O_{F_v}G, F_v^c) \tag{10.7}$$

of the maps Θ^t and $K\Theta^t$ respectively. The homomorphism Θ^t commutes with local completion, and $K\Theta^t$ commutes with the localisation maps

$$\lambda_v : K_0(O_FG, F^c) \to K_0(O_{F_v}G, F_v^c).$$

Definition 10.3. We define the group of ideles $J(\Lambda(FG))$ of $\Lambda(FG)$ to be the restricted direct product over all places v of F of the groups $\Lambda(F_vG)^\times$ with respect to the subgroups $\Lambda(O_{F_v}G)^\times$. □

For all finite places v of F not dividing the order of G, as $O_{F_v}G$ is an O_{F_v}-maximal order in F_vG, we have that (cf. Proposition 4.5(ii))

$$\Theta^t_v(\Lambda(O_{F_v}G)) \subseteq \mathrm{Hom}_{\Omega_{F_v}}(A_G, (O_{F^c_v})^\times) = \mathrm{Det}(\mathcal{H}(O_{F_v}G)),$$

and so

$$K\Theta^t_v(\Lambda(O_{F_v}G)) \subseteq K_0(O_{F_v}G, O_{F^c_v}).$$

It follows that the homomorphisms Θ^t_v combine to yield an idelic transpose Stickelberger homomorphism

$$K\Theta^t : J(\Lambda(FG)) \to J(K_0(O_FG, F^c)). \tag{10.8}$$

We shall see in the next subsection that the idelic homomorphism $K\Theta^t$ is closely related to the homomorphism

$$\Psi^{id} : J(H^1_t(F, G)) \to J(K_0(O_FG, F^c))$$

of Definition 6.2.

10.3. **Prime F-elements.**

Definition 10.4. Let v be a place of F. For each element $s \neq e$ of $\Sigma_v(G)$ (see Definition 7.2 and (8.1)), define $f_{v,s} \in \Lambda(F_vG)^\times$ by

$$f_{v,s}(c) = \begin{cases} -1 & \text{if } v \text{ is real and } c = c(s); \\ \varpi_v, & \text{if } v \text{ is finite and } c = c(s); \\ 1, & \text{otherwise.} \end{cases} \tag{10.9}$$

Observe that $f_{v,s}$ is Ω_{F_v}-equivariant because $s \in \Sigma_v(G)$ and so Ω_{F_v} fixes $c(s)$ when s is viewed as an element of $G(-1)$. The element $f_{v,s}$ depends only upon the conjugacy class $c(s)$ of s. For all places v of F, we define $f_{v,e} \in (\Lambda(F_vG))^\times$ to be the constant function $f_{v,e} = 1$.

Write

$$\mathbf{F}_v := \{f_{v,s} \mid s \in \Sigma_v(G)\},$$

and define the subset $\mathbf{F} \subset J(\Lambda(FG))$ of prime $\mathbf{F}$-elements by

$$f \in \mathbf{F} \iff f \in J(\Lambda(FG)) \text{ and } f_v \in \mathbf{F}_v \text{ for all places } v \text{ of } F.$$

Following [7, Definition 7.1], we define the *support* $\mathrm{Supp}(f)$ of $f \in \mathbf{F}$ to be set of all places v of F for which $f_v \neq 1$. We say that f is *full* if, for each $s \in G$ there is a place v with $f_v = f_{v,s}$. □

Our interest in the set $\mathbf{F}$, as well as the relationship between $K\Theta^t$ and Ψ^{id}, is explained by the following result.

Proposition 10.5. *Let v be a place of F.*

(a) For each $s \in \Sigma_v(G)$, we have

$$\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s})) = K\Theta^t_v(f_{v,s})$$

in $K_0(O_{F_v}G, F_v^c)$.

(b) Suppose that $s_1, s_2 \in \Sigma_v(G)$ with

$$\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s_1})) = \mathrm{Det}(\mathbf{r}_G(\varphi_{v,s_2})). \tag{10.10}$$

Then $\langle s_1\rangle$ is conjugate in G to $\langle s_2\rangle$.

(c) Suppose that v is finite. Let $\pi_1, \pi_2 \in \mathrm{Hom}(\Omega_{F_v}, G)$ with $[\pi_i] \in H^1_t(F_v, G)$ for each i, and set $s_i = \pi_i(\sigma_v)$ (cf. (7.5)). Let a_i be a normal integral basis generator of $F_{v,\pi_i}/F_v$, and let

$$\mathbf{r}_G(a_i) = u_i \cdot \mathbf{r}_G(a_{i,nr}) \cdot \mathbf{r}_G(\varphi_{s_i})$$

be a Stickelberger factorisation of $\mathbf{r}_G(a_i)$ (see Definition 7.12). Suppose that

$$\mathrm{Det}(\mathbf{r}_G(a_1)) \cdot \mathrm{Det}(\mathbf{r}_G(a_2))^{-1} \in \mathrm{Det}((O_{F_v^c}G)^\times). \tag{10.11}$$

Then

$$\mathrm{Det}(\mathbf{r}_G(\varphi_{s_1})) = \mathrm{Det}(\mathbf{r}_G(\varphi_{s_2}))$$

and for some integer m and some $h \in G$, the equality

$$\pi_1(\omega) = h \cdot \pi_2(\omega)^m \cdot h^{-1}$$

holds for all $\omega \in I_v$.

Proof. (a) The proof of this assertion is very similar to that of [21, Proposition 5.4].

It suffices to show that the equality

$$\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s})) = \Theta^t_v(f_{v,s})$$

holds in $\mathrm{Hom}(A_G, (F_v^c)^\times)$.

Let $\chi \in R_G$, and write

$$\chi\,|_{<s>} = \sum_{\eta} a_\eta \eta,$$

where the sum is over irreducible characters η of $\langle s \rangle$.

Suppose first that v is finite. Using (7.2), we see that (cf. [21, Proposition 5.4])

$$\begin{aligned}[\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s}))](\chi) &= \prod_{\eta} \left(\sum_{i=0}^{|s|-1} \sigma_v^i(\beta_s)\eta(s^{-i}) \right)^{a_\eta} \\ &= \varpi_v^{\langle \sum_\eta a_\eta \eta, s\rangle_{\langle s\rangle}} \\ &= \varpi_v^{\langle \chi, s\rangle_G}, \end{aligned} \tag{10.12}$$

and so it follows that

$$[\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s}))](\alpha) = \varpi_v^{\langle \alpha, s\rangle_G}$$

for all $\alpha \in A_G$.

If v is real, then then the proof of Proposition 8.2 shows directly that

$$[\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s}))](\chi) = (-1)^{\langle \chi, s\rangle_G},$$

and so we have

$$[\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s}))](\alpha) = (-1)^{\langle \alpha, s\rangle_G}$$

for all $\alpha \in A_G$ in this case also.

Now suppose that v is either finite or real. If $\alpha \in A_G$, then we have

$$\begin{aligned}(\Theta_v^t(f_{v,s}))(\alpha) &= f_{v,s}(\Theta(\alpha)) \\ &= f_{v,s}\left(\sum_{g\in G} \langle \alpha, g\rangle_G \cdot g \right) \\ &= \prod_{g\in G} f_{v,s}(g)^{\langle \alpha, g\rangle_G} \\ &= \begin{cases} \varpi_v^{\langle \alpha, s\rangle_G}, & \text{if } v \text{ is finite;} \\ (-1)^{\langle \alpha, s\rangle_G}, & \text{if } v \text{ is real.} \end{cases} \end{aligned}$$

The desired result now follows.

(b) The proof of (a) above shows that if (10.10) holds, then

$$\langle \chi, s_1\rangle_G = \langle \chi, s_2\rangle_G$$

for every $\chi \in R_G$. It therefore follows from Corollary 9.4 that $\langle s_1 \rangle$ is conjugate in G to $\langle s_2 \rangle$.

(c) Observe that (10.11) holds if and only if

$$\mathrm{Det}(\mathbf{r}_G(\varphi_{s_1})) \cdot \mathrm{Det}(\mathbf{r}_G(\varphi_{s_2})^{-1}) \in \mathrm{Det}((O_{F_v^c}G)^\times), \tag{10.13}$$

and the proof of part (a) (see (10.12)) implies that (10.13) holds if and only if

$$\mathrm{Det}(\mathbf{r}_G(\varphi_{s_1})) = \mathrm{Det}(\mathbf{r}_G(\varphi_{s_2})).$$

Part (b) therefore implies that $\langle s_1 \rangle$ and $\langle s_2 \rangle$ are conjugate. Hence

$$s_1 = h \cdot s_2^m \cdot h^{-1}$$

for some $m \in \mathbf{Z}$ and $h \in G$, and so

$$\mathbf{r}_G(\varphi_{s_1}) = h \cdot \mathbf{r}_G(\varphi_{s_2^m}) \cdot h^{-1}$$

(see (7.3)).

For any $\omega \in \Omega_{F_v^{nr}}$, we have

$$\pi_i(\omega) = \mathbf{r}_G(a_i)^{-1} \cdot \mathbf{r}_G(a_i)^\omega = \mathbf{r}_G(\varphi_{s_i})^{-1} \cdot \mathbf{r}_G(\varphi_{s_i})^\omega.$$

Applying the map $F_v^cG \to F_v^cG$ defined by $\sum_g a_g g \mapsto \sum_g a_g g^m$ to this equality (when $i = 2$) yields

$$\pi_2(\omega)^m = \mathbf{r}_G(\varphi_{s_2^m})^{-1} \cdot \mathbf{r}_G(\varphi_{s_2^m})^\omega.$$

The final assertion now follows. □

10.4. **The Stickelberger pairing revisited.** In this subsection we shall briefly describe an alternative definition of the Stickelberger pairing that involves a direct connection with resolvends of local normal integral basis generators. This will not be used in the sequel.

Let v be a finite place of F. There is a natural pairing

$$\{-,-\}_{G,v} : \mathrm{Irr}(G) \times H^1(F_v^{nr}, G) \to \mathbf{Q}/\mathbf{Z}; \quad (\chi, [\pi]) \mapsto [v(\mathrm{Det}(\mathbf{r}_G(a(\pi)))(\chi))], \tag{10.14}$$

where $a(\pi)$ is any normal basis generator of $F_{v,\pi}^{nr}/F_v^{nr}$. Recall that every element of $H_t^1(F_v^{nr}, G)$ is of the form $\tilde{\varphi}_{v,s}$ for some $s \in G$ with $v \nmid |s|$ (see Remark 7.11). The restriction of $\{-,-\}_{G,v}$ to $\mathrm{Irr}(G) \times H_t^1(F_v^{nr}, G)$ yields a refined pairing

$$\{-,-\}_{G,v}^{(1)} : \mathrm{Irr}(G) \times H_t^1(F_v^{nr}, G) \to \mathbf{Q}; \quad (\chi, \tilde{\varphi}_{v,s}) \mapsto v(\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s}))(\chi)). \tag{10.15}$$

This leads to the following definition.

Definition 10.6. Suppose that v is finite and that $v \nmid |G|$. We define a pairing

$$[-,-]_{G,v} : \mathrm{Irr}(G) \times G \to \mathbf{Q}; \quad (\chi, g) \mapsto v(\mathrm{Det}(\mathbf{r}_G(\varphi_{v,g}))(\chi)), \tag{10.16}$$

and we extend this to a pairing on $\mathbf{Q}R_G \times \mathbf{Q}G$ via linearity. □

Proposition 10.7. *Suppose that v is finite and that $v \nmid |G|$. Then for each $\chi \in \mathrm{Irr}(G)$ and $g \in G$, we have*

$$[\chi, g]_{G,v} = [\chi\,|_{\langle g\rangle}, g]_{\langle g\rangle, v}. \tag{10.17}$$

Proof. Set $H := \langle g\rangle$. The property (10.17) is a direct consequence of the fact that the restriction map $R_G \to R_H$ induces a homomorphism $\mathrm{Hom}(R_H, (F_v^c)^\times) \to \mathrm{Hom}(R_G, (F_v^c)^\times)$ such that the following diagram commutes:

$$\begin{array}{ccc} (F_v^c H)^\times & \xrightarrow{\subseteq} & (F_v^c G)^\times \\ \big\downarrow \mathrm{Det} & & \big\downarrow \mathrm{Det} \\ \mathrm{Hom}(R_H, (F_v^c)^\times) & \longrightarrow & \mathrm{Hom}(R_G, (F_v^c)^\times) \end{array}$$

(see e.g. [15, p. 436] or [17, p. 118]). □

Proposition 10.8. *Suppose that v is finite and that $v \nmid |G|$. Then for each $\chi \in \mathrm{Irr}(G)$ and $g \in G$, we have*

$$[\chi, g]_{G,v} = \langle \chi, g\rangle_G. \tag{10.18}$$

In particular, $[-,-]_{G,v}$ is independent of our choice of v.

Proof. Proposition 10.7 implies that we may assume that G is cyclic. The equality (10.18) may then be established via an argument identical to that used in the proof of Proposition 10.5(a) (see also [21, Proposition 5.4]). □

11. Modified ray class groups

Definition 11.1. Let $\mathfrak{a}$ be an integral ideal of O_F. For each finite place v of F, recall that

$$U_{\mathfrak{a}}(O_{F_v^c}) := (1 + \mathfrak{a} O_{F_v^c}) \cap (O_{F_v^c})^\times.$$

We define

$$U'_{\mathfrak{a}}(\Lambda(O_{F_v} G)) \subseteq \Lambda(F_v G)^\times = \mathrm{Map}_{\Omega_{F_v}}(\mathcal{C}(G(-1)), (F_v^c)^\times)$$

by

$$U'_{\mathfrak{a}}(\Lambda(O_{F_v} G)) := \left\{ g_v \in \Lambda(F_v G)^\times \mid g_v(c) \in U_{\mathfrak{a}}(O_{F_v^c}) \quad \forall c \neq 1 \right\}$$

(with $g_v(1)$ allowed to be arbitrary).

Set

$$U'_{\mathfrak{a}}(\Lambda(O_F G)) := \left(\prod_v U'_{\mathfrak{a}}(\Lambda(O_{F_v} G)) \right) \cap J(\Lambda(FG)).$$

□

Definition 11.2. For each real place v of F, we define

$$\Lambda(F_vG)^\times_+ := \{g_v \in \Lambda(F_vG)^\times \mid g_v(c) \in \mathbf{R}^\times_{>0} \text{ for all } c \in \mathcal{C}(G(-1))\}$$

(with $g_v(1)$ allowed to be arbitrary).

If v is complex, we set $\Lambda(F_vG)^\times_+ := \Lambda(F_vG)^\times$. We define

$$U'_\infty(\Lambda(O_FG)) := \left(\prod_{v|\infty} \Lambda(FG)^\times\right) \cap J(\Lambda(FG)),$$

and

$$U'_\infty(\Lambda(O_FG))_+ := \left(\prod_{v|\infty} \Lambda(FG)^\times_+\right) \cap J(\Lambda(FG)).$$

□

Definition 11.3. The *modified ray class group modulo* $\mathfrak{a}$ of $\Lambda(O_FG)$ is defined by

$$\mathrm{Cl}'_\mathfrak{a}(\Lambda(O_FG)) := \frac{J(\Lambda(FG))}{\Lambda(FG)^\times \cdot U'_\mathfrak{a}(\Lambda(O_FG)) \cdot U'_\infty(\Lambda(O_FG))}.$$

The *modified narrow ray class group modulo* $\mathfrak{a}$ is defined by

$$\mathrm{Cl}'^{+}_\mathfrak{a}(\Lambda(O_FG)) := \frac{J(\Lambda(FG))}{\Lambda(FG)^\times \cdot U'_\mathfrak{a}(\Lambda(O_FG)) \cdot U'_\infty(\Lambda(O_FG))_+}.$$

We refer to the elements of $\mathrm{Cl}'_\mathfrak{a}(\Lambda(O_FG))$ (respectively $\mathrm{Cl}'^{+}_\mathfrak{a}(\Lambda(O_FG))$) as the *modified ray classes* (respectively *modified narrow ray classes*) of $\Lambda(O_FG)$ modulo $\mathfrak{a}$. □

Remark 11.4. Fix a set of representatives T of $\Omega_F \backslash \mathcal{C}(G(-1))$, and for each $t \in T$, let $F(t)$ be the smallest extension of F such that $\Omega_{F(t)}$ fixes t. Then the Wedderburn decomposition of $\Lambda(FG)$ is given by

$$\Lambda(FG) = \mathrm{Map}_{\Omega_F}(\mathcal{C}(G(-1)), F^c) \simeq \prod_{t \in T} F(t), \tag{11.1}$$

where the isomorphism is induced by evaluation on the elements of T.

The group $\mathrm{Cl}'_\mathfrak{a}(\Lambda(O_FG))$ (respectively $\mathrm{Cl}'^{+}_\mathfrak{a}(\Lambda(O_FG))$) above is finite, and is isomorphic to the product of the ray class groups $\mathrm{Cl}_\mathfrak{a}(O_{F(t)})$ (respectively the narrow ray class groups $\mathrm{Cl}^{+}_\mathfrak{a}(O_{F(t)})$) modulo $\mathfrak{a}$ of the Wedderburn components $F(t)$ of $\Lambda(FG)$ with $t \neq 1$. There is a natural surjection

$$\mathrm{Cl}'^{+}_\mathfrak{a}(\Lambda(O_FG)) \to \mathrm{Cl}'_\mathfrak{a}(\Lambda(O_FG))$$

with kernel an elementary abelian 2-group.

If $|G|$ is odd, then (as no non-trivial element of G is conjugate to its inverse), $F(t)$ has no real places when $t \neq 1$, and so $\mathrm{Cl}_{\mathfrak{a}}(O_{F(t)}) = \mathrm{Cl}^{+}_{\mathfrak{a}}(O_{F(t)})$. Hence we have

$$\mathrm{Cl}'^{+}_{\mathfrak{a}}(\Lambda(O_F G)) = \mathrm{Cl}_{\mathfrak{a}}(\Lambda(O_F G))$$

whenever G is of odd order. □

Proposition 11.5. *Let $\mathfrak{a}$ be any integral ideal of O_F. Then the inclusion $\mathbf{F} \to J(\Lambda(FG))$ induces a surjection $\mathbf{F} \to \mathrm{Cl}'^{+}_{\mathfrak{a}}(\Lambda(O_F G))$. In particular, each modified narrow ray class modulo $\mathfrak{a}$ of $\Lambda(O_F G)$ contains infinitely many elements of $\mathbf{F}$.*

Proof. Let $I(\Lambda(O_F G))$ denote the group of fractional ideals of $\Lambda(O_F G)$. Then via the Wedderburn decomposition (11.1) of $\Lambda(FG)$, we see that each fractional ideal $\mathfrak{B}$ in $\Lambda(O_F G)$ may be written in the form $\mathfrak{B} = (\mathfrak{B}_t)_{t \in T}$, where each $\mathfrak{B}_t$ is a fractional ideal of $O_{F(t)}$. For each conjugacy class $t \in T$, let $o(t)$ denote the Ω_F-orbit of t in $\mathcal{C}(G(-1))$, and write $|t|$ for the order of any element of t.

For each idele $\nu \in J(\Lambda(FG))$, let

$$\mathrm{co}(\nu) := [\mathrm{co}(\nu)_t]_{t \in T} \in I(\Lambda(O_F G)) \simeq \prod_{t \in T} I(O_{F(t)})$$

denote the ideal obtained by taking the idele content of ν. If v is a place of F, we view $\mathbf{F}_v$ as being a subset of $\mathbf{F}$ via the obvious embedding $\Lambda(F_v G)^{\times} \subseteq J(\Lambda(FG))$, and we set

$$\mathcal{F}_v := \{\mathrm{co}(f_v) \mid f_v \in \mathbf{F}_v\}.$$

Now suppose that v is finite, and consider the ideal

$$\mathrm{co}(f_{v,s}) = [\mathrm{co}(f_{v,s})_t]_{t \in T}$$

in $I(\Lambda(O_F G))$. If $c(s) \notin o(t)$, then it follows from the definition of $f_{v,s}$ that $\mathrm{co}(f_{v,s})_t = O_{F(t)}$. Suppose that $c(s) \in o(t)$. Since $s \in \Sigma_v(G)$, it follows that $v(|s|) = 0$ and that Ω_{F_v} fixes $c(s)$. Hence $F_v(t) = F_v$, and so we see that $\mathrm{co}(f_{v,s})_t$ is a prime ideal of $O_{F(t)}$ of degree one lying above v (cf. [21, pages 287–289]). Furthermore, if $t \in T$ and if v is a finite place of F that is totally split in $F(t)$, then $f_{v,s} \in \mathbf{F}_v$ for all $c(s) \in o(t)$.

We therefore deduce that if v is finite, the set $\mathcal{F}_v$ consists precisely of the invertible prime ideals $\mathfrak{p} = (\mathfrak{p}_t)_{t \in T}$ of $\Lambda(O_F G)$ with $\mathfrak{p}_{t_1}$ a prime of degree one above v in $F(t_1)$ for some $t_1 \in T$ with $v(|t_1|) = 0$ and $\mathfrak{p}_t = O_{F(t)}$ for all $t \neq t_1$. For every $t \in T$, the narrow ray class modulo $\mathfrak{a}$ of $F(t)$ contains infinitely many primes of degree one, and this implies that $\mathbf{F}$ surjects onto $\mathrm{Cl}'^{+}_{\mathfrak{a}}(\Lambda(O_F G))$ as claimed. □

Our next result describes a transpose Stickelberger homomorphism on modified narrow ray class groups $\mathrm{Cl}'^{+}_{\mathfrak{a}}(\Lambda(O_F G))$ for a suitable choice of $\mathfrak{a}$. Before stating it, we remind the reader that Proposition 6.3 implies that $\prod_v \mathrm{Im}(\Psi_v^{nr})$ is a subgroup of $J(K_0(O_F G, F^c))$.

Proposition 11.6. *Let N be an integer, and set $\mathfrak{a} := N \cdot O_F$. Then if N is divisible by a sufficiently high power of $|G|$, the idelic transpose Stickelberger homomorphism*

$$K\Theta^t : J(\Lambda(FG)) \to J(K_0(O_F G, F^c))$$

induces a homomorphism

$$\Theta^t_{\mathfrak{a}} : \mathrm{Cl}'^{+}_{\mathfrak{a}}(\Lambda(O_F G)) \to \frac{J(K_0(O_F G, F^c))}{\lambda[\partial^1(K_1(F^c G))] \cdot \prod_v \mathrm{Im}(\Psi_v^{nr})}.$$

Proof. To show this, we first observe that Proposition 4.6 implies that if N is divisible by a sufficiently high power of $|G|$ and v is any finite place of F, then we have

$$\Theta^t_v(U'_{\mathfrak{a}}(\Lambda(O_{F_v} G))) \subseteq \mathrm{Det}((O_{F_v} G)^\times / G) \subseteq \mathrm{Det}(\mathcal{H}(O_{F_v} G)) = \mathrm{Im}(\Psi_v^{nr}),$$

and so it follows that

$$K\Theta^t(U'_{\mathfrak{a}}(\Lambda(O_F G))) \subseteq \prod_v \mathrm{Im}(\Psi_v^{nr})$$

in $J(K_0(O_F G, F^c))$.

Suppose that v is a real place of F and that $h \in \Lambda(F_v G)^\times_+$. Then for each $\chi \in R_G$, we have (recalling that $\langle \chi, e \rangle_G = 0$)

$$\Theta^t_v(h)(\chi) = \prod_{g \in G} h(c(g))^{\langle \chi, g \rangle_G} > 0,$$

and so $\Theta^t_v(h) \in \mathrm{Hom}^+_{\Omega_{F_v}}(R_G, (F_v^c)^\times)$. This implies that $K\Theta^t(h) = 1$ in $K_0(O_{F_v} G, F_v^c)$. Hence $K\Theta^t(U'_\infty(\Lambda(O_F G))) = 1$ in $J(K_0(O_F G, F^c))$.

It now follows that $K\Theta^t$ induces a homomorphism

$$\Theta^t_{\mathfrak{a}} : \mathrm{Cl}'^{+}_{\mathfrak{a}}(\Lambda(O_F G)) \to \frac{J(K_0(O_F G, F^c))}{\lambda[\partial^1(K_1(F^c G))] \cdot \prod_v \mathrm{Im}(\Psi_v^{nr})},$$

as claimed. □

12. Proof of Theorem 6.6

In this section we shall prove Theorem 6.6. Recall that we wish to show that if

$$\overline{\Psi^{id}} : J(H^1_t(F, G)) \to \frac{J(K_0(O_F G, F^c))}{\lambda[\partial^1(K_1(F^c G))] \cdot \prod_v \mathrm{Im}(\Psi_v^{nr})}$$

denotes the map of pointed sets given by the composition of the map Ψ^{id} with the quotient homomorphism

$$q_1 : J(K_0(O_F G, F^c)) \to \frac{J(K_0(O_F G, F^c))}{\lambda[\partial^1(K_1(F^c G))] \cdot \prod_v \mathrm{Im}(\Psi_v^{nr})},$$

then the image of $\overline{\Psi^{id}}$ is in fact a group.

To show this, we choose an ideal $\mathfrak{a} = N \cdot O_F$ as in Proposition 11.6, and we consider the following diagram:

$$\begin{array}{ccccc} & & & & J(H_t^1(F,G)) \\ & & & & \Big\downarrow{\scriptstyle \Psi^{id}} \\ \mathbf{F} & \xrightarrow{\subset} & J(\Lambda(FG)) & \xrightarrow{K\Theta^t} & J(K_0(O_F G, F^c)) \\ \Big\downarrow{\scriptstyle q_2} & & \Big\downarrow{\scriptstyle q_2} & & \Big\downarrow{\scriptstyle q_1} \\ \mathrm{Cl}'_{\mathfrak{a}}{}^{+}(\Lambda(O_F G)) & = & \mathrm{Cl}'_{\mathfrak{a}}{}^{+}(\Lambda(O_F G)) & \xrightarrow{\Theta^t_{\mathfrak{a}}} & \dfrac{J(K_0(O_F G, F^c))}{\lambda[\partial^1(K_1(F^c G))] \cdot \prod_v \mathrm{Im}(\Psi_v^{nr})} \end{array} \tag{12.1}$$

Here q_2 denotes the obvious quotient map. Proposition 11.6 shows that the right-hand square commutes, and Proposition 11.5 shows that the left-most vertical arrow is surjective.

It follows from Proposition 10.5(a) that

$$\begin{aligned} q_1[K\Theta^t(\mathbf{F})] &= q_1[\Psi^{id}(J(H_t^1(F,G)))] \\ &= \mathrm{Im}\,\overline{\Psi^{id}}. \end{aligned}$$

On the other hand, we also have that

$$q_1[K\Theta^t(\mathbf{F})] = \Theta^t_{\mathfrak{a}}(\mathrm{Cl}'_{\mathfrak{a}}{}^{+}(\Lambda(O_F G))),$$

which is a group. It therefore follows that $\mathrm{Im}(\overline{\Psi^{id}})$ is indeed a group, as claimed.

This completes the proof of Theorem 6.6. □

13. Realisable classes from field extensions

In this section, after first proving that the kernel of Ψ is finite, we explain how a slightly weaker form of Conjecture B implies that every element of $\mathcal{R}(O_F G)$ may be realised by the ring of integers of a tame field (as opposed to merely a Galois algebra) G-extension of F.

Recall that G' denotes the derived subgroup of G, and note that we may view $H^1(F, G')$ and $H^1(F_v, G')$ as being pointed subsets of $H^1(F, G)$ and $H^1(F_v, G)$ respectively via taking Galois cohomology of the exact sequence of groups

$$0 \to G' \to G \to G^{ab} \to 0.$$

Recall also that we write $H^1_{fnr}(F,G')$ for the set of isomorphism classes of G'-Galois F-algebras that are unramified at all finite places of F.

Proposition 13.1. *(a) Let v be a finite place of F. Then* $\mathrm{Ker}(\Psi_v) \subseteq H^1_{nr}(F_v,G')$.

(b) Suppose that $[\pi] \in \mathrm{Ker}(\Psi)$. *Then* $[\pi] \in H^1_{fnr}(F,G') \subseteq H^1(F,G)$. *We have that* $\mathrm{Ker}(\Psi)$ *is finite.*

(c) Suppose that $F/\mathbf{Q}$ is at most tamely ramified at all primes dividing $|G|$. Then $H^1_{nr}(F,G') \subseteq \mathrm{Ker}(\Psi)$.

(d) Suppose that G has no irreducible symplectic characters or that F has no real places. Suppose also that $F/\mathbf{Q}$ is at most tamely ramified at all primes dividing $|G|$. Then $\mathrm{Ker}(\Psi) = H^1_{fnr}(F,G')$.

Proof. (a) Let v be a finite place of F. Suppose that $[\pi_v] \in H^1_t(F_v,G)$, and that $O_{\pi_v} = O_{F_v}G \cdot a_v$. Recall (see Sections 5 and 6) that we have

$$\Psi_v : H^1_t(F_v,G) \to K_0(O_{F_v}G, F_v^c) \simeq \frac{\mathrm{Det}(F_v^cG)^\times}{\mathrm{Det}(O_{F_v}G)^\times},$$

and that $\Psi_v([\pi_v]) = [\mathrm{Det}(\mathbf{r}_G(a_v))]$ (see also Definition 4.1 and Remark 4.2). It follows that $\Psi_v([\pi_v]) = 0$ if and only if $\mathrm{Det}(\mathbf{r}_G(a_v)) \in \mathrm{Det}(O_{F_v}G)^\times$.

Hence, if $\Psi_v([\pi_v]) = 0$, then for each $\omega \in \Omega_{F_v}$, we have

$$\mathrm{Det}(\mathbf{r}_G(a_v)^{-1}) \cdot \mathrm{Det}(\mathbf{r}_G(a_v))^\omega = 1,$$

and so we deduce from (3.8) that $[\pi_v]$ lies in the kernel of the natural map $H^1(F_v,G) \to H^1(F_v,G^{ab})$ of pointed sets. This implies that $[\pi_v] \in H^1(F_v,G')$. Finally, we see from (7.11) and Proposition 10.5(c) that $\mathrm{Det}(\mathbf{r}_G(a_v)) \in \mathrm{Det}((O_{F_v}G)^\times)$ only if $[\pi_v] \in H^1_{nr}(F_v,G)$. We now conclude that if $[\pi_v] \in \mathrm{Ker}(\Psi_v)$, then $[\pi_v] \in H^1_{nr}(F_v,G')$. This establishes part (a).

(b) Suppose that $[\pi] \in H^1(F,G)$ satisfies $\Psi([\pi]) = 0$. Then $\Psi_v(\mathrm{loc}_v([\pi])) = 0$ for each place v, and so it follows from part (a) that $\mathrm{loc}_v([\pi]) \in H^1_{nr}(F_v,G')$ for all finite places v of F. Therefore $[\pi] \in H^1(F,G')$, and π is unramified at each finite place of F, i.e. $[\pi] \in H^1_{fnr}(F,G')$. As there are only finitely many unramified extensions of F of bounded degree, it follows that $H^1_{fnr}(F,G')$ is finite, and so $\mathrm{Ker}(\Psi)$ is finite, as claimed.

(c) Suppose that $[\pi] \in H^1_{nr}(F,G') \subseteq H^1_t(F,G)$, and write $O_{\pi_v} = O_{F_v}G \cdot a_v$ for each finite place v of F. As π is unramified at v, it follows that $\mathrm{Det}(\mathbf{r}_G(a_v)) \in \mathrm{Det}(O_{F_v^{nr}}G)^\times$. Since $\mathrm{loc}_v([\pi])$ lies in the kernel of the natural map $H^1(F_v,G) \to H^1(F_v,G^{ab})$, we see from the diagram (3.8) that the image of $\mathrm{Det}(\mathbf{r}_G(a_v))$ in $Z(F_vG)^\times \backslash \mathcal{H}(Z(F_vG))$ is trivial, and so in fact $\mathrm{Det}(\mathbf{r}_G(a_v)) \in [\mathrm{Det}(O_{F_v^{nr}}G)^\times]^{\Omega_{F_v}}$. Note that $\mathrm{Det}(\mathbf{r}_G(a_v))$ is defined over the finite, unramified extension $F_v^{\pi_v}$ of F_v (see (2.2)). Let L denote an arbitrary finite, unramified extension of F_v.

If $v \nmid |G|$, then $O_L G$ is an O_L-maximal order in LG, and we have (see (4.12))

$$\begin{aligned}[\mathrm{Det}(O_L G)^\times]^{\Omega_{F_v}} &\simeq [\mathrm{Hom}_{\Omega_L}(R_G, (O_{F_v^c})^\times)]^{\Omega_{F_v}} \\ &\simeq \mathrm{Hom}_{\Omega_{F_v}}(R_G, (O_{F_v^c})^\times) \\ &\simeq \mathrm{Det}(O_{F_v} G)^\times.\end{aligned}$$

If $v \mid |G|$, then because $F/\mathbf{Q}$ is at most tamely ramified at all primes dividing $|G|$, it follows from M. J. Taylor's fixed point theorem for group determinants (see e.g. [34, Chapter VIII]) that

$$[\mathrm{Det}(O_L G)^\times]^{\Omega_{F_v}} = \mathrm{Det}(O_{F_v} G)^\times.$$

Hence, for each finite place v of F, we see that $\mathrm{Det}(\mathbf{r}_G(a_v)) \in \mathrm{Det}(O_{F_v} G)^\times$, and so $\Psi_v([\pi_v]) = 0$ (cf. part (a) above).

Since $H^1_{nr}(F_v, G) = 0$ for all infinite places of F, it follows that $\Psi_v([\pi_v]) = 0$ for all places v of F. This in turn implies that $\lambda(\Psi([\pi])) = 0$. As the localisation map λ is injective (see Proposition 5.9(a)), it follows that $\Psi([\pi]) = 0$. Hence $H^1_{nr}(F, G') \subseteq \mathrm{Ker}(\Psi)$, as claimed.

(d) The proof of this assertion is very similar to that of part (c) above, and so here we shall be brief. Suppose that $[\pi] \in H^1_{fnr}(F, G')$. Arguing exactly as in part (c), we see that $\Psi_v([\pi]_v) = 0$ for all finite places v of F, which in turn implies that $\lambda_f(\Psi([\pi])) = 0$. Under our hypotheses, Proposition 5.9(b) implies that the localisation map λ_f is injective, and so $\Psi([\pi]) = 0$. Hence we see that $H^1_{fnr}(F, G') \subseteq \mathrm{Ker}(\Psi)$, and so it follows from part (b) above that in fact $H^1_{fnr}(F, G') = \mathrm{Ker}(\Psi)$, as asserted. □

Definition 13.2. Suppose that $x \in \mathrm{LC}(O_F G)$ (see Definition 6.4). We say that x is *unramified* (respectively *ramified*) at a place v of F if $\lambda_v(x) \in \mathrm{Im}(H^1_{nr}(F_v, G))$ (respectively if $\lambda_v(x) \notin \mathrm{Im}(H^1_{nr}(F_v, G))$).

If S is any finite set of places of F, we denote the set of $x \in \mathrm{LC}(O_F G)$ that are unramified at all places in S by $\mathrm{LC}(O_F G)_S$. □

Before stating our next result, it will be helpful to introduce the following notation. Suppose that $x \in \mathrm{LC}(O_F G)$ and let $[(x_v)_v, x_\infty] \in J(K_1(FG)) \times \mathrm{Det}(F^c G)^\times$ be a representative of x. Then $\lambda(x) \in J(K_0(O_F G, F^c))$ is represented by the element $(x_v \cdot \mathrm{loc}_v(x_\infty)) \in \prod_v \mathrm{Det}(F_v^c G)^\times$. Hence it follows from Theorem 7.9 and Proposition 10.5(a) that we have an equality

$$[(x_v \cdot \mathrm{loc}_v(x_\infty))] = [a(x)] \cdot K\Theta^t(f(x)) \tag{13.1}$$

in $J(K_0(O_F G, F^c))$, where $a(x) = (a(x)_v) \in \prod_v \mathrm{Det}(\mathcal{H}(O_{F_v} G))$ and $f(x) \in \mathbf{F}$.

Definition 13.3. We say that $x \in \mathrm{LC}(O_F G)$ is *fully ramified* if $f(x)$ is full (see Definition 10.4—note in particular that this does *not* mean that x is ramified at all places of F, which would of course be absurd!). □

Let us also recall that $\partial^0(x) \in \mathrm{Cl}(O_F G)$ is represented by the idele $(x_v)_v \in J(K_1(FG))$ (see Remark 5.5).

Proposition 13.4. *Suppose that S is any finite set of places of F, and that $x \in \mathrm{LC}(O_F G)$. Then there exist infinitely many $y \in \mathrm{LC}(O_F G)_S$ with $\partial^0(y) = \partial^0(x)$ in $\mathrm{Cl}(O_F G)$. Hence we have*

$$\partial^0(LC(O_F G)) = \partial^0(LC(O_F G)_S). \tag{13.2}$$

Proof. Let $\mathfrak{a}$ be an ideal of F chosen as in Proposition 11.6 (so $\mathfrak{a}$ is divisible by a sufficiently high power of $|G|$ for the homomorphism $\Theta^t_{\mathfrak{a}}$ to be defined). Proposition 11.5 implies that there are infinitely many choices of $g \in \mathbf{F}$ such that $\mathrm{Supp}(g)$ is disjoint from S and g lies in the same modified narrow ray class modulo $\mathfrak{a}$ as $f(x)$, i.e.

$$f(x) \equiv g \pmod{\Lambda(FG)^\times \cdot U'_{\mathfrak{a}}(\Lambda(O_F G)) \cdot U'_\infty(\Lambda(O_F G))_+}.$$

Hence for any such g, we have

$$K\Theta^t(f(x)) = K\Theta^t(\beta \cdot b \cdot g)$$

where $\beta \in \Lambda(FG)^\times$ and $b = (b_v) \in U'_{\mathfrak{a}}(\Lambda(O_F G)) \cdot U'_\infty(\Lambda(O_F G))_+$. Now $K\Theta^t(\beta) \in \partial^1(K_1(F^c G))$ (see (10.3), (10.4), and (10.5)), while $K\Theta^t(b)$ lies in the image of $\prod_v \mathrm{Det}(\mathcal{H}(O_{F_v} G))$ in $J(K_0(O_F G, F^c))$, by virtue of our choice of $\mathfrak{a}$. We therefore see from (13.1) that we have the equality

$$[(x_v \cdot \mathrm{loc}_v(x_\infty))] \cdot K\Theta^t(\beta)^{-1} = [a(x)] \cdot K\Theta^t(b) \cdot K\Theta^t(g)$$

in $J(K_0(O_F G, F^c))$. Then the class

$$y = [(x_v \cdot \mathrm{loc}_v(x_\infty))] \cdot K\Theta^t(\beta)^{-1}$$

in $J(K_0(O_F G, F^c))$ satisfies the desired conditions.

The final assertion follows immediately from the exact sequence (6.1). □

Proposition 13.5. *Suppose that S is any finite set of places of F, and that $x \in \mathrm{LC}(O_F G)$. Then there exist infinitely many $y \in \mathrm{LC}(O_F G)_S$ such that y is fully ramified and $\partial^0(y) = \partial^0(x)$ in $\mathrm{Cl}(O_F G)$.*

Proof. This is a generalisation of [20, Proposition 6.14], and it may be proved in the same way as [7, Proposition 7.4].

We begin by constructing a full element h of $\mathbf{F}$ as follows. Let M/F be a finite Galois extension such that Ω_M acts trivially on $\mathcal{C}(G(-1))$. For each $s \in G$, choose a place $v(s)$ of F that splits completely in M/F; the Chebotarev density theorem implies that this may be done so that the places $v(s)$ are distinct and disjoint from S. Then the element $h = \prod_{s\in G} f_{v(s),s}$ is full.

Next, we choose an ideal $\mathfrak{a}$ of F as in Proposition 11.6 and observe that Proposition 11.5 implies that there are infinitely many choices of $g \in \mathbf{F}$ with $\mathrm{Supp}(g)$ disjoint from $S \cup \mathrm{Supp}(h)$ such that g lies in the same modified narrow ray class of $\Lambda(O_F G)$ modulo $\mathfrak{a}$ as $f(x) \cdot h^{-1}$. Then, for any such g, we have that

$$f(x) \equiv g \cdot h \pmod{\Lambda(FG)^\times \cdot U_{\mathfrak{a}}(\Lambda(O_F G)) \cdot U'_\infty(\Lambda(O_F G))_+},$$

and $g \cdot h \in \mathbf{F}$ is full. Now exactly as in the proof of Proposition 13.4 we may replace $f(x)$ by $g \cdot h$ in (13.1), changing the other terms in the equality as needed, to obtain $y \in K_0(O_F G, F^c)$ satisfying the stated conditions. □

Theorem 13.6. *Let S be any finite set of places of F, and suppose that Conjecture B holds for $\mathrm{LC}(O_F G)_S$, i.e. that*

$$\mathrm{LC}(O_F G)_S \subseteq K\mathcal{R}(O_F G) = \mathrm{Im}(\Psi). \tag{13.3}$$

Then $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$. If $c \in \mathcal{R}(O_F G)$, then there exist infinitely many $[\pi] \in H^1_t(F, G)$ such that F_π is a field and $(O_\pi) = c$. The extensions F_π/F may be chosen to have ramification disjoint from S.

Proof. To prove the first assertion, it suffices to show that, under the given hypotheses, we have

$$\partial^0(\mathrm{LC}(O_F G)) = \mathcal{R}(O_F G) \tag{13.4}$$

(cf. the proof of Theorem 6.7, especially (6.2)).

We plainly have $\mathcal{R}(O_F G) \subseteq \partial^0(\mathrm{LC}(O_F G))$. Suppose that $x \in \mathrm{LC}(O_F G)$, and set $c_x = \partial^0(x)$. Then Proposition 13.5 implies that there exists $y \in \mathrm{LC}(O_F G)_S$ with $\partial^0(y) = c_x$. By hypothesis, we have $y \in \mathrm{Im}(\Psi)$, and so $\partial^0(y) = c_x \in \mathcal{R}(O_F G)$. This implies that $\partial^0(\mathrm{LC}(O_F G)) \subseteq \mathcal{R}(O_F G)$. Hence (13.4) holds, and so $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$, as claimed.

Next, we observe that if $c \in \mathcal{R}(O_F G)$, then (13.4) and Proposition 13.5 imply that there are infinitely many $x \in \mathrm{LC}(O_F G)_S$ such that x is fully ramified and $\partial^0(x) = c$. For each such x, our hypotheses imply that there exists $\pi_x \in \mathrm{Hom}(\Omega_F, G)$ with $[\pi_x] \in H^1_t(F, G)$

and $\Psi([\pi_x]) = x$. The set of primes that ramify in F_{π_x}/F is equal to $\mathrm{Supp}(f(x))$, and so F_{π_x}/F has ramification disjoint from S. As $f(x)$ is full, we see that for each non-identity element $s \in G$, there is a place $v(s) \in \mathrm{Supp}(f(x))$ such that $\pi_x(\sigma_{v(s)}) \in c(s)$ (cf. (7.5) and Proposition 10.5 (a) and (b)). Hence $\mathrm{Im}(\pi_x)$ has non-trivial intersection with every conjugacy class of G and so is equal to the whole of G, by a lemma of Jordan (see [28, p. 435, Theorem 4']). Therefore π_x is surjective, and so F_{π_x} is a field. This establishes the result. □

14. Abelian groups

In this section we shall prove that Conjecture 6.5 holds for abelian groups. We shall also show that the map Ψ is injective in this case.

Let G be abelian, and suppose that L is any finite extension of F or of F_v for some place v of F. As G is abelian, the reduced norm map induces isomorphisms

$$(LG)^\times \simeq \mathrm{Det}(LG)^\times, \quad (O_LG)^\times \simeq \mathrm{Det}(O_LG)^\times, \quad (L^cG)^\times \simeq \mathrm{Det}(L^cG)^\times. \tag{14.1}$$

For each finite place v of F, Lemma 5.7 and (14.1) imply that there are isomorphisms

$$K_0(O_{F_v}G, F_v^c) \simeq \frac{\mathrm{Det}(F_v^cG)^\times}{\mathrm{Det}(O_{F_v}G)^\times} \simeq \frac{(F_v^cG)^\times}{(O_{F_v}G)^\times}.$$

Proposition 14.1. *Let G be abelian, and suppose that v is a finite place of F. Then the map Ψ_v is injective.*

Proof. Suppose that $[\pi_{v,i}] \in H_t^1(F_v, G)$ $(i = 1, 2)$, with $O_{\pi_{v,i}} = O_{F_v}G \cdot a_{v,i}$. Then $\Psi_v([\pi_{v,i}]) = [\mathbf{r}_G(a_{v,i})]$ in $(F_v^cG)^\times/(O_{F_v}G)^\times$. Hence if $\Psi([\pi_{v,1}]) = \Psi([\pi_{v,2}])$, then we have $\mathbf{r}_G(a_{v,1}) \cdot \mathbf{r}_G(a_{v,2})^{-1} \in (O_{F_v}G)^\times$. This implies that $[\pi_{1,v}] = [\pi_{2,v}]$ in $H_t^1(F_v, G)$, and so it follows that Ψ_v is injective, as claimed. □

Again because G is abelian, the pointed set of resolvends $H_t(LG)$ is an abelian group, and the exact sequences (3.3) and (3.4) show that there is an isomorphism

$$\tau : H_t^1(L, G) \xrightarrow{\sim} \frac{H_t(LG)}{(LG)^\times} \tag{14.2}$$

defined as follows: if $[\pi] \in H_t^1(L, G)$ with $L_\pi = LG \cdot b_\pi$, then $\tau([\pi]) = [\mathbf{r}_G(b_\pi)]$.

Note also that Theorem 5.4(b) and (14.1) imply that $K_0(O_FG, F^c)$ is isomorphic to the cokernel of the homomorphism

$$\Delta_{O_FG, F^c} : (FG)^\times \to \frac{J(FG)}{\prod_v (O_{F_v}G)^\times} \times (F^cG)^\times$$

induced by

$$(FG)^\times \to J(FG) \times (F^cG)^\times; \quad x \mapsto ((\mathrm{loc}_v(x))_v, x^{-1}).$$

Theorem 14.2. *Conjecture 6.5 is true when G is abelian.*

Proof. Suppose that $x \in \mathrm{LC}(O_FG)$, and let $[(x_v)_v, x_\infty] \in J(FG) \times (F^cG)^\times$ be a representative of x. We shall explain how to construct an element $[\pi] \in H^1_t(F, G)$ such that $\lambda_v(x) = \lambda_v(\Psi([\pi]))$ for all finite places v of F. Since G is abelian, and therefore admits no irreducible symplectic characters, this will imply that $x = \Psi([\pi])$ (see Proposition 5.9(b)).

For each v, we have that $x_v \cdot \mathrm{loc}_v(x_\infty) \in H_t(F_vG)$. As $x_v \in (F_vG)^\times$, this implies that $\mathrm{loc}_v(x_\infty) \in H_t(F_vG)$ for each v. It follows from Proposition 2.3 that $x_\infty \in H(FG)$, and we see in addition that in fact $x_\infty \in H_t(FG)$. Hence x_∞ is the resolvend of a normal basis generator of a tame extension F_π/F. Set $\pi_v := \mathrm{loc}_v(\pi)$. Then for each finite v, we have

$$\tau(\Psi_v^{-1}(\lambda_v(x))) = [\mathrm{loc}_v(x_\infty)] = \tau([\pi_v])$$

in $H_t(F_vG)/(F_vG)^\times$, which in turn implies that

$$\lambda_v(x) = \Psi_v([\pi_v]) = \lambda_v(\Psi([\pi])).$$

Hence $x = \Psi([\pi])$, as required. □

Proposition 14.3. *If G is abelian, then the map Ψ is injective.*

Proof. Let $[\pi] \in H^1_t(F_v, G)$, and suppose that $[(x_v)_v, x_\infty] \in J(K_1(FG)) \times (F^cG)^\times$ is a representative of $\Psi([\pi])$. Then it follows from the proof of Theorem 14.2 that $\tau([\pi]) = x_\infty$ in $H_t(FG)/(FG)^\times$. Since τ is an isomorphism, we deduce that Ψ is injective. □

15. Neukirch's Lifting Theorem

Our main purpose in this section is to describe certain results, mainly from [24], that will be used in the proof of Theorem E. We refer the reader to [24] or [25, IX.5] for full details regarding these topics.

Let D be an arbitrary finite group. Consider the category $\mathcal{D}$ of homomorphisms $\eta : \mathcal{G} \to D$ of arbitrary profinite groups $\mathcal{G}$ into D in which a morphism between two objects $\eta_1 : \mathcal{G}_1 \to D$ and $\eta_2 : \mathcal{G}_2 \to D$ is defined to be a homomorphism $\nu : \mathcal{G}_1 \to \mathcal{G}_2$ such that $\eta_1 = \eta_2 \circ \nu$. We say that two such morphisms $\nu_i : \mathcal{G}_1 \to \mathcal{G}_2$ $(i = 1, 2)$ are *equivalent* if there is an element $k \in \mathrm{Ker}(\eta_2)$ such that $\nu_1(\omega) = k \cdot \nu_2(\omega) \cdot k^{-1}$ for all $\omega \in \mathcal{G}_1$. Write $\mathcal{H}om_D(\mathcal{G}_1, \mathcal{G}_2)$ for the set of equivalence classes of homomorphisms $\mathcal{G}_1 \to \mathcal{G}_2$, and $\mathcal{H}om_D(\mathcal{G}_1, \mathcal{G}_2)_{\mathrm{epi}}$ for the subset of $\mathcal{H}om_D(\mathcal{G}_1, \mathcal{G}_2)$ consisting of equivalence classes of surjective homomorphisms.

Suppose now that we have an exact sequence

$$0 \to B \to G \xrightarrow{q} D \to 0$$

with B abelian, and that L is a number field or a local field. Let $h : \Omega_L \to D$ be a fixed homomorphism. We view $\Omega_L \xrightarrow{h} D$ and $G \xrightarrow{q} D$ as being elements of $\mathcal{D}$. The group D acts on B via inner automorphisms, and this in turn induces an action of Ω_L on B via h. We write $L(B)$ for the smallest extension of L such that $\Omega_{L(B)}$ fixes B (i.e. $L(B)$ is the field of definition of B).

It may be shown that the group $H^1(L, B)$ acts on $\mathcal{H}om_D(\Omega_L, G)$ in the following way. Let $z \in Z^1(L, B)$ be any 1-cocycle representing $[z] \in H^1(L, B)$, and let $\nu \in \mathrm{Hom}(\Omega_L, G)$ be any homomorphism, representing an element $[\nu] \in \mathcal{H}om_D(\Omega_L, G)$. Define $z \cdot \nu : \Omega_L \to G$ by

$$(z \cdot \nu)(\omega) = z(\omega) \cdot \nu(\omega)$$

for all $\omega \in \Omega_L$. It is not hard to check that

$$h = q \circ (z \cdot \nu),$$

and that the element $[z \cdot \nu] \in \mathcal{H}om_D(\Omega_L, G)$ is independent of the choices of z and ν. It may also be shown that $\mathcal{H}om_D(\Omega_L, G)$ is a principal homogeneous space over $H^1(L, B)$.

For a number field F, and a finite place v of F, we let $\mathcal{H}om_D(\Omega_{F_v}, G)_{nr}$ denote the set of classes of homomorphisms $\Omega_{F_v} \to G$ that are trivial on I_v. We write $J_f(\mathcal{H}om_D(\Omega_F, G))$ for the restricted direct product over all finite places of F of the sets $\mathcal{H}om_D(\Omega_{F_v}, G)$ with respect to the subsets $\mathcal{H}om_D(\Omega_{F_v}, G)_{nr}$.

Now we can state Neukirch's Lifting Theorem.

Theorem 15.1. *Let F be a number field and let $h : \Omega_F \to D$ be a fixed, surjective homomorphism. Suppose that*

$$0 \to B \to G \xrightarrow{q} D \to 0$$

is an exact sequence for which B is a simple Ω_F-module. (This implies that $l \cdot B = 0$ for a unique prime l.) Assume that the field of definition $F(B)$ of B contains no non-trivial l-th roots of unity, and that $J_f(\mathcal{H}om_D(\Omega_F, G)) \neq \emptyset$. Let S be any finite set of finite places of F. Then the natural map

$$\mathcal{H}om_D(\Omega_F, G)_{\mathrm{epi}} \to \prod_{v \in S} \mathcal{H}om_D(\Omega_{F_v}, G)$$

is surjective.

Proof. This is [24, Main Theorem, p. 148]. □

The following result implies that $\mathcal{H}om_D(\Omega_{F_v}, G) \neq \emptyset$ for all but finitely many v.

Proposition 15.2. *(*[24, Lemma 5]*) Let F be a number field, and let v be a finite place of F. Suppose that $\mathcal{G}_1 \to \mathcal{G}_2$ is a surjective homomorphism of arbitrary profinite groups, and that there exists an unramified homomorphism $h_v : \Omega_{F_v} \to \mathcal{G}_2$. Then $\mathcal{H}om_{\mathcal{G}_2}(\Omega_{F_v}, \mathcal{G}_1)_{nr} \neq \emptyset$, and so $\mathcal{H}om_{\mathcal{G}_2}(\Omega_{F_v}, \mathcal{G}_1) \neq \emptyset$ also.*

Proof. If h_v is unramified, then h_v factors through $\Omega_{F_v}/I_v \simeq \hat{\mathbf{Z}}$, and a map $\hat{\mathbf{Z}} \to \mathcal{G}_2$ may always be lifted to a map $\hat{\mathbf{Z}} \to \mathcal{G}_1$ by lifting the image of a topological generator of $\hat{\mathbf{Z}}$. □

We now turn to two results of a local-global nature that will play a role in the proof of Theorem 16.4. In order to describe them, we let Γ be a finite abelian group equipped with an action of Ω_F such that Γ is a simple Ω_F-module. Then $l \cdot \Gamma = 0$ for a unique prime l. Write $F(\Gamma)$ for the field of definition of Γ.

Theorem 15.3. *Let M/F be a Galois extension with $F(\Gamma) \subseteq M$ and $\mu_l \nsubseteq M$, and let $\mathcal{N}/M$ be a finite abelian extension. Let S be a finite set of finite places of F, and suppose given an element $y_v \in H^1(F_v, \Gamma)$ for each $v \in S$. Then there exists an element $z \in H^1(F, \Gamma)$ satisfying the following local conditions:*

(i) $z_v = y_v$ for each $v \in S$.

(ii) If $v \notin S$, then z_v is cyclic (i.e. is trivialised by a cyclic extension of F_v), and if z_v is ramified, then v splits completely in $\mathcal{N}/F$.

Proof. This is [24, Theorem 1]. □

In order to state our next result, we introduce the following notation.

Definition 15.4. Let $T := \{v_1, \ldots, v_r\}$ be any finite set of finite places of F containing all places that ramify in $F(\Gamma)/F$ and all places above l. Let $\mathfrak{p}_i$ denote the prime ideal of F corresponding to v_i. Proposition 4.8 implies that we may choose an integer $N = N(T)$ such that for each $1 \leq i \leq r$ and for every place w of $F(\Gamma)$ lying above v_i, we have

$$\mathrm{Hom}_{\Omega_{F(\Gamma)_w}}(A_\Gamma, U_{\mathfrak{p}_i^N}(O_{F(\Gamma)^c_w})) \subseteq \mathrm{rag}[\mathrm{Hom}_{\Omega_{F(\Gamma)_w}}(R_\Gamma, O^\times_{F(\Gamma)^c_w})].$$

Set

$$\mathfrak{a} = \mathfrak{a}(T) = \prod_{i=1}^{r} \mathfrak{p}_i.$$

Let $F(\mathfrak{a}^N)$ denote the ray class field of F modulo $\mathfrak{a}^N$. □

Theorem 15.5. *Let $v \notin T$ be any finite place of F that splits completely in $F(\mathfrak{a}^N)$, and suppose that s is any non-trivial element of Γ. Then there is an element $b = b(v;s) \in H^1(F,\Gamma)$ satisfying the following local conditions:*

(i) $\mathrm{loc}_{v_i}(b) = 0$ *for* $1 \leq i \leq r$;

(ii) $b\,|_{I_v} = \tilde{\varphi}_{v,s}$ *(see Remark 7.11);*

(iii) b is unramified away from v.

Proof. Let $\mathfrak{p}$ be the prime ideal of F corresponding to v. Our hypotheses on v imply that $\mathfrak{p}$ is principal, with $\mathfrak{p} \equiv 1 \pmod{\mathfrak{a}^N}$. Set $M := F(\Gamma)$. As Γ is abelian, we have that $\mathcal{H}(M\Gamma) \simeq \mathrm{Hom}_{\Omega_M}(A_\Gamma, (M^c)^\times)$ (cf. (4.6)). Let ϖ be a generator of $\mathfrak{p}$, and define $\rho \in \mathrm{Hom}_{\Omega_M}(A_\Gamma, (M^c)^\times)$ by

$$\rho(\alpha) = \varpi^{\langle \alpha, s\rangle_\Gamma}.$$

(This homomorphism is Ω_M-equivariant because Ω_M fixes Γ.) Then ρ is the reduced resolvend of a normal basis generator of an extension $M_{\pi(\rho)}/M$ corresponding to $[\pi(\rho)] \in H^1(M,\Gamma)$. Since $\mathfrak{p} \equiv 1 \pmod{\mathfrak{a}^N}$, for each place w of M lying above a place v_i in T, we have

$$\mathrm{loc}_w(\rho) \in \mathrm{Hom}_{\Omega_{M_w}}(A_\Gamma, U_{\mathfrak{p}_i^N}(O_{M_w^c})) \subseteq \mathrm{rag}[\mathrm{Hom}_{\Omega_{M_w}}(R_\Gamma, O_{M_w^c}^\times)],$$

and so it follows that $\mathrm{loc}_w(\pi(\rho)) = 0$ (see (4.7)). In particular, $\pi(\rho)$ is unramified at all places above T.

For all places w' of M not lying above T or v we have that

$$\mathrm{loc}_{w'}(\rho) \in \mathrm{Hom}_{\Omega_{M_{w'}}}(A_\Gamma, O_{M_{w'}^c}^\times),$$

and so $\pi(\rho)$ is unramified at w'. This implies that $\pi(\rho)$ is unramified away from v, since we have already seen that $\pi(\rho)$ does not ramify at any place above T. It is also easy to see that

$$b\,|_{I_{w(v)}} = \tilde{\varphi}_{w(v),s}$$

for any place $w(v)$ of M lying above v (cf. the proof of Proposition 10.5(a)).

As $\varpi \in F$, we have that $\pi(\rho) \in H^1(M,\Gamma)^{\mathrm{Gal}(M/F)}$. Since $\Gamma^{\Omega_F} = 0$ (because Γ is a simple Ω_F-module), the restriction map $H^1(F,\Gamma) \to H^1(M,\Gamma)$ is injective and induces an isomorphism $H^1(F,\Gamma) \simeq H^1(M,\Gamma)^{\mathrm{Gal}(M/F)}$. Hence $\pi(\rho)$ is the image of an element $b \in H^1(F,\Gamma)$ satisfying the conditions (i), (ii) and (iii) of the theorem. □

16. Soluble groups

In this section we shall use Neukirch's Lifting Theorem to prove a result (see Theorem 16.4 below) that implies Theorem E of the Introduction. In order to describe this result, it will be helpful to formulate the following definition.

Definition 16.1. Let S be any finite (possibly empty) set of places of F. We shall say that $\mathrm{LC}(O_F G)_S$ *satisfies Property R* if the following holds. Suppose given any fully ramified $x \in \mathrm{LC}(O_F G)_S$. For each finite place v of F, suppose also given a homomorphism $\pi_{v,x} \in \mathrm{Hom}(\Omega_{F_v}, G)$ such that $[\pi_{v,x}] \in H^1_t(F_v, G)$ and $\lambda_v(x) = \Psi_v([\pi_{v,x}])$. (Note that in general, such a choice of $\pi_{v,x}$ is not unique.) Then there exists $\Pi \in \mathrm{Hom}(\Omega_F, G)$ with $[\Pi] \in H^1_t(F, G)$ such that

(a) $x = \Psi([\Pi])$;

(b) $\Pi\,|_{I_v} = \pi_{v,x}\,|_{I_v}$ for each finite place v of F.

(So in particular, x is cohomological.) □

Proposition 16.2. *If G is abelian, then $\mathrm{LC}(O_F G)$ satisfies Property R.*

Proof. We shall in fact prove a slightly stronger result. Suppose that G is abelian, and let $x \in \mathrm{LC}(O_F G)$. (Note that we do not assume that x is fully ramified.) Then Theorem 14.2 implies that x is cohomological. As G is abelian, the maps Ψ and Ψ_v are injective (see Propositions 14.1 and 14.3). Hence it follows that there is a unique $[\Pi] \in H^1_t(F, G)$ such that $x = \Psi([\Pi])$, and a unique $[\pi_{v,x}] \in H^1_t(F_v, G)$ such that $\lambda_v(x) = \Psi_v([\pi_{v,x}])$. We therefore see that

$$\lambda_v(x) = \Psi_v([\Pi_v]) = \Psi([\pi_{v,x}]),$$

and so $\Pi_v = \pi_{v,x}$. This implies that $\mathrm{LC}(O_F G)$ satisfies Property R. □

Theorem 16.3. *Suppose that $\mathrm{LC}(O_F G)_S$ satisfies Property R. Then $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$. If $c \in \mathcal{R}(O_F G)$, then there exist infinitely many $[\pi] \in H^1_t(F, G)$ such that F_π is a field and $(O_\pi) = c$. The extensions F_π/F may be chosen to have ramification disjoint from S.*

Proof. This is an immediate consequence of Theorem 13.6. □

Our proof of Theorem E rests on the following result.

Theorem 16.4. *Suppose that there is an exact sequence*

$$0 \to B \to G \to D \to 0,$$

where B is an abelian minimal normal subgroup of G with $l \cdot B = 0$ for an odd prime l. Let S be any finite set of finite places of F containing all places dividing $|G|$. Assume that the following conditions hold:

(i) The set $\mathrm{LC}(O_F D)_S$ satisfies Property R;

(ii) We have $(|G|, h_F) = 1$, where h_F denotes the class number of F;

(iii) Either G admits no irreducible symplectic characters, or F has no real places;

(iv) The field F contains no non-trivial l-th roots of unity.

Then $\mathrm{LC}(O_F G)_S$ satisfies Property R.

Proof. We shall establish this result in several steps, one of which crucially involves Neukirch's Lifting Theorem (see Theorem 15.1).

Suppose that $x \in \mathrm{LC}(O_F G)_S$ is fully ramified. For each finite place v of F, choose $\pi_{v,x} \in \mathrm{Hom}(\Omega_{F_v}, G)$ such that $[\pi_{v,x}] \in H^1_t(F_v, G)$ with

$$\lambda_v(x) = \Psi_v([\pi_{v,x}]).$$

The choice of $\pi_{v,x}$ is not unique. However, if $a(\pi_{v,x})$ is any normal integral basis generator of $F_{\pi_{v,x}}/F_v$, with Stickelberger factorisation (see Definition 7.12)

$$\mathbf{r}_G(a(\pi_{v,x})) = u(a(\pi_{v,x})) \cdot \mathbf{r}_G(a_{nr}(\pi_{v,x})) \cdot \mathbf{r}_G(\varphi(\pi_{v,x})), \tag{16.1}$$

then Proposition 10.5(c) implies that $\mathrm{Det}(\mathbf{r}_G(\varphi(\pi_{v,x})))$ is independent of the choice of $\pi_{v,x}$. Hence, if $\varphi(\pi_{v,x}) = \varphi_{v,s}$, say, then it follows from Proposition 10.5(b) that the subgroup $\langle s \rangle$ of G (up to conjugation) and the determinant $\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s}))$ of the resolvend $\mathbf{r}_G(\varphi_{v,s})$ do not depend upon the choice of $\pi_{v,x}$.

We write $q : G \to D$ for the obvious quotient map, and we use the same symbol q for the induced maps

$$K_0(O_F G, F^c) \to K_0(O_F D, F^c), \quad H^1(F, G) \to H^1(F, D),$$
$$H^1(F_v, G) \to H^1(F_v, D).$$

Set

$$\overline{x} := q(x), \quad \pi_{v,\overline{x}} := q(\pi_{v,x}).$$

Then $\overline{x} \in \mathrm{LC}(O_F D)_S$ with

$$\lambda_v(\overline{x}) = \Psi_{D,v}(\pi_{v,\overline{x}})$$

for each finite place v of F, and $\overline{x}$ is fully ramified.

By hypothesis, $\mathrm{LC}(O_F D)_S$ satisfies Property R, and so there exists $\rho \in \mathrm{Hom}(\Omega_F, D)$ with $[\rho] \in H^1_t(F, D)$ such that

$$\overline{x} = \Psi_D([\rho]) \tag{16.2}$$

and

$$\rho \mid_{I_v} = \pi_{v,\overline{x}} \mid_{I_v} \tag{16.3}$$

for each finite place v of F. Hence, for each such v, we have that

$$\mathrm{Det}(\mathbf{r}_D(\varphi(\rho_v))) = \mathrm{Det}(\mathbf{r}_D(\varphi(\pi_{v,\overline{x}}))),$$

using the notation established in (16.1) above concerning Stickelberger factorisations. As $\overline{x}$ is fully ramified, we see from the proof of Theorem 13.6 that ρ is surjective, and so F_ρ is a field. We also see that, as $\overline{x} \in \mathrm{LC}(O_F D)_S$, the extension F_ρ/F is unramified at all places dividing $|D|$. Furthermore, if $v \mid l$ (so $v \in S$), then since $\pi_{v,x}$ is unramified, the same is true of $\pi_{v,\overline{x}}$, and so F_ρ/F is also unramified at v. Hence, as $F \cap \mu_l = \{1\}$ by hypothesis, it follows that $F_\rho \cap \mu_l = \{1\}$ also.

For each finite place v of F, we are now going to use the fact that $x \in \mathrm{LC}(O_F G)$ to construct a lift $\tilde{\rho}_v \in \mathrm{Hom}(\Omega_{F_v}, G)$ of ρ_v such that $[\tilde{\rho}_v] \in H^1_t(F_v, G)$ with

$$\tilde{\rho}_v \mid_{I_v} = \pi_{v,x} \mid_{I_v} . \tag{16.4}$$

To do this, we first observe that if $\varphi(\pi_{v,x}) = \varphi_{v,s}$, then $\varphi(\pi_{v,\overline{x}}) = \varphi_{v,\overline{s}}$, where $\overline{s} = q(s)$, and so we have

$$\varphi(\rho_v) = \varphi(\pi_{v,\overline{x}}) = \varphi_{v,\overline{s}}$$

(see (16.3)).

Next, we write

$$\rho_v = \rho_{v,r} \cdot \rho_{v,nr},$$

with $[\rho_{v,nr}] \in H^1_{nr}(F_v, D)$ (see (7.7)). Since $\rho_{v,nr}$ is unramified, Proposition 15.2 implies that $[\rho_{v,nr}]$ may be lifted to $[\tilde{\rho}_{v,nr}] \in H^1_{nr}(F_v, G)$. Let $a(\tilde{\rho}_{v,nr})$ be a normal integral basis generator of $F_{\tilde{\rho}_{v,nr}}/F_v$. Then $\mathbf{r}_G(a(\tilde{\rho}_{v,nr})) \cdot \mathbf{r}_G(\varphi_{v,s})$ is the resolvend of a normal integral basis generator of a tame Galois G-extension $F_{\tilde{\rho}_v}/F_v$ such that $q([\tilde{\rho}_v]) = \rho_v$ (cf. Corollary 7.8 and Theorem 7.9). As $\varphi(\pi_{v,x}) = \varphi_{v,s}$, we see from the construction of $\tilde{\rho}$ that

$$\tilde{\rho}_v \mid_{I_v} = \pi_{v,x} \mid_{I_v} = \tilde{\varphi}_{v,s},$$

where $[\tilde{\varphi}_{v,s}] \in H^1_t(I_v, G)$ is defined in Remark 7.11. The map $\tilde{\rho}_v$ is our desired lift of ρ_v.

We are now ready to apply the results contained in Section 15. Consider the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & G & \xrightarrow{q} & D & \longrightarrow & 0 \\ & & & & & & \uparrow{\scriptstyle \rho} & & \\ & & & & & & \Omega_F & & \end{array}$$

The group D acts on B via inner automorphisms, and we view B as being an Ω_F-module via ρ. Then B is a simple Ω_F-module because B is a minimal normal subgroup of G and ρ is surjective. The field of definition $F(B)$ of B is contained in the field F_ρ, and so in particular $F(B)$ contains no non-trivial l-th roots of unity. We are going to construct an element $\Pi \in \mathcal{H}om_D(\Omega_F, G)$ such that

$$\Pi\,|_{I_v} = \pi_{v,x}\,|_{I_v}$$

for each finite place v of F. This will be accomplished in the following three steps:

I. We begin by observing that our construction above of a lift $\tilde{\rho}_v$ of ρ_v for each finite v shows that $J_f(\mathcal{H}om_D(\Omega_F, G))$ is non-empty. Let $\mathcal{S}$ be the set of finite places v of F at which x is ramified or $v \mid |G|$. Theorem 15.1 implies that there exists $\Pi_1 \in \mathcal{H}om_D(\Omega_F, G)$ such that $\Pi_{1,v} = \tilde{\rho}_v$ for all $v \in \mathcal{S}$. Observe that Π_1 is unramified at all $v \mid |G|$ because $\tilde{\rho}_v$ is unramified at these places (see (16.4)). Note also that Π_1 may well be ramified outside $\mathcal{S}$.

II. Recall that $\mathcal{H}om_D(\Omega_F, G)$ (respectively $\mathcal{H}om_D(\Omega_{F_v}, G)$ for each finite v) is a principal homogeneous space over $H^1(F, B)$ (respectively $H^1(F_v, B)$). Let $\mathcal{S}_1$ denote the set of finite places $v \notin \mathcal{S}$ of F at which Π_1 is ramified. For each $v \in \mathcal{S}_1$, choose $y_v \in H^1(F_v, B)$ so that $y_v \cdot \Pi_{1,v} \in \mathcal{H}om_D(\Omega_{F_v}, G)$ is unramified.

Now apply Definition 15.4 (with $\Gamma = B$ and $T = \mathcal{S}$) to obtain an ideal $\mathfrak{a} = \mathfrak{a}(\mathcal{S})$ and an integer $N = N(\mathcal{S})$ as described there. Theorem 15.3 implies that there exists an element $z \in H^1(F, B)$ such that

(z1) $z_v = y_v$ for all $v \in \mathcal{S}_1$;

(z2) $z_v = 1$ for all $v \in \mathcal{S}$;

(z3) If $v \notin \mathcal{S} \cup \mathcal{S}_1$, then z_v is cyclic, and if z_v is ramified, then v splits completely in $(F(B) \cdot F(\mathfrak{a}^N))/F$, where $F(\mathfrak{a}^N)$ denotes the ray class field of F modulo $\mathfrak{a}^N$.

Set $\Pi_2 := z \cdot \Pi_1 \in \mathcal{H}om_D(\Omega_F, G)$. Note that, as z might possibly be ramified, the homomorphism Π_2 might be ramified outside $\mathcal{S}$. We shall eliminate any such potential ramification in the third and final step.

III. Let $\mathcal{S}_z$ be the set of places of F at which z is ramified (so $\mathcal{S} \cap \mathcal{S}_z = \emptyset$). We see from (z3) that each $v \in \mathcal{S}_z$ is totally split in $F(\mathfrak{a}^N)/F$. Hence Theorem 15.5 implies that for each $v \in \mathcal{S}_z$, we may choose $b(v) \in H^1(F, B)$ such that

(b1) $b(v)_w = 1$ for all $w \in \mathfrak{S}$;
(b2) $b(v) \mid_{I_v} = z_v^{-1} \mid_{I_v}$;
(b3) $b(v)$ is unramified away from v.
Set

$$\Pi := \left[\left(\prod_{v \in S_z} b(v) \right) \cdot z \right] \cdot \Pi_2.$$

Then it follows directly from the construction of Π that we have

$$\Pi \mid_{I_v} = \pi_{v,x} \mid_{I_v} \tag{16.5}$$

for all finite places v of F.

We claim that

$$x = \Psi(\Pi).$$

To show this, let $\tau = \Psi(\Pi)^{-1} \cdot x$. We see from (16.5) that

$$\lambda_v(\tau) \in \mathrm{Im}(\Psi_v^{nr})$$

for every finite place v of F. As either G admits no irreducible symplectic characters or F has no real places, and as $(h_F, |G|) = 1$ by hypothesis, Proposition 6.8(b) implies that $\tau = 0$. Hence $x = \Psi(\Pi)$, as claimed.

This completes the proof that $\mathrm{LC}(O_F G)_S$ satisfies Property R. □

Theorem 16.4 (in conjunction with Proposition 16.2) yields an abundant supply of groups G for which $\mathrm{LC}(O_F G)_S$ satisfies Property R (for a suitable choice of S), and therefore also for which Theorem 16.3 holds. Here is an example of this.

Theorem 16.5. *Let G be of odd order. Suppose that $(|G|, h_F) = 1$ and that F contains no non-trivial $|G|$-th roots of unity. Let S be any finite set of finite places of F containing all places dividing $|G|$. Then $\mathrm{LC}(O_F G)_S$ satisfies Property R.*

Proof. We shall establish this result by induction on the order of G. We first note that Proposition 16.2 implies that the theorem holds if G is abelian.

Suppose now that G is an arbitrary finite group of odd order. As $|G|$ is odd, a well known theorem of Feit and Thompson (see [14]) implies that G is soluble. Hence G has an abelian minimal normal subgroup B such that $l \cdot B = 0$ for some odd prime l (see e.g. [26, Theorem 5.24]), and there is an exact sequence

$$0 \to B \to G \to D \to 0$$

with D soluble. As $|G|$ is odd, G admits no non-trivial irreducible symplectic characters. We may therefore suppose by induction on the order of G that $\mathrm{LC}(O_F D)_S$ satisfies Property R. The desired result now follows from Theorem 16.4. □

Remark 16.6. It follows from Theorem 14.2 that in Theorem 16.4, we may take D to be a finite abelian group of arbitrary order (subject of course to the obvious constraint that the number field F is such that all other conditions of Theorem 16.4 are satisfied). This enables one to show that Property R holds for many non-abelian groups of even order (e.g. S_3). However, if for example G is a non-abelian 2-group (e.g. H_8), then because $\mu_2 \subseteq F$ for any number field F, we can no longer appeal to Neukirch's Lifting Theorem, and our proof of Theorem 16.4 fails. It appears very likely that new ideas are needed to establish Property R in such cases (cf. also the remarks contained in the final paragraph of [24, Introduction], where a similar difficulty is briefly discussed in the context of the inverse Galois problem for finite groups). □

We can now prove Theorem E of the Introduction.

Theorem 16.7. *Let G be of odd order and suppose that $(|G|, h_F) = 1$, where h_F denotes the class number of F. Suppose also that F contains no non-trivial $|G|$-th roots of unity. Then $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$. If $c \in \mathcal{R}(O_F G)$, then there exist infinitely many $[\pi] \in H^1_t(F, G)$ such that F_π is a field and $(O_\pi) = c$. The extensions F_π/F may be chosen to have ramification disjoint from any finite set S of places of F.*

Proof. This is an immediate consequence of Theorems 16.5 and 16.3. □

References

[1] A. Agboola, *Counting rings of integers as Galois modules*, J. Reine Angew. Math. **663** (2012), 1–31.

[2] A. Agboola, D. Burns, *On the Galois structure of equivariant line bundles on curves*, Amer. J. Math. **120** (1998), 1121–1163.

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

[4] A. Agboola, D. Burns, *On Grothendieck groups of bundles on varieties over finite fields*, K-Theory **23** (2001), 251–303.

[5] M. Bueno, S. Furtado, J. Karkoska, K. Mayfield, R. Samalis, A. Telatovich, *The kernel of the matrix* $[i \cdot j \pmod n]$ *when* n *is prime*, Involve **9** (2016), 265–280.

[6] D. M. Burton, *An elementary introduction to the theory of numbers*, McGraw Hill, 2007.

[7] N. Byott, *Tame realisable classes over Hopf orders*, J. Algebra **201** (1998), 284–316.

[8] N. Byott, B. Sodaigui, *Realisable Galois module classes for tetrahedral extensions*, Compositio Mathematica **141** (2005), 573–582.

[9] N. Byott, C. Greither, B. Sodaigui, *Classes réalisables d'éxtensions non-abéliennes*, Crelle **601** (2006), 1–27.

[10] T. Chinburg, *Galois structure of de Rham cohomology of tame covers of schemes*, Ann. of Math. **140** (1994), 443–490.

[11] C. W. Curtis, I. Reiner, *Methods of Representation Theory, Volume I*, Wiley, 1981.

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

[13] M. Farhat, B. Sodaigui, *Classes réalisables d'extensions non abéliennes de degré* p^3, J. Number Theory **152** (2015), 55–89.

[14] W. Feit, J. Thompson, *Solvability of groups of odd order*, Pacific J. Math **13** (1963), 775–1029.

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

[16] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Ergebnisse **3**, Springer, Berlin, 1983.

[17] A. Fröhlich, *Classgroups and Hermitian modules*, Birkhäuser, 1984.

[18] D. Hilbert, *The Theory of Algebraic Number Fields*, Springer, 1998.

[19] G. Malle, *On the distribution of Galois groups*, J. Number Theory **92** (2002), 315–329.

[20] L. R. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra **82** (1983), 102–134.

[21] L. R. McCulloh, *Galois module structure of abelian extensions*, Crelle **375/376** (1987), 259–306.

[22] L. R. McCulloh, *From Galois module classes to Steinitz classes*, Lecture in Oberwolfach, February 6, 2002. (arXiv preprint 1207.5702.)

[23] L. R. McCulloh, *On realisable classes for non-abelian extensions*, Lecture in Luminy, March 22, 2011.

[24] J. Neukirch, *On solvable number fields*, Invent. Math. **33** (1979), 135–164.

[25] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields (second edition)*, Springer, Berlin, 2008.

[26] J. Rotman, *An introduction to the theory of groups (fourth edition)*, Springer, Berlin, 1995.

[27] J.-P. Serre, *Galois cohomology*, Springer, Berlin, 1997.

[28] J.-P. Serre, *On a theorem of Jordan*, Bull. A. M. S. **40** (2003), 429–440.

[29] I. Shafarevich, *Construction of fields of algebraic numbers with given soluble Galois group*, Izv. Akad. Nauk. SSSR, Ser. Mat. **18** (1954), 525–578.

[30] A. Siviero, *Class invariants for tame Galois algebras*, PhD Thesis, Université de Bordeaux and Universiteit Leiden, (2013).

[31] A. Siviero, *Realisable classes, Stickelberger subgroup, and its behaviour under change of the base field*, Publications mathématiques de Besançon, Algèbre et théorie des nombres (2015), 69–92.

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

[33] R. Swan, G. Evans, *K-theory of finite groups and orders*, Springer Lecture Notes in Mathematics **149**, (1970).

[34] M. J. Taylor, *Classgroups of Group Rings*, Cambridge University Press, 1984.

[35] C. Tsang, *On the Galois module structure of the square root of the inverse different in tame extensions*, J. Number Theory **160** (2016), 759–804.

[36] C. Tsang, *On the realisable classes of the square root of the inverse different in the unitary class group*, Int. J. Number Theory **13** (2017), 913–932.

[37] D. Wright, *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. **58** (1989), 17–50.

Department of Mathematics, University of California, Santa Barbara, CA 93106.
E-mail address: agboola@math.ucsb.edu

Department of Mathematics, University of Illinois, 1409 W. Green Street, Urbana, IL 61801.
E-mail address: mcculloh@math.uiuc.edu