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. When G is nilpotent, we show (subject to certain conditions) that the set of realisable classes is a subgroup of $\mathrm{Cl}(O_F G)$. This may be viewed as being an analogue of a classical theorem of Scholz and Reichardt on the inverse Galois problem for nilpotent groups in the setting of Galois module theory.

Contents

Date: Preliminary version. October 17, 2014.

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 classgroup $\mathrm{Cl}(O_FG)$ 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

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

which is never a group homomorphism, even when G is abelian. 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.

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 [9]). In particular, he has shown that $\mathcal{R}(O_FG)$ is in fact a group. In subsequent unpublished work [11], he showed that, for arbitrary G, the set $\mathcal{R}(O_FG)$ is always contained in the kernel of this Stickelberger homomorphism, and he raised the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. We refer the reader to the papers [3] and [4], and to their bibliographies for further information concerning some of the more recent 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 [9] and [11] with techniques involving relative algebraic K-theory and categorical twisted forms introduced by D. Burns and the first-named author in [1]. This enables us to both clarify certain aspects of the theory of realisable classes and to establish new results. Although our perspective is perhaps somewhat different, it should be stressed that many of the main ideas that we use are in fact already present in some form in [9] and [11].

Let us now describe the contents of this paper in more detail. In Section 2 we recall some basic facts concerning Galois algebras and resolvends; the latter 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.

We begin Section 4 by outlining the results we need about twisted forms and relative algebraic K-groups from [1]. We show how each tame G-extension F_π/F of F 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 of the map ψ above. 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 8.12 below):

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

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 $K_0(O_F G, F^c)$. We define a pointed set of ideles $J(H^1_t(F, G))$ of $H^1_t(F, G)$ (see Definition 5.2) and a group of ideles $J(K_0(O_F G, F^c))$ of $K_0(O_F G, F^c)$ (see Definition 4.6). We show that there is an injective localisation map

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

(see Proposition 4.7), and we construct 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 5.2). We conjecture that $\lambda(K\mathcal{R}(O_F G))$ may be described as follows (see Conjecture 5.5 below):

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

By applying the methods of [9] and [11] in the present context, we show that Conjecture B implies an affirmative answer to the second-named author's question concerning $\mathcal{R}(O_F G)$ (see Theorems 5.6 and 5.7 below):

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

When G is abelian, we obtain the following refinement of [9, Theorem 6.7] (see Theorem 5.8 below):

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

We also prove the following result, which may be viewed as being a Galois module analogue of a classical theorem of Scholz and Reichardt (see e.g. [13, Theorem 2.1.1]) on the inverse Galois problem for nilpotent groups (see Theorem 5.9 below):

Theorem E. *Suppose that* G *is a nilpotent, and that* $(|G^{ab}|, h_F) = 1$, *where* h_F *denotes the class number of* F. *If the order of* G *is even, we further suppose that* F *has no real places. Then Conjecture B holds, and so* $\mathcal{R}(O_F G)$ *is a subgroup of* $\mathrm{Cl}(O_F G)$.

Here is an outline of the rest of this paper. In Section 6, we explain a hitherto unpublished result of the second-named author that describes how resolvends of normal integral bases of tamely ramified local extensions admit certain *Stickelberger factorisations* (see Definition 6.7); this is a non-abelian analogue of Stickelberger's factorisation of abelian Gauss sums. In Section 7 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 [9, Theorem 2.14]).

In Section 8, we recall the definitions and properties of the Stickelberger pairing and Stickelberger homomorphism from [11], and we give a new description of the former (see Proposition 8.2) that is used to prove Proposition A. By using variants of the Stickelberger homomorphism taking values in relative algebraic K-groups, we give a proof of Theorem C in Section 9. In Section 10, we recall certain facts concerning embedding problems for nilpotent groups that are required for the proof of Theorem E. Finally, in Section 11, we complete the proof of Theorem E.

We are very grateful to Andrea Siviero for extremely detailed and helpful comments on an earlier draft of this paper.

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 local field, then O_L denotes the ring of integers of L.

Throughout this paper, F will denote a number field. For each finite 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}.

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 of H. 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 congugacy 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'.

For any group Γ upon which Ω_F acts continuously, we identify Γ-Galois algebras of F with elements of the set $Z^1(\Omega_F, G)$ of Γ-valued continuous 1-cocycles of Ω_F (see Section 2 below). If $\pi \in Z^1(\Omega_F, \Gamma)$, then we write F_π/F for the corresponding Γ-extension of F, and O_π for the integral closure of O_F in F_π. It may be shown that if $\pi_1, \pi_2 \in Z^1(\Omega_F, \Gamma)$, then $F_{\pi_1} \simeq F_{\pi_2}$ if and only if π_1 and π_2 differ by a coboundary. Every Γ-Galois algebra F_π is a Γ-torsor over F in the sense of [14, Chapter I, §5.2], and the set of isomorphism classes of Γ-Galois algebra extensions of F may be identified with the pointed cohomology set $H^1(F, \Gamma) := H^1(\Omega_F, \Gamma)$. We write $[\pi] \in H^1(F, \Gamma)$ for the class of F_π in $H^1(F, \Gamma)$, and we write $H^1_t(F, \Gamma)$ for the subset of $H^1(F, \Gamma)$ consisting of those $[\pi] \in H^1(F, \Gamma)$ for which F_π/F is at most tamely ramified. We denote the subset of $H^1_t(F, \Gamma)$ consisting of those $[\pi] \in H^1_t(F, \Gamma)$ for which F_π/F is everywhere unramified by $H^1_{nr}(F, \Gamma)$.

If A is any algebra, we write $Z(A)$ for the centre of A. If in addition 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. [6, Chapter II, §1]).

2. Galois algebras and resolvends

In this section we shall describe some basic facts concerning Galois algebras and resolvends.

2.1. **Galois algebras.** [9, Section 1], [2, Section 1]. Let Γ be any finite group upon which Ω_F acts continuously from the left, and write $Z^1(\Omega_F, \Gamma)$ for the set of Γ-valued continuous Ω_F 1-cocycles. If $\pi \in Z^1(\Omega_F, \Gamma)$, then we write ${}^{\pi}\Gamma$ for the set Γ endowed with the following modified action of Ω_F: if

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

is the identity map on the underlying sets, then

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

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

We define an associated Γ-Galois F-algebra F_{π} by

$$F_{\pi} := \mathrm{Map}_{\Omega_F}({}^{\pi}\Gamma, F^c);$$

this consists of the algebra of F^c-valued functions on ${}^{\pi}\Gamma$ that are fixed under the action of Ω_F. The algebra

$$A := (F^c\Gamma)^{\Omega_F}$$

acts on F_{π} via the rule

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

for all $\gamma \in \Gamma$ and $\alpha = \sum_{g \in G} \alpha_g \cdot g \in A$. It may be shown that every Γ-Galois F-algebra is isomorphic to an algebra of the form F_{π} for some π, and so every Γ-Galois F-algebra may be viewed as lying in the F^c-algebra $\mathrm{Map}(\Gamma, F^c)$. It is easy to check that

$$F_{\pi} \otimes_F F^c = F^c\Gamma \cdot \ell_{\Gamma},$$

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

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

This implies that F_{π} is a free, rank one A-module.

The Wedderburn decomposition of F_{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_F, and set

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

Then

$$F_\pi \simeq \prod_{\Omega_F \backslash {}^\pi\Gamma} F^\pi.$$

where $\Omega_F \backslash {}^\pi\Gamma$ denotes the set of Ω_F-orbits of ${}^\pi\Gamma$. In general, the field F^π is not normal over F. However, if Ω_F acts trivially on Γ, then $Z^1(\Omega_F, \Gamma) = \mathrm{Hom}(\Omega_F, \Gamma)$, and

$$F^\pi = (F^c)^{\mathrm{Ker}(\pi)}$$

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

$$F_\pi \simeq \prod_{\Gamma/\pi(\Omega_F)} F^\pi, \tag{2.1}$$

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

2.2. **Resolvends.** [9, Section 1] [2, Section 2].

Since every Galois algebra may be viewed as lying in $\mathrm{Map}(\Gamma, F^c)$, it is natural to consider the Fourier transforms of elements of $\mathrm{Map}(\Gamma, F^c)$. These arise via the *resolvend map*

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

The map $\mathbf{r}_\Gamma$ is an isomorphism of left $F^c\Gamma$-modules, but not of algebras, because it does not preserve multiplication. It is easy to show that for any $a \in \mathrm{Map}(\Gamma, F^c)$, we have that $a \in F_\pi$ if and only if $\mathbf{r}_\Gamma(a)^\omega = \mathbf{r}_\Gamma(a) \cdot \pi(\omega)$ for all $\omega \in \Omega_F$. It may also be shown that an element $a \in F_\pi$ generates F_π as an A-module if and only if $\mathbf{r}_\Gamma(a) \in (F^c\Gamma)^\times$. Two elements $a_1, a_2 \in \mathrm{Map}(\Gamma, F^c)$ with $\mathbf{r}_\Gamma(a_1), \mathbf{r}_\Gamma(a_2) \in (F^c\Gamma)^\times$ generate the same Γ-Galois F-algebra as an A-module if and only if $\mathbf{r}_\Gamma(a_1) = b \cdot \mathbf{r}_\Gamma(a_2)$ for some $b \in A^\times$. Every Galois Γ-algebra F_π is a Γ-torsor over F (see [14, Chapter I, §5.2]). If a is any generator of F_π as an A-module, then a Γ-valued Ω_F 1-cocycle that represents the class of F_π/F in the pointed cohomology set $H^1(F,\Gamma)$ is given by

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

Suppose that L is any extension of F, and set $A_L := A \otimes_F L$. We define

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

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

If v is a finite place of F, and L_v is any algebraic extension of F_v, write L_v^t for the maximal, tamely ramified extension of L_v. We set

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

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

3. Resolvends and cohomology

Recall that G is a finite group upon which Ω_F acts trivially. In this section, we explain, following [9, §2], how resolvends may be used to compute discriminants of rings of integers of G-Galois extensions of F, and how this may be applied to describe certain cohomology groups in terms of resolvends.

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

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

yields a trace map

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

via restriction. This in turn gives 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

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

where the symbol $[- : -]_{O_F}$ denotes the O_F-module index. We see from the isomorphism (2.1) that we have

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

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

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

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 $H^1(F, G)$, $\operatorname{Map}(G, F^c)$, 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*

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

Proof. This may be verified via a straightforward calculation (see e.g. [8, (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 $\operatorname{Tr}(a^s b^t) = \delta_{s,t}$.

(ii) $(O_FG \cdot a)^* = O_FG \cdot b$.

(iii) $[(O_FG \cdot a)^* : O_FG \cdot a]_{O_F} = [O_FG : O_FG \cdot \mathbf{r}_G(a) \cdot \mathbf{r}_G(a)^{[-1]}]_{O_F}$.

(iv) $r_G(a) \in (O_F^cG)^\times$ if and only if $O_\pi = O_FG \cdot a$ and $\operatorname{disc}(O_\pi/O_F) = O_F$.

Analogous results hold if F is replaced by F_v for any finite place v of F.

Proof. Exactly as in [9, 2.10 and 2.11]. □

Theorem 3.4. *(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 any finite place v of F.

Proof. When G is abelian, parts (a) and (b) are proved in [9, 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

$$1 \to G \to (O^c_{F_v}G)^\times \to (O^c_{F_v}G)^\times/G \to 1$$

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 [9, page 268]. Let us briefly describe the argument. Taking Ω_F-cohomology of the exact sequence (3.5) of pointed sets yields an exact sequence

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

and we wish to show that this sequence is surjective on the right. Suppose therefore, 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 required.

Part (b) follows from Corollary 3.3(iv) (cf. the proof of (2.12) on [9, page 273]).

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

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

and

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

respectively, using the argument given in [9, page 268] that we have described above. □

Recall that $Z(FG)$ denotes the centre of FG. Before stating our next result, we note that the reduced norm map

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

induces an injection $G^{ab} \to Z(FG)^\times$. In what follows, we shall identify G^{ab} with its image in $Z(FG)^\times$ under this map. For any extension L of F, 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 $\mathcal{H}(Z(\mathfrak{A}))$ analogously for any O_L-order $\mathfrak{A}$ in LG.

Proposition 3.5. *For any extension L of F, there is an exact sequence of abelian groups:*

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

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

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

and noting that $H^1(\Omega_L, Z(L^cG)^\times) = 0$, via Hilbert's Theorem 90. □

It follows from Theorem 3.4 and Proposition 3.5 that, for any extension L of F, 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:

$$\begin{tikzcd}
H^1(L,G) \arrow[r, "\sim"] \arrow[d] & (LG)^\times \backslash \mathcal{H}(LG) \arrow[d, "\mathrm{nrd}"] \\
H^1(L,G^{ab}) \arrow[r, "\sim"] & Z(LG)^\times \backslash \mathcal{H}(Z(LG)).
\end{tikzcd} \tag{3.8}$$

(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 5.

Proposition 3.6. *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), there is a commutative diagram

$$\begin{tikzcd}
H^1_{nr}(F_v,G) \arrow[r, "\sim"] \arrow[d] & (O_{F_v}G)^\times \backslash \mathcal{H}(O_{F_v}G) \arrow[d, "\mathrm{nrd}"] \\
H^1_{nr}(F_v,G^{ab}) \arrow[r] & Z(O_{F_v}G)^\times \backslash \mathcal{H}(Z(O_{F_v}G)).
\end{tikzcd} \tag{3.9}$$

The lower horizontal arrow is 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 result, it suffices to show that the left vertical arrow is surjective. That this is indeed the case is an immediate consequence of the fact that the Galois group $\mathrm{Gal}(F_v^{nr}/F_v)$ is topologically cyclic. □

4. 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 [1] and [17, Chapter 15] for some of the details that we omit.

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 finitely generated R-algebra satisfying $\mathfrak{A} \otimes_R L \simeq LG$.

Definition 4.1. 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 4.2. If F_π/F is any G-extension, and $\mathcal{L}_\pi \subseteq F_\pi$ is any projective O_FG-module, then $(\mathcal{L}_\pi, O_FG; \mathbf{r}_G)$ is a categorical F^c-twisted O_FG-form. In particular, if F_π/F is a tame G-extension, then $(O_\pi, O_FG; \mathbf{r}_G)$ is a categorical F^c-twisted O_FG-form. Similarly, if v is any place of F, then (still assuming

F_π/F to be tame) $(O_{\pi,v}, O_vG; \mathbf{r}_G)$ is a categorical F_v^c-twisted O_vG-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 $K_0(\mathfrak{A}, \Lambda)$. Recall (see [17, Theorem 15.5] that there is a long exact sequence of relative algebraic K-theory:

$$K_1(\mathfrak{A}) \to K_1(\mathfrak{A} \otimes_R \Lambda) \xrightarrow{\partial^1_{\mathfrak{A},\Lambda}} K_0(\mathfrak{A}, \Lambda) \xrightarrow{\partial^0_{\mathfrak{A},\Lambda}} K_0(\mathfrak{A}) \to K_0(\mathfrak{A} \otimes_R \Lambda). \quad (4.1)$$

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.

4.1. **Idelic description and localisation.** Let us retain the notation established above, and suppose in addition that we now work over our number field F. For each finite place v of F, the reduced norm map

$$\mathrm{nrd} : K_1(F_vG) \xrightarrow{\sim} Z(F_vG)^\times$$

is an isomorphism, and it is frequently convenient to identify $K_1(\mathfrak{A}_v)$ with its image in $K_1(F_vG)$ via this map. We write

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

for the obvious localisation map.

Definition 4.3. We define the idele group $J(K_1(FG))$ of $K_1(FG)$ to be the restricted direct product of the groups $K_1(F_vG)$ with respect to the subgroups $K_1(O_{F_v}G)$ for all finite places v of F. □

If E is any extension of F, then the homomorphism

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

induces a homomorphism

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

The following result is proved in [1, Theorem 3.5].

Theorem 4.4. *There is a natural isomorphism*

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

□

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 $h_{\mathfrak{A},E}([M, N; \lambda])$ may be described as follows.

For each finite place v of F, we choose $\mathfrak{A}_v$-bases m_v of M and n_v of N. 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 $n_v = \nu_v \cdot n_\infty$, wth $\nu_v \in (F_vG)^\times$. 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 $(\theta_E^{-1} \circ \xi)(n_\infty) = \nu_\infty \cdot n_\infty$ for some $\nu_\infty \in (EG)^\times$. Then a representative of $h_{\mathfrak{A},E}([M, N; \lambda])$ is given by the image of $[(\mu_v \cdot \nu_v^{-1})_v, \nu_\infty]$ in $J(K_1(FG)) \times K_1(EG)$.

Lemma 4.5. *Suppose that v is a finite place of F and that E_v is any extension of F_v. Then there is an isomorphism*

$$K_0(\mathfrak{A}_v, E_v) \simeq K_1(E_vG)/K_1(\mathfrak{A}_v).$$

Proof. This follows directly from the long exact sequence of relative K-theory (4.1) applied to $K_0(\mathfrak{A}_v, E_v)$. □

For each finite 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 4.4 and Lemma 4.5, the map λ_v is that induced by the homomorphism (which we denote by the same symbol λ_v)

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

Definition 4.6. We define the idele group $J(K_0(O_FG, F^c))$ of $K_0(O_FG, F^c)$ to be the restricted direct product of the groups $K_0(O_{F_v}G, F_v^c)$ with respect to the subgroups $K_0(O_{F_v}G, O_{F_v^c})$. □

Proposition 4.7. *(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) The image of λ lies in the idele group $J(K_0(O_FG, F^c))$.

Proof. (a) Suppose that $\alpha \in K_0(\mathfrak{A}, E)$ lies in the kernel of λ, and let $[(x_v)_v, x_\infty] \in J(K_1(FG)) \times K_1(EG)$ be a representative of α. Then for each v, we have that $x_v \cdot \mathrm{loc}_v(x_\infty) \in K_1(\mathfrak{A}_v)$. Hence, α is also represented by

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

This implies that $\mathrm{loc}_v(x_\infty) \in K_1(F_vG)$ for every v, whence it follows that $x_\infty \in K_1(FG)$. Hence we see that $\alpha = 0$ in $K_0(\mathfrak{A}, E)$, and so λ is injective, as claimed.

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

5. 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 5.1. We define maps Ψ and Ψ_v (for each finite place v of F) by

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

and

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

We set

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

□

Definition 5.2. We define the pointed set of ideles $J(H_t^1(F, G))$ of $H_t^1(F, G)$ to be the restricted direct product of the pointed sets $H_t^1(F_v, G)$ with respect to the pointed subsets $H_{nr}^1(F_v, G)$, and we write

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

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

In general, $K\mathcal{R}(O_F G)$ is not a subgroup of $K_0(O_F G, F^c)$. However, the following result holds.

Proposition 5.3. *Let v be any finite place of F, and write Ψ_v^{nr} for the restriction of Ψ_v to $H^1_{nr}(F_v, G)$. Then $\mathrm{Im}(\Psi_v)$ is a subgroup of $K_0(O_{F_v}G, F_v^c)$.*

Proof. This follows from Proposition 3.6 and Lemma 4.5. □

Definition 5.4. We say that an element $x \in K_0(O_F G, F^c)$ 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 finite places v of F. □

The long exact sequence of relative K-theory (4.1) applied to $K_0(O_F G, F^c)$ yields a long exact sequence

$$K_1(O_F G) \to K_1(F^c G) \xrightarrow{\partial^1} K_0(O_F G, F^c) \xrightarrow{\partial^0} \mathrm{Cl}(O_F G) \to 0, \tag{5.1}$$

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

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

and we write

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

The second-named author has conjectured that that $\mathcal{R}(O_F G)$ is always a subgroup of $\mathrm{Cl}(O_F G)$, and he has proved that this is true whenever G is abelian (see [9]). The following conjecture gives a precise characterisation of the image $K\mathcal{R}(O_F G)$ of Ψ.

Conjecture 5.5. An element of $K_0(O_F G, F^c)$ is cohomological if and only if it is locally cohomological. In other words, we have that

$$\lambda(K\mathcal{R}(O_F G)) = \mathrm{Im}(\lambda) \cap \mathrm{Im}(\Psi^{id}).$$

□

Let us now explain why Conjecture 5.5 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 [9] and [11].

Theorem 5.6. *Let*

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

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

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

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

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

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

This theorem will be proved in Section 9 . It implies the following result.

Theorem 5.7. *If Conjecture 5.5 holds, then* $\mathcal{R}(O_F G)$ *is a subgroup of* $\mathrm{Cl}(O_F G)$.

Proof. It follows from the exact sequence (5.1) 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 5.5 is true, then Theorem 5.6 implies that $\partial^1(K_1(F^c G)) \cdot K\mathcal{R}(O_F G)$ is the kernel of the homomorphism

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

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

Theorem 5.8. *Conjecture 5.5 is true when* G *is abelian.*

Proof. When G is abelian, the maps Ψ and Ψ^{id} are injective because the reduced norm map induces an isomorphism $(EG)^{\times} \simeq K_1(EG)$ for any extension E of F. Suppose that $x \in K_0(O_F G, F^c)$ is locally cohomological, and let $[(x_v)_v, x_\infty] \in J(FG) \times (F^c G)^{\times}$ be a representative of x. Then, for each v, we have that $x_v \cdot \operatorname{loc}_v(x_\infty) \in H_t(F_v G)$, and so it follows that $x_\infty \in H_t(FG)$. If π denotes the element of $\operatorname{Hom}(\Omega_F, G)$ afforded by x_∞, then $[\pi] \in H^1_t(F, G)$ and $x = \Psi([\pi])$. □

In Section 11 we shall prove the following result.

Theorem 5.9. *Suppose that G is a nilpotent group of and that $(|G^{ab}|, h_F) = 1$, where h_F denotes the class number of F. If $|G|$ is even, suppose also that F has no real places. Then Conjecture 5.5 holds.*

Theorem 5.7 therefore implies:

Corollary 5.10. *Under the hypotheses of Theorem 5.9, we have that $\mathcal{R}(O_F G)$ is a subgroup of $\operatorname{Cl}(O_F G)$.*

6. Local extensions

The goal of this section is to describe how resolvends of normal integral bases of tamely ramified local extensions admit *Stickelberger factorisations* (see Definition 6.7). 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 from 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^t (resp. F_v^{nr}) denotes the maximal tamely ramified (resp. unramified) extension of F_v. Then

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

The group $\Omega_v^{nr} := \mathrm{Gal}(F_v^{nr}/F_v)$ is topologically generated by the Frobenius element ϕ_v, and we have that

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

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

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

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

$$\phi_v \cdot \sigma_v \cdot \phi_v^{-1} = \sigma_v^{q_v}. \tag{6.1}$$

We set $\Omega_v^{\mathrm{tot}} := \mathrm{Gal}(F_v^t)/F_v^{nr}$.

Definition 6.1. 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 $c(s) \subseteq \Sigma_v(G)$. Let us also remark that if $s \in \Sigma_v(G)$, then the order $|s|$ of s is coprime to q_v.

If $s \in \Sigma_v(G)$, we set

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

and we define $\varphi_{v,s} \in \mathrm{Map}(G, O_{F_v^c})$ by setting

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

Then

$$\mathbf{r}_G(\varphi_{v,s}) = \sum_{i=0}^{|s|-1} \varphi_{v,s}(s^i) s^{-i} = \sum_{i=0}^{|s|-1} \sigma^i(\beta) s^{-i}. \tag{6.2}$$

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

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

and so

$$\mathrm{nrd}(\mathbf{r}_G(\varphi_{v,g^{-1}sg})) = \mathrm{nrd}(\mathbf{r}_G(\varphi_{v,s})), \tag{6.3}$$

i.e. the element $\mathrm{nrd}(\mathbf{r}_G(\varphi_{v,s}))$ depends only upon the conjugacy class $c(s)$ of s in G.

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 $\varphi_{v,s}$ are n.i.b. generators of tame (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 McCulloh's decomposition of resolvends of normal integral basis generators of L_π/L (see [11] and also [2, Section 6]). When G is abelian, this is an analogue 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 $\pi_r, \pi_{nr} \in \mathrm{Hom}(\Omega^t, G)$ by setting

$$\pi_r(\sigma^m \phi^n) = \pi(\sigma^m) = s^m,$$

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

If $\omega_i \in \Omega^t$ $(i = 1, 2)$ with $\omega_i = \sigma^{m_i} \cdot \phi^{n_i}$, then a straightforward calculation using (6.1) shows that

$$\omega_1 \cdot \omega_2 = s^{m_1 + q^{m_1 m_2}} \cdot t^{m_1 + m_2}.$$

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

$$\pi(\omega) = \pi_r(\omega) \cdot \pi_{nr}(\omega) \tag{6.4}$$

for every $\omega = \phi^n \cdot \sigma^n \in \Omega^t$. The map $\pi_{nr} \in \mathrm{Hom}(\Omega^{nr}, G)$ corresponds to an unramified Galois G-extension $L_{\pi_{nr}}$ of L. 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)).

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 $\omega \in \Omega_L$ and $g \in G$.)

Lemma 6.2. *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 $\pi, \pi_{nr} \in \mathrm{Hom}(\Omega^t, G)$ 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 6.3. We write ${}^{\pi_r}G(\pi_{nr})$ for the group 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 6.2 implies that if $\omega_1, \omega_2 \in \Omega^t$, then

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

We set

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

The algebra $(L^cG(\pi_{nr}))^{\Omega^t}$ 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 $\alpha = \sum_{g \in G} \alpha_g \cdot g \in (L^cG(\pi_{nr}))^{\Omega^t}$.

Proposition 6.4. *(a) 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 [2, Lemma 6.6], which is in turn an analogue of [9, 5.4].

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

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

may be identified with a subfield of L^t via identifying $b \in L^H$ 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 $\mathfrak{A}(\pi_{nr})_H := (O_{L^c}H)^{\Omega^t}$, then for each integer k with $0 \leq k \leq e-1$, it is not hard to check that

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

and so we see that

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

A straightforward computation (cf. [9, 5.4]) also shows that

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

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

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

as claimed.

□

Corollary 6.5. *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 6.4 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 6.6. *If $a_{nr} \in L_{\pi_{nr}}$ is any n.i.b. generator of $L_{\pi_{nr}}/L$, then the element $a \in L_\pi$ defined by*

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

is an n.i.b. 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 [9, (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 (2.1)) that we may write $L_\pi \simeq \oplus_{G/\pi(\Omega^t)} L^\pi$, 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

$$\mathrm{disc}(O_\pi / O) = \varpi^{(|s|-1)|G|/|s|} \cdot O_L. \tag{6.5}$$

Now $\mathbf{r}_G(a_{nr}) \in (O_{L^{nr}} G)^\times$, and we see from the proof of Proposition 6.4(b) and 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

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

it follows that

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

and this establishes the desired result. □

Definition 6.7. Let a be any n.i.b. generator of L_π/L. Theorem 6.6 implies that we may write

$$\mathbf{r}_G(a) = u \cdot \mathbf{r}_G(a_{nr}) \cdot \mathbf{r}_G(\varphi_s), \tag{6.6}$$

where $u \in (OG)^\times$ and a_{nr} is any n.i.b. generator of $L_{\pi_{nr}}/L$. This may be viewed as being a non-abelian analogue of Stickelberger's factorisation of abelian Gauss sums, and so we call (6.6) a *Stickelberger factorisation* of $\mathbf{r}_G(a)$. □

7. Determinants and character maps

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

We first recall that the absolute Galois group Ω_F of F acts on the ring R_G of virtual characters of G according to the following rule: if $\chi \in \operatorname{Irr}(G)$ and $\omega \in \Omega_F$, then, for each $g \in G$, we have $(\omega \circ \chi)(g) = \omega(\chi(\omega^{-1}(g)))$.

Definition 7.1. For each element a of $\mathrm{GL}_n(F^cG)$, we define an element

$$\operatorname{Det}(a) \in \operatorname{Hom}_{\Omega_F}(R_G, (F^c)^\times) \simeq Z(FG)^\times$$

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

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

It may be shown that this definition depends only upon the character ϕ, and not upon the choice of representation T. (See [6, Chapter II], for example.) □

Remark 7.2. The map Det above is essentially the same as the reduced norm map. Let

$$\mathrm{nrd} : (F^c G)^\times \to Z(F^c G)^\times \tag{7.1}$$

denote the reduced norm. If G is abelian, then (7.1) is an isomorphism; in general, (7.1) induces an isomorphism

$$\mathrm{nrd} : K_1(F^c G) \to Z(F^c G)^\times \simeq \mathrm{Hom}(R_G, (F^c)^\times).$$

Suppose now that ϕ is any F^c-valued character of G, and let $a \in (F^c G)^\times$. Then we have that

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

(see [7, Chapter I, Proposition 2.7]). A similar result holds if $(F^c G)^\times$ is replaced by $(F^c_v G)^\times$ for any place v of F.

If v is any finite place of F, and $\mathcal{M}_v$ is a maximal order in $F_v G$ containing $O_{F_v} G$, then we have

$$\mathrm{nrd}(\mathcal{M}_v^\times) = Z(\mathcal{M}_v)^\times \simeq \mathrm{Hom}_{\Omega_{F_v}}(R_G, (O^c_{F_v})^\times). \tag{7.2}$$

We shall make frequent use of these facts in what follows. □

Definition 7.3. 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 F^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 $R_G \to \mathrm{Irr}(G^{ab})$ by defining

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

and we set

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

Hence we have an exact sequence of groups

$$0 \to A_G \to R_G \xrightarrow{\det} \mathrm{Irr}(G^{ab}) \to 0. \tag{7.3}$$

□

Applying the functor $\mathrm{Hom}(-,(F^c)^\times)$ to (7.3), we obtain the sequence

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

which is exact on the right because $(F^c)^\times$ is divisible. It follows that there is an Ω_F-equivariant isomorphism

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

A similar argument with F replaced by F_v for any finite place v of F yields an analogous Ω_{F_v}-equivariant isomorphism

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

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

Recall that if v is a finite place of F, of residue characteristic coprime to $|G|$, then $O_{F_v}G$ is a maximal order in F_vG, and we have that

$$\mathrm{Det}((O_{F_v}^cG)^\times) = \mathrm{Hom}(R_G,(O_{F_v}^c)^\times),$$

and

$$\mathrm{Det}(\mathcal{H}(O_{F_v}G)) = Z(O_{F_c^v}G)/G^{ab} = \mathrm{Hom}_{\Omega_{F_v}}(A_G,(O_{F_v}^c)^\times).$$

On the other hand, if v is not coprime to $|G|$, then we have

$$\mathrm{Det}(\mathcal{H}(O_{F_v}G)) = Z(O_{F^v_c}G)/G^{ab} \subseteq \mathrm{Hom}_{\Omega_{F_v}}(A_G, (O^c_{F_v})^\times),$$

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

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

and write $U_\alpha(O^c_{F_v})$ instead of $U_{\mathfrak{a}}(O^c_{F_v})$ when $\mathfrak{a} = \alpha O_F$. We shall need the following result of Siviero (which is variant of [9, Theorem 2.14]) in Section 8 .

Proposition 7.4. *(Siviero) If N is any sufficiently large power of $|G|$, then*

$$\mathrm{Hom}_{\Omega_{F_v}}(A_G, U_N(O^c_{F_v})) \subseteq \mathrm{Det}((O_{F_v}G)^\times/G) \subseteq \mathrm{Hom}_{\Omega_{F_v}}(A_G, (O^c_{F_v})^\times)$$

for all finite places v of F.

Proof. This is shown in [16, Theorem 5.1.10] when G is abelian, and the proof for arbitrary finite G is quite similar.

We first observe that the group

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

is annihilated by $|G^{ab}|[\mathrm{Det}(\mathcal{M}_v^\times) : (O_{F_v}G)^\times]$, where $\mathcal{M}_v$ denotes any 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 $\mathrm{Hom}_{\Omega_{F_v}}(A_G, (O^c_{F_v})^\times)$ and so is an open subgroup of $\mathrm{Hom}_{\Omega_{F_v}}(A_G, (O^c_{F_v})^\times)$. The result now follows from the fact that the groups $\mathrm{Hom}_{\Omega_{F_v}}(A_G, U_n(O^c_{F_v}))$ form a fundamental system of neighbourhoods of the identity of $\mathrm{Hom}_{\Omega_{F_v}}(A_G, (O^c_{F_v})^\times)$ as n varies.

□

8. The Stickelberger pairing and homomorphism

Definition 8.1. The *Stickelberger pairing* is a $\mathbf{Q}$-bilinear pairing

$$\langle -, - \rangle : \mathbf{Q}R_G \times \mathbf{Q}G \to \mathbf{Q} \tag{8.1}$$

that is defined as follows.

Let $\zeta_{|G|}$ be a fixed, primitive $|G|$-th root of unity (cf. the conventions established at the begining of Section 6), and suppose first that G is abelian. Then if $\chi \in \mathrm{Irr}(G)$ and $g \in G$, we may write $\chi(g) = \zeta_N^r$ for some integer r. We define

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

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

$$\langle \chi, g \rangle = \langle \mathrm{Res}_G^{<g>}(\chi), g \rangle.$$

□

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 write $|s|$ for the order of s, and 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 characters of $\langle s \rangle$. Then it follows from Definition 8.1 that

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

Define

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

Proposition 8.2. *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. □

Corollary 8.3. *Suppose that s_1 and s_2 are elements of G. Then $\langle \chi, s_1\rangle = \langle \chi, s_2\rangle$ for all $\chi \in R_G$ if and only if $c(s_1) = c(s_2)$.*

Proof. 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 $\langle \chi, s \rangle$ depends only upon the conjugacy class of s in G. Hence, if $c(s_1) = c(s_2)$, then $\langle \chi, s_1 \rangle = \langle \chi, s_2 \rangle$ for all $\chi \in R_G$.

To show the converse, we use Proposition 8.2. We first note that a straightforward computation shows that the degree of the virtual character $\Xi(s)$ is equal to $|G|(|s|-1)/2|s|$, and so $\Xi(s)$ determines $|s|$.

To ease notation, set $H := \langle s \rangle$, and let M be a $\mathbf{Z}H$-module with character $|s| \cdot \Xi(s)$. Let $t_1 = \mathbf{1}, \dots, t_{m_s}$ be a set of coset representatives of G/H. Then $\oplus_{i=1}^{m_s} t_i M$ is a $\mathbf{Z}G$-module with character $|s| \cdot \mathrm{Ind}_H^G(\Xi(s))$, and G acts transitively on the set $\{t_1 M = M, \dots, t_{|s|}M\}$. Since the stabiliser of M is H, this last set is isomorphic to G/H as a G-set, and so it follows that $\Xi(s)$ determines the G-set G/H.

Hence if $\langle \chi, s_1 \rangle = \langle \chi, s_2 \rangle$ for all $\chi \in R_G$, then Proposition 8.2 implies that

$$\mathrm{Ind}_{\langle s_1 \rangle}^G \Xi(s_1) = \mathrm{Ind}_{\langle s_2 \rangle}^G \Xi(s_2),$$

and so $G/\langle s_1 \rangle \simeq G/\langle s_2 \rangle$ as G-sets, whence $c(s_1) = c(s_2)$, as claimed. □

Definition 8.4. The *Stickelberger map*

$$\Theta = \Theta_G : \mathbf{Q}R_G \to \mathbf{Q}G \tag{8.2}$$

is defined by

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

□

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

Proposition 8.5. *(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) We have that $\Theta(\chi) \in \mathbf{Z}G$ if and only if $\chi \in A_G$. Hence Θ induces a homomorphism $A_G \to \mathbf{Z}G$.

(c) Let $G(-1)$ denote the group G endowed with an action of Ω_F via the inverse cyclotomic character. Then the map

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

is Ω_F-equivariant.

Proof. The proofs of these assertions are essentially the same as those in the case of abelian G. See [9, 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 $\langle \chi, g \rangle$ depends only on 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

$$\mathrm{res}_G^{<g>}(\chi) = \sum_\eta a_\eta \eta,$$

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

$$\begin{aligned}(\det(\chi))(g) &= \det(\mathrm{res}_G^{<g>}(\chi))(g) \\ &= \prod_\eta \eta(g)^{a_\eta} \\ &= \prod_\eta \zeta_{|g|}^{|g|\langle a_\eta, g\rangle} \\ &= \zeta_{|g|}^{|g|\sum_\eta \langle a_\eta \eta, g\rangle} \\ &= \zeta_{|g|}^{|g|\sum_\eta \langle \mathrm{res}_G^{<g>}(\chi), g\rangle}.\end{aligned}$$

It now follows that $\langle \mathrm{res}_G^{<g>}(\chi), g\rangle \in \mathbf{Z}$ 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

$$\langle \chi^{\omega}, g \rangle = \langle \chi, g^{\kappa(\omega)} \rangle. \tag{8.3}$$

It follows via bilinearity that (8.3) holds for all $\chi \in R_G$ and all $g \in G$. Hence, if we view $\Theta_G(\chi)$ as being an element of $\mathbf{Q}G(-1)$, then

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

□

We see from Proposition 8.5 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*

$$\Theta^t : \mathrm{Hom}(Z(\mathbf{Z}G(-1)), (F^c)^{\times}) \to \mathrm{Hom}(A_G, (F^c)^{\times}). \tag{8.4}$$

Composing (8.4) with the homomorphism

$$\mathrm{Hom}(A_G, (F^c)^{\times}) \xrightarrow{\sim} Z(F^cG)^{\times}/G^{ab} \to \frac{K_1(F^cG)}{K_1(O_FG)} \to K_0(O_FG, F^c)$$

yields an Ω_F-equivariant homomorphism

$$K\Theta^t : \mathrm{Hom}(Z(\mathbf{Z}G(-1)), (F^c)^{\times}) \to K_0(O_FG, F^c). \tag{8.5}$$

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

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

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

$$\Theta_v^t : \mathrm{Hom}(Z(\mathbf{Z}G(-1)), (F_v^c)^\times) \to \mathrm{Hom}(A_G, (F_v^c)^\times) \tag{8.6}$$

and

$$K\Theta_v^t : \Lambda(F_vG)^\times \to K_0(O_{F_v}G, F_v^c) \tag{8.7}$$

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

For all places v of F not dividing the order of G, we have that

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

and so

$$K\Theta^t(\Lambda(O_{F_v}G)) \subseteq K_0(O_{F_v}G, O_{F_v^c}).$$

It follows that the homomorphisms Θ_v^t combine to yield an idelic transpose Stickelberger homomorphism

$$K\Theta^t : J(\Lambda(FG)) \to J(K_0(O_F G, F^c)). \tag{8.8}$$

Definition 8.7. 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

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

by

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

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

Set

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

The *modified ray class group modulo* $\mathfrak{a}$ of $\Lambda(O_F G)$ is defined by

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

□

Remark 8.8. 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

$$\Lambda(FG) = \mathrm{Map}_{\Omega_F}(\mathcal{C}(G(-1)), F^c) \simeq \prod_{t \in T} F(t), \tag{8.9}$$

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

The group $\mathrm{Cl}'_{\mathfrak{a}}(\Lambda(O_F G))$ above is finite, and is isomorphic to the product of the ray class groups modulo $\mathfrak{a}$ of the Wedderburn components $F(t)$ of $\Lambda(FG)$ with $t \neq \mathbf{1}$. □

Definition 8.9. Let v be a finite place of F. For each element s of $\Sigma_v(G)$, define $f_{v,s} \in (\Lambda(F_vG))^\times$ by

$$f_{v,s}(c) = \begin{cases} \varpi_v, & \text{if } c = c(s) \neq 1; \\ 1, & \text{otherwise.} \end{cases} \tag{8.10}$$

Observe that we have $f_{v,1} = 1$, and 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.

Write

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

and define $\mathbf{F} \subset J(\Lambda(FG))$ by

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

Proposition 8.10. *Let $\mathfrak{A}$ be any integral ideal of O_F. Then the inclusion $\mathbf{F} \to J(\Lambda(FG))$ induces a surjection $\mathbf{F} \to \mathrm{Cl}'_{\mathfrak{A}}(\Lambda(O_FG))$.*

Proof. Let $I(\Lambda(O_FG))$ denote the group of fractional ideals of $\Lambda(O_FG)$. Then via the Wedderburn decomposition (8.9) of $\Lambda(FG)$, we see that each ideal $\mathfrak{B}$ in $\Lambda(O_FG)$ 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 $\nu \in J(F\Lambda)$, let $\mathrm{co}(\nu) \in I(\Lambda(O_FG)$ denote the ideal obtained by taking the idele content of ν. If v is a finite place of F, we view $\mathbf{F}_v$ as being a subset of $\mathbf{F}$ via the obvious embedding $\Lambda(F_vG)^\times \subseteq J(\Lambda(FG))$, and we set

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

Now 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. [9, 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 $f_{v,s} \in F_v$ for all $c(s) \in o(t)$.

We therefore deduce that the set $\mathcal{F}_v$ consists precisely of the invertible prime ideals $\mathfrak{p} = (\mathfrak{p}_t)_{t \in T}$ of Λ 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 ray class modulo $\mathfrak{A}$ of $F(t)$ contains infinitely many primes of degree one, and this implies that $\mathbf{F}$ surjects onto $\mathrm{Cl}'_{\mathfrak{A}}(\Lambda)$ as claimed. □

Proposition 8.11. *Let v be a finite place of F.*

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

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

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

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

$$\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s_1})) = \mathrm{Det}(\mathbf{r}_G(\varphi_{v,s_2})). \tag{8.11}$$

Then $c(s_1) = c(s_2)$.

Proof. (a) The proof of this assertion is very similar to that of [9, Proposition 5.4].

It suffices to show that

$$r_G(\varphi_{v,s}) = \Theta_v^t(f_{v,s})$$

Suppose that $\chi \in R_G$, and write

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

where the sum is over irreducible characters η of $< s >$. Using (6.2), we see that (cf. [9, Proposition 5.4])

$$\begin{aligned}\mathbf{r}_G(\varphi_{v,s})(\chi) &= \prod_{\psi} \left(\sum_{i=0}^{e-1} \sigma_v^i(\beta_s)\eta(s^{-i}) \right)^{a_\eta} \\ &= \varpi_v^{\langle \sum_\eta \eta, s\rangle} \\ &= \varpi_v^{\langle \chi, s\rangle},\end{aligned}$$

and so it follows that

$$\mathbf{r}_G(\varphi_{v,s})(\alpha) = \varpi_v^{\langle \alpha, s\rangle}$$

for all $\alpha \in A_G$.

On the other hand, if $\alpha \in A_G$, then we have

$$\begin{aligned}(\Theta^t(f_{v,s}))(\alpha) &= f_{v,s}(\Theta(\alpha)) \\ &= f_{v,s}\left(\sum_{g \in G} \langle \alpha, g\rangle g \right) \\ &= \prod_{g \in G} f_{v,s}(g)^{\langle \alpha, g\rangle} \\ &= \varpi_v^{\langle \alpha, s\rangle},\end{aligned}$$

and so the desired result follows.

(b) The proof of (a) above shows that if (8.11) holds, then

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

for every $\chi \in R_G$. It follows from Corollary 8.3(b) that $c(s_1) = c(s_2)$. □

Our next result concerns the kernels of the maps Ψ and Ψ_v. Before stating it, we recall that G' denotes the derived subgroup of G, and we 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

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

Proposition 8.12. *Let S be the set of all finite places of F such that v divides $|G'|$ and $F/\mathbf{Q}$ is wildly ramified at v.*

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

(b) If $v \notin S$, then $\ker(\Psi_v) = H^1_{nr}(F_v, G')$*.*

(c) We have that $\ker(\Psi) \subseteq H^1_{nr}(F, G')$*. In particular,* $\ker(\Psi)$ *is finite.*

Proof. (a) Suppose that $[\pi_v] \in H^1_t(F_v, G)$, and that $O_{\pi_v} = O_{F_v}G \cdot a_v$. Then it follows from the definition of Ψ_v that $\Psi_v([\pi_v]) = 0$ if and only if $\mathrm{nrd}(\mathbf{r}_G(a_v)) \in \mathrm{nrd}(K_1(O_{F_v}G))$. We see from (6.6) and Proposition 8.11 that $\mathrm{nrd}(\mathbf{r}_G(a_v)) \in \mathrm{nrd}(K_1(O_{F_v}G))$ only if $[\pi_v] \in H^1_{nr}(F_v, G)$. Furthermore, if $\Psi_v([\pi_v]) = 0$, then for each $\omega \in \Omega_{F_v}$, we have that $\mathbf{r}_G(a_v)^{-1} \cdot \mathbf{r}_G(a_v)^{\omega} \in G'$, which in turn implies that $[\pi_v] \in H^1_{nr}(F_v, G')$. This establishes (a).

(b) If $[\pi_v] \in H^1_{nr}(F_v, G')$, then $\mathbf{r}_G(a_v) \in H(O_{F_v}G)$, and for every $\omega \in \Omega_{F_v}$, we have that $\mathbf{r}_G(a_v)^{-1} \cdot \mathbf{r}_G(a_v)^{\omega} \in G'$. Hence $\mathrm{nrd}(\mathbf{r}_G(a_v))$ lies in $(\mathrm{nrd}(O_{F_v^{nr}}G')^{\times})^{\Omega_{F_v}}$. It follows from M. J. Taylor's fixed point theorem for group determinants (see [18, Chapter VIII]) that

$$(\mathrm{nrd}(O_{F_v^{nr}}G')^{\times})^{\Omega_{F_v}} = \mathrm{nrd}(O_{F_v}G')^{\times},$$

except possibly when both v divides $|G'|$ and $F/\mathbf{Q}$ is wildly ramified at v. Hence, if $v \notin S$, and $[\pi_v] \in H^1_{nr}(F_v, G')$ we see that $\Psi_v([\pi_v]) = 0$, as claimed.

(c) Suppose that $[\pi] \in H^1(F, G)$ satisfies $\Psi([\pi]) = 0$. Then $\Psi_v(\mathrm{loc}_v([\pi])) = 0$ for each 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. This implies the result. □

9. Proof of Theorem 5.6

In this section we shall prove Theorem 5.6. Recall that we wish to show that if

$$\overline{\Psi^{id}} : J(H^1_t(F,G)) \to \frac{J(K_0(O_FG, F^c))}{\lambda \circ \partial^1(K_1(F^cG)) \cdot \prod_v \mathrm{Im}(\Psi^{nr}_v)}$$

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

$$J(K_0(O_FG, F^c)) \to \frac{J(K_0(O_FG, F^c))}{\lambda \circ \partial^1(K_1(F^cG)) \cdot \prod_v \mathrm{Im}(\Psi^{nr}_v)},$$

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

We see from Theorem 6.6 and Proposition 8.11(a) that the desired result will follow if we show that the image $\iota(K\Theta^t(\mathbf{F}))$ of $K\Theta^t(\mathbf{F})$ in

$$\frac{J(K_0(O_FG, F^c))}{\lambda \circ \partial^1(K_1(F^cG)) \cdot \prod_v \mathrm{Im}(\Psi^{nr}_v)}$$

is a group.

To show this last fact, we first observe that Proposition 7.4 implies that if N is any sufficiently large power of $|G|$ and v is any finite place of F with $v \mid |G|$, then, setting $\mathfrak{a} := NO_F$, we have

$$\Theta^t(U'_{\mathfrak{a}}(\Lambda(O_{F_v}G))) \subseteq \mathrm{Det}((O_{F_v}G)^\times/G) \subseteq \mathrm{Det}(\mathcal{H}(O_{F_v}G)) = \mathrm{Im}(\Psi^{nr}_v).$$

Since for any v with $v \nmid |G|$ we have

$$\Theta^t(\Lambda(O_{F_v}G)) \subseteq \mathrm{Det}(\mathcal{H}(O_{F_v}G)) = \mathrm{Im}(\Psi^{nr}_v),$$

it follows that

$$K\Theta^t(U'_{\mathfrak{a}}(\Lambda(O_FG))) \subseteq \prod_v \mathrm{Im}(\Psi^{nr}_v)$$

in $J(K_0(O_FG, F^c))$, and so $K\Theta^t$ induces a homomorphism

$$K\Theta^t_{\mathfrak{a}} : \mathrm{Cl}'_{\mathfrak{a}}(\Lambda(O_FG)) \to \frac{J(K_0(O_FG, F^c))}{\lambda \circ \partial^1(K_1(F^cG)) \cdot \prod_v \mathrm{Im}(\Psi^{nr}_v)}.$$

Proposition 8.10 implies that

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

and so we see that $\iota(K\Theta^t(\mathbf{F}))$ is indeed a group, as claimed. □

10. An embedding problem

In this section we shall describe, following [14, §2.1], a solution to a certain embedding problem for nilpotent groups that will be used in the proof of Theorem 5.9.

Let G be a nilpotent group, and let l be the smallest prime dividing the order of G. If $l = 2$, we also assume that F is totally imaginary. Let C be a central subgroup of G of order l, and set $\overline{G} := G/C$. Recall that, for each finite place v of F, we write I_v for the inertia subgroup of Ω_{F_v}. Suppose that $\pi \in \mathrm{Hom}(\Omega_F, \overline{G})$ with $[\pi] \in H^1_t(F, \overline{G})$. We first show that, under our given hypotheses, π may always be lifted to an element of $\mathrm{Hom}(\Omega_F, G)$.

Lemma 10.1. *(*[14, Lemma 2.1.5]*) Let $\xi \in H^2(F, \overline{G})$ denote the class of the extension*

$$1 \to C \to G \xrightarrow{q} \overline{G} \to 1,$$

and write $\pi^* : H^2(\overline{G}, C) \to H^2(F, C)$ for the homomorphism induced by π. Then $\pi^*(\xi) = 0$, and so there exists a lift of π to $\mathrm{Hom}(\Omega_F, G)$*.*

Proof. We first observe that the restriction map

$$H^2(F, C) \to H^2(F(\mu_l), C)$$

is injective and so so we may without loss of generality assume that $F = F(\mu_l)$. Next, we note that the Brauer-Hasse-Noether theorem implies that the natural map

$$H^2(F, C) \to \prod_v H^2(F_v, C)$$

(where the product is over all finite places of v—the infinite places may be ignored when l is odd or F has no real places) is injective. Hence, in order to show that $\pi^*(\xi) = 0$, it suffices to show that each local homomorphism $\pi_v \in \mathrm{Hom}(\Omega_{F_v}, \overline{G})$ may be lifted to $\mathrm{Hom}(\Omega_{F_v}, G)$. To show that such local liftings exist, we may without loss of generality further suppose that the order of G is a power of l.

If π_v is unramified, then π_v factors through $\Omega_{F_v}/I_v \simeq \hat{\mathbf{Z}}$, and a map $\hat{\mathbf{Z}} \to \overline{G}$ may always be lifted to a map $\hat{\mathbf{Z}} \to G$ by lifting the image of a generator of $\hat{\mathbf{Z}}$.

If π_v is ramified, then by hypothesis, π_v is tamely ramified, and so π_v factors through a Galois group $\mathrm{Gal}(E/F_v)$, where E/F_v is tame, and $\mathrm{Gal}(E/F_v)$ is abelian of type (l^m, l^m) for some integer m; this last group is a projective object in the category of abelian groups annihilated by l^m. It therefore follows that $q^{-1}(\overline{G})$ is abelian and annihilated by l^m, and that π_v may be lifted (see [14, pages 14–15]). □

Lemma 10.2. *(cf.* [14, Lemma 2.1.6]*) For each finite place v of F, let $\varepsilon_v \in \mathrm{Hom}(\Omega_{F_v}, C)$. Suppose that almost all of the homomorphisms ε_v are unramified. Then there exists $\varepsilon \in \mathrm{Hom}(\Omega_F, C)$ such that*

$$\varepsilon|_{I_v} = \varepsilon_v|_{I_v}$$

for all v.

Proof. We may view the homomorphisms ε_v as being homomorphisms $\varepsilon_v : F_v^\times \to C$, via local class field theory. Each map $\varepsilon_v|_{O_{F_v}^\times}$ is trivial on a closed subgroup of the form $1 + \varpi_v^{n_v} O_{F_v}$, and almost all of the integers n_v are equal to zero. For each v, let $\mathfrak{p}_v$ denote the prime ideal of O_F corresponding to v, and set $\mathcal{N} := \prod_v \mathfrak{p}_v^{n_v}$. We define ε to be the Galois character associated to the homomorphism

$$\tilde{\varepsilon} : (O_F/\mathcal{N})^\times \to C; \quad \alpha \mapsto \prod_v \varepsilon_v(\alpha^{-1});$$

then it follows via class field theory that $\varepsilon\,|_{I_v} = \varepsilon_v\,|_{I_v}$ for each v, as desired. □

For each place v of F, let $\tilde{\pi}_v \in \mathrm{Hom}(\Omega_{F_v}, G)$ be a lift of π_v chosen so that $\tilde{\pi}_v$ is unramified if π_v is unramified. (Such a choice is always possible because there is no obstruction to lifting an element of $\mathrm{Hom}(\hat{\mathbf{Z}}, \overline{G})$—cf. the proof of Lemma 10.1.)

Proposition 10.3. *With the above hypotheses and notation, there exists* $\Pi \in \mathrm{Hom}(\Omega_F, G)$ *with* $[\Pi] \in H^1_t(F, G)$ *such that* Π *is a lift of* π *and*

$$\Pi|_{I_v} = \tilde{\pi}_v|_{I_v}$$

for each finite place v of F. (Hence Π *is unramified at every finite place of F at which π is unramified.)*

Proof. As $[\pi] \in H^1_t(F, \overline{G})$, Lemma 10.1 implies that we may choose a lifting $\tilde{\Pi} \in \mathrm{Hom}(\Omega_F, G)$ of π. For each place v of F, let $\tilde{\pi}_v \in \mathrm{Hom}(\Omega_{F_v}, G)$ be a lift of π_v chosen so that $\tilde{\pi}_v$ is unramified if π_v is unramified. (Such a choice is always possible because there is no obstruction to lifting an element of $\mathrm{Hom}(\hat{\mathbf{Z}}, \overline{G})$—cf. the proof of Lemma 10.1.)

As C is central in G, it is easy to see that for every v, there exists a homomorphism $\varepsilon_v : \Omega_{F_v} \to C$ such that $\tilde{\Pi}(\alpha) = \varepsilon_v(\alpha)\tilde{\pi}_v(\alpha)$ for all $\alpha \in \Omega_{F_v}$. Lemma 10.2 implies that there exists a homomorphism $\varepsilon : \Omega_F \to C$ such that $\varepsilon|I_v = \varepsilon_v|I_v$ for all v. Hence, if we set $\Pi := \tilde{\Pi} \cdot \varepsilon^{-1}$, then it follows that Π is unramified at every finite place of F at which π is unramified, and that

$$\Pi|_{I_v} = \tilde{\pi}_v|_{I_v}$$

for all v, as required. □

11. Proof of Theorem 5.9

In this section we shall prove Theorem 5.9.

Let G be a nilpotent group, and let l be the smallest prime dividing $|G|$. If $l = 2$, assume also that F has no real places. Let C be a central subgroup of

G of order l, and set $\overline{G} := G/C$. We may assume by induction on the order of G that Theorem 5.9 holds for $\overline{G}$.

Suppose that $x \in K_0(O_F G, F^c)$ is locally cohomological. Then, for each v, we may write

$$\lambda_v(x) = \Psi_{G,v}([\pi_v(x)])$$

for some $[\pi_v(x)] \in H^1_t(F_v, G)$. The choice of $\pi_v(x)$ is not unique. However, if $a(\pi_v(x))$ is any n.i.b. generator of $F_{\pi_v(x)}/F_v$, with Stickelberger factorisation (see Definition 6.7)

$$\mathbf{r}_G(a(\pi_v(x))) = u(\pi_v(x)) \cdot \mathbf{r}_G(a_{nr}(\pi_v(x))) \cdot \mathbf{r}_G(\varphi(\pi_v(x))),$$

then $\mathrm{Det}(\mathbf{r}_G(\varphi(\pi_v(x))))$ is independent of the choice of $\pi_v(x)$. Hence, if $\varphi(\pi_v(x)) = \varphi_{v,s}$, say, then $c(s)$ does not depend upon $\pi_v(x)$.

Write

$$q_1 : K_0(O_F G, F^c) \to K_0(O_F \overline{G}, F^c), \quad q_2 : H^1(F, G) \to H^1(F, \overline{G}),$$
$$q_{2,v} : H^1(F_v, G) \to H^1(F_v, \overline{G}),$$

for the maps induced by the quotient map $q : G \to \overline{G}$. Set

$$\overline{x} := q_2(x), \quad \pi_v(\overline{x}) := q_{2,v}(\pi_v(x)).$$

Then $\overline{x} \in K_0(O_F \overline{G}, F^c)$ is locally cohomological, with

$$\lambda_v(\overline{x}) = \Psi_{\overline{G},v}(q_{2,v}(\pi_v(x)))$$

for each finite place v of F. By induction, $\overline{x}$ is globally cohomological, and so there exists $[\rho(\overline{x})] \in H^1_t(F, \overline{G})$ such that

$$\Psi_{\overline{G},v}([\rho_v(\overline{x})]) = \Psi_{\overline{G},v}([\pi_v(\overline{x})])$$

for each v. Hence, for each v, we have that

$$\mathrm{Det}(\mathbf{r}_{\overline{G}}(\varphi(\rho_v(\overline{x})))) = \mathrm{Det}(\mathbf{r}_{\overline{G}}(\varphi(\pi_v(\overline{x})))),$$

using the notation established above concerning Stickelberger factorisations.

For each v, we shall now construct a lift $\rho_v(x) \in \mathrm{Hom}(\Omega_{F_v}, G)$ of $\rho_v(\overline{x})$ such that

$$\mathrm{Det}(\mathbf{r}_G(\varphi(\rho_v(x)))) = \mathrm{Det}(\mathbf{r}_G(\varphi(\pi_v(x)))).$$

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 that $\varphi_v(\rho_v(\overline{x})) = \varphi_{v,\overline{s}_1}$ for some $s_1 \in G$ with $c(s_1) = c(s)$. Next, we write

$$\rho_v(\overline{x}) = \rho_v(\overline{x})_r \cdot \rho_v(\overline{x})_{nr},$$

with $\rho_v(\overline{x})_{nr} \in H^1_{nr}(F_v, \overline{G})$ (see (6.4)). Since $\rho_v(\overline{x})_{nr}$ is unramified, it may be lifted to $[\rho_v(x)_{nr}] \in H^1_{nr}(F_v, G)$. Let $a(\rho_v(x)_{nr})$ be an n.i.b. generator of $F_{\rho_v(x)_{nr}}/F_v$. Then $\mathbf{r}_G(a(\rho_v(x)_{nr})) \cdot \mathbf{r}_G(\varphi_{v,s_1})$ is an n.i.b. generator of a tame Galois G-extension $F_{\rho_v(x)}$ of F_v such that $q_{2,v}([\rho_v(x)]) = \rho_v(\overline{x})$. By construction, we have that

$$\mathrm{Det}(\mathbf{r}_G(\varphi(\rho_v(x)))) = \mathrm{Det}(\mathbf{r}_G(\varphi_{v,s_1})) = \mathrm{Det}(\mathbf{r}_G(\varphi_{v,s})) = \mathrm{Det}(\mathbf{r}_G(\varphi(\pi_v(x)))),$$

as desired.

We now apply Proposition 10.3 to choose $\Pi(x) \in \mathrm{Hom}(\Omega_F, G)$ such that $\Pi(x)|_{I_v} = \rho_v(x)|_{I_v}$. If $a(\Pi_v(x))$ is any n.i.b. generator of $F_{\Pi_v(x)}/F_v$, with Stickelberger factorisation

$$\mathbf{r}_G(a(\Pi_v(x))) = u(\Pi_v(x)) \cdot \mathbf{r}_G(a_{nr}(\Pi_v(x))) \cdot \mathbf{r}_G(\varphi(\Pi_v(x))),$$

then

$$\mathrm{Det}(\mathbf{r}_G(\varphi(\Pi_v(x)))) = \mathrm{Det}(\mathbf{r}_G(\varphi(\pi_v(x)))).$$

Hence, for each v, it follows that $\lambda_v(x^{-1} \cdot \Psi_G([\Pi(x)]))$ is represented by

$$\mathrm{nrd}[u(\pi_v(x))^{-1}\mathbf{r}_G(a_{nr}(\pi_v(x)))^{-1}u(\Pi_v(x))\mathbf{r}_G(a_{nr}(\Pi_v(x)))] \in K_1(O_{F_v^c}G).$$

We deduce that $x^{-1} \cdot \Psi_G([\Pi(x)]))$ lies in the kernel of the map

$$\beta : K_0(O_F G, F^c) \xrightarrow{\lambda} J(K_0(O_F G, F^c) \to \frac{J(K_0(O_F G, F^c))}{\prod_v \mathrm{Im}(\Psi^{nr}_{G,v})},$$

(where the last arrow denotes the obvious quotient homomorphism). To conclude the proof, we appeal to the following result.

Proposition 11.1. *Let L be the maximal, abelian, extension of F of exponent $|G^{ab}|$, and suppose that $y \in K_0(O_F G, F^c)$ lies in the kernel of the map*

$$\beta : K_0(O_F G, F^c) \to \frac{J(K_0(O_F G, F^c))}{\prod_v \mathrm{Im}(\Psi^{nr}_{G,v})}.$$

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

$$e : K_0(O_F G, F^c) \to K_0(O_L G, F^c).$$

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

Proof. Suppose that $y = [(y_v), y_\infty]$ lies in the kernel of β. Then $y_v \cdot \mathrm{loc}_v(y_\infty) \in \mathrm{Im}(\Psi^{nr}_{G,v})$ for each v. Hence, for each v, $\mathrm{loc}_v(y_\infty)$ is an unramified G^{ab}-resolvend over F_v. This implies that y_∞ is a global unramified G^{ab}-resolvend over F, and so $y_\infty \in K_1(LG)$. Now since $y_v \cdot \mathrm{loc}_v(y_\infty) \in \mathrm{Im}(\Psi^{nr}_v)$ for each v, we see that in fact $y_v \cdot \mathrm{loc}_v(y_\infty) \in K_1(O_{L_v} G)$ for each v. Hence $e(y)$ is in the kernel of the localisation map

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

and since λ_L is injective (see Proposition 4.7) it follows that $e(y) = 0$. □

It follows from Proposition 11.1 that if $(h_F, |G^{ab}|) = 1$, then

$$x = \Psi_G(\Pi(x)),$$

and so x is globally cohomological as claimed. This completes the proof of Theorem 5.9.

References

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

[2] N. Byott, *Tame realisable classes over Hopf orders*, J. Algebra **201** (1998), 284–316.

[3] N. Byott, B. Sodaigui, *Realisable Galois module classes for tetrahedral extensions*, Compositio Mathematica **141** (2005), 573–582.

[4] N. Byott, C. Greither, B. Sodaigui, *Classes réalisables d'éxtensions non-abéliennes*, Crelle **601** (2006), 1–27.

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

[6] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Ergebnisse **3**, Springer, Berlin, 1983.

[7] A. Fröhlich, *Classgroups and Hermitian modules*, Birkhaüser, 1984.

[8] L. R. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra **82** (1983), 102–134.

[9] L. R. McCulloh, *Galois module structure of abelian extensions*, Crelle **375/376** (1987), 259–306.

[10] L. R. McCulloh, *Galois module to Steinitz classes*, Lecture in Oberwolfach, February 6, 2002. (arXiv preprint 1207.5702.)

[11] L. R. McCulloh, *On realisable classes for non-abelian extensions*, Lecture in Luminy, March 22, 2011.

[12] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers (third edition)*, Springer, Berlin, 2004.

[13] J.-P. Serre, *Topics in Galois theory*, Jones and Bartlett, 1992.

[14] J.-P. Serre, *Galois cohomology*, Springer, Berlin, 1997.

[15] I. Shafarevich, *Construction of fields of algebraic numbers with given soluble Galois group*, Izv. Akad. Nauk. SSR, Ser. Mat. **18** (1954), 525–578.

[16] A. Siviero, *Class invariants for tame Galois algebras*, PhD Thesis, Université de Bordeaux and Universiteit Leiden, (2013).

[17] R. Swan, *Algebraic K-theory*, SLNM 76, (1968).

[18] M. J. Taylor *Classgroups of Group Rings*, CUP 1984.

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